The explicit isomorphism problem

Mickaël Montessinos
(Vilnius University)

Bayreuth University's Arithmetic Geometry Seminar
Thursday 19th January, 2023

The matter at hand

Structure constants

Let k be a field, $V = k^n$ with canonical basis $(e_1, \ldots, e_n)$.
A k-algebra structure on V is given by a family $c \in k^{n^3} \simeq (V^\wedge)^{\otimes 2} \otimes V$ giving the multiplication law

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

The c_{ijk} are called the *structure constants* of A.

Explicit Isomorphism Problem

Let A be a k-algebra, that is known to be isomorphic to $M_n(k)$. Find an explicit isomorphism

$$\varphi : A \simeq M_n(k).$$

The structure of algebras

Convention

Every k-algebra is associative, unital and finite dimensional.

Theorem(Jacobson, Wedderburn, Artin, Malcev...)

Let k be a perfect field, A a k-algebra.

$$A = J \oplus W,$$

where J is the Jacobson radical of A and W is the Wedderburn-Malcev complement:

$$W \simeq A_1 \oplus \ldots \oplus A_r,$$

and the A_i are simple algebras, hence there are unique division algebras D_i such that

$$A_i \simeq M_{n_i}(D_i)$$

Algorithmic assay of an algebra

Let k be a finite field or a number field.

Algorithm (Cohen, Ivanyos, Wales)

There is a polynomial algorithm which computes the Jacobson radical of a k-algebra.

Algorithm (De Graaf, Ivanyos, Küronya, Rónyai)

There is a polynomial algorithm which computes a Wedderburn-Malcev complement of the Jacobson radical in a k-algebra.

Algorithm (Eberly, Giesbrecht)

There is an probabilistic polynomial algorithm which computes the decomposition

$$W \simeq A_1 \oplus \ldots \oplus A_r$$

Explicit isomorphism to a simple algebra

Algorithm (Rónyai)

If k is a finite field, there is a polynomial algorithm which solves the explicit isomorphism problem. Since any division k-algebra is commutative, this fully solves the problem.

Theorem (Ivanyos, Rónyai, Schicho)

The problem of computing an explicit isomorphism $A \simeq M_n(D)$ reduces to identifying n and D, and constructing an explicit isomorphism $A^{op} \otimes M_n(D) \simeq M_{n^2}(k)$.

Theorem (Rónyai,Voight)

The explicit isomorphism problem over a number field is at least as hard as the quadratic residuosity problem.

Known results

Quaternion algebras A Las Vegas probabilistic *ff*-algorithm[1] for quaternion algebras over the rationals (Rönyai) and over a quadratic number field (Kutas).

Rational numbers An *ff*-algorithm for n bounded (Cremona, Fisher, O'Neil,Simon,Stoll ; Ivanyos,Rónyai,Schicho,Lelkes).

Number fields An *ff*-algorithm for n bounded and K fixed (Ivanyos,Rónyai,Schicho,Lelkes).

Rational function fields $\mathbb{F}_q(T)$ An *f*-algorithm[2], polynomial in n (Ivanyos, Kutás, Ronyai) .

Quadratic extensions of known cases An *ff*-algorithm for biquaternion algebras (Csahók, Kutas, Zábrádi, M).[3]

Global function fields Open problem.

[1] A deterministic polynomial reduction to factoring integers and polynomials over finite fields.

[2] A deterministic polynomial reduction to factoring polynomials over a finite field.

[3] Currently under revision

From zero divisor to hero divisor

Assume $A \simeq M_n(k)$, and we know some zero divisor $z \in A$ such that $\dim_k Az = n$ (*i.e* z corresponds to a rank one matrix). Set $V = Az$.

1. The vector space V is a simple A-module. Hence, we explicitely get $A \simeq \mathrm{End}_k(V)$
2. Using linear algebra, we may easily compute a basis of V. This yields an explicit isomorphism $V \simeq k^n$.
3. This, in turn, yields an explicit $A \simeq M_n(k)$.

Example

$$z = \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}, \; M_n(k)z = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in k \right\}$$

An example

Consider the quaternion algebra $B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$ given by $i^2 = j^2 = 1$ and $ij = -ji$.
We know a zero divisor $z = i - 1$ (indeed, $(i-1)(i+1) = i^2 - 1^2 = 0$).
We get an isomorphism and compute the image of ij.

1. $z = i - 1$ is a zero-divisor. The space $V = Bz$ is generated by the family $(i - 1, 1 - i, -j - ij, -j - ij)$.
2. $e_1 := i - 1$ and $e_2 := j + ij$ form a basis of $V = Bz$.
3. We compute: $ije_1 = -j - ij = -e_2$ and $ije_2 = i - 1 = e_1$
4. We obtain: $\varphi(ij) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Higher rank zero divisors are partial victories

Assume $A \simeq M_3(\mathbb{Q})$ and $z \in A$ has rank 2. For instance, $z = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

1. The space $V = Az$ has dimension 6, and contains matrices of the form $\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 0 \end{pmatrix}$.
2. It admits a right unit $e = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.
3. Then, AeA is the subalgebra of rank 4 containing matrices of the form $\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix}$.
4. In fact, $AeA \simeq M_2(\mathbb{Q})$.
5. The problem has been reduced to a smaller instance.

A needle in a haystack

Problem

Given structure constants for a k-algebra A, find a zero-divisor, ideally of rank 1.

Caveat

Let $A \simeq M_n(k)$ have basis $(e_1, \ldots, e_{n^2})$. By the Schwartz-Zippel lemma, if $S \subset k$ is finite,

$$\frac{\#\left\{z \in \bigoplus_{1 \leq i \leq n^2} Se_i \mid z \text{ is a zero divisor}\right\}}{\#\bigoplus_{1 \leq i \leq n^2} Se_i} \leq \frac{n}{|S|^n}$$

The case of $\mathbb{Q}$ and number fields: A smallish box of hay

Idea

Let Λ be a maximal $\mathbb{Z}$-order in $A \simeq M_n(\mathbb{Q})$. Embed $A \in M_n(\mathbb{R})$, and get a Frobenius norm $||.||$ on A. Then, one may prove that there exists a rank one $z \in \Lambda$ such that $||z|| \leq n$

Difficulty

Once a LLL-reduced basis of Λ is obtained, one needs to check vectors with coordinates bounded by $c_m\sqrt{n}$, where $m = n^2$ and $c_m = \gamma_m^{\frac{m}{2}} \left(\frac{3}{2}\right)^m 2^{\frac{m(m-1)}{2}}$.[a]

[a] Subsequent work improves the constant c_m when $n \leq 43$.

Even harder!

If $\mathbb{Q}$ is replaced by a number field of degree d and discriminant Δ, an analogous method yields a simial approach. The bound on the coefficient for the search now also has a factor in $|\Delta|^{1/d}$ and $m = n^2 d$.

Interlude

The road so far

- The explicit isomorphism problem is the hard part in assaying associative algebras over a field.
- It is solved by finding a rank one zero divisor.
- So far, we know
  1. A polynomial algorithm over finite fields.
  2. An *ff*-algorithm over number fields, for fixed n and field, using Minkowski theory to reduce the search to a *smallish* box.

Further ideas

1. Using a solution to the problem on a field K and Galois descent to get a solution on a finite extension L/K.
2. Using algebaic geometry to solve the problem on function fields.

Bootstrapping via Galois descent

Main idea

Consider an extension L/K, and $A \simeq M_n(L)$. Then, find a K-subalgebra of L and solve the problem over K.

Problem

Let $A \simeq M_n(L)$. Find a K-subalgebra of A that contains zero divisors.

Lemma

Let $L|K$ be Galois of group G. Let ρ be a semi-linear G-action on A. That is,

$$\forall \sigma \in G,\ \forall x \in L \subset A,\ \rho_\sigma(x) = \sigma(x).$$

Then A^ρ is a K-subalgebra of A of degree n.

Twisted actions via involutions

Definition

Assume L/K is quadratic with non-trivial automorphism σ. An involution is a linear map $\iota : A \to A$, such that $\iota^2 = Id_A$ and for $x, y \in A$, $\iota(xy) = \iota(y)\iota(x)$. An involution may be of the

First kind if for $x \in L$, $\iota(x) = x$,

Second kind if for $x \in L$, $\iota(x) = \sigma(x)$.

Fact

Let A be a central simple L-algebra, with involutions ι and ρ respectively of the first and second kind.
If $\iota \circ \rho = \rho \circ \iota$, then $\iota \circ \rho$ is a semi-linear Galois action on A.

Finding an involution of the second kind (part one)

Let L/K be separable quadratic. $\mathrm{Gal}(L/K) = \{Id, \sigma\}$. Let A be a central simple L-algebra.

Definition

$A^\sigma = A \otimes_L L^\sigma$. It has the structure constants of A conjugated by σ.

Definition

$N_{L/K}(A)$ is the K-algebra of fixed points by the "switch" involution in $A^\sigma \otimes A$.

Theorem (Albert, Riehm, Scharlau)

The following are equivalent:

1. There is an involution of the second kind on A which leaves K invariant.
2. The norm algebra $N_{L/K}(A)$ is split.

Finding an involution of the second kind (part two)

The algorithm

Input: An L-algebra A. Output: A zero divisor in A or an involution of the second kind over A.

1. Compute a maximal right ideal I in $N_{L/K}(A)$.
2. Let $I_L = I \otimes_K L \subset A^\sigma \otimes A$. Compute $I_L \cap 1 \otimes A$.
3. If $I_L \cap 1 \otimes A \neq \{0\}$, we have a zero divisor in A.
4. Otherwise, $I_L \oplus 1 \otimes A = A^\sigma \otimes A$.
5. Then, for $a \in A$, there is a unique $\rho(a)$ such that $a^\sigma \otimes 1 - 1 \otimes \rho(a) \in I_L$.
6. ρ is an involution of the second kind on A.

Putting things together

The algorithm

Input: Two quaternion L-algebras A_1 and A_2 such that $A = A_1 \otimes_L A_2 \simeq M_4(L)$. We assume that K is a global fields. Output: A zero divisor in A or a K-subalgebra which contains one.

1. Compute either an involution of the second-kind ρ or a zero divisor.
2. If you have an involution of the second kind, find a conjugate ι of $\iota_1 \circ \iota_2$ which commutes with ρ.[a]
3. Compute $A_K = A^{\iota \circ \rho}$.
4. Either $A_K \simeq M_4(K)$ or $A_K \simeq M_2(D)$ with D a division quaternion algebra.

[a] This part is under revision after we found an error.

Caveat

Although polynomial, the reduction is made impractical by the cost of computing a maximal order in a degree 16 algebra.

Function fields: a geometric approach

Let K be the function field of a regular curve X over $\mathbb{F}_q$. Let $A \simeq M_n(K)$

Differences with $\mathbb{Q}$

- Replace $\mathbb{Z}$ with X
- An X-order O of a K-algebra A is a locally free $\mathcal{O}_X$-algebra generically isomorphic to A.

Fact

Let $\mathcal{A}$ be an $\mathcal{O}_X$-algebra. Then, the following are equivalent:

1. $\mathcal{A}$ is a maximal X-order in $M_n(K)$.
2. $\mathcal{A}$ is an Azumaya algebra of degree n over X.
3. $\mathcal{A} \simeq \mathcal{E}\mathrm{nd}(V)$ for some rank n vector bundle over X.

The genus 0 case

Here, $K = \mathbb{F}_q(X)$ is the field of rational functions.

Theorem

Let O be a maximal X-order in A. Then the $\mathbb{F}_q$-algebra $H^0(X, O)$ is finite dimensional and contains a rank one idempotent

Proof

Let V be such that $O \simeq \mathcal{E}\mathrm{nd}(V)$. Then, by a theorem of Grothendieck, there are integers $d_1 \leq \ldots \leq d_n$ such that

$$V \simeq \mathcal{O}_X(d_1) \oplus \ldots \oplus \mathcal{O}_X(d_n).$$

Then, the map $Id_{\mathcal{O}_X(d_1)} \oplus 0_{\mathcal{O}_X(d_2)} \oplus \ldots \oplus 0_{\mathcal{O}_X(d_n)}$ has rank one and is defined everywhere.

Concrete algorithm

Algorithm

Let $A \simeq M_n(\mathbb{F}_q(X))$. Let R be the valuation ring for the degree valuation in $\mathbb{F}_q(X)$.

1. Compute O_{fi}, a maximal $\mathbb{F}_q[X]$-order in A.
2. Compute O_{inf}, a maximal R-order in A.
3. By the local-global principle, these yield a maximal X-order O.
4. Using lattice reduction, compute $C = H^0(X, O) = O_{fi} \cap O_{inf}$.
5. Split $C = J \oplus W$
6. Split $W = C_1 \oplus \ldots \oplus C_r$ as a sum of simple $\mathbb{F}_q$ algebras.
7. For each C_i, find a maximal orthogonal family of idempotents.
8. One of them must have rank one in A.

A fine line between genus and insanity

Bad news!

For curves of higher genera, there are indecomposable vector bundles of higher rank.

Theorem (Atiyah, Tillmann, Arason, Elman, Jacob, Pumplün)

Let X be an elliptic curve over k. Let $\overline{\mathcal{E}}_X(r,d)$ be the set of *absolutely indecomposable* (*i.e* indecomposable over $\overline{k}$) vector bundles of rank r and degree d verifies

$$\overline{\mathcal{E}}(r,d) \simeq X(k).$$

Different approach: understanding the indecomposables

Recall

Let $A \simeq M_n(K)$, let $O \simeq \mathcal{E}\mathrm{nd}(V)$ be a maximal X-order in A, with X a smooth model for K.
If $H^0(X, \mathcal{O})$ contains no zero-divisor, then V is an indecomposable vector bundle.

Idea

For each isomorphism class of indecomposable vector bundles V, find a line bundle $\mathcal{L}_V$ such that $H^0(X, \mathcal{E}\mathrm{nd}(V)) \otimes \mathcal{L}_V$ is small and contains a rank one idempotent.

Note

From this point on, this is joint ongoing research, in collaboration with Péter Kutas and Aurel Page.

Implementing the idea: Genus 1

Recall

1. $\overline{\mathcal{E}}_X(r,d)$ is the set of isomorphism classes of absolutely indecomposable vector bundles over X of rank r and degree d.
2. $\mathcal{E}_X(r,d)$ is the set of isomorphism classes of indecomposable vector bundles of rank r and degree d.

Recall Atiyah's result

For $r, d \in \mathbb{N}$, there is a bijection $\overline{\mathcal{E}}(r,d)$.
Furthermore, fix a divisor D of degree 1. There is a bijection

$$\begin{array}{ccc} \overline{\mathcal{E}}(r,d) & \to & \overline{\mathcal{E}}(r,d+r) \\ V & \mapsto & V \otimes \mathcal{L}(D) \end{array}.$$

Fact

An indecomposable vector bundle of rank r over X is the restriction of scalars of an absolutely indecomposable vector bundle on X_L, for some finite extension L/K of degree dividing r.

Consequences

Upshot

The size of the set of isomorphism classes of maximal X-orders in $M_n(K)$ with no idempotent global section is bounded by a polynomial in q.

Strategies

1. If possible, construct these orders for the generic elliptic curve $X : y^2 = x^3 + Ax + B$ over $\mathbb{F}_q[A, B]$ and derive general formulas for line bundles to twist with and find global rank one idempotents.
2. For a given curve X, compute line bundles $\mathcal{L}_V$ to cover each maximal X-order O with no global zero-divisor.

Main takeaways

Theorem (Csahók, Kutas, Zábrádi, M))

There is[a] a polynomial reduction from splitting biquaternion algebras over a quadratic extension of a global field to splitting central simple algebras (of degree ≤ 16) on the base field.

[a] Provided our revision is successful

Ongoing work (Kutas,Page,M)

There might be an f-algorithm for the isomorphism problem over function fields of elliptic curves

Future work

We need a faster algorithm for computing maximal orders!

Thank you very much to the organisers and the audience.