Splitting central simple algebras of degree 4

Janka Pílniková
RICAM Linz, Austria

Nikolaus Conference
Aachen, 10 December 2005

Outline

(i) Central simple algebras.

(ii) Identifying $M_2(F)$.

(iii) Identifying $M_4(\mathbb{Q})$.

Central simple algebras

An algebra A over F is *central simple*, if

(i) $\mathbf{C}(A) \cong F$, where $\mathbf{C}(A) = \{a \in A \mid ax = xa \ \forall x \in A\}$.

(ii) A has no nontrivial ideals,

(iii) $[A : F] < \infty$.

WEDDERBURN'S STRUCTURE THEOREM, 1908.

(i) If A is a central simple algebra over F, then $A \cong M_n(\Delta)$, where Δ is a central division algebra over F.

(ii) If $M_n(\Delta) \cong M_{n'}(\Delta')$, then $n = n'$ and $\Delta \cong \Delta'$.

FACT. For any central simple algebra A over F, there is $d \in \mathbb{N}$ s.t. $[A : F] = d^2$. We call d the *degree* of A.

TASK: Given A such that $A \cong M_4(\mathbb{Q})$, find an isomorphism $\varphi\colon A \to M_4(\mathbb{Q})$.

Cyclic algebra of degree 2

E - quadratic field extension of F,
$G = \mathrm{Gal}(E|F)$, i.e. $G = \{1, \sigma\}$,
$\gamma \in F^*$.

The *cyclic algebra* (E, G, γ) is a vector space over F with the basis $\{1, c, u, cu\}$ together with the multiplication rules

(i) $E = F(c)$,

(ii) $uc = \sigma(c)u$,

(iii) $u^2 = \gamma$.

c – *cyclic element*,

u – *principal generator* of (E, G, γ) over E.

PROPOSITION. (E, G, γ) is a central simple algebra of degree 2.

Cyclic algebra of degree 2 – continued

PROPOSITION. Any central simple algebra of degree 2 is cyclic.

EXAMPLE. Quaternion algebra over $\mathbb{Q}$:

basis: $\{1, i, j, k\}$

multiplication: $i^2 = j^2 = k^2 = -1,\ \ ij = k,\ \ jk = i,\ \ ki = j$.

cyclic element $c = i$:

$\mu_i(\xi) = \xi^2 + 1$ is irreducible over $\mathbb{Q}$,

$E = \mathbb{Q}(i)$,

$\mu_i(\xi) = (\xi - i)(\xi + i)$, so $\sigma(i) = -i$.

principal generator $u = j$:

j is a nontrivial solution to $ui = \sigma(i)u = -iu$.

$\gamma = j^2 = -1$.

Reduction to the norm equation

LEMMA. The cyclic algebra (E, G, γ) over F is isomorphic to $M_2(F)$ if and only if there is $s \in E$ such that

$$s\sigma(s) = \frac{1}{\gamma}. \tag{1}$$

PROOF: If s is a solution to the norm equation (1), then $\{1 + su, c(1 + su)\}$ is a basis of a left ideal in (E, G, γ), where $c \in E, c \notin F$ and u is a principal generator of A over E.

REMARK. If A is a central simple algebra of degree 2 over $\mathbb{Q}$, then there are much faster methods for deciding and finding an isomorphism with $M_2(\mathbb{Q})$.

Left ideals and zero divisors in $M_n(F)$

A – central simple algebra of degree n over F,
$\mathcal{L}$ – left ideal in A.
Then $[\mathcal{L} : \mathbb{Q}] \in \{0, n, 2n, \ldots, n^2\}$.

PROPOSITION. Let $\mathcal{L}$ be an n-dimensional left ideal in A.
For $a \in A$ we define $\varphi_a\colon \mathcal{L} \to \mathcal{L}$, $x \mapsto ax$.

Then $\varphi\colon A \to M_n(F)$, $a \mapsto$ the matrix of φ_a
is an isomorphism of algebras.

$A \cong M_4(\mathbb{Q})$,
$d \in A$ – a zero divisor.
$\rho_d\colon A \to A$, $x \mapsto xd$ (a vector space endomorphism).

Then $\operatorname{Ker}\rho_d$, $\operatorname{Im}\rho_d$ are nontrivial left ideals: $[\operatorname{Ker}\rho_d : \mathbb{Q}], [\operatorname{Im}\rho_d : \mathbb{Q}] \in \{4, 8, 12\}$.
Another left ideal: $\operatorname{Ker}\rho_d \cap \operatorname{Im}\rho_d$.

Using a zero divisor in $A \cong M_4(\mathbb{Q})$

For a fixed $d \in A$, $\rho_d\colon\ A \to A$, $x \mapsto xd$,

$\lambda_d\colon\ A \to A$, $x \mapsto dx$.

LEMMA. Assume $A \cong M_4(\mathbb{Q})$.
Let d be a zero divisor in A such that $[\operatorname{Ker}\rho_d : \mathbb{Q}] = [\operatorname{Im}\rho_d : \mathbb{Q}] = 8$ and $\operatorname{Ker}\rho_d \cap \operatorname{Im}\rho_d = 0$.

Then $\operatorname{Im}\rho_d \cap \operatorname{Im}\lambda_d \cong M_2(\mathbb{Q})$.

If $d \in A$ is a zero divisor as in the Lemma, then

1. set $A_2 = \operatorname{Im}\rho_d \cap \operatorname{Im}\lambda_d$,
2. find an isomorphism $A_2 \to M_2(\mathbb{Q})$,
3. take a zero divisor d' in A_2,
4. for $d' \in A$ then holds $[\operatorname{Im}\rho_{d'} : \mathbb{Q}] = 4$.

Using a zero divisor in $A \cong M_4(\mathbb{Q})$ – continued

LEMMA. Assume $A \cong M_4(\mathbb{Q})$.
Let d be a zero divisor in A such that $\operatorname{Ker} \rho_d = \operatorname{Im} \rho_d$ so that $[\operatorname{Ker} \rho_d : \mathbb{Q}] = 8$.

Then the centralizer $\mathbf{C}_A(d) = \{x \in d \mid xd = dx\}$ is an associative algebra of dimension 8 over $\mathbb{Q}$ and $\mathbf{C}_A(d)/\mathcal{R} \cong M_2(\mathbb{Q})$ ($\mathcal{R} =$ Jacobson radical of $\mathbf{C}_A(d)$).

If $d \in A$ is a zero divisor as in the Lemma, then

1. set $A_1 = \mathbf{C}_A(d)$,
2. set $A_2 = A_1/\mathcal{R}$ and let $\pi\colon\ A_1 \to A_2$, $x \mapsto x + \mathcal{R}$,
3. find an isomorphism $A_2 \to M_2(\mathbb{Q})$,
4. take a zero divisor d_2 in A_2,
5. for a generic $d' \in \pi^{-1}(d_2)$ then holds $[\operatorname{Ker} \rho_{d'} : \mathbb{Q}] = 4$.

Finding a zero divisor in $A \cong M_4(\mathbb{Q})$

Double Centralizer Theorem. Let B be a central simple algebra over F. Let C be a simple subalgebra of B. Then

(i) $\mathbf{C}_B(C)$ is a simple subalgebra of B,

(ii) $[C : F][\mathbf{C}_B(C) : F] = [B : F]$,

(iii) $\mathbf{C}_B(\mathbf{C}_B(C)) = C$.

1. Find $a \in A$ such that μ_a of a is irreducible of degree 2.
2. $F = \mathbb{Q}(a)$ is a simple subalgebra of A and $[\mathbb{Q}(a) : \mathbb{Q}] = 2$.
3. Then $A_2 = \mathbf{C}_A(a)$ is a simple subalgebra of A such that
   $[A_2 : \mathbb{Q}] = 8$,
   $\mathbf{C}(A_2) = \mathbb{Q}(a)$,
4. Hence A_2 can be regarded as a central simple algebra over $F = \mathbb{Q}(a)$. Then $[A_2 : \mathbb{Q}(a)] = 4$.

Finding a zero divisor in $A \cong M_4(\mathbb{Q})$ – continued

Set $F = \mathbb{Q}(a)$ and regard A_2 as an algebra over F.

LEMMA. $A_2 \cong M_2(F)$.

1. Write A_2 as a cyclic algebra:
   (a) Take $c \in A_2$ such that $\mu_c(\xi) \in F[\xi]$ of c is quadratic irreducible.
   (b) By factoring μ_c over $F(c)$ find $\sigma(c)$:
   $\mu_c(\xi) = (\xi - c)(\xi - \sigma(c))$, where $\sigma \in \mathrm{Gal}(F(c)|F)$.
   (c) Set u to be any nontrivial solution of the system $uc = \sigma(c)u$ and set $\gamma = u^2$.
2. Find $s \in F(c)$ such that $s\sigma(s) = \frac{1}{\gamma}$.
   Then $(su)^2 = susu = s\sigma(s)u^2 = 1$.
3. The minimum polynomial $\mu_{su}(\xi) = \xi^2 - 1 = (\xi - 1)(\xi + 1)$,
   so $su - 1$ and $su + 1$ are zero divisors.