Internship Report

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

Tommy Chakroun

Supervised by

Travis Morrison

June 2025

Abstract

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

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

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

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

Contents

1. Introduction

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

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

`Explicit Isomorphism Problem`Let $\mathcal{B}$ be a central simple F-algebra given by a basis and structure constants. Suppose that $\mathcal{B} \cong \mathcal{M}_n(F)$ as F-algebras. Compute an explicit isomorphism $\phi : \mathcal{B} \to \mathcal{M}_n(F)$, i.e., return n^2 matrices with entries in F representing the images of the basis elements of $\mathcal{B}$ under ϕ.

A slight variant is the following:

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

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

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

- $n = 2$: The problem reduces to solving a ternary quadratic equation $ax^2 + by^2 + cz^2 = 0$ over F, with $a, b, c \in F$. See [12], Main Theorem 5.4.4.
- $n = 2$, $F = \mathbb{Q}$: ...
- $n = 3$, F ...
- $n = 4$, $F = \mathbb{Q}$: See [6] for efficient methods.

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

Quaternion Algebras. Quaternion algebras are central simple algebras of dimension 4. When $\operatorname{char}(F) \neq 2$, these algebras admit a very concrete description: they have a basis $1, i, j, ij$, with $i^2 = a \in F^\times$, $j^2 = b \in F^\times$, and $ij = -ji$. See [12]. Quaternion algebras are closely related to ternary quadratic forms over F, which underpins the first case in the state of the art.

Motivation from Elliptic Curve Theory. Section 7 is dedicated to motivations coming from the theory of elliptic curves. Elliptic curves are special projective plane curves that carry a natural abelian group structure. The computational properties of these groups are of great interest in cryptography due to the hardness of the discrete logarithm problem. On a more abstract level, one can define *isogenies* between elliptic curves—morphisms of algebraic varieties that are also group homomorphisms. In particular, for an elliptic curve E, the set $\operatorname{End}(E)$ 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 $\operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ has the structure of a quaternion algebra over $\mathbb{Q}$.

Goals and Methods of this Paper. The goal of this paper is to study the General Explicit Isomorphism Problem over $\mathbb{Q}$ for algebras of dimension 4, i.e., quaternion algebras. Specifically, given two quaternion algebras over $\mathbb{Q}$ known to be isomorphic, we aim to compute an explicit isomorphism between them. By the aforementioned reduction, this is equivalent to solving the Explicit Isomorphism Problem for a 16-dimensional $\mathbb{Q}$-algebra isomorphic to $\mathcal{M}_4(\mathbb{Q})$.

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

Contents. This article is structured to provide a self-contained introduction to the explicit isomorphism problem in the context of quaternion algebras, along with its motivation and computational aspects. We begin by introducing the general framework of central simple algebras in Section 2, setting the stage for our discussion. In Section 3, we focus on quaternion algebras as a central class of examples, describing their structure and properties.

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

The core topic of this work—the explicit isomorphism problem—is formulated in general in Section 7. To motivate its relevance in arithmetic geometry, we present in Section 8 a brief interlude discussing connections to the theory of elliptic curves, in particular through isogenies and endomorphism rings. Section 9 then revisits the explicit isomorphism problem, now specialized to the case of quaternion algebras, and outlines algorithmic strategies for solving it in this setting.

Finally, Appendix A provides additional details on the implementation of the algorithms discussed in the main text. Appendix B recalls the Hasse–Minkowski theorem.

2. Central simple algebra

All algebra B over a field F are suppose unitary and associative, so that we can view $F \subset B$. We recall that the center of B is the set $Z(B)$ of element $b \in B$ which 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 both side inverse. Note that the center of an division algebra is a field an every division algebra has as structure of algebra over its center.
An algebra B, or more generally a ring, is *simple* it the only both sided ideals of B are $\{0\}$ and B. It is equivalent to say that for all non zero ring R, ever ring homomorphism $B \to R$ is injective.
Now we define an important class of algebra.

Definition 2.1. Let F be a field. A *central simple algebra* over F is a finite dimensional algebra with its center exactly F and with no non trivial both side ideals.

The standard example of central simple algebra is $B = \mathcal{M}_n(F)$, called the *split* central simple algebra of dimension n^2. The goal of this section is to show that, by extending the field, every central simple algebra are isomorphic to the split one.

First as simple algebra, central simple algebra enjoy the strong foolowing structure theorem.

Wederburn Artin theorem and consequences.

Theorem 2.2 (Wederburn Artin theorem, weak version)**.** *Let B be a finite dimensional simple algebra over F, then there exist a division algebra D over F and an integer $n \geq$ such that B is isomorphic to $\mathcal{M}_n(D)$. Moreover D is unique up to $F-$ algebra homomorphism.*

For the proof we follow Philippe Gille and Tamás Szamuely [4] Section 2.1.

Proof. Let I be a minimal nonzero left ideal of B. Suppose $f : I \to I$ is a B-linear map, meaning f is additive and satisfies $f(bx) = bf(x)$ for all $b \in B$, $x \in I$.

Then both $\ker f$ and $\operatorname{Im} f$ are left B-submodules of I. Since I is a minimal left ideal, it has no nontrivial B-submodules. Therefore, either $\ker f = \{0\}$ or $\ker f = I$, and similarly for the image.

Because $f \neq 0$, we must have $\ker f = \{0\}$ and $\operatorname{Im} f = I$. Hence, f is an isomorphism. We conclude that $D = \operatorname{End}_B(I)$, the subalgebra of $\operatorname{End}_F(I)$ consisting of B-linear endomorphisms, is a division algebra. (Note that the inverse of a B-linear map is automatically B-linear.)

So far, we have not used the simplicity of B. Now, consider $\operatorname{End}_D(B)$, the subalgebra of $\operatorname{End}_F(B)$ consisting of maps commuting with the right D-action.

We claim that the map

$$\varphi : B \to \operatorname{End}_D(B), \quad b \mapsto (z \mapsto bz)$$

defines an F-algebra isomorphism. ... □

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

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

Proof. See Philippe Gille and Tamás Szamuely [4], Lemma 2.2.2. □

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

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

Reduced trace. Let F be a field and let B be a central simple algebra over F. By the previous section let K/F be a field extension such that $B \otimes_F K \cong \mathcal{M}_n(K)$. Hence we can embedded B in $\mathcal{M}_n(K)$ by $\varphi : B \to \mathcal{M}_n(K), b \mapsto b \otimes 1$. We defined the *reduced trace* of $b \in B$ by

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

Proposition 2.5. *The reduced trace of b lies in F and doesn't depend on the chosen field extension K/F. More precisely when F is of characteristic 0 and B of dimension n^2 , for $b \in B$ we have*

$$trd(b) = \frac{1}{n} T_{B/F}(b)$$

where $T_{B/F}(b)$ is the trace of th $F-$linear map $B \to B, z \mapsto bz$.

Lemma 2.6 (Skolem-Nother Theorem for matrix ring)**.** *Let K be a field. Every automorphism of $\mathcal{M}_n(K)$ are inner and so preserve the trace.*

3. Quaternion algebras

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

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

We denote

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

as such an algebra.

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 a field of characteristic not 2, $M_2(F) \simeq \left(\frac{1,1}{F}\right)$ 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, 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 doesn't 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 enjoy the following properties :
transition to the next section...

Standard involution.

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

If B has a standard involution, then we have also $x + \overline{x} \in F$ 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 called the *reduced trace* of x $\mathrm{trd}(x) = x + \overline{x}$ and *reduced norm* o of x $\mathrm{nrd}(x) = x\overline{x}$. To check that an involution is standard it is not enough to check that $x\overline{x} \in F$ hold for x in a basis of B. But we have the following lemma.

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

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

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

lies in F. $\square$

An other remark is that if B has a standard involution then every $x \in B$ satisfy the polynomial of degree two with coefficient in F

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

In particular if B has a standard involution and $e_1, \dots, e_2$ 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: B an algebra over a field F with a basis $e_1 = 1, e_2, \dots, e_2$
Output: True if B has a standard involution, False otherwise.
1. 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 $\overline{\xi} := t(\xi) - \xi$.
2. If $\overline{e_i e_j} \neq \overline{e_j e_i}$ for some $2 \leq i, j \leq n$, return False
3. If $n_i := e_i\overline{e_i}$ or $n_{ij} := (e_i + e_j)(\overline{e_i + e_j})$ is not in F for some $2 \leq i, j \leq n$ return False, else return True.

Proof of correctness. If B has a standrad involution, the algorithm return True, OK.
... $\square$

Quadratic forms.

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

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

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:

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

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

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

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

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

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

Local global principle. See appendix on Hasse Minkowski theorem.

Theorem 3.4 (Local-Global Principle for Quaternion Algebras over $\mathbb{Q}$)**.** *Let B be a quaternion algebra over $\mathbb{Q}$. Then B is determined up to isomorphism by the set of places v of $\mathbb{Q}$ where B is ramified. More precisely, for each place v of $\mathbb{Q}$, let $B_v = B \otimes_{\mathbb{Q}} \mathbb{Q}_v$. Then B is uniquely determined (up to isomorphism) by the set*

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

which is a finite set of even cardinality.

Hilbert symbol over $\mathbb{Q}_p$
application to the problem `IdentifyMatrixwRing`.

4. Orders in central simple algebra

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

Theorem 4.2. *If Λ is an R-order in B, then for all $x \in \Lambda$, we have $trd(x) \in R$.*

Proof. Since R is a principal ideal domain, it is integrally closed. Thus, ... □

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

5. Discriminant

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

Let Λ be an R-order in B. For elements $a_1, \dots, a_N \in \Lambda$, define:

$$d(a_1, \dots, a_N) := \det \Big(\operatorname{trd}(a_i a_j) \Big)_{1 \le i,j \le N}.$$

By Theorem 4.2, each $\operatorname{trd}(a_i a_j) \in R$, so $d(a_1, \dots, a_N) \in R$.

The *discriminant* of Λ is the ideal $\operatorname{disc}(\Lambda) \subset R$ generated by all such $d(a_1, \dots, a_N)$ for $a_1, \dots, a_N \in \Lambda$. Since R is a principal ideal domain, this ideal is principal, say

$$\operatorname{disc}(\Lambda) = d_\Lambda R,$$

where $d_\Lambda \in R$ is uniquely determined up to a unit. That is, for $r \in R$,

$$r \in \mathrm{disc}(\Lambda) \iff d_\Lambda \mid r \quad \text{in } R.$$

Lemma 5.1. *If Λ is given by an R-basis $\Lambda = Re_1 \oplus \cdots \oplus Re_N$, then*

$$d_\Lambda = d(e_1, \ldots, e_N)$$

up to a unit in R.

Proof. By definition, $d_\Lambda \mid d(e_1, \ldots, e_N)$. For the reverse divisibility, for any $a_1, \ldots, a_N \in \Lambda$, we can write

$$a_i = m_{i,1}e_1 + \cdots + m_{i,N}e_N \quad \text{for some } m_{i,j} \in R.$$

Let $M = (m_{i,j}) \in \mathcal{M}_N(R)$. Then,

$$d(a_1, \ldots, a_N) = \det\left(\mathrm{trd}(a_i a_j)\right) = \cdots = \det(M)^2 \cdot d(e_1, \ldots, e_N),$$

so $d(a_1, \ldots, a_N) \in d(e_1, \ldots, e_N)R$, and hence $d_\Lambda \mid d(e_1, \ldots, e_N)$. □

Theorem 5.2. *If $\Lambda \subset \Gamma$ are two R-orders in B, then $d_\Gamma \mid d_\Lambda$ in R, and if $d_\Gamma = d_\Lambda$ up to a unit, then $\Gamma = \Lambda$.*

Proof. Write $\Lambda = Re_1 \oplus \cdots \oplus Re_N$ and $\Gamma = Rf_1 \oplus \cdots \oplus Rf_N$. Since $\Lambda \subset \Gamma$, we have $d(e_1, \ldots, e_N) \in \mathrm{disc}(\Gamma)$, i.e., $d_\Gamma \mid d(e_1, \ldots, e_N)$. ... □

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 of elements in R (with respect to divisibility). In particular, if

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

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 in R there cannot be an infinite strictly descending chain for the divisibility relation. (In a general ring not assumed to be a principal ideal domain, one typically uses Zorn's Lemma to prove the existence of maximal orders.)

Theorem 5.3. *Let Λ be an R-order in B. If d_Λ is a unit in R (i.e., disc$(\Lambda) = R$), then Λ is a maximal R-order. If $B \cong \mathcal{M}_n(F)$ for some integer n, then the converse is also true.*

Proof. ... □

6. Computing Maximal Orders

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

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

We describe a method following [5] 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 6.1 (Detection of Non-Maximality)**.** *With the notation above, suppose $\Lambda \subset B$ is not a maximal order. Then there exists a prime $p \mid d_\Lambda$, and an ideal $\mathcal{K} \subset \mathcal{C}_p$, either the zero ideal or a minimal nonzero ideal, such that the preimage*

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

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

Proof. Since Λ is not maximal, Theorem 5.3 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 2: Find a strictly bigger $\mathbb{Z}$-order ([5], 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 [3, Section 2.3.2] or [7, 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 $M \in \mathcal{M}_{r,N}(\mathbb{Z})$ 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 $MX \equiv 0 \mod p$.

- 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 $MX \equiv 0 \mod d$, 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 [2, Section 3].

7. Explicit isomorphism problem

In this section we give a solution to the `ExplicitIsomorphismProblem` for central simple algebra over $\mathbb{Q}$. We follow [6].

`ExplicitIsomorphismProblem`: Given a central simple algebra C isomorphic to $M_n(F)$, compute an isomorphism $\varphi : C \to M_n(F)$.

8. Interlude: Motivation from elliptic curve theory

Short definition of elliptic curve.
Short definition of the endomorphism ring $End(E)$.
Short definition and existence of the dual endomorphism map $End(E) \to End(E), \alpha \mapsto \hat{\alpha}$
Implication that $End(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ could be a quaternion algebra sometimes.
Short definition of super singular elliptic curve.
Why are they interesting ?
Statement that if E is super singular then $End(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is well an quaternion algebra over $\mathbb{Q}$
If E is super singular over F_p and ...., $End(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is exactly $B_{p,\infty}$.
Computational problem believe to be hard.

9. Explicit isomorphism of quaternion algebras

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

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

Lemma 9.1. *Let A be a central simple algebra of dimension N, there exist an isomorphism $\varphi : A \otimes A^{op} \to End_{\mathbb{Q}}(A)$ 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 $\mathcal{M}_N(\mathbb{Q})$.*

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

Proposition 9.2. *Let A, B be two central simple algebra of dimension N. Then A and B are isomorphic if and only if $A \otimes B^{op}$ is isomorphic to $M_N(F)$.*

A. Implementation and Precise Algorithms

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

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

A.1. Reduction $\varphi : A \otimes_{\mathbb{Q}} B^{op} \to M_4(\mathbb{Q})$ to $f : A \to B$. Let A, B be two central simple algebras of same dimension n. In Proposition 9.2 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 $e_1, \ldots, e_N$ a basis of A and $f_1, \ldots, f_n$ 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 2.6 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 $M_i = (m_{kj}^{(i)})_{1 \le k,j \le N} \in M_N(\mathbb{Q})$.

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

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

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 3: 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:*

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

  end

end

Complexity. Not evaluated yet.

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

Algorithm 4: ModularMatrixKernel

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

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

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

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

maximal_orders/maximal_orders_utilities.sage.

Complexity. Not evaluated yet.

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

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

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 $b_1, \dots, b_N$ any basis of B, then for all i there exists $t_i \in \mathbb{Z}_{>0}$ such that $t_i b_i \in O_L(I)$.

Now we want to compute explicitly a $\mathbb{Z}$-basis $f_1, \dots, f_N$ of $O_L(I)$. First note that there exists $s \in \mathbb{Z}_{>0}$ such that $s \cdot 1_B \in I$. Hence $O_L(I) \cdot s \subset I$ so $O_L(I) \subset s^{-1}I$. After, for $\alpha \in s^{-1}I$ that we write $\alpha = s^{-1}(x_1e_1 + \cdots + x_Ne_N)$ 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 $e_1, \dots, e_N$, 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 5: LeftOrder

Input: B a finite dimensional algebra over $\mathbb{Q}$; $e_1, \ldots, e_N$ 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 $1_B = r_1e_1 + \cdots + r_Ne_N$ 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 $e_1, \ldots, e_N$, that is $e_ie_j = \sum c_{i,j,k}e_k$
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 $X_1, \ldots, X_\ell \in \mathbb{Z}^N$ be a $\mathbb{Z}$-basis of solutions of $AX \equiv 0 \pmod d$
6. **return** $f_1, \ldots, f_\ell \in B$ *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 ($\mathcal{O}(N^2 \times N^2)$). Solving the system $AX \equiv 0 \pmod d$ with A of size $N^2 \times N$ and X of size N ($\mathcal{O}(??)$).
Total: $\mathcal{O}(??)$.

Remark A.1. If we suppose in addition that B is a division algebra or even just that every element of the $\mathbb{Z}$-basis $e_1, \ldots, e_N$ 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 $(e_j^{-1}e_1, \ldots, e_j^{-1}e_N)$ is still a $\mathbb{Q}$-basis of B since $z \mapsto e_j^{-1}z$ is a $\mathbb{Q}$-linear automorphism of B.

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

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

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

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

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

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

Proof. Let us fix an isomorphism as above. The image of $\mathrm{M}_{n_i}(D_i)$ 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 A.3. *Conversely, if $e_1, \dots, e_r$ are central orthogonal idempotents summing to 1, then the ideals Ae_i are exactly the minimal nonzero two-sided ideals of A, up to permutation.*

Proof. ... □

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

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

where each K_i/F is a finite field extension.

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

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

of finite field extensions of F. Find a maximal family $e_1, \ldots, e_r$ 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 6: CentralIdempotentsCommutativeSplit

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

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

foreach *a in Z* **do**

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

      end
   12. **return** Res

   end

end

13. **return** *the list* 1_A

Implementation. The function `central_idempotent_commutative_split` is available at minimal_ideals/minimal_ideals_manually.sage.

Comments. The algorithm is deterministic in theory with complexity at worst $\text{Card}(Z) = p^n$. It really depends on the size of the prime p and the dimension n. If both are relatively small we can easily iterate on Z. Otherwise if p is a very large prime around 100 bits then we can't reasonably iterate on Z so we prefer to pick a finite random number of elements of Z. Luckily when p is large and n small it happens that the probability that a is *decomposable* that is $s \geq 2$ in the algorithm is very high. Actually when p is very large in comparison to n we can use an easier algorithm. For example in our purpose of computing a maximal order containing an order O in the matrix ring $\mathcal{M}_4(\mathbb{Q})$, for each prime dividing 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 disc$O$ are much bigger than 16, the following algorithm may give the correct answer with a high probability and less computation time.

Algorithm 7: CentralIdempotentsCommutativeOneTime

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

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

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 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. We denote also n the $\mathbb{F}_p$-dimension of Z, that is:

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

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

Now let us define two subsets of Z :

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

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

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

Then:

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

B. Proof of the Hasse-Minkowski Theorem

Theorem B.1 (Hasse-Minkowski theorem)**.** *A quadratic form over Q is isotropic if and only if it is isotropic over $\mathbb{Q}_p$ for all prime p and over $\mathbb{R}$. In other words if n is a positive integer, and $a_1, \ldots, a_n \in \mathbb{Q}$ then $a_1x_1^2 + \cdots + a_nx_n^2 = 0$ has a non trivial in $\mathbb{Q}^n$ if and only if it has nontrivial solution over $\mathbb{Q}_p$ for all prime p and $\mathbb{R}$.*

Lemma B.2. *This hold for ternary quadratic forms, that's mean $n = 3$.*

Proof of lemma B.2. Let Q be a ternary quadratic form over Q, by digonaliztion theorem Q is equivalent over Q (and so over all the Q_p to a diganal quadratic form :

$$aX^2 + bY^2 + cZ^2.$$

Multiplying by $-c$, Q is similar we can suppose that

$$aX^2 + bY^2 - Z^2$$

□

References

[1] Tímea Csahók, Péter Kutas, Mickaël Montessinos, and Gergely Zábrádi. Explicit isomorphisms of quaternion algebras over quadratic global fields, 2022.

[2] W. Eberly and M. Giesbrecht. Efficient decomposition of associative algebras. In Y. N. Lakshman, editor, *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation (ISSAC'96)*, pages 170–178, New York, 1996. ACM.

[3] Wayne Eberly. *Computations for Algebras and Group Representations.* PhD thesis, University of Toronto, 1989. http://www.cpsc.ucalgary.ca/~eberly/Research/Papers/phdthesis.pdf.

[4] Philippe Gille and Tamás Szamuely. *Central Simple Algebras and Galois Cohomology*, volume 101 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2006.

[5] Gábor Ivanyos and Lajos Rónyai. Finding maximal orders in semisimple algebras over q. *Computational Complexity*, 3:245–261, 1993.

[6] Gábor Ivanyos, Ádám D. Lelkes, and Lajos Rónyai. Improved algorithms for splitting full matrix algebras, 2012.

[7] Lajos Rónyai. Computing the structure of finite algebras. *Journal of Symbolic Computation*, 9(3):355–373, 1990.

[8] Lajos Rónyai. Algorithmic properties of maximal orders in simple algebras over q. *Computational Complexity*, 2:225–243, 1992.

[9] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009.

[10] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2013.

[11] John Voight. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms, 2012.

[12] John Voight. *Quaternion Algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer, Cham, 2021.