Computing the Cassels-Tate pairing

Tom Fisher

DPMMS
University of Cambridge

CNTA XV Laval University 10^{th} July 2018

Central simple algebras

Definition. Let A be a finite dimensional associative K-algebra.

$$A \text{ is a } \textit{central simple algebra} \iff A \otimes_K \overline{K} \cong \mathrm{Mat}_n(\overline{K})$$

We may represent A by n^6 structure constants $c_{ijk} \in K$, i.e. if A has basis $x_1, \ldots, x_{n^2}$ then $x_i x_j = \sum_k c_{ijk} x_k$.

Trivialisation problem. Given A known to be isomorphic to $\mathrm{Mat}_n(\mathbb{Q})$ find such an isomorphism explicitly. (N.B. $n = 2 \leftrightarrow$ solving a conic.)

Isomorphism problem. Given A_1 and A_2 central simple algebras over $\mathbb{Q}$, that we know are isomorphic, find such an isomorphism explicitly.

Central simple algebras (ctd)

Trivialisation problem. Given A known to be isomorphic to $\mathrm{Mat}_n(\mathbb{Q})$ find such an isomorphism explicitly.

Method of solution. See Cremona, F., O'Neil, Simon, Stoll (2015) and Ivanyos, Rónyai, Schicho (2011).

(i) Compute a maximal order $\Lambda \subset A$.
(ii) Compute a real trivialisation $A \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{Mat}_n(\mathbb{R})$.
(iii) Look for short vectors in the lattice $\Lambda \subset \mathbb{R}^{n^2}$.
If we find a zerodivisor then the problem reduces to a smaller one (i.e. n replaced by a proper divisor).

Remark. $\exists$ analogue over number fields K. However unless n and K are both small then Step (iii) is impractical.

Central simple algebras (ctd)

Isomorphism problem. Given A_1 and A_2 central simple algebras over $\mathbb{Q}$, that we know are isomorphic, find such an isomorphism explicitly.

Method of solution. Reduce to trivialisation problem using

$$A_1 \cong A_2 \iff A_1 \otimes A_2^{\mathrm{op}} \cong \mathrm{Mat}_{n^2}(\mathbb{Q}).$$

Suppose $\mathrm{Gal}(L/K) \cong C_n = \langle \sigma \rangle$ and $b \in K^\times$. The *cyclic algebra* $(L/K, b)$ is $\{a_0 + a_1 v + \ldots + a_{n-1} v^{n-1} | a_i \in L\}$ with multiplication determined by $va = \sigma(a)v$ for all $a \in L$, and $v^n = b$.

$$\frac{K^\times}{N_{L/K}(L^\times)} \cong \mathrm{Br}(L/K) := \ker(\mathrm{Br}(K) \to \mathrm{Br}(L))$$
$$b \mapsto (L/K, b)$$

Descent on elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve and $n \geq 2$ an integer.

$$\begin{array}{ccccccccc} E(\mathbb{Q}) & \xrightarrow{\times n^2} & E(\mathbb{Q}) & \longrightarrow & S^{(n^2)}(E/\mathbb{Q}) & \longrightarrow & Ш(E/\mathbb{Q})[n^2] & \longrightarrow & 0 \\ \downarrow{\scriptstyle \times n} & & \| & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \times n} & & \\ E(\mathbb{Q}) & \xrightarrow{\times n} & E(\mathbb{Q}) & \longrightarrow & S^{(n)}(E/\mathbb{Q}) & \longrightarrow & Ш(E/\mathbb{Q})[n] & \longrightarrow & 0 \end{array}$$

Cassels-Tate pairing

$$\langle \ , \ \rangle_{\mathrm{CT}} : S^{(n)}(E/\mathbb{Q}) \times S^{(n)}(E/\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$$

Properties: bilinear, alternating, kernel is $\mathrm{im}(\alpha)$.

Computing $\langle \ , \ \rangle_{\mathrm{CT}}$ improves our upper bound on rank $E(\mathbb{Q})$ coming from n-descent to that coming from n^2-descent.

Previous work

	$n = 2$	$n = 3$
n^2-descent	Siksek (1995) Womack (2003) Stamminger (2005)	Creutz (2010)
CTP via Weil pairing definition	Cassels (1998)	F., Newton (2014)
CTP via homogeneous space definition	Donnelly (2015)	**This talk**

CTP on 2-power isogeny Selmer groups: F. (2017).
CTP on 3-isogeny Selmer groups: van Beek (2015).

An example (via the Brauer-Manin obstruction)

$$E = 1913b1 : \qquad y^2 + xy = x^3 + x^2 - 34x - 135$$

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \qquad Ш(E/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^2$$

One of the non-trivial elements in $S^{(3)}(E/\mathbb{Q})$ is represented by $C = \{f_1(x, y, z) = 0\} \subset \mathbb{P}^2$ where

$$f_1 = x^3 + y^3 + z^3 - xy^2 + y^2 z + xz^2 + 5yz^2 + xyz.$$

A proof that $C(\mathbb{Q}) = \emptyset$.
Let $L = \mathbb{Q}(\zeta_7) \cap \mathbb{R}$ and $g = 3x^3 + 4x^2 y + 7x^2 z - 6xy^2 + 3y^3$.
Let $\mathcal{A} = (L/\mathbb{Q}, g) \in \mathrm{Br}(\mathbb{Q}(C))$.
We find that $\mathcal{A} \in \mathrm{Br}(C)$ and for every $P_p \in C(\mathbb{Q}_p)$

$$\mathrm{inv}_p(\mathcal{A}(P_p)) = \begin{cases} 0 & \text{if } p \neq 7 \\ 1/3 & \text{if } p = 7 \end{cases}$$

But if $P \in C(\mathbb{Q})$ then $\sum_p \mathrm{inv}_p(\mathcal{A}(P)) = 0$ by class field theory.

How did we find $\mathcal{A} = (L/\mathbb{Q}, g)$?

Let C, D be plane cubics representing elements of $S^{(3)}(E/K)$.

Method to compute $\langle [C], [D] \rangle_{CT}$**.**
(i) Find a K-rational line meeting $D \subset \mathbb{P}^2$ in a point $P_D \in D(L)$ where L/K is a cyclic cubic extension, say $\mathrm{Gal}(L/K) = \langle \sigma \rangle$.
(ii) Let $H \in \mathrm{Div}^3_K(C)$ be a hyperplane section. Find $H' \in \mathrm{Div}^3_L(C)$ such that

$$\begin{aligned} \mathrm{Pic}^0(C) &\cong \mathrm{Pic}^0(D) \\ [H' - H] &\leftrightarrow [P_D - \sigma(P_D)] \end{aligned}$$

(iii) Solve for $g \in K[x, y, z]$ a cubic form with

$$C \cap \{g = 0\} = H' + \sigma H' + \sigma^2 H'.$$

Then

$$\frac{H^1(K, E)}{\langle [C] \rangle} \cong \frac{\mathrm{Br}(C)}{\mathrm{Br}(K)}$$

$$[D] \mapsto (L/K, g) =: \mathcal{A}$$

and $\langle [C], [D] \rangle_{CT} = \sum_v \mathrm{inv}_v \, \mathcal{A}(P_v)$.

Remarks on Step (i)

Let D/K be a plane cubic with $D(K_v) \neq \emptyset$ for all v.

(i) Find a K-rational line meeting $D \subset \mathbb{P}^2$ in a point $P_D \in D(L)$ where L/K is a cyclic cubic extension.

If $D(K) \neq \emptyset$ then the pairing is trivial. Otherwise, intersecting with a line gives a point $P_D \in D(L)$ for L/K a Galois extension with $\mathrm{Gal}(L/K) \cong C_3$ or S_3.

It is an open question whether cubic points always exist, related to the arithmetic of K3 surfaces: see van Luijk (2011).

If they don't always exist, or are hard to find, then the fall-back is to replace our base field K by a quadratic extension. This won't destroy the pairing we are trying to compute, but will make all the computations harder.

Remarks on Step (ii)

Recall that $\mathrm{Gal}(L/K) \cong C_3 = \langle \sigma \rangle$.

Step (ii) comes down to the trivialisation problem for a 9-dimensional central simple algebra A over L.

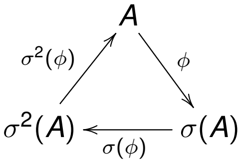
Two methods to construct A:

- via theta groups (Cremona, F., O'Neil, Simon, Stoll, 2008)
- via generators and relations (Kuo, 2011)

Lemma. If $[C] + [D] = [C']$ for some plane cubic C' (as always happens for Selmer group elements) then $A \cong \sigma(A)$.

Using a combination of the above two constructions I can write down a specific isomorphism $\phi : A \to \sigma(A)$.

Conjecture. The diagram



commutes.

Assuming the conjecture we have $A \cong A_0 \otimes_K L$ for some K-algebra A_0. However, even in cases where $A \cong \mathrm{Mat}_3(L)$ we need not have $A_0 \cong \mathrm{Mat}_3(K)$.

Two possible solutions.

- Find a better choice of ϕ.
- By computing the local invariants of A_0, solve for $b \in K^\times$ such that $A_0 \cong (L/K, b)$. The trivialization problem over L is then reduced to the isomorphism problem over K.

THE END