COMPUTING IDEAL CLASSES REPRESENTATIVES IN QUATERNION ALGEBRAS

ARIEL PACETTI AND NICOLÁS SIROLLI

Abstract. Let K be a totally real number field and let B be a totally definite quaternion algebra over K. In this article, given a set of representatives for ideal classes for a maximal order in B, we show how to construct in an efficient way a set of representatives of ideal classes for any Bass order in B. The algorithm does not require any knowledge of class numbers, and improves the equivalence checking process by using a simple calculation with global units. As an application, we compute ideal classes representatives for an order of discriminant 30 in an algebra over the real quadratic field $\mathbb{Q}[\sqrt{5}]$.

Introduction

The theory of quaternion algebras over number fields plays a central role in many computations related to modular forms. For example, orders in totally definite quaternion algebras over totally real fields can be used to compute Hilbert modular forms, as explained in [Piz80] for classical modular forms and in [DD08] for Hilbert modular forms over totally real fields of even degree. These methods require first to find a suitable order in such algebra, and then compute representatives for the equivalence classes of its left ideals. The purpose of this article is to compute both things in an efficient way, and in a rather general setting, which includes Eichler orders and many others - for example, the orders used in [PT07] to compute half-integral weight modular forms in Shimura correspondence with modular forms of level p^2.

Let K be a number field and let B be a quaternion algebra over K. When computing ideal classes representatives, locally isomorphic orders in B can be regarded as equal, since two such orders have a connecting ideal, and multiplication by this ideal gives a bijection between ideal classes representatives for both orders. Hence, it is natural to group locally isomorphic orders into *genera*. Our first main result is the following theorem.

Theorem A. *There is an algorithm that, given a Bass order R in B, computes suborders of R of any given genus.*

In particular, Theorem A allows us to calculate any Bass order in any quaternion algebra, since by [Voi10] we know how to obtain maximal orders in this general setting.

2010 *Mathematics Subject Classification.* Primary: 11R52.

Key words and phrases. Quaternion algebras, ideal classes representatives, Bass orders.

The first author was partially supported by PIP 2010-2012 GI and UBACyT X867. The second author was partially supported by a CONICET PhD Fellowship.

The second main result concerns the computation of left ideal classes representatives for Bass orders, assuming that K is totally real and B is totally definite.

Theorem B. *There is an algorithm that, given a Bass order R in B and a set of representatives S of left R-ideal classes, computes left ideal classes representatives for suborders of R of any given genus. Furthermore, the set of norms of the computed ideals is the same as the set of norms of the ideals in S.*

Hence, starting from a set of representatives for a maximal order (which can be obtained following [Piz80] or [SW05] in certain particular cases, and [KV10] in the general setting), we can compute representatives for any Bass order in B.

The algorithm is such that that the constructed ideals are contained in the given ones. This allows to, in comparison to the methods *à la Pizer* (see, e.g., [Piz80], [CS01], [SW05]), avoid the repeated usage of norm forms for checking equivalences between ideals (see [Piz80], Propositions 1.18 and 2.27), using this technique just once (see Remark 3.23).

Bass orders can be described locally in terms of certain ternary quadratic forms. The strategy for proving Theorems A and B is to reduce the situation to the case of considering *maximal* Bass suborders of R. This allows to construct both the desired suborder and its ideal classes representatives in terms of local computations related to the forms in correspondence with the orders. In this special case, we also give a method to compute the ideal classes representatives by global means.

The article is organized as follows. In the first section we give the basic definitions that will be used throughout the article. In the second section we prove Theorem A, first recalling the local description of Bass orders. The third section is devoted to prove Theorem B. In the fourth section we present an example of our algorithm: we show how to construct representatives of ideal classes for an Eichler order of discriminant 30 in the quaternion algebra B over $\mathbb{Q}[\sqrt{5}]$ ramified at the two infinite places.

Throughout the article, in order to make the exposition clearer, we assume that no dyadic primes occur in the discriminants of the orders considered. This case, with the extra assumption that 2 is inert in K, is treated separately in the appendix.

Acknowledgements: We would like to thank Gonzalo Tornaría and Lassina Dembélé for the useful conversations we held with them.

1. Basic notions and notation

We start recalling some basic definitions and properties of quaternion algebras that will be used during the paper. A more detailed exposition can be found, for example, in [Vig80] and [Kap69].

Let $\mathcal{O}$ be a Dedekind domain, and let K denote its fraction field. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$. By $\mathcal{O}_\mathfrak{p}$ we denote the completion of $\mathcal{O}$ at $\mathfrak{p}$, and we denote completions of other objects in a similar way. By $v_\mathfrak{p}$ we denote the $\mathfrak{p}$-adic valuation on $K_\mathfrak{p}$. The residue field $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is denoted by $k_\mathfrak{p}$, and by $\pi_\mathfrak{p}$ we denote an element of $\mathcal{O}$ which is a local uniformizer of $\mathfrak{p}\mathcal{O}_\mathfrak{p}$.

Let B be a *quaternion algebra* over K, that is, a four dimensional, central and simple K-algebra with unity. Then B has a natural involution $x \mapsto \bar{x}$, that induces the linear form *(reduced) trace* given by $\mathrm{Tr}(x) = x + \bar{x}$ and the quadratic form *(reduced) norm* given by $N(x) = x\bar{x}$. The bilinear form corresponding to the latter is $(x, y) \mapsto \mathrm{Tr}(x\bar{y})$.

A *lattice* Λ in B is a finitely generated $\mathcal{O}$-module such that $\Lambda \otimes_{\mathcal{O}} K \simeq B$. Given a lattice Λ, its *dual lattice* $\Lambda^\vee$ is defined by

$$\Lambda^\vee = \{x \in B : \mathrm{Tr}(x\Lambda) \subseteq \mathcal{O}\}.$$

An *order* is a lattice R which is also a subring with unity. Its *(reduced) discriminant* is the ideal $d(R) \subseteq \mathcal{O}$ whose square is the ideal generated by $\{\det(\mathrm{Tr}(x_i\bar{x_j})) : x_1, \ldots, x_4 \in R\}$.

Given a lattice Λ, the set

$$R_l(\Lambda) = \{x \in B : x\Lambda \subseteq \Lambda\}$$

is an order called *the left order of* Λ. The right order is defined and denoted in a similar way. We define the *inverse* of Λ by

$$\Lambda^{-1} = \{x \in B : \Lambda x \Lambda \subseteq \Lambda\}.$$

We say that Λ is *invertible* if $\Lambda\Lambda^{-1} = R_l(\Lambda)$ and $\Lambda^{-1}\Lambda = R_r(\Lambda)$. An order R is called a *Gorenstein* order if every lattice Λ such that $R_l(\Lambda) = R$ is invertible, and it is called a *Bass* order if every order containing it is a Gorenstein order.

Given two lattices $\Lambda \supseteq \Lambda'$ in B, the *index* of Λ' in Λ is the ideal $[\Lambda : \Lambda'] \subseteq \mathcal{O}$ generated by $\{\det(\phi) : \phi \in \mathrm{End}_K(B),\ \phi(\Lambda) \subseteq \Lambda'\}$.

Let R be an order in B. A *left R-(invertible) ideal* is an invertible lattice I such that $R_l(I) = R$. Two left R-ideals I and J are called *equivalent* if there exists $x \in B^\times$ such that $I = Jx$, and the set of equivalence classes is denoted by $Cl(R)$. A left R-ideal I is called *principal* if it is equivalent to R, i.e., if there exists $x \in B^\times$ such that $I = Rx$. A lattice I is invertible if and only if $I_\mathfrak{p}$ is principal for all $\mathfrak{p}$.

Let R, R' be orders in B. We say that they are in the same *genus* if $R_\mathfrak{p} \simeq R'_\mathfrak{p}$ for all $\mathfrak{p}$. This is equivalent to the existence of an ideal I connecting R and R', i.e., such that $R_l(I) = R$ and $R_r(I) = R'$.

Notation index

- $\mathfrak{p}, \mathfrak{q}, \ldots$: prime ideals of $\mathcal{O}$.
- $\Lambda, \Lambda', \ldots$: lattices in B.
- $R, R', \ldots$: orders in B.
- $R^{\times,1} = \{x \in R : N(x) = 1\}$.
- $I, J, \ldots$: invertible lattices in B.
- $\langle a_1, \ldots, a_n \rangle$: the quadratic form $\sum_{i=1}^n a_i x_i^2$
- $\mathrm{diag}(a_1, \ldots, a_n)$: the diagonal matrix with a_i as (i, i) coefficient.

2. Constructing suborders

The aim of this section is to prove Theorem A. Its proof, together with a precise description of the input of the algorithm, will we given at the end of the section, once we have developed the necessary tools.

The problem can be reduced to compute *maximal* suborders of R in any given genus. The index of a maximal suborder of a given order is known, according to Corollary 1.11 of [Brz83], which we recall here.

Proposition 2.1. *Let R be an order in B, and let R' be a maximal suborder of R. Then, there exists $\mathfrak{p}$ such that $[R : R'] = \mathfrak{p}$ or $\mathfrak{p}^2$ and $\mathfrak{p}R' \subseteq R$.*

Hence, maximal suborders of a given order R can be obtained by describing the maximal suborders of $R_\mathfrak{p}$ for every $\mathfrak{p}$.

Local Bass orders. ¿From here on we assume that $\mathfrak{p} \nmid 2$, and we fix $\delta \in \mathcal{O}$ such that $(\frac{\delta}{\mathfrak{p}}) = -1$.

The correspondence between isomorphism classes of Gorenstein orders in quaternion algebras over local fields and ternary quadratic forms was developed in [Brz82]. This correspondence was explored further in [Lem11], where it is refined to describe Bass orders. We summarize here the results we extract from this article.

Let $R_\mathfrak{p}$ be an order, and let $\mathcal{E} = \{f_0, f_1, f_2, f_3\}$ be a basis of $R_\mathfrak{p}^\vee$ satisfying

$$\mathrm{Tr}(f_0) = 1, \quad \mathrm{Tr}(f_1) = \mathrm{Tr}(f_2) = \mathrm{Tr}(f_3) = 0. \tag{2.2}$$

Denote by $M_\mathcal{E}$ the Gram matrix of the norm form in the trace zero submodule of $R_\mathfrak{p}^\vee$ corresponding to $\mathcal{E}$, i.e.

$$M_\mathcal{E} = \big(\mathrm{Tr}(f_i \bar{f}_j)\big)_{1 \le i,j \le 3}.$$

Then $d \cdot M_\mathcal{E}$ is the ternary quadratic form associated to $R_\mathfrak{p}$, where d is any generator of $d(R_\mathfrak{p})$.

Conversely, to an integral ternary quadratic form f over $\mathcal{O}_\mathfrak{p}$ can be associated an order $C_0(f)$ in a quaternion algebra over $K_\mathfrak{p}$: the order and the algebra are given by the even part of the Clifford algebras associated to f over $\mathcal{O}_\mathfrak{p}$ and $K_\mathfrak{p}$ respectively.

By Propositions 5.8 and 5.10 of [Lem11], the maps $R_\mathfrak{p} \mapsto d \cdot M_\mathcal{E}$ and $f \mapsto C_0(f)$ give a bijection between isomorphism classes of Bass orders in quaternion algebras over $K_\mathfrak{p}$ and the set of ternary quadratic forms of Table 2.1, where we group forms into *classes* that will be treated in a unified way when convenient.

Class	Form	Parameters	Hilbert Symbol
A1	$\langle 1, -1, \pi_\mathfrak{p}^s \rangle$	$s \ge 0$	1
A2	$\langle 1, -\delta, \pi_\mathfrak{p}^s \rangle$	$s \ge 1$	$(-1)^s$
B	$\langle 1, \pi_\mathfrak{p}, \epsilon_1 \pi_\mathfrak{p} \rangle$	$\epsilon_1 \in \{1, \delta\}$	$\left(\frac{-\epsilon_1}{\mathfrak{p}}\right)$
C	$\langle 1, \epsilon_1 \pi_\mathfrak{p}, \epsilon_2 \pi_\mathfrak{p}^s \rangle$	$\epsilon_1, \epsilon_2 \in \{1, \delta\}$, $s \ge 2$	$\left(\frac{\epsilon_1}{\mathfrak{p}}\right)^s \left(\frac{-\epsilon_2}{\mathfrak{p}}\right)$

TABLE 2.1. Ternary quadratic forms in correspondence with local Bass orders.

In particular, every Bass order R in B induces a family $(f_\mathfrak{p})_\mathfrak{p}$ of ternary quadratic forms, by letting $f_\mathfrak{p}$ be the form from Table 2.1 corresponding to $R_\mathfrak{p}$. This family satisfies that $f_\mathfrak{p} = \langle 1, -1, 1 \rangle$ for almost every $\mathfrak{p}$, and is independent of the genus of R.

Equation (2.6) below implies that, given a form $f = \langle 1, a, b\rangle$, then the quaternion algebra $C_0(f) \otimes_{\mathcal{O}_\mathfrak{p}} K_\mathfrak{p}$ is a matrix algebra if and only if $\langle a, b, ab\rangle$ is isotropic, i.e., if and only if the Hilbert symbol $(\frac{-a,-b}{\mathfrak{p}})$ equals 1. The sign for each case is shown in Table 2.1.

The graphs on Figure 2.1 show how the isomorphism classes of Bass orders in quaternion algebras over $K_\mathfrak{p}$ are distributed. Each vertex represents an isomorphism class of Bass orders, and there is an edge between two vertices if and only if there is an order $R_\mathfrak{p}$ corresponding to the top vertex, and an order $R'_\mathfrak{p}$ corresponding to the bottom vertex, such that $R'_\mathfrak{p}$ is a maximal suborder of $R_\mathfrak{p}$; if f and g are respectively the corresponding forms from Table 2.1, we will say that g is *beneath* f. Note that these graphs reflect the assertion of Proposition 2.1.

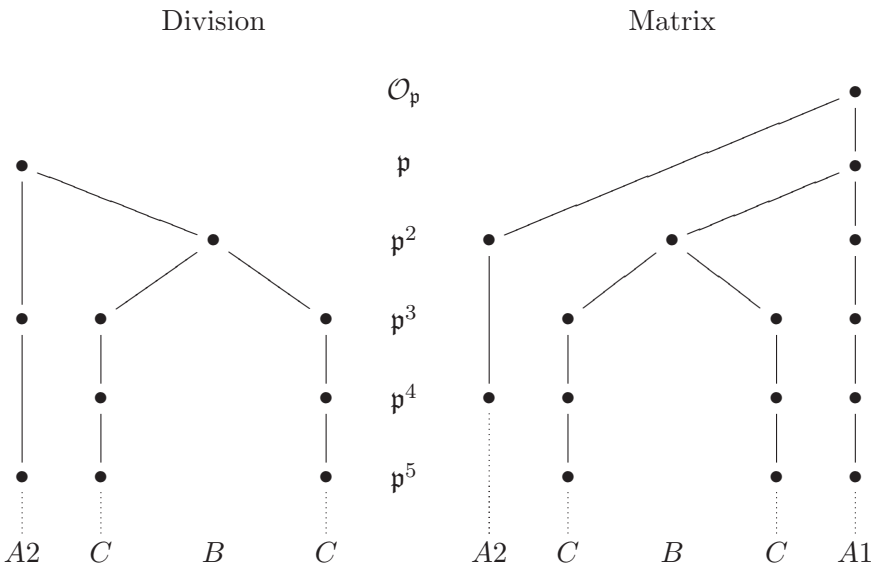

FIGURE 2.1. Isomorphism classes of Bass orders

All the orders in the left graph lie in the division quaternion algebra, while all the orders in the right one lie in the matrix algebra. Horizontally aligned vertices have the same discriminant, which is indicated in the middle column. Vertically aligned vertices correspond to forms of the same *class*, which is indicated in the bottom row. The orders of class A1 are the so called *Eichler orders* (see, e.g., Section 2 of [Brz83]), and the orders of class A2 are the *orders of level* p^{2r+1} considered in [Piz76].

Example 2.3. Let $s \geq 0$. The order $E_s = \left(\begin{smallmatrix} \mathcal{O}_\mathfrak{p} & \mathcal{O}_\mathfrak{p} \\ \pi_\mathfrak{p}^s\mathcal{O}_\mathfrak{p} & \mathcal{O}_\mathfrak{p} \end{smallmatrix}\right) \subseteq M_2(\mathcal{O}_\mathfrak{p})$ is a Bass order of class A1 and discriminant $\mathfrak{p}^s$. E_{s+1} is a maximal suborder of E_s.

Definition 2.4. Let $R_\mathfrak{p}$ be a Bass order in correspondence with the form $f = \langle 1, a, b\rangle$, and let $\mathcal{B} = \{1, e_1, e_2, e_3\}$ be a basis of $R_\mathfrak{p}$ as an $\mathcal{O}_\mathfrak{p}$-module.

We say that $\mathcal{B}$ is a *good basis* if the e_i satisfy

$$\begin{array}{lll} e_1^2 = -ab, & e_2^2 = -b, & e_3^2 = -a, \\ e_1e_2 = -be_3, & e_2e_3 = -e_1, & e_3e_1 = -ae_2, \\ e_2e_1 = be_3, & e_3e_2 = e_1, & e_1e_3 = ae_2. \end{array} \tag{2.5}$$

Every Bass order has a good basis (see Section 4 of [Lem11], and also [GL09]), and in such basis the norm form is given by

$$N = \langle 1, ab, b, a\rangle. \tag{2.6}$$

Example 2.7. A good basis for the order E_s defined above is given by

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad e_1 = \begin{pmatrix} 0 & 1 \\ \pi_{\mathfrak{p}}^s & 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & 1 \\ -\pi_{\mathfrak{p}}^s & 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Let $R_{\mathfrak{p}}$ be an order in correspondence with the form $f = \langle 1, a, b\rangle$, and let $\mathcal{E} = \{f_0, f_1, f_2, f_3\}$ be a basis of $R_{\mathfrak{p}}^\vee$ satisfying (2.2). Let $e_i = 4ab \cdot f_j \bar{f}_k$, where (i, j, k) is an even permutation of $(1, 2, 3)$, and define $\mathcal{E}^\dagger = \{1, e_1, e_2, e_3\}$. Then $\mathcal{E}^\dagger$ is a basis of $R_{\mathfrak{p}}$ (see [Lem11], Theorem 4.3).

Proposition 2.8. *With the notation as above, if $\mathcal{E}$ is such that*

$$2ab \cdot M_{\mathcal{E}} = \operatorname{diag}(1, a, b), \tag{2.9}$$

then $\mathcal{E}^\dagger$ is a good basis of $R_{\mathfrak{p}}$ (see [Lem11], Theorem 4.3).

Remark 2.10. Conversely, if $\mathcal{B}$ is a good basis of $R_{\mathfrak{p}}$, then $M_{\mathcal{B}^\vee}$ satisfies (2.9), where given a basis $\mathcal{B} = \{e_0, e_1, e_2, e_3\}$ of $R_{\mathfrak{p}}$, we denote by $\mathcal{B}^\vee = \{f_0, f_1, f_2, f_3\}$ the basis of $R_{\mathfrak{p}}^\vee$ characterized by the equations $\operatorname{Tr}(e_i \bar{f}_j) = \delta_{ij}$.

Constructing maximal suborders, the local case. Given an order $R_{\mathfrak{p}}$ corresponding to a form f from Table 2.1, we construct a representative for each of the one or two isomorphism classes of maximal suborders of $R_{\mathfrak{p}}$ (see Figure 2.1). The way to do this is, given a good basis $\{1, e_1, e_2, e_3\}$ of $R_{\mathfrak{p}}$ and a form g from Table 2.1 beneath f, find elements $d_1, d_2, d_3 \in R_{\mathfrak{p}}$ satisfying the equations (2.5) corresponding to the form g. Then, the order $R'_{\mathfrak{p}} = \langle 1, d_1, d_2, d_3\rangle_{\mathcal{O}_{\mathfrak{p}}}$ is a maximal suborder of $R_{\mathfrak{p}}$ in correspondence with the form g, for which $\{1, d_1, d_2, d_3\}$ is a good basis.

Using Hensel's Lemma, take $\alpha_0, \alpha_1, \beta_0, \beta_1, \mu, \nu \in \mathcal{O}_{\mathfrak{p}}$ satisfying:

- $\alpha_0^2 - \alpha_1^2 = \pi_{\mathfrak{p}}$.
- $\beta_0^2 + \beta_1^2 = \delta$.
- $\mu^2 = -1$, when $(\frac{-1}{\mathfrak{p}}) = 1$.
- $\nu^2 = -\delta$, when $(\frac{-1}{\mathfrak{p}}) = -1$.

Proposition 2.11. *The elements d_1, d_2, d_3 defined by Table 2.2 satisfy the equations (2.5) corresponding to the form g.*

Proof. In each case, it is straightforward to check that the d_i's satisfy the equations (2.5) corresponding to g, using that the e_i's satisfy the equations corresponding to f. □

Form	Form beneath	Good basis for $R'_{\mathfrak{p}}$
$\langle 1,-1,\pi_{\mathfrak{p}}^{s}\rangle$	$\langle 1,-1,\pi_{\mathfrak{p}}^{s+1}\rangle$	$d_1=\alpha_0e_1+\alpha_1e_2,$ $d_2=\alpha_1e_1+\alpha_0e_2, d_3=e_3$
$\langle 1,-1,1\rangle$	$\langle 1,-\delta,\pi_{\mathfrak{p}}^{2}\rangle$	$d_1=\pi_{\mathfrak{p}}(\beta_1e_1-\beta_0e_3),$ $d_2=\pi_{\mathfrak{p}}e_2, d_3=\beta_0e_1+\beta_1e_3$
$\langle 1,-1,\pi_{\mathfrak{p}}\rangle$	$\langle 1,\pi_{\mathfrak{p}},\pi_{\mathfrak{p}}\rangle$, if $(\frac{-1}{\mathfrak{p}})=1$	$d_1=\mu\pi_{\mathfrak{p}}e_3, d_2=\mu e_1, d_3=e_2$
	$\langle 1,\pi_{\mathfrak{p}},\delta\pi_{\mathfrak{p}}\rangle$, if $(\frac{-1}{\mathfrak{p}})=-1$	$d_1=\nu\pi_{\mathfrak{p}}e_3, d_2=\nu e_1, d_3=e_2$
$\langle 1,-\delta,\pi_{\mathfrak{p}}^{s}\rangle$	$\langle 1,-\delta,\pi_{\mathfrak{p}}^{s+2}\rangle$	$d_1=\pi_{\mathfrak{p}}e_1, d_2=\pi_{\mathfrak{p}}e_2, d_3=e_3$
$\langle 1,-\delta,\pi_{\mathfrak{p}}\rangle$	$\langle 1,\pi_{\mathfrak{p}},\delta\pi_{\mathfrak{p}}\rangle$, if $(\frac{-1}{\mathfrak{p}})=1$	$d_1=\mu\pi_{\mathfrak{p}}e_3, d_2=\mu e_1, d_3=e_2$
	$\langle 1,\pi_{\mathfrak{p}},\pi_{\mathfrak{p}}\rangle$, if $(\frac{-1}{\mathfrak{p}})=-1$	$d_1=\nu^{-1}\pi_{\mathfrak{p}}e_3, d_2=\nu^{-1}e_1,$ $d_3=e_2$
$\langle 1,\pi_{\mathfrak{p}},\pi_{\mathfrak{p}}\rangle$	$\langle 1,\pi_{\mathfrak{p}},\pi_{\mathfrak{p}}^{2}\rangle$	$d_1=\pi_{\mathfrak{p}}e_2, d_2=e_1, d_3=e_3$
	$\langle 1,\delta\pi_{\mathfrak{p}},\pi_{\mathfrak{p}}^{2}\rangle$	$d_1=\pi_{\mathfrak{p}}(-\beta_1e_2+\beta_0e_3),$ $d_2=e_1, d_3=\beta_0e_2+\beta_1e_3$
$\langle 1,\pi_{\mathfrak{p}},\delta\pi_{\mathfrak{p}}\rangle$	$\langle 1,\pi_{\mathfrak{p}},\delta\pi_{\mathfrak{p}}^{2}\rangle$	$d_1=\pi_{\mathfrak{p}}e_2, d_2=e_1, d_3=e_3$
	$\langle 1,\delta\pi_{\mathfrak{p}},\delta\pi_{\mathfrak{p}}^{2}\rangle$	$d_1=\pi_{\mathfrak{p}}e_3, d_2=e_1, d_3=e_2$
$\langle 1,\pi_{\mathfrak{p}},\pi_{\mathfrak{p}}^{s}\rangle$	$\langle 1,\pi_{\mathfrak{p}},\pi_{\mathfrak{p}}^{s+1}\rangle$	$d_1=\pi_{\mathfrak{p}}e_2, d_2=e_1, d_3=e_3$
$\langle 1,\delta\pi_{\mathfrak{p}},\pi_{\mathfrak{p}}^{s}\rangle$	$\langle 1,\delta\pi_{\mathfrak{p}},\delta\pi_{\mathfrak{p}}^{s+1}\rangle$	$d_1=\delta\pi_{\mathfrak{p}}e_2, d_2=e_1, d_3=e_3$
$\langle 1,\pi_{\mathfrak{p}},\delta\pi_{\mathfrak{p}}^{s}\rangle$	$\langle 1,\pi_{\mathfrak{p}},\delta\pi_{\mathfrak{p}}^{s+1}\rangle$	$d_1=\pi_{\mathfrak{p}}e_2, d_2=e_1, d_3=e_3.$
$\langle 1,\delta\pi_{\mathfrak{p}},\delta\pi_{\mathfrak{p}}^{s}\rangle$	$\langle 1,\delta\pi_{\mathfrak{p}},\pi_{\mathfrak{p}}^{s+1}\rangle$	$d_1=\delta\pi_{\mathfrak{p}}e_2, d_2=\delta^{-1}e_1,$ $d_3=e_3$

TABLE 2.2. Suborders

Remark 2.12. It can be proved that this construction is general, in the sense that every maximal suborder of $R_{\mathfrak{p}}$ can be obtained by the previous procedure, if we start with a suitable good basis of $R_{\mathfrak{p}}$.

Quasi-good bases. So far, given an order $R_{\mathfrak{p}}$, we must obtain a good basis of it to compute its suborders. This involves diagonalizing a ternary quadratic form over $\mathcal{O}_{\mathfrak{p}}$, which is not desirable from the computational viewpoint. Nevertheless, as we will show in this subsection, this can be reduced to diagonalize the corresponding form modulo $\mathfrak{p}^n$ for a certain small non-negative integer n.

Definition 2.13. Let $\mathcal{B}=\{1,e_1,e_2,e_3\}$ be a basis of $R_{\mathfrak{p}}$. We say that $\mathcal{B}$ is a *quasi-good* basis if there exists a good basis $\tilde{\mathcal{B}}=\{1,\tilde{e}_1,\tilde{e}_2,\tilde{e}_3\}$ of $R_{\mathfrak{p}}$ satisfying

$$\tilde{e}_i \equiv e_i \mod (\mathfrak{p}R_{\mathfrak{p}}) \quad (1\le i\le 3).$$

Proposition 2.14. *Let $\mathcal{B}=\{1,e_1,e_2,e_3\}$ be a quasi-good basis of an order $R_{\mathfrak{p}}$ in correspondence with a form f, and let g be a form beneath f. Let d_1,d_2,d_3 be as in Table 2.2. Then,*

$$R'_{\mathfrak{p}}=\langle 1,d_1,d_2,d_3\rangle_{\mathcal{O}_{\mathfrak{p}}}$$

is a maximal suborder of $R_{\mathfrak{p}}$ in correspondence with the form g.

Proof. Let $\tilde{\mathcal{B}}=\{1,\tilde{e}_1,\tilde{e}_2,\tilde{e}_3\}$ be a good basis of $R_{\mathfrak{p}}$ as in Definition 2.13. In terms of these elements and the form g, define elements $\tilde{d}_1,\tilde{d}_2,\tilde{d}_3$ according

to Table 2.2, and let $R'_{\mathfrak{p}} = \left\langle 1, \tilde{d}_1, \tilde{d}_2, \tilde{d}_3 \right\rangle_{\mathcal{O}_{\mathfrak{p}}}$. The table shows that $\tilde{d}_i \equiv d_i \mod (\mathfrak{p}R_{\mathfrak{p}})$ for every $1 \leq i \leq 3$. Then, since $\mathfrak{p}R_{\mathfrak{p}} \subseteq R'_{\mathfrak{p}}$, we have that

$$R'_{\mathfrak{p}} = R'_{\mathfrak{p}} + \mathfrak{p}R_{\mathfrak{p}} = \left\langle 1, \tilde{d}_1, \tilde{d}_2, \tilde{d}_3 \right\rangle_{\mathcal{O}_{\mathfrak{p}}} + \mathfrak{p}R_{\mathfrak{p}} \supseteq \langle 1, d_1, d_2, d_3 \rangle_{\mathcal{O}_{\mathfrak{p}}}.$$

Letting $\Lambda_{\mathfrak{p}}$ denote the lattice on the right-hand side of this equation, it suffices to see that $d(R'_{\mathfrak{p}}) = d(\Lambda_{\mathfrak{p}})$ to complete the proof.

Let $e \in \{1, 2\}$ be such that $[R_{\mathfrak{p}} : R'_{\mathfrak{p}}] = \mathfrak{p}^e$. Following Table 2.2 case by case, it can be proved that $d(\Lambda_{\mathfrak{p}}) = \mathfrak{p}^e d(R_{\mathfrak{p}})$. Since $d(R'_{\mathfrak{p}}) = \mathfrak{p}^e d(R_{\mathfrak{p}})$, we are done.

□

Remark 2.15. Let $m = v_{\mathfrak{p}}(d(R'_{\mathfrak{p}}))$. The proof shows that, when constructing the d_i's, the elements $\alpha_0, \alpha_1, \ldots$ in Table 2.2 need to be calculated only up to precision $\pi_{\mathfrak{p}}^{m+1}$, since in that case the ideal $d(\Lambda_{\mathfrak{p}})$ remains unchanged.

It shows also that $\{1, d_1, d_2, d_3\}$ needs not to be a quasi-good basis for $R'_{\mathfrak{p}}$, since we only get that $\tilde{d}_i \equiv d_i \mod (\mathfrak{p}R_{\mathfrak{p}})$. Nevertheless, since $\mathfrak{p}^2 R_{\mathfrak{p}} \subseteq \mathfrak{p}R'_{\mathfrak{p}}$, it is a quasi-good basis if the stronger congruence $\tilde{e}_i \equiv e_i \mod (\mathfrak{p}^2 R_{\mathfrak{p}})$ holds.

Proposition 2.14 shows that obtaining quasi-good bases is enough for our purpose of computing suborders. In what follows we show how to obtain these bases.

Let $f = \langle 1, a, b \rangle$ be the form in correspondence with $R_{\mathfrak{p}}$, and let $\mathcal{E} = \{f_0, f_1, f_2, f_3\}$ be a basis of $R_{\mathfrak{p}}^{\vee}$ satisfying (2.2). The existence of good bases implies that there exists $C \in GL_3(\mathcal{O}_{\mathfrak{p}})$ such that $2ab \cdot C^t M_{\mathcal{E}} C = \operatorname{diag}(1, a, b)$. Hence, $2ab \cdot M_{\mathcal{E}} \in M_3(\mathcal{O}_{\mathfrak{p}})$ and $\det(M_{\mathcal{E}}) = 8^{-1}(ab)^{-2}u^2$ for some $u \in \mathcal{O}_{\mathfrak{p}}^{\times}$.

Proposition 2.16. *Let $n = 2v_{\mathfrak{p}}(a)+1$. Assume that $\mathcal{E}$ satisfies the following conditions.*

(a) There exists $\tilde{b} \in \mathcal{O}_{\mathfrak{p}}$ such that

$$2ab \cdot M_{\mathcal{E}} \equiv \operatorname{diag}(1, a, \tilde{b}) \mod (M_3(\mathfrak{p}^n \mathcal{O}_{\mathfrak{p}})).$$

(b) $\det(M_{\mathcal{E}}) = 8^{-1}(ab)^{-2}u^2$.

Then, $\mathcal{E}^{\dagger}$ is a quasi-good basis of $R_{\mathfrak{p}}$.

Remark 2.17. The congruence in *(a)* is the really relevant hypothesis. If this congruence is satisfied and $u \in \mathcal{O}_{\mathfrak{p}}^{\times}$ is such that $\det(M_{\mathcal{E}}) = 8^{-1}(ab)^{-2}u^2$, then the basis $\{f_0, f_1, f_2, u^{-1}f_3\}$ satisfies *(a)* and also *(b)*.

The proof of Proposition 2.16 is based on the following lifting lemma.

Lemma 2.18. *Let r, m be non negative integers such that $m > 2r$, and let $A \in M_3(\mathcal{O}_{\mathfrak{p}})$ be a symmetric matrix. Suppose that there exists $C \in GL_3(\mathcal{O}_{\mathfrak{p}})$ such that*

$$C^t A C \equiv \operatorname{diag}(\alpha, \beta, \gamma) \mod (M_3(\mathfrak{p}^m \mathcal{O}_{\mathfrak{p}})),$$

with $v_{\mathfrak{p}}(\alpha) = 0$ and $v_{\mathfrak{p}}(\beta) = r$. Then, there exists $C' \in GL_3(\mathcal{O}_{\mathfrak{p}})$ satisfying $C' \equiv C \mod (M_3(\mathfrak{p}^{m-r}\mathcal{O}_{\mathfrak{p}}))$ such that

$$C'^t A C' \equiv \operatorname{diag}(\alpha', \beta', \gamma') \mod (M_3(\mathfrak{p}^{m+1}\mathcal{O}_{\mathfrak{p}})),$$

with $\alpha' \equiv \alpha \mod (\mathfrak{p}^{m-r}\mathcal{O}_{\mathfrak{p}})$ and $\beta' \equiv \beta \mod (\mathfrak{p}^m \mathcal{O}_{\mathfrak{p}})$.

Proof. Write

$$C^tAC = \mathrm{diag}(\alpha,\beta,\gamma) + \pi_{\mathfrak{p}}^m \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix},$$

with $a, b, \ldots, f \in \mathcal{O}_{\mathfrak{p}}$. We claim that there exists a matrix $C_0 \in GL_3(\mathcal{O}_{\mathfrak{p}})$ such that

$$C_0^tAC = \begin{pmatrix} \alpha + a\pi_{\mathfrak{p}}^m & 0 & c'\pi_{\mathfrak{p}}^m \\ -b\pi_{\mathfrak{p}}^r & \beta + d'\pi_{\mathfrak{p}}^m & e'\pi_{\mathfrak{p}}^m \\ -c\pi_{\mathfrak{p}}^r & -e\pi_{\mathfrak{p}}^r & \gamma + f'\pi_{\mathfrak{p}}^m \end{pmatrix},$$

with $c', d', e', f' \in \mathcal{O}_{\mathfrak{p}}$. This can be shown by performing row operations on C^tAC, using the diagonal entries as pivots to first obtain zeroes at the $(3,1),(2,1),(1,2)$ and $(3,2)$ entries, and then obtain $-c\pi_{\mathfrak{p}}^r, -e\pi_{\mathfrak{p}}^r$ and $-b\pi_{\mathfrak{p}}^r$ at the $(3,1),(3,2)$ and $(2,1)$ entries respectively.

Let $C' = C + \pi_{\mathfrak{p}}^{m-r}C_0$. Then,

$$C'^tAC' = \begin{pmatrix} \alpha' & 0 & c'\pi_{\mathfrak{p}}^{2m-r} \\ 0 & \beta' & e'\pi_{\mathfrak{p}}^{2m-r} \\ c'\pi_{\mathfrak{p}}^{2m-r} & e'\pi_{\mathfrak{p}}^{2m-r} & \gamma' \end{pmatrix} + \pi_{\mathfrak{p}}^{2(m-r)}C_0^tAC_0.$$

where $\alpha' = \alpha + a\pi_{\mathfrak{p}}^m + 2\pi_{\mathfrak{p}}^{m-r}(\alpha + a\pi_{\mathfrak{p}}^m)$ and $\beta' = \beta + d'\pi_{\mathfrak{p}}^m + 2\pi_{\mathfrak{p}}^{m-r}(\beta + d'\pi_{\mathfrak{p}}^m)$. Since $2(m-r) \geq m+1$, we are done. □

Proof of Proposition 2.16. Let $r = v_{\mathfrak{p}}(a)$. By letting $m \to \infty$ in the previous lemma, we get a matrix $C = (c_{ij}) \in GL_3(\mathcal{O}_{\mathfrak{p}})$ satisfying $C \equiv I \mod (M_3(\mathfrak{p}^{2r+1}\mathcal{O}_{\mathfrak{p}}))$ such that

$$2ab \cdot C^tM_{\mathcal{E}}C = \mathrm{diag}(\alpha,\beta,\gamma),$$

with $\alpha \equiv 1 \mod (\pi_{\mathfrak{p}}^{r+1})$ and $\beta \equiv a \mod (\pi_{\mathfrak{p}}^{2r+1})$. Using Hensel's lemma, take $x_1, x_2 \in \mathcal{O}_{\mathfrak{p}}^{\times}$ satisfying $x_i \equiv 1 \mod (\pi_{\mathfrak{p}}^{r+1})$ such that $\alpha = x_1^2$ and $\beta = x_2^2a$. Taking determinants we see that $\gamma = x_3^2b$, where $x_3 = \frac{\det(C)}{x_1x_2}$.

Now let $\tilde{C} = C \cdot \mathrm{diag}(x_1,x_2,x_3)^{-1}$. Then $\tilde{C}$ satisfies that

$$2ab \cdot \tilde{C}^tM_{\mathcal{E}}\tilde{C} = \mathrm{diag}(1,a,b).$$

Let $\tilde{f}_i = \sum_{j=1}^3 \tilde{c}_{ji}f_j$, where $\tilde{C} = (\tilde{c}_{ij})$, let $\tilde{f}_0 = f_0$, and let $\tilde{\mathcal{E}} = \{\tilde{f}_0, \tilde{f}_1, \tilde{f}_2, \tilde{f}_3\}$. Then $\tilde{\mathcal{E}}^{\dagger}$ is a good basis of $R_{\mathfrak{p}}$, for (2.9) is verified by $M_{\tilde{\mathcal{E}}}$. The congruences satisfied by the x_i's and C imply that $\tilde{f}_i \equiv f_i \mod (\mathfrak{p}R_{\mathfrak{p}}^{\vee})$ for $1 \leq i \leq 3$. Hence $\mathcal{E}^{\dagger}$ is a quasi-good basis of $R_{\mathfrak{p}}$, since Proposition 3.2 of [Brz82] gives that $4ab \cdot R_{\mathfrak{p}}^{\vee}R_{\mathfrak{p}}^{\vee} \subseteq R_{\mathfrak{p}}$.

□

From local to global. Let Λ be a lattice in B, and let $\Lambda'_{\mathfrak{p}} \subseteq \Lambda_{\mathfrak{p}}$ be a sublattice of index $\mathfrak{p}^e$, where e is a non-negative integer. Let $\Lambda' \subseteq B$ be the lattice given by

$$\Lambda'_{\mathfrak{q}} = \begin{cases} \Lambda_{\mathfrak{q}} & \text{if } \mathfrak{q} \neq \mathfrak{p}, \\ \Lambda'_{\mathfrak{p}} & \text{if } \mathfrak{q} = \mathfrak{p}. \end{cases}$$

Given a set of generators for Λ as an $\mathcal{O}$-module and a set of generators for $\Lambda'_{\mathfrak{p}}$ as an $\mathcal{O}_{\mathfrak{p}}$-module, how can we construct a set of generators for Λ' as an $\mathcal{O}$-module?

Assume that $\Lambda = \langle v_1, v_2, \dots, v_m \rangle_{\mathcal{O}}$ and that $\Lambda'_{\mathfrak{p}} = \langle w_1, w_2, \dots, w_n \rangle_{\mathcal{O}_{\mathfrak{p}}}$. For each i write $w_i = \sum_j a_{ij} v_j$, with $a_{ij} \in \mathcal{O}_{\mathfrak{p}}$. There exist elements $b_{ij} \in \mathcal{O}$ and $c_{ij} \in \pi_{\mathfrak{p}}^e \mathcal{O}_{\mathfrak{p}}$ such that $a_{ij} = b_{ij} + c_{ij}$ (they can be constructed, for example, looking at the $\mathfrak{p}$-adic expansion of the a_{ij}). Consider the vectors $\tilde{w}_i = \sum_j b_{ij} v_j$ (which belong to Λ). Then we have

Proposition 2.19.

$$\Lambda' = \mathfrak{p}^e \Lambda + \langle \tilde{w}_1, \tilde{w}_2, \dots, \tilde{w}_n \rangle_{\mathcal{O}}.$$

Proof. It is enough to check that these two lattices coincide at all localizations. Denote by Λ'' the lattice in the right hand side.

- If $\mathfrak{q} \neq \mathfrak{p}$, then $\pi_{\mathfrak{p}}$ is a unit in $\mathcal{O}_{\mathfrak{q}}$. So $\mathfrak{p}^e \Lambda_{\mathfrak{q}} = \Lambda_{\mathfrak{q}}$, which implies that $\Lambda''_{\mathfrak{q}} = \Lambda_{\mathfrak{q}} + \langle \tilde{w}_1, \tilde{w}_2, \dots, \tilde{w}_n \rangle_{\mathcal{O}_{\mathfrak{q}}} = \Lambda_{\mathfrak{q}}$.
- Since $\mathfrak{p}^e \Lambda_{\mathfrak{p}} \subseteq \Lambda'_{\mathfrak{p}}$, we have that $\Lambda''_{\mathfrak{p}} \subseteq \Lambda_{\mathfrak{p}}$; the reverse inclusion is deduced from the fact that $\tilde{w}_i \equiv w_i \mod (\mathfrak{p}^e \Lambda_{\mathfrak{p}})$.

□

Remark 2.20. Using the Hermite Normal Form algorithm (see [Coh00], Chapter I), for every lattice in B we can compute a generating set over $\mathcal{O}$ with at most five elements. In particular, this can be done for the sum describing Λ', and we can assume that Λ is given in this way.

The algorithm. We are now ready to prove our first main result, which we recall here.

Theorem A. *There is an algorithm that, given a Bass order R in B, computes suborders of R of any given genus.*

Proof. It suffices to give an algorithm which computes maximal suborders of R in any given genus. So we assume that we are given a prime $\mathfrak{p}$, the form $f_{\mathfrak{p}}$ corresponding to $R_{\mathfrak{p}}$, and a form $g_{\mathfrak{p}}$ beneath $f_{\mathfrak{p}}$. The algorithm, which we describe below, will return a Bass order $R' \subseteq R$ with $R'_{\mathfrak{q}} = R_{\mathfrak{q}}$ for all $\mathfrak{q} \neq \mathfrak{p}$, and such that $R'_{\mathfrak{p}}$ corresponds to $g_{\mathfrak{p}}$.

Algorithm 2.21.

Step 1. Use Proposition 2.16 to find a quasi-good basis for $R_{\mathfrak{p}}$.

Step 2. Use Proposition 2.14 to construct a suborder $R'_{\mathfrak{p}} \subseteq R_{\mathfrak{p}}$ corresponding to the form $g_{\mathfrak{p}}$.

Step 3. Use Proposition 2.19 to construct an order R' such that

$$R'_{\mathfrak{q}} = \begin{cases} R_{\mathfrak{q}} & \text{if } \mathfrak{q} \neq \mathfrak{p}, \\ R'_{\mathfrak{p}} & \text{if } \mathfrak{q} = \mathfrak{p}. \end{cases}$$

□

3. Computing ideal classes representatives for suborders

The aim of this section is to prove Theorem B. We start with some notation and definitions.

If R is an order in B, we denote by $I(R)$ the set of left R-ideals and by $Cl(R)$ the set of equivalence classes of left R-ideals. The equivalence class

of an ideal I is denoted by $[I]$. The *norm* of an ideal I is defined as the fractional ideal $N(I) \subseteq K$ generated by the elements $N(x)$ as x runs over I.

Throughout this section, let $R' \subseteq R$ be orders in B.

Definition 3.1. If $I \in I(R)$, we define

$$\Psi_{R'}^{R}(I) = \{J \in I(R') : RJ = I\},$$

and we denote that set simply by $\Psi(I)$ when there is no possible confusion on which are the orders under consideration.

These sets will be considered for orders in B as well as for their completions. Both cases can and will be treated in an unified way.

Remark 3.2. When considering orders in B, identifying ideals with ideles, the set $\Psi(I)$ is simply the preimage of I under the natural map

$$\widehat{R'}^{\times} \backslash \widehat{B}^{\times} \longrightarrow \widehat{R}^{\times} \backslash \widehat{B}^{\times},$$

where $\widehat{\ }$ denotes tensor with $\widehat{\mathbb{Z}}$ over $\mathbb{Z}$.

Remark 3.3. The sets $\Psi(I)$ were studied in [PRV05] to construct modular forms of weight 2 and level p^2 considering an order of discriminant p^2, in the quaternion algebra over $\mathbb{Q}$ ramified at p and at ∞ - compare Corollary 3.17 below and equation (1) in [PRV05]. They were later used in [PT07] to construct modular forms of weight $3/2$ and level p^2 considering in that algebra an order of class C at p.

By $[\Psi(I)]$ we denote the set of classes of elements of $\Psi(I)$, i.e.

$$[\Psi(I)] = \{[J] : J \in \Psi(I)\}.$$

Note that if $[I_1] = [I_2]$, then $[\Psi(I_1)] = [\Psi(I_2)]$.

Proposition 3.4.

$$Cl(R') = \coprod_{[I] \in Cl(R)} [\Psi(I)].$$

Proof. This is straightforward using the idelic description of $\Psi(I)$, but we give a direct proof.

Let $J \in I(R')$. Take $I = RJ$. Then it is clear that $I \in I(R)$ and $J \in \Psi(I)$. This shows that the union on the right hand side gives all of $Cl(R')$.

It is clear that the union is disjoint, since if there are $J_i \in \Psi_{R'}^{R}(I_i)$ for $i = 1, 2$ such that $[J_1] = [J_2]$, then $[I_1] = [I_2]$. Indeed, let $x \in B^{\times}$ be such that $J_1 = J_2 x$. Then,

$$I_1 = RJ_1 = RJ_2 x = I_2 x.$$

□

This proposition shows that the sets $\Psi(I)$ can be used to give a system of representatives for $Cl(R')$, in terms of a system of representatives for $Cl(R)$. The next proposition shows that by constructing representatives for $Cl(R')$ using these sets, we will not enlarge the norms of the R-ideals that we start with.

Proposition 3.5. *Let $J \in I(R')$ such that $J \subseteq I$. Then, $J \in \Psi(I)$ if and only if $N(I) = N(J)$.*

Proof. Let $\mathfrak{q}$ be a prime of $\mathcal{O}$. Since $J_\mathfrak{q} \subseteq I_\mathfrak{q}$ we can write $I_\mathfrak{q} = R_\mathfrak{q} x_\mathfrak{q}$ and $J_\mathfrak{q} = R'_\mathfrak{q} z_\mathfrak{q} x_\mathfrak{q}$, with $z_\mathfrak{q} \in R_\mathfrak{q}$. Then, $N(I_\mathfrak{q}) = N(J_\mathfrak{q})$ if and only if $z_\mathfrak{q} \in R_\mathfrak{q}^\times$, which is equivalent to the equality $R_\mathfrak{q} J_\mathfrak{q} = I_\mathfrak{q}$. These local facts imply the global statement. □

We have an action of the group $R_r(I)^\times$ on $\Psi(I)$ by right multiplication, which stabilizes the left R'-ideal classes.

Proposition 3.6. *If $J \in \Psi(I)$, then the action of $R_r(I)^\times$ on $[J] \cap \Psi(I)$ is transitive and the stabilizer of J is $R_r(J)^\times$. In particular, $\#\big([J] \cap \Psi(I)\big) = [R_r(I)^\times : R_r(J)^\times]$.*

Proof. To prove that the action is transitive, let $J_1, J_2 \in \Psi(I)$ be such that $[J_1] = [J_2]$. If $x \in B^\times$ is such that $J_1 = J_2 x$, then $x \in R_r(I)^\times$, since $I = RJ_1 = RJ_2 x = Ix$. The other two statements are clear. □

The corollary below, which follows immediately, can be used to get information about the class numbers, as we will see in Section 4.

Corollary 3.7.

$$\#\Psi(I) = \sum_{[J] \in [\Psi(I)]} [R_r(I)^\times : R_r(J)^\times].$$

In what follows, we describe two different methods for calculating the set $\Psi(I)$ for a given $I \in I(R)$. The first one will rely on the action of the units described above, in the local setting, whereas the second one will only involve global calculations.

Local method: The action by $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$.

Proposition 3.8. *Let $I_\mathfrak{p} \in I(R_\mathfrak{p})$, say $I_\mathfrak{p} = R_\mathfrak{p} x_\mathfrak{p}$. Then, the map*

$$\begin{aligned} (R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times &\longrightarrow \Psi(I_\mathfrak{p}) \\ \alpha_\mathfrak{p} &\mapsto R'_\mathfrak{p}(\alpha_\mathfrak{p} x_\mathfrak{p}) \end{aligned}$$

is bijective.

Proof. This map is the composition of the maps

$$\begin{aligned} (R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times &\longrightarrow \Psi(R_\mathfrak{p}), & \Psi(R_\mathfrak{p}) &\longrightarrow \Psi(I_\mathfrak{p}). \\ \alpha_\mathfrak{p} &\mapsto R'_\mathfrak{p}\alpha_\mathfrak{p} & J_\mathfrak{p} &\mapsto J_\mathfrak{p} x_\mathfrak{p} \end{aligned}$$

Both maps are bijective. This is clear for the second map, and for the first one this follows by Lemma 3.6, since all $R_\mathfrak{p}$-ideals are equivalent.

□

Proposition 3.9. *Suppose that $[R : R'] = \mathfrak{p}^e$ for some $e \geq 1$. Let $I \in I(R)$. The map*

$$\begin{aligned} \Psi^R_{R'}(I) &\longrightarrow \Psi^{R_\mathfrak{p}}_{R'_\mathfrak{p}}(I_\mathfrak{p}) \\ J &\mapsto J_\mathfrak{p} \end{aligned}$$

is bijective. In particular, $\#\Psi^R_{R'}(I) = [R_\mathfrak{p}^\times : (R'_\mathfrak{p})^\times]$.

Proof. The fact that $I_\mathfrak{q} = J_\mathfrak{q}$ for all $\mathfrak{q} \neq \mathfrak{p}$ implies that the map is bijective. The equality follows from Corollary 3.8. □

These propositions imply immediately the following result.

Corollary 3.10. *Suppose that* $[R : R'] = \mathfrak{p}^e$ *for some* $e \geq 1$. *Let* $I \in I(R)$, *and write* $I_\mathfrak{p} = R_\mathfrak{p} x_\mathfrak{p}$. *If* $\{\alpha_j\}$ *is a system of representatives for* $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$, *then* $\Psi_{R'}^R(I) = \{J_j\}$, *where* J_j *is locally given by*

$$(J_j)_\mathfrak{q} = \begin{cases} I_\mathfrak{q} & \text{if } \mathfrak{q} \neq \mathfrak{p}, \\ R'_\mathfrak{p}(\alpha_j x_\mathfrak{p}) & \text{if } \mathfrak{q} = \mathfrak{p}. \end{cases}$$

Remark 3.11. A way to construct a local generator at $\mathfrak{p}$ of an ideal I is to consider the entry with minimum valuation at $\mathfrak{p}$ of the Gram matrix of a generating set $\{w_1, \ldots, w_5\}$ for I over $\mathcal{O}$, since the norm is generated by an element with minimum valuation in such matrix. If this minimum is attached in the entry (i, j), then a local generator is $w_i + w_j$ if $i \neq j$, and w_i if $i = j$.

Proposition 3.12. *Assume that* $\mathfrak{p}R_\mathfrak{p} \subseteq R'_\mathfrak{p}$. *Then, the natural map*

$$\phi : (R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times \longrightarrow (\mathfrak{p}R_\mathfrak{p} \backslash R'_\mathfrak{p})^\times \backslash (\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p})^\times.$$

is bijective.

Proof. Consider the ring morphism $\phi_1 : R_\mathfrak{p} \to \mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p}$. We claim that the induced group homomorphism $\phi_1 : R_\mathfrak{p}^\times \to (\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p})^\times$ is surjective. Indeed, let $[x] \in (\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p})^\times$. Then there exist $y, z \in R_\mathfrak{p}$ such that $xy = 1 + \pi_\mathfrak{p} z$. Then $N(xy) \equiv 1 \mod (\pi_\mathfrak{p})$, and hence $x \in R_\mathfrak{p}^\times$ as claimed.

Compose ϕ_1 with the map p that projects $(\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p})^\times$ onto the quotient set $(\mathfrak{p}R_\mathfrak{p} \backslash R'_\mathfrak{p})^\times \backslash (\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p})^\times$. Then $p \circ \phi_1$ is surjective, and passes to the quotient set $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$ to give a surjective map $\phi : (R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times \to (\mathfrak{p}R_\mathfrak{p} \backslash R'_\mathfrak{p})^\times \backslash (\mathfrak{p}R_\mathfrak{p} \backslash R_\mathfrak{p})^\times$.

We claim that ϕ is injective. Indeed, let $x, y \in R_\mathfrak{p}^\times$ be such that $\phi(x) = \phi(y)$. Then, since $(R'_\mathfrak{p})^\times \to (\mathfrak{p}R_\mathfrak{p} \backslash R'_\mathfrak{p})^\times$ is also an epimorphism, we have $z \in (R'_\mathfrak{p})^\times$ and $w \in R_\mathfrak{p}$ such that $x = zy + \pi_\mathfrak{p} w$. Hence, $x = (z + \pi_\mathfrak{p} w y^{-1})y$, which shows that $[x] = [y] \in (R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$, since $\pi_\mathfrak{p} w y^{-1} \in \mathfrak{p}R_\mathfrak{p} \subseteq R'_\mathfrak{p}$ and hence $z + \pi_\mathfrak{p} w y^{-1} \in (R'_\mathfrak{p})^\times$. □

By Proposition 2.1, this result shows that, to give a system of representatives for the sets $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$ when $R'_\mathfrak{p}$ is a maximal suborder of $R_\mathfrak{p}$, it will be enough to do the calculations modulo $\mathfrak{p}$.

Given a quasi-good basis $\mathcal{B} = \{1, e_1, e_2, e_3\}$ of $R_\mathfrak{p}$, and assuming that $R'_\mathfrak{p}$ is obtained from $R_\mathfrak{p}$ by means of Algorithm 2.21, we proceed to give a system of representatives for the sets $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$, in terms of the form g corresponding with $R'_\mathfrak{p}$. The indexes $[R_\mathfrak{p}^\times : (R'_\mathfrak{p})^\times]$ are known (see [Brz90], Theorems 3.3 and 3.10), so it will suffice to give in each case the right amount of non-equivalent units.

Let q denote the order of the residue field $k_\mathfrak{p}$, and let $\{a_1, a_2, \ldots, a_q\} \subseteq \mathcal{O}_\mathfrak{p}$ be a set of representatives for $k_\mathfrak{p}$ such that $a_1 = 1, a_2 = -1$ and $a_q = 0$. Let δ, β_0, β_1 be as in Proposition 2.11. Finally, let $S = \{\tilde{\gamma} \in k_\mathfrak{p} \times k_\mathfrak{p} : 1 - \delta\tilde{\gamma}_1^2 + \tilde{\gamma}_2^2 \neq 0\}$, and each $\tilde{\gamma} \in S$ take $\gamma \in \mathcal{O}_\mathfrak{p} \times \mathcal{O}_\mathfrak{p}$ any lift of $\tilde{\gamma}$.

Proposition 3.13. *With the previous notation, Table 3.1 gives a system of representatives for* $(R'_\mathfrak{p})^\times \backslash R_\mathfrak{p}^\times$.

$R_\mathfrak{p}$-class	$R'_\mathfrak{p}$-class	$[R_\mathfrak{p}^\times : (R'_\mathfrak{p})^\times]$	Representatives	Condition
A1	A1	$q+1$	$e_1, 1+\frac{a_i}{2}(e_1-e_2) \quad (1\le i\le q)$	$d(R_\mathfrak{p})=1$
		q	$1+\frac{a_i}{2}(e_1-e_2) \quad (1\le i\le q)$	$d(R_\mathfrak{p})\neq 1$
	A2	$q(q-1)$	$e_2, 1+\gamma_1(\beta_1 e_3-\beta_0 e_1)+\gamma_2 e_2 \quad (\tilde{\gamma}\in S)$	
	B	$q-1$	$1, a_i+e_3 \quad (3\le i\le q)$	
A2	A2	q^2	$1+a_i e_1+a_j e_2 \quad (1\le i,j\le q)$	
	B	$q+1$	$1, a_i+e_3 \quad (1\le i\le q)$	
B	C	q	$1, a_i+e_2 \quad (1\le i\le q-1)$	$g\neq\langle 1,\delta\pi_\mathfrak{p},\delta\pi_\mathfrak{p}^2\rangle$
			$1, a_i+e_3 \quad (1\le i\le q-1)$	$g=\langle 1,\delta\pi_\mathfrak{p},\delta\pi_\mathfrak{p}^2\rangle$
C	C	q	$1, a_i+e_2 \quad (1\le i\le q-1)$	

TABLE 3.1. Representatives for $(R'_\mathfrak{p})^\times\backslash R_\mathfrak{p}^\times$

Proof. According to the Proposition 3.12 we may assume that $\mathcal{B}$ is a good basis, and it suffices to calculate a system of representatives for the set $(\mathfrak{p}R_\mathfrak{p}\backslash R'_\mathfrak{p})^\times\backslash(\mathfrak{p}R_\mathfrak{p}\backslash R_\mathfrak{p})^\times$.

First notice that $\mathfrak{p}R_\mathfrak{p}\backslash R_\mathfrak{p}$ is a $k_\mathfrak{p}$-algebra that inherits naturally from $B_\mathfrak{p}$ a norm form $N : \mathfrak{p}R_\mathfrak{p}\backslash R_\mathfrak{p} \to k_\mathfrak{p}$ such that $(\mathfrak{p}R_\mathfrak{p}\backslash R_\mathfrak{p})^\times = \{x \in \mathfrak{p}R_\mathfrak{p}\backslash R_\mathfrak{p} : N(x)\neq 0\}$. This allows us to easily check that all the given representatives are indeed units, and also to give the needed description of $(\mathfrak{p}R_\mathfrak{p}\backslash R'_\mathfrak{p})^\times$.

We will do the details in a single case, namely when $R_\mathfrak{p}$ has class A1 and $R'_\mathfrak{p}$ has class B. The rest of the cases can be treated similarly.

Let $x = x_0 + x_1e_1 + x_2e_2 + x_3e_3 \in \mathfrak{p}R_\mathfrak{p}\backslash R_\mathfrak{p}$. In these coordinates we have that the norm form is given by $N(x) = x_0^2 - x_3^2$ (see (2.6)), and that $x \in \mathfrak{p}R_\mathfrak{p}\backslash R'_\mathfrak{p}$ if and only if $x_3 = 0$.

Hence, the elements of the form $a_i + e_3$ belong to $(\mathfrak{p}R_\mathfrak{p}\backslash R_\mathfrak{p})^\times$, if $i \ge 3$. They are not equivalent modulo $(\mathfrak{p}R_\mathfrak{p}\backslash R'_\mathfrak{p})^\times$, since if

$$\begin{aligned}(a_i+e_3)(x_0+x_1e_1+x_2e_2) &= \\ &= a_ix_0 + (a_ix_1+x_2)e_1 + (a_ix_2+x_1)e_2 + x_0e_3 = a_j + e_3,\end{aligned}$$

then $x_0 = 1$ and hence $i = j$. And they are not equivalent to 1, since they do not belong to $\mathfrak{p}R_\mathfrak{p}\backslash R'_\mathfrak{p}$. □

Global method: The colon lattice. Let $I \in I(R)$. We introduce an alternative method to calculate $\Psi(I)$, using global tools. Consider the lattice

$$\Lambda_I = \{y \in B : yI^{-1} \subseteq R'\}.$$

It satisfies that $\Lambda_I = \Lambda_R I$. For simplicity, we will just consider $\Lambda = \Lambda_R$. It is clear that $\Lambda \subseteq R'$ and $R \subseteq R_r(\Lambda)$.

Lemma 3.14. *The lattice Λ satisfies the following properties:*

(a) $\mathfrak{p}R \subseteq \Lambda$, and hence $[R:\Lambda] \mid \mathfrak{p}^4$.
(b) $\Lambda \subseteq J$ for all $J \in \Psi(R)$.

Proof. The inclusion in *(a)* follows from the fact that $\mathfrak{p}R' \subseteq R$. The inclusion in *(b)* is clear if we consider the completion at primes $\mathfrak{q} \neq \mathfrak{p}$, so we will look only at the completion at $\mathfrak{p}$. Let $J \in \Psi(R)$, and write $J_\mathfrak{p} = R'_\mathfrak{p}u_\mathfrak{p}$ with $u_\mathfrak{p} \in R_\mathfrak{p}^\times$. Then,

$$\alpha_\mathfrak{p} \in \Lambda_\mathfrak{p} \Rightarrow \alpha_\mathfrak{p}R_\mathfrak{p} \subseteq R'_\mathfrak{p} \Rightarrow \alpha_\mathfrak{p}u_\mathfrak{p}^{-1} \in R'_\mathfrak{p} \Rightarrow \alpha_\mathfrak{p} \in R'_\mathfrak{p}u_\mathfrak{p} = J_\mathfrak{p}.$$

□

Since $\mathfrak{p}R_\mathfrak{p} \subseteq R'_\mathfrak{p}$, we can consider $R_\mathfrak{p}/R'_\mathfrak{p}$ as a $k_\mathfrak{p}$-vector space. When $e = 2$, we can go further. Since in that case $R'_\mathfrak{p}$ has class A2, the ring $\mathcal{O}_\mathfrak{p} + \sqrt{\delta}\mathcal{O}_\mathfrak{p}$ embeds into $R'_\mathfrak{p}$, and hence into $R_\mathfrak{p}$. Then we can consider $R_\mathfrak{p}/R'_\mathfrak{p}$ as a $\mathbb{K}_\mathfrak{p}$-vector space, where $\mathbb{K}_\mathfrak{p}$ is the quadratic extension of $k_\mathfrak{p}$ given by $\mathbb{K}_\mathfrak{p} = (\mathcal{O}_\mathfrak{p} + \sqrt{\delta}\mathcal{O}_\mathfrak{p})/\mathfrak{p}(\mathcal{O}_\mathfrak{p} + \sqrt{\delta}\mathcal{O}_\mathfrak{p})$.

Lemma 3.15.

(a) If $e = 1$, then $\dim_{k_\mathfrak{p}}(R_\mathfrak{p}/R'_\mathfrak{p}) = 1$.
(b) If $e = 2$, then $\dim_{\mathbb{K}_\mathfrak{p}}(R_\mathfrak{p}/R'_\mathfrak{p}) = 1$.

Proof. It follows immediately from the fact that $|R_\mathfrak{p}/R'_\mathfrak{p}| = q^e$. □

Proposition 3.16. *$[R' : \Lambda] = \mathfrak{p}^e$, and hence $[R : \Lambda] = \mathfrak{p}^{2e}$. In particular, if $e = 2$ then $\Lambda = \mathfrak{p}R$.*

Proof. It is enough to consider the completion at $\mathfrak{p}$. Then, we need to show that $|R'_\mathfrak{p}/\Lambda_\mathfrak{p}| = q^e$. Consider the morphism (of additive groups)

$$\psi : R'_\mathfrak{p} \to \mathrm{End}(R_\mathfrak{p}/R'_\mathfrak{p})$$
$$\alpha \mapsto (v \mapsto \alpha \cdot v).$$

Its kernel is $\Lambda_\mathfrak{p}$. The induced morphism $\psi : R'_\mathfrak{p}/\Lambda_\mathfrak{p} \to \mathrm{End}(R_\mathfrak{p}/R'_\mathfrak{p})$ is easily seen to be also a $k_\mathfrak{p}$-vector space (respectively $\mathbb{K}_\mathfrak{p}$-vector space) morphism when $e = 1$ (respectively $e = 2$). Note that since $1 \notin \Lambda_\mathfrak{p}$, it is not the null morphism. Hence, the result follows from the previous lemma. □

Corollary 3.17. *The set $\Psi(I)$ is given by*

$$\Psi(I) = \{J : RJ = I,\ R_l(J) = R',\ \Lambda_I \subseteq J \subseteq I,\ [I : J] = [J : \Lambda_I] = \mathfrak{p}^e\}.$$

Proof. When $I = R$, the result follows immediately from Lemma 3.14 and Proposition 3.16. The arguments used for the general case are entirely analogous. □

In particular, to calculate $\Psi(I)$ (whose cardinality we already know by Proposition 3.9), we can limit ourselves to calculate the lattices between Λ_I and I with the indicated indexes, and then determine which of them satisfy the first two equalities. Furthermore, the equality $R_l(J) = R'$ can be replaced by the equality $N(J) = N(I)$, which sometimes is easier to verify.

Remark 3.18. If $e = 1$, then $[I : \Lambda_I] = \mathfrak{p}^2$, and there are $q + 1$ lattices between these two. We have seen that the number of elements of $\Psi(I)$ is $q - 1$, q or $q + 1$. Hence, almost all lattices constructed are needed. This makes the method effective.

Remark 3.19. In the case $e = 2$, we know that the elements in $\Psi(I)$ have a $(\mathcal{O}_\mathfrak{p} + \sqrt{\delta}\mathcal{O}_\mathfrak{p})$-module structure. If we only consider lattices between Λ_I and I which have this extra structure, there are $q^2 + 1$ such lattices. The order of $\Psi(I)$ is $q^2 - q$ if R is the maximal order and R' is of class A2, and q^2 if both orders are of class A2. Hence, except for the maximal order, this construction is effective as well.

The algorithm. We now prove our second main result, which we first recall.

Theorem B. *There is an algorithm that, given a Bass order R in B and a set of representatives S of left R-ideal classes, computes left ideal classes representatives for suborders of R of any given genus. Furthermore, the set of norms of the computed ideals is the same as the set of norms of the ideals in S.*

Proof. It suffices to give an algorithm that works when considering maximal suborders of R. In particular, we assume that we are given the same input as in Algorithm 2.21, plus the set S. The algorithm will return a set S' of representatives for left ideal classes representatives for the suborder R' obtained by Algorithm 2.21.

By Proposition 3.4, it suffices to give an algorithm which calculates, for each $I \in S$, a set of representatives S'_I for $[\Psi(I)]$, and then return $S' = \bigcup_{I\in S} S'_I$. The algorithm works as follows.

Algorithm 3.20.

Step 1. Using Proposition 3.13, compute a set of representatives for the set $(R'_{\mathfrak{p}})^\times \backslash R_{\mathfrak{p}}^\times$.

Step 2. Using Remark 3.11, find a local generator for $I_{\mathfrak{p}}$.

Step 3. Using Corollary 3.10 and Proposition 2.19, compute the set $\Psi(I)$.

Step 4. Set $T = \Psi(I)$ and set $S'_I = \emptyset$

Step 4.1. Pick $J \in T$ and compute $[J] \cap \Psi(I)$ by letting $R_r(J)^\times \backslash R_r(I)^\times$ act on J (see Proposition 3.6).

Step 4.2. Set $S'_I = S'_I \cup \{J\}$. If $T\backslash[J] = \emptyset$, return S'_I. Elseif, let $T = T\backslash[J]$, and go to Step 4.1.

□

Remark 3.21. We can replace Steps 1, 2 and 3 by the global method to compute $\Psi(I)$ given in Corollary 3.17, although to our knowledge there is no advantage of one over the other.

We do not have a general method to, given $J \in \Psi(I)$, compute a system of representatives for the (finite) set $R_r(J)^\times \backslash R_r(I)^\times$ needed in Step 4.1. However, if B is totally definite (i.e., if K is totally real and B ramifies at every infinite place of K), then the set $\mathcal{O}^\times \backslash R_r(I)^\times$ is finite and can be used as well to compute $[J] \cap \Psi(I)$.

The finiteness of the set $\mathcal{O}^\times \backslash R_r(I)^\times$, as well as a method to compute it, can be obtained considering the exact sequence

$$1 \longrightarrow \{\pm 1\} \backslash R_r(I)^{\times,1} \longrightarrow \mathcal{O}^\times \backslash R_r(I)^\times \xrightarrow{N} (\mathcal{O}^\times)^2 \backslash \mathcal{O}_+^\times, \tag{3.22}$$

where $\mathcal{O}_+^\times$ denotes the group of totally positive units of $\mathcal{O}$. Assuming B totally definite, the quadratic form $\mathrm{Tr}_{K/\mathbb{Q}} \circ N : B \to \mathbb{Q}$ is positive definite, and hence the group $R_r(I)^{\times,1}$ is finite and can be calculated using LLL. Furthermore, its possible group structures are known (see [Vig76]). The group $(\mathcal{O}^\times)^2 \backslash \mathcal{O}_+^\times$ is always finite, and equals the null group in many cases, such as for fields K having narrow class number equal to 1 (see [EMP86]).

Remark 3.23. Since $R_r(J)^\times \subseteq R_r(I)^\times$ for every $J \in \Psi(I)$, when iterating the algorithm we need to apply the previous procedure to compute the sets $\mathcal{O}^\times \backslash R_r(I)^\times$ only for the initial set of ideals.

4. Example: The Consani-Scholten quintic

In this section we are going to show how we can use our method to compute ideal classes representatives for an Eichler order of discriminant 30 in the quaternion algebra ramified at the two infinite places of the real quadratic field $K = \mathbb{Q}[\sqrt{5}]$.

This example was considered in [CS01] to conjecture the modularity of a Galois representation attached to the third étale cohomology of a quintic threefold (see [CS01], Theorem 1 for details). In that article the algebra considered is ramified also at 2 and 3, since the Galois representation associated to the quintic has semi-stable reduction at those places. The representatives are constructed following the method of Pizer (see [Piz80]), which implies seeking for ideals and checking for equivalence between the constructed ones until the class number (which has to be precomputed or can be deduced during the computation using the Mass formula) is reached. We consider instead the quaternion algebra ramified only at the two infinite places, since in that case the maximal order has class number equal to 1, which makes calculations simpler. We make use first of Theorem A to compute an Eichler order of discriminant 30 and then we make use of Theorem B to compute its left ideal class representatives. Most of the computations were made with the aid of `SAGE` ([Sa11]).

Denote by $\omega = \frac{1+\sqrt{5}}{2}$ and let $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega$ be the ring of integers of K. Let B be the quaternion algebra $(-1,-1)_K$, i.e., the algebra over K generated by $1, i, j, k$, where $i^2 = j^2 = -1, ij = k = -ji$. It is clearly unramified at all finite places not dividing 2, and it is ramified at the two infinite places. Since 2 is inert in the extension $K/\mathbb{Q}$, B does not ramify at 2 (by parity reasons).

4.1. **Constructing the orders.** Starting with a maximal order in B as input, we compute an Eichler order in B of discriminant 30. Considering the prime factorization of 30 in $\mathcal{O}$, we iterate Algorithm 2.21 to construct a chain

$$R(1) \supseteq R(2) \supseteq R(3) \supseteq R(6) \supseteq R(6\sqrt{5}) \supseteq R(30),$$

where $R(\mathfrak{N})$ denotes an order of discriminant $\mathfrak{N}$.

The maximal order we use is the order given in Chapter V of [Vig80], namely

$$R(1) = \left\langle \frac{1+\omega^{-1}i+\omega j}{2}, \frac{\omega^{-1}i+j+\omega k}{2}, \frac{\omega i+\omega^{-1}j+k}{2}, \frac{i+\omega j+\omega^{-1}k}{2} \right\rangle_{\mathcal{O}}.$$

4.1.1. *Discriminant 2.* In this first step we use Algorithm 2.21 referring to the Appendix.

Step 1. The order $R(1)_2$ is in correspondence with the form $f = H \perp \langle 1 \rangle$. Using the basis for $R(1)$ given above, we get that

$$\mathcal{B} = \left\{1, \tfrac{1}{2}(1+\omega^{-1}i+\omega j), \tfrac{1}{2}(\omega i+\omega^{-1}j+k), \tfrac{1}{2}(i+\omega j+\omega^{-1}k)\right\}$$

is a basis for $R(1)_2$. Its dual basis is

$$\mathcal{B}^\vee = \{f_0, \omega i - (1+\omega)k, \tfrac{1}{2}\big((1+\omega)i - j - \omega k\big), \\ \tfrac{1}{2}\big(-(1+2\omega)i + \omega j + (1+3\omega)k\big)\},$$

where $f_0 = \frac{1}{2}(1 - \omega i + (1+\omega)k)$. Diagonalizing $M_{\mathcal{B}^\vee}$ (as a ternary quadratic form), we see that letting

$$f_1 = \tfrac{1}{5}\big((2+\omega)i - j - (1+\omega)k\big),$$
$$f_2 = \tfrac{1}{2}\big((1+\omega)i - j + (6+11\omega)k\big),$$
$$f_3 = \tfrac{1}{5}\big(-(47+88\omega)i + (11+26\omega)j + (43+32\omega)k\big),$$

the hypotheses of Proposition 5.8 are satisfied by $\mathcal{E} = \{f_0, f_1, f_2, f_3\}$. Hence, letting

$$e_1 = \tfrac{1}{2}\big(-(232+384\omega) - (79+119\omega)i - (265+212\omega)j - (2-5\omega)k\big),$$
$$e_2 = \tfrac{1}{25}\big(268 + 444\omega + (6-31\omega)i - (17+84\omega)j - (1+\omega)k\big),$$
$$e_3 = \tfrac{1}{10}\big(13 + 24\omega - (7+12\omega)i - (10+21\omega)j) - k\big),$$

we get that $\mathcal{E}^\dagger = \{1, e_1, e_2, e_3\}$ is a quasi-good basis for $R(1)_2$.

Step 2. We are descending from $f = H \perp \langle 1\rangle$ to $g = H \perp \langle 2\rangle$. To illustrate Remark 2.12, we show that we can construct a well-known order of discriminant 2. For this purpose, we conjugate the quasi-good basis found above by $x = e_1 + e_2$ (which belongs to $R(1)_2^\times$, by Table 5.3), thus obtaining another quasi-good basis of $R(1)_2$. Proposition 5.6 gives then that $\{1, xe_1x^{-1}, 2\cdot xe_2x^{-1}, xe_3x^{-1}\}$ is a basis of $R(2)_2$.

Step 3. Applying Proposition 2.19 to this basis, we obtain that

$$R(2) = \left\langle 1, i, j, \frac{1+i+j+k}{2} \right\rangle_{\mathcal{O}}$$

is an Eicher order of discriminant 2. Note that the given basis is a basis for the classical maximal order in the quaternion algebra $(-1,-1)_{\mathbb{Q}}$.

4.1.2. *Discriminant 6.* Diagonalizing modulo 3 the quadratic form associated to $\{x \in R(2)_3{}^\vee : \mathrm{Tr}(x) = 0\}$, we obtain using Proposition 2.16 that $\{1, \frac{1}{2}(i+j), \frac{k}{2}, 2(i-j)\}$ is a quasi-good basis for $R(2)_3$.

We use Table 2.2 to descend from $\langle 1,-1,1\rangle$ to $\langle 1,-1,3\rangle$, using $\alpha_0 = 2, \alpha_1 = -1$ as parameters, and we get that a basis for $R(6)_3$ is given by $\{1, i+j-\frac{k}{2}, -\frac{1}{2}(i+j)+k, 2(i-j)\}$. Using Proposition 2.19, we get that

$$R(6) = \left\langle 1, i+2k, 3k, \frac{1+i+j+k}{2} \right\rangle_{\mathcal{O}}$$

is an Eichler order of discriminant 6.

4.1.3. *Discriminant* $6\sqrt{5}$. The basis $\mathcal{E} = \{\frac{1}{2}, -i, -\frac{k}{2}, -\frac{j}{4}\}$ of $R(6)_{\sqrt{5}}{}^\vee$ satisfies the hypotheses of Proposition 2.16, but with a stronger congruence in *(a)*, namely mod $(\sqrt{5})^2$. This implies that the basis for $R(6\sqrt{5})_{\sqrt{5}}$ obtained below is a quasi-good basis (see Remark 2.15).

We apply Table 2.2 using $\alpha_0 = 2 + \frac{\omega}{3}, \alpha_1 = -2$ as parameters, and obtain $\{1, -(1+\frac{\omega}{6})i + 2k, i - (2+\frac{\omega}{3})k, -2j\}$ as a basis for $R(6\sqrt{5})_{\sqrt{5}}$. Then Proposition 2.19 gives

$$R(6\sqrt{5}) = \left\langle 1, i + 2k, 3\sqrt{5}k, \frac{1+i+j+7k}{2} \right\rangle_{\mathcal{O}}.$$

4.1.4. *Discriminant* 30. To construct $R(30)$, we use the quasi-good basis obtained in the previous step and $\alpha_0 = \frac{139}{82} + \frac{61}{123}\omega, \alpha_1 = -2$ as parameters. The basis for $R(30)_{\sqrt{5}}$ obtained in this way is $\{1, -(\frac{34}{9} + \frac{31}{36}\omega)i + (\frac{303}{41} + \frac{68}{41}\omega)k, (\frac{303}{82} + \frac{34}{41}\omega)i - (\frac{68}{9} + \frac{31}{18}\omega)k, -2j\}$. Applying Proposition 2.19, we obtain

$$R(30) = \left\langle 1, i + 2k, 15k, \frac{1+i+j+7k}{2} \right\rangle_{\mathcal{O}}.$$

4.2. **Constructing the ideals.** We now proceed to compute ideal classes representatives for $R(30)$ iterating Algorithm 3.20, and using the quasi-good bases obtained above.

Before starting, note that Equation (3.22) implies that only norm one global units need to be considered when checking for equivalence of ideals in Step *4.1*, since K has narrow class number 1.

In [Vig80] it is shown that $R(1)$ has class number equal to one. It is also shown that $R(1)^{\times,1} = E_{120}$, where E_{120} is the binary icosahedral group. Using this explicit description we can avoid the use of LLL. Furthermore, by Remark 3.23, this group contains all of the global units needed in our computations.

4.2.1. *Discriminant 2.* The calculation of $Cl(R(2))$ can be done without using the algorithm. Since $|R(2)^{\times,1}| = 24$ and $[R(1)_2^{\times} : R(2)_2^{\times}] = 5$ (see Table 5.3), Corollary 3.7 implies that $\left[\Psi_{R(2)}^{R(1)}(R(1))\right] = [R(2)]$, from which we conclude that $R(2)$ has class number equal to 1 as well.

4.2.2. *Discriminant 6.* We now compute $Cl(R(6))$, following closely Algorithm 3.20. We have $S = \{R(2)\}$ as input.

Step 1. To obtain a set of representatives for $R(6)_3^{\times} \backslash R(2)_3^{\times}$, we use $\{0, 1, 2, \omega, 2\omega, \omega+1, \omega+2, 2\omega+1, 2\omega+2\}$ as a set of representatives for k_3.

Step 2. The ideal $R(2)_3$ is trivially generated by 1, so there is no need to use Remark 3.11 in this case.

Steps 3 and 4. The set $\Psi_{R(6)}^{R(2)}(R(2))$ has ten ideals, which we do not list for length reasons. The action of $R(2)^{\times,1}$ on $\Psi_{R(6)}^{R(2)}(R(2))$ has two orbits, namely $[I]$ and $[J]$, where $I = R(6)$ and J is the $R(6)$-ideal corresponding to the fifth generator of $R(6)_3^{\times} \backslash R(2)_3^{\times}$, which is given by

$$J = \left\langle i + (\omega-1)k, j - (\omega+1)k, 3k, 1 + \frac{\omega}{2}(3 - i - j - 3k) \right\rangle_{\mathcal{O}}.$$

This result agrees with Corollary 3.7, since $|R_r(I)^{\times,1}| = 6$, $|R_r(J)^{\times,1}| = 4$ and $[R(2)_3^{\times} : R(6)_3^{\times}] = 10$.

Hence, the algorithm gives that $Cl(R(6)) = \{[I], [J]\}$.

4.2.3. *Discriminant* $6\sqrt{5}$. We compute $Cl(R(6\sqrt{5}))$ in the same way as before. We avoid writing down all the details but give enough information so the reader may verify the computations easily.

- We take $\{0,1,2,3,4\}$ as a set of representatives for $k_{\sqrt{5}}$.
- 1 is a local generator of $J_{\sqrt{5}}$, since $J_{\sqrt{5}} = R(6)_{\sqrt{5}}$.
- Denote $\Psi^{R(6)}_{R(6\sqrt{5})}(I) = \{I_1, \dots I_6\}$ and $\Psi^{R(6)}_{R(6\sqrt{5})}(J) = \{J_1, \dots J_6\}$, where the notation is such that the n-th ideal corresponds to the n-th representative of $R(6\sqrt{5})^{\times}_{\sqrt{5}} \backslash R(6)^{\times}_{\sqrt{5}}$.
- The action of $R_r(I)^{\times,1}$ on $\Psi^{R(6)}_{R(6\sqrt{5})}(I)$ gives that $\left[\Psi^{R(6)}_{R(6\sqrt{5})}(I)\right] = \{[I_1],[I_4]\}$, and the action of $R_r(J)^{\times,1}$ on $\Psi^{R(6)}_{R(6\sqrt{5})}(J)$ gives that $\left[\Psi^{R(6)}_{R(6\sqrt{5})}(J)\right] = \{[J_1],[J_2],[J_3],[J_5]\}$ (see Table 4.1 for an explicit description of these ideals).

Hence, $Cl(R(6\sqrt{5})) = \{[I_1],[I_4],[J_1],[J_2],[J_3],[J_5]\}$. This agrees with Corollary 3.7, since we have that $|R_r(I_1)^{\times,1}| = |R_r(I_4)^{\times,1}| = |R_r(J_1)^{\times,1}| = |R_r(J_3)^{\times,1}| = 2$, and $|R_r(J_2)^{\times,1}| = |R_r(J_5)^{\times,1}| = 4$.

Ideal	Basis	Ideal above
I_1	$i+2k, 3\sqrt{5}k, 1, \frac{1}{2}(1+i+j+7k)$	I
I_4	$i+2k, 3\sqrt{5}k, j+14k, \frac{1}{2}(1+i+j+19k)$	
J_1	$i+(\omega-1)k, 3\sqrt{5}k, j-(\omega+7)k, \frac{1}{2}(1-i-j+(18+\sqrt{5})k)$	J
J_2	$i+(\omega-1)k, 3\sqrt{5}k, j-(\omega+4)k, \frac{1}{2}(1-i-j+(6+\sqrt{5})k)$	
J_3	$i+(\omega-1)k, 3\sqrt{5}k, j-(\omega+1)k, \frac{1}{2}(1-i+j+(6-\sqrt{5})k)$	
J_5	$i+(\omega-1)k, 3\sqrt{5}k, j-(\omega-5)k, \frac{1}{2}(1-i-j+\sqrt{5}k)$	

TABLE 4.1. Representatives for $Cl(R(6\sqrt{5}))$

4.2.4. *Discriminant* 30. Finally, we compute $Cl(R(30))$.

- The residue field is the same as before, so we take the same representatives for $k_{\sqrt{5}}$.
- The local generators at $\sqrt{5}$ for the ideals in $Cl(R(6\sqrt{5}))$ were constructed using Corollary 3.10. They are $1, 1-\frac{3}{4}i+\frac{3}{2}k, 1, 1-\frac{i}{4}+\frac{k}{2}, 1-\frac{i}{2}+k$ and $1-i+2k$ for I_1, I_4, J_1, J_2, J_3 and J_5 respectively.
- Since $R_r(I_1)^{\times,1} = R_r(I_4)^{\times,1} = R_r(J_1)^{\times,1} = R_r(J_3)^{\times,1} = \{\pm 1\}$, between the ideals belonging to $\Psi^{R(6\sqrt{5})}_{R(30)}(I_1), \Psi^{R(6\sqrt{5})}_{R(30)}(I_4), \Psi^{R(6\sqrt{5})}_{R(30)}(J_1)$ and $\Psi^{R(6\sqrt{5})}_{R(30)}(J_3)$ there are no equivalences.
- The action of $R_r(J_2)^{\times,1}$ on $\Psi^{R(6\sqrt{5})}_{R(30)}(J_2)$ gives that $\left[\Psi^{R(6\sqrt{5})}_{R(30)}(J_2)\right] = \{[J_{2,1}],[J_{2,2}],[J_{2,3}]\}$, and the action of $R_r(J_5)^{\times,1}$ on $\Psi^{R(6\sqrt{5})}_{R(30)}(J_5)$ gives that $\left[\Psi^{R(6\sqrt{5})}_{R(30)}(J_5)\right] = \{[J_{5,1}],[J_{5,2}],[J_{5,3}]\}$ (see Table 4.2).

In particular, $\#Cl(R(30)) = 4 \cdot 5 + 6 = 26$.

We end this section remarking that all the results obtained agree with Eichler's mass formula ([Vig80], Corollaire V.2.3).

Ideal	Basis	Ideal above
$I_{1,1}$	$i+2k, 15k, 1, \frac{1}{2}(1+i+j+7k)$	
$I_{1,2}$	$i+2k, 15k, j+2(1+3\omega)k, , \frac{1}{2}(1+i+j+(7-6\sqrt{5})k)$	
$I_{1,3}$	$i+2k, 15k, j-(1+3\omega)k, \frac{1}{2}(1+i+j+(-8+3\sqrt{5})k)$	I_1
$I_{1,4}$	$i+2k, 15k, j-(4-3\omega)k, \frac{1}{2}(1+i+j+(8+3\sqrt{5})k)$	
$I_{1,5}$	$i+2k, 15k, j-(7+6\omega)k, \frac{1}{2}(1+i+j+(7+6\sqrt{5})k)$	
$I_{4,1}$	$i+2k, 15k, j+2(2-3\omega)k, \frac{1}{2}(1+i+j-(11+6\sqrt{5})k)$	
$I_{4,2}$	$i+2k, 15k, j-(7+3\omega)k, \frac{1}{2}(1+i+j+(4+3\sqrt{5})k)$	
$I_{4,3}$	$i+2k, 15k, j+(5+3\omega)k, \frac{1}{2}(1+i+j+(1-6\sqrt{5})k)$	I_4
$I_{4,4}$	$i+2k, 15k, j+2(1-3\omega)k, \frac{1}{2}(1+i+j+(19+6\sqrt{5})k)$	
$I_{4,5}$	$i+2k, 15k, j+14k, \frac{1}{2}(1+i+j+19k)$	
$J_{1,1}$	$i+(2-5\omega)k, 15k, j+5(1+\omega)k, \frac{1}{2}(1+i+j+(2-5\sqrt{5})k)$	
$J_{1,2}$	$i+(2-5\omega)k, 15k, j+(2-4\omega)k, \frac{1}{2}(1+i+j+(17+4\sqrt{5})k)$	
$J_{1,3}$	$i+(2-5\omega)k, 15k, j+(2-\omega)k, \frac{1}{2}(1+i+j-(13+2\sqrt{5})k)$	J_1
$J_{1,4}$	$i+(2-5\omega)k, 15k, j-(4+7\omega)k, \frac{1}{2}(1+i+j+(2+7\sqrt{5})k)$	
$J_{1,5}$	$i+(2-5\omega)k, 15k, j-(1+7\omega)k, \frac{1}{2}(1+i+j+(2+\sqrt{5})k)$	
$J_{2,1}$	$i+(2-5\omega)k, 15k, j+(5-7\omega)k, \frac{1}{2}(1+i+j-(4+5\sqrt{5})k)$	
$J_{2,2}$	$i+(2-5\omega)k, 15k, j+(5-4\omega)k, \frac{1}{2}(1+i+j+(11+4\sqrt{5})k)$	J_2
$J_{2,3}$	$i+(2-5\omega)k, 15k, j+2(1+\omega)k, \frac{1}{2}(1+i+j+(11-2\sqrt{5})k)$	
$J_{3,1}$	$i+(2-5\omega)k, 15k, j-(4-5\omega)k, \frac{1}{2}(1+i+j-(10+5\sqrt{5})k)$	
$J_{3,2}$	$i+(2-5\omega)k, 15k, j-(7+4\omega)k, \frac{1}{2}(1-i+j+(5+4\sqrt{5})k)$	
$J_{3,3}$	$i+(2-5\omega)k, 15k, j+(5+2\omega)k, \frac{1}{2}(1+i+j+(5-2\sqrt{5})k)$	J_3
$J_{3,4}$	$i+(2-5\omega)k, 15k, j+(2-7\omega)k, \frac{1}{2}(1+i+j+(20+7\sqrt{5})k)$	
$J_{3,5}$	$i+(2-5\omega)k, 15k, j+(1+\omega)k, \frac{1}{2}(1+i+j-(10-\sqrt{5})k)$	
$J_{5,1}$	$i+(2-5\omega)k, 15k, j+(2+5\omega)k, \frac{1}{2}(1+i+j+(8-5\sqrt{5})k)$	
$J_{5,2}$	$i+(2-5\omega)k, 15k, j-(1+4\omega)k, \frac{1}{2}(1+i+j+(15+4\sqrt{5})k)$	J_5
$J_{5,3}$	$i+(2-5\omega)k, 15k, j-2(2-\omega)k, \frac{1}{2}(1-i+j-(6-3\sqrt{5})k)$	

TABLE 4.2. Representatives for $Cl(R(30))$

5. Appendix: The case $\mathfrak{p} = (2)$

Assume that $\mathfrak{p} = (2)$, i.e. that 2 is inert in $K/\mathbb{Q}$. The only difference with the case $\mathfrak{p} \nmid 2$ lays in the ternary quadratic forms that we need to consider to describe Bass orders. We will study these forms in this section.

Consider the matrices

$$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad J = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix},$$

and given f, g quadratic forms, let $f \perp g$ denote their orthogonal sum. According to Propositions 5.8 and 5.12 of [Lem11], isomorphism classes of Bass orders in quaternion algebras over K_2 are in one to one correspondence with the forms f of Table 5.1. As in the case $\mathfrak{p} \nmid 2$, orders of class A1 are the so called *Eichler orders*.

On the right column of Table 5.1 we indicate with 1 or -1 whether the order $C_0(f)$ belongs to the matrix algebra or to the division algebra. As before, this depends on whether the norm form associated to $C_0(f)$ is isotropic or not. We omit the calculations.

Figure 5.1 shows how isomorphism classes of Bass orders in quaternion algebras over K_2 are distributed.

Class	Form	Parameters	Condition	Algebra
A1	$H \perp \langle 2^s \rangle$	$s \geq 0$		1
A2	$J \perp \langle 2^s \rangle$	$s \geq 1$		$(-1)^s$
B	$\langle 1, 1, \delta_1 2^s \rangle$	$s \geq 0, \delta_1 \in \{1, 3\}$	$\delta_1 = 1$	-1
			$\delta_1 = 3$	1
C	$\langle 1, 6, \delta_1 2^s \rangle$	$s \geq 1, \delta_1 \in \{1, 3\}$	$\delta_1 = 1$	$(-1)^s$
			$\delta_1 = 3$	$(-1)^{s+1}$
D	$\langle 1, 5, \delta_1 2^s \rangle$	$s \geq 3, \delta_1 \in \{1, 3\}$	$\delta_1 = 1$	$(-1)^{s+1}$
			$\delta_1 = 3$	$(-1)^s$
E	$\langle 1, 2, \delta_2 2^s \rangle$	$s \geq 3, \delta_2 \in \{1, 5\}$	$\delta_2 = 1$	-1
			$\delta_2 = 5$	1
F	$\langle 1, 14, \delta_2 2^s \rangle$	$s \geq 4, \delta_2 \in \{1, 5\}$	$\delta_2 = 1$	1
			$\delta_2 = 5$	-1
G	$\langle 1, 10, \delta_2 2^s \rangle$	$s \geq 4, \delta_2 \in \{1, 5\}$	$\delta_2 = 1$	$(-1)^{s+1}$
			$\delta_2 = 5$	$(-1)^s$

TABLE 5.1. Ternary quadratic forms, when $\mathfrak{p} = (2)$.

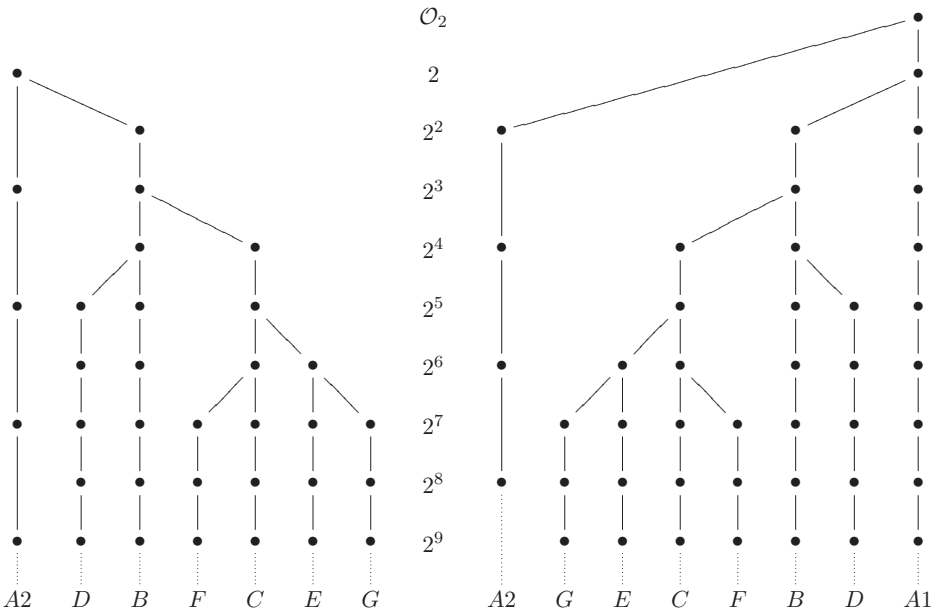

FIGURE 5.1. Isomorphism classes of Bass orders, when $\mathfrak{p} = (2)$.

The notion of good basis must be extended to include the non-diagonal forms of Table 5.1.

Definition 5.1. Let R_2 be a Bass order in correspondence with the form $f = H \perp \langle 2^s \rangle$ (respectively, $f = J \perp \langle 2^s \rangle$). A basis $\mathcal{B} = \{1, e_1, e_2, e_3\}$ of R_2

as an $\mathcal{O}_2$-module is *good* if the e_i satisfy

$$\begin{array}{lll} e_1^2 = 0, & e_1e_2 = 2^s(1-e_3), & e_2e_1 = 2^s e_3, \\ e_2^2 = 0, & e_2e_3 = 0, & e_3e_2 = e_2, \\ e_3^2 = e_3, & e_3e_1 = 0, & e_1e_3 = e_1. \end{array} \tag{5.2}$$

Respectively, if the e_i satisfy

$$\begin{array}{lll} e_1^2 = -2^s, & e_1e_2 = 2^s(1-e_3), & e_2e_1 = 2^s e_3, \\ e_2^2 = -2^s, & e_2e_3 = -e_1, & e_3e_2 = e_1+e_2, \\ e_3^2 = e_3 - 1, & e_3e_1 = -e_2, & e_1e_3 = e_1+e_2. \end{array} \tag{5.3}$$

Note that in such bases the norm form is given by

$$N(x) = \begin{cases} x_0^2 + x_0x_3 - 2^s x_1x_2, & f = H \perp \langle 2^s \rangle, \\ x_0^2 + x_0x_3 + x_3^2 - 2^s x_1x_2 + 2^s x_1^2 + 2^s x_2^2, & f = J \perp \langle 2^s \rangle. \end{cases} \tag{5.4}$$

Remark 5.5. We can extend Remark 2.10 to non-diagonal forms as follows. Let R_2 be an order in correspondence with $f = H \perp \langle 2^s \rangle$, and let $\mathcal{B}$ be a good basis of R_2. Then,

$$-2^s \cdot M_{\mathcal{B}^\vee} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2^{s+1} \end{pmatrix}.$$

Respectively if R_2 is in correspondence with $f = J \perp \langle 2^s \rangle$, then

$$2^s 3 \cdot M_{\mathcal{B}^\vee} = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 2^{s+1} \end{pmatrix}.$$

In order to state the analogue of Proposition 2.11, using Hensel's lemma take $\mu_1, \dots, \mu_8 \in \mathcal{O}_2$ satisfying:

- $\mu_1^2 = -7$
- $3\mu_2^2 = -13$
- $25\mu_3^2 = 1$
- $9\mu_4^2 = 1$
- $3\mu_5^2 = -5$
- $\mu_6^2 = -15$
- $3\mu_7^2 = -29$
- $3\mu_8^2 = -533$.

Proposition 5.6. *Let R_2 be an order corresponding to a form f from Table 5.1, and let $\{1, e_1, e_2, e_3\}$ be a good basis for R_2. Let g be a form beneath f, and let d_1, d_2, d_3 be as in Table 5.2.*

Then, $R_2' = \langle 1, d_1, d_2, d_3 \rangle_{\mathcal{O}_2}$ is a maximal suborder of R_2 in correspondence with the form g, of which $\{1, d_1, d_2, d_3\}$ is a good basis.

Proof. All the cases can be easily checked. Many of them follow from Propositions 5.11, 5.12 and 5.13 below (see the proof of Proposition 5.14). □

The notion of quasi-good basis remains unchanged, as well as the use of such bases for computing suborders and representatives for the quotients $(R_2')^\times \backslash R_2^\times$. We must show how to quasi-good bases in the 2-adic case.

Form	Form beneath	Good basis for $R'_{\mathfrak{p}}$
$H \perp \langle 1\rangle$	$J \perp \langle 4\rangle$	$d_1 = 2(\mu_1 - 2e_1 - 3e_2 - 2\mu_1 e_3)$, $d_2 = 2(-\mu + 3e_1 + 2e_2 + 2\mu_1 e_3)$, $d_3 = -2 - \mu_1 e_1 \mu_1 e_2 + 5e_3$
$H \perp \langle 2^s\rangle$	$H \perp \langle 2^{s+1}\rangle$	$d_1 = e_1, d_2 = 2e_2, d_3 = e_3$
$H \perp \langle 2\rangle$	$\langle 1,1,3\rangle$	$d_1 = \mu_1 - e_1 + 2e_2 - 2\mu_1 e_3$, $d_2 = -5 + 2\mu_1 e_1 + \mu_1 e_2 + 10e_3$, $d_3 = \mu_1 + 3e_1 + e_2 - 2\mu_1 e_3$
$J \perp \langle 2^s\rangle$	$J \perp \langle 2^{s+2}\rangle$	$d_1 = 2e_1, d_2 = 2e_2, d_3 = e_3$
$J \perp \langle 2\rangle$	$\langle 1,1,1\rangle$	$d_1 = \mu_2 - e_1 + 2e_2 - 2\mu_2 e_3$, $d_2 = \mu_2 - 2e_1 + e_2 - 2\mu_2 e_3$, $d_3 = -3 - \mu_2 e_1 + \mu_2 e_2 + 6e_3$
$\langle 1,1,\delta_1 2^s\rangle$	$\langle 1,1,\delta_1 2^{s+1}\rangle$	$d_1 = e_1 - e_2, d_2 = e_1 + e_2, d_3 = e_3$
$\langle 1,2,\delta_2 2^s\rangle$	$\langle 1,2,\delta_3 2^{s+1}\rangle$	$d_1 = -2e_2, d_2 = e_1, d_3 = e_3$
$\langle 1,5,2^s\rangle$	$\langle 1,5,3\cdot 2^{s+1}\rangle$	$d_1 = e_1 - 5e_2, d_2 = e_1 + e_2, d_3 = e_3$
$\langle 1,6,2^s\rangle$	$\langle 1,6,3\cdot 2^{s+1}\rangle$	$d_1 = -6e_2, d_2 = e_1, d_3 = e_3$
$\langle 1,10,2^s\rangle$	$\langle 1,10,5\cdot 2^{s+1}\rangle$	$d_1 = -10e_2, d_2 = e_1, d_3 = e_3$
$\langle 1,1,6\rangle$	$\langle 1,6,6\rangle$	$d_1 = 6e_3, d_2 = e_2, d_3 = -e_1$
$\langle 1,1,2\rangle$	$\langle 1,6,2\rangle$	$d_1 = 2e_1 + 6e_3, d_2 = e_2, d_3 = 2e_3 - e_1$
$\langle 1,1,2^2\rangle$	$\langle 1,5,3\cdot 2^3\rangle$	$d_1 = e_1 - 5e_2 + 4e_3, d_2 = e_1 + e_2 + 4e_3$, $d_3 = e_3 - e_1$
$\langle 1,14,\delta_2 2^s\rangle$	$\langle 1,14,\delta_2 2^{s+1}\rangle$	$d_1 = e_1 - 14\mu_1 e_2, d_2 = \mu_1 e_1 + e_2, d_3 = e_3$
$\langle 1,5,3\cdot 2^s\rangle$	$\langle 1,5,2^{s+1}\rangle$	$d_1 = e_1 - 5\mu_2 e_2, d_2 = \mu_2 e_1 + e_2, d_3 = e_3$
$\langle 1,10,5\cdot 2^s\rangle$	$\langle 1,10,2^{s+1}\rangle$	$d_1 = -10\mu_3 e_2, d_2 = \mu_3 e_1, d_3 = e_3$
$\langle 1,6,3\cdot 2^s\rangle$	$\langle 1,6,2^{s+1}\rangle$	$d_1 = 2e_1 - 6\mu_4 e_2, d_2 = \mu_4 e_1 + 2e_2$, $d_2 = \mu_4 e_1 + 2e_2, d_3 = e_3$
$\langle 1,6,3\cdot 2^2\rangle$	$\langle 1,2,2^3\rangle$	$d_1 = 6\mu_4(-\mu_5 e_2 + 2e_3), d_2 = \mu_4 e_1$, $d_3 = e_2 + \mu_5 e_3$
$\langle 1,2,2^3\rangle$	$\langle 1,1,2^4\rangle$	$d_1 = -2e_2 + 8e_3, d_2 = e_1, d_3 = e_2 + 5e_3$
$\langle 1,2,5\cdot 2^3\rangle$	$\langle 1,10,5\cdot 2^4\rangle$	$d_1 = -2\mu_6 e_2 + 40e_3, d_2 = e_1$, $d_3 = e_2 + \mu_6 e_3$
$\langle 1,6,3\cdot 2^3\rangle$	$\langle 1,14,2^4\rangle$	$d_1 = 6\mu_4(-\mu_5 e_2 + 4e_3), d_2 = \mu_4 e_1$, $d_3 = e_2 + \mu_5 e_3$
$\langle 1,6,2^2\rangle$	$\langle 1,2,5\cdot 2^3\rangle$	$d_1 = 2(\mu_7 e_1 - 3\mu_7 e_2 - 10e_3)$, $d_2 = e_1 + 2e_2, d_3 = e_1 - 3e_2 + \mu_7 e_3$
$\langle 1,6,2^3\rangle$	$\langle 1,14,5\cdot 2^4\rangle$	$d_1 = 2(\mu_7 e_1 - 3\mu_7 e_2 - 60e_3)$, $d_2 = e_1 + 2e_2, d_3 = 3e_1 - 9e_2 + \mu_7 e_3$

TABLE 5.2. Suborders

Remark 5.7. Proposition 2.16 still holds for diagonal forms, setting $n = 3v_2(a) + 2$ in order to be able to use Hensel's lemma in its proof.

Proposition 5.8. *Let R_2 be an order in correspondence with $f = H \perp \langle 2^s\rangle$. Let $\mathcal{E} = \{f_0, f_1, f_2, f_3\}$ be a basis of $R_2^\vee$ satisfying (2.2). Assume that $\mathcal{E}$ satisfies the following conditions.*

(a) There exists $\beta \in \mathcal{O}_2$ *such that*

$$-2^s \cdot M_{\mathcal{E}} \equiv \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & \beta \end{pmatrix} \mod (M_3(2^3\mathcal{O}_2)).$$

(b) $\det(M_{\mathcal{E}}) = 2^{1-2s}$.

Let $e_i = -2^s \cdot f_j \bar{f}_k$, *where* (i,j,k) *is an even permutation of* $(1,2,3)$. *Then,* $\mathcal{E}^\dagger = \{1, e_1, e_2, e_3\}$ *is a quasi-good basis of* R_2.

The following lifting lemma is needed in the proof of Proposition 5.8, which is quite similar to the proof of Proposition 2.16, and we omit.

Lemma 5.9. *Let* m *be an integer such that* $m \geq 3$, *and let* $A \in M_3(\mathcal{O}_2)$ *be a symmetric matrix. Assume that there exists* $C \in GL_3(\mathcal{O}_2)$ *such that*

$$C^t A C \equiv \begin{pmatrix} 0 & \alpha & 0 \\ \alpha & 0 & 0 \\ 0 & 0 & \beta \end{pmatrix} \mod (M_3(2^m\mathcal{O}_2)),$$

with $v_2(\alpha) = 0$. *Then, there exists* $C' \in GL_3(\mathcal{O}_2)$ *satisfying* $C' \equiv C \mod (M_3(2^{m-1}\mathcal{O}_2))$ *such that*

$$C'^t A C' \equiv \begin{pmatrix} 0 & \alpha' & 0 \\ \alpha' & 0 & 0 \\ 0 & 0 & \beta' \end{pmatrix} \mod (M_3(2^{m+1}\mathcal{O}_2)),$$

with $\alpha' \equiv \alpha \mod (2^{m-1}\mathcal{O}_2)$.

Proof. Write

$$C^t A C = \begin{pmatrix} 0 & \alpha & 0 \\ \alpha & 0 & 0 \\ 0 & 0 & \beta \end{pmatrix} + 2^m \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix},$$

with $a, b, \ldots, f \in \mathcal{O}_2$. We claim that there exists a matrix $C_0 \in GL_3(\mathcal{O}_2)$ such that

$$C_0^t A C = \begin{pmatrix} -a & b' & c'2^m \\ d' & -d & e'2^m \\ -2c & -2e & f' \end{pmatrix},$$

with $b', c', d', e', f' \in \mathcal{O}_2$. This can be shown by performing row operations on $C^t A C$, using the $(1,2)$ and $(2,1)$ entries as pivots to first obtain zeroes at the $(1,1), (2,2), (3,1)$ and $(3,2)$ entries, and then obtain $-a, -d, -2c$ and $-2e$ at the $(1,1), (2,2), (3,1)$ and $(3,2)$ entries respectively.

Now let $C' = C + 2^{m-1}C_0$. Then,

$$C'^t A C' = \begin{pmatrix} 0 & \alpha' & c'2^{2m-1} \\ \alpha' & 0 & e'2^{2m-1} \\ c'2^{2m-1} & e'2^{2m-1} & \beta' \end{pmatrix} + 2^{2(m-1)} C_0^t A C_0.$$

where $\alpha' = \alpha + 2^{m-1}(b' + d')$. Since $2(m-1) \geq m+1$, we are done. □

For orders of class A2 we only state the corresponding analogue of Proposition 5.8.

Proposition 5.10. *Let R_2 be an order in correspondence with $f = J \perp \langle 2^s \rangle$. Let $\mathcal{E} = \{f_0, f_1, f_2, f_3\}$ be a basis of $R_2^\vee$ satisfying (2.2). Assume that $\mathcal{E}$ satisfies the following conditions.*

(a) There exists $\beta \in \mathcal{O}_2$ such that

$$2^s 3 \cdot M_{\mathcal{E}} \equiv \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & \beta \end{pmatrix} \mod (M_3(2^3\mathcal{O}_2)).$$

(b) $\det(M_{\mathcal{E}}) = 2^{1-2s}3^{-2}$.

Let $e_i = 2^s 3 \cdot f_j \bar{f}_k$, where (i, j, k) is an even permutation of $(1, 2, 3)$. Then, $\mathcal{E}^\dagger = \{1, e_1, e_2, e_3\}$ is a quasi-good basis of R_2.

Finally, we proceed to give systems of representatives for the quotient sets $(R_2')^\times \backslash R_2^\times$ when R_2' is a maximal suborder of R_2 obtained using Algorithm 2.21. We start stating three general results which, though stated and used only when $\mathfrak{p} = (2)$, hold without restrictions on $\mathfrak{p}$.

Let $\mathcal{B} = \{1, e_1, e_2, e_3\}$ be a good basis for R_2. Let q be the order of the residue field k_2, and let $a_1, a_2, \ldots, a_q \in \mathcal{O}_2$ be a set of representatives for k_2.

Proposition 5.11. *Suppose that R_2 is in correspondence with the form $f = \langle 1, a, b \rangle$, and let $\lambda \in \mathcal{O}_2$. Assume that there exist $\alpha_0, \alpha_3 \in \mathcal{O}_2$ such that $\alpha_0^2 + a\alpha_3^2 = \lambda$. Let $v = \alpha_0 + \alpha_3 e_3$, and let $d_1 = ve_1, d_2 = ve_2, d_3 = e_3$.*

Then, $R_2' = \langle 1, d_1, d_2, d_3 \rangle_{\mathcal{O}_2}$ is a suborder of R_2 in correspondence with the form $g = \langle 1, a, \lambda b \rangle$, of which $\{1, d_1, d_2, d_3\}$ is a good basis. Furthermore, if $v_2(\lambda) = 1$ and $v_2(b) \geq 1$, then R_2' is a maximal suborder of R_2, the index of $(R_2')^\times$ in $R_2^\times$ is q, and a set of representatives for the set $(R_2')^\times \backslash R_2^\times$ is given by $\{1 + a_i e_2 : 1 \leq i \leq q\}$.

Proof. The first assertion is easily checked. To prove the second one, we use Proposition 3.12. Since $v_2(b) \geq 1$, by (2.6) the norm form on $2R_2 \backslash R_2$ is given by $N(x) = x_0^2 + ax_3^2$. Hence, $|(2R_2 \backslash R_2)^\times| = c \cdot q^2$, where $c = \#\{(x_0, x_3) \in k_2 : x_0^2 + ax_3^2 \neq 0\}$.

We have that

$$2R_2 \backslash R_2' = \big\{x \in 2R_2 \backslash R_2 : x_0, x_3 \in k_2, (x_1, x_2) \in A(k_2)\big\},$$

where $A \in \mathrm{End}_{k_2}(k_2 \times k_2)$ is the morphism given by left multiplication by $\left(\begin{smallmatrix} \alpha_0 & \alpha_3 \\ -\alpha_3 & \alpha_0 \end{smallmatrix}\right)$. Since $\alpha_0^2 + a\alpha_3^2 = \lambda$ and $v_2(\lambda) = 1$, this matrix has rank 1. Hence, $|(2R_2 \backslash R_2')^\times| = c \cdot q$, which shows that $[R_2^\times : (R_2')^\times] = q$.

To see that the given units are not equivalent, take $x \in (2R_2 \backslash R_2')^\times$. Then, it is easy to see that

$$\begin{aligned}(1 + a_i e_2)x &= x_0 + (x_1 - a_i x_2 x_3)e_1 + (a_i x_0 + x_2)e_2 + x_3 e_3 \\ &= 1 + a_j e_2\end{aligned}$$

implies that $i = j$.

□

The next two results can be proved following the same ideas as the ones used above.

Proposition 5.12. *Suppose that R_2 is in correspondence with the form $f = \langle 1, a, b\rangle$, and let $\mu \in \mathcal{O}_2$. Assume that there exist $\alpha_0, \alpha_2 \in \mathcal{O}_2$ such that $\alpha_0^2 + b\alpha_2^2 = \mu$. Let $v = \alpha_0 + \alpha_2 e_2$, and let $d_1 = ve_1, d_2 = e_2, d_3 = ve_3$.*

Then, $R_2' = \langle 1, d_1, d_2, d_3\rangle_{\mathcal{O}_2}$ is a suborder of R_2 in correspondence with the form $g = \langle 1, \mu a, b\rangle$, of which $\{1, d_1, d_2, d_3\}$ is a good basis. Furthermore, if $v_2(\mu) = 1$ and $v_2(b) \geq 1$, then R_2' is a maximal suborder of R_2, the index of $(R_2')^\times$ in $R_2^\times$ is q, and a set of representatives for the set $(R_2')^\times \backslash R_2^\times$ is given by $\{1 + a_i e_3 : 1 \leq i \leq q\}$.

Proposition 5.13. *Suppose that R_2 is in correspondence with the form $f = \langle 1, a, b\rangle$. Let $a', b' \in \mathcal{O}_2$. Assume that there exist $\alpha_1, \alpha_2, \alpha_3 \in \mathcal{O}_2$ such that $ab\alpha_1^2 = b'$, and $a\alpha_3^2 + b\alpha_2^2 = a'$. Let $d_2 = \alpha_1 e_1, d_3 = \alpha_2 e_2 + \alpha_3 e_3, d_1 = d_3 d_2$.*

Then, $R_2' = \langle 1, d_1, d_2, d_3\rangle_{\mathcal{O}_2}$ is a suborder of R_2 in correspondence with the form $g = \langle 1, a', b'\rangle$, of which $\{1, d_1, d_2, d_3\}$ is a good basis. Furthermore, if $v_2(b') = v_2(b) + 1, v_2(a) = v_2(a') = 1$ and $v_2(b) \geq 1$, then R_2' is a maximal suborder of R_2, the index of $(R_2')^\times$ in $R_2^\times$ is q, and a set of representatives for the set $(R_2')^\times \backslash R_2^\times$ is given by $\{1 + a_i e_3 : 1 \leq i \leq q\}$.

Assume that the given system of representatives for k_2 is such that $a_1 = 1$, and that a_{q-1} and a_q are the two solutions in k_2 of $t^2 + t + 1 = 0$, when $q = 2^s$ with even s.

Proposition 5.14. *Let $\mathcal{B} = \{1, e_1, e_2, e_3\}$ be a quasi-good basis of R_2, and assume that R_2' is a maximal suborder of R_2 that has been built using Algorithm 2.21. Then, Table 5.3 gives the index of $(R_2')^\times$ in $R_2^\times$ and a system of representatives for the quotient set.*

R_2-class	R_2'-class	$[R_2^\times : (R_2')^\times]$	Representatives	Condition
A1	A1	$q+1$	$e_1 + e_2, 1 + a_i e_2 \quad (1 \leq i \leq q)$	$s = 0$
		q	$1 + a_i e_2 \quad (1 \leq i \leq q)$	$s \geq 1$
	A2	$q(q-1)$	$(1 + a_i e_2)(e_1 + a_j e_2) \quad (1 \leq i, j \leq q, a_j \neq 0)$	r odd
		$q(q+1)$	$(1 + a_i e_2)(e_1 + a_j e_2) \quad (1 \leq i, j \leq q, a_j \neq 0)$, $(1 + a_i e_2)(a_j + e_1) \quad (1 \leq i \leq q, q - 2 \leq j \leq q)$	r even
	B	$q-1$	$1 + a_i e_2 \quad (1 < i \leq q)$	
A2	A2	q^2	$1 + a_i e_1 + a_j e_2 \quad (1 \leq i, j \leq q)$	
	B	$q-1$	$e_3, 1 + a_i e_3 \quad (1 \leq i \leq q-2)$	r even
		$q+1$	$e_3, 1 + a_i e_3 \quad (1 \leq i \leq q)$	r odd
B	B	q	$e_2, 1 + a_i e_2 \quad (1 < i \leq q)$	$s = 0$
			$1 + a_i e_2 \quad (1 \leq i \leq q)$	$s \geq 1$
	C	q	$1 + a_i e_3 \quad (1 \leq i \leq q)$	
	D	q	$1 + a_i e_2 \quad (1 \leq i \leq q)$	
C	C	q	$1, a_i + e_2 \quad (1 \leq i \leq q)$	
	E	q	$1, a_i + e_2 \quad (1 \leq i \leq q)$	$\delta_1 = 1$
			$1, a_i + e_3 \quad (1 \leq i \leq q)$	$\delta_1 = 3$
	F	q	$1, a_i + e_2 \quad (1 \leq i \leq q)$	$\delta_1 = 1$
			$1, a_i + e_3 \quad (1 \leq i \leq q)$	$\delta_1 = 3$
D	D	q	$1, a_i + e_2 \quad (1 \leq i \leq q)$	
E	E	q	$1, a_i + e_2 \quad (1 \leq i \leq q)$	
	G	q	$1, a_i + e_3 \quad (1 \leq i \leq q)$	
F	F	q	$1, a_i + e_2 \quad (1 \leq i \leq q)$	
G	G	q	$1, a_i + e_2 \quad (1 \leq i \leq q)$	

TABLE 5.3. $[R_2^\times : (R_2')^\times]$ and representatives for $(R_2')^\times \backslash R_2^\times$

Proof. As in the $\mathfrak{p} \nmid 2$ case, by Proposition 3.12, we may assume that $\mathcal{B}$ is a good basis for R_2, as well as we may perform all calculations modulo $2R_2$.

The cases B to B, C to C, D to D, E to E, F to F and G to G are covered by Proposition 5.11. The case B to C is covered by Proposition 5.12.

To prove the case B to D, use Proposition 5.12 to descend from $\langle 1, 1, 2^2\rangle$ to $\langle 1, 5, 2^2\rangle$, and Proposition 5.11 to descend from this form to $\langle 1, 5, 3 \cdot 2^3\rangle$. A similar argument works for the other form of class B.

The cases C to E (with $\delta_1 = 3$), C to F (with $\delta_1 = 3$) and E to G are covered by Proposition 5.13.

Now we will prove the case from A2 to B. The remaining cases can be treated in a similar way, with no further difficulties.

By (5.4), the norm form on $2R_2\backslash R_2$ is given by $N(x) = x_0^2 + x_0x_3 + x_3^2$. Hence, a standard calculation shows that

$$|(2R_2\backslash R_2)^\times| = \begin{cases} q^4 - q^2(2q-1), & \text{if } r \text{ is even} \\ q^4 - q^2, & \text{if } r \text{ is odd} \end{cases}$$

Since $d_1 = 1 + e_1, d_2 = 1 + e_2$ and $d_3 = 1 + e_1 + e_2$ in $2R_2\backslash R_2$, we have that $2R_2\backslash R_2' = \langle 1, e_1, e_2\rangle_{k_2}$. Hence $|(2R_2\backslash R_2)^\times| = q^3 - q^2$, and this proves the equality on $[R_2^\times : (R_2')^\times]$.

Now we need to find the right amount of non equivalent units. It is easily seen that the elements in the set $\{1 + a_ie_3 : 1 \le i \le q\} \cup \{e_3\}$ are not mutually equivalent modulo $(2R_2\backslash R_2)^\times$, and they are all units, except for $1 + a_{q-1}e_3$ and $1 + a_qe_3$ when $q = 2^s$ with even s.

□

References

[Brz82] Juliusz Brzezinski. A characterization of Gorenstein orders in quaternion algebras. *Math. Scand.*, 50(1):19–24, 1982.

[Brz83] Juliusz Brzezinski. On orders in quaternion algebras. *Comm. Algebra*, 11(5):501–522, 1983.

[Brz90] Juliusz Brzezinski. On automorphisms of quaternion orders. *J. Reine Angew. Math.*, 403:166–186, 1990.

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[CS01] Caterina Consani and Jasper Scholten. Arithmetic on a quintic threefold. *Internat. J. Math.*, 12(8):943–972, 2001.

[DD08] Lassina Dembélé and Steve Donnelly. Computing Hilbert modular forms over fields with nontrivial class group. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 371–386. Springer, Berlin, 2008.

[EMP86] H. M. Edgar, R. A. Mollin, and B. L. Peterson. Class groups, totally positive units, and squares. *Proc. Amer. Math. Soc.*, 98(1):33–37, 1986.

[GL09] Benedict H. Gross and Mark W. Lucianovic. On cubic rings and quaternion rings. *J. Number Theory*, 129(6):1468–1478, 2009.

[Kap69] Irving Kaplansky. Submodules of quaternion algebras. *Proc. London Math. Soc. (3)*, 19:219–232, 1969.

[KV10] Markus Kirschmer and John Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM J. Comput.*, 39(5):1714–1747, 2010.

[Lem11] Stefan Lemurell. Quaternion orders and ternary quadratic forms. 2011. http://arxiv.org/abs/1103.4922.

[Piz76] Arnold Pizer. On the arithmetic of quaternion algebras. II. *J. Math. Soc. Japan*, 28(4):676–688, 1976.

[Piz80] Arnold Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. *J. Algebra*, 64(2):340–390, 1980.

[PRV05] Ariel Pacetti and Fernando Rodriguez Villegas. Computing weight 2 modular forms of level p^2. *Math. Comp.*, 74(251):1545–1557 (electronic), 2005. With an appendix by B. Gross.

[PT07] Ariel Pacetti and Gonzalo Tornaría. Shimura correspondence for level p^2 and the central values of L-series. *J. Number Theory*, 124(2):396–414, 2007.

[Sa11] W. A. Stein et al. *Sage Mathematics Software (Version 4.7.2)*. The Sage Development Team, 2011. http://www.sagemath.org.

[SW05] Jude Socrates and David Whitehouse. Unramified Hilbert modular forms, with examples relating to elliptic curves. *Pacific J. Math.*, 219(2):333–364, 2005.

[Vig76] Marie-France Vignéras. Simplification pour les ordres des corps de quaternions totalement définis. *J. Reine Angew. Math.*, 286/287:257–277, 1976.

[Vig80] Marie-France Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[Voi10] John Voight. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. 2010. http://arxiv.org/abs/1004.0994

E-mail address: apacetti@dm.uba.ar

Departamento de Matemática, Universidad de Buenos Aires - Pabellón I, Ciudad Universitaria (C1428EGA), Buenos Aires, Argentina

E-mail address: nsirolli@dm.uba.ar

Departamento de Matemática, Universidad de Buenos Aires - Pabellón I, Ciudad Universitaria (C1428EGA), Buenos Aires, Argentina