Trivializing a central simple algebra of degree 4 over the rational numbers

Jana Pílniková

RICAM, Austrian Academy of Sciences, Altenbergerstrasse 69, A-4040 Linz, Austria

Received 10 January 2006; accepted 8 January 2007
Available online 17 January 2007

Abstract

We give an algorithm for finding an isomorphism of a given central simple algebra of degree 4 over the rationals and the full matrix algebra, provided it exists. It reduces the task to classical problems in number theory, for which there are already known algorithms.

Keywords: Central simple algebra; Zero divisor

1. Introduction

A central simple algebra $A$ is a finite-dimensional algebra over a field $F$ such that the center $C(A)$ is isomorphic to $F$ and there are no nontrivial two-sided ideals. By Wedderburn’s theorem on the structure of central simple algebras, any such algebra is isomorphic to $M_n(\Delta)$ for a unique $n \in \mathbb{N}$ and a central division algebra $\Delta$ over $F$ which is defined up to isomorphism. The dimension of any central simple algebra is always a square; therefore we can talk about the degree of the algebra, which is the integer $\sqrt{[A:F]}$, where $[A:F]$ denotes the dimension of $A$ as an $F$-vector space.

In the algorithm described in this paper we assume that the given central simple algebra of degree 4 is isomorphic to $M_4(\mathbb{Q})$. There are already efficient algorithms for deciding whether a given central simple algebra over $\mathbb{Q}$ is isomorphic to a full matrix algebra (see for example Ivanyos and Rónyai (1993)). Nevertheless, the decision algorithms, like the one mentioned above, do not give an explicit isomorphism in the case where it exists.
The problem addressed by the paper is related to finding minimal irreducible module of a representation of the algebra. Since the algebra $A$ is simple, its regular representation is faithful. Any left ideal in $A$ is a 4-dimensional submodule in the natural $M_{16}(\mathbb{Q})$-module afforded by the regular representation. Finding an isomorphism $A \to M_4(\mathbb{Q})$ is therefore equivalent to finding an irreducible $A$-submodule in the 16-dimensional module. For case of group algebras the Meat-Axe in characteristic zero (see Parker (1998)) gives relevant algorithms. Similarly to our approach, a zero divisor in the algebra is found and used afterwards for finding an irreducible module. But the Meat Axe relies on finding a zero divisor by random choice. In our work we give a deterministic algorithm which finds such element.

Effective algorithms are known for finding an isomorphism of a given central simple algebra of degree 2 with $M_2(\mathbb{Q})$, see Cremona and Rusin (2003), Ivanyos and Szántó (1996) and Simon (2005), some even implemented in Magma (Bosma et al., 1997). Construction of an isomorphism of an algebra of degree 3 with $M_3(\mathbb{Q})$ can be found in de Graaf et al. (2006). The same paper and the current one also give together an algorithm for finding an isomorphism over $\mathbb{Q}$ of a given Severi–Brauer threefold and the three-dimensional projective space.

The algorithm presented in the paper can be applied for any number field. Except the fast method of finding a zero divisor in $M_2(\mathbb{Q})$, which can be replaced by reduction to solving a norm equation (see Proposition 3), it does not use any special properties of the rational numbers.

Throughout the whole paper $A$ denotes an algebra over $\mathbb{Q}$ isomorphic to $M_4(\mathbb{Q})$ given for instance by structure constants.

2. Left ideals in $M_4(\mathbb{Q})$

Since $A \cong M_4(\mathbb{Q})$, it contains one-sided ideals. We will be focused mainly on left ideals. Every minimal left ideal in this algebra has dimension 4 and any nontrivial left ideal is a direct sum of minimal left ideals, and hence has dimension 4, 8 or 12.

Let $\mathcal{L}$ be a four-dimensional left ideal in $A$. For any $a \in A$ we have that $\varphi_a : \mathcal{L} \to \mathcal{L}$, $x \mapsto ax$ is an endomorphism of $\mathcal{L}$ as a vector space. Let us fix a basis $b_1, b_2, b_3, b_4$ of $\mathcal{L}$. Let $\varphi : A \to M_4(\mathbb{Q})$ assign to $a \in A$ the matrix of $\varphi_a$ with respect to this basis, i.e. the $i$-th column of $\varphi(a)$ contains the coordinates of $ab_i$, so $ab_i = \sum_j \varphi(a)_{ij}b_j$.

Proposition 1. $\varphi$ is an isomorphism of algebras.

Proof. Firstly, $\varphi$ is a homomorphism of algebras. Further $\varphi$ is a bijection, since otherwise $\ker \varphi \neq 0$ would be a nontrivial ideal in $A$. \hfill \Box

To make use of the theorem we have to find a four-dimensional left ideal in the algebra $A$. Here we achieve it by finding a suitable zero divisor. For any $d \in A$ we define the vector space endomorphism $\rho_d$ of $A$, $x \mapsto xd$. Then both the kernel and the image of $\rho_d$ are left ideals of $A$. If $d \in A$ is a zero divisor, $\ker \rho_d$ is clearly nontrivial, and the same with $\operatorname{Im} \rho_d$, since $1.d \neq 0$. If $\dim \ker \rho_d = 4$ or $\dim \operatorname{Im} \rho_d = 4$ or $\dim(\ker \rho_d \cap \operatorname{Im} \rho_d) = 4$, we are done since we can already use Proposition 1 and find an isomorphism $A \to M_4(\mathbb{Q})$. The remaining questions are how to use other kinds of zero divisors and how to find a zero divisor at all. This is solved in the rest of the paper.

3. Splitting a central simple algebra of degree 2

As a subproblem in our algorithm we will need to find an isomorphism of a given central simple algebra of degree 2 and full matrix algebra, once over $\mathbb{Q}$ and once over a quadratic
extension of \( \mathbb{Q} \). Finding an isomorphism over \( \mathbb{Q} \) is equivalent to finding a zero divisor in \( M_2(\mathbb{Q}) \) or to finding a rational point on a plane conic, and there are already algorithms for solving this; see for example Cremona and Rusin (2003), Ivanyos and Szántó (1996) and Simon (2005).

For finding an isomorphism of the algebra \( B \) and \( M_2(\mathbb{F}) \), \( \mathbb{F} \) being a quadratic extension of \( \mathbb{Q} \), we first try to write \( B \) as a cyclic algebra.

**Definition 2.** \( B \) is a cyclic algebra of degree 2 if there are elements \( c, u \in B \) so that \( 1, c, u, cu \) is a basis of \( B \) over its ground field \( \mathbb{F} \) and the multiplication in \( B \) is defined by the following:

(i) \( 1, c \) is a basis of a quadratic field extension \( \mathbb{E} \) of \( \mathbb{F} \),
(ii) \( uc = \sigma(c)u \), where \( \sigma \) is the nontrivial automorphism of \( \mathbb{E} \) over \( \mathbb{F} \),
(iii) \( u^2 = \gamma 1 \), where \( \gamma \in \mathbb{F}^* \).

We will call \( c \) a cyclic element and \( u \) a principal generator of \( B \) over \( \mathbb{F}(c) \).

When looking for a cyclic element \( c \) we pick an arbitrary noncentral element in \( B \). Its minimum polynomial \( \mu_c(\xi) \) is quadratic. In the case where it is reducible over \( \mathbb{F} \), \( \mu_c(\xi) = p_1(\xi)p_2(\xi) \), we have also found a zero divisor, namely \( p_1(c) \), and can construct an isomorphism \( B \to M_2(\mathbb{F}) \) as described in Section 2, using the two-dimensional left ideal \( \text{Ker} \rho_{p_1(c)} \). Otherwise \( c \) generates in \( B \) a quadratic field extension of \( \mathbb{F} \). By factoring \( \mu_c(\xi) \) over \( \mathbb{E} = \mathbb{F}(c) \) we find \( \sigma(c) \).

Then we find a principal generator \( u \) by solving the linear system of equations \( uc = \sigma(c)u \). There exists such invertible \( u \), because the matrices \( c \) and \( \sigma(c) \) have the same invariant factors and therefore are similar; cf. Wedderburn (1964). Finally, since \( c \) and \( u \) are generators of \( B \) and \( u^2c = cu^2 \), it follows \( u^2 \in \mathbb{C}(B) \cong \mathbb{F} \).

**Proposition 3.** Let \( B \) be a cyclic algebra of degree 2 generated by \( c, u \) as in **Definition 2**. Then \( B \cong M_2(\mathbb{F}) \) if and only if there exists \( s \in \mathbb{E} \subset B \) such that

\[
\sigma(s) = \frac{1}{\gamma} \tag{1}
\]

where \( \mathbb{F} \), \( \mathbb{E} \), \( \sigma \) and \( \gamma \) are as in **Definition 2**.

**Proof.** A proof for cyclic algebras of arbitrary degree can be found for example in Pierce (1982), Section 15.1. Nevertheless for the sake of completeness, we give here a proof for algebras of degree 2.

Since \( B \) is a central simple algebra of degree 2, by Wedderburn’s structure theorem it can be either \( M_2(\mathbb{F}) \) or a division algebra over \( \mathbb{F} \). It is the matrix algebra exactly if it has a two-dimensional left ideal. Let \( \mathcal{L} \) be such an ideal and let \( 0 \neq c_01+c_1u \in \mathcal{L}, c_1 \in \mathbb{E} = \mathbb{F}(c) \). Then \( c_0 \) is nonzero, for otherwise \( u \cdot c_1u \) would be an invertible element in \( \mathcal{L} \). Therefore we may suppose \( c_0 = 1 \) and then \( \mathcal{L} \) is spanned by \( 1 + c_1u \) and \( c(1 + c_1u) \). From \( u(1 + c_1u) = \sigma(c_1)\gamma + u \in \mathcal{L} \) we get that \( c_1 \) is a solution to the norm equation (1). On the other hand, if \( s \in \mathbb{E} \) solves the norm equation (1), then \( 1 + su \) generates a two-dimensional left ideal in \( B \). \( \Box \)

**Remark 4.** Note that the proof of the previous theorem delivers also an algorithm for finding an isomorphism of a cyclic algebra \( B \) and \( M_2(\mathbb{F}) \): if the norm equation (1) is solvable, then by the theorem we have \( B \cong M_2(\mathbb{F}) \) and using a solution of the norm equation we can construct a two-dimensional left ideal.

There are algorithms for finding a solution to the norm equation (1); see Garbanati (1980) and Simon (2002). This step turns out to be the bottleneck of the algorithm.
4. Using a zero divisor

Recall that for a zero divisor $d \in A$ both the kernel and the image of the vector space endomorphism $\rho_d$ of $A$, $x \mapsto xd$ are nontrivial left ideals.

Lemma 5. Let $\varphi: A \to M_4(\mathbb{Q})$ be an isomorphism and let $d \in A$ be a zero divisor such that none of $\text{Ker} \rho_d$, $\text{Im} \rho_d$, $\text{Ker} \rho_d \cap \text{Im} \rho_d$ has dimension 4. Then $\varphi(d)$ is similar to one of the following block matrices:

\[
(1) \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}, \text{ where } D \in M_2(\mathbb{Q}) \text{ is an invertible matrix,}
\]
\[
(2) \begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix}, \text{ where } B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.
\]

Proof. We consider the Jordan normal form of $\varphi(d)$. Since $\dim \text{Ker} \rho_d = 8$, we can conclude that $\varphi(d)$ has at most two nonzero eigenvalues. Therefore the minimum polynomial $\mu_d(\xi)$ is reducible and divisible by $\xi^2$. If $\mu_d(\xi) = \xi^4$, then we get the case (2) for the Jordan normal form of $\varphi(d)$. If $\xi$ appears in $\mu_d(\xi)$ in degree 3 (i.e. $\varphi(d)$ has exactly one nonzero eigenvalue), then at least one of the three left ideals $\text{Im} \rho_d$, $\text{Ker} \rho_d \cap \text{Im} \rho_d$ is four dimensional. Lastly, if $\xi$ appears in $\mu_d(\xi)$ exactly in degree 2, we get that the case (1). \qed

If $\text{Ker} \rho_d \cap \text{Im} \rho_d = 0$, then $d$ is a zero divisor of type (1) in Lemma 5. We define another vector space endomorphism $\lambda_d$ of $A$, $x \mapsto dx$. The intersection $A_1 = \text{Im} \rho_d \cap \text{Im} \lambda_d$ is mapped by $\varphi$ to the subalgebra of all block matrices, where only the upper left $2 \times 2$ block in nonzero, so $A_1 \cong M_2(\mathbb{Q})$. We find a zero divisor $d_1$ in $A_1$ as mentioned in Section 3. Then $\text{Im} \rho_{d_1}$ is a four-dimensional left ideal in $A$.

The second case is a bit more tricky. Let $d$ be a zero divisor of type (2). We denote by $A_d$ the centralizer $C_A(d)$ and by $\mathcal{R}(A_d)$ the Jacobson radical of $A_d$. Then there is the natural projection $\pi: A_d \to A_d/\mathcal{R}(A_d)$ and for this we have

Lemma 6. The algebra $\pi(A_d)$ is isomorphic to $M_2(\mathbb{Q})$. If $e \in \pi(A_d)$ is a zero divisor, then for a generic element $f$ in $\pi^{-1}(e)$ we have $\dim \text{Ker} \rho_f = 4$.

Remark 7. By saying that something holds for a “generic element” we mean that all elements, for which the assertion is true, form a dense Zariski open subset in the set of all elements considered. Therefore we can easily find an element satisfying the condition, for example as is done in the algorithm at the end of the section.

Proof. Again we may suppose that $\varphi(d)$ is actually equal to the matrix (2) in Lemma 5. Then the image of $A_d = C_A(d)$ under $\varphi$ is

\[
\varphi(A_d) = \left\{ \begin{pmatrix} \alpha_1 & \beta_1 & \alpha_2 & \beta_2 \\ 0 & \alpha_1 & 0 & \alpha_2 \\ \alpha_3 & \beta_3 & \alpha_4 & \beta_4 \\ 0 & \alpha_3 & 0 & \alpha_4 \end{pmatrix} \mid \alpha_i, \beta_i \in \mathbb{Q} \right\} (2).
\]

The Jacobson radical in $\mathcal{R}(\varphi(A_d))$ is the set of all $a \in \varphi(A_d)$ such that $\alpha_i = 0$, $i = 1, \ldots, 4$, and $\varphi(A_d)/\mathcal{R}(\varphi(A_d)) \cong \{ a \in \varphi(A_d) \mid \beta_i = 0, i = 1, \ldots, 4 \}$, which is clearly isomorphic to $M_2(\mathbb{Q})$. Let us denote the natural projection $\varphi(A_d) \to \varphi(A_d)/\mathcal{R}(\varphi(A_d))$ by $\pi'$. If $e$ is a zero divisor in $M_2(\mathbb{Q})$, then the preimage $(\pi')^{-1}(e)$ consists of such elements in (2) that the $\alpha_i$’s are fixed and $\alpha_1 \alpha_4 = \alpha_2 \alpha_3$. 


Note that at least one of elements \(\beta_i\)’s. Hence for a generic \(f' \in (\pi')^{-1}(e)\) we have \(\dim \ker \rho_{f'} = 4\), so \(\varphi^{-1}(f')\) gives us a minimal left ideal in \(A\).

From the proof of the previous lemma it also follows that we can compute the Jacobson radical of \(A\) very easily, namely \(\mathcal{R}(A_d) = \ker \rho_d \cap \ker \lambda_d\), where \(\lambda_d : x \mapsto dx\).

**FUNCTION: FindMinimalLeftIdeal**

**INPUT:** \(A\) – an associative algebra isomorphic to \(M_4(\mathbb{Q})\),

\(d\) – a zero divisor in \(A\).

**OUTPUT:** \(L\) – a four-dimensional left ideal in \(A\).

1. if \(\dim \ker \rho_d = 4\) then return \(\ker \rho_d\);
   
   elseif \(\dim \im \rho_d = 4\) then return \(\im \rho_d\);
   
   else if \(\ker \rho_d \cap \im \rho_d = 4\) then return \(\ker \rho_d \cap \im \rho_d\);
   
   end if;

2. if \(\ker \rho_d \cap \im \rho_d = 0\) then
   
   \(A_1 := \im \rho_d \cap \im \lambda_d\);

   \(d_1 := \text{zero divisor in } A_1\);

   return \(\im \rho_{d_1}\) (\(d_1\) dealt here as an element in \(A\));

   end if;

3. \(\mathcal{R} := \ker \rho_d \cap \ker \lambda_d\);

   \(A_d := A/\mathcal{R}\); let \(\pi\) be the natural projection \(A_d \to A_d/\mathcal{R}\);

   \(e := \text{zero divisor in } A_d\);

   // find \(f' \in \pi^{-1}(e)\) such that \(\dim \ker \rho_{f'} = 4\)

   fix an element \(f' \in \pi^{-1}(e)\) and let \((b_1, b_2, b_3, b_4)\) be a basis of \(\pi^{-1}(e) - f'_0\);

   if \(\dim \ker \rho_{f'} = 4\) then return \(\ker \rho_{f'}\); end if;

   for \(i \in \{1, 2, 3, 4\}\) do

   if \(\dim \ker \rho_{f' + b_i} = 4\) then return \(\ker \rho_{f' + b_i}\); end if;

   end for;

**Remark 8.** Note that at least one of elements \(f', f' + b_i\) \((i = 1, \ldots, 4)\) in the last four lines of the algorithm gives a four-dimensional ideal. For, these five points span the whole affine space \(\pi^{-1}(e)\). All elements \(e' \in \pi^{-1}(e)\) such that \(\dim \ker \rho_d > 4\) form a three-dimensional affine subspace, i.e. spanned by only four points.

### 5. Finding a zero divisor

The last point to explain is the first step of the algorithm: finding any zero divisor. We start by finding a quadratic element, i.e. an element \(a\) such that the minimum polynomial \(\mu_a(\xi)\) is irreducible quadratic.

In the following \(A[\xi]\) denotes the ring of polynomials in \(\xi\) over the algebra \(A\), where \(\xi\) commutes with all elements in \(A\). As usual we say that \(b \in A\) is a root of \(p(\xi) = a_0 + a_1\xi + \cdots + a_n\xi^n\), if \(a_0 + a_1b + \cdots + a_nb^n = 0\). If \(b\) is a root of \(p(\xi) \in A[\xi]\), then \(p(\xi) = q(\xi)(\xi - b)\) for some \(q(\xi) \in A[\xi]\), see Wedderburn (1964).
Theorem 9 (Wedderburn’s Factorization Theorem). Let \( c \in A \) have the minimum polynomial \( \mu_c(\xi) \) and \( m \in A[\xi] \) be such that \( \mu_c(\xi) = m(\xi)(\xi - c) \). Then for any \( y \in A \) such that \([y, c]\) is invertible, \( c' = [y, c][y, c]^{-1} \) is a root of \( m(\xi) \).

Proof. We partly follow Jacobson (1996), Theorem 2.9.1, where the claim is proven for division algebras.

Since \( \mu_c \) is a polynomial over the field, we have \( \mu_c(\xi)y = y\mu_c(\xi) \) and hence \( m(\xi)(y\xi - cy) = ym(\xi)(\xi - c) \). Here the left hand side can be written as \( m(\xi)(y\xi - cy) = m(\xi)y(\xi - c) + m(\xi)[y, c] \), therefore together it gives \( m(\xi)[y, c] = (ym(\xi) - m(\xi)y)(\xi - c) \). After multiplying by the inverse of \([y, c]\) we get \( m(\xi) = (ym(\xi) - m(\xi)y)[y, c]^{-1}(\xi - [y, c][y, c]^{-1}) \). □

Lemma 10 (Rowen). Let \( c \in A \) have the minimum polynomial \( \mu_c(\xi) = \xi^4 + \alpha_2\xi^2 + \alpha_1\xi + \alpha_0 \). Then for any factorization \( \mu_c(\xi) = (\xi^2 + a'\xi + b')(\xi^2 + a\xi + b) \) in \( A[\xi] \) we have \([Q(a^2) : Q] < 4\).

Proof. First define \( v(\xi) = (\xi^2 + a\xi + b)(\xi^2 + a'\xi + b') = \xi^4 + \beta_2\xi^2 + \beta_1\xi + \beta_0 \), with the \( \beta_j \)'s possibly in the algebra. We multiply \( v(\xi) \) from the right by \( (\xi^2 + a\xi + b) \), getting thus \( v(\xi)\xi^2 + a\xi + b) = (\xi^2 + a'\xi + b')\mu_c(\xi) \). By comparing coefficients in the last equation we obtain \( v(\xi) = \mu_c(\xi) \). Further we basically follow the proof in Rowen (1978), where a slightly stronger assertion is proven for division algebras.

By matching coefficients in \( \mu_c(\xi) \) we get \( a' = -a \) and

\[
\begin{align*}
\alpha_2 &= b + b' + a'a = b + b' - a^2, \\
\alpha_1 &= a'b + b'a = -ab + b'a, \\
\alpha_0 &= b'b = bb' \quad (\text{from } \alpha_0 = \beta_0).
\end{align*}
\]

Case 1: \( ab = ba \). Then \( a' = (b' - b)a \) and \( a^2 = ((b' + b)^2 - 4\alpha_0)a^2 = ((a^2 + \alpha_2)^2 - 4\alpha_0)a^2 = (a^2)^3 + 2a_2(a^2)^2 + (a^2 - 4\alpha_0)a^2 \), so \([Q(a^2) : Q] \leq 3\).

Case 2: \( ab \neq ba \). By multiplying \( \alpha_2 = b + b' - a^2 \) by \( b \) from left and right we get \( a^2b = ba^2 \). Therefore \( a \not\in Q(a^2) \), so \([Q(a^2) : Q] < [Q(a) : Q] \leq 4 \). □

Rowen’s lemma gives a recipe for finding a quadratic element as follows. We start with an arbitrary noncentral \( c \in A \). If \( c \) happens to be a zero divisor or the minimum polynomial \( \mu_c \) is reducible then we are done and do not need to continue in finding a quadratic element. So we can assume now that \( c \) is not a zero divisor and also \( \mu_c \) is not reducible. Then the minimum polynomial \( \mu_c \) is not cubic. Indeed, the characteristic polynomial is \( \chi_c(\xi) = \mu_c(\xi)\lambda(\xi) \). \( \lambda \in Q[\xi] \) linear, and since every irreducible factor of the characteristic polynomials also divides the minimum polynomial, we have \( \lambda(\xi) | \mu_c(\xi) \). Hence if \( c \) is not quadratic, its minimum polynomial is irreducible, of degree 4. After applying a linear substitution eliminating the cubic term in \( \mu_c(\xi) \) we may use Wedderburn’s factorization theorem to construct a factorization as in Rowen’s lemma. If \( a^2 = ba \) is not a zero divisor and the minimum polynomial of \( a^2 \) is not reducible (in which case we would be done), then there are three possibilities left:

(a) \([Q(a^2) : Q] = 2\), so \( a^2 \) is quadratic, or
(b) \( a^2 \in Q^+ \), then \( a \) is quadratic, since otherwise the factorization constructed according to Rowen’s lemma would be a factorization over \( Q \), or lastly
(c) \( a^2 = a = 0 \), then \( \mu_c(\xi) = \xi^4 + \alpha_2\xi^2 + \alpha_0 \) and \( c^2 \) is quadratic.

In sequel we will need the well-known

Theorem 11 (Double Centralizer Theorem). Let \( B \) be a central simple algebra over \( F \) and suppose that \( C \) is a simple subalgebra of \( B \). Then
(i) \( C_B(C) \) is simple,
(ii) \([C : F][C_B(C) : F] = [B : F]\),
(iii) \( C_B(C_B(C)) = C \).

**Proof.** See Pierce (1982), p. 232. \( \square \)

Let \( a \in A \) be a quadratic element, so \( \mathbb{Q}(a) \) is a subfield of \( A \) and \([\mathbb{Q}(a) : \mathbb{Q}] = 2\). Then by Double Centralizer Theorem \( C_A(a) \) of \( a \) in \( A \) is a simple algebra of dimension 8 over \( \mathbb{Q} \). The center of \( C_A(a) \) is the field \( \mathbb{Q}(a) \), and therefore \( C_A(a) \) can be understood as a central simple algebra over \( \mathbb{Q}(a) \). We denote this algebra by \( A_2 \).

**Lemma 12.** \( A_2 \) is isomorphic to \( M_2(\mathbb{Q}(a)) \).

**Proof.** Let \( \mathcal{L} \) be a four-dimensional left ideal in \( A \). If we consider \( A_2 = C_A(a) \) as an algebra over \( \mathbb{Q} \), then \( \mathcal{L} \) is also a four-dimensional \( A_2 \)-module. Let \( 0 \neq b_1 \in \mathcal{L} \) and let \( b_2 \in \mathcal{L} \) be such that \( b_2 \notin C(A_2)b_1 \). Then \( b_1, b_2 \) is a basis of \( \mathcal{L} \) over \( \mathbb{Q}(a) \). So we have a two-dimensional \( A_2 \)-module over \( \mathbb{Q}(a) \), where \( A_2 \) is now taken to be an algebra over \( \mathbb{Q}(a) \). Since \( A_2 \) acts faithfully on \( \mathcal{L} \), this gives an embedding of \( A_2 \) into \( M_2(\mathbb{Q}(a)) \). Now the assertion of the lemma follows from \([A_2 : \mathbb{Q}(a)] = 4\). \( \square \)

After finding the algebra \( A_2 \) as the centralizer of a quadratic element \( a \), we write \( A_2 \) as a cyclic algebra over \( F = \mathbb{Q}(a) \), so we find a cyclic element \( c \in A_2 \) and \( u' \) such that \((u')^2 = \gamma \in F^*\). By Proposition 3 there is \( s \in F(c) \) such that \( s\sigma(s) = 1/\gamma \). Then also \( u = su' \) is a principal generator of \( A_2 \) over \( F(a) \) and moreover \( u^2 = 1 \). We have found an element \( u \in A \) with the reducible minimum polynomial \( \mu_u(\xi) = \xi^2 - 1 \); therefore \( u + 1 \) is a zero divisor.

**FUNCTION:** FindZeroDivisor
**INPUT:** \( A \) – an associative algebra isomorphic to \( M_4(\mathbb{Q}) \).
**OUTPUT:** \( d \) – a zero divisor in \( A \).

(1) \# find a quadratic element \( a \in A \)
\[ c := a \text{ a noncentral element in } A; \]
\[ c := c + c_3/4 \neq 1, \text{ where } c_3 \text{ is the cubic coefficient in } \mu_c; \]
\[ \text{if } \deg \mu_c = 2 \text{ then } a := c; \]
\[ \text{elif } \mu_c(\xi) = \xi^4 + 2\alpha_2\xi^2 + \alpha_0 \text{ then } a := c^2; \# \text{ case (c)} \]
\[ \text{else} \]
\[ \text{find a factorization } \mu_c(\xi) = (\xi^2 + a'\xi + b')(\xi^2 + a\xi + b) \text{ over } A; \]
\[ \text{if } a^2 \notin \mathbb{Q} \text{ then } a := a^2; \text{ end if}; \# \text{ cases (a) and (b)} \]
\[ \text{end if}; \]

(2) \( A_2 := \) the centralizer of \( a \) in \( A \) regarded as a four dimensional central algebra over \( \mathbb{Q}(a) \).

(3) \# write \( A_2 \) as a cyclic algebra over \( \mathbb{Q}(a) \)
\[ c := a \text{ a noncentral element in } A_2; \]
\[ \text{find } \sigma(c) \in \mathbb{Q}(a, c) \text{ such that } \mu_c(\xi) = (\xi - c)(\xi - \sigma(c)); \]
\[ u' := a \text{ a nonzero solution of the linear system } u'c = \sigma(c)u'; \]
\[ \gamma := (u')^2; \# \text{ (\( \gamma \in \mathbb{Q}(a) \))} \]

(4) \# if \( \exists r \in \mathbb{Q}(a) \) such that \( r^2 = \gamma \) then \( u := u'/r \);
\[ \text{else} \]
\[ s := a \text{ a solution of the norm equation } s\sigma(s) = 1/\gamma; \# (s \in \mathbb{Q}(a)); \]
\[ u := su'; \]
\[ \text{end if}; \]

(5) \text{return } u + 1.
For each element $a \in A$ arising during the computation it is first tested whether $a$ is a zero divisor or whether the minimal polynomial $\mu_a$ is reducible. In each case we would have found a zero divisor $d$. So we can skip the rest of the computation; in particular we can avoid the time-expensive solving of the norm relative equation.

**Acknowledgements**

The author is grateful to Josef Schicho and the anonymous referees for helpful comments and suggestions, and also to RISC, Linz, Austria, for a stimulating atmosphere during the doctoral study.

The author was supported by SFB Grant F1303 of the Austrian FWF.

**References**


