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 $K$. 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, ideal classes for Eichler 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 [CS01] for Hilbert modular forms over $\mathbb{Q}[\sqrt{5}]$. These methods require first to find a suitable order in such an algebra, and then to compute representatives for its ideal classes. The purpose of this article is to compute both things in an efficient way, and in a rather general setting.

Note that although in [DD08] the authors, using a smart cohomological trick, manage to compute Hilbert modular forms for any level using only maximal orders (which avoids computing representatives for other orders), their approach cannot be used for computing preimages for the Shimura map on Hilbert modular forms of half-integral weight. The calculation of preimages for the Shimura map was explained in [PT07] for classical modular forms, and its generalization to the Hilbert setting will appear in an article by the second author.

We consider a broad family of orders, namely the Bass orders. Besides the well-known Eichler orders (which we call orders of class A1), this family includes the orders considered by Pizer in [Piz76] (of class A2), the orders used in [PRV05] for computing modular forms of level $p^2$ (of class B), and the orders considered in [PT07] for computing preimages for such forms under the Shimura correspondence (of class C). The rest of the Bass orders are included for completeness.

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 Bass 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.

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 Bass 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 the constructed ideals are contained in the given ones. This avoids, in contrast with the methods à la Pizer (see, e.g., [Piz80], [CS01], [SW05]), the repeated usage of norm forms for checking equivalences between ideals (see [Piz80], Proposition 1.18). The details are explained in Remark 3.20.

Since the full implantation (in SAGE) of our algorithm is still in progress, we cannot make a systematic large scale comparison of running times; however, in [PRV02] there is an algorithm, which can be considered as a special case of ours, that computes ideal classes representatives for orders of discriminant $p^2$ in the algebra over $\mathbb{Q}$ ramified exactly at $p$ and at infinity. This algorithm has a much better performance than MAGMA’s in some simple cases. For example, when computing ideal representatives for an order of discriminant 103$^2$ in the algebra over $\mathbb{Q}$ ramified exactly at 103 and at infinity, with an Intel Core™2 CPU 6600 with 2 Gb of RAM memory, MAGMA (V2.16-6) needs 1254.96 seconds, whereas the routines in PARI/GP (V2.5.0) take 0.00218 seconds.

In [Lem11] it was shown that 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 us 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 proving 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 exactly at the two infinite places.
Throughout this 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.

1. Basic notions and notation

We start by recalling some basic definitions and properties of quaternion algebras that will be used in the paper. A more detailed exposition can be found 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 $K$. 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 $\text{Tr}(x) = x + \bar{x}$ and the quadratic form (reduced) norm given by $N(x) = xx$. The bilinear form corresponding to the latter is given by $(x, y) \mapsto \text{Tr}(xy)$.

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

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

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 $\{\det(\text{Tr}(x_i \bar{x}_j)) : x_1, \ldots, x_4 \in R\}$.

Given a lattice $\Lambda$, the set

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

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

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

We say that $\Lambda$ 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 $\Lambda$ 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 $\Lambda'$ in $\Lambda$ is the ideal $[\Lambda : \Lambda'] \subseteq \mathcal{O}$ generated by $\{\det(\phi) : \phi \in \text{End}_K(B), \phi(\Lambda) \subseteq \Lambda'\}$.

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 $\text{Cl}(R)$. 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

- $\mathfrak{p}, q, \ldots$: prime ideals of $\mathcal{O}$.
- $\Lambda, \Lambda', \ldots$: lattices in $B$. 
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 be 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 \( p \) such that \([R : R'] = p \) or \( p^2 \) and \( pR \subseteq R' \).

Hence, maximal suborders of a given order \( R \) can be obtained by describing the maximal suborders of \( R_p \) for every \( p \).

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

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 \( R_p \) be an order, and let \( \mathcal{E} = \{f_0, f_1, f_2, f_3\} \) be a basis of \( R_p^\vee \) satisfying

\[
\begin{align*}
\text{Tr}(f_0) &= 1, \\
\text{Tr}(f_1) &= \text{Tr}(f_2) = \text{Tr}(f_3) = 0.
\end{align*}
\]

Denote by \( M_\mathcal{E} \) the Gram matrix of the norm form in the trace zero submodule of \( R_p^\vee \) corresponding to \( \mathcal{E} \), i.e.,

\[
M_\mathcal{E} = \left( \text{Tr}(f_i f_j) \right)_{1 \leq i, j \leq 3}.
\]

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

Conversely, to an integral ternary quadratic form \( f \) over \( \mathcal{O}_p \) we can associate an order \( C_0(f) \) in a quaternion algebra over \( K_p \): the order and the algebra are given by the even part of the Clifford algebras associated to \( f \) over \( \mathcal{O}_p \) and \( K_p \), respectively.

By Propositions 5.8 and 5.10 of [Lem11], the maps \( R_p \mapsto d \cdot M_\mathcal{E} \) and \( f \mapsto C_0(f) \) give a bijection between isomorphism classes of Bass orders in quaternion algebras over \( K_p \) 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.

In particular, every Bass order \( R \) induces a family \( (f_p)_p \) of ternary quadratic forms, letting \( f_p \) be the form in Table 2.1 corresponding to \( R_p \). This family satisfies that \( f_p = \langle 1, -1, 1 \rangle \) for almost every \( p \), and is independent of the genus of \( R \).

Equation (2.3) below implies that, given a form \( f = \langle 1, a, b \rangle \), the quaternion algebra \( C_0(f) \otimes \mathcal{O}_p \) \( K_p \) is a matrix algebra if and only if \( \langle a, b, ab \rangle \) is isotropic, i.e., if and only if the Hilbert symbol \( (\frac{-a}{p}, -b) \) equals 1. The sign for each case is shown in Table 2.1.
The graphs in Figure 2.1 show how the isomorphism classes of Bass orders in quaternion algebras over $K_p$ 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 $R_p$ corresponding to the top vertex, and an order $R'_p$ corresponding to the bottom vertex, such that $R'_p$ is a maximal suborder of $R_p$; if $f$ and $g$ are 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.

### Table 2.1. Ternary quadratic forms in correspondence with local Bass orders.

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

### Division algebra

```
• O_p
  • p
  • p^2
  • p^3
  • p^4
  • p^5
```

### Matrix algebra

```
• A2
  • C
  • B
  • C
  • A1
```

**Figure 2.1.** Graph of isomorphism classes of local Bass orders, ordered by inclusion.
All the orders in the left graph lie in the division quaternion algebra, while all the orders in the right graph 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 in the division algebra are the orders of level $p^{2r+1}$ considered in [Piz76] (see also Section 3 of [Brz83]). Also in the division algebra, the orders of class B are the orders of level $p^2$ considered in [PRV05], and the vertices of class C and discriminant $p^3$ are represented by the orders $\mathcal{O}^+, \mathcal{O}^-$ considered in [PT07].

**Example 2.2.** Let $s \geq 0$. The order $E_s = \langle \pi_p^s \mathcal{O}_p, \mathcal{O}_p \rangle \subseteq M_2(\mathcal{O}_p)$ is a Bass order of class A1 and discriminant $p^s$. $E_{s+1}$ is a maximal suborder of $E_s$.

**Definition 2.3.** Let $R_p$ 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 $R_p$ as an $\mathcal{O}_p$-module. We say that $\mathcal{B}$ is a good basis if the $e_i$ satisfy

$$
eq 1 = ab, \quad e_2^2 = -b, \quad e_3^2 = -a,$$

(2.2) $$e_1 e_2 = -b e_3, \quad e_2 e_3 = -e_1, \quad e_3 e_1 = a e_2,$$

$$e_2 e_1 = b e_3, \quad e_3 e_2 = e_1, \quad e_1 e_3 = a e_2.$$

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

$$N = \langle 1, ab, b, a \rangle.$$

**Example 2.4.** A good basis for the order $E_s$ defined above is given by

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

Let $R_p$ 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 $R_p$ satisfying (2.1). Let $e_i = 4ab \cdot f_j f_k$, where $(i, j, k)$ is an even permutation of $(1, 2, 3)$, and define $\mathcal{E}^+ = \{1, e_1, e_2, e_3\}$. Then $\mathcal{E}^+$ is a basis of $R_p$ (see [Lem11], Section 4).

**Proposition 2.5.** With the notation as above, if $\mathcal{E}$ is such that

(2.4) $$2ab \cdot M_\mathcal{E} = \text{diag}(1, a, b),$$

then $\mathcal{E}^+$ is a good basis of $R_p$.

For a proof see [Lem11], Section 4.

**Remark 2.6.** Conversely, if $\mathcal{B}$ is a good basis of $R_p$, then $M_{\mathcal{B}^+}$ satisfies (2.4), where given a basis $\mathcal{B} = \{e_0, e_1, e_2, e_3\}$ of $R_p$, we denote by $\mathcal{B}^+ = \{f_0, f_1, f_2, f_3\}$ the basis of $R_p^\vee$ characterized by the equations $\text{Tr}(e_i f_j) = \delta_{ij}$.

**Constructing maximal suborders, the local case.** Given an order $R_p$ 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 $R_p$ (see Figure 2.1). To do this, given a good basis $\{1, e_1, e_2, e_3\}$ of $R_p$ and a form $g$ from Table 2.1, we write an element $d_1, d_2, d_3 \in R_p$ satisfying equations (2.2) corresponding to the
form \( g \). Then, the order \( R'_p = \langle 1, d_1, d_2, d_3 \rangle_{\mathcal{O}_p} \) is a maximal suborder of \( R_p \) in correspondence with the form \( g \), for which \( \{1, d_1, d_2, d_3\} \) is a good basis.

Using Hensel’s lemma, take \( \alpha_0, \alpha_1, \beta_0, \beta_1, \mu, \nu \in \mathcal{O}_p \) satisfying:

- \( \alpha_0^2 - \alpha_1^2 = \pi_p \).
- \( \beta_0^2 + \beta_1^2 = \delta \).
- \( \mu^2 = -1 \), when \( \left( \frac{-1}{p} \right) = 1 \).
- \( \nu^2 = -\delta \), when \( \left( \frac{-1}{p} \right) = -1 \).

**Proposition 2.7.** The elements \( d_1, d_2, d_3 \) defined by Table 2.2 satisfy the equations (2.2) corresponding to the form \( g \).

**Table 2.2.** Construction of maximal suborders, in terms of good bases and ternary quadratic forms.

| Form                  | Form beneath                  | Good basis for \( R'_p \)                                      |
|-----------------------|-------------------------------|---------------------------------------------------------------|
| \( \langle 1, -1, \pi^*_p \rangle \) | \( \langle 1, -1, \pi^{*+1}_p \rangle \) | \( d_1 = \alpha_0 e_1 + \alpha_1 e_2, \) \( d_2 = \alpha_1 e_1 + \alpha_0 e_2, d_3 = e_3 \) |
| \( \langle 1, -1, 1 \rangle \)   | \( \langle 1, -\delta, \pi^2_p \rangle \)   | \( d_1 = \pi_p (\beta_1 e_1 - \beta_0 e_3), \) \( d_2 = \pi_p e_2, d_4 = \beta_0 e_1 + \beta_1 e_3 \) |
| \( \langle 1, -1, \pi_p \rangle \) | \( \langle 1, \pi_p, \pi_p \rangle \), if \( \left( \frac{-1}{p} \right) = 1 \) | \( d_1 = \mu \pi_p e_3, d_2 = \mu e_1, d_3 = e_2 \) |
|                       | \( \langle 1, \pi_p, \pi_p \rangle \), if \( \left( \frac{-1}{p} \right) = -1 \) | \( d_1 = \nu \pi_p e_3, d_2 = \nu e_1, d_3 = e_2 \) |
| \( \langle 1, -\delta, \pi^*_p \rangle \) | \( \langle 1, -\delta, \pi^{*+2}_p \rangle \) | \( d_1 = \pi_p e_1, d_2 = \pi_p e_2, d_3 = e_3 \) |
| \( \langle 1, -\delta, \pi_p \rangle \) | \( \langle 1, \pi_p, \delta \pi_p \rangle \), if \( \left( \frac{-1}{p} \right) = 1 \) | \( d_1 = \mu \pi_p e_3, d_2 = \mu e_1, d_3 = e_2 \) |
|                       | \( \langle 1, \pi_p, \pi_p \rangle \), if \( \left( \frac{-1}{p} \right) = -1 \) | \( d_1 = \nu^{-1} \pi_p e_3, d_2 = \nu^{-1} e_1, d_3 = e_2 \) |
| \( \langle 1, \pi_p, \pi_p \rangle \) | \( \langle 1, \pi_p, \pi^2_p \rangle \) | \( d_1 = \pi_p e_2, d_2 = e_1, d_3 = e_3 \) |
|                       | \( \langle 1, \delta \pi_p, \pi^2_p \rangle \) | \( d_1 = \pi_p e_2, d_2 = e_1, d_3 = e_3 \) |
| \( \langle 1, \delta \pi_p, \pi^*_p \rangle \) | \( \langle 1, \pi_p, \pi^{*+1}_p \rangle \) | \( d_1 = \pi_p e_2, d_2 = e_1, d_3 = e_3 \) |
| \( \langle 1, \pi_p, \delta \pi^*_p \rangle \) | \( \langle 1, \pi_p, \delta \pi^{*+1}_p \rangle \) | \( d_1 = \pi_p e_2, d_2 = e_1, d_3 = e_3 \) |
| \( \langle 1, \pi_p, \delta \pi^*_p \rangle \) | \( \langle 1, \pi_p, \delta \pi^{*+1}_p \rangle \) | \( d_1 = \pi_p e_2, d_2 = \delta^{-1} e_1, d_3 = e_3 \) |
| \( \langle 1, \delta \pi_p, \delta \pi^*_p \rangle \) | \( \langle 1, \delta \pi_p, \delta \pi^{*+1}_p \rangle \) | \( d_1 = \delta \pi_p e_2, d_2 = \delta^{-1} e_1, d_3 = e_3 \) |

*Proof.* In each case, it is easy to check that the \( d_i \)'s satisfy equations (2.2) corresponding to \( g \), using that the \( e_i \)'s satisfy the equations corresponding to \( f \). \( \square \)
Remark 2.8. It can be proved that this construction is general, in the sense that every maximal suborder of $R_p$ can be obtained by the previous procedure, if we start with a suitable good basis of $R_p$.

Quasi-good bases. So far, given an order $R_p$, we must obtain a good basis of it to compute its suborders. This involves diagonalizing a ternary quadratic form over $\mathcal{O}_p$, which is not desirable from the computational point of view. Nevertheless, as we will show in this subsection by introducing the notion of quasi-good bases, this can be reduced to diagonalize the corresponding form modulo quasi-good bases.

Definition 2.9. Let $\mathcal{B} = \{1, e_1, e_2, e_3\}$ be a basis of $R_p$. 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 $R_p$ satisfying

$$\tilde{e}_i \equiv e_i \mod (pR_p) \quad (1 \leq i \leq 3).$$

Proposition 2.10. Let $\mathcal{B} = \{1, e_1, e_2, e_3\}$ be a quasi-good basis of an order $R_p$ 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

$$R'_p = \langle 1, d_1, d_2, d_3 \rangle \mathcal{O}_p$$

is a maximal suborder of $R_p$ 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 $R_p$ as in Definition 2.9. 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 $\Lambda_p = \langle 1, \tilde{d}_1, \tilde{d}_2, \tilde{d}_3 \rangle \mathcal{O}_p$. The table shows that $\tilde{d}_i \equiv d_i \mod (pR_p)$ for every $1 \leq i \leq 3$. Since $pR_p \subset \Lambda_p$, we have that

$$\Lambda_p = \langle 1, \tilde{d}_1, \tilde{d}_2, \tilde{d}_3 \rangle \mathcal{O}_p + pR_p \supset R'_p.$$  

Then, it suffices to see that $d(R'_p) = d(\Lambda_p)$ to complete the proof.

Let $e \in \{1, 2\}$ be such that $[R_p : \mathcal{A}_p] = p^e$. Following Table 2.2 case by case, it can be proved that $d(R'_p) = p^e d(R_p)$. Since $d(\Lambda_p) = p^e d(R_p)$, we are done. $\square$

Remark 2.11. Let $m = v_p(d(R'_p))$. 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 $\pi_p^{m+1}$, since in that case the ideal $d(\Lambda)$ remains unchanged.

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

Proposition 2.10 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 the order $R_p$, and let $\mathcal{E} = \{f_0, f_1, f_2, f_3\}$ be a basis of $R'_p$ satisfying (2.1). The existence of good bases implies that there exists $C \in GL_3(\mathcal{O}_p)$ such that $2ab \cdot C^t M_{\mathcal{E}} C = \text{diag}(1, a, b)$. Hence, $2ab \cdot M_{\mathcal{E}} \in M_3(\mathcal{O}_p)$ and $\det(M_{\mathcal{E}}) = 8^{-1}(ab)^{-2} u^2$ for some $u \in \mathcal{O}_p^\times$.

Proposition 2.12. Let $n = 2v_p(a) + 1$. Assume that $\mathcal{E}$ satisfies the following conditions.

1. There exists $\tilde{b} \in \mathcal{O}_p$ such that

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

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

Then, $E^1$ is a quasi-good basis of $R_p$.

Remark 2.13. The congruence in (1) is the really relevant hypothesis. If this
congruence is satisfied and $u \in O_p^+$ is such that $\det(M_p) = 8^{-1}(ab)^{-2}u^2$, then the basis
$\{f_0, f_1, f_2, u^{-1}f_3\}$ satisfies (1) and also (2).

The proof of Proposition 2.12 is based on the following lifting lemma.

Lemma 2.14. Let $r, m$ be nonnegative integers such that $m > 2r$, and let $A \in
M_3(O_p)$ be a symmetric matrix. Suppose that there exists $C \in GL_3(O_p)$ such that

$$C^tAC \equiv \text{diag}(\alpha, \beta, \gamma) \mod (M_3(p^nO_p)),$$

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

$$C'^tAC' \equiv \text{diag}(\alpha', \beta', \gamma') \mod (M_3(p^{m+1}O_p)),$$

with $\alpha' \equiv \alpha \mod (p^{m-r}O_p)$ and $\beta' \equiv \beta \mod (p^mO_p)$.

Proof. Write

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

with $a, b, \ldots, f \in O_p$. We claim that there exists a matrix $C_0 \in GL_3(O_p)$ such that

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

with $c', d', e', f' \in O_p$. 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 $-c\pi_p^r, -e\pi_p^r$ and $-b\pi_p^r$ at the (3, 1), (3, 2) and (2, 1) entries, respectively.

Let $C' = C + \pi_p^{m-r}C_0$. Then

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

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

Proof of Proposition 2.12. Let $r = v_p(a)$. By letting $m \to \infty$ in the previous
lemma, we get a matrix $C = (c_{ij}) \in GL_3(O_p)$ satisfying $C \equiv I \mod (M_3(p^{r+1}O_p))$ such that

$$2ab \cdot C^tM_pC = \text{diag}(\alpha, \beta, \gamma),$$

with $\alpha \equiv 1 \mod (\pi_p^{r+1})$ and $\beta \equiv a \mod (\pi_p^{2r+1})$. Using Hensel's lemma, take
$x_1, x_2 \in O_p^+$ satisfying $x_1 \equiv 1 \mod (\pi_p^{r+1})$ 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 $\tilde{C} = C \cdot \text{diag}(x_1, x_2, x_3)^{-1}$. Then $\tilde{C}$ satisfies that
$$2ab \cdot \tilde{C}^t M_\mathcal{E} \tilde{C} = \text{diag}(1, a, b).$$

Let $\tilde{f}_i = \sum_{j=1}^{3} \tilde{e}_{ij} f_j$, where $\tilde{C} = (\tilde{e}_{ij})$, let $\tilde{f}_0 = f_0$, and let $\tilde{E} = \{\tilde{f}_0, \tilde{f}_1, \tilde{f}_2, \tilde{f}_3\}$. Then $\tilde{E}^\dagger$ is a good basis of $R_p$, for $(2.3)$ is verified by $M_{\tilde{E}}$. The congruences satisfied by the $x_i$’s and $C$ imply that $\tilde{f}_i \equiv f_i \mod (pR_p^\dagger)$ for $1 \leq i \leq 3$. Hence $E^\dagger$ is a quasi-good basis of $R_p$, since Proposition 3.2 of [Brz82] gives that $4ab \cdot R_p^\dagger R_p^\dagger \subseteq R_p$. □

From local to global. Let $\Lambda$ be a lattice in $B$, and let $\Lambda'_p \subseteq \Lambda_p$ be a sublattice of index $p^e$, where $e$ is a nonnegative integer. Let $\Lambda' \subseteq B$ be the lattice given by
$$\Lambda'_q = \begin{cases} \Lambda_q & \text{if } q \neq p, \\
\Lambda'_p & \text{if } q = p. \end{cases}$$

Given a set of generators for $\Lambda$ as an $O$-module and a set of generators for $\Lambda'_p$ as an $O_p$-module, how can we construct a set of generators for $\Lambda'$ as an $O$-module?

Assume that $\Lambda = \langle v_1, v_2, \ldots, v_n \rangle_O$ and that $\Lambda'_p = \langle w_1, w_2, \ldots, w_n \rangle_{O_p}$. For each $i$ write $w_i = \sum_j a_{ij} v_j$, with $a_{ij} \in O_p$. There exist elements $b_{ij} \in O$ and $c_{ij} \in \pi_p O_p$ such that $a_{ij} = b_{ij} + c_{ij}$ (they can be constructed, for example, by looking at the $p$-adic expansion of the $a_{ij}$). Let $\tilde{w}_i = \sum_j b_{ij} v_j$.

Proposition 2.15. With the notation as above, we have
$$\Lambda' = p^e \Lambda + \langle \tilde{w}_1, \tilde{w}_2, \ldots, \tilde{w}_n \rangle_O.$$

Proof. It is enough to check that these two lattices coincide at all completions. Denote by $\Lambda''$ the lattice on the right-hand side.

- If $q \neq p$, then $\pi_p$ is a unit in $O_q$. So $p^e \Lambda_q = \Lambda_q$, which implies that $\Lambda'' = \Lambda + \langle \tilde{w}_1, \tilde{w}_2, \ldots, \tilde{w}_n \rangle_{O_q} = \Lambda_q$.
- Since $p^e \Lambda_p \subseteq \Lambda'_p$, we have that $\Lambda'' \subseteq \Lambda_p$; the reverse inclusion is deduced from the fact that $\tilde{w}_i \equiv w_i \mod (p^e \Lambda_p)$. □

Remark 2.16. Using the Hermite Normal Form algorithm (see [Coh00], Chapter I), for every lattice in $B$ we can compute a generating set over $O$ with at most five elements. In particular, this can be done for the sum describing $\Lambda'$, and we can assume that $\Lambda$ 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 Bass 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 $p$, the form $f_p$ corresponding to $R_p$, and a form $g_p$ beneath $f_p$. The algorithm, which we describe below, will return a Bass order $R' \subseteq R$ with $R'_q = R_q$ for all $q \neq p$, and such that $R'_p$ corresponds to $g_p$.

Algorithm 2.17. Step 1. Use Proposition 2.12 to find a quasi-good basis for $R_p$.
Step 2. Use Proposition 2.10 to construct a suborder $R'_p \subseteq R_p$ corresponding to the form $g_p$. 

Step 3. Use Proposition 2.15 to construct an order $R'$ such that

$$R'_q = \begin{cases} R_q & \text{if } q \neq p, \\ R'_p & \text{if } q = p. \end{cases}$$



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 of which orders are under consideration.

This definition was introduced in [PRV05], and later used in [PT07]. We will consider these sets for orders in $B$ as well as for their completions. Both cases can and will be treated in an unified way.

**Remark 3.2.** Identifying ideals with ideles, the set $\Psi(I)$ is simply the preimage of $I$ under the natural map

$$\hat{R}^\times \setminus \hat{B}^\times \rightarrow \hat{R}^\times \setminus \hat{B}^\times,$$

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

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 3.3.**

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

**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 $J_1 = J_2x$. Then

$$I_1 = RJ_1 = RJ_2x = I_2x.$$ 

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 3.4. 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 $q$ be a prime of $O$. Since $J_q \subseteq I_q$ we can write $I_q = R_q x_q$ and $J_q = R_q z_q x_q$, with $z_q \in R_q$. Then, $N(I_q) = N(J_q)$ if and only if $z_q \in R_q^x$, which is equivalent to the equality $R_q J_q = I_q$. These local facts imply the global statement. \hfill \Box

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

Proposition 3.5. 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, $\#([J] \cap \Psi(I)) = [R_r(I)^\times : R_r(J)^\times]$.

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 $I = R J_1 = R J_2 x = I x$. The other two statements are clear. \hfill \Box

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

Corollary 3.6.

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

In what follows, we describe two different methods for computing 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 $(R'_p)^\times \setminus R_p^\times$.

Proposition 3.7. Let $I_p \in I(R_p)$, say, $I_p = R_p x_p$. Then the map

$$(R'_p)^\times \setminus R_p^\times \to \Psi(I_p)$$

$$\alpha_p \mapsto R'_p(\alpha_p x_p)$$

is bijective.

Proof. This map is the composition of the maps

$$(R'_p)^\times \setminus R_p^\times \to \Psi(R_p), \quad \Psi(R_p) \to \Psi(I_p),$$

$$\alpha_p \mapsto R'_p \alpha_p, \quad J_p \mapsto J_p x_p.$$  

Both maps are bijective. This is clear for the second map. For the first one, this follows by Proposition 3.5 since all $R_p$-ideals are equivalent. \hfill \Box

Proposition 3.8. Suppose that $[R : R'] = p^e$ for some $e \geq 1$. Let $I \in I(R)$. The map

$$\Psi^R(I) \to \Psi^R_{R'}(I_p)$$

$$J \mapsto J_p$$

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

Proof. The fact that $I_q = J_q$ for all $q \neq p$ implies that the map is bijective. The equality follows from Proposition 3.7. \hfill \Box

These propositions imply immediately the following result.
Corollary 3.9. Suppose that $[R : R'] = p^e$ for some $e \geq 1$. Let $I \in I(R)$, and write $I_p = R_p x_p$. If $\{ \alpha_j \}$ is a system of representatives for $(R'_p)^* \setminus R_p^*$, then $\Psi^R_R(I) = \{ J_j \}$, where $J_j$ is locally given by

$$(J_j)_q = \begin{cases} I_q & \text{if } q \neq p, \\ R_p(\alpha_j x_p) & \text{if } q = p. \end{cases}$$

Remark 3.10. 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 a 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 3.11. Assume that $pR_p \subseteq R'_p$. Then, the natural map

$$\phi : (R'_p)^* \setminus R_p^* \longrightarrow (pR_p \setminus R'_p)^* \setminus (pR_p \setminus R_p)^*$$

is bijective.

Proof. Consider the ring morphism $\phi_1 : R_p \rightarrow pR_p \setminus R_p$. We claim that the induced group homomorphism $\phi_1 : R_p^* \rightarrow (pR_p \setminus R_p)^*$ is surjective. Indeed, let $[x] \in (pR_p \setminus R_p)^*$. Then there exist $y, z \in R_p$ such that $xy = 1 + \pi_p z$. Then $N(xy) \equiv 1 \mod (\pi_p)$, and hence $x \in R_p^*$ as claimed.

Compose $\phi_1$ with the map $p$ that projects $(pR_p \setminus R_p)^*$ onto the quotient set $(pR_p \setminus R'_p)^* \setminus (pR_p \setminus R_p)^*$. Then $p \circ \phi_1$ is surjective, and passes to the quotient set $(R'_p)^* \setminus R_p^*$ to give a surjective map $\phi : (R'_p)^* \setminus R_p^* \rightarrow (pR_p \setminus R'_p)^* \setminus (pR_p \setminus R_p)^*$.

We claim that $\phi$ is injective. Indeed, let $x, y \in R_p^*$ be such that $\phi(x) = \phi(y)$. Then, since $(R'_p)^* \rightarrow (pR_p \setminus R'_p)^*$ is also an epimorphism, we have $z \in (R'_p)^*$ and $w \in R_p$ such that $x = zy + \pi_p w$. Hence, $x = (z + \pi_p w y^{-1})y$, which shows that $[x] = [y] \in (R'_p)^* \setminus R_p^*$, since $\pi_p w y^{-1} \in pR_p \subseteq R'_p$ and hence $z + \pi_p w y^{-1} \in (R'_p)^*$. □

By Proposition 2.1 this result shows that, to give a system of representatives for the sets $(R'_p)^* \setminus R_p^*$ when $R'_p$ is a maximal suborder of $R_p$, 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 $R_p$, and assuming that $R'_p$ is obtained from $R_p$ by means of Algorithm 2.17, we proceed to give a system of representatives for the sets $(R'_p)^* \setminus R_p^*$, in terms of the form $g$ corresponding to $R'_p$.

The indexes $[R_p^* : (R'_p)^*]$ are well known in the Eichler case, and are computed in [Brz90] Theorems 3.3 and 3.10] in the remaining cases, so it will suffice to give in each case the correct number of non-equivalent units.

Let $g$ denote the order of the residue field $k_p$, and let $\{ a_1, a_2, \ldots, a_q \} \subseteq \mathcal{O}_p$ be a set of representatives for $k_p$ such that $a_1 = 1, a_2 = -1$ and $a_q = 0$. Let $\delta, \beta_0, \beta_1$ be as in Proposition 2.7. Finally, let $S = \{ \tilde{\gamma} \in k_p \times k_p : 1 - \delta \tilde{\gamma}_1^2 + \tilde{\gamma}_2^2 \neq 0 \}$, and for each $\tilde{\gamma} \in S$ let $\gamma \in \mathcal{O}_p \times \mathcal{O}_p$ be any lift of $\tilde{\gamma}$.

Proposition 3.12. With the previous notation, Table 3.1 gives a system of representatives for $(R'_p)^* \setminus R_p^*$.

Proof. According to Proposition 3.11 we may assume that $\mathcal{B}$ is a good basis, and it suffices to calculate a system of representatives for the set $(pR_p \setminus R'_p)^* \setminus (pR_p \setminus R_p)^*$.

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

We will discuss the details in a single case, namely when \(R_p\) has class A1 and \(R_p'\) has class B. The rest of the cases can be treated similarly.

Let \(x = x_0 + x_1e_1 + x_2e_2 + x_3e_3 \in pR_p \setminus R_p\). In these coordinates we have that the norm form is given by \(N(x) = x_0^2 - x_3^2\) (see (2.3)), and that \(x \in pR_p \setminus R_p'\) if and only if \(x_3 = 0\).

Hence, the elements of the form \(a_i + e_3\) belong to \((pR_p \setminus R_p')^\times\), if \(i \geq 3\). They are not equivalent modulo \((pR_p \setminus R_p')^\times\), since if
\[
(a_i + e_3)(x_0 + x_1e_1 + x_2e_2) = a_i x_0 + (a_i x_1 + x_2) e_1 + (a_i x_2 + x_1) e_2 + x_0 e_3 = a_j + e_3,
\]
then \(x_0 = 1\) and hence \(i = j\); they are not equivalent to 1, since they do not belong to \(pR_p \setminus R_p'\).

**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 \(\Lambda_I = \Lambda_{RI}\). For simplicity, we will just consider \(\Lambda = \Lambda_R\). It is clear that \(\Lambda \subseteq R'\) and \(R \subseteq R_\Lambda(\Lambda)\).

**Lemma 3.13.** The lattice \(\Lambda\) satisfies the following properties:

1. \(pR \subseteq \Lambda\), and hence \([R : \Lambda] \mid p^4\).
2. \(\Lambda \subseteq J\) for all \(J \in \Psi(R)\).

**Proof.** The inclusion in (1) follows from the fact that \(pR \subseteq R'\). The inclusion in (2) is clear if we consider the completion at primes \(q \neq p\), so we will look only at the completion at \(p\). Let \(J \in \Psi(R)\), and write \(J_p = R_p' u_p\) with \(u_p \in R_p^\times\). Then
\[
\alpha_p \in \Lambda_p \Rightarrow \alpha_p R_p \subseteq R_p' \Rightarrow \alpha_p u_p^{-1} \in R_p' \Rightarrow \alpha_p \in R_p' u_p = J_p.
\]

Since \(pR_p \subseteq R_p'\), we can consider \(R_p / R_p'\) as a \(k_p\)-vector space. When \(e = 2\), we can go further. Since in that case \(R_p'\) has class A2, the ring \(O_p + \sqrt{d}O_p\) embeds into \(R_p'\), and hence into \(R_p\). Then we can consider \(R_p / R_p'\) as a \(k_p\)-vector space, where \(k_p\) is the quadratic extension of \(k\) given by \(k_p = (O_p + \sqrt{d}O_p) / p(O_p + \sqrt{d}O_p)\).
Lemma 3.14.

1. If \( e = 1 \), then \( \dim_{k_p} (R_p/R'_p) = 1 \).
2. If \( e = 2 \), then \( \dim_{K_p} (R_p/R'_p) = 1 \).

Proof. It follows immediately from the fact that \( |R_p/R'_p| = q^e \). \( \square \)

Proposition 3.15. The lattice \( \Lambda \) satisfies that \( [R' : \Lambda] = p^e \), and hence \( [R : \Lambda] = p^{2e} \). In particular, if \( e = 2 \), then \( \Lambda = pR \).

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

\[
\psi : R'_p \to \text{End}(R_p/R'_p)
\]

\[
\alpha \mapsto (v \mapsto \alpha \cdot v).
\]

Its kernel is \( \Lambda_p \). The induced morphism \( \psi : R'_p/\Lambda_p \to \text{End}(R_p/R'_p) \) is easily seen to be also a \( k_p \)-vector space (respectively \( K_p \)-vector space) morphism when \( e = 1 \) (respectively \( e = 2 \)). Note that since \( 1 \not\in \Lambda_p \), it is not the null morphism. Hence, the result follows from the previous lemma. \( \square \)

Corollary 3.16. The set \( \Psi(I) \) is given by

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

Proof. When \( I = R \), the result follows immediately from Lemma 3.13 and Proposition 3.15. The arguments used for the general case are entirely analogous. \( \square \)

In particular, to calculate \( \Psi(I) \) (whose cardinality we already know by Proposition 3.8), we can limit ourselves to calculate the lattices between \( \Lambda_I \) 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 3.17. If \( e = 1 \), then \( [I : \Lambda_I] = p^2 \), 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 3.18. In the case \( e = 2 \), we know that the elements in \( \Psi(I) \) have a \((O_p + \sqrt{\delta}O_p)\)-module structure. If we only consider lattices between \( \Lambda_I \) 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. We assume that \( K \) is totally real and \( B \) is totally definite (i.e., \( B \) ramifies at every infinite place of \( K \)).

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 Bass 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 2.17 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 2.17.

By Proposition 3.15 it suffices to give an algorithm which calculates, for each $I \in S$, a set of representatives $S'_I$ for $[\Psi(I)]$, and then returns $S' = \bigcup_{I \in S} S'_I$.

The hypothesis of $K$ being totally real and $B$ being totally definite is used in Step 4.1, as we explain below. The algorithm works as follows.

Algorithm 3.19. Step 1. Using Proposition 3.12 compute a set of representatives for $(R'_p)^\times \setminus R'_p^\times$.
Step 2. Using Remark 3.10 find a local generator for $I_p$.
Step 3. Using Corollary 3.9 and Proposition 2.15 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 $R_p(J)^\times \setminus R_p(I)^\times$ act on $J$ (see Proposition 3.5).
Step 4.2. Set $S'_I = S'_I \cup \{J\}$. If $T \setminus [J] = \emptyset$, return $S'_I$. Else, let $T = T \setminus [J]$ and go to Step 4.1. □

We do not have a general method for, given $J \in \Psi(I)$, computing a system of representatives for the (finite) set $R_p(J)^\times \setminus R_p(I)^\times$ needed in Step 4.1; otherwise, the algorithm would work without the hypotheses on $K$ and $B$. Under these hypotheses, the set $O^\times \setminus R_p(I)^\times$ is finite and can be used as well to compute $[J] \cap \Psi(I)$.

The finiteness of the set $O^\times \setminus R_p(I)^\times$, as well as a method to compute it, can be obtained considering the exact sequence
\begin{equation}
1 \longrightarrow \{\pm 1\} \setminus R_p(I)^{\times,1} \longrightarrow O^\times \setminus R_p(I)^\times \xrightarrow{N} (O^\times)^2 \setminus O_+^\times,
\end{equation}
where $O_+^\times$ denotes the group of totally positive units of $O$. Assuming $B$ totally definite, the quadratic form $\text{Tr}_{K/\mathbb{Q}} \circ N : B \to \mathbb{Q}$ is positive definite, and hence the group $R_p(I)^{\times,1}$ is finite and can be calculated using lattice basis reduction algorithms. Furthermore, its possible group structures are known (see [Vig76]). The group $(O^\times)^2 \setminus O_+^\times$ 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 3.20. Since $R_p(J)^\times \subseteq R_p(I)^\times$ for every $J \in \Psi(I)$, when iterating the algorithm we need to apply the previous procedure to compute the sets $O^\times \setminus R_p(I)^\times$ only for the initial set of ideals.

Remark 3.21. We can compute $\Psi(I)$ by the global method given in Corollary 3.16 instead of using Steps 1, 2 and 3, although to our knowledge there is no advantage of one method over the other.

4. Example: The Consani-Scholten quintic

In this section we will show how we can use our method to compute ideal classes representatives for an Eichler order of discriminant 30 in the quaternion algebra ramified exactly 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 0.3 for details). In that article the algebra considered is ramified also at 2 and 3, since the Galois representation associated to the quintic has semistable reduction at those places. The representatives are constructed following the
method of Pizer (see [Piz80]), which involves searching 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 first make use of Theorem A to compute an Eichler order of discriminant 30 and then we make use of Theorem B to compute its left ideal classes 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).

**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 2.17 to construct a chain

\[
R(1) \supseteq R(2) \supseteq R(6) \supseteq R(6\sqrt{5}) \supseteq R(30),
\]

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

\[
R(1) = \left\{ \frac{1 + \omega^{-1}i + \omega j}{2}, \frac{\omega^{-1}i + j + \omega k}{2}, \frac{\omega + \omega^{-1}j + k}{2}, \frac{i + \omega j + \omega^{-1}k}{2} \right\}_{\mathcal{O}}.
\]

**Discriminant 2.** In this first step we use Algorithm 2.17 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

\[
\mathcal{B} = \{ 1, \frac{1}{2}(1 + \omega^{-1}i + \omega j), \frac{1}{2}(\omega i + \omega^{-1}j + k), \frac{1}{2}(i + \omega j + \omega^{-1}k) \}
\]

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

\[
\mathcal{B}^\vee = \{ f_0, \omega i - (1 + \omega)k, \frac{1}{2}((1 + \omega)i - j - \omega k), \frac{1}{2}(-(1 + 2\omega)i + \omega j + (1 + 3\omega)k) \},
\]

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

\[
\begin{align*}
f_1 &= \frac{1}{5}((2 + \omega)i - j - (1 + \omega)k), \\
f_2 &= \frac{1}{5}((1 + \omega)i - j + (6 + 11\omega)k), \\
f_3 &= \frac{1}{5}(-(47 + 88\omega)i + (11 + 26\omega)j + (43 + 32\omega)k),
\end{align*}
\]

the hypotheses of Proposition 5.5 are satisfied by \( \mathcal{E} = \{ f_0, f_1, f_2, f_3 \} \). Hence, letting

\[
\begin{align*}
e_1 &= \frac{1}{10}(-(232 + 384\omega) - (79 + 119\omega)i - (265 + 212\omega)j - (2 - 5\omega)k), \\
e_2 &= \frac{1}{10}(268 + 444\omega + (6 - 31\omega)i - (17 + 84\omega)j - (1 + \omega)k), \\
e_3 &= \frac{1}{10}(13 + 24\omega - (7 + 12\omega)i - (10 + 21\omega)j - k),
\end{align*}
\]

we get that \( \mathcal{E}^\perp = \{ 1, e_1, e_2, e_3 \} \) 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 2.8 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 $R(1)^{x}$, by Table 5.3), thus obtaining another quasi-good basis of $R(1)$2. Then Proposition 5.3 gives that $\{1, xe_1 x^{-1}, 2 \cdot xe_2 x^{-1}, xe_3 x^{-1}\}$ is a basis of $R(2)$2.

Step 3. Applying Proposition 2.15 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 Eichler order of discriminant 2. Note that the given basis is a basis for the classical maximal order in the quaternion algebra $(-1, -1)_\mathbb{Q}$.

Discriminant 6. Diagonalizing modulo 3 the quadratic form associated to $\{x \in R(2)_3^\vee : \text{Tr}(x) = 0\}$, using Proposition 2.12 we obtain that $\{1, \frac{1}{2}(i + j), \frac{1}{2}, 2(i - j)\}$ is a quasi-good basis for $R(2)_3$.

We use Table 2.2 to descend from $(1, -1, 1)$ to $(1, -1, 3)$, using $\alpha_0 = 2, \alpha_1 = -1$ as parameters, and we get that a basis for $R(6)_3$ is given by $\{1, 2 + j - k, -\frac{1}{2}(i + j) + k, 2(i - j)\}$. Using Proposition 2.15 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.

Discriminant $6\sqrt{5}$. The basis $\mathcal{E} = \{\frac{1}{2}, -i, -\frac{k}{2}, -\frac{j}{2}\}$ of $R(6)^{\sqrt{5}}_\mathcal{O}^{\vee}$ satisfies the hypotheses of Proposition 2.12 but with a stronger congruence in (1), namely mod $(\sqrt{5})^2$. This implies that the basis for $R(6\sqrt{5})^{\sqrt{5}}_\mathcal{O}^{\vee}$ obtained below is a quasi-good basis (see Remark 2.11).

We apply Table 2.2 using $\alpha_0 = 2 + \frac{\omega}{3}, \alpha_1 = -2$ as parameters, and obtain $\{1, -(1 + \frac{\omega}{3})i + 2k, i - (2 + \frac{\omega}{3})k, -2j\}$ as a basis for $R(6\sqrt{5})^{\sqrt{5}}_\mathcal{O}^{\vee}$. Then Proposition 2.15 gives

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

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 $R(30)^{\sqrt{5}}_\mathcal{O}^{\vee}$ obtained in this way is $\{1, -(\frac{34}{9} + \frac{31}{60}\omega)i + (\frac{303}{82} + \frac{34}{47}\omega)k, (\frac{303}{82} + \frac{34}{47}\omega)i - (\frac{68}{9} + \frac{34}{150}\omega)k, -2j\}$. Applying Proposition 2.15 we obtain

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

Constructing the ideals. We now proceed to compute ideal classes representatives for $R(30)$ iterating Algorithm 5.19 and using the quasi-good bases obtained above.

Before starting, note that equation (3.1) 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 $R(1)^{x,1} = E_{120}$, where $E_{120}$ is the binary icosahedral group. Using this explicit description we can avoid the use of lattice basis reduction algorithms. Furthermore, by Remark 3.20 this group contains all of the global units needed for our computations.
Discriminant 2. The calculation of \( \text{Cl}(R(2)) \) can be done without using the algorithm. Since \(|R(2)^{\times,1}| = 24\) and \(|R(1)^{\times,2}:R(2)^{\times,2}| = 5\) (see Table 5.3), Corollary 3.6 implies that \([\Psi^{R(1)}_{R(2)}(R(1))] = [R(2)]\), from which we conclude that \(R(2)\) has class number equal to 1 as well.

Discriminant 6. We now compute \(\text{Cl}(R(6))\), following Algorithm 3.19 closely. We have \(S = \{R(2)\}\) as input.

Step 1. To obtain a set of representatives for \([R(6)^{\times,3}\setminus R(2)^{\times,2}]\), 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 3.10 in this case.

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

\[
J = \left\{ i + (\omega - 1)k, j - (\omega + 1)k, 3k_1 + \frac{\omega}{2}(3 - i - j - 3k) \right\}.
\]

This result agrees with Corollary 3.6 since \(|R_r(I)^{\times,1}| = 6, |R_r(J)^{\times,1}| = 4\) and \(|R(2)^{\times,3}:R(6)^{\times,2}| = 10\).

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

Discriminant 6\(\sqrt{5}\). We compute \(\text{Cl}(R(6\sqrt{5}))\) 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 \(\Psi^{R(6)}_{R(6\sqrt{5})}(I) = \{I_1, \ldots, I_6\}\) and \(\Psi^{R(6)}_{R(6\sqrt{5})}(J) = \{J_1, \ldots, J_6\}\), where the notation is such that the \(n\)-th ideal corresponds to the \(n\)-th representative of \([R(6\sqrt{5})^{\times,3}\setminus R(6)^{\times,2}]\), following the labeling given in Table 5.3.
- The action of \(R_r(I)^{\times,1}\) on \(\Psi^{R(6)}_{R(6\sqrt{5})}(I)\) gives that \([\Psi^{R(6)}_{R(6\sqrt{5})}(I)] = \{[I_1], [I_4]\}\), and the action of \(R_r(J)^{\times,1}\) on \(\Psi^{R(6)}_{R(6\sqrt{5})}(J)\) gives that \([\Psi^{R(6)}_{R(6\sqrt{5})}(J)] = \{[J_1], [J_2], [J_3], [J_5]\}\) (see Table 4.1 for an explicit description of these ideals).

Hence, \(\text{Cl}(R(6\sqrt{5})) = \{[I_1], [I_4], [J_1], [J_2], [J_3], [J_5]\}\). This agrees with Corollary 3.6 since we have that \(|R_r(I_1)^{\times,1}| = |R_r(I_4)^{\times,1}| = |R_r(J_1)^{\times,1}| = |R_r(J_3)^{\times,1}| = 2, \text{ and } |R_r(J_2)^{\times,1}| = |R_r(J_5)^{\times,1}| = 4\).

Discriminant 30. Finally, we compute \(\text{Cl}(R(30))\).

- 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 \(\text{Cl}(R(6\sqrt{5}))\) were constructed using Corollary 3.9. They are \(1, 1 - \frac{3}{2}i + \frac{3}{2}k, 1, 1 - \frac{i}{4} + \frac{k}{2}, 1 - \frac{i}{2} + k\) and \(1 - i + 2k\) for \(I_1, I_4, J_1, J_2, J_3\) and \(J_5\), respectively.
Table 5.1. As in the case $p = (2)$, orders of class $A_1$ are the so-called Eichler orders.

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 ($\text{Vig80}$ Corollaire V.2.3)).

5. Appendix: The case $p = (2)$

If $p | (2)$, we can apply the same techniques used in the previous sections, but local Bass orders are described in terms of a different set of ternary quadratic forms. This set is described in $\text{Lem11}$ in the case $p = (2)$, i.e., if 2 is inert in $K/Q$, which is the case that we will consider in this appendix. The remaining cases are more involved, and remain to be studied.

Consider the matrices

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

Given $f, g$ quadratic forms, let $f \perp g$ denote their orthogonal sum. According to Propositions 5.8 and 5.12 of $\text{Lem11}$, 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 $p | (2)$, orders of class $A_1$ are the so-called Eichler orders.

In 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.
Table 4.2. Representatives for Cl(R(30)).

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

The notion of good basis must be extended to include the nondiagonal 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 $\mathcal{B} = \{e_1, e_2, e_3\}$ of $R_2$ as an $\mathcal{O}_2$-module
Table 5.1. Ternary quadratic forms in correspondence with local Bass orders, when $p = (2)$.

| 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     | $\langle 1, 1, 2^s \rangle$ | $s \geq 0, \delta_1 \in \{1, 3\}$ | $\delta_1 = 1$ | $-1$ |
| C     | $\langle 1, 6, 2^s \rangle$ | $s \geq 1, \delta_1 \in \{1, 3\}$ | $\delta_1 = 1$ | $(-1)^s$ |
| D     | $\langle 1, 5, 2^s \rangle$ | $s \geq 3, \delta_1 \in \{1, 3\}$ | $\delta_1 = 1$ | $(-1)^{s+1}$ |
| E     | $\langle 1, 2, 2^s \rangle$ | $s \geq 3, \delta_2 \in \{1, 5\}$ | $\delta_2 = 1$ | $-1$ |
| F     | $\langle 1, 14, 2^s \rangle$ | $s \geq 4, \delta_2 \in \{1, 5\}$ | $\delta_2 = 1$ | 1 |
| G     | $\langle 1, 10, 2^s \rangle$ | $s \geq 4, \delta_2 \in \{1, 5\}$ | $\delta_2 = 1$ | $(-1)^{s+1}$ |

is good if the $e_i$ satisfy

$$
\begin{align*}
e_1^2 &= 0, & e_1e_2 &= 2^s(1 - e_3), & e_2e_1 &= 2^s e_3, \\
e_2^2 &= 0, & e_2e_3 &= 0, & e_3e_2 &= e_2, \\
e_3^2 &= 2^s, & e_3e_1 &= 0, & e_1e_3 &= e_1;
\end{align*}
$$

(5.1)

respectively, if the $e_i$ satisfy

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

(5.2)

Note that in such bases the norm form is given by

$$
N(x) = \begin{cases} x_0^2 + x_0x_3 - 2^sx_1x_2, & f = H \perp \langle 2^s \rangle, \\
x_0^2 + x_0x_3 + x_3^2 - 2^sx_1x_2 + 2^sx_1^2 + 2^sx_2^2, & f = J \perp \langle 2^s \rangle. \end{cases}
$$

(5.3)

Remark 5.2. We can extend Remark 2.6 to nondiagonal forms as follows. Let $R_2$ be an order in correspondence with $f = H \perp \langle 2^s \rangle$, and let $B$ be a good basis of $R_2$. Then

$$
-2^s \cdot M_B^v = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2^{s+1} \end{pmatrix}.
$$
Proposition 5.3. 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 of the cases can be easily checked. Many of them follow from Propositions 5.8, 5.9 and 5.10 below (see the proof of Proposition 5.11).
Table 5.2. Construction of maximal suborders, in terms of good bases and ternary quadratic forms, when \( p = 2 \).

| Form          | Form beneath | Good basis for \( R'_2 \) |
|---------------|--------------|-----------------------------|
| \( H \perp \langle 1 \rangle \) | \( J \perp \langle 4 \rangle \) | \( d_1 = 2(\mu_1 - 2e_1 - 3e_2 - 2\mu_1e_3), \)  
\( d_2 = 2(-\mu + 3e_1 + 2e_2 + 2\mu_1e_3), \)  
\( d_3 = -2 - \mu_1e_1\mu_1e_2 + 5e_3 \) |
| \( H \perp \langle 2^* \rangle \) | \( H \perp \langle 2^{*+1} \rangle \) | \( d_1 = e_1, d_2 = 2e_2, d_3 = e_3 \)  
\( d_3 = -5 + 2\mu_1e_1 + \mu_1e_2 + 10e_3 \)  
\( d_4 = \mu_1 + 3e_1 + e_2 - 2\mu_1e_3 \) |
| \( H \perp \langle 2 \rangle \) | \( \langle 1, 1, 3 \rangle \) | \( d_1 = \mu_1 - e_1 + 2e_2 - 2\mu_1e_3, \)  
\( d_2 = -5 + 2\mu_1e_1 + \mu_1e_2 + 10e_3 \)  
\( d_3 = \mu_1 + 3e_1 + e_2 - 2\mu_1e_3 \) |
| \( J \perp \langle 2^* \rangle \) | \( J \perp \langle 2^{*+2} \rangle \) | \( d_1 = 2e_1, d_2 = 2e_2, d_3 = e_3 \)  
\( d_2 = -5 + 2\mu_1e_1 + \mu_1e_2 + 10e_3 \)  
\( d_3 = \mu_1 + 3e_1 + e_2 - 2\mu_1e_3 \) |
| \( J \perp \langle 2 \rangle \) | \( \langle 1, 1, 1 \rangle \) | \( d_1 = -5 + 2\mu_1e_1 + \mu_1e_2 + 10e_3 \)  
\( d_2 = -5 + 2\mu_1e_1 + \mu_1e_2 + 10e_3 \)  
\( d_3 = \mu_1 + 3e_1 + e_2 - 2\mu_1e_3 \) |
| \( \langle 1, 1, \delta, 2^* \rangle \) | \( \langle 1, 1, \delta, 2^{*+1} \rangle \) | \( d_1 = e_1 - e_2, d_2 = e_1 + e_2, d_3 = e_3 \) |
| \( \langle 1, 2, \delta, 2^* \rangle \) | \( \langle 1, 2, \delta, 2^{*+1} \rangle \) | \( d_1 = -2e_2, d_2 = e_1, d_3 = e_3 \) |
| \( \langle 1, 5, 2^* \rangle \) | \( \langle 1, 5, 3 \cdot 2^{*+1} \rangle \) | \( d_1 = e_1 - 5e_2, d_2 = e_1 + e_2, d_3 = e_3 \) |
| \( \langle 1, 6, 2^* \rangle \) | \( \langle 1, 6, 3 \cdot 2^{*+1} \rangle \) | \( d_1 = -6e_2, d_2 = e_1, d_3 = e_3 \) |
| \( \langle 1, 10, 2^* \rangle \) | \( \langle 1, 10, 5 \cdot 2^{*+1} \rangle \) | \( d_1 = -10e_2, d_2 = e_1, d_3 = e_3 \) |
| \( \langle 1, 1, 6 \rangle \) | \( \langle 1, 6, 6 \rangle \) | \( d_1 = 6e_3, d_2 = e_2, d_3 = -e_1 \) |
| \( \langle 1, 1, 2 \rangle \) | \( \langle 1, 6, 2 \rangle \) | \( d_1 = 2e_1 + 6e_3, d_2 = e_2, d_3 = 2e_3 - e_1 \) |
| \( \langle 1, 1, 2^* \rangle \) | \( \langle 1, 5, 3 \cdot 2^3 \rangle \) | \( d_1 = e_1 - 5e_2 + 4e_3, d_2 = e_1 + e_2 + 4e_3, \)  
\( d_3 = e_3 - e_1 \) |
| \( \langle 1, 14, \delta_2, 2^* \rangle \) | \( \langle 1, 14, \delta_2, 2^{*+1} \rangle \) | \( d_1 = e_1 - 14\mu_1e_2, d_2 = \mu_1e_1 + e_2, d_3 = e_3 \) |
| \( \langle 1, 5, 3 \cdot 2^* \rangle \) | \( \langle 1, 5, 2^{*+1} \rangle \) | \( d_1 = e_1 - 5\mu_2e_2, d_2 = \mu_2e_1 + e_2, d_3 = e_3 \) |
| \( \langle 1, 10, 5 \cdot 2^* \rangle \) | \( \langle 1, 10, 2^{*+1} \rangle \) | \( d_1 = -10\frac{1}{5}e_2, d_2 = \frac{1}{5}e_1, d_3 = e_3 \) |
| \( \langle 1, 6, 3 \cdot 2^* \rangle \) | \( \langle 1, 6, 2^{*+1} \rangle \) | \( d_2 = \frac{1}{3}e_1 + 2e_2, d_3 = e_3 \) |
| \( \langle 1, 6, 3 \cdot 2^2 \rangle \) | \( \langle 1, 2, 2^3 \rangle \) | \( d_1 = 6 \frac{1}{3}(-\mu_3e_2 + 2e_3), d_2 = \frac{1}{3}e_1, \)  
\( d_3 = e_2 + \mu_3e_3 \) |
| \( \langle 1, 2, 2^3 \rangle \) | \( \langle 1, 1, 2^4 \rangle \) | \( d_1 = -2e_2 + 8e_3, d_2 = e_1, d_3 = e_2 + 5e_3 \) |
| \( \langle 1, 2, 5 \cdot 2^3 \rangle \) | \( \langle 1, 10, 5 \cdot 2^4 \rangle \) | \( d_1 = -2\mu_3e_2 + 40e_3, d_2 = e_1, \)  
\( d_3 = e_2 + \mu_3e_3 \) |
| \( \langle 1, 6, 3 \cdot 2^3 \rangle \) | \( \langle 1, 14, 2^3 \rangle \) | \( d_1 = 6 \frac{1}{3}(-\mu_3e_2 + 4e_3), d_2 = \frac{1}{3}e_1, \)  
\( d_3 = e_2 + \mu_3e_3 \) |
| \( \langle 1, 6, 2^2 \rangle \) | \( \langle 1, 2, 5 \cdot 2^3 \rangle \) | \( d_1 = 2(\mu_5e_1 - 3\mu_5e_2 - 10e_3), \)  
\( d_2 = e_1 + 2e_2, d_3 = e_1 - 3e_2 + \mu_5e_3 \) |
| \( \langle 1, 6, 2^3 \rangle \) | \( \langle 1, 14, 5 \cdot 2^4 \rangle \) | \( d_1 = 2(\mu_5e_1 - 3\mu_5e_2 - 60e_3), \)  
\( d_2 = e_1 + 2e_2, d_3 = 3e_1 - 9e_2 + \mu_6e_3 \) |

The notion of quasi-good basis remains unchanged, as well as the use of such bases for computing suborders and representatives for the quotients \((R'_2)^\times \setminus R'_2^\times\). We must show how to obtain quasi-good bases in this setting.

Remark 5.4. Proposition 2.12 still holds for diagonal forms, setting \( n = 3\nu_2(a) + 2 \) in order to be able to use Hensel’s lemma in its proof.
Proposition 5.5. Let $R_2$ be an order in correspondence with $f = H \perp \langle 2^s \rangle$. Let $E = \{f_0, f_1, f_2, f_3\}$ be a basis of $R_2^3$ satisfying (2.1). Assume that $E$ satisfies the following conditions.

1. There exists $\beta \in O_2$ such that

$$-2^s \cdot M_E \equiv \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \beta \\ 1 & 0 & 0 \end{pmatrix} \pmod{(M_3(2^3O_2))}.$$

2. $\det(M_E) = 2^{1-2s}$.

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

The following lifting lemma is needed in the proof of Proposition 5.5, which we omit, since it is quite similar to the proof of Proposition 2.12.

Lemma 5.6. Let $m$ be an integer such that $m \geq 3$, and let $A \in M_3(O_2)$ be a symmetric matrix. Assume that there exists $C \in GL_3(O_2)$ such that

$$C^t AC \equiv \begin{pmatrix} 0 & \alpha & 0 \\ \alpha & 0 & 0 \\ 0 & 0 & \beta \end{pmatrix} \pmod{(M_3(2^mO_2))},$$

with $v_2(\alpha) = 0$.

Then, there exists $C' \in GL_3(O_2)$ satisfying $C' \equiv C \pmod{(M_3(2^{m-1}O_2))}$ such that

$$C'^t AC' \equiv \begin{pmatrix} 0 & \alpha' & 0 \\ \alpha' & 0 & 0 \\ 0 & 0 & \beta' \end{pmatrix} \pmod{(M_3(2^{m+1}O_2))},$$

with $\alpha' \equiv \alpha \pmod{(2^{m-1}O_2)}$.

Proof. Write

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

with $a, b, \ldots, f \in O_2$. We claim that there exists a matrix $C_0 \in GL_3(O_2)$ such that

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

with $b', c', d', e', f' \in O_2$. This can be shown by performing row operations on $C^t AC$, 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

$$C'^t AC' = \begin{pmatrix} 0 & \alpha' & c'2^{m-1} \\ \alpha' & 0 & \beta' \\ c'^{2^{m-1}} & \beta' & 0 \end{pmatrix} + 2^{2(m-1)}C_0^t AC_0,$$

where $\alpha' = \alpha + 2^{m-1}(b' + d')$. Since $2(m - 1) \geq m + 1$, we are done. \qed
For orders of class A2 we only state the corresponding analogue of Proposition 5.8.

**Proposition 5.7.** 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 \( R_2^\perp \) satisfying (2.11). Assume that \( \mathcal{E} \) satisfies the following conditions.

1. There exists \( \beta \in \mathcal{O}_2 \) such that
   \[
   2^s 3 \cdot M_\mathcal{E} \equiv \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & \beta \end{pmatrix} \mod (M_3(2^3 \mathcal{O}_2)).
   \]

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

Let \( e_i = 2^s \cdot f_j f_k \), 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 \((R_2')^\times \setminus R_2^\times\) when \( R_2' \) is a maximal suborder of \( R_2 \) obtained using Algorithm 2.17.

We start by stating three general results which, though only used when \( p = 2 \), hold without restrictions on \( p \).

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 5.8.** 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 \( \alpha_0^3 + a\alpha_3^2 = \lambda \). 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 \( R_2'' \) is \( q \), and a set of representatives for the set \((R_2')^\times \setminus R_2^\times\) 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 3.11. Since \( v_2(b) \geq 1 \), by (2.3) the norm form on \( 2R_2' \setminus R_2 \) is given by \( N(x) = x_0^2 + ax_2^2 \). Hence, \( |(2R_2' \setminus R_2')^\times| = c q^2 \), where \( c = \# \{(x_0, x_3) \in k_2 \times k_2 : x_0^2 + ax_2^2 \neq 0\} \).

We have that
\[
2R_2' \setminus R_2' = \{ x \in 2R_2' \setminus R_2 : x_0, x_3 \in k_2, (x_1, x_2) \in A(k_2 \times k_2) \},
\]
where \( A \in \text{End}_{k_2}(k_2 \times k_2) \) is the morphism given by left multiplication by \( (\alpha_0, \alpha_3, 0) \). Since \( \alpha_0^3 + a\alpha_3^2 = \lambda \) and \( v_2(\lambda) = 1 \), this matrix has rank 1. Hence, \( |(2R_2' \setminus R_2')^\times| = c q \), which shows that \( \text{ord}(2R_2') = 2 \) is \( q \).

To see that the given units are not equivalent, take \( x \in (2R_2' \setminus R_2')^\times \). Then, it is easy to see that
\[
(1 + a_i e_2)x = x_0 + (x_1 - a_i x_2 x_3)e_1 + (a_i x_0 + x_2)e_2 + x_3 e_3 = 1 + a_j e_2
\]
implies that \( i = j \). \( \square \)

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

**Proposition 5.9.** 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 \( \alpha_0^3 + b\alpha_2^2 = \mu \). Let \( v = \alpha_0 + \alpha_2 e_2 \), and let \( d_1 = ve_1, d_2 = e_2, d_3 = ve_3 \).
Then, $R_2' = \langle 1, d_1, d_2, d_3 \rangle_{O_2}$ 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 $(R_2')^\times \setminus R_2^\times$ is given by $\{1 + a_i e_3 : 1 \leq i \leq q\}$.

**Proposition 5.10.** Suppose that $R_2$ is in correspondence with the form $f = \langle 1, a, b \rangle$. Let $a', b' \in O_2$. Assume that there exist $\alpha_1, \alpha_2, \alpha_3 \in O_2$ such that $a b \alpha_1^2 = b'$, and $a a_3^2 + b \alpha_2^2 = a'$. Let $d_2 = \alpha_1 e_1, d_3 = \alpha_2 e_2 + \alpha_3 e_3, d_1 = d_3 d_2$.

Then $R_2' = \langle 1, d_1, d_2, d_3 \rangle_{O_2}$ 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 $(R_2')^\times \setminus R_2^\times$ 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 5.11.** Let $B = \{1, e_1, e_2, e_3\}$ be a quasi-good basis of $R_2$, and assume that $R_0'$ is a maximal suborder of $R_2$ that has been built using Algorithm 2.17. Then Table 5.3 gives the index of $(R_2')^\times$ in $R_2^\times$ and a system of representatives for the quotient set.

**Table 5.3.** The indexes $[R_2^\times : (R_2')^\times]$ and representatives for $(R_2')^\times \setminus R_2^\times$.

| $R_2$-class | $R_2'$-class | $[R_2^\times : (R_2')^\times]$ | Representatives | Condition |
|-------------|-------------|-------------------------------|-----------------|-----------|
| A1          | A1          | $q + 1$                       | $e_1 + e_2, 1 + a_i e_2$ (1 ≤ i ≤ q) | $s = 0$ |
|             | A2          | $q(q - 1)$                    | $(1 + a_i e_2)(e_1 + a_j e_2)$ (1 ≤ i, j ≤ q, a_i ≠ 0) | odd |
|             |             | $q(q + 1)$                    | $(1 + a_i e_2)(e_1 + a_j e_2)$ (1 ≤ i, j ≤ q, a_i ≠ 0), $(1 + a_i e_2)(a_j + e_1)$ (1 ≤ i ≤ q, q - 2 ≤ j ≤ q) | even |
| B           | B           | $q - 1$                       | $1 + a_i e_2$ (1 < i ≤ q) | |
|             | A2          | $q^2$                         | $1 + a_i e_1 + a_j e_2$ (1 ≤ i, j ≤ q) | even |
|             | B           | $q - 1$                       | $e_3, 1 + a_i e_3$ (1 ≤ i ≤ q - 2) | even |
|             |             | $q + 1$                       | $e_3, 1 + a_i e_3$ (1 ≤ i ≤ q) | odd |
| B           | B           | $q$                           | $e_2, 1 + a_i e_2$ (1 < i ≤ q) | $s = 0$ |
|             |             | $q$                           | $1 + a_i e_2$ (1 ≤ i ≤ q) | $s \geq 1$ |
| C           | C           | $q$                           | $1 + a_i e_3$ (1 ≤ i ≤ q) | |
| D           | D           | $q$                           | $1 + a_i e_2$ (1 ≤ i ≤ q) | |
| E           | E           | $q$                           | $1 + a_i e_2$ (1 ≤ i ≤ q) | $\delta_1 = 1$ |
|             | F           | $q$                           | $1 + a_i e_3$ (1 ≤ i ≤ q) | $\delta_1 = 3$ |
|             | F           | $q$                           | $1 + a_i e_2$ (1 ≤ i ≤ q) | $\delta_1 = 1$ |
|             | G           | $q$                           | $1 + a_i e_3$ (1 ≤ i ≤ q) | $\delta_1 = 3$ |
|             | G           | $q$                           | $1 + a_i e_2$ (1 ≤ i ≤ q) | |
Proof. As in the case of \( p \mid 2 \), by Proposition 3.11 we may assume that \( \mathcal{B} \) is a good basis for \( R_2 \), and we can perform all calculations modulo \( 2R_2 \).

The cases \( \mathcal{B} \to \mathcal{B}, \mathcal{C} \to \mathcal{C}, \mathcal{D} \to \mathcal{D}, \mathcal{E} \to \mathcal{E}, \mathcal{F} \to \mathcal{F} \) and \( \mathcal{G} \to \mathcal{G} \) are covered by Proposition 5.8. The case \( \mathcal{B} \to \mathcal{C} \) is covered by Proposition 5.9.

To prove the case \( \mathcal{B} \to \mathcal{D} \), use Proposition 5.9 to descend from \( \langle 1, 1, 2^2 \rangle \) to \( \langle 1, 5, 2^2 \rangle \), and Proposition 5.8 to descend from this form to \( \langle 1, 5, 3 \cdot 2^3 \rangle \). A similar argument works for the other forms of class \( \mathcal{B} \).

The cases \( \mathcal{C} \to \mathcal{E} \) (with \( \delta_1 = 3 \)), \( \mathcal{C} \to \mathcal{F} \) (with \( \delta_1 = 3 \)) and \( \mathcal{E} \to \mathcal{G} \) are covered by Proposition 5.10.

Now we will prove the case from \( A_2 \to \mathcal{B} \). The remaining cases can be treated in a similar way, with no further difficulties.

By (5.3), the norm form on \( 2R_2 \setminus R_2 \) is given by \( N(x) = x_0^2 + x_0x_3 + x_3^2 \). Hence, a standard calculation shows that

\[
|\langle 2R_2 \setminus R_2 \rangle^x| = \begin{cases} q^3 - q^2(2q - 1), & \text{if } r \text{ is even}, \\ q^3 - q^2, & \text{if } r \text{ is odd}. \end{cases}
\]

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

Now we need to find the right amount of nonequivalent units. It is easily seen that the elements in the set \( \{1 + a_i e_3 : 1 \leq i \leq q\} \cup \{e_3\} \) are not mutually equivalent modulo \( \langle 2R_2 \setminus R_2 \rangle^x \), and they are all units, except for \( 1 + a_{q-1} e_3 \) and \( 1 + a_q e_3 \) when \( q = 2^s \) with even \( s \).

\[\square\]

Acknowledgments

The authors would like to thank Gonzalo Tornaría and Lassina Dembélé for the useful conversations we held with them. Also, the authors would like to thank the referee for useful suggestions and corrections that we received.

References

[Brz82] Juliusz Brzeziński, *A characterization of Gorenstein orders in quaternion algebras*, Math. Scand. **50** (1982), no. 1, 19–24. MR0645044 (83i:16009)

[Brz83] Juliusz Brzeziński, *On orders in quaternion algebras*, Comm. Algebra **11** (1983), no. 5, 501–522, DOI 10.1080/00927878308822861. MR0693798 (85c:16011)

[Brz90] Juliusz Brzeziński, *On automorphisms of quaternion orders*, J. Reine Angew. Math. **403** (1990), 166–186, DOI 10.1515/crll.1990.403.166. MR1030414 (90m:11182)

[Coh00] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR1728313 (2000k:11144)

[CS01] Caterina Consani and Jasper Scholten, *Arithmetic on a quintic threefold*, Internat. J. Math. **12** (2001), no. 8, 943–972, DOI 10.1142/S0129167X01001118. MR1863287 (2002h:11058)

[DD08] Lassina Dembélé and Steve Donnelly, *Computing Hilbert modular forms over fields with nontrivial class group*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., 5011 Springer, Berlin, 2008, 371–386. MR2467859 (2010d:11149)

[EMP86] H. M. Edgar, R. A. Mollin, and B. L. Peterson, *Class groups, totally positive units, and squares*, Proc. Amer. Math. Soc. **98** (1986), no. 1, 33–37, DOI 10.2307/2045762. MR848870 (87i:11166)

[GL09] Benedict H. Gross and Mark W. Lucianovic, *On cubic rings and quaternion rings*, J. Number Theory **129** (2009), no. 6, 1468–1478, DOI 10.1016/j.jnt.2008.06.003. MR2521487 (2010b:11044)

[Kap69] Irving Kaplansky, *Submodules of quaternion algebras*, Proc. London Math. Soc. (3) **19** (1969), 219–232. MR0240142 (39 #1496)
Markus Kirschmer and John Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput. **39** (2010), no. 5, 1714–1747, DOI 10.1137/080734467. MR2592031 (2011c:11171)

Stefan Lemurell, *Quaternion orders and ternary quadratic forms*, 2011, [http://arxiv.org/abs/1103.4922](http://arxiv.org/abs/1103.4922).

Arnold Pizer, *On the arithmetic of quaternion algebras. II*, J. Math. Soc. Japan **28** (1976), no. 4, 676–688. MR0432600 (55 #5587).

Arnold Pizer, *An algorithm for computing modular forms on \( \Gamma_0(N) \)*, J. Algebra **64** (1980), no. 2, 340–390, DOI 10.1016/0021-8693(80)90151-9. MR579066 (83g:10020).

Ariel Pacetti and Fernando Rodriguez Villegas, [http://www.ma.utexas.edu/users/villegas/cnt/cnt.html](http://www.ma.utexas.edu/users/villegas/cnt/cnt.html).

Ariel Pacetti and Fernando Rodriguez Villegas, *Computing weight 2 modular forms of level \( p^2 \)*, Math. Comp. **74** (2005), no. 251, 1545–1557 (electronic), DOI 10.1090/S0025-5718-04-01709-0. With an appendix by B. Gross. MR2137017 (2006a:11053).

Ariel Pacetti and Gonzalo Tornarà, *Shimura correspondence for level \( p^2 \) and the central values of L-series*, J. Number Theory **124** (2007), no. 2, 396–414, DOI 10.1016/j.jnt.2006.10.011. MR2232170 (2008e:11055).

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

Jude Socrates and David Whitehouse, *Unramified Hilbert modular forms, with examples relating to elliptic curves*, Pacific J. Math. **219** (2005), no. 2, 333–364, DOI 10.2140/pjm.2005.219.333. MR2175121 (2007c:11059).

Marie-France Vignéras, *Simplification pour les ordres des corps de quaternions totalement définis*, J. Reine Angew. Math. **286/287** (1976), 257–277. MR0429841 (55 #2851).

Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980 (French). MR580949 (82i:12016).

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