Explicit isomorphisms of quaternion algebras over quadratic global fields

Tímea Csahók, Péter Kutas, Mickaël Montessinos, Gergely Zábrádi

11th August 2022, ANTS XV, Bristol

Finite-dimensional algebras

- An algebra over a field K is a vector space that is also a ring
- Finite dimensional, if it is finite dimensional as a K-vector space
- Radical: intersection of all maximal left ideals (equivalently, collection of strongly nilpotent elements)
- Simple: No nontrivial two-sided ideals
- $A/Rad(A)$ is the direct sum of simple algebras (as they are automatically Artinian)
- Simple algebra is isomorphic to $M_n(D)$ where D is a division algebra

Algorithmic problems

- In our models the algebra is represented by a K-basis and a multiplication table (structure constant representation)
- Motivation for such a representation: computational representation theory
- Natural problem: compute the structure of the algebra, in this lecture we focus on the case where K is a global field
- Computing the radical $\rightarrow$ polynomial-time
- Computing the semisimple components $\rightarrow$ can be reduced to factoring polynomials in $K[x]$
- The hardest part is computing explicit isomorphisms between a simple algebra and $M_n(D)$

Brauer group

- Central simple K-algebra: a simple algebra whose center is exactly K
- Two central simple K-algebras A, B are Brauer-equivalent if they are isomorphic to $M_n(D)$ and $M_m(D)$ respectively
- Brauer classes of central simple K-algebras form a group under the tensor product
- The identity is the class of K and inverse is provided by the opposite algebra
- The Brauer group is actually isomorphic to $H^2(G, \overline{K})$ where G is the absolute Galois group of K (important for later)
- The isomorphism problem between A and B can be reduced to finding an explicit isomorphism between $A \otimes B^{op}$ and a full matrix algebra $M_n(K)$

Applications

- Solving norm equations in cyclic extensions: $A = (L|K, \sigma, \gamma)$ where $\gamma \in K$; then A is isomorphic to $M_n(K)$ iff γ is in the image of the norm map
- Finding an explicit isomorphism is equivalent to solving the norm equation
- Finding K-rational points on conics is a special case of this
- Explicit n-descent on elliptic curves: a procedure that allows you to compute the generators of $E(K)/nE(K)$ (Cremona, Fisher, O'Neil, Simon, Stoll)
- The key step is finding an explicit isomorphism between $M_n(K)$ and an object called the obstruction algebra
- Parametrizing Severi-Brauer varieties
- Factoring Ore-polynomials

Some remarks

- If $A \cong M_n(K)$, then the rank of a matrix m is just $dim(\{xm|x \in A\})/n$
- Finding an explicit isomorphism is equivalent finding a rank 1 element
- Finding a zero divisor reduces the problem to a smaller instance as for an idempotent of e of rank k one has that $eAe \cong M_k(K)$
- So from now on I will talk mostly on finding zero divisors
- Hardness: one is looking for an element in a Zariski closed set

Previous work

- If $A \cong M_2(\mathbb{Q})$, then the problem is equivalent to factoring (Rónyai, Ivanyos, Szántó, Cremona, Rusin, Simon, Voight)
- When $A \cong M_n(K)$ and K is a number field, then there is an algorithm that is polynomial in the size of the structure constants and exponential in every other parameter (Ivanyos,Rónyai,Schicho)
- When $A \cong M_n(K)$ and $K = \mathbb{F}_q(t)$, then there exists a polynomial-time algorithm (Ivanyos, K., Rónyai)
- When $A \cong M_2(L)$ and L is a quadratic extension of $\mathbb{Q}$ then there is a polynomial-time algorithm modulo factoring (K., Fisher)
- When $A \cong M_2(L)$ and L is a quadratic extension of $\mathbb{F}_q(t)$ and q is odd then there is a polynomial-time algorithm

This work

- We study the isomorphism problem of two quaternion algebras over quadratic global fields
- Not covered by previous research as the tensor product of the two quaternion algebras is isomorphic to $M_4(K)$
- We also include the characteristic 2 case
- The methods used give a more conceptual proof/algorithms of previous work
- We also provide a Magma implementation
- Key idea: a form of explicit Galois descent

Corestriction of central simple algebras

- The Brauer group is isomorphic to a second cohomology group hence one has restriction and corestriction on the cohomology side
- Restriction just corresponds to extensions of scalars
- Let $L|K$ be a separable quadratic extension, then corestriction maps a central simple L-algebra to a central simple K-algebra
- This is not quite obvious how to do this on the level of algebras, we will define it for quadratic extensions

Corestriction of central simple algebras II

- Let $L|K$ be a separable quadratic extension and let σ be the generator of the Galois group
- Let A be a central simple L-algebra and define A^σ as the set of symbols $\{a^\sigma | a \in A\}$ with the rules $a^\sigma b^\sigma = ab^\sigma$, $a^\sigma + b^\sigma = (a+b)^\sigma$ and $(\alpha b)^\sigma = \sigma(\alpha) b^\sigma$ for every $\alpha \in L$
- Now there is a switch map on $A^\sigma \otimes A$ that sends an elementary tensor $a^\sigma \otimes b$ to $b^\sigma \otimes a$ and this can be extended K-linearly
- Fixed elements of the switch map form a central simple K-algebra which is the called the corestriction of A
- Problem: does not give you Galois descent as it is not a subalgebra of A

Involutions

- An involution of a CSA is a linear map that has order two and reverses multiplication
- Restricted to the center it is an automorphism of order at most 2
- When it fixes the center then it is called an involution of the first kind,otherwise an involution of the second kind
- Let $L|K$ be a separable quadratic extension and let A be a central simple L-algebra. Then A possesses an involution of the second kind if and only if its corestriction is split

Computing an involution of the second kind

- The above theorem is explicit
- If you find a right ideal I of the corestriction such that $A^\sigma \otimes_L A = I_L \oplus (1 \otimes A)$, then you can construct an involution of the second kind explicitly
- A maximal right ideal will satisfy that most of the time
- If not, then you have found a zero divisor in A
- Finding a maximal right ideal is exactly the same problem as finding a rank 1 element in the corestriction

Main algorithm I

- In order to find an explicit isomorphism between two quaternion algebras A, B (over L) it is enough to find a rank 1 element in $A \otimes B^{op}$
- $A \otimes B^{op}$ comes equipped with an involution σ_1 of the first kind as it is a product of quaternion algebras
- One can compute an involution of the second kind σ_2 by finding a maximal right ideal in the corestriction or a zero divisor (if one finds the latter than we are done)
- This works because the corestriction is a central simple K-algebra (although its dimension is higher)

Main algorithm II

- Now one can compute the composition of σ_1 and σ_2 and take the set of invariant elements
- The set of invariant elements C is a Galois descent (a central simple K-subalgebra such that $C \otimes_K L = A \otimes B^{op}$)
- Since C is split by a quadratic extension it can't be a division algebra
- Hence C is either $M_2(D)$ or $M_4(K)$
- One can use existing subroutines for finding a zero divisor in C (from a zero divisor one can also find a rank 1 element efficiently)

Important subroutines

- Finding zero divisors in an algebra B isomorphic to $M_2(L)$
- Finding zero divisors in an algebra B isomorphic to $M_4(K)$
- Finding zero divisors in $M_2(D)$,where D is a quaternion algebra over K
- Finding rank 1 elements in an algebra B isomorphic to $M_{16}(K)$
- This reductions work over any field essentially and they all admit polynomial-time algorithms for the rationals and rational function fields

Implementation

- Every algorithm runs in polynomial time (the number field one modulo factoring) but the IRS algorithm has a huge hidden constant, hence we opted for implementing the function field case (in odd characteristic)
- The main algorithm for finding maximal right ideals in $M_n(\mathbb{F}_q(t))$ relies on computing maximal orders which is a polynomial-time algorithm
- Unfortunately, the maximal order algorithm in Magma scales very poorly and here we needed to compute a maximal order in a CSA of dimension 256 (degree 16) as that is the dimension of the corestriction
- We provided some optimization tricks which bring down the asymptotic complexity of maximal order computation significantly
- The main idea is that $A \otimes B^{op}$ comes equipped with rather large order that maps to a rather large order in the corestriction

Open problems

- Find better algorithms for computing maximal orders
- Can the Galois descent approach be generalized to cyclic extensions?
- The current approach is somehow a double twist, does there exists a more direct approach?
- Potential applications: if one has a split quaternion algebra over an odd cyclic extension L of $K = \mathbb{Q}$ or $K = \mathbb{F}_q(t)$, then finding a Galois descent immediately leads to zero divisor (can be used to find L-rational points on conics)
- Similarly might improve on current algorithms for certain norm equations