HOW TO TRIVIALISE A CENTRAL SIMPLE ALGEBRA

TOM FISHER

Let K be a field. Let A be a finite-dimensional associative K-algebra with 1 with basis $a_1, \ldots, a_d$, given by a list of structure constants c_{ijk} such that $a_i a_j = \sum_{k=1}^d c_{ijk} a_k$ for $i, j = 1, \ldots, d$.

Problem: Determine whether $A \simeq \mathrm{Mat}_n(K)$ for some n, and if so, find an isomorphism explicitly.

We may assume that $d = n^2$.

Remarks 1.

(i) We may assume the following, since otherwise the answer is clearly no:
- A is central (i.e., the centre is K)
- A is simple (i.e., no 2-sided ideals)

(ii) Wedderburn: Then $A \simeq \mathrm{Mat}_r(D)$ where $r \geq 1$ and D is a skew field with centre K. We have $[A : K] = r^2[D : K]$.

Consequence: If $[A : K] = p^2$, then $A \simeq \mathrm{Mat}_p(K)$ if and only if A contains a zero-divisor.

Algorithmic version: Every left A-module is isomorphic to $M \oplus \cdots \oplus M$ where M is the unique (faithful) simple left A-module. Assume A contains a zero-divisor. Then $[M : K] = p$. Given a zero-divisor $x \in A$, put $N_1 = Ax$. Then $N_1 \simeq M^s$ with $0 < s < p$. Construct a sequence $N_1, N_2, \ldots$ of nonzero left A-modules of decreasing dimension. Initially taking $B = A$, pick $0 \neq \phi \in \mathrm{Hom}_A(N_i, B)$. If ϕ is not injective, take $N_{i+1} = \ker(\phi)$. Otherwise, replace B by $\mathrm{coker}(\phi)$, and choose a new ϕ. Consequence: we construct M. Then $A \simeq \mathrm{End}_K M = \mathrm{Mat}_p(K)$.

Remark 2. If $a \in A$ has reducible minimal polynomial $m(x) = m_1(x)m_2(x)$, then $m_1(a)$ is a zerodivisor.

Let K be a number field. Then class field theory (local-global principle) implies that if $A \otimes_K K_v \simeq \mathrm{Mat}_n(K_v)$ for all places v, then $A \simeq \mathrm{Mat}_n(K)$.

Consider the case $K = \mathbb{Q}$ and $n = 3$.

Step 1: Compute a maximal order $\mathcal{O} \subset A$: this will be conjugate to $\mathrm{Mat}_3(\mathbb{Z})$.

Step 2: Trivialise over $\mathbb{R}$. View $A \subset \mathrm{Mat}_3(\mathbb{R})$.

Step 3: Find a shortest vector M in the lattice $\mathcal{O} \subset \mathrm{Mat}_3(\mathbb{R}) = \mathbb{R}^9$.

Theorem 3. *M is a zerodivisor.*

Proof. We have $\mathcal{O} = P^{-1}\,\mathrm{Mat}_3(\mathbb{Z})P$ where $P \in \mathrm{GL}_3(\mathbb{R})$. Therefore $\mathcal{O}$ has covolume 1. So $\|M\|^2 \leq \gamma_9$, where γ_9 is the Hermite constant: $\gamma_9 < 2.2406\ldots$. Thus $\|M\|^2 < 3$. Write $M = QR$, where Q is orthogonal and R is upper triangular with diagonal entries r_1, r_2, r_3. Then $|\det M|^{2/3} = \left(\prod_{i=1}^3 r_i^2\right)^{1/3} \leq \frac{1}{3}\sum_{i=1}^3 r_i^2 \leq \frac{1}{3}||M||^2 < 1$. So $|\det M| < 1$. But $\det M \in \mathbb{Z}$. Therefore $\det M = 0$. $\square$

Date: July 22, 2007.