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 3, 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 la Section 3, 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

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

Quaternion Algebras. Quaternion algebras are central simple algebras of dimension 4. When $\mathrm{char}(F) \neq 2$, 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 $ij = -ji$. We denote such an algebra by $\left(\frac{a,b}{F}\right)$. See [12]. Quaternion algebras are closely related to ternary quadratic forms over F, a fact which underpins many computational methods.

Isomorphism of Quaternion Algebras: Statement of the Problem. The central computational task of this report is to solve the following problem.

> `Explicit Isomorphism of Quaternion Algebras`
>
> Let $A = \left(\frac{a,b}{\mathbb{Q}}\right)$ and $B = \left(\frac{c,d}{\mathbb{Q}}\right)$ be two quaternion algebras over $\mathbb{Q}$. Given that A and B are isomorphic as $\mathbb{Q}$-algebras, compute an explicit isomorphism $f : A \to B$. This means expressing the images of the basis elements of A under f in terms of the basis of B.

Motivation from Elliptic Curve Theory. Section 3 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 $\mathrm{End}(E)$ 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 $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ has the structure of a quaternion algebra over $\mathbb{Q}$.

Methods of this Report. Let $A = \left(\frac{a,b}{\mathbb{Q}}\right)$ and $B = \left(\frac{c,d}{\mathbb{Q}}\right)$ be two quaternion algebras over $\mathbb{Q}$ that are assumed to be isomorphic. We investigate two main approaches to compute an explicit isomorphism $f : A \to B$.

The first method, a natural and direct approach, is to determine the algebraic conditions that the images of the basis elements of A must satisfy in B. This leads to a system of equations. We will see that this problem can always be reduced to

solving several equations of the type $aX^2 + bY^2 + cZ^2 = 0$ over $\mathbb{Q}$ or a number field. This equation defines a (diagonal) ternary quadratic form. Fortunately, solving such equations is a classical problem, and efficient algorithms exist. We discuss the literature on this topic in more detail in subsection 4.1.

The second method is more conceptual and relies on the structure theory of central simple algebras. A key theorem states that $A \cong B$ if and only if the tensor product algebra $A \otimes_{\mathbb{Q}} B^{\mathrm{op}}$ is a matrix algebra, specifically $A \otimes_{\mathbb{Q}} B^{\mathrm{op}} \cong \mathrm{M}4\mathbb{Q}$. Letting $C = A \otimes_{\mathbb{Q}} B^{\mathrm{op}}$, we can compute its structure constants for a basis $e_1, \ldots, e_{16}$ where $e_i e_j = \sum_k c_{ijk} e_k$. The problem is thus reduced to the following more general, and well-studied, problem.

Explicit Isomorphism Problem
Given a $\mathbb{Q}$-algebra C by its structure constants, which is known to be isomorphic to $\mathrm{M}_n(\mathbb{Q})$, compute an explicit isomorphism from C to $\mathrm{M}_n(\mathbb{Q})$.

In the literature, the main strategy to solve this is to find special elements in C, such as zero divisors or rank-one elements (whose rank is independent of the choice of isomorphism to $\mathrm{M}_n(\mathbb{Q})$). A significant advantage of this method is its connection to the arithmetic of the algebras. Given maximal orders in A and B, one can deduce a maximal order in C with minimal computation. The knowledge of such an order can then be leveraged to find the required special elements in C more efficiently.

Contents. Section 2 defines quaternion algebras and states their basic properties, including different definitions, the standard involution, and the correspondence with ternary quadratic forms. Section 3 provides the motivation for computing isomorphisms of quaternion algebras from the theory of elliptic curves. Section 4 details the first method, which relies on solving ternary quadratic forms. Section 5 presents the reduction for the second main approach: reducing the problem to finding an isomorphism $A \otimes B^{\mathrm{op}} \cong \mathrm{M}4\mathbb{Q}$. Section 6 tackles the problem of splitting a matrix ring by reducing it to finding special elements within the algebra, suggesting the use of orders, and summarizing the literature. Section 7 covers the necessary preliminaries about orders in central simple algebras, concluding with an algorithm to compute a maximal order, particularly for an algebra isomorphic to $\mathrm{M}n\mathbb{Q}$. Section 8 describes a method to find zero divisors in a matrix algebra by reduction to a finite field and then lifting the result, a potentially heuristic process. Appendix A provides foundational material on central simple algebras. Appendix B gives more precise algorithms and implementation details. Appendix C presents a formula for the number of matrices in $\mathrm{M}n\mathbb{F}_p$ with an irreducible minimal polynomial, used to justify certain randomized algorithms.

Implementation. An implementation of most of the algorithms presented in this report, and more, is available on GitHub:

`https://github.com/TommyChakroun/quat_alg_project`

In particular, we provide functions to: compute an isomorphism by solving ternary quadratic forms; compute a maximal order in a central simple algebra over $\mathbb{Q}$; deduce an isomorphism from an explicit isomorphism $A \otimes B^{\mathrm{op}} \to \mathrm{M4}\mathbb{Q}$; and attempt to compute rank-one elements in an algebra isomorphic to $\mathrm{M4}\mathbb{Q}$.

2. 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 $\mathrm{M}_2(F) \simeq \left(\frac{1,1}{F}\right)$ 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:

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

The conjugation on B enjoys the following properties:

- Transition to the next section...

Standard involution.

Definition 2.1. Let F be a field and B be an F-algebra. An *involution* on B is an F-linear map $\overline{\ } : B \to B$ such that $\overline{1} = 1$ and for all $x, y \in B$, $\overline{\overline{x}} = x$ and $\overline{xy} = \overline{yx}$. An involution is *standard* if for all $x \in B$, $x\overline{x} \in F$.

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

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

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

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

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

Lemma 2.2. *An involution over a finite-dimensional algebra B is standard if and only if there exists a basis $e_1, \ldots, e_n$ of B such that for all $1 \leq i, j \leq n$, we have $e_i\overline{e_i} \in F$ and $(e_i + e_j)\overline{(e_i + e_j)} \in F$.*

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

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

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:

$$T^2 - \mathrm{trd}(x)T + \mathrm{nrd}(x).$$

In particular, if B has a standard involution and $e_1, \ldots, e_n$ is a basis of B with $e_1 = 1$, then for $i \geq 2$, the coefficient of e_i in e_i^2 is $\mathrm{trd}(e_i)$.

Algorithm 1: Has Standard Involution

Input: A finite-dimensional algebra B over a field F with a basis $e_1 = 1, e_2, \ldots, e_n$

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 $\overline{\xi} := t(\xi) - \xi$.

If $\overline{e_ie_j} \neq \overline{e_je_i}$ for some $2 \leq i, j \leq n$, return False.

If $n_i := e_i\overline{e_i}$ or $n_{ij} := (e_i + e_j)(\overline{e_i} + \overline{e_j})$ 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. □

Quadratic forms.

Theorem 2.3. *Let F be a field of characteristic not 2. Then the map*

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

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 $f : B \to C$. The standard involution s is preserved, so $f(B^0) = C^0$, and f induces an F-linear isomorphism $u : F^3 \to F^3$ 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:

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

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... □

Local-Global Principle. See appendix on Hasse-Minkowski theorem.

Theorem 2.4 (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

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

which is a finite set of even cardinality.

Hilbert symbol over $\mathbb{Q}_p$.

Application to the problem `IdentifyMatrixwRing`.

3. Interlude: Motivation from Elliptic Curve Theory

Short definition of elliptic curve.
Short definition of the endomorphism ring $\mathrm{End}(E)$.
Short definition and existence of the dual endomorphism map $\mathrm{End}(E) \to \mathrm{End}(E), \alpha \mapsto \hat{\alpha}$
Implication that $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ 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 $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is well an quaternion algebra over $\mathbb{Q}$
If E is super singular over $\mathbb{F}_p$ and ..., $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is exactly $B_{p,\infty}$.
Computational problem believed to be hard.

4. Isomorphism via Ternary Quadratic Forms

In this section, we present what is perhaps the most natural approach to compute an explicit isomorphism between two quaternion algebras $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ and $B = \left(\frac{a,b}{\mathbb{Q}}\right)$.

Basically, if $f : A \to B$ is such an isomorphism, then $\mu = f(i)$ must be a pure quaternion in B such that $\mu^2 = \alpha$. Our first task is to find such an element μ. We will use a standard technique that reduces this problem to solving an equation over a quadratic extension of $\mathbb{Q}$. After finding μ, we can easily find a pure quaternion $\nu \in B$ that anticommutes with μ (i.e., $\nu\mu = -\mu\nu$) and whose square is a non-zero element of $\mathbb{Q}$, say $\nu^2 = \gamma$.

It follows that $\{1, \mu, \nu, \mu\nu\}$ is a basis for B such that $\mu^2 = \alpha$ and $\nu^2 = \gamma$. However, we may have $\gamma \neq \beta$. To conclude, we modify this basis by taking a new element $\nu' = (x + y\mu)\nu$ for some $x, y \in \mathbb{Q}$, such that $(\nu')^2 = \beta$. This is equivalent to solving a norm equation of the form $x^2 - \alpha y^2 = \beta/\gamma$.

We will treat the case where A and B are split separately. In this scenario, the problem reduces to finding a zero divisor in each algebra, which only requires solving a ternary quadratic form over $\mathbb{Q}$ and is therefore more efficient.

This section is organized as follows. We begin with an overview of the computational theory for solving ternary quadratic forms. We then present the algorithm for the split case before finishing with the general case for non-split algebras.

4.1. Ternary Quadratic Forms. By solving a ternary quadratic form over a field K, we refer to finding a non-trivial solution to an equation of the form

$$aX^2 + bY^2 + cZ^2 = 0,$$

where $a, b, c \in K^\times$ are coefficients and the unknowns are $X, Y, Z \in K$.

The problem of solving such equations is well-studied in computational number theory. We will only need the case where K is $\mathbb{Q}$ or a quadratic number field. Over $\mathbb{Q}$, efficient algorithms exist see, e.g., . When K is a number field, the strategy typically involves several reduction steps, eventually culminating in solving a norm equation. For a comprehensive treatment, one may consult the Magma Handbook .

4.2. Isomorphism between Split Quaternion Algebras. Let $A = \left(\frac{a,b}{\mathbb{Q}}\right)$ be a quaternion algebra over $\mathbb{Q}$. The following are equivalent:

- A is split, i.e., isomorphic to $\mathrm{M}_2(\mathbb{Q})$.

- There exists a non-zero pure quaternion $e \in A$ such that $e^2 = 0$.
- The ternary quadratic form $aX^2 + bY^2 - abZ^2 = 0$ has a non-trivial rational solution.

Moreover, these equivalences are effective: given a solution to the quadratic form, one can efficiently construct an explicit isomorphism. The equivalence between (2) and (3) is clear: if $e = Xi + Yj + Zk$ is a pure quaternion, then its square is $e^2 = aX^2 + bY^2 - abZ^2$. If $\phi : \mathrm{M}_2(\mathbb{Q}) \to A$ is an isomorphism, the image of a non-zero nilpotent matrix is a pure quaternion $e \in A$ with $e^2 = 0$. Conversely, if such an e exists, $V = Ae$ is a two-dimensional right ideal of A. The map from A to $\mathrm{End}_{\mathbb{Q}}(V)$ given by left multiplication is an isomorphism, and choosing a basis for V yields an explicit isomorphism $A \cong \mathrm{M}_2(\mathbb{Q})$.

This yields the following algorithm.

Algorithm 2: Isomorphism from a split algebra to $\mathrm{M}_2(\mathbb{Q})$

Input: A split quaternion algebra $A = \left(\frac{a,b}{\mathbb{Q}}\right)$.
Output: An isomorphism $f : A \to \mathrm{M}_2(\mathbb{Q})$.

1. Find a non-trivial solution (X, Y, Z) to $aX^2 + bY^2 - abZ^2 = 0$;
2. Define the non-zero element $e = Xi + Yj + Zk \in A$. Note that $e^2 = 0$;
3. Find an element $v \in A$ such that $ev \neq 0$. For instance, choose v from $\{i, j\}$;
4. Let the set $\mathcal{B} = \{ev, e(ev)\}$ be the basis for the right ideal Ae;
5. Construct the isomorphism $f : A \to \mathrm{M}_2(\mathbb{Q})$ by mapping an element $u \in A$ to the matrix representing left multiplication by u with respect to the basis $\mathcal{B}$;

The only computationally difficult step is the first one.

4.3. Isomorphism between Quaternion Algebras. Let $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ and $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ be two isomorphic, non-split quaternion algebras over $\mathbb{Q}$.

First, we want to find an element $\mu \in B$ such that $\mu^2 = \alpha$. Since α is not a square in $\mathbb{Q}$, μ must be a pure quaternion. Writing $\mu = Xi + Yj + Zk$ requires solving $aX^2 + bY^2 - abZ^2 = \alpha$, an inhomogeneous equation that is difficult to solve directly.

Instead, we use the following technique. Let $K = \mathbb{Q}(\sqrt{\alpha})$. Since $A \cong B$, their extensions of scalars A_K and B_K are also isomorphic. The algebra A_K is split, so $B_K = \left(\frac{a,b}{K}\right)$ must also be split. This implies that the norm form on B_K is isotropic, which means we can find a non-trivial solution to $U^2 - aV^2 - bW^2 = 0$ with $U, V, W \in K$. We can be sure that $W \neq 0$, otherwise a would be a square in K. Scaling the solution, we can assume $W = 1$. Thus, we find $U, V \in K$ such that $U^2 - aV^2 = b$.

This means the element $\zeta = U + Vi + j \in B_K$ has reduced norm $\mathrm{nrd}(\zeta) =$

$U^2 - aV^2 - b = 0$. Now, write $U = u_1 + u_2\sqrt{\alpha}$ and $V = v_1 + v_2\sqrt{\alpha}$ for $u_i, v_i \in \mathbb{Q}$. We can express ζ as $\zeta_1 + \zeta_2\sqrt{\alpha}$, where $\zeta_1 = u_1 + v_1 i + j$ and $\zeta_2 = u_2 + v_2 i$ are elements of B. The element ζ_2 must be invertible; otherwise, $U, V \in \mathbb{Q}$, which would imply B is split, a contradiction. The condition $\mathrm{nrd}(\zeta) = 0$ implies $\mathrm{nrd}(\zeta_1\zeta_2^{-1} + \sqrt{\alpha}) = 0$.

Let $\mu = \zeta_1\zeta_2^{-1}$. One can check that μ is a pure quaternion, and the norm condition becomes $\mathrm{nrd}(\mu) + \alpha = 0$, which simplifies to $-\mu^2 + \alpha = 0$. Thus, $\mu^2 = \alpha$, as desired.

Next, we find a pure quaternion $\nu \in B$ that is orthogonal to μ (i.e., $\mu\nu = -\nu\mu$). This amounts to solving a system of linear equations for the coefficients of ν. Let $\nu^2 = \gamma$.

So far, we have a basis $\{1, \mu, \nu, \mu\nu\}$ for B with $\mu^2 = \alpha$ and $\nu^2 = \gamma$. Since $A \cong B$, we must have that β/γ is a norm from the extension $K/\mathbb{Q}$. We can therefore find $x, y \in \mathbb{Q}$ by solving the norm equation $X^2 - \alpha Y^2 = \beta/\gamma$. Since α is not a square, this is equivalent to finding a rational point on the conic $X^2 - \alpha Y^2 - (\beta/\gamma)Z^2 = 0$. Any non-trivial solution will have $Z \neq 0$, and we can scale it to get a solution with $Z = 1$.

Finally, we define $\nu' = (x + y\mu)\nu$. This new element ν' still anticommutes with μ, and its square is $(\nu')^2 = (x + y\mu)\nu(x + y\mu)\nu = (x + y\mu)(x - y\mu)\nu^2 = (x^2 - \alpha y^2)\gamma = (\beta/\gamma)\gamma = \beta$. The isomorphism $f : A \to B$ is then given by $f(i) = \mu$ and $f(j) = \nu'$.

5. Isomorphism via Splitting Matrix Algebra

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

`GeneralExplicitIsomorphismProblem`: Given two isomorphic central simple algebras A and B, compute an isomorphism $f : A \to B$.

Lemma 5.1. *Let A be a central simple algebra of dimension N. There exists an isomorphism $\varphi : A \otimes A^{op} \to \mathrm{End}_{\mathbb{Q}}(A)$ such that for all $a, b \in A$, $\varphi(a \otimes b)$ is $A \to A; z \mapsto azb$. Consequently, $A \otimes A^{op}$ is isomorphic to $\mathrm{M}_N(\mathbb{Q})$.*

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

Proposition 5.2. *Let A, B be two central simple algebras of dimension N. Then A and B are isomorphic if and only if $A \otimes B^{op}$ is isomorphic to $\mathrm{M}_N(F)$.*

6. Splitting a Matrix Algebra

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 $\mathrm{M}_4(\mathbb{Q})$. 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 $\mathrm{M}_n(F)$, compute an explicit isomorphism $\varphi : A \to \mathrm{M}_n(F)$.

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 $\mathbb{Q}$.

6.1. 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 $a_1, \ldots, a_N$ and *structure constants* $(c_{i,j,k})_{1 \leq i,j,k \leq N}$. That is,

$$A = Fa_1 \oplus \cdots \oplus Fa_N \quad \text{and} \quad a_i a_j = \sum_{k=1}^{N} c_{i,j,k} a_k \quad (1 \leq i, j \leq N)$$

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

Assume that A is isomorphic to $\mathrm{M}_n(F)$ as an F-algebra. We want to compute an explicit isomorphism $\varphi : A \to \mathrm{M}_n(F)$, that is, to output a list of $N = n^2$ matrices with entries in F: $M_1, \ldots, M_N$ such that the unique F-linear map from A to $\mathrm{M}_n(F)$ 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 $\mathrm{M}_n(F)$. 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 $\varphi : A \to \mathrm{M}_n(F)$, we have

$$n \cdot \mathrm{rank}(\varphi(x)) = \dim_F(\mathrm{M}_n(F)\varphi(x)) = \dim_F(\varphi(Ax)) = \dim_F(Ax).$$

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

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

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 $\mathrm{M}_n(F)$ is equivalent to finding a rank-one element in A. Indeed, if we know $\varphi : A \to \mathrm{M}_n(F)$, we just have to express a rank-one matrix, for example, the matrix $S \in \mathrm{M}_n(F)$ with only 1 in the first row and 0 on other lines, in the basis $\varphi(a_1), \ldots, \varphi(a_N)$: $S = \lambda_1\varphi(a_1) + \cdots + \lambda_N\varphi(a_N)$; then $x := \lambda_1 a_1 + \cdots + \lambda_N a_N$ 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 $\varphi : A \to \mathrm{End}_F(Ax), a \mapsto (z \mapsto az)$ 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 $Ax \to Ax, z \mapsto a_i z$ 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 $\mathrm{M}_k(F)$ 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 $\varphi : A \to \mathrm{M}_n(F)$, $X := \varphi(x)$ has rank r, so there exist P, Q invertible matrices such that $X = PJ_rQ$, where

$$J_r := \mathrm{diag}(1, \ldots, 1, 0, \ldots, 0).$$

We see that $XZX = X$ has a solution $Z \in \mathrm{M}_n(F)$, namely $Z = Q^{-1}J_rP^{-1}$. 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 $B \cong \mathrm{M}_r(F)$: to show this, again we use our isomorphism φ. Let $E := \varphi(e) \in \mathrm{M}_n(F)$. E satisfies $E^2 = E$ and has rank $r < n$. By linear algebra, there exists an invertible matrix P such that $E = PJ_rP^{-1}$. Then as F-algebras, we have the isomorphisms $B \cong E\mathrm{M}_n(F)E \cong PJ_rP^{-1}\mathrm{M}_n(F)PJ_rP^{-1} \cong J_r\mathrm{M}_n(F)J_r \cong \mathrm{M}_r(F)$. 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 $\mathrm{M}_r(F)$, we see that $\mathrm{rank}_A(y) = \mathrm{rank}_B(y) = 1$.

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 $e^2 = e$.

6.2. The case $\mathrm{M}_4(\mathbb{Q})$. To solve the explicit isomorphism problem in $\mathrm{M}_4(\mathbb{Q})$, we only need to be able to find a zero divisor in $\mathrm{M}_4(\mathbb{Q})$ and $\mathrm{M}_2(\mathbb{Q})$. Indeed, if $A \cong \mathrm{M}_4(\mathbb{Q})$ 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 $\mathrm{M}_2(\mathbb{Q})$, 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 $A \cong \mathrm{M}_2(\mathbb{Q})$ 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: [11, Theorem 7.19], algorithm: [1, Algorithm I], [8, Theorem 3], [10, Algorithm 3.4].

7. Orders in Central Simple Algebras

7.1. 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 [12], 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 $\Lambda = Re_1 \oplus \cdots \oplus Re_N$.
- 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 7.1. 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 7.2. *If Λ is an R-order in B, then for all $\alpha \in \Lambda$, α is integral over R; hence* $\mathrm{trd}(\alpha) \in R$.

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

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

is represented by some matrix $M \in \mathrm{M}_m(R)$ 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. □

Definition 7.3. 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

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

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

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

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 7.4. *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 $a_1, \ldots, a_N \in B$ 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. □

7.2. 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 7.5. Let $\Lambda = Re_1 \oplus \cdots \oplus Re_N$ be an R-order in B. The *discriminant* of Λ is defined as

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

Since for all $1 \le i, j \le N$, the element $e_i e_j$ lies in Λ, its reduced trace lies in R by Proposition 7.2. Hence, d_Λ is indeed an element of R, and it is nonzero since the bilinear form $(x, y) \mapsto \operatorname{trd}(xy)$ is non-degenerate by Proposition A.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 $M \in \mathrm{M}_N(F)$ be the matrix expressing the e_k in terms of the f_i, that is,

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

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

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

In matrix form, this reads

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

and hence,

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

We deduce all the desired properties from this relation:

- If $\Lambda = \Gamma$, then M is invertible over $\mathrm{M}_N(R)$, 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 $\mathrm{M}_N(R)$. 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

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

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 $(x, y) \mapsto \mathrm{trd}(xy)$ 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 $B \cong \mathrm{M}_n(F)$—is justified by the following normalization:

Theorem 7.6. *Let Λ be an R-order in B. If d_Λ is a unit in R (i.e., $\mathrm{disc}(\Lambda) = R$), then Λ is a maximal R-order. If $B \cong \mathrm{M}_n(F)$ for some integer n, then the converse is also true.*

Proof. The direct implication is immediate.
Conversely, suppose $B \cong \mathrm{M}_n(F)$. Then the converse is more subtle and will require further work... □

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 $\mathrm{M}_4(\mathbb{Q})$.

7.3. 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 $\mathcal{A}_p$:

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

Let

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

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 7.7 (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 7.6 implies that $d_\Lambda \in \mathbb{Z}$ is not a unit and hence divisible by some prime p. ... □

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 3: 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 $d_\Lambda = d(e_1, \ldots, e_N) \in \mathbb{Z}$. 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 $\Lambda \to \mathcal{A}$.
3. Compute a $\mathbb{F}_p$-basis of $\mathrm{Rad}(\mathcal{A})$.
4. Compute the $\mathbb{F}_p$-algebra $\mathcal{C} = \mathcal{A}/\mathrm{Rad}(\mathcal{A})$ and the projection $\phi : \mathcal{A} \to \mathcal{C}$.
5. Compute the total projection $\Phi : \Lambda \to \mathcal{C}$.
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 $\mathcal{C} \to \mathcal{C}/\mathcal{K}$.
10. Compute the total projection $\Phi_\mathcal{K} : \Lambda \to \mathcal{C}/\mathcal{K}$.
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 $O_L(\mathcal{I}_r)$ *strictly contains* Λ **then**

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

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 [9, 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 $M \in \mathrm{M}_{r,N}(\mathbb{Z})$ 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 $(e_1, \ldots, e_r)$ 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 $(e_1, \ldots, e_r)$ 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].

8. Algorithms for Finding Zero Divisors

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

In $\mathrm{M}_n(\mathbb{F}_p)$ Let p be a prime. We consider the ring $\mathrm{M}_n(\mathbb{F}_p)$, equipped with the uniform probability distribution. Let M be a random variable uniformly distributed in $\mathrm{M}_n(\mathbb{F}_p)$. 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 $p \to \infty$. 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 C, we give an exact formula for the probability that a uniformly chosen matrix in $\mathrm{M}_n(\mathbb{F}_p)$ has a reducible minimal polynomial. In particular, we show that

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

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:

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

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 $\mathrm{M}_n(\mathbb{F}_p)$ with a reducible minimal polynomial. Consequently, the explicit isomorphism problem is relatively easy in $\mathrm{M}_n(\mathbb{F}_p)$.

In $\mathrm{M}_n(\mathbb{R})$ In $\mathrm{M}_n(\mathbb{R})$, 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 $\mathrm{M}_n(\mathbb{R})$.

In $\mathrm{M}_n(\mathbb{Q})$ In $\mathrm{M}_n(\mathbb{Q})$, 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 $\mathrm{M}_n(\mathbb{Q})$ can't be efficiently solved by randomly picking elements.

8.2. Heuristic Lifting of Idempotents over $\mathbb{Q}$. Let A be a finite-dimensional $\mathbb{Q}$-algebra of dimension $N = n^2$ assumed to be isomorphic to $\mathrm{M}_4(\mathbb{Q})$. Since we know how to compute a $\mathbb{Z}$-basis of a maximal order in A, we can view

$$A = \mathbb{Q}a_1 \oplus \cdots \oplus \mathbb{Q}a_N \cong \mathrm{M}_4(\mathbb{Q})$$

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 $\mathrm{M}_n(\mathbb{Z})$) 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 $a_1, \ldots, a_N$ 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 6.1, 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 $b = r_1 a_1 + \cdots + r_N a_N$ 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 $f = x_1 a_1 + \cdots + x_N a_N$ 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 $e := \tilde{x_1}a_1 + \cdots + \tilde{x_N}a_N \in A$ satisfies that $e^2 - e$ has small rational coefficients in the basis $a_1, \ldots, a_N$.

With $K = \mathbb{F}_p$. In $O_{\mathbb{F}_p} := \mathbb{F}_p a_1 \oplus \cdots \oplus \mathbb{F}_p a_N$, we can easily, by using randomization, build $f \in O_{\mathbb{F}_p}$, a non-trivial idempotent. By writing $f = x_1 a_1 + \cdots + x_N a_N$ 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 $e := y_1 a_1 + \cdots + y_N a_N \in O \subset A$ satisfies $e^2 - e \equiv 0 \pmod{p}$, i.e., $e^2 - e$ has integer coefficients divisible by p in the basis $a_1, \ldots, a_N$.

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 $a_1, \ldots, a_N$, 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.

A. 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 $B \to R$ is injective. Now we define an important class of algebras.

Definition A.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 $B = \mathrm{M}_n(F)$, 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 A.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 $\mathrm{M}_n(D)$. 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:

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

This is a sub-F-algebra of $\mathrm{End}_F(I)$, and we claim that it is a division algebra. Indeed, if $f : I \to I$ 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 $\mathrm{im}(f) \neq \{0\}$. By the minimality of I, we must have $\ker(f) = \{0\}$ and $\mathrm{im}(f) = I$. Therefore, f is an isomorphism and thus has an inverse in D.

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

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

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

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

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

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., $\Phi(1) = \mathrm{id}_I$), 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 $f \in \mathrm{End}_D(I)$. We have:

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

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

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

$$\mathrm{End}_D(I) \cong \mathrm{End}_D(D^n) \cong \mathrm{M}_n(D^{op}) \cong \mathrm{M}_n(D)$$

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

It follows that if K is an algebraically closed field, then every central simple algebra over K is isomorphic to some matrix algebra $\mathrm{M}_n(K)$. 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 A.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. □

Proposition A.4. *Let B be a finite dimensional algebra over F. Then there exists a field extension K/F such that $B \otimes_F K \cong \mathrm{M}_n(K)$ as a 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. □

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 $B \otimes_F K \cong \mathrm{M}_n(K)$. Hence, we can embed B into $\mathrm{M}_n(K)$ via

$$\varphi : B \to \mathrm{M}_n(K), \quad b \mapsto b \otimes 1.$$

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

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

Proposition A.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*

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

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

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

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

Lemma A.6 (Skolem-Noether Theorem for matrix rings)**.** *Let K be a field. Every K-algebra automorphism of $\mathrm{M}_n(K)$ is inner, that is, of the form $M \mapsto PMP^{-1}$ for some $P \in \mathrm{GL}_n(K)$.*

Proof of Lemma A.6. Let $\phi : \mathrm{M}_n(K) \to \mathrm{M}_n(K)$ be a K-algebra automorphism. Let $I \subset \mathrm{M}_n(K)$ 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

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

For any $M \in \mathrm{M}_n(K)$ 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 $\mathrm{M}_n(K)$. Since $Pu_0 \neq 0$, the kernel is not all of K^n, and since the only ideals of $\mathrm{M}_n(K)$ are $\{0\}$ and $\mathrm{M}_n(K)$, the kernel must be zero. Hence, P is an isomorphism, and

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

□

Proof of Proposition A.5. The well-definedness follows directly from Lemma A.6. For any field K of characteristic 0 and any matrix $M \in \mathrm{M}_n(K)$, we have

$$\mathrm{trace}(M) = \frac{1}{n}\mathrm{trace}_F(\mathrm{M}_n(K) \to \mathrm{M}_n(K),\ Z \mapsto MZ).$$

Hence,

$$\mathrm{trd}(b) = \mathrm{trace}_F(\mathrm{M}_n(K) \to \mathrm{M}_n(K),\ Z \mapsto \varphi(b\otimes 1)Z) = \mathrm{trace}_F(B\otimes_F K \to B\otimes_F K,\ z \mapsto (b\otimes 1)z).$$

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

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

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

Hence,

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

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 $\mathrm{M}_n(K)$ 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 $K = F^{\mathrm{alg}}$ 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 $\mathrm{trd}(x) = \mathrm{trace}(A) \in F$, and R is integrally closed in F, it follows that $\mathrm{trd}(x) \in R$. This proves the third point. □

B. 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.

B.1. Reduction $\varphi : A \otimes_{\mathbb{Q}} B^{op} \to \mathrm{M}_4(\mathbb{Q})$ to $f : A \to B$. Let A, B be two central simple algebras of same dimension n. In Proposition 5.2 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 $\varphi : A \otimes_{\mathbb{Q}} B^{op} \to M_4(\mathbb{Q})$ 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:

$$\lambda_v : A \to V, \quad a \mapsto \varphi(a \otimes 1)v$$
$$\mu_v : B \to V, \quad b \mapsto \varphi(1 \otimes b)v.$$

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 $f : A \to B$, $a \mapsto \mu_v^{-1}(\lambda_v(a))$ 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 $f : A \to B$ an isomorphism and denote $\varphi_f : A \otimes_{\mathbb{Q}} B^{op} \to M_N(\mathbb{Q})$ the other isomorphism obtained. By Lemma A.6 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

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

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

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

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

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

$$\begin{pmatrix} M_1 v & \cdots & M_N v \end{pmatrix}.$$

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 $P_A(v_1, \ldots, v_N)$ for some $P_A \in \mathbb{Q}[T_1, \ldots, T_N]$.

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 $\mathrm{Card}(Z(P_A) \cap S^N) \leq N\,\mathrm{Card}(S)^{N-1}$.

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

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 $2N\,\mathrm{Card}(S)^{N-1} < \mathrm{Card}(S)^N$ this is possible. This concludes the proof and we deduce the following algorithm.

Algorithm 4: Isomorphism $f : A \to B$ from $\varphi : A \otimes B^{op} \to M_N(\mathbb{Q})$

Input: A, B two central simple algebras of dimension n and $\varphi : A \otimes B^{op} \to M_N(\mathbb{Q})$ 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: $f : A \to B$ an isomorphism

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

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

2. Compute U the matrix of $A \to V$, $a \mapsto \varphi(a \otimes 1)v$ in the basis of A and the canonical basis of V
3. Compute M the matrix of $B \to V$, $b \mapsto \varphi(1 \otimes b)v$ 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** *$f : A \to B$ given in the basis of A by:*

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

end

end

Complexity. Not evaluated yet.

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

Algorithm 5: ModularMatrixKernel

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

Output: $X_1, \ldots, X_k \in \mathbb{Z}^n$ 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: $U \in \mathrm{GL}_m(\mathbb{Z})$, $V \in \mathrm{GL}_n(\mathbb{Z})$ such that $UAV = D$ is in diagonal form
2. If $t = \min(n, m)$, let $Y_1, \ldots, Y_t$ be defined by $Y_i = (0, \ldots, 0, \frac{d}{\gcd(d, D_{i,i})}, 0, \ldots, 0)$
3. If $n > m$, complete with $Y_j = (0, \ldots, 0, 1, 0, \ldots, 0)$ for $t < j \leq n$
4. **return** $VY_1, \ldots, VY_k$

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

Complexity. Not evaluated yet.

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

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

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 $b_1, \ldots, b_N$ 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 $f_1, \ldots, f_N$ 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 $\alpha = s^{-1}(x_1e_1 + \cdots + x_Ne_N)$ with $x_i \in \mathbb{Z}$:

$$\alpha \in O_L(I) \iff \forall j, \alpha e_j \in I \iff \forall j, s^{-1}(x_1e_1e_j + \cdots + x_Ne_Ne_j) \in \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_N$$

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

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

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 $X = (x_1, \ldots, x_N) \in \mathbb{Z}^N$ 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 6: LeftOrder

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

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

1. Write $1_B = r_1 e_1 + \cdots + r_N e_N$ 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 $A = (d \cdot s \cdot c_{i,j,k})_{1 \le i \le N; 1 \le j,k \le N} \in M_{N^2,N}(\mathbb{Z})$
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* $f_i = \frac{1}{s}(X_{i,1}e_1 + \cdots + X_{i,N}e_N)$

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 ($\mathcal{O}(N^4)$). 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 B.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 $I = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_N$ 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.

B.4. Randomized Computation of Central 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 $n_1, \ldots, n_r$ and division algebras $D_1, \ldots, D_r$ over F such that

$$A \cong \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r).$$

Lemma B.2. *Consequently, A has exactly r minimal nonzero two-sided ideals $I_1, \ldots, I_r$, 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 $e_1, \ldots, e_r$ are central orthogonal idempotents, and e_i is the identity of I_i.*

Proof. Let us fix an isomorphism as above. The image of $\mathrm{M}_{n_i}(D_i)$ 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. □

Lemma B.3. *Conversely, if $e_1, \ldots, e_r$ 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 $e_1, \ldots, e_r$ 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 $e_1, \ldots, e_r$ of central orthogonal idempotents in Z.

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

$$\pi_a = \operatorname{lcm}(\pi_{a_1}, \ldots, \pi_{a_r}),$$

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

If $s \geq 2$, by the Chinese Remainder Theorem, there exist polynomials $h_1, \ldots, h_s$ 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:

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

which gives a central orthogonal idempotent.

If $s = r$, then the w_i are exactly the elementary idempotents $(0, \ldots, 0, 1, 0, \ldots, 0)$, 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 $\pi_a = \pi_1 \ldots \pi_s$, 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 7: CentralIdempotentsCommutativeSplit

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

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

foreach *a in Z* **do**

1. Compute the minimal polynomial $\pi_a \in \mathbb{F}_p[T]$ of a.
2. Factor $\pi_a = \pi_1 \ldots \pi_s$ in $\mathbb{F}_p[T]$.
3. **if** $s \geq 2$ **then**
   4. By the Chinese remainder theorem, compute $h_1, \ldots, h_s \in \mathbb{F}_p[T]$ 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 $i = 1, \ldots, s$.
   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** $i = 1, \ldots, s$ **do**
      10. Compute recursively $e_1, \ldots, e_k = \text{CentralIdempotentsCommutative}(A_i)$.
      11. Lift $e_1, \ldots, e_k$ 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 $\text{M}_4(\mathbb{Q})$, 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 $\mathcal{A}/\text{Rad}(A)$ 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 $\operatorname{disc} O$ are much bigger than 16, the following algorithm may give the correct answer with a high probability and less computation time.

Algorithm 8: CentralIdempotentsCommutativeOneTime

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

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

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

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 of Z satisfying good algebraic properties. To compute this proportion, we can as well work directly on

$$Z = K_1 \times \cdots \times K_r$$

where $K_i/\mathbb{F}_p$ are finite field extensions. Let us denote $s_i = [K_i : \mathbb{F}_p]$, so that $K_i \cong \mathbb{F}_{p^{s_i}}$. We denote also n the $\mathbb{F}_p$-dimension of Z, that is:

$$n = \sum_{i=1}^{r} s_i = [K_1 : \mathbb{F}_p] + \cdots + [K_r : \mathbb{F}_p]$$

The total number of elements in the algebra is thus $\operatorname{Card} Z = p^n$.

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 (as $s_i \geq 1$, we have $r \leq n$).

Now let us define two subsets of Z:

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

where π_x denotes the minimal polynomial of x over $\mathbb{F}_p$.

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

and let us denote $d_i = \frac{\operatorname{Card} S_i}{\operatorname{Card} Z}$ 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.

Computation of the density d_0. Let $a = (a_1, \ldots, a_r) \in S_0$. By definition, all components a_i share the same minimal polynomial over $\mathbb{F}_p$, let's call it $P(X)$. Let $\deg(P) = d$. For $P(X)$ to be the minimal polynomial of $a_i \in K_i = \mathbb{F}_{p^{s_i}}$, its degree d must be a divisor of s_i. This must hold for all $i = 1, \ldots, r$. Therefore, the degree d of any such common minimal polynomial must divide $g = \gcd(s_1, \ldots, s_r)$.

Let $N_d(p)$ be the number of monic irreducible polynomials of degree d over $\mathbb{F}_p$. For a fixed such polynomial $P(X)$ of degree d, the number of its roots in any field extension K_i where $d \mid s_i$ is exactly d. To form an element of S_0 corresponding to this polynomial $P(X)$, we must choose one of its d roots for each component a_i. This gives d^r choices.

Summing over all possible polynomials, we get the cardinality of S_0:

$$\operatorname{Card} S_0 = \sum_{d \mid g} N_d(p) \cdot d^r$$

To show that this quantity is small compared to $\operatorname{Card} Z$, we can bound it. Since $d \leq g$ for any $d \mid g$, we have $d^r = d \cdot d^{r-1} \leq d \cdot g^{r-1}$.

$$\begin{aligned} \operatorname{Card} S_0 &\leq \sum_{d \mid g} N_d(p) \cdot (d \cdot g^{r-1}) \\ &= g^{r-1} \sum_{d \mid g} N_d(p) \cdot d \end{aligned}$$

Using the classical identity $\sum_{d \mid m} N_d(p) \cdot d = p^m$, we obtain:

$$\operatorname{Card} S_0 \leq g^{r-1} p^g$$

The density d_0 is therefore bounded by:

$$d_0 = \frac{\operatorname{Card} S_0}{\operatorname{Card} Z} \leq \frac{g^{r-1} p^g}{p^{\sum s_i}}$$

Since $g = \gcd(s_1, \ldots, s_r) \leq s_i$ for all i, we have $\sum s_i \geq r \cdot g$. This gives:

$$d_0 \leq \frac{g^{r-1} p^g}{p^{rg}} = \frac{g^{r-1}}{p^{g(r-1)}} = \left(\frac{g}{p^g}\right)^{r-1}$$

For the algorithm to be in a non-trivial case, we must have $r > 1$. Since $p \geq 2$ and $g \geq 1$, the term p^g grows much faster than g, ensuring that $\frac{g}{p^g} < 1$. For instance, if $p = 2$ and $g = 1$, the ratio is $1/2$. If $g \geq 2$, the ratio is even smaller. Thus, for $r > 1$, the density d_0 is very small, confirming that picking an element from S_0 at random is a low-probability event. For example, if we take the smallest possible values $p = 2, r = 2, g = 1$, we get $d_0 \leq 1/2$. If $r = 3$, $d_0 \leq 1/4$, and so on. The probability decreases exponentially with r.

Computation of the density d_1. (The mathematical analysis for this section will be completed later.)

C. Number of Irreducible Matrices in $\mathrm{M}_n(\mathbb{F}_p)$

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 $\mathrm{M}_n(\mathbb{F}_p)$, that is, matrices with an irreducible minimal polynomial. This will allow us to calculate the probability that a uniformly random matrix in $\mathrm{M}_n(\mathbb{F}_p)$ 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 $\mathcal{A}_\pi$. 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

$$D_\pi = \mathrm{diag}(C_\pi, \ldots, C_\pi)$$

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

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

The set $\mathcal{A}_\pi$ is the orbit of D_π under the conjugation action of $\mathrm{GL}_n(\mathbb{F}_p)$ on $\mathrm{M}_n(\mathbb{F}_p)$.

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

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

$$|\mathcal{A}_\pi| = \frac{|\,\mathrm{GL}_n(\mathbb{F}_p)|}{|C_{\mathrm{GL}_n(\mathbb{F}_p)}(D_\pi)|}$$

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

Let's compute the centralizer of D_π. A matrix $P \in \mathrm{M}_n(\mathbb{F}_p)$, 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 $i, j \in \{1, \ldots, k\}$. 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 $\mathrm{M}_n(\mathbb{F}_p)$, denoted $C_{\mathrm{M}_n(\mathbb{F}_p)}(D_\pi)$, consists of block matrices where each block P_{ij} is in $\mathbb{F}_p[C_\pi]$. This ring is isomorphic to the matrix ring $\mathrm{M}_k(\mathbb{F}_p[C_\pi])$, and thus to $\mathrm{M}_k(\mathbb{F}_{p^d})$. The centralizer in $\mathrm{GL}_n(\mathbb{F}_p)$ is the group of invertible matrices in this ring, which is isomorphic to $\mathrm{GL}_k(\mathbb{F}_{p^d})$. Therefore, $|C_{\mathrm{GL}_n(\mathbb{F}_p)}(D_\pi)| = |\,\mathrm{GL}_k(\mathbb{F}_{p^d})|$, where $k = n/d$.

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

$$|\mathcal{A}_\pi| = \frac{|\,\mathrm{GL}_n(\mathbb{F}_p)|}{|\,\mathrm{GL}_{n/d}(\mathbb{F}_{p^d})|}$$

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

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

with

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

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

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 2: Counts and Probabilities of Irreducible Matrices

(n,p)	$I(n,p)$	Total Matrices (p^{n^2})	P(irreducible)	P(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

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 $\mathrm{M}_n(\mathbb{F}_p)$ 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 $p \to \infty$, 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 $p \to \infty$ if $d < n$, and to $\frac{1}{n}$ if $d = n$. Hence,

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

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.

[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/CBO9780511607219.

[6] Gábor Ivanyos, Ádám D. Lelkes, and Lajos Rónyai. *Improved algorithms for splitting full matrix algebras*. 2012. arXiv: 1211.1356 [math.RA]. URL: https://arxiv.org/abs/1211.1356.

[7] Gábor Ivanyos and Lajos Rónyai. "Finding maximal orders in semisimple algebras over Q". In: *Computational Complexity* 3 (1993), pp. 245–261. DOI: 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] 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.

[10] Denis Simon. "Solving quadratic equations using reduced unimodular quadratic forms". In: *Mathematics of Computation* 74.251 (2005), pp. 1531–1543.

[11] John Voight. *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*. 2012. arXiv: 1004.0994 [math.NT]. URL: https://arxiv.org/abs/1004.0994.

[12] 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. URL: https://link.springer.com/book/10.1007/978-3-030-56694-4.