A reduction from Hawk to the principal ideal problem in a quaternion algebra

Clémence Chevignard[1], Pierre-Alain Fouque[1], Guilhem Mureau[2],
Alice Pellet-Mary[2], and Alexandre Wallet[3]

[1] Univ Rennes, Inria, CNRS, Irisa, UMR 6074, France
clemence.chevignard@inria.fr
pierre-alain.fouque@irisa.fr
[2] Univ Bordeaux, CNRS, Inria, Bordeaux INP, IMB, UMR 5251, Talence, France
guilhem.mureau@math.u-bordeaux.fr
alice.pellet-mary@math.u-bordeaux.fr
[3] PQ Shield Ltd., United Kingdom
alexandre.wallet@pqshield.com

Abstract. In this article we present a non-uniform reduction from rank-2 module-LIP over Complex Multiplication fields, to a variant of the Principal Ideal Problem, in some fitting quaternion algebra. This reduction is classical deterministic polynomial-time in the size of the inputs. The quaternion algebra in which we need to solve the variant of the principal ideal problem depends on the parameters of the module-LIP problem, but not on the problem's instance. Our reduction requires the knowledge of some special elements of this quaternion algebras, which is why it is non-uniform.
In some particular cases, these elements can be computed in polynomial time, making the reduction uniform. This is in particular the case for the Hawk signature scheme: we show that breaking Hawk is no harder than solving a variant of the principal ideal problem in a fixed quaternion algebra (and this reduction is uniform).

1 Introduction

Two lattices L, L' are isomorphic when there exists a linear isometry between them, and the Lattice Isomorphism Problem (LIP) asks to compute such an isometry. It has been studied in [14,23,33] as a standalone algorithmic problem, and these works achieved an algorithm with $n^{O(n)}$ time complexity for lattices of rank n. Stemming from this apparent hardness, LIP has recently been introduced as a security assumption to found cryptographic primitives in [1,3,13], joining other isomorphism-finding-based assumptions already in use in multivariate or code-based cryptography. Soon after, the signature scheme Hawk was presented [12], relying on a structured variant of LIP called module-LIP. In this variant, L and L' are now module lattices (a transition identical to that of LWE to module-LWE in more standard lattice-based cryptography) and an isometry compatible with the module structure must be found. This design leads to an eponymous submission[4]

[4] https://hawk-sign.info/

to the second call for post-quantum digital signatures organized by the NIST. The resulting scheme demonstrates efficiency and signature sizes comparable to Falcon and Dilithium, the two lattice-based signatures selected by NIST during the first call [31]. Owing to its recent cryptographic introduction, the cryptanalysis of module-LIP and thus of Hawk is however quite young, making it an attractive target for cryptanalysts.

In the simplest version of module-LIP [12], an attacker is given a (module-compatible) rotation of $\mathcal{O}_K^2$, where $\mathcal{O}_K$ is the ring of algebraic integers of a number field K, and is asked to recover the corresponding isometry. As there may be many more symmetries linked to the algebraic structure of K, it can be hoped that finding isometries of module lattices can be an easier task than for the plain case. At Eurocrypt 2024, Mureau et al. [29] focused on the case of *totally real*[5] number field and proposed a (heuristic) algorithm to solve module-LIP over such fields. In the special case of the module $\mathcal{O}_K^2$ and for some totally real number fields, this algorithm runs in polynomial time. On the one hand, this confirmed the intuition that module-LIP could be significantly easier than LIP (in our current state of knowledge). But, on the other hand, the current representative of module-LIP-based schemes, Hawk, is *not* designed over totally real fields. Instead, it is designed over the pervasive power-of-two cyclotomic fields, which are by nature totally imaginary. One notes that a cyclotomic field $K = \mathbb{Q}(\zeta)$ always comes with a totally real maximal subfield $F = \mathbb{Q}(\zeta + \zeta^{-1})$, but the authors of [29] could not use this to their advantage to extend their algorithm to Hawk's design. This work aims at narrowing this gap.

Contributions. Our main contribution is a reduction from the rank-2 version of module-LIP over complex multiplication number fields (or, CM-fields),[6] to the reduced-norm-Principal Ideal Problem (nrdPIP). This second problem consists in computing a generator of a principal ideal in a suitable (not necessarily commutative) extension of K, given a generator for its so-called reduced norm from the extension. Depending on the application context, our reduction has different precomputation and computation cost. A notable particular case, that includes Hawk's instances, is the following:

Theorem 1.1 (Informal, particular case). *Let K be a power-of-two cyclotomic field of degree $d \geq 32$ and let $G = V^*V \in \mathcal{O}_K^{2\times 2}$ with $V \in \mathbf{GL}_2(\mathcal{O}_K)$ a basis of $\mathcal{O}_K^2$. Given access to an oracle solving nrdPIP in polynomial time, module-LIP on input G (i.e., the task of computing all $U \in \mathbf{GL}_2(\mathcal{O}_K)$ such that $U^*U = G$) can be solved in time polynomial in d and in the size of its input, by making only one call to the oracle.*

The general reduction involves quaternion algebras and ideals. While being somewhat common objects in isogeny-based cryptography, such structures have

[5] Any number field comes with a set of embeddings into either $\mathbb{R}$ or $\mathbb{C}$. The field is said totally real (resp. totally imaginary) when all these embeddings map to $\mathbb{R}$ (resp. none of these embeddings maps to $\mathbb{R}$).

[6] A CM field K is a totally imaginary field which is a degree 2 extension of some totally real subfield F.

less exposure or involvement in lattice-based cryptography (they can be seen as a particular case of cyclic algebras, studied in a lattice context in e.g. [27]). In essence, we extend the reduction of Mureau et al. [29] to cover the case of *CM-fields*, which includes cyclotomic fields. Our reduction technique subsumes theirs, improving on their polynomial time algorithm to solve the problem over totally real fields, and additionally removing the need for a heuristic assumption.

We stress that, when the field where LIP needs to be solved is a cyclotomic field, there are *no known* polynomial time algorithm to solve the quaternionic version of the principal ideal problem with given reduced norm. In other words, this work *does not* break Hawk. The best algorithm we found to solve the nrdPIP instances generated by our reduction is due to Kirschmer and Voight [26, Alg. 6.3]. It runs in polynomial time[7] except for one call to an SVP instance in a lattice of dimension $2d$, where d is the degree of K (see Lemma 2.28 for details). This proves in particular that a single call to an SVP solver in dimension $2d$ is sufficient to break Hawk (a fact that seemed folklore so far, but was never proven anywhere to the best of our knowledge). In the original Hawk article [12], the authors explain in Section 4.2 that the best algorithms solving (module-)LIP require *at least* one SVP call, so to be conservative they "assume that the best key recovery attack requires one to find a single shortest vector". Our result shows that this assumption is tight: one SVP call is indeed enough for a key recovery attack.

While our reduction provides an easy way to prove this fact about Hawk, it is probably an overkill: the underlying module is free, has rank two and its shortest vectors are orthogonal. There are probably more straightforward ways to show that a single SVP call in a large lattice is enough. For *general rank* 2 modules over a CM-field K, this does not seem to be the case anymore, and the arithmetic now plays a more cumbersome role through the fractional ideals appearing in pseudo-bases. Our reduction covers this case as well, and reduces the module-LIP problem in any *rank-2* module of K^2 to a single instance of the shortest vector problem in an *ideal* lattice of a non-commutative ring (via the nrdPIP problem). Any improvement for solving the nrdPIP problem (or SVP in ideals of quaternion algebras) would directly impact the hardness of rank-two module-LIP and thus, the security of Hawk.

Finally we mention here that the ideas of this work can be adapted to the totally real regime too, by replacing the quaternionic extension of F with a CM-extension $K = F(i)$. This improves the result of Mureau et al. [29], by removing the heuristic argument of their work and providing a polynomial time algorithm for all modules of rank 2 included in K^2 (whereas the reduction of [29] was polynomial time only for some rank-2 modules). We delay the technical details of this adaptation to a longer journal version combining both results.

Technical overview. Let us recall the main idea of Mureau et al., as it provides enough background to understand our ideas. Computing isomorphisms of lattices

[7] Because we provide the reduced norm of a generator, the expensive computation of the field infrastructure can be avoided.

is equivalently formulated as finding integral equivalence of quadratic forms: one is given $Q = B^T B$ with a public lattice basis B and $Q' := B'^T B' = U^T Q U$ with a secret basis $B' = BU$ and a secret unimodular matrix $U \in \mathbf{GL}_n(\mathcal{O}_K)$. The goal is to recover U (or equivalently B'). Let us consider the simpler case where $B = Q = I_2$, the identity matrix, which is Hawk's setting (and conveys enough intuition for this overview). In this case, the first observation of [29] was that, when the underlying field K is totally real, the diagonal entries of Q' are of the form $q = x^2 + y^2$, where $(x, y) \in \mathcal{O}_F^2$ are the columns of B'. In other words, they are sums of two squares. Following Dedekind's work on the famous theorem of Fermat, it is equivalently written as $q = (x + iy)(x - iy) =: \mathrm{nrd}(x + iy)$, seeing now $x + iy$ as an element in the extension $K(i)$ for $i^2 = -1$.[8] Over integers the situation is well-understood thanks to the set of Gaussian integers $\mathbb{Z}[i]$. Over algebraic integers, one can restate the problem as finding the correct generator $x + iy$ of a principal ideal in $K(i)$, given a description of this ideal and its relative norm q in F. Finding the candidate principal ideal requires factoring a large number (see also Howgrave-Graham-Szydlo's algorithm [24]). To maintain a polynomial time reduction, Mureau et al. randomize the instances to get a power of a prime instead — this is where they need a heuristic assumption about the success rate of this procedure. If $K(i)$ is in fact a cyclotomic field,[9] the algorithm of Gentry-Szydlo [20] then finds the needed generator in polynomial time.

Now let us assume that the field K where LIP needs to be solved is a power-of-two cyclotomic field, with maximal totally real field F. In this case we have $Q = B^* B$, where B^* is the transpose-conjugate of B. The diagonal entries of Q are of the form $q = x\bar{x} + y\bar{y} \in F$, where $\bar{\cdot}$ stands for the complex conjugation. Going down to F, actually these entries are now sums of four squares in $\frac{1}{2}\mathcal{O}_F$ as $q = a^2 + b^2 + c^2 + d^2$ if $x = a + ib$ and $y = c + id$.[10] We are led to a generalization of Lagrange's famous theorem, which admits an algebraic-geometric proof using *quaternion* arithmetic. This proof can be turned into an algorithm, illustrated by the work of Rabin and Shallit [34] to find such four-squares decomposition, but just as above, we need here an extension to algebraic numbers. Let us set $\mathcal{A} := F\langle i, j\rangle$ with $j^2 = -1$ and such that $ij = -ij$, so that we have an extension of F-algebras $\mathcal{A}/K/F$. The non-commutative algebra $\mathcal{A}$ is known as a quaternion algebra over F, and comes with a reduced norm $\mathrm{nrd}(a + ib + jc + ijd) := a^2 + b^2 + c^2 + d^2 = q$. The technical part here is then to elucidate the quaternionic version of the reduction of Mureau et al., as subtleties arise from the non-commutative setting. In the end, there are currently no known polynomial-time algorithms to solve nrdPIP over quaternion algebras, so we rely on a oracle to complete the reduction in this setting.

[8] Here, we use the notation nrd to refer to the relative norm of the extension $K(i)/K$, this is by analogy with the quaternion algebra case that will be discussed below.

[9] A larger class of fields is reached using Lenstra and Silverberg's algorithm [25]

[10] Note that even if x and y are in $\mathcal{O}_K$, then a,b,c and d are only guaranteed to be in $\frac{1}{2}\mathcal{O}_F$ (the inclusion can be seen by observing that $2a = x + \bar{x} \in \mathcal{O}_K \cap F = \mathcal{O}_F$).

We observe additionally that the work of [29] did not use all the public information given by the public form Q. As our reductions are similar whether the "highest" considered extension of F is $\mathcal{A}$ or K, let us write temporarily E for either of these for the sake of simplicity. From our description above, one realises that they have not used the anti-diagonal entries, although these entries also gives constraints on the set of solutions to compute. Our formulation naturally involves these terms as well, and we show that from all the public data[11] one can obtain a fraction $\alpha\beta^{-1}$ of E, whose numerator and denominator encode the secret columns of B' — a flavor similar to the NTRU setting where $h = f/g \bmod q$ and (f, g) is the first column of a secret basis. With some ideal arithmetic, we are then able to build a principal ideal $\alpha\mathcal{O}$, for a maximal order $\mathcal{O}$ in E. The nrdPIP oracle gives us a candidate for α, that is, up to an element of $\mathcal{O}^1$, the group of elements of reduced norm 1. When K is already totally real (i.e., when we are in the context of [29]), Lenstra-Silverberg's algorithm computes such an α in polynomial time. Then, we show that it allows to efficiently build all possible lattice isomorphims. By using quaternion algebras of more general forms than the one behind Lagrange's theorem, we can also extend our reduction to all CM extensions K/F.

The general case of the module-LIP problem covers rank 2 modules over a field K, which are known to not all be of the form $\mathcal{O}_K^2$: such objects admits so-called pseudo-bases, involving fractional ideals in K. As ideals in K do not commute anymore when extended to an ambient quaternion algebra, tailoring the reduction to this broader context adds a thin layer of technicalities. We borrow and extend some tools introduced in [29] to general CM extensions, in order to handle any rank 2 modules with minimal hassle. We note that one of these tools, the Gram ideal, was involved in the complexity of the algorithm in [29] as its algebraic norm needed to be factored. Our reduction strategy bypasses this annoyance, making the resulting complexity independent of (the time to factor) the Gram ideal. Interestingly, we also do not need to rely on a heuristic assumption anymore: this makes our new reduction rigorously proven, and removes the need for one in [29]. On top of simplifying the resulting algorithm compared to [29], an additional benefit is also to reduce the amounts of nrdPIP instance to be solved to a single one. Since this is by far the most computationally expensive task of their work, this should significantly improve the practical runtime.

Computationally, ideals in quaternionic algebras over F or in a quadratic extension K can also be seen as $\mathcal{O}_F$-modules of rank 2 or 4, which is enough for our purpose. In particular, there are known polynomial-time algorithms to handle their arithmetic and representations [8, Chap. 2]. As explained we need at some point the group $\mathcal{O}^1$ of elements of reduced norm 1 in a maximal order $\mathcal{O}$ of the considered extension of F. In the number field case, there is a unique maximal order, and this amounts to finding the roots of unity in the field, which

[11] More precisely, the determinant of B' must also be known, at least up to a root of unity in K. We give a polynomial-time algorithm to compute it from $\det Q'$ and $\det B$.

is a computationally easy task. For quaternion algebras, the situation is more dire: there are several maximal orders, which are not trivially related to one another. In other words, knowing $\mathcal{O}^1$ does not mean we know another $\tilde{O}^1$. At last, the order $\mathcal{O}$ involved in our work can be computed from the parameters of the module-LIP problem in polynomial time. Thus for $E = \mathcal{A}$, we assume that this $\mathcal{O}^1$ has been precomputed, or given as additional input. We also note that in our context, such groups are always *finite*, and belongs to a small, *explicit* list of groups of small cardinalities (at most polynomial in the degree of F) [39, Chap. 32].

Related works. The Principal Ideal Problem over number field (say, F-PIP) has been coined as a central problem in algorithmic number theory (e.g. [7]). One could hope that only deciding principality is easier, but it turns out that all known algorithms that test for principality try to compute a generator. In an arbitrary number field, the state-of-the-art classical algorithms are heuristic and run in subexponential time [6,4] or quantum polynomial time [5]. We note that all these algorithms reduce to the problem of computing the unit group and the class group of the underlying field. In lattice-based cryptography, F-PIP appeared in important results [9,10] on the hardness of the Ideal-SVP problem. Over quaternion algebras, say $\mathcal{A}$-PIP, the situation can roughly be separated into the *totally definite* case and the *indefinite* case. In the former, an algorithm to compute a generator of a principal ideal $I \subset \mathcal{A}$ is provided in [26, Alg. 6.3], reducing to the computation of the class group of F and to a short vector computation in a rank-$4d$ $\mathbb{Z}$-lattice. While computing the class group may be done in quantum polynomial time, computing short vectors in lattices is believed to be hard even for quantum computers. In indefinite algebras, the situation is even less favorable; Page presents a heuristic exponential time algorithm in [32].

With the additional information of the reduced norm of a generator of a principal ideal (say, F-nrdPIP), the situation changes drastically and (classical) polynomial time complexity can be achieved for CM extensions. For cyclotomic fields, this observation goes back to Gentry and Szydlo's algorithm [21] to attack NTRU encryption. Variants of this algorithm [24,19,15,17] were subsequently used to attack lattice-based signatures in several context, and a more general version was described by Lenstra and Silverberg [25], covering in particular all CM fields. On the other hand, for the quaternion variant $\mathcal{A}$-nrdPIP, there are (to our knowledge) no known polynomial time algorithms, and thus the problem is solved by using a $\mathcal{A}$-PIP solver instead.

Regarding the computation of the group $\mathcal{O}^1$ for an order $\mathcal{O}$ in a totally definite quaternion algebra, there is no specific algorithm presented in the litterature.[12] In the commutative setting and with the maximal order $\mathcal{O} = \mathcal{O}_F$ of a number field F, computing $\mathcal{O}^1$ reduces to finding the roots of unity in F. This task can be achieved in classical polynomial time. For a quaternion algebra which splits at exactly one real place (this algebra is not totally definite) the group $\mathcal{O}^1$ is not

[12] By computation we mean an abstract finite presentation of a group G, together with an isomorphism $G \simeq \mathcal{O}^1$.

finite but Voight gave an algorithm to compute a minimal presentation of it, see [37]. All we can say in the totally definite case is that $\mathcal{O}^1$ falls into some known lists of finite groups.

In a concurrent work [16], Espitau and Pliatsok proved a reduction from module-LIP over CM fields for certain rank-2 modules[13] to the shortest vector problem in rank-2 modules with additional symmetries. These rank-2 modules with symmetries are closely related the ideal in $\mathcal{A}$ that is produced by our reduction. We let a more detailed comparison of the two approaches open for the moment.

Organisation of the paper. In section 2, we present the necessary algebraic structures for this work. We recall the worst-case search module Lattice Isomorphism Problem (wc-smodLIP) in rank 2, and define the reduced norm Principal Ideal Problem (nrdPIP). We discuss the representation and concrete handling of every object we manipulate in our reduction. In section 3, we prove our main reduction from rank-2 module-LIP in CM fields to nrdPIP in a well-chosen maximal order of a quaternion algebra. The proofs of some technical results from preliminaries are delayed to the appendices.

Acknowledgement. We are grateful to John Voight for helpful discussions but also for his great book on quaternion algebras, from which we learnt most of the material on this topic. We thank Alice Silverberg and Hendrik Lenstra for inspiring exchanges. Our thanks also go to Aurel Page and Renaud Coulangeon for many discussions and suggestions. Finally, we are grateful to Thomas Espitau and Heorhii Pliatsok for sharing their approach of the result, which is somehow complementary to ours.

Alice Pellet-Mary was supported by the CHARM ANR-NSF grant (ANR-21-CE94-0003) and the TOTORO ANR (ANR-23-CE48-0002). All the authors were supported by the France 2030 program, managed by the French National Research Agency under grant agreement No. ANR-22-PETQ-0008 PQ-TLS.

2 Preliminaries

For a ring R, we denote $R^\times$ its set of invertible elements (that is, whose inverse are in R). The set of invertible $n \times n$ matrices with entries in R is denoted $\mathbf{GL}_n(R)$. The set of squares in R is $R^{(2)}$. We use bold letters to denote vectors.

2.1 Number Fields

Generalities on number fields. A number field K is a finite extension of the field of rational numbers $\mathbb{Q}$. It is isomorphic to $\mathbb{Q}[X]/P(X)$, where $P(X)$ is an

[13] Their reduction is restricted to rank-2 modules with relative Gram ideal equal to $\mathcal{O}_K$ (see Definition 2.3 for the definition of the relative Gram ideal of a module).

irreducible monic polynomial of $\mathbb{Q}[X]$. The degree $d := [K : \mathbb{Q}]$ of K over $\mathbb{Q}$ is exactly the degree of $P(X)$. A number field K of degree d has d embeddings $K \to \mathbb{C}$, sending the class of X to a complex root of P. Any embedding $\sigma_i : K \to \mathbb{R}$ is called a real embedding. An embedding σ_i which is not real is called complex, and it can be composed with complex conjugation in $\mathbb{C}$ to obtain a different complex embedding $\overline{\sigma_i}$. The canonical embedding of K is defined as

$$\sigma(e) := (\sigma_1(e), \ldots, \sigma_d(e)) \in \mathbb{C}^d, \quad \forall e \in K$$

where the σ_i are all the embeddings of K. When all the embedding of $K \to \mathbb{C}$ are actually real embeddings, we say that K is *totally real*. When none of them are, we say that K is *totally imaginary*. An element $a \in K$ is totally positive, resp. totally negative, if all its embeddings are positive, resp. negative real numbers (in particular, all its embeddings are real numbers). The (absolute) trace and norm of $e \in K$ are $\mathrm{Tr}(e) = \sum_i \sigma_i(e)$ and $N(e) = \prod_i \sigma_i(e) \in \mathbb{Q}$.

We note $\mathcal{O}_K$ the ring of integers of a number field K. It is defined as the ring containing all elements $e \in K$ such that there exists a monic polynomial $Q(X) \in \mathbb{Z}[X]$ such that $Q(e) = 0$. It is a free $\mathbb{Z}$-module of rank d. The (absolute) discriminant of K is $\Delta_K = |\det([\mathrm{Tr}(\beta_i\beta_j)]_{i,j})|$, for any $\mathbb{Z}$-basis $(\beta_i)_i$ of $\mathcal{O}_K$. We also note $\mu(K)$ the set of roots of unity of K, which is of size $\leqslant 2d^2$ (see, e.g., [29, Corollary 2.11]).

CM fields. A Complex Multiplication (CM) number field K is a totally imaginary quadratic extension of a totally real number field F (we also say K/F is a CM-extension). Equivalently, here F is a totally real number field and there exists a totally negative element $a \in F$ such that $K = F(\sqrt{a})$ [40, Page 38]. From now on, K/F will denote a CM extension. A fundamental example of CM fields for cryptographic applications are cyclotomic fields. Let $m \in \mathbb{N}_{>2}$ and ζ_m be a primitive m-th root of unity. Then, $K_m = \mathbb{Q}(\zeta_m)$ is a totally complex number field of degree $d = \varphi(m)$ containing the totally real field $F_m = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ and K/F is quadratic.[14] In full generality we have $K_m = F_m(\sqrt{a_m})$ where $a_m = (\zeta_m - \zeta_m^{-1})^2 = \zeta_m^2 + \zeta_m^{-2} - 2 \in F_m$. In the case where m is divisible by 4, the element $i = \zeta_m^{m/4}$ is a square root of -1, thus $i \in K_m \setminus F_m$ and we can write $K_m = F_m(\sqrt{-1})$. In a CM-extension K/F, there is a unique non-trivial automorphism of K fixing F pointwise, which is called complex conjugation. With the notation $K = F(\sqrt{a})$, it acts on K by $\tau : \sqrt{a} \mapsto -\sqrt{a}$. In particular, the relative norm of the extension K/F is defined by $N_{K/F}(x + y\sqrt{a}) := (x + y\sqrt{a})\tau(x + y\sqrt{a}) = (x + y\sqrt{a})(x - y\sqrt{a}) = x^2 - ay^2$, for all $x + y\sqrt{a} \in K$. The following lemma justifies why the automorphism τ is also called complex conjugation.

Lemma 2.1 ([29, Lemma 2.7]). *Let K/F be a CM extension of number fields. For any embedding $\sigma_i : K \to \mathbb{C}$ and $x \in K$, we have $\overline{\sigma_i(x)} = \sigma_i(\tau(x))$.*

[14] Since $\zeta_m \notin F_m$ we have $[K_m : F_m] > 1$ and one can check that ζ_m is a root of $\Psi_m(X) = X^2 - (\zeta_m + \zeta_m^{-1})X + 1 \in F_m[X]$, so $[K_m : F_m] \leq 2$.

In the rest of this article, to simplify notations, we will write $\bar{x}$ instead of $\tau(x)$. For $\ell \in \mathbb{N}_{>0}$ we equip K^ℓ with the form $\langle \mathbf{v}, \mathbf{v} \rangle_K := \sum_i v_i \overline{w_i} \in K$, where $\mathbf{v} = (v_i)_i, \mathbf{w} = (w_i)_i \in K^\ell$. The scalar square of $\mathbf{v}$ is $\langle \mathbf{v}, \mathbf{v} \rangle_K$. It defines an element of F.

Ideals. An integral ideal $\mathfrak{a}$ of K is an additive subgroup of $\mathcal{O}_K$, such that $\forall x \in K, x\mathfrak{a} \subseteq \mathfrak{a}$. A fractional ideal $\mathfrak{a}$ of K is an additive subgroup of K such that there exists $x \in K \setminus \{0\}$ such that $x\mathfrak{a}$ is an integral ideal. If $\mathfrak{a}$ is generated by a single element x, it is said to be *principal*, and is noted $\mathfrak{a} = x\mathcal{O}_K$. We will use fraktur-letters to denote fractional ideals of K or F.

The product of two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ is the smallest ideal containing all products xy for $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$, and is denoted by $\mathfrak{a}\mathfrak{b}$. Given two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$, we have that $\mathfrak{a} \subseteq \mathfrak{b}$ if and only if there exists an integral ideal $\mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. When this is the case, we say that $\mathfrak{c}$ divides $\mathfrak{a}$. An integral ideal $\mathfrak{p}$ is prime whenever $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Prime ideals are the maximal ideals in $\mathcal{O}_K$. When dealing with number fields, we have unique factorization of integral ideals into prime ideals (up to permutation of the factors). More precisely, given a prime integer $p \in \mathbb{Z}$, the ideal $p \cdot \mathcal{O}_K$ is a product $\prod_i \mathfrak{p}_i^{e_i}$ of at most $[K : \mathbb{Q}]$ prime ideals ([30, Chapter I, Proposition 8.3]). Moreover this factorization can be computed in polynomial time.

Lemma 2.2 ([8, Section 6.2.5]). *There exists a polynomial time algorithm that takes as input any prime integer $p \in \mathbb{Z}$ and a basis of the ring of integers $\mathcal{O}_K$ of a number field K, and computes all the prime ideals of $\mathcal{O}_K$ dividing $p \cdot \mathcal{O}_K$.*

When K/F is a CM extension and $\mathfrak{a}$ is a fractional ideal of K, the set $\overline{\mathfrak{a}} := \{\overline{x} \,|\, x \in \mathfrak{a}\}$ is again a fractional ideal of K, called the conjugate of $\mathfrak{a}$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$. Recall from [30, Chapter I, (8.3) & (9.1)] that $\mathfrak{p}\mathcal{O}_K$ factorizes in $\mathcal{O}_K$ either as

$$\mathfrak{p}\mathcal{O}_K = \begin{cases} \mathfrak{q}\overline{\mathfrak{q}} \text{ with } \mathfrak{q} \neq \overline{\mathfrak{q}} \text{ prime ideals (split case)} \\ \mathfrak{q}^2 \text{ with } \mathfrak{q} = \overline{\mathfrak{q}} \text{ prime ideal (ramified case)} \\ \mathfrak{q} \quad \text{with } \mathfrak{q} = \overline{\mathfrak{q}} \text{ prime ideal (inert case).} \end{cases} \tag{1}$$

In the split and ramified cases, we have $\mathfrak{q}\overline{\mathfrak{q}} \cap F = \mathfrak{p}\mathcal{O}_K \cap \mathcal{O}_F = \mathfrak{p}$ ([28, Chapter 3, Exercise 9 (c)]). For the inert case, $\mathfrak{q}\overline{\mathfrak{q}} \cap F = \mathfrak{p}^2\mathcal{O}_K \cap \mathcal{O}_F = \mathfrak{p}^2$. The relative norm of a prime ideal $\mathfrak{q} \subset \mathcal{O}_K$ is then defined as $N_{K/F}(\mathfrak{q}) = \mathfrak{q}\overline{\mathfrak{q}} \cap F$. Thanks to the previous observation, this definition coincides with the one given in [30, Chapter III, §1]. The relative norm is then extended multiplicatively to the set of fractional ideals of K. In particular it is multiplicative *i.e.,* $N_{K/F}(\mathfrak{a}\mathfrak{b}) = N_{K/F}(\mathfrak{a})N_{K/F}(\mathfrak{b})$ holds. In fact $N_{K/F}(\mathfrak{a})$ is also equal to the ideal of F generated by $\{N_{K/F}(x) \,|\, x \in \mathfrak{a}\}$, see [30, Chapter III, (1.6)]. For a principal ideal $\mathfrak{a} = g \cdot \mathcal{O}_K$, we have $N_{K/F}(\mathfrak{a}) = N_{K/F}(g) \cdot \mathcal{O}_F$. Finally we define the relative trace of a fractional ideal $\mathfrak{a} \subset K$ by $\mathrm{Tr}_{K/F}(\mathfrak{a}) := (\mathfrak{a} + \overline{\mathfrak{a}}) \cap F$.

Modules. The main reference for this paragraph is the first chapter from [8]. Let V be a finite-dimensional vector space over a number field K. We call module (in V) any set of the form $\mathfrak{a}_1\mathbf{b}_1+\cdots+\mathfrak{a}_\ell\mathbf{b}_\ell$, where the $\mathfrak{a}_i$'s are fractional ideals in K and the $\mathbf{b}_i$'s are K-linearly independent.[15] The data of $((\mathbf{b}_1,\mathfrak{a}_1),\ldots,(\mathbf{b}_\ell,\mathfrak{a}_\ell))$ is called a pseudo-basis of M and the integer ℓ is called the rank of the module. We write $\mathbf{B}=(B,\{\mathfrak{a}_i\}_{i\leq\ell})$ where B is the (column) matrix of the $\mathbf{b}_i$'s, and we call it a pseudo-basis of the module. We use bold capital letters to denote pseudo-bases. In this article we always consider modules with full rank, and let $\dim_K(V)=\ell$. A module $M\subset K^\ell$ (resp. $\mathcal{O}_K^\ell$) is said to be rational (resp. integer).

Two pseudo-bases $\mathbf{B}=(B,\{\mathfrak{a}_i\}_{1\leq i\leq\ell})$ and $\mathbf{B}'=(B',\{\mathfrak{b}_i\}_{1\leq i\leq\ell})$ generate the same module if and only if there exists $U=(u_{i,j})_{1\leq i,j\leq\ell}\in\mathbf{GL}_\ell(K)$ such that $B'=BU$ and $u_{i,j}\in\mathfrak{a}_i\mathfrak{b}_j^{-1}$ for all $1\leq i,j\leq\ell$ and $\mathfrak{a}_1\cdots\mathfrak{a}_\ell=(\det U)\mathfrak{b}_1\cdots\mathfrak{b}_\ell$ ([8, Proposition 1.4.2]). Finally, for any module M and a non-zero fractional ideal $\mathfrak{m}\subset K$, we define $\mathfrak{m}\cdot M$ to be the smallest module containing $e_m\cdot\mathbf{v}$ for all $(e_m,\mathbf{v})\in\mathfrak{m}\times M$. If $\mathbf{B}=(B,\{\mathfrak{a}_i\}_{1\leq i\leq\ell})$ is a pseudo-basis of M, then $\mathfrak{m}\cdot\mathbf{B}:=(B,\{\mathfrak{m}\cdot\mathfrak{a}_i\}_{1\leq i\leq\ell})$ is a pseudo-basis of $\mathfrak{m}\cdot M$.

When K is a CM-field, the pseudo-Gram matrix associated to a pseudo-basis $\mathbf{B}=(B,\{\mathfrak{a}_i\}_{i\leq\ell})$ is $\mathbf{G}=(B^*B,\{\mathfrak{a}_i\}_{i\leq\ell})$, where $B^*=\overline{B}^t$ is the conjugate-transpose matrix (where the complex conjugation of K is taken on each matrix coefficient).[16]In the following we define three ideals attached to a module over a CM field. This is an extension of [29, Definition 4.1], which was defined only for modules over totally real number fields.

Definition 2.3 (Extension of [29, Definition 4.1]). *Let K/F be a CM extension and $M\subset K^\ell$ be a module with pseudo-basis $\mathbf{B}=((b_{i,j})_{i,j},\{\mathfrak{a}_i\}_i)$ and associated pseudo-Gram matrix $\mathbf{G}=((g_{i,j})_{i,j},\{\mathfrak{a}_i\}_i)$. We define the following fractional ideals*

$$\mathcal{G}(M):=\sum_{1\leq i\leq\ell}g_{i,i}\cdot N_{K/F}(\mathfrak{a}_i)\ +\sum_{1\leq i<j\leq\ell}\mathrm{Tr}_{K/F}(g_{i,j}\cdot\mathfrak{a}_i\overline{\mathfrak{a}_j})$$

$$\mathcal{C}(M):=\sum_{1\leq i,j\leq\ell}b_{i,j}\cdot\mathfrak{a}_j\quad;\quad\mathcal{RG}(M):=\mathcal{G}(M)\cdot N_{K/F}(\mathcal{C}(M))^{-1}.$$

$\mathcal{C}(M)$ is a fractional ideal of K called the coefficient ideal of M, while the Gram ideal $\mathcal{G}(M)$ and the relative Gram ideal $\mathcal{RG}(M)$ are both fractional ideals of F.

As in [29, Lemma 4.2], we prove that these ideals depend only on M, and not on the choice of a pseudo-basis for M.

Lemma 2.4 (Extension of [29, Lemma 4.2]). *Let K/F be a CM extension and $M\subset K^\ell$ a module with pseudo-basis $\mathbf{B}$ and associated pseudo-Gram matrix*

[15] In full generality, these should be called finitely generated, torsion-free $\mathcal{O}_K$-modules in V. Since we will only consider these kind of modules, we drop the "finitely generated, torsion free" part, to make it easier to read.

[16] The pseudo-Gram matrix can be more generally defined for any number field [29, Definition 3.6], but in this work we will only be interested in CM-field.

$\mathbf{G}$. *Then $\mathcal{G}(M)$ is the smallest ideal of F containing the set $\{\langle \mathbf{v}, \mathbf{v}\rangle_K \mid \mathbf{v} \in M\}$, and $\mathcal{C}(M)$ is the smallest ideal of K containing the set $\{v_j \mid \mathbf{v} = (v_i)_i \in M,\ 1 \leq j \leq \ell\}$. In particular, they do not depend on the choice of a pseudo-basis of M.*

Proof. The proof is similar to the one of Lemma [29, Lemma 4.2] over totally real fields, but now we have to take care about the complex conjugation. The property on $\mathcal{C}(M)$ follows from its definition. Any module vector can be uniquely written $\mathbf{v} = \sum_i x_i \cdot \mathbf{b}_i$, where $x_i \in \mathfrak{a}_i$ and $\mathbf{b}_i$ is the i-th column of B (with $\mathbf{B} = (B, \{\mathfrak{a}_i\}_i)$). Let us denote $\mathbf{G} = ((g_{i,j})_{i,j}, \{\mathfrak{a}_i\})$ and notice that $g_{j,i} = \overline{g_{i,j}}$, since $G^* = G$. Then,

$$\begin{aligned}\langle \mathbf{v}, \mathbf{v}\rangle_K &= \sum_{1\leq i\leq \ell} g_{i,i} x_i \overline{x_i} + \sum_{1\leq i<j\leq \ell} (g_{i,j} x_i \overline{x_j} + g_{j,i} \overline{x_i} x_j) \\ &= \sum_{1\leq i\leq \ell} g_{i,i} N_{K/F}(x_i) + \sum_{1\leq i<j\leq \ell} \mathrm{Tr}_{K/F}(g_{i,j} x_i \overline{x_j}) \in \mathcal{G}(M),\end{aligned}$$

Conversely, let $\mathfrak{g}$ be a fractional ideal of F containing the scalar squares $\langle \mathbf{v}, \mathbf{v}\rangle_K$ for all $\mathbf{v} \in M$. Then $\mathfrak{g}$ contains $\langle x_i \mathbf{b}_i, x_i \mathbf{b}_i\rangle_K = g_{i,i} N_{K/F}(x_i)$ for all $x_i \in \mathfrak{a}_i, i \leq \ell$, hence it contains $g_{i,i} \cdot N_{K/F}(\mathfrak{a}_i)$ for all $i \leq \ell$. Since $\mathfrak{g}$ is an ideal, it must also contain $\langle x_i \mathbf{b}_i + x_j \mathbf{b}_j, x_i \mathbf{b}_i + x_j \mathbf{b}_j\rangle - \langle x_i \mathbf{b}_i, x_i \mathbf{b}_i\rangle - \langle x_j \mathbf{b}_j, x_j \mathbf{b}_j\rangle = g_{i,j} x_i \overline{x_j} + g_{i,j} x_j \overline{x_i} = \mathrm{Tr}_{K/F}(g_{i,j} x_i \overline{x_j})$ for all $x_i \in \mathfrak{a}_i$, $x_j \in \mathfrak{a}_j$. Hence $\mathfrak{g}$ contains the ideals $\mathrm{Tr}_{K/F}(g_{i,j} \mathfrak{a}_i \overline{\mathfrak{a}_j})$ for all $1 \leq i, j \leq \ell$. Therefore, $\mathfrak{g}$ contains $\mathcal{G}(M)$. □

Thanks to the coefficient ideal, and up to multiplication by its inverse, we may always assume that a rational module is integer.

Lemma 2.5 (Extension of [29, Lemma 4.4]). *Let K/F be a CM extension, $\mathfrak{c}$ be a fractional ideal of K and $M \subset K^\ell$ a module. Then,*

1. *$\mathcal{G}(\mathfrak{c} \cdot M) = N_{K/F}(\mathfrak{c}) \cdot \mathcal{G}(M)$;*
2. *$\mathcal{C}(\mathfrak{c} \cdot M) = \mathfrak{c} \cdot \mathcal{C}(M)$;*
3. *$\mathcal{RG}(\mathfrak{c} \cdot M) = \mathcal{RG}(M)$;*
4. *$\mathcal{C}(M)^{-1} \cdot M \subset \mathcal{O}_K^\ell$ is an integer module.*

Proof. The proof of *2.* and *4.* are exactly the same as in [29, Lemma 4.4]. Notice that *1.* implies *3.*, by multiplicativity of the relative norm for ideals. By Lemma 2.4, $\mathcal{G}(\mathfrak{c} \cdot M)$ is the fractional ideal of F generated by the scalar squares $\langle x \cdot \mathbf{v}, x \cdot \mathbf{v}\rangle_K = N_{K/F}(x) \cdot \langle \mathbf{v}, \mathbf{v}\rangle$ for all $x \in \mathfrak{c}$ and $\mathbf{v} \in M$. This proves the inclusion $\mathcal{G}(\mathfrak{c} \cdot M) \subset N_{K/F}(\mathfrak{c}) \cdot \mathcal{G}(M)$. Conversely, let $x \in N_{K/F}(\mathfrak{c}) \cdot \mathcal{G}(M)$. By definition of the product of two ideals, x can be expressed as a finite sum $x = \sum_i n_i g_i$, where $n_i \in N_{K/F}(\mathfrak{c})$ and $g_i \in \mathcal{G}(M)$. Since $N_{K/F}(\mathfrak{c})$ coincides with the ideal generated by $\{N_{K/F}(c)\}_{c\in\mathfrak{c}}$, one can write finite sums $n_i = \sum_j c_{i,j} \overline{c_{i,j}}$ with $c_{i,j} \in \mathfrak{c}$ and for all i. In the same way, $g_i = \sum_k \langle \mathbf{v}_{i,k}, \mathbf{v}_{i,k}\rangle_K$ where $\mathbf{v}_{i,k} \in M$. Finally, $x = \sum_{i,j,k} c_{i,j} \overline{c_{i,j}} \langle \mathbf{v}_{i,k}, \mathbf{v}_{i,k}\rangle_K$ is a finite sum of elements in $\mathcal{G}(\mathfrak{c} \cdot M)$, so this proves $x \in \mathcal{G}(\mathfrak{c} \cdot M)$ and the other inclusion. □

Again, the proof of Lemma 2.5 goes as the proof of Lemma [29, Lemma 4.4]. A consequence of this Lemma is that the coefficient ideal of $\mathcal{C}(M)^{-1} \cdot M \subset \mathcal{O}_K^\ell$ is $\mathcal{O}_K$.

2.2 Quaternion algebras

We now give the background on quaternion algebras that is needed in this work. A general reference for this topic is [39], from which we borrow most of the material. For a field F, a F-algebra is a F-linear space which is also a ring (its elements can be multiplied together into another ring element). In this work, we are interested in one type of quaternion algebra, defined below. From now on, F is a totally real field, a is a totally negative element in F, so that $K = F(\sqrt{a})$ is a CM-extension.

Definition 2.6. *The quaternion algebra* $\mathcal{A} := (\frac{a,-1}{F})$ *is the* F*-algebra of dimension 4 with basis* $\{1, i, j, ij\}$ *and satisfying the rules*

$$i^2 = a \quad ; \quad j^2 = -1 \quad ; \quad ij = -ji.$$

Because of the rule $ij = -ji$, $\mathcal{A}$ is a non commutative algebra. Its center (the set of elements that commute with every other) is equal to F. A quaternion algebra is also equipped with an involution $\overline{\cdot}$ defined by $\overline{x + iy + jz + ijt} = x - iy - jz - ijt$. This map is F-linear and satisfies $\overline{\overline{\alpha}} = \alpha$ and $\overline{\alpha\beta} = \overline{\beta} \cdot \overline{\alpha}$ for any $\alpha, \beta \in \mathcal{A}$ (see [39, Section 3.2]). The reduced norm on $\mathcal{A}$ is the map $\mathrm{nrd} : \mathcal{A} \to F$ defined by $\alpha = x + iy + jz + ijt \mapsto \alpha\overline{\alpha} = x^2 - ay^2 + z^2 - at^2$. We have $\mathrm{nrd}(\alpha\beta) = \mathrm{nrd}(\alpha)\mathrm{nrd}(\beta)$ for all $\alpha, \beta \in \mathcal{A}$ [39, Par. 3.3.4].

Example 2.7. Consider the quaternion algebra $(\frac{-1,-1}{\mathbb{Q}})$. The standard involution acts as $\overline{x + iy + jz + ijt} = x - iy - jz - ijt$ and the reduced norm is given by $\mathrm{nrd}(x + iy + jz + ijt) = x^2 + y^2 + z^2 + t^2$.

Because of our choice for a, the quaternion algebras $(\frac{a,-1}{F})$ are said to be *totally definite.* In this article, we will not need to know precisely what a totally definite algebra is, but we will use results that hold only for totally definite algebras. We provide the following lemma which confirms that the algebras we are interested in are totally definite.

Proposition 2.8 ([22, Page 3], adapted). *If* F *is a totally real number field and* $a \in F$ *are totally negative, then the quaternion algebra* $(\frac{a,-1}{F})$ *is totally definite.*

A notable property of algebras of the form $\mathcal{A} = (\frac{a,-1}{F})$ with F totally real and a totally negative is that they are division algebras — that is, all their elements are invertible, or equivalently, they are non-commutative fields. To see this, note that by definition, all the embeddings of $-a$ are positive numbers. Hence, for any $\alpha = x+iy+jz+ijt \in \mathcal{A}\backslash\{0\}$, all the embeddings of $\mathrm{nrd}(\alpha) = x^2 - ay^2 + z^2 - at^2$ also positive (they are a sum of four non-negative real numbers and at least one of them has to be non-zero since $\alpha \neq 0$), which implies that $\mathrm{nrd}(\alpha)$ is a non-zero element of F. We know that an element $\alpha \in \mathcal{A}$ is invertible if and only if its reduced norm is non-zero (see [39, Lemma 3.3.6]), in which case its inverse is $\alpha^{-1} = \mathrm{nrd}(\alpha)^{-1}\overline{\alpha}$. Hence, we conclude that for our algebras, $\mathcal{A}^\times = \mathcal{A}\backslash\{0\}$.

More details about the definition and notion of definiteness for quaternion algebras are given in Appendix A.1 for the interested readers.

Quaternion orders and ideals. Let us fix a quaternion algebra $\mathcal{A} = (\frac{a,-1}{F})$ over a totally real field F. We begin by the definition of $\mathcal{O}_F$-lattices in $\mathcal{A}$.

Definition 2.9 ([39, Definition 9.3.1]). *An $\mathcal{O}_F$-lattice in $\mathcal{A}$ is a finitely generated $\mathcal{O}_F$-module contained in $\mathcal{A}$ and with full-rank in $\mathcal{A}$ (i.e., it is a rank-4 $\mathcal{O}_F$-module included in $\mathcal{A}$).*

We can now define the notions orders in $\mathcal{A}$.

Definition 2.10 ([39, Definition 10.2.1]). *An $\mathcal{O}_F$-order $\mathcal{O} \subseteq \mathcal{A}$ is an $\mathcal{O}_F$-lattice in $\mathcal{A}$ that is also a subring of $\mathcal{A}$ (in particular, $1 \in \mathcal{O}$). An $\mathcal{O}_F$-order of $\mathcal{A}$ is said to be maximal if it is not strictly contained in another $\mathcal{O}_F$-order.*

One could also define analogously $\mathbb{Z}$-orders of $\mathcal{A}$, as full-rank finitely generated $\mathbb{Z}$-modules that are also a subring of $\mathcal{A}$. This is why the usual notation emphasizes the ring on which the order is considered. In this article, we will only be interested in $\mathcal{O}_F$-orders, so we will abuse the terminology and simply call them orders.

Lemma 2.11 ([39, Prop. 15.5.2], adapted). *In the quaternion algebra $\mathcal{A}$, there exists (at least) one maximal order, and every order $\mathcal{O}$ is contained in a maximal order $\widetilde{\mathcal{O}}$.*

Example 2.12. Over $F = \mathbb{Q}$, the $\mathbb{Z}$-module $\mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + ij\mathbb{Z}$ is an order but is not maximal. However, it is contained in the maximal order $\mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + \omega\mathbb{Z}$, where $\omega = \frac{1+i+j+ij}{2}$.

Contrary to the case of number fields where the ring of integers is the unique maximal order, there can be many maximal orders in a quaternion algebra.

Proposition 2.13 ([39, Lemma 10.2.7 and Definition 10.2.8]). *Let $I \subseteq \mathcal{A}$ be an $\mathcal{O}_F$-lattice. The set $\mathcal{O}_\ell(I) := \{x \in \mathcal{A} \,|\, xI \subseteq I\}$ is an order of $\mathcal{A}$, called the left order of I. Similarly, the set $\mathcal{O}_r(I) := \{x \in \mathcal{A} \,|\, Ix \subset I\}$ is an order of $\mathcal{A}$ called the right order of I.*

Given an order $\mathcal{O}$, a left (resp. right) fractional $\mathcal{O}$-ideal is an $\mathcal{O}_F$-lattice $I \subseteq \mathcal{A}$ satisfying $xI \subseteq I$ (resp. $Ix \subseteq I$) for all $x \in \mathcal{O}$. Since a left fractional $\mathcal{O}$-ideal is in particular an $\mathcal{O}_F$-lattice in $\mathcal{A}$, we can define its left order $\mathcal{O}_\ell(I)$. By definition, this order contains $\mathcal{O}$, but it can be larger. We say that I is a *sated* left fractional $\mathcal{O}$-ideal if $\mathcal{O} = \mathcal{O}_\ell(I)$ (i.e., if $\mathcal{O}$ is the largest order for which I is a left ideal) [39, Definition 16.2.11]. A similar definition holds for right $\mathcal{O}$-ideals.

An important observation that follows from the definition above is that any $\mathcal{O}_F$-lattice $I \subseteq \mathcal{A}$ is a left fractional $\mathcal{O}$-ideal for some order $\mathcal{O}$, namely its left order $\mathcal{O}_\ell(I)$ (it is even a sated left fractional $\mathcal{O}_\ell(I)$-ideal). In the rest of this section, we will review some definitions and lemmas, that extend similar results for ideals in number fields. These results will be stated for $\mathcal{O}_F$-lattices in $\mathcal{A}$ (but keep in mind that these are left fractional $\mathcal{O}$-ideals for some order $\mathcal{O}$, depending on the lattice).

Let I and J be two $\mathcal{O}_F$-lattices in $\mathcal{A}$. The sum of I and J is defined by $I + J := \{\alpha + \beta \,|\, \alpha \in I, \beta \in J\}$ and their product IJ is the set of all finite sums

$\sum_i \alpha_i\beta_i$, where $\alpha_i \in I, \beta_i \in J$. It can be checked that $I+J$ and IJ are still $\mathcal{O}_F$-lattices in $\mathcal{A}$ (the sum of two finitely generated $\mathcal{O}_F$-modules is still a finitely generated $\mathcal{O}_F$-module whose rank is larger than or equal to the maximum of the ranks of the two modules; for the product see [39, p.260]). We say that I is *integral* if $I^2 \subset I$ [39, Definition 16.2.7].

For an $\mathcal{O}_F$-lattice I of $\mathcal{A}$, the reduced norm of I, denoted by $\mathrm{nrd}(I)$, is the (fractional) ideal of F generated by the set $\{\mathrm{nrd}(\alpha) \,|\, \alpha \in I\}$ [39, Definition 16.3.1 and Proposition 16.3.2]. Let $\overline{I} := \{\overline{\alpha} \,|\, \alpha \in I\}$, then this forms another $\mathcal{O}_F$-lattice which we will call the conjugate of I [39, 16.6.6].

We say that an $\mathcal{O}_F$-lattice is principal if there exists $\alpha \in \mathcal{A}^\times$ such that $I = \alpha\mathcal{O}_r(I) = \mathcal{O}_\ell(I)\alpha$ [39, Definition 16.2.1, 16.2.2]. For any $\mathcal{O}_F$-lattice I, if there exists $\alpha \in \mathcal{A}^\times$ such that $I = \alpha\mathcal{O}_r(I)$, then it also automatically holds that $I = \mathcal{O}_\ell(I)\alpha$ [39, 16.2.3]. Hence, to test if an $\mathcal{O}_F$-lattice is principal, it suffices to test if it is left (or right) principal.

The quasi-inverse of an $\mathcal{O}_F$-lattice $I \subset \mathcal{A}$ is the set $I^{-1} := \{\alpha \in \mathcal{A} \,|\, I\alpha I \subseteq I\}$, which is, again, an $\mathcal{O}_F$-lattice [39, Def. 16.5.5 and Le. 16.5.7]. Using the definition of the left order of an $\mathcal{O}_F$-lattice, one can check that the above definition is equivalent to $I^{-1} = \{\alpha \in \mathcal{A} \,|\, I\alpha \subseteq \mathcal{O}_\ell(I)\}$ (because for all $x \in \mathcal{A}$, we have $x \in \mathcal{O}_\ell(I)$ if and only if $xI \subseteq I$). By definition, we always have $II^{-1} \subseteq \mathcal{O}_\ell(I)$ and $I^{-1}I \subseteq \mathcal{O}_r(I)$. We say that I is invertible when the previous inclusions are in fact equalities [39, Prop. 16.5.8]. We say that a left fractional $\mathcal{O}$-ideal I is invertible if it is invertible as an $\mathcal{O}_F$-lattice and if it is sated as a left $\mathcal{O}$-ideal (i.e., $\mathcal{O}_\ell(I) = O$). The following lemma gives a sufficient condition for an $\mathcal{O}_F$-lattice to be invertible and an expression of its inverse.

Lemma 2.14 ([39, Prop. 16.6.15 (b) and 16.6.14]). *Let $I \subseteq \mathcal{A}$ be an $\mathcal{O}_F$-lattice.*

1. *Whenever $\mathcal{O}_\ell(I)$ or $\mathcal{O}_r(I)$ is maximal, then both are and I is invertible.*
2. *If I is invertible, then we have $I^{-1} = \mathrm{nrd}(I)^{-1}\overline{I}$.*

Invertible $\mathcal{O}_F$-lattices enjoy nice properties. Among other, if I is an invertible $\mathcal{O}_F$-lattice, then it holds that $I\overline{I} = \mathrm{nrd}(I)\mathcal{O}_\ell(I)$ and $\overline{I}I = \mathrm{nrd}(I)\mathcal{O}_r(I)$ [39, 16.6.14]. We will use the following lemma on reverse inclusion of quasi-inverses.

Lemma 2.15. *Let $I, J \subseteq \mathcal{A}$ be $\mathcal{O}_F$-lattices with the same left order, i.e., $\mathcal{O}_\ell(I) = \mathcal{O}_\ell(J)$. If $J \subseteq I$, then the inclusion of quasi-inverses $I^{-1} \subseteq J^{-1}$ holds.*

Proof. Using the second definition of the quasi-inverse, we have $I^{-1} = \{\alpha \in \mathcal{A} \,|\, I\alpha \subseteq \mathcal{O}_\ell(I)\}$. Similarly $J^{-1} = \{\alpha \in \mathcal{A} \,|\, J\alpha \subseteq \mathcal{O}_\ell(J)\}$. Using the fact that $J \subseteq I$ and that $\mathcal{O}_\ell(I) = \mathcal{O}_\ell(J)$, we have that any element $\alpha \in I^{-1}$ verifies $J\alpha \subseteq I\alpha \subseteq \mathcal{O}_\ell(I) = \mathcal{O}_\ell(J)$, so $\alpha \in J^{-1}$. □

Recall that for a given order $\mathcal{O}$, a sated fractional left $\mathcal{O}$-ideal I is an $\mathcal{O}_F$-lattice with $\mathcal{O}_\ell(I) = \mathcal{O}$. When $\mathcal{O}$ is a maximal order of $\mathcal{A}$, such sated left $\mathcal{O}$-ideals enjoy many nice properties. A first property is that I is always invertible by Lemma 2.14. Analogously as the situation for fractional ideals of the ring of integers in a number field, invertible $\mathcal{O}_F$-lattices in $\mathcal{A} = (\frac{a,-1}{F})$ are locally principal ([39, Thm. 16.6.1]). A precise definition of this notion is not needed for the core of this work; rather, it is enough to know that such lattices have nice properties with respect to the reduced norm, and that the quaternionic ideals we will consider in this work are all sated. We say that I is compatible with J if $\mathcal{O}_r(I) = \mathcal{O}_\ell(J)$ [39, Definition 16.2.5].

Lemma 2.16 ([39, Le. 16.3.7, 16.3.5 and 16.3.8]). *Let I, J be two $\mathcal{O}_F$-lattices in $\mathcal{A}$, with I invertible.*

1. *If I is compatible with J, then $\mathrm{nrd}(IJ) = \mathrm{nrd}(I)\mathrm{nrd}(J)$.*
2. *We have $I = \mathcal{O}_\ell(I)\alpha$ if and only if $\alpha \in I$ and $\mathrm{nrd}(\alpha)\mathcal{O}_F = \mathrm{nrd}(I)$.*

In the same fashion, when dealing with compatible ideals, we can also state the following lemma:

Lemma 2.17 ([39, Le. 16.5.11], adapted). *Let I, J be two $\mathcal{O}_F$-lattices in $\mathcal{A}$, with I invertible. If I is compatible with J, then $\mathcal{O}_r(IJ) = \mathcal{O}_r(J)$.*

The proof of this proposition goes exactly as the proof of [39, Le. 16.5.11], but the other way around.

Lemma 2.18. *Let I, J be two $\mathcal{O}_F$-lattices in $\mathcal{A}$, with I invertible and $\mathcal{O}_\ell(I) = \mathcal{O}_\ell(J)$ or $\mathcal{O}_r(I) = \mathcal{O}_r(J)$. If $I \subset J$ and $\mathrm{nrd}(I) = \mathrm{nrd}(J)$, then $I = J$.*

Proof. We do the proof when $\mathcal{O}_\ell(I) = \mathcal{O}_\ell(J)$, the case where $\mathcal{O}_r(I) = \mathcal{O}_r(J)$ being analogous. Since I invertible and $I \subset J$, we have $I^{-1}I = \mathcal{O}_r(I) \subset I^{-1}J$. By hypothesis the latter is a product of compatible ideals, hence by Lemma 2.16 *1.*, $\mathrm{nrd}(I^{-1}J) = \mathrm{nrd}(I^{-1})\mathrm{nrd}(J)$. Since $\mathcal{O}_F = \mathrm{nrd}(II^{-1}) = \mathrm{nrd}(I)\mathrm{nrd}(I^{-1})$, we have $\mathrm{nrd}(I^{-1}) = \mathrm{nrd}(I)^{-1}$ and $\mathrm{nrd}(I^{-1}J) = \mathrm{nrd}(I)^{-1}\mathrm{nrd}(J) = \mathcal{O}_F$. Thus, the element $1 \in \mathcal{O}_r(I) \subset I^{-1}J$ generates $\mathrm{nrd}(1)\mathcal{O}_F = \mathcal{O}_F = \mathrm{nrd}(I^{-1}J)$, so by Lemma 2.16 *2.*, $I^{-1}J = \mathcal{O}_r(J)$ and we conclude $I = J$. □

When $\mathcal{O}$ is maximal, a left-$\mathcal{O}$-ideal is sated. This implies in particular that if I and J are two sated left $\mathcal{O}$-ideals, then their sum is still a sated left $\mathcal{O}$-ideal. Indeed, $I + J$ is a left $\mathcal{O}$-ideal, and since $\mathcal{O}$ is maximal then it has to be sated. When $\mathcal{O}$ is maximal, we also have the following proposition, which gives us a description of the quasi-inverse[17] of a sum of sated left $\mathcal{O}$-ideals.

Proposition 2.19. *Let n be a positive integer, $\mathcal{O}$ be a maximal order in $\mathcal{A}$ and $J_1, \ldots, J_n$ be sated fractional left $\mathcal{O}$-ideals in $\mathcal{A}$. Then, the sum $I = J_1 + \cdots + J_n$ has quasi-inverse*

$$I^{-1} = J_1^{-1} \cap \cdots \cap J_n^{-1}.$$

Proof. Since $\mathcal{O}$ is maximal, we know that I is a sated left $\mathcal{O}$-ideal, i.e., $\mathcal{O}_\ell(I) = \mathcal{O} = \mathcal{O}_\ell(J_i)$ for all i. Moreover, for any $1 \leq i \leq n$, we have $J_i \subset I$ so we can apply Lemma 2.15, which gives $I^{-1} \subset J_i^{-1}$. Therefore, $I^{-1} \subset J_1^{-1} \cap \cdots \cap J_n^{-1}$.

Conversely, let $x \in J_1^{-1} \cap \cdots \cap J_n^{-1}$. Then $Ix = (J_1 + \cdots + J_n)x = J_1x + \cdots + J_nx$. Since $x \in J_i^{-1}$ for all i, and by the second definition of the quasi-inverse, it holds that $J_ix \subseteq \mathcal{O}_\ell(J_i) = \mathcal{O}$. Thus $Ix \subset \mathcal{O} = \mathcal{O}_\ell(I)$ which means $x \in I^{-1}$. We conclude that $J_1^{-1} \cap \cdots \cap J_n^{-1} \subset I^{-1}$, as wanted. □

[17] The same result holds for sums of invertible ideals of number fields.

Definition 2.20. *Let $\mathcal{O} \subseteq \mathcal{A}$ be any order and $S \subseteq \mathcal{A}$ be a subset of $\mathcal{A}$ that is included in some $\mathcal{O}_F$-lattice in $\mathcal{A}$.*[18] *Then, the left (resp. right) $\mathcal{O}$-ideal generated by S is the smallest fractional left $\mathcal{O}$-ideal of $\mathcal{A}$ containing the elements $s \cdot \alpha$ (resp. $\alpha \cdot s$), for $(s, \alpha) \in S \times \mathcal{O}$. It is denoted by $\mathcal{O}S$ (resp. $S\mathcal{O}$).*

In the case where $S = \{\alpha\}$ is a singleton, the left (resp. right) $\mathcal{O}$-ideal generated by $\{\alpha\}$ is called the principal left (resp. right) $\mathcal{O}$-ideal generated by α. It is equal to $\mathcal{O}\alpha = \{x\alpha \,|\, x \in \mathcal{O}\}$ (resp. $\alpha\mathcal{O} = \{\alpha x \,|\, x \in \mathcal{O}\}$).

Note that if the order $\mathcal{O}$ is maximal, the left $\mathcal{O}$-ideal generated by S in the definition above is necessarily a sated left $\mathcal{O}$-ideal.

The group $\mathcal{O}^1$. The subgroup of norm 1 elements in a order $\mathcal{O} \subset \mathcal{A}$ is $\mathcal{O}^1 := \{\alpha \in \mathcal{O} \,|\, \mathrm{nrd}(\alpha) = 1\}$. It is a multiplicative subgroup of $\mathcal{O}^\times$. In totally definite quaternion algebras, $\mathcal{O}^1$ is always a finite group, and $\mathcal{O}^1/\{\pm 1\}$ falls into some known list of groups, up to automorphism. See A.3 for details.

To conclude this subsection, we introduce the norm reduced-Principal Ideal Problem in quaternion orders. In the commutative version of this problem, K is typically a cyclotomic number field, and the input are (a $\mathbb{Z}$-basis of) a principal ideal $a \cdot \mathcal{O}_K$ and the relative norm $a\bar{a}$ of one of its generator. The so-called Gentry-Szydlo algorithm [21] then recovers a in polynomial time — for more general context, one can also use Lenstra-Silverberg's algorithm [25].

Definition 2.21 ($\mathcal{O}$-nrdPIP). *For an order $\mathcal{O}$ in $\mathcal{A}$, the $\mathcal{O}$-norm reduced Principal Ideal Problem ($\mathcal{O}$-nrdPIP) is, given as input a left $\mathcal{O}$-ideal I and an element $q \in F$ such that $\mathrm{nrd}(I) = q \cdot \mathcal{O}_F$, to compute, if it exists, an element $g \in I$ with $\mathrm{nrd}(g) = q$.*

Remark 2.22. If g is a solution to $\mathcal{O}$-nrdPIP with input I and q, then by Lemma 2.16 *2.*, the ideal I must be principal with left generator g. An element $g' \in \mathcal{A}$ is another solution *i.e.,* is a left generator of I with reduced norm q, if and only if there exists $u \in \mathcal{O}^1$ such that $g' = ug$.

2.3 Algorithmic considerations

This section gives precisions on how we represent each mathematical object, concretely, to carry actual computations. We borrow most arguments from [29, Section 2.3].

Lattices in $\mathbb{R}^\ell$ Consider integers $1 \leqslant r \leqslant \ell$, and a fixed set of r independents vectors of $\mathbb{R}^\ell$, noted $\boldsymbol{b}_1, \dots, \boldsymbol{b}_r$. The $\mathbb{Z}$-lattice of $\mathbb{R}^\ell$ of dimension r generated by the $\boldsymbol{b}_i$'s, is the set $\mathcal{L}(\boldsymbol{b}_1 | \dots | \boldsymbol{b}_r) := \{\sum a_i \boldsymbol{b}_i,\ a_i \in \mathbb{Z}\}$. This set is discrete and stable by addition. When $r = \ell$, we say that $\mathcal{L}$ is *full rank.*

From now on, we will only manipulate full rank lattices when dealing with lattices in $\mathbb{R}^\ell$. Consider a matrix $B \in \mathbf{GL}_\ell(\mathbb{R})$. Since B is invertible, their column vectors are independent, and span a full rank lattice $\mathcal{L}(B)$. To represent lattices in $\mathbb{R}^\ell$, we use such matrices B, in a form that is called "LLL-reduced".

[18] In more standard terms, the condition "S is included in some $\mathcal{O}_F$-lattice in $\mathcal{A}$" means that the $\mathcal{O}_F$-submodule of $\mathcal{A}$ generated by S is finitely generated.

Representations of ground objects. While we consider several sets of numbers, they are all built on a ground, totally real, number field F of degree d. We therefore chose this field as the base for representing all elements. Let $\alpha_1, \ldots, \alpha_d$ be a $\mathbb{Z}$-basis[19] of $\mathcal{O}_F$. An element $x \in F$ is represented by its rational coordinates in the basis $(\alpha_1, \ldots, \alpha_d)$. The size of a rational is the sum of the bit-size of its numerator and denominator, and the size of an element $x \in F$ is defined as $\operatorname{size}(x) = \sum_i \operatorname{size}(x_i)$, where x_i are the coordinates of x in the give basis of $\mathcal{O}_F$. A fractional $\mathcal{O}_F$-ideal $\mathfrak{a}$ is also a $\mathbb{Z}$-module of rank d, and admits a $\mathbb{Z}$-basis $(a_1, \ldots, a_d)$ — this includes the case of $\mathcal{O}_F$. There are many such bases for a given ideal, but we can always assume that $(\sigma(a_1), \ldots, \sigma(a_d))$ is LLL-reduced for the so-called T_2-norm $\|a\|^2 := \sum_i |\sigma_i(a)|^2$. Then the size of an ideal will be $\operatorname{size}(I) = \sum_i \operatorname{size}(a_i)$, where the a_i's are reduced in the sense above.

By LLL-reducedness and following the arguments presented in [29, Section 2.3], one can show that $\operatorname{size}(x) \leq \operatorname{poly}(\log \Delta_F, \|\sigma(x)\|)$ as well as $\|\sigma(x)\| \leq \operatorname{poly}(\log \Delta_F, \operatorname{size}(x))$ for all $x \in K$. Additionally, an integral $\mathcal{O}_F$-ideal $\mathfrak{a}$ can be represented with $\operatorname{size}(\mathfrak{a}) = \operatorname{poly}(\log \Delta_F, \log N(I))$, where $N(\mathfrak{a}) = [\mathcal{O}_F : \mathfrak{a}]$ is the algebraic norm of the ideal $\mathfrak{a}$.

Representations in extensions and of modules. Recall that we are in the setting of a totally negative $a \in F$ and a quaternion algebra $\mathcal{A} = (\frac{a,-1}{F})$. Then, the CM-extension $K = F(\sqrt{a})$ can be seen as a F-linear space of dimension 2 and basis $\{1, \sqrt{a}\}$. All $x \in K$ have coordinates $(x_1, x_2) \in F^2$ in this basis, and can thus be represented as a vector in $\mathbb{Q}^{2d}$. Likewise, since $\mathcal{A}$ is 4-dimensional over F with basis $\{1, i, j, ij\}$, every element of $\mathcal{A}$ has 4 coordinates in this basis, and corresponds to a vector in $\mathbb{Q}^{4d}$. The size of elements of K and $\mathcal{A}$ is then the sum of the sizes of their F-coordinates. For a matrix B with entries in F and ℓ columns b_i, its size is $\operatorname{size}(B) := \sum_{i \leq \ell} \operatorname{size}(b_i)$.

Fractional $\mathcal{O}_K$-ideals can be viewed as rank 2 modules over $\mathcal{O}_F$ living in $K \simeq F^2$; similarly, quaternionic ideals in $\mathcal{A}$ are also $\mathcal{O}_F$-modules (of rank 4) in $\mathcal{A}$. Any such module has a pseudo-basis $(B, \{\mathfrak{a}_i\}_{i \leq \ell})$. According to the representation of elements above, B is a 2 by 2 or 4 by 4 matrix with entries in F and the $\mathfrak{a}_i$'s are fractional $\mathcal{O}_F$-ideals given by a LLL-reduced basis. The size of such an object M is then $\operatorname{size}(M) := \operatorname{size}(B) + \sum_i \operatorname{size}(\mathfrak{a}_i)$. Likewise, pseudo-Gram matrices $\boldsymbol{G}$ are represented by tuples $(G, \{\mathfrak{a}_i\}_{i \leq \ell})$, with G that is also a 2 by 2 or 4 by 4 matrix with entries in F, and $\mathfrak{a}_i$ fractional $\mathcal{O}_F$-ideals that supports the same assumptions as above. Therefore, $\operatorname{size}(\boldsymbol{G}) := \operatorname{size}(G) + \sum_i \operatorname{size}(\mathfrak{a}_i)$.

These kind of representation differ from the $\mathbb{Z}$-basis representation of ideals and modules, where those objects are represented by a square matrix in $\mathbb{Q}$, whose rank repend of the dimension of the objects over $\mathbb{Q}$. In case we are given such $\mathbb{Z}$-basis, to represent our objects, we can translate those into pseudo-basis in the following way. The Algorithm 2.4.9 of [8] gives a generic way of computing the pseudo basis of $\mathcal{O}_K$ over $\mathcal{O}_F$, with a tacite use of [8, Theorem 10.2.9]. This can

[19] Note however that computing such a basis may be an expensive task. It is a standard practice to assume that such a basis is available, at the cost of having non-uniform reductions. In most of practical usecases, a good basis is explicitely known.

also be done, in our specific case, using [8, Proposition 2.6.1] and the following remark. Then, [7, Algorithm 4.7.10], and [8, Algorithm 2.3.8,Lemma 2.3.7] allows to compute a pseudo-basis representation over $\mathcal{O}_F$ for $\mathcal{O}_K$ ideals. From this point, all quaternionic ideals we need to construct can be known by their pseudo-basis representation. The cost of all of those operations is polynomial. For extensive details, see [8].

Basic algorithms for number fields and quaternion algebras. Still following [29, Section 2.3], we have $\text{size}(x \cdot y) \leq \text{poly}(\text{size}(x), \text{size}(y), \log(\Delta_F))$ for all $x, y \in F$. The computation of the product can be done in $\text{poly}(\text{size}(x), \text{size}(y), \log(\Delta_K))$. One can multiply two ideals I and J of $\mathcal{O}_F$ in time $\text{poly}(\text{size}(I), \text{size}(J), \log \Delta_F)$. We restate results of [29, Section 2.3] for the sake of reusability. The computation of roots of unity is handled by the following lemma.

Lemma 2.23 (Factoring polynomials over a number field [2]). *There is a polynomial time algorithm that given a number field K and a polynomial $P \in K[X]$, factorizes P in K.*

Corollary 2.24 (Computing roots of unity [29, Cor. 2.11]). *Let F be a degree d number field. Then, F has at most $2d^2$ roots of unity and there is a polynomial time algorithm that given a basis of $\mathcal{O}_F$, computes the roots of unity in F.*

We now provide sources for algorithms to handle the computation of left, right orders and of quaternionic ideals arithmetic. In the following, F denotes a number field of degree d and $\mathcal{A}$ is a quaternion algebra over F.

Proposition 2.25 ([18, Alg. 2.16 and Prop. 2.18]). *Given a fractionnal ideal I of $\mathcal{A}$, there exists an algorithm allowing to compute the left and right orders of I, in time $O(d^4)$ arithmetical operations in F.*

Lemma 2.26 ([18, Alg. 2.24 and Prop. 2.25]). *There exists an algorithm that, given two quaternion ideals I and J in $\mathcal{A}$, computes the product $I \cdot J$ in $O(d^4)$ arithmetical operations in F.*

Since, for an invertible quaternion ideal, $I^{-1} = \overline{I}/\text{nrd}(I)$, with $\text{nrd}(I) \subset F$, this lemma and the remark above also implies that the division of a quaternion ideal by an invertible one can be done in $O(d^4)$ arithmetical operations in F.

Lemma 2.27 ([18, Cor. 1.17 and Prop. 2.23]). *There exists an algorithm that, given two quaternion ideals I and J in $\mathcal{A}$, computes the intersection $I \cap J$ in $O(d^3)$ arithmetical operations in F. It consists in intersecting the two $\mathbb{R}$-lattices corresponding to their $\mathbb{Z}$-basis.*

In [26] the authors proposed algorithms for solving various arithmetic problems in quaternion algebras, including the Principal Ideal Problem in both indefinite and definite algebras [26, Alg. 6.3]. Looking carefuly at the latter, we deduce an algorihtm for solving nrdPIP, which amout to solve SVP in dimension $4d$ once.

Lemma 2.28 (Consequence of [26, Alg. 6.3]). *Suppose that $\mathcal{A}$ is totally definite. Let $\mathcal{O}$ be an order in $\mathcal{A}$ and I an integral left fractional $\mathcal{O}$-ideal such that $\mathrm{nrd}(I) = q \cdot \mathcal{O}_F$, where $q \in \mathcal{O}_F$ is totally positive. Then nrdPIP on input I and q is solved by computing one shortest vector in I.*

Proof. Note that we suppose q to be totally positive, so step (1) of [26, Alg. 6.3] is free. Since we are looking for a generator of I with reduced norm exactly q, it is enough to run step (2) of *loc. cit.* only with $z = 1$. In particular, notice that the computation of $\mathcal{O}_F^\times$ is not needed. □

2.4 Module-LIP and Gram factorization

Here we introduce the problem we aim at reducing.

Definition 2.29 (Congruent pseudo-Gram matrices). *Two pseudo-Gram matrices $\mathbf{G} = (G, \{\mathfrak{a}_i\}_{1\leq i\leq \ell})$ and $\mathbf{G}' = (G', \{\mathfrak{b}_i\}_{1\leq i\leq \ell})$ are said to be congruent if there exists a matrix $U = (u_{i,j})_{1\leq i,j\leq \ell} \in \mathbf{GL}_\ell(K)$ such that:*

1. *$G' = U^*GU$.*
2. *$\forall\, i, j \in \{1, \ldots, \ell\},\ u_{i,j} \in \mathfrak{a}_i\mathfrak{b}_j^{-1}$.*
3. *$\prod_i \mathfrak{a}_i = (\det U) \prod_i \mathfrak{b}_j$.*

The set of congruence matrices between $\mathbf{G}$ and $\mathbf{G}'$ is denoted by $\mathrm{Cong}(\mathbf{G}, \mathbf{G}')$.

Definition 2.30 (wc-smodLIP$_K^{\mathbf{B}}$ [29, Definition 3.11]). *Let $\mathbf{B}$ be a pseudo-basis of a module $M \subset K^\ell$, and $\mathbf{G}$ the pseudo-Gram matrix associated to $\mathbf{B}$. Let $\mathbf{G}'$ be a pseudo-gram matrix congruent to $\mathbf{G}$. The worst-case search module Lattice Isomorphism Problem with parameters F and $\mathbf{B}$ (wc-smodLIP$_K^{\mathbf{B}}$) and input $\mathbf{G}'$, is to compute an element of* $\mathrm{Cong}(\mathbf{G}, \mathbf{G}')$.

Lemma 2.31. *Let $\boldsymbol{B} = (B, \{\mathfrak{a}_i\}_i)$ be a pseudo-matrix and $J \subset F$ a fractional ideal. Let $\boldsymbol{B}_J = (B, \{\mathfrak{a}_i{\cdot}J\}_i)$. Then, wc-smodLIP$_K^{\boldsymbol{B}}$ is equivalent to wc-smodLIP$_K^{\boldsymbol{B}_J}$.*

Proof. Let $\mathbf{G}$ and $\mathbf{G}_J$ be the pseudo-Gram matrices associated to $\mathbf{B}$ and $\mathbf{B}_J$, and let **G'** $= (G', \{\mathfrak{b}_i\})$ be an instance of wc-smodLIP$_F^{\mathbf{B}}$. Any $U = (u_{i,j})_{i,j} \in \mathbf{GL}_\ell(K)$ is a solution if and only if it satisfies $G' = U^*GU$ and $u_{i,j} \in \mathfrak{a}_i\mathfrak{b}_j$. However, $G_J = G$ and $(\mathfrak{a}_iJ)(\mathfrak{b}_jJ)^{-1} = \mathfrak{a}_i\mathfrak{b}_j$ (and the same works for the coefficients of U), so U is a solution if and only if it is a solution to wc-smodLIP$_K^{\mathbf{B}_J}$ with input **G'**. □

The lemma above allows to restrain ourselves to manipulating integer modules.

Corollary 2.32. *Any module-LIP problem reduces to a second module-LIP problem where the underlying module is integer and has trivial coefficient ideal.*

Proof. Let $\mathbf{B}$ be a pseudo-basis of a module $M \subset K^\ell$. We apply Lemma 2.31 with $J = \mathcal{C}(M)^{-1}$. Using properties of the coefficient ideal proved in Lemma 2.5, $\mathbf{B}_J$ is the pseudo-basis of an integral M' with $\mathcal{C}(M') = \mathcal{O}_K$. □

This being said, let us precise what objects we are dealing with.

Definition 2.33 (Integral pseudo-matrix). *A pseudo-matrix* $\boldsymbol{B} = ((b_{i,j})_{i,j}, \{\mathfrak{a}_i\}_i)$ *is said to be integral if* $b_{i,j}\mathfrak{a}_j \subset \mathcal{O}_K$ *for all* $1 \leq i, j \leq \ell$*. If* $\det(B) \neq 0$*, this is equivalent to say that the module associated to* $\mathbf{B}$ *is integer.*

Definition 2.34 (Integral factorization of a pseudo-Gram matrix). *Let* $\mathbf{G} = (G, \{\mathfrak{a}_i\}_i)$ *be a pseudo-matrix. We say that* $\mathbf{C} = (C, \{\mathfrak{a}_i\}_i)$ *is an integral factorization of* $\mathbf{G}$ *if* $\mathbf{C}$ *is integral (c.f., Definition 2.33) and if* $C^*C = G$*. The set of integral factorizations of* $\mathbf{G}$ *is denoted by* $\mathrm{IntFact}(\mathbf{G})$*.*

Remark 2.35. A pseudo-Gram matrix may have no integral factorization, *e.g.,* there exist Gram matrices $G \in \mathcal{S}_2(\mathbb{Z})$ which do not admit a factorization in $\mathbb{Z}$. However, the set of solutions is finite. For example in rank two, matrices $C = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ such that C^*C must satisfy $a\overline{a} + b\overline{b} = q_{0,0}$ and $c\overline{c} + d\overline{d} = q_{1,1}$ so the coefficients have bounded euclidean norm.

In the following we investigate the link between module-LIP and integral factorization of pseudo-Gram matrices. This doesn't rely on novel algorithmic techniques and can be exposed here. The equivalence between LIP and Gram factorization has already been noticed by Szydlo in [36], for rotations of $\mathbb{Z}^n$, in which case the equivalence with SVP also holds.

Lemma 2.36 (Computing the determinant). *Let* $\mathbf{G} = (G, \{\mathfrak{a}_i\}_i)$ *and* $\mathbf{G}' = (G', \{\mathfrak{b}_i\}_i)$ *be two congruent pseudo-Gram matrices. Congruence matrices between* $\mathbf{G}$ *and* $\mathbf{G}'$ *all have the same determinant, up to root of a unity of* K*.*

Moreover, there is a polynomial time algorithm that given $\mathbf{G}$ *and* $\mathbf{G}'$*, computes a representant of this class in* $K^\times/\mu(K)$*.*

Proof. Let U be a congruence matrix between $\mathbf{G}$ and **G'**. By definition U satisfies $G' = U^*GU$ so taking the determinant we see that $\det U$ is a solution to the norm equation $\overline{x}x = \det G'/\det G$. Another property of U is that $\prod_i \mathfrak{a}_i = (\det U)\prod_i \mathfrak{b}_i$. In particular, $\det U$ is a generator of the fractional ideal $I = \prod_i \mathfrak{a}_i\mathfrak{b}_i^{-1}$. Any other congruence matrix U' satisfies again these two conditions: $\det U'$ is a generator of I, so one can write $\det U' = u \cdot \det U$ with $u \in \mathcal{O}_K^\times$, and the fact that $\det U'$ is a solution to the same norm equation gives $\overline{u}u = 1$. By Kronecker's theorem, we conclude that u is a root of unity.

Knowing $\mathbf{G}$ and **G'**, we can call the Gentry-Szydlo [21] algorithm with inputs I and relative norm $\det G'/\det G$. Any output is a representant of this class. □

Proposition 2.37. *Let* $\mathbf{B} = (B, \{\mathfrak{a}_i\}_i)$ *be a pseudo-basis of an integer module* $M \subset \mathcal{O}_K^\ell$*, with associated pseudo-Gram matrix* $\mathbf{G}$ *and let* $\mathbf{G}' = (G', \{\mathfrak{b}_i\}_i)$ *be a pseudo-Gram matrix congruent to* $\mathbf{G}$*. Denote by* $\overline{\delta}$ *the determinant class of the congruence matrices between* $\mathbf{G}$ *and* $\mathbf{G}'$*, c.f., Lemma 2.36. Then, there is a bijection*

$$\begin{aligned} \mathrm{Cong}(\mathbf{G}, \mathbf{G}') &\longrightarrow \mathfrak{C} := \{\mathbf{C} = (C, \{\mathfrak{b}_i\}_i) \in \mathrm{IntFact}(\mathbf{G}') \mid \det(B^{-1}C) \in \overline{\delta}\} \\ U &\longmapsto (BU, \{\mathfrak{b}_i\}_i) \end{aligned}$$

Moreover, $\mathfrak{C}$ is the disjoint union $\mathfrak{C} = \bigsqcup_{\mu \in \mu(K)} \mathfrak{C}_{\delta\mu}$, where $\delta \in K$ is any lift of $\overline{\delta}$ and $\mathfrak{C}_\gamma = \{\mathbf{C} = (C, \{\mathfrak{b}_i\}_i) \in \mathrm{IntFact}(\mathbf{G}') \mid \det(B^{-1}C) = \gamma\}$. For any $\mu \in \mu(K)$, there is a bijection $\mathfrak{C}_\delta \to \mathfrak{C}_{\delta\mu}$ given by $(C, \{\mathfrak{b}_i\}_i) \mapsto (\mathrm{diag}(\mu, 1) \cdot C, \{\mathfrak{b}_i\}_i)$.

Proof. First we prove that this map is well defined. Let U be a congruence matrix between $\mathbf{G}$ and $\mathbf{G}'$. By definition, $G' = U^*GU = (BU)^*(BU)$ and $\mathbf{C} := (BU, \{\mathfrak{b}_i\}_i)$ is a pseudo-basis of M so it must be integral. This shows that $\mathbf{C}$ is an integral factorization of $\mathbf{G}'$, *c.f.,* Definition 2.34. Moreover, $\det(BU) = \det B \cdot \det U \in \det B \cdot \overline{\delta}$, by Lemma 2.36. Conversely, it is clear that if the map $\mathbf{C} = (C, \{\mathfrak{b}_i\}_i) \mapsto B^{-1}C$ is well defined, then it is the reciprocal. We prove that if $\mathbf{C} = (C, \{\mathfrak{b}_i\}_{1 \leq i \leq \ell})$ belongs to the right-hand set, then $V = (v_{i,j})_{1 \leq i,j \leq \ell} := B^{-1}C \in \mathrm{Cong}(\mathbf{G}, \mathbf{G}')$. We must verify three conditions to check if it is indeed a congruence matrix, *c.f.,* Definition 2.29. First of all, $V^*GV = C^*(B^{-1})^*(B^*B)B^{-1}C = C^*C = G'$. Also, we have the equality of fractional ideals $\prod_i \mathfrak{a}_i = (\delta) \prod_i \mathfrak{b}_i$ where $\delta \in K$ is any lift of $\overline{\delta}$. In particular, the equality holds with $\delta = \det V$. The last thing to verify is that $v_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$ holds for all $i, j \in \{1, \ldots, \ell\}$. Let us write B_j (resp. C_j) for the j-th column of B (resp. of C) and $b_{i,j}$ (resp. $c_{i,j}$) its coordinates. Since $M = \bigoplus_j \mathfrak{a}_j B_j$ is integral, we have $\mathfrak{a}_j b_{i,j} \subset \mathcal{O}_K$ hence $b_{i,j} \in \mathfrak{a}_j^{-1}$ for all $i, j \in \{1, \ldots, \ell\}$. In the same way, and because $\mathbf{C}$ is integral, we obtain $c_{i,j} \in \mathfrak{b}_j^{-1}$ for all $i, j \in \{1, \ldots, \ell\}$. Let us denote $b'_{i,j}$ the coefficients of B^{-1}. By the comatrix formula $B^{-1} = (\det B)^{-1}$ $\mathrm{com}(B)^T$, the coefficient $b'_{i,j}$ is then

$$b'_{i,j} = \pm(\det B)^{-1} \sum_{\substack{\sigma \in \mathfrak{S}_\ell \\ \sigma(i) = j}} \varepsilon(\sigma) \prod_{\substack{k=1 \\ k \neq i}}^{\ell} b_{\sigma(k),k} \in (\det B)^{-1} \prod_{\substack{k=1 \\ k \neq i}} \mathfrak{a}_k^{-1} \subset \mathfrak{a}_i,$$

where the inclusion comes from $\det B = \sum_{\sigma \in \mathfrak{S}_\ell} \varepsilon(\sigma) \prod_{k=1}^{\ell} b_{k,\sigma(k)} \in \prod_k \mathfrak{a}_k^{-1}$. Finally we can conclude that $v_{i,j} = \sum_{k=1}^{\ell} b'_{i,k} c_{k,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$.

Fix a representative $\delta \in K$ of the class $\overline{\delta}$. Since $\{\delta\mu\}_{\mu \in \mu(K)}$ ranges over all the representatives of $\overline{\delta}$ in K, the union $\mathfrak{C} = \cup_{\mu \in \mu(K)} \mathfrak{C}_{\delta\mu}$ is clear and it must be disjoint by the condition on the determinant. Now fix $\mu \in \mu(K)$ and $\mathbf{C}' = (C', \{\mathfrak{b}_i\}_i) \in \mathfrak{C}_{\delta\mu}$, and put $D = \mathrm{diag}(\mu^{-1}, 1)$. We claim that $\mathbf{C} := (D \cdot C', \{\mathfrak{b}_i\}_i)$ is in $\mathfrak{C}_\delta$. Since $D \in \mathbf{GL}_2(\mathcal{O}_K)$ and $D^*D = Id$, $\mathbf{C}$ is an integral pseudo-matrix satisfying $(D \cdot C')^*(D \cdot C') = C'^*C' = G'$. Moreover $\det(D \cdot C') = \mu^{-1}\delta\mu = \delta$, so $\mathbf{C} \in \mathfrak{C}_\delta$ as claimed. This proves that the map $\mathfrak{C}_\delta \to \mathfrak{C}_{\delta\mu}$ is surjective. It is also injective because D is invertible. □

3 A reduction from modLIP to nrdPIP

Let K/F be a CM extension of number fields where $K = F(\sqrt{a})$ and $\mathcal{A}$ denotes the totally definite quaternion algebra $\mathcal{A} = (\frac{a,-1}{F})$ over F. Through this section we fix a maximal order $\mathcal{O}$ in $\mathcal{A}$ containing the order $\mathcal{O}_0 = \mathcal{O}_K \oplus \mathcal{O}_K \cdot j$.

In this section we prove the main result of this paper, namely, a polynomial time reduction from module-LIP for rank-2 modules in K^2 to nrdPIP, the problem of computing a generator of a (right) principal ideal in $\mathcal{A}$, with given reduced norm (see Definition 2.21). Thanks to Proposition 2.37, module-LIP can be reinterpreted as the task of computing integral factorizations of a pseudo-Gram matrix, with given determinant (up to a root of unity).

The key point is the isomorphism $\mathcal{A} = K \oplus K \cdot j \simeq K^2$ of K-vector spaces. As a consequence, to a matrix $C \in M_2(K)$ corresponds a unique pair $(\alpha, \beta) \in \mathcal{A}^2$ (applying the previous isomorphism on each column of C). We prove in Lemma 3.5 that when $C^*C = G'$ holds, then the quotient $\alpha\beta^{-1}$ can be obtained from an elementary computation involving only G' and $\det C$. In the setting of module-LIP, this determinant can be computed (up to a root of unity of K) in polynomial time, using Lemma 2.36 and the correspondance in Proposition 2.37. We won't be able to obtain α directly from $\alpha\beta^{-1}$, still we show how to build a principal ideal generated by α.

Again, the isomorphism $K^2 \simeq \mathcal{A}$ allows to associate to a module $M \subset K^2$ a left $\mathcal{O}$-ideal in $\mathcal{A}$: the left ideal of $\mathcal{A}$ generated by all the vectors of M, when seen as element of $\mathcal{A}$ via the isomorphism. This ideal, denoted by I_M, is efficiently computable from any pseudo-basis of M (Lemma 3.2). In Proposition 3.6, we use the knowledge of $\alpha\beta^{-1}$ and I_M to build a principal right $\mathcal{O}'$-ideal $\alpha \cdot \mathcal{O}'$, where $\mathcal{O}'$ is some maximal order in $\mathcal{A}$, efficiently computable from I_M but different from $\mathcal{O}$ in general.

Since $\alpha \cdot \mathcal{O}'$ is known, as well as $\mathrm{nrd}(\alpha)$ (see Lemma 3.5), this defines an instance of $\mathcal{O}'$-nrdPIP. The set of integral factorizations of $\mathbf{G}'$ is then obtained from the set of generators of $\alpha \cdot \mathcal{O}'$ with reduced norm $\mathrm{nrd}(\alpha)$. Notice that once such a generator has been computed, the other are its (right) multiples by the elements of $\mathcal{O}'^1$. From the set of generators, one recovers efficiently the set of integral factorizations (see the proof of Theorem 3.7).

Most of the objects used in the reduction depends only on the parameters of module-LIP and not on its input. We will therefore assume that several structures have been precomputed: $\mathbb{Z}$-bases of $\mathcal{O}_F$ and $\mathcal{O}_K$, pseudo-bases of $\mathcal{O}$, I_M and $\mathcal{O}'$ (as $\mathcal{O}_F$-modules, see the previous section). We will also assume that the finite group $\mathcal{O}'^1$ has been precomputed. It is a standard assumption that bases for $\mathcal{O}_F$ and $\mathcal{O}_K$ have been precomputed; in most practical usecases, these bases are even explicit. For the other structures, we give details in Appendix A for the case of cyclotomic fields K, and F their totally real subfield. More precisely, we explain how to compute a maximal order $\mathcal{O}$ containing $\mathcal{O}_0$ (see subsection A.2) and the group $\mathcal{O}^1$ (see subsection A.3).

3.1 The reduction

Embedding modules. Let us recall the setting for an instance of module-LIP. We are given a pseudo-basis $\mathbf{B} = (B, \mathfrak{a}_1, \mathfrak{a}_2)$ of a rank-two module $M \subset K^2$, with associated pseudo-Gram matrix $\mathbf{G}$. Then, wc-smodLIP$_K^{\mathbf{B}}$ takes as input a pseudo-Gram matrix $\mathbf{G}'$ and asks to compute the set $\mathrm{Cong}(\mathbf{G}, \mathbf{G}')$. Thanks to Lemma 2.31, we can suppose that $M \subset \mathcal{O}_K^2$ is integer. Recall the relation $\mathcal{A} = K \oplus K \cdot j$. In particular,

$$\begin{aligned} \varphi : K^2 &\longrightarrow \mathcal{A} \\ (x, y) &\longmapsto x + yj \end{aligned}$$

is an isomorphism of K-vectors spaces, where K acts both on K^2 and $\mathcal{A}$ by left multiplication.

Definition 3.1. *Let $M \subset K^2$ be a module. Then, I_M is defined as the left $\mathcal{O}$-ideal generated by $\varphi(M)$, i.e,*

$$I_M = \mathcal{O} \cdot \varphi(M),$$

where we recall that $\mathcal{O}$ is a maximal order of $\mathcal{A}$ containing $\mathcal{O}_0 = \mathcal{O}_K \oplus \mathcal{O}_K \cdot j$, which has been fixed once and for all.

The ideal I_M can be computed using any pseudo-basis of M.

Lemma 3.2. *Let $\mathbf{B} = ((b_1 \,|\, b_2), \mathfrak{a}_1, \mathfrak{a}_2)$ be a pseudo-basis of a module $M \subset K^2$. Then, the following equality of left $\mathcal{O}$-ideals holds*

$$I_M = \mathcal{O}\mathfrak{a}_1\alpha + \mathcal{O}\mathfrak{a}_2\beta,$$

where $\alpha = \varphi(b_1)$ and $\beta = \varphi(b_2)$. Moreover if M is integer, then the latter ideal is an integral left $\mathcal{O}$-ideal.

Proof. Since φ is left K-linear and $M = \mathfrak{a}_1 b_1 + \mathfrak{a}_2 b_2$ we have $\varphi(M) = \mathfrak{a}_1\alpha + \mathfrak{a}_2\beta$, so $I_M \subset \mathcal{O}\mathfrak{a}_1\alpha + \mathcal{O}\mathfrak{a}_2\beta$. Conversely, $\varphi(M)$ contains the rank one submodule $\mathfrak{a}_1\alpha$ so it holds that $\mathcal{O}\mathfrak{a}_1\alpha \subset I_M$, and in the same way $\mathcal{O}\mathfrak{a}_2\beta \subset I_M$. As I_M is stable by addition, it must contain the sum $\mathcal{O}\mathfrak{a}_1\alpha + \mathcal{O}\mathfrak{a}_2\beta$. If $M \subset \mathcal{O}_K^2$, then $\varphi(M) \subset \varphi(\mathcal{O}_K^2) = \mathcal{O}_0 \subset \mathcal{O}$, so I_M is $\mathcal{O}$-integral. □

By construction, the left order of I_M is $\mathcal{O}$, a maximal order containing $\mathcal{O}_K + \mathcal{O}_K \cdot j$. Its right order $\mathcal{O}' := \mathcal{O}_r(I_M)$ is a priori different from $\mathcal{O}$, except for special cases such as when $M = \mathcal{O}_K^2$ (in this case $\varphi(M) = \mathcal{O}_0$ and $I_M = \mathcal{O}$). The following proposition and its corollary give a more general condition under which the ideal I_M is equal to $\mathcal{O}$. This will be useful to state simplified version of our reduction, for particular modules.

Proposition 3.3. *Let $M \subset K^2$ be a module. Then,*

$$\mathcal{G}(M) \subset \mathrm{nrd}(I_M).$$

Proof. One observes that for any $\mathbf{v} = (v_1 \, v_2)^T \in M$, we have $\langle \mathbf{v}, \mathbf{v} \rangle_K = v_1\overline{v_1} + v_2\overline{v_2} = \mathrm{nrd}(v_1 + v_2 \cdot j) = \mathrm{nrd}(\varphi(\mathbf{v}))$. Recall from Lemma 2.4 that $\mathcal{G}(M)$ is the smallest ideal of F containing the scalar squares $\langle \mathbf{v}, \mathbf{v} \rangle_K$, for $\mathbf{v} \in M$. This proves the inclusion $\mathcal{G}(M) \subset \mathrm{nrd}(I_M)$. □

Corollary 3.4. *Let $M \subseteq \mathcal{O}_K^2$ be an integer module with $\mathcal{G}(M) = \mathcal{O}_F$. Then $I_M = \mathcal{O}$.*

Proof. Since M is integer, we have $I_M \subseteq \mathcal{O}$ (see Lemma 3.2). By Lemma 3.3, we have the inclusion $\mathcal{O}_F = \mathcal{G}(M) \subset \mathrm{nrd}(I_M) \subset \mathrm{nrd}(\mathcal{O}) = \mathcal{O}_F$. So $\mathrm{nrd}(I_M) = \mathcal{O}_F$ and Lemma 2.18 implies $I_M = \mathcal{O}$. Note that we can apply Lemma 2.18 because $\mathcal{O}_\ell(I_M) = \mathcal{O}_\ell(\mathcal{O}) = \mathcal{O}$ and I_M is invertible by Lemma 2.14 since its left order is maximal. □

Gram matrices and quaternions. We can identify $M_2(K)$ with $K^2 \times K^2$ (taking the column vectors) and thus with $\mathcal{A}^2$, applying φ coordinate wise. Therefore to a matrix $C \in M_2(K)$ corresponds a unique pair $(\alpha, \beta) \in \mathcal{A}^2$. In the following lemma, we prove that if C is a factorization of G', then the quotient $\alpha\beta^{-1}$ is expressible in terms of the coefficients of G' and $\det(C)$. We note that Equation (2) below and its proof are very similar to Equation (3) (p.13) from the concurrent work [16].

Lemma 3.5. *Let* $C = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} \in \mathbf{GL}_2(K)$ *be such that* $C^*C = G' = \begin{pmatrix} q_{1,1} & q_{1,2} \\ \overline{q_{1,2}} & q_{2,2} \end{pmatrix}$. *Let α and β be the elements in $\mathcal{A}$ defined by $\alpha = \varphi(x_1, y_1)$ and $\beta = \varphi(x_2, y_2)$. Then, we have the following equalities in $\mathcal{O}_F$*

$$\mathrm{nrd}(\alpha) = q_{1,1} \quad \textit{and} \quad \mathrm{nrd}(\beta) = q_{2,2},$$

and the following holds in $\mathcal{A}$

$$\alpha\beta^{-1} = q_{1,1}(\det(C)j + q_{1,2})^{-1}. \tag{2}$$

Proof. Expanding the product $C^*C = G'$ gives the equality $q_{1,1} = x_1\overline{x_1} + x_2\overline{x_2}$. If one writes $x_1 = x_{1,1} + x_{1,2}\sqrt{a}$ and $x_2 = x_{2,1} + x_{2,2}\sqrt{a}$ in the basis $\{1, \sqrt{a}\}$ of K over F, then the previous equality reads $q_{1,1} = x_{1,1}^2 - ax_{1,2}^2 + x_{2,1}^2 - ax_{2,2}^2$, which is precisely the reduced norm of $x_{1,1} + x_{1,2}\sqrt{a} + (x_{2,1} + x_{2,2}\sqrt{a})j = x_1 + x_2 j = \alpha$. In the same way, $q_{2,2} = \mathrm{nrd}(\beta)$. Note that since $C \in \mathbf{GL}_2(K)$, then $q_{1,1}$ and $q_{2,2}$ are non-zero and so α and β are invertible in $\mathcal{A}$ with inverse $\alpha^{-1} = q_{1,1}^{-1} \cdot \overline{\alpha}$ and $\beta^{-1} = q_{2,2}^{-1} \cdot \overline{\beta}$.

Using multiplication rules for quaternions and the relation $jx = \overline{x}j$ which holds for any $x \in K$, we compute :

$$\begin{aligned} \beta\alpha^{-1}q_{1,1} &= (x_2 + y_2 j)(x_1 + y_1 j)^{-1}q_{1,1} = (x_2 + y_2 j)\overline{(x_1 + y_1 j)} \\ &= (x_2 + y_2 j)(\overline{x_1} - y_1 j) = x_2\overline{x_1} + y_2\overline{y_1} + y_2 x_1 j - x_2 y_1 j \\ &= q_{1,2} + (y_2 x_1 - x_2 y_1)j \\ &= q_{1,2} + \det(C)j. \end{aligned}$$

The equality is then obtained by taking inverses and multiplying both sides by $q_{1,1}$, which lies in F, the center of $\mathcal{A}$. □

Knowing $\alpha\beta^{-1}$, our goal is to recover α. Using the ideal I_M defined in the previous paragraph, we will see how to build a principal ideal generated by α.

Proposition 3.6. *Let $\mathbf{C} = ((c_1 \,|\, c_2), \mathfrak{a}, \mathfrak{b})$ be a pseudo-basis for a module $M \subset K^2$. Let $\alpha = \varphi(c_1)$, $\beta = \varphi(c_2)$ and $\mathcal{O}' = \mathcal{O}_r(I_M)$. Then $\mathcal{O}' = I_M^{-1} I_M$ is a maximal order, and we have the following equality of right $\mathcal{O}'$-ideals*

$$\alpha\mathcal{O}' = \mathfrak{a}^{-1} I_M \cap \alpha\beta^{-1}\mathfrak{b}^{-1} I_M.$$

Proof. Recall that $\mathcal{O}_\ell(I_M) = \mathcal{O}$ which is a maximal order. Hence, Lemma 2.14 tells us that I_M is invertible and that $\mathcal{O}' = \mathcal{O}_r(I_M)$ is maximal too. By definition of invertibility of an $\mathcal{O}_F$-lattice, we also have that $\mathcal{O}' = \mathcal{O}_r(I_M) = I_M^{-1} I_M$ as stated.

Using Proposition 2.19 and the definition of I_M from Lemma 3.2 yields $I_M^{-1} = (\mathcal{O}\mathfrak{a}\alpha)^{-1} \cap (\mathcal{O}\mathfrak{b}\beta)^{-1}$. Using Lemma 2.14 and that $\mathcal{O}_K \subset \mathcal{O}$, we readily compute that $(\mathcal{O}\mathfrak{a}\alpha)^{-1} = \alpha^{-1}\mathfrak{a}^{-1}\mathcal{O}$ and $(\mathcal{O}\mathfrak{b}\beta)^{-1} = \beta^{-1}\mathfrak{b}^{-1}\mathcal{O}$.

Now multiplying I_M^{-1} by α on the left and by I_M on the right (the product of ideals is compatible), and according to Lemma 2.17, we obtain the result. □

Now we have everything to prove the main result of this paper.

```
Algorithm 1: Reduction of wc-smodLIP to nrdPIP
Input: $\mathbf{B} = (B, \mathfrak{a}_1, \mathfrak{a}_2)$ a pseudo-basis of an integer rank two module
       $M \subset \mathcal{O}_K^2$, of associated pseudo-Gram matrix $\mathbf{G}$;
       $\mathbf{G}' = (G' = (q_{i,j})_{1\le i,j\le 2}, \mathfrak{b}_1, \mathfrak{b}_2)$ a pseudo-Gram matrix
       congruent to $\mathbf{G} = (G, \mathfrak{a}_1, \mathfrak{a}_2)$; pseudo-bases of $\mathcal{O}$, $I_M$ and
       $\mathcal{O}' = \mathcal{O}_r(I_M)$ over $\mathcal{O}_F$; $\mu(K)$; $\mathcal{O}'^1$; an oracle $\mathfrak{D}$ solving
       $\mathcal{O}'$-nrdPIP
Output: The set of congruence matrices $\mathrm{Cong}(\mathbf{G}, \mathbf{G}')$
$\mathrm{Cong}(\mathbf{G}, \mathbf{G}') \leftarrow \{\}$;
$\delta \leftarrow \mathrm{GentrySzydlo}(\mathfrak{a}_1\mathfrak{a}_2\mathfrak{b}_1^{-1}\mathfrak{b}_2^{-1}, \det G'/\det G)$      ▷ c.f., Lemma 2.36;
$\gamma \leftarrow \delta \cdot \det B$;
$q \leftarrow q_{1,1}(\gamma j + q_{1,2})^{-1} \in (\frac{K,-1}{F})$                  ▷ c.f., Lemma 3.5;
$I \leftarrow \mathfrak{b}_1^{-1} I_M \cap q\mathfrak{b}_2^{-1} I_M$                    ▷ c.f., Proposition 3.6;
$\alpha' \leftarrow \mathfrak{D}(I, q_{1,1})$;
$S \leftarrow \alpha' \cdot \mathcal{O}'^1$;
for $\alpha$ in $S$ do
    $\beta \leftarrow q^{-1}\alpha$;
    $B' \leftarrow (\varphi^{-1}(\alpha) \,|\, \varphi^{-1}(\beta))$;
    if $(B', \mathfrak{b}_1, \mathfrak{b}_2) \in \mathfrak{C}_\delta$ (c.f., Proposition 2.37) then
        $U \leftarrow B'B^{-1}$;
        $\mathrm{Cong}(\mathbf{G}, \mathbf{G}') \leftarrow \mathrm{Cong}(\mathbf{G}, \mathbf{G}') \cup \{\mathrm{diag}(\mu, 1) \cdot U \,|\, \mu \in \mu(K)\}$  ▷ c.f.,
         Proposition 2.37;
Return $\mathrm{Cong}(\mathbf{G}, \mathbf{G}')$.
```

Theorem 3.7 (modLIP to $\mathcal{O}'$-nrdPIP). *Let $\mathbf{B} = (B, \mathfrak{a}_1, \mathfrak{a}_2)$ be a pseudo-basis of an integer rank two module $M \subset \mathcal{O}_K^2$, with associated pseudo-Gram matrix $\mathbf{G}$ and let $\mathbf{G}' = (G' = (q_{i,j})_{1 \leq i,j \leq 2}, \mathfrak{b}_1, \mathfrak{b}_2)$ be a pseudo-Gram matrix congruent to $\mathbf{G}$. Assume that pseudo-bases over $\mathcal{O}_F$ of $\mathcal{O}$, I_M and $\mathcal{O}' = \mathcal{O}_r(I_M)$ have been precomputed, as well as the finite groups $\mu(K)$ and $\mathcal{O}'^1$. Finally, assume that we are given an oracle $\mathfrak{O}$ that solves $\mathcal{O}'$-nrdPIP. Then Algorithm 1 returns precisely the full set of solutions to wc-smodLIP$_K^{\mathbf{B}}$ on input $\mathbf{G}'$. Moreover, it runs in time*

$$\mathrm{poly}(\deg(K), \mathrm{size}(\mathbf{G})) \;+\; T_{\mathfrak{O}}(\mathfrak{G}),$$

where $T_{\mathfrak{O}}(\mathfrak{G})$ is the worst running time of $\mathfrak{O}$ when the bit length of the input is bounded by $\mathfrak{G}$, and $\mathfrak{G} = \mathrm{poly}(\mathrm{size}(\mathbf{G}'))$.

Proof. Correctness: Let $\delta \in K$ be a representative of the determinant class given by Lemma 2.36. Proposition 2.37 first tells us that the problem is precisely to compute the set $\mathfrak{C}$ of all the integral factorizations $\mathbf{C} = (C, \mathfrak{b}_1, \mathfrak{b}_2)$ of $\mathbf{G}'$ with determinant in $\Gamma := \{\delta \cdot \det B \cdot \mu \mid \mu \in \mu(K)\}$. The second part of *loc. cit.* tells us that it is in fact enough to seek for $\mathbf{C}$ with $\det C = \delta \cdot \det B$ *i.e.,* to compute $\mathfrak{C}_\delta$.

Suppose that there exists $\mathbf{C} = ((c_1 \mid c_2), \mathfrak{b}_1, \mathfrak{b}_2) \in \mathfrak{C}_\delta$. According to Lemma 3.5, Step 4 computes the quaternion $\alpha\beta^{-1}$ from $\mathbf{G}'$ and δ, where $\alpha = \varphi(c_1)$ and $\beta = \varphi(c_2)$. Using Proposition 3.6 and Lemma 3.2, one can compute a pseudo-basis of $\alpha \cdot \mathcal{O}'$, as done in Step 5. Calling our oracle $\mathfrak{O}$ on the latter ideal and $q_{1,1} = \mathrm{nrd}(\alpha)$ returns a left generator α' of $\alpha \cdot \mathcal{O}'$ with reduced norm $\mathrm{nrd}(\alpha') = \mathrm{nrd}(\alpha)$. Thus the quaternion α, corresponding to the first column c_1 of C, belongs to the set $S := \alpha' \cdot \mathcal{O}'^1$. In the same way c_2, corresponding to β, belongs to $(\alpha\beta^{-1})^{-1} S^{-1}$ where $S^{-1} = \{s^{-1} \mid s \in S\}$. To each pair of candidates (α, β), one checks at Step 11 if $((\varphi^{-1}(\alpha) \mid \varphi^{-1}(\beta)), \mathfrak{b}_1, \mathfrak{b}_2) \in \mathfrak{C}_\delta$. If so, Proposition 2.37 implies that the matrix U computed at Step 12 is in $\mathrm{Cong}(\mathbf{G}, \mathbf{G}')$. Moreover for any such B' and U computed at Step 11 and 12, and for all $\mu \in \mu(K)$, *loc. cit.* guarantees that $(\mathrm{diag}(\mu, 1) \cdot B', \mathfrak{b}_1, \mathfrak{b}_2) \in \mathfrak{C}_{\delta\mu}$ thus $\mathrm{diag}(\mu, 1) \cdot U$ is also in $\mathrm{Cong}(\mathbf{G}, \mathbf{G}')$. At the end, all the solutions are contained in the set $\mathrm{Cong}(\mathbf{G}, \mathbf{G}')$.

Complexity: According to Lemma 2.36, a representative δ of the determinant class can be computed in polynomial time. One computes a candidate product $\alpha\beta^{-1}$ from Lemma 3.5 and build the ideal $\mathfrak{b}_1^{-1} I_M \cap \alpha\beta^{-1}\mathfrak{b}_2^{-1} I_M$ in polynomial time, according to Lemma 2.27. If a factorization with determinant γ exists, then the latter ideal should be equal to $\alpha\mathcal{O}'$ by Proposition 3.6. In this case, a generator α' with norm $q_{1,1}$ is recovered in time $T_{\mathfrak{O}}(B)$ where B is a bound on $\mathrm{size}(\alpha\mathcal{O}') = \mathrm{poly}(\mathrm{size}(\mathbf{G}'))$. All generators of $\alpha\mathcal{O}$ and reduced norm $q_{1,1}$ are obtained by mutiplying α' on the right by the elements of $\mathcal{O}'^1$. By Proposition A.19, this is achieved in time $\mathrm{poly}(\mathrm{size}(\alpha'), |\mathcal{O}'^1|) = \mathrm{poly}(\mathrm{size}(\mathbf{G}'), \deg(K))$. From this set, one recovers the candidates for β, as described above and again in time $\mathrm{poly}(|\mathcal{O}'^1|, \mathrm{size}(\mathbf{G}))$. The verification in Step 11 can be done in time $\mathrm{poly}(\mathrm{size}(\mathbf{G}'))$ and there are $|S| = |\mathcal{O}'^1|$ matrices to check. During Step 13, $|\mu(K)| \leq 2\deg(K)^2$ products are computed. Each factor having its size polynomial in $\mathrm{size}(\mathbf{G})$, this step is achived in time $\mathrm{poly}(\mathrm{size}(\mathbf{G}'), \deg(K))$. □

When working over a cyclotomic CM extension K/F, some precomputations in the previous algorithm can be made explicit. Since $\mathcal{O}_K = \mathcal{O}_F + \zeta\mathcal{O}_F$ (where $K = \mathbb{Q}(\zeta)$), we know a (pseudo-)basis of $\mathcal{O}_0 = \mathcal{O}_K + \mathcal{O}_K \cdot j$ over $\mathcal{O}_F$ and a maximal order $\mathcal{O}$ containing $\mathcal{O}_0$ can be computed in polynomial time thanks to Proposition A.18. This observation leads to the following corollary.

Corollary 3.8 (modLIP to $\mathcal{O}'$-nrdPIP, cyclotomic case). *Let K/F be a cyclotomic CM extension, $\mathbf{B} = (B, \mathfrak{a}_1, \mathfrak{a}_2)$ be a pseudo-basis of an integer rank two module $M \subset \mathcal{O}_K^2$, with associated pseudo-Gram matrix $\mathbf{G}$ and let $\mathbf{G}' = (G' = (q_{i,j})_{1\leq i,j\leq 2}, \mathfrak{b}_1, \mathfrak{b}_2)$ be a pseudo-Gram matrix congruent to $\mathbf{G}$. Assume that a pseudo-basis of $\mathcal{O}'$ over $\mathcal{O}_F$ has been computed, as well as the finite group $\mathcal{O}'^1$. Suppose that we are given an oracle $\mathfrak{O}$ that solves $\mathcal{O}'$-nrdPIP. Then Algorithm 1 returns precisely the full set of solutions to wc-smodLIP$_K^{\mathbf{B}}$ on input $\mathbf{G}'$. Moreover, it runs in time*

$$\mathrm{poly}(\deg(K), \mathrm{size}(\mathbf{G})) \ + \ T_{\mathfrak{O}}(\mathbf{G}'),$$

where $T_{\mathfrak{O}}(\mathfrak{G})$ is the worst running time of $\mathfrak{O}$ when the bit length of the input is bounded by $\mathfrak{G}$, and $\mathfrak{G} = \mathrm{poly}(\mathrm{size}(\mathbf{G}))$.

Still over cyclotomic fields and with the extra hypothesis that M satisfies $\mathcal{G}(M) = \mathcal{O}_F$ (or more generally when $\mathcal{RG}(M) = \mathcal{O}_F$), *c.f.,* Definition 2.3, it holds that $\mathcal{O}'$ is in fact equal to $\mathcal{O}$. In particular $\mathcal{O}'^1 = \mathcal{O}^1$ is known (see Appendix A.3). We state a second corollary in this case, which contains the module-LIP instances involved in Hawk. To avoid $\mathcal{O}^1$ to be an exceptional group, we suppose that K is a cyclomic field of big enough degree.

Corollary 3.9 (modLIP to $\mathcal{O}$-nrdPIP, Hawk). *Let $K = \mathbb{Q}(\zeta_m)/F$ be a CM cyclotomic extension and suppose $m \geq 31$. Let $M \subset K^2$ be a rank two module such that $\mathcal{RG}(M) = \mathcal{O}_F$, (c.f., Definition 2.3) given by a pseudo-basis $\mathbf{B} = (B, \mathfrak{a}_1, \mathfrak{a}_2)$ and with associated pseudo-Gram matrix $\mathbf{G}$. Let $\mathbf{G}' = (G' = (q_{i,j})_{1\leq i,j\leq 2}, \mathfrak{b}_1, \mathfrak{b}_2)$ be a pseudo-Gram matrix congruent to $\mathbf{G}$. Suppose that we are given an oracle $\mathfrak{O}$ that solves $\mathcal{O}$-nrdPIP. Then, one can solve wc-smodLIP$_K^{\mathbf{B}}$ on input $\mathbf{G}'$ in time*

$$\mathrm{poly}(\deg(K),\ \mathrm{size}(\mathbf{G})) \ + \ T_{\mathfrak{O}}(\mathbf{G}'),$$

where $\deg(K) = \varphi(m)$*, $T_{\mathfrak{O}}(\mathfrak{G})$ is the worst running time of $\mathfrak{O}$ when the bit length of the input is bounded by $\mathfrak{G}$, and $\mathfrak{G} = poly(size(\mathbf{G}))$.*

Proof. Correctness. From (the pseudo-basis of) M one builds the integer module $M' = \mathcal{C}(M)^{-1} \cdot M$ which satisfies $\mathcal{G}(M') = \mathcal{RG}(M) = \mathcal{O}_F$ by Lemma 2.5. Thanks to Corollary 2.32, the scaling does not change the set of matrices we aim at. Corollary 3.4 then implies that $I_{M'} = \mathcal{O}$. In particular, $\mathcal{O}' = \mathcal{O}_r(I_{M'}) = \mathcal{O}$ and $\mathcal{O}^1$ is known (see Proposition A.28). The result follows from Corollary 3.8.

Complexity. The coefficient ideal $\mathcal{C}(M)$ can be computed via its definition (Definition 2.3) and in time $\mathrm{poly}(\mathrm{size}(\mathbf{B})) = \mathrm{poly}(\mathrm{size}(\mathbf{G}))$. Its inverse is obtained in time $\mathrm{poly}(\log \Delta_K, \mathrm{size}(\mathbf{G})) = \mathrm{poly}(\deg(K), \mathrm{size}(\mathbf{G}))$. A pseudo-basis of $M' = \mathcal{C}(M)^{-1} \cdot M$ is thus computed with the same complexity. Finally, it follows from

A.3 that $\mathcal{O}^1/\pm 1$ is a dihedral group of order $2\deg(K)$ so $|\mathcal{O}^1| = 4\deg(K)$. The final complexity follows from the one of Corollary 3.8, with the previous observations. □

References

1. Léo Ackermann, Adeline Roux-Langlois, and Alexandre Wallet. Public-key encryption from lip. In *International Workshop on Coding and Cryptography (WCC)*, 2024.
2. Karim Belabas, Mark van Hoeij, Jürgen Klüners, and Allan Steel. Factoring polynomials over global fields. *Journal de théorie des nombres de Bordeaux*, 21(1):15–39, 2009.
3. Huck Bennett, Atul Ganju, Pura Peetathawatchai, and Noah Stephens-Davidowitz. Just how hard are rotations of $\mathbb{Z}^n$? algorithms and cryptography with the simplest lattice. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 252–281. Springer, 2023.
4. Jean-François Biasse, Thomas Espitau, Pierre-Alain Fouque, Alexandre Gélin, and Paul Kirchner. Computing generator in cyclotomic integer rings - A subfield algorithm for the principal ideal problem in L(1/2) and application to the cryptanalysis of a FHE scheme. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*, volume 10210 of *Lecture Notes in Computer Science*, pages 60–88, 2017.
5. Jean-François Biasse and Fang Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In Robert Krauthgamer, editor, *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*, pages 893–902. SIAM, 2016.
6. Jean-François Biasse and Claus Fieker. Subexponential class group and unit group computation in large degree number fields. *LMS Journal of Computation and Mathematics*, 17(A):385–403, 2014.
7. Henri Cohen. *A Course in Computational Algebraic Number Theory.* Springer Publishing Company, Incorporated, 2010.
8. Henri Cohen. *Advanced topics in computational number theory*, volume 193. Springer Science & Business Media, 2012.
9. Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016*, volume 9666 of *Lecture Notes in Computer Science*, pages 559–585. Springer, 2016.
10. Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short stickelberger class relations and application to ideal-svp. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017*, volume 10210 of *Lecture Notes in Computer Science*, pages 324–348, 2017.
11. Artūras Dubickas and Chris Smyth. Two variations of a theorem of kronecker. *Expositiones Mathematicae*, 23(3):289–294, 2005.
12. Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel P. J. van Woerden. Hawk: Module LIP makes lattice signatures fast, compact and simple. In Shweta Agrawal and Dongdai Lin, editors, *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, volume 13794 of *Lecture Notes in Computer Science*, pages 65–94. Springer, 2022.

13. Léo Ducas and Wessel P. J. van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 643–673. Springer, 2022.
14. Mathieu Dutour Sikirić, Anna Haensch, John Voight, and Wessel PJ van Woerden. A canonical form for positive definite matrices. *Open Book Series*, 4(1):179–195, 2020.
15. Thomas Espitau, Pierre-Alain Fouque, Benoît Gérard, and Mehdi Tibouchi. Side-channel attacks on BLISS lattice-based signatures: Exploiting branch tracing against strongswan and electromagnetic emanations in microcontrollers. In Bhavani Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, pages 1857–1874. ACM, 2017.
16. Thomas Espitau and Heorhii Pliatsok. On hermitian decomposition lattices and the module-LIP problem in rank 2. Personal communication, 2024.
17. Pierre-Alain Fouque, Paul Kirchner, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu. Key recovery from gram-schmidt norm leakage in hash-and-sign signatures over NTRU lattices. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part III*, volume 12107 of *Lecture Notes in Computer Science*, pages 34–63. Springer, 2020.
18. Carsten Friedrichs. german-thesis-quat-order. 01 2001.
19. Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2013.
20. Craig Gentry and Michael Szydlo. Cryptanalysis of the revised NTRU signature scheme. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 299–320. Springer, 2002.
21. Craig Gentry and Michael Szydlo. Cryptanalysis of the revised NTRU signature scheme. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 299–320. Springer, 2002.
22. Emmanuel Hallouin and Christian Maire. Cancellation in totally definite quaternion algebras. *Journal für die reine und angewandte Mathematik*, 2006(595):189–213, 2006.

23. Ishay Haviv and Oded Regev. On the lattice isomorphism problem. pages 391–404, 2014.
24. Nick Howgrave-Graham and Michael Szydlo. A method to solve cyclotomic norm equations. In Duncan A. Buell, editor, *Algorithmic Number Theory, 6th International Symposium, ANTS-VI, Burlington, VT, USA, June 13-18, 2004, Proceedings*, volume 3076 of *Lecture Notes in Computer Science*, pages 272–279. Springer, 2004.
25. Hendrik W. Lenstra Jr. and Alice Silverberg. Testing isomorphism of lattices over cm-orders. *SIAM J. Comput.*, 48(4):1300–1334, 2019.
26. Markus Kirschmer and John Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM Journal on Computing*, 39(5):1714–1747, 2010.
27. Cong Ling and Andrew Mendelsohn. NTRU in quaternion algebras of bounded discriminant. In Thomas Johansson and Daniel Smith-Tone, editors, *Post-Quantum Cryptography - 14th International Workshop, PQCrypto 2023, College Park, MD, USA, August 16-18, 2023, Proceedings*, volume 14154 of *Lecture Notes in Computer Science*, pages 256–290. Springer, 2023.
28. Daniel Marcus. *Number Fields.* 01 1977.
29. Guilhem Mureau, Alice Pellet-Mary, Georgii Pliatsok, and Alexandre Wallet. Cryptanalysis of rank-2 module-lip in totally real number fields. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part VI*, volume 14656 of *Lecture Notes in Computer Science*, pages 226–255. Springer, 2024.
30. Jürgen Neukirch. *Algebraic Number Theory.* 05 1999.
31. NIST. Round 4 standardisation results for the post-quantum cryptography standardization process, 2024.
32. A. Page. An algorithm for the principal ideal problem in indefinite quaternion algebras. *LMS Journal of Computation and Mathematics*, 17(A):366–384, 2014.
33. Wilhelm Plesken and Bernd Souvignier. Computing isometries of lattices. *Journal of Symbolic Computation*, 24(3-4):327–334, 1997.
34. Michael O. Rabin and Jeffery Shallit. Randomized algorithm in number theory. In *Communications on Pure and Applied Mathematics*, volume 39 of *Lecture Notes in Computer Science*, pages 239–256, 1986.
35. Jean-Pierre Serre. *A course in arithmetic*, volume 7. Springer Science & Business Media, 2012.
36. Michael Szydlo. Hypercubic lattice reduction and analysis of GGH and NTRU signatures. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 433–448. Springer, 2003.
37. John Voight. Computing fundamental domains for fuchsian groups. *Journal de théorie des nombres de Bordeaux*, 21(2):467–489, 2009.
38. John Voight. *Identifying the Matrix Ring: Algorithms for Quaternion Algebras and Quadratic Forms*, pages 255–298. Springer New York, New York, NY, 2013.
39. John Voight. *Quaternion Algebras.* Springer Nature, 01 2021.
40. Lawrence C. Washington. *Introduction to Cyclotomic Fields.* 01 1982.

A Supplementary material

A.1 Discriminant of a quaternion algebra

Places and ramification. The complex embeddings σ of a number field F provides absolute values $v_\sigma(x) = |\sigma(x)|$, and completing F with respect to them yields $\mathbb{R}$ or $\mathbb{C}$, depending on whether σ is real or complex — these are often called archimedian absolute values. Other absolute values can be obtained by looking at prime ideals. For a prime ideal $\mathfrak{p}$ of a number field F, the $\mathfrak{p}$-adic valuation of $x \in \mathcal{O}_F$ is the largest integer $e_\mathfrak{p}(x)$ such that $\mathfrak{p}^e | x\mathcal{O}_F$. This yields a corresponding $\mathfrak{p}$-adic absolute value $v_\mathfrak{p}(x) = N(\mathfrak{p})^{-e_\mathfrak{p}(x)}$, and accordingly a corresponding $\mathfrak{p}$-adic completion $F_\mathfrak{p}$. In a generic way, from now on we denote by v an arbitrary absolute value of F, and the completion of F at v as the field F_v. We may also call v a *place*[20] of F. Given a quaternion algebra $\mathcal{A}$ over F and a place v of F, one can extend the scalars of $\mathcal{A}$ from F to F_v, giving the quaternion algebra $\mathcal{A}_v := \mathcal{A} \otimes_F F_v$ over F_v.

Wedderburn-Artin theorem [39, Corollary 7.3.12] states that a quaternion algebra $\mathcal{A}$ over a field F is either isomorphic to $M_2(F)$, or a division algebra (i.e., a non necessarily commutative ring in which every non zero element has an inverse). In the first case, called the split case, all the completions are isomorphic to a matrix algebra : $\mathcal{A}_v \simeq M_2(F) \otimes_F F_v = M_2(F_v)$. When $\mathcal{A}$ is a division ring, $\mathcal{A}_v$ can be either a matrix algebra or again a division ring. This leads to the notion of ramification.

Definition A.1 ([39, 14.5.1 and 14.3.1]). *Let v a place of F. We say that the algebra $\mathcal{A}$ is ramified at v if $\mathcal{A}_v = \mathcal{A} \otimes_F F_v$ is a division ring, which means that every nonzero element has an inverse. Otherwise we say that $\mathcal{A}$ is split (or unramified) at v.*

We denote $\operatorname{Ram}\mathcal{A}$ the set of ramified places of $\mathcal{A}$. This set is finite [39, Lem. 14.5.3]. Analogously as the discriminant for relative extensions of number fields, the discriminant of $\mathcal{A}$ is an integral ideal of $\mathcal{O}_F$, defined as the product of the finite ramified places in $\mathcal{A}$.

$$disc_F(\mathcal{A}) := \prod_{\substack{\mathfrak{p} \in \mathrm{Ram}(\mathcal{A}) \\ \mathfrak{p} \text{ finite}}} \mathfrak{p}.$$

From its definition, it is clear that the discriminant encodes the ramification at finite places. The behaviour at infinite places leads to the definition of totally definite and indefinite algebras. In the core this paper we focused on the algebras $(\frac{a,-1}{F})$ where $K = F(\sqrt{a})/F$ is a CM extension. They fall into the category of totally definite quaternion algebras, an important property which implies, for example, the finiteness of the groups $\mathcal{O}^1$ (see A.3).

Definition A.2 ([39], 14.5.7). *We say that $\mathcal{A}$ is totally definite if all archimedean places of F are ramified in $\mathcal{A}$; otherwise, we say $\mathcal{A}$ is indefinite.*

[20] Formally, the language of *places* allows to avoid explicit choices of valuations, since a place of a number field F is defined as an equivalence class of non-trivial absolute values on F.

Hilbert symbol. To check if a quaternion algebra $\mathcal{A}$ over F ramifies at some place v of F, one can compute a Hilbert symbol. In the following we give the definition of the Hilbert symbol and we stand some properties useful for our purpose. A standard reference for the theory of Hilbert symbol is [35, Chapter III] but all the following results can be found in [39].

Definition A.3. *Let $\mathcal{A} = (\frac{a,b}{F})$ be a quaternion algebra over a number field F and v be a place of F (either finite of infinite). The Hilbert symbol of $\mathcal{A}$ at v is*

$$\left(\frac{a,b}{v}\right) := \begin{cases} 1 \text{ if } x^2 - ay^2 - bz^2 = 0 \text{ has a non trivial solution in } (F_v)^3 \\ -1 \text{ otherwise} \end{cases}$$

Let us link the Hilbert symbol with the ramification. Recall that an element $\alpha = x + iy + jz + kt \in \mathcal{A}$ has reduced norm $\mathrm{nrd}(\alpha) = x^2 - ay^2 - bz^2 + abt^2$. In this expression, one recognizes the quadratic form involved in the definition of the Hilbert symbol, with an extra term abt^2. If there exists a non trivial solution $(x_0, y_0, z_0) \in (F_v)^3$ to $x^2 - ay^2 - bz^2 = 0$, one can consider the quaternion $\alpha_0 = x_0 + iy_0 + jz_0 \in \mathcal{A}_v$, which reduced norm is zero, by construction. Since the invertible elements in $\mathcal{A}_v$ are the ones with non zero reduced norm, we conclude that $\alpha_0 \neq 0$ is not invertible and $\mathcal{A}_v$ can't be a division ring (and so $\mathcal{A}$ does not ramify at v).

The converse is actually true, that is, any element in $\mathcal{A} \setminus \{0\}$ with reduced norm equal to zero gives a non trivial zero in $(F_v)^3$ to the quadratic form $x^2 - ay^2 - bz^2$. As a consequence, we obtain that the Hilbert symbol is non trivial exactly at the ramified places.

$$\left(\frac{a,b}{v}\right) = \begin{cases} 1 \text{ if } \mathcal{A} \text{ is split at } v \\ -1 \text{ if } \mathcal{A} \text{ is ramified at } v \end{cases}$$

Hilbert reciprocity law states that the product $\prod_v (\frac{a,b}{v})$ over all places v of F is always equal to 1. As a consequence, the set $\mathrm{Ram}(\mathcal{A}) = \{v \mid (\frac{a,b}{v}) = -1\}$ of ramified places has even cardinal.

Lemma A.4 (Hilbert reciprocity law, [39, 14.6.3]). *Let F be a number field and $a, b \in F^\times$. Then,*

$$\prod_v \left(\frac{a,b}{v}\right) = 1, \tag{3}$$

where the product is taken over all places v of F. In particular when F is totally real of even degree and $\mathcal{A}$ is totally definite, the same holds when the product is indexed over finite places of F.

This is a powerful result which sometimes makes us able to decide if the ramification at a place is impossible or must occur, without computing any Hilbert symbol. Finally, we state a formula for computing Hilbert symbols, in the particular case of our quaternion algebras $(\frac{a_m, -1}{F_m})$. We emphasize that the following formula does not hold for prime ideals above 2.

Lemma A.5 ([39, 12.4.10]). *Let F be a number field and $\mathcal{A} = (\frac{a,-1}{F})$. For any prime ideal $\mathfrak{p}$ of F such that $\mathfrak{p} \nmid (2)$, the Hilbert symbol of $\mathcal{A}$ at $\mathfrak{p}$ is given by*

$$\left(\frac{a,-1}{\mathfrak{p}}\right) = \left(\frac{-1}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(a)},$$

where $\left(\frac{-1}{\mathfrak{p}}\right) := \begin{cases} 1 \textit{ if } -1 \textit{ is a square in } (\mathcal{O}_F/\mathfrak{p})^\times \\ -1 \textit{ otherwise} \end{cases}$ *is the Legendre symbol of* -1 *at* $\mathfrak{p}$ *and* $v_{\mathfrak{p}}(a) := \max\{e \in \mathbb{N} \mid a \in \mathfrak{p}^e\}$ *is the* $\mathfrak{p}$*-adic valuation of* a.

Algorithms. In [38], the authors gave deterministic polynomial time algorithms for computing Hilbert symbols, treating the case where $\mathfrak{p}$ is above 2 separately.

Lemma A.6 ([38, Theorem 6.1]). *Let F be a number field and let v be a place of F. There exists an algorithm to evaluate the Hilbert symbol $(\frac{a,b}{v})$ for $a, b \in F^\times$, that is deterministic polynomial time in the size of the inputs.*

Corollary A.7. *There exists an algorithm that given a quaternion algebra $\mathcal{A} = (\frac{a,-1}{F})$ and the prime factorization of $a \cdot \mathcal{O}_F$, computes* $\mathrm{disc}_F(\mathcal{A})$*. Moreover, this algorithm is deterministic and runs in polynomial time.*

Proof. According to Lemma A.5, it is enough to check if the prime ideals dividing $a \cdot \mathcal{O}_F$ ramify in $\mathcal{A}$, as well as the prime ideals above 2. The latters can be computed in polynomial time thanks to Lemma 2.2. For each prime ideal $\mathfrak{p}$ dividing either $a \cdot \mathcal{O}_F$ or $2 \cdot \mathcal{O}_F$, the Hilbert symbol $(\frac{a,-1}{\mathfrak{p}})$ is computed in deterministic polynomial time, using Lemma A.6. There are at most $2 \cdot [F : \mathbb{Q}]$ such ideals. □

A.2 Computing maximal orders

Discriminant of orders. The discriminant of an order $\mathcal{O}$ in a quaternion algebra $\mathcal{A}$ over F is the following ideal of $\mathcal{O}_F$:

$$\mathrm{disc}(\mathcal{O}) := \{\det(\mathrm{trd}(\alpha_i\alpha_j)_{1 \leqslant i,j \leqslant 4}),\ \alpha_1, \dots, \alpha_4 \in \mathcal{O}\} \cdot \mathcal{O}_F,$$

where $\mathrm{trd}(a) := a + \overline{a}$ is the reduced trace map on $\mathcal{A}$, and $\mathrm{trd}(a_ia_j)_{1 \leqslant i,j \leqslant 4}$ is a 4×4 matrix with coefficients in F. Given a pseudo-basis $\mathcal{O} = \mathfrak{a}_1\alpha_1 \oplus \cdots \oplus \mathfrak{a}_4\alpha_4$, and according to [39, Corollary 15.2.7, Paragraph 15.2.8], we have

$$\mathrm{disc}(\mathcal{O}) = (\mathfrak{a}_1 \cdots \mathfrak{a}_4)^2 \cdot \det(\mathrm{trd}(\alpha_i\alpha_j)_{1 \leqslant i,j \leqslant 4}) \cdot \mathcal{O}_F$$

In fact $\mathrm{disc}(\mathcal{O})$ is the square of an ideal of $\mathcal{O}_F$ and we call reduced discriminant of $\mathcal{O}$ the ideal such that $\mathrm{discrd}(\mathcal{O})^2 = \mathrm{disc}(O)$. It somehow measures how far $\mathcal{O}$ is from being a maximal order, in the sense that it is a maximal order if and only if its (reduced) discriminant is equal to the one of $\mathcal{A}$.

Lemma A.8 ([39, Proposition 15.5.5]). *A quaternion order $\mathcal{O}$ in a quaternion algebra $\mathcal{A}$ is maximal if and only if* $\mathrm{discrd}(\mathcal{O}) = \mathrm{disc}(\mathcal{A})$.

Notice that relative discriminants in a CM (so quadratic) extension K/F are defined in the same fashion

$$\mathrm{disc}(\mathcal{O}) := \{\det(\mathrm{trd}(a_i a_j))_{1\leqslant i,j\leqslant 1},\ a_1, a_2 \in \mathcal{O}\} \cdot \mathcal{O}_F,$$

for any order $\mathcal{O} \subset \mathcal{O}_K$. For the maximal order $\mathcal{O} = \mathcal{O}_K$, we denote $\Delta_{K/F} := \mathrm{disc}(\mathcal{O}_K)$.

Example A.9. Consider $\mathcal{A} = (\frac{-1,-1}{\mathbb{Q}})$. According to [39, Example 15.5.7] we have $\mathrm{disc}(\mathcal{A}) = 2\mathbb{Z}$. The order $\mathcal{O} := \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$ has basis $\{1, i, j, k\}$ and one computes $\mathrm{disc}(\mathcal{O}) = (\det \mathrm{diag}(2, -2, -2, -2)) \cdot \mathbb{Z}$ so $\mathrm{discrd}(\mathcal{O}) = 4\mathbb{Z}$ and $\mathcal{O}$ is not maximal. So this order is not maximal in $\mathcal{A}$. Now consider $\mathcal{O}' := \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\gamma$, where $\gamma = \left(\frac{1+i+j+k}{2}\right)$. Then one computes $\mathrm{disc}(\mathcal{O}') = (\det \mathrm{diag}(2, -2, -2, -1/2)) \cdot \mathbb{Z}$ so $\mathrm{discrd}(\mathcal{O}') = 2\mathbb{Z}$ and $\mathcal{O}'$ is thus maximal.

Algorithms. Before focusing on the case of the algebras $\mathcal{A}_m$, we give a generic procedure to compute a maximal order $\widetilde{O}$ containing some given order $\mathcal{O}$ in a quaternion algebra $\mathcal{A}$. As in the commutative case, the algorithm can be described iteratively. Given a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, we say that $\mathcal{O}$ is $\mathfrak{p}$-maximal if $v_\mathfrak{p}(\mathrm{discrd}(\mathcal{O}))$ is minimal, *i.e.,* when $v_\mathfrak{p}(\mathrm{discrd}(\mathcal{O})) = v_\mathfrak{p}(\mathrm{disc}_F(\mathcal{A}))$ holds. Therefore, the maximal orders of $\mathcal{A}$ are precisely the orders which are $\mathfrak{p}$-maximal for every prime ideal. It is enough to look at the prime ideals $\mathfrak{p}$ dividing $\mathrm{discrd}(\mathcal{O})$ (since $\mathfrak{q} \nmid \mathrm{discrd}(\mathcal{O})$ implies that $v_\mathfrak{q}(\mathrm{discrd}(\mathcal{O}))$ is already minimal). Once the factorization of $\mathrm{discrd}(\mathcal{O})$ is known, a $\mathfrak{p}$-maximal order containing $\mathcal{O}$ can be computed in deterministic polynomial-time. Repeating this step for each prime $\mathfrak{p} \mid \mathrm{discrd}(\mathcal{O})$ leads to a maximal order $\mathcal{O}$, as desired.

Lemma A.10 ([38, Algorithm 7.10]). *Let $\mathcal{O}$ and $\mathcal{A}$ be as above and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$. There exists an algorithm that given as input a pseudo-basis of $\mathcal{O}$ and $\mathfrak{p}$, computes a pseudo-basis of a $\mathfrak{p}$-maximal order containing $\mathcal{O}$. It is deterministic and it runs in polynomial-time in* $\mathrm{rank}_\mathbb{Z}(\mathcal{O}) = 4 \cdot [F : \mathbb{Q}]$ *and in the size of $\mathcal{O}$.*

Remark A.11. The complexity of this algorithm is not mentionned in [38] however it is guaranteed to run in deterministic polynomial-time thanks to the following result.

Lemma A.12 ([38, Theorem 7.14]). *Let $\mathcal{O}$ and $\mathcal{A}$ be as above and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$. There exists an algorithm that given as input a pseudo-basis of $\mathcal{O}$, computes a pseudo-basis of a maximal order $\widetilde{O} \supset \mathcal{O}$. It is deterministic polynomial-time reducible to the problem of factoring* $\mathrm{discrd}(\mathcal{O})$ *in $\mathcal{O}_F$.*

An explicit computation in cyclotomic fields. Let $K_m = F_m(a_m)$ be the m-th cyclotomic field with maximal totally real subfield F_m, and $\mathcal{A}_m$ be the quaternion algebra $(\frac{a_m,-1}{F_m})$ over F_m. We investigate the maximality of the order $\mathcal{O}_m = \mathcal{O}_{K_m} \oplus \mathcal{O}_{K_m} \cdot j \subset \mathcal{A}_m$, and we give a polynomial time algorithm for computing a maximal order containing it. In Corollary A.17, we prove that $\mathcal{O}_m$ is often maximal and always not far from being maximal, in the sense that $\mathrm{discrd}(\mathcal{O}_m)$ is either $\mathcal{O}_{F_m}$, a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{F_m}$ or $\mathfrak{p}^2$. Since $\mathrm{discrd}(\mathcal{O}_m) \subset \mathrm{disc}_{F_m}(\mathcal{A}_m)$ holds (as for any order in $\mathcal{A}_m$) we get as a corollary the prime factorization of $\mathrm{disc}_{F_m}(\mathcal{A}_m)$. Once given the factorizations of $\mathrm{disc}_{F_m}(\mathcal{A}_m)$ and $\mathrm{discrd}(\mathcal{O}_m)$, we are then able to compute a maximal order containing $\mathcal{O}_m$ in polynomial time.

Lemma A.13 ([39, 15.2.12]). *We have the equality* $\mathrm{disc}_{F_m}(\mathcal{O}_m) = \Delta^2_{K_m/F_m}$.

Proof. Apply [39, 15.2.12] with the $\mathcal{O}_{F_m}$-order $S = \mathcal{O}_{K_m}$, whose discriminant relatively to $\mathcal{O}_{F_m}$ is by definition Δ_{K_m/F_m}. □

So, computing $\mathrm{disc}_{F_m}(\mathcal{O}_m)$ boils down to computing the factorization of Δ_{K_m/F_m}. This is done in two steps. First, we recall how this ideal can be built efficiently. Then, a property says that the prime ideals of $\mathcal{O}_{F_m}$ dividing Δ_{K_m/F_m} are the ones which ramify in $\mathcal{O}_{K_m}$ (this is in fact an equivalence, see [30, Chapter III, Corollary 2.12]). Ramification in cyclotomic CM-extensions is well-understood: Lemma A.15 recalls those ramified prime ideals. Additionally, the (relative) different ideal $\mathcal{D}_{K/F}$ is an ideal of $\mathcal{O}_K$ whose prime factors are exactly the primes of $\mathcal{O}_K$ over the ones in F that ramify. Morally, $\mathcal{D}_{K/F}$ encodes the ramification in K/F, as $\Delta_{K/F}$ does, but at the level of K. Below we recall how these ideals are linked.

Lemma A.14 ([30, Chap. 3, Prop. 2.4]). *Let $K = F(\alpha)/F$ be an extension of number fields and suppose that $\mathcal{O}_K = \mathcal{O}_F[\alpha]$. Then,*

$$\mathcal{D}_{K/F} = (T'(\alpha)) \cdot \mathcal{O}_K$$
$$\Delta_{K/F} = N_{K/F}(T'(\alpha)) \cdot \mathcal{O}_F,$$

where $T(X) \in \mathcal{O}_F[X]$ is the minimal polynomial of α over F.

In our case, $K_m = F_m(\zeta_m)$, $\mathcal{O}_{K_m} = \mathcal{O}_{F_m}[\zeta_m]$[21] and the minimal polynomial of ζ_m over F_m is $T(X) = X^2 - (\zeta_m + \zeta_m^{-1})X + 1$ so $\Delta_{K_m/F_m} = N_{K_m/F_m}(2\zeta_m - (\zeta_m + \zeta_m^{-1})) \cdot \mathcal{O}_{F_m} = N_{K_m/F_m}(\zeta_m - \zeta_m^{-1}) \cdot \mathcal{O}_{F_m} = (\zeta_m - \zeta_m^{-1})^2 \cdot \mathcal{O}_{F_m}$. Moreover, from the identity $\zeta_m^{-1} - \zeta_m = \zeta_m^{-1}(1 - \zeta_m)(1 + \zeta_m)$, we have $\mathcal{D}_{K_m/F_m} = (1 - \zeta_m)(1 + \zeta_m) \cdot \mathcal{O}_{K_m}$.

Lemma A.15 ([40, Proposition 2.15]). *If $m = p^e$ or $2p^e$ with p an odd prime, then K_m/F_m is ramified at the unique prime ideal above p and unramified everywhere else. In the other cases, K_m/F_m is unramified.*[22]

Corollary A.16. *If $m = p^e$ or $2p^e$ with p an odd prime, then $\Delta_{K_m/F_m} = \mathfrak{p}$ where $\mathfrak{p} = (\zeta_m + \zeta_m^{-1} - 2)$ is the unique prime ideal above p. If $m = 2^e$ is a power of two, then $\Delta_{K_m/F_m} = \mathfrak{p}_2^2$ where $\mathfrak{p}_2 = (\zeta_m + \zeta_m^{-1})$ is the unique prime ideal above 2. Otherwise, $\Delta_{K_m/F_m} = \mathcal{O}_{F_m}$.*

[21] In fact for cyclotomic rings of integers we have $\mathcal{O}_{K_m} = \mathbb{Z}[\zeta_m]$. But then $\mathcal{O}_{F_m}[\zeta_m]$ is a sub order containing both $\mathbb{Z}$ and ζ_m, so we must have equality.

[22] Note that when $m = 2p^e$ with p an odd prime, then $K_m = K_{p^e}$. Indeed, $K_{p^e} \subset K_m$ holds and $\varphi(p^e) = \varphi(m)$ so the fields have same degree over $\mathbb{Q}$ and are thus equal.

Before proving this corollary, recall that, given a field extension K_m/F_m, the relative norm of $a \in K_m$ over F_m is $N_{K_m/F_m}(a) = a\bar{a}$. Then, given an ideal $\mathfrak{a}$ of K_m, the relative norm of $\mathfrak{a}$ over F_m is the F_m-ideal generated by the set $\{N_{K_m/F_m}(a) \mid a \in \mathfrak{a}\}$, and noted $N_{K_m/F_m}(\mathfrak{a})$. The absolute norm of $\mathfrak{a}$ is the $\mathbb{Z}$-fractional ideal $N_{K_m/\mathbb{Q}}(\mathfrak{a})$ (equal to $|\mathcal{O}_{K_m}/\mathfrak{a}| \cdot \mathbb{Z}$ when $\mathfrak{a}$ is an integral ideal, as seen in subsection 2.3).

Proof. Thanks to [30, Chapter III, Corollary 2.3 and 2.12], the primes ideals of F_m dividing Δ_{K_m/F_m} are the ramified primes in $\mathcal{O}_{K_m}$. So, by Lemma A.15, there are three cases to distinguish. If m is not a prime power, then no prime ideal ramifies so $\Delta_{K_m/F_m} = \mathcal{O}_{F_m}$. If $m = p^e$, then 2 is coprime to m and therefore $1+\zeta_m = \frac{1-\zeta_m^2}{1-\zeta_m}$ is a cyclotomic unit, see *c.f.,* [40, §8.1]. Since K_m/F_m is ramified at the unique prime ideal above p by Lemma A.15, $1-\zeta_m$ cannot also be a unit, and so we have $\mathcal{D}_{K_m/F_m} = (1-\zeta_m)\mathcal{O}_K$ as the sole ideal above the prime $\mathfrak{p}$ in F that ramifies in K_m, and $\mathfrak{p} = (\zeta_m + \zeta_m^{-1} - 2)\mathcal{O}_{F_m}$ as claimed, by computing the relative norm of $1-\zeta_m$. Note that the case where $m = 2p^e$ with p odd prime leads to the same result, since $K_m = K_{p^e}$.

Now suppose that $p = 2$. Then both ζ_m and $-\zeta_m$ are primitive m-th roots of the unity. This means that $N_{K_m/\mathbb{Q}}(1-\zeta_m) = N_{K_m/\mathbb{Q}}(1+\zeta_m)$. Using that $-\zeta_m = \zeta^{m/2+1}$, we have the identity $(1-\zeta_m)\sum_{i=0}^{m/2}\zeta_m^i = 1+\zeta_m$, so that $\sum_{i=0}^{m/2}\zeta_m^i \in \mathcal{O}_{K_m}$ has norm 1: it is a unit. Hence we have $(1-\zeta_m)\cdot\mathcal{O}_{K_m} = (1+\zeta_m)\cdot\mathcal{O}_{K_m}$. We compute the relative norm as $N_{K_m/F_m}((1-\zeta_m)^2) = (\zeta_m + \zeta_m^{-1} - 2)^2$ and our claim $\Delta_{K_m/F_m} = \mathfrak{p}_2^2$ follows. □

Corollary A.17. *The following assertions hold:*

1. *If* $m = 2^e$ $(m \neq 4)$ *then* $\operatorname{discrd}(\mathcal{O}_m) = \mathfrak{p}_2^2$*, where* $\mathfrak{p}_2 = (\zeta_m + \zeta_m^{-1})$ *is the unique prime ideal above* 2*, whereas* $\operatorname{disc}_{F_m}(\mathcal{A}_m) = \mathcal{O}_{F_m}$.
2. *If* $m = p^e$ *or* $2p^e$ *with* $p = 1 \pmod 4$ *then* $\operatorname{discrd}(\mathcal{O}_m) = \mathfrak{p}$*, where* $\mathfrak{p} = (\zeta_m + \zeta_m^{-1} - 2)$ *is the unique prime ideal above* p*, whereas* $\operatorname{disc}_{F_m}(\mathcal{A}_m) = \mathcal{O}_{F_m}$.
3. *If* $m = p^e$ *or* $2p^e$ *with* $p = 3 \pmod 4$ *then* $\operatorname{discrd}(\mathcal{O}_m) = \mathfrak{p}$*, where* $\mathfrak{p} = (\zeta_m + \zeta_m^{-1} - 2)$ *is the unique prime ideal above* p*, whereas* $\operatorname{disc}_{F_m}(\mathcal{A}_m) = \mathfrak{p}$*. In particular,* $\mathcal{O}_m$ *is maximal.*
4. *Otherwise,* $\operatorname{discrd}(\mathcal{O}_m) = \operatorname{disc}_{F_m}(\mathcal{A}_m) = \mathcal{O}_{F_m}$*. In particular,* $\mathcal{O}_m$ *is maximal.*

Proof. In all cases we will use the inclusion of ideals $\operatorname{discrd}(\mathcal{O}_m) \subset \operatorname{disc}_{F_m}(\mathcal{A}_m) \subset \mathcal{O}_{F_m}$, so that any prime ideal dividing the first discriminant must also divide the second. Again we use the fact that $K_m = K_{p^e}$ when $m = 2p^e$ with p an odd prime.

1. If $m = 2^e$ and $e > 2$, then we have $\operatorname{disc}_{F_m}(\mathcal{O}_m) = \Delta_{K_m/F_m}^2$, by Lemma A.13 and $\Delta_{K_m/F_m} = \mathfrak{p}_2^2$ by Corollary A.16 so $\operatorname{discrd}(\mathcal{O}_m) = \mathfrak{p}_2^2$. There are $[F_m : \mathbb{Q}] = \varphi(m)/2 = 2^{e-2} \in 2\mathbb{Z}$ infinite places in F_m which all ramify in $\mathcal{A}_m$. Since $\operatorname{disc}_{F_m}(\mathcal{A}_m) \mid \operatorname{discrd}(\mathcal{O}_m)$, the unique finite place of F_m which

can potentially ramify in $\mathcal{A}_m$ is $\mathfrak{p}_2$. But then by Hilbert reciprocity law (3),

$$1 = \underbrace{\prod_{v_\infty} \left(\frac{a_m, -1}{v_\infty}\right)}_{=(-1)^{deg(F_m)}=1} \cdot \prod_{\mathfrak{p}} \left(\frac{a_m, -1}{\mathfrak{p}}\right) = \left(\frac{a_m, -1}{\mathfrak{p}_2}\right) \cdot \prod_{\mathfrak{p} \nmid (2)} \underbrace{\left(\frac{a_m, -1}{\mathfrak{p}}\right)}_{=1} = \left(\frac{a_m, -1}{\mathfrak{p}_2}\right).$$

so $\mathcal{A}_m$ does not ramify at $\mathfrak{p}_2$ and $\mathrm{disc}_{F_m}(\mathcal{A}_m) = \mathcal{O}_{F_m}$.

2. If $m = p^e$ or $2p^e$ with $p = 1 \pmod 4$, then Corollary A.16 gives $\Delta_{K_m/F_m} = \mathfrak{p}$ so $\mathrm{discrd}(\mathcal{O}_m) = \mathfrak{p}$. There are $[F_m : \mathbb{Q}] = \varphi(m)/2 = (p-1)p^{e-1}/2 \in 2\mathbb{Z}$ infinite places in F_m which all ramify in $\mathcal{A}_m$. In the same way, the unique finite place of F_m which can potentially ramify in $\mathcal{A}_m$ is $\mathfrak{p}$. Again by Hilbert reciprocity law, $\mathcal{A}_m$ can't ramify at $\mathfrak{p}$ so $\mathrm{disc}_{F_m}(\mathcal{A}_m) = \mathcal{O}_{F_m}$.
3. If $m = p^e$ or $2p^e$ with $p = 3 \pmod 4$, then Corollary A.16 gives $\Delta_{K_m/F_m} = \mathfrak{p}$ so $\mathrm{discrd}(\mathcal{O}_m) = \mathfrak{p}$. There are $[F_m : \mathbb{Q}] = \varphi(m)/2 = (p-1)p^{e-1}/2 \in (2\mathbb{Z}+1)$ infinite places in F_m which all ramify in $\mathcal{A}_m$. In the same way, the unique finite place of F_m which can potentially ramify in $\mathcal{A}_m$ is $\mathfrak{p}$. Now Hilbert reciprocity law implies that $\mathcal{A}_m$ must ramify at $\mathfrak{p}$, so $\mathrm{disc}_{F_m}(\mathcal{A}_m) = \mathfrak{p}$. Finally, $\mathrm{discrd}(\mathcal{O}_m) = \mathrm{disc}_{F_m}(\mathcal{A}_m)$ so $\mathcal{O}_m$ is maximal, by Lemma A.8.
4. In all other cases, Corollary A.16 gives $\Delta_{K_m/F_m} = \mathcal{O}_{F_m}$ so $\mathrm{disc}_{F_m}(\mathcal{A}_m) = \mathrm{discrd}(\mathcal{O}_m) = \mathcal{O}_{F_m}$ and $\mathcal{O}_m$ is maximal, by Lemma A.8.

□

Algorithm 2: Computing a maximal order $\widetilde{\mathcal{O}_m} \supset \mathcal{O}_m = \mathcal{O}_{K_m} \oplus \mathcal{O}_{K_m} \cdot j$

```
Input: An integer $m \in \mathbb{N}_{>2}$ ($m \neq 4$), a primitive $m$-th root of unity $\zeta_m$.
       $K_m = \mathbb{Q}(\zeta_m)$ (resp. $F_m = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$). A pseudo-basis
       $(B, \{\mathfrak{a}, \mathfrak{b}\})$ of $\mathcal{O}_{K_m} = \mathbb{Z}[\zeta_m]$ over $\mathcal{O}_{F_m} = \mathbb{Z}[\zeta_m + \zeta_m^{-1}]$.
Output: A pseudo-basis over $\mathcal{O}_{F_m}$ of a maximal order containing $\mathcal{O}_m$.
Check if $m = 2^e$, $p^e$ or $2p^e$ and if $p = 1$ or $3 \pmod 4$;
Compute (the prime factorization of) $\mathrm{disc}_{F_m}(\mathcal{A}_m)$ and $\mathrm{discrd}(\mathcal{O}_m)$   ▷
  Thanks to Corollary A.17;
if $\mathrm{disc}_{F_m}(\mathcal{A}_m) = \mathrm{discrd}(\mathcal{O}_m)$ then
    return $(\mathrm{diag}(B, B), \{\mathfrak{a}, \mathfrak{b}, \mathfrak{a}, \mathfrak{b}\})$
else
    $\widetilde{O_m} \leftarrow \mathfrak{p}$-maximal order containing $\mathcal{O}_m$   ▷ Using Lemma A.10;
    return $(\widetilde{\mathcal{O}_m})$
```

Proposition A.18. *For $m \in \mathbb{N}_{>2}, m \neq 4$ and with the previous notations, Algorithm 2 computes (a pseudo-basis of) a maximal order $\widetilde{O_m}$ of $\mathcal{A}_m$ containing the order $\mathcal{O}_m = \mathcal{O}_{K_m} \oplus \mathcal{O}_{K_m} \cdot j$. Moreover, it runs in polynomial time in the degree $d_m = [K_m : \mathbb{Q}]$.*

Proof. Correctness. If $\mathrm{disc}_{F_m}(\mathcal{A}_m) = \mathrm{discrd}(\mathcal{O}_m)$, then Lemma A.8 ensures that $\mathcal{O}_m$ is already maximal. Otherwise, Corollary A.17 tells us that we have $\mathrm{discrd}(\mathcal{O}_m) = \mathfrak{p}$ or $\mathfrak{p}^2$. In both cases, $v_{\mathfrak{p}}(\mathrm{disc}_{F_m}(\mathcal{A}_m)) = 0$ and $v_{\mathfrak{q}}(\mathrm{disc}_{F_m}(\mathcal{A}_m)) =$

$v_{\mathfrak{q}}(\text{discrd}(\mathcal{O}_m)) = 0$ for any prime $\mathfrak{q} \neq \mathfrak{p}$, so it is enough to build an order $\widetilde{O_m} \supset \mathcal{O}_m$ which is $\mathfrak{p}$-maximal *i.e.,* such that $v_{\mathfrak{p}}(\text{discrd}(\widetilde{O_m}))$ is maximal. This is done in step 6, according to Lemma A.10.

Complexity. One can check if m is either of the form 2^e, p^e or $2p^e$, in polynomial time in m. Step 6 is achieved in polynomial time in $\text{rank}_{\mathbb{Z}}(\mathcal{O}) = 2d$ and in $\text{size}(\mathcal{O}) = \text{poly}(d_m, \log \Delta_{K_m}) = \text{poly}(d_m)$, as $\log \Delta_{K_m} = \text{poly}(d_m)$ holds for cyclotomic fields. □

A.3 Units of reduced norm 1 of an order

Recall that our setting is a CM extension K/F of number fields, and a totally definite quaternion algebra $\mathcal{A} = (\frac{a,-1}{F})$, where a is such that $K = F(a)$. Let $\mathcal{A}^\times$ resp. $\mathcal{A}^1$ is the set of elements with non-zero reduced norm (equivalently, invertible), resp. reduced norm equal to 1. For any order $\mathcal{O}$ in $\mathcal{A}$, we let $\mathcal{O}^\times = \mathcal{A}^\times \cap \mathcal{O}$ (so, the units of $\mathcal{O}$) and $\mathcal{O}^1 = \mathcal{A}^1 \cap \mathcal{O}$. Lastly, we let $\mathcal{O}_K^\times, \mathcal{O}_K^1$ and $\mathcal{O}_F^\times, \mathcal{O}_F^1$ the intersection of $\mathcal{A}^\times$ resp. $\mathcal{A}^1$ with $\mathcal{O}_K$, resp. $\mathcal{O}_F$.

We now precise the structure of $\mathcal{O}^\times$ and $\mathcal{O}^1$.

Proposition A.19 ([39, Proposition 32.3.7]). *Let $\mathcal{O}$ be a maximal order of a definite quaternion algebra $\mathcal{A}$. Then $\mathcal{O}^1$ is a finite group.*

We are mostly concerned with the possible size of $\mathcal{O}^1$, and the goal of this section is to show that it remains small. The structure of $\mathcal{O}^1$ can sometimes be elucidated, but followig [39, Chap. 32], it is easier to understand working modulo signs. Let $P\mathcal{A}^\times := \mathcal{A}^\times / F^\times$. In the totally definite case, $\mathcal{O}^1/\{\pm 1\}$ is not only a finite subgroup of $P\mathcal{A}^1$, but its structure is also known to some extent. A dihedral group D_m can be understood as the group of symmetry of a regular polygon with m vertices, and thus is generated by a reflexion τ and a cyclic permutation σ of order m. It is non commutative when $m > 2$, as we have $\tau\sigma\tau = \sigma^{-1}$. Recall that S_n is the group of all the permutations of n symbols, and A_n is its subgroup of even permutations.

Proposition A.20 ([39, Proposition 32.4.1]). *The finite subgroups of $P\mathcal{A}^\times$ are cyclic, dihedral, or isomorphic to a permutation group A_4, S_4, A_5. In particular, the group $\mathcal{O}^1/\{\pm 1\}$ is of this form.*

Finite groups of $P\mathcal{A}^\times$ isomorphic to a permutation group are called exceptional. Their size is constant (respectively $12, 24$ and 60), and particularly independent of the CM extension $K|F$. We will show that for many (and the most interesting) cases, $\mathcal{O}^1/\{\pm 1\}$ will not be an exceptional group.

There are known characterizations and even descriptions (up to isomorphism) of each of the possible situations above, proved in [39, Proposition 32.5.1, 32.5.5, 32.5.8, 32.6.6, 32.7.1]. We separate the exceptional and non-exceptional cases for clarity.

Proposition A.21 (Characterizations of non-exceptional groups).

- *$P\mathcal{A}^\times$ contains a cyclic subgroup Γ of order $m > 2$ if and only there exists a primitive mth root of unity ζ_m in an algebraic closure of F, such that $\zeta_m + \zeta_m^{-1} \in F$ and $F(\zeta_m) = K$.*
- *$P\mathcal{A}^1$ contains a cyclic subgroup of order m if and only if $P\mathcal{A}^\times$ contains one of order $2m$. In this case, it contains $\langle \zeta_{2m} \rangle$, of order m.*
- *$P\mathcal{A}^1$ contains a dihedral group of order $2m > 4$ if and only if, with the notation ζ_m as above, we have $K = F(1 + \zeta_m)$.*

When there exists a cyclic group Γ in $P\mathcal{A}^\times$, then it is conjugated to $\langle 1 + \zeta_m \rangle$, the group generated by $1 + \zeta_m$, by an element of $\mathcal{A}^\times$.

Proposition A.22 (Characterizations of exceptional groups). *The group $P\mathcal{A}^1$ contains a subgroup isomorphic to:*

- *A_4 if and only if $a^2 = -1$;*
- *S_4 if and only if $a^2 = -1$ and $\sqrt{2} \in F$;*
- *A_5 if and only if $a^2 = -1$ and $\sqrt{5} \in F$.*

Any such subgroups are isomorphic if and only if they are conjugated by an element of $\mathcal{A}^\times$.

These exceptional characterizations can be understood informally by the presence of $\frac{1}{\sqrt{2}}(1 \pm \epsilon)$, of order 4 (modulo sign) and $\frac{1}{\sqrt{2}}(\epsilon \pm \epsilon')$ of order 2 (modulo sign) when $\sqrt{2} \in F$, for ϵ, ϵ' distinct in $\{i, j, k\}$. Algebraically, one then works out the structure of S_4, or identifies these quaternions to symmetries of regular polygons. In the typical usecase where K is a power-of-two cyclotomic field, these exceptional groups appear in $P\mathcal{A}^1$. The case of $\sqrt{5}$ involves the golden ratio and can also be worked out similarly, see [39, Chap. 11].

While copies of all these well-identified groups can be explicitely written out in $P\mathcal{A}^\times$, without the knowledge of the conjugating element $\delta \in \mathcal{A}^\times$, we only know them "up to isomorphism" and cannot explicitely compute with them. We now characterize the elements of norm 1 of $\mathcal{O}_K + \mathcal{O}_K \cdot j$. Recall that $\mu(K)$ is the group of roots of unity in the number field K, which is cyclic [30, 7.4].

Proposition A.23 ([11, Theorem K]). *Let K be a CM number field and $a \in \mathcal{O}_K$. If a is non zero and if all its conjugates have absolute value smaller than or equal to 1, then a is a root of unity.*

Corollary A.24. *Let K be a CM number field and $a, b \in \mathcal{O}_K$ be such that $a\overline{a} + b\overline{b} = 1$. Then, either a is a root of unity and $b = 0$ or $a = 0$ and b is a root of unity.*

Proof. For all embeddings σ_i of K, $\sigma_i(a\overline{a}) = |\sigma_i(a)|^2$ and $\sigma_i(b\overline{b}) = |\sigma_i(b)|^2$ are both ≥ 0 . Moreover, $\sigma_i(a\overline{a}) + \sigma_i(b\overline{b}) = \sigma_i(1) = 1$. Suppose that $a \neq 0$, so $0 < \sigma_i(a\overline{a}) \leq 1$ for all i's and Lemma A.23 implies that $a\overline{a}$ must be a root of unity in K. But $a\overline{a}$ is totally positive so $a\overline{a} = 1$ and $b = 0$. Applying again Lemma A.23 to a which satisfies $|\sigma_i(a)| = 1$, we conclude that a is a root of unity. □

Corollary A.25. *Let $\mathcal{O}_0 := \mathcal{O}_K + \mathcal{O}_K \cdot j$. We have $\mathcal{O}_0^1 = \langle j, \mu(K)\rangle$, that is, $\mathcal{O}_0^1$ is the group generated by j and $\mu(K)$*

Proof. Let $x = a+bj \in \mathcal{O}_0$. We have $x \in \mathcal{O}_0^1$ if and only if $\mathrm{nrd}(x) = aa^*+bb^* = 1$. Corollary A.24 gives the solutions. □

This tells us that $\mathcal{O}_0^1/\{\pm1\}$ is a dihedral group of size at least $|\mu(K)|$. When $\mu(K)$ is large enough, $\mathcal{O}^1/\{\pm1\}$ then cannot be exceptional. We sum-up these observations in the next proposition.

Proposition A.26. *Let $\mathcal{O}$ be a maximal order containing $\mathcal{O}_0$ and $d = [F : \mathbb{Q}]$. If $|\mu(K)| \geq 61$, then $\mathcal{O}^1/\{\pm1\}$ is dihedral and $\mathcal{O}^1$ has at most $16d^2$ elements.*

Proof. By inclusion, we have $\mathcal{O}^1 \supset \langle j, \mu(K)\rangle = \mathcal{O}_0^1$. Let G, G_0 be respectively $\mathcal{O}^1/\{\pm1\}$ and $\mathcal{O}_0^1/\{\pm1\}$. Because $|G_0| > 60$, neither G or G_0 can be any of the exceptional groups, thus they are cyclic or dihedral. In any of this cases, the cyclic component of G, generated by γ (say), contains the cyclic component $\mu(K)/\{\pm1\}$ of G_0 generated by ζ. This means that γ commutes with ζ, and that $\pm\gamma^k = \pm\zeta$, for some integer $k \geq 1$. By cardinality of $\mu(K)$, we also see that $\gamma \neq -1$ and therefore $\gamma \notin F$. Now, ζ or $-\zeta$ is a primitive root of 1 in $K \setminus F$, so we have $F \subsetneq F(z) \subset K$. Because K is quadratic over F, this means that we have $K = F(\zeta) \subset F(\gamma) \subset \mathcal{A}$. Since all elements in $\mathcal{A}$ have degree at most 2 over F, with minimal polynomial $T^2 - (\gamma + \overline{\gamma})T + \mathrm{nrd}(\gamma)$, $F(\gamma)$ has degree 2 over F and thus actually $F(\gamma) = K$. We deduce that γ and $-\gamma$ are roots of unity in K, and one (or both) of them any generator of $\mu(K)$. The conclusion comes from Corollary 2.24. □

A more general version of this proposition is as follows:

Proposition A.27. *Let K be a CM field, such that $K = F[\sqrt{a}]$ is a quadratic extension of a totally real field F of degree $d = [F : \mathbb{Q}]$. Let $\mathcal{O}'$ be an order in $\mathcal{A} = (\frac{K,-1}{F})$. If $d > 2$, then $\mathcal{O}'^1$ has at most $16d^2$ elements.*

Proof. $\mathcal{O}'^1/\{\pm1\}$ is a finite subgroup of $P\mathcal{A}^1$. According to Proposition A.21, and [39, Proposition 32.7.1], the finites subgroup of $P\mathcal{A}^1$ are either dihedral, cyclic, or conjugated to an exceptionnal subgroup A_4,A_5 or S_4. If $\mathcal{O}'^1/\{\pm1\}$ falls in the latter case, considering the size of each of these groups, this means that $|\mathcal{O}'^1/\{\pm1\}| \leqslant 60$.

Suppose now that $\mathcal{O}'^1/\{\pm1\}$ is cyclic of order m. Then by Proposition A.21, it is conjugated to the group generated by ζ_{2m}, where ζ_{2m} is a $2m^{th}$ root of unity in $\mathcal{A}$ (so a m^{th} root of -1) such that $\mathcal{A} = (\frac{F[\zeta_{2m}],-1}{F})$. Again by Proposition A.21, $\zeta_{2m}+\zeta_{2m}^{-1} \in F$, so the minimal polynomial of ζ_{2m} in $F[T]$ is $T^2-(\zeta_{2m}+\zeta_{2m}^{-1})T+1$. This polyomial is of degree 2, and so $[F[\zeta_{2m}] : F] = 2$. We know, according to Corollary 2.24, that $\mu(F)$ is a cyclic group of order $\leqslant 2d^2$, so $\mu(F[\zeta_{2m}])$ is a cyclic group of order $\leqslant 8d^2$, so $2m$ is at most equal to $8d^2$. To sum up, in this case, we have $|\mathcal{O}'^1/\{\pm1\}| \leqslant 4d^2$, and $|\mathcal{O}'^1| \leqslant 8d^2$.

Finally, if $\mathcal{O}'^1/\{\pm 1\}$ is dihedral of order $2m > 4$, then by Proposition A.21, it contains a cyclic subgroup of order m. As per the same argument as above, $m \leqslant 4d^2$, $|\mathcal{O}'^1/\{\pm 1\}| \leqslant 8d^2$, and $|\mathcal{O}'^1| \leqslant 16d^2$.

Since we assumed in the Proposition that $d > 2$, we have $16d^2 > 120$, and so, to sum up, $|\mathcal{O}'^1| \leqslant 16d^2$. □

Quaternion algebra over cyclotomic fields. The special case of cyclotomic CM extensions can be made explicit for large conductors, so we isolate its formulation for the sake of clarity and reusability. Recall the notation K_m for the cyclotomic field $\mathbb{Q}(\zeta_m)$, with maximal totally real subfield F_m. Denote by $\mathcal{A}_m$ the quaternion algebra $K_m + K_m \cdot j$ over F_m, with order $\mathcal{O}_m = \mathcal{O}_{K_m} + \mathcal{O}_{K_m} \cdot j$. Finally, $\widetilde{\mathcal{O}_m}$ denotes a maximal order containing $\mathcal{O}_m$. The following result explicits $\widetilde{\mathcal{O}_m}$ in all but one cases.

Corollary A.28. *Let $m \geq 2$ be an integer. If m is of the form $m = 2^e$ or $m = p^e$ or $2p^e$ with $p = 1 \pmod 4$ prime, suppose furthermore that $m \geq 31$. Then,*

$$\widetilde{\mathcal{O}_m}^{\,1} = \mathcal{O}_m^1 = \langle \pm\zeta_m, j \rangle.$$