The splitting problem in central simple algebras

Mickaël Montessinos
(Vilnius University)[1]

Atelier PARI/GP 2024
Tuesday 9th January, 2024

[1] Joint implementation work with Abdelrahman Zighem

The matter at hand

Structure constants

Let k be a field, $V = k^n$ with canonical basis $(e_1, \dots, e_n)$.
A k-algebra structure on V is given by a family $c \in V^3 \simeq (V^\wedge)^{\otimes 2} \otimes V$ 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 assumed to be isomorphic to $M_n(k)$. Find an explicit isomorphism

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

From zero divisor to hero divisor

Reduction

The explicit isomorphism problem reduces to finding a rank one element.

Example

Consider the quaternion algebra $A = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$ 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 φ and compute the image of ij:

1. $z = i - 1$ is a zero-divisor. The space $V = Az$ 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.
3. We compute: $ije_1 = -j - ij = -e_2$ and $ije_2 = i - 1 = e_1$.
4. We obtain: $\varphi(ij) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Pilnikova's algorithm for algebras of degree 4

Input A $\mathbb{Q}$-algebra $A \simeq M_4(\mathbb{Q})$.

Output A rank one zero divisor in A.

1. Find a quadratic element $a \in A$.
2. The centralizer C of a in A is a split quaternion algebra over $\mathbb{Q}(a)$. Find a quaternionic basis.
3. Find a zero divisor $z \in C$ (Either solve a square root/norm equation or use Kutas' algorithm).
4. If $\operatorname{rank} z = 1$, return z.
5. Let e be a right unit of the left ideal Az.
6. If $\operatorname{rank} e = 3$, return $1 - e$.
7. Else, find a zero divisor in quaternion $\mathbb{Q}$-algebra eAe.

Ivanyos et al's general degree algorithm

Input A $\mathbb{Q}$-algebra $A \simeq M_n(\mathbb{Q})$.

Output A rank one zero divisor in A.

1. Compute a maximal order $\mathcal{O}$ in A.
2. Compute an embedding ϵ of A into $M_n(\mathbb{R})$.
3. Compute embedding ϵ with the appropriate precision.
4. $\epsilon(\mathcal{O})$ is a lattice in $M_n(\mathbb{R})$. Compute an LLL-reduced basis $\mathcal{B}$ of $\epsilon(\mathcal{O})$
5. If $n > 43$ and some $b \in \mathcal{B}$ is a zero divisor, either return b if rank $b = 1$ or use b to compute an idempotent e and recursively apply the algorithm to algebra eAe of degree equal to rank e.
6. Look for a rank one element in $\bigoplus_{b\in\mathcal{B}}[0\,..\,c_{n^2}\sqrt{n}]b$, where $c_m = \gamma_m^{\frac{m}{2}}\left(\frac{3}{2}\right)^m 2^{\frac{m(m-1)}{2}}$, and γ_m is Hermite's constant.