Special Genera of Hermitian Lattices and Applications to HAWK

Guilhem Mureau[1]

Univ Bordeaux, CNRS, Inria, Bordeaux INP, IMB, UMR 5251, Talence, France
guilhem.mureau@math.u-bordeaux.fr

Abstract. In its decisional form, the module-Lattice Isomorphism Problem (decision module-LIP) has received first attention in [12]. The authors gave a polynomial-time algorithm to distinguish spinor genera within the genus of a quadratic binary $\mathcal{O}_F$-lattice, assuming that $\mathcal{O}_F$ is a principal ideal domain. However, this algorithm would not impact cryptographic schemes based on decision module-LIP for lattices such as those employed in HAWK [5], *i.e.*, for binary $\mathcal{O}_K$-lattices equipped with a Hermitian form (with K a cyclotomic number field). Motivated by HAWK's framework, we investigate a concept that serves as an analogue of the spinor genus for Hermitian lattices, called special genus. This notion was studied by Shimura [20] who provided a complete set of invariants for describing special genera. Building on this result, we propose an algorithm to determine whether two Hermitian lattices belong to the same special genus. Specifically for HAWK's lattice and siblings, our algorithm runs in classical polynomial-time. Nevertheless we provide numerical evidence suggesting that the ability to distinguish special genera does not, in practice, constitute a significative advantage for solving decision module-LIP.

Introduction

The primary motivation for this work arises from a recent problem in lattice-based cryptography, namely the module-Lattice Isomorphism Problem (module-LIP). First introduced in [5], it is employed as a security assumption for the signature scheme and NIST candidate HAWK. It can be described informally as follows: Given the ring of integers $\mathcal{O}_F$ of a number field F and two $\mathcal{O}_F$-lattices that are *isomorphic* (*i.e.*, such that there exists a distance-preserving F-linear map that transforms one into the other), the search variant of module-LIP —the one related to HAWK's security— asks to compute such a map. In contrast, [12] investigated the decisional variant of module-LIP which entails determining if two given $\mathcal{O}_F$-lattices are isomorphic. Although this variant of module-LIP has not yet been employed for cryptographic schemes, van Woerden and Ducas built schemes based on the decisional form of the (plain) Lattice Isomorphism Problem (for Euclidean lattices and called dLIP, see [6]) which may be adapted to lattices over number fields one day.

Isomorphic lattices share several properties, such as their volume or minimal distances, and numerous algebraic invariants are also preserved under isometry. Lattices sharing these invariants are said to be in the same *genus*. However, the genus does not constitute a complete set of invariants for the isometry relation, that is, isomorphic lattices belong to the same genus but the converse does not hold in general. In [12], Ling, Liu and Mendelsohn initiated an algorithmic investigation into finer invariants beyond the genus, namely into *spinor genera*, and explored their potential applications to solve decision module-LIP. Building on results of Earnest and Estes [7], the authors proposed a quantum algorithm to distinguish spinor genera

among the genus of a rank-2 *quadratic* $\mathcal{O}_F$-lattice, assuming that $\mathcal{O}_F$ is a principal ideal domain. However, as noted by the authors, this algorithm does not apply to decision module-LIP for *Hermitian* rank-2 lattices over cyclotomic fields, such as those used in [5]. Specifically, in HAWK, one considers $\mathcal{O}_K^2$, where $K = \mathbb{Q}(\zeta_m)$ is a cyclotomic field whose conductor is a power-of-two ($m \in \{512, 1024, 2048\}$), and it is endowed with the Hermitian form $\Phi\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = x\overline{x} + y\overline{y}$.

We emphasize that the notion of spinor genus is specific to quadratic lattices, *i.e.*, to lattices equipped with a quadratic form. Therefore the question of whether there exists similar computable invariants for (rank-2) Hermitian lattices was left open.

Contributions. We consider for the first time the *special genus* as a novel invariant for the decisional variant of module-LIP (instantiated on Hermitian lattices). Originally introduced by Shimura in [20], the special genus is specific to Hermitian lattices and, similarly to the spinor genus, it serves as an intermediate classification between the genus and isometry classes (see Figure 1). Thanks to Shimura's classification

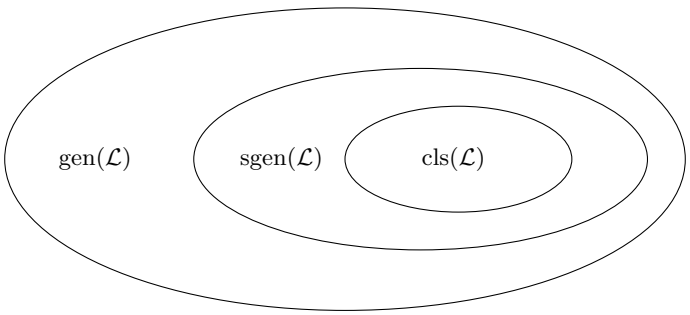

Fig. 1: The special genus of $\mathcal{L}$ fits between its genus and isometry class.

(see Theorem 2.8 and Corollary 2.11), we provide a necessary and sufficient set of conditions for determining whether two Hermitian lattices belong to the same special genus. This leads to the development of Algorithm 1, which takes as input two (pseudo-)bases of Hermitian lattices (of arbitrary rank) in the same genus, and decides if the lattices lie in the same special genus. The latter relies on a technical lemma (see Lemma 1.32) which prevents us to fully provide the time complexity of the algorithm. However for a large family of Hermitian lattices including the one we are interested in for cryptographic applications, this assumption is not needed (see Remark 3.4) and classical polynomial-time complexity is achieved.

The core of this paper concerns the use of the special genus in solving decision module-LIP. Due to the definition of the problem (see Definition 3.2), Algorithm 1 is however not suited to module-LIP's framework. To be concrete, Algorithm 1 requires pseudo-bases of Hermitian lattices as input whereas in a module-LIP instance, only pseudo-Gram matrices are known. Moreover working with pseudo-Gram matrices instead of pseudo-bases induces a lack of information and makes the computation of the special genus invariants even more difficult. Therefore we restrict ourselves to a family of Hermitian lattices which are still of interest for cryptographic applications, and for which the invariants are easier to compute. When restricting to these lattices, we are able to state Algorithm 2, whose complexity is provable. Our main contribution can be summarized as follows whereas a full statement can be found in Corollary 3.5.

Theorem (Main, Informal). For HAWK's lattice $\mathcal{O}_K^2$ over a cyclotomic number field K, there is a polynomial-time algorithm which takes as input a (pseudo-)Gram matrix corresponding to a Hermitian lattice $\mathcal{M}$, and decides whether $\mathcal{M}$ belongs to the special genus of $\mathcal{O}_K^2$.

Particular attention is adressed to the case of rank-2 Hermitian lattices, as it contains HAWK's lattice $\mathcal{H} = \mathcal{O}_K^2$. Namely in Section 3 we obtain estimates on the number of isomorphism classes within the genus of $\mathcal{H}$ (resp. whithin a special genus of $\mathcal{H}$). Our computations show that the special genus is indeed finer than the genus, reducing the number of classes to distinguish by a factor $2^{\Omega(d)}$ (where d is the degree of K). For cryptographic-size parameters, the comparison is summarized in Figure 2 (assuming that all special genera contain approximately the same number of isometry classes). More details can be found in Figure 3.

m	d	Number of isometry classes within the genus of $\mathcal{O}_K^2$	Number of isometry classes within a special genus of $\mathcal{O}_K^2$
128	64	$\simeq 2^{150}$	$\simeq 2^{130}$
256	128	$\simeq 2^{400}$	$\simeq 2^{350}$
512	256	$\simeq 2^{1050}$	$\simeq 2^{850}$ (Under GRH)

Fig. 2: Estimates for HAWK's lattice $\mathcal{O}_K^2$ over $K = \mathbb{Q}(\zeta_m)$.

Technical overview. The question of whether two ($\mathcal{O}_K$-)Hermitian lattices $\mathcal{L}$ and $\mathcal{M}$ belong to the same special genus was answered by Shimura in [20], and Corollary 2.11 gives a complete set of conditions. The latter are divided in two types, the first one being a *global* condition on the module index $I = [\mathcal{L} : \mathcal{M}]_{\mathcal{O}_K}$, a fractional ideal of K which can be interpreted as the covolume of $\mathcal{M}$ in $\mathcal{L}$. Precisely, a necessary condition for $\mathcal{L}$ and $\mathcal{M}$ to be in the same special genus is that $I = g \cdot \mathcal{O}_K$ is a principal ideal with $g \in K$ and $g\overline{g} = 1$. Notice that Shimura's theorem implies $I \cdot \overline{I} = \mathcal{O}_K$ as soon as $\mathcal{L}$ and $\mathcal{M}$ are in the same genus (not necessarily the same special genus). As a consequence, we can make use of Lenstra and Silverberg algorithm (see [11] or Lemma 1.35) to test efficiently if I is a principal ideal and if so, to compute a generator g with $g\overline{g} = 1$.

On the other hand there are *local* conditions to check. In our setting, $\mathcal{O}_K$ denotes the ring of integers of a number field K (*e.g.*, a cyclotomic number field) which contains a subfield F such that $\dim_F(K) = 2$. To any prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, the ring of integers of F, are associated Hermitian lattices $\mathcal{L}_\mathfrak{p}$ and $\mathcal{M}_\mathfrak{p}$, and the so-called local determinant groups $\mathcal{E}(\mathcal{L}_\mathfrak{p})$ and $\mathcal{E}(\mathcal{M}_\mathfrak{p})$ (see Subsection 2.1 for definitions). Only a finite set of prime ideals $\mathfrak{p}$ lead to non-trivial local determinant groups —this set only depends on the genus of $\mathcal{L}$— and for each of these exceptional primes, Corollary 2.11 asks to verify a certain relation between the generator g of I and the determinant of a local isometry mapping $\mathcal{L}_\mathfrak{p}$ into $\mathcal{M}_\mathfrak{p}$. In practice, we explain how this determinant can be computed from the *Jordan decompositions* of $\mathcal{L}_\mathfrak{p}$ and $\mathcal{M}_\mathfrak{p}$, see Lemma 1.32.

As mentionned above, module-LIP deals with pseudo-Gram matrices, say $\mathbf{G}$ and $\mathbf{H}$, instead of pseudo-bases of $\mathcal{L}$ and $\mathcal{M}$. This convention introduces some complications in the computation of the special genus. First, $\mathbf{G}$ and $\mathbf{H}$ alone are not sufficient to compute the module-index I (see Lemma 1.14 for the formula).

Still, we show in Proposition 3.3 that they allow to decide whether I is principal and has a generator g such that $g\overline{g} = 1$ (without even having to compute it). Sadly, the Jordan decompositions of $\mathcal{L}_\mathfrak{p}$ and $\mathcal{M}_\mathfrak{p}$ seem to be out of reach when manipulating only $\mathbf{G}$ and $\mathbf{H}$, making the local conditions above impossible to verify. Instead, we restrict ourselves to Hermitian lattices $\mathcal{L}$ having an odd rank orthogonal sublattice (*e.g.* such that $\mathbf{G}$ has a row whose non-diagonal elements are equal to zero). For these particular $\mathcal{L}$, there are no local conditions to check and deciding whether $\mathcal{M}$ is in the special genus of $\mathcal{L}$ boils down to testing if I is a principal ideal generated by an element of norm 1. This condition may seem restrictive but it contains HAWK's lattice $\mathcal{O}_K^2$, see Corollary 3.5.

Thanks to Shimura's Theorem 2.8, one can moreover compute the number of special genera within a genus. Over a cyclotomic field $K = \mathbb{Q}(\zeta_m)$, this number equals the quotient of class numbers h_K/h_F for a large family of binary Hermitian ($\mathcal{O}_K$-)lattices which includes $\mathcal{O}_K^2$. Moreover, the subfield $F = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ is known (or at least conjectured) to have $h_F = 1$ for several conductors m, including powers of two, which are relevant for cryptography. Consequently, the special genus is an invariant that refines the genus, allowing the distinction of h_K classes within the genus. This conclusion is indeed consistent with the fact that, for these particular lattices, the special genus is entirely determined by the class of the module index in the class group of K. On the other hand, Siegel's mass formulas (see [9, Chapter 4]) gives estimates on the number of isomorphism classes within the genus of a lattice. Using the obtained numbers, we get an estimate of the number of isometry classes within a special genus (assuming each contains roughly the same number). This number, although still exponential in the degree of K, represents an exponential gain compared to the number of classes in a full genus.

Impact. In [6, Section 7] the authors provided recommendations to make decision-LIP (for plain lattices) a hard problem. Since the genus is an efficiently computable invariant, a necessary condition is therefore to choose lattices within the same genus. In the case of an adaptation to Hermitian lattices over a number field, we show the necessity to choose them not only in the same genus but in the same special genus.

Although this reduces the number of classes to distinguish, the impact on decision module-LIP is very limited. Indeed, one can easily design non-isomorphic lattices lying in the same special genus. For instance, a straightforward adaptation of [6, Section 8] would be to consider $\mathcal{L} = \mathfrak{a}\mathbf{b_1} \oplus \mathfrak{b}\mathbf{b_2}$ and $\mathcal{M} = \mathbf{b_1} \oplus \mathfrak{a}\mathfrak{b}\mathbf{b_2}$, where $\mathbf{b_1} = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \mathbf{b_2} = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$ and $\mathfrak{a}, \mathfrak{b}$ are coprime ideals of $\mathcal{O}_K$. The fact that $\mathcal{L}$ and $\mathcal{M}$ are in the same special genus is proved in Remark 3.14.

It should be noted that a large number of classes within a (special) genus does not necessarily imply that the module-LIP instance is actually hard to solve. For certain lattices enjoying remarkable geometric properties, as in HAWK (and more generally for smooth or dense lattices, see [26]), the number of classes to distinguish may be significantly reduced, taking into account that these properties must be preserved. On the contrary, the problem could be still hard for some instances, even if the (special) genus contains only few classes.

Recently, van Gent and van Woerden [24] gave a search to distinguish reduction of module-LIP for certain module lattices, extending the idea of Szydlo in [22]. Regarding the discussion above, their result combined with our partial distinguisher has, in practice, no impact on search module-LIP problem for $\mathcal{O}_K^2$ and thus on the security of HAWK.

Conclusion. The special genus is a finer invariant than the genus, which improves the current state-of-the-art on decision module-LIP. Moreover for several lattices, we show that this invariant is efficiently computable. This includes HAWK's lattice $\mathcal{O}_K^2$ over a cyclotomic field K, for which distinguishing special genera amounts to testing the principality of its module index ideal, which can be done efficiently using Lenstra and Silverberg's algorithm [11]. This paper settles the question of using the special genus in the cryptanalysis of decision module-LIP and more generally, in light of the mathematical literature, the question of finding other computable refinements of the genus for Hermitian lattices. Experiments lead in Section 3 suggest that despite the large number of special genera in the genus of $\mathcal{O}_K^2$, it is far from sufficient to distinguish isomorphism classes. Indeed the number of classes in a special genus seems to be still exponential in the degree of the field.

Organisation of the paper. Section 1 provides the theoretical background for dealing with Hermitian lattices over number fields, their genera and special genera, and stating Shimura's Theorem 2.8. Particular emphasis is placed on the concept of module index, including its efficient computation, as it plays a fundamental role in the classification of special genera.

In Section 2, we present Shimura's Theorem 2.8 and derive from it a criterion for determining whether two Hermitian lattices belong to the same special genus, as stated in Corollary 2.11. This leads us to an algorithm (Algorithm 1) for distinguishing special genera of Hermitian lattices (given their pseudo-bases).

Finally, Section 3 explores the applications to the decisional variant of module-LIP. The latter is formally defined in Definition 3.2 and we adapt the previous algorithm to its framework. Algorithm 2 decides whether the module index $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}_K}$ is a principal ideal generated by an element of norm 1, given only pseudo-Gram matrices of $\mathcal{L}$ and $\mathcal{M}$. In some cases, this turns out to be a complete invariant for having $\mathcal{M}$ in the special genus of $\mathcal{L}$.

Acknowledgement. The author would like to express its gratitude to Alice Pellet-Mary and Renaud Coulangeon for helpful disscusions and comments on the draft. Thanks to Marius Kirschmer for answering technical questions. The author was supported by the France 2030 program, managed by the French National Research Agency under grant agreement No. ANR-22-PETQ-0008 PQTLS.

Notations

For a ring R, we denote by $R^\times$ the set of invertible elements of R. The set of matrices with n rows, ℓ columns and with coefficients in R is denoted by $\mathcal{M}_{n,\ell}(R)$, or simply $\mathcal{M}_n(R)$ if $\ell = n$. The invertible elements of the ring $\mathcal{M}_n(R)$ form the group $\mathbf{GL}_n(R)$. Finally we use bold letters to denote (columns) vectors.

1 Preliminaries

This section provides the necessary background for dealing with Hermitian lattices over Dedekind domains. Our goal is to introduce key concepts such as the special genus and Shimura's Theorem 2.8, which serves as the central theoretical result. Moreover, we state some algorithmic tools that will be needed later on.

1.1 Algebraic number theory

Ideals. Let $\mathfrak{o}$ be a commutative and unitary domain with characteristic 0 and fraction field F. An *integral ideal* $\mathfrak{a}$ of $\mathfrak{o}$ is an additive subgroup of $\mathfrak{o}$ such that $x\mathfrak{a} \subseteq \mathfrak{a}$ for all $x \in \mathfrak{o}$. A *fractional ideal* $\mathfrak{a}$ of F is an additive subgroup of F such that $x\mathfrak{a}$ is an integral ideal of F for some $x \in F \setminus \{0\}$. We say that $\mathfrak{a}$ is *principal* if $\mathfrak{a} = x \cdot \mathfrak{o}$ consists of all multiples of some $x \in F$ by the elements of $\mathfrak{o}$. In that case x is called a *generator* of $\mathfrak{a}$ and $y \in \mathfrak{a}$ is another generator if and only if $y \in x \cdot \mathfrak{o}^\times$. The ideal *generated* by a finite subset $S \subset F$ is the smallest fractional ideal (for the inclusion) which contains S.

A *prime* ideal is an integral ideal of F, usually denoted by $\mathfrak{p}$, such that for all $x, y \in \mathfrak{o}$, $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. The set of prime ideals is denoted by $\mathbb{P}(\mathfrak{o})$. For any fractional ideals $\mathfrak{a}, \mathfrak{b}$, their product $\mathfrak{ab}$ is defined as the smallest fractional ideal containing all the products xy for $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. We say that $\mathfrak{b}$ *divides* $\mathfrak{a}$ whenever $\mathfrak{a} = \mathfrak{bc}$ holds for some integral ideal $\mathfrak{c}$. Finally, $\mathfrak{a}$ is *maximal* if there is no integral ideal $\mathfrak{b}$ such that $\mathfrak{a} \subsetneq \mathfrak{b}$.

Dedekind domains. In this paper, $\mathfrak{o}$ will denote either the ring of integers of a number field F or a valutation ring obtained by completing a number field F at some prime ideal (these notions are defined below). To cover uniformly both cases, we will work with the more general notion of *Dedekind domains*. Recall that in a Dedekind domain $\mathfrak{o}$, any integral ideal $\mathfrak{a}$ is a product of finitely many prime ideals $\mathfrak{a} = \prod_i \mathfrak{p}_i^{e_i}$. Moreover this factorization is unique, up to ordering the factors. Also, any integral ideal $\mathfrak{a}$ admits an inverse, *i.e.,* there exists a fractional ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathfrak{o}$. The inverse of $\mathfrak{a}$ will be denoted by $\mathfrak{a}^{-1}$.

Further, let $\alpha \in F$ and put $K = F[X]/(X^2 - \alpha)$. We will denote the class of X in K by $\sqrt{\alpha}$. Then K is a 2-dimensional F-algebra equipped with an involution $\overline{\cdot} : v_1\sqrt{\alpha} + v_2 \mapsto -v_1\sqrt{\alpha} + v_2$.[1] The trace and norm maps on K are defined by $\mathrm{Tr} : K \to F\,;\, a \mapsto a + \overline{a}$ and $\mathrm{N} : K \to F\,;\, a \mapsto a\overline{a}$ respectively. We define $\mathcal{O} := \{a \in K \mid \mathrm{Tr}(a) \in \mathfrak{o} \text{ and } \mathrm{N}(a) \in \mathfrak{o}\}$. When K is a quadratic extension of F, then $\mathcal{O}$ is the ring of integers of K and thus a Dedekind domain. Otherwise, $K \simeq F \times F$ and $\mathcal{O} \simeq \mathfrak{o} \times \mathfrak{o}$ (see [20, 2.9]). In the second case, we call fractional ideal of $\mathcal{O}$ any finitely generated $\mathfrak{o}$-module $\mathfrak{A} \subset K$ such that $\mathcal{O} \cdot \mathfrak{A} \subseteq \mathfrak{A}$. Finally, the trace (resp. norm) of a fractional ideal $\mathfrak{A} \subset K$ is the fractional ideal $\mathrm{T}(\mathfrak{A})$ (resp. $\mathrm{N}(\mathfrak{A})$) of F generated by the traces (resp. norms) of elements in $\mathfrak{A}$.

Number fields. Let F be a *number field*, *i.e.,* an algebraic extension of the field of rational numbers $\mathbb{Q}$ with finite dimension, and let $\mathfrak{o}$ be the *ring of integers* of F. Then, F is the field of fractions of $\mathfrak{o}$ and the latter is a Dedekind domain. The set of fractional ideals of F, equipped with the multiplication of ideals, forms an abelian group denoted by $\mathcal{I}(\mathfrak{o})$. The *class group* of $\mathfrak{o}$ is then obtained as the quotient of $\mathcal{I}(\mathfrak{o})$ by the subgroup of principal ideals, and it is denoted by $\mathrm{Cl}(\mathfrak{o})$. Let $\alpha \in F \setminus F^2$ and set $K = F[X]/(X^2 - \alpha)$ as above. Then K is a number field and $\mathcal{O}$ defined as above is its ring of integers. The inverse different ideal of K/F is defined by $\mathfrak{D}^{-1} = \{a \in K \mid \mathrm{Tr}(a \cdot \mathcal{O}) \subseteq \mathfrak{o}\}$. Then the discriminant of K/F is the norm of the different ideal $\Delta := \mathrm{N}(\mathfrak{D})$, it is a fractional ideal of F. We will say that a prime ideal $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ is *ramified* if it divides Δ, and that it is *unramified* otherwise. If all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ are unramified, then we say that K/F is unramified.

[1] K is a quadratic extension of F when α is not a square in F and it is isomorphic to $F \times F$ otherwise.

CM number fields. Let F be a number field of degree d, *i.e.,* with dimension d over the field of rational numbers. There are d field homomorphisms $\sigma : F \to \mathbb{C}$ called *complex embeddings*. Concretely if $F \simeq \mathbb{Q}[X]/(P)$, the complex embeddings are given by the evaluation maps $X \mapsto \alpha_i$, where the α_i's are the complex roots of P. We say that F is a *totally real* number field when $\sigma(F) \subset \mathbb{R}$ for all complex embedding σ, or equivalently if all the α_i's are real numbers. Additionally, a quadratic extension $K = F[X]/(X^2 - \alpha)$ of a totally real field F is called a *CM* (complex multiplication) number field if α is totally negative, *i.e.,* $\sigma(\alpha) < 0$ for all complex embeddings of F. We will also say that K/F is a *CM extension*.

An example largely used in cryptography are the *cyclotomic* numbers fields. The cyclotomic number field of conductor $m \geq 2$ is $K = \mathbb{Q}[X]/(\Phi_m)$, where $\Phi_m(X) \in \mathbb{Z}[X]$ is the m-th cyclotomic polynomial. Alternatively $K \simeq \mathbb{Q}(\zeta_m)$, where ζ_m is a primitive m-th root of unity. It has degree $d = \varphi(m)$, where φ denotes Euler's totient function, and its ring of integers is $\mathcal{O} = \mathbb{Z}[X]/(\Phi_m) \simeq \mathbb{Z}[\zeta_m]$. It is a CM number field since $K = F[X]/(X^2 - \alpha)$, where $F = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ is totally real and $\alpha = (\zeta_m - \zeta_m^{-1})^2 = (\zeta_m + \zeta_m^{-1})^2 - 4 \in F^\times \setminus F^{\times 2}$ is totally negative. Moreover the ramification in cyclotomic number fields is well known.

Lemma 1.1 ([27], Proposition 2.15 & [16], Chapter I, Lemma 10.1). *If $m = p^r$ is a prime power, then $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ is ramified at the unique prime ideal above p and unramified everywhere else. Moreover, $p \cdot \mathcal{O} = \mathfrak{P}^d$, where $\mathfrak{P} = (1 - \zeta_m) \cdot \mathcal{O}$ and $d = \varphi(p^r)$. If m is composite, then $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ is unramified.*

Completions. Suppose that $\mathfrak{o}$ is the ring of integers of a number field F and $K = F[X]/(X^2 - \alpha)$ is a quadratic extension of F, whose ring of integers is $\mathcal{O}$ as above. Let $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ and $v_\mathfrak{p} : F \to \mathbb{Z} \cup \{\infty\}$ be the valuation on F defined by $v_\mathfrak{p}(x) = \max\{e \in \mathbb{Z} \,|\, x \cdot \mathfrak{o} \subset \mathfrak{p}^e\}$ for $x \neq 0$, and $v_\mathfrak{p}(0) = \infty$. The *completion* of F with respect to $v_\mathfrak{p}$ is a field denoted by $F_\mathfrak{p}$. Moreover $v_\mathfrak{p}$ extends to $F_\mathfrak{p}$ and the *valuation ring* associated is $\mathfrak{o}_\mathfrak{p} = \{x \in F_\mathfrak{p} \,|\, v_\mathfrak{p}(x) \geq 0\}$. It is a Dedekind domain with a unique prime ideal $\{x \in F_\mathfrak{p} \,|\, v_\mathfrak{p}(x) > 0\}$, which is still denoted by $\mathfrak{p}$. Moreover this ideal is principal and a generator of it is called a *uniformizer* of $F_\mathfrak{p}$. Consequently, any fractional ideal $\mathfrak{a}$ of $F_\mathfrak{p}$ is principal, since it is a power of $\mathfrak{p}$ (if $\mathfrak{a} \neq \{0\}$).

Let $K_\mathfrak{p} := K \otimes_F F_\mathfrak{p}$ and $\mathcal{O}_\mathfrak{p} := \mathcal{O} \otimes_\mathfrak{o} \mathfrak{o}_\mathfrak{p}$.[2] The involution $\bar{\cdot}$ on K extends to $K_\mathfrak{p}$ by $k \otimes f \mapsto \bar{k} \otimes f$, and likewise for Tr, N : $K_\mathfrak{p} \to F_\mathfrak{p}$.[3] In the case where $\mathfrak{p}$ *splits* in $\mathcal{O}$, *i.e.* when $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1\mathfrak{P}_2$ with $\mathfrak{P}_1, \mathfrak{P}_2$ distinct prime ideals of $\mathcal{O}$, then we fix $\mathfrak{P} = \mathfrak{P}_i$ for some $i \in \{1, 2\}$ and a field isomorphism $K_\mathfrak{P} \simeq F_\mathfrak{p}$.[4] It yields a ring isomorphism $K_\mathfrak{p} \simeq F_\mathfrak{p} \times F_\mathfrak{p}$, $k \otimes f \mapsto (kf, \bar{k}f)$. In the same way, $\mathcal{O}_\mathfrak{p} \simeq \mathfrak{o}_\mathfrak{p} \times \mathfrak{o}_\mathfrak{p}$ (see [20, 2.9]) and we denote by $\mathfrak{P}$ as well the integral ideal of $K_\mathfrak{p}$ generated by $\mathfrak{p}$, *i.e.*, $\mathfrak{P} = \{(x, y) \,|\, x, y \in \mathfrak{p}\}$. Otherwise, $K_\mathfrak{p}$ is a quadratic extension of $F_\mathfrak{p}$ (in fact, $K_\mathfrak{p}$ is the completion of K at the unique prime above $\mathfrak{p}$, see [18, §1]) and $\mathcal{O}_\mathfrak{p}$ is a Dedekind domain with a unique maximal ideal, denoted by $\mathfrak{P}$.[5] In both cases, we let π be a uniformizer of $K_\mathfrak{p}$ (*i.e.,* a generator of $\mathfrak{P}$), and we fix $u_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times$ such that $\overline{\pi} = \pi \cdot u_\mathfrak{p}$.

[2] Since $K = F[X]/(X^2 - \alpha)$, one has $K_\mathfrak{p} = F_\mathfrak{p}[X]/(X^2 - \alpha)$.

[3] It holds that $\mathcal{O}_\mathfrak{p} = \{x \in K_\mathfrak{p} \,|\, \mathrm{Tr}(x) \in \mathfrak{o}_\mathfrak{p} \text{ and } \mathrm{N}(x) \in \mathfrak{o}_\mathfrak{p}\}$ is the integral closure of $\mathfrak{o}_\mathfrak{p}$ in $K_\mathfrak{p}$, see *e.g.*, [21, Lemma 10.147.2] with $(R, S, A, B) = (\mathfrak{o}, \mathfrak{o}_\mathfrak{p}, \mathcal{O}, K)$.

[4] $K_{\mathfrak{P}_1}$ and $K_{\mathfrak{P}_2}$ are both field extensions of $F_\mathfrak{p}$ and it follows from [16, Chapter II, §8.4] that $[K : F] = 2 = [K_{\mathfrak{P}_1} : F_\mathfrak{p}] + [K_{\mathfrak{P}_2} : F_\mathfrak{p}]$, so $[K_{\mathfrak{P}_1} : F_\mathfrak{p}] = [K_{\mathfrak{P}_2} : F_\mathfrak{p}] = 1$.

[5] In both cases, $\mathfrak{P}$ is the largest ideal $\mathfrak{p} \subseteq \mathfrak{P} \subsetneq \mathcal{O}_\mathfrak{p}$ such that $\overline{\mathfrak{P}} = \mathfrak{P}$.

1.2 Hermitian Spaces

Let V be a free K-module with finite rank n. We fix an implicit K-basis of V and we use bold letters to denote both the elements in V or their (column) coordinate vectors (in K^n), with respect to this basis.

Definition 1.2. *We say that V is a Hermitian space over K if it is equipped with a map $\Phi : V \times V \to K$ satisfying for any $\mathbf{v}, \mathbf{v}', \mathbf{w}, \mathbf{w}' \in V$ and $a, b \in K$,*

$$\begin{aligned}\Phi(a\mathbf{v} + b\mathbf{v}', \mathbf{w}) &= a\Phi(\mathbf{v}, \mathbf{w}) + b\Phi(\mathbf{v}', \mathbf{w}),\\ \Phi(\mathbf{v}, a\mathbf{w} + b\mathbf{w}') &= \overline{a}\Phi(\mathbf{v}, \mathbf{w}) + \overline{b}\Phi(\mathbf{v}, \mathbf{w}'),\\ \Phi(\mathbf{w}, \mathbf{v}) &= \overline{\Phi(\mathbf{v}, \mathbf{w})}.\end{aligned}$$

We also say that Φ is a Hermitian form on V. We will denote $\Phi(\mathbf{v}, \mathbf{v})$ by $\Phi(\mathbf{v})$.

Example 1.3. A relevant example for applications is when $K = \mathbb{Q}(\zeta)$ is a cyclotomic field, $F = \mathbb{Q}(\zeta + \zeta^{-1})$ its maximal totally real subfield and $V = K^n$. Then $\mathcal{O} = \mathbb{Z}[\zeta]$ and $\mathfrak{o} = \mathbb{Z}[\zeta + \zeta^{-1}]$, and the *standard Hermitian form* on K^n is defined for any $\mathbf{v} = (v_i)_{1 \le i \le n}, \mathbf{w} = (w_i)_{1 \le i \le n} \in V$ by

$$\Phi(\mathbf{v}, \mathbf{w}) = \sum_{i=1}^{n} v_i \overline{w_i}.$$

If $\mathbf{b} = \{\mathbf{v_1}, \ldots, \mathbf{v_n}\}$ is a basis of V over K, the *Gram matrix* of $\mathbf{b}$ with respect to a Hermitian form Φ on V is $G := (\Phi(\mathbf{v_i}, \mathbf{v_j}))_{1 \le i,j \le n}$. This matrix is Hermitian, *i.e.*, it is equal to its transpose-conjugate $G^* := \overline{G}^T$.

Definition 1.4. *Let Φ be a Hermitian form on V, the unitary group of (V, Φ) is*

$$\mathrm{U}(V, \Phi) = \{\sigma \in \mathbf{GL}(V) \mid \Phi(\sigma(\mathbf{v}), \sigma(\mathbf{w})) = \Phi(\mathbf{v}, \mathbf{w}) \text{ for all } \mathbf{v}, \mathbf{w} \in V\}.$$

The special unitary group of (V, Φ) is defined by

$$\mathrm{SU}(V, \Phi) = \{\sigma \in \mathrm{U}(V, \Phi) \mid \det(\sigma) = 1\}.$$

1.3 Generalities on Lattices

Let $\mathfrak{o}$ be a Dedekind domain and $(\mathfrak{o}, F, \mathcal{O}, K)$ as in Section 1.1, paragraph *Dedekind domains*. Further, let V be a free K-module of rank n.

Pseudo-bases. We begin this section by giving generalities on lattices in V. Notice that the following definitions and properties do not involve any Hermitian structure on V for the moment. For more details on this topic, we refer to [3, 17, 20].

Definition 1.5 ($\mathcal{O}$-lattice). *An $\mathcal{O}$-lattice $\mathcal{L}$ in V is a finitely generated $\mathcal{O}$-module in V. The rank of an $\mathcal{O}$-lattice $\mathcal{L}$ in V, denoted by* $\mathrm{rank}(\mathcal{L})$*, is the rank of the ambient space $K\mathcal{L}$ over K. We say that $\mathcal{L}$ has full rank when $K\mathcal{L} = V$, i.e., when $\mathcal{L}$ contains a K-basis of V.*

Definition 1.6 (Pseudo-basis). *Let $\mathcal{L}$ be an $\mathcal{O}$-lattice in V with rank ℓ. Suppose the existence of K-linearly independent vectors $\mathbf{v_1}, \ldots, \mathbf{v}_\ell \in V$ and fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell$ of K such that*

$$\mathcal{L} = \mathfrak{a}_1\mathbf{v_1} \oplus \cdots \oplus \mathfrak{a}_\ell\mathbf{v}_\ell.$$

Then the data of $\mathbf{B} = (B, \{\mathfrak{a}_i\}_{1 \le i \le n})$, where $B = (\mathbf{v_1} | \cdots | \mathbf{v}_\ell) \in \mathcal{M}_{n,\ell}(K)$, is called a pseudo-basis of $\mathcal{L}$. Moreover when $\mathcal{O}$ is a Dedekind domain, $[\mathfrak{a}_1 \cdots \mathfrak{a}_\ell] \in \mathrm{Cl}(\mathcal{O})$ is called the Steinitz class of $\mathbf{B}$.

Remark 1.7. It is a standard fact that $\mathcal{O}$-lattices in V admit a pseudo-basis whenever $\mathcal{O}$ is a Dedekind domain (see *e.g*, [17, Theorem 81.3]). Additionally, Shimura proved in [20, Proposition 3.2] that the same property holds for the split case $\mathcal{O} \simeq \mathfrak{o} \times \mathfrak{o}$. However, in the case where we consider *global* $\mathcal{O}$-lattices —that is, when $\mathfrak{o}$ is the ring of integers of the number field F— we will always assume that K is a field extension of F and therefore that $\mathcal{O}$ is a Dedekind domain. Accordingly, the following properties are stated only in the case where $\mathcal{O}$ is a Dedekind domain.[6]

Remark 1.8. Unless stated otherwise, we will only consider full rank $\mathcal{O}$-lattices. In particular, the matrix part of a pseudo-basis belongs to $\mathbf{GL}_n(K)$.

The results mentionned above ensure that $\mathcal{O}$-lattices always admit a pseudo-basis. In the case where $\mathcal{O}$ is a Dedekind domain, pseudo-bases corresponding to the same $\mathcal{O}$-lattice are related in the following way.

Proposition 1.9 ([3], Proposition 1.4.2). *Suppose that $\mathcal{O}$ is a Dedekind domain. Let $\mathbf{B} = (B, \{\mathfrak{a}_i\}_{1\leq i\leq n})$ be the pseudo-basis of an $\mathcal{O}$-lattice $\mathcal{L}$ in V. Then $\mathbf{C} = (C, \{\mathfrak{b}_i\}_{1\leq i\leq n})$ is a pseudo-basis of $\mathcal{L}$ if and only if there exists $U = (u_{i,j})_{1\leq i,j\leq n} \in \mathbf{GL}_n(K)$ satisfying the following properties.*

1. $C = BU$;
2. $\forall\, i, j \in \{1, \ldots, n\}$, $u_{i,j} \in \mathfrak{a}_i\mathfrak{b}_j^{-1}$;
3. $\prod_{i=1}^n \mathfrak{a}_i = (\det U) \prod_{i=1}^n \mathfrak{b}_i$

With the same notations as above, it follows from *3.* that the pseudo-bases $\mathbf{B}$ and $\mathbf{C}$ of $\mathcal{L}$ define the same Steinitz class. Thus the Steinitz class depends only on $\mathcal{L}$ and not on some pseudo-basis of it.

Definition 1.10. *Assuming $\mathcal{O}$ is a Dedekind ring, the Steinitz class of $\mathcal{L}$, denoted by $\mathrm{St}(\mathcal{L})$, is defined as the Steinitz class of $\mathbf{B}$, where $\mathbf{B}$ is any pseudo-basis of $\mathcal{L}$.*

Module index. It will appear clearly in Section 2 that the module index plays a fundamental role in the classification of special genera. It can be defined abstractly via the following result due to Steinitz, but we will make use of Lemma 1.14 to compute it efficiently from pseudo-bases.

Theorem 1.11 (Steinitz, [17] Theorem 81.11). *Suppose that $\mathcal{O}$ is a Dedekind domain and let $\mathcal{L}$, $\mathcal{M}$ be two (full-rank) $\mathcal{O}$-lattices in V. Then there exists a pseudo-basis $((\mathbf{v_1}|\cdots|\mathbf{v_n}), \{\mathfrak{a}_i\}_{1\leq i\leq n})$ of $\mathcal{L}$ and unique fractional ideals $\mathfrak{d}_1 \supseteq \cdots \supseteq \mathfrak{d}_n$ such that $((\mathbf{v_1}|\cdots|\mathbf{v_n}), \{\mathfrak{d}_i\mathfrak{a}_i\}_{1\leq i\leq n})$ is a pseudo-basis of $\mathcal{M}$.*

Definition 1.12. *With the same notations as in Theorem 1.11, the ideals $\mathfrak{d}_1, \ldots, \mathfrak{d}_n$ are called the invariant factors of $\mathcal{L}$ and $\mathcal{M}$. The module index of $\mathcal{M}$ in $\mathcal{L}$ is the fractional ideal*

$$[\mathcal{L} : \mathcal{M}]_{\mathcal{O}} := \prod_{i=1}^{n} \mathfrak{d}_i.$$

Remark 1.13. Notice that the module index of $\mathcal{M}$ in $\mathcal{L}$ is well defined even if $\mathcal{M}$ is not contained in $\mathcal{L}$. For instance taking $K/F = \mathbb{Q}(i)/\mathbb{Q}$ and $V = K^2$, $\mathcal{L} = \mathbb{Z}[i] + \mathbb{Z}[i]$ and $\mathcal{M} = \mathbb{Z}[i] + 2\mathbb{Z}[i]$, we have $[\mathcal{L} : \mathcal{M}]_{\mathbb{Z}[i]} = 2\mathbb{Z}[i]$ and $[\mathcal{M} : \mathcal{L}]_{\mathbb{Z}[i]} = \frac{1}{2}\mathbb{Z}[i]$.

[6] The only reason why we do not define $\mathcal{O}$-lattices exclusively for Dedekind domains $\mathcal{O}$ is to treat uniformly *local* $\mathcal{O}_\mathfrak{p}$-lattices where $\mathcal{O}_\mathfrak{p}$ is either a Dedekind domain or $\mathcal{O}_\mathfrak{p} \simeq \mathfrak{o}_\mathfrak{p} \times \mathfrak{o}_\mathfrak{p}$.

Lemma 1.14. *Suppose that $\mathcal{O}$ is a Dedekind domain and let $\mathcal{L}$, $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{O}$-lattices in V. Then,*

1. $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}} \cdot [\mathcal{M} : \mathcal{N}]_{\mathcal{O}} = [\mathcal{L} : \mathcal{N}]_{\mathcal{O}}$.

Moreover suppose that $(B, \{\mathfrak{a}_i\}_{1\leq i\leq n})$ and $(C, \{\mathfrak{c}_i\}_{1\leq i\leq n})$ are pseudo-bases of $\mathcal{L}$ and $\mathcal{M}$ respectively. Then the following properties hold

2. $[\mathcal{O}^n : \mathcal{L}]_{\mathcal{O}} = \det(B) \cdot \mathfrak{a}_1 \cdots \mathfrak{a}_n$;
3. $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}} = \det(B^{-1}C) \cdot \mathfrak{a}_1^{-1}\mathfrak{b}_1 \cdots \mathfrak{a}_n^{-1}\mathfrak{b}_n$.

Proof. Notice first that the module index of $\mathcal{M}$ in $\mathcal{L}$ as defined above coincides with the ideal $\chi(\mathcal{L}, \mathcal{M})$ defined in [19, Chapter III, §1]. Hence we refer to [19, Chapter III, §1, Proposition 1] for a proof of the first property. For *2.* we apply Theorem 1.11 to $\mathcal{O}^n$ and $\mathcal{L}$: there exists a pseudo-basis $(B_0, \{\mathfrak{u}_i\}_{1\leq i\leq n})$ of $\mathcal{O}^n$ and fractional ideals $\mathfrak{d}_1, \ldots, \mathfrak{d}_n$ such that $(B_0, \{\mathfrak{u}_i\mathfrak{d}_i\}_{1\leq i\leq n})$ is a pseudo-basis of $\mathcal{L}$. Since $(I_n, \{\mathcal{O}\}_{1\leq i\leq n})$ is also a (pseudo-)basis of $\mathcal{O}^n$, Proposition 1.9 implies that $\det(B_0) \cdot \mathcal{O} = (\mathfrak{u}_1 \cdots \mathfrak{u}_n)^{-1}$. Similarly with $\mathcal{L}$, there exists $U \in \mathbf{GL}_n(K)$ such that $B = B_0U$ and $\det(U) \cdot \mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{u}_1\mathfrak{d}_1 \cdots \mathfrak{u}_n\mathfrak{d}_n$. It yields

$$\begin{aligned}[\mathcal{O}^n : \mathcal{L}]_{\mathcal{O}} &= \mathfrak{d}_1 \cdots \mathfrak{d}_n \\ &= \det(U) \cdot (\mathfrak{u}_1 \cdots \mathfrak{u}_n)^{-1} \cdot \mathfrak{a}_1 \cdots \mathfrak{a}_n \\ &= \det(B) \cdot \mathfrak{a}_1 \cdots \mathfrak{a}_n.\end{aligned}$$

For *3.*, notice that *1.* implies $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}} = [\mathcal{L} : \mathcal{O}^n]_{\mathcal{O}} \cdot [\mathcal{O}^n : \mathcal{M}]_{\mathcal{O}}$ and $[\mathcal{L} : \mathcal{O}^n]_{\mathcal{O}} = [\mathcal{O}^n : \mathcal{L}]_{\mathcal{O}}^{-1}$. The result then follows from *2.* □

We state an immediate corollary of *3.* which will be useful in Section 3.

Corollary 1.15. *Suppose that $\mathcal{O}$ is a Dedekind domain and let $\mathcal{L}$ and $\mathcal{M}$ be $\mathcal{O}$-lattices in V. Then, the module index $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}}$ is a principal ideal if and only if* $\mathrm{St}(\mathcal{L}) = \mathrm{St}(\mathcal{M})$.

Proof. This follows from Lemma 1.14, property *3.* □

1.4 Hermitian Lattices

Suppose that V is equipped with a Hermitian form Φ. This form can be restricted to $\mathcal{O}$-lattices in V, giving rise to several geometrical features. In what follows, we will refer to $\mathcal{O}$-lattices in (V, Φ) as *Hermitian lattices in* (V, Φ). First we define an analog of Gram matrices for Hermitian lattices. It will be the central object studied in module-LIP.

Definition 1.16. *Let $\mathbf{B} = (B, \{\mathfrak{a}_i\}_{1\leq i\leq n})$ be the pseudo-basis of a Hermitian lattice $\mathcal{L}$ in (V, Φ). The pseudo-Gram matrix associated to $\mathbf{B}$ is the pseudo-matrix*

$$\mathbf{G} = \left((\Phi(\mathbf{v_i}, \mathbf{v_j}))_{1\leq i,j\leq n}, \{\mathfrak{a}_i\}_{1\leq i\leq n}\right).$$

Example 1.17. Taking $V = K^n$ with the standard Hermitian form, the pseudo-Gram matrix associated to $\mathbf{B} = (B, \{\mathfrak{a}_i\}_{1\leq i\leq n})$ is $\mathbf{G} = (G, \{\mathfrak{a}_i\}_{1\leq i\leq n})$, where $G = B^*B$. Hence one recovers the definition given in [15, Definition 3.6].

Definition 1.18. *Let $\mathcal{L}$ be a Hermitian lattice in (V, Φ).*

1. *The dual of* $\mathcal{L}$ *is*
$$\mathcal{L}^{\#} := \{\mathbf{v} \in V \,|\, \Phi(\mathbf{v}, \mathcal{L}) \subset \mathcal{O}\},$$
it is a Hermitian lattice in (V, Φ) *as well.*
2. *If* $\mathcal{L} = \mathfrak{a}\mathcal{L}^{\#}$ *holds for some fractional ideal* $\mathfrak{a}$ *of* $\mathcal{O}$*, then* $\mathcal{L}$ *is said to be* $\mathfrak{a}$*-modular.*
3. *The scale of* $\mathcal{L}$*, denoted by* $\mathfrak{s}(\mathcal{L})$*, is the* $\mathcal{O}$*-ideal generated by* $\{\Phi(\mathbf{v}, \mathbf{w}) \,|\, \mathbf{v}, \mathbf{w} \in \mathcal{L}\}$.
4. *The norm of* $\mathcal{L}$*, denoted by* $\mathfrak{n}(\mathcal{L})$*, is the* $\mathfrak{o}$*-ideal generated by* $\{\Phi(\mathbf{v}, \mathbf{v}) \,|\, \mathbf{v}, \mathbf{v} \in \mathcal{L}\}$.

Remark 1.19 ([9], Remark 2.3.4). Let $\mathcal{L}$ be a Hermitian lattice in (V, Φ) with pseudo-basis $((\mathbf{v}_1|\cdots|\mathbf{v}_n), \{\mathfrak{a}_i\}_{1\leq i\leq n})$. Denote by $(\mathbf{v}_1^{\#}, \ldots, \mathbf{v}_n^{\#})$ the basis of V which is dual to $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ with respect to Φ. Then a pseudo-basis for $\mathcal{L}^{\#}$ is

$$\mathcal{L}^{\#} = (\overline{\mathfrak{a}_1})^{-1}\mathbf{v}_1^{\#} \oplus \cdots \oplus (\overline{\mathfrak{a}_n})^{-1}\mathbf{v}_n^{\#}. \tag{1}$$

Moreover, the scale and norm can be computed efficiently from a pseudo-Gram matrix $\mathbf{G} = ((g_{i,j})_{1\leq i,j\leq n}, \{\mathfrak{a}_i\}_{1\leq i\leq n})$ of $\mathcal{L}$. Indeed, one has

$$\mathfrak{s}(\mathcal{L}) = \sum_{1\leq i,j\leq n} g_{i,j}\mathfrak{a}_i\overline{\mathfrak{a}_j} \quad \text{and} \quad \mathfrak{n}(\mathcal{L}) = \sum_{i=1}^{n} g_{i,i}\mathrm{N}(\mathfrak{a}_i) \quad + \sum_{1\leq i<j\leq n} \mathrm{Tr}(g_{i,j}\mathfrak{a}_i\overline{\mathfrak{a}_j}).$$

In [15] and over totally real number fields, the norm of $\mathcal{L}$ was called the "Gram ideal" of $\mathcal{L}$. We stick to the first one which is more standard in the litterature.

Genera and classes. From now on, suppose furthermore that $\mathfrak{o}$ is the ring of integers of a number field F and K is a quadratic extension as before. Recall that $\mathcal{O}$ is the ring of integers of K. Let $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ and set $V_{\mathfrak{p}} = V \otimes_K K_{\mathfrak{p}}$. Scalar extension extends the form Φ to $V_{\mathfrak{p}}$, turning $(V_{\mathfrak{p}}, \Phi)$ into a Hermitian space over $K_{\mathfrak{p}}$.[7] Therefore $(\mathfrak{o}_{\mathfrak{p}}, F_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}, K_{\mathfrak{p}}, V_{\mathfrak{p}})$ falls within the scope of the previous paragraphs.

Finally, we let $\mathcal{L}$ be a Hermitian lattice in (V, Φ) and set $\mathcal{L}_{\mathfrak{p}} := \mathcal{L} \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$. Then, $\mathcal{L}_{\mathfrak{p}}$ defines a Hermitian ($\mathcal{O}_{\mathfrak{p}}$-)lattice in $(V_{\mathfrak{p}}, \Phi)$.

Definition 1.20. *Two Hermitian lattices* $\mathcal{L}, \mathcal{L}' \subset (V, \Phi)$ *are said to be isometric if there exists* $\sigma \in \mathrm{U}(V, \Phi)$ *such that* $\mathcal{L}' = \sigma(\mathcal{L})$*. We write* $\mathcal{L} \simeq_{\mathcal{O}} \mathcal{L}'$ *when* $\mathcal{L}$ *and* $\mathcal{L}'$ *are isometric. The isometry class of* $\mathcal{L}$ *is*

$$\mathrm{cls}(\mathcal{L}) = \{\textit{Hermitian lattices } \mathcal{M} \textit{ in } (V, \Phi) \,|\, \mathcal{L} \simeq_{\mathcal{O}} \mathcal{M}\},$$

and the automorphism group of $\mathcal{L}$ *is the subgroup of* $\mathrm{U}(V, \Phi)$ *given by* $\mathrm{Aut}(\mathcal{L}) = \{\sigma \in \mathrm{U}(V, \Phi) \,|\, \sigma(\mathcal{L}) = \mathcal{L}\}$*. On the other hand, the genus of* $\mathcal{L}$ *is*

$$\mathrm{gen}(\mathcal{L}) = \{\textit{Hermitian lattices } \mathcal{M} \textit{ in } (V, \Phi) \,|\, \forall\, \mathfrak{p} \in \mathbb{P}(\mathfrak{o}),\ \mathcal{L}_{\mathfrak{p}} \simeq_{\mathcal{O}_{\mathfrak{p}}} \mathcal{M}_{\mathfrak{p}}\}.$$

Remark 1.21. There is an inclusion $\mathrm{cls}(\mathcal{L}) \subseteq \mathrm{gen}(\mathcal{L})$ but it is in general strict. Also, the number of isomorphism classes in a genus is finite (see [9, Theorem 2.4.5]).

Definition 1.22 (Class number of $\mathcal{L}$). *The class number of a Hermitian lattice* $\mathcal{L}$ *in* (V, Φ) *is the number of isometry classes in* $\mathrm{gen}(\mathcal{L})$*. It is denoted by* $h(\mathcal{L})$.

[7] The form Φ is extended to $V_{\mathfrak{p}} = V \otimes_K K_{\mathfrak{p}}$ by putting $\Phi(\mathbf{v}\otimes k_1, \mathbf{w}\otimes k_2) := \Phi(\mathbf{v}, \mathbf{w}) \cdot k_1 \cdot \overline{k_2}$.

Jordan decompositions. Locally, $\mathcal{L}_\mathfrak{p}$ is almost orthogonal in the sense that it is an orthogonal sum of rank one or two sublattices. This splitting is essentially unique and it gives a description of $\mathrm{gen}(\mathcal{L})$, as $\mathfrak{p}$ runs in $\mathbb{P}(\mathfrak{o})$. Recall that for each $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$, we define $\mathfrak{P}$ as the largest ideal of $\mathcal{O}_\mathfrak{p}$ which contains $\mathfrak{p}$ and such that $\overline{\mathfrak{P}} = \mathfrak{P}$.

Definition 1.23. *An orthogonal sum $\bigoplus_{i=1}^t \mathcal{L}_i$ of Hermitian lattices in $(V_\mathfrak{p}, \Phi)$ is called a Jordan decomposition if the $\mathcal{L}_i$'s are $\mathfrak{P}^{s_i}$-modular with $s_1 < s_2 < \cdots < s_t$. Two Jordan decompositions $\bigoplus_{i=1}^t \mathcal{L}_i$ and $\bigoplus_{i=1}^{t'} \mathcal{L}'_i$ are said to be of the same Jordan type if $t = t'$ and the following properties are satisfied:*

1. *$\mathcal{L}_i$ and $\mathcal{L}'_i$ have the same rank.*
2. *$\mathfrak{s}(\mathcal{L}_i) = \mathfrak{s}(\mathcal{L}'_i)$.*
3. *$\mathfrak{n}(\mathcal{L}_i)\mathcal{O} = \mathfrak{s}(\mathcal{L}_i)$ if and only if $\mathfrak{n}(\mathcal{L}'_i)\mathcal{O} = \mathfrak{s}(\mathcal{L}'_i)$.*

Proposition 1.24 ([9], Theorem 3.3.3). *For any Hermitian lattice $\mathcal{L}$ in (V, Φ) and $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$, the Hermitian lattice $\mathcal{L}_\mathfrak{p}$ in $(V_\mathfrak{p}, \Phi)$ admits a Jordan decomposition $\mathcal{L}_\mathfrak{p} = \bigoplus_{i=1}^t \mathcal{L}_i$. Moreover any two Jordan decompositions of $\mathcal{L}_\mathfrak{p}$ are of the same type.*

Remark 1.25. It follows from [9, Algorithm 3.3.2] that the components appearing in a Jordan decomposition have rank at most two. We will refer to these sublattices as the *Jordan blocks* of the decomposition. With the notations of Definition 1.23, $\mathcal{L}_i$ is the orthogonal sum of the Jordan blocks which are $\mathfrak{P}^{s_i}$-modular.

Remark 1.26. Except if $\mathfrak{p}$ is a ramified prime, a Jordan type of $\mathcal{O}_\mathfrak{p}$-lattices fully determines a local isometry class. In other words, two Hermitian lattices $\mathcal{L}, \mathcal{M} \subset (V, \Phi)$ are locally isomorphic at $\mathfrak{p}$ (*i.e.,* $\mathcal{L}_\mathfrak{p} \simeq_{\mathcal{O}_\mathfrak{p}} \mathcal{M}_\mathfrak{p}$) if and only if $\mathcal{L}_\mathfrak{p}$ and $\mathcal{M}_\mathfrak{p}$ are of the same Jordan type (see [9, Theorem 3.3.6, 4]).

The $\mathfrak{P}^s$-modular Hermitian lattices in $(V_\mathfrak{p}, \Phi)$ admit an orthogonal basis, except in a few cases. Moreover, a Gram matrix can be made explicit (*c.f.*, [9, Proposition 3.3.5]). Exceptions occur when $\mathfrak{p}$ is ramified, giving rise to rank-two Hermitian lattices in $(V_\mathfrak{p}, \Phi)$. To cover these exceptions we will need the following definition.

Definition 1.27. *For $k \in \mathbb{N}$, we denote by $H(k)$ the (isometry) class of rank-two Hermitian lattices in $(V_\mathfrak{p}, \Phi)$ whose Gram matrix is $\left(\begin{smallmatrix} 0 & \pi^k \\ \overline{\pi}^k & 0 \end{smallmatrix}\right)$.*

1.5 Algorithmic Considerations

Lemma 1.28. *There is a polynomial-time algorithm that given pseudo-bases $\mathbf{B}$ and $\mathbf{C}$ of (full rank) $\mathcal{O}$-lattices $\mathcal{L}$ and $\mathcal{M}$ in V, computes the module index $[\mathcal{L} : \mathcal{M}]_\mathcal{O}$.*

Proof. Let us write $\mathbf{B} = (B, \{\mathfrak{a}_i\}_{1 \le i \le n})$ and $\mathbf{C} = (C, \{\mathfrak{b}_i\}_{1 \le i \le n})$ for the pseudo-bases given as input. According to Lemma 1.14 *3.*, the module index can be computed as $[\mathcal{L} : \mathcal{M}]_\mathcal{O} = \det(B^{-1}C) \cdot \mathfrak{a}_1^{-1}\mathfrak{b}_1 \cdots \mathfrak{a}_n^{-1}\mathfrak{b}_n$. This is done in polynomial-time in the size of $\mathbf{B}$ and $\mathbf{C}$. □

Lemma 1.29 ([9], Algorithm 3.3.2). *Let $\mathcal{L}$ be a Hermitian lattice in (V, Φ) and $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$. There is an algorithm that given a pseudo-basis of $\mathcal{L}$ and $\mathfrak{p}$, computes a Jordan decomposition of $\mathcal{L}_\mathfrak{p}$. Moreover, the output is a sum of orthogonal sublattices of $\mathcal{L}_\mathfrak{p}$ with rank at most two.*

Remark 1.30. Notice that Algorithm 3.3.2 from [9] can be performed on input $\mathfrak{p}$ and a pseudo-Gram matrix $\mathbf{G}$ of $\mathcal{L}$ instead of pseudo-basis. The output is then a Gram matrix of a Jordan decomposition of $\mathcal{L}_\mathfrak{p}$.

Remark 1.31. Although the complexity of this algorithm is not discussed in [9], Lemma 3.3.4 from *loc. cit.* may be used to show that, when $2 \notin \mathfrak{p}$, the running time is polynomial in the size of its input. In [9, Section 3.3.2] the case $2 \in \mathfrak{p}$ is treated, and the computation of several invariants allows one to obtain a Jordan decomposition.

In the following we provide an algorithm for computing the determinant of a local isometry between two isomorphic $\mathcal{O}_\mathfrak{p}$-lattices, up to some precision. This computation will be needed for Algorithm 1, for which we will not provide a complexity analysis. Let us specify that for cryptographic applications, our Algorithm 2 does not rely on this step. Moreover, for the latter, we will be able to prove a polynomial complexity.

Lemma 1.32. *Let (V, Φ) a Hermitian space and $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$. Given two pseudo-bases of Hermitian $\mathcal{O}$-lattices $\mathcal{L}$, $\mathcal{M} \subset (V, \Phi)$ in the same genus, there exists an algorithm for computing $\det(\sigma_\mathfrak{p}) \pmod{\mathfrak{P}^e}$ for any $e \in \mathbb{N}_{>0}$, where $\sigma_\mathfrak{p}$ is an element of $\mathrm{U}(V_\mathfrak{p}, \Phi)$ mapping $\mathcal{L}_\mathfrak{p}$ on $\mathcal{M}_\mathfrak{p}$.*

Proof. For simplicity (and practical interest), we make a proof only when $V = K^n$ is equipped with the Hermitian form $\sum_i x_i\overline{y_i}$. The algorithm starts by computing a basis $\{b_1, b_2\}$ of $\mathcal{O}_\mathfrak{p}$ over $\mathfrak{o}_\mathfrak{p}$.[8] From the pseudo-bases $\mathbf{B}$ and $\mathbf{C}$ of $\mathcal{L}$ and $\mathcal{M}$, the algorithm computes bases $B_\mathfrak{p}$ and $C_\mathfrak{p}$ of $\mathcal{L}_\mathfrak{p}$ and $\mathcal{M}_\mathfrak{p}$ respectively. By assumption, $\mathcal{L}_\mathfrak{p} \simeq_{\mathcal{O}_\mathfrak{p}} \mathcal{M}_\mathfrak{p}$ so there exist $\Sigma_\mathfrak{p} \in \mathbf{GL}_n(K_\mathfrak{p})$ and $U_\mathfrak{p} = (u_{i,j})_{1 \le i,j \le n} \in \mathbf{GL}_n(\mathcal{O}_\mathfrak{p})$ such that $\Sigma_\mathfrak{p} B_\mathfrak{p} = C_\mathfrak{p} U_\mathfrak{p}$ and $\Sigma_\mathfrak{p}^* \Sigma_\mathfrak{p} = \mathrm{Id}$. Our goal is to output $\det(\Sigma_\mathfrak{p}) \pmod{\mathfrak{P}^e}$ for such a matrix $\Sigma_\mathfrak{p}$. The algorithm then computes the Gram matrices $G_\mathfrak{p} = {B_\mathfrak{p}}^* B_\mathfrak{p}$ and $H_\mathfrak{p} = {C_\mathfrak{p}}^* C_\mathfrak{p}$ associated to these bases. Scaling if necessary $B_\mathfrak{p}$ and $C_\mathfrak{p}$ by a common power of π, one may assume that $G_\mathfrak{p}$ and $H_\mathfrak{p}$ have their coefficients in $\mathcal{O}_\mathfrak{p}$. Because of the relation between $B_\mathfrak{p}$ and $C_\mathfrak{p}$, it holds that

$$G_\mathfrak{p} = U_\mathfrak{p}^* H_\mathfrak{p} U_\mathfrak{p}, \tag{2}$$

where $G_\mathfrak{p}, H_\mathfrak{p} \in \mathcal{M}_n(\mathcal{O}_\mathfrak{p})$ and $U_\mathfrak{p} \in \mathbf{GL}_n(\mathcal{O}_\mathfrak{p})$ is unknown. Morever writing the coordinates of the $u_{i,j}$'s in the basis $\{b_1, b_2\}$, one can transform Equation (2) into a system of polynomial equations $\mathbf{f}(\mathbf{u}) = \mathbf{0}$ whose indeterminates lie in $\mathfrak{o}_\mathfrak{p}$. The algorithm solves this system modulo $\mathfrak{p}^e$, *i.e.*, it seeks for solutions with shape $f_0 + pf_1 + \cdots + f_{e-1}p^{e-1}$, where p is a uniformizer of $\mathfrak{o}_\mathfrak{p}$ and the f_i's run through a (finite) set of representatives for $\mathfrak{o}_\mathfrak{p}/\mathfrak{p}$. This can be done naively by an exhaustive search. Once a solution has been found, one obtains a solution $\widetilde{U}_\mathfrak{p}$ to $G_\mathfrak{p} = \widetilde{U}_\mathfrak{p}^* H_\mathfrak{p} \widetilde{U}_\mathfrak{p} \pmod{\mathfrak{p}^e\mathcal{O}}$.[9] However this solution modulo $\mathfrak{p}^e\mathcal{O}$ might not lift to a solution of Equation (2) in $\mathcal{O}_\mathfrak{p}$. To avoid this issue, we rely on a multivariable version of Hensel's lemma (see [4]): if the solution modulo $\mathfrak{p}^e\mathcal{O}$ we found cannot be lifted, the algorithm computes another one. It may happen that no solution modulo $\mathfrak{p}^e$ can be lifted. In such cases, the algorithm computes solutions modulo $\mathfrak{p}^{e+1}, \mathfrak{p}^{e+2}$, and so on until the lifting condition is satisfied.[10] Ultimately, the algorithm computes a solution $\widetilde{U}_\mathfrak{p}$ modulo $\mathfrak{p}^{e+k}$ for some $k \in \mathbb{N}_{>0}$. Since $\mathfrak{P}^e$ divides $\mathfrak{p}^{e+k}$, it finally outputs $\det(C_\mathfrak{p} B_\mathfrak{p}^{-1}) \det(\widetilde{U}_\mathfrak{p}) \pmod{\mathfrak{P}^e}$.[11] □

[8] Recall that $\mathfrak{o}_\mathfrak{p}$ is a principal ideal domain so $\mathcal{O}_\mathfrak{p}$ must be free over $\mathfrak{o}_\mathfrak{p}$.

[9] Notice that $\mathfrak{p}^e\mathcal{O} = b_1\mathfrak{p}^e + b_2\mathfrak{p}^e$.

[10] The existence of a solution to Equation (2) guarantees that there are solutions modulo $\mathfrak{p}^k$ for any k, but in some exceptional cases none of these solutions may be guaranteed to lift. In fact this is the case if all the solutions in $\mathcal{O}_\mathfrak{p}$ are multiple roots of $\mathbf{f}$. In this highly unlikely case, one possible solution would be to randomize the system by sampling some $V_\mathfrak{p} \in \mathbf{GL}_n(\mathcal{O}_\mathfrak{p})$ and trying to solve $G_\mathfrak{p} = U_\mathfrak{p}^* H'_\mathfrak{p} U_\mathfrak{p}$ where $H'_\mathfrak{p} := V_\mathfrak{p}^* H_\mathfrak{p} V_\mathfrak{p}$.

[11] Since $\Sigma_\mathfrak{p} B_\mathfrak{p} = C_\mathfrak{p} U_\mathfrak{p}$ and $\det(\Sigma_\mathfrak{p}), \det(U_\mathfrak{p}) \in \mathcal{O}_\mathfrak{p}^\times$, we know that $\det(C_\mathfrak{p} B_\mathfrak{p}^{-1}) \in \mathcal{O}_\mathfrak{p}^\times$ as well. Morever, the latter can be computed with arbitrary precision from $B_\mathfrak{p}$ and $C_\mathfrak{p}$.

Remark 1.33. Although at this stage we are not concerned with efficiency, we describe a less naive way to solve the equation $G_{\mathfrak{p}} = \widetilde{U}_{\mathfrak{p}}^* H_{\mathfrak{p}} \widetilde{U}_{\mathfrak{p}} \pmod{\mathfrak{P}^e}$, at least when the prime $\mathfrak{p}$ is unramified. Under this hypothesis, Jordan decompositions for $\mathcal{L}_{\mathfrak{p}}$ and $\mathcal{M}_{\mathfrak{p}}$ are orthogonal bases (see [9, Lemma 3.3.4]) which can be computed thanks to Lemma 1.29. Therefore, one obtains Gram matrices $G_{\mathfrak{p}}$ and $H_{\mathfrak{p}}$ which are diagonal. Still with the assumption that $\mathfrak{p}$ is unramified, the norm map $\mathrm{N} : \mathcal{O}_{\mathfrak{p}}^{\times} \to \mathfrak{o}_{\mathfrak{p}}^{\times}$ is surjective (see [19, Chapter V, §2]) so there must exists a solution $U_{\mathfrak{p}}$ to Equation (2) which is diagonal.

Example 1.34. We illustrate the previous algorithm on an example. Let us take $(\mathfrak{o}, F, \mathcal{O}, K) = (\mathbb{Z}, \mathbb{Q}, \mathbb{Z}[i], \mathbb{Q}(i))$ and $\mathcal{L}$ (resp. $\mathcal{M}$) the $\mathcal{O}$-lattice in K^2 with basis $B = \left(\begin{smallmatrix} 2+2i & 0 \\ 0 & 3i \end{smallmatrix}\right)$ (resp. with basis $C = \left(\begin{smallmatrix} 3-2i & 3+3i \\ 4+3i & -3+3i \end{smallmatrix}\right)$). We choose $p = e = 3$ and $\mathfrak{P} = 3 \cdot \mathcal{O}$. Then, $\{1, i\}$ is a basis of $\mathcal{O}_{\mathfrak{p}}$ over $\mathfrak{o}_{\mathfrak{p}}$. Our objective is to compute $\det(\Sigma_{\mathfrak{p}}) \pmod{27}$, where $\Sigma_{\mathfrak{p}}$ maps $\mathcal{L}_p$ on $\mathcal{M}_p$ and $\Sigma_{\mathfrak{p}}^* \Sigma = \mathrm{Id}$.

Following the notations in the proof of Lemma 1.32 and the remark above, we notice that $B = B_p$ is already a Jordan decomposition $\mathcal{L}_1 \oplus \mathcal{L}_2$ of $\mathcal{L}_p$, where $\mathcal{L}_1 = \left(\begin{smallmatrix} 2+2i \\ 0 \end{smallmatrix}\right) \cdot \mathcal{O}_p$ is unimodular, and $\mathcal{L}_2 = \left(\begin{smallmatrix} 0 \\ 3i \end{smallmatrix}\right) \cdot \mathcal{O}_p$ is $\mathfrak{P}^2$-modular. Further, a Jordan decomposition of $\mathcal{M}_p$ is obtained by Gram-Schmidt orthogonalization: if we denote the columns of C by c_1, c_2, then $C_p = (c_1' | c_2')$, where $c_1' = c_1$ and

$$c_2' = c_2 - \frac{c_1^* c_2}{c_1^* c_1} c_1 = \begin{pmatrix} \frac{21}{19} + \frac{3}{19} i \\ -\frac{3}{19} - \frac{15}{19} i \end{pmatrix}.$$

Moreover the Gram matrices are $G_p = \left(\begin{smallmatrix} 8 & 0 \\ 0 & 9 \end{smallmatrix}\right)$ and $H_p = \left(\begin{smallmatrix} 38 & 0 \\ 0 & 36/19 \end{smallmatrix}\right)$. In particular, one checks that $\mathcal{L}_p$ and $\mathcal{M}_p$ are of the same Jordan type (*c.f.*, Definition 1.23) and [9, Theorem 3.3.6] ensures that $\mathcal{L}_p$ and $\mathcal{M}_p$ are isometric over $\mathcal{O}_p$. According to the previous remark, there exists a solution $U_p = \left(\begin{smallmatrix} u_1+u_2 i & 0 \\ 0 & u_3+u_4 i \end{smallmatrix}\right)$ to $H_p = U_p^* G_p U_p$, where $u_1, u_2, u_3, u_4 \in \mathfrak{o}_p = \mathbb{Z}_3$ and $(u_1 + u_2 i)(u_3 + u_4 i) \in \mathcal{O}_p^{\times}$. Modulo 27 we have:

$$\begin{aligned} G_p = U_p^* H_p U_p \pmod{27} &\iff \begin{pmatrix} 8 & 0 \\ 0 & 9 \end{pmatrix} = \begin{pmatrix} 38\mathrm{N}(u_1 + u_2 i) & 0 \\ 0 & \frac{36}{19}\mathrm{N}(u_3 + u_4 i) \end{pmatrix} \pmod{27} \\ &\iff \begin{cases} {u_1}^2 + {u_2}^2 = 13 \pmod{27} \\ {u_3}^2 + {u_4}^2 = 25 \pmod{27}. \end{cases} \end{aligned}$$

Let $f_1(U_1, U_2) = {U_1}^2 + {U_2}^2 - 13$ and $f_2(U_3, U_4) = {U_3}^2 + {U_4}^2 - 25$. Then the system above is equivalent to $f_1(U_1, U_2) = 0 \pmod{27}$ and $f_2(U_3, U_4) = 0 \pmod{27}$. Moreover for the solution $\mathbf{u}_0 = (3, 2, 21, 4)$, we compute $(\nabla f_1)(3, 2) = (6, 4)$ and $(\nabla f_2)(21, 4) = (42, 8)$. With the notations of [4], one has $|f_1(3, 2)|_3 < ||(\nabla f_1)(3, 2)||_3^2$ and $|f_2(21, 4)|_3 < ||(\nabla f_2)(21, 4)||_3^2$ and Theorem 2.1 of *loc. cit.* ensures that $\mathbf{u}_0$ can be lifted to a solution of $f_1(U_1, U_2) = f_2(U_3, U_4) = 0$ in $\mathbb{Z}_3^4$. Consequently, a solution modulo 27 is $\widetilde{U}_p = \left(\begin{smallmatrix} 3+2i & 0 \\ 0 & 21+4i \end{smallmatrix}\right)$ and the algorithm outputs $\det(C_p' B_p^{-1}) \det(\widetilde{U}_p) \pmod{27} = 1 \pmod{27}$. Indeed, one can check that $\Sigma_p = \frac{1}{2} \left(\begin{smallmatrix} 1+i & -1-i \\ 1-i & 1-i \end{smallmatrix}\right)$ is unitary, has determinant 1 and maps it $\mathcal{L}_p$ on $\mathcal{M}_p$.

A key ingredient will be an algorithm originally due to Gentry and Szydlo [8], latter revisited by Lenstra and Silverberg [11] for solving efficiently the Principal Ideal Problem (PIP) in K. Testing if an ideal is principal (and if so computing a generator) is known as a hard algorithmic problem (for classical computers only, polynomial-time complexity can be achieved given access to a quantum computer, see [1]). However there is an important speedup when one is given the relative norm of a generator as an extra information, reaching classical polynomial-time complexity.

Lemma 1.35 ([11], Theorem 1.3). *Let K/F be a CM extension. There exists a deterministic polynomial-time algorithm* `LenstraSilverberg` *that given a $\mathbb{Z}$-basis of $\mathcal{O}$, the ring of integers of K, a fractional ideal I of K and an element $w \in F$ satisfying $I \cdot \overline{I} = w \cdot \mathcal{O}$, decides whether there exists $v \in K$ such that $I = v \cdot \mathcal{O}$ and $v\overline{v} = w$, and if so computes such an element v. Moreover if no such v exists, the algorithm returns " False ".*

2 Special genera

Let $(\mathfrak{o}, F, \mathcal{O}, K, V, \Phi)$ be as in Section 1.4 and let $\mathcal{L}$ be a Hermitian lattice in (V, Φ). Suppose furthermore that K/F is a CM extension of number fields and $\mathfrak{o}$ (resp. $\mathcal{O}$) is the ring of integers of F (resp. of K).

Definition 2.1 (Special genus). *A Hermitian lattice $\mathcal{M}$ in (V, Φ) is in the special genus of $\mathcal{L}$ if there exists $\sigma \in \mathrm{U}(V, \Phi)$ and for all $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$, there exists $\varphi_\mathfrak{p} \in \mathrm{SU}(V_\mathfrak{p}, \Phi)$ such that $\mathcal{M}_\mathfrak{p} = \sigma(\varphi_\mathfrak{p}(\mathcal{L}_\mathfrak{p}))$.*[12]

Remark 2.2. If $\mathcal{M}$ is in the special genus of $\mathcal{L}$, then $\mathcal{M}$ is *a fortiori* in $\mathrm{gen}(\mathcal{L})$. Moreover being in the same special genus defines an equivalence relation $\sim$ on $\mathrm{gen}(\mathcal{L})$.

Definition 2.3 (Special class number). *The equivalence class of $\mathcal{L}$ for $\sim$ will be denoted by $\mathrm{sgen}(\mathcal{L})$. Further, the number of special genera in $\mathrm{gen}(\mathcal{L})$ is a finite number called the special class number of $\mathcal{L}$ and denoted by $sh(\mathcal{L})$.*[13]

2.1 Shimura's Theorem

In [20], Shimura gave a complete set of invariants for the relation $\sim$ on $\mathrm{gen}(\mathcal{L})$. Morally it is given by the module index and the local determinant groups, for a few prime ideals. We follow Kirschmer's presentation [9, Section 5.4.2].

Definition 2.4. *Let $\mathcal{I}(\mathcal{O})$ be the group of fractional ideals of $\mathcal{O}$ with subgroups*

$$J = \{\mathfrak{a} \in \mathcal{I}(\mathcal{O}) \,|\, \mathfrak{a}\overline{\mathfrak{a}} = \mathcal{O}\} \quad \text{and} \quad J_0 = \{g\mathcal{O} \,|\, g \in K^\times,\, g\overline{g} = 1\}. \tag{3}$$

For $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$, we define the subgroups of $\mathcal{O}_\mathfrak{p}^\times$:

$$\begin{gathered} \mathcal{E}_{\mathfrak{p},0} = \{\varepsilon \in \mathcal{O}_\mathfrak{p}^\times \,|\, \varepsilon\overline{\varepsilon} = 1\} \quad ; \quad \mathcal{E}_{\mathfrak{p},1} = \{\overline{\varepsilon}\varepsilon^{-1} \,|\, \varepsilon \in \mathcal{O}_\mathfrak{p}^\times\} \\ \text{and} \quad \mathcal{E}(\mathcal{L}_\mathfrak{p}) = \{\det(\sigma) \,|\, \sigma \in \mathrm{Aut}(\mathcal{L}_\mathfrak{p})\}. \end{gathered} \tag{4}$$

The set $\mathcal{E}(\mathcal{L}_\mathfrak{p})$ will be refered as the local determinant group of $\mathcal{L}$ at $\mathfrak{p}$.

Notice that we have inclusions $J_0 \leq J \leq \mathcal{I}(\mathcal{O})$ and $\mathcal{E}_{\mathfrak{p},1}, \mathcal{E}(\mathcal{L}_\mathfrak{p}) \leq \mathcal{E}_{\mathfrak{p},0}$. The following proposition shows how to compute the local determinant groups from a Jordan decomposition.

Proposition 2.5. *Let $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ and $\mathfrak{P} \in \mathcal{I}(\mathcal{O})$ above $\mathfrak{p}$ as is Section 1.4.*

1. *If $\mathfrak{p}$ is unramified in K or if $\mathcal{L}_\mathfrak{p}$ has a Jordan block of odd rank, then*

$$\mathcal{E}(\mathcal{L}_\mathfrak{p}) = \mathcal{E}_{\mathfrak{p},0}.$$

[12] Notice that $\sigma \in \mathrm{U}(V, \Phi)$ can be extended to $V_\mathfrak{p} = V \otimes_K K_\mathfrak{p}$ by $\sigma(\mathbf{v} \otimes k) := \sigma(\mathbf{v}) \otimes k$.

[13] The finiteness of the class number $h(\mathcal{L})$ implies that there are only finitely many special genera in $\mathrm{gen}(\mathcal{L})$.

2. *If* $\mathfrak{p}$ *is ramified in* K *and* $2 \notin \mathfrak{p}$*, then*

$$\mathcal{E}(\mathcal{L}_\mathfrak{p}) = \begin{cases} \mathcal{E}_{\mathfrak{p},0} & \text{if } \mathcal{L}_\mathfrak{p} \text{ has a } \mathfrak{P}^i\text{-modular Jordan block for some } i \text{ even;} \\ \mathcal{E}_{\mathfrak{p},1} & \text{otherwise.} \end{cases}$$

3. *If* $\mathfrak{p}$ *is ramified in* K *and* $2 \in \mathfrak{p}$*, set* $e := v_\mathfrak{P}(\mathfrak{D})$.[14] *Then,*

$$\mathcal{E}(\mathcal{L}_\mathfrak{p}) = \begin{cases} \mathcal{E}_{\mathfrak{p},1} & \text{if } m = \operatorname{rank}(\mathcal{L}_\mathfrak{p}) \text{ is even and } \mathcal{L}_\mathfrak{p} \simeq \bigoplus_{i=1}^{m/2} H(s_i) \text{ with } s_i = e \pmod 2 \\ & \text{for all } 1 \leq i \leq \frac{m}{2} \text{ c.f., Definition 1.27;} \\ \mathcal{E}_{\mathfrak{p},0} & \text{otherwise.} \end{cases}$$

Proof. Cases *1.* and *2.* can be found in [20] or [9, Proposition 5.4.13]. For the ramified dyadic case, this was proven by Kirschmer in [10, Theorem 3.7]. □

We need a few more definitions to state Shimura's theorem.

Definition 2.6. *Let* $\mathrm{Cl}(\mathcal{O})$ *be the class group of* $\mathcal{O}$*, we put*

$$\mathrm{C}_0 := \{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}) \,|\, \overline{\mathfrak{a}} = \mathfrak{a}\} \leq \mathrm{Cl}(\mathcal{O}).$$

It is generated by $\{[\mathfrak{P}] \in \mathrm{Cl}(\mathcal{O}) \,|\, \mathfrak{P} \text{ is ramified in } \mathcal{O}\} \cup \{[\mathfrak{a}\mathcal{O}] \,|\, [\mathfrak{a}] \in \mathrm{Cl}(\mathfrak{o})\}$.

Definition 2.7. *Let* $P(\mathcal{L})$ *be the set of* $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ *such that* $\mathcal{E}(\mathcal{L}_\mathfrak{p}) = \mathcal{E}_{\mathfrak{p},1}$*. We define*

1. $\mathcal{E}(\mathcal{L}) = \prod_{\mathfrak{p} \in P(\mathcal{L})} \mathcal{E}_{\mathfrak{p},0}/\mathcal{E}_{\mathfrak{p},1}$;
2. $R = \{(\varepsilon\mathcal{E}_{\mathfrak{p},1})_{\mathfrak{p}\in P(\mathcal{L})} \in \mathcal{E}(\mathcal{L}) \,|\, \varepsilon \in \mathcal{O}^\times \text{ such that } \varepsilon\overline{\varepsilon} = 1\}$;
3. $H = \{(\varepsilon\mathcal{O}, (\varepsilon\mathcal{E}_{\mathfrak{p},1})_{\mathfrak{p}\in P(\mathcal{L})} \in J \times \mathcal{E}(\mathcal{L}) \,|\, \varepsilon \in K^\times \text{ such that } \varepsilon\overline{\varepsilon} = 1\}$.

The set $\mathcal{E}(\mathcal{L})$ *will be refered as the determinant group of* $\mathcal{L}$*.*

Theorem 2.8 (Shimura, [18] Theorem 2.10). *The map*

$$\Psi : \ \mathrm{gen}(\mathcal{L}) \longrightarrow J \times \mathcal{E}(\mathcal{L}) \quad ; \quad \mathcal{M} \longmapsto ([\mathcal{L} : \mathcal{M}]_\mathcal{O}, (\det(\sigma_\mathfrak{p})\mathcal{E}_{\mathfrak{p},1})_{\mathfrak{p}\in P(\mathcal{L})}), \tag{5}$$

where we choose $\sigma_\mathfrak{p} \in \mathrm{U}(V_\mathfrak{p}, \Phi)$ *such that* $\mathcal{M}_\mathfrak{p} = \sigma_\mathfrak{p}(\mathcal{L}_\mathfrak{p})$ *for all* $\mathfrak{p} \in P(\mathcal{L})$*, is well defined and it induces a bijection between the set of special genera in* $\mathrm{gen}(\mathcal{L})$ *and* $(J \times \mathcal{E}(\mathcal{L}))/H$*. Moreover, the number of special genera in* $\mathrm{gen}(\mathcal{L})$ *is*

$$sh(\mathcal{L}) = [J : J_0] \cdot [\mathcal{E}(\mathcal{L}) : R] = [\mathrm{Cl}(\mathcal{O}) : \mathrm{C}_0] \cdot [\mathcal{E}(\mathcal{L}) : R]. \tag{6}$$

Remark 2.9. The map Ψ from Equation 5 is well defined in the sense that it does not depend on the choice of $\sigma_\mathfrak{p}$. Indeed if we choose another isometry $\sigma'_\mathfrak{p}$ mapping $\mathcal{L}_p$ on $\mathcal{M}_p$, then $\sigma'_\mathfrak{p} = \sigma_\mathfrak{p} \circ \tau_\mathfrak{p}$, where $\tau_\mathfrak{p} \in \mathrm{Aut}(\mathcal{L}_\mathfrak{p})$. In particular, $\det(\tau_\mathfrak{p}) \in \mathcal{E}_{\mathfrak{p},1}$ (because $\mathfrak{p} \in P(\mathcal{L})$) and $\det(\sigma'_\mathfrak{p}) = \det(\sigma_\mathfrak{p})\det(\tau_\mathfrak{p}) = \det(\sigma_\mathfrak{p}) \pmod{\mathcal{E}_{\mathfrak{p},1}}$.

Remark 2.10. By Shimura's theorem, the module index $I = [\mathcal{L} : \mathcal{M}]_\mathcal{O}$ belongs to J, *i.e.*, it satisfies $I \cdot \overline{I} = \mathcal{O}$ whenever $\mathcal{L}$ and $\mathcal{M}$ are in the same genus. Further, asking for I to be a principal ideal is a necessary condition for having $\mathcal{M} \in \mathrm{sgen}(\mathcal{L})$.

Corollary 2.11. *Let* $\mathcal{M} \in \mathrm{gen}(\mathcal{L})$ *and for all* $\mathfrak{p} \in P$*, let us fix* $\sigma_\mathfrak{p} \in \mathrm{U}(V_\mathfrak{p}, \Phi)$ *such that* $\mathcal{M}_\mathfrak{p} = \sigma_\mathfrak{p}(\mathcal{L}_\mathfrak{p})$*. Then we have* $\mathcal{M} \in \mathrm{sgen}(\mathcal{L})$ *if and only if there exists* $\varepsilon \in K$ *such that* $\varepsilon\overline{\varepsilon} = 1$ *and*

$$\begin{cases} [\mathcal{L} : \mathcal{M}]_\mathcal{O} = \varepsilon \cdot \mathcal{O}; \\ \det(\sigma_\mathfrak{p}) = \varepsilon \pmod{\mathcal{E}_{\mathfrak{p},1}}, \text{ for all } \mathfrak{p} \in P(\mathcal{L}). \end{cases} \tag{7}$$

Proof. Observe that $\Psi(\mathcal{L}) = (\mathcal{O}, (\mathcal{E}_{\mathfrak{p},1})_{\mathfrak{p}\in P(\mathcal{L})}) \in H$. It follows from Theorem 2.8 implies that $\mathcal{M} \in \mathrm{sgen}(\mathcal{L})$ if and only if $\Psi(\mathcal{M}) \in H$. □

[14] Recall that $\mathfrak{D}$ is the different ideal of K/F, defined in Section 1. Moreover in the ramified case, [10, Lemma 3.1] ensures that $v_\mathfrak{P}(\mathfrak{D}) = v_\mathfrak{P}(\pi - \overline{\pi})$.

2.2 An Algorithm to Distinguish Special Genera

In [18], Schiemann turned Theorem 2.8 into an algorithmic method for computing representatives of the special genera in $\mathrm{gen}(\mathcal{L})$ (see also [9, Algorithm 5.4.15]).[15] Based on Corollary 2.11, we build an algorithm to decide if $\mathcal{M} \in \mathrm{gen}(\mathcal{L})$ belongs to $\mathrm{sgen}(\mathcal{L})$. This reduces to checking if the two conditions in Equation (7) are satisfied. The main trick is to use Lenstra and Silverberg algorithm (see Lemma 1.35) to test the first condition efficiently.

Algorithm 1: Distinguish $\mathrm{sgen}(\mathcal{L})$ within $\mathrm{gen}(\mathcal{L})$

Input:
- $\mathbb{Z}$-bases of $\mathfrak{o}$ and $\mathcal{O}$;
- $\alpha \in F^\times$ such that $K = F[X]/(X^2 - \alpha)$ is a CM number field;
- Basis of a n-dimensional vector space V;
- Hermitian form $\Phi : V \to K$;
- The list $Q = \{\mathfrak{p} \in \mathbb{P}(\mathfrak{o}) \mid \mathfrak{p} \text{ ramifies in } K\}$ and the different ideal $\mathfrak{D}$;
- Pseudo-bases of Hermitian lattices $\mathcal{L}$, $\mathcal{M}$ in (V, Φ) with $\mathcal{M} \in \mathrm{gen}(\mathcal{L})$.

Output:
- 1 if $\mathcal{M} \in \mathrm{sgen}(\mathcal{L})$;
- 0 otherwise.

```
Compute the module index I := [L : M]_O. // c.f., Lemma 1.28
Run LenstraSilverberg on input (O, I, 1). // c.f., Lemma 1.35
if the output is " False " then
    Return 0. // The first condition in Equation (7) is not satisfied
    else
        It returns ε ∈ K such that I = ε · O and ε·ε̄ = 1.
    end
end
for p in Q do
    Compute Jordan decompositions of L_p and M_p. // c.f., Lemma 1.29
    Decide whether E(M_p) = E_{p,0} or E(M_p) = E_{p,1}. // c.f., Proposition 2.5
    if E(M_p) = E_{p,1} then
        Add p to P.
    end
end
if P = { } then
    Return 1. // The second condition in Equation 7 is empty.
    else
        for p in P do
            Compute det(σ_p) (mod P^e), where σ_p(L_p) = M_p is a local isometry
              and e = v_P(D). // c.f., Lemma 1.32
            if det(σ_p)ε^{-1} − 1 ∉ P^e then
                Return 0. // c.f., Lemma 2.12
            end
        end
    end
end
Return 1.
```

[15] Precisely, Schiemann's algorithm computes a set of representatives for the isometry classes in $\mathrm{gen}(\mathcal{L})$, by first computing representatives for the special genera and then iterating a neighbouring method on it.

Before proving that Algorithm 1 is correct, we explain how the local conditions in Equation (7) can be checked. This is done along with the loop starting at Step 19. For $\mathfrak{p} \in P(\mathcal{L})$, the determinant of a local isometry mapping $\mathcal{L}_\mathfrak{p}$ on $\mathcal{M}_\mathfrak{p}$ can be computed with the desired precision thanks to Lemma 1.32. Then, the local condition at $\mathfrak{p}$ asks for the value of $\det(\sigma_\mathfrak{p})\varepsilon^{-1}$ modulo $\mathcal{E}_{\mathfrak{p},1}$.[16] We rely on the following result.

Lemma 2.12 ([10], Lemma 3.5). *Suppose that $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ ramifies in K. Then,*

$$\mathcal{E}_{\mathfrak{p},1} = \{\varepsilon \in \mathcal{E}_{\mathfrak{p},0} \,|\, \varepsilon - 1 \in \mathfrak{P}^e\},$$

where e is the $\mathfrak{P}$-adic valuation of $\mathfrak{D}$.

Consequently, if $\det(\sigma_\mathfrak{p})$ is known with precision e, one can compute $\det(\sigma_\mathfrak{p})\varepsilon^{-1} \pmod{\mathfrak{P}^e}$ (recall that $\varepsilon \in K \hookrightarrow K_\mathfrak{p}$ is known exactly) and Lemma 2.12 (materialized by Step 21) gives the answer.

Moreover, let us mention that the $\mathfrak{P}$-adic valuation $\mathfrak{D}$ can be determined *a priori* (see [10, §3] for a description).

Proposition 2.13. *On input $(\mathfrak{o}, \mathcal{O}, \alpha, V, \Phi)$, the list Q of ramified prime ideals in K/F, the different ideal $\mathfrak{D}$ and pseudo-bases of Hermitian lattices $\mathcal{L}$, $\mathcal{M}$ in (V, Φ) with $\mathcal{M} \in \mathrm{gen}(\mathcal{L})$, Algorithm 1 outputs 1 if $\mathcal{M} \in \mathrm{sgen}(\mathcal{L})$ and 0 otherwise.*

Proof. Recall that $\mathcal{M} \in \mathrm{sgen}(\mathcal{L})$ if and only if all conditions in Equation 7 are satisfied. At Step 4, the algorithm outputs 0 only if the first condition is not satisfied. By the end of the loop starting at Step 9, the set P is precisely equal to $P(\mathcal{L})$, *c.f.*, Definition 2.7. Therefore if P is in fact empty, there are no local conditions to check so we are guaranteed that $\mathcal{M} \in \mathrm{sgen}(\mathcal{L})$. Otherwise, for each $\mathfrak{p} \in P$, Step 21 tests if $\det(\sigma_\mathfrak{p}) = \varepsilon \pmod{\mathcal{E}_{\mathfrak{p},1}}$, which is the local condition given by Equation 7 at $\mathfrak{p}$. By the end of the loop starting at Step 19, and if the algorithm has not returned 0, then all the conditions are satisfied and $\mathcal{M}$ belongs to the special genus of $\mathcal{L}$. □

Remark 2.14. A rigorous complexity analysis of Algorithm 1 is set aside, since the complexity of Step 20 is unknown. Except for the latter (and Step 10 if $2 \in \mathfrak{p}$, see Remark 1.31), all the other steps can be executed in polynomial time in the size of the input. Moreover notice that the list Q given as input may be hard to compute for arbitrary fields. Nonetheless for cyclotomic fields $K = \mathbb{Q}(\zeta_m)$, Lemma 1.1 ensures that Q is either empty (if m is composite) or contains only one prime ideal, which is completely determined (if m is a prime power).

3 Consequences on module-LIP

In this section we expose the cryptographic motivation and applications behind the study of special genera and Algorithm 1. We fix $m \in \mathbb{N}_{>0}$ and a primitive m-th root of unity ζ_m, and we set $K = \mathbb{Q}(\zeta_m) \simeq \mathbb{Q}[X]/(\Phi_m)$ to be the cyclotomic field with conductor m and degree $d = \varphi(m)$. The maximal order of K is $\mathcal{O} = \mathbb{Z}[\zeta_m]$. Further, let $F = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ and $\mathfrak{o} = \mathbb{Z}[\zeta_m + \zeta_m^{-1}]$.

As mentionned in Section 1, K/F is a CM extension of number fields thus $(\mathfrak{o}, F, \mathcal{O}, K)$ falls under the scope of Section 2. Finally we let $n \in \mathbb{N}_{>0}$ and $V = K^n$ endowed with the standard Hermitian form $\Phi(\mathbf{v}, \mathbf{w}) = \sum_{i=1}^n v_i \overline{w_i}$.

[16] It follows from [9, Remark 5.4.12, 2.] that the quotient group $\mathcal{E}_{\mathfrak{p},0}/\mathcal{E}_{\mathfrak{p},1}$ has two elements and a system of representatives is given by $\{1, \overline{\pi}\pi^{-1}\} = \{1, u_\mathfrak{p}\}$.

3.1 Search and Decision module-LIP

The (search variant of the) module-Lattice Isomorphism Problem (module-LIP) has been defined in a more general framework than the one presented here, see [15]. Let us recall the notion of pseudo-Gram matrix given in Definition 1.16. In particular for any pseudo-Gram matrix $\mathbf{G} = (G, \{\mathfrak{a}_i\}_{1\leq i\leq n})$, there always exists an underlying $B \in \mathbf{GL}_n(K)$ such that $G = B^*B$.[17] Following [15, Section 3.1], we say that two pseudo-Gram matrices $\mathbf{G} = (G, \{\mathfrak{a}_i\}_{1\leq i\leq n})$ and $\mathbf{H} = (H, \{\mathfrak{b}_i\}_{1\leq i\leq n})$ are *congruent* whenever there exists $U = (u_{i,j})_{1\leq i,j\leq n} \in \mathbf{GL}_n(K)$ such that $H = U^*GU$ and *2.* and *3.* of Proposition 1.9 are satisfied. Such a matrix U, called a *congruence matrix* between $\mathbf{G}$ and $\mathbf{H}$.

Definition 3.1 (search-modLIP$^{\mathbf{B}}_K$, Definition 3.11 [15]). *Let $\mathbf{B}$ be a pseudo-basis of a Hermitian lattice $\mathcal{L}$ in (V, Φ), and $\mathbf{G}$ the pseudo-Gram matrix associated to $\mathbf{B}$. Let $\mathbf{H}$ be a pseudo-Gram matrix congruent to $\mathbf{G}$. Then the (worst-case) search module Lattice Isomorphism Problem with parameters K and $\mathbf{B}$ (search-modLIP$^{\mathbf{B}}_K$) and input $\mathbf{H}$, is to compute a congruence matrix between $\mathbf{G}$ and $\mathbf{H}$.*

On the other hand, the decisional variant has been defined previously but only for Euclidean lattices (called dLIP, see [6, Section 2.2]). Its definition is naturally adapted for Hermitian lattices in (V, Φ).

Definition 3.2 (decision-modLIP$^{\mathbf{B}}_K$). *Let $\mathbf{B}$ be a pseudo-basis of a Hermitian lattice $\mathcal{L}$ in (V, Φ), and $\mathbf{G}$ the pseudo-Gram matrix associated to $\mathbf{B}$. Let $\mathbf{H}$ be a pseudo-Gram matrix. Then the decision module Lattice Isomorphism Problem with parameters K and $\mathbf{B}$ (decision-modLIP$^{\mathbf{B}}_K$) and input $\mathbf{H}$, is to decide if $\mathbf{G}$ and $\mathbf{H}$ are congruent.*

An important observation is that $\mathbf{G}$ and $\mathbf{H}$ are congruent if and only if they are associated to pseudo-bases of isomorphic Hermitian lattices in (V, Φ). Thanks to this rephrasing, there is a well defined notion of genus (resp. special genus) for pseudo-Gram matrices, *i.e.*, we say that $\mathbf{G}$ and $\mathbf{H}$ are in the same *genus*, denoted $\mathbf{H} \in \mathrm{gen}(\mathbf{G})$ (resp. *special genus*, denoted $\mathbf{H} \in \mathrm{sgen}(\mathbf{G})$) when they are associated to pseudo-bases of Hermitian lattices in the same genus (resp. special genus).

3.2 An algorithm for HAWK's lattice

Given $\mathbf{G}$ and $\mathbf{H}$, one can decide whether $\mathbf{H}$ is in $\mathrm{gen}(\mathbf{G})$ by computing and comparing Jordan decompositions (see Lemma 1.29 and Remark 1.30). Thus in order to make decision-modLIP$^{\mathbf{B}}_K$ a hard problem, the input $\mathbf{H}$ has to be chosen in the genus of $\mathbf{G}$. Now concerning the special genus, unfortunately Algorithm 1 is not suited to the setting of decision-modLIP, since the computation of $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}}$, where $\mathcal{L}$ (resp. $\mathcal{M}$) is associated to $\mathbf{G}$ (resp. $\mathbf{H}$), in Step 1 requires pseudo-bases of $\mathcal{L}$ and $\mathcal{M}$.[18] As a consequence, we relax the conditions in Corollary 2.11. Concretely, we put aside the

[17] In [15], pseudo-Gram matrices are defined more generally for *module-lattices* in $(K_{\mathbb{R}})^n$, where $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$. A subtle point in this setting is that a (pseudo)-Gram matrix G with coefficients in K is not necessarily associated with a Hermitian lattice $\mathcal{L} \subset K^n$, *i.e.*, a factorization $G = B^*B$ with $B \in \mathbf{GL}_n(K)$ may not exist. However, such a (Cholesky) factorization is always possible over $K_{\mathbb{R}}$, see [15, Lemma 3.10].

[18] We emphasize that computing a factorization of H in $\mathbf{GL}_n(K)$ is in general a hard task. A so-called Cholesky factorization of G is efficiently computable, but it has usually its coefficients in $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$ instead of K, see [15, Proposition 3.4].

local conditions and we focus on testing if $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}}$ is a principal ideal generated by an element of norm 1; a necessary condition for having $\mathcal{M} \in \mathrm{sgen}(\mathcal{L})$, according to Theorem 2.8 and Remark 2.10.

In fact the local conditions in Corollary 2.11 only have a negligible contribution in the size of $sh(\mathcal{L}) = [\mathrm{Cl}(\mathcal{O}) : \mathrm{C}_0] \cdot [\mathcal{E}(\mathcal{L}) : R]$ (see Equation (6)). Indeed, $[\mathcal{E}(\mathcal{L}) : R] \leq \#\mathcal{E}(\mathcal{L}) \leq 2^{\#P(\mathcal{L})}$ and $P(\mathcal{L})$ is contained in the set of primes of F which ramify in K. For cyclotomic fields, there is at most one ramified prime ideal (see Lemma 1.1) so $[\mathcal{E}(\mathcal{L}) : R] \leq 2$. Moreover using only pseudo-Gram matrices, we show how Lenstra and Silverberg's algorithm (Lemma 1.35) allows to decide whether $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}}$ is a principal ideal generated by an element of norm 1 (although it does not give access to any generator).

Algorithm 2: Decide if $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}}$ is generated by an element of norm 1

Input: • Pseudo-Gram matrices $\mathbf{G} = (G, \{\mathfrak{a}_i\}_{1 \leq i \leq n})$ and $\mathbf{H} = (H, \{\mathfrak{b}_i\}_{1 \leq i \leq n})$ of (unknown) Hermitian lattices $\mathcal{L}$, $\mathcal{M}$ with $\mathbf{H} \in \mathrm{gen}(\mathbf{G})$.

Output: • 1 if $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}}$ is principal;
• 0 otherwise.

Set $\gamma = \det(G^{-1}H)$ and build the fractional ideal $J = \gamma \cdot \mathfrak{a}_1^{-1}\mathfrak{b}_1 \cdots \mathfrak{a}_n^{-1}\mathfrak{b}_n$.
Run `LenstraSilverberg`(J, γ). `// c.f., Lemma 1.35`
if *the output is « False »* **then**
  Return 0. `// The first condition in Equation (7) is not verified`
  else
    It returns $\eta \in K$ such that $J = \eta \cdot \mathcal{O}$ and $\eta\overline{\eta} = \gamma$.
    Return 1.
  end
end

Proposition 3.3. *Let K be a cyclotomic number field and $\mathbf{G} = (G, \{\mathfrak{a}_i\}_{1 \leq i \leq n})$, $\mathbf{H} = (H, \{\mathfrak{b}_i\}_{1 \leq i \leq n}) \in \mathrm{gen}(\mathbf{G})$ be pseudo-Gram matrices associated to Hermitian lattices $\mathcal{L}$ and $\mathcal{M}$ in K^n. On input $\mathbf{G}$ and $\mathbf{H}$, Algorithm 2 decides whether the module index $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}}$ is a principal ideal generated by an element of norm 1. Moreover, the algorithm runs in polynomial-time in the size of the input.*

Proof. Recall from Corollary 1.15 that $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}}$ is principal if and only if $\mathrm{St}(\mathcal{L}) = \mathrm{St}(\mathcal{M})$, *i.e.*, if and only if $[\mathfrak{a}_1 \cdots \mathfrak{a}_n] = [\mathfrak{b}_1 \cdots \mathfrak{b}_n]$ in $\mathrm{Cl}(\mathcal{O})$. We introduce $J := \overline{\det(B^{-1}C)} \cdot [\mathcal{L} : \mathcal{M}]_{\mathcal{O}}$. Thanks to Lemma 1.14, J equals $\det(G^{-1}H) \cdot \prod_i \mathfrak{a}_i^{-1}\mathfrak{b}_i$. Hence it is a fractional ideal of K efficiently computable from $\mathbf{G}$ and $\mathbf{H}$. We compute $J \cdot \overline{J} = \det(G^{-1}H) \cdot [\mathcal{L} : \mathcal{M}]_{\mathcal{O}} \cdot \overline{[\mathcal{L} : \mathcal{M}]_{\mathcal{O}}}$ and according to Theorem 2.8 and Remark 2.10, we have $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}} \cdot \overline{[\mathcal{L} : \mathcal{M}]_{\mathcal{O}}} = \mathcal{O}$ so $J \cdot \overline{J} = \det(G^{-1}H) \cdot \mathcal{O}$.

One observes that J is principal if and only if $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}}$ is, and it has a generator of norm $\det(G^{-1}H)$ if and only if $[\mathcal{L} : \mathcal{M}]_{\mathcal{O}}$ has a generator of norm 1. Since a basis of J is known, as well as a generator of $J \cdot \overline{J}$, then a call to Lenstra and Silverberg algorithm (Lemma 1.35) on input $(J, \det(G^{-1}H))$ allows to conclude. □

Remark 3.4. Interestingly, the set $P(\mathcal{L})$ can be shown to be empty for several Hermitian lattices, including HAWK's lattice $\mathcal{O}^2$. As a result, there are no local conditions to verify for these lattices, and Algorithm 2 alone suffices to determine whether two such Hermitian lattices lie in the same special genus.

Corollary 3.5 (HAWK). *Let K be a cyclotomic number field. Suppose that $\mathbf{B}$ is a pseudo-basis of HAWK's lattice $\mathcal{O}^2$ and $\mathbf{G}$ is the pseudo-Gram matrix associated. Let $\mathbf{H}$ be an input of decision-modLIP$^{\mathbf{B}}_K$. Then on input $\mathbf{B}$ and $\mathbf{H}$, Algorithm 2 decides in polynomial-time whether $\mathbf{H} \in \mathrm{sgen}(\mathbf{G})$.*

Proof. If a Hermitian lattice $\mathcal{L}$ admits an orthogonal decomposition $\mathcal{L} = \mathcal{L}_1 \perp \mathcal{L}_2$ in which $\mathcal{L}_1$ has rank one, then each completion $\mathcal{L}_\mathfrak{p}$ contains a Jordan block of odd rank. In this case, Proposition 2.5 implies that $P(\mathcal{L})$ is empty. By Corollary 2.11, deciding whether a lattice $\mathcal{M} \in \mathrm{gen}(\mathcal{L})$ belongs to the special genus $\mathrm{sgen}(\mathcal{L})$ reduces to checking whether the ideal index $[\mathcal{L} : \mathcal{M}]_\mathcal{O}$ is principal and generated by an element of norm 1. For such lattices, we conclude that Algorithm 2 correctly distinguishes $\mathrm{sgen}(\mathcal{L})$ within $\mathrm{gen}(\mathcal{L})$. In particular, this immediately applies to HAWK's lattice $\mathcal{O}^2$. □

3.3 Numerical Estimates for HAWK's lattice

Ultimately, we take a closer look at HAWK's lattice $\mathcal{O}^2$. For this specific lattice, we compute exactly the number $sh(\mathcal{O}^2)$ of special genera contained in its genus, using Equation (6). Subsequently, we derive bounds on $h(\mathcal{L})$, the number of isometry classes within the genus of $\mathcal{O}^2$. Taken together, these results provide numerical evidence that distinguishing special genera within $\mathrm{gen}(\mathcal{O}^2)$ offers limited advantage for solving the decision module-LIP problem (for the parameter K and lattice $\mathcal{O}^2$).

Proposition 3.6. *Let K be the cyclotomic number field of conductor m and with maximal totally real subfield F. The number of special genera in $\mathrm{gen}(\mathcal{O}^2)$ equals*

$$sh(\mathcal{O}^2) = \frac{h_K}{h_F}, \tag{8}$$

where h_K (resp. h_F) is the class number of K (resp. F).

Proof. Recall from Theorem 2.8 that $sh(\mathcal{O}^2) = [\mathrm{Cl}(\mathcal{O}) : \mathrm{C}_0] \cdot [\mathcal{E}(\mathcal{O}^2) : R]$. We compute these two factors individually. Recall the notations for $\mathrm{Cl}(\mathcal{O})$ and C_0 from Definition 2.6. In our case, C_0 is generated by the classes $[\mathfrak{a}\mathcal{O}]$ where $\mathfrak{a} \in \mathcal{I}(\mathfrak{o})$ and eventually if m is a prime power, the class of the unique ramified prime $\mathfrak{P}$. But $\mathfrak{P} = (1 - \zeta_m) \cdot \mathcal{O}$ (see Lemma 1.1) so $[\mathfrak{P}] = [\mathcal{O}]$ and $[\mathrm{Cl}(\mathcal{O}) : \mathrm{C}_0] = h_K/h_F$. For the second term, Remark 3.4 yields $[\mathcal{E}(\mathcal{O}^2) : R] = 1$. □

Remark 3.7. More generally for a rank-2 Hermitian lattice $\mathcal{L}$ in K^2, the same proof as above shows that $sh(\mathcal{L}) \in \{\frac{h_K}{h_F}, \frac{2h_K}{h_F}\}$ (this is because $[\mathcal{E}(\mathcal{L}) : R] \leq \#\mathcal{E}(\mathcal{L}) \leq 2$).

Remark 3.8. Even if it means to assume GRH, $h_F = 1$ holds for several conductors m including a lot of primes and all power-of-two up to 512 (see [14] and [13]). More generally for power-of-two conductors, Weber conjectured that $h_F = 1$ always holds.

One the other hand, bounds on $h(\mathcal{O}^2)$, *i.e.*, the number of isometry classes in the genus of $\mathcal{O}^2$, can be obtained by computing the *mass* of $\mathcal{O}^2$. In full generality, the mass of a Hermitian lattice is defined as follows.

Definition 3.9. *Let $\mathcal{L}$ be a Hermitian lattice in (V, Φ). The mass of $\mathcal{L}$ is*

$$\mathrm{Mass}(\mathcal{L}) := \sum_{\mathcal{L}'} \frac{1}{\#(\mathrm{Aut}(\mathcal{L}'))},$$

where the sums ranges on a set of representatives for the isometry classes in $\mathrm{gen}(\mathcal{L})$.

Remark 3.10. Estimates on the automorphism groups $\mathrm{Aut}(\mathcal{L}')$ yield bounds on $h(\mathcal{L})$ in terms of $\mathrm{Mass}(\mathcal{L})$. For instance since $\mu(K)$ embeds in $\mathrm{Aut}(\mathcal{L}')$ for any Hermitian lattice $\mathcal{L}'$, the lower bound $\#(\mathrm{Aut}(\mathcal{L}')) \geq \#(\mu(K)) = m$ holds, giving $\mathrm{Mass}(\mathcal{L}) \leq h(\mathcal{L})/m$.[19] For rank-2 Hermitian lattices, Chevignard *et. al.* proved in [2, Theorem 3.12] the upper bound $\mathrm{Aut}(\mathcal{L}') \leq 32d^2m$. Altogether we obtain

$$\mathfrak{B}_- := m \cdot \mathrm{Mass}(\mathcal{L}) \leq h(\mathcal{L}) \leq 32d^2m \cdot \mathrm{Mass}(\mathcal{L}) =: \mathfrak{B}_+, \tag{9}$$

for any rank-2 Hermitian lattice $\mathcal{L}$.

Moreover the mass of $\mathcal{L}$ can be computed using a formula due to Siegel. We specialize this formula to rank-2 Hermitian lattices in K^2.

Theorem 3.11 (Siegel's mass formula, [9], Proposition 4.2.7 *3.*). *Let $\mathcal{L}$ be a rank-2 Hermitian lattice in K^2. Then,*

$$\mathrm{Mass}(\mathcal{L}) = \frac{1}{2^{d-1}} \cdot \prod_{\mathfrak{p} \in \mathbb{P}(\mathfrak{o})} \lambda(\mathcal{L}_\mathfrak{p}) \cdot \left| \frac{\zeta_K}{\zeta_F}(0) \right| \cdot |\zeta_F(-1)|\,, \tag{10}$$

where the local factors $\lambda(\mathcal{L}_\mathfrak{p})$ are defined in [9, Definition 4.2.6] and ζ_F, ζ_K are the Dedekind zeta functions of F and K respectively.

The computation of $\mathrm{Mass}(\mathcal{O}^2)$ was done by van Gent [25] for power-of-two conductors $m \in \{512, 1024, 2048\}$. For completeness, we generalize [25, Lemma 4] to any conductor.

Lemma 3.12 ([25], Lemma 4). *Let $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$. Then,*

$$\lambda(\mathcal{O}_\mathfrak{p}{}^2) = \begin{cases} \frac{1}{2}(p+1) & \text{if } m = p^r \text{ and } \mathfrak{p} \text{ is the unique ramified prime above } p; \\ 3 & \text{if } m = 2^r \text{ and } \mathfrak{p} \text{ is the unique ramified prime above } 2; \\ 1 & \text{otherwise.} \end{cases}$$

Proof. The formula for the local factors is given by [9, Lemma 4.2.9], for which $m_0 = 2$ and $m_1 = 0$. Suppose first that the conductor m is composite. Then by Lemma 1.1, $\mathfrak{p}$ is unramified and the local factor is either equal to $\left(\frac{2}{2}\right)_2 = 1$ (split case) or to $|\left(\frac{2}{2}\right)_{-2}| = 1$ (inert case). Now assume that $m = p^r$ with p an odd prime number. If $p \notin \mathfrak{p}$, the same computation as before gives $\lambda(\mathcal{O}_\mathfrak{p}{}^2) = 1$. Otherwise $\mathfrak{p}$ is the unique prime ideal above p and the local factors equals $\frac{1}{2}(p+1)\left(\frac{1}{0}\right)_{p^2} = \frac{1}{2}(p+1)$. Finally the case of power-of-two conductors was treated in [25, Lemma 4] (for arbitrary rank). □

Together with Equation (9), we obtain an estimation on the class number of $\mathcal{L}$. We do the computations for power-of-two conductors $m \in \{128, 256, 512, 1024\}$ but also for the prime $m = 131$ and $m = 134$. These conductors are taken such that $h_F = 1$ (see [28] and [14] for the values of h_K), in order to maximize $sh(\mathcal{O}^2)$. We obtain the following results using the same PARI/GP [23] code as in [25].

Remark 3.13. The results above for $\mathcal{O}^2$ do not differ much for an arbitrary rank-2 Hermitian lattice $\mathcal{L}$. Indeed the special class number of $\mathcal{L}$ is either equal to h_K/h_F or $2h_K/h_F$ if $[\mathcal{E}(\mathcal{L}) : R] = 2$, and [25, Corollary 6] states the inequality $\mathrm{Mass}(\mathcal{L}) \geq \frac{1}{3}\mathrm{Mass}(\mathcal{O}^2)$ so the class number of $\mathcal{L}$ cannot be way smaller.

[19] The roots of unity $\mu(K)$ embed in $\mathrm{Aut}(\mathcal{L}')$ by the diagonal mapping $\mu \mapsto \mathrm{diag}(\mu, \ldots, \mu)$.

m	d	$\log_2(\mathfrak{B}_-)$	$\log_2(\mathfrak{B}_+)$	$\log_2(\frac{h_K}{h_F})$
128	64	138	155	18
134	66	123	154	20
256	128	397	416	63
131	130	387	420	65
512	256	1040	1062	182 (GRH)
1024	512	2564	2607	?

Fig. 3: Bit size estimations for the bounds on $h(\mathcal{O}^2)$ and $\frac{h_K}{h_F} = sh(\mathcal{O}^2)$.

Remark 3.14. We conclude this section by giving an example of $\mathcal{O}$-lattices which are not isomorphic but belong to the same special genus. Let $\mathcal{L} = \mathfrak{a}\mathbf{b_1} \oplus \mathfrak{b}\mathbf{b_2}$ and $\mathcal{M} = \mathbf{b_1} \oplus \mathfrak{a}\mathfrak{b}\mathbf{b_2}$, where $\mathbf{b_1} = \binom{1}{0}, \mathbf{b_2} = \binom{0}{1}$ and $\mathfrak{a}, \mathfrak{b} \subset K$ are coprime integral ideals. If $\mathfrak{p} \in \mathbb{P}(\mathfrak{o})$ does not divide $\mathfrak{a}$ or $\mathfrak{b}$, then $\mathcal{L}_\mathfrak{p} \simeq_{\mathcal{O}_\mathfrak{p}} \mathcal{O}_\mathfrak{p}\mathbf{b_1} \oplus \mathcal{O}_\mathfrak{p}\mathbf{b_2} \simeq_{\mathcal{O}_\mathfrak{p}} \mathcal{M}_\mathfrak{p}$. Now if $\mathfrak{p}$ divides $\mathfrak{a}$, one has $\mathcal{L}_\mathfrak{p} \simeq_{\mathcal{O}_\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}\mathbf{b_1} \oplus \mathcal{O}_\mathfrak{p}\mathbf{b_2} \simeq_{\mathcal{O}_\mathfrak{p}} \mathcal{M}_\mathfrak{p}$, because $\mathfrak{p} \nmid \mathfrak{b}$. In the same way, $\mathcal{L}_\mathfrak{p} \simeq_{\mathcal{O}_\mathfrak{p}} \mathcal{M}_\mathfrak{p}$ if $\mathfrak{p} \mid \mathfrak{b}$. Therefore, $\mathcal{L}$ and $\mathcal{M}$ are in the same genus. Moreover, the Steinitz class of $\mathcal{L}$ and $\mathcal{M}$ are both equal to $[\mathfrak{a}\mathfrak{b}]$ so Remark 3.4 gives the claim.

References

1. 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*, pages 893–902. SIAM, 2016.
2. Clémence Chevignard, Pierre-Alain Fouque, Guilhem Mureau, Alice Pellet-Mary, and Alexandre Wallet. A reduction from hawk to the principal ideal problem in a quaternion algebra. *Cryptology ePrint Archive*, 2024.
3. Henri Cohen. *Advanced topics in computational number theory*, volume 193. Springer Science & Business Media, 2012.
4. Keith Conrad. A multivariable hensel's lemma. *Lecture note available at http://kconrad. math. uconn. edu/blurbs*, 4, 2020.
5. Léo Ducas, Eamonn W Postlethwaite, Ludo N Pulles, and Wessel van Woerden. Hawk: Module lip makes lattice signatures fast, compact and simple. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 65–94. Springer, 2022.
6. Léo Ducas and Wessel van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 643–673. Springer, 2022.
7. AG Earnest and Dennis R Estes. Class groups in the genus and spinor genus of binary quadratic lattices. *Proceedings of the London Mathematical Society*, 3(1):40–52, 1980.
8. Craig Gentry and Mike Szydlo. Cryptanalysis of the revised ntru signature scheme. In *International conference on the theory and applications of cryptographic techniques*, pages 299–320. Springer, 2002.
9. Markus Kirschmer. Definite quadratic and hermitian forms with small class number. *Habilitation, RWTH Aachen University*, 2016.
10. Markus Kirschmer. Determinant groups of hermitian lattices over local fields. *Archiv der Mathematik*, 113(4):337–347, 2019.
11. Hendrik W Lenstra Jr and Alice Silverberg. Testing isomorphism of lattices over cm-orders. *SIAM Journal on Computing*, 48(4):1300–1334, 2019.

12. Cong Ling, Jingbo Liu, and Andrew Mendelsohn. On the spinor genus and the distinguishing lattice isomorphism problem. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 329–358. Springer, 2024.
13. John C Miller. Class numbers of totally real fields and applications to the weber class number problem. *arXiv preprint arXiv:1405.1094*, 2014.
14. John C Miller. Real cyclotomic fields of prime conductor and their class numbers ii (algebraic number theory and related topics 2014). 64:19–32, 2017.
15. Guilhem Mureau, Alice Pellet-Mary, Georgii Pliatsok, and Alexandre Wallet. Cryptanalysis of rank-2 module-lip in totally real number fields. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 226–255. Springer, 2024.
16. Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.
17. Onorato Timothy O'Meara. *Introduction to quadratic forms*, volume 117. Springer, 2013.
18. Alexander Schiemann. Classification of hermitian forms with the neighbour method. *Journal of Symbolic Computation*, 26(4):487–508, 1998.
19. Jean-Pierre Serre. *Local fields*, volume 67. Springer Science & Business Media, 2013.
20. Goro Shimura. Arithmetic of unitary groups. *Annals of Mathematics*, 79(2):369–409, 1964.
21. The Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu, 2018.
22. Michael Szydlo. Hypercubic lattice reduction and analysis of ggh and ntru signatures. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 433–448. Springer, 2003.
23. The PARI Group, Univ. Bordeaux. *PARI/GP version 2.16.2*, 2024. available from http://pari.math.u-bordeaux.fr/.
24. Daniël van Gent and Wessel van Woerden. A search to distinguish reduction for the isomorphism problem on direct sum lattices. *Cryptology ePrint Archive*, 2025.
25. Daniël MH van Gent. A note on the genus of the hawk lattice. *Cryptology ePrint Archive*, 2025.
26. Wessel van Woerden. Dense and smooth lattices in any genus. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 386–417. Springer, 2024.
27. Lawrence C Washington. *Introduction to cyclotomic fields*, volume 83. Springer Science & Business Media, 2012.
28. Wikipedia. Cyclotomic field — Wikipedia, the free encyclopedia. http://en.wikipedia.org/w/index.php?title=Cyclotomic%20field&oldid=1263364879, 2025.