IDENTIFYING THE MATRIX RING: ALGORITHMS FOR QUATERNION ALGEBRAS AND QUADRATIC FORMS

JOHN VOIGHT

Abstract. We discuss the relationship between quaternion algebras and quadratic forms with a focus on computational aspects. Our basic motivating problem is to determine if a given algebra of rank 4 over a commutative ring R embeds in the 2×2-matrix ring $\mathrm{M}_2(R)$ and, if so, to compute such an embedding. We discuss many variants of this problem, including algorithmic recognition of quaternion algebras among algebras of rank 4, computation of the Hilbert symbol, and computation of maximal orders.

Since the discovery of the division ring of quaternions over the real numbers by Hamilton, and continuing with work of Albert and many others, a deep link has been forged between quadratic forms in three and four variables over a field F and quaternion algebras over F. Starting with a *quaternion algebra* over F, a central simple F-algebra of dimension 4, one obtains a quadratic form via the reduced norm (restricted to the trace zero subspace); the split quaternion algebra over F, the 2×2-matrix ring $\mathrm{M}_2(F)$, corresponds to an isotropic quadratic form, one that represents zero nontrivially. (Conversely, one recovers the quaternion algebra via the Clifford algebra of the quadratic form.) In this article, we give an exposition of this link relating quaternion algebras and quadratic forms from an explicit, algorithmic perspective and in a wider context.

Let R be a noetherian, commutative domain. We say that R is *computable* if there exists an encoding of R into bits with algorithms to perform ring operations in R and to test if an element of R is zero. The following basic algorithmic problem, along with its many variants, forms the core of this article. (See §1 for further definitions and algorithmic specifications.)

Problem (IsMatrixRing)**.** *Given a computable domain R and an R-algebra $\mathcal{O}$ of rank 4, determine if $\mathcal{O}$ embeds in $\mathrm{M}_2(R)$ and, if so, compute an explicit embedding $\mathcal{O} \hookrightarrow \mathrm{M}_2(R)$ of R-algebras.*

The problem (IsMatrixRing) captures in an important way the link between quadratic forms and quaternion algebras. In the simplest case where $R = F$ is a field—when such an embedding is necessarily an isomorphism—this problem corresponds to asking if a ternary quadratic form over F represents zero nontrivially, and for this reason it arises in a wide variety of situations. When F is a local field, this problem corresponds to the computation of the Hilbert symbol. In the case where R is a local ring, it corresponds to the computation of an (explicit) integral splitting of a quaternion order and thereby appears as a foundational step in many

Date: June 5, 2013.

1991 *Mathematics Subject Classification.* Primary 11R52; Secondary 11E12.

Key words and phrases. Quadratic forms, quaternion algebras, maximal orders, algorithms, matrix ring, number theory.

algorithms in arithmetic geometry (as in work of Kirschmer and the author [18]). Finally, when R is a Dedekind domain, roughly speaking, the problem of approximating (IsMatrixRing) naturally gives rise to the problem of computing a maximal order containing $\mathcal{O}$. In these and other ways, therefore, the problem (IsMatrixRing) will serve as kind of unifying and motivating question.

In §1, we introduce the basic terminology we will use throughout concerning computable rings and quaternion algebras. In §2, we consider algebras equipped with a standard involution and we exhibit an algorithm to test if an F-algebra B has a standard involution. In §3, we relate algebras with a standard involution to quadratic forms via the reduced norm; we introduce the theory of quadratic forms over local PIDs, providing an algorithm to compute a *normalization* of such a form. As a consequence, we exhibit an algorithm to test if an F-algebra B is a quaternion algebra and, if so, to compute *standard generators* for B. With these reductions, we turn in §4 to Problem (IsMatrixRing) for quaternion algebras and prove that this problem is deterministic polynomial-time equivalent to the problem of determining if a conic defined over F has an F-rational point (and, if so, to exhibit one).

In §5, we consider Problem (IsMatrixRing) in the case where F is a local field, which corresponds to the computation of the Hilbert symbol; in §6 we treat the more delicate case of a local dyadic field, and putting these together prove that there is a deterministic polynomial-time algorithm to compute the Hilbert symbol (Theorem 6.1). We thereby exhibit an algorithm to compute the generalized Jacobi symbol for computable Euclidean domains. In §7, we turn to the case of a Dedekind domain R and relate Problem (IsMatrixRing) to the problem of computing a maximal R-order; we prove that the problem of computing a maximal order for a quaternion algebra B over a number field F is probabilistic polynomial-time equivalent to the problem of factoring integers. Finally, in §8, we consider the problem (IsMatrixRing) over $\mathbb{Q}$, and show that recognizing the matrix ring is deterministic polynomial-time equivalent to the problem of quadratic residuosity.

Many of the results in this paper fit into the more general setting of semisimple algebras; however, we believe that the special link to quadratic forms, along with the wide application of quaternion algebras (analogous to that of quadratic field extensions), justifies the specialized treatment they are afforded here.

The author would like to thank his Ph.D. advisor Hendrik Lenstra for his many helpful comments, the Magma group at the University of Sydney for their support while writing this paper, and David Kohel for his valuable input. We are indebted to Carl Pomerance for the citation [2] and would like to thank Asher Auel, Jonathan Hanke, Kate Thompson, and the referee for helpful corrections and suggestions. Some of the results herein occur in the author's Ph.D. thesis [39]. Writing this paper was partially supported by the National Security Agency under Grant Number H98230-09-1-0037 and the National Science Foundation under Grant No. DMS-0901971.

1. Rings and algebras

We begin by introducing some notation and background that will be used throughout. Let R be a commutative, noetherian domain (with 1), and let F be the field of fractions of R.

Let $\mathcal{O}$ be an *R-algebra*, an associative ring with 1 equipped with an embedding $R \hookrightarrow \mathcal{O}$ of rings (taking $1 \in R$ to $1 \in \mathcal{O}$) whose image lies in the center of $\mathcal{O}$; we identify R with its image under this embedding. We will assume without further mention that $\mathcal{O}$ is a finitely generated, projective (equivalently, locally free) R-module of rank $n \in \mathbb{Z}_{\geq 1}$.

Computable rings and algebras. We will follow the conventions of Lenstra [22] for rings and algorithms, with the notable exception that we do not require all rings to be commutative.

A domain R is *computable* if R comes equipped with a way of encoding elements of R in bits (i.e. the elements of R are recursively enumerable, allowing repetitions) along with deterministic algorithms to perform ring operations in R (addition, subtraction, and multiplication) and to test if $x = 0 \in R$; a ring is *polynomial-time computable* if these algorithms run in polynomial time (in the bit size of the input). A field is *computable* if it is a computable ring and furthermore there exists an algorithm to divide by a nonzero element. For precise definitions and a thorough survey of the subject of computable rings we refer to Stoltenberg-Hansen and Tucker [34] and the references contained therein.

Example 1.1. A domain R which is the localization of a ring which is finitely generated over its prime ring is computable by the theory of Gröbner bases [13]. For example, any finitely generated algebra over $\mathbb{Z}$ or $\mathbb{Q}$ (without zerodivisors, since we restrict to domains) is computable, and in particular the coordinate ring of any integral affine variety over a finitely generated field is computable.

Example 1.2. If R is a computable domain, then F is a computable field if elements are represented in bits as pairs of elements of R in the usual way.

Remark 1.3. Inexact fields (e.g. local fields, such as $\mathbb{Q}_p$ or $\mathbb{R}$) are not computable, since they are uncountable! However, see the discussion in §5 for the use of a computable subring which works well in our situation.

Example 1.4. A number field F is computable, specified by the data of the minimal polynomial of a primitive element (itself described by the sequence of its coefficients, given as rational numbers); elements of F are described by their standard representation in the basis of powers of the primitive element [6, §4.2.2]. For a detailed exposition of algorithms for computing with a number field F, see Cohen [6, 7] and Pohst and Zassenhaus [27].

Remark 1.5. *Global function fields*, i.e. finite extensions of $k(T)$ with k a finite field, can be treated in a parallel fashion to number fields. Unfortunately, at the present time the literature is much less complete in providing a suite of algorithms for computing with integral structures in such fields—particularly in the situation where one works in a relative extension of such fields—despite the fact that some of these algorithms have already been implemented in Magma [3] by Hess [14]. Therefore, in this article we will often consider just the case of number fields and content ourselves to notice that the algorithms we provide will generalize with appropriate modifications to the global function field setting.

Throughout this article, when discussing algorithms, we will assume that the domain R and its field of fractions F are computable.

Let B be a F-algebra with $\dim_F B = n$ and basis $e_1, e_2, \dots, e_n$ (as an F-vector space), and suppose $e_1 = 1$. A *multiplication table* for B is a system of n^3 elements

$(c_{ijk})_{i,j,k=1,\dots,n}$ of F, called *structure constants*, such that multiplication in B is given by

$$e_i e_j = \sum_{k=1}^{n} c_{ijk} e_k$$

for $i, j \in \{1, \dots, n\}$.

An F-algebra B is represented in bits by a multiplication table and elements of F are represented in the basis e_i. Note that basis elements in B can be multiplied directly by the multiplication table but multiplication of arbitrary elements in B requires $O(n^3)$ arithmetic operations (additions and multiplications) in F; in either case, note the output is of polynomial size in the input for fixed B.

Remark 1.6. We have assumed that B is associative as an F-algebra; however, this property can be verified by simply checking the associative law on a basis.

Remark 1.7. We require that the element 1 be included as a generator of B, since by our definition an F-algebra is equipped with an embedding $F \hookrightarrow B$. This is not a serious restriction, for the equations which uniquely define the element 1 in B are linear equations and so $1 \in B$ can be (uniquely) recovered by linear algebra over F. (And an algebra without 1 embeds inside an algebra with 1.)

An R-algebra $\mathcal{O}$ is represented in bits by the F-algebra $B = \mathcal{O} \otimes_R F$ and a set of R-module generators $x_1, \dots, x_m \in B$ with $x_1 = 1$. A morphism between R-algebras is represented by the underlying R-linear map, specified by a matrix in the given sets of generators for the source and target.

Quaternion algebras. We refer to Vignéras [38] and Reiner [28] for background relevant to this section.

An F-algebra B is *central* if the center of B is equal to F, and B is *simple* if the only two-sided ideals of B are (0) and B (or equivalently that any F-algebra homomorphism with domain B is either the zero map or injective).

Remark 1.8. One can compute the center of B by solving the n linear equations $xe_i = e_i x$ for $x = x_1 e_1 + \dots + x_n e_n$ and thereby, for example, verify that B is central.

Definition 1.9. A *quaternion algebra* B over F is a central simple F-algebra with $\dim_F B = 4$.

An F-algebra B is a quaternion algebra if and only if there exist $i, j \in B$ which generate B as an F-algebra such that

$$i^2 = a, \quad j^2 = b, \quad ji = -ij \tag{1.10}$$

with $a, b \in F^\times$ if $\operatorname{char} F \neq 2$, and

$$i^2 + i = a, \quad j^2 = b, \quad ji = (i+1)j \tag{1.11}$$

with $a \in F$ and $b \in F^\times$ if $\operatorname{char} F = 2$. We give an algorithmic proof of this equivalence in §3. We accordingly denote an algebra (1.10)–(1.11) by $B = \left(\dfrac{a, b}{F}\right)$, say that B is in *standard form*, and call the elements i, j *standard generators*. Note that B has basis $1, i, j, ij$ as an F-vector space, so indeed $\dim_F B = 4$.

Example 1.12. The ring $\mathrm{M}_2(F)$ of 2×2-matrices with coefficients in F is a quaternion algebra over F. Indeed, we have $\left(\dfrac{1,1}{F}\right) \cong \mathrm{M}_2(F)$ with $j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and

$$i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{or} \quad i \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

according as $\operatorname{char} F \neq 2$ or $\operatorname{char} F = 2$.

Every quaternion algebra over a separably (or algebraically) closed field F is isomorphic to $\mathrm{M}_2(F)$.

Example 1.13. The $\mathbb{R}$-algebra $\mathbb{H} = \left(\dfrac{-1,-1}{\mathbb{R}}\right)$, generated by i, j satisfying $i^2 = j^2 = (ij)^2 = -1$ is the usual division ring of quaternions over $\mathbb{R}$. Every quaternion algebra over $\mathbb{R}$ is isomorphic to either $\mathrm{M}_2(\mathbb{R})$ or $\mathbb{H}$, according to the theorem of Frobenius.

Let B be an F-algebra. An *R-order* in B is a subring $\mathcal{O} \subset B$ that is finitely generated as an R-module and such that $\mathcal{O}F = B$. We see that an R-algebra $\mathcal{O}$ is an R-order in $B = \mathcal{O} \otimes_R F$, and we will use this equivalence throughout, sometimes thinking of $\mathcal{O}$ as an R-algebra on its own terms and at other times thinking of $\mathcal{O}$ as arising as an order inside an algebra over a field.

A *quaternion order* over R is an R-order in a quaternion algebra B over F. Equivalently, an R-algebra $\mathcal{O}$ is a quaternion order if $B = \mathcal{O} \otimes_R F$ is a quaternion algebra over F.

Example 1.14. $\mathrm{M}_2(R)$ is a quaternion order in $\mathrm{M}_2(F)$.

If $a, b \in R \setminus \{0\}$, then $\mathcal{O} = R \oplus Ri \oplus Rj \oplus Rij$ is a quaternion order in $B = \left(\dfrac{a,b}{F}\right)$. So for example $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}ij$ is a $\mathbb{Z}$-order in the rational Hamiltonians $B = \left(\dfrac{-1,-1}{\mathbb{Q}}\right)$.

Further examples of quaternion orders will be defined in the next section (see Lemma 2.11).

Modules over Dedekind domains. Let R be a Dedekind domain, an integrally closed (noetherian) domain in which every nonzero prime ideal is maximal. Every field is a Dedekind domain (vacuously), as is the integral closure of $\mathbb{Z}$ or $\mathbb{F}_p[T]$ in a finite (separable) extension of $\mathbb{Q}$ or $\mathbb{F}_p(T)$, respectively. The localization of a Dedekind domain at a multiplicative subset is again a Dedekind domain. If R is the ring of integers of a number field, then we call R a *number ring.*

Over a Dedekind domain R, every projective R-module M can be represented as the direct sum of projective R-modules of rank 1, which is to say that there exist projective (equivalently, locally principal) R-modules $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subset F$ (also known as *fractional ideals* of R) and elements $x_1, \dots, x_n \in M$ such that

$$M = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_n x_n;$$

we say then that the elements x_i are a *pseudobasis* for M with *coefficient ideals* $\mathfrak{a}_i$. More generally, if $M = \mathfrak{a}_1 x_1 + \cdots + \mathfrak{a}_m x_m$ (the sum not necessarily direct), then we say the elements x_i are a *pseudogenerating set* for M (with *coefficient ideals* $\mathfrak{a}_i$).

In fact, the above characterization can be made computable as follows.

Proposition 1.15. *Let R be a number ring. Then there exists an algorithm which, given a projective R-module M specified by a pseudogenerating set, returns a pseudobasis for M.*

The algorithm in Proposition 1.15 is a generalization of the Hermite normal form (HNF) for matrices over $\mathbb{Z}$; see Cohen [7, Chapter 1]. Therefore, from now on we represent a quaternion order $\mathcal{O}$ over a number ring R by a pseudobasis; in such a situation, we may and do assume that $\mathfrak{a}_1 = R$ and $x_1 = 1$ (by employing the HNF).

Remark 1.16. Recalling Remark 1.5, in particular there seems to be no comprehensive reference for results akin to Proposition 1.15 in the global function field case.

2. Standard involutions and degree

Quaternion algebras, or more generally algebras which have a standard involution, possess a quadratic form called the reduced norm. In this section, we discuss this association and we give an algorithm which verifies that an algebra has a standard involution. As a reference, see Jacobson [17, §1.6], Knus [19], and work of the author [40].

In this section, let R be an integrally closed (noetherian) domain with field of fractions F. Let $\mathcal{O}$ be an R-algebra and let $B = \mathcal{O} \otimes_R F$.

Degree. We first generalize the notion of degree from field extensions to R-algebras.

Definition 2.1. The *degree* of $x \in \mathcal{O}$ over R, denoted $\deg_R(x)$, is the smallest positive integer n such that x satisfies a monic polynomial of degree n with coefficients in R. The *degree* of $\mathcal{O}$ over R, denoted $\deg_R(\mathcal{O})$, is the smallest positive integer n such that every element of $\mathcal{O}$ has degree at most n.

Every $x \in \mathcal{O}$ satisfies the characteristic polynomial of (left) multiplication by x on a set of generators for $\mathcal{O}$ as an R-module, and consequently $\deg_R(\mathcal{O}) < \infty$ (under our continuing hypothesis that $\mathcal{O}$ is projective of finite rank).

Lemma 2.2. *We have* $\deg_R(\mathcal{O}) = \deg_F(B)$.

Proof. Since $\mathcal{O}$ is finitely generated as an R-module and R is noetherian, the R-submodule $R[x] \subset \mathcal{O}$ is finitely generated, so x is integral over R. Since R is integrally closed, the minimal polynomial of $x \in \mathcal{O}$ over F has coefficients in R by Gauss's lemma, so $\deg_R(x) = \deg_F(x)$ and thus $\deg_R(\mathcal{O}) \leq \deg_F(B)$. On the other hand, if $y \in B$ then there exists $0 \neq d \in R$ such that $x = yd \in \mathcal{O}$ so $\deg_F(x) = \deg_F(y) = \deg_R(y)$ so $\deg_F(B) \leq \deg_R(\mathcal{O})$. □

From the lemma, we need only consider the degree of an algebra over a field.

Example 2.3. B has degree 1 if and only if $B = F$.

If K is a separable field extension of F with $\dim_F K = n$, then K has degree n as a F-algebra (in the above sense) by the primitive element theorem.

If $\dim_F B = n$, then B has degree at most n but even if B is commutative one may still have $\deg_F(B) < \dim_F B$: for example, $B = F[x,y,z]/(x,y,z)^2$ has rank 4 over the field F but has degree 2.

Standard involutions. We will see in a moment that quaternion orders and algebras are algebras of degree 2; this will be a consequence of the fact that they possess a standard involution. Indeed, the link between algebras with an involution and quadratic forms forms the heart of much important work [20].

Definition 2.4. An *anti-automorphism* of $\mathcal{O}$ is an R-linear map $\overline{} : \mathcal{O} \to \mathcal{O}$ with $\overline{1} = 1$ and $\overline{xy} = \overline{y}\,\overline{x}$ for all $x \in \mathcal{O}$. An *involution* is an anti-automorphism such that $\overline{\overline{x}} = x$ for all $x \in \mathcal{O}$. An involution is *standard* if $x\overline{x} \in R$ for all $x \in \mathcal{O}$.

Note that if $x\overline{x} \in R$ for all $x \in \mathcal{O}$, then $(x+1)(\overline{x}+1) = x\overline{x} + (x+\overline{x}) + 1 \in R$ and hence $x + \overline{x} \in R$ for all $x \in \mathcal{O}$ as well. Note that $\overline{x}x = x\overline{x}$ for all $x \in \mathcal{O}$ since $x(x+\overline{x}) = (x+\overline{x})x$ (and R is central in $\mathcal{O}$).

Example 2.5. If $\mathcal{O} = \mathrm{M}_n(R)$, then the transpose map is an anti-automorphism which is standard if and only if $n = 1$; the adjoint map is a standard involution for $n \leq 2$ but is not R-linear for $n \geq 3$.

Suppose now that $\mathcal{O}$ has a standard involution $\overline{}$. Then we define the *reduced trace* and *reduced norm*, respectively, to be the maps

$$\begin{aligned} \operatorname{trd} : \mathcal{O} &\to R \\ x &\mapsto x + \overline{x} \end{aligned} \qquad\qquad \begin{aligned} \operatorname{nrd} : \mathcal{O} &\to R \\ x &\mapsto x\overline{x} = \overline{x}x \end{aligned}$$

We have

$$x^2 - \operatorname{trd}(x)x + \operatorname{nrd}(x) = x^2 - (x+\overline{x})x + x\overline{x} = 0 \tag{2.6}$$

for all $x \in \mathcal{O}$. It follows that if $\mathcal{O}$ has a standard involution then either $\mathcal{O} = R$ (so the standard involution is the identity and $\mathcal{O} = R$ has degree 1) or $\mathcal{O}$ has degree 2.

Example 2.7. Let $B = \left(\dfrac{a,b}{F}\right)$ be a quaternion algebra over F. Then B has a standard involution, defined as follows. For $x = t + ui + vj + wk$, we have

$$\overline{x} = t - ui - vj - wk$$

so $\operatorname{trd}(x) = 2t$ and $\operatorname{nrd}(x) = t^2 - au^2 - bv^2 + abw^2$ if $\operatorname{char} F \neq 2$ and

$$\overline{x} = t + (u+1)i + vj + wk$$

so $\operatorname{trd}(x) = 2u$ and $\operatorname{nrd}(x) = t^2 + tu + au^2 + bv^2 + bvw + abw^2$ if $\operatorname{char} F = 2$.

Lemma 2.8. *$\mathcal{O}$ has a standard involution if and only if $B = \mathcal{O} \otimes_R F$ has a standard involution.*

Proof. If $\mathcal{O}$ has a standard involution, we obtain one on B by extending F-linearly. Conversely, suppose B has a standard involution and let $x \in \mathcal{O}$. Then as in the proof of Lemma 2.2, x is integral over R so its minimal polynomial over F has coefficients in R. If $x \in R$, then $\overline{x} = x$ and there is nothing to prove. If $x \notin R$, this minimal polynomial must be given by (2.6), so $\operatorname{trd}(x) = x + \overline{x} \in R$ and thus $\overline{x} = \operatorname{trd}(x) - x \in \mathcal{O}$ has $x\overline{x} = \operatorname{nrd}(x) \in R$ as well. □

An R-algebra S is *quadratic* if S has rank 2 as an R-module.

Lemma 2.9. *Let S be a quadratic R-algebra. Then S is commutative and has a unique standard involution.*

Proof. By Lemma 2.8, it suffices to prove the lemma for $K = S \otimes_R F$. But then for any $x \in K \setminus F$ we have $K = F \oplus Fx$ so K is commutative. Moreover, we have $x^2 - tx + n = 0$ for some unique $t, n \in F$ and so the (necessarily unique) standard involution is given by $x \mapsto t - x$, extending by F-linearity. (See also Scharlau [33, §8.11] for a proof of this lemma.) □

Corollary 2.10. *If $\mathcal{O}$ has a standard involution, then this involution is unique.*

This corollary follows immediately from Lemma 2.9 by restricting to quadratic subalgebras K of B.

Quaternion orders. Having identified the standard involution on a quadratic algebra, we now generalize the construction of quaternion algebras (1.10)–(1.11) to quaternion orders. Let S be a quadratic R-algebra, and suppose S is *separable*, so the minimal polynomial of every $x \in S$ has distinct roots over the algebraic closure $\overline{F}$ of F. Let $J \subset S$ be an invertible S-ideal (equivalently, a locally principal S-module) and let $b \in R \setminus \{0\}$. We denote by $\left(\dfrac{S, J, b}{R}\right)$ the R-algebra $S \oplus Jj$ subject to the relations $j^2 = b$ and $ji = \overline{i}j$ for all $i \in S$, where $\overline{}$ denotes the unique standard involution on S obtained from Lemma 2.9. We say that such an algebra is in *standard form*.

Lemma 2.11. *The R-algebra $\mathcal{O} = \left(\dfrac{S, J, b}{R}\right)$ is a quaternion order.*

Proof. We consider $B = \mathcal{O} \otimes_R F$. Let $K = S \otimes_R F$ and let $i \in K \setminus F$. Since K is separable, if $\operatorname{char} F \neq 2$ by completing the square we may assume $i^2 = a$ with $a \in F^\times$; if $\operatorname{char} F = 2$, we may assume $i^2 + i = a$ with $a \in F$. Now since J is projective we have $J \otimes_R F = J \otimes_S K \cong K$ so $B \cong K \oplus Kj$ as an F-algebra. Finally, since $ji = \overline{i}j = (\operatorname{trd}(i) - i)j$ and $\operatorname{trd}(i) = 0, 1$ according as $\operatorname{char} F \neq 2$ or not, we have identified B as isomorphic to the quaternion algebra $\left(\dfrac{a, b}{F}\right)$. □

Algorithmically identifying a standard involution. We conclude this section with an algorithm to test if an F-algebra B (of dimension n) has a standard involution.

First, we note that if B has a standard involution $\overline{} : B \to B$, then this involution and hence also the reduced trace and norm can be computed efficiently. Indeed, let $\{e_i\}_i$ be a basis for B; then $\operatorname{trd}(e_i) \in F$ is simply the coefficient of e_i in e_i^2, and so $\overline{e_i} = \operatorname{trd}(e_i) - e_i$ for each i can be precomputed for B; one recovers the involution on B (and hence also the trace) for an arbitrary element of B by F-linearity. Therefore the involution and the reduced trace can be computed using $O(n)$ arithmetic operations in F (with output linear in the input for fixed B) and the reduced norm using $O(n^2)$ operations in F (with output quadratic in the input).

Algorithm 2.12. Let B be an F-algebra given by a multiplication table in the basis $e_1, \dots, e_n$ with $e_1 = 1$. This algorithm returns true if and only if B has a standard involution.

1. For $i = 2, \dots, n$, let $t_i \in F$ be the coefficient of e_i in e_i^2, and let $n_i = e_i^2 - t_i e_i$. If some $n_i \notin F$, return false.
2. For $i = 2, \dots, n$ and $j = i + 1, \dots, n$, let $n_{ij} = (e_i + e_j)^2 - (t_i + t_j)(e_i + e_j)$. If some $n_{ij} \notin F$, return false. Otherwise, return true.

Proof of correctness. Let $F[x] = F[x_1, \dots, x_n]$ be the polynomial ring over F in n variables, and let $B_{F[x]} = B \otimes_F F[x]$. Let $\xi = x_1 + x_2 e_2 + \dots + x_n e_n \in B_{F[x]}$, and define

$$t_\xi = \sum_{i=1}^n t_i x_i$$

and

$$n_\xi = \sum_{i=1}^n n_i x_i^2 + \sum_{1 \le i < j \le n} (n_{ij} - n_i - n_j) x_i x_j.$$

Let

$$\xi^2 - t_\xi \xi + n_\xi = \sum_{i=1}^n c_i(x_1, \dots, x_n) e_i$$

with $c_i(x) \in F[x]$. Each $c_i(x)$ is a homogeneous polynomial of degree 2. The algorithm then verifies that $c_i(x) = 0$ for $x \in \{e_i\}_i \cup \{e_i + e_j\}_{i,j}$, and this implies that each $c_i(x)$ vanishes identically. Therefore, the specialization of the map $\xi \mapsto \overline{\xi} = t_\xi - \xi$ is the unique standard involution on B. □

Remark 2.13. Algorithm 2.12 requires $O(n)$ arithmetic operations in F, since e_i^2 can be computed directly from the multiplication table and hence $(e_i + e_j)^2 = e_i^2 + e_i e_j + e_j e_i + e_j^2$ can be computed using $O(4n) = O(n)$ operations.

3. Algebras with a standard involution and quadratic forms

In this section, we describe a relationship between R-algebras with a standard involution and quadratic forms over R. The main result of this section is an algorithm which verifies that an R-algebra $\mathcal{O}$ over a local PID is a quaternion order and, if so, exhibits standard generators for $\mathcal{O}$. Specializing, we will thereby recognize quaternion algebras over a field F. We then extend this to recognizing quaternion orders over a number ring R. Over fields, a reference for this section is Lam [21], and for more about algebras equipped with a quadratic norm form, we refer the reader to Knus [19].

Quadratic forms over rings. We begin by defining quadratic forms over a (noetherian) domain R.

Definition 3.1. A *quadratic form* over R is a map $Q : M \to R$, where M is a finitely generated projective R-module, such that:

(i) $Q(ax) = a^2 Q(x)$ for all $a \in R$ and $x \in M$; and

(ii) The map $T : M \times M \to R$ defined by

$$T(x, y) = Q(x + y) - Q(x) - Q(y)$$

is R-bilinear.

A symmetric bilinear form $T : M \times M \to R$ is *even* if $T(x, x) \in 2R$ for all $x \in M$. If T arises from a quadratic form, then T is even, and conversely if T is even and 2 is a nonzerodivisor in R then one recovers the quadratic form as $Q(x) = T(x, x)/2$.

Let $Q : M \to R$ be a quadratic form and suppose that M is free over R with basis $e_1, \dots, e_n$. The *Gram matrix* of Q with respect to the basis $e_1, \dots, e_n$ is the matrix $A = (T(e_i, e_j))_{i,j=1,\dots,n} \in \mathrm{M}_n(R)$. The matrix A has the property that $x^t A y = T(x, y)$, where we identify $x = x_1 e_1 + \dots + x_n e_n$ with the column vector $(x_1, \dots, x_n)^t$, and similarly for y. In particular we have $x^t A x = 2Q(x)$.

Let $Q : M \to R$ be a quadratic form. We say $x, y \in M$ are *orthogonal* (with respect to Q) if $T(x, y) = 0$.

Example 3.2. Let $\mathcal{O}$ be an R-algebra with a standard involution $\overline{}$. Then the reduced norm $\operatorname{nrd} : \mathcal{O} \to R$ (defined by $x \mapsto x\overline{x}$ for $x \in \mathcal{O}$) is a quadratic form on $\mathcal{O}$ with associated bilinear form

$$T(x, y) = x\overline{y} + y\overline{x} = \operatorname{trd}(x\overline{y}) = \operatorname{trd}(x)y + \operatorname{trd}(y)x - (xy + yx) = \operatorname{trd}(\overline{x}y) \tag{3.3}$$

for $x, y \in \mathcal{O}$. In particular $T(1, x) = T(x, 1) = \operatorname{trd}(x)$. Note that $x, y \in \mathcal{O}$ are orthogonal if and only if $x\overline{y} = -y\overline{x}$, and if further $\operatorname{trd}(x) = \operatorname{trd}(y) = 0$ then $\overline{x} = -x$ and $\overline{y} = -y$ so x, y are orthogonal if and only if $xy = -yx$.

Example 3.4. Let $\mathcal{O}_0 = \{x \in \mathcal{O} : \operatorname{trd}(x) = 0\}$ be the R-submodule of elements of reduced trace zero. Then $\mathcal{O}/\mathcal{O}_0$ is torsion-free, since if $rx \in \mathcal{O}_0$ then $\operatorname{trd}(rx) = r\operatorname{trd}(x) = 0$ so $\operatorname{trd}(x) = 0$ so $x \in \mathcal{O}_0$. Thus $\mathcal{O}_0$ is a projective R-submodule of $\mathcal{O}$ and $\mathcal{O} \supset R \oplus \mathcal{O}_0$. We therefore obtain a quadratic form $\operatorname{nrd}_0 = \operatorname{nrd}|_{\mathcal{O}_0} : \mathcal{O}_0 \to R$.

If $Q : M \to R$ and $Q' : M' \to R$ are quadratic forms, we define the form $Q \perp Q'$ on $M \oplus M'$ by requiring that $(T \perp T')(x + x') = T(x) + T(x')$ and $(Q \perp Q')(x + x') = Q(x) + Q(x')$. (Note that $T(x, x) = 2Q(x)$ for all $x \in M$ so if $2 \neq 0 \in R$ then the second condition follows from the first.)

Let $Q : M \to R$ be a quadratic form and suppose that M is free (of finite rank). In this case, a basis $e_1, \dots, e_n$ for M gives an isomorphism $M \cong R^n$ in which Q can be written

$$Q(x) = Q(x_1e_1 + \dots + x_ne_n) = \sum_i Q(e_i)x_i^2 + \sum_{i<j} T(e_i, e_j)x_ix_j$$

with $x = (x_1, \dots, x_n) \in R^n$.

For $a \in R$, the quadratic form $Q(x) = ax^2$ on R is denoted $\langle a \rangle$; similarly, for $a_1, \dots, a_n \in R$, we abbreviate $\langle a_1 \rangle \perp \dots \perp \langle a_n \rangle = \langle a_1, \dots, a_n \rangle$. For $a, b, c \in R$, the quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ on R^2 is denoted $[a, b, c]$.

Example 3.5. Let $B = \left(\dfrac{a, b}{F}\right)$ be a quaternion algebra over F. Then as in Example 2.7, in the basis $1, i, j, ij$ we have $\operatorname{nrd} \cong \langle 1, -a, -b, ab \rangle \cong \langle 1, -a \rangle \perp -b\langle 1, -a \rangle$ if $\operatorname{char} F \neq 2$ and $\operatorname{nrd} \cong [1, 1, a] \perp b[1, 1, a]$ if $\operatorname{char} F = 2$.

Similarly, for $\operatorname{nrd}_0 : B_0 \to F$ we have $\operatorname{nrd}_0 \cong \langle -a, -b, ab \rangle \cong \langle -a \rangle \perp -b\langle 1, -a \rangle$ if $\operatorname{char} F \neq 2$ and $\operatorname{nrd}_0 \cong \langle 1 \rangle \perp b[1, 1, a]$ if $\operatorname{char} F = 2$.

Quadratic forms over DVRs. Now let R be a local PID. Then R has valuation $\operatorname{ord}_v : R \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ and uniformizer π. If $R = F$ is a field, then $\pi = 1$ and the valuation is trivial, i.e. $\operatorname{ord}_v(x) = 0$ for $x \in F^\times$ (and $\operatorname{ord}_v(0) = \infty$).

Let $Q : M \to R$ be a quadratic form over R. Then since R is a PID, M is free; let n be the rank of M over R. We will now seek to find a basis for R^n in which a quadratic form Q has a particularly simple form: we will seek to diagonalize Q as far as possible. In cases where $2 \in R^\times$, we can accomplish a full diagonalization; otherwise, we can at least break up the form as much as possible, as follows.

A quadratic form Q over R is *atomic* if either:

(i) $Q \cong \langle a \rangle$ for some $a \in R^\times$, or

(ii) $2 \notin R^\times$ and $Q \cong [a, b, c]$ with $a, b, c \in R$ satisfying

$$\operatorname{ord}_v(b) < \operatorname{ord}_v(2a) \leq \operatorname{ord}_v(2c) \text{ and } \operatorname{ord}_v(a)\operatorname{ord}_v(b) = 0.$$

In case (ii), we necessarily have $\operatorname{ord}_v(2) > 0$ and $\operatorname{ord}_v(b^2 - 4ac) = 2\operatorname{ord}_v(b)$.

Example 3.6. If $2 \in R^\times$, then a quadratic form Q is atomic if and only if $Q(x) = ax^2$ for $a \in R^\times$.

Example 3.7. If $R = F$ is a field with $\operatorname{char} F = 2$, then $[a, b, c]$ is atomic if and only if $b \in F^\times$; scaling y by a/b realizes this form as isomorphic to $a[1, 1, ca/b^2]$ with $a \in F^\times$. Therefore, over fields, recording the middle coefficient is unnecesary, and indeed other texts use $[a, b]$ to denote the quadratic form $ax^2 + xy + by^2$.

For example, take $R = \mathbb{Z}_2[\sqrt{2}]$ with normalized valuation $\operatorname{ord}_v(\sqrt{2}) = 1$ and let $Q(x, y) = x^2 + \sqrt{2}xy$. Then according to our definition, Q is atomic, since $\operatorname{ord}_v(b) = 1 < \operatorname{ord}_v(2a) = 2 \le \operatorname{ord}_v(2c) = \infty$ and $\operatorname{ord}_v(a) = 0$. But this form is not globally divisible by any element of positive valuation, and a calculation shows that any isomorphic (equivalent) form has middle coefficient of positive valuation.

Example 3.8. Suppose $R = \mathbb{Z}_2$ is the ring of 2-adic integers, so that $\operatorname{ord}_v(x) = \operatorname{ord}_2(x)$ is the largest power of 2 dividing $x \in \mathbb{Z}_2$. Recall that $\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2}$ is represented by the elements $\pm 1, \pm 5$, therefore a quadratic form Q over $\mathbb{Z}_2$ is atomic of type (i) above if and only if $Q(x) \cong \pm x^2$ or $Q(x) \cong \pm 5x^2$. For forms of type (ii), the conditions $\operatorname{ord}_v(b) < \operatorname{ord}_v(2a) = \operatorname{ord}_v(a) + 1$ and $\operatorname{ord}_v(a)\operatorname{ord}_v(b) = 0$ imply in fact $\operatorname{ord}_v(b) = 0$, and so a quadratic form Q over $\mathbb{Z}_2$ is atomic of type (ii) if and only if $Q(x, y) \cong ax^2 + xy + cy^2$ with $\operatorname{ord}_2(a) \le \operatorname{ord}_2(c)$. Replacing x by ux and y by $u^{-1}y$ for $u \in \mathbb{Z}_2^\times$ we may assume a is a power of 2, and then the atomic representative $[2^t, 1, c]$ of the isomorphism class of Q is unique.

A quadratic form Q is *decomposable* if Q can be written as the orthogonal sum of two quadratic forms ($Q \cong Q_1 \perp Q_2$) and is *indecomposable* otherwise.

It follows by induction on the rank of M that Q is the orthogonal sum of indecomposable forms. We will soon give an algorithmic proof of this fact and write each indecomposable form as a scalar multiple of an atomic form. We begin with the following lemma.

Lemma 3.9. *An atomic form Q is indecomposable.*

Proof. If Q is atomic of type (i) then the space underlying Q has rank 1, so this is clear. So suppose $Q = [a, b, c]$ is atomic of type (ii) and suppose Q is decomposable. It follows that if $x, y \in M$ then $T(x, y) \in 2R$. Thus we cannot have $\operatorname{ord}_v(b) = 0$, so $\operatorname{ord}_v(a) = 0$, and further $\operatorname{ord}_v(b) \ge \operatorname{ord}_v(2) = \operatorname{ord}_v(2a)$; this contradicts the fact that Q is atomic. □

Proposition 3.10. *Let R be a local PID and let $Q : M \to R$ be a quadratic form. Then there exists a basis of M such that the form Q can be written*

$$Q \cong \pi^{e_1}Q_1 \perp \cdots \perp \pi^{e_n}Q_n$$

where the forms Q_i are atomic and $0 \le e_1 \le \cdots \le e_n \le \infty$.

In the above proposition, we interpret $\pi^\infty = 0$. A form as presented in Proposition 3.10 is called *normalized*, and the integer e_i is called the *valuation* of $\pi^{e_i}Q_i$. The tuple of valuations e_i for Q is unique.

Example 3.11. By Example 3.5, if B is a quaternion algebra over a field F then the quadratic form nrd is normalized in the basis $1, i, j, ij$, with a similar statement for nrd_0.

We give an algorithmic proof of Proposition 3.10. (Over fields, see Lam [21, §1.2], and see Scharlau [33, §9.4] for fields of characteristic 2.)

Algorithm 3.12. Let R be a computable ring which is a local PID with (computable) valuation $\operatorname{ord}_v : R \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$.

Let $Q : M \to R$ be a quadratic form over R and let $e_1, \dots, e_n$ be a basis for M. This algorithm returns a basis of M in which Q is normalized.

1. If $T(e_i, e_j) = 0$ for all i, j, return $f_i := e_i$. Otherwise, let (i, j) with $1 \leq i \leq j \leq n$ be such that $\operatorname{ord}_v T(e_i, e_j)$ is minimal, taking $i = j$ if possible and if not taking i minimal.
2. If $i = j$, let $f_1 := e_i$ and proceed to Step 3. If $i \neq j$ and $2 \in R^\times$, let $f_1 := e_i + e_j$ and proceed to Step 3. Otherwise, proceed to Step 4.
3. Let $e_i := e_1$. For $k = 2, \dots, n$ let
$$f_k := e_k - \frac{T(f_1, e_k)}{T(f_1, f_1)} f_1.$$
Let $m = 2$ and proceed to Step 5.
4. (We have $2 \notin R^\times$ and $i \neq j$.) Let
$$f_1 := \frac{\pi^{\operatorname{ord}_v T(e_i, e_j)}}{T(e_i, e_j)} e_i,$$
$f_2 := e_j$, $e_i := e_1$ and $e_j := e_2$. Let $d := T(f_1, f_1)T(f_2, f_2) - T(f_1, f_2)^2$. For $k = 3, \dots, n$, let
$$\begin{aligned} t_k &:= T(f_1, f_2)T(f_2, e_k) - T(f_2, f_2)T(f_1, e_k) \\ u_k &:= T(f_1, f_2)T(f_1, e_k) - T(f_1, f_1)T(f_2, e_k) \end{aligned}$$
and let
$$f_k := e_k + \frac{t_k}{d} f_1 + \frac{u_k}{d} f_2.$$
Let $m = 3$.
5. Recursively call the algorithm with $M = Rf_m \oplus \cdots \oplus Rf_n$, and return $f_1, \dots, f_{m-1}$ concatenated with the output basis.

Given such a basis, one recovers the normalized quadratic form by factoring out in each atomic form the minimal valuation achieved. (One can also keep track of this valuation along the way in the above algorithm, if desired.)

Remark 3.13. Note that if $2 \in R^\times$, then this algorithm computes a diagonalization of the form Q, ordering the coefficients by their valuation.

Proof of correctness. In Step 3, we verify that $\operatorname{ord}_v T(f_1, f_1) \leq \operatorname{ord}_v T(f_1, e_k)$. Indeed, we have
$$T(f_1, f_1) = T(e_i, e_i) + 2T(e_i, e_j) + T(e_j, e_j)$$
and so $\operatorname{ord}_v T(f_1, f_1) = \operatorname{ord}_v T(e_i, e_j)$ by the ultrametric inequality and the hypotheses that $\operatorname{ord}_v T(e_i, e_j) < \operatorname{ord}_v T(e_i, e_i), T(e_j, e_j)$ and $\operatorname{ord}_v(2) = 0$. So Steps 2 and 3 give correct output.

We have left to check Step 4. This is proven by letting $f_k = e_k + t_k f_1 + u_k f_2$ and solving the linear equations $T(f_1, f_k) = T(f_2, f_k) = 0$ for t_k, u_k. The result then follows from a direct calculation, coupled with the fact that $\operatorname{ord}_v(d) =$

$2\operatorname{ord}_v T(f_1, f_2) \leq \operatorname{ord}_v(t_k)$ (and similarly with u_k). This case only arises if (and only if)

$$\operatorname{ord}_v T(f_1, f_2) < \operatorname{ord}_v T(f_1, f_1) = \operatorname{ord}_v(2Q(f_1)) \leq \operatorname{ord}_v(2Q(f_2))$$

so the corresponding block is indeed atomic. □

Example 3.14. Consider the binary quadratic form $[a, b, c]$ over $\mathbb{Z}_2$. Then $T(e_1, e_1) = 2a$, $T(e_1, e_2) = b$, and $T(e_2, e_2) = 2c$. We follow the course of Algorithm 3.12. If $\operatorname{ord}_v(2a)$ is minimal, then in Steps 2 and 3 we diagonalize (complete the square): we have $f_1 = e_1$ and $f_2 = e_2 - (b/2a)e_1$ and so we obtain the (isomorphic) form $\langle a, c + b^2/4a\rangle$. If $\operatorname{ord}_v(2c)$ is minimal, then we similarly obtain $\langle c, a + b^2/4c\rangle$. Finally, if $\operatorname{ord}_2(b)$ is minimal, then we enter Step 4. Since (i, j) was taken with i minimal, for illustration we may suppose $i = 1$ and $j = 2$. Then we have $t = \operatorname{ord}_v(b) < \operatorname{ord}_v(2a) \leq \operatorname{ord}_v(2c)$. Writing $a = 2^t a'$, $b' = 2^t b'$ and $c' = 2^t c'$, in Step 4, we simply have $f_1 = (1/b')e_1$ and $f_2 = e_2$ and we obtain the form $2^t[a'/(b')^2, 1, c']$ and $[a'/(b')^2, 1, c']$ is indeed atomic.

Example 3.15. Consider the form $q(x, y, z) = xy + xz$ over $\mathbb{Z}_2$. We enter Step 4 with $f_1 = e_1$ and $f_2 = e_2$. We compute that $d = -T(f_1, f_2) = -1$, and $t_3 = 0$ and $u_3 = 1$. Thus $f_3 = e_3 - f_2 = e_3 - e_2$, and we obtain the form $[0, 1, 0] \perp \langle 0\rangle$.

We note that Algorithm 3.12 requires $O(n^2)$ arithmetic operations in R. This algorithm can be modified suitably to operate on the Gram matrix $(T(e_i, e_j))_{i,j}$ of the quadratic form Q, which as explained above recovers the quadratic form when $2 \neq 0 \in R$.

For a quadratic form $Q : M \to R$, we define

$$\operatorname{rad}(Q) = \{x \in M : T(x, y) = 0 \text{ for all } y \in M\};$$

we say Q is *nonsingular* if $\operatorname{rad}(Q) = \{0\}$.

Example 3.16. We have $\operatorname{rad}(Q \perp Q') = \operatorname{rad}(Q) \oplus \operatorname{rad}(Q')$, and if Q is atomic then $\operatorname{rad}(Q) = \{0\}$. In particular, one can read off $\operatorname{rad}(Q)$ directly from a normalized form by the corresponding valuations.

Identifying quaternion algebras. Using the above normalization of a quadratic form in the case where $R = F$ is a field, we can directly identify quaternion algebras amongst algebras with a standard involution.

Proposition 3.17. *Let B be an F-algebra with a standard involution. If $\dim_F B = 4$, then B is a quaternion algebra if and only if* nrd *is nonsingular.*

Proof. If B is a quaternion algebra, then nrd is nonsingular by Example 3.5.

Conversely, B has a basis $1, i, j, k$ which is a normalized basis for Q. First suppose $\operatorname{char} F \neq 2$. By orthogonality we have $\operatorname{trd}(i) = 0$ so $i^2 = -\operatorname{nrd}(i) = a \neq 0$ by nonsingularity and similarly $j^2 = b \neq 0$, and $ji + ij = 0$ from (3.3) so $(ij)^2 = -ab$. Thus $B \supset \left(\dfrac{a, b}{F}\right)$ hence this map is an isomorphism. The case $\operatorname{char} F = 2$ follows similarly: now instead we have $i^2 + i = a$ and $ji = \bar{i}j = (i + 1)j$. □

Proposition 3.17 yields the following algorithm.

Algorithm 3.18. Let B be an F-algebra with $\dim_F B = 4$ (specified by a multiplication table). This algorithm returns `true` if and only if B is a quaternion algebra, and if so returns an isomorphism $B \cong \left(\dfrac{a, b}{F}\right)$.

1. Verify that B has a standard involution by calling Algorithm 2.12. If not, return false.
2. Compute a normalized basis $1, i, j, k$ for the quadratic form $\operatorname{nrd} : B \to F$ by calling Algorithm 3.12.
3. Test if nrd is nonsingular as in Example 3.16. If so, return true and the quaternion algebra $\left(\dfrac{a,b}{F}\right)$ given by the standard generators i, j.

Remark 3.19. Given a quaternion algebra over $\mathbb{Q}$, Rónyai [29, Theorem 2.1] gives an algorithm to compute a standard representation, but this algorithm tests a polynomial of degree 2 over $\mathbb{Q}$ for irreducibility; the above algorithm requires no such test.

Remark 3.20. If in Step 3 one finds that nrd is not nonsingular, then one has the further refinement of Algorithm 3.18 as follows.

We denote by $\operatorname{rad}(B)$ the *Jacobson radical* of B, the largest two-sided *nil ideal* of B, i.e. the largest two-sided ideal in which every element is nilpotent. An algebra B for which $\operatorname{rad}(B) = \{0\}$ is called *semisimple*. We claim that $\operatorname{rad}(B) = \operatorname{rad}(\operatorname{nrd})$. Indeed, let $e \in B$ be nilpotent, so that $e^2 = 0$. For any $x \in B$, we have by (3.3) that

$$xe + ex = \operatorname{trd}(x)e + \operatorname{trd}(xe).$$

It follows that e generates a nil ideal if and only if $T(x, e) = 0$ for all $x \in B$, which holds if and only if $x \in \operatorname{rad}(\operatorname{nrd})$. Thus $\operatorname{rad}(B) = \operatorname{rad}(\operatorname{nrd})$. One can then easily modify the algorithm to output $\operatorname{rad}(B) = \operatorname{rad}(\operatorname{nrd})$.

Remark 3.21. Another algorithm which tests if B is a quaternion algebra (but does not give a standard representation) under the assumption $\operatorname{char} F = 0$ runs as follows. (See Lam [21, Chapter 4] for the standard facts we use.) By the Wedderburn-Artin theorem and a dimension count, the algebra B over F is a quaternion algebra if and only if B is central and semisimple. We verify that B is central as in Remark 1.8. To verify semisimplicity, if $\operatorname{char} F = 0$, Dickson [10, §66] showed that B with $\dim_F B = n$ is semisimple if and only if the matrix $(\operatorname{Tr}(e_i e_j))_{i,j=1,\dots,n}$ has full rank n, where Tr is the (left) algebra trace.

In view of Algorithm 3.18, we assume from now on that a quaternion algebra B over a field F is given as input by a standard representation.

Over a general domain R, the above algorithms do not generalize directly, as we cannot hope to normalize a quadratic form in such a simple way for over rings that are no longer local PIDs. Indeed, the category of quadratic forms over a general domain R can be quite complicated—already forms over the integers $\mathbb{Z}$ are of significant interest. However, over Dedekind domains, we can still recognize quaternion orders, and one instead understands these orders as in Section 1 via their localizations, a subject which will consume the later sections of this article.

Identifying quaternion orders. Let F be a number field and let $\mathbb{Z}_F$ be its ring of integers. In this section, we give an algorithm which allows us in many cases to put quaternion orders in a standard form as in the discussion of Lemma 2.11.

Algorithm 3.22. Let $\mathcal{O} \subset B$ be a quaternion order over $\mathbb{Z}_F$. Let $\iota : K \to B$ be an embedding of F-algebras with K a field such that $[K : F] = 2$ and $\iota(K) \cap \mathcal{O} = \mathbb{Z}_K$

is maximal. This algorithm returns a fractional ideal $\mathfrak{b}$ of K, an element $j \in \mathcal{O}$ such that $\mathcal{O} = \iota(\mathbb{Z}_K) \oplus \iota(\mathfrak{b})j \cong \left(\dfrac{\mathbb{Z}_K, \mathfrak{b}, b}{\mathbb{Z}_F}\right)$.

1. Identify K with $\iota(K)$. Let $K = F \oplus Fi$ with $i \in B$. Compute $j \in B$ orthogonal to $1, i$.
2. Let $x_1, \dots, x_m$ be a generating set for $\mathcal{O}$ as a $\mathbb{Z}_F$-module. Write $x_k = a_k + b_k j$ with $a_k, b_k \in K$ for $k = 1, \dots, m$.
3. Compute a pseudo-basis $\mathbb{Z}_K \oplus \mathfrak{b}j$ for the $\mathbb{Z}_K$-module generated by (a_k, b_k) for $k = 1, \dots, m$ using a HNF.
4. Let a, b be generators for $\mathfrak{b}$ as an $\mathbb{Z}_F$-module. If $\operatorname{trd}(j) \neq 0$, then let $c := \operatorname{trd}(bj)a - \operatorname{trd}(aj)b$, let $j := cj$ and $\mathfrak{b} := (1/c)\mathfrak{b}$. Return $\mathfrak{b}$ and the element j.

Proof of correctness. In Step 4, we check directly that $\operatorname{trd}(j) = \operatorname{trd}(ij) = 0$, as desired. □

Remark 3.23. One can extend Algorithm 3.22 when $\iota(K) \cap \mathcal{O} = S$ is no longer maximal by an appropriate modification of the HNF algorithm over S.

4. Identifying the matrix ring

In this section, we continue the pursuit of our motivating question and address the computational complexity of identifying the matrix ring over a field. Throughout this section, let F be a computable field. We represent a quaternion algebra B over F by a standard form $B = \left(\dfrac{a, b}{F}\right)$.

Problem (IsMatrixRing)**.** *Given a quaternion algebra B over F, determine if $B \cong \mathrm{M}_2(F)$.*

We may also ask for a solution to the more difficult problem of constructing an explicit isomorphism.

Problem (ExhibitMatrixRing)**.** *Given a quaternion algebra B over F, determine if $B \cong \mathrm{M}_2(F)$ and, if so, output such an isomorphism.*

Zerodivisors. Let B be a quaternion algebra. The following structural lemma allows us to address the above problems.

Lemma 4.1. *The following are equivalent:*

(i) *$B \cong \mathrm{M}_2(F)$;*
(ii) *B is not a division ring;*
(iii) *There exists a nonzero $e \in B$ such that $e^2 = 0$; and*
(iv) *B has a proper, nonzero left (or right) ideal I.*

If $B \cong \mathrm{M}_2(F)$, we say that B is *split*. More generally, if $K \supset F$ is a field containing F, then we say K is a *splitting field* for B if $B_K = B \otimes_F K$ is split.

We give a proof of Lemma 4.1 in an algorithmically effective way in this section. The implication (i) ⇒ (ii) is clear. The implication (ii) ⇒ (iii) is obtained as follows.

Algorithm 4.2. Let $x \in B$ be a zerodivisor. This algorithm returns a nonzero element $e \in B$ such that $e^2 = 0$.

1. If $\operatorname{trd}(x) = 0$, return x.

2. Compute $0 \neq y \in B$ orthogonal to $1, x$ with respect to the quadratic form nrd. If $xy = 0$, return y; otherwise, return xy.

Proof of correctness. The element $x \neq 0$ is a zerodivisor if and only if $\operatorname{nrd}(x) = x\overline{x} = 0$. Since y is orthogonal to 1 we have $\operatorname{trd}(y) = 0$ so $\overline{y} = -y$; similarly, since y is orthogonal to x we have $\operatorname{trd}(xy) = -\operatorname{trd}(x\overline{y}) = 0$. If $xy = 0$ then y is a zerodivisor. If $xy \neq 0$ then $\operatorname{nrd}(xy) = \operatorname{nrd}(x)\operatorname{nrd}(y) = 0$, as desired. □

The implication (iii) ⇒ (iv) follows, since e generates a proper left (or right) ideal. Below, in the proof of correctness of the following algorithm, we will show that if $I = Be$ then $\dim_F I = 2$; the final implication (iv) ⇒ (i) then follows since left multiplication gives a nonzero F-algebra map $B \to \operatorname{End}_F(I) \cong \mathrm{M}_2(F)$ which is injective since B is simple and therefore an isomorphism as $\dim_F B = 4 = \dim_F \mathrm{M}_2(F)$.

Algorithm 4.3. Let $e \in B$ satisfy $e^2 = 0$. This algorithm returns a standard representation $B \cong \left(\dfrac{1,1}{F}\right) \cong \mathrm{M}_2(F)$.

1. Find $k \in \{i, j, ij\}$ such that $\operatorname{trd}(ek) = s \neq 0$. Let $t = \operatorname{trd}(k)$ and $n = \operatorname{nrd}(k)$, and let $e' = (1/s)e$.
2. Let $j' = k + (-tk + n + 1)e'$ and let

$$i' = \begin{cases} e'k - (k+t)e', & \text{if } \operatorname{char} F \neq 2; \\ k + ((t+1)k + n + 1)e', & \text{if } \operatorname{char} F = 2. \end{cases}$$

Return i', j'.

Proof of correctness. In Step 1, if $\operatorname{trd}(ek) = 0$ for all such k then $e \in \operatorname{rad}(\operatorname{nrd})$, contradicting Lemma 3.17. We have $\operatorname{trd}(e'k) = \operatorname{trd}(ke') = 1$ so $\operatorname{trd}(\overline{e'k}) = -1$.

Consider $I = Fe' + Fke'$. Note $\operatorname{trd}(ke') \neq 0$ implies that e', ke' are linearly independent. Let A be the subalgebra of B generated by e' and k. We have $e'k + ke' = te' + 1$ from (3.3) and $k^2 = tk - n$, and thus we compute that left multiplication yields a map

$$\begin{aligned} A &\to \operatorname{End}_F(I) \cong \mathrm{M}_2(F) \\ e', k &\mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -n \\ 1 & t \end{pmatrix}. \end{aligned}$$

A direct calculation then reveals that $j' \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $i' \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ if $\operatorname{char} F \neq 2$ and $i' \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ if $\operatorname{char} F = 2$, as in Example 1.12.

It follows all at once that $A = B$, that $I = Be'$, and that the map $B \to \mathrm{M}_2(F)$ is an isomorphism. □

Remark 4.4. An algorithm like the above which requires linear algebra in F is claimed but not exhibited explicitly by Rónyai [29]; see also further of Rónyai [32, §5.1].

Conics. We have already seen in Lemma 4.1 that $B \cong \mathrm{M}_2(F)$ if and only if there exists $0 \neq e \in B$ such that $e^2 = 0$. To this end, as in the previous section let

$$B_0 = \{e \in B : \operatorname{trd}(e) = 0\}.$$

We have $\dim_F B_0 = 3$, and given a standard representation for $B = \left(\dfrac{a,b}{F}\right)$, we have a basis for B_0 given by i, j, ij if $\operatorname{char} F \neq 2$ and $1, j, ij$ if $\operatorname{char} F = 2$, as in Example 3.5.

We may identify the set $\mathbb{P}(B_0) = B_0^\times / F^\times$ with the points of the projective plane $\mathbb{P}^2(F)$ over F. Then the equation $\operatorname{nrd}_0(x,y,z) = 0$ yields a *conic* $C \subset \mathbb{P}^2_F$ defined over F, a nonsingular projective plane curve of degree 2.

Lemma 4.5. *The following are equivalent:*

(i) $B \cong \mathrm{M}_2(F)$*;*

(v) *The quadratic form* $Q = \operatorname{nrd}|_{B_0}$ *associated to* B *represents zero over* F*; and*

(vi) *The conic* C *associated to* B *has an* F*-rational point.*

Therefore we are led to the following problems.

Problem 4.6 (HasPoint)**.** *Given a conic* C *defined over a field* F*, determine if* C *has an* F*-rational point.*

Problem 4.7 (ExhibitPoint)**.** *Given a conic* C *defined over a field* F*, determine if* C *has an* F*-rational point and, if so, output such a point.*

These problems could be equivalently formulated as follows: given a nonsingular ternary quadratic form $Q : V \to F$, determine if F is *isotropic* (represents zero nontrivially) and, if so, find $0 \neq x \in V$ such that $Q(x) = 0$. We find the geometric language here to be more suggestive, but really these are equivalent ways to describe the same situation.

By Algorithm 3.12, given a conic C over F, there is a (deterministic, polynomial-time) algorithm which computes a change of coordinates in which C is given by the equation

$$ax^2 + by^2 + cz^2 = 0$$

if $\operatorname{char} F \neq 2$, with $a, b, c \in F^\times$, and

$$ax^2 + axy + aby^2 + cz^2 = 0$$

if $\operatorname{char} F = 2$, with $a, c \in F^\times$ and $b \in F$ by Example 3.7. In the first case, multiplying through by $abc \neq 0$ we obtain $bc(ax)^2 + ac(by)^2 + (abc^2)z^2 = 0$ which arises as the form associated to $\left(\dfrac{-bc, -ac}{F}\right)$; in the second case, we multiply through by $c \neq 0$ to obtain $(ac)x^2 + (ac)xy + b(ac)y^2 + (cz)^2 = 0$ which is associated to $\left(\dfrac{b, ac}{F}\right)$. Together with Algorithm 4.3, therefore, we arrive at the following lemma.

Proposition 4.8. *The association* $B \mapsto C = \operatorname{nrd}_0$ *gives a bijection between quaternion algebras over* F *up to isomorphism and conics over* F *up to isomorphism.*

Problems (IsMatrixRing)*,* (ExhibitMatrixRing) *are (deterministic polynomial-time) equivalent to Problems* (HasPoint)*,* (ExhibitPoint)*, respectively.*

Proof. We need only identify isomorphisms: we need to show that two quaternion algebras $B \cong B'$ are isomorphic if and only if the induced conics $C \cong C'$ are isomorphic.

We treat only the case $\operatorname{char} F \neq 2$; the case $\operatorname{char} F = 2$ follows similarly. If $\phi : B \to B'$ is an isomorphism of quaternion algebras, then $\phi(1) = 1$ so $\phi(B_0) = B_0'$, and the reduced norm is determined by the standard involution which is unique, so $\operatorname{nrd}_B = \operatorname{nrd}_{B'} \circ \phi$.

Conversely, suppose $\psi : C \to C'$ is an isomorphism. Choose a quadratic form Q so that C is given by $Q = 0$ in $\mathbb{P}^2_F$, normalized and scaled so that $Q \cong \operatorname{nrd}_0$ for some $B \cong \left(\dfrac{a,b}{F}\right)$. Choose similarly Q' for C'. Then ψ is given by an element of $\operatorname{PGL}_3(F)$ and there exists a lift of ψ to $\operatorname{GL}_3(F)$ such that $Q = Q' \circ \psi$. The F-linear map $\psi : B_0 \to B_0'$ extends naturally (defining $\phi(1) = 1$) to an F-linear map which we also denote $\psi : B \to B'$, and we must show that ψ is an F-algebra isomorphism.

Suppose $B = \left(\dfrac{a,b}{F}\right)$. Then we have $\operatorname{nrd}(\psi(i)) = \operatorname{nrd}(i) = -a$ and $\operatorname{nrd}(\psi(i)) = \psi(i)\overline{\psi(i)} = -\psi(i)^2$ so $\psi(i)^2 = a$. Similarly we have $\psi(j)^2 = b$. We have $ji = -ij$ since i, j are orthogonal, but then $\psi(i), \psi(j)$ are orthogonal so $\psi(j)\psi(i) = -\psi(i)\psi(j)$. Finally, we have that both $\psi(ij)$ and $\psi(i)\psi(j)$ are orthogonal to $1, \psi(i), \psi(j)$, and $\psi(ij)^2 = -ab = (\psi(i)\psi(j))^2$, so $\psi(ij) = \pm\psi(i)\psi(j)$. If the negative sign occurs, we replace ψ by the linear map defined on the basis $1, i, j, ij$ unmodified on $1, i, j$ but negated on ij; this map is now an F-algebra homomorphism. Together, these imply that $B' \cong \left(\dfrac{a,b}{F}\right)$ as well. □

We conclude this section by considering a simple case of the above problems. First, let $F = \mathbb{F}_q$ be a finite field with q elements. Indeed, Problem (HasPoint) is trivial: since every conic over a finite field has a point (an elementary argument), one can simply always output true!

For problem (ExhibitPoint), we will make use of the following related problem.

Problem 4.9 (SquareRoot)**.** *Given $a \in F^{\times 2}$, output $b \in F^\times$ such that $b^2 = a$.*

We have two cases. First, if q is even, then one can solve Problem (SquareRoot) in deterministic polynomial time (by repeated squaring, since $q - 1 = \#\mathbb{F}_{2^r}^\times$ is odd); for a conic in the form given in Example 3.5, given up to scaling by $x^2 + by^2 + byz + abz^2$ with $a, b \in \mathbb{F}_q$ and $b \neq 0$, this is already sufficient to solve Problem (ExhibitPoint). If q is odd, then there exists a deterministic polynomial-time algorithm to solve (ExhibitPoint) over $\mathbb{F}_q$ by work of van de Woestijne [37]. There also exists a probabilistic polynomial-time algorithm, which intersects the conic with a random line and then calls (SquareRoot), and there is a probabilistic polynomial-time algorithm to solve (SquareRoot) but no deterministic such algorithm (without further assumption of a generalized Riemann hypothesis). The latter algorithm is extremely efficient in practice.

Remark 4.10. It would also be interesting to study the corresponding problem where $\mathrm{M}_2(F)$ is replaced by another quaternion algebra B': in other words, to test if two quaternion algebras B, B' over F are isomorphic and, if so, to compute an explicit isomorphism. Since the reduced norm is determined by the standard involution on a quaternion algebra, and this involution is unique, it follows that if $B \cong B'$ then $\operatorname{nrd}_B \cong \operatorname{nrd}_{B'}$; in fact, this is an equivalence even when restricted to the trace zero subspace [21]. Therefore one is led to consider the problem of determining if two quadratic forms are isometric and, if so, to compute an explicit isometry.

Remark 4.11. More generally, one can establish a functorial bijection between twisted similarity classes of ternary quadratic forms over a commutative ring R and quaternion rings over R via the Clifford algebra; see work of the author [41]. It would be interesting to investigate the algorithmic implications of this correspondence.

5. Splitting fields and the Hilbert symbol

In this section, we exhibit algorithms for solving the Problem (IsMatrixRing) over a local field with residue characteristic not 2: in this setting, our problem is otherwise known as computing the Hilbert symbol.

Hilbert symbol. Let F be a field with $\operatorname{char} F \neq 2$, and let $a, b \in F^\times$. The *Hilbert symbol* is defined to be

$$(a,b)_F = \begin{cases} 1, & \text{if } \left(\dfrac{a,b}{F}\right) \cong \mathrm{M}_2(F); \\ -1, & \text{otherwise.} \end{cases}$$

We begin by recalling a well-known criterion [38, Corollaire 2.4].

Lemma 5.1. *A quaternion algebra* $\left(\dfrac{a,b}{F}\right)$ *is split if and only if* $b \in N_{K/F}(K^\times)$, *where* $K = F[i]$.

Here, we write $K = F[i] = F \oplus Fi$ to be the quadratic F-algebra generated by i.

Proof. If $\mathrm{N}_{K/F}(u+vi) = \operatorname{nrd}(u+vi) = b$ with $x, y \in F$, then $x = u + vi + j$ has $\operatorname{nrd}(x) = \operatorname{nrd}(u+vi+j) = \operatorname{nrd}(u+vi) + \operatorname{nrd}(j) = b - b = 0$, so B is not a division ring, so $B \cong \mathrm{M}_2(F)$ by Lemma 4.1. Conversely, if $B \xrightarrow{\sim} \mathrm{M}_2(F)$, then after conjugating by an element of $\mathrm{GL}_2(F)$ we may assume $i \mapsto \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$ (rational canonical form). The condition that $ji = -ij$ implies that $j \mapsto \begin{pmatrix} u & -av \\ v & -u \end{pmatrix}$ and $j^2 = u^2 - av^2 = b = \mathrm{N}_{K/F}(u+vi)$. □

Lemma 5.2. *We have* $(a,b)_F = (b,a)_F$ *and* $(a,b)_F = (-ab,b)_F$. *If* $u, v \in F^\times$ *then* $(a,b)_F = (au^2, bv^2)_F$.

Proof. Interchanging i, j gives an isomorphism $\left(\dfrac{a,b}{F}\right) \cong \left(\dfrac{b,a}{F}\right)$; replacing i, j by ui, vj gives an isomorphism $\left(\dfrac{a,b}{F}\right) \cong \left(\dfrac{u^2a, v^2b}{F}\right)$. By considering the algebra generated by ij, j we see that $\left(\dfrac{a,b}{F}\right) \cong \left(\dfrac{a,-ab}{F}\right)$. □

Local Hilbert symbol. For the rest of this section, let F be a number field. For a place v of F, let F_v denote the completion of F at v and let R_v be its valuation ring. Let π_v be a uniformizer for F_v and let k_v be the residue field of F_v.

If $a, b \in F_v^\times$, we abbreviate $(a,b)_v = (a,b)_{F_v}$. We now proceed to discuss the computability of $(a,b)_v$, and thereby Problem (IsMatrixRing) for local fields F_v with $\operatorname{char} k_v \neq 2$.

Remark 5.3. With Lemma 5.1 in mind, we recall the following facts about local norms. There is a unique unramified quadratic extension K_v of F_v, obtained from the corresonding unique such extension of residue fields. Then $\mathrm{N}_{K_v/F_v}(K_v^\times) = R_v^\times \times \pi_v^{2\mathbb{Z}}$ by Hensel's lemma, since the norm map in an extension of finite fields is surjective. For further details, see Neukirch [25, Corollary V.1.2] or Fröhlich [12, Proposition 7.3].

We begin by recalling the following fundamental result concerning division quaternion algebras over a local field [38, Théorèmes II.1.1, II.1.3].

Lemma 5.4. *Let v be a noncomplex place of F. Then there is a unique quaternion algebra B_v over F_v which is a division ring, up to F_v-algebra isomorphism.*

Note that there is no division quaternion algebra over $\mathbb{C}$ since $\mathbb{C}$ is algebraically closed. The unique division algebra over $\mathbb{R}$ is the classical ring of Hamiltonians $\mathbb{H} = \left(\dfrac{-1,-1}{\mathbb{R}}\right)$. If v is nonarchimedean, then the unique division ring over F_v is given by $B_v \cong \left(\dfrac{K_v, \pi_v}{F_v}\right)$, where K_v is the (unique) unramified quadratic extension of F_v.

Let B be a quaternion algebra over F. We say B is *unramified* (or *split*) at v if $B \otimes_F F_v \cong \mathrm{M}_2(F_v)$, i.e. F_v is a splitting field for B; otherwise (if B_v is a division ring) we say B is *ramified* at v.

A place v of F is *odd* if either v is real or v is nonarchimedean and $\#k_v$ is odd; v is *even* if v is nonarchimedean and $\#k_v$ is even. (A complex place is neither odd nor even.) For an odd place v and $a \in F_v^\times$, we define the *square symbol*

$$\left\{\frac{a}{v}\right\} = \begin{cases} 1, & \text{if } a \in F_v^{\times 2}; \\ -1, & \text{if } a \notin F_v^{\times 2} \text{ and } \operatorname{ord}_v(a) \text{ is even;} \\ 0, & \text{if } a \notin F_v^{\times 2} \text{ and } \operatorname{ord}_v(a) \text{ is odd.} \end{cases}$$

Here we set the convention that v is a real place then $\pi_v = -1$ is a uniformizer for $F_v \cong \mathbb{R}$ and that $a = (-1)^{\operatorname{ord}_v(a)}|a|$; in other words, $\left\{\dfrac{a}{v}\right\} = 1$ or 0 according as $a > 0$ or $a < 0$.

Suppose v is nonarchimedean. If $\operatorname{ord}_v(a) = 0$, then $\left\{\dfrac{a}{v}\right\} = \left(\dfrac{a}{v}\right)$ is the usual Legendre symbol (see (5.7) below); in fact, $\left\{\dfrac{a}{v}\right\} = 0$ if and only if $\operatorname{ord}_v(a)$ is odd. Note that the square symbol is not multiplicative, for example $\left\{\dfrac{\pi_v^2}{v}\right\} = 1 \neq 0 = \left\{\dfrac{\pi_v}{v}\right\}^2$; it is multiplicative when restricted to the the subgroup of elements with even valuation, however.

Finally, we note that $\left\{\dfrac{a}{v}\right\} = -1$ if and only if $F_v(\sqrt{a})$ is an unramified field extension of F_v and $\left\{\dfrac{a}{v}\right\} = 0$ if and only if $F_v(\sqrt{a})$ is ramified; when v is real, we follow the convention that $\mathbb{C}$ is considered to be ramified over $\mathbb{R}$.

Proposition 5.5. *Let v be an odd place of F and let $a, b \in F_v^\times$. Then $(a,b)_v = 1$ if and only if*

$$\left\{\frac{a}{v}\right\} = 1 \quad \textit{or} \quad \left\{\frac{b}{v}\right\} = 1 \quad \textit{or} \quad \left\{\frac{-ab}{v}\right\} = 1 \quad \textit{or} \quad \left\{\frac{a}{v}\right\} = \left\{\frac{b}{v}\right\} = \left\{\frac{-ab}{v}\right\} = -1.$$

Proof. First, suppose v is archimedean. Then $(a,b)_v = 1$ if and only if $v(a) > 0$ or $v(b) > 0$ if and only if $\left\{\dfrac{a}{v}\right\} = 1$ or $\left\{\dfrac{b}{v}\right\} = 1$. So we suppose v is nonarchimedean.

Let $B_v = \left(\dfrac{a,b}{F_v}\right)$, and let $K_v = F_v[i]$, where we recall $i^2 = a$. Since $(a,b)_v = (b,a)_v = (a,-ab)_v$, the statement is symmetric in interchanging a, b and replacing b by $-ab$. If one of $\left\{\dfrac{a}{v}\right\} = 1$ or $\left\{\dfrac{b}{v}\right\} = 1$ or $\left\{\dfrac{-ab}{v}\right\} = 1$, then we may suppose $\left\{\dfrac{a}{v}\right\} = 1$; consequently, K_v is not a field, so B_v is not a division ring and by Lemma 4.1 we have $(a,b)_v = 1$. We cannot have $\left\{\dfrac{a}{v}\right\} = \left\{\dfrac{b}{v}\right\} = \left\{\dfrac{-ab}{v}\right\} = 0$. Thus we have only to consider the case $\left\{\dfrac{a}{v}\right\} = -1$.

If $\left\{\dfrac{b}{v}\right\} = -1$, then since K_v is the unique unramified quadratic extension of F_v and $\operatorname{ord}_v(b)$ is even, we have $b \in \mathrm{N}_{K_v/F_v}(K_v^\times)$ by Remark 5.3, so by Lemma 5.1 we have that B_v is split so $(a,b)_v = 1$. Otherwise, $\left\{\dfrac{b}{v}\right\} = 0$. But now $F_v[i] = K_v$ is the unramified quadratic extension of F_v so $b \notin \mathrm{N}_{K_v/F_v}(K_v^\times)$ and thus B_v is a division ring by Lemma 5.1, so $(a,b)_v = -1$. □

Corollary 5.6. *Let $a, b \in R_v \setminus \{0\}$ and suppose $a \in R_v^\times$. Then $(a,b)_v = \left(\dfrac{a}{v}\right)^{\operatorname{ord}_v b}$.*

Representing local fields. When discussing computability for local fields, we immediately encounter the following issue: a local field F_v is uncountable, so it is not computable.

One has at least two choices for overcoming this obstacle. One possibility is to use *exact local field arithmetic*, where one includes with the specification of an element its precision. One then requires the output of algorithms to be a continuous function of the input and to be correct with whatever output precision is given. This way of working with $\mathbb{R}$ (or $\mathbb{C}$) also goes by the name *exact real* (or *complex*) *arithmetic.* This model has several advantages. In practice, for many applications this works extremely well: if more precision is required in the output, one simply gives more precision in the input. Consequently this model is also very efficient. Although this method does not realize a local field F as a computable field, all of the algorithms we discuss in this article work well in this model for F_v.

A second method is simply to work in a computable subfield F of the local field F_v. Indeed, any subfield F which is countably generated over its prime field is computable. In this article, we will take this approach; it is more appropriate for the theoretical discussion below (even as it will be less efficient in practice).

With this discussion in mind, we represent a local field as follows. First, let F be a number field. Let v be a place of F. If v is archimedean, then it is specified by some ordering of the roots of f in $\mathbb{C}$. If v is nonarchimedean, then v is specified by a prime ideal in the ring of integers in F. We can thereby compute a uniformizer $\pi_v \in F$ for the place v by the Chinese remainder theorem.

We then represent the local field as $F_v^{\mathrm{alg}} = \overline{F} \cap F_v$, an algebraic closure of F in F_v. Given a (monic) polynomial g with coefficients in F, there exists a deterministic algorithm which returns the roots of g in F_v (as elements of F_v^{alg}). In the nonarchimedean case, Hensel's lemma provides the essential ingredient to show that one can (efficiently) compute with F_v^{alg}. With this choice, by computing in the subfield generated by any element $x \in F_v^{\mathrm{alg}}$ we can compute the discrete valuation $\mathrm{ord}_v : F \to \mathbb{Z} \cup \{\infty\}$ as well as the reduction map $R_v \to k_v$ modulo π_v. When v is real, we recall that $\mathrm{ord}_v(a) = 0, 1$ according as $a > 0$ or $a < 0$, and so the computability of ord_v follows from well-known algorithms for exact real root finding.

The above discussion applies equally well to the case of global function fields; see Remark 1.5. For more on computably algebraically closed fields, we refer again to Stoltenberg-Hansen and Tucker [34].

Computing the local Hilbert symbol. To conclude, we discuss the computability of the Hilbert symbol for odd places using Proposition 5.5. We use Proposition 5.5 and the correspondence above to relate Problem (HasPoint) to the problem of computing the square symbol.

Suppose F_v is archimedean. The Hilbert symbol for $F_v \cong \mathbb{C}$ is trivial. If v is real, then $\left\{\dfrac{a}{v}\right\} = 1, 0$ according as $a > 0$ or $a < 0$, so by the correspondence above this solves (HasPoint) for these fields. It follows that Problem (ExhibitPoint) is equivalent to Problem (SquareRoot), and there is a deterministic algorithm to solve this problem in the computable subfield $F_v^{\mathrm{alg}} = \overline{F} \cap \mathbb{R}$ by hypothesis.

Next, suppose F_v is nonarchimedean and that v is odd. Then we can evaluate $\left\{\dfrac{a}{v}\right\}$ by simply computing $\mathrm{ord}_v(a) = e$; if e is odd then $\left\{\dfrac{a}{v}\right\} = 0$, whereas if e is even then $\left\{\dfrac{a}{v}\right\} = \left(\dfrac{a_0}{v}\right)$ where $a_0 = a\pi_v^{-e} \in R_v$ and $\left(\dfrac{a_0}{v}\right) = \left(\dfrac{a_0}{\mathfrak{p}}\right)$ is the usual Legendre symbol, defined by

$$\left(\frac{a_0}{\mathfrak{p}}\right) = \begin{cases} 0, & \text{if } a_0 \equiv 0 \pmod{\mathfrak{p}}; \\ 1, & \text{if } a_0 \not\equiv 0 \pmod{\mathfrak{p}} \text{ and } a_0 \text{ is a square modulo } \mathfrak{p}; \\ -1, & \text{otherwise.} \end{cases} . \tag{5.7}$$

The Legendre symbol can be computed in deterministic polynomial time by Euler's formula

$$\left(\frac{a_0}{\mathfrak{p}}\right) \equiv a_0^{(q-1)/2} \pmod{\mathfrak{p}}$$

using repeated squaring, where $q = \#k_v$.

To solve Problem (HasPoint), by Proposition 5.5 we have two cases. In the first case, where one value of the square symbol is equal to 1, we reduce to Problem (SquareRoot) over F_v^{alg} which we can solve by the above. Otherwise, if all three symbols in Proposition 5.5 are -1, then also by Hensel's lemma, Problem (ExhibitPoint) over F_v^{alg} is reducible to Problem (ExhibitPoint) over k_v, which was discussed at the end of the previous section.

If we restrict our input to a global field F, then a runtime analysis of the above method yields the following.

Proposition 5.8. *Let F be a number field and let v be an odd place of F. Then there exists a deterministic polynomial-time algorithm to evaluate the Hilbert symbol $(a,b)_v$ for $a,b \in F^\times$.*

Remark 5.9. By *Hilbert reciprocity*, we have

$$\prod_v (a,b)_v = 1 \tag{5.10}$$

whenever F is a global field and $a,b \in F^\times$. Consequently, if one can compute all but one local Hilbert symbol $(a,b)_v$, then the final symbol can be recovered from the above relation. In particular, this means for a number field F, if there exists a unique prime above 2 (e.g. when $F = \mathbb{Q}$) then one can evaluate $(a,b)_2$ in this way.

6. The even local Hilbert symbol

In this section, we discuss the computation of the local Hilbert symbol for an even place of a number field F. The main result of this section is the following theorem.

Theorem 6.1. *Let F be a number field and let v be a place of F. Then there exists a deterministic polynomial-time algorithm to evaluate the Hilbert symbol $(a,b)_v$ for $a,b \in F^\times$.*

If v is complex, this theorem is trivial; if v is an odd place of F then Theorem 6.1 follows from Proposition 5.8. So suppose that v is an even place of F, i.e. $\#k_v$ is even. Let $\mathbb{Z}_F$ be the ring of integers of F and let $\mathfrak{p}$ be the prime of $\mathbb{Z}_F$ corresponding to v.

We first give an algorithm which gives a solution to an integral norm form via a Hensel-like lift.

Algorithm 6.2. Let $\mathfrak{p}$ an even prime with ramification index $e = \operatorname{ord}_{\mathfrak{p}} 2$, and let $a,b \in F$ be such that $\operatorname{ord}_{\mathfrak{p}}(a) = 0$ and $\operatorname{ord}_{\mathfrak{p}}(b) = 1$. This algorithm outputs a solution to the congruence

$$1 - ay^2 - bz^2 \equiv 0 \pmod{\mathfrak{p}^{2e}}$$

with $y,z \in \mathbb{Z}_F/\mathfrak{p}^{2e}$ and $y \in (\mathbb{Z}_F/\mathfrak{p})^\times$.

1. Let $f \in \mathbb{Z}_{\geq 1}$ be the residue class degree of $\mathfrak{p}$ (so that $\#(\mathbb{Z}_F/\mathfrak{p}) = 2^f$) and let $q = 2^f$. Let π be a uniformizer at $\mathfrak{p}$.
2. Initialize $(y,z) := (1/\sqrt{a}, 0)$.
3. Let $N := 1 - ay^2 - bz^2 \in \mathbb{Z}_F/4\mathbb{Z}_F$ and let $t := \operatorname{ord}_{\mathfrak{p}}(N)$. If $t \geq 2e$, return y,z. Otherwise, if t is even, let

$$y := y + \sqrt{\frac{N}{a\pi^t}}\pi^{t/2}$$

and if t is odd, let

$$z := z + \sqrt{\frac{N}{b\pi^{t-1}}}\pi^{\lfloor t/2 \rfloor}.$$

Return to Step 3.

In this algorithm, when we write $\sqrt{u}$ for $u \in (\mathbb{Z}_F/\mathfrak{p}^{2e})^\times$ we mean any choice of a lift of $\sqrt{u} \in (\mathbb{Z}_F/\mathfrak{p})^\times$ to $\mathbb{Z}_F/\mathfrak{p}^{2e}$.

Proof of correctness. The key calculation in Step 3 is as follows: if t is even, we make the substitution

$$1 - a(y + u\pi^{t/2})^2 - bz^2 = N - 2au\pi^{t/2}y - au^2\pi^t \equiv 0 \pmod{\mathfrak{p}^{t+1}}$$

and solve for u. Note that since $t < 2e$ we have $\operatorname{ord}_\mathfrak{p}(2\pi^{t/2}) = e+t/2 \geq t+1$; solving we get $u^2 \equiv N/(a\pi^t) \pmod{\mathfrak{p}}$ as claimed. The case where t is odd is similar: we have

$$\begin{aligned} 1 - ay^2 - b(z + \sqrt{N/b\pi^{t-1}}\pi^{\lfloor t/2 \rfloor})^2 &= N - 2bz\sqrt{N/b\pi^{t-1}}\pi^{\lfloor t/2 \rfloor} - b(N/b\pi^{t-1})\pi^{t-1} \\ &\equiv N - N \equiv 0 \pmod{\mathfrak{p}^{t+1}} \end{aligned}$$

and the middle term above vanishes modulo $\mathfrak{p}^{t+1}$ since $t < 2e$ implies $e+1+\lfloor t/2 \rfloor = e + 1 + (t-1)/2 \geq t + 1$. □

Remark 6.3. Alternatively, we can compute a solution modulo 2 directly. The map

$$\begin{aligned} (\mathbb{Z}_F/\mathfrak{p}^e)^2 &\to \mathbb{Z}_F/2\mathbb{Z}_F \\ (y, z) &\mapsto 1 - ay^q - bz^q \end{aligned}$$

is $\mathbb{Z}_F/\mathfrak{p} \cong \mathbb{F}_q$-linear since $2 \equiv 0 \pmod{\mathfrak{p}^e}$. Let (y_0, z_0) be in the kernel of this map. Letting $(x, y, z) := (1, y_0^{q/2}, z_0^{q/2})$, we see $1 - ay^2 - bz^2 \equiv 0 \pmod{2}$.

Remark 6.4. This is better than the algorithm provided in Simon's thesis [35] because we do not need to make a brute force search, which might not run in polynomial time.

We reduce to the above Hensel lift by the following algorithm.

Algorithm 6.5. Let $\mathfrak{p}$ an even prime with ramification index $e = \operatorname{ord}_\mathfrak{p} 2$ and let $a, b \in F^\times$ be such that $v(a) = 0$ and $v(b) \in \{0, 1\}$. This algorithm outputs $y, z, w \in \mathbb{Z}_F/\mathfrak{p}^{2e}$ such that

$$1 - ay^2 - bz^2 + abw^2 \equiv 0 \pmod{\mathfrak{p}^{2e}}$$

and $y \in (\mathbb{Z}_F/\mathfrak{p})^\times$. Let π be a uniformizer for $\mathfrak{p}$.

1. If $v(b) = 1$, return the output $(y, z, 0)$ of Algorithm 6.2 with input a, b.
2. Suppose $a \in (\mathbb{Z}_F/\mathfrak{p}^e\mathbb{Z}_F)^{\times 2}$ and $b \in (\mathbb{Z}_F/\mathfrak{p}^e\mathbb{Z}_F)^{\times 2}$. Let $(a_0)^2 a \equiv 1 \pmod{\mathfrak{p}^e}$ and $(b_0)^2 b \equiv 1 \pmod{\mathfrak{p}^e}$. Return
$$y := a_0,\ z := b_0,\ w := a_0 b_0.$$
3. Swap a, b if necessary so that $a \in (\mathbb{Z}_F/\mathfrak{p}^e\mathbb{Z}_F)^\times \setminus (\mathbb{Z}_F/\mathfrak{p}^e\mathbb{Z}_F)^{\times 2}$. Let t be the largest integer such that $a \in (\mathbb{Z}_F/\mathfrak{p}^t)^{\times 2}$ but $a \notin (\mathbb{Z}_F/\mathfrak{p}^e)^{\times 2}$. Then t is odd; write $a = a_0^2 + \pi^t a_t$ with $a_0, a_t \in \mathbb{Z}_F$. Let y, z be the output of Algorithm 6.2 with input $a' := a$, $b' := -\pi a_t/b$. Return
$$y' := \frac{1}{a_0},\ z' := \frac{\pi^{\lfloor t/2 \rfloor}}{a_0 z},\ w' := \frac{y\pi^{\lfloor t/2 \rfloor}}{a_0 z}$$

(reswapping if necessary).

Proof of correctness. In Step 2, writing $aa_0^2 = 1 + 2a'$ and $bb_0^2 = 1 + 2b'$ with $a', b' \in \mathbb{Z}_F$ we indeed have

$$1-a(a_0)^2-b(b_0)^2+ab(a_0b_0)^2 = 1-(1+2a')-(1+2b')+(1+2a')(1+2b') \equiv 0 \pmod{\mathfrak{p}^{2e}}$$

since $4 \in \mathfrak{p}^{2e}$.

Now we discuss Step 3. Write $a = a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1}$ with $a_i \in \mathbb{Z}_F/\mathfrak{p}$. Then indeed $a \in (\mathbb{Z}_F/\mathfrak{p}^e)^{\times 2}$ if and only if and $a_i = 0$ for i odd by the freshperson's dream, so in particular $t < e$ is odd. Now suppose from Algorithm 6.2 we have

$$1 - ay^2 + (\pi a_t/b)z^2 \equiv 0 \pmod{\mathfrak{p}^{2e}}.$$

Note $\operatorname{ord}_{\mathfrak{p}}(z) \le \lfloor t/2 \rfloor = (t-1)/2$ since otherwise $a \in (\mathbb{Z}_F/\mathfrak{p}^{t+1})^{\times 2}$, a contradiction. Multiplying by $-b\pi^{t-1}/z^2 = -b(\pi^{\lfloor t/2 \rfloor}/z)^2$ gives

$$-b(\pi^{\lfloor t/2 \rfloor}/z)^2 + ab(y\pi^{\lfloor t/2 \rfloor}/z)^2 - \pi^t a_t \equiv 0 \pmod{\mathfrak{p}^{2e}}$$

so

$$a_0^2 - (a_0^2 + \pi^t a_t) - b(\pi^{\lfloor t/2 \rfloor}/z)^2 + ab(y\pi^{\lfloor t/2 \rfloor}/z)^2 \equiv 0 \pmod{\mathfrak{p}^{2e}}$$

so since $a = a_0^2 + \pi^t a_t$, dividing by a_0^2 we have the result. □

We say that $\pi^{-1} \in F$ is an *inverse uniformizer* for $\mathfrak{p}$ if $\operatorname{ord}_{\mathfrak{p}}(\pi^{-1}) = -1$ and $\operatorname{ord}_{\mathfrak{q}}(\pi^{-1}) \ge 0$ for all $\mathfrak{q} \ne \mathfrak{p}$.

We are now prepared to evaluate the even Hilbert symbol.

Algorithm 6.6. Let $B = \left(\dfrac{a, b}{F}\right)$ be a quaternion algebra with $a, b \in F^\times$, and let $\mathfrak{p}$ be an even prime of F. This algorithm returns the value of the Hilbert symbol $(a, b)_{\mathfrak{p}}$.

1. Scale a, b if necessary by an element of $\mathbb{Q}^{\times 2} \cap \mathbb{Z}$ so that $a, b \in \mathbb{Z}_F$.
2. Let π^{-1} be an inverse uniformizer for $\mathfrak{p}$. Let $a := (\pi^{-1})^{2\lfloor \operatorname{ord}_{\mathfrak{p}}(a)/2 \rfloor} a$ and $b := (\pi^{-1})^{2\lfloor \operatorname{ord}_{\mathfrak{p}}(b)/2 \rfloor} b$. If $\operatorname{ord}_{\mathfrak{p}} a = \operatorname{ord}_{\mathfrak{p}} b = 1$, let $a := (\pi^{-1})^2(-ab)$. Swap if necessary so that $\operatorname{ord}_{\mathfrak{p}} a = 0$.
3. Call Algorithm 6.5, and let $i' := (1 + yi + zj + wij)/2$. Let $f(T) = T^2 - T + \operatorname{nrd}(i')$ be the minimal polynomial of i'. If f has a root modulo $\mathfrak{p}$, return 1.
4. Let $j' := (zb)i - (ya)j$ and let $b' := (j')^2$. If $\operatorname{ord}_v b'$ is even, return 1, otherwise return -1.

Proof of correctness. If in Step 2 we have a root modulo $\mathfrak{p}$, then by Hensel's lemma, f has a root $t \in F_{\mathfrak{p}}$, hence $t - i'$ is a zero divisor and we return 1 correctly. Otherwise, by Lemma 5.4, we have $K_{\mathfrak{p}} = F_{\mathfrak{p}}[i']$ is the unramified field extension of $F_{\mathfrak{p}}$. We compute that $\operatorname{trd}(j') = \operatorname{trd}(i'j') = 0$, so $B_{\mathfrak{p}} \cong \left(\dfrac{K_{\mathfrak{p}}, b'}{F_{\mathfrak{p}}}\right)$ and $B_{\mathfrak{p}}$ is split if and only if $\operatorname{ord}_{\mathfrak{p}} b'$ is even. □

Note that the above algorithms run in deterministic polynomial time.

Example 6.7. Let $F = \mathbb{Q}(u)$ where $u = \sqrt[8]{500}$. Then $2\mathbb{Z}_F = (2, \sqrt[8]{500})^4 = \mathfrak{p}^4$, so $\mathbb{Z}_{F,\mathfrak{p}}$ is a ramified extension of $\mathbb{Z}_2$ of residue degree 2 and ramification degree $e = 4$. Using Algorithm 6.6, we compute $(a, b)_{\mathfrak{p}}$ where $b = u^2 + 40$ and $a = u^2 + u + 1$.

In Step 2, we compute the inverse uniformizer $\pi^{-1} = u^3/10$ satisfying the polynomial $T^8 - 5/4$. We compute $\operatorname{ord}_{\mathfrak{p}}(a) = 0$ and $\operatorname{ord}_{\mathfrak{p}}(b) = 2$. So we let $b := (\pi^{-1})^2 b = \frac{1}{5}(2u^6 + 25)$ with now $\operatorname{ord}_{\mathfrak{p}}(b) = 0$.

In Step 3, we call Algorithm 6.5. We use the uniformizer $\pi = u$. We compute that $b \equiv 1 \pmod{\mathfrak{p}^e}$ so $b \in (\mathbb{Z}_F/\mathfrak{p}^e\mathbb{Z}_F)^{\times 2}$ but $a \equiv 1 + \pi + \pi^2 \pmod{\mathfrak{p}^e}$. So we write $a = a_0 + \pi^t a_t$ with $a_0 = 1$ and $a_t = u + 1$.

We then call Algorithm 6.2 with input $a' := a$ and $b' := -\pi a_t/b$. We initialize $(y, z) = (1, 0)$. In Step 3 of this algorithm, we have $N := 1-(1+u+u^2) = -(u+u^2)$ with valuation $t := 1$. We let $z := \sqrt{N/b} = 1$ and return; now $N := 1 - ay^2 - bz^2$ has valuation $t := 9 > 2e$, so we exit the loop with output $y = z = 1$.

We then exit Algorithm 6.5 with $y' := 1/a_0 = 1$, $z' := \pi^{\lfloor t/2 \lfloor}/(a_0 z) = 1$, and $w' := y\pi^{\lfloor t/2 \lfloor}/(a_0 z) = 1$. We verify that $1-a(y')^2-b(z')^2+ab(w')^2 = 1-a-b+ab \equiv 0 \pmod 4$.

Returning to Algorithm 6.6, we let $i' := (1+i+j+ij)/2$ and compute $\operatorname{nrd}(i') = 1/10(w^7 + 10w^2 + 10w + 500) \equiv 0 \pmod{\mathfrak{p}}$, so $f(T) = T^2 - T + \operatorname{nrd}(i')$ has a root modulo $\mathfrak{p}$, and we return $(a, b)_{\mathfrak{p}} = 1$.

Computing the Jacobi symbol. An interesting consequence of the above algorithm is that one can evaluate the Jacobi symbol in deterministic polynomial time in certain cases analogous to the way ("reduce and flip") that one computes this symbol using quadratic reciprocity in the case $F = \mathbb{Q}$. (See Lenstra [23] for an alternative approach which works in greater generality.)

We extend the definition of the Legendre symbol (5.7) to a symbol $\left(\dfrac{a}{\mathfrak{b}}\right)$ with $\mathfrak{b}$ odd by multiplicativity, and we define $\left(\dfrac{a}{b}\right) = \left(\dfrac{a}{b\mathbb{Z}_F}\right)$.

We write $v \mid 2\infty$ for the set of finite even places and real archimedean places of F.

Proposition 6.8. *Let $a, b \in \mathbb{Z}_F$ satisfy $a\mathbb{Z}_F + b\mathbb{Z}_F = \mathbb{Z}_F$, with b odd, and suppose $a = a_0 a_1$ with a_1 odd. Then*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a_1}\right) = \prod_{v \mid 2\infty} (a, b)_v.$$

Proof. By Hilbert reciprocity (5.10), we have

$$\prod_v (a, b)_v = 1 = \prod_{v \mid 2\infty} (a, b)_v \prod_{\mathfrak{p} \nmid 2} (a, b)_{\mathfrak{p}}.$$

By Lemma 5.5, if $\mathfrak{p}$ is odd and $\operatorname{ord}_{\mathfrak{p}}(a) = \operatorname{ord}_{\mathfrak{p}}(b) = 0$ then $(a, b)_{\mathfrak{p}} = 1$. Therefore

$$\prod_{\mathfrak{p} \mid a_1 b} (a, b)_{\mathfrak{p}} = \prod_{v \mid 2\infty} (a, b)_v.$$

For $\mathfrak{p}$ odd, if $\operatorname{ord}_{\mathfrak{p}} a_1 > 0$ then $\operatorname{ord}_{\mathfrak{p}} b = 0$ by assumption and thus

$$(a, b)_{\mathfrak{p}} = \left(\frac{b}{\mathfrak{p}}\right)^{\operatorname{ord}_{\mathfrak{p}} a} = \left(\frac{b}{\mathfrak{p}}\right)^{\operatorname{ord}_{\mathfrak{p}} a_1}.$$

Similarly if $\operatorname{ord}_{\mathfrak{p}} b > 0$ then $(a, b)_{\mathfrak{p}} = \left(\frac{a}{\mathfrak{p}}\right)^{\operatorname{ord}_{\mathfrak{p}} b}$, hence

$$\prod_{\mathfrak{p} \mid a_1 b} (a, b)_{\mathfrak{p}} = \left(\frac{a}{b}\right)\left(\frac{b}{a_1}\right).$$

The result follows. □

A *Euclidean function* on F is a map $N : \mathbb{Z}_F \backslash \{0\} \to \mathbb{Z}_{\geq 0}$ such that for all $a, b \in \mathbb{Z}_F$ we have $N(ab) = N(a)N(b)$ and there exists $q, r \in \mathbb{Z}_F$ such that $a = qb + r$ with either $r = 0$ or $N(r) < N(b)$. A Euclidean function is *computable* if given a, b, the elements q, r as above are computable.

Algorithm 6.9. Let F be a number field with a computable Euclidean function N and let $a, b \in \mathbb{Z}_F \setminus \{0\}$. This algorithm returns the Jacobi symbol $\left(\dfrac{a}{b}\right)$.

1. Initialize $z = 1$.
2. If $b\mathbb{Z}_F = \mathbb{Z}_F$, return z. Otherwise, compute $q, r \in \mathbb{Z}_F$ such that $a = qb + r$. If $r = 0$, return 0. Let $a := r$. Write $a = a_0 a_1$ with $a_1 \in \mathbb{Z}_F$ odd.
3. Multiply z by $\prod_{v \mid 2,\infty} (a, b)_v$, computed using Algorithm 6.6. Return to Step 2, with $(a, b) = (b, a_1)$.

Proof of correctness. The division algorithm associated to N implies that $\mathbb{Z}_F$ has unique factorization, so we can indeed write $a = a_0 a_1$ with a_1 odd. The algorithm terminates because in Step 4 we have $N(a_1) \leq N(a) = N(r) < N(b)$. □

Remark 6.10. For any fixed F, one can precompute a table of the values $(a, b)_{\mathfrak{p}}$ for a, b in appropriate residue classes modulo an even prime $\mathfrak{p}$; this is what is usually done for $F = \mathbb{Q}$, for example.

Relationship to conics. In view of the results in Section 4, we now relate the above algorithms to the geometric problem of rational points on conics.

Theorem 6.11 (Hasse-Minkowski). *A quaternion algebra B has $B \cong \mathrm{M}_2(F)$ if and only if B is unramified at all places.*

Equivalently, a conic C has $C(F) \neq \emptyset$ if and only if $C(F_v) \neq \emptyset$ for all places v of F. For a proof of the Hasse-Minkowski Theorem, see Lam [21], O'Meara [26], or Vignéras [38, §III.3.1]

Proposition 6.12. *Problem* (IsMatrixRing) *is deterministic polynomial-time reducible to the problem of factoring ideals in $\mathbb{Z}_F$.*

Proof. Given a quaternion algebra $B = \left(\dfrac{a, b}{F}\right)$, we have $B_v \cong \mathrm{M}_2(F_v)$ for all $v \nmid 2ab\infty$, and by factoring by the above algorithms for each $v \mid 2ab\infty$ we check if $B_v \cong \mathrm{M}_2(F_v)$ by computing the Hilbert symbol $(a, b)_v$ in deterministic polynomial time. □

7. Maximal orders

In this section, we consider some integral versions (for orders) of the above algorithms relating quadratic forms and quaternion algebras. Our main result relates identifying the matrix ring to computing a maximal order. Throughout this section, let F be a number field, let $\mathbb{Z}_F$ be its ring of integers, and let $\mathcal{O}$ be a ($\mathbb{Z}_F$-)order in a quaternion algebra B over F. For further reading, see Reiner [28] or Vignéras [38].

Computing maximal orders, generally. There exists a deterministic algorithm to compute the ring of integers $\mathbb{Z}_F$ (see Cohen [6, §6.1], [7, Algorithm 2.4.9]): in fact, computing $\mathbb{Z}_F$ is deterministic polynomial-time equivalent to the problem of finding the largest square divisor of a positive integer [5, 22]; no polynomial-time algorithm is known for this problem (though see work of Buchmann and Lenstra [4] for a way of "approximating" $\mathbb{Z}_F$).

Example 7.1. If $F = \mathbb{Q}(\sqrt{D})$, then $R = \mathbb{Z} \oplus \mathbb{Z}(d + \sqrt{d})/2$ where $D = df^2$ and f^2 is the largest square divisor of D subject to the requirement that $d \equiv 0, 1 \pmod 4$.

We consider in this section the noncommutative analogues of this problem. We have the following general result due to Ivanyos and Rónyai [16, Theorem 5.3], which was rediscovered by Nebe and Steel [24]; see also Friedrichs [11].

Theorem 7.2. *There exists an explicit algorithm which, given a semisimple F-algebra B, computes a maximal order $\mathcal{O} \subset B$. This algorithm runs in deterministic polynomial time given oracles for the problems of factoring integers and factoring polynomials over finite fields.*

At present, it is not known if there exist deterministic polynomial-time algorithms to solve either of these latter two problems. Indeed, we have already noted that computing a maximal order in F is as hard as computing the largest squarefree divisor of a positive integer; therefore, it is reasonable to expect that the problem for a noncommutative algebra B is no less complicated. (See a more precise characterization of this complexity at the end of this section.)

We do not discuss the algorithm exhibited in Theorem 7.2; rather, we consider the special case of quaternion algebras, and by manipulations with quadratic forms we obtain a simpler algorithm.

Discriminants. We begin by analyzing the following problem.

Problem 7.3 (IsMaximal)**.** *Given an order $\mathcal{O} \subset B$, determine if $\mathcal{O}$ is a maximal order.*

This problem has a very simple solution as follows. The *discriminant* $\mathfrak{D}(B)$ of B is the ideal equal to the product of all primes of $\mathbb{Z}_F$ where B is ramified:

$$\mathfrak{D}(B) = \prod_{\mathfrak{p} \text{ ramified}} \mathfrak{p}.$$

On the other hand, the *discriminant* $\operatorname{disc}(\mathcal{O})$ of an order $\mathcal{O} \subset B$ is the ideal generated by the set

$$\{\det(\operatorname{trd}(x_i x_j))_{i,j=1,\dots,4} : x_1, \dots, x_4 \in \mathcal{O}\}.$$

The discriminant $\operatorname{disc}(\mathcal{O})$ is the square of an ideal in $\mathbb{Z}_F$, and the *reduced discriminant* $\mathfrak{d}(\mathcal{O})$ of $\mathcal{O}$ is the ideal satisfying $\mathfrak{d}(\mathcal{O})^2 = \operatorname{disc}(\mathcal{O})$.

Given a pseudobasis $(\mathfrak{a}_i, x_i)$ for $\mathcal{O}$ we have

$$\operatorname{disc}(\mathcal{O}) = (\mathfrak{a}_1 \cdots \mathfrak{a}_4)^2 \det(\operatorname{trd}(x_i x_j))_{i,j=1,\dots,4}.$$

Remark 7.4. Although we will not use this in the sequel, the reduced discriminant can in fact be computed more simply: if $\mathcal{O} = \mathbb{Z}_F \oplus \mathfrak{a}i \oplus \mathfrak{b}j \oplus \mathfrak{c}k$ then

$$\mathfrak{d}(\mathcal{O}) = \mathfrak{abc}\operatorname{trd}((ij - ji)\overline{k}).$$

Lemma 7.5. *An order $\mathcal{O} \subset B$ is maximal if and only if $\mathfrak{d}(\mathcal{O}) = \mathfrak{D}(B)$.*

Proof. We give only a sketch of the proof. For a prime $\mathfrak{p}$ of $\mathbb{Z}_F$, let $\mathbb{Z}_{F,\mathfrak{p}}$ be the completion of $\mathbb{Z}_F$ at $\mathfrak{p}$ and $F_\mathfrak{p}$ the completion of F at $\mathfrak{p}$; write $\mathcal{O}_\mathfrak{p} = \mathcal{O} \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{p}}$ and similarly $B_\mathfrak{p} = B \otimes_F F_\mathfrak{p}$.

We have $\mathfrak{d}(\mathcal{O}) = \mathfrak{D}(B)$ if and only if $\mathfrak{d}(\mathcal{O})_\mathfrak{p} = \mathfrak{d}(\mathcal{O}_\mathfrak{p}) = \mathfrak{D}(B_\mathfrak{p}) = \mathfrak{D}(B)_\mathfrak{p}$ for all primes $\mathfrak{p}$, and the order $\mathcal{O}$ is maximal if and only if $\mathcal{O}_\mathfrak{p}$ is maximal for every prime $\mathfrak{p}$ of $\mathbb{Z}_F$ (see [28, 11.2]). So it suffices to note that if $\mathfrak{p}$ is unramified then any maximal order of $B_\mathfrak{p}$ has discriminant $\mathbb{Z}_{F,\mathfrak{p}}$ and if $\mathfrak{p}$ is ramified then the unique maximal order of $B_\mathfrak{p}$ has reduced discriminant $\mathfrak{p}\mathbb{Z}_{F,\mathfrak{p}}$ [28, Theorem 14.9]. □

Putting these together with the computation of the local Hilbert symbol, we have shown that one can solve Problem (IsMaximal) in deterministic polynomial time given an oracle to factor integers and polynomials over finite fields, since this allows the factorization of the discriminant $\mathfrak{D}(B)$ [6, Proposition 6.2.8, Algorithm 6.2.9]; note that this need only be done once for a quaternion algebra B.

Computing maximal orders. We now turn to the problem of computing a maximal order in a quaternion algebra.

Problem 7.6 (AlgebraMaxOrder). *Given a quaternion algebra B over F, compute a maximal order $\mathcal{O} \subset B$.*

A more general problem is as follows.

Problem 7.7 (MaxOrder). *Given an order $\Lambda \subset B$ in a quaternion algebra B over F, compute a maximal order $\mathcal{O} \supset \Lambda$.*

One immediately reduces from the former to the latter by exhibiting any order in B, as follows. (First, we compute $\mathbb{Z}_F$ as above; this can be considered a precomputation step if F is fixed.) If $B = \left(\dfrac{a,b}{F}\right)$, we may scale a, b by a nonzero square integer so that $a, b \in \mathbb{Z}_F$, and then

$$\Lambda = \mathbb{Z}_F \oplus \mathbb{Z}_F i \oplus \mathbb{Z}_F j \oplus \mathbb{Z}_F ij \tag{7.8}$$

is an order, where i, j are the standard generators for B.

An order $\mathcal{O}$ is $\mathfrak{p}$-*maximal* for a prime $\mathfrak{p}$ if $\mathcal{O}_\mathfrak{p} = \mathcal{O} \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{p}}$ is maximal (as an $\mathbb{Z}_{F,\mathfrak{p}}$-order). Note that if $\mathrm{ord}_\mathfrak{p}(\mathfrak{d}(\mathcal{O}_\mathfrak{p})) = 0$ then necessarily $\mathcal{O}$ is $\mathfrak{p}$-maximal. To solve Problem (MaxOrder), we recursively compute a $\mathfrak{p}$-maximal order for every prime $\mathfrak{p} \mid \mathfrak{d}(\mathcal{O})$, proceeding in two steps.

We say an order $\mathcal{O}$ is $\mathfrak{p}$-*saturated* if $\mathrm{nrd}\,|_{\mathcal{O}_\mathfrak{p}}$ has a normalized basis $1, i, j, k$ (see Proposition 3.10) such that each atomic block has valuation at most 1; we then say that $1, i, j, k$ is a $\mathfrak{p}$-*saturated* basis for $\mathcal{O}$.

We compute a $\mathfrak{p}$-saturated order in the following straightforward way. Recall that $\pi^{-1} \in F$ is an *inverse uniformizer* for $\mathfrak{p}$ if $\mathrm{ord}_\mathfrak{p}(\pi^{-1}) = -1$ and $\mathrm{ord}_\mathfrak{q}(\pi^{-1}) \geq 0$ for all $\mathfrak{q} \neq \mathfrak{p}$.

Algorithm 7.9. Let

$$\Lambda = \mathbb{Z}_F \oplus \mathfrak{a} i \oplus \mathfrak{b} j \oplus \mathfrak{c} k \subset B$$

be an order and let $\mathfrak{p}$ be prime. This algorithm computes a $\mathfrak{p}$-saturated order $\mathcal{O} \supset \Lambda$ and a $\mathfrak{p}$-saturated basis for $\mathcal{O}$.

1. Choose $d \in \mathfrak{a}$ such that $\mathrm{ord}_\mathfrak{p}(d) = \mathrm{ord}_\mathfrak{p}(\mathfrak{a})$ and let $i := di$; compute similarly with j, k. Let $\mathcal{O} := \Lambda$.

2. Run Algorithm 3.12 over the localization of $\mathbb{Z}_F$ at $\mathfrak{p}$ with input the quadratic form $\operatorname{nrd}|_{\mathcal{O}}$ and the basis $1, i, j, k$; let $1, i^*, j^*, k^*$ be the output. Let $c \in \mathbb{Z}_F$ be such that $\operatorname{ord}_{\mathfrak{p}} c = 0$ and such that $ci^* \in \mathcal{O}$, and let $i := ci^*$; compute similarly with j, k.
3. Let π^{-1} be an inverse uniformizer for $\mathfrak{p}$. For each atomic form Q in $\operatorname{nrd}_{\mathcal{O}}$, let e be the valuation of Q, and multiply each basis element in Q by $(\pi^{-1})^{\lfloor e/2 \rfloor}$. Return $\mathcal{O} := \Lambda + (\mathbb{Z}_F i \oplus \mathbb{Z}_F j \oplus \mathbb{Z}_F k)$ and the basis $1, i, j, k$.

Proof of correctness. In Step 3, we are asserting that the output of Algorithm 3.12 leaves 1 as the first basis element. Indeed, we note that $\operatorname{ord}_{\mathfrak{p}} \operatorname{trd}(j) \leq \operatorname{ord}_{\mathfrak{p}} \operatorname{trd}(i(ij))$ since $\operatorname{trd}(i(ij)) = \operatorname{trd}(i)^2 - \operatorname{trd}(j)\operatorname{nrd}(i)$ and similarly $\operatorname{ord}_{\mathfrak{p}} \operatorname{trd}(i) \leq \operatorname{ord}_{\mathfrak{p}} \operatorname{trd}((ij)j)$.

Let $1, i, j, k$ be the basis computed in Step 3. By definition, this basis is $\mathfrak{p}$-saturated; we need to show that $\mathcal{O}$ is indeed an order. But $\mathcal{O}$ is an order if and only if $\mathcal{O}_{\mathfrak{q}}$ is an order for all primes $\mathfrak{q}$, and we have $\mathcal{O}_{\mathfrak{q}} = \Lambda_{\mathfrak{q}}$ for all primes $\mathfrak{q} \neq \mathfrak{p}$.

For any $x, y \in B$ we have $xy + yx = \operatorname{trd}(y)x + \operatorname{trd}(x)y - T(x,y)$, so if $\mathcal{O}$ is an order then $\mathcal{O} + \mathbb{Z}_F x$ is multiplicatively closed if and only if $T(x,y) \in \mathbb{Z}_F$ for all $y \in \mathcal{O}$. We have $T(x,y) = 0$ if x, y are orthogonal, and if x, y are a basis for an atomic block Q then by definition the valuation of $T(x,y)$ is at least the valuation of Q and so we can multiply each by $(\pi^{-1})^{\lfloor e/2 \rfloor}$, preserving integrality. □

After $\mathfrak{p}$-saturating, one can compute a maximal order as follows.

Algorithm 7.10. Let Λ be an order and let $\mathfrak{p}$ be prime. This algorithm computes a $\mathfrak{p}$-maximal order $\mathcal{O} \supset \Lambda$.

1. Compute a $\mathfrak{p}$-saturated order $\mathcal{O} \supset \Lambda$ and let $1, i, j, k$ be a $\mathfrak{p}$-saturated basis for $\mathcal{O}$. Let π^{-1} be an inverse uniformizer for $\mathfrak{p}$.
2. Suppose $\mathfrak{p}$ is odd. Swap i for j or k if necessary so that $a := i^2$ has $\operatorname{ord}_{\mathfrak{p}}(a) = 0$. Let $b := j^2$. If $\operatorname{ord}_{\mathfrak{p}} b = 0$, return $\mathcal{O}$. Otherwise, if $\operatorname{ord}_{\mathfrak{p}} b = 1$ and $(a/\mathfrak{p}) = 1$, solve
$$x^2 \equiv a \pmod{\mathfrak{p}}$$
for $x \in \mathbb{Z}_F/\mathfrak{p}$. Adjoin the element $\pi^{-1}(x - i)j$ to $\mathcal{O}$, and return $\mathcal{O}$.
3. Otherwise, $\mathfrak{p}$ is even. Let $t := \operatorname{trd}(i)$, let $a := -\operatorname{nrd}(i)$, and let $b := j^2$.
   a. Suppose $\operatorname{ord}_{\mathfrak{p}} t = 0$. If $\operatorname{ord}_{\mathfrak{p}} b = 0$, return $\mathcal{O}$. If $\operatorname{ord}_{\mathfrak{p}} b = 1$ and $T^2 - tT + a = 0$ has a root x modulo $\mathfrak{p}$, and return $\mathcal{O} + \mathbb{Z}_F \pi^{-1}(x - i)j$.
   b. Suppose $\operatorname{ord}_{\mathfrak{p}} \operatorname{trd}(i) > 0$. Let y, z, w be the output of Algoritm 6.5 with input a, b. Let
$$i' := (\pi^{-1})^e (1 + yi + zj + wij).$$
   Adjoin i' to $\mathcal{O}$, and return to Step 1.

Proof of correctness. At every step in the algorithm, for each prime $\mathfrak{q} \neq \mathfrak{p}$ the order $\mathcal{O}_{\mathfrak{q}}$ does not change, so we need only verify that $\mathcal{O}_{\mathfrak{p}}$ is indeed a maximal order.

In Step 2, we have that b is a uniformizer for $\mathfrak{p}$, that $\mathfrak{d}(\mathcal{O}_{\mathfrak{p}}) = 4ab\mathbb{Z}_{F,\mathfrak{p}}$. If $\operatorname{ord}_{\mathfrak{p}}(b) = 0$ then $\operatorname{ord}_{\mathfrak{p}} \mathfrak{d}(\mathcal{O}_{\mathfrak{p}}) = 0$ so $\mathcal{O}$ is indeed maximal. Otherwise, we have $\mathfrak{d}(\mathcal{O}_{\mathfrak{p}}) = \mathfrak{p}$ and $B_{\mathfrak{p}} \cong \left(\dfrac{K_{\mathfrak{p}}, b}{F_{\mathfrak{p}}}\right)$ where $K_{\mathfrak{p}} = F_{\mathfrak{p}}[i]$. We conclude that $B_{\mathfrak{p}}$ is a division ring (and hence $\mathcal{O}_{\mathfrak{p}}$ is maximal) if and only if $(a/\mathfrak{p}) = -1$. If $(a/\mathfrak{p}) = 1$ and $j' = \pi^{-1}(x - i)j$, then $1, i, j', ij'$ form the $\mathbb{Z}_{F,\mathfrak{p}}$-basis for a maximal order, since $(j')^2 = (\pi^{-1})^2(x^2 - a)b \in \mathbb{Z}_{F,\mathfrak{p}}$ and $j'i = -ij'$.

In Step 3, first note that ij is also orthogonal to $1, i$: we have i orthogonal to j so $\operatorname{trd}(ij) = 0$ so ij is orthogonal to 1, and similarly $\operatorname{trd}(ij\bar{i}) = \operatorname{trd}(\operatorname{nrd}(i)j) = 0$.

In particular, we have $B_{\mathfrak{p}} = \left(\dfrac{K_{\mathfrak{p}}, b}{F_{\mathfrak{p}}}\right)$ where $K_{\mathfrak{p}} = F_{\mathfrak{p}}[i]$. By a comparison of discriminants, using the fact that the basis is normalized, we see that $1, i, j, ij$ is a $\mathfrak{p}$-saturated basis for $\mathcal{O}$ as well, so without loss of generality we may take $k = ij$.

Suppose first that $\operatorname{ord}_{\mathfrak{p}} \operatorname{trd}(i) = 0$, so we are in Step 3a. If $\operatorname{ord}_{\mathfrak{p}} b = 0$, then $\operatorname{ord}_{\mathfrak{p}} \mathfrak{d}(\mathcal{O}_{\mathfrak{p}}) = 0$ so $\mathcal{O}_{\mathfrak{p}}$ is maximal. If $\operatorname{ord}_{\mathfrak{p}} b > 0$, then since the basis is $\mathfrak{p}$-saturated we have $\operatorname{ord}_{\mathfrak{p}} b = 1$. Thus as in the case for $\mathfrak{p}$ odd, we have $B_{\mathfrak{p}}$ is a division ring if and only if $K_{\mathfrak{p}}$ is not a field, and as above the adjoining the element $\pi^{-1}(x - i)j$ yields a maximal order.

So suppose we are in Step 3b, so $\operatorname{ord}_{\mathfrak{p}} \operatorname{trd}(i) > 0$. Since $1, i, j, k$ is normalized, we have $\operatorname{ord}_{\mathfrak{p}} \operatorname{trd}(i) = \operatorname{ord}_{\mathfrak{p}} T(1, i) \le \operatorname{ord}_{\mathfrak{p}} T(j, k)$. Adjoining i' to $\mathcal{O}$ gives a $\mathbb{Z}_{F,\mathfrak{p}}$-module with basis $1, i', j, i'j$ since $y \in (\mathbb{Z}_F/\mathfrak{p})^{\times}$; adjoining j' gives a module with basis $1, i', j', i'j'$ for the same reason. We verify that $\mathcal{O}_{\mathfrak{p}}$ after these steps is indeed an order: we have $\operatorname{trd}(i') = 2(\pi^{-1})^e \in \mathbb{Z}_{F,\mathfrak{p}}$ and $\operatorname{nrd}(i') = (\pi^{-1})^{2e}(1 - ay^2 - bz^2 + abw^2) \in \mathbb{Z}_{F,\mathfrak{p}}$ by construction, so at least $\mathbb{Z}_{F,\mathfrak{p}}[i] = \mathbb{Z}_{F,\mathfrak{p}} \oplus \mathbb{Z}_{F,\mathfrak{p}} i$ is a ring. Similarly we have $(j')^2 = b' \in \mathbb{Z}_{F,\mathfrak{p}}$. Finally, we have $\operatorname{trd}(i'i) = 2(\pi^{-1})^e ya$ and $\operatorname{trd}(i'j) = 2(\pi^{-1})^e zb$, so it follows that $\operatorname{trd}(i'j') = 0$, and hence $j'i' = -\overline{i'}j' = -i'j' - \operatorname{trd}(i')j'$, so indeed we have an order. □

Remark 7.11. One must really treat the even and odd prime cases separately. Consider, for example, $F = \mathbb{Q}$, and the quaternion algebra $B = \left(\dfrac{-3, 5}{\mathbb{Q}}\right)$. Then we have the maximal orders $\mathbb{Z}[(1+i)/2] \subset \mathbb{Q}(i) \cong \mathbb{Q}(\sqrt{-3})$ and $\mathbb{Z}[(1+j)/2] \subset \mathbb{Q}(j) \cong \mathbb{Q}(\sqrt{5})$, but we find that

$$\left(\frac{1+j}{2}\right)\left(\frac{1+i}{2}\right) = \left(\frac{1-i}{2}\right)\left(\frac{1+j}{2}\right) + \frac{ij}{2},$$

which is not integral (since $ij/2$ has norm $15/4$).

Remark 7.12. In the proof of correctness for Algorithm 7.10, in each case where $\mathfrak{p}$ is ramified in B we have in fact written $B_{\mathfrak{p}} \cong \left(\dfrac{K_{\mathfrak{p}}, \pi}{F_{\mathfrak{p}}}\right)$ where $K_{\mathfrak{p}}$ is the unramified extension of $F_{\mathfrak{p}}$. The reader will note the similarity between this algorithm and the algorithm to compute the Hilbert symbol: the former extends the latter by taking a witness for the fact that the algebra is split, namely a zerodivisor modulo $\mathfrak{p}$, and uses this to compute a larger order (giving rise therefore to the matrix ring).

Combining these two algorithms, we have the following immediate corollary.

Corollary 7.13. *There exists an algorithm to solve* (ExhibitMatrixRing) *for orders over* $\mathbb{Z}_{F,\mathfrak{p}}$.

(We recall the discussion in Section 4 for the representation of local fields and rings.) In other words, if $\mathcal{O} \subset B$ is an order in a quaternion algebra B over a number field F and $\mathfrak{p}$ is prime of $\mathbb{Z}_F$ which is unramified in B, then there exists an algorithm to compute an explicit embedding $\mathcal{O} \hookrightarrow \mathrm{M}_2(\mathcal{O}_{\mathfrak{p}})$.

Putting these two algorithms together, we have proved the following theorem.

Theorem 7.14. *Problem* (MaxOrder) *is deterministic polynomial-time reducible to the problem of factoring ideals in* $\mathbb{Z}_F$.

Proof. Given any order Λ, we factor its discriminant $\mathfrak{d}(\Lambda)$, and for each prime $\mathfrak{p} \mid \mathfrak{d}(\Lambda)$, we compute a $\mathfrak{p}$-saturated order containing Λ from Algorithm 7.9 and a $\mathfrak{p}$-maximal order $\mathcal{O}$ containing it using Algorithm 7.10. □

Complexity analysis. Given Theorem 7.14, we prove the following result which characterizes the abstract complexity class of this problem, following a hint of Ronyai [30, §6].

Theorem 7.15. *Problem* (AlgebraMaxOrder) *for any fixed number field F is probabilistic polynomial-time equivalent to the problem of factoring integers.*

To prove the theorem, we will use two lemmas. The first lemma is a standard fact.

Lemma 7.16. *The problem of factoring integral ideals $\mathfrak{a}$ of an arbitrary number field is probabilistic polynomial-time equivalent to the problem of factoring integers.*

Proof. Suppose $\mathfrak{a}$ is an integral ideal of F. After factoring the absolute discriminant d_F of F, we can in deterministic polynomial time compute the ring of integers $\mathbb{Z}_F$ of F as above. Now let $\mathfrak{a}$ be an ideal with norm $\mathrm{N}(\mathfrak{a}) = a$. After we factor a, for each prime $p \mid a$, we decompose $p\mathbb{Z}_F = \prod_i \mathfrak{p}_i^{e_i}$ into primes by a probabilistic polynomial time algorithm due to Buchmann and Lenstra [6, Algorithm 6.2.9]: this algorithm uses a probabilistic algorithm to factor polynomials over a finite field, such as the Cantor-Zassenhaus algorithm; see von zur Gathen and Gerhard [13, Theorem 14.14] or Cohen [6, §3.4]. (In fact, for our applications, it suffices to have an algorithm to compute a square root in a finite field, for which we may use the algorithm of Tonelli and Shanks [6, §1.5.1].)

From this list of primes we easily obtain the factorization of $\mathfrak{a}$. Conversely, if one has an algorithm to factor ideals, then one may factor $a\mathbb{Z}_F$ into primes and computing norms we recover the prime factorization of a over $\mathbb{Z}$. □

Remark 7.17. Deterministically, already the problem of finding a nonsquare modulo a prime p is difficult; one unconditional result known is that the smallest quadratic nonresidue of a prime p is of size exponential in $\log p$; under condition of a generalized Riemann hypothesis, one can find a quadratic nonresidue which is of polynomial size in $\log p$.

We will also make use of one other lemma.

Lemma 7.18. *Let $\mathfrak{a}$ be an ideal of $\mathbb{Z}_F$ which is odd, not a square, and not a prime power. Let*

$$S = \left\{ b \in (\mathbb{Z}_F/\mathfrak{a})^\times : \textit{there exist } \mathfrak{p}^e, \mathfrak{q}^f \parallel \mathfrak{a} \textit{ with } \left(\frac{b}{\mathfrak{p}}\right)^e = -1 \textit{ and } \left(\frac{b}{\mathfrak{q}}\right)^f = 1 \right\}.$$

Then $\#S \geq \dfrac{1}{2}\#(\mathbb{Z}_F/\mathfrak{a})^\times$.

Proof. For an ideal $\mathfrak{b}$, let $\Phi(\mathfrak{b}) = \#(\mathbb{Z}_F/\mathfrak{b})^\times$. First consider the case where $\mathfrak{a} = \mathfrak{p}^e\mathfrak{q}^f$ is the product of two prime powers. Without loss of generality, we may assume e is odd. If f is even, then $b \in S$ if and only if $(b/\mathfrak{p}) = -1$, so $\#S = \Phi(\mathfrak{p}^e)/2 \cdot \Phi(\mathfrak{q}^f) = \Phi(\mathfrak{a})/2$. If f is odd, then $\#S = 2(\Phi(\mathfrak{p}^e)/2)(\Phi(\mathfrak{q}^f)/2) = \Phi(\mathfrak{a})/2$.

To conclude, write $\mathfrak{a} = \mathfrak{p}^e\mathfrak{q}^f\mathfrak{b}$ with $\mathfrak{b}$ coprime to $\mathfrak{p}\mathfrak{q}$ and e odd. Then by the preceding paragraph $\#S \geq (1/2)\Phi(\mathfrak{p}^e\mathfrak{q}^f)\Phi(\mathfrak{b}) = \Phi(\mathfrak{a})/2$. □

Proof of Theorem 7.15. Since one can factor ideals in probabilistic polynomial time given an algorithm to factor integers by Lemma 7.16, we may compute a maximal order as in the previous section as the resulting computations run in (deterministic) polynomial time.

Now we prove the converse. Suppose we have an algorithm to solve Problem (AlgebraMaxOrder). Let $a \in \mathbb{Z}_{>0}$ be the integer to be factored, which we may assume without loss of generality is odd, not a prime power, and not a square. We can in constant time (for fixed F) factor the absolute discriminant d_F, so we may also assume $\gcd(a, d_F) = 1$. It follows that the ideal $a\mathbb{Z}_F$ is also odd, not a prime power, and not a square.

We compute a random $b \in \mathbb{Z}_F/a\mathbb{Z}_F$ with $b \neq 0$. Since $\mathrm{N}(a\mathbb{Z}_F) = a^d$ where $d = [F : \mathbb{Q}]$, if $\mathrm{N}(b\mathbb{Z}_F)$ is not a power of a then dividing $\gcd(a^d, \mathrm{N}(b))$ by powers of a we obtain a factor of a. Otherwise, $\mathfrak{a} = a\mathbb{Z}_F + b\mathbb{Z}_F$ is a proper divisor of $a\mathbb{Z}_F$, and we repeat, computing a random $b \in \mathbb{Z}_F/\mathfrak{a}$—in at most d steps, we will either factor a or find an element b such that $a\mathbb{Z}_F + b\mathbb{Z}_F = \mathbb{Z}_F$. Note d depends only on F and not on B, so we find such a b in probabilistic polynomial time.

By Lemma 7.18, we can find in probabilistic polynomial time $b \in (\mathbb{Z}_F/a\mathbb{Z}_F)^\times$ such that $\mathfrak{p}^e, \mathfrak{q}^f \parallel a$ with $(b/\mathfrak{p})^e = -1$ and $(b/\mathfrak{q})^f = 1$, say. Let $B = \left(\dfrac{a, b}{F}\right)$. By hypothesis, calling an algorithm to solve (AlgebraMaxOrder) we may compute a maximal order $\mathcal{O} \subset B$.

We claim that $\mathfrak{p} \mid \mathfrak{d}(\mathcal{O})$ but $\mathfrak{q} \nmid \mathfrak{d}(\mathcal{O})$. Assuming this, we have that $\gcd(\mathrm{N}(\mathfrak{d}(\mathcal{O})), a)$ is a proper factor of a, and the proof is complete.

First we prove that $\mathfrak{p} \mid \mathfrak{d}(\mathcal{O})$. Since $\mathfrak{p}$ is prime to d_F, we know that $\mathfrak{p}$ is unramified in F, and since $\mathfrak{p}^e \parallel a\mathbb{Z}_F$ with e odd, the extension $F(\sqrt{a})/F$ is ramified at $\mathfrak{p}$. Since $(b/\mathfrak{p}) = -1$, by Corollary 5.5, the algebra B is ramified at $\mathfrak{p}$. Therefore by Lemma 7.5, $\mathfrak{p}$ divides the discriminant $\mathfrak{d}(\mathcal{O})$.

Now we show that $\mathfrak{q} \nmid \mathfrak{d}(\mathcal{O})$. If f is even, since $\mathfrak{q}^f \parallel a\mathbb{Z}_F$, we have that $F(\sqrt{a})/F$ is unramified at $\mathfrak{q}$; since also $(b/\mathfrak{q}) \neq 0$, by the same corollary, B is unramified at $\mathfrak{q}$. And if f is odd, then since $(b/\mathfrak{q})^f = 1$ we must have $(b/\mathfrak{q}) = 1$, and again by the corollary it follows that B is unramified. □

Relationship to conics. We return once again to the theme of rational points on conics.

We have seen that given an algorithm to factor integers, one can solve both problems (IsMatrixRing), or equivalently (HasPoint), over a number field F in probabilistic polynomial time by factoring the discriminant and computing Hilbert symbols. We have also seen that (AlgebraMaxOrder) over a number field F is probabilistic polynomial time equivalent to the problem of factoring integers.

We are left to consider (ExhibitMatrixRing), or equivalently (ExhibitPoint). In the special case where $F = \mathbb{Q}$, one shows that again they are reducible to the problem of integer factorization.

Theorem 7.19 (Cremona-Rusin [8], Ivanyos-Szántó [15], Simon [36])**.** *There exists an explicit algorithm to solve* (ExhibitPoint) *over $\mathbb{Q}$ which runs in deterministic polynomial time given an oracle to factor integers.*

From our point of view, the algorithm(s) described in the above theorem can be rephrased in the following way: there exists an explicit algorithm which, given a order $\mathcal{O}$ over $\mathbb{Z}$ of discriminant 1 which is split at ∞, computes a zerodivisor $x \in \mathcal{O}$. This algorithm proceeds by computing a reduced basis of $\mathcal{O}$ with respect to the reduced norm nrd, a kind of indefinite LLL-algorithm.

Question 7.20. Does there exist an algorithm which, given an order $\mathcal{O}$ over $\mathbb{Z}_F$ of discriminant 1 which is split at all real places of F, computes a zerodivisor $x \in \mathcal{O}$?

One possible approach to this conjecture, then, is to provide an indefinite LLL algorithm over F in the special case of $\mathbb{Z}_F$-module of rank 4 and discriminant 1. Perhaps one can prove this at least in the case where $\mathbb{Z}_F$ is computably Euclidean?

We discuss the computational complexity of problem (IsMatrixRing) over $\mathbb{Q}$ in the next section (and relate this to the problem of factoring integers). From the discussion above, it seems reasonable to conjecture the following.

Conjecture 7.21. *Problem* (ExhibitPoint) *over* $\mathbb{Q}$ *is (probabilistic) polynomial-time equivalent to the problem of factoring integers.*

Having treated the case of number fields in some detail, we note that over more general fields, the literature is much less complete.

Question 7.22. For which computable fields F is there an effective algorithm to solve Problems (HasPoint) and (ExhibitPoint)?

For example, one may ask for which fields F is there an effective version of the Hasse-Minkowski theorem? Of course, if one can solve (HasPoint), then given a conic which is known to have a solution one can always simply enumerate the points of $\mathbb{P}^2(F)$ until a solution is found.

8. Residuosity

In this final section, we return to Problem (IsMatrixRing) and characterize its computational complexity. Let F be a number field with ring of integers $\mathbb{Z}_F$.

For a nonzero ideal $\mathfrak{b}$ of $\mathbb{Z}_F$, let $\operatorname{sqrad}(\mathfrak{b})$ be the product of the prime ideals $\mathfrak{p}$ dividing $\mathfrak{b}$ to odd exponent, or equivalently the quotient of $\mathfrak{b}$ by the largest square ideal dividing $\mathfrak{b}$.

Problem (QuadraticResiduosity)**.** *Given an odd ideal* $\mathfrak{b}$ *and* $a \in \mathbb{Z}_F$*, determine if* $a \in (\mathbb{Z}_F/\operatorname{sqrad}(\mathfrak{b}))^{\times 2}$*, i.e., determine if* a *is a quadratic residue modulo* $\operatorname{sqrad}(\mathfrak{b})$.

Problem (QuadraticResiduosity) reduces to the more familiar problem of quadratic residuosity when $\mathfrak{b}$ is a squarefree ideal, namely, to determine if $a \in (\mathbb{Z}_F/\mathfrak{b})^{\times 2}$. If $\mathfrak{b} = \mathfrak{p}$ is a prime ideal, one has $a \in (\mathbb{Z}_F/\mathfrak{p})^{\times 2}$ if and only if $(a/\mathfrak{p}) = 1$, and this Legendre symbol can be evaluated in deterministic polynomial time (as discussed above, by repeated squaring). In general, for $\mathfrak{b}$ squarefree, we have $a \in (\mathbb{Z}_F/\mathfrak{b})^{\times 2}$ if and only if $a \in (\mathbb{Z}_F/\mathfrak{p})^{\times 2}$ for all primes $\mathfrak{p} \mid \mathfrak{b}$. In particular, by this reduction if one can factor $\mathfrak{b}$, one can solve Problem (QuadraticResiduosity). It is a terrific open problem in number theory to determine if the converse holds, even for the case $F = \mathbb{Q}$ and $\mathfrak{b}$ generated by pq with p, q distinct primes.

We first relate the problems (IsMatrixRing) and (QuadraticResiduosity) as follows.

Proposition 8.1. *Problem* (IsMatrixRing) *over* F *is deterministic polynomial-time reducible to Problem* (QuadraticResiduosity) *over* F.

Proof. Let $B = \left(\dfrac{a, b}{F}\right)$ be a quaternion algebra over F. Scaling a, b by an integer square, we may assume $a, b \in \mathbb{Z}_F$. Recall that $B \cong \mathrm{M}_2(F)$ if and only if every place v of F is unramified in B, i.e., if $(a, b)_v = 1$ for all places v of F.

For fixed F, we can in constant (deterministic) time compute the set of even places of F. We then compute the Hilbert symbol $(a,b)_v$ for v real easily and for v even by Algorithm 6.6.

For the odd places, we first apply Lemma 5.5, which implies that we need only check primes $\mathfrak{p} \mid ab\mathbb{Z}_F$. We compute $\mathfrak{g} = a\mathbb{Z}_F + b\mathbb{Z}_F$ and then by small linear combinations we find $g \in \mathfrak{g}^{-1}$ such that $g\mathfrak{g}^{-1}$ is coprime to $a\mathbb{Z}_F$ and $b\mathbb{Z}_F$ and $(a+b)\mathbb{Z}_F$. Now $\left(\dfrac{a,b}{F}\right) \cong \left(\dfrac{a',b'}{F}\right)$ where $a' = a+b$ and $b' = -abg^2$. We claim that after repeating this eventually we will have a and b coprime. Indeed, if $\operatorname{ord}_{\mathfrak{p}}(a) = \operatorname{ord}_{\mathfrak{p}}(b)$ then already $\operatorname{ord}_{\mathfrak{p}}(-abg^2) = 0$, and if $\operatorname{ord}_{\mathfrak{p}}(a) > \operatorname{ord}_{\mathfrak{p}}(b) > 0$, say, then $\operatorname{ord}_{\mathfrak{p}}(-abg^2) = \operatorname{ord}_{\mathfrak{p}}(a) - \operatorname{ord}_{\mathfrak{p}}(b)$ and $\operatorname{ord}_{\mathfrak{p}}(a+b) = \operatorname{ord}_{\mathfrak{p}}(b)$, so then $\operatorname{ord}_{\mathfrak{p}}(a) + \operatorname{ord}_{\mathfrak{p}}(b) > \operatorname{ord}_{\mathfrak{p}}(a) = \operatorname{ord}_{\mathfrak{p}}(a') + \operatorname{ord}_{\mathfrak{p}}(b')$, and since this is a sequence of nonnegative integers eventually either we will have either $\operatorname{ord}_{\mathfrak{p}}(a) = 0$ or $\operatorname{ord}_{\mathfrak{p}}(b) = 0$.

Then for any prime $\mathfrak{p} \mid b\mathbb{Z}_F$, we have that $\mathfrak{p}$ is ramified in B if and only if $\mathfrak{p} \mid \operatorname{sqrad}(b\mathbb{Z}_F)$ and $(a/\mathfrak{p}) = -1$. We can test this latter condition for all $\mathfrak{p} \mid b\mathbb{Z}_F$ by calling the algorithm to solve (QuadraticResiduosity) by determining if a is a quadratic residue modulo $\operatorname{sqrad}(b\mathbb{Z}_F)$. We then repeat this step with a,b interchanged, and we return true if and only if both of these quadratic residuosity tests return true. □

When $F = \mathbb{Q}$, in fact these problems are equivalent.

Theorem 8.2. *Problem* (IsMatrixRing) *over* $\mathbb{Q}$ *is probablistic polynomial-time equivalent to Problem* (QuadraticResiduosity) *over* $\mathbb{Q}$.

Remark 8.3. Rónyai [29, 31] conditionally proves exactly Theorem 8.2 (under the assumption of the Generalized Riemann Hypothesis).

Before proving this theorem, we derive one preliminary result.

Lemma 8.4. *Let* $a,b \in \mathbb{Z}_{>0}$ *be such that* b *is odd and* $(a/b) = 1$. *Let* ℓ *be an odd prime such that* $\ell b \in (\mathbb{Z}/a\mathbb{Z})^{\times 2}$ *and* $\left(\dfrac{a}{\ell}\right) = 1$. *Then* $\left(\dfrac{a,\ell b}{\mathbb{Q}}\right) \cong \mathrm{M}_2(\mathbb{Q})$ *if and only if* a *is a square modulo* $\operatorname{sqrad}(b)$.

Proof. Again, we have $\left(\dfrac{a,\ell b}{\mathbb{Q}}\right) \cong \mathrm{M}_2(F)$ if and only if $(a,\ell b)_v = 1$ for all places v of $\mathbb{Q}$. Since $a > 0$, we know $(a,\ell b)_\infty = 1$. By hypothesis, for all odd $p \mid a$ we have $(\ell b/p) = 1$ hence $(a,\ell b)_p = 1$, and similarly $(a,\ell b)_\ell = 1$. Moreover, since $(a/b) = 1$, the number of primes $p \mid \operatorname{sqrad}(b)$ such that $(a/p) = -1$ must be even, and since the quaternion algebra $\left(\dfrac{a,\ell b}{\mathbb{Q}}\right)$ is ramified at an even number of places, we conclude that $(a,\ell b)_2 = 1$. Therefore $\left(\dfrac{a,\ell b}{\mathbb{Q}}\right) \cong \mathrm{M}_2(F)$ if and only if $(a,\ell b)_p = 1$ for all $p \mid \operatorname{sqrad}(b)$ if and only if a is a square modulo $\operatorname{sqrad}(b)$. □

The preceding lemma shows that the two problems in Theorem 8.2 can be linked by finding a suitable prime ℓ. The conditions on ℓ are congruence conditions, so by the theorem on primes in arithmetic progression, such primes are abundant. Explicitly, we rely on the specialization of a result from analytic number theory, stated by Adleman, Pomerance, and Rumely [2, Proposition 8] and attributed to the proof of Linnik's theorem by Bombieri (using results of Gallagher and related to a result of Tatuzawa); see their paper for further discussion.

Lemma 8.5. *There exist effectively computable (absolute) constants $x_0, \delta \in \mathbb{R}_{>0}$ such that whenever $x \geq x_0$, we have*

$$\left| \sum_{\substack{\ell \leq x \\ \ell \equiv b \pmod{q}}} \log \ell - \frac{x}{\phi(q)} \right| \leq \frac{x}{2\phi(q)}$$

for all q with $1 \leq q \leq x^\delta$ and all b with $\gcd(b,q) = 1$, except possibly for those q which are multiples of a certain integer $q_0(x) > (\log x)^{3/2}$.

Proof of Proposition 8.2. We must show that if we are able to solve (IsMatrixRing), then we can solve Problem (QuadraticResiduosity) in probabilistic polynomial time.

Let $x = \max((4b)^{1/\delta}, x_0)$, with x_0, δ as in Lemma 8.5. Let c be a random integer with $1 \leq c < b$. We compute $q \equiv ac^2 \pmod{4b}$ with $1 \leq q < 4b$ and $q \equiv 1 \pmod{4}$. Then q is a random element in $[1, 4b] \cap \mathbb{Z}$ such that $aq \in (\mathbb{Z}/b\mathbb{Z})^{\times 2}$ and $q \equiv 1 \pmod{4}$. Let

$$Q = \{1 \leq q < b : aq \in (\mathbb{Z}/b\mathbb{Z})^{\times 2} \text{ and } q \equiv 1 \pmod{4}\}.$$

From Lemma 8.5, we have $\sum_{\ell \leq x,\ \ell \equiv a \pmod{q}} \log \ell < x/(2\phi(q))$ only if q is divisible by $q_0(x) > (\log x)^{3/2}$; thus the set of such $q \in Q$ has cardinality at most $\#Q/(\log x)^{3/2}$. Using partial summation (a standard argument which can be found in Davenport [9, p.112]), it follows that a random $q \in Q$ has probability $1 - 1/(\log x)^{3/2}$ of satisfying

$$\pi(x; q, b) = \#\{\ell \leq x : \ell \text{ prime},\ \ell \equiv b \pmod{q}\} < \frac{1}{2\phi(q)} \frac{x}{\log x}$$

whenever $\gcd(b,q) = 1$. We then compute a random integer $1 \leq \ell < x$ with $\ell \equiv b \pmod{q}$ and test if ℓ is prime, which can be done in (deterministic) polynomial time [1]. Combining these, in probabilistic polynomial time, we may assume that ℓ indeed is prime.

We conclude by calling the algorithm to solve (IsMatrixRing) on $B = \left(\dfrac{q, \ell b}{\mathbb{Q}}\right)$. We have

$$\left(\frac{q}{\ell}\right) = \left(\frac{\ell}{q}\right) = \left(\frac{b}{q}\right) = \left(\frac{q}{b}\right) = \left(\frac{a}{b}\right) = 1$$

since $q \equiv 1 \pmod{4}$, and $\ell b \equiv 1 \pmod{q}$. So by Lemma 8.4, we have $B \cong \mathrm{M}_2(\mathbb{Q})$ if and only if q is a square modulo $\operatorname{sqrad}(b)$, which holds only if a is a square modulo $\operatorname{sqrad}(b)$, as desired. □

We leave the natural generalization where $\mathbb{Q}$ is replaced by a number field F as an open question.

References

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, *PRIMES is in P*, Ann. of Math. (2) **160** (2004), no. 2, 781–793.

[2] Leonard M. Adleman, Carl Pomerance, and Robert S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. (2) **117** (1983), no. 1, 173–206.

[3] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), vol. 3–4, 235–265.

[4] J. A. Buchmann and H. W. Lenstra, Jr., *Approximating rings of integers in number fields*, J. Théor. Nombres Bordeaux **6** (1994), no. 2, 221–260.

[5] A. L. Chistov, *The complexity of the construction of the ring of integers of a global field*, Soviet Math. Dokl. **39** (1989), no. 3, 597–600.

[6] Henri Cohen, *Computational algebraic number theory*, Grad. Texts in Math., vol. 193, Springer, Berlin, 2000.

[7] Henri Cohen, *Advanced topics in computational algebraic number theory*, Grad. Texts in Math., vol. 193, Springer, Berlin, 2000.

[8] J. E. Cremona and D. Rusin, *Efficient solution of rational conics*, Math. Comp. **72** (2003), no. 243, 1417–1441.

[9] Harold Davenport, *Multiplicative number theory*, 3rd. ed., Graduate texts in mathematics, vol. 74, Springer-Verlag, Berlin, 2000.

[10] Leonard Eugene Dickson, *Algebras and their arithmetics*, Dover, New York, 1960.

[11] Carsten Friedrichs, *Berechnung von Maximalordnungen uber Dedekindringen*, Ph. D. dissertation, Technischen Universität Berlin, 2000.

[12] A. Fröhlich, *Local fields*, in *Algebraic number theory*, J.W.S. Cassels and A. Fröhlich, eds., Thompson Book Company, Washington, 1967, 1–41.

[13] Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, 2nd edition, Cambridge University Press, Cambridge, 2003.

[14] Florian Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445.

[15] Gábor Ivanyos and Ágnes Szántó, *Lattice basis reduction for indefinite forms and an application*, Proceedings of the 5th Conference on Formal Power Series and Algebraic Combinatorics (Florence, 1993), Discrete Math. **153** (1996), no. 1–3, 177–188.

[16] Gábor Ivanyos and Lajos Rónyai, *Finding maximal orders in semisimple algebras over* $\mathbb{Q}$, Comput. Complexity **3** (1993), no. 3, 245–261.

[17] Nathan Jacobson, *Finite-dimensional division algebras over fields*, Springer-Verlag, Berlin, 1996.

[18] Markus Kirschmer and John Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput. (SICOMP) **39** (2010), no. 5, 1714–1747.

[19] Max-Albert Knus, *Quadratic forms, Clifford algebras and spinors*, Seminários de Matemática, 1, Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Ciência da Computaç ã o, Campinas, 1988.

[20] Max-Albert Knus, Alexander Merkurjev, and Jean-Pierre Tignol, *The book of involutions*, American Math. Soc. Colloquium Publications, vol. 44, AMS, Providence, RI, 1998.

[21] T.Y. Lam, *A first course in noncommutative rings*, 2nd ed., Graduate texts in mathematics, vol. 131, American Math. Soc., Providence, 2001.

[22] H.W. Lenstra, Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. (N.S.) **26** (1992), no. 2, 211–244.

[23] H. W. Lenstra, Jr., *Computing Jacobi symbols in algebraic number fields*, Nieuw Arch. Wisk. (4) **13** (1995), no. 3, 421–426.

[24] Gabriele Nebe and Allan Steel, *Recognition of division algebras*, J. Algebra **322** (2009), no. 3, 903–909.

[25] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999.

[26] O. Timothy O'Meara, *Introduction to quadratic forms*, Classics in Mathematics, Springer-Verlag, Berlin, 2000.

[27] Michael Pohst and Hans Zassenhaus, *Algorithmic algebraic number theory*, Revised reprint, Encyclopedia of Mathematics and its Applications, vol. 30, Cambridge University Press, Cambridge, 1997.

[28] Irving Reiner, *Maximal orders*, Clarendon Press, Oxford, 2003.

[29] Lajos Rónyai, *Zero divisors in quaternion algebras*, J. Algorithms **9** (1988), 494–506.

[30] Lajos Rónyai, *Algorithmic properties of maximal orders in simple algebras over* $\mathbb{Q}$, Comput. Complexity **2** (1992), no. 3, 225–243.

[31] Lajos Rónyai, *Simple algebras are difficult*, Proceedings, 19th ACM Symp. on Theory of Computing, 1990, 398-408.

[32] Lajos Rónyai, *Computing the structure of finite algebras*, J. Symbolic Computation **9** (1990), 355–373.

[33] Winfried Scharlau, *Quadratic and Hermitian forms*, Springer-Verlag, Berlin, 1985.

[34] Viggo Stoltenberg-Hansen and John V. Tucker, Computable rings and fields, *Handbook of computability theory*, ed. Edward R. Griffor, North-Holland, Amsterdam, 1999, 336–447.

[35] Dénis Simon, *Equations dans les corps de nombres et discriminants minimaux*, thèse, Universit Bordeaux I, 1998.

[36] Dénis Simon, Solving quadratic equations using reduced unimodular quadratic forms, Math. Comp. **74** (2005), no. 251, 1531–1543.

[37] Christiaan van de Woestijne, *Deterministic equation solving over finite fields*, ISSAC'05, ACM, New York, 2005, 348–353.

[38] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture notes in mathematics, vol. 800, Springer, Berlin, 1980.

[39] John Voight, *Quadratic forms and quaternion algebras: Algorithms and arithmetic*, Ph.D. thesis, University of California, Berkeley, 2005.

[40] John Voight, *Rings of low rank with a standard involution*, accepted to Illinois J. Math.

[41] John Voight, *Characterizing quaternion rings over an arbitrary base*, J. Reine Angew. Math. **657** (2011), 113-134

Department of Mathematics and Statistics, University of Vermont, 16 Colchester Ave, Burlington, VT 05401, USA

E-mail address: jvoight@gmail.com