# Solving the Explicit Isomorphism Problem using Amitsur cohomology

Mickaël Montessinos[1]

[1]Eötvös Loránd University, Hungary

Tuesday 9th June, 2026

Number theory seminar, Bordeaux

# The Explicit Isomorphism Problem

### Main problem

Given a $\mathbb{Q}$-algebra $A$ of dimension $n^2$, compute if it exists an isomorphism between $A$ and $M_n(\mathbb{Q})$.

### Reduction

Let $D$ be a central division $\mathbb{Q}$-algebra (e.g. a quaternion algebra). Computing an isomorphism between $A$ and $M_n(D)$ reduces to computing an isomorphism between $A \otimes M_n(D)^{op}$ and $M_{n^2 d^2}(\mathbb{Q})$.

# Application to superspecial abelian varieties

Let $X$ be a polarised superspecial abelian variety of genus $n$ over some finite field $\mathbb{F}_{p^2}$.

## Knowing the endomorphism ring

**Geometric data** Endomorphisms $f_1, \ldots, f_{4n^2}$ of $X$ which generate the ring $\mathrm{End}(X)$ as a $\mathbb{Z}$-module, the dual endomorphisms $f_i^\vee$ (and some additional information).

**Algebraic data** A maximal order $\mathcal{O}$ in $M_n(B)$ ($B$ the quaternion algebra of discriminant $p$) and a definite positive involution of $M_n(B)$ that leaves $\mathcal{O}$ invariant.

## Getting the algebraic data from the geometric data

Reduces to computing an isomorphism

$$\mathrm{End}(X) \otimes \mathbb{Q} \to M_n(B).$$

# Two different approaches in a nutshell

## The lattice approach

- Embed $A$ into $M_n(\mathbb{R})$;
- Maximal orders of $A$ become lattices;
- Given a maximal order, an element of bounded norm will have rank one;
- An element of rank one may be used to compute an isomorphism to $M_n(\mathbb{Q})$.

## The cohomological approach

- Get some adequate maximal commutative subalgebra $K \subset A$;
- Compute some compact algebraic presentation of $A$;
- Compute an isomorphism to $M_n(\mathbb{Q})$ by solving a (system of) multiplicative equation(s) over $K$.

# Known results

- The lattice approach (Exponential in $n$ and discriminant of base field, requires factorisation oracle):
  - First version – Cremona, Fisher, O'Neil, Simon and Stoll (2011);
  - Rigorous, generalized version – Ivanyos, Lelkes, Rónyai, Schicho (2012-2013);
  - Over a rational function field on a finite field – Ivanyos, Kutas and Rónyai (2018);
  - No factorisation oracle if a maximal order is known – Page, Robert, Soumier (2026);
- The cohomology approach (Requires an adequate maximal commutative subalgebra and an oracle for computation of groups of $S$-units):
  - Given a cyclic subfield – Simon (and folklore) (2002);
  - If $n = 3$ – de Graaf, Harrison, Pílniková, Schicho (2006);
  - If $n = 4$ – Pílniková (2007);
  - Given a Galois subfield – Fieker (and folklore) (2009);
  - Given no additional information – Kutas and M. (2024);

# Algebraic presentations of central simple algebras

- Cyclic algebras (from a cyclic field extension)– Dickson (1905);
- Brauer factor sets (from a separable field extension)– Brauer (1928);
- Crossed product (from a Galois field extension)– Noether (1929);
- Differential crossed products (from a purely inseparable field extension) – Hoschild (1955);
- Amitsur cohomology classifies central simple algebras – Amitsur (1959);
- Constructing a central separable algebra using a commutative algebra over a ring (with extra hypotheses) using Amitsur cohomology – Rosenberg, Zelinsky (1960)

$\vdots$

# Cyclic algebras

Let $K/\mathbb{Q}$ be a cyclic number field of degree $n$, with Galois group $G = \langle \sigma \rangle$.

## Cyclic Algebras

Let $a \in \mathbb{Q}^\times$, $V \simeq K^n$ with basis $(1, y, \ldots, y^{n-1})$. Make $V$ a $\mathbb{Q}$-algebra $A$ with multiplication defined by

$$\begin{aligned} y^n &= a; \\ y^i y^j &= y^{i+j}; \\ y\alpha &= \sigma(\alpha) y \quad \forall \alpha \in K; \end{aligned}$$

Then $A$ is a *cyclic algebra*, denoted by $\langle K, \sigma, a \rangle$.

## Example: Quaternion algebras

The quaternion algebra $\left(\frac{a,b}{\mathbb{Q}}\right)$ is isomorphic to the cyclic algebra $\langle \mathbb{Q}(\sqrt{a}), \sigma, b \rangle$.

# Isomorphy classes of cyclic algebras

Let $K$ be a cyclic number field of degree $n$, with Galois group $G = \langle \sigma \rangle$. Let $a, b \in \mathbb{Q}^\times$. Assume that $c \in K^\times$ such that $a = N_{K/\mathbb{Q}}(c)b$. Then, the map

$$\begin{array}{ccc} \langle K, \sigma, a \rangle & \to & \langle K, \sigma, b \rangle \\ y & \mapsto & cy \end{array}$$

is an isomorphism of $\mathbb{Q}$-algebras.

**Fact**

The algebras $\langle K, \sigma, a \rangle$ and $\langle K, \sigma, b \rangle$ are isomorphic if and only if there exists $c \in K^\times$ such that $a = N_{K/\mathbb{Q}}(c)b$.

# Splitting a cyclic algebra

Let $K$ be a cyclic number field of degree $n$, with Galois group $G = \langle \sigma \rangle$. For $\alpha \in K$, let $m_\alpha$ be the multiplication-by-alpha map on $K$.

**Fact**

The map

$$\begin{array}{ccc} \langle K, \sigma, 1 \rangle & \to & \mathrm{End}_{\mathbb{Q}}(K) \\ y & \mapsto & \sigma \\ K \ni \alpha & \mapsto & m_\alpha \end{array}$$

is an isomorphism of $\mathbb{Q}$-algebras.

**Theorem**

The cyclic algebra $\langle K, \sigma, a \rangle$ is isomorphic to $M_n(\mathbb{Q})$ if and only if $a \in N_{K/\mathbb{Q}}(K^\times)$.

# Solving the EIP using cyclic algebras

**Algorithm**

INPUT: Structure constants for an algebra $A$ isomorphic to $M_n(\mathbb{Q})$
INPUT: An embedding $K \to A$, with $K$ a cyclic number field of degree $n$
OUTPUT: An isomorphism $A \to M_n(\mathbb{Q})$

1. Compute an isomorphism $A \to \langle K, \sigma, a \rangle$ for some $a \in \mathbb{Q}$;
2. Compute $c \in K^\times$ such that $N_{K/\mathbb{Q}}(c) = a$;
3. Compute an isomorphism $A \to \langle K, \sigma, 1 \rangle$;
4. Compute an isomorphism $A \to M_n(\mathbb{Q})$;

## The harsh reality

Let $A \simeq M_n(\mathbb{Q})$.

### Heuristic

- A random element $z \in A$ has an irreducible characteristic polynomial $\chi_z$.
- The number field $K = \mathbb{Q}(z)$ has a normal closure $L$ of degree $n!$.
- Its Galois group is the permutation group $S_n$.

### Overcoming the hurdle

- Brauer factor sets provide an algebraic presentation given any embedded number field $K \subset A$ of degree $n$.
- But the computations happen in the normal closure of $K$.
- We provide an equivalent construction, where computations happen in $K \otimes K \otimes K$ instead.

# Étale algebras

**Definition (Étale algebra)**

An *étale $\mathbb{Q}$-algebra* is a commutative $\mathbb{Q}$-algebra $K$ that splits uniquely as a direct product

$$K = K_1 \times \cdots \times K_r$$

of number fields.

**Fact**

Let $A$ be a $\mathbb{Q}$-algebra isomorphic to $M_n(\mathbb{Q})$. Let $z \in A^\times$ have a minimal polynomial of degree $n$ that is separable. Then, $\mathbb{Q}(z) \subset A$ is an étale $\mathbb{Q}$-algebra of degree $n$.

# Constructing Amitsur algebras

Let $A \simeq M_n(\mathbb{Q})$, let $K \subset A$ be an étale $\mathbb{Q}$-algebra of dimension $n$. Write $K^{\otimes n}$ for $K \otimes_{\mathbb{Q}} K \otimes_{\mathbb{Q}} \cdots \otimes_{\mathbb{Q}} K$.

## Facts

- $A$ is a $K^{\otimes 2}$-module, via $(\alpha \otimes \beta)x = \alpha x \beta$.
- $A$ is cyclic as a $K^{\otimes 2}$-module: there exists $v \in A$ such that $A = K^{\otimes 2} v$.

## Example

Let $B = \left(\frac{-1,5}{\mathbb{Q}}\right)$, with $i^2 = -1$ and $j^2 = 5$. Set $K = \mathbb{Q}(i)$ and $v = 1 + j$:

$$(1 \otimes 1)v = 1 + j \qquad (1 \otimes i)v = i - k$$
$$(i \otimes 1)v = i + k \qquad (i \otimes i)v = -1 + j$$

# The product on $K^{\otimes 2}$

## Factoring through $K^{\otimes 3}$

$$\begin{tikzcd}
(avb, a'vb') \arrow[r, mapsto] & avba'vb' \arrow[r, equal] & \sum_{i\in I} \alpha_i v \beta_i \\
A \times A \arrow[r] \arrow[d, "\sim"] & A \arrow[r, equal] & A \arrow[d, "\sim"] \\
K^{\otimes 2} \times K^{\otimes 2} \arrow[r] & K^{\otimes 3} \arrow[u] \arrow[r, dashed, "\pi_A"] & K^{\otimes 2} \\
(a \otimes b, a' \otimes b') \arrow[r, mapsto] & a \otimes ba' \otimes b' \arrow[r, mapsto] & \sum_{i\in I} (\alpha_i \otimes \beta_i)
\end{tikzcd}$$

## Observations

- Via the map $a \otimes b \mapsto a \otimes 1 \otimes b$, the ring $K^{\otimes 3}$ is a $K^{\otimes 2}$-algebra that is a free module.
- The map $\pi_A$ is $K^{\otimes 2}$-linear form.
- There exists $c_A \in R^{\otimes 3}$ such that $\pi_A \colon t \mapsto \mathrm{Tr}_{R^{\otimes 3}/R^{\otimes 2}}(tc_A)$.

# A quaternion example

**Fact**

$$\mathrm{Tr}_{K^{\otimes 3}/K^{\otimes 2}}(\alpha \otimes \beta \otimes \gamma) = \mathrm{Tr}_{K/\mathbb{Q}}(\beta)(\alpha \otimes \gamma).$$

Consider our prior example: $B = \left(\frac{-1,5}{\mathbb{Q}}\right)$, $i^2 = -1$, $j^2 = 5$, $K = \mathbb{Q}(i)$ and $v = 1 + j$.
We compute:

$$v^2 = 6 + 2j = 4v - 2ivi \implies \pi_B(1 \otimes 1 \otimes 1) = 4 \otimes 1 - 2i \otimes i$$
$$viv = -4i = -2vi - 2iv \implies \pi_B(1 \otimes i \otimes 1) = -2 \otimes i - 2i \otimes 1$$

A quick computation yields:

$$c_B = 2 \otimes 1 \otimes 1 - i \otimes 1 \otimes i + 1 \otimes i \otimes i + i \otimes i \otimes 1$$

# Amitsur algebras

Let $K$ be an étale $\mathbb{Q}$-algebra.

## The $\varepsilon$ maps

We define the following maps, for $n \in \mathbb{N}$ and $0 \leq i \leq n+1$:

$$\begin{array}{cccc} \varepsilon_i^n : & K^{\otimes(n+1)} & \to & K^{\otimes(n+2)} \\ & a_0 \otimes \cdots \otimes a_n & \mapsto & a_0 \otimes \cdots \otimes a_{i-1} \otimes 1 \otimes a_i \otimes \cdots \otimes a_n \end{array}$$

## Definition (Amitsur algebras)

Let $c \in K^{\otimes 3}$. The *Amitsur algebra* $A(K, c)$ is the $\mathbb{Q}$-algebra with underlying vector space $K^{\otimes 2}$ and product defined by

$$\pi_c(x, y) = \mathrm{Tr}_{K^{\otimes 3}/K^{\otimes 2}}(\varepsilon_2^1(x) c \varepsilon_0^2(y))$$

That is,

$$(a \otimes b)(a' \otimes b') = \mathrm{Tr}((a \otimes ba' \otimes b)c)$$

# The trivial Amitsur algebra

Consider the map

$$\begin{array}{rccc} \varphi\colon & K \otimes K & \to & \mathrm{End}_{\mathbb{Q}}(K) \\ & a \otimes b & \mapsto & \left(x \mapsto \mathsf{Tr}_{K/\mathbb{Q}}(xb)a\right) \end{array}$$

We get the composition law:

$$\varphi(a \otimes b) \circ \varphi(a' \otimes b')(x) = \varphi(a \otimes b)(\mathsf{Tr}(b'x)a') = \mathsf{Tr}(b'x)\,\mathsf{Tr}(a'b)a$$

Therefore,

$$\begin{aligned} \varphi(a \otimes b) \circ \varphi(a' \otimes b') &= \varphi\left(\mathsf{Tr}_{K/\mathbb{Q}}(ba')a \otimes b'\right) \\ &= \varphi\left(\mathsf{Tr}_{K^{\otimes 3}/K^{\otimes 2}}(a \otimes ba' \otimes b')\right) \end{aligned}$$

**Fact**

The map $\varphi$ above yields an isomorphism from $A(K, 1^{\otimes 3})$ to $\mathrm{End}_{\mathbb{Q}}(K)$.

# Amitsur cohomology

For $n \in \mathbb{N}$, we set $C^n(K) = \mathbb{G}_m\left(K^{\otimes(n+1)}\right)$. We consider the maps

$$\begin{array}{rccc} \partial^n: & C^n(K) & \to & C^{n+1}(K) \\ & t & \mapsto & \prod_{i=0}^{n+1} \varepsilon_i^n(t)^{(-1)^i} \end{array}$$

## Definition (Amitsur cohomology)

The group of Amitsur $n$-cocycles of $K$ is

$$Z^n(K) = \mathrm{Ker}(\partial^n).$$

The group of Amitsur $n$-coboundaries of $K$ is

$$B^n(K) = \mathrm{Im}(\partial^{n-1}) \quad \text{and } B^0(K) = \{1\}.$$

The Amitsur $n$-th cohomology goup of $K$ is

$$H^n(K) = Z^n(K)/B^n(K).$$

# Amitsur cohomology and Amitsur algebras

## Amitsur algebras and Amitsur cocycles

The Amitsur algebra $A(K,c)$ is a central simple $\mathbb{Q}$-algebra of degree $n$ if and only if $c \in Z^2(K)$.

## Amitsur algebras and Amitsur coboundaries

Let $c, c' \in Z^n(K)$, and let $a \in C^1(K)$ be such that $c = \partial^1(a)c'$. Then, the map

$$\begin{array}{ccc} A(K,c) & \to & A(K,c') \\ x & \mapsto & ax \end{array}$$

is an isomorphism.

## Theorems

1. The map $c \mapsto A(K,c)$ yields an isomorphism from $H^2(K)$ to $\mathrm{Br}(K/F)$.
2. We have $A(K,c) \simeq M_n(\mathbb{Q})$ if and only if $c \in B^2(K)$.

# The quaternion example continued

Recall our setting: $B = \left(\frac{-1,5}{\mathbb{Q}}\right)$, $i^2 = -1, j^2 = 5$, $K = \mathbb{Q}(i)$, $v = 1 + j$,

$$c = 2 \otimes 1 \otimes 1 - i \otimes 1 \otimes i + 1 \otimes i \otimes i + i \otimes i \otimes 1.$$

We have the isomorphisms

$$\begin{array}{ccc} A(K, c) & \to & B \\ a \otimes b & \mapsto & avb. \end{array}$$

and

$$\begin{array}{ccccc} A(K, 1^{\otimes 3}) & \to & \mathrm{End}_{\mathbb{Q}}(K) & \to & M_2(\mathbb{Q}) \\ a \otimes b & \mapsto & (x \mapsto a\,\mathrm{Tr}(bx)) & \mapsto & \begin{pmatrix} 2b_1 a_1 & -2b_2 a_1 \\ 2b_1 a_2 & -2b_2 a_2 \end{pmatrix} \end{array}$$

# Primes of an étale algebra

Let $K = K_1 \times \cdots \times K_r$ be an étale algebra over $\mathbb{Q}$.

## Definitions

- A *prime* of $K$ is a pair $(i, \mathfrak{p})$, where $\mathfrak{p}$ is a prime of $K_i$.
- The rational prime below a prime $(i, \mathfrak{p})$ of $K$ is the rational prime below $\mathfrak{p}$.
- If $b = (b_1, \ldots, b_r) \in K^\times$, the *support* of $b$, $\mathrm{Supp}(b)$, is the set of rational primes below the primes in the support of the $b_i$.
- The class group of $K$ is the disjoint union

$$\mathrm{Cl}(K) = \bigsqcup_{i=1}^{r} \mathrm{Cl}(K_i).$$

- Let $S$ be a set of rational primes. The group $U_S(K)$ of *$S$-units* of $K$ is the group

$$U_S(K) = \left\{ x \in K^\times : \ \mathrm{Supp}(x) \subset S \right\}.$$

# Integrating the coboundary

We adopt a strategy similar to Simon's algorithm for solving norm equations:

**Theorem (Kutas, M.)**

Let $K$ be an étale $\mathbb{Q}$-algebra and let $b \in C^2(K)$. Let $S$ be a finite set of primes such that:

- $S$ contains the primes that ramify in $K$;
- Primes above $S$ generate the class group of $K$;
- $S$ contains the support of $b$.

Then, $b \in B^2(K)$ iff there exists $a \in U_S(K)$ such that $b = \partial^1(a)$.

**Corollary**

The equation $b = \partial^1(a)$ turns into a $\mathbb{Z}$-linear equation over groups of $S$-units.

# Quaternion example: moving to products of number fields

Recall our setting: $B = \left(\frac{-1,5}{\mathbb{Q}}\right)$, $i^2 = -1, j^2 = 5$, $K = \mathbb{Q}(i)$, $v = 1 + j$,

$$c = 2 \otimes 1 \otimes 1 - i \otimes 1 \otimes i + 1 \otimes i \otimes i + i \otimes i \otimes 1.$$

We have the isomorphisms

$$\begin{array}{cccc} \Theta_2 : & K^{\otimes 2} & \to & K^2 \\ & \alpha \otimes \beta & \mapsto & (\alpha\beta, \alpha\overline{\beta}) \end{array}$$

and

$$\begin{array}{cccc} \Theta_3 : & K^{\otimes 3} & \to & K^4 \\ & \alpha \otimes \beta \otimes \gamma & \mapsto & (\alpha\beta\gamma, \alpha\beta\overline{\gamma}, \alpha\overline{\beta}\gamma, \alpha\overline{\beta\gamma}). \end{array}$$

We split our coboundary $c$ in product form:

$$\begin{aligned} \Theta_3(c) &= (2,2,2,2) - (-1,1,-1,1) + (-1,1,1,-1) + (-1,-1,1,1) \\ &= (1,1,5,1) \end{aligned}$$

# Quaternion example: integrating the coboundary

We must solve the equation

$$\Theta_3 \circ \partial^1(a) = (1, 1, 5, 1).$$

For this purpose, we compute an expression of $\Theta_3 \circ \partial^1 \circ \Theta_2^{-1}$. For $\alpha, \beta \in K$,

$$\begin{aligned}
\Theta_3 \circ \varepsilon_0^1 \circ \Theta_2^{-1}(\alpha, \beta) &= (\alpha, \beta, \overline{\beta}, \overline{\alpha}) \\
\Theta_3 \circ \varepsilon_1^1 \circ \Theta_2^{-1}(\alpha, \beta) &= (\alpha, \beta, \alpha, \beta) \\
\Theta_3 \circ \varepsilon_2^1 \circ \Theta_2^{-1}(\alpha, \beta) &= (\alpha, \alpha, \beta, \beta) \\
\Theta_3 \circ \partial^1 \circ \Theta_2^{-1}(\alpha, \beta) &= (\alpha, \alpha, \alpha^{-1} N_{K/\mathbb{Q}}(\beta), \overline{\alpha})
\end{aligned}$$

Then, we easily find the solution

$$a = \Theta_2^{-1}(1, 2 + i).$$

# Quaternion example: putting things together (part 1)

We have the chain of isomorphisms

$$B \to A(K, c) \to A(K, 1^{\otimes 3}) \to M_2(\mathbb{Q})$$

We compute, for instance, the image of $j \in B$. Recall that $v = 1 + j$. We get:

$$j = \frac{1}{2}(v + ivi),$$

so we map $j$ to $\frac{1}{2}(1 \otimes 1 + i \otimes i)$. Now,

$$\Theta_2\left(\frac{1}{2}(1 \otimes 1 + i \otimes i)\right) = (0, 1).$$

Then,

$$\frac{a}{2}(1 \otimes 1 + i \otimes i) = \Theta_2^{-1}(0, 2 + i) = 1 \otimes 1 + i \otimes i + \frac{1}{2}(i \otimes 1 - 1 \otimes i).$$

# Quaternion example: putting things together (part 2)

From what precedes, the image of $j$ in $A(K, 1^{\otimes 3})$ is

$$\Theta_2^{-1}(0,5) = 1 \otimes 1 + i \otimes i + \frac{1}{2}(i \otimes 1 - 1 \otimes i).$$

Recall that $(\alpha_1 + i\alpha_2) \otimes (\beta_1 + i\beta_2) \in A(K, 1^{\otimes 3})$ is sent to the matrix

$$\begin{pmatrix} 2b_1 a_1 & -2b_2 a_1 \\ 2b_1 a_2 & -2b_2 a_2 \end{pmatrix}.$$

As a result, the image of $j$ in $M_2(\mathbb{Q})$ is

$$J = \begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix}.$$

# Thank you!

For further details, consider looking up

Our paper:

`https://arxiv.org/abs/2307.00261`

My dissertation:

`https://doi.org/10.15388/vu.thesis.726`