université de BORDEAUX

Département de Mathématiques

Master Thesis

On the Module-Lattice Isomorphism Problem

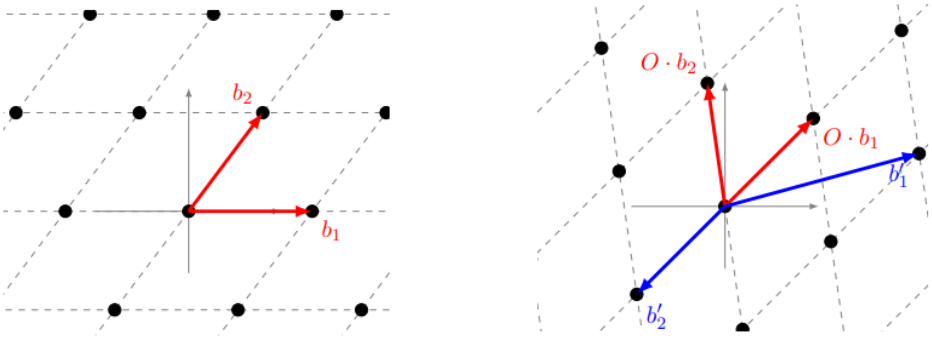
Guilhem Mureau

Under the supersivion of Alice Pellet-Mary

Spring 2023

Introduction

Two lattices $\mathcal{L}_1, \mathcal{L}_2 \subset \mathbb{R}^n$ are said to be isomorphic if there exists an isometry (orthogonal linear transformation) of $\mathbb{R}^n$ sending one to the other, *i.e.*, if $\mathcal{L}_2 = O \cdot \mathcal{L}_1 = \{O \cdot v \,|\, v \in \mathcal{L}_1\}$ for some $O \in \mathcal{O}_n(\mathbb{R})$. The Lattice Isomorphism Problem (LIP) asks, given two isomorphic lattices represented by bases $B_1, B_2 \in \mathbf{GL}_n(\mathbb{R})$, to find $O \in \mathcal{O}_n(\mathbb{R})$ and a unimodular transformation $U \in \mathbf{GL}_n(\mathbb{Z})$ such that $B' = OBU$. It has recently been used by cryptographers to build schemes (L. Ducas, W. van Woerden in [12] and L. Ducas, E. W. Postlethwaite, L. N. Pulles, W. van Woerden in [13]) and it appears to be a good candidate for post-quantum cryptography. State-of-the-art algorithms solving LIP have running time $n^{O(n)}$ ([16]) and require to solve the Shortest Vector Problem (SVP) which is a well-known hard lattice problem.



(a) $\mathcal{L}_1$ with known basis $B = (b_1, b_2)$. (b) $\mathcal{L}_2$ with known basis $B' = (b_1', b_2')$.

Figure 1: (LIP) Find $O \in \mathcal{O}_n(\mathbb{R})$ and $U \in \mathbf{GL}_n(\mathbb{Z})$ such that $B' = OBU$.

In this document we first give an overview of LIP, together with the background needed on lattices and classical algorithms for lattices. In [12], LIP is stated in two equivalent ways, one in terms of lattices and the other with (positive definite) quadratic forms. This reformulation is helpful as it somehow allows us to forget about the isometry and also because quadratic forms are easier to deal with. Our goal is to study the problem for module lattices *i.e.*, lattices which are modules over the ring of integers $\mathcal{O}_K$ of a number field K. One can ask if the extra algebraic structure makes LIP easier to solve. The motivation of this work is Hawk, the signature scheme introduced by L. Ducas, W. van Woerden in [12]. It deals with free rank two module lattices ($\mathcal{L} = \mathcal{O}_K^2$) and its security lies on an instance of LIP. To do so, the second part proposes a reminder on algebraic number theory and it contains the main results of the theory of modules over Dedekind rings.

The third section contains contributions ; we propose a Lattice Isomorphism Problem for any $\mathcal{O}_K$-modules contained in K^l (for some $l \geq 1$) (mod-LIP), generalizing the setting of Hawk. Minkowski embedding allows us to see any module lattice as a lattice ($\subset \mathbb{R}^{nl}$), but this identification obliterates the structure. The problem we define is more natural when handling module lattices, it is compatible with basic properties of modules over Dedekind rings, such as the pseudo-base change. As well as for unstructured lattices, a restatement of mod-LIP in terms of Hermitian forms is possible, but only when seeing the problem in $K_{\mathbb{R}}^l$; to prove it, we establish the existence of a Cholesky factorization for definite positive Hermitian matrices over $K_{\mathbb{R}}$. An important tool when dealing with lattices is Discrete Gaussian Sampling (DGS)

which permits to sample lattice vectors. We give some details on DGS over module lattices. This allows us to generate instances for mod-LIP and therefore we can define an average-case version of the problem. We prove a worst-case to average-case reduction. Finally we explore an algebraic attack for free rank two modules when K is a totally real number field. Knowing that $q \in \mathcal{O}_K$ is the sum of two squares in $\mathcal{O}_K$, we find all such decompositions. We exhibit an algorithm solving mod-LIP in this case which runs, on average, in quasi-polynomial time.

Remerciements

Mes remerciements s'adressent à Alice Pellet-Mary (CNRS, Université de Bordeaux) pour la suggestion de ce sujet, les nombreux conseils et relectures, et pour ce premier pas dans le monde de la cryptographie. Merci à Razvan Barbulescu (CNRS, Université de Bordeaux) et Gilles Zémor, Professeur à l'Université de Bordeaux, pour leur lecture de ce travail et leur présence à la soutenance de ce mémoire. Je remercie également Wessel van Woerden (post-doc, Université de Bordeaux) pour l'article à l'origine de ce sujet et pour les discussions à l'IMB. Merci à Alexandre Bailleul, AGPR à l'ENS de Paris-Saclay, pour les discussions sur Erdös-Kac et d'autres sujets de théorie des nombres. Je remercie Hugo Beguinet et Gaspard Billaud (Thalès) pour cette journée à l'IMB. Merci Barbara, Benjamin, Maximilien et Mohamedenne pour les échanges et le soutien tout au long de ce stage.

Representation of the objects

All along this paper we deal with operations on algebraic objects. This paragraph enlightens on how these elements should be represented in a computer.

• A number field K is (isomorphic to) a quotient $\mathbb{Q}[X]/(P)$ where $P \in \mathbb{Q}[X]$ is irreducible an monic. It has a basis $\{1, X, \ldots, X^{\deg(P-1)}\}$ and elements of K are represented by their coordinates in this $\mathbb{Q}$-basis. Basic operations in K require doing Euclidean division in $\mathbb{Q}[X]$ and the running time depends on the size of the coefficients of P.

• The ring of integer $\mathcal{O}_K$ and more generally any integral ideal $\mathfrak{a}$ are represented by a $\mathbb{Z}$-basis : $\mathfrak{a} = \sum_i \xi_i \mathbb{Z}$, where $\xi \in \mathcal{O}_K$. If K is given by an integral basis, then each x_i can be represented by its coordinates in this basis (it is a vector with coefficients in $\mathbb{Z}$) thus $\mathfrak{a}$ is represented by a $n \times n$ integer matrix, preferably in HNF. A fractional ideal $\mathfrak{b}$ which is not integral is represented by an integral ideal $\mathfrak{a}$ and a denominator d.

Contents

1 Lattice Background and the Lattice Isomorphism Problem

Lattices are well-studied objects combining both algebraic and geometrical aspects, and having various applications in different fields such as the geometry of numbers. Further in a remainder on number theory we will give a survey of Minkowski theory and its application to algebraic number fields. The interest for cryptography is more recent (see for example M. Ajtai [1]). Most of the cryptographic schemes used today are based on prime factorization and on the discrete logarithm problem, both of them are solved by Shor's quantum algorithm [33] in polynomial time. On the other hand, classical lattice algorithmic problems are supposed to be hard to solve even with a quantum computer, which makes lattice-based cryptography a good candidate for post-quantum security.

1.1 Unstructured lattices

Definition. A n-dimensional $\mathbb{Z}$-lattice $\mathcal{L}$ is a discrete additive subgroup of $\mathbb{R}^n$. Its rank is the dimension of the sub-vector space of $\mathbb{R}^n$ spanned by $\mathcal{L}$: $\text{rank}(\mathcal{L}) := \dim(\text{span}(\mathcal{L}))$. We will often consider full rank lattices, *i.e* lattices with rank n.

Definition. A set of k linearly independent vectors $\{b_1, \dots, b_k\} \subset \mathbb{R}^n$ is a basis of a lattice $\mathcal{L} \subset \mathbb{R}^n$ if it satisfies :

$$\mathcal{L} = \left\{ \sum_{i=1}^{k} a_i b_i \mid \forall\, i \in \{1, \dots, k\},\, a_i \in \mathbb{Z} \right\}.$$

Conversely, given linearly independent vectors $\{b_1, \dots, b_k\} \subset \mathbb{R}^n$, it forms a basis for the rank k lattice $B \cdot \mathbb{Z}^k$, where B is the $n \times k$ matrix whose columns are the b_i's. This lattice is also denoted $\mathcal{L}(B)$.

Theorem 1.1. *Any rank k lattice $\mathcal{L} \subset \mathbb{R}^n$ admits a basis. Bases of $\mathcal{L}$ have same cardinal k.*

Remarks. • A $\mathbb{R}$-basis of $\text{span}(\mathcal{L})$ made of vectors of $\mathcal{L}$ may not be a basis of $\mathcal{L}$.

• A lattice of rank ≥ 2 has many bases ; for any $B, C \in M_{n\times k}(\mathbb{R})$, we have $\mathcal{L}(B) = \mathcal{L}(C)$ if and only if there exists $U \in \mathbf{GL}_k(\mathbb{Z})$ such that $C = BU$. Therefore, the set of all full rank n-dimensional lattices is in bijection with $\mathbf{GL}_n(\mathbb{R}) \setminus \mathbf{GL}_n(\mathbb{Z})$, where $\mathbf{GL}_n(\mathbb{Z})$ acts by right multiplication.

From now on, all lattices we consider are supposed to be full rank, unless stated otherwise.

Definition. Given a basis $\{b_1, \dots, b_n\} \subset \mathbb{R}^n$ of a lattice $\mathcal{L}$, we define the determinant (or volume) of $\mathcal{L}$ as the quantity $\det(\mathcal{L}) := |\det(b_1, \dots, b_n)| = |\det(B)|$. This is well defined *i.e.*, it does not depend on the choice of a basis since other bases are of the form BU for some unimodular matrix U.

Remarks. • The volume of $\mathcal{L}$ is also equal to $\sqrt{\det(B^T B)}$. The matrix $B^T B$ is the Gram matrix associated to the basis B.

• Geometrically, one can see $\det(\mathcal{L})$ as the volume of the fundamental parallelepiped $\mathcal{P}(B) := \{\sum_{i=1}^{n} \lambda_i b_i \,|\, (\lambda_i)_{1\leq i\leq n} \in [0;1]^n\}$.

Definition. The minimum distance of a lattice $\mathcal{L} \subset \mathbb{R}^n$ is :

$$\lambda_1(\mathcal{L}) := \min_{x\in\mathcal{L}\setminus\{0\}} ||x|| = \min_{x,y\in\mathcal{L},\ x\neq y} ||x-y||,$$

where $||\cdot||$ denotes the euclidean norm on $\mathbb{R}^n$. This is well defined since a lattice is by definition, a discrete subgroup. Similarly, we define the successive minima of $\mathcal{L}$:

$$\forall\, i \in \{1,\dots,n\}, \quad \lambda_i(\mathcal{L}) := \min_{r>0}\{\dim(\mathrm{span}(\overline{\mathcal{B}}(0,r)\cap\mathcal{L})) \geq i\},$$

where $\overline{\mathcal{B}}(0,r)$ is the closed ball centered at 0 and of radius r, for the norm $||\cdot||$. We have the inequalities :

$$\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n.$$

Example. For the orthogonal lattice $\mathbb{Z}^n$, we have $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 1$.

Theorem 1.2 (Minkowski [27])**.** *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice. Any convex, centrally symmetric body $S \subset \mathbb{R}^n$ of volume $Vol(S) > 2^n \det(\mathcal{L})$ contains a non zero lattice point.*

Corollary 1.1 (Minkowski's inequality [27])**.** *For any lattice $\mathcal{L} \subset \mathbb{R}^n$, we have*

$$\lambda_1(\mathcal{L}) \leq \sqrt{n}\det(\mathcal{L})^{1/n}.$$

Remark. Notice that the quantity $\lambda_1(\mathcal{L})/\det(\mathcal{L})^{1/n}$ is invariant by dilatation or orthogonal transformation of the lattice. Its square is called the Hermite constant of $\mathcal{L}$. In practice, the length of a shortest vector is expected to be roughly equal to the right-hand side of the inequality, which is called the Gaussian heuristic of $\mathcal{L}$.

1.2 Algorithmic problems and tools

In this paragraph we define some of the most famous algorithmic problems based on lattices, essential for cryptographic purposes. We also present the LLL algorithm, historically introduced to factorize polynomial over the field of rationnal numbers, it is an important polynomial time running algorithm to compute « reduced » basis of a given lattice. In particular it solves the approximate shortest vector problem with approximation factor exponential in the dimension of the lattice.

Some classical problems on lattices. The following are classical algorithmic problems in lattice based cryptography.

γ-SVP : Given a lattice basis of $\mathcal{L}$ and an approximation factor $\gamma \geq 1$, the γ-approximate Shortest Vector Problem (γ-SVP) is to find a non zero vector $x \in \mathcal{L}$ such that $||x|| \leq \gamma \cdot \lambda_1(\mathcal{L})$.

γ-HSVP : Given a lattice basis of $\mathcal{L}$ and an approximation factor $\gamma \geq 1$, the γ-approximate Hermite Shortest Vector Problem (γ-HSVP) is to find a non zero vector $x \in \mathcal{L}$ such that $||x|| \leq \gamma \cdot \sqrt{n}(\det(\mathcal{L}))^{1/n}$.

γ-CVP : Given a lattice basis of $\mathcal{L}$, an approximation factor $\gamma \geq 1$ and a target vector $t \in \text{span}(\mathcal{L})$, the γ-approximate Closest Vector Problem is to find a vector $x \in \mathcal{L}$ such that $||x-t|| \leq \gamma \cdot \delta(t, \mathcal{L})$, where $\delta(t, \mathcal{L})$ is the distance of t to $\mathcal{L}$, *i.e.*, the minimum of $||x-t||$ where x runs though all lattice vectors.

BDD : Given a basis of $\mathcal{L}$ and a target vector $t \in \text{span}(\mathcal{L})$ with distance from $\mathcal{L}$ at most $\lambda_1(\mathcal{L})/2$, the Bounded Distance Decoding Problem is to compute the closest lattice vector to t.

LLL Algorithm. Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice with basis $\mathbf{b} = (b_1, \ldots, b_n)$. Recall that the result of Gram-Schmidt process applied to $\mathbf{b}$ is an orthogonal basis of $\mathbb{R}^n$, denoted $\mathbf{b}^* = (b_1^*, \ldots, b_n^*)$ (these vectors may not be in $\mathcal{L}$) such that for all $i \geq 1$, $\{b_1^*, \ldots, b_i^*\}$ generate the same sub-vector space of $\mathbb{R}^n$ as $\{b_1, \ldots, b_i\}$. Namely, if we define for all $1 \leq i, j \leq n$, $a_i^2 := \langle b_i^*, b_i^* \rangle$ and $u_{i,j} := \langle b_i, b_j^* \rangle / a_j^2$, then $b_1^* := b_1$ and $b_i^* := b_i - \sum_{j=1}^{i-1} u_{i,j} b_j^*$ for all $i \geq 2$.

Definition. With the same notations, the basis $\mathbf{b}$ is said LLL-reduced if it satisfies :
1) $|u_{i,j}| \leq 1/2$ for all $1 \leq j \leq i \leq n$. (size condition)
2) $a_i^2 \geq (3/4 - u_{i,i-1}^2) a_{i-1}^2$ for all $1 \leq i \leq n$ (Lovász condition)

Proposition 1.1 (Théorème 1 of [3])**.** *With the notations of the definition above, a LLL-reduced basis* $\mathbf{b}$ *verifies :*
1) $\det(\mathcal{L}) \leq \prod_{i=1}^n ||b_i||^2 \leq 2^{\frac{n-1}{2}} \det(\mathcal{L})$
2) $||b_j||^2 \leq 2^{i-1} a_i^2$*, for all* $1 \leq j \leq i \leq n$
3) $||b_1|| \leq 2^{\frac{n-1}{4}} \det(\mathcal{L})^{1/n}$.
4) $||b_1|| \leq 2^{\frac{n-1}{2}} \lambda_1(\mathcal{L})$.

Algorithm 1.1 (Lenstra-Lenstra-Lovász, 1982)**.** *Given a lattice* $\mathcal{L} \subset \mathbb{R}^n$ *and* $(g_1, \ldots, g_m)$ *a set of generators of* $\mathcal{L}$ *with* $||g_i|| \leq B$ *for* $i \in \{1, \ldots, m\}$*, the LLL algorithm returns a LLL-reduced basis* $(b_1, \ldots, b_n)$ *of* $\mathcal{L}$*. The complexity of this algorithm is* $O(m^6 \ln(B)^3)$*.*

This algorithm consists in two steps successively repeated. Suppose $(b_1, \ldots, b_{k-1})$ satisfies both conditions ($k-1 \leq n$). A reduction step allows us to construct b_k such that $|u_{k,j}| \leq 1/2$ for every $j \leq k-1$. If Lovász's condition is not verified at step k, we swap b_k with b_{k-1}, compute the new Gram-Schmidt vectors and then we come back to step $k-1$. For more details, see [3] or [10].

Corollary 1.2. **γ-SVP** *is solvable in polynomial time for* $\gamma = 2^{\frac{n-1}{2}}$*.*

Hermite Normal Form. From any generating set of a lattice $\mathcal{L} \subset \mathbb{Z}^m$, [1] we can recover a (unique) basis whose matrix $B = (b_{i,j})$ is in reduced echelon form on the lines (if $p(i)$ corresponds to the index column of the first non-zero element on the line i, we have $p(i) > p(i-1)$ for all i. Also, $b_{i,p(i)} > 0$ and $0 \leq b_{j,p(i)} < b_{i,p(i)}$ for every $j > i$). We say that a matrix $M \in M_{m,n}(\mathbb{Z})$ is in HNF if there exists an integer r such that the r first columns are equal to 0 and if the $n-r$ other columns form a reduced echelon (on the lines) matrix.

Theorem 1.3 (Existence and uniqueness of the HNF)**.** *For* $G \in M_{m,n}(\mathbb{Z})$*, there exists a unique matrix* $B \in M_{m,n}(\mathbb{Z})$ *in HNF such that* $B = GU$ *with* $U \in \mathbf{GL}_n(\mathbb{Z})$*.*

[1] For cryptographic application, lattices considered are often $\subset \mathbb{Z}^m$.

Remarks. • Given a set of generators of a lattice $\mathcal{L}$, represented by a matrix $G \in M_{m,n}(\mathbb{Z})$, the non-zero columns of the HNF of G form a basis of $\mathcal{L}$.

• There is a polynomial time algorithm computing the HNF of $G \in M_{m,n}(\mathbb{Z})$. It is faster than LLL reduction algorithm but we have no information on the length of the basis vectors obtained, it is somehow a bad basis.

Cholesky decomposition. Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice with basis $B \in \mathbf{GL}_n(\mathbb{R})$ and $Q := B^T B$. It is a positive definite quadratic form which encodes the geometry of $\mathcal{L}$ in the sense that for any lattice vector $x \in \mathcal{L}$, there exists $y \in \mathbb{Z}^n$ such that $x = By$ and

$$||x|| = ||y||_Q,$$

where $||\cdot||$ is the Euclidean norm on $\mathbb{R}^n$ and $||\cdot||_Q$ is the norm given by $||z||_Q := ||Bz|| = \sqrt{z^T Q z}$. A question arising is, from a positive definite quadratic form Q, to recover a matrix $B \in \mathbf{GL}_n(\mathbb{R})$ such that $Q = B^T B$. If B satisfies this relation, then the set of solutions is precisely $\{OB\}_{O \in \mathcal{O}_n(\mathbb{R})\}}$. In terms of lattices, this corresponds to a family of isomorphic lattices (*i.e.*, the same lattice up to a rotation of the space) with same geometry induced by Q. More generally, to any positive definite Hermitian matrix (*i.e.*, a matrix $A \in M_n(\mathbb{C})$ such that $A^* := \overline{A}^T = A$ and $x^* A x > 0$ for all $x \in \mathbb{C}^n \setminus \{0\}$) we can ask for a decomposition $A = B^* B$.

Proposition 1.2 (See [36] for details)**.** *Let $A \in M_n(\mathbb{C})$ be a positive definite Hermitian matrix. There exists a unique upper-triangular matrix $R \in \mathbf{GL}_n(\mathbb{C})$ with strictly positive real diagonal coefficients and such that $A = R^* R$. Moreover, R is efficiently computable.*

Proof. First we deal with the existence part. As A is Hermitian, it is a normal matrix (it commutes with its adjoint matrix) so there exist $P, D \in \mathbf{GL}_n(\mathbb{C})$ with D diagonal such that $A = P^* D P$. Also, D has real strictly positive coefficients (the eigenvalues of A) so it has a real square root matrix $D^{1/2}$ obtained by taking positive square roots of each diagonal element. Then, $A = (PD^{1/2})^*(PD^{1/2})$ and $PD^{1/2} \in \mathbf{GL}_n(\mathbb{C})$ has a QR decomposition ; there exist $Q \in U_n(\mathbb{C})$ a unitary matrix (*i.e.*, $Q^*Q = Id$) and $R \in \mathbf{GL}_n(\mathbb{C})$ an upper-triangular matrix with strictly positive diagonal coefficients such that $PD^{1/2} = QR$. Thus, $A = (QR)^*(QR) = R^* R$.
Now for the uniqueness, suppose we have two decompositions $R^*R = A = S^*S$ where R, S are upper-triangular with strictly positive diagonal. Then, $RS^{-1} = (R^*)^{-1}S^*$ and the left-hand side is an upper-triangular matrix while the right-hand side is lower triangular, thus $RS^{-1} = D = (R^*)^{-1}S^*$ with D a diagonal matrix. Since D satisfies $DS = R$, its coefficients are strictly positive. Moreover, $(D^*)^{-1} = (SR^{-1})^{-1} = RS^{-1} = D$ so $D^*D = Id$ and this implies D has its coefficients on the unit circle. Since the coefficients must be positive, we conclude that $D = Id$ thus $S = R$.
Explicitly, let $A = (a_{i,j})_{1 \le i,j \le n} \in \mathcal{H}_n^{>0}(\mathbb{C})$ and $R = (r_{i,j})_{1 \le i,j \le n} \in \mathbf{GL}_n(\mathbb{C})$ an upper-triangular matrix satisfying $A = R^*R$. For any $1 \le i, j \le n$, we have $a_{i,j} = \sum_{k=1}^{n} \overline{r_{k,i}} r_{k,j}$ but R is upper-triangular so $r_{k,l} = 0$ whenever $k > l$ thus $a_{i,j} = \sum_{k<l} \overline{r_{k,i}} r_{k,j} = \overline{r_{i,i}} r_{i,j} + \sum_{k=1}^{i-1} \overline{r_{k,i}} r_{k,j}$. Knowing the $(i-1)$-th first rows of L we can compute the i-th row (starting with the diagonal

element) :

$$r_{i,i} = \sqrt{a_{i,i} - \sum_{k=1}^{i-1} |r_{k,i}|^2} \quad \text{and} \quad r_{i,j} = \frac{1}{r_{i,i}} \left(a_{i,j} - \sum_{k=1}^{i-1} \overline{r_{k,i}} r_{k,j} \right), \quad i+1 \leq j. \tag{1}$$

The argument under the square root must be positive and we take the positive root. Notice that if A has real coefficients (if A is a real symmetric positive definite matrix) then its Cholesky factor R is a real matrix. □

1.3 The Lattice Isomorphism Problem

We give an overview of the Lattice Isomorphism Problem (LIP) for unstructured lattices. It will be stated in a lattice version and translated in terms of (positive definite) quadratic forms. This reformulation allows us to see any lattice $\mathcal{L} \subset \mathbb{R}^n$ as $\mathbb{Z}^n$, but with the geometry induced by the quadratic form. Also, moving to quadratic forms is convenient for cryptographic purposes. Indeed, starting from a quadratic form Q, the Discrete Gaussian Sampling (DGS, see Section 3.2.1) allows us to sample an equivalent form Q', the secret key then consists in the unimodular transformation between Q and Q' (Algorithm 1 of [12]). This is used to build cryptographic schemes (see the signature scheme of [12]) and prove, for example, worst-case to average-case reductions (Lemma 3.9 of [12]).

1.3.1 Equivalent formulations

Definition. Two lattices $\mathcal{L}$, $\mathcal{L}' \subset \mathbb{R}^n$ are isomorphic if there exists an orthonormal transformation $O \in \mathcal{O}_n(\mathbb{R})$ such that $\mathcal{L}' = O \cdot \mathcal{L} := \{O \cdot v \,|\, v \in \mathcal{L}\}$.

We have seen that the set of full rank n-dimensional lattices can be interpreted as $\mathbf{GL}_n(\mathbb{R})/\mathbf{GL}_n(\mathbb{Z})$. Let $\mathcal{L} = \mathcal{L}(B)$, $\mathcal{L}' = \mathcal{L}'(B')$ be two isomorphic lattices represented by bases $B, B' \in \mathbf{GL}_n(\mathbb{R})$. By definition, there exists an orthonormal transformation $O \in \mathcal{O}_n(\mathbb{R})$ such that OB is a basis of $\mathcal{L}'$. Then, there exists a unimodular transformation $U \in \mathbf{GL}_n(\mathbb{Z})$ such that $B' = OBU$. The Lattice isomorphism problem is precisely to find O and U *i.e.*, we want to reconstruct (or even test) equivalence in the double quotient $\mathcal{O}_n(\mathbb{R}) \setminus \mathbf{GL}_n(\mathbb{R}) / \mathbf{GL}_n(\mathbb{Z})$.

Definition (wc-sLIP^B)**.** For $B \in \mathbf{GL}_n(\mathbb{R})$ a basis of a lattice $\mathcal{L} \subset \mathbb{R}^n$, the worst-case search Lattice Isomorphism Problem with parameter B (wc-sLIP^B) is, given any isomorphic lattice $\mathcal{L}' \subset \mathbb{R}^n$ with basis $B' \in \mathbf{GL}_n(\mathbb{R})$, to find an orthonormal transformation $O \in \mathcal{O}_n(\mathbb{R})$ and a unimodular transformation $U \in \mathbf{GL}_n(\mathbb{Z})$ such that $B' = OBU$.

Quadratic form setting. Instead of working with bases, one can consider the Gram matrices associated; the idea is to work in the same double quotient but first considering $\mathcal{O}_n(\mathbb{R}) \setminus \mathbf{GL}_n(\mathbb{R})$. In fact, the map $\mathbf{GL}_n(\mathbb{R}) \to \mathcal{S}_n^{>0}(\mathbb{R})$; $B \mapsto Q = B^T B$ is surjective and the preimage of $B^T B$ is exactly $\mathcal{O}_n(\mathbb{R}) \cdot B$. Now if $B' = OBU$, with the notations above, then for $Q := B^T B$ and $Q' := B'^T B'$ we have :

$$Q' = U^T B^T O^T O B U = U^T Q U.$$

Definition. Two quadratic forms Q, $Q' \in \mathcal{S}_n^{>0}(\mathbb{R})$ are equivalent if their exists a unimodular $U \in \mathbf{GL}_n(\mathbb{Z})$ such that $Q' = U^T Q U$.

Definition (wc-sLIP^Q)**.** For a quadratic form $Q \in \mathcal{S}_n^{>0}(\mathbb{R})$, the worst-case search LIP problem with parameter Q (wc-sLIP^Q) is, given any equivalent quadratic form $Q' \in \mathcal{S}_n^{>0}(\mathbb{R})$, to find a unimodular transformation $U \in \mathbf{GL}_n(\mathbb{Z})$ such that $Q' = U^T Q U$.

Proposition 1.3. *Let $B \in \mathbf{GL}_n(\mathbb{R})$ and $Q = B^T B \in \mathcal{S}_n^{>0}(\mathbb{R})$. Then,* wc-sLIP^B *is equivalent to* wc-sLIP^Q*.*

Proof. Suppose we are given an oracle solving wc-LIP^Q (with $Q = B^T B$). For any B' in the same class as B in $\mathcal{O}_n(\mathbb{R}) \backslash \mathbf{GL}_n(\mathbb{R}) / \mathbf{GL}_n(\mathbb{Z})$, we get $U \in \mathbf{GL}_n(\mathbb{Z})$ using our oracle with $Q' = B'^T B'$ and $O := B'(BU)^{-1} \in \mathcal{O}_n(\mathbb{R})$ (check that $O^T O = (B^T)^{-1}(U^{-1})^T B'^T B' U^{-1} B^{-1} = \mathrm{Id}$) are such that $B' = OBU$. Converlsy, if we have an oracle solving wc-LIP^B and a quadratic form Q' equivalent to Q, we apply Cholesky decomposition to Q' and obtain B' such that $B'^T B' = Q'$. Then we call the oracle to get $O \in \mathcal{O}_n(\mathbb{R})$ and $U \in \mathbf{GL}_n(\mathbb{Z})$ which verify $B' = OBU$ so $Q' = U^T Q U$. □

Finally we define the decision problem associated to LIP. In pratice, this problem is used to build cryptographic schemes, see for example the Zero Knowledge Proof of Knowledge, Key Encapsulation Mechanism and Signature schemes in [12].

Definition (wc-Δ-LIP^{Q_0,Q_1})**.** For two quadratic forms Q_0, $Q_1 \in \mathcal{S}_n^{>0}$ the worst-case distinguishing Lattice Isomorphism Problem (wc-Δ-LIP^{Q_0,Q_1}) with parameters Q_0, Q_1 is, given any quadratic form $Q \in \mathcal{S}_n^{>0}$ equivalent to Q_b (for some b in $\{0,1\}$), to find b.

1.3.2 Invariants for Δ-LIP

A general method to help deciding whether Q is equivalent to Q_0 or to Q_1 is to compute invariants *i.e.*, quantities related to Q which are constant on the equivalence class $[Q]$. On the other side, to make Δ-LIP hard enough, Q_0 and Q_1 must share « many » invariants.

Arithmetic invariants. We can first discuss the problem of finding whether or not two quadratic rational forms Q_0, Q_1 are equivalent over $\mathbb{Q}$ (*i.e.*, if there exists $P \in \mathbf{GL}_n(\mathbb{Q})$ such that $Q_1 = P^T Q_0 P$). The answer is given by Hasse-Minkowsi theorem which states that this occurs if and only if the forms have a common list of arithmetic invariants. Namely, their signature must be the same (in our setting this is always verified, as we consider positive definite forms) as well as their discriminant. For any prime number p, we associate a p-adic invariant to $Q_b = (q_{i,j}^b)_{1 \le i,j \le n}$ ($b \in \{0, 1\}$), called the Cassel-Hasse invariant at p, and defined with Hilbert symbols : $\varepsilon_p(Q_b) = \prod_{i<j} (a_i, a_j)_p$ where $a_i = e_i^T Q e_i$, $\{e_i\}_i$ is any orthogonal basis for Q_b and $(\cdot,\cdot)_p$ denotes the Hilbert symbol at p.

Theorem 1.4 (Hasse-Minkowski, [31])**.** *Q_0, Q_1 are equivalent over $\mathbb{Q}$ if and only if they are over $\mathbb{R}$ and $\mathbb{Q}_p$ for any prime p, if and only if they have same signature, discriminant and $\varepsilon(Q_0)_p = \varepsilon(Q_1)_p$ for any prime p.*

These invariants can be efficiently computed (see [10]). In Δ-LIP we consider integrally equivalent forms (*i.e.*, with $P \in \mathbf{GL}_n(\mathbb{Z})$), this condition is more restrictive than equivalence

over the rationals, and we only have a partial answer given by a list of arithmetic invariants. Observe that the quantity $\gcd(Q_0) := \gcd\{q_{i,j}^0\}_{1\leq i,j\leq n}$ is an invariant, as well as the parity $\mathrm{par}(Q_0) \in \{1,2\}$ defined by $\gcd\{x^T Q_0 x \,|\, x \in \mathbb{Z}^n\} = \mathrm{par}(Q_0) \cdot \gcd(Q_0)$.
Indeed, any coefficient $q_{i,j}^1$ of Q_1 can be written as $\varepsilon_i^T Q_1 \varepsilon_j$ where $\varepsilon_i = (\delta_{i,k})_k$ so it is an integral combination of the $q_{i,j}^0$ thus $\gcd(Q_0) \mid \gcd(Q_1)$. Since P is invertible, the argument is symmetrical and we get $\gcd(Q_0) = \gcd(Q_1)$. Writing $x^T Q_0 x = \sum_i q_{i,i}^0 x_i^2 + 2\sum_{i\neq j} x_j q_{i,j}^0 x_i$, we see that $\gcd(Q_0) \mid \gcd\{x^T Q_0 x \,|\, x \in \mathbb{Z}^n\}$ and $2q_{i,j}^0 = (\varepsilon_i + \varepsilon_j)^T Q_0 (\varepsilon_i + \varepsilon_j) - \varepsilon_i^T Q_0 \varepsilon_i - \varepsilon_j^T Q_0 \varepsilon_j$ so $\gcd\{x^T Q_0 x \,|\, x \in \mathbb{Z}^n\} \mid 2\gcd(Q_0)$ thus $\mathrm{par}(Q_0) \in \{1,2\}$ is well-defined. The quantities $\gcd\{x^T Q_0 x \,|\, x \in \mathbb{Z}^n\}$ and $\gcd\{x^T Q_1 x \,|\, x \in \mathbb{Z}^n\}$ are equal because P is invertible, thus $\mathrm{par}(Q_0)$ is an invariant. The following list is a (partial) system of invariants.

$$\mathrm{ari}(Q) = (\det(Q), \gcd(Q), \mathrm{par}(Q), [Q]_{\mathbb{Q}}, ([Q]_{\mathbb{Z}_p})_p).$$

Each of them are efficiently computable so we must take care that $\mathrm{ari}(Q_0) = \mathrm{ari}(Q_1)$ when instantiating Δ-LIP.

Geometric invariants. Isomorphic lattices have the same successive minima $\lambda_1, \ldots, \lambda_n$ and the sets of lattice vectors with same length are in bijection. All these geometric invariants are caught in the (formal) Theta-series

$$\Theta_{\mathcal{L}}(z) := \sum_{l\geq 0} N_l z^l,$$

with $N_l = |\{y \in \mathcal{L} \,|\, y^T y = l\}| = |\{x \in \mathbb{Z}^n \,|\, x^T Q x = l\}|$, and where $B \in \mathbf{GL}_n(\mathbb{Z})$ is any basis of $\mathcal{L}$ and $Q = B^T B \in \mathcal{S}_n^{>0}(\mathbb{Z})$.

In practice, the Theta-series and all the quantities it involves are hard to compute. It requires enumerating short vectors. Assuming $\lambda(Q_0) < \lambda(Q_1)$ and $\gamma := \lambda(Q_1)/\lambda(Q_0)$, then solving Δ-LIP is no harder than γ-**SVP**, this is the hardness conjecture made in [12].

1.3.3 State-of-the-art for computing isometries

Haviv-Regev algorithm. An algorithm due to Haviv and Regev (see [16]) solves the task of computing all isometries between two isomorphic lattices (which is harder than solving search-LIP) with complexity $n^{O(n)}$. This running time is moreover optimal, up to a constant in the exponent. Indeed, isometries of $\mathcal{L} = \mathbb{Z}^n$ to itself are made of all the permutations of the canonical basis vectors and sign change which gives $2^n n! = n^{O(n)}$ isometries. However, the question of finding a more efficient algorithm solving search-LIP is still open.

The principle is a refinement of the « naive » method : enumerate enough short independents vectors in both lattices and then compute isometries matching pairs of vectors with same norm. The first part is related to the Shortest Vector Problem (SVP), which can be solved in time $2^{\widetilde{O}(n)}$. The second part consists in finding an isomorphism between graphs (whose vertices are the short vectors and the edges are the scalar products between them) preserving edges, known as Graph Isomorphism Problem (GIP), and has running time $2^{O((\log m)^3)}$ ([17]) where m is the number of vertices. In the case where there is a unique shortest vector (up to sign) *i.e.*, $\lambda_1(\mathcal{L}) < \lambda_2(\mathcal{L})$, this gives only two possibilities to define its image by an isometry.

Then projecting the lattice to the orthogonal space of this vector, we see that the problem can be solved recursively so the worst-case appears when $\mathcal{L}$ has a lot of shortest vectors. This number, known as *kissing number*, could be huge (always upper-bounded by 2^{n+1}) but in general one would expect it to be quite small.

In [16], the authors use a trick to produce all sets of linearly independent short vectors in $\mathcal{L}_1$ and $\mathcal{L}_2$, using dual lattices and the isolation lemma (Theorem 4.2 of [16]). Given a lattice $\mathcal{L}$, its dual is the lattice defined by $\mathcal{L}^* := \{u \in \mathbb{R}^n \,|\, \forall\, v \in \mathcal{L},\ \langle u, v\rangle \in \mathbb{Z}\}$. Consider the special case where $\lambda_1 = \lambda_2 = \cdots = \lambda_n$. The algorithm enumerates sets $A_i \subset \mathcal{L}_i$ of shortest lattices vectors and $W_i \subset \mathcal{L}_i^*$ of lattices vectors with norm less than $5n^{17/2} \cdot \lambda_1(\mathcal{L}_i^*)$ ($i \in \{1, 2\}$). The running time of this step is $(5n^{17/2} \cdot n)^{O(n)} = n^{O(n)}$, using Corollary 2.16 of [16], and the sets have size $|A_i| = 2^{O(n)}$, $|W_i| = n^{O(n)}$. Each vector $w_1 \in W_1$ uniquely defines n linearly independent lattice vectors $x_1, \ldots, x_n \in \mathcal{L}_1$, *via* the isolation lemma. Similarly for any $w_2 \in W_2$, we get lattice vectors $y_1, \ldots, y_n \in \mathcal{L}_2$, and we check if the linear transformation O mapping x_i on y_i is orthogonal. The claim is that this method reaches every orthogonal linear transformation that maps $\mathcal{L}_1$ to $\mathcal{L}_2$. For the general case, we compute the vector spaces $V_1 = \mathrm{span}(A_1)$, $V_2 = \mathrm{span}(A_2)$ (they must have the same dimension otherwise the lattices are not isomorphic) and we apply the previous special case to $\mathcal{L}_1 \cap V_1$ and $\mathcal{L}_2 \cap V_2$. Then we call recursively this step to the projected lattices $\pi_{V_i^\perp}(\mathcal{L}_i)$ (orthogonal projection to $V_i^\perp$).

Plesken-Souvignier algorithm. Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice with basis $B = (b_1, \ldots, b_n)$ and equipped with a positive definite bilinear form Φ (one may think of Φ as the canonical scalar product on $\mathbb{R}^n$). In [28] is presented a method to compute automorphisms of $\mathcal{L}$ *i.e.*, linear transformations $\theta : \mathbb{R}^n \to \mathbb{R}^n$ such that $\theta(\mathcal{L}) = \mathcal{L}$ and $\Phi(\theta(b_i), \theta(b_j)) = \Phi(b_i, b_j)$ for every $1 \leq i, j \leq n$. Let $F = (f_{i,j})_{1 \leq i,j \leq n}$ be the Gram matrix of Φ in the basis B (if $\Phi = \langle \cdot\,, \cdot \rangle_{\mathrm{E}}$, $F = B^T B$ is the usual Gram matrix associated to B).

We call k-partial automorphism any tuple $(v_1, \ldots, v_k) \in \mathcal{L}^k$ satisfying $\Phi(v_i, v_j) = \Phi(b_i, b_j)$ for every $1 \leq i, j \leq k$. It is clear that any n-partial automorphism defines an automorphism of $\mathcal{L}$ by $\theta : b_i \mapsto v_i$ and conversely the image vectors of B by any automorphism θ satisfy the inner product conditions. Let S be the finite set of lattice vectors v such that $\Phi(v, v) \leq \max_{i \in \{1,\ldots,n\}}\{f_{i,i}\}$ (think of S as a set of short vectors, it is efficiently enumerable). Not every k-partial automorphism can be extended to a $(k+1)$-automorphism and the idea is to reject partial automorphism which can't be extended as soon as possible, using backtrack informations[2]. This is done using two quantities efficiently computable for any partial automorphism and invariant by automorphism. Then we compute these data for the trivial automorphism $\theta = id$ with k-partial automorphisms $\{(b_1, \ldots, b_k)\}_k$ and compare for each non-trivial partial automorphism $(v_1, \ldots, v_k)$. If it coincides, we extend and keep on, if not, we reject it.

For the first invariant, notice that the number of extensions of a k-partial automorphism is preserved by the automorphism of $\mathcal{L}$[3], so the algorithm first computes the number of extensions of the trivial k-partial automorphism $(b_1, \ldots, b_k)$. More precisely, the fingerprint

[2] It is reasonably easy to check if a partial automorphism can be extended.

[3] For any automorphism θ of $\mathcal{L}$, there are the same number of extensions of $(b_1, \ldots, b_k)$ as $(\theta(b_1), \ldots, \theta(b_k))$.

of B is the upper-triangular matrix $f = (f_{k,i})_{1\leq k,i\leq n}$ defined by $f_{k,i} = 0$ if $i < k$ and $f_{k,i} = |\{v \in S \,|\, \Phi(v,v) = f_{k,k} \text{ and } \Phi(v,b_j) = f_{k,j},\ \forall j \leq i-1\}|$ otherwise. So $f_{k,i}$ counts the number of extensions of $(b_1,\ldots,b_{i-1})$ to a i-partial automorphism $(b_1,\ldots,b_{i-1},v)$ with $\Phi(v,v) = f_{k,k}$ and the fingerprint matrix f stores all these numbers. One may reorder the basis B such that the diagonal elements of the fingerprint matrix are minimal among the coefficients of their own row ; smaller coefficients lead to fewer possible extensions of partial automorphisms. This operation can be done while computing the fingerprint matrix : after computing each k-th row of the fingerprint, test if the entry $f_{k,k}$ is the minimal non-zero entry in the row. If so, we do nothing. Otherwise, we swap the k-th column of the fingerprint with any column containing the minimal non-zero entry in the row involved. From this results a test to know if a k-partial automorphism $(v_1,\ldots,v_k)$ can be extended.

However, the test of the fingerprint alone may not detect early enough dead ends so we use a second invariant, based on vector sums. Let $\underline{v} = (v_1,\ldots,v_k)$ be a k-partial automorphism of $\mathcal{L}$ and $s = (s_1,\ldots,s_k) \in \mathbb{Z}^k$, we define $X_s(\underline{v}) := \{v \in S \,|\, \Phi(v,v_i) = s_i,\ \forall i \leq k\}$. It is a finite set (as S is finite) and the vector sum of $\underline{v}$ with respect to s is $\overline{X}_s(\underline{v}) := \sum_{v\in X_s(\underline{v})} v \in \mathcal{L}$. Then, one can check that for any automorphism θ of $\mathcal{L}$, we have equality $\theta(\overline{X}_s(b_1,\ldots,b_k)) = \overline{X}_s(\theta(b_1),\ldots,\theta(b_k))$. Thus, it provides a second test for a partial automorphism to be extended. This step requires the computation of vector sums for $(b_1,\ldots,b_k)$ $(1 \leq k \leq n)$. Plesken-Souvignier algorithm can be adapted to compute (one or all) isometries between two isomorphic lattices $(\mathcal{L}_1,\Phi_1)$ and $(\mathcal{L}_2,\Phi_2)$ (*e.g.*, with $\Phi_1 = \Phi_2 = \langle\cdot,\cdot\rangle_{\mathrm{E}}$). Once given an isometry $\omega : \mathcal{L}_1 \to \mathcal{L}_2$, the set of all isometries is given by $\{\omega\circ\theta \,|\, \theta \text{ is an isometry of } \mathcal{L}_1\}$. It needs a lot of precomputation such as the set S of short vectors so the overall method runs in exponential time. For all details we refer to [28] and [2].

2 Algebraic Number Theory Background

2.1 Reminder on number fields

In this section we recall some general properties of number fields *i.e.*, finite extensions of $\mathbb{Q}$ (with a special attention to cyclotomic power of 2 extensions, which are the number fields commonly used in cryptography). Most of the proofs can be found in [30] and [23]. For our purposes, fundamental results on Dedekind rings are stated only in the special case of ring of integers. Complex embeddings and Minkowski embedding play a key role as they allow us to see rings of integers as lattices (and more generally any projective module of finite type over a ring of integers, see the next section). Let K be a number field of degree n over $\mathbb{Q}$, and L/K a finite extension of degree m.

2.1.1 Integral extensions

Recall that the ring of integers of K is the set of elements of K which are annihilated by a monic polynomial with coefficients in $\mathbb{Z}$, it is a Dedekind ring denoted $\mathcal{O}_K$. The inclusion $\mathcal{O}_K \subset \mathcal{O}_L$ is an extension of Dedekind rings and the integral closure of $\mathcal{O}_K$ in L is precisely $\mathcal{O}_L$.

Proposition 2.1 (Théorème 1 and Corollaire, §2.7 of [30])**.** *$\mathcal{O}_L$ is a sub-$\mathcal{O}_K$-module of a free rank m module over $\mathcal{O}_K$. Moreover, if $\mathcal{O}_K$ is a PID, then $\mathcal{O}_L$ is free of rank m over $\mathcal{O}_K$.*

Definition. A consequence of this proposition is that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. A basis of $K/\mathbb{Q}$ made of elements of $\mathcal{O}_K$ is called an integral basis of $K/\mathbb{Q}$.

Example. For a power-of-two cyclotomic extension, namely $L = \mathbb{Q}[X]/(X^n + 1)$ with n a power of two,[4] its ring of integers is $\mathcal{O}_L = \mathbb{Z}[X]/(X^n + 1)$ (this is a general result for cyclotomic fields, see Theorem 4, IV, §1 of [20]) so $\{1, \zeta, \ldots, \zeta^{n-1}\}$ is an integral basis of $L/\mathbb{Q}$. The subfield $K = \mathbb{Q}[\zeta + \zeta^{-1}]$ is such that L/K is quadratic. It is called the maximal real subfield of L. For our purposes, we will use the fact that $\mathcal{O}_K = \mathbb{Z}[\zeta + \zeta^{-1}]$ (this comes from a general result on integral bases of the maximal real subfield of a cyclotomic field, see [22] or [38] for a proof).

Remark. In general $\mathcal{O}_K$ is not a PID and $\mathcal{O}_L$ is not free over $\mathcal{O}_K$. However, by Proposition 2.1, it is a finite $\mathcal{O}_K$-module. In Section 2.2.1, we will see that $\mathcal{O}_L$ is « almost » free over $\mathcal{O}_K$, in the sense that there always exists a pseudo-basis.

Theorem 2.1. *Every ideal $\{0\} \neq \mathfrak{a} \subset \mathcal{O}_K$ can be uniquely written (up to permutation of the factors) as a product*

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i},$$

where the $\mathfrak{p}_i$'s are pairwise distinct maximal ideals of $\mathcal{O}_K$ (these are exactly the maximal ideals containing $\mathfrak{a}$) and $\alpha_i \geq 1$.

Definition. With the notations of the theorem above, for any $1 \leq i \leq r$, $\mathfrak{p}_i \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ so it is equal to $p_i\mathbb{Z}$ for some prime integer p_i. Thus, $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p}$ is a finite extension of fields, whose degree is called the residual degree at $\mathfrak{p}_i$ and is denoted f_i.

[4] If n is a power of two, $X^n + 1$ is the $2n$-th cyclotomic polynomial. In particular it is irreducible over $\mathbb{Q}$ and has degree n.

Proposition 2.2 (Lemme 3.1.32 and Corollaire 3.1.33 of [23]).
1) Let $\mathfrak{a} \subset \mathcal{O}_K$ be a non trivial ideal. Then, any ideal of $\mathcal{O}_K/\mathfrak{a}$ is principal.
2) Every ideal of $\mathcal{O}_K$ is generated by at most two elements.

Fractional ideals. A fractional ideal $\mathfrak{a}$ of K is a sub-$\mathcal{O}_K$-module of K such that there exists $d \in \mathcal{O}_K$ satisfying $d\mathfrak{a} \subset \mathcal{O}_K$. Equivalently, $\mathfrak{a}$ is a fractional ideal of K if and only if there exists $\alpha \in K$ and $I \subset \mathcal{O}_K$ an ideal such that $\mathfrak{a} = \alpha I$. We denote by $I(\mathcal{O}_K)$ the set of fractional ideal of K. Endowed with the multiplication of ideals, it is a commutative monoid. For any fractional ideal $\mathfrak{a}$ of K we define

$$\mathfrak{a}^{-1} := \{x \in K \,|\, x\mathfrak{a} \subset \mathcal{O}_K\}.$$

It is a fractional ideal of K and we have $\mathfrak{a}\mathfrak{a}^{-1} \subset \mathcal{O}_K$.

Proposition 2.3. *$I(\mathcal{O}_K)$ is a commutative group and the inverse of $\mathfrak{a} \in I(\mathcal{O}_K)$ is $\mathfrak{a}^{-1}$. Every fractional ideal $\mathfrak{a} \neq \{0\}$ of K can be uniquely written (up to permutation of the factors) as a product*

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i},$$

where the $\mathfrak{p}_i$'s are pairwise distinct maximal ideals of $\mathcal{O}_K$ and $\alpha_i \in \mathbb{Z} \setminus \{0\}$.

Proof. See Lemme 3.1.15 and Corollaire 3.1.18 in [23]. □

Definition. With the notations of the proposition above and for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the $\mathfrak{p}$-adic valuation of $\mathfrak{a}$, denoted $v_\mathfrak{p}(\mathfrak{a})$, is the integer $\alpha_i \in \mathbb{Z}$ if $\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ and equal to 0 otherwise.

2.1.2 Embeddings and norms

Embeddings. Any number field K is isomorphic to $\mathbb{Q}(\theta)$ for some $\theta \in \mathbb{C}$, this is the primitive element theorem. In particular if K has degree n, it comes naturally with n embeddings $K \to \mathbb{C}$ corresponding to the conjugates of θ. Any embedding $\sigma : K \to \mathbb{C}$ such that $\sigma(K) \subset \mathbb{R}$ (resp. $\sigma(K) \not\subset \mathbb{R}$) is called a real embedding (resp. a complex embedding). Any complex embedding σ comes with another distinct embedding $\overline{\sigma}$. We denote by n_1 the number of real embeddings and n_2 the number of complex embeddings up to complex conjugation, so that $n = n_1 + 2n_2$. The pair (n_1, n_2) is called the signature of K. For any pair of conjugate complex embeddings we fix arbitrarly one of them. Embeddings are numbered as follow : $\sigma_1, \ldots, \sigma_{n_1}$ are the real embeddings and $\sigma_{n_1+1}, \ldots, \sigma_{n_1+n_2}, \overline{\sigma_{n_1+1}}, \ldots, \overline{\sigma_{n_1+n_2}}$ are the complex embeddings.

Example. Let $\zeta \in \mathbb{C}$ be a primitive n-th root of unity ($n \geq 3$), then the cyclotomic field $K = \mathbb{Q}(\zeta)$ has degree $\varphi(n)$ and signature $(0, \varphi(n)/2)$. The sub-extension $K' = \mathbb{Q}(\zeta + \zeta^{-1})$ has degree $\varphi(n)/2$ and signature $(\varphi(n)/2, 0)$.

Trace, norm and discriminant Let $x \in L$ and $[x]$ the map $L \to L$ corresponding to the multiplication by x. It is a K-linear morphism of L.

Definition. The trace (resp. the norm) of x over K is $Tr_{L/K}(x) := Tr([x])$ (resp. $N_{L/K}(x) :=$

$\det([x])$). This is well defined *i.e.*, the definition does not depend on a K-basis of L (by general properties of the trace and determinant) but just on the extension L/K.

Remark. The norm over $\mathbb{Q}$ is called the algebraic norm. When an extension of number fields L/K is fixed, we refer to $N_{L/K}$ as the relative norm.

Lemma 2.1. *$Tr_{L/K} : L \to K$ is K-linear, $N_{L/K} : L \to K$ is multiplicative and $N_{L/K}(ax) = a^m N_{L/K}(x)$ for any $a \in K$. Also, if $L/F/K$ is a tower of number fields, then*

$$Tr_{L/K} = Tr_{F/K} \circ Tr_{L/F} \quad \textit{and} \quad N_{L/K} = N_{F/K} \circ N_{L/F}.$$

Proof. The non-trivial result is the last formula for the norms, see [7], III, §9, n°4, Prop 6. □

Lemma 2.2 (Théorème 2.2.17 of [23])**.** *For any $x \in L$,*

$$Tr_{L/K}(x) = \sum_{\sigma \in \mathrm{Isom}_K(L, \overline{\mathbb{Q}})} \sigma(x) \quad \textit{and} \quad N_{L/K}(x) = \prod_{\sigma \in \mathrm{Isom}_K(L, \overline{\mathbb{Q}})} \sigma(x),$$

where the sum and product are taken over the embeddings σ of L fixing K pointwise.

Remarks. • Suppose L/K is Galois and F/K is a sub-extension, then the restriction map $\mathrm{Gal}(L/K) \to \mathrm{Isom}_K(F, \overline{K})$ is surjective and each $\tau \in \mathrm{Isom}_K(F, \overline{K})$ has $[L : F]$ pre-images. The lemma can be first proved when L/K is Galois, see [23].

• For $K = \mathbb{Q}$, the sum and product are indexed over all the embeddings of L.

Proposition 2.4 (Propositions 2.2.9, 2.2.14 and 5.1.2 of [23])**.** *Let $x \in L$ and $m_{x,K}(X) \in K[X]$ its minimal polynomial over K. Then, $x \in \mathcal{O}_L$ if and only if $m_{x,K}(X) \in \mathcal{O}_K[X]$. In particular if $x \in \mathcal{O}_L$, then $Tr_{L/K}(x) = [L : K(x)] Tr_{K(x)/K}(x)$ and $N_{L/K}(x) = N_{K(x)/K}(x)^{[L:K(x)]}$ are elements of $\mathcal{O}_K$. Also, if $x \in \mathcal{O}_L$ then x is invertible if and only if $N_{L/\mathbb{Q}}(x) = \pm 1$.*

Proof. If $x \in \mathcal{O}_L$, all its conjugates are also in $\mathcal{O}_L$ so by Viète formulae (and because $m_x(X)$ is monic), the coefficients of $m_x(X)$ are in $\mathcal{O}_K$. The converse is clear.
Since $Tr_{K[x]/K}(x)$ and $N_{K[x]/K}(x)$ are, up to the sign, coefficients of $m_x(X)$, this gives the second part of the proposition. If $x \in \mathcal{O}_L$ is invertible with inverse y, then $1 = N_{L/\mathbb{Q}}(xy) = N_{L/\mathbb{Q}}(x) N_{L/\mathbb{Q}}(y)$ is a product in $\mathbb{Z}$, so $N_{L/\mathbb{Q}}(x) = \pm 1$. Conversely if $x \in \mathcal{O}_L$ has norm ± 1, then evaluating $m_{x,\mathbb{Q}}(X)$ in x gives a relation $x(x^{m-1} + a_{m-1}x^{m-2} + \cdots + a_1) = -a_0 = \pm N_{K/\mathbb{Q}}(x) = \pm 1$, so x is invertible in $\mathcal{O}_L$. □

Definition. Let $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n)$ be an integral basis of K, the number $\det(Tr_{K/\mathbb{Q}}(\varepsilon_i \varepsilon_j)_{1 \le i,j \le n}) \in \mathbb{Z}$ is independant of the choice of the basis ε. It is called the discriminant of K and is denoted Δ_K.

Proposition 2.5. *For any integral basis $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n)$ of K, we have*

$$\Delta_K = \det(\sigma_i(\varepsilon_j)_{1 \le i,j \le n})^2.$$

In particular, $\Delta_K \neq 0$.

Proof. See [30], §2.7, Proposition 3. □

Algebraic norm of an ideal.

Lemma 2.3 (and definition)**.** *Let $\mathfrak{a} \subset \mathcal{O}_K$ be a non trivial ideal, then the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite. The absolute norm of I is defined by $N_{K/\mathbb{Q}}(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$.*

Proof. Let $b \in \mathfrak{a}\backslash\{0\}$. Its minimal polynomial over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$, say $m_b(X) = X^m + a_{m-1}X^m + \cdots + a_1X + a_0$ with $a_i \in \mathbb{Z}$ and $a_0 \neq 0$. Then, $a_0 = -(b^m + a_{m-1}b^m + \cdots + a_1 b) \in \mathfrak{a}$ so the ideal $a_0\mathcal{O}_K$ is contained in the kernel of the canonical projection $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}$. It induces a surjective morphism $\mathcal{O}_K/a_0\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}$. By proposition 2.1, there is an isomorphism $\mathcal{O}_K \simeq \mathbb{Z}^n$ thus the composition

$$\mathbb{Z}^n/a_0\mathbb{Z}^n \simeq \mathcal{O}_K/a_0\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}$$

is surjective. The left term is finite (it has a_0^n elements) so $\mathcal{O}_K/\mathfrak{a}$ must be finite. □

Lemma 2.4. *Let $\mathfrak{p} \subset \mathcal{O}_K$ be a non trivial prime ideal of $\mathcal{O}_K$ and p the prime integer such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Then, for any positive integer r,*

$$N_{K/\mathbb{Q}}(\mathfrak{p}^r) = p^{r f_\mathfrak{p}},$$

where $f_\mathfrak{p} = [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$ is the degree of the residual extension.

Proof. We proceed by induction on r. The case $r = 1$ is trivial and if $r \geq 2$, then the canonical surjection $\mathcal{O}_K/\mathfrak{p}^r \to \mathcal{O}_K/\mathfrak{p}^{r-1}$ has kernel $\mathfrak{p}^r/\mathfrak{p}^{r-1} \simeq \mathcal{O}_K/\mathfrak{p}$ which cardinal is $p^{f_\mathfrak{p}}$. □

Proposition 2.6. *1) Let $\mathfrak{a} \subset \mathcal{O}_K$ be a non-trivial ideal and $\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$ its prime decomposition. Denote by p_i the prime integer such that $\mathfrak{p}_i \cap \mathbb{Z} = p_i\mathbb{Z}$ and f_i the degree of the residual extension at $\mathfrak{p}_i$. Then,*

$$N_{K/\mathbb{Q}}(\mathfrak{a}) = \prod_{i=1}^r p_i^{e_i f_i}.$$

2) (The absolute norm is multiplicative) Let $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ be two non trivial ideal. Then,

$$N_{K/\mathbb{Q}}(\mathfrak{ab}) = N_{K/\mathbb{Q}}(\mathfrak{a})N_{K/\mathbb{Q}}(\mathfrak{b}).$$

Proof. 1) The $\mathfrak{p}_i$'s are pairwise distinct so the Chinese remainder theorem gives $\mathcal{O}_K/\mathfrak{a} \simeq \prod_{i=1}^r \mathcal{O}_K/\mathfrak{p}_i^{e_i}$. Taking the cardinal and applying the previous lemma, we obtain the result.
2) Decompose $\mathfrak{a}, \mathfrak{b}$ in product of prime ideals and apply 1). □

Relative norm of an ideal. Recall that fractional ideals of K form a group $I(\mathcal{O}_K)$. There is a notion of relative norm for ideals which generalizes the algebraic norm. As stated by Serre in [32], we consider the map $N_{L/K} : I(\mathcal{O}_L) \to I(\mathcal{O}_K)$ defined for prime ideals $\mathfrak{q} \subset \mathcal{O}_L$ by

$$N_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f_\mathfrak{q}},$$

where $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$ and $f_\mathfrak{q} := [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$. It is then extended by multiplicativity to $I(\mathcal{O}_L)$.

Proposition 2.7 (« Compléments sans démonstrations » [30]). *Let $L/F/K$ be a tower of number fields.*
1) $N_{L/K} : I(\mathcal{O}_L) \to I(\mathcal{O}_K)$ is multiplicative.
2) Let $\mathfrak{a} \in I(\mathcal{O}_L)$, then $N_{L/K}(\mathfrak{a})$ is the (fractional) ideal of $\mathcal{O}_K$ generated by $\{N_{L/K}(x) \,|\, x \in \mathfrak{a}\}$.
3) For any $x \in L$, $N_{L/K}(x\mathcal{O}_L) = N_{L/K}(x)\mathcal{O}_K$.
4) Let $\mathfrak{a} \subset \mathcal{O}_K$, then $N_{L/K}(\mathfrak{a}\mathcal{O}_L) = \mathfrak{a}^{[L:K]}$.
5) If $K = \mathbb{Q}$ and $\mathfrak{a} \subset \mathcal{O}_K$ is non trivial, $N_{K/\mathbb{Q}}(\mathfrak{a})$ is the ideal of $\mathbb{Z}$ generated by $|\mathcal{O}_K/\mathfrak{a}|$.
6) For any (fractional) ideal $\mathfrak{a}$ of $\mathcal{O}_L$, $N_{L/K}(\mathfrak{a}) = N_{F/K}(N_{L/F}(\mathfrak{a}))$.

Remark. For a proof of this proposition, we refer to [34] where the notion of module index is discussed. Our relative norm for ideals in number fields is just a special case of module index. Namely, if A is a Dedekind ring with fraction field K, suppose we have two finitely generated A-modules M, N which span the same K-vector space V and $\mathfrak{p}$ is any prime ideal of A, then $M_\mathfrak{p}$ and $N_\mathfrak{p}$ are isomorphic $A_\mathfrak{p}$-modules (which is a PID). It extends to a unique K-automorphism φ of V. Module indices are fractional ideals defined by

$$(M_\mathfrak{p} : N_\mathfrak{p})_{A_\mathfrak{p}} := (\det \varphi)A \quad \text{and} \quad (M : N)_A := \bigcap_\mathfrak{p} (M_\mathfrak{p} : N_\mathfrak{p})_{A_\mathfrak{p}}.$$

For example if $A = \mathbb{Z}$ and $N \subset M$, then $(M : N)_\mathbb{Z}$ is the usual index $(M : N) = |M/N|$. We recover a relative norm for ideals in number fields L/K by considering the morphism $I(\mathcal{O}_L) \to I(\mathcal{O}_K)$; $\mathfrak{a} \mapsto (\mathcal{O}_L : \mathfrak{a})_{\mathcal{O}_K}$ (this is well defined even if $\mathfrak{a}$ is not integral).

2.2 Minkowski theory

Combining the n embeddings of K there is a natural embedding from K to $\mathbb{C}^n$ called Minkowski embedding (or canonical embedding) of K. It will allow us to see any (finitely generated and torsion-free) module over $\mathcal{O}_K$ as a lattice.

Definition. The following map is called the Minkoswki embedding of K.

$$\begin{aligned} \mu : K &\longrightarrow \mathbb{C}^n \\ x &\longmapsto (\sigma_1(x), \dots, \sigma_n(x)). \end{aligned}$$

2.2.1 The Minkowski space $K_\mathbb{R}$.

The real vector-space generated by the image of K via Minkowski embedding is called the Minkowski space and it is denoted $K_\mathbb{R}$.

$$K_\mathbb{R} := \Big\{ z = (z_i)_i \in \mathbb{C}^n \,|\, z_1, \dots, z_{n_1} \in \mathbb{R},\ \overline{z_{n_1+i}} = z_{n_1+n_2+i},\ (1 \le i \le n_2) \Big\}.$$

It is a ring containing $\mu(K)$, endowed with component-wise multiplication, but not an integral domain. Depending on the context, elements of K will be identified with their images in $K_\mathbb{R}$. Also, $K_\mathbb{R}$ is naturally isomorphic to $\mathbb{R}^n$ thanks to the map

$$\begin{aligned} f \,:\, K_\mathbb{R} &\longrightarrow \mathbb{R}^n \\ z = (z_i)_i &\longmapsto (x_i)_i \end{aligned}$$

defined by $(x_i)_i = (z_1, \dots, z_{n_1}, \sqrt{2}\Re(z_{n_1+1}), \sqrt{2}\Im(z_{n_1+1}), \dots, \sqrt{2}\Re(z_{n_1+n_2}), \sqrt{2}\Im(z_{n_1+n_2}))$. There is a scalar product $\langle \cdot, \cdot \rangle_{\mathbb{K}_\mathbb{R}} : K_\mathbb{R} \times K_\mathbb{R} \to \mathbb{R}$ on $K_\mathbb{R}$ induced by the canonical Hermitian form on $\mathbb{C}^n$ for which $f : (K_\mathbb{R}, \langle \cdot, \cdot \rangle_{\mathbb{K}_\mathbb{R}}) \to (\mathbb{R}^n, \langle \cdot, \cdot \rangle_\mathrm{E})$ is an isometry (where $\langle \cdot, \cdot \rangle_\mathrm{E}$ is the Euclidean scalar product on $\mathbb{R}^n$). To any $z = (z_i)_i \in K_\mathbb{R}$ we associate its complex conjugate $\bar{z}$ by taking complex conjugates component-wise. The trace map on $K_\mathbb{R}$ is the $\mathbb{R}$-linear map :

$$\begin{aligned} Tr \ : \ K_\mathbb{R} &\longrightarrow \mathbb{R} \\ z = (z_i)_i &\longmapsto z_1 + \cdots + z_n \end{aligned}$$

Finally, remark that the composition $Tr \circ \mu$ on K is the usual trace $Tr_{K/\mathbb{Q}}$.

Lemma 2.5. *For any $x, y \in K_\mathbb{R}$, we have*

$$\langle f(x), f(y) \rangle_\mathrm{E} = Tr(x\overline{y}) = Tr(\overline{x}y).$$

Proof. Observe that for any $s, t \in \mathbb{C}$, $s\bar{t} + \bar{s}t = 2(\Re(s)\Re(t) + \Im(s)\Im(t))$.
Let $x = (x_i)_i, \ y = (y_i)_i \in K_\mathbb{R}$. By definition of f,

$$\begin{aligned} \langle f(x), f(y) \rangle_\mathrm{E} &= \sum_{i=1}^{n_1} x_i y_i \ + \sum_{i=n_1+1}^{n_1+n_2} 2(\Re(x_i)\Re(y_i) + \Im(x_i)\Im(y_i)) \\ &= \sum_{i=1}^{n_1} x_i y_i \ + \sum_{i=n_1+1}^{n_1+n_2} x_i\overline{y_i} \ + \ \overline{x_i\overline{y_i}} \\ &= Tr(x\overline{y}). \end{aligned}$$

The second equality follows from the symmetry of $\langle \cdot, \cdot \rangle_E$. □

An element $z = (z_i)_i \in K_\mathbb{R}$ is invertible if and only if $z_i \neq 0$ for all $1 \leq i \leq n$. Invertible elements form a multiplicative group $K_\mathbb{R}^\times$. $K_\mathbb{R}^+$ is defined as the subset of $K_\mathbb{R}$ which elements have real positive coordinates. In particular for any $x \in K_\mathbb{R}$, we have $x\bar{x} \in K_\mathbb{R}^+$. There is a square root map $\sqrt{\cdot} : K_\mathbb{R}^+ \to K_\mathbb{R}^+$ defined coordinate-wise.

Lemma 2.6 (Proposition 1, §4.2 of [30], adapted)**.** *Let M be a free rank n sub-$\mathbb{Z}$-lattice of K with a $\mathbb{Z}$-basis $(x_i)_{1 \leq i \leq n}$. Then, $\mu(M)$ is a full-rank lattice of $\mathbb{C}^n \simeq \mathbb{R}^{2n}$ with volume :*

$$\det(\mu(M)) = |\det(\sigma_i(x_j))_{1 \leq i,j \leq n}|.$$

Proof. The volume we want to compute is given by $|\det M|$, where M is the matrix whose i-th column are the coordinates of $\mu(x_i)$ in the canonical basis of $\mathbb{C}^n$. For any $1 \leq i \leq n$, these coordinates are $\sigma_1(x_i), \dots, \sigma_n(x_i)$. Since the $x_i's$ form a $\mathbb{Q}$-basis of K, this determinant is non zero thus $\mu(M)$ is a full-rank lattice of $\mathbb{C}^n$ and has the volume announced. □

Proposition 2.8 (Proposition 2, §4.2 of [30], adapted)**.** *Let $\mathfrak{a} \subset \mathcal{O}_K$ be a non-zero ideal, then $\mu(\mathcal{O}_K)$ and $\mu(\mathfrak{a})$ are lattices of $\mathbb{R}^n$ with volume*

$$\det(\mu(\mathcal{O}_K)) = \sqrt{|\Delta_K|} \ ; \ \det(\mu(\mathfrak{a})) = \sqrt{|\Delta_K|} N_{K/\mathbb{Q}}(\mathfrak{a}).$$

Proof. $\mathcal{O}_K$ and $\mathfrak{a}$ are both free $\mathbb{Z}$-modules of rank n so we can apply the previous lemma. By definition of the discriminant we get the first equality. For the second, remark that $\mu(\mathfrak{a})$ has index $N_{K/\mathbb{Q}}(\mathfrak{a})$ in $\mu(\mathcal{O}_K)$ so a fundamental domain for $\mu(\mathfrak{a})$ is given by a disjoint union of $N_{K/\mathbb{Q}}(\mathfrak{a})$ fundamental domains of $\mu(\mathcal{O}_K)$. □

2.2.2 Application to number fields.

Embeddings play a key role ; they relate algebraic properties of number fields to geometric properties of lattices. We recall two important results using this correspondence, namely the finiteness of the class group and Dirichlet's unit theorem.

Definition. Fractional ideal of K form a group $I(\mathcal{O}_K)$ and the set of principal fractional ideals $F(\mathcal{O}_K)$ is a subgroup. The quotient group $Cl(K) := I(\mathcal{O}_K)/F(\mathcal{O}_K)$ is called the class group of $\mathcal{O}_K$ (or K). Its cardinal is called the class number of K and is denoted h_K. The class group is trivial if and only if $\mathcal{O}_K$ is a PID.

Theorem 2.2 (Finiteness of the class group, Corollaire 1, §4.3 of [30])**.** *$Cl(\mathcal{O}_K)$ is a finite group and every class has a representative $\mathfrak{a}$ with norm*

$$N_{K/\mathbb{Q}}(\mathfrak{a}) \leq C_K \sqrt{|\Delta_K|},$$

where $C_K = \left(\frac{4}{\pi}\right)^{n_2} \frac{n!}{n^n}$ is the Minkowski constant of K.

Corollary 2.1. *$Cl(\mathcal{O}_K)$ is generated by prime ideals $\mathfrak{p}$ above prime numbers $p \leq C_K \sqrt{|\Delta_K|}$.*

Theorem 2.3 (Dirichlet, Théorème 1, §4.4 of [30])**.** *The Log-embedding of K is defined by*

$$\mathrm{Log} : K \longrightarrow \mathbb{R}^{n_1+n_2} \ ; \ x \longmapsto (\ln(|\sigma_1(x)|), \ldots, \ln(|\sigma_{n_1}(x)|), 2\ln(|\sigma_{n_1+1}(x)|), \ldots, 2\ln(|\sigma_{n_1+n_2}(x)|)).$$

We have an isomorphism of groups

$$\mathcal{O}_K^\times \simeq \mathbb{U}_K \times \mathbb{Z}^{n_1+n_2-1},$$

where $\mathbb{U}_K$ is the set of roots of unity of K, it is a finite cyclic group. The image of $\mathcal{O}_K^\times$ by the Log-embedding is a lattice of $\mathbb{R}^{n_1+n_2}$ with rank $r := n_1 + n_2 - 1$. The kernel of $\mathrm{Log}_{|\mathcal{O}_K^\times}$ is exactly $\mathbb{U}_K$.

Remarks. • The theorem implies the existence of units $u_1, \ldots, u_r$ such that every $u \in \mathcal{O}_K^\times$ can be uniquely written $u = z u_1^{a_1} \ldots u_r^{a_r}$, with $a_i \in \mathbb{Z}$ and z a root of unity in K. Such a set $\{u_i\}_{1 \leq i \leq r}$ is called a system of fundamental units of $\mathcal{O}_K$.

• By definition of the norm, any $u \in \mathcal{O}_K^\times$ satisfies $\prod_{1 \leq i \leq n} \sigma_i(u) = 1$ so its image by the Log map lies in the hyperplane $H := \{(x_1, \ldots, x_{r+1}) \in \mathbb{R}^{r+1} \mid \sum_{1 \leq i \leq r+1} x_i = 0\}$. Therefore for any system of fundamental units $\{u_1, \ldots, u_r\}$, the $r \times (r+1)$ matrix $(N_j \ln(|\sigma_j(u_i)|))_{1 \leq i \leq r,\ 1 \leq j \leq r+1}$ (with $N_j = 1$ if $j \leq n_1$ and $N_j = 2$ otherwise) has the property that the sum of any row is equal zero. Thus, the absolute value of the determinant of the submatrix formed by deleting

one column is independent of the column ; this number is called the regulator of K and denoted $\mathrm{Reg}(K)$. The Log-unit lattice has volume $\mathrm{Reg}(K)\sqrt{r}$.

• Let $\zeta \in K$ be a generator of $\mathbb{U}_K$ and $d \in \mathbb{N}_{>0}$ its order. That means ζ is a primitive d-th root of unity so its minimal polynomial over $\mathbb{Q}$ is $\Phi_d(X)$ and has degree $\varphi(d)$. Since the conjugates of ζ are powers of ζ, we have $\mathbb{Q}(\zeta) \subset K$ and $\varphi(d) = [\mathbb{Q}(\zeta) : \mathbb{Q}] \leq [K : \mathbb{Q}] = n$. Using classical inequality $\sqrt{d} \leq \varphi(d)$ (for $d > 6$) we get $(|\mathbb{U}_K| =)\, d \leq n^2$.

The notions introduced in this paragraph are linked together by to the following formula.

Theorem 2.4 (Analytic class number formula)**.** *Let K be a number field with signature (n_1, n_2) then,*

$$\mathrm{Res}_1(\zeta_K) = \frac{2^{n_1} \cdot (2\pi)^{n_2} \cdot h_K \cdot \mathrm{Reg}(K)}{\omega_K \cdot \sqrt{|\Delta_K|}}, \tag{2}$$

where ω_K is the number of roots of unity in K and $\mathrm{Res}_1(\zeta_K) = \lim_{s\to 1}(s-1)\zeta_K(s)$ is the residue of the Dedekind zeta function of K at 1, defined by $\zeta_K(s) = \sum_{\mathfrak{a}\subset\mathcal{O}_K} \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{a})^s}$.

Cyclotomic units. Let $\zeta \in \mathbb{C}$ be a n-th primitive root of unity and $L = \mathbb{Q}(\zeta)$, with n a power of a prime p. There is a subgroup of $\mathcal{O}_L^\times$ called the cyclotomic units subgroup with explicit generators and finite index in $\mathcal{O}_L^\times$.

Definition. For $1 < a < n$ and $(a, p) = 1$, the elements $b_a := \frac{\zeta^a - 1}{\zeta - 1}$ belong to $\mathcal{O}_L^\times$ and the group C generated by -1, ζ and the $(b_a)_a$ is called the subgroup of cyclotomic units.

Indeed for such $1 < a < n$, we have $b_a = 1 + \zeta + \cdots + \zeta^{a-1} \in \mathcal{O}_L$ and since a is coprime to p, ζ^a is also a primitive n-th root of unity so one can write $\zeta = (\zeta^a)^m$ for some integer m and then $(\zeta - 1)/(\zeta^a - 1) = 1 + \zeta^a + \cdots + (\zeta^a)^{m-1} \in \mathcal{O}_L$. Then, b_a is a unit.

Theorem 2.5 (Lemma 8.1 and Theorem 8.2 of [37])**.** *Let $K := \mathbb{Q}(\zeta + \zeta^{-1})$ be the maximal real subfield of L. Then the cyclotomic units C have finite index in $\mathcal{O}_L^\times$ and,*

$$h_K = [\mathcal{O}_L^\times : C].$$

Conjecture (Weber's class number problem)**.** *For power-of-two cyclotomic fields, the class number of the maximal real subfield is $h_K = 1$.*

2.3 Ramification of number fields

Let $\mathfrak{p}$ denotes a prime ideal of $\mathcal{O}_K$ and $\mathfrak{p}\mathcal{O}_L$ be the ideal of $\mathcal{O}_L$ generated by $\mathfrak{p}$. As $\mathcal{O}_L$ is a Dedekind ring, the latter can be uniquely written

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{s} \mathfrak{q}_i^{e_i}, \tag{3}$$

where the $\mathfrak{q}_i$ are distinct prime ideals of $\mathcal{O}_L$ and $e_i \geq 1$ is called the ramification index of $\mathfrak{q}_i$ over $\mathcal{O}_K$. For every $1 \leq i \leq s$, we have $\mathfrak{q}_i \cap \mathcal{O}_K = \mathfrak{p}$ so this defines an extension of fields $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{q}_i$, whose degree is called the residual degree of $\mathfrak{q}_i$ over $\mathcal{O}_K$ and is denoted $f_i \geq 1$. These quantities satisfy the fundamental following formula.

Theorem 2.6 (Théorème 1, §5.2 and Proposition 1, §6.2 of [30]). *With the notations introduced above, we have the relation*

$$\sum_{i=1}^{s} e_i f_i = m = [L : K].$$

Moreover, in the case where L/K is Galois, we have $e_i = e_j$ and $f_i = f_j$ for all $1 \leq i, j \leq s$.

For any prime $\mathfrak{q}_i$ in the formula (3), we say that the extension $\mathcal{O}_K \subset \mathcal{O}_L$ is unramified at $\mathfrak{q}_i$ if $e_i = 1$, otherwise it is said ramified. Also, if the extension is unramified at all the $\mathfrak{q}_i$'s, we say that $\mathcal{O}_K \subset \mathcal{O}_L$ is unramified above $\mathfrak{p}$. Consider the special case where L/K is quadratic ; the ideal $\mathfrak{p}\mathcal{O}_L$ can be either a prime ideal of $\mathcal{O}_L$ (we say $\mathfrak{p}$ is inert), either the product of two distinct prime ideals (we say $\mathfrak{p}$ splits) or it can be the square of a prime ideal (this is the case where $\mathfrak{p}$ ramifies).
The following proposition tells us which prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ ramify in $\mathcal{O}_L$.

Definition. The ideal discriminant of L over K is the ideal of $\mathcal{O}_K$ generated by the elements $D_{L/K}(\varepsilon) := \mathrm{disc}(Tr_{L/K}, \varepsilon)$ where $Tr_{L/K} : L \times L \to K$ is the K-bilinear form $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ and $\varepsilon = \{x_1, \ldots, x_n\} \subset \mathcal{O}_L$ ranges over the K-basis of L contained in $\mathcal{O}_K$. This ideal is denoted $D_{L/K}$.

Proposition 2.9 (Théorème 1, §5.3 of [30]). *A prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ ramifies in $\mathcal{O}_L$ if and only if it contains $D_{L/K}$. In particular, the set of prime ideals of $\mathcal{O}_K$ which ramify $\mathcal{O}_L$ is finite.*

Example. In the case where $K = \mathbb{Q}$, the notion of ideal discriminant coincide with the usual discriminant. If $\zeta \in \mathbb{C}$ is a primitive n-th root of unity with $n = 2^r$ and $L = \mathbb{Q}(\zeta)$, then the discriminant can be computed : $D_{L/\mathbb{Q}} = \pm 2^{2^{r-1}(2r-r-1)}$ (see Theorem 3, IV, §1 of [20]) so the only prime number which ramifies in $\mathcal{O}_L = \mathbb{Z}[\zeta]$ is 2.

2.3.1 Dedekind-Kummer theorem

We end this reminder by a very useful result for computing the splitting in equation (3).

Theorem 2.7 (Dedekind-Kummer, Proposition 25, I, §8 of [20]). *Suppose $\mathcal{O}_L = \mathcal{O}_K[\theta]$ and let $m(X) \in \mathcal{O}_K[X]$ be the minimal polynomial of θ over K. Fix a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ and put $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ the residue field. Let $\overline{m}(X) \in k(\mathfrak{p})[X]$ be the reduction $m(X)$ mod $\mathfrak{p}$, and let*

$$\overline{m}(X) = h_1(X)^{r_1} \ldots h_s(X)^{r_s}$$

be the factorization of $\overline{m}(X)$ into powers of monic irreducible factors over $k(\mathfrak{p})$. For each $1 \leq i \leq s$, let $H_i \in \mathcal{O}_K[X]$ be a monic lift of h_i and put $\mathfrak{q}_i := \mathfrak{p}\mathcal{O}_L + H_i(\theta)\mathcal{O}_L$. Then, the $\mathfrak{q}_i$'s are pairwise distinct maximal ideals of $\mathcal{O}_L$ containing $\mathfrak{p}$, we have $r_i = e_i$ and $\deg H_i(X) = f_i$ for all $1 \leq i \leq s$, and the following formula holds

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{s} \mathfrak{q}_i^{e_i}.$$

It is the splitting of $\mathfrak{p}$ in $\mathcal{O}_L$.

Example. Suppose $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta)$ is a power-of-two cyclotomic field. The only prime integer which ramifies in $\mathcal{O}_L$ is 2, and the reduction of the minimal polynomial mod 2 is just $X^n + \bar{1} = (X + \bar{1})^n$, so in virtue of Dedekind-Kummer's theorem (2.7) we have the splitting $2\mathcal{O}_L = \mathfrak{q}^n$, where $\mathfrak{q} = (2, 1 + \zeta)$.

Remark. • Suppose $L = K(\theta)$, the conductor of $\mathcal{O}_K[\theta]$ in $\mathcal{O}_L$ is the biggest ideal $\mathfrak{c}$ of $\mathcal{O}_L$ contained in $\mathcal{O}_K[\theta]$, namely

$$\mathfrak{c} = \{\alpha \in \mathcal{O}_L \,|\, \alpha\mathcal{O}_L \subset \mathcal{O}_K[\theta]\}.$$

Then, the hypothesis « $\mathcal{O}_L = \mathcal{O}_K[\theta]$ » in theorem 2.7 can be replaced by « $\mathfrak{p}\mathcal{O}_K[\theta]$ is coprime to the conductor of $\mathcal{O}_K[\theta]$ in $\mathcal{O}_L$ ». See Proposition 6.16 of [34] or Proposition 8.3 Chapter I of [25] for a proof.

• Further, we will discuss the efficiency of this theorem. See Lemma 3.7.

2.4 Lattices over a Dedekind domain

With Minkowski embedding we are able to identify the ring of integers $\mathcal{O}_K$ of a number field K with a lattice of $\mathbb{R}^n$. More generally any projective module of finite type over $\mathcal{O}_K$ included in K^n embeds into a real vector space (*e.g.*, any ideal of $\mathcal{O}_K$). In this section we give results on the structure of torsion-free modules of finite type over a Dedekind ring (such modules are projective, see Theorem 2.1.19 of [11]). Notice that a Dedekind ring is not a PID in general so the well-known structure of modules over a PID does not apply. However we have similar results ; there is a notion of pseudo-basis and an invariant factors theorem. Also, we will focus on the extension of the HNF algorithm given by Cohen in [11] to this context.

2.4.1 Structure theorems

In the following we fix a Dedekind domain $\mathcal{O}$ with fraction field K, V a n-dimensional vector space over K and $M \subset V$ a finitely generated torsion-free module over $\mathcal{O}$. The subspace of V spanned by M is denoted $KM := K \otimes_R M$.

Definition. What we call a module over $\mathcal{O}$ is a finitely generated torsion-free (hence projective) $\mathcal{O}$-module $N \subset V$ such that $KN = V$.

From now on, M denotes a $\mathcal{O}$-module. The main result of this section is the following, we follow the proof given in [11], Chapter 1.

Theorem 2.8 (Theorem 1.2.19 of [11])**.** *There exists an ideal $\mathfrak{a}$ of $\mathcal{O}$ such that*

$$M \simeq \mathcal{O}^{n-1} \oplus \mathfrak{a}. \tag{4}$$

Moreover if $n, m \in \mathbb{N}_{>0}$ and $\mathfrak{a}, \mathfrak{b}$ are fractional ideal[5] of $\mathcal{O}$, then we have $\mathcal{O}^{n-1} \oplus \mathfrak{a} \simeq \mathcal{O}^{m-1} \oplus \mathfrak{b}$ if and only if $n = m$ and $\mathfrak{a}, \mathfrak{b}$ are in the same ideal class (i.e., there exists $\alpha \in K \setminus \{0\}$ such that $\mathfrak{a} = \alpha\mathfrak{b}$). Therefore, M is fully determined by its rank and the class $Cl(M) := Cl(\mathfrak{a})$,

[5] A fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is a sub-$\mathcal{O}$-module of K such that there exists $d \in R$ satisfying $d\mathfrak{a} \subset \mathcal{O}$.

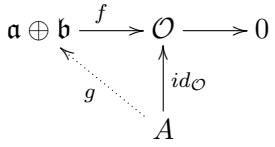
called the Steinitz class of M.

When (4) is an equality, this is called an almost free (or Steinitz) representation of M.

Lemma 2.7 (Lemma 1.2.20 of [11]). *Let $\mathfrak{a}, \mathfrak{b}$ be two fractional ideals of $\mathcal{O}$. Then,*

$$\mathfrak{a} \oplus \mathfrak{b} \simeq \mathcal{O} \oplus \mathfrak{ab}.$$

Proof. For any $\alpha \in K \setminus \{0\}$, $\alpha\mathfrak{a}$ is isomorphic to $\mathfrak{a}$, so we can suppose that $\mathfrak{a}, \mathfrak{b}$ are integral. Let $\mathfrak{a}' \sim \mathfrak{a}^{-1}$ be an integral ideal and $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ the list of primes ideals dividing $\mathfrak{b}$. By the Chinese remainder theorem, there exists an element $r \in \mathfrak{a}$ such that $v_{\mathfrak{p}_i}(r) = v_{\mathfrak{p}_i}(\mathfrak{a}')$ for all $i \in \{1, \dots, n\}$[6]. The ideal $r\mathcal{O}$ is contained in $\mathfrak{a}$ so by Theorem 2.1, there exists an integral ideal $\mathfrak{c}$ such that $r\mathcal{O} = \mathfrak{a}'\mathfrak{c}$ and by construction $v_{\mathfrak{p}_i}(\mathfrak{c}) = v_{\mathfrak{p}_i}(r) - v_{\mathfrak{p}_i}(\mathfrak{a}') = 0$ so $\mathfrak{c}$ is coprime to $\mathfrak{b}$. Also, $\mathfrak{a}'\mathfrak{c}$ is principal so $\mathfrak{c} \sim \mathfrak{a}'^{-1} \sim \mathfrak{a}$. Therefore, without loss of generality, we can suppose $\mathfrak{a}, \mathfrak{b}$ are integral and coprime.
Thus, the linear map $f : \mathfrak{a} \oplus \mathfrak{b} \to \mathcal{O} = \mathfrak{a} + \mathfrak{b}$ given by $(a, b) \mapsto a - b$ is surjective and has kernel $\{(a, a) \,|\, a \in \mathfrak{a} \cap \mathfrak{b}\} \simeq \mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$ since $\mathfrak{a}$ and $\mathfrak{b}$ are coprime. It remains to prove that $\mathfrak{a} \oplus \mathfrak{b} \simeq \mathcal{O} \oplus \ker f$. As $\mathcal{O}$ is trivially a projective $\mathcal{O}$-module, the identity map of $\mathcal{O}$ extends to a linear map $g : \mathfrak{a} + \mathfrak{b} \to \mathcal{O}$ such that



is a commutative diagram *i.e.*, we get a section g of f. Then, for any $x \in \mathfrak{a} \oplus \mathfrak{b}$, the element $y = x - g(f(x))$ satisfies $f(y) = 0$ so $\mathfrak{a} \oplus \mathfrak{b} \subset g(\mathcal{O}) + \ker f$ and the inverse inclusion is clear. Now if $y \in g(\mathcal{O}) \cap \ker f$, we can write $y = g(x)$ hence $0 = f(y) = f(g(x)) = x$ and $y = g(0) = 0$, so $g(\mathcal{O}) \cap \ker f = \{0\}$. Finally, the relation $f \circ g = id_{\mathcal{O}}$ implies that g is injective so $g(\mathcal{O}) \simeq \mathcal{O}$ and $\mathfrak{a} \oplus \mathfrak{b} = g(R) \oplus \ker f \simeq \mathcal{O} \oplus \mathfrak{ab}$. □

Lemma 2.8 (Lemma 1.2.22 of [11]). *Let e be a non-zero vector of $V = KM$ and*

$$\mathfrak{a} := \{\lambda \in K \,|\, \lambda e \in M\}.$$

1) $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}$
2) $M/\mathfrak{a}e$ is a torsion-free $\mathcal{O}$-module of rank $n - 1$.

Proof. 1) $\mathfrak{a}$ is a non-zero $\mathcal{O}$-module and $\mathfrak{a} \simeq e\mathfrak{a} \subset M$ is a sub-module. Since $\mathcal{O}$ is Noetherian and M is finitely generated, we deduce that $\mathfrak{a}$ is a finitely generated $\mathcal{O}$-module. Let d be a common denominator of the generators of $\mathfrak{a}$, then $d\mathfrak{a} \subset \mathcal{O}$ *i.e.*, $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}$.
2) Let $\overline{x} \in M/\mathfrak{a}e$ be a torsion element ; there exists $r \in \mathcal{O} \setminus \{0\}$ such that $rx \in Ie \subset Ke$. Then, $x \in M \cap Ke$ so one can write $x = \lambda e \in M$ and $\lambda \in K$ is by definition an element of $\mathfrak{a}$.

[6] More precisely, let $\mathfrak{a}_i := \mathfrak{p}_1 \dots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1}\mathfrak{p}_n$ ($i \in \{1, \dots, n\}$), then $\mathfrak{a}_i\mathfrak{a}' \cap \mathfrak{p}_i\mathfrak{a}' \subsetneq \mathfrak{a}_i\mathfrak{a}'$ (because $v_{\mathfrak{p}_i}(\mathfrak{a}_i\mathfrak{a}' \cap \mathfrak{p}_i\mathfrak{a}') = v_{\mathfrak{p}_i}(\mathfrak{p}_i\mathfrak{a}') > v_{\mathfrak{p}_i}(\mathfrak{a}') = v_{\mathfrak{p}_i}(\mathfrak{a}_i\mathfrak{a}')$) so we can take $r_i \in \mathfrak{a}_i\mathfrak{a}'$ such that $r_i \notin \mathfrak{p}_i\mathfrak{a}'$. This means we get $r_i \in \mathfrak{a}'$ with $\mathfrak{p}_i$-valuation $v_{\mathfrak{p}_i}(\mathfrak{a}')$ ($i \in \{1, \dots, n\}$). Then $r := r_1 + \dots + r_n \in \mathfrak{a}'$ satisfies $v_{\mathfrak{p}_i}(r) = v_{\mathfrak{p}_i}(r_i) = v_{\mathfrak{p}_i}(\mathfrak{a}')$ for all $i \in \{1, \dots, n\}$.

This means $x \in \mathfrak{a}e$ so $\overline{x} = \overline{0}$.
Recall that the rank of $M/\mathfrak{a}e$ is the dimension of $K(M/\mathfrak{a}e)$ as a K-vector space. But $K(M/\mathfrak{a}e) = (KM)/(Ke)$ and Ke has dimension 1 so $M/\mathfrak{a}e$ has rank $n-1$. □

Proof. (of Theorem 2.8). If M has rank 0, then $M = \{0\}$ since it is torsion-free. Now suppose $n > 0$ and the result is proved up to rank $n-1$. Let M be a module of rank n and $e \in M$ a non-zero element. By the lemma above, $M/\mathfrak{a}e$ is torsion-free of rank $n-1$ so by assumption there exists an ideal $\mathfrak{b} \subset \mathcal{O}$ such that $M/Ie \simeq \mathcal{O}^{n-2} \oplus \mathfrak{b}$ (take $\mathfrak{b} = \{0\}$ if $n = 1$). The canonical projection $f : M \to M/\mathfrak{a}e$ has a section g (same argument 2.7 and because $M/\mathfrak{a}e$ is a projective $\mathcal{O}$-module) so we get $M \simeq g(M/\mathfrak{a}e) \oplus Ie \simeq M/\mathfrak{a}e \oplus \mathfrak{a}e$ (because g is injective). Then,

$$\begin{aligned} M &\simeq \mathcal{O}^{n-2} \oplus \mathfrak{b} \oplus \mathfrak{a}e \\ &\simeq \mathcal{O}^{n-2} \oplus \mathfrak{b} \oplus \mathfrak{a} \\ &\simeq \mathcal{O}^{n-1} \oplus \mathfrak{a}\mathfrak{b}, \quad \text{by Lemma 2.7.} \end{aligned}$$

This completes the induction and finishes the first part of the proof. For the « unicity » part, first observe that if $\mathfrak{a}$ is principal, then $\mathcal{O}^{n-1} \otimes \mathfrak{a}$ is a free $\mathcal{O}$-module. The converse is true, this is Theorem 1.2.23 of [11] and we omit the proof. Now let $n, m \in \mathbb{N}_{>0}$ and $\mathfrak{a}, \mathfrak{b}$ fractional ideals such that $R^{n-1} \oplus \mathfrak{a} \simeq R^{m-1} \oplus \mathfrak{b}$. Since $\mathfrak{a}, \mathfrak{b}$ have rank 1, we must have $n = m$. Also,

$$\begin{aligned} &\mathcal{O}^{n-1} \oplus \mathfrak{a} \simeq \mathcal{O}^{n-1} \oplus \mathfrak{b} \\ \Rightarrow\ &\mathcal{O}^{n-1} \oplus \mathfrak{a} \oplus \mathfrak{a}^{-1} \simeq \mathcal{O}^{n-1} \oplus \mathfrak{b} \oplus \mathfrak{a}^{-1} \\ \Rightarrow\ &\mathcal{O}^{n+1} \simeq \mathcal{O}^{n} \oplus \mathfrak{b}\mathfrak{a}^{-1}, \quad \text{using Lemma 2.7 on both sides.} \end{aligned}$$

Thus, by Theorem 1.2.23 of [11] we find out $\mathfrak{b}\mathfrak{a}^{-1}$ is principal *i.e.*, $\mathfrak{a} \sim \mathfrak{b}$. □

Pseudo-basis. Theorem 2.8 gives a full description of the isomorphism classes of $\mathcal{O}$-modules. A direct consequence of this result is the existence of pseudo-basis. This notion is the natural object to represent module-lattices and do computations with them. For algorithmic purposes, lattices over Dedekind rings will always be assumed to be given by a pseudo-basis.

Theorem 2.9 (Corollary 1.2.25 of [11])**.** *There exist elements $b_1, \ldots, b_n \in V$ and fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ of $\mathcal{O}$ (called coefficient ideals) such that*

$$M = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n.$$

The Steinitz class of M is the class of the product $\mathfrak{a}_1 \ldots \mathfrak{a}_n$.

Proof. By Theorem 2.8 there exists a non-zero[7] (fractional) ideal $\mathfrak{a}$ of $\mathcal{O}$ such that $M \simeq \mathcal{O}^{n-1} \oplus \mathfrak{a}$. Let $a \in \mathfrak{a} \setminus \{0\}$, as $\mathfrak{a}$ is isomorphic to the fractional ideal $\frac{1}{a}\mathfrak{a}$, we can further suppose $1 \in \mathfrak{a}$. Let $f : \mathcal{O}^{n-1} \oplus \mathfrak{a} \to M$ be the isomorphism and for $i \in \{1, \ldots, n\}$, denote by e_i the element of $\mathcal{O}^{n-1} \oplus \mathfrak{a}$ with coordinates $(0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 at the i-th coordinate, and let $b_i = f(e_i) \in M$. Since f is an isomorphism, we have $M = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n$ with $\mathfrak{a}_1 = \cdots = \mathfrak{a}_{n-1} = \mathcal{O}$ and $\mathfrak{a}_n = \mathfrak{a}$.

[7] Since M has rank n, $\mathfrak{a}$ must be non-trivial.

Applying Lemma 2.7 several times, we get $\mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n \simeq \mathcal{O}^{n-1} \oplus \mathfrak{a}_1 \ldots \mathfrak{a}_n$ so the Steinitz class of M is the class of $\mathfrak{a}_1 \ldots \mathfrak{a}_n$. □

Definition. Let $(b_i)_{1\leq i\leq n} \in V^n$ and $(\mathfrak{a}_i)_{1\leq i\leq n}$ be a set of fractional ideals of $\mathcal{O}$. We say that $(b_i, \mathfrak{a}_i)_{1\leq i\leq n}$ is pseudo-basis of M if we have the equality

$$M = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_n b_n. \tag{5}$$

Remarks. • By Theorem 2.9, modules over $\mathcal{O}$ always have a pseudo-basis.

• Coefficient ideals can be taken integral ; let $d_i \in \mathcal{O} \setminus \{0\}$ such that $d_i \mathfrak{a}_i \subset \mathcal{O}$, then $b_i \mathfrak{a}_i = \frac{b_i}{d_i} d_i \mathfrak{a}_\mathfrak{i}$. In the same way, we can suppose $b_i \in M$ and adjust the coefficient ideals. However it is not possible, in general, to have both conditions. In the following, we fix the convention that the vectors of a pseudo-basis belong to the module.

• The writing (5) is not unique ; the following proposition gives a condition for two pseudo-bases to represent the same module.

Proposition 2.10 (Pseudo-base change, Proposition 1.4.2 of [11])**.**
Let $(b_i, \mathfrak{a}_i)_{1\leq i\leq n}$ and $(b'_i, \mathfrak{b}_i)_{1\leq i\leq n}$ be two pseudo-bases for M and $U = (u_{i,j})_{1\leq i,j\leq n} \in \mathbf{GL}_n(K)$ the matrix expressing the b'_i in terms of the b_i ; that is $b'_j = \sum_{i=1}^n u_{i,j} b_i$ for every $j \in \{1, \ldots, n\}$. Then,

$$u_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1} \quad \textit{and} \quad \mathfrak{a} = (\det U)\mathfrak{b},$$

where $\mathfrak{a} = \mathfrak{a}_1 \ldots \mathfrak{a}_n$ and $\mathfrak{b} = \mathfrak{b}_1 \ldots \mathfrak{b}_n$.
Conversely, if we have $U = (u_{i,j})_{1\leq i,j\leq n} \in \mathbf{GL}_n(K)$ and fractional ideals $(\mathfrak{b}_i)_{1\leq i\leq n}$ such that $u_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$ and $\mathfrak{a} = (\det U)\mathfrak{b}$, then $(b'_i, \mathfrak{b}_i)_{1\leq i\leq n}$ is a pseudo-basis of M, where $b'_j = \sum_{i=1}^n u_{i,j} b_i$.

Proof. For $j \in \{1, \ldots, n\}$, since $b'_j \mathfrak{b}_j \subset M$, we get $b'_j \in \bigoplus_{i=1}^n \mathfrak{b}_j^{-1} \mathfrak{a}_i b_i$, so $u_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$ and

$$\det U = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \underbrace{u_{1,\sigma(1)} \ldots u_{n,\sigma(n)}}_{\in \mathfrak{a}_1 \mathfrak{b}_{\sigma(1)}^{-1} \ldots \mathfrak{a}_n \mathfrak{b}_{\sigma(n)}^{-1} = \mathfrak{a}\mathfrak{b}^{-1}} \in \mathfrak{a}\mathfrak{b}^{-1}.$$

From $\det U \in \mathfrak{a}\mathfrak{b}^{-1}$, we deduce that $(\det U)\mathfrak{b} \subset \mathfrak{a}$. Playing the same game with U^{-1} we get $(\det U^{-1})\mathfrak{a} \subset \mathfrak{b}$ so finally $\mathfrak{a} = (\det U)\mathfrak{b}$.

Conversely, suppose that $u_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$ and $\mathfrak{a} = (\det U)\mathfrak{b}$. Let adj$(U)$ be the adjugate matrix of U, so that adj$(\mathrm{U})_{i,j}$ is equal, up to the sign, to the minor $\det U_{i,j}$ of U. This determinant is

$$\det U_{i,j} = \sum_{\substack{\sigma \in \mathfrak{S}_n \\ \sigma(i)=j}} \varepsilon(\sigma) \prod_{\substack{l=1 \\ l\neq i}}^{n} u_{l,\sigma(l)} \in (\mathfrak{a}_1 \ldots \mathfrak{a}_{i-1} \mathfrak{a}_{i+1} \ldots \mathfrak{a}_n)(\mathfrak{b}_1^{-1} \ldots \mathfrak{b}_{j-1}^{-1} \mathfrak{b}_{j+1}^{-1} \ldots \mathfrak{b}_n^{-1}),$$

so $\mathrm{adj}(U)_{i,j} \mathfrak{a}_i \mathfrak{b}_j^{-1} \subset \mathfrak{a}\mathfrak{b}^{-1} = (\det U)R$. Since the inverse matrix $V = (v_{i,j})_{1\leq i,j\leq n}$ of U is given by $V = \frac{1}{\det U} \mathrm{adj}(U)^T$, we deduce that $v_{i,j} \in \mathfrak{a}_j^{-1} \mathfrak{b}_i$. Now let m and $X = (x_1, \ldots, x_n)^T$ the columns vectors of its components in the pseudo-basis $(b_i, \mathfrak{a}_i)_{1\leq i\leq n}$. Then, $m = (b_1, \ldots, b_n)X = (b'_1, \ldots, b'_n)U^{-1}X$ and $U^{-1}X =: (y_1, \ldots, y_n)^T$ satisfies $y_i \in \mathfrak{b}_i$ for $1 \leq i \leq n$. Also, the y_i are

uniquely determined so we have a direct sum $M = \bigoplus_{i=1}^{n} \mathfrak{b}_i b'_i$ *i.e.*, $(b'_i, \mathfrak{b}_i)_{1 \leq i \leq n}$ is a pseudo-basis for M. □

Remark. We proved that if U satisfies $u_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$ and $\mathfrak{a} = (\det U)\mathfrak{b}$, then the inverse matrix $V = (v_{i,j})_{1 \leq i,j \leq n}$ is such that $v_{i,j} \in \mathfrak{b}_i \mathfrak{a}_j^{-1}$.

We end this theoretical section with the elementary divisor theorem for modules over Dedekind rings. Its proof is omitted and we refer to [11].

Theorem 2.10 (Elementary divisors, Theorem 1.2.35 of [11])**.** *Let $N \subset M$ be a sub-$\mathcal{O}$-module of rank $m \leq n$. Then, there exists a pseudo-basis $(b_i, \mathfrak{b}_i)_{1 \leq i \leq n}$ of M and fractional ideals $\mathfrak{d}_1, \ldots, \mathfrak{d}_m$ of $\mathcal{O}$ such that*

$$N = \mathfrak{d}_1 \mathfrak{b}_1 b_1 \oplus \cdots \oplus \mathfrak{d}_m \mathfrak{b}_m b_m,$$

and $\mathfrak{d}_{i-1} \subset \mathfrak{d}_i$ for all $2 \leq i \leq m$. Moreover, the ideals $\mathfrak{d}_i$ and the classes of the products $\mathfrak{b}_1 \ldots \mathfrak{b}_m$ and $\mathfrak{b}_{m+1} \ldots \mathfrak{b}_n$ (if $m < n$) depends only on M and N.

2.4.2 Algorithmic tools

Computing a pseudo-basis. In [19] Section 2 is given an algorithm to compute a pseudo-basis of a module-lattice from a set of generators. This and the CHNF algorithm are based on the following theorem which is somehow a generalization of the extended Euclidean algorithm to Dedekind rings.

Theorem 2.11 (Theorem 1.3.3 of [11])**.** *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two (fractional) ideals of K and $a, b \in K$ not both equal to zero. Put $\mathfrak{d} = a\mathfrak{a} + b\mathfrak{b}$ It is possible to find in polynomial time elements $u \in \mathfrak{a}\mathfrak{d}^{-1}$ and $v \in \mathfrak{b}\mathfrak{d}^{-1}$ such that $au + bv = 1$.*

Proposition 2.11 (Corollary A.2. of [6])**.** *There exists a probabilistic polynomial-time algorithm that given nonzero integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ of K returns an element $x \in K \setminus \{0\}$ such that $x\mathfrak{a}$ is integral and coprime to $\mathfrak{b}$.*

Corollary 2.2. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two (fractional) ideals of K, there exists a probabilistic polynomial-time algorithm that computes $\alpha_1 \in \mathfrak{a}$, $\alpha_2 \in \mathfrak{b}$, $\beta_1 \in \mathfrak{a}^{-1}$ and $\beta_2 \in \mathfrak{b}^{-1}$ such that $\alpha_1\beta_1 + \alpha_2\beta_2 = 1$*

Proof. Multiplying by an element of $\mathbb{Q} \setminus \{0\}$, we can reduce to the case where $\mathfrak{a}^{-1}$, $\mathfrak{b}$ are integral. By the proposition above, we can find in polynomial time an element $x \in \mathcal{O}$ such that $x\mathfrak{a}^{-1}$ is integral and coprime to $\mathfrak{b}$, with positive probability. Then with the algorithm of Theorem (2.11), we get in (deterministic) polynomial-time elements $u \in x\mathfrak{a}^{-1}$ and $v \in \mathfrak{b}$ ($b = 1$ and $\mathfrak{d} = \mathcal{O}$ by coprimality) such that $u + v = 1$. Taking $\alpha_1 = u$, $\alpha_2 = v$, $\beta_1 = u/x$ and $\beta_2 = 1$ we get the result. □

Algorithm 1 Compute a pseudo-basis of a torsion-free R-module from a generating set

Require: A set of vectors $\{m_1, \dots, m_s\}$ generating a rank r module M ($r \leq s$).
Ensure: A pseudo-basis $(b_i, \mathfrak{a}_i)_{1 \leq i \leq r}$ of M.

$(v_1, \dots, v_r) \leftarrow$ a K-basis of KM.
if $r = 0$ **then**
  return $\emptyset$
end if
for $i \in \{1, \dots, s\}$ **do**
  Compute $(\nu_{i,j})_{1 \leq j \leq r} \in K^r$ such that $m_i = \sum_{j=1}^{r} \nu_{i,j} v_j$.
end for
$\mathfrak{a}_1 \leftarrow \sum_{i=1}^{s} \nu_{i,1} R$.
Use Corollary 2.2 to compute $\alpha_1, \alpha_2 \in \mathfrak{a}_1$ and $\beta_1, \beta_2 \in \mathfrak{a}_1^{-1}$ such that $\alpha_1\beta_1 + \alpha_2\beta_2 = 1$.
for $l \in \{1, 2\}$ **do**
  Compute $(r_{i,l})_{1 \leq i \leq r} \in R^r$ such that $\alpha_l = \sum_{i=1}^{r} r_{i,l} \nu_{i,1}$.
  $h_l \leftarrow \sum_{i=1}^{r} r_{i,l} m_i$.
  $w_l \leftarrow \alpha_l v_1 - h_l \in \bigoplus_{k \leq 2} v_k K$.
end for
$b_1 \leftarrow v_1 - (\beta_1 w_1 + \beta_2 w_2)$.
for $i \in \{1, \dots, s\}$ **do**
  $m'_i \leftarrow m_i - \nu_{i,1} b_1$.
end for
$(b_i, \mathfrak{a}_i)_{2 \leq i \leq r} \leftarrow$ the output of Algorithm 1 with $\{m'_2, \dots, m'_s\}$.
return $(b_i, \mathfrak{a}_i)_{1 \leq i \leq r}$.

Lemma 2.9. *Given a torsion-free module M over R of rank r with generating set $\{m_1, \ldots, m_s\}$ $(s \geq r)$, Algorithm 1 outputs a pseudo-basis of M.*

Proof. For $l \in \{1, 2\}$, w_l is in $\bigoplus_{k=2}^{r} Kv_k$ because $h_l = \sum_{i=1}^{r} r_{i,l} m_i = \sum_{j=1}^{r} (\sum_{i=1}^{r} r_{i,l}\nu_{i,j}) v_j = \alpha_l v_1 + \sum_{j=2}^{r} (\sum_{i=1}^{r} r_{i,l}\nu_{i,j}) v_j$. Also at step 15, $b_1 = v_1 - (\beta_1 w_1 + \beta_2 w_2) = v_1 - (\beta_1(\alpha_1 v_1 - h_1) + \beta_2(\alpha_2 v_1 - h_2)) = \beta_1 h_1 + \beta_2 h_2$ (using $\alpha_1\beta_1 + \alpha_2\beta_2 = 1$). Since $h_1, h_2 \in M$ and $\beta_1, \beta_2 \in \mathfrak{a}_1^{-1}$, it gives $b_1 \in \mathfrak{a}_1^{-1} M$. Let $i \in \{1, \ldots, s\}$, then $\nu_{i,1} \in \mathfrak{a}_1$ implies $\mathfrak{a}_1^{-1} \subset (\nu_{i,1} R)^{-1} = \nu_{i,1}^{-1} R$, so $\nu_{i,1} b_1 \in M$ and this proves $m_i' \in M$.
For any $i \in \{1, \ldots, s\}$, we have by construction $m_i' \in M$ and $m_i - m_i' = \nu_{i,1} b_1 \in \mathfrak{a}_1 b_1 \cap M$ thus $\mathfrak{a}_1 b_1 \subset M$ (by definition of $\mathfrak{a}_1$). Using the latter equality and the fact that $\{m_i\}_{1 \leq i \leq s}$ is a generating set of M, we obtain

$$M = \mathfrak{a}_1 b_1 + \sum_{i=1}^{s} m_i' R. \tag{6}$$

Also, $b_1 \in \{v_1\} + \bigoplus_{k=2}^{r} Kv_k$ so for any $i \in \{1, \ldots, s\}$,

$$\begin{aligned} m_i' &= m_i - \nu_{i,1} b_1 \\ &= m_i - \nu_{i,1} v_1 + \nu_{i,1}(\beta_1 w_1 + \beta_2 w_2) \\ &= \sum_{j=2}^{r} \nu_{i,j} v_j + \nu_{i,1}(\beta_1 w_1 + \beta_2 w_2) \\ &\in \bigoplus_{k=2}^{r} Kv_k. \end{aligned}$$

Therefore, the sum in (6) is direct and $M' := \sum_{i=1}^{s} m_i' R \subset \bigoplus_{k=2}^{r} Kv_k$ so M' has rank $r - 1 = \mathrm{rank}(M) - 1$. An induction on the rank of M completes the proof. □

Remark. Another application of Lemma 2.11 is an algorithmic procedure to transform a pseudo-basis of M into a Steinitz representation (see Fig. 5 of [15] or Algorithm 4.6.2 of [18]).
Pseudo-matrices and the CHNF. In his book [11], Cohen defines the notion of pseudo-matrices and he gives an algorithm to compute their CHNF (Cohen-Hermite Normal Form), which is an adaptation of the HNF to pseudo-matrices.

Definition. A pseudo-matrix is a pair $(B, (\mathfrak{a}_i)_i)$ where $B \in M_{l \times m}(K)$ and $(\mathfrak{a}_i)_i$ is a list of m fractional ideals. Another convention to represent the pseudo-matrix $(B, (\mathfrak{a}_i)_i)$ is

$$\begin{pmatrix} \mathfrak{a}_1 & \ldots & \mathfrak{a}_m \\ b_1 & \ldots & b_m \end{pmatrix},$$

where $(b_i)_{1 \leq i \leq m}$ are the column vectors of B. The module associated with this pseudo-matrix is $M = \sum_{1 \leq i \leq m} \mathfrak{a}_i b_i \subset K^l$.[8] Two pseudo-matrices $(B, (\mathfrak{a}_i)_i)$, $(B', (\mathfrak{b}_i)_i)$ such that $B \in M_{l \times m}(K)$ and $B' \in M_{l \times m'}(K)$ are said multiplication equivalent if there exists $U = (u_{i,j}) \in M_{m \times m'}(K)$ and $V = (v_{i,j}) \in M_{m' \times m}(K)$ satisfying :

[8] This means $(b_i, \mathfrak{a}_i)_i$ is a (pseudo-)generating set for M but it is *a priori* not a pseudo-basis since the sum is not direct.

- $BU = B'$.
- For all $i \in \{1, \dots, m\}$ and $j \in \{1, \dots, m'\}$, $u_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$.
- $B = B'V$
- For all $i \in \{1, \dots, m'\}$ and $j \in \{1, \dots, m\}$, $v_{i,j} \in \mathfrak{b}_i \mathfrak{a}_j^{-1}$.

Lemma 2.10. *Multiplication equivalence is an equivalence relation on the set of pseudo-matrices. Two pseudo-matrices are equivalent if and only if the modules associated are equal.*

Proof. See Proposition 4.3.2 of [18]. □

Now we are interested in giving a « canonical » representative of an orbit for this action : the Cohen-Hermite Normal Form.

Theorem 2.12 (Cohen-Hermite Normal Form in Dedekind domains, Theorem 1.4.6 of [11])**.** *Let $(B, (\mathfrak{a}_i)_i)$ be a pseudo-matrix with $B \in M_{l \times m}(K)$ of rank l and M be the module-lattice of K^l associated. Then, B is equivalent to a pseudo-matrix of the form*

$$\begin{pmatrix} \mathfrak{d}_1 & \dots & \mathfrak{d}_{m-l} & \mathfrak{d}_{m-l+1} & \dots & \mathfrak{d}_m \\ 0 & \dots & 0 & b'_1 & \dots & b'_l \end{pmatrix} \quad \text{and} \quad H := (b'_1 | \dots | b'_l) = \begin{pmatrix} 1 & * & \dots & * \\ 0 & 1 & \dots & * \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & 1 \end{pmatrix} \in \mathbf{GL}_l(K)$$

is reduced echelon on the lines. Putting $\mathfrak{b}_i := \mathfrak{d}_{m-l+i}$ for $1 \leq i \leq l$, we say that $(H, (\mathfrak{b}_i)_{1 \leq i \leq l})$ is in CHNF (Cohen-Hermite Normal Form). Moreover, $(b'_i, \mathfrak{b}_i)_{1 \leq i \leq l}$ is a pseudo-basis of M.

Proof. The construction of $U \in \mathbf{GL}_{l \times k}(K)$ such that $BU = (0|H)$ is given as an algorithm in [11]. We refer to section 4.5 of [18] or [4] for more details. By the previous lemma, the module generated by $(H, (\mathfrak{b}_i)_{1 \leq i \leq l})$ is equal to M *i.e.*, $M = \sum_{1 \leq i \leq l} b'_i \mathfrak{b}_i$ and the sum must be direct because H is a triangular matrix. □

Proposition 2.12. *With the notations used in the previous theorem, the pseudo-matrix $(H, (\mathfrak{b}_i)_i)$ is unique in the sense that two equivalent pseudo-matrices in CHNF are equal.*

Thus, H is called the CHNF of M (it depends only on M and not on the choice of a pseudo-generating set).

Proof. See Proposition 4.4.4 in [18]. □

Proposition 2.13 (Algorithm 5 and Theorem 34 of [4])**.** *There is a probabilistic polynomial-time algorithm computing the CHNF of a full rank pseudo-matrix.*

Corollary 2.3 (Corollary A.3. of [6])**.** *There is a probabilistic polynomial-time algorithm that given a pseudo-generating set of a module $M \subset K^l$, computes a Steinitz form for M*

2.4.3 Module lattices and their representations.

In the case of a module M contained in K^l, it is possible to embed M into $\mathbb{R}^{nl}$ (where $n = [K : \mathbb{Q}]$ and l is the rank of M), by applying component-wise Minkowski embedding. The result is a full-rank lattice denoted $f \circ \mu(M)$. Whereas M is a purely algebraic object, the embedded lattice must also have geometric considerations.

Definition. A rank l module-lattice over K is a module $M \subset K^l$ (in the sense of the previous paragraph) identified with the lattice $\mu(M) \subset \mathbb{R}^{nl}$ which is equipped with the geometry induced by the one of $\mathbb{R}^{nl}$.

Let M be a rank l module-lattice over K with pseudo-basis $(b_i, \mathfrak{a}_i)_{1 \leq i \leq l}$ and integral coefficient ideals (or equivalently the module-lattice associated to the pseudo-matrix $\mathbf{B} = ((b_1 | \dots | b_l), (\mathfrak{a}_i)_{1 \leq i \leq l})$). We give a $\mathbb{R}$-basis for the lattice $\mu(M)$ (or equivalently the image of $\mathbf{B}$ by the canonical embedding). Recall that each (integral) ideal $\mathfrak{a}_i$ is represented by a $\mathbb{Z}$-basis $\{\varepsilon_1^{(i)}, \dots, \varepsilon_n^{(i)}\} \subset K$ therefore for any $i \in \{1, \dots l\}$, the image of the rank one $\mathcal{O}_K$-module $b_i\mathfrak{a}_i \subset K^l$ is a rank n lattice of $\mathbb{R}^{nl}$ with matrix (in the canonical basis)

$$M_i := \begin{pmatrix} \boxed{f \circ \mu\left(b_{i,1}\varepsilon_1^{(i)}\right)}^T & \cdots & \boxed{f \circ \mu\left(b_{i,1}\varepsilon_n^{(i)}\right)}^T \\ \vdots & \cdots & \vdots \\ \boxed{f \circ \mu\left(b_{i,l}\varepsilon_1^{(i)}\right)}^T & \cdots & \boxed{f \circ \mu\left(b_{i,l}\varepsilon_n^{(i)}\right)}^T \end{pmatrix} \in M_{nl,n}(\mathbb{R}),$$

where b_i has coordinates $(b_{i,1}, \dots b_{i,l})^T$ in the canonical basis of K^l and $\mu\left(b_{i,j}\varepsilon_k^{(i)}\right) \in \mathbb{R}^n$ is a row vector. Equivalently, M_i is the image of the pseudo matrix $(b_i, \mathfrak{a}_i)$. Then, a basis for $\mu(M)$ in the canonical basis of $\mathbb{R}^{nl}$ is

$$\mathrm{emb}(\mathbf{B}) := (M_1 | \dots | M_l) \in M_{nl}(\mathbb{R}).$$

3 Contributions to module-LIP

In [13] is introduced (the uncompressed version of) Hawk, a signature scheme which security relies on a Lattice Isomorphism Problem (LIP) problem in the special case where $K = \mathbb{Q}(\zeta)$ is a power-of-two cyclotomic field and $\mathcal{L}$ is the free rank 2 module-lattice $\mathcal{O}_K^2$. Explicitly, the secret key is given by a basis $B \in \mathbf{GL}_2(\mathcal{O}_K)$ of $\mathcal{L}$ and the public key is the Hermitian form $Q = B^*B$. To sign a message $\mathbf{m}$, first hash $\mathbf{m}$ and a salt $\mathbf{r}$ to a point $\mathbf{h} = (h_0, h_1)^T \in \{0,1\}^{2n}$ and compute the target $\mathbf{t} = \frac{1}{2}B \cdot \mathbf{h}$. Then sample an element $\mathbf{x}$ in the target coset's $\mathcal{O}_K^2 + \frac{1}{2}B \cdot \mathbf{h}$ close to $\mathbf{t}$, using Gaussian sampling. Finally, $\mathbf{s} := \frac{1}{2}\mathbf{h} \pm B^{-1}\mathbf{x} \in \mathcal{O}_K^2$ should be close to $\frac{1}{2}\mathbf{h}$ with respect to $||\cdot||_Q$. The verification step is to compute $||\frac{1}{2}\mathbf{h} - \mathbf{s}||_Q$ and this only requires the public key Q. Notice that the problem of recovering the secret key B from Q is indeed a LIP problem (stated with hermitian forms) : the two Hermitians forms $\mathrm{Id}_2(K)$ and Q are equivalent and the problem asks for finding a matrix $U \in \mathbf{GL}_2(\mathcal{O}_K)$ such that $U^*\mathrm{Id}_2(K)U = U^*U = Q$. Lattices considered there have a special shape compared to module lattices in general. Indeed, free module lattices have a basis and not only a pseudo-basis, or said equivalently, their coefficient ideals are trivial. A first goal of this section is to define a lattice isomorphism problem for module lattices generalizing the example used in Hawk. We need to incorporate coefficient ideals to the problem so the natual objects to consider are pseudo-bases or pseudo-Gram matrices (in perspective of a reformulation in terms of Hermitian forms).

3.1 The module-Lattice Isomorphism Problem

As for unstructured lattices, we state the Lattice Isomorphism Problem over modules in two different ways, the first in terms of module-lattices and the second with pseudo-Gram matrices. Let K be a number field of degree n, $\mathcal{O}_K$ its ring of integers and $l \geq 1$ an integer. $M \subset K^l$ denotes a module-lattice with pseudo-basis $\mathbf{B} = (B, (\mathfrak{a}_i)_{1 \leq i \leq l})$. The latter is a pseudo-matrix, as defined in [11]. In [13] the authors ask for the secret key U to have coefficients in $\mathcal{O}_K$ and determinant one, in order to make key generation more effective (see Algorithms 4 and 6 in [13]). This is not a condition we can keep in general, as U is the matrix of a pseudo-base change.

3.1.1 Statements

Module-lattice setting. Let $M' \subset K^l$ be a module-lattice, we say that M, M' are isomorphic if there exists a unitary transformation $O \in U_l(K_\mathbb{R})$ (*i.e.*, $O \in M_l(K_\mathbb{R})$ satisfying $O^*O = Id$) such that $M' = O \cdot M$.

Let **B'** $= (B', (\mathfrak{b}_i)_{1 \leq i \leq l})$ be a pseudo-basis for M', then M and M' are isomorphic if and only if there exists a unitary transformation $O \in U_l(K_\mathbb{R})$ such that

$$M' = b'_1\mathfrak{b}_1 \oplus \cdots \oplus b'_l\mathfrak{b}_l = Ob_1\mathfrak{a}_1 \oplus \cdots \oplus Ob_l\mathfrak{a}_l = O \cdot M,$$

where the b_i (resp. b'_i) are the columns vectors of B (resp. B'). Applying proposition 2.10, this means there exists $U = (u_{i,j})_{1 \leq i,j \leq l} \in \mathbf{GL}_l(K)$ such that $B' = OBU$ and $u_{i,j} \in \mathfrak{a}_i\mathfrak{b}_j^{-1}$, $\mathfrak{a} = (\det U)\mathfrak{b}$, where $\mathfrak{a} = \mathfrak{a}_1 \dots \mathfrak{a}_l$ and $\mathfrak{b} = \mathfrak{b}_1 \dots \mathfrak{b}_l$. We saw in the proof of this proposition

that the conjunction of these two last conditions is equivalent to

$$\begin{cases} u_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1} \\ v_{i,j} \in \mathfrak{b}_i \mathfrak{a}_j^{-1} \end{cases} (\star)$$

for any $i, j \in \{1, \ldots, l\}$ and where $V = (v_{i,j})_{1 \leq i,j \leq l}$ is the inverse of U. From now on, $(\star)$ will refer to the system of conditions above. Finding such O and U is what we define to be a (worst-case) search module-lattice isomorphism problem.

Definition (wc-smodLIP$_K^{\mathbf{B}}$)**.** For $\mathbf{B} = (B, (\mathfrak{a}_i)_{1 \leq i \leq l})$ a pseudo-basis of a module-lattice $M \subset K^l$, the worst-case search module-Lattice Isomorphism Problem with parameters K and $\mathbf{B}$ denoted by wc-smodLIP$_K^{\mathbf{B}}$ is, given any pseudo-basis $\mathbf{B'} = (B', (\mathfrak{b}_i)_{1 \leq i \leq l})$ representing an isomorphic module-lattice $M' \subset K^l$, to find a unitary transformation $O \in U_l(K_{\mathbb{R}})$ and $U = (u_{i,j})_{1 \leq i,j \leq l} \in \mathbf{GL}_l(K)$ such that $B' = OBU$ and $(\star)$ are satisfied.

Remark. Finding either U or O in wc-smodLIP$_K^{\mathbf{B}}$ is sufficient to find the other one efficiently, using linear algebra.

Hermitian form setting. Let $\mathcal{H}_l^{>0}(K)$ be the set of Hermitian definite positive matrices (*i.e.*, the set of matrices $G \in M_l(K)$ such that $G^* = G$ and $x^* G x \in K_{\mathbb{R}}^+ \setminus \{0\}$ for all $x \in \mathbb{K}^l \setminus \{0\}$.)

Definition. A pseudo-matrix $(G, (\mathfrak{b}_i)_{1 \leq i \leq l})$ with $G \in \mathcal{H}_l^{>0}(K)$ is called a pseudo-Gram matrix. To the pseudo basis $\mathbf{B} = (B, (\mathfrak{a}_i)_{1 \leq i \leq l})$ of M we associate a pseudo-Gram matrix defined by $\mathbf{G} := (G, (\mathfrak{a}_i)_{1 \leq i \leq l})$, where $G = B^* B \in \mathcal{H}_l^{>0}(K)$. There is a natural notion of equivalence of pseudo-Gram matrices, compatible with the pseudo-basis change property.

Let $G' \in \mathcal{H}_l^{>0}(K)$ and $(\mathfrak{b}_i)_{1 \leq i \leq l}$ a list of fractional ideals of K. We say that the pseudo-matrix $\mathbf{G'} = (G', (\mathfrak{b}_i)_{1 \leq i \leq l})$ is equivalent to $\mathbf{G}$ if there exists $U = (u_{i,j})_{1 \leq i,j \leq l} \in \mathbf{GL}_l(K)$ such that $G' = U^* G U$ and condition $(\star)$ is verified. This defines an equivalence relation on the set of pseudo-Gram matrices (of size $l \times l$). The class of $\mathbf{G}$ is denoted $[\mathbf{G}]$.

Proposition 3.1. *Let $\boldsymbol{B} = (B, (\mathfrak{a}_i)_{1 \leq i \leq l})$ be a pseudo-basis of M and $G = B^* B \in \mathcal{H}_l^{>0}(K)$. Then, the ideal $(\det G)(\mathfrak{a}_1 \ldots \mathfrak{a}_l)^2$ depends only on M and not on the pseudo-basis $\boldsymbol{B}$. It is called the discriminant ideal of M and denoted disc(M).*

Proof. Let $(B', (\mathfrak{b}_i)_{1 \leq i \leq l})$ be another pseudo-basis for M. By Proposition 2.10, there exists $U \in \mathbf{GL}_l(K)$ such that $B' = BU$ and $\mathfrak{a} = (\det U)\mathfrak{b}$ (with same notations as the proposition). Let $G' = B'^* B' = U^* G U$ then,

$$(\det G')\mathfrak{b}^2 = (\det G)(\det U)^2 \mathfrak{b}^2 = (\det G)\mathfrak{a}^2.$$

□

Definition (wc-smodLIP$_K^{\mathbf{G}}$)**.** For $\mathbf{G} := (G, (\mathfrak{a}_i)_{1 \leq i \leq l})$ with $G \in \mathcal{H}_l^{>0}(K)$, the worst-case search module-Lattice Isomorphism Problem with parameter K and $\mathbf{G}$ denoted wc-smodLIP$_K^{\mathbf{G}}$ is, given any equivalent pseudo-matrix $\mathbf{G'} = (G', (\mathfrak{b}_i)_{1 \leq i \leq l})$, to find a matrix $U = (u_{i,j})_{1 \leq i,j \leq l} \in \mathbf{GL}_l(K)$ such that $G' = U^* G U$ and condition $(\star)$ is verified.

Finally, we define the decisional problem associated to module-LIP.

Definition (wc-Δ-modLIP$_K^{\mathbf{G}_1,\mathbf{G}_2}$)**.** For two pseudo-Gram matrices $\mathbf{G}_0$, $\mathbf{G}_1$ the worst-case distinguishing Lattice Isomorphism Problem (wc-Δ-modLIP$_K^{\mathbf{G}_1,\mathbf{G}_2}$) with parameters $\mathbf{G}_1$,$\mathbf{G}_2$ is, given any pseudo-Gram matrix $\mathbf{G}$ equivalent to G_b (for some b in $\{0,1\}$), to find b.

3.1.2 Equivalence over $K_{\mathbb{R}}$.

Cholesky factorization over $K_{\mathbb{R}}$. For unstructured lattices, we have seen in Proposition 1.3 that the search-LIP problems stated with lattices or quadratic forms are equivalent. The proof uses the fact that from a positive definite quadratic form Q we can efficiently recover B such that $B^TB = Q$ *e.g.*, the Cholesky factorization of Q. For Hermitian forms over K, the Cholesky factorization may not have coefficients in K (the formula (1) requires taking square roots) so the same argument fails. However, we have a factorization for positive definite Hermitian forms over $K_{\mathbb{R}}$. We follow the definitions given by Okuda and Yano in [26] to extend the objects involved in mod-LIP over K to $K_{\mathbb{R}}$.

Definition. A Hermitian form G with coefficients in $K_{\mathbb{R}}$ is said positive definite if for all $x \in (K_{\mathbb{R}})^l \setminus \{0\}$, $x^*Gx \in K_{\mathbb{R}}^+ \setminus \{0\}$. The norm associated to G is $||x||_G := Tr(x^*Gx)$, where $x \in (K_{\mathbb{R}})^l$. This set of matrices is denoted $\mathcal{H}_l^{>0}(K_{\mathbb{R}})$. Two forms $G, G' \in \mathcal{H}_l^{>0}(K_{\mathbb{R}})$ are said K-equivalent if there exists $U \in \mathbf{GL}_l(K)$ such that $G' = U^*GU$. To any matrix $B = (b_{i,j})_{1\leq i,j\leq l} \in \mathbf{GL}_l(K)$, we associate $\tilde{B} := (\mu(b_{i,j}))_{1\leq i,j\leq l} \in \mathbf{GL}_l(K_{\mathbb{R}})$. Notice that if $G \in \mathcal{H}_l^{>0}(K)$, then $\widetilde{G} \in \mathcal{H}_l^{>0}(K_{\mathbb{R}})$.

Remark. For any $B \in \mathbf{GL}_l(K_{\mathbb{R}})$, we have $B^*B \in \mathcal{H}_l^{>0}(K_{\mathbb{R}})$ as for any $y = (y_1, \ldots, y_l)^T \in (K_{\mathbb{R}})^l \setminus \{0\}$, $y^*y = \sum_{i=1}^l \overline{y_i}y_i \in K_{\mathbb{R}}^+$.

Proposition 3.2 (Cholesky factorization over $K_{\mathbb{R}}$)**.** *Let $G \in \mathcal{H}_l^{>0}(K_{\mathbb{R}})$, then there exists a Cholesky factorization $G = R^*R$ with coefficient in $K_{\mathbb{R}}$ and it is computable in polynomial time.*

Proof. For $l = 1$, we have $G = (g)$ with $g \in K_{\mathbb{R}}^+$ so it has a square root $R = (r) \in K_{\mathbb{R}}$. Now suppose there is a factorization for all $G_0 \in \mathcal{H}_{l-1}^{>0}(K_{\mathbb{R}})$ and let $G \in \mathcal{H}_l^{>0}(K_{\mathbb{R}})$. We write G as

$$G = \left(\begin{array}{c|c} G_0 & g \\ \hline g^* & e \end{array}\right),$$

where $G_0 \in \mathcal{H}_{l-1}^{>0}(K_{\mathbb{R}})$ (it is positive definite by restriction of G to $(K_{\mathbb{R}})^{l-1} \times \{0\}$), $g \in M_{l-1,1}(K_{\mathbb{R}})$ and $e \in K_{\mathbb{R}}$. By hypothesis, there exists $R_0 \in \mathbf{GL}_{l-1}(K_{\mathbb{R}})$ upper-triangular such that $G_0 = R_0^*R_0$. We look for $R \in \mathbf{GL}_l(K_{\mathbb{R}})$ such that $G = R^*R$ and with shape

$$R = \left(\begin{array}{c|c} R_0 & r \\ \hline 0 & s \end{array}\right),$$

where $r \in M_{l-1,1}(K_{\mathbb{R}})$ and $s \in K_{\mathbb{R}}$. From $G = R^*R$ we obtain the conditions $R_0^*r = g$ and $r^*r + \overline{s}s = e$, so $r = (R_0^*)^{-1}g$ and $\overline{s}s = e - g^*R_0^{-1}(R_0^*)^{-1}g = e - g^*G_0^{-1}g$. Therefore

the only thing to prove is that $e - g^*G_0^{-1}g \in K_{\mathbb{R}}^+$ (this implies the existence of s). Let $v = \begin{pmatrix} -G_0^{-1}g \\ 1 \end{pmatrix} \in M_{l,1}(K_{\mathbb{R}})$, we check that

$$v^*Gv = (-g^*G_0^{-1}\ 1)\left(\begin{array}{c|c} G_0 & g \\ \hline g^* & e \end{array}\right)\begin{pmatrix} -G_0^{-1}g \\ 1 \end{pmatrix} = (-g^*G_0^{-1}\ 1)\begin{pmatrix} 0 \\ -g^*G_0^{-1}g + e \end{pmatrix} = e - g^*G_0^{-1}g.$$

The computation of R is effective since it is given by the formulae 1. □

Modules over $K_{\mathbb{R}}$. A natural extension of module-lattices is to consider $\mathcal{O}_K$-modules $M \subset (K_{\mathbb{R}})^l$ which admit a pseudo-basis *i.e.*, $\mathcal{O}_K$-modules of the form

$$M = \mathfrak{a}_1 b_1 \oplus \cdots \oplus \mathfrak{a}_l b_l,$$ [9]

with fractional ideals $\mathfrak{a}_i \in I(\mathcal{O}_K)$ and $b_i \in (K_{\mathbb{R}})^l$ are $K_{\mathbb{R}}$-linearly independent vectors. We call pseudo-matrices with coefficients in $K_{\mathbb{R}}$ the pseudo-objects $(B, \{\mathfrak{a}_i\}_{1\le i\le l})$ with $B \in \mathbf{GL}_l(K_{\mathbb{R}})$.

One can prove that for any module M as above, there exists $g \in \mathbf{GL}_l(K_{\mathbb{R}})$ such that $g(M)$ is a module-lattice (contained in K^l). Considering its Steinitz form $g(M) \simeq \mathcal{O}_K^{l-1} \oplus \mathfrak{a}$ and a system of representatives $\mathcal{O}_K, \mathfrak{a}_1, \dots \mathfrak{a}_r$ for the class group $Cl(\mathcal{O}_K)$, we see that the set of modules in $(K_{\mathbb{R}})^l$ can be identified with the disjoint union $\bigsqcup_{1\le i\le} \mathcal{L}_i$ where $\mathcal{L}_i$ is the $\mathbf{GL}_l(K_{\mathbb{R}})$-orbit of $\mathcal{O}_K^{l-1} \oplus \mathfrak{a}_i$. Pseudo-bases change for modules in $(K_{\mathbb{R}})^l$ formulates identically as 2.10.

Representing modules in $(K_{\mathbb{R}})^l$. Let $B = (b_{i,j})_{1\le i,j\le l} \in \mathbf{GL}_l(K_{\mathbb{R}})$, $\mathfrak{a}_1, \dots, \mathfrak{a}_l \subset \mathcal{O}_K$ and $\varepsilon^{(i)} = \{\varepsilon_1^{(i)}, \dots, \varepsilon_l^{(i)}\}$ a $\mathbb{Z}$-basis of $\mathfrak{a}_i$ ($i \in \{1, \dots, l\}$). The lattice associated to $\mathbf{B}$:$= (B, (\mathfrak{a}_i)_{1\le i\le l})$ has rank nl with basis

$$\varphi(\mathbf{B}) = \begin{pmatrix} \boxed{f\left(b_{1,1}\varepsilon_1^{(i)}\right)}^T & \cdots & \boxed{f\left(b_{1,1}\varepsilon_n^{(i)}\right)}^T & \cdots & \boxed{f\left(b_{l,1}\varepsilon_1^{(i)}\right)}^T & \cdots & \boxed{f\left(b_{l,1}\varepsilon_n^{(i)}\right)}^T \\ \vdots & \cdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ \boxed{f\left(b_{1,l}\varepsilon_1^{(i)}\right)}^T & \cdots & \boxed{f\left(b_{1,l}\varepsilon_n^{(i)}\right)}^T & \cdots & \boxed{f\left(b_{l,l}\varepsilon_1^{(i)}\right)}^T & \cdots & \boxed{f\left(b_{l,l}\varepsilon_n^{(i)}\right)}^T \end{pmatrix},$$

where $f : \mathbb{K}_{\mathbb{R}} \to \mathbb{R}^n$ is the canonical isometry defined in Section 2.2.1 and the $\varepsilon_j^{(i)}$ are seen as elements of $K_{\mathbb{R}}$. Thus, $\varphi(\mathbf{B}) \in \mathbf{GL}_{nl}(\mathbb{R})$ is a basis of a full-rank lattice $\subset \mathbb{R}^{nl}$.

Definition (wc-smodLIP$^{\mathbf{B}}_{K_{\mathbb{R}}}$)**.** For $\mathbf{B} = (B, (\mathfrak{a}_i)_{1\le i\le l})$ a pseudo-basis of a module-lattice $M \subset (K_{\mathbb{R}})^l$, the worst-case search module-Lattice Isomorphism Problem with parameters K and $\mathbf{B}$ denoted by wc-smodLIP$^{\mathbf{B}}_{K_{\mathbb{R}}}$ is, given any pseudo-basis $\mathbf{B'} = (B', (\mathfrak{b}_i)_{1\le i\le l})$ representing an isomorphic module-lattice $M' \subset (K_{\mathbb{R}})^l$, to find a unitary transformation $O \in U_l(K_{\mathbb{R}})$ and $U = (u_{i,j})_{1\le i,j\le l} \in \mathbf{GL}_l(K)$ such that $B' = OBU$ and ($\star$) are satisfied.

Definition (wc-smodLIP$^{\mathbf{G}}_{K_{\mathbb{R}}}$)**.** For $\mathbf{G} := (G, (\mathfrak{a}_i)_{1\le i\le l})$ with $G \in \mathcal{H}_l^{>0}(K_{\mathbb{R}})$, the worst-case

[9] The theory of modules over a Dedekind ring does not apply anymore since KM is not a K-vector space of finite dimension, so the existence of a pseudo-basis is not guaranteed. We restrict ourselves to modules with this shape, as defined in [26].

search module-Lattice Isomorphism Problem with parameters K and $\mathbf{G}$ denoted wc-smodLIP$^{\mathbf{G}}_{K_{\mathbb{R}}}$ is, given any K-equivalent pseudo-matrix $\mathbf{G'} = (G', (\mathfrak{b}_i)_{1\leq i\leq l})$, to find $U = (u_{i,j})_{1\leq i,j\leq l} \in \mathbf{GL}_l(K)$ such that $G' = U^*GU$ and condition $(\star)$ is verified.

Proposition 3.3. *For $G = B^*B$,* wc-smodLIP$^{\boldsymbol{B}}_{\mathrm{K}_{\mathbb{R}}}$ *is equivalent to* wc-smodLIP$^{\boldsymbol{G}}_{\mathrm{K}_{\mathbb{R}}}$.

Proof. Given an oracle that solves wc-smodLIP$^{\mathbf{B}}_{K_{\mathbb{R}}}$ in time $T(\cdot)$ and any pseudo-matrix $\mathbf{G'} = (G', (\mathfrak{b}_i)_{1\leq i\leq l})$ K-equivalent to $\mathbf{G}$, one can solve wc-smodLIP$^{\mathbf{G}}_{K_{\mathbb{R}}}$ by first computing $B' \in \mathbf{GL}_l(K_{\mathbb{R}})$ such that $B'^*B' = G'$ using Cholesky decomposition over $K_{\mathbb{R}}$, in time $poly(l)$, and then apply the oracle to $(B', (\mathfrak{b}_i)_{1\leq i\leq l})$; we obtain $O \in U_l(K_{\mathbb{R}})$ and $U \in \mathbf{GL}_l(K)$ such that $B' = OBU$ and $(\star)$ are verified. In particular, $G' = U^*GU$, so this solves wc-smodLIP$^{\mathbf{G}}_{K_{\mathbb{R}}}$ instantiated with $\mathbf{G'}$ in time $T(\mathbf{B'}) + poly(l)$.
Conversely, suppose we can solve wc-smodLIP$^{\mathbf{G}}_{K_{\mathbb{R}}}$ in time $S(\cdot)$ and let $\mathbf{B'} = (B', (\mathfrak{b}_i)_{1\leq i\leq l})$ be a pseudo-basis of an isomorphic module-lattice $M' \subset ({K_{\mathbb{R}}}^l)$. Let $G' = B'^*B' \in \mathcal{H}^l_{>0}(K_{\mathbb{R}})$ and $\mathbf{G'} = (G', (\mathfrak{b}_i)_{1\leq i\leq l})$. This time, our oracle applied to $\mathbf{G'}$ gives $U \in \mathbf{GL}_l(K)$ such that $G' = U^*GU$ and $(\star)$ is satisfied, in time $S(\mathbf{G'})$. Then, $O = B'(BU)^{-1} \in \mathbf{GL}_l(K_{\mathbb{R}})$ and we check $O \in U_l(K_{\mathbb{R}})$ so (O, U) is a solution to wc-smodLIP$^{\mathbf{B}}_{K_{\mathbb{R}}}$ instantiated with $\mathbf{B'}$ and it is computed in time $S(\mathbf{G'}) + poly(l)$. □

3.2 Average-case problem

3.2.1 Gaussian sampling

Discrete Gaussian Sampling (DGS) is a useful tool in lattice-based cryptography ; from a (secret) basis of a lattice $\mathcal{L}$ we are able to sample short vectors of $\mathcal{L}$, following a Gaussian distribution and without leaking any information on the basis. This has been developed for general lattices, *i.e.*, unstructured lattices, so we state the fundamental properties of the DGS in this context. This section is inspired from [12] where the authors did a worst-case to average-case reduction for free rank two module-lattices.

Notations. Let $Q \in \mathcal{S}^{>0}_m(\mathbb{R})$ be a positive definite quadratic form on $\mathbb{R}^m$, B_Q be the result of Cholesky algorithm applied to Q and B^*_Q the Gram Schmidt orthogonalisation of B_Q. The norm on $\mathbb{R}^m$ associated to Q is defined by

$$||x||^2_Q := x^T Q x, \quad \text{for } x \in \mathbb{R}^m.$$

For $i \in \{1, \ldots, m\}$, $\lambda_i(Q)$ is the smallest positive real number r such that $\{x \in \mathbb{Z}^m \,|\, ||x||_Q \leq r\}$ spans a vector space of dimension at least i. Notice that this corresponds to $\lambda_i(\mathcal{L})$, where $\mathcal{L}$ is the lattice of $\mathbb{R}^m$ with basis B_Q. Indeed, every lattice vector y in $\mathcal{L}$ can be written $y = B_Q \cdot x$ with $x \in \mathbb{Z}^m$ thus $||y||$ is equal to $||x||_Q$. Finally, we define $||B^*_Q||$ to be the max of the euclidean norms of the columns vectors of B^*_Q.

Definition. The Gaussian function on $\mathbb{R}^m$ with parameter $s > 0$ (and centered at the origin) is defined by

$$\forall\, x \in \mathbb{R}^m, \quad \rho_{Q,s}(x) := \exp(-\pi ||x||^2_Q / s^2).$$

The Discrete Gaussian Distribution $\mathcal{D}_{Q,s}$ is the distribution on $\mathbb{Z}^m$ obtained by

$$\mathop{\mathbb{P}}_{X\sim\mathcal{D}_{Q,s}}(X=x) := \begin{cases} \rho_{Q,s}(x)/\rho_{Q,s}(\mathbb{Z}^m), & \text{if } x\in\mathbb{Z}^m. \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 3.1 (Lemma 2.3 of [8]). *There is an algorithm* ***DiscreteSample***(Q,s) *that given Q and a parameter $s \geq ||B_Q^*||\sqrt{\log(2m+4)/\pi}$, returns a sample $y\in\mathbb{Z}^m$ distributed as $\mathcal{D}_{Q,s}$. It runs in time poly$(m,\log s)$.*

3.2.2 Worst-case to average-case reduction

In the following, we fix a number field K of degree n over $\mathbb{Q}$ and an integer $l\geq 1$. Let $\mathbf{G}=(G,(\mathfrak{a}_i)_{1\leq i\leq l})$ be a pseudo-Gram matrix with coefficient in K, using DGS and the CHNF algorithm of [11], we give an algorithm sampling pseudo-Gram matrices equivalent to $\mathbf{G}$ such that the distribution depends only on the class of equivalence $[\mathbf{G}]$ and not on $\mathbf{G}$, in a sense that will be precised in Lemma 3.4 (this provides security against an opponent having access to the sampling algorithm). From this follows an average case version of smod-LIP (with parameters K and $\mathbf{G}$) called ac-smodLIP$_K^{\mathbf{G}}$; the input is an equivalent form sampled from this distribution and the problem is still to find the pseudo-base change. Finally, we prove a reduction result : if one can solve the average-case problem, then the worst-case can be solved (within approximately same time).

Sampling from a class of equivalence. First we describe a method to sample elements in $\mathfrak{a}_1\times\cdots\times\mathfrak{a}_l$ following a Gaussian distribution. This combined with the CHNF algorithm of [11] produces equivalent forms ; this is Algorithm 2. To be able to sample in $\mathfrak{a}_1\times\cdots\times\mathfrak{a}_l$, we consider $\mathbb{Z}$-basis of each ideal and we use DGS in $\mathbb{R}^{nl}$. This requires to associate a quadratic form $Q\in\mathcal{S}_{nl}^{>0}(\mathbb{R})$ to the pseudo-Gram matrix $\mathbf{G}$. This can be done in the following way.

Definition. For any $g\in K$ and ordered set $\varepsilon=\{\varepsilon_1,\ldots,\varepsilon_n\}\subset K$ we put

$$\psi_\varepsilon(g) := \left(Tr\left(\overline{\varepsilon_i}\cdot g\cdot\varepsilon_j\right)\right)_{1\leq i,j\leq n}\in M_n(\mathbb{R}).$$

Now writing $G=(g_{i,j})_{1\leq i,j\leq l}$ and given $\mathbb{Z}$-bases $\varepsilon^{(i)}=\{\varepsilon_1^{(i)},\ldots,\varepsilon_n^{(i)}\}$ of $\mathfrak{a}_i$ for every $i\in\{1,\ldots,l\}$, we define

$$\psi(\mathbf{G}) := \begin{pmatrix} \boxed{\psi_{\varepsilon^{(1)}}(g_{1,1})} & \cdots & \boxed{\psi_{\varepsilon^{(l)}}(g_{1,l})} \\ \vdots & \ldots & \vdots \\ \boxed{\psi_{\varepsilon^{(1)}}(g_{l,1})} & \cdots & \boxed{\psi_{\varepsilon^{(l)}}(g_{l,l})} \end{pmatrix}\in\mathcal{S}_{nl}(\mathbb{R}).$$

Lemma 3.2. *Given a Cholesky factorization $B_G\in\mathbf{GL}_l(K_\mathbb{R})$ of $\widetilde{G}$, we have*

$$\psi(\boldsymbol{G}) = \varphi(\boldsymbol{B_G})^T\cdot\varphi(\boldsymbol{B_G}),$$

where $\boldsymbol{B_G}=(B_G,(\mathfrak{a}_i)_{1\leq i\leq l})$. In particular $\psi(\boldsymbol{G})$ is positive and definite.

Proof. By assumption, $(g_{i,j})_{1\leq i,j\leq l} := \widetilde{G} = B_G^* B_G$ so $g_{i,j} = \sum_{k=1}^{n} \overline{b_{k,i}} \cdot b_{k,j}$, where $B_G = (b_{i,j})_{1\leq i,j\leq l}$. Let $1 \leq s,t \leq nl$ and $s = in + \alpha$, $t = jn + \beta$ the Euclidean divisions by n. We define $a := \alpha + 1$ and $b := \beta + 1$ so $a, b \in \{1, \ldots, n\}$ and the s-th column of $\varphi(\mathbf{B_G})$ is $\left(f\left(b_{1,i}\varepsilon_a^{(i)}\right) \ \ldots \ f\left(b_{l,i}\varepsilon_a^{(i)}\right)\right)^T$ and the t-th column is $\left(f\left(b_{1,j}\varepsilon_b^{(j)}\right) \ \ldots \ f\left(b_{l,j}\varepsilon_b^{(j)}\right)\right)^T$. Using Lemma 2.5, the coefficient (s,t) of $\varphi(\mathbf{B_G})^T \cdot \varphi(\mathbf{B_G})$ is

$$\sum_{k=1}^{l} \left\langle f\left(b_{k,i}\varepsilon_a^{(i)}\right), f\left(b_{k,j}\varepsilon_b^{(j)}\right)\right\rangle_{\mathrm{E}} = \sum_{k=1}^{l} Tr\left(\overline{b_{k,i}\varepsilon_a^{(i)}} b_{k,j}\varepsilon_b^{(j)}\right) = Tr\left(\overline{\varepsilon_a^{(i)}} \cdot g_{i,j} \cdot \varepsilon_b^{(j)}\right).$$

which is by definition the coefficient (s,t) of $\psi(\mathbf{G})$. □

Definition. The distribution $D_{\mathbf{G},s}$ on $\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_l$ with parameter $s > 0$ is defined by

$$\underset{X\sim\mathcal{D}_{\mathfrak{a}_1\times\cdots\times\mathfrak{a}_l,s}}{\mathbb{P}(X = x)} := \frac{\exp(-\pi||x||_G^2/s^2)}{\sum\limits_{y\in\mathfrak{a}_1\times\cdots\times\mathfrak{a}_l} \exp(-\pi||y||_G^2/s^2)},$$

where $x \in \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_l$ and $||y||_G^2 := Tr\left(y^*\widetilde{G}y\right) \geq 0$, for any $y \in \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_l$.

Lemma 3.3. *Let $\varepsilon^{(i)} = \{\varepsilon_1^{(i)}, \ldots, \varepsilon_n^{(i)}\}$ be a $\mathbb{Z}$-basis of $\mathfrak{a}_i$ and $x := (x_1, \ldots, x_l) \in \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_l$. For every $1 \leq i \leq l$ we put $\left(z_j^{(i)}\right)_j$ the coefficients of x_i in the $\mathbb{Z}$-basis of $\mathfrak{a}_i$ i.e., $x_i = \sum_{j=1}^{n} z_j^{(i)}\varepsilon_j^{(i)}$ and $z = \left(z_j^{(i)}\right)_{i,j}^T \in \mathbb{Z}^{nl}$. Then for any $s > 0$,*

$$\underset{X\sim\mathcal{D}_{\mathfrak{a}_1\times\cdots\times\mathfrak{a}_l,s}}{\mathbb{P}(X = x)} = \underset{X\sim\mathcal{D}_{\psi(\boldsymbol{G}),s}}{\mathbb{P}(X = z)}.$$

Proof. Let $s > 0$. It is enough to prove that

$$\exp(-\pi||x||_G^2/s^2) = \rho_{\psi(\mathbf{G}),s}(z) = \exp(-\pi(z^T\psi(\mathbf{G})z)/s^2).$$

Let $B_G = (b_1 \mid \ldots \mid b_l) \in \mathbf{GL}_l(K_{\mathbb{R}})$ be a Cholesky factorization of $\widetilde{G}$, then by the previous lemma $z^T\psi(\mathbf{G})z = (\varphi(B_G)z)^T\varphi(B_G)z$ and if $\widetilde{b_{ni+a}} \in \mathbb{R}^{nl}$ denotes the $(ni+a)$-th column of $\varphi(B_G)$, then

$$\varphi(B_G)\cdot z = \sum_{i=1}^{l}\sum_{a=1}^{n} \widetilde{b_{n(i-1)+a}} \cdot z_a^{(i)} = f\Big(\sum_{i=1}^{l} b_i \sum_{a=1}^{n} \varepsilon_a^{(i)} \cdot z_a^{(i)}\Big) = f\Big(\sum_{i=1}^{l} b_i x_i\Big) = f(B_G \cdot x).$$

Therefore, $z^T\psi(\mathbf{G})z = \langle\varphi(\mathbf{B}_G)z, \varphi(\mathbf{B}_G)z\rangle_E = Tr\Big((B_G\cdot x)^*(B_G\cdot x)\Big) = Tr\Big(x^*\widetilde{G}x\Big) = ||x||_G^2$.□

Using the algorithm **DiscreteSample** with inputs $\psi(\mathbf{G})$ and $s > 0$ we deduce a sampling algorithm in $\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_l$ (recall that the ideal coefficients are represented with a $\mathbb{Z}$-basis so any output of **DiscreteSample**($\psi(\mathbf{G})$,s) corresponds to a coordinate vector of an element in the product). Suppose that $\mathbf{G}$ is a pseudo-Gram matrix associated to a pseudo-basis of a module lattice M then, sampling enough vectors in the product of ideals (enough to get a rank l matrix), we can apply the CHNF algorithm to extract another pseudo-basis of M together with the pseudo-basis change matrix. It follows a pseudo-Gram matrix equivalent to $\mathbf{G}$. Details are given in the following pseudo-code and lemma.

Algorithm 2 Sample equivalent pseudo-Gram matrix.

Require: A pseudo-Gram matrix $\mathbf{G} = (G, (\mathfrak{a}_i)_{1\leq i\leq l})$ coming from a known pseudo-basis of M, and some $s > 0$.

Ensure: A pseudo-Gram matrix **G'** $= (G', (\mathfrak{b}_i)_{1\leq i\leq l})$ equivalent to $\mathbf{G}$ together with the pseudo-base change matrix $U = (u_{i,j})_{1\leq i,j\leq l} \in \mathbf{GL}_l(K)$ such that $G' = U^*GU$.

1: $C \leftarrow 1 - (1 + e^{-\pi})^{-1}$ and $m \leftarrow \lceil \frac{2l}{C} \rceil$
2: **for** $1 \leq i \leq m$ **do**
3: $\quad \mathbb{Z}^{nl} \ni z_i \leftarrow$ **DiscreteSample**$(\psi(\mathbf{G}), s)$
4: $\quad \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_l \ni y_i$ with coordinates z_i.
5: **end for**
6: $Y \leftarrow (y_1 \,|\, \ldots \,|\, y_m) \in M_{l\times m}(K)$
7: **if** Y has rank $< l$ **then**
8: $\quad$ Restart
9: **end if**
10: $(H, (\mathfrak{b}_i^{-1})_{1\leq i\leq l}, U_0) \leftarrow \mathrm{CHNF}(Y^T, (\mathfrak{a}_i^{-1})_{1\leq i\leq l})$, Algorithm 1.4.7 of [11]
11: $U \leftarrow U_0^{-T}$
12: **return** $(\mathbf{G'} = (U^*GU, (\mathfrak{b}_i)_{1\leq i\leq l}), U)$

Lemma 3.4. *For any pseudo-Gram matrix $\boldsymbol{G} = (G, (\mathfrak{a}_i)_{1\leq i\leq l})$ with Cholesky decomposition $B_G \in \mathbf{GL}_l(K_{\mathbb{R}})$ and parameter*

$$s \geq \max\left\{\lambda_{nl}(\psi(\boldsymbol{G})),\ ||\varphi(B_G)^*||\sqrt{\log(2nl+4)/\pi}\right\},$$

*Algorithm 2 returns a pseudo-Gram matrix **G'** $= (G', (\mathfrak{b}_i)_{1\leq i\leq l})$ equivalent to $\boldsymbol{G}$ together with $U = (u_{i,j})_{1\leq i,j\leq l} \in \mathbf{GL}_l(K)$ such that $G' = U^*GU$ and $(\star)$ is verified, with the notation of the previous section. Is it a probabilistic algorithm which runs in expected time poly(n,l,* $\log s$*).*

Moreover, the result depends only on the equivalence class of the input, in the sense that for any equivalent pseudo-Gram matrix $\boldsymbol{H} = (W^*GW, (\mathfrak{d}_i)_{1\leq i\leq l})$, running steps 9-11 with $\boldsymbol{H}$ and $W^{-1}Y$ instead of $\boldsymbol{G}$ and Y gives the same pseudo-Gram matrix. Thus, Algorithm 2 defines a distribution over $[\boldsymbol{G}]$ which follows a Gaussian distribution. This is called the Gaussian form distribution with parameter $s > 0$, denoted $\mathcal{D}_s([\boldsymbol{G}])$.

Proof. Correctness. At step 9, properties of the CHNF give $u^0_{i,j} \in \mathfrak{a}_i^{-1}\mathfrak{b}_j$ (where $U_0 = (u^0_{i,j})_{1\leq i,j\leq l}$), and $\mathfrak{a}^{-1} = (\det U_0)\mathfrak{b}^{-1}$. Thus at step 10, the matrix U has coefficient $u_{i,j} \in \mathfrak{a}_i\mathfrak{b}_j^{-1}$ and $\mathfrak{a} = (\det U)\mathfrak{b}$, so the algorithm ensures an equivalent pseudo-Gram matrix **G'** together with the pseudo-base change.

Complexity. Sampling with **DiscreteSample** (from Lemma 3.1) and the CHNF Algorithm of [11] run in polynomial time in nl and $\log s$. We need to estimate the probability of failure at step 6. Let T be the random variable counting the number of iteration before founding a set of full rank vectors. By Lemma 5.1 of [16] (and because $s \geq \lambda_{nl}(\psi(\mathbf{G}))$), for any $i \in \{1, \ldots, l-1\}$ and set of vectors $\{y_1, \ldots, y_i\}$ sampled with **DiscreteSample**, the probability that $y \leftarrow$ **DiscreteSample** does not belong to the span of $y_1, \ldots, y_i$ is greater than $C := 1 - (1 + e^{-\pi})^{-1}$. Let $m = \lceil \frac{2l}{C} \rceil$ and $X_1, \ldots, X_l$ Bernoulli variables with succes parameter

C, and $S_l = X_1 + \cdots + X_m$. Then, the probability p_{fail} of not finding l linearly independent vectors within m sampled vectors is upper bounded by the probability $\mathbb{P}(S_l \leq n-1)$, where S_m follows a binomial distribution with parameters m and C *i.e.*,

$$p_{fail} \leq \mathbb{P}(S_m \leq l-1).$$

Using Hoeffding's inequality,

$$\begin{aligned} p_{fail} &\leq \mathbb{P}\Big(\frac{S_m}{m} - C \leq \frac{l-1}{m} - C\Big) \\ &\leq \exp\Big(-2m\Big(C - \frac{l-1}{m}\Big)^2\Big) \\ &\leq \exp(-mC) \\ &\leq \exp(-2l) \\ &\leq e^{-2}. \end{aligned}$$

Therefore,

$$\mathbb{E}[T] \leq \frac{1}{1-p_{\text{fail}}} < 2.$$

Independance from G. Finally we prove that the result depends only on the equivalence class of $\mathbf{G}$. Let $(W^*GW, (\mathfrak{a}'_i)_{1\leq i\leq l})$ be equivalent to $\mathbf{G}$, where $W = (w_{i,j})_{1\leq i,j\leq l} \in \mathbf{GL}_l(K)$. Denote by $(H', (\mathfrak{b}'^{-1}_i)_{1\leq i\leq l}, U'_0)$ the CHNF Algorithm of [11] applied to the pseudo-matrix $(Y^TW^{-T}, (\mathfrak{a}'^{-1}_i)_{1\leq i\leq l})$ and $U' = U'^{-T}_0$. By unicity of the CHNF (there is a unique pseudo-matrix in CHNF in the orbit of $\mathbf{G}$ for the multiplication equivalence relation), we obtain

$$(U')^{-1}W^{-1}Y = U'^T_0 W^{-1}Y = (Y^TW^{-T}U'_0)^T = H' = H = (Y^TU_0)^T = U^{-1}Y,$$

so $(U')^{-1}W^{-1} = U^{-1}$ and $U' = W^{-1}U$. Then,

$$(U')^*W^*GWU' = U^*W^{-*}W^*GWW^{-1}U = U^*GU.$$

Also, the unicity of the CHNF implies $\mathfrak{b}'_i = \mathfrak{b}_i$ for all $1 \leq i \leq n$ so the pseudo-Gram matrix returned is the same and this concludes the proof. □

Average-case problem. To build cryptographic schemes based on LIP (such as Hawk [13]), one needs to efficiently sample equivalent forms (*e.g.*, to generate keys). Thus, the security relies on a weaker problem than wc-smodLIP (because the distribution is known) and this defines an average-case version of LIP. We must make sure that this problem is not to easy, to provide security.

Definition (ac-smodLIP$^{\mathbf{G},s}_K$)**.** The average-case search module-Lattice Isomorphism Problem with parameter K and $\mathbf{G}$ is, given any equivalent pseudo-matrix $\mathbf{G'} = (G', (\mathfrak{b}_i)_{1\leq i\leq l})$ sampled with Algorithm 2 with parameter $s > 0$, to find $U = (u_{i,j})_{1\leq i,j\leq l} \in \mathbf{GL}_l(K)$ such that $G' = U^*GU$ and $(\star)$ is verified.

The main result of this paragraph is a worst-case to average-case reduction *i.e.*, solving $\text{ac} - \text{smodLIP}^{\mathbf{G}}_K$ is as hard as solving $\text{wc} - \text{smodLIP}^{\mathbf{G}}_K$.

Proposition 3.4 (ac-smodLIP$^{\mathbf{G}}_K \geq$ wc-smodLIP$^{\mathbf{G}}_K$)**.** *Given an oracle that solves ac-smodLIP$^{\boldsymbol{G}}_{K,s}$ in time τ with probability $p > 0$, one can solve wc-smodLIP$^{\boldsymbol{G}}_K$ in time $\tau + poly(n, l, \log s)$ and probability p, where $s \geq \max\{\lambda_{nl}(\psi(\boldsymbol{G})),\ ||\varphi(B_G)^*||\sqrt{\log(2nl+4)/\pi}\}$.*

Proof. Let **G'**=$(G', (\mathfrak{b}_i)_i)$ be any pseudo-Gram matrix equivalent to **G**. First, we sample **G"**=$(G', (\mathfrak{d}_i)_i)$ equivalent to **G** together with $U'' = (u''_{i,j})$ such that $G'' = U''^* G U''$ and $u''_{i,j} \in \mathfrak{a}_i \mathfrak{d}_j^{-1}$. This is done in time $poly(n, l, \log s)$. Now we can apply our oracle to solve an average-case LIP instance ; we find $U' = (u'_{i,j})$ with inverse $V' = (v'_{i,j})$ such that $G'' = U'^* G' U'$ and $u'_{i,j} \in \mathfrak{b}_i \mathfrak{d}_j^{-1}$, $v'_{i,j} \in \mathfrak{d}_i \mathfrak{b}_j^{-1}$. Let $U = U'' U'^{-1} =: (u_{i,j}) \in \mathbf{GL}_l(K)$, then $G' = U^* G U$ and

$$\forall\, (i,j) \in \{1, \ldots, l\}^2,\ u_{i,j} = \sum_{k=1}^{l} \underbrace{u''_{i,k} \cdot v'_{k,j}}_{\in (\mathfrak{a}_i \mathfrak{d}_k^{-1})(\mathfrak{d}_k \mathfrak{b}_j^{-1})} \in \mathfrak{a}_i \mathfrak{b}_j^{-1},$$

so U is a solution to the worst-case problem. □

3.3 Attack for free rank 2 modules

This section deals with a special case of module-LIP problem which contains Hawk setting. Let K be a number field (not necessarily a cyclotomic extension), $\mathcal{L}$ the free rank-two lattice $\mathcal{O}_K^2$ with a basis $B_0 \in \mathbf{GL}_2(\mathcal{O}_K)$, and put $Q = B_0^* B_0$.

Definition (sq-modLIP$_K$)**.** For a number field K, the squared module-Lattice Isomorphism Problem (sq-modLIP$_K$) with parameter K is, given $Q = B_0^* B_0$ (where $B_0 \in \mathbf{GL}_2(\mathcal{O}_K)$), to recover any $B_1 \in \mathbf{GL}_2(\mathcal{O}_K)$ such that $B_1^* B_1 = Q$.

Remark. A solution $B_1 \in \mathbf{GL}_2(\mathcal{O}_K)$ to sq-modLIP$_K$ is not unique. More precisely, $B_2 \in \mathbf{GL}_2(\mathcal{O}_K)$ is another solution if and only if it is in the orbit of B_1 under the action of $\mathcal{O}_2(K)$.

3.3.1 The case of totally real number fields.

We give a method to solve sq-modLIP$_K$ when K is a totally real number field (in fact we will compute all matrices B such that $B^*B = Q$, which is stronger than solving sq-modLIP$_K$). It is relevant to first consider the simplest case, namely $K = \mathbb{Q}$ and $\mathcal{O}_K = \mathbb{Z}$. Let $Q \in \mathcal{S}_2^{>0}(\mathbb{Z})$ be a Gram matrix (so it can be expressed as $Q = B_0^* B_0$ for some $B_0 \in \mathbf{GL}_2(\mathbb{Z})$), we consider the set of matrices $B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Z})$ such that

$$Q = B^*B = \begin{pmatrix} a\overline{a} + b\overline{b} & * \\ * & c\overline{c} + d\overline{d} \end{pmatrix}.$$

The first coefficient q_1 and the last coefficient q_4 of Q are therefore sum of two squares in $\mathbb{Z}$. Also, we must have $|a|^2, |b|^2, |c|^2, |d|^2 \leq \max\{q_1, q_4\}$ so this set of matrices is finite. Integers which can be written as the sum of two squares are well described ; these are the integers whose prime factors $p = 3 \pmod 4$ have even valuation. A standard proof of this result uses the fact that such integers can be written as norms of Gaussian integers (see §5.6 in [30]). Let $L = \mathbb{Q}(i)$ (so $\mathcal{O}_L = \mathbb{Z}[i]$), the idea is to look for all $z = z_1 + iz_2 \in \mathbb{Z}[i]$ such that $z_1^2 + z_2^2 = N_{L/K}(z) = q_1$, so that one of them has to be $z_1 = a$ and $z_2 = b$. We can enumerate all such z and do the same for q_4. For every guess, we can efficiently check if the corresponding matrix satisfies the relation, so by the end we should be able to find a solution B_1. Now let's see how to generalize this method to arbitrary totally real number fields.

Overview of the method. Let K be a totally real number field and $L = K(i)$ (for example, $K = \mathbb{Q}(\zeta + \zeta^{-1})$ and $L = \mathbb{Q}(\zeta) = K(i)$, whenever ζ is a n-th primitive root of unity, with n a power-of-two integer). Similarly, consider $M = \mathcal{O}_K^2$ and a (secret) basis $B_0 \in \mathbf{GL}_2(\mathcal{O}_K)$ of M. Suppose we are given the associated (public) Gram matrix $Q = B_0^* B_0$. As K is a totally real number field, the first coefficient q_1 of Q is a sum of two squares in $\mathcal{O}_K$. We want to compute all elements $z = z_1 + iz_2 \in \mathcal{O}_K + i\mathcal{O}_K$ such that $z_1^2 + z_2^2 = N_{L/K}(z) = q_1$. Notice that $\mathcal{O}_K + i\mathcal{O}_K \subset \mathcal{O}_L$ but the equality may not be true in general. As for the case of Gaussian integers, there are finitely many such elements.

Lemma 3.5. *Given a totally real number field K, the extension $L = K(i)$ and an element $y \in \mathcal{O}_K$, there are finitely many $z \in \mathcal{O}_L$ with relative norm $N_{L/K}(z) = y$.*

Proof. There are finitely many integral ideals $J \subset \mathcal{O}_L$ of absolute norm $N := N_{K/\mathbb{Q}}(y)$. Also, if $N_{L/K}(J) = y\mathcal{O}_K$, then $N_{L/\mathbb{Q}}(J) = N_{K/\mathbb{Q}}(y\mathcal{O}_K) = N$ by transitivity. *A fortiori*, there are finitely many integral ideals $J \subset \mathcal{O}_L$ such that $N_{L/K}(J) = y\mathcal{O}_K$. Now, if $z, z' \in \mathcal{O}_L$ are such that $z\mathcal{O}_L = z'\mathcal{O}_L$ and $N_{L/K}(z) = N_{L/K}(z') = y$, then there exists $u \in \mathcal{O}_L^\times$ such that $z' = zu$. The condition on the norms implies that $1 = N_{L/K}(u) = u\bar{u} = |u|^2$ and this implies u is a root of unity in L. Indeed, the $2n$ complex embeddings of L come from the n real embeddings of K extended to L by $i \mapsto i$ or $i \mapsto -i$. Therefore, for any $x \in L$ and $\sigma : L \to \mathbb{C}$ embedding, we have $\sigma(\overline{x}) = \overline{\sigma(x)}$. In particular this proves $|\sigma(u)|^2 = \sigma(u)\overline{\sigma(u)} = \sigma(u)\sigma(\overline{u}) = \sigma(u\overline{u}) = 1$, so all the conjugates of u have module 1. The minimal polynomial of u over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$ and all its roots have module 1. A theorem of Kronecker[10] implies u and its conjugates are roots of unity. As the degree of L over $\mathbb{Q}$ is finite, there are finitely many roots of unity in L. □

To find elements of $\mathcal{O}_L$ with relative norm q_1 (resp. q_4) we compute all principal ideal of $\mathcal{O}_L$ of relative norm $q_1\mathcal{O}_K$ (resp. $q_4\mathcal{O}_K$). For instance, let $I := q_1\mathcal{O}_K$; its factorization in $\mathcal{O}_K$ and the data of the primes of $\mathcal{O}_L$ above its factors allow us to compute all ideal J of $\mathcal{O}_L$ with relative ideal norm I (see Algorithm 4 below). Among these ideals, we keep the principal ones and compute generators. Say we found $J = z\mathcal{O}_L$ with $N_{L/K}(z)\mathcal{O}_K = N_{L/K}(J) = I$. Then, $N_{L/K}(z)$ is equal to q_1 up to a unit. To remove this unit and find an element with relative norm exactly q_1, we use Algorithm 3. Then we test if this element belongs to $\mathcal{O}_K + i\mathcal{O}_K$. Finally, for each pair of elements $(z_1 + iz_2, w_1 + iw_2) \in (\mathcal{O}_K + i\mathcal{O}_K)^2$ such that $N_{L/K}(z_1 + iz_2) = q_1$ and $N_{L/K}(w_1 + iw_2)$, we check if it is a solution *i.e.*, if

$$B^T B = Q, \quad \text{where } B = \begin{pmatrix} z_1 & w_1 \\ z_2 & w_2 \end{pmatrix}.$$

Algorithms. For our needs, we present a preliminary algorithm that computes a unit of $\mathcal{O}_L$ with given relative norm (when it is possible). In [35] (Section 6) are presented algorithms for finding S-units solutions to the norm equation $N_{L/K}(z) = q_1$ when q_1 is a S-unit (S is a fixed set of prime ideals of $\mathcal{O}_K$ and an element in K^* (resp. in L^*) is a S-unit if it is divisible only by prime ideals in S (resp. by prime ideals above those in S)). The idea is first to enumerate fundamental systems of S-units $(u_i)_i$ of K and $(v_i)_i$ of L ; this is [35, Algorithm 6.1], it supposes known the structure of the class group $Cl(\mathcal{O}_K)$. [35, Algorithm 6.3] is applied to express the norms $N_{L/K}(v_i)$ and q_1 in terms of powers of the u_i's. Then, a linear algebra step gives the result. Now we present an algorithm which solves the norm equation for units (*i.e.*, given $N \in \mathcal{O}_K^\times$, we look for $v \in \mathcal{O}_L^\times$ such that $N_{L/K}(v) = N$). It is based on the linear algebra step of [35, Algorithm 6.9], and we assume we are given sets of fundamental units of $\mathcal{O}_K$ and $\mathcal{O}_L$. We denote by $\mathcal{O}_K^\times \cap K_\mathbb{R}^+$ the set of units u of $\mathcal{O}_K$ such that $\mu(u) \in K_\mathbb{R}^+$ *i.e.*, units whose embeddings are all positive numbers.

Lemma 3.6. *For any unit $N \in \mathcal{O}_K^\times \cap K_\mathbb{R}^+$ and sets of fundamental units $\mathcal{V} = \{v_1, \ldots, v_{n-1}\}$ (resp. $\mathcal{U} = \{u_1, \ldots, v_{n-1}\}$) of $\mathcal{O}_L$ (resp. $\mathcal{O}_K$), Algorithm 3 runs in classical polynomial-time, it returns a unit $v \in \mathcal{O}_L^\times$ such that $N_{L/K}(v) = N$ if it exists, and outputs $\perp$ otherwise.*

Proof. Correctness. As K is totally real, the group of roots of unity of K must be $\mathbb{U}_K = \{\pm 1\}$. Indeed, for any $\zeta \in \mathbb{U}_K$ and σ embedding of K, we have by definition $\sigma(\zeta) \in \mathbb{R}$ and if $\zeta^n = 1$

[10] Let $P \in \mathbb{Z}[X]$ be a monic polynomial such that $P(0) \neq 0$. If all the complex roots of P have module less or equal to 1, then these are roots of unity.

Algorithm 3 Compute a unit of $\mathcal{O}_L$ of given relative norm

Require: A totally real number field K of degree n, $L = K(i)$ and a unit $N \in \mathcal{O}_K^\times \cap K_\mathbb{R}^+$. A set of fundamental units $\mathcal{V} = \{v_1, \dots, v_{n-1}\}$ (resp. $\mathcal{U} = \{u_1, \dots, u_{n-1}\}$) of $\mathcal{O}_L$ (resp. $\mathcal{O}_K$)
Ensure: $v \in \mathcal{O}_L^\times$ such that $N_{L/K}(v) = N$ or $\perp$
1: Compute $(\beta_i)_{1 \le i \le n-1} \in \mathbb{Z}^{n-1}$ such that $N = \pm \prod_{i=1}^{n-1} u_i^{\beta_i}$
2: $B \leftarrow (\beta_1, \dots, \beta_{n-1})^T$
3: **for** $i \in \{1, \dots, n-1\}$ **do**
4: Compute $(\alpha_{i,j})_{1 \le j \le n-1} \in \mathbb{Z}^{n-1}$ such that $N_{L/K}(v_i) = \pm \prod_{j=1}^{n-1} u_j^{\alpha_{i,j}}$
5: **end for**
6: $A \leftarrow (\alpha_{i,j})_{1 \le i,j \le n-1}$
7: $X \leftarrow$ a solution to $AX = B$ or $\perp$ if no solution exist
8: **if** $X \neq \perp$ **then**
9: $X = (x_1, \dots, x_{n-1})^T$
10: $v \leftarrow \prod_{i=1}^{n-1} v_i^{x_i}$
11: **end if**
12: **return** v or $\perp$

for some $n \in \mathbb{N}_{>0}$, then $\sigma(\zeta)^n = \sigma(\zeta^n) = 1$ *i.e.*, $\sigma(\zeta)$ is a real root of unity, so $\sigma(\zeta) \in \{\pm 1\}$. As σ fixes rational numbers and is injective, we must have $\zeta \in \{\pm 1\}$. Also, K has $n_1 = n$ real embeddings and $L = K(i)$ is totally imaginary with $2n$ imaginary embeddings (the n embeddings of K are extended to L by $i \mapsto i$ or $i \mapsto -i$). By Dirichlet's unit theorem 2.3, the free parts of $\mathcal{O}_K^\times$ and $\mathcal{O}_L^\times$ have same rank $n-1$, and N (resp. $N_{L/K}(v_i) \in \mathcal{O}_K^\times$) can be uniquely expressed as in step 1 (resp. step 4).
The matrix A built at step 6 has size $(n-1) \times (n-1)$ and if the linear system at step 7 has a solution, then the unit $v = \prod_{i=1}^{n-1} v_i^{x_i}$ has relative norm

$$\begin{aligned} N_{L/K}(v) &= \prod_{i=1}^{n-1} N_{L/K}(v_i)^{x_i} \\ &= \pm \prod_{j=1}^{n-1} u_j^{\sum_{i=1}^{n-1} \alpha_{i,j} x_i} \\ &= \pm \prod_{j=1}^{n-1} u_j^{\beta_j} = \pm N. \end{aligned}$$

As N and $N_{L/K}(v) \in K_\mathbb{R}^+$ (the relative norm here is just $|\cdot|^2$), we must have equality $N_{L/K}(v) = N$. Finally if such v exist, the linear system $AX = B$ must have a solution so the algorithm ensures $\perp$ if and only no v exist.

Complexity. Steps 1 and 4 reduce to linear algebra by taking the Log map (see the definition in 2.3) and solving linear systems. These systems have solutions because $\mathcal{V}$ and $\mathcal{U}$ are fundamental systems, and N, $N_{L/K}(v_i) \in \mathcal{O}_K^\times$. If it exists, the solution can be computed in classical polynomial-time. □

Remark. To run the previous algorithm, sets of fundamental units for $\mathcal{O}_K^\times$ and $\mathcal{O}_L^\times$ are needed. More generally the problem of computing the unit group of a number field (*i.e.*,

computing a set of fundamental units and the group of roots of unity) can be done in quantum polynomial-time in the degree and the logarithm of its discriminant, see [14]. For the case of power-of-two cyclotomic fields and under Weber's conjecture 2.2.2, explicit systems of fundamental units are known (lemma 8.1 in [37]), as well as the torsion group.

Let us recall quickly our idea to solve sq-modLIP$_K$. Fix $Q \in \mathcal{H}_2^{>0}(\mathcal{O}_K)$ a Gram matrix, its first coefficient q_1 is a sum of two squares in $\mathcal{O}_K$ and we want to enumerate all such writings. This is equivalent to find all the elements in $\mathcal{O}_L$ ($L = K(i)$) with relative norm q_1. To do so, we build all the integral ideal of L with relative norm ideal $q_1\mathcal{O}_K$ and keep only the principal ones, from which we compute a generator. These generators have relative norm q_1 up to a unit which we are able to remove using Algorithm 3. Knowing the prime factorization of $N_{K/\mathbb{Q}}(q_1) \in \mathbb{Z}$, we can use Dedekind-Kummer theorem to compute the decomposition $q_1\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$ (see the following lemma). An ideal of $\mathcal{O}_L$ with relative norm ideal $q_1\mathcal{O}_K$ has its prime factors among the set of primes above the $\mathfrak{p}_i$'s. Once computed this list of prime ideals, it is then possible to enumerate all the ideals of $\mathcal{O}_L$ with good relative norm.

Lemma 3.7. *Given a number field K represented by an irreducible polynomial P such that $K \simeq \mathbb{Q}[X]/(P)$, there is an algorithm which computes the prime factorization of any ideal $I \subset \mathcal{O}_K$, it runs in polynomial quantum-time in $\log|\Delta_K|$ and $\log|N_{K/\mathbb{Q}}(I)|$.*

Proof. Compute $N := N_{K/\mathbb{Q}}(I) \in \mathbb{Z}$ and its prime factorization $N = \pm\prod_{i=1}^{m} p_i^{\alpha_i}$. This can be done in quantum polynomial-time in $\log|N|$ by Shor's algorithm (see section 5 of [33]). For each prime factor p_i, use Dedekind-Kummer theorem 2.7 to compute the splitting of $p_i\mathcal{O}_K$: this requires to compute the factorization of $\overline{m}(X)$ in $\mathbb{F}_{p_i}$ and it can be performed in classical polynomial-time in $\deg m(X) = n = [K : \mathbb{Q}]$, using for example Berlekamp or Cantor-Zassenhaus algorithms. Above each prime factor are at most n ideals of $\mathcal{O}_K$, whence the complexity. □

Lemma 3.8. *Given a number field K of degree with discriminant Δ_K, there is an algorithm deciding if an ideal $I \subset \mathcal{O}_K$ is principal and if it is, it computes a generator of I. It runs in polynomial quantum-time in $\log N_{K/\mathbb{Q}}(I)$ and $\log|\Delta_K|$.*

Proof. See [5]. □

Proposition 3.5. *Given a totally real number field K of degree n with ring of integers $\mathcal{O}_K$, discriminant Δ_K and the quadratic extension $L = K(i)$ with ring of integers $\mathcal{O}_L$, Algorithm 4 takes as input $q_1 \in \mathcal{O}_K$ and returns the set of all elements $z \in \mathcal{O}_K + i\mathcal{O}_K \subset \mathcal{O}_L$ with relative norm $N_{L/K}(z) = q_1$ in quantum time*

$$poly(\log|N_{K/\mathbb{Q}}(q_1)|, \log|\Delta_K|) \cdot (\log|N_{K/\mathbb{Q}}(q_1)|)^r,$$

where r is the number of distinct prime ideals of $\mathcal{O}_K$ appearing in the decomposition of $q_1\mathcal{O}_K$.

Algorithm 4 Compute elements in $\mathcal{O}_K + i\mathcal{O}_K$ of given relative norm

Require: A totally real number field K with ring of integers $\mathcal{O}_K$, the extension $L = K(i)$ with ring of integers $\mathcal{O}_L$ and an element q_1 which is a sum of two squares in $\mathcal{O}_K$.

Ensure: All elements $z \in \mathcal{O}_K + i\mathcal{O}_K$ such that $N_{L/K}(z) = q_1$.

Factorize $q_1\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$
$J_0 \leftarrow \{\mathfrak{q} \subset \mathcal{O}_L \text{ prime ideal} \mid \exists\, i \in \{1, \ldots, r\} : \mathfrak{q} \mid \mathfrak{p}_i\mathcal{O}_L\}$
$\mathfrak{J} \leftarrow \{J = \mathfrak{q}_1 \ldots \mathfrak{q}_s \mid s \leq r, \mathfrak{q}_i \in J_0,\ N_{L/K}(J) = q_1\mathcal{O}_K\}$
$\mathcal{U} \leftarrow \{u_1, \ldots, u_{n-1}\}$ a set of fundamental units of $\mathcal{O}_K$
$\mathcal{V} \leftarrow \{v_1, \ldots, v_{n-1}\}$ a set of fundamental units of $\mathcal{O}_L$
$\mathbb{U}_L \leftarrow$ the set of roots of unity in L
for $J \in \mathfrak{J}$ **do**
    Test if J is principal and compute a generator g_J
    $v_J \leftarrow$ Run Algorithm 3 with $N = q_1 N_{L/K}(g_J)^{-1} \in \mathcal{O}_K^{\times}$, $\mathcal{V}$ and $\mathcal{U}$
    if $v_J \neq \perp$ **then**
        $z_J \leftarrow v_J g_J$
        $S_J \leftarrow \{\zeta \times z_J \mid \zeta \in \mathbb{U}_L\}$
    end if
    for $s_J \in S_J$ **do**
        $a_{s_J} + ib_{s_J} \leftarrow s_J$
        if $a_{s_J}, b_{s_J} \in \mathcal{O}_K$ **then**
            S.append$(a_{s_J} + ib_{s_J})$
        end if
    end for
end for
return S

Proof. Correctness. To apply Algorithm 3 at step 9 we must check that $N = q_1 N_{L/K}(g_J)^{-1} \in \mathcal{O}_K^\times \cap K_\mathbb{R}^+$. First notice that $q_1 \in K_\mathbb{R}^+$ since it is the sum of two squares in $\mathcal{O}_K$ (and K is totally real so squares are positive), and $N_{L/K}(g_J) \in K_\mathbb{R}^+$ because the relative norm is just $|\cdot|^2$. By construction we have $N_{L/K}(g_J)\mathcal{O}_K = N_{L/K}(J) = q_1\mathcal{O}_K$ so $N_{L/K}(g_J)$ is equal to q_1 up to a unit, thus $N \in \mathcal{O}_K^\times$. By construction, for any $J \in \mathfrak{J}$ we have $N_{L/K}(v_J g_J) = q_1$. At the end all the elements in S are in $\mathcal{O}_K + i\mathcal{O}_K$ (checked at step 11) with relative norm q_1 (because $N_{L/K}(\zeta) = 1$ for any $\zeta \in \mathbb{U}_L$). Now let us explain why the algorithm returns all such elements. First of all, steps 1-3 build all ideals of $\mathcal{O}_L$ with relative norm $q_1\mathcal{O}_K$. Indeed, consider an ideal $I \subset \mathcal{O}_L$ with relative norm $q_1\mathcal{O}_K$ and write its decomposition in $\mathcal{O}_L$: $I = \prod_{j=1}^s \mathfrak{q}_j^{\beta_j}$. With the notation of step 1, $\prod_{j=1}^s N_{L/K}(\mathfrak{q}_j)^{\beta_j} = \prod_{i=1}^r \mathfrak{p}_i^{\alpha_i}$. The latter is a decomposition in prime ideals of $\mathcal{O}_K$. By unicity of the writting in theorem 2.1, we deduce that for any $j \in \{1, \dots, s\}$, there exists $i_j \in \{1, \dots, r\}$ such that $\mathfrak{p}_{i_j} \mid N_{L/K}(\mathfrak{q}_j)$. This means I has all its prime factors above the $\mathfrak{p}_i$'s, so they must be contained in the set J_0. Thus for any $z \in \mathcal{O}_L$ such that $N_{L/K}(z) = q_1$, the corresponding principal ideal $I = z\mathcal{O}_L$ is in $\mathfrak{J}$ (step 3).
When it is possible, steps 9-11 construct a generator with relative norm q_1 for each ideal in $\mathfrak{J}$ (step 9 always succeeds when a solution exists) and the proof of Lemma 3.5 shows any other generator with same relative norm differs from a root of unity. At step 12 we multiply the generators with good norm by all the roots of unity, so the set S_J contains all the solution in $\mathcal{O}_L$. Among them, we keep those in $\mathcal{O}_K + i\mathcal{O}_K$ (step 16).

Complexity. Step 1 can be done *via* lemma 3.7 in quantum polynomial-time in n and $\log|N_{K/\mathbb{Q}}(q_1)|$. Following the notation of step 1, above each $\mathfrak{p}_i$ are at most two prime ideals of $\mathcal{O}_L$ (this is a consequence of Theorem 3 because L/K is quadratic). More precisely there are three possible cases :

$$\mathfrak{p}_i\mathcal{O}_L = \begin{cases} \mathfrak{q}_{i,0} & \text{is prime (inert case).} \\ \mathfrak{q}_{i,1}\,\mathfrak{q}_{i,2} & \text{is the product of two distinct primes (split case).} \\ \mathfrak{q}_{i,3}^2 & \text{is the square of a prime (ramified case).} \end{cases}$$

Also, the relative norm ideals are : $N_{L/K}(\mathfrak{q}_{i,0}) = \mathfrak{p}_i{}^2$; $N_{L/K}(\mathfrak{q}_{i,1}) = N_{L/K}(\mathfrak{q}_{i,2}) = \mathfrak{p}_i$; $N_{L/K}(\mathfrak{q}_{i,3}) = \mathfrak{p}_i$. To find the $\mathfrak{q}_{i,j}$'s we apply again Lemma 3.7 to each $\mathfrak{p}_i$; since $\mathfrak{p}_i \mid q_1\mathcal{O}_K$, we have $N_{K/\mathbb{Q}}(\mathfrak{p}_i) \leq N_{K/\mathbb{Q}}(q_1)$ so all the factorizations can be computed in quantum polynomial-time in $[L : \mathbb{Q}] = 2n$ and $\log|N_{K/\mathbb{Q}}(q_1)|$. This must be repeated r times, where r is the number of distinct prime ideals dividing $q_1\mathcal{O}_K$. Complexity of step 2 is thus $r \cdot \mathrm{poly}(n, \log|N_{K/\mathbb{Q}}(q_1)|)$.

To build the set $\mathfrak{J}$ from the set of prime ideals $\mathfrak{q}_{i,j}$, we proceed as follows. Let $\mathfrak{p}_i$ be a prime factor of $q_1\mathcal{O}_K$. Any ideal $I \in \mathfrak{J}$ is divisible by a prime ideal above $\mathfrak{p}_i$. From the condition on the norm of I and the computation of the $N_{L/K}(\mathfrak{q}_{i,j})$, we can enumerate all the possibilities for the prime factors of I. First consider the case where $\mathfrak{p}_i\mathcal{O}_L = \mathfrak{q}_{i,0}$ is inert, then α_i is an even number and I must have $\mathfrak{q}_{i,0}$-valuation $\alpha_i/2$. If $\mathfrak{p}_i\mathcal{O}_L = \mathfrak{q}_{i,3}^2$ ramifies, then I has $\mathfrak{q}_{i,0}$-valuation α_i. The last case is the most interesting, as it leads to more solutions. If $\mathfrak{p}_i\mathcal{O}_L = \mathfrak{q}_{i,1}\,\mathfrak{q}_{i,2}$ splits, then we have to choose $(a, b) \in \mathbb{N}^2$ such that $a+b = \alpha_i$, so that $\mathfrak{q}_{i,1}^a\,\mathfrak{q}_{i,2}^b$ divides I. There are exactly $\alpha_i + 1$ acceptable pairs (a, b) (choose $0 \leq a \leq \alpha_i$, then b is determined) and this number is bounded by $(\log|N_{K/\mathbb{Q}}(q_1)| + 1)$ so we get at most $(\log|N_{K/\mathbb{Q}}(q_1)| + 1)^r$ different ways to choose the prime factors of I ; this is a bound for the cardinal of $\mathfrak{J}$.

As mentioned in the previous remark, $\mathcal{U}$, $\mathcal{V}$ and $\mathbb{U}_L$ are computed in time $\mathrm{poly}(n, \log|\Delta_K|)$. Step 8 runs in time $\mathrm{poly}(n, \log N_{K/\mathbb{Q}}(q_1), \log|\Delta_K|)$, by lemma 3.8. Algorithm 3 runs in (classical) polynomial-time and the set S_J at step 12 has size at most n^2 (see the remark following Dirichlet's unit theorem 2.3). We assume step 15 can be done in polynomial time and step 16 can be checked easily (we have a $\mathbb{Z}$-basis of $\mathcal{O}_K$). Finally, the set S has cardinal at most $n^2|\mathfrak{J}| = n^2(\log|N_{K/\mathbb{Q}}(q_1)|+1)^r$. □

Remarks. • In the case where $\mathcal{O}_L = \mathcal{O}_K[i]$, the prime ideals $\mathfrak{q}_{i,j} \subset \mathcal{O}_L$ can be computed using Dedekind-Kummer theorem 2.7 in the quadratic extension L/K : keeping the same notations, $m(X)$ is X^2+1 and to compute its factorization in $k(\mathfrak{p}_i) = \mathbb{F}_{q_i}$ ($q_i = p_i^{f_i}$, where $p_i\mathbb{Z} = \mathfrak{p}_i \cap \mathbb{Z}$ and $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_{p_i}]$) comes down to testing if -1 is a square in $\mathbb{F}_{q_i}$ and computing square roots, see [10].

• If the estimation $\alpha_i \leq \log|N_{K/\mathbb{Q}}(q_1)|$ is tight, then the number of prime factors r is small.

Heuristic. Let ω denote the arithmetic function which associates to $n \in \mathbb{N}\setminus\{0\}$ the number of distinct prime factors of n. A famous result of Erdös and Kac states that in general, one would expect $\omega(n)$ to be of order $\log\log n$. This result transposes perfectly to number fields. An ideal $I \subset \mathcal{O}_K$ has on average $\log\log|N_{K/\mathbb{Q}}(I))|$ distinct prime factors in $\mathcal{O}_K$, in the sense that the quantity $\left(\omega(I) - \log\log|N_{K/\mathbb{Q}}(I))|\right)/\sqrt{\log\log|N_{K/\mathbb{Q}}(I)|}$ follows a normal distribution. We refer to [24] Corollary 1, or [29] Theorem 1 (for counting the principal divisors). Therefore, Algorithm 4 runs in average time

$$\mathrm{poly}(n, \log|N_{K/\mathbb{Q}}(q_1)|, \log|\Delta_K|) \cdot \exp\left((\log\log|N_{K/\mathbb{Q}}(q_1)|)^2\right).$$

Proposition 3.6. *Let K be a totally real number field. There is a quantum algorithm that given a Gram matrix $Q = \begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix}$ with coefficients in $\mathcal{O}_K$, computes all the matrices $B \in \mathbf{GL}_2(\mathcal{O}_K)$ such that $B^*B = Q$, in time*

$$\mathit{poly}(\log B, \log|\Delta_K|) \cdot (\log B)^{r_{max}},$$

with $B = \max\{\log|N_{K/\mathbb{Q}}(q_1)|, \log|N_{K/\mathbb{Q}}(q_4)|\}$ and $r_{max} = \max\{r, s\}$, where the decompositions in distinct prime ideals are $q_1\mathcal{O}_K = \prod_{i=1}^r \mathfrak{p}_i^{\alpha_i}$ and $q_4\mathcal{O}_K = \prod_{i=1}^s \mathfrak{p}_i'^{\beta_i}$.

In particular, this algorithm computes the secret key of the signature scheme Hawk in a totally real number fields.

Proof. Run Algorithm 4 with q_1 and q_4. This builds two finite sets S, $S' \subset \mathcal{O}_K + i\mathcal{O}_K$ within the time complexity announced. For each pair $(a+ib, c+id) \in S \times S'$, we can efficiently check if the matrix $B = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ satisfies $B^*B = Q$. If it does, we add this matrix to a set $\mathcal{S}$. There are at most $n^4(\log B+1)^{r+s}$ trials. At the end, the set $\mathcal{S}$ contains all the solutions. □

4 Related works on module-LIP

This last section contains known results which can be applied to module-LIP. In [21], the authors present an algorithm to test equality in the Witt-Picard group of a CM-order. For example, $\mathcal{O}_K$ is a CM-order whenever K is a cyclotomic field and its Witt-Picard group is the quotient of the multiplicative group $\{(I, v) \in I(\mathcal{O}_K) \times (K_{\mathbb{R}}^+ \cap K) \,|\, \text{such that } I \cdot \overline{I} = v\mathcal{O}_K\}$ by the subgroup $\{(v\mathcal{O}_K, v\overline{v}) \,|\, v \in K^\times\}$. This can be done in classical polynomial time and it is based on a variant of Gentry-Szydlo algorithm. Also, Plesken-Souvignier algorithm can be adapted to module-lattices so that the outputs are automorphisms preserving the structure. As well as the original algorithm, it can be modified to compute isometries between module-lattices.

4.1 Module-LIP for ideal lattices over CM-fields.

Suppose K is a degree n CM extension of $\mathbb{Q}$ (*i.e.*, a number field equipped with an involution $^-\colon K \to K$ that mimics complex conjugation. Equivalently, it is the totally imaginary quadratic extension of a totally real number field. One may think of a cyclotomic field $K = \mathbb{Q}(\zeta)$ with the usual complex conjugation). For rank one module *i.e.*, ideal lattices over $\mathcal{O}_K$, the problem is known to be solved in classical-polynomial time, using a variant of Gentry-Szydlo algorithm. A rank one module M over $\mathcal{O}_K$ has a pseudo-basis $\mathbf{B} = (b, \mathfrak{a})$ where $b \in K \setminus \{0\}$ and $\mathfrak{a} \in I(\mathcal{O}_K)$, so that $M = b\mathfrak{a}$. We can always suppose that $b \in \mathcal{O}_K$. Then the associated pseudo-Gram « matrix » is $\mathbf{G} = (g, I)$, where $g = \overline{b}b \in K_{\mathbb{R}}^+ \cap \mathcal{O}_K$ and the problem is, given any equivalent $\mathbf{G'} = (g', J)$, to find $u \in IJ^{-1} \subset K$ such that $g' = u\overline{u}g$.

Lemma 4.1 (Theorem 1.4 of [21], adapted)**.** *There is a deterministic polynomial-time algorithm that given $\mathcal{O}_K$ (where K is a CM number field), fractional ideals $I_1, I_2 \in I(\mathcal{O}_K)$, and elements $v_1, v_2 \in K_{\mathbb{R}}^+ \cap K$ satisfying $I_1 \cdot \overline{I_1} = v_1\mathcal{O}_K$ and $I_2 \cdot \overline{I_2} = v_2\mathcal{O}_K$, decides whether there exists $u \in K$ such that $I_2 = uI_1$ and $v_2 = u\overline{u}v_1$, and if so computes such an element u.*

Then wc-smodLIP$_K^{\mathbf{G}}$ can be solved applying the previous lemma with $I_1 = b\mathcal{O}_K$, $I_2 = b'\mathcal{O}_K$ where $b' \in \mathcal{O}_K$ satisfies $b\overline{b} = g'$ and $v_1 = g$, $v_2 = g'$.

4.2 Plesken-Souvignier algorithm for module lattices

A module-lattice $M \subset K^l$ naturally embeds into $K_{\mathbb{R}}^l \simeq \mathbb{R}^{nl}$ *via* Minkowski embedding so Plesken-Souvignier [28] algorithm can be applied using this identification but this increases the dimension. In [9], the author adapts the algorithm to avoid this issue (although the identification is still needed when enumerating sets of short vectors). Let $\mathbf{B} = (B, (\mathfrak{a}_i)_{1 \le i \le l})$ be a pseudo-basis for $M \subset K^l$. Using the identification and applying Plesken-Souvignier algorithm to M we get $\theta \in \mathbf{GL}_K(K^l)$ (bijective K-linear map $\theta : K^l \to K^l$) preserving M and such that $\langle \theta(b_i), \theta(b_j) \rangle = \langle b_i, b_j \rangle$ for any $i, j \in \{1, \ldots, l\}$ and where $B = (b_1, \ldots, b_l)$. However, this does not guarantee that θ is orthogonal. Orthogonality is characterized with the following lemma (Proposition 3.0.12 of [9]).

Lemma 4.2. *Let M as above and $\boldsymbol{e} = (e_1, \ldots, e_n)$ be a $\mathbb{Q}$-basis of K. Then, $\theta \in \mathbf{GL}_K(K^l)$ is orthogonal if and only if $\langle \theta(e_r b_i), \theta(e_s b_j) \rangle = \langle e_r b_i, e_s b_j \rangle$ for any $1 \le i, j \le l$ and $1 \le r, s \le n$.*

Proof. This is clearly necessary and the converse comes from the fact that any $x \in K^l$ can be written $x = \sum_{i,r} x_{i,r} e_r b_i$, with $x_{i,r} \in \mathbb{Q}$ for all $1 \le i \le l$ and $1 \le r \le n$. □

Thus we modify the notion of k-partial automorphisms : Fixing a basis $\mathbf{e} = (e_1, \ldots, e_n)$ of K over $\mathbb{Q}$ and a pseudo-basis $\mathbf{B}$ of M (in fact only B is to consider since the coefficient ideals are not involved in the algorithm), a k-partial automorphism of M is a tuple $(v_1, \ldots, v_k) \in M^k$ such that $\langle e_r v_i, e_s v_j \rangle = \langle e_r b_i, e_s b_j \rangle$ for any $1 \leq i, j \leq l$ and $1 \leq r, s \leq n$. As well as the unstructured case, the fingerprint provides an invariant and a first test to see if a partial automorphism can be extended. The set short vectors $S = \{v \in M \,|\, ||v|| \leq \max_{i,j} ||e_i b_j||\}$ is computed and vector sums are defined, for $\underline{v} = (v_1, \ldots, v_k)$ a k-partial automorphism of M and $s = (s_{i,r,s})_{1 \leq i \leq k,\ 1 \leq r,s \leq n} \in \mathcal{O}_K^{kn^2}$, by $\overline{X}_s(\underline{v}) := \sum_{v \in X_s(\underline{v})} v \in M$, where $X_s(\underline{v}) := \{v \in S \,|\, \langle e_r v, e_s b_i \rangle = s_{i,r,s},\ \forall 1 \leq i \leq k,\ 1 \leq r, s \leq n\}$. It is still true that any automorphism θ of M satisfies $\theta(\overline{X}_s(b_1, \ldots, b_k)) = \overline{X}_s(\theta(b_1), \ldots, \theta(b_k))$ (Proposition 3.2.3 of [9]) so we get a second invariant.

The precomputation step of the algorithm consists in enumerating the set S, computing the fingerprint and the vector sums of $(b_1, \ldots, b_k)$. Given a 1-partial automorphism of M *i.e.*, an element $v \in S$ such that $\langle e_r v, e_s v \rangle = \langle e_r b_1, e_s b_1 \rangle$, we recursively extend v as follows : suppose v is a k-partial automorphism of M, if $k = l$ we are done. Otherwise, we compute the set $\{x \in S \,|\, (v, x)$ is a $(k+1)$-partial automorphism $\}$. Explicitly, it is given by $C_{k+1} := \{x \in S \,|\, \langle e_r x, e_s x \rangle = \langle e_r b_{k+1}, e_s b_{k+1} \rangle$ $(1 \leq r, s \leq n)$ and $\langle e_r x, e_s v_i \rangle = \langle e_r b_{k+1}, e_s b_i \rangle$ $(1 \leq r, s \leq n,$ $1 \leq i \leq k)\}$. Choosing $x \in C_{k+1}$, we check if (v, x) passes the fingerprint and vector sums tests [9, Algorithm 3]. If it does, we take $v_{k+1} = x$ and go to the next step. If it doesn't, we take another $x \in C_{k+1}$, and if all $x \in C_{k+1}$ have been tested, we go to the previous step, see [9, Algorithm 4].

Conclusion

Module-LIP is in some sense the natural way to define a Lattice Isomorphism Problem on module lattices, taking into account the algebraic structure. It can be seen as a special case of LIP, *via* Minkowski embedding, with restricted set of solutions. Current methods to solve module-LIP over an arbitrary number field and arbitrary rank are not more efficient than the ones solving LIP. However in the setting of Hawk, *i.e.*, for free rank two modules, it is possible to efficiently recover the secret key when K is a totally real field (*e.g.*, when $K = \mathbb{Q}(\zeta + \zeta^{-1})$ is the maximal real subfield of a cyclotomic extension). But in general, the first and last coefficients of the public key in Hawk are still sum of four squares in the real subfield (when $K = \mathbb{Q}(\zeta)$ with ζ a power-of-two primitive root of unity, $q_1, q_4 \in \mathcal{O}_K$ are sums of four squares in $\mathbb{Z}[\zeta + \zeta^{-1}]$) and the effectiveness of this decomposition (if fact we are interested in finding all such decompositions) permits to recover the secret key.

Besides the search version of module-LIP, the distinguishing problem also deserves attention. Invariants for isometry classes of module lattices arise from the completion at finite and infinite places. More precisely, isomorphic $\mathcal{O}_K$-module lattices $\mathcal{L}, \mathcal{L}'$ are isomorphic locally everywhere *i.e.*, $\mathcal{L}_\mathfrak{p} \simeq \mathcal{L}'_\mathfrak{p}$ for any prime ideal or complex embedding $\mathfrak{p}$; we say that $\mathcal{L}, \mathcal{L}'$ are in the same genus. However the converse is in general not true and a theorem of Borel shows that the genus decomposes into a finite disjoint union of classes. A further question would be to distinguish algorithmically between isometry classes with same genus.

Algorithm 5 Finding all congruence matrices for integral rank 2 modules.

Require: A pseudo-basis $\vec{B} = (B, (\mathfrak{a}_1, \mathfrak{a}_2))$ with pseudo-Gram matrix $\vec{G}$, and $\vec{G'} = (G, (\mathfrak{b}_1, \mathfrak{b}_2)) \sim \vec{G}$ an instance of wc-smodLIP$_K^{\vec{B}}$.

Ensure: All congruence matrices between $\vec{G}$ and $\vec{G'}$.

1: $q \leftarrow 0$; $\mathfrak{S} \leftarrow \emptyset$
2: **while** $q \cdot \mathcal{O}_K = \{0\}$ **or** $q \cdot \mathcal{O}_K$ is not a prime ideal **do**
3: $\quad \mathfrak{b}_1 \times \mathfrak{b}_2 \ni (u, v) \leftarrow$ **DiscreteSample**$(\vec{G'}, s)$, using Algorithm ??
4: $\quad q \leftarrow (u, v) \cdot G' \cdot (u, v)^T$.
5: **end while**
6: $\mathcal{S} \leftarrow \{(t_1, t_2) \in \mathcal{O}_K^2 \,|\, t_1^2 + t_2^2 = q\}$, using Theorem 2.
7: Go to 1 and run 2-5 to get (u', v') non-colinear to (u, v) and q'.
8: $\mathcal{S}' \leftarrow \{(t_1', t_2') \,|\, {t_1'}^2 + {t_1'}^2 = q'\}$, using Theorem 2.
9: **for** $((t_1, t_2), (t_1', t_2')) \in \mathcal{S} \times \mathcal{S}'$ **do**
10: $\quad$ Solve the linear system

$$\begin{pmatrix} t_1 & t_1' \\ t_2 & t_2' \end{pmatrix} = D \cdot \begin{pmatrix} u & u' \\ v & v' \end{pmatrix}$$

11: $\quad V \leftarrow B^{-1} \cdot D$
12: **end for**
13: **return** $\mathfrak{S}$.

References

[1] Miklós Ajtai. "Generating hard instances of lattice problems". In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 1996, pp. 99–108.

[2] Malonguemfo Teagho Amandine. *Algorithms for Isometries of Lattices, Master Thesis*. 2018.

[3] Christine Bachoc. *Réseaux et Cryptographie Master CSI, UE Cryptanalyse*.

[4] Jean-François Biasse, Claus Fieker, and Tommy Hofmann. "On the computation of the HNF of a module over the ring of integers of a number field". In: *Journal of Symbolic Computation* 80 (2017), pp. 581–615.

[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: *Proceedings of the twenty-seventh annual ACM-SIAM symposium on Discrete algorithms*. SIAM. 2016, pp. 893–902.

[6] Werner Bley, Tommy Hofmann, and Henri Johnston. "Computation of lattice isomorphisms and the integral matrix similarity problem". In: *Forum of Mathematics, Sigma*. Vol. 10. Cambridge University Press. 2022, e87.

[7] Nicolas Bourbaki. *Algèbre: Chapitres 1 à 3*. Springer Science & Business Media, 2007.

[8] Zvika Brakerski et al. "Classical hardness of learning with errors". In: *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*. 2013, pp. 575–584.

[9] Thomas Camus. "Computing automorphisms of algebraic lattices". In: (2015).

[10] Henri Cohen. *A course in computational algebraic number theory*. Vol. 138. Springer Science & Business Media, 2013.

[11] Henri Cohen. *Advanced topics in computational number theory*. Vol. 193. Springer Science & Business Media, 2012.

[12] Léo Ducas and Wessel van Woerden. "On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography". In: *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*. Springer. 2022, pp. 643–673.

[13] Léo Ducas et al. "Hawk: Module LIP makes lattice signatures fast, compact and simple". In: *Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part IV*. Springer. 2023, pp. 65–94.

[14] Kirsten Eisenträger et al. "A quantum algorithm for computing the unit group of an arbitrary degree number field". In: *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*. 2014, pp. 293–302.

[15] Claus Fieker and Damien Stehlé. "Short Bases of Lattices over Number Fields." In: *ANTS*. Springer. 2010, pp. 157–173.

[16] Ishay Haviv and Oded Regev. "On the lattice isomorphism problem". In: *Proceedings of the twenty-fifth annual ACM-SIAM symposium on Discrete algorithms*. SIAM. 2014, pp. 391–404.

[17] Harald Andrés Helfgott. “Isomorphismes de graphes en temps quasi-polynomial (d’apr\es Babai et Luks, Weisfeiler-Leman...)” In: *arXiv preprint arXiv:1701.04372* (2017).

[18] Andreas Hoppe. *Normal forms over Dedekind domains, efficient implementation in the computer algebra system KANT*. na, 1998.

[19] Markus Kirschmer. “Definite quadratic and hermitian forms with small class number”. In: *Habilitation, RWTH Aachen University* (2016).

[20] Serge Lang. *Algebraic number theory*. Vol. 110. Springer Science & Business Media, 2013.

[21] Hendrik W Lenstra Jr and Alice Silverberg. “Testing isomorphism of lattices over CM-orders”. In: *SIAM Journal on Computing* 48.4 (2019), pp. 1300–1334.

[22] Joseph J Liang. “On the integral basis of the maximal real subfield of a cyclotomic field.” In: (1976).

[23] Qing Liu. *Cours de Théorie des Nombres, option M1, 2019-2020*.

[24] Yu-Ru Liu. “A generalization of the Erdös-Kac theorem and its applications”. In: *Canadian Mathematical Bulletin* 47.4 (2004), pp. 589–606.

[25] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Springer Science & Business Media, 2013.

[26] Kenji Okuda and Syouji Yano. “A generalization of Voronoı’s Theorem to algebraic lattices”. In: *Journal de théorie des nombres de Bordeaux* 22.3 (2010), pp. 727–740.

[27] Chris Peikert. *Lattices in Cryptography, Lecture 1*. 2013.

[28] Wilhelm Plesken and Bernd Souvignier. “Computing isometries of lattices”. In: *Journal of Symbolic Computation* 24.3-4 (1997), pp. 327–334.

[29] Paul Pollack. “An elemental ErdHos–Kac theorem for algebraic number fields”. In: *Proceedings of the American Mathematical Society* 145.3 (2017), pp. 971–987.

[30] Pierre Samuel. *Théorie algébrique des nombres...* Hermann, 1967.

[31] Jean-Pierre Serre. *Cours d’arithmétique*. Vol. 2. Presses Universitaires de France-PUF, 1977.

[32] Jean-Pierre Serre. *Local fields*. Vol. 67. Springer Science & Business Media, 2013.

[33] Peter W Shor. “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”. In: *SIAM review* 41.2 (1999), pp. 303–332.

[34] Andrew Shuterland. *Ideal norms and the Dedekind-Kummer theorem, Lectures notes 6 of Number Theory I, Fall 2015*.

[35] Denis Simon. “Solving norm equations in relative number fields using -units”. In: *Mathematics of computation* 71.239 (2002), pp. 1287–1305.

[36] Marco Taboga. *"Cholesky decomposition", Lectures on matrix algebra, 2021*.

[37] Lawrence C Washington. *Introduction to cyclotomic fields*. Vol. 83. Springer Science & Business Media, 1997.

[38] Koji Yamagata and Masakazu Yamagishi. “On the ring of integers of real cyclotomic fields”. In: (2016).