

INTERNSHIP REPORT

Computing Explicit Isomorphisms Between Quaternion Algebras: Algorithms and Elliptic Curve Applications

Tommy Chakroun

Supervised by

Travis MORRISON

June 2025

Abstract

In number theory, quaternion algebras are special algebras of dimension 4. They appear in pure number theory in the study of ternary quadratic forms

They also appear in elliptic curve theory as the endomorphism ring of an elliptic curve extended to the rationals. For reasons detailed in Section 6, the algorithmic problem of determining whether two quaternion algebras are isomorphic, and if so computing an explicit isomorphism, is interesting.

En théorie des nombres, les algèbres de quaternions sont des algèbres particulières de dimension 4. Elles apparaissent en théorie des nombres pure dans l'étude des formes quadratiques ternaires

Elles interviennent également dans la théorie des courbes elliptiques comme anneaux d'endomorphismes d'une courbe elliptique étendus aux rationnels. Pour des raisons détaillées dans Section 6, le problème algorithmique consistant à déterminer si deux algèbres de quaternions sont isomorphes, et le cas échéant à calculer un isomorphisme explicite, présente un intérêt.

Contents

1	Introduction	4
2	Central Simple Algebras	6
3	Quaternion algebras	10
4	Orders in central simple algebras	13
5	Discriminant	16
6	Computing Maximal Orders	18
7	The Explicit Isomorphism Problem	21
7.1	Reduction to Finding Zero Divisors and Idempotents	22
7.2	The case $M_4(\mathbb{Q})$	23
7.3	Use of randomization depending on the ground field	24
7.4	Lifting and approximation of non-trivial idempotents over \mathbb{Q}	25
8	Explicit isomorphism problem directly for $M_4(\mathbb{Q})$	26
9	Interlude: Motivation from elliptic curve theory	27
10	Explicit isomorphism of quaternion algebras	27
A	Implementation and Precise Algorithms	28
A.1	Reduction $\varphi : A \otimes_{\mathbb{Q}} B^{op} \rightarrow M_4(\mathbb{Q})$ to $f : A \rightarrow B$	28
A.2	Solution to a System $AX \equiv 0 \pmod{d}$ for Integral Matrices	31
A.3	Computation of Left Order	31
A.4	Randomized Computation of Central Simple Idempotents over a Finite Field	33

1. Introduction

Throughout this report, all fields are assumed to be commutative, and all algebras are assumed to be unital and associative.

The Explicit Isomorphism Problem. Let F be a field. A *central simple algebra* over F is a finite-dimensional F -algebra whose center is exactly F and which is simple as a ring—that is, it has no nontrivial two-sided ideals. For every integer n , the matrix algebra $M_n(F)$ is a central simple algebra. A fundamental problem in computational algebra, known as the *explicit isomorphism problem*, is formulated as follows:

Explicit Isomorphism Problem

Let \mathcal{B} be a central simple F -algebra given by a basis and structure constants.

Suppose that $\mathcal{B} \cong M_n(F)$ as F -algebras. Compute an explicit isomorphism $\phi : \mathcal{B} \rightarrow M_n(F)$, i.e., return n^2 matrices with entries in F representing the images of the basis elements of \mathcal{B} under ϕ .

A slight variant is the following:

General Explicit Isomorphism Problem

Let A and B be two central simple algebras over F , given by bases and structure constants. Suppose that $A \cong B$ as F -algebras. Compute an explicit isomorphism $f : A \rightarrow B$, i.e., express the images of the basis elements of A under f in terms of the basis of B .

One can show that the second problem reduces in polynomial time to the first: finding an isomorphism between two central simple algebras of dimension n reduces to finding an isomorphism between a central simple algebra of dimension n^2 and $M_n(F)$.

State of the Art. The explicit isomorphism problem has been well studied in the literature. The known solutions depend heavily on the properties of the base field F and the dimension n . It is often considered when F is the field of fractions of a ring R , particularly when R is a *Dedekind domain* (a Noetherian integrally closed domain in which every nonzero prime ideal is maximal). Here are some of the main results from the literature:

- $n = 2$: The problem reduces to solving a ternary quadratic equation $ax^2 + by^2 + cz^2 = 0$ over F , with $a, b, c \in F$. See [14], Main Theorem 5.4.4.
- $n = 2, F = \mathbb{Q}$: ...

- $n = 3$, $F \dots$
- $n = 4$, $F = \mathbb{Q}$: See [6] for efficient methods.
- General case: For any $n \geq 1$ and F an algebraic number field, there is a polynomial-time ff-algorithm using an oracle for integer factorization. See [6], Section 3, and further improvements for $n \leq 43$.

Quaternion Algebras. Quaternion algebras are central simple algebras of dimension 4. When $\text{char}(F) \neq 2$, these algebras admit a very concrete description: they have a basis $1, i, j, ij$, with $i^2 = a \in F^\times$, $j^2 = b \in F^\times$, and $ij = -ji$. See [14]. Quaternion algebras are closely related to ternary quadratic forms over F , which underpins the first case in the state of the art.

Motivation from Elliptic Curve Theory. Section 7 is dedicated to motivations coming from the theory of elliptic curves. Elliptic curves are special projective plane curves that carry a natural abelian group structure. The computational properties of these groups are of great interest in cryptography due to the hardness of the discrete logarithm problem. On a more abstract level, one can define *isogenies* between elliptic curves—morphisms of algebraic varieties that are also group homomorphisms. In particular, for an elliptic curve E , the set $\text{End}(E)$ of isogenies from E to itself forms a ring under composition. This endomorphism ring gives rise to computational problems with cryptographic applications.

A surprising result is that for certain elliptic curves called *supersingular*, the extended endomorphism ring $\text{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ has the structure of a quaternion algebra over \mathbb{Q} .

Goals and Methods of this Paper. The goal of this paper is to study the General Explicit Isomorphism Problem over \mathbb{Q} for algebras of dimension 4, i.e., quaternion algebras. Specifically, given two quaternion algebras over \mathbb{Q} known to be isomorphic, we aim to compute an explicit isomorphism between them. By the aforementioned reduction, this is equivalent to solving the Explicit Isomorphism Problem for a 16-dimensional \mathbb{Q} -algebra isomorphic to $M_4(\mathbb{Q})$.

Our approach follows the general algorithm of [6], which is based on the notion of *maximal orders*. We also provide a full implementation of the final algorithm in SageMath.

Contents. This article is structured to provide a self-contained introduction to the explicit isomorphism problem in the context of quaternion algebras, along with

its motivation and computational aspects. We begin by introducing the general framework of central simple algebras in Section 2, setting the stage for our discussion. In Section 3, we focus on quaternion algebras as a central class of examples, describing their structure and properties.

We introduce the notion of orders in Section 4, followed by a detailed examination of the discriminant of an order in Section 5. These foundational notions are crucial for understanding the computation of maximal orders, which we present in Section 6.

The core topic of this work—the explicit isomorphism problem—is formulated in general in Section 7. To motivate its relevance in arithmetic geometry, we present in Section 9 a brief interlude discussing connections to the theory of elliptic curves, in particular through isogenies and endomorphism rings. Section 10 then revisits the explicit isomorphism problem, now specialized to the case of quaternion algebras, and outlines algorithmic strategies for solving it in this setting.

Finally, Appendix A provides additional details on the implementation of the algorithms discussed in the main text.

2. Central Simple Algebras

All algebras B over a field F are assumed to be unitary and associative, so that we can view $F \subset B$. We recall that the center of B is the set $Z(B)$ of elements $b \in B$ that commute with every $x \in B$. It is a sub- F -algebra of B .

An algebra is a *division algebra* if every non-zero element has a two-sided inverse. Note that the center of a division algebra is a field, and every division algebra has the structure of an algebra over its center.

An algebra B , or more generally a ring, is *simple* if its only two-sided ideals are $\{0\}$ and B . This is equivalent to saying that for any non-zero ring R , every ring homomorphism $B \rightarrow R$ is injective.

Now we define an important class of algebras.

Definition 2.1. Let F be a field. A *central simple algebra* over F is a finite-dimensional algebra over F whose center is exactly F and which has no non-trivial two-sided ideals.

The standard example of a central simple algebra is $B = M_n(F)$, called the *split* central simple algebra of dimension n^2 . The goal of this section is to show that, by extending the base field, every central simple algebra becomes isomorphic to a split one.

First, as simple algebras, central simple algebras enjoy the following strong structure

theorem.

Wedderburn-Artin Theorem and Consequences.

Theorem 2.2 (Wedderburn-Artin Theorem, weak version). *Let B be a finite-dimensional simple algebra over F . Then there exists a division algebra D over F and an integer $n \geq 1$ such that B is isomorphic to $M_n(D)$. Moreover, D is unique up to F -algebra isomorphism.*

The proof follows [5, Section 2.1] by Philippe Gille and Tamás Szamuely.

Proof. Let I be a minimal non-zero left ideal of B . Such an ideal exists because a left ideal is an F -subspace, so we can choose one of minimal positive dimension. Define the ring D to be the ring of B -linear endomorphisms of I :

$$D := \text{End}_B(I) = \{f : I \rightarrow I \mid f \text{ is a group homomorphism and } f(bx) = bf(x) \text{ for all } x \in I, b \in B\}.$$

This is a sub- F -algebra of $\text{End}_F(I)$, and we claim that it is a division algebra. Indeed, if $f : I \rightarrow I$ is a non-zero B -linear map, then its kernel and image are left ideals of B contained in I . Since $f \neq 0$, $\ker(f) \neq I$ and $\text{im}(f) \neq \{0\}$. By the minimality of I , we must have $\ker(f) = \{0\}$ and $\text{im}(f) = I$. Therefore, f is an isomorphism and thus has an inverse in D .

Now, we consider the ring of D -linear endomorphisms of I :

$$\text{End}_D(I) = \{f : I \rightarrow I \mid f \text{ is a group homomorphism and } f \circ g = g \circ f \text{ for all } g \in D\}.$$

It is also a sub- F -algebra of $\text{End}_F(I)$.

For any $b \in B$, the map of left multiplication by b is in $\text{End}_D(I)$. This allows us to define a map:

$$\Phi : B \rightarrow \text{End}_D(I); \quad b \mapsto (x \mapsto bx).$$

It is immediate that Φ is an F -algebra homomorphism. Furthermore, $\ker(\Phi)$ is a two-sided ideal of B . Since Φ is non-zero (e.g., $\Phi(1) = \text{id}_I$), its kernel cannot be all of B . By the simplicity of B , $\ker(\Phi) = \{0\}$, so Φ is injective. Let us show surjectivity. First, note that the set

$$IB := \left\{ \sum_{i=1}^r x_i b_i \mid r \in \mathbb{Z}_{\geq 0}, x_i \in I, b_i \in B \right\}$$

is a non-zero two-sided ideal of B , and thus $IB = B$ by simplicity. Hence, we can write $1 = \sum_{i=1}^r x_i b_i$ for some integer $r > 0$. Now let $f \in \text{End}_D(I)$. We have:

$$f = f\Phi(1) = \sum_{i=1}^r f \circ \Phi(x_i) \circ \Phi(b_i).$$

For $i = 1, \dots, r$, and $z \in I$, since $\text{id}_I \cdot z$ is in $\text{End}_D(I)$, by definition f commutes with $\text{id}_I \cdot z$. This yields

$$f \circ \Phi(x_i)(z) = f(x_i z) = f(x_i)z = \Phi(f(x_i))(z),$$

hence $f \circ \Phi(x_i) = \Phi(f(x_i))$.

And finally,

$$f = \Phi\left(\sum f(x_i)b_i\right).$$

This concludes the proof of surjectivity. Thus, Φ realizes an F -algebra isomorphism between B and $\text{End}_D(I)$.

Finally, by the theory of modules over a division ring, I is a free D -module of some rank n , i.e., $I \cong D^n$. It follows that

$$\text{End}_D(I) \cong \text{End}_D(D^n) \cong M_n(D^{op}) \cong M_n(D)$$

as rings, and therefore as F -algebras. This completes the proof. \square

It follow that if K is a field algebraically closed, then every central simple algebra over K are isomorphic to some matrix algebra $M_n(K)$. Indeed if D is a division algebra over K then $D = K$: for all $x \in D$ the minimal polynomial of x over K is irreducible (because D is a domain) and so is of degree 1, hence $x \in K$.

Lemma 2.3. *Let B be a finite dimensional algebra over F and K/F be a field extension. Then B is a central simple algebra over F if and only if $B \otimes_F K$ is a central simple algebra over K .*

Proof. See Philippe Gille and Tamás Szamuely [5], Lemma 2.2.2. \square

Proposition 2.4. *Let B be a finite dimensional algebra over F . Then there exist K/F a field extension such that $B \otimes_F K \cong M_n(K)$ as K -algebra, for some integer n .*

Proof. It follows from taking K to be the algebraic closure of F in the previous lemma and the previous remark. \square

Reduced trace. Let F be a field and let B be a central simple algebra over F . Let K be an algebraic closure of F so that $B \otimes_F K \cong M_n(K)$. Hence, we can embed B into $M_n(K)$ via

$$\varphi : B \rightarrow M_n(K), \quad b \mapsto b \otimes 1.$$

We define the *reduced trace* of $b \in B$ by

$$\text{trd}(b) := \text{trace}(\varphi(b)) \in K.$$

Proposition 2.5. *Assume that F is of characteristic 0. The reduced trace of b does not depend on the choice of the isomorphism. It satisfies the following properties:*

1. *For all $b \in B$, we have*

$$\text{trd}(b) = \frac{1}{n} \text{trace}_F(B \rightarrow B, x \mapsto bx),$$

hence $\text{trd}(b) \in F$, and $\text{trd} : B \rightarrow F$ is an F -linear form.

2. *The map $B \times B \rightarrow F$, $(x, y) \mapsto \text{trd}(xy)$ is a non-degenerate F -bilinear form.*

3. *If $F = \text{Frac}(R)$ for some principal ideal domain R , and if $x \in B$ is integral over R , then $\text{trd}(x) \in R$.*

Lemma 2.6 (Skolem-Noether Theorem for matrix rings). *Let K be a field. Every K -algebra automorphism of $M_n(K)$ is inner, that is, of the form $M \mapsto PMP^{-1}$ for some $P \in \text{GL}_n(K)$.*

Proof of Lemma 2.6. Let $\phi : M_n(K) \rightarrow M_n(K)$ be a K -algebra automorphism. Let $I \subset M_n(K)$ be the left ideal of matrices with only the first column nonzero. Fix a nonzero $u_0 \in K^n$. Since ϕ is an automorphism, $\phi((u_0 \mid 0 \mid \cdots \mid 0)) \neq 0$. Thus, we can choose $x_0 \in K^n$ such that

$$\phi((u_0 \mid 0 \mid \cdots \mid 0))x_0 \neq 0.$$

Define the K -linear endomorphism

$$P : K^n \rightarrow K^n, \quad u \mapsto \phi((u \mid 0 \mid \cdots \mid 0))x_0.$$

For any $M \in M_n(K)$ and any $u \in K^n$, we have $PMu = \phi(M)Pu$, so $PM = \phi(M)P$. The kernel of P is stable under left multiplication by any matrix in $M_n(K)$. Since $Pu_0 \neq 0$, the kernel is not all of K^n , and since the only ideals of $M_n(K)$ are $\{0\}$ and $M_n(K)$, the kernel must be zero. Hence, P is an isomorphism, and

$$\phi(M) = PMP^{-1}.$$

□

Proof of Proposition 2.5. The well-definedness follows directly from Lemma 2.6. For any field K of characteristic 0 and any matrix $M \in M_n(K)$, we have

$$\text{trace}(M) = \frac{1}{n} \text{trace}_F(M_n(K) \rightarrow M_n(K), Z \mapsto MZ).$$

Hence,

$$\text{trd}(b) = \text{trace}_F(M_n(K) \rightarrow M_n(K), Z \mapsto \varphi(b \otimes 1)Z) = \text{trace}_F(B \otimes_F K \rightarrow B \otimes_F K, z \mapsto (b \otimes 1)z).$$

Since we can choose a K -basis of $B \otimes_F K$ of the form $e_1 \otimes 1, \dots, e_N \otimes 1$, where e_1, \dots, e_N is an F -basis of B , this trace equals that of the map $B \rightarrow B$, $z \mapsto bz$. This proves the first point, as F -linearity is evident.

Now let $x \in B$, and assume that $\text{trd}(xy) = 0$ for all $y \in B$. Then

$$\text{trace}(\varphi(xy \otimes 1)) = 0 \quad \text{for all } y \in B.$$

Hence,

$$\text{trace}(\varphi(x \otimes 1)\varphi(y \otimes 1)) = 0 \quad \text{for all } y \in B.$$

Since the set $\{y \otimes 1 \mid y \in B\}$ spans $B_K = B \otimes_F K$ over K , it follows that $\varphi(x \otimes 1)$ is orthogonal to all matrices in $M_n(K)$ under the trace pairing, and thus must be zero. Hence, $x \otimes 1 = 0$, and therefore $x = 0$. This proves the second point.

Finally, suppose that $x \in B$ is integral over R . Then the matrix $A := \varphi(x \otimes 1)$ is integral over R , so its eigenvalues lie in $K = F^{\text{alg}}$ and are integral over R . Therefore, the trace of A , being the sum of its eigenvalues, is also integral over R . But since we have already seen that $\text{trd}(x) = \text{trace}(A) \in F$, and R is integrally closed in F , it follows that $\text{trd}(x) \in R$. This proves the third point. \square

3. Quaternion algebras

Definition. Let F be a field of characteristic not 2. For all $a, b \in F^\times$, there exists a unique unitary and associative F -algebra B , up to F -algebra isomorphism, with two elements $i, j \in B$ such that $1, i, j, ij$ form an F -basis and satisfy the relations:

$$i^2 = a, \quad j^2 = b, \quad \text{and} \quad ij = -ji. \tag{1}$$

We denote such an algebra by

$$\left(\frac{a, b}{F} \right) = F \oplus Fi \oplus Fj \oplus Fij.$$

These are called *quaternion algebras*.

The uniqueness up to F -algebra isomorphism is clear, and to check the existence, it suffices to write down the unique possible multiplication table which respects associativity and the relations (1) and then check that the whole table is well associative.

An important example: If F is a field of characteristic not 2, then $M_2(F) \simeq \left(\frac{1,1}{F}\right)$ for the basis:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad ij = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Let $B = \left(\frac{a,b}{F}\right)$ be a quaternion algebra over a field F of characteristic not 2, and denote $1, i, j, ij$ an adapted basis. The sub F -vector space H spanned by i, j, ij is exactly the set of the elements $x \in B$ such that $x \notin F$ and $x^2 \in F$. Thus, H is a supplement of F in B which does not depend on the choice of the basis. We define the conjugate of an element $s \in B$ to be the symmetric in the direction of H parallel to F :

$$\bar{s} := \lambda - h.$$

The conjugation on B enjoys the following properties:

- Transition to the next section...

Standard involution.

Definition 3.1. Let F be a field and B be an F -algebra. An *involution* on B is an F -linear map $\bar{\cdot} : B \rightarrow B$ such that $\bar{\bar{1}} = 1$ and for all $x, y \in B$, $\overline{\bar{x}} = x$ and $\overline{xy} = \bar{y}\bar{x}$. An involution is *standard* if for all $x \in B$, $x\bar{x} \in F$.

If B has a standard involution, then we also have $x + \bar{x} \in F$ for all $x \in B$. Indeed, $(1+x)\overline{(1+x)} \in F$ and we can write

$$(1+x)\overline{(1+x)} = (1+x)(1+\bar{x}) = 1 + x + \bar{x} + x\bar{x}.$$

We also have $x\bar{x} = \bar{x}x$.

We call $\text{trd}(x) = x + \bar{x}$ the *reduced trace* of x and $\text{nrd}(x) = x\bar{x}$ the *reduced norm* of x .

To check that an involution is standard, it is not enough to check that $x\bar{x} \in F$ holds for x in a basis of B . But we have the following lemma.

Lemma 3.2. *An involution over a finite-dimensional algebra B is standard if and only if there exists a basis e_1, \dots, e_n of B such that for all $1 \leq i, j \leq n$, we have $e_i\bar{e}_i \in F$ and $(e_i + e_j)\overline{(e_i + e_j)} \in F$.*

Proof. The direct sense is immediate. For the converse, denote $n_i = e_i\bar{e}_i$ and $n_{i,j} = (e_i + e_j)\overline{(e_i + e_j)}$. Then for all $x = \sum x_i e_i$,

$$x\bar{x} = \sum x_i e_i \sum x_j \bar{e}_j = \sum x_i^2 n_i + \sum x_i x_j (e_i \bar{e}_j + e_j \bar{e}_i) = \sum x_i^2 n_i + \sum x_i x_j (n_{i,j} - n_i - n_j)$$

lies in F . □

Another remark is that if B has a standard involution, then every $x \in B$ satisfies the polynomial of degree two with coefficients in F :

$$T^2 - \text{tr}dxT + \text{nrd}x.$$

In particular, if B has a standard involution and e_1, \dots, e_n is a basis of B with $e_1 = 1$, then for $i \geq 2$, the coefficient of e_i in e_i^2 is $\text{tr}de_i$.

Algorithm 1: Has Standard Involution

Input: A finite-dimensional algebra B over a field F with a basis

$$e_1 = 1, e_2, \dots, e_n$$

Output: True if B has a standard involution, False otherwise.

Let $t(e_1) = 2$ and for $2 \leq i \leq n$, let $t(e_i) \in F$ be the coefficient of e_i in e_i^2 . Extend t by F -linearity on B and for all $\xi \in B$, let $\bar{\xi} := t(\xi) - \xi$.

If $\bar{e}_i \bar{e}_j \neq \bar{e}_j \bar{e}_i$ for some $2 \leq i, j \leq n$, return False.

If $n_i := e_i \bar{e}_i$ or $n_{ij} := (e_i + e_j)(\bar{e}_i + \bar{e}_j)$ is not in F for some $2 \leq i, j \leq n$, return False; else, return True.

Proof of correctness. If B has a standard involution, the algorithm returns True. Conversely, if the algorithm returns True, then B has a standard involution. \square

Quadratic forms.

Theorem 3.3. *Let F be a field of characteristic not 2. Then the map*

$$\left[\left(\frac{a, b}{F} \right) \right] \mapsto [-aX^2 - bY^2 + abZ^2]$$

induces a bijection between the classes of quaternion algebras over F up to F -algebra isomorphism and the classes of non-degenerate ternary quadratic forms over F up to similarity.

Proof. Well-defined: Let $B = \left(\frac{a, b}{F} \right)$ and $C = \left(\frac{c, d}{F} \right)$ be isomorphic via $f : B \rightarrow C$. The standard involution s is preserved, so $f(B^0) = C^0$, and f induces an F -linear isomorphism $u : F^3 \rightarrow F^3$ such that for $x, y, z \in F$,

$$f(xi + yj + zij) = u_1(x, y, z)i + u_2(x, y, z)j + u_3(x, y, z)ij.$$

Hence:

$$\begin{aligned} \text{nrd}(xi + yj + zij) &= -ax^2 - by^2 + abz^2, \\ &= \text{nrd}(f(xi + yj + zij)) \\ &= -cu_1^2 - du_2^2 + cdu_3^2. \end{aligned}$$

So the forms $-aX^2 - bY^2 + abZ^2$ and $-cX^2 - dY^2 + cdZ^2$ are equivalent.

Surjectivity: Let $Q \sim aX^2 + bY^2 + cZ^2$ with $a, b, c \in F^\times$. Then:

$$Q \sim abc(aX^2 + bY^2 + cZ^2) \sim (bc)X^2 + (ac)Y^2 + (ab)Z^2.$$

This form has discriminant $1 \in F^\times/F^{\times 2}$. Write it as $-\alpha X^2 - \beta Y^2 + \gamma Z^2$. Since $\alpha\beta\gamma$ is a square, $\frac{\alpha\beta}{\gamma}$ is a square, so the form is equivalent to $-\alpha X^2 - \beta Y^2 + \alpha\beta Z^2$.

Injectivity: Suppose $-aX^2 - bY^2 + abZ^2$ and $-cX^2 - dY^2 + cdZ^2$ are similar. Since they have the same discriminant... \square

Local global principle. See appendix on Hasse Minkowski theorem.

Theorem 3.4 (Local-Global Principle for Quaternion Algebras over \mathbb{Q}). *Let B be a quaternion algebra over \mathbb{Q} . Then B is determined up to isomorphism by the set of places v of \mathbb{Q} where B is ramified.*

More precisely, for each place v of \mathbb{Q} , let $B_v = B \otimes_{\mathbb{Q}} \mathbb{Q}_v$. Then B is uniquely determined (up to isomorphism) by the set

$$\text{Ram}(B) := \{v \text{ place of } \mathbb{Q} : B_v \text{ is a division algebra}\},$$

which is a finite set of even cardinality.

Hilbert symbol over \mathbb{Q}_p .

Application to the problem `IdentifyMatrixwRing`.

4. Orders in central simple algebras

In this section, we fix R to be a principal ideal domain, F its field of fractions, and B a central simple algebra over F . (We will apply the results of this section with $R = \mathbb{Z}$ or $R = \mathbb{Z}_{(p)}$ for some prime p , so $F = \mathbb{Q}$ always.)

The assumption that R is a principal ideal domain allows us to give a simpler definition of an order. For more general cases over different rings, see [14], Chapters 9 and 10.

An R -order in B is a subring $\Lambda \subset B$ such that:

- Λ is an R -full lattice in B ; that is, there exists an F -basis e_1, \dots, e_N of B such that $\Lambda = Re_1 \oplus \dots \oplus Re_N$.

- Λ is a subring of B ; in particular, $1 \in \Lambda$.

In particular, Λ is a free R -module with R -basis e_1, \dots, e_N .

Remark 4.1. If B is a central simple algebra over \mathbb{Q} , then we can view \mathbb{Q} as the field of fractions of \mathbb{Z} or of $\mathbb{Z}_{(p)}$ for some prime p . In this context, there is a meaningful distinction between a \mathbb{Z} -order and a $\mathbb{Z}_{(p)}$ -order in B .

Theorem 4.2. *If Λ is an R -order in B , then for all $\alpha \in \Lambda$, α is integral over R ; hence $\text{trd}(\alpha) \in R$.*

Proof. Let $R[\alpha] := \{P(\alpha) \mid P \in R[X]\}$, which is an R -submodule of $\Lambda \cong R^n$. Since R is a principal ideal domain, it follows that $R[\alpha] \cong R^m$ for some integer $1 \leq m \leq n$. By choosing an R -basis of $R[\alpha]$, the multiplication-by- α map

$$R[\alpha] \rightarrow R[\alpha], \quad z \mapsto \alpha z$$

is represented by some matrix $M \in M_m(R)$ in this basis. Hence the characteristic polynomial of M is a monic polynomial in $R[X]$ that vanishes at α , so α is integral.

The second assertion follows because R is integrally closed and by the same reasoning. \square

Definition 4.3. An R -order is *maximal* if it is maximal with respect to inclusion among the R -orders in B .

Let us now specialize to the case of most interest to us, namely when $F = \mathbb{Q}$ and $R = \mathbb{Z}$ or $\mathbb{Z}_{(p)}$. Let B be a central simple algebra over \mathbb{Q} , and let

$$\Lambda = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_N$$

be a \mathbb{Z} -order in B . We define its localization at a prime p as

$$\Lambda_{(p)} := \mathbb{Z}_{(p)}e_1 \oplus \dots \oplus \mathbb{Z}_{(p)}e_N = \mathbb{Z}_{(p)}\Lambda.$$

The second expression justifies that this localization does not depend on the choice of \mathbb{Z} -basis. It is clear that $\Lambda_{(p)}$ is a $\mathbb{Z}_{(p)}$ -order in B .

We also observe that

$$\Lambda = \bigcap_{p \text{ prime}} \Lambda_{(p)},$$

which follows componentwise from $\mathbb{Z} = \bigcap_p \mathbb{Z}_{(p)}$.

The main result is the local-global correspondence:

Theorem 4.4. *Let Λ be a \mathbb{Z} -order in a central simple \mathbb{Q} -algebra B . Then Λ is a maximal \mathbb{Z} -order if and only if $\Lambda_{(p)}$ is a maximal $\mathbb{Z}_{(p)}$ -order for every prime p .*

Proof. The forward direction is straightforward. Suppose that for all primes p , the localized order $\Lambda_{(p)}$ is maximal. Now, assume $\Lambda \subset \Gamma$ for some \mathbb{Z} -order Γ . Then for all primes p , we have $\Lambda_{(p)} \subset \Gamma_{(p)}$, and by maximality of $\Lambda_{(p)}$, it follows that $\Lambda_{(p)} = \Gamma_{(p)}$. Hence, by the identity

$$\Lambda = \bigcap_p \Lambda_{(p)} = \bigcap_p \Gamma_{(p)} = \Gamma,$$

we conclude that $\Lambda = \Gamma$, so Λ is maximal.

Conversely, suppose Λ is maximal, but there exists a prime p and a $\mathbb{Z}_{(p)}$ -order $\mathcal{O}(p)$ in B such that

$$\Lambda_{(p)} \subsetneq \mathcal{O}(p).$$

For each prime $q \neq p$, define $\mathcal{O}(q) := \Lambda_{(q)}$, and set

$$\Gamma := \bigcap_q \mathcal{O}(q).$$

We claim that Γ is a \mathbb{Z} -order in B , and that $\Gamma_{(q)} = \mathcal{O}(q)$ for all primes q . Moreover, we will show that $\Lambda \subsetneq \Gamma$, which will contradict the maximality of Λ .

Let $\Lambda = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_N$ and $\mathcal{O}(p) = \mathbb{Z}_{(p)}f_1 \oplus \cdots \oplus \mathbb{Z}_{(p)}f_N$. Since both are $\mathbb{Z}_{(p)}$ -lattices of full rank, there exists an integer $s > 0$ such that

$$s\Lambda_{(p)} \subset \mathcal{O}(p) \subset s^{-1}\Lambda_{(p)}.$$

This same inclusion holds for all primes q , since for $q \neq p$, we have $\mathcal{O}(q) = \Lambda_{(q)}$, so trivially:

$$s\Lambda_{(q)} \subset \mathcal{O}(q) \subset s^{-1}\Lambda_{(q)}.$$

Taking intersections over all primes q , and using the identity $\Lambda = \bigcap_q \Lambda_{(q)}$, we obtain:

$$s\Lambda \subset \Gamma \subset s^{-1}\Lambda.$$

This shows that Γ lies between two scalar multiples of Λ , so Γ is also a full \mathbb{Z} -lattice in B . In particular, there exist elements $a_1, \dots, a_N \in B$ such that

$$\Gamma = \mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_N.$$

Now consider the localization

$$\Gamma_{(q)} = \mathbb{Z}_{(q)}a_1 \oplus \cdots \oplus \mathbb{Z}_{(q)}a_N.$$

We claim that $\Gamma_{(q)} = \mathcal{O}(q)$ for all primes q . Indeed, for each q , we have:

$$\Gamma_{(q)} = \left(\bigcap_r \mathcal{O}(r) \right)_{(q)} = \bigcap_r \mathcal{O}(r)_{(q)}.$$

But $\mathcal{O}(r)_{(q)} = B$ when $r \neq q$, so this intersection reduces to $\Gamma_{(q)} = \mathcal{O}(q)$, as desired.

Thus, Γ is a \mathbb{Z} -order in B , and since $\Gamma_{(p)} = \mathcal{O}(p) \supsetneq \Lambda_{(p)}$, we must have $\Gamma \supsetneq \Lambda$, contradicting the maximality of Λ . Therefore, no such $\mathcal{O}(p)$ can exist, and all $\Lambda_{(p)}$ must be maximal. \square

5. Discriminant

We use the same setup as in the previous section: R is a principal ideal domain, F its field of fractions, and B a central simple algebra over F . Denote $N := \dim_F(B)$.

The notion of the *discriminant* of an order is intended to measure inclusion relations between orders. In summary, we define the discriminant to satisfy the following properties:

1. For any R -order Λ in B , the discriminant d_Λ is a nonzero element of R , well-defined up to a unit, i.e., it corresponds to a unique nonzero ideal of R .
2. For any R -orders $\Lambda, \Gamma \subset B$, if $\Lambda \subset \Gamma$, then $d_\Gamma \mid d_\Lambda$.
3. If $\Lambda \subset \Gamma$ and $d_\Gamma = d_\Lambda$ up to a unit, then $\Lambda = \Gamma$.

Definition 5.1. Let $\Lambda = Re_1 \oplus \cdots \oplus Re_N$ be an R -order in B . The *discriminant* of Λ is defined as

$$d_\Lambda := \det(\text{trd}(e_i e_j))_{1 \leq i, j \leq N} \bmod R^\times.$$

Since for all $1 \leq i, j \leq N$, the element $e_i e_j$ lies in Λ , its reduced trace lies in R by Proposition 4.2. Hence, d_Λ is indeed an element of R , and it is nonzero since the bilinear form $(x, y) \mapsto \text{trd}(xy)$ is non-degenerate by Proposition 2.5.

We are going to prove that the definition of the discriminant does not depend on the choice of the R -basis of Λ , and thereby verify properties 2 and 3 regarding inclusion.

Suppose Λ, Γ are two R -orders in B , given by R -bases:

$$\Lambda = Re_1 \oplus \cdots \oplus Re_N, \quad \Gamma = Rf_1 \oplus \cdots \oplus Rf_N.$$

Let $M \in M_N(F)$ be the matrix expressing the e_k in terms of the f_i , that is,

$$e_k = M_{1,k}f_1 + \cdots + M_{N,k}f_N \quad \text{for } 1 \leq k \leq N.$$

Then, for all $1 \leq i, j \leq N$,

$$\text{trd}(e_i e_j) = \text{trd} \left(\left(\sum_{k=1}^N M_{k,i} f_k \right) \left(\sum_{\ell=1}^N M_{\ell,j} f_\ell \right) \right) = \sum_{k,\ell=1}^N M_{k,i} M_{\ell,j} \text{trd}(f_k f_\ell).$$

In matrix form, this reads

$$(\text{trd}(e_i e_j)) = M^\top (\text{trd}(f_i f_j)) M,$$

and hence,

$$\det(\text{trd}(e_i e_j)) = \det(M)^2 \det(\text{trd}(f_i f_j)).$$

We deduce all the desired properties from this relation:

- If $\Lambda = \Gamma$, then M is invertible over $M_N(R)$, so $\det(M)^2 \in R^\times$, and the discriminant is well-defined up to a unit.
- If $\Lambda \subset \Gamma$, then M has entries in R , so $\det(M)^2 \in R$, and hence $d_\Gamma \mid d_\Lambda$.
- If $\Lambda \subset \Gamma$ and $d_\Gamma = d_\Lambda$ up to a unit, then $\det(M)^2 \in R^\times$. Since R is a domain, this implies $\det(M) \in R^\times$, so M is invertible over $M_N(R)$. Thus, the f_i are R -linear combinations of the e_j , so $f_i \in \Lambda$, and therefore $\Lambda = \Gamma$.

An important consequence is the following: if

$$\Lambda_1 \subset \Lambda_2 \subset \cdots \subset \Lambda_r$$

is a chain of strictly increasing R -orders, then the corresponding sequence of discriminants

$$d_r \mid d_{r-1} \mid \cdots \mid d_1$$

is a strictly decreasing sequence (with respect to divisibility) of elements in R . In particular, if

$$d_1 = \pi_1^{\alpha_1} \cdots \pi_s^{\alpha_s}$$

is the factorization of d_1 into irreducibles, then $r \leq \alpha_1 + \cdots + \alpha_s$.

This shows that there exists a maximal order containing Λ_1 , since R cannot have an infinite strictly descending chain with respect to divisibility.

So far, we have only used the fact that trd respects integrality, is F -linear, and that the bilinear form $(x, y) \mapsto \text{trd}(xy)$ is non-degenerate. While one could define a discriminant using another F -linear form with these properties, the choice of trd —which coincides with the usual trace when $B \cong M_n(F)$ —is justified by the following normalization:

Theorem 5.2. *Let Λ be an R -order in B . If d_Λ is a unit in R (i.e., $\text{disc}(\Lambda) = R$), then Λ is a maximal R -order. If $B \cong M_n(F)$ for some integer n , then the converse is also true.*

Proof. The direct implication is immediate.

Conversely, suppose $B \cong M_n(F)$. Then the converse is more subtle and will require further work... \square

In general, a maximal order does not necessarily have discriminant 1. However, the easy characterization of maximal orders in matrix algebras provides a concrete way to verify maximality, which is especially useful for our SageMath implementation in the case where the algebra is isomorphic to $M_4(\mathbb{Q})$.

6. Computing Maximal Orders

Let B be a finite-dimensional central simple algebra over \mathbb{Q} , and let Λ be a \mathbb{Z} -order in B given by a \mathbb{Z} -basis:

$$\Lambda = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_N.$$

We describe a method following [7] to construct a \mathbb{Z} -basis of a maximal order $\Gamma \supseteq \Lambda$.

For each prime p , define $\mathcal{A}_p := \Lambda/p\Lambda$, which is the quotient of Λ by the two-sided ideal $p\Lambda$. Then:

$$\mathcal{A}_p = \mathbb{F}_p e_1 \oplus \cdots \oplus \mathbb{F}_p e_N,$$

with the structure of a finite-dimensional \mathbb{F}_p -algebra of dimension $N = \dim_{\mathbb{Q}}(B)$. Concretely, the structure constants of \mathcal{A}_p can be computed by multiplying the basis elements $e_i e_j \in \Lambda$, writing the result in terms of the e_k , and reducing the coefficients modulo p .

We now consider the *Jacobson radical* of \mathcal{A}_p :

$$\text{Rad}(\mathcal{A}_p) := \{x \in \mathcal{A}_p \mid xM = 0 \text{ for all simple } \mathcal{A}_p\text{-modules } M\}.$$

Let

$$\mathcal{C}_p := \mathcal{A}_p / \text{Rad}(\mathcal{A}_p)$$

be the semisimple quotient algebra. Define the composition of natural projections:

$$\Phi_p : \Lambda \xrightarrow{\text{mod } p} \mathcal{A}_p \twoheadrightarrow \mathcal{C}_p.$$

Since Λ is a ring and a free \mathbb{Z} -module, \mathcal{C}_p inherits at least a \mathbb{Z} -module structure (not necessarily free). The map Φ_p is a homomorphism of \mathbb{Z} -modules.

We now state the main result:

Theorem 6.1 (Detection of Non-Maximality). *With the notation above, suppose $\Lambda \subset B$ is not a maximal order. Then there exists a prime $p \mid d_\Lambda$, and an ideal $\mathcal{K} \subset \mathcal{C}_p$, either the zero ideal or a minimal nonzero ideal, such that the preimage*

$$\mathcal{I} := \Phi_p^{-1}(\mathcal{K})$$

satisfies $O_L(\mathcal{I}) \supsetneq \Lambda$; that is, the left order of \mathcal{I} strictly contains Λ .

Proof. Since Λ is not maximal, Theorem 5.2 implies that $d_\Lambda \in \mathbb{Z}$ is not a unit and hence divisible by some prime p \square

This theorem leads directly to an algorithm: given a \mathbb{Z} -order Λ in B , the above procedure either produces a strictly larger order or certifies that Λ is maximal.

Algorithm 2: Find a strictly bigger \mathbb{Z} -order ([7], Section 5)

Input: B -algebra over \mathbb{Q} of dimension N , given by structure constants;

Λ -order given by \mathbb{Z} -basis $\Lambda = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_N$.

Output: A \mathbb{Z} -basis of a strictly bigger order Γ , if one exists; otherwise, report that Λ is maximal.

1. Compute the discriminant $d_\Lambda = d(e_1, \dots, e_N) \in \mathbb{Z}$. Factor d_Λ .

foreach *prime p dividing d_Λ* **do**

2. Compute the \mathbb{F}_p -algebra $\mathcal{A} = \mathbb{F}_p e_1 \oplus \cdots \oplus \mathbb{F}_p e_N$ by structure constants and the projection $\Lambda \rightarrow \mathcal{A}$.

3. Compute a \mathbb{F}_p -basis of $\text{Rad}(\mathcal{A})$.

4. Compute the \mathbb{F}_p -algebra $\mathcal{C} = \mathcal{A}/\text{Rad}(\mathcal{A})$ and the projection $\phi : \mathcal{A} \rightarrow \mathcal{C}$.

5. Compute the total projection $\Phi : \Lambda \rightarrow \mathcal{C}$.

6. Compute a \mathbb{Z} -basis of $\mathcal{I}_0 = \ker(\Phi)$.

7. Compute a \mathbb{Z} -basis of $O_L(\mathcal{I}_0)$.

if $O_L(\mathcal{I}_0)$ *strictly contains* Λ **then**

 | **return** $\Gamma = O_L(\mathcal{I}_0)$

end

8. Compute the list of \mathbb{F}_p -bases of the minimal nonzero two-sided ideals $\mathcal{K} \subseteq \mathcal{C}$.

foreach \mathcal{K} *in the list* **do**

9. Compute the \mathbb{F}_p -algebra \mathcal{C}/\mathcal{K} by structure constant and the projection $\mathcal{C} \rightarrow \mathcal{C}/\mathcal{K}$.

10. Compute the total projection $\Phi_{\mathcal{K}} : \Lambda \rightarrow \mathcal{C}/\mathcal{K}$.

11. Compute a \mathbb{Z} -basis of $\mathcal{I} = \ker(\Phi_{\mathcal{K}})$.

12. Compute a \mathbb{Z} -basis of $O_L(\mathcal{I})$.

if $O_L(\mathcal{I})$ *strictly contains* Λ **then**

 | **return** $\Gamma = O_L(\mathcal{I})$

end

end

end

13. Return that Λ is maximal.

Comments.

- Computing the discriminant is relatively easy, but factoring it can be hard.
- To compute a basis of the radical, we use SageMath's internal implementation (`A.basis_radical()`), which is based on the algorithm in [4, Section 2.3.2] or [10, Section 2]. **Complexity:** ...
- Computing the quotient, projection, and composition is straightforward.

- To compute the kernel of a \mathbb{Z} -module homomorphism Φ from a free \mathbb{Z} -module of rank N to an \mathbb{F}_p -algebra of dimension r over \mathbb{F}_p , we choose a matrix $M \in M_{r,N}(\mathbb{Z})$ such that

$$\Phi(e_i) = M_{1,i}f_1 + \cdots + M_{r,i}f_r.$$

Then computing the kernel is equivalent to finding a \mathbb{Z} -basis of the solutions $X \in \mathbb{Z}^N$ to the equation $MX \equiv 0 \pmod{p}$.

- Computing a \mathbb{Z} -basis of a left order can be reduced to finding the integer solutions $X \in \mathbb{Z}^N$ to the equation $MX \equiv 0 \pmod{d}$, where M is an integer matrix of size $N^2 \times N$. This can be computationally expensive.
- If \mathcal{C} is a semisimple finite-dimensional algebra over the finite field \mathbb{F}_p , then its minimal nonzero ideals satisfy

$$\mathcal{C} = \mathcal{I}_1 \oplus \cdots \oplus \mathcal{I}_r.$$

To compute them, it suffices to find a family (e_1, \dots, e_r) of central elements (i.e., elements that commute with all elements of \mathcal{C}), which are idempotent ($e_i^2 = e_i$), pairwise orthogonal ($e_i e_j = 0$ for $i \neq j$), and such that $e_1 + \cdots + e_r = 1$, with (e_1, \dots, e_r) maximal for these conditions. Then take $\mathcal{I}_s = \mathcal{C}e_s = e_s\mathcal{C}$. This is implemented internally in Magma (`CentralIdempotent(C)`, Magma Handbook, Section 81.3.4), which uses the algorithm from [3, Section 3].

7. The Explicit Isomorphism Problem

In this section, we give a solution to the `ExplicitIsomorphismProblem`, with a special focus on the case where a \mathbb{Q} -algebra A is isomorphic to $M_4(\mathbb{Q})$. Our approach follows the methods in [6]. To construct a solution over \mathbb{Q} , we will first need to study the problem over other fields, such as a finite field \mathbb{F}_p or the field of real numbers \mathbb{R} , and for matrix algebras of smaller dimension ($n \leq 4$).

The central problem can be stated as follows:

ExplicitIsomorphismProblem

Given a central simple algebra A over a field F , presented by a basis, that is isomorphic to $M_n(F)$, compute an explicit isomorphism $\varphi : A \rightarrow M_n(F)$.

Our strategy is to first reduce the problem to the search for specific types of elements within the algebra. We then develop algorithms to find these elements over \mathbb{F}_p and \mathbb{R} . Finally, we address the main challenge of lifting these solutions from the simpler fields back to \mathbb{Q} .

7.1. Reduction to Finding Zero Divisors and Idempotents. Let F be a field, $n \geq 2$ be an integer, and A be an F -algebra of dimension $N = n^2$ given by an F -basis a_1, \dots, a_N and *structure constants* $(c_{i,j,k})_{1 \leq i,j,k \leq N}$. That is,

$$A = Fa_1 \oplus \dots \oplus Fa_N$$

and

$$a_i a_j = \sum_{k=1}^N c_{i,j,k} a_k \quad (1 \leq i, j \leq N)$$

with $c_{i,j,k} \in F$.

Assume that A is isomorphic to $M_n(F)$ as an F -algebra. We want to compute an explicit isomorphism $\varphi : A \rightarrow M_n(F)$, that is, to output a list of $N = n^2$ matrices with entries in F : M_1, \dots, M_N such that the unique F -linear map from A to $M_n(F)$ which maps a_i onto M_i is an F -algebra isomorphism.

First, we know that A inherits the following algebraic properties which hold in $M_n(F)$. The minimal polynomial of an element of A has a degree of at most n . An element in A is invertible if and only if it is invertible on the left or on the right. An element $x \in A$ is non-invertible if and only if it is a left zero divisor (there exists $y \in A$ such that $xy = 0$) if and only if it is a right zero divisor (there exists $y \in A$ such that $yx = 0$).

We can characterize the zero divisors in A more precisely. One can define the *rank* of an element $x \in A$ as follows. For every isomorphism $\varphi : A \rightarrow M_n(F)$, we have

$$n \cdot \text{rank}(\varphi(x)) = \dim_F(M_n(F)\varphi(x)) = \dim_F(\varphi(Ax)) = \dim_F(Ax).$$

Hence we define the *rank* of an element $x \in A$ by

$$\text{rank}_A(x) := \frac{1}{n} \dim_F(Ax) = \text{rank}(\varphi(x)) \quad (\text{for any isomorphism } \varphi : A \rightarrow M_n(F)).$$

In this section, we start by giving three efficient successive reductions of the problem based on finding some special kinds of elements in A . And then we will discuss which of these elements can be guessed by random picking, depending on the ground field F .

The first reduction is to seek a rank-one element in A . Finding an explicit isomorphism between A and $M_n(F)$ is equivalent to finding a rank-one element in A . Indeed, if we know $\varphi : A \rightarrow M_n(F)$, we just have to express a rank-one matrix, for example, the matrix $S \in M_n(F)$ with only 1 in the first row and 0 on other lines, in the basis $\varphi(a_1), \dots, \varphi(a_N) : S = \lambda_1 \varphi(a_1) + \dots + \lambda_N \varphi(a_N)$; then $x := \lambda_1 a_1 + \dots + \lambda_N a_N$ is a rank-one element. This involves solving an invertible linear system of size N , which is in $\mathcal{O}(n^6)$. Conversely, if $x \in A$ is a rank-one element, then Ax has dimension n over F , and $\varphi : A \rightarrow \text{End}_F(Ax), a \mapsto (z \mapsto az)$ is a non-zero F -algebra homomorphism,

so it is injective because A is simple as a ring and hence bijective by a dimension argument. We start by building a basis \mathcal{B} of Ax ; this consists of extracting a linearly independent family from a generating set, which can be done in $\mathcal{O}(n^5)$. Then, for each $1 \leq i \leq N$, we write down the matrix of the map $Ax \rightarrow Ax, z \mapsto a_i z$ in the basis \mathcal{B} . This can be done in $\mathcal{O}(Nn^2) = \mathcal{O}(n^4)$. Hence we get an explicit isomorphism.

The second reduction is to seek a zero divisor in A , that is, an element with rank $0 < r < n$. We claim that if we can find a zero divisor in algebras isomorphic to $M_k(F)$ for all $2 \leq k < n$, then we can find a rank-one element in A . We proceed by induction on n . For $n = 2$, it is clear. Assume the reduction holds for all $k < n$. Let $x \in A$ be a zero divisor and let $r < n$ be the rank of x . By choosing an isomorphism $\varphi : A \rightarrow M_n(F)$, $X := \varphi(x)$ has rank r , so there exist P, Q invertible matrices such that $X = PJ_r Q$, where

$$J_r := \text{diag}(1, \dots, 1, 0, \dots, 0).$$

We see that $XZX = X$ has a solution $Z \in M_n(F)$, namely $Z = Q^{-1}J_r P^{-1}$. Hence the equation $xzx = x$ has a solution $z \in A$, and we can compute one solution by solving a system of N^2 linear equations in N^2 variables. Let $e := zx \in A$; e satisfies $e^2 = e$ and has rank r . Then $B := eAe$ is a subalgebra of A with unit e . One can easily compute a basis of B and the structure constants of B in this basis. We have $B \cong M_r(F)$: to show this, again we use our isomorphism φ . Let $E := \varphi(e) \in M_n(F)$. E satisfies $E^2 = E$ and has rank $r < n$. By linear algebra, there exists an invertible matrix P such that $E = PJ_r P^{-1}$. Then as F -algebras, we have the isomorphisms $B \cong EM_n(F)E \cong PJ_r P^{-1}M_n(F)PJ_r P^{-1} \cong J_r M_n(F)J_r \cong M_r(F)$. Hence we can apply our induction hypothesis to build $y \in B$, a rank-one element in B . By viewing y in the isomorphism to $M_r(F)$, we see that $\text{rank}_A(y) = \text{rank}_B(y) = 1$.

The third reduction is to find an element with a reducible minimal polynomial. Indeed, if $x \in A$ has a reducible minimal polynomial $\pi = fg$ in $F[T]$, then $f(x)$ is a zero divisor in A . Note that computing the minimal polynomial of x can be done by computing the matrix of the map $z \mapsto xz$ and then computing its minimal polynomial. The complexity of this task depends on the field F and the available algorithms to factorize polynomials in $F[T]$.

The fourth, very concrete reduction that we will try to use the most is to find a *non-trivial idempotent* in A , that is, $e \in A$ such that $e \neq 0, 1$ and $e^2 = e$.

7.2. The case $M_4(\mathbb{Q})$. To solve the explicit isomorphism problem in $M_4(\mathbb{Q})$, we only need to be able to find a zero divisor in $M_4(\mathbb{Q})$ and $M_2(\mathbb{Q})$. Indeed, if $A \cong M_4(\mathbb{Q})$ and $x \in A$ is a zero divisor, then the rank r of x is $r = 1, 2$, or 3 . If $r = 1$, we are done. If $r = 3$, we can compute y such that $xy = 0$. For that, we compute $\pi(T)$, the minimal polynomial of x over \mathbb{Q} . We can write $\pi(T) = Tg(T)$ and let $y = g(x)$. Hence y has

rank one (thinking in the matrix space), and we are done. If $r = 2$, we compute $e \in A$ of rank 2 such that $e^2 = e$, we compute the algebra $B := eAe$ which is isomorphic to $M_2(\mathbb{Q})$, and then a zero divisor in B is a rank-one element in A and we are done.

The problem to find a zero divisor in $A \cong M_2(\mathbb{Q})$ is computationally equivalent to finding a non-trivial rational solution to a ternary quadratic form of the type

$$-aX^2 - bY^2 + abZ^2 = 0.$$

There exist some algorithms for this in the literature: statement: [13, Theorem 7.19], algorithm: [1, Algorithm I], [8, Theorem 3], [12, Algorithm 3.4].

7.3. Use of randomization depending on the ground field. Let $n \geq 2$ be an integer.

In $M_n(\mathbb{F}_p)$ Let p be a prime. We consider the ring $M_n(\mathbb{F}_p)$, equipped with the uniform probability distribution. Let M be a random variable uniformly distributed in $M_n(\mathbb{F}_p)$. Then

$$\mathbb{P}(M \text{ is a zero divisor}) = \frac{p^{n^2} - 1 - (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})}{p^{n^2}},$$

which tends to zero as $p \rightarrow \infty$. Thus, finding a zero divisor by random sampling is not guaranteed.

However, for polynomials over \mathbb{F}_p , we have:

$$\mathbb{P}(f \in \mathbb{F}_p[T] \text{ of degree } d \text{ is reducible}) = 1 - \frac{1}{dp^d} \sum_{k|d} \mu\left(\frac{d}{k}\right) p^k \approx 1 - \frac{1}{d},$$

where μ denotes the Möbius function.

More precisely, in Appendix B, we give an exact formula for the probability that a uniformly chosen matrix in $M_n(\mathbb{F}_p)$ has a reducible minimal polynomial. In particular, we show that

$$\mathbb{P}(M \in M_n(\mathbb{F}_p) \text{ has a reducible minimal polynomial}) \geq \frac{1}{2}$$

for all $n \geq 2$ and all primes p . We also discuss the asymptotic behavior of this probability. Here are the values for small n and p :

Overall, this probability is always relatively high (at least $\frac{1}{2}$). Therefore, by repeatedly sampling random matrices, one can efficiently find a matrix in $M_n(\mathbb{F}_p)$ with a reducible minimal polynomial. Consequently, the explicit isomorphism problem is relatively easy in $M_n(\mathbb{F}_p)$.

Table 1: Probability of a Reducible Minimal Polynomial

$p \setminus n$	2	3	4
2	0.7500	0.9023	0.9367
3	0.7407	0.8243	0.8729
5	0.6720	0.7542	0.8171

In $M_n(\mathbb{R})$ In $M_n(\mathbb{R})$, for the Lebesgue measure on \mathbb{R}^{n^2} , the set of zero divisors has measure 0. However, the probability that a real monic polynomial of degree d with coefficients uniformly distributed in $[-M, M]$ is irreducible is low (it is even 0 if d is odd). Consequently, the explicit isomorphism problem is "easy" in $M_n(\mathbb{R})$.

In $M_n(\mathbb{Q})$ In $M_n(\mathbb{Q})$, for any finite subset $S \subset \mathbb{Q}$, the probability that a matrix with entries in S has a reducible minimal polynomial is very low. Hence the explicit isomorphism problem in $M_n(\mathbb{Q})$ can't be efficiently solved by randomly picking elements.

7.4. Lifting and approximation of non-trivial idempotents over \mathbb{Q} . Let A be a finite-dimensional \mathbb{Q} -algebra of dimension $N = n^2$ assumed to be isomorphic to $M_4(\mathbb{Q})$. Since we know how to compute a \mathbb{Z} -basis of a maximal order in A , we can view

$$A = \mathbb{Q}a_1 \oplus \cdots \oplus \mathbb{Q}a_N \cong M_4(\mathbb{Q})$$

such that the \mathbb{Z} -algebra

$$O = \mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_N$$

is a maximal order in A (and thus isomorphic to $M_n(\mathbb{Z})$) and the structure constants are $c_{i,j,k} \in \mathbb{Z}$:

$$a_i a_j = \sum_{k=1}^N c_{i,j,k} a_k \quad (1 \leq i, j \leq N).$$

The fact that $c_{i,j,k} \in \mathbb{Z}$ allows us to define for every field K , and especially finite fields, the K -algebra:

$$O_K := Ka_1 \oplus \cdots \oplus Ka_N$$

in the sense that O_K has a basis a_1, \dots, a_N with structure constants being the images of the integers $c_{i,j,k}$ in K .

We want to solve the explicit isomorphism problem for A . As we saw in Section 7.1, it suffices to find $e \in A$ such that $e \neq 0, 1$ and $e^2 = e$. One approach is the following: We choose a field K such that it is easy with randomization to find a non-trivial $f \in O_K$ such that $f^2 = f$, and then we try to lift f to an element in A .

With $K = \mathbb{R}$. In $O_{\mathbb{R}} := \mathbb{R}a_1 \oplus \cdots \oplus \mathbb{R}a_N$, we can randomly pick a $b = r_1a_1 + \cdots + r_Na_N$ with coefficients in \mathbb{Q} such that the minimal polynomial of b over \mathbb{Q} , $\pi_{b,\mathbb{Q}}$, has a real root $\gamma \in \mathbb{R}$. Then $c := g(b)$ where $\pi_{b,\mathbb{Q}}(T) = (T - \gamma)g(T)$ is a zero divisor in $O_{\mathbb{R}}$, and we can deduce a non-trivial idempotent $f \in O_{\mathbb{R}}$ with coefficients in $\mathbb{Q}(\gamma)$. Concretely, we can write $f = x_1a_1 + \cdots + x_Na_N$ with $x_i \in \mathbb{Q}(\gamma)$, and the relation $f^2 = f$ is equivalent to the relations:

$$\left(\sum_{1 \leq i, j \leq N} x_i x_j c_{i,j,k} \right) - x_k = 0 \quad (1 \leq k \leq N).$$

Hence by taking \tilde{x}_i , rational approximations of x_i , the element $e := \tilde{x}_1a_1 + \cdots + \tilde{x}_Na_N \in A$ satisfies that $e^2 - e$ has small rational coefficients in the basis a_1, \dots, a_N .

With $K = \mathbb{F}_p$. In $O_{\mathbb{F}_p} := \mathbb{F}_pa_1 \oplus \cdots \oplus \mathbb{F}_pa_N$, we can easily, by using randomization, build $f \in O_{\mathbb{F}_p}$, a non-trivial idempotent. By writing $f = x_1a_1 + \cdots + x_Na_N$ with $x_i \in \mathbb{F}_p$ and taking any lift $y_i \in \mathbb{Z}$ of $x_i \in \mathbb{F}_p$, the element $e := y_1a_1 + \cdots + y_Na_N \in O \subset A$ satisfies $e^2 - e \equiv 0 \pmod{p}$, i.e., $e^2 - e$ has integer coefficients divisible by p in the basis a_1, \dots, a_N .

With $K = \mathbb{Q}_p$. By the previous paragraph, we can, in particular, build an element $e \in O \subset O_{\mathbb{Q}_p}$ such that $e^2 - e \equiv 0 \pmod{p}$. Then, using a version of Hensel's Lemma, as in [2] Lemma 5.1, if we define by induction $e_0 := e$ and $e_{k+1} := 3e_k^2 - 2e_k^3$, the sequence (e_k) satisfies $e_k^2 - e_k \equiv 0 \pmod{p^{2^k}}$, $e_{k+1} \equiv e_k \pmod{p^{2^k}}$, and $e_k \equiv e \pmod{p}$. Hence, the sequence (e_k) converges in $O_{\mathbb{Q}_p}$ to an element $f \in O_{\mathbb{Q}_p}$ such that $f^2 = f$. This element f is non-trivial because it is equal to e modulo p . The approximation e_k of f gives a non-trivial element of O that is quasi-idempotent, in the sense that the coefficients of $e_k^2 - e_k$ are divisible by p^{2^k} .

Provisional conclusion For the moment, we are able to build in A an element $e \neq 0, 1$ such that $e^2 - e$ has small coefficients in the basis a_1, \dots, a_N , either for the absolute value or for the p -adic absolute value. If we manage to find an element $e \in A$ such that $e^2 - e$ is exactly 0, we are done.

8. Explicit isomorphism problem directly for $M_4(\mathbb{Q})$

Here we present a direct way, without using a maximal order in $A \cong M_4(\mathbb{Q})$, to find a zero divisor in A , based on the algorithm `FindZeroDivisor` in [9].

First, we find an element $a \in A$ such that its minimal polynomial has degree 2 and is irreducible over \mathbb{Q} . Then the algebra $B := C_A(a) := \{x \in A \mid ax = xa\}$ can be computed with its structure constants. One can show that B has dimension 8 over \mathbb{Q}

and so dimension 4 over $E = \mathbb{Q}(a)$. Moreover, one can show that as a $\mathbb{Q}(a)$ -algebra, $B \cong M_2(E)$. It suffices to find a zero divisor in B . For that, first, it is not too hard to construct $i, j \in B$ and $\lambda, \mu \in E$ such that $1, i, j, ij$ is an E -basis of B , which allows us to view B as a quaternion algebra $B = \left(\frac{\lambda, \mu}{E}\right)$. Then concretely, finding a zero divisor is equivalent to finding a solution to one of the equations:

$$-\lambda X^2 - \mu Y^2 + \lambda\mu Z^2 = 0 \quad (\text{for } X, Y, Z \in E \text{ not all zero})$$

or

$$\lambda X^2 + \mu Y^2 = 1 \quad (\text{for } X, Y \in E)$$

or the norm equation

$$\mathcal{N}_{E(\sqrt{\lambda})/E}(z) = \mu \quad (\text{for } z \in E(\sqrt{\lambda})).$$

For the last one, an algorithm is presented in [11].

9. Interlude: Motivation from elliptic curve theory

Short definition of elliptic curve.

Short definition of the endomorphism ring $End(E)$.

Short definition and existence of the dual endomorphism map $End(E) \rightarrow End(E), \alpha \mapsto \hat{\alpha}$

Implication that $End(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ could be a quaternion algebra sometimes.

Short definition of super singular elliptic curve.

Why are they interesting ?

Statement that if E is super singular then $End(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is well an quaternion algebra over \mathbb{Q}

If E is super singular over F_p and, $End(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is exactly $B_{p,\infty}$.

Computational problem believe to be hard.

10. Explicit isomorphism of quaternion algebras

We finish by solving the `GeneralExplicitIsomorphismProblem` between central simple algebra over \mathbb{Q} . And we will see how this can be improve when A and B are actually quatenrion algebra and we know maximal order in each.

GeneralExplicitIsomorphismProblem: Given two isomorphic central simple algebra A and B , compute an isomorphism $f : A \rightarrow B$.

Lemma 10.1. *Let A be a central simple algebra of dimension N , there exist an isomorphism $\varphi : A \otimes A^{op} \rightarrow \text{End}_{\mathbb{Q}}(A)$ such that for all $a, b \in A$, $\varphi(a \otimes b)$ is $A \rightarrow A; z \mapsto azb$. consequently, $A \otimes A^{op}$ is isomorphic to $M_N(\mathbb{Q})$.*

Proof. The map $A \times A^{op} \rightarrow \text{End}_{\mathbb{Q}}(A)$ which map a, b to $z \mapsto azb$, is F -bilinear. By universal properties of tensor product this yields to a F -linear map $\varphi : A \otimes A^{op} \rightarrow \text{End}_{\mathbb{Q}}(A)$ satisfying $\varphi(a \otimes b)$ is $A \rightarrow A; z \mapsto azb$ for all a, b . It is easily check that φ respect the multiplication on pure tensor and everywhere. Since $A \otimes A^{op}$ is simple, φ is injective and then bijective by dimension. \square

Proposition 10.2. *Let A, B be two central simple algebra of dimension N . Then A and B are isomorphic if and only if $A \otimes B^{op}$ is isomorphic to $M_N(F)$.*

A. Implementation and Precise Algorithms

We present here most of the harder algorithms used in the implementation: https://github.com/TommyChakroun/quat_alg_project

We give as well the mathematical idea and the algorithm together with a comment on the complexity or randomization if we used randomized algorithms.

A.1. Reduction $\varphi : A \otimes_{\mathbb{Q}} B^{op} \rightarrow M_4(\mathbb{Q})$ to $f : A \rightarrow B$. Let A, B be two central simple algebras of same dimension n . In Proposition 10.2 we showed the equivalence

$$A \cong B \iff A \otimes_{\mathbb{Q}} B \cong M_{n^2}(\mathbb{Q}).$$

The proof of the direct implication was already explicit and efficient, but for the converse we had argued theoretically with the Wedderburn decomposition. Here we present an efficient but randomized algorithm to show this converse implication.

Suppose we have $\varphi : A \otimes_{\mathbb{Q}} B^{op} \rightarrow M_4(\mathbb{Q})$ an isomorphism. Fix us e_1, \dots, e_N a basis of A and f_1, \dots, f_n a basis of B . Denote $N = n^2$ and $V = \mathbb{Q}^N$. For each $v \in V$ we consider:

$$\begin{aligned} \lambda_v : A &\rightarrow V, & a &\mapsto \varphi(a \otimes 1)v \\ \mu_v : B &\rightarrow V, & b &\mapsto \varphi(1 \otimes b)v. \end{aligned}$$

Both λ_v and μ_v are \mathbb{Q} -linear maps.

First we claim that if we find $v \in V$ such that both λ_v and μ_v are \mathbb{Q} -linear isomorphisms, then $f : A \rightarrow B, a \mapsto \mu_v^{-1}(\lambda_v(a))$ is a \mathbb{Q} -algebra isomorphism. Indeed f

is a \mathbb{Q} -linear isomorphism, $\mu_v(1) = v = \lambda_v(1)$ so f maps 1_A to 1_B . For the preservation of the product: let $a, a' \in A$ and $b = f(a)$, $b' = f(a')$ in B . Then

$$\begin{aligned}
\mu_v(f(aa')) &= \varphi(aa' \otimes 1)v \\
&= \varphi(a \otimes 1)\varphi(a' \otimes 1)v \\
&= \varphi(a \otimes 1)\varphi(1 \otimes b')v \\
&= \varphi(1 \otimes b')\varphi(a \otimes 1)v \\
&= \varphi(1 \otimes b')\varphi(1 \otimes b)v \\
&= \varphi(1 \otimes bb')v \\
&= \mu_v(bb')
\end{aligned}$$

This shows $f(aa') = f(a)f(a')$.

Hence it suffices to show the existence of a suitable $v \in V$. We do this for λ . This comes from the theoretical existence of an isomorphism from A to B as follows. Choose $f : A \rightarrow B$ an isomorphism and denote $\varphi_f : A \otimes_{\mathbb{Q}} B^{op} \rightarrow M_N(\mathbb{Q})$ the other isomorphism obtained. By Lemma ?? there exists some invertible matrix $P \in M_N(\mathbb{Q})$ such that:

$$\forall c \in A \otimes_{\mathbb{Q}} B^{op}, \quad \varphi(c) = P\varphi_f(c)P^{-1}.$$

Then for $v \in V$ and $a \in A$ we have

$$P\lambda_{P^{-1}v}(a) = P\varphi(a \otimes 1)P^{-1}v = \varphi_f(a \otimes 1)v = \text{Mat}(b \mapsto f(a)b)v.$$

Hence if we take v to be the coordinates of 1_B in the basis of B we obtain:

$$P\lambda_{P^{-1}v} : A \rightarrow V, \quad a \mapsto \text{Mat}(f(a), B)$$

so it is an isomorphism.

Now from the existence of a suitable v we are going to deduce that almost all $v \in V$ satisfy this condition in the following sense.

Fix a basis e_1, \dots, e_N of A , and let $M_i = \varphi(e_i \otimes 1) \in M_N(\mathbb{Q})$. For all $v = (v_1, \dots, v_N) \in V$:

The matrix of λ_v in the basis e_1, \dots, e_N of A and the canonical basis of $V = \mathbb{Q}^N$ is, by columns:

$$(M_1v \quad \dots \quad M_Nv).$$

Expanding, we have:

$$\begin{pmatrix} \sum_{j=1}^N m_{1j}^{(1)} v_j & \cdots & \sum_{j=1}^N m_{1j}^{(N)} v_j \\ \sum_{j=1}^N m_{2j}^{(1)} v_j & \cdots & \sum_{j=1}^N m_{2j}^{(N)} v_j \\ \vdots & \ddots & \vdots \\ \sum_{j=1}^N m_{Nj}^{(1)} v_j & \cdots & \sum_{j=1}^N m_{Nj}^{(N)} v_j \end{pmatrix}$$

where $M_i = (m_{kj}^{(i)})_{1 \leq k, j \leq N} \in M_N(\mathbb{Q})$.

So the determinant is of the form $P_A(v_1, \dots, v_N)$ for some $P_A \in \mathbb{Q}[T_1, \dots, T_N]$.

The fact that we found one suitable v proves that P_A is not identically zero. Then by the Schwartz-Zippel lemma for all finite subset $S \subset \mathbb{Q}$ we have $\text{Card}(Z(P_A) \cap S^N) \leq N \text{Card}(S)^{N-1}$.

Similarly for P_B associated to B and μ , $\text{Card}(Z(P_B) \cap S^N) \leq N \text{Card}(S)^{N-1}$.

Then a $v \in V$ satisfies both λ_v and μ_v are isomorphisms if and only if v is not a zero of P_A neither P_B . By taking $S \subset \mathbb{Q}$ sufficiently large such that $2N \text{Card}(S)^{N-1} < \text{Card}(S)^N$ this is possible. This concludes the proof and we deduce the following algorithm.

Algorithm 3: Isomorphism $f : A \rightarrow B$ from $\varphi : A \otimes B^{op} \rightarrow M_N(\mathbb{Q})$

Input: A, B two central simple algebras of dimension n and

$\varphi : A \otimes B^{op} \rightarrow M_N(\mathbb{Q})$ an isomorphism given in a basis $e_i \otimes f_j$ which is the tensor product of a basis of A and a basis of B

Output: $f : A \rightarrow B$ an isomorphism

1. Choose a finite subset $S \subset \mathbb{Q}$ such that $2N \text{Card}(S)^{N-1} < \text{Card}(S)^N$

foreach $v \in S^N$ **do**

2. Compute U the matrix of $A \rightarrow V$, $a \mapsto \varphi(a \otimes 1)v$ in the basis of A and the canonical basis of V

3. Compute M the matrix of $B \rightarrow V$, $b \mapsto \varphi(1 \otimes b)v$ in the basis of B and the canonical basis of V

4. **if** M and U are invertible **then**

5. Compute M^{-1}

6. **return** $f : A \rightarrow B$ given in the basis of A by:

$$f(e_i) = \sum_{j=1}^N M_{j,i}^{-1} U_{j,i} f_j$$

end

end

Complexity. Not evaluated yet.

A.2. Solution to a System $AX \equiv 0 \pmod{d}$ for Integral Matrices.

Algorithm 4: ModularMatrixKernel

Input: $A \in M_{m \times n}(\mathbb{Z})$, $d \in \mathbb{Z}_{>0}$

Output: $X_1, \dots, X_k \in \mathbb{Z}^n$ a \mathbb{Z} -basis of the \mathbb{Z} -submodule $\{X \in \mathbb{Z}^n \mid AX \equiv 0 \pmod{d}\}$

1. Compute the Smith normal form of A : $U \in \text{GL}_m(\mathbb{Z})$, $V \in \text{GL}_n(\mathbb{Z})$ such that $UAV = D$ is in diagonal form
 2. If $t = \min(n, m)$, let Y_1, \dots, Y_t be defined by $Y_i = (0, \dots, 0, \frac{d}{\gcd(d, D_{i,i})}, 0, \dots, 0)$
 3. If $n > m$, complete with $Y_j = (0, \dots, 0, 1, 0, \dots, 0)$ for $t < j \leq n$
 4. **return** VY_1, \dots, VY_k
-

Implementation. The function `kernel_mod(A,d)` is available at

[maximal_orders/maximal_orders_utilities.sage](#).

Complexity. Not evaluated yet.

A.3. Computation of Left Order. Let B be a finite dimensional algebra over \mathbb{Q} of dimension N . Let

$$I = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_N$$

be a \mathbb{Z} -(full) lattice in B . The *left order* of I is the set

$$O_L(I) := \{\alpha \in B \mid \alpha I \subset I\}.$$

We claim that $O_L(I)$ is indeed an order. Indeed $O_L(I)$ is a \mathbb{Z} -submodule of B , is stable under multiplication, contains 1. It remains to show that $O_L(I)$ contains a \mathbb{Q} -basis of B . Starting from b_1, \dots, b_N any basis of B , then for all i there exists $t_i \in \mathbb{Z}_{>0}$ such that $t_i b_i \in O_L(I)$.

Now we want to compute explicitly a \mathbb{Z} -basis f_1, \dots, f_N of $O_L(I)$. First note that there exists $s \in \mathbb{Z}_{>0}$ such that $s \cdot 1_B \in I$. Hence $O_L(I) \cdot s \subset I$ so $O_L(I) \subset s^{-1}I$. After, for $\alpha \in s^{-1}I$ that we write $\alpha = s^{-1}(x_1 e_1 + \dots + x_N e_N)$ with $x_i \in \mathbb{Z}$:

$$\alpha \in O_L(I) \iff \forall j, \alpha e_j \in I \iff \forall j, s^{-1}(x_1 e_1 e_j + \dots + x_N e_N e_j) \in \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_N$$

Let's write the *structure constants* of the basis e_1, \dots, e_N , that is:

$$e_i e_j = \sum_{k=1}^N c_{ijk} e_k \quad (1 \leq i, j \leq N), \quad c_{ijk} \in \mathbb{Q}.$$

Then

$$\alpha \in O_L(I) \iff \forall j, k, \sum_{i=1}^N s^{-1} c_{ijk} x_i \in \mathbb{Z}$$

or equivalently by denoting $X = (x_1, \dots, x_N) \in \mathbb{Z}^N$ and $T = (s^{-1} c_{ijk})$ the rational matrix with N^2 rows and N columns:

$$\alpha \in O_L(I) \iff TX \in \mathbb{Z}^{N^2}.$$

Finally by multiplying both sides by the least common multiple of the denominators of T this yields solving $AX \equiv 0 \pmod{d}$ for some integer matrix A of size $N^2 \times N$. Hence together with the previous algorithm we deduce a method to compute the left order of I .

Algorithm 5: LeftOrder

Input: B a finite dimensional algebra over \mathbb{Q} ; e_1, \dots, e_N a \mathbb{Q} -basis of B
representing $I = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_N$

Output: A \mathbb{Z} -basis of the left order $O_L(I)$

1. Write $1_B = r_1 e_1 + \dots + r_N e_N$ with $r_i \in \mathbb{Q}$
 2. Let $s \in \mathbb{Z}_{>0}$ be the least common multiple of the denominators of r_i
 3. Compute $c_{i,j,k}$ the structure constants of the basis e_1, \dots, e_N , that is
 $e_i e_j = \sum c_{i,j,k} e_k$
 4. Let d be the lcm of the denominators of the $s \cdot c_{i,j,k}$ and let
 $A = (d \cdot s \cdot c_{i,j,k})_{1 \leq i \leq N; 1 \leq j, k \leq N} \in M_{N^2, N}(\mathbb{Z})$
 5. Let $X_1, \dots, X_\ell \in \mathbb{Z}^N$ be a \mathbb{Z} -basis of solutions of $AX \equiv 0 \pmod{d}$
 6. **return** $f_1, \dots, f_\ell \in B$ where $f_i = \frac{1}{s}(X_{i,1}e_1 + \dots + X_{i,N}e_N)$
-

Implementation. The function `left_order(B, Zbasis_I)` is available at

[maximal_orders/maximal_orders_utilities.sage](#).

Complexity: In number of additions/multiplications. Computing structure constants: one inversion of $N \times N$ matrix ($\mathcal{O}(N^3)$), N^2 products of matrix-vector of size N ($\mathcal{O}(N^2 \times N^2)$). Solving the system $AX \equiv 0 \pmod{d}$ with A of size $N^2 \times N$ and X of size N ($\mathcal{O}(??)$).

Total: $\mathcal{O}(??)$.

Remark A.1. If we suppose in addition that B is a division algebra or even just that every element of the \mathbb{Z} -basis e_1, \dots, e_N of the lattice $I = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_N$ are

invertible in B , then we can use a more efficient algorithm as follows. Let $\alpha \in B$, we have

$$\alpha \in O_L(I) \iff \forall j, \alpha e_j \in I \iff \forall j, \alpha \in e_j^{-1}I = \mathbb{Z}e_j^{-1}e_1 \oplus \cdots \oplus \mathbb{Z}e_j^{-1}e_N$$

The last direct sum holds because $(e_j^{-1}e_1, \dots, e_j^{-1}e_N)$ is still a \mathbb{Q} -basis of B since $z \mapsto e_j^{-1}z$ is a \mathbb{Q} -linear automorphism of B .

Hence to compute the left order it suffices to compute an intersection of lattices. There are efficient algorithms for this based on the Hermite normal form. This is the method used in SageMath for the case of division quaternion algebras.

A.4. Randomized Computation of Central Simple Idempotents over a Finite Field. We begin with some general notions about rings. Let R be an arbitrary (unital) ring. There is a correspondence between:

1. The decomposition of R into ideals: $R = I_1 \oplus \cdots \oplus I_r$,
2. The decomposition of 1_R into *central orthogonal idempotents* $1_R = e_1 + \cdots + e_r$, where $e_i \in Z(R)$, $e_i^2 = e_i$, and $e_i e_j = 0$ if $i \neq j$.

Now we turn to algebras over finite fields. Fix a finite field $F = \mathbb{F}_p$. If A is a *semisimple algebra* (i.e., an algebra isomorphic to a direct product of simple algebras), then by the Wedderburn–Artin theorem, there exist integers n_1, \dots, n_r and division algebras D_1, \dots, D_r over F such that

$$A \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r).$$

Lemma A.2. *Consequently, A has exactly r minimal nonzero two-sided ideals I_1, \dots, I_r , which satisfy $A = I_1 \oplus \cdots \oplus I_r$. Moreover, writing $1 = e_1 + \cdots + e_r$ for the corresponding decomposition of the identity, the elements e_1, \dots, e_r are central orthogonal idempotents, and e_i is the identity of I_i .*

Proof. Let us fix an isomorphism as above. The image of $M_{n_i}(D_i)$ in A is simple, so its image I_i is a minimal nonzero two-sided ideal of A , and $A = I_1 \oplus \cdots \oplus I_r$. By the correspondence above, we obtain a decomposition of 1 into central orthogonal idempotents e_i , each acting as the identity on I_i .

Suppose J is another minimal nonzero two-sided ideal of A . Choose $x \in J$, $x \neq 0$, and write $x = x_1 + \cdots + x_r$ with $x_i \in I_i$. Since $x \neq 0$, assume $x_1 \neq 0$. Then $e_1 x = x_1 \neq 0$, so $I_1 \cap J \neq 0$. But both I_1 and J are minimal two-sided ideals, so $I_1 = J$. Hence, any minimal two-sided ideal must be one of the I_i . \square

Lemma A.3. *Conversely, if e_1, \dots, e_r are central orthogonal idempotents summing to 1, then the ideals Ae_i are exactly the minimal nonzero two-sided ideals of A , up to permutation.*

Proof. ... □

Finding central orthogonal idempotents e_1, \dots, e_r summing to 1 in A reduces to finding them in the center $Z(A)$. We have:

$$Z(A) \cong Z(D_1) \times \cdots \times Z(D_r) \cong K_1 \times \cdots \times K_r,$$

where each K_i/F is a finite field extension.

So we are reduced to the following problem: let Z be a finite F -algebra isomorphic to a product

$$Z \cong K_1 \times \cdots \times K_r,$$

of finite field extensions of F . Find a maximal family e_1, \dots, e_r of central orthogonal idempotents in Z .

To solve this, we study the structure of F -algebras isomorphic to such a product. Let $a = (a_1, \dots, a_r) \in K_1 \times \cdots \times K_r$. The minimal polynomial of a over F is

$$\pi_a = \text{lcm}(\pi_{a_1}, \dots, \pi_{a_r}),$$

which is square-free and can be written as $\pi_a = \pi_1 \dots \pi_s$, with $\{\pi_1, \dots, \pi_s\} = \{\pi_{a_1}, \dots, \pi_{a_r}\}$.

If $s \geq 2$, by the Chinese Remainder Theorem, there exist polynomials h_1, \dots, h_s such that

$$h_i \equiv 1 \pmod{\pi_i}, \quad h_i \equiv 0 \pmod{\pi_j} \text{ for } j \neq i.$$

Then for each i , $h_i(a)$ has the form:

$$w_i = h_i(a) = (h_i(a_1), \dots, h_i(a_r)) = (0, 0, \dots, 0, 1, 0, \dots, 0),$$

which gives a central orthogonal idempotent.

If $s = r$, then the w_i are exactly the elementary idempotents $(0, \dots, 0, 1, 0, \dots, 0)$, which form a maximal list of central orthogonal idempotents in $K_1 \times \cdots \times K_r$.

This procedure can be applied in A since minimal polynomials and their factorization are abstract notions that can be computed from structure constants. So we randomly choose $a \in A$, compute its minimal polynomial π_a , factor it as $\pi_a = \pi_1 \dots \pi_s$, and attempt the construction above.

If $s \geq 2$, then

$$A = A\omega_1 \oplus \cdots \oplus A\omega_s,$$

where each $A\omega_i$ is a unital subalgebra with identity $\omega_i = h_i(a)$. We can then recurse within each $A\omega_i$.

Note that the case $s = r$ may not occur when the prime p is small and r is large; for example, when $A \cong \mathbb{F}_p^r$.

Still, if $r \geq 2$, then $s \geq 2$ occurs for most $a \in A$, so a randomized approach works: pick random elements of A until the minimal polynomial splits. If no such element is found, then A is a field and we return 1_A .

We deduce a deterministic algorithm in theory, but the reasonable complexity is randomized.

Algorithm 6: CentralIdempotentsCommutativeSplit

Input: Z Semisimple commutative algebra over a finite field \mathbb{F}_p given by structure constants

Output: Primitive central idempotents $e_1, e_2, \dots, e_r \in A$

foreach a *in* Z **do**

1. Compute the minimal polynomial $\pi_a \in \mathbb{F}_p[T]$ of a .
2. Factor $\pi_a = \pi_1 \dots \pi_s$ in $\mathbb{F}_p[T]$.
3. **if** $s \geq 2$ **then**
 4. By the Chinese remainder theorem, compute $h_1, \dots, h_s \in \mathbb{F}_p[T]$ such that $h_i \equiv 1 \pmod{\pi_i}$, $h_i \equiv 0 \pmod{\pi_j}$ for $j \neq i$.
 5. Compute $\omega_i := h_i(a) \neq 0$ for $i = 1, \dots, s$.
 6. Compute a basis BA_i of $A_i := A\omega_i$.
 7. Compute the structure constants of A_i in BA_i and build the abstract version of A_i .
 8. $Res = []$;
 9. **foreach** $i = 1, \dots, s$ **do**
 10. Compute recursively
 $e_1, \dots, e_k = \text{CentralIdempotentsCommutative}(A_i)$.
 11. Lift e_1, \dots, e_k in Z and add it to res .
 - end**
12. **return** Res

end

end

13. **return** the list 1_A

Implementation. The function `central_idempotent_commutative_split` is available at [minimal_ideals/minimal_ideals_manually.sage](#).

Comments. The algorithm is deterministic in theory with complexity at worst $\text{Card}(Z) = p^n$. It really depends on the size of the prime p and the dimension n . If both are relatively small we can easily iterate on Z . Otherwise if p is a very large prime around 100 bits then we can't reasonably iterate on Z so we prefer to pick a finite random number of elements of Z . Luckily when p is large and n small it happens that the probability that a is *decomposable* that is $s \geq 2$ in the algorithm is very high. Actually when p is very large in comparison to n we can use an easier algorithm. For example in our purpose of computing a maximal order containing an order O in the matrix ring $M_4(\mathbb{Q})$, for each prime dividing $\text{disc}O$ we compute a finite dimensional algebra \mathcal{A} over \mathbb{F}_p of dimension 16 then we quotient \mathcal{A} by its radical so $\mathcal{A}/\text{Rad}(\mathcal{A})$ has dimension less than 16 over \mathbb{F}_p and consequently its center Z has dimension at most 16 over \mathbb{F}_p . It is in this final algebra Z that we run our algorithm. Hence provided that all prime factors of $\text{disc}O$ are much bigger than 16, the following algorithm may give the correct answer with a high probability and less computation time.

Algorithm 7: CentralIdempotentsCommutativeOneTime

Input: Z Semisimple commutative algebra over a finite field \mathbb{F}_p given by structure constants

Output: Primitive central idempotents $e_1, e_2, \dots, e_r \in A$

1. Pick a random $a \in Z$.
 2. Compute the minimal polynomial $\pi_a \in \mathbb{F}_p[T]$ of a .
 3. Factor $\pi_a = \pi_1 \dots \pi_s$ in $\mathbb{F}_p[T]$.
 4. By the Chinese remainder theorem, compute $h_1, \dots, h_s \in \mathbb{F}_p[T]$ such that $h_i \equiv 1 \pmod{\pi_i}$, $h_i \equiv 0 \pmod{\pi_j}$ for $j \neq i$.
 5. Compute $\omega_i := h_i(a) \neq 0$ for $i = 1, \dots, s$.
 6. **return** the list e_1, \dots, e_s
-

Implementation. The function `central_idempotent_commutative` is available at [minimal_ideals/minimal_ideals_manually.sage](#).

Precise evaluation of the probabilities. The success and complexity of the previous algorithm depend directly on the proportion of elements Z satisfying good algebraic properties. To compute this proportion, we can as well work directly on

$$Z = K_1 \times \dots \times K_r$$

where K_i/\mathbb{F}_p are finite field extensions. We denote also n the \mathbb{F}_p -dimension of Z , that is:

$$n = [K_1 : \mathbb{F}_p] + \dots + [K_r : \mathbb{F}_p]$$

Since we will not know a priori the value of r when running the algorithm, n is the only reasonable bound that we can put on r .

Now let us define two subsets of Z :

$$S_0 := \{a = (a_1, \dots, a_r) \in Z \mid \pi_{a_1} = \dots = \pi_{a_r}\}$$

$$S_1 := \{a = (a_1, \dots, a_r) \in Z \mid \exists i \neq j \quad \pi_{a_i} = \pi_{a_j}\}$$

and let us denote $d_i = \frac{\text{Card}S_i}{\text{Card}Z}$ their densities: $0 \leq d_i \leq 1$

Then:

1. The success of the algorithm `CentralIdempotentsCommutativeSplit` depends on whether d_0 is near zero for the first split, and afterward we have to deal with the recursion.
2. The success of the algorithm `CentralIdempotentsCommutativeOneTime` depends only on whether d_1 is near zero.

B. Number of Irreducible Matrices in $M_n(\mathbb{F}_p)$

Let $n > 0$ be an integer and let p be a prime.

In this appendix, we give an explicit formula for the number $I(n, p)$ of *irreducible* matrices in $M_n(\mathbb{F}_p)$, that is, matrices with an irreducible minimal polynomial. This will allow us to calculate the probability that a uniformly random matrix in $M_n(\mathbb{F}_p)$ has a reducible minimal polynomial. If the minimal polynomial π_M of a matrix M is reducible, say $\pi_M = fg$ where f, g are non-constant polynomials, then $f(M)$ is a non-zero matrix (since $\deg(f) < \deg(\pi_M)$) which is a zero divisor because $f(M)g(M) = \pi_M(M) = 0$.

First, we recall and we will use the classical result: for an integer $d > 0$, the number of monic irreducible polynomials in $\mathbb{F}_p[X]$ of degree d is

$$N_d(p) = \frac{1}{d} \sum_{k|d} \mu\left(\frac{d}{k}\right) p^k$$

where μ is the Möbius function.

For $M \in M_n(\mathbb{F}_p)$, we denote by π_M its minimal polynomial. First, if $M \in M_n(\mathbb{F}_p)$ has a minimal polynomial π_M that is irreducible of degree d , then d must divide n .

Indeed, let χ_M be the characteristic polynomial of M . We have that π_M divides χ_M . Since π_M is irreducible, the rational canonical form of M is composed of blocks of the companion matrix of π_M . This implies that $\chi_M = \pi_M^k$ for some integer k . By comparing degrees, we have $n = \deg(\chi_M) = k \cdot \deg(\pi_M) = kd$, and hence d divides n .

Conversely, let us fix $\pi \in \mathbb{F}_p[X]$ as a monic irreducible polynomial of degree $d \geq 1$ such that $d \mid n$. Let

$$\mathcal{A}_\pi := \{M \in M_n(\mathbb{F}_p) \mid \pi_M = \pi\}$$

and let us count the cardinal of \mathcal{A}_π . By the theory of rational canonical forms, a matrix M has the minimal polynomial π (with π irreducible of degree d) if and only if it is similar to a block diagonal matrix

$$D_\pi = \text{diag}(C_\pi, \dots, C_\pi)$$

where there are $k = n/d$ blocks, and C_π is the $d \times d$ companion matrix of π . If $\pi(X) = X^d + a_{d-1}X^{d-1} + \dots + a_0$, then

$$C_\pi = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{d-1} \end{pmatrix}$$

The set \mathcal{A}_π is the orbit of D_π under the conjugation action of $GL_n(\mathbb{F}_p)$ on $M_n(\mathbb{F}_p)$.

$$\mathcal{A}_\pi = \{PD_\pi P^{-1} \mid P \in GL_n(\mathbb{F}_p)\}$$

By the orbit-stabilizer theorem, the size of this orbit is

$$|\mathcal{A}_\pi| = \frac{|GL_n(\mathbb{F}_p)|}{|C_{GL_n(\mathbb{F}_p)}(D_\pi)|}$$

where $C_{GL_n(\mathbb{F}_p)}(D_\pi) = \{P \in GL_n(\mathbb{F}_p) \mid PD_\pi = D_\pi P\}$ is the centralizer of D_π in $GL_n(\mathbb{F}_p)$.

Let's compute the centralizer of D_π . A matrix $P \in M_n(\mathbb{F}_p)$, written as a $k \times k$ block matrix (P_{ij}) with blocks of size $d \times d$, commutes with D_π if and only if $P_{ij}C_\pi = C_\pi P_{ij}$ for all $i, j \in \{1, \dots, k\}$. The centralizer of a companion matrix C_π of an irreducible polynomial π is the ring of polynomials in C_π , denoted $\mathbb{F}_p[C_\pi]$. Since π is irreducible of degree d , this ring is a field isomorphic to \mathbb{F}_{p^d} . Thus, the centralizer of D_π in $M_n(\mathbb{F}_p)$, denoted $C_{M_n(\mathbb{F}_p)}(D_\pi)$, consists of block matrices where each block P_{ij} is in $\mathbb{F}_p[C_\pi]$. This ring is isomorphic to the matrix ring $M_k(\mathbb{F}_p[C_\pi])$, and thus to $M_k(\mathbb{F}_{p^d})$. The centralizer in $GL_n(\mathbb{F}_p)$ is the group of invertible matrices in this ring, which is isomorphic to $GL_k(\mathbb{F}_{p^d})$. Therefore, $|C_{GL_n(\mathbb{F}_p)}(D_\pi)| = |GL_k(\mathbb{F}_{p^d})|$, where $k = n/d$.

Finally, we have found that for a given irreducible polynomial π of degree $d|n$:

$$|\mathcal{A}_\pi| = \frac{|GL_n(\mathbb{F}_p)|}{|GL_{n/d}(\mathbb{F}_{p^d})|}$$

To conclude, the total number of irreducible matrices in $M_n(\mathbb{F}_p)$ is the sum of $|\mathcal{A}_\pi|$ over all possible irreducible polynomials π :

$$I(n, p) = \sum_{d|n} \sum_{\substack{\pi \text{ irreducible} \\ \deg(\pi)=d}} |\mathcal{A}_\pi| = \sum_{d|n} N_d(p) \cdot \frac{|GL_n(\mathbb{F}_p)|}{|GL_{n/d}(\mathbb{F}_{p^d})|}.$$

with

$$N_d(p) = \frac{1}{d} \sum_{k|d} \mu\left(\frac{d}{k}\right) p^k \quad \text{and} \quad |GL_m(\mathbb{F}_q)| = \prod_{i=0}^{m-1} (q^m - q^i)$$

This gives a complete, albeit complex, formula for $I(n, p)$. We compute this for small values of n and p .

Table 2: Counts and Probabilities of Irreducible Matrices				
(n,p)	$I(n, p)$	Total Matrices (p^{n^2})	$P(\text{irreducible})$	$P(\text{reducible})$
(2,2)	4	16	0.2500	0.7500
(2,3)	21	81	0.2593	0.7407
(3,2)	50	512	0.0977	0.9023
(3,3)	3459	19683	0.1757	0.8243

Hence, the probability that a matrix has a reducible minimal polynomial is $1 - I(n, p)/p^{n^2}$, which is given in the following table for small n, p :

Table 3: Probability of a Reducible Minimal Polynomial

$p \setminus n$	2	3	4
2	0.7500	0.9023	0.9367
3	0.7407	0.8243	0.8729
5	0.6720	0.7542	0.8171

Asymptotic Comment. We analyze the behavior of the probability

$$P(n, p) = \frac{I(n, p)}{p^{n^2}}$$

that a random matrix in $M_n(\mathbb{F}_p)$ has an irreducible minimal polynomial. We have:

$$P(n, p) = \sum_{d|n} \frac{1}{p^{n^2}} \cdot N_d(p) \cdot \frac{|\mathrm{GL}_n(\mathbb{F}_p)|}{|\mathrm{GL}_{n/d}(\mathbb{F}_{p^d})|}$$

where

$$N_d(p) = \frac{1}{d} \sum_{k|d} \mu\left(\frac{d}{k}\right) p^k \quad \text{and} \quad |\mathrm{GL}_m(\mathbb{F}_q)| = \prod_{i=0}^{m-1} (q^m - q^i).$$

Fix n . This is a finite sum over the divisors $d \mid n$, and we can analyze each term asymptotically. For such a divisor d , as $p \rightarrow \infty$, we have:

$$N_d(p) = \frac{p^d}{d} + \mathcal{O}(p^{d/2}),$$

and

$$\frac{|\mathrm{GL}_n(\mathbb{F}_p)|}{|\mathrm{GL}_{n/d}(\mathbb{F}_{p^d})|} = \frac{p^{n^2(1+o(1))}}{p^{n^2/d(1+o(1))}} = p^{n^2(1-\frac{1}{d})}(1+o(1)).$$

So the term corresponding to d in $P(n, p)$ behaves as

$$\frac{p^d}{d} \cdot p^{n^2(1-\frac{1}{d})} \cdot p^{-n^2}(1+o(1)) = \frac{1}{d} p^{d-\frac{n^2}{d}}(1+o(1)).$$

This tends to 0 as $p \rightarrow \infty$ if $d < n$, and to $\frac{1}{n}$ if $d = n$. Hence,

$$P(n, p) \longrightarrow \frac{1}{n} \quad \text{as } p \rightarrow \infty.$$

Moreover, based on initial values from a table, it appears that $P(n, p)$ increases with p . Therefore, we may conjecture that for all n and p ,

$$P(n, p) \leq \frac{1}{n} \leq \frac{1}{2}.$$

References

- [1] J. E. Cremona and D. Rusin. “Efficient solution of rational conics”. In: *Mathematics of Computation* 72.243 (2003), pp. 1417–1441.
- [2] Alexander J. Diesl, Samuel J. Dittmer, and Pace P. Nielsen. “Idempotent lifting and ring extensions”. In: *Proceedings of the American Mathematical Society* 143.9 (2015), pp. 3807–3811. DOI: [10.1090/S0002-9939-2015-12543-9](https://doi.org/10.1090/S0002-9939-2015-12543-9).
- [3] W. Eberly and M. Giesbrecht. “Efficient decomposition of associative algebras”. In: *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation (ISSAC’96)*. Ed. by Y. N. Lakshman. New York: ACM, 1996, pp. 170–178.
- [4] Wayne Eberly. “Computations for Algebras and Group Representations”. <http://www.cpsc.ucalgary.ca/~eberly/Research/Papers/phdthesis.pdf>. PhD thesis. University of Toronto, 1989.
- [5] Philippe Gille and Tamás Szamuely. *Central Simple Algebras and Galois Cohomology*. Vol. 101. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006. ISBN: 978-0-521-86103-8. DOI: [10.1017/CB09780511607219](https://doi.org/10.1017/CB09780511607219).
- [6] Gábor Ivanyos, Ádám D. Lekes, and Lajos Rónyai. *Improved algorithms for splitting full matrix algebras*. 2012. arXiv: [1211.1356](https://arxiv.org/abs/1211.1356) [math.RA]. URL: <https://arxiv.org/abs/1211.1356>.
- [7] Gábor Ivanyos and Lajos Rónyai. “Finding maximal orders in semisimple algebras over \mathbb{Q} ”. In: *Computational Complexity* 3 (1993), pp. 245–261. DOI: [10.1007/BF01271370](https://doi.org/10.1007/BF01271370). URL: <https://link.springer.com/article/10.1007/BF01271370>.
- [8] Gábor Ivanyos and Ágnes Szántó. “Lattice basis reduction for indefinite forms and an application”. In: *Discrete Mathematics* 153.1-3 (1996). Proceedings of the 5th Conference on Formal Power Series and Algebraic Combinatorics (Florence, 1993), pp. 177–188.
- [9] Jana Pílníková. “Trivializing a central simple algebra of degree 4 over the rational numbers”. In: *Journal of Symbolic Computation* 42.6 (2007), pp. 579–586. ISSN: 0747-7171.
- [10] Lajos Rónyai. “Computing the structure of finite algebras”. In: *Journal of Symbolic Computation* 9.3 (1990), pp. 355–373. DOI: [10.1016/S0747-7171\(08\)80072-7](https://doi.org/10.1016/S0747-7171(08)80072-7).

- [11] Denis Simon. “Solving norm equations in relative number fields using S -units”. In: *Mathematics of Computation* 71.239 (2002), pp. 1301–1321. ISSN: 0025-5718. DOI: [10.1090/S0025-5718-02-01309-1](https://doi.org/10.1090/S0025-5718-02-01309-1). URL: <https://www.ams.org/journals/mcom/2002-71-239/S0025-5718-02-01309-1/S0025-5718-02-01309-1.pdf>.
- [12] Denis Simon. “Solving quadratic equations using reduced unimodular quadratic forms”. In: *Mathematics of Computation* 74.251 (2005), pp. 1531–1543.
- [13] John Voight. *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*. 2012. arXiv: [1004.0994](https://arxiv.org/abs/1004.0994) [math.NT]. URL: <https://arxiv.org/abs/1004.0994>.
- [14] John Voight. *Quaternion Algebras*. Vol. 288. Graduate Texts in Mathematics. Cham: Springer, 2021. ISBN: 978-3-030-56692-0. DOI: [10.1007/978-3-030-56694-4](https://doi.org/10.1007/978-3-030-56694-4). URL: <https://link.springer.com/book/10.1007/978-3-030-56694-4>.