THE CHAIN LEMMA FOR KUMMER ELEMENTS OF DEGREE 3

MARKUS ROST

Abstract. Let A be a skew field of degree 3 over a field containing the 3^{rd} roots of unity. We prove a sort of chain equivalence for Kummer elements in A. As a consequence one obtains a common slot lemma for presentations of A as a cyclic algebra.

Chaînes d'éléments de Kummer en degré 3

Résumé. Soit k un corps contenant les racines cubiques de l'unité, et soit A un corps gauche de centre k, avec $[A:k]=9$. Nous montrons que deux éléments de Kummer de A peuvent être joints par une chaîne de longueur 4.

Version française abrégée

Soit k un corps contenant une racine primitive n-ème de l'unité ζ, et soit A une k-algèbre centrale simple de degré n. Un *élément de Kummer* de A est un élément dont le polynôme caractéristique est de la forme $t^n - a$, avec $a \in k^*$. Par une *ζ-paire* on entend un couple (X, Y) d'éléments de Kummer de A tels que $YX = \zeta XY$. Une telle paire donne une présentation de A comme produit croisé cyclique :

$$A = \langle\, X, Y \mid X^n = a,\, Y^n = b,\, YX = \zeta XY \,\rangle, \quad \text{avec} \quad a, b \in k^*.$$

Soient X, Y deux éléments de Kummer de A, et soit m un entier ≥ 1. Une *chaîne de longueur m joignant X à Y* est une suite de $m+1$ éléments de Kummer :

$$X = Z_0, Z_1, \ldots, Z_m = Y$$

tels que (Z_{i-1}, Z_i) soit une ζ-paire pour $i = 1, \ldots, m$.

Supposons que A soit un corps gauche. Si $n = 2$ (i.e. si A est un corps de quaternions), il est facile de voir que tout couple d'éléments de Kummer peut être joint par une chaîne de longueur 2. Si $n = 3$, J.-P. Tignol a donné des exemples de couples (X, Y) d'éléments de Kummer tels qu'il n'existe aucune chaîne de longueur 2 joignant X à Y (ni même à un conjugué de Y, cf. Appendice) ; dans ce qui suit, nous montrons qu'un tel couple peut être joint par une chaîne de longueur 4. La démonstration s'inspire de celle donnée par Petersson-Racine [1] pour un résultat analogue dans les algèbres de Jordan exceptionnelles. Comme conséquence, on obtient un "common slot lemma" pour les algèbres de degré 3.

Date: February 19, 1999.
The text appeared as: C. R. Acad. Sci. Paris Sér. I Math. 328 (1999), no. 3, 185–190.

Introduction

The well known common slot lemma for quaternion algebras asserts that if (a, b) is split over $k(\sqrt{c})$, then $(a, b) \simeq (a, e) \simeq (c, e)$ for some e.

Till a few years ago not much has been known about similar statements for algebras of degree > 2. Tignol has given an example (cf. Appendix) which shows that a common slot lemma with just one additional "slot" does not hold in general for algebras of degree 3. The first positive result was obtained by Petersson and Racine [1] who proved, taking up a suggestion of J-P. Serre, a common slot lemma for exceptional Jordan algebras over quadratically closed fields.

The major purpose of this Note is to present the Petersson-Racine arguments in the much simpler case of central simple algebras of degree 3. They yield a sort of chain equivalence for Kummer elements. As a consequence one obtains a common slot lemma for such algebras.

I am indebted to Jean-Pierre Tignol for leaving his text on the counterexample as an appendix to this Note.

1. Kummer elements

Let $n \geq 2$ and let k be a field containing a primitive n^{th} root of unity ζ. For a, $b \in k^*$ we denote by (a, b) the k-algebra defined by the presentation

$$(*) \qquad \langle\, X, Y \mid X^n = a,\ Y^n = b,\ YX = \zeta XY \,\rangle.$$

Let A be a central simple algebra of degree n over k. A *Kummer element* in A is an element $X \in A$ whose characteristic polynomial P_X is of the form $P_X(t) = t^n - a$ for some $a \in k^*$.

Lemma 1.1. *Let $X \in A$ be a Kummer element and let*

$$E(X, \zeta) = \{\, Z \in A \mid ZX = \zeta XZ \,\}.$$

(i) *$L = k[X]$ is the centralizer of X in A.*
(ii) *There exists $Y \in A^*$ such that $YXY^{-1} = \zeta X$.*
(iii) *For Y as in* (ii) *one has $E(X, \zeta) = YL = LY$.*

Proof. (i) follows from $\dim_k L = \deg A$, (ii) from the Skolem-Noether theorem, and (iii) from (i) and (ii). □

By a *ζ-pair* we understand a pair (X, Y) of invertible elements X, $Y \in A$ such that $YX = \zeta XY$.

Lemma 1.2. *Let (X, Y) be a ζ-pair.*

(i) *X and Y are Kummer elements.*
(ii) *If $A = M_n(k)$ and $X^n = Y^n = 1$, then the pair (X, Y) is conjugate to the pair (X_0, Y_0), where X_0 is the diagonal matrix* $\operatorname{diag}(1, \zeta, \zeta^2, \dots, \zeta^{n-1})$ *and where Y_0 is the permutation matrix $e_i \mapsto e_{i-1}$ with i taken* mod n.
(iii) *The algebra A has the presentation $(*)$.*

Proof. Since $YXY^{-1} = \zeta X$, the n different powers of ζ are roots of P_X, whence $P_X(t) = t^n - a$ for some $a \in k$. Further, X is invertible and therefore $a \neq 0$. Similarly one sees $P_Y(t) = t^n - b$ for some $b \in k^*$. This proves (i). For (ii) note that any matrix X with $P_X(t) = t^n - 1$ is conjugate to X_0 and we may therefore assume $X = X_0$. Then necessarily $Y = UY_0$ where U is in the centralizer $L = k[X]$ of X. One has $N_{L/k}(U) = Y^n = 1$. Therefore there exist $V \in L^*$ such that

$U = VY_0V^{-1}Y_0^{-1}$. It follows that $V^{-1}YV = Y_0$, which proves the claim. For (iii) one may assume that k is algebraically closed and that $A = M_n(k)$. The claim follows from (ii) after replacing X by $X/\sqrt[n]{a}$ and Y by $Y/\sqrt[n]{b}$. □

2. Chains

Let $X, Y \in A$ be Kummer elements. By a *chain* from X to Y of length m we understand a sequence $X = Z_0, Z_1, \dots, Z_m = Y$ of Kummer elements in A such that (Z_{i-1}, Z_i) is a ζ-pair for $i = 1, \dots, m$.

Let $Z_0, \dots, Z_m$ be a chain of Kummer elements in A and let $a_i = Z_i^n$. Then

$$A \simeq (a_{i-1}, a_i)$$

for $i = 1, \dots, m$. This shows that a chain of Kummer elements gives rise to a sequence of presentations $(*)$ with "common slots".

If there exists a chain from X to Y of length m, then there exists also a chain from X to Y of length m' for any $m' \geq m$ (if X, Y is a chain of length 1, then X, YX, Y is a chain of length 2).

Given Kummer elements X and Y, does there exist a chain from X to Y?

Let us consider the case $n = 2$. Then A is a quaternion algebra and $X \in A$ is a Kummer element if and only if X is invertible and $\text{trace}(X) = 0$. Given Kummer elements X and Y, let $Z = XY - YX$. If Z is invertible, then X, Z, Y is chain from X to Y. If $Z = 0$, then X and Y are scalar multiples of each other and any Kummer element Z' anti-commuting with X gives rise to a chain X, Z', Y. It follows that for quaternion skew fields there exist always chains from X to Y of length 2. In the case $A = M_2(k)$ is not difficult to see that there exist always chains of length 3 and to give examples of Kummer elements X, Y for which there does not exist a chain of length 2.

We now assume $n = 3$.

Proposition 2.1. *Let A a skew field of degree 3 over a field containing a primitive 3^{rd} root of unity ζ. Then for any two Kummer elements $X, Y \in A$ there exists a chain of length 4 from X to Y.*

As an immediate consequence of the proposition one obtains:

Corollary 2.2. *Suppose that (a, b) is split over $k(\sqrt[3]{c})$. Then there exist e, f, $g \in k^*$ such that*

$$(a, b) \simeq (a, e) \simeq (f, e) \simeq (f, g) \simeq (c, g).$$

Proof. Let $A = (a, b)$. If A is split, one takes $e = f = g = 1$. Assume that A is a skew field and choose Kummer elements $X, Y \in A$ with $X^3 = a$ and $Y^3 = c$. By Proposition 2.1 there exists a chain X, Z_1, Z_2, Z_3, Y. It suffices to take $e = Z_1^3$, $f = Z_2^{-3}$, and $g = Z_3^{-3}$. □

Tignol's example in the appendix shows that there exist an algebra A of degree 3 and Kummer elements $X, Y \in A$ for which there is no chain of length 2 from X to any conjugate of Y. The question for chains of length 3 is more delicate: it turns out that for generic X, Y there exist exactly 2 chains of length 3 which however might be defined only over a quadratic extension of the ground field. We hope to provide details for this at another occasion.

3. Proof of Proposition 2.1

Let k be a field with $\operatorname{char} k \neq 3$ containing a primitive 3^{rd} root of unity ζ. Moreover let A be a skew field of degree 3 and let X, $Y \in A$ be Kummer elements. Let $L = k[X] \subset A$ be the subfield generated by X. Then

$$A = L \oplus E(X,\zeta) \oplus E(X,\zeta^2). \qquad (**)$$

We show that there exist invertible elements Z_1, Z_2, $Z_3 \in A$ such that:

(1) $Z_1 \in E(X,\zeta)$,
(2) $Z_2 Z_1 = \zeta Z_1 Z_2$,
(3) $Z_3 Z_2 = \zeta Z_2 Z_3$,
(4) $Z_3 \in E(Y,\zeta^2)$,
(5) $Z_2 \in X^2 k \oplus E(X,\zeta^2)$,
(6) $Z_3 \in E(X,\zeta) \oplus E(X,\zeta^2)$.

Conditions (1)–(4) mean that X, Z_1, Z_2, Z_3, Y is a chain. The additional conditions (5) and (6) are taken from [1]. Their significance lies in the fact that for generic X, Y the system of equations (1)–(6) has a solution (Z_1, Z_2, Z_3), $Z_i \neq 0$ which is *unique* up to scalar factors of the Z_i. It would be interesting to understand more about the geometry of the system (1)–(6). In the following we merely present a solution.

Lemma 3.1. *There exist $Z_3 \neq 0$ satisfying* (4) *and* (6)*.*

Proof. One has $\dim_k E(Y,\zeta^2) = 3$ and $\dim_k\big(E(X,\zeta) \oplus E(X,\zeta^2)\big) = 6$. Both vector spaces lie in the 8-dimensional vector subspace of A of trace zero elements. Hence they have a nontrivial intersection. □

We choose Z_3 as in Lemma 3.1. It remains to find Z_1, $Z_2 \in A^*$ satisfying (1), (2), (3), and (5).

Let $Z \in E(X,\zeta)$, $Z \neq 0$. Then $E(X,\zeta) = ZL$ and $E(X,\zeta^2) = LZ^{-1}$. Write

$$Z_3 = Z\mu' + \mu'' Z^{-1}$$

with μ', $\mu'' \in L$.

If $\mu' = 0$, then $Z_3 \in E(X,\zeta^2)$ and $Z_1 = Z_3^{-1}$, $Z_2 = X^2$ do the job.

If $\mu'' = 0$, then $Z_3 \in E(X,\zeta)$ and $Z_1 = Z_3 X$, $Z_2 = Z_3^2 X$ do the job.

Assume that $\mu' \neq 0$ and $\mu'' \neq 0$. After replacing Z by $Z\mu''$ we have $Z_3 = Z\mu + Z^{-1}$ for some nonzero $\mu \in L$.

Lemma 3.2. *Let (X, Z) be a ζ-pair, let $\mu = m_0 + m_1 X + m_2 X^2$, $m_i \in k$, and let $T = Z\mu + Z^{-1}$. Let further c_2 be the second coefficient of the characteristic polynomial of T. Then $c_2 = -3m_0$.*

Proof. One has $\operatorname{trace}(T) = 0$ and $\operatorname{trace}(T^2) = 2\operatorname{trace}(\mu) = 6m_0$. Since $2c_2 = \operatorname{trace}(T)^2 - \operatorname{trace}(T^2)$, it follows that $2c_2 = -6m_0$. This proves the claim for $\operatorname{char} k \neq 2$. For $\operatorname{char} k = 2$, consider $c_2 = -3m_0$ as a polynomial identity in the variables m_i. It suffices to verify this identity for a standard ζ-pair (X, Z) in $M_3(\mathbb{Z}[\zeta])$. This follows from the characteristic 0 case. □

For the Kummer element $T = Z_3$ one has $c_2 = 0$ and Lemma 3.2 shows that

$$\mu = m_1 X + m_2 X^2, \quad Z_3 = Z(m_1 X + m_2 X^2) + Z^{-1}$$

for some m_1, $m_2 \in k$.

If $m_1 = 0$, then $Z_1 = Z$ and $Z_2 = (ZX)^{-1}$ do the job.

Otherwise let

$$b = Z^{-3}, \quad c = \zeta m_1 b / N_{L/k}(\mu), \quad \lambda = c\mu X,$$
$$Z_1 = Z\lambda, \quad Z_2 = X^2\bigl(1 + (Z\lambda)^{-1}\bigr).$$

With these settings, (1), (2), and (5) are obvious. It remains to verify (3):

$$(Z\mu + Z^{-1})X^2\bigl(1 + (Z\lambda)^{-1}\bigr) = \zeta X^2\bigl(1 + (Z\lambda)^{-1}\bigr)(Z\mu + Z^{-1}).$$

To check this, one considers the components with respect to the decomposition (∗∗). For the first component one gets $Z\mu X^2\lambda^{-1}Z^{-1} = \zeta X^2\lambda^{-1}Z^{-1}Z\mu$, which follows from $\mu X^2\lambda^{-1} = Xc^{-1}$ and $ZX = \zeta XZ$. For the third component one gets $Z^{-1}X^2 = \zeta X^2 Z^{-1}$, which is immediate from $ZX = \zeta XZ$. For the second component one gets

$$Z\mu X^2 + Z^{-1}X^2\lambda^{-1}Z^{-1} = \zeta X^2 Z\mu + \zeta X^2\lambda^{-1}Z^{-1}Z^{-1}.$$

This is equivalent to both of the following equations:

$$X^2\mu + Z^{-2}X^2\lambda^{-1}Z^{-1} = \zeta^2 X^2\mu + \zeta^2 X^2 Z^{-1}\lambda^{-1}Z^{-2},$$
$$(1-\zeta^2)X^2\mu = \zeta^2 X^2 Z^{-1}\lambda^{-1}Z^{-2} - Z^{-2}X^2\lambda^{-1}Z^{-1}.$$

For the right hand side of the last equation one computes

$$\begin{aligned}\text{r. h. s.} &= \zeta^2 X^2 Z^{-1}(c\mu X)^{-1}Z^{-2} - \zeta^2 X^2 Z^{-2}(c\mu X)^{-1}Z^{-1}\\ &= c^{-1}XZ^{-1}\mu^{-1}Z^{-2} - c^{-1}\zeta XZ^{-2}\mu^{-1}Z^{-1}\\ &= bc^{-1}X(Z^{-1}\mu Z)^{-1} - bc^{-1}\zeta X(Z^{-2}\mu Z^2)^{-1}.\end{aligned}$$

We multiply both sides with the conjugates $Z^{-1}\mu Z$ and $Z^{-2}\mu Z^2$ of μ. Then our equation reads as

$$\begin{aligned}(1-\zeta^2)X^2 N_{L/k}(\mu) &= bc^{-1}X(Z^{-2}\mu Z^2) - bc^{-1}\zeta X(Z^{-1}\mu Z)\\ &= bc^{-1}X(m_1\zeta X + m_2\zeta^2X^2) - bc^{-1}\zeta X(m_1\zeta^2 X + m_2\zeta X^2)\\ &= bc^{-1}m_1\zeta X^2(1-\zeta^2).\end{aligned}$$

The equality is now clear.

Appendix

With the kind permission of Jean-Pierre Tignol we reproduce here his text on

A "common slot" counterexample in degree 3

Notation: For a, b nonzero elements in a field F containing a primitive cube root of unity ω, the symbol (a, b) denotes the element of the Brauer group of F represented by the F-algebra generated by elements α, β subject to

$$\alpha^3 = a, \qquad \beta^3 = b, \qquad \beta\alpha = \omega\alpha\beta.$$

Let a_1, b_1, $a_2 \in F^\times$. If there exist x, $y \in F^\times$ such that

$$(*) \qquad (a_1, b_1) = (a_1, x) + (a_1, y), \quad (a_1, x) = -(a_2, x), \quad (a_1, y) = (a_2, y),$$

then the additivity of symbols yields $(a_1, b_1) = (a_2, x^{-1}y)$. However, the next example shows that when (a_1, b_1) is split by $F(\sqrt[3]{a_2})$, there need not exist elements x, y satisfying (∗).

Example: *A global field F containing a primitive cube root of unity and elements a_1, b_1, a_2, b_2 such that $(a_1, b_1) = (a_2, b_2)$, but no couple of elements x, y satisfying $(*)$. In particular (taking $x = 1$), the field F does not contain any element y such that*

$$(a_1, b_1) = (a_1, y) = (a_2, y) = (a_2, b_2).$$

Let $F = \mathbb{F}_7(t)$, where t is an indeterminate, $a_1 = t$ and $a_2 = t(1-t)$. Note that $(a_1, a_2) = 0$. Therefore, for all places v of F, the local invariant $(a_1, a_2)_v$ is trivial. It follows that in the completion F_v of F at v we have either $a_1 \in F_v^{\times 3}$ or $a_1 \equiv a_2 \bmod F_v^{\times 3}$ or $a_1 \equiv a_2^2 \bmod F_v^{\times 3}$ or $a_2 \in F_v^{\times 3}$, since the (generalized) Hilbert symbol $(\ ,\ )_v \colon (F_v^\times / F_v^{\times 3}) \times (F_v^\times / F_v^{\times 3}) \to \frac{1}{3}\mathbb{Z}/\mathbb{Z}$ is a nondegenerate alternating pairing.

Consider in particular v_1 the t-adic place and v_2 the $(t+3)$-adic place. Since a_1, a_2 are uniformizing parameters at v_1, we have a_1, $a_2 \notin F_{v_1}^{\times 3}$; but $a_1 \equiv a_2 \bmod F_{v_1}^{\times 3}$. On the other hand, a_1 and a_2 have non-cube residues at v_2, hence a_1, $a_2 \notin F_{v_2}^{\times 3}$ but $a_1 \equiv a_2^{-1} \bmod F_{v_2}^{\times 3}$.

Let now A be the central simple F-algebra with local invariants $1/3$ at v_1, $2/3$ at v_2 and 0 everywhere else. If v is a place of F where $a_1 \in F_v^{\times 3}$, then $v \neq v_1$, v_2 hence $[A]_v = 0$. It follows that A is split by $F(\sqrt[3]{a_1})$, hence we may find $b_1 \in F^\times$ such that $[A] = (a_1, b_1)$ in the Brauer group of F. Similarly, A is split by $F(\sqrt[3]{a_2})$ hence we may find $b_2 \in F^\times$ such that $[A] = (a_2, b_2)$; thus,

$$(a_1, b_1) = (a_2, b_2).$$

Suppose now x, $y \in F^\times$ satisfy $(*)$. Since $a_1 \equiv a_2 \bmod F_{v_1}^{\times 3}$, the relation $(a_1, x)_{v_1} = -(a_2, x)_{v_1}$ implies $(a_1, x)_{v_1} = 0$. On the other hand, since $a_1 \equiv a_2^{-1} \bmod F_{v_2}^{\times 3}$, it follows from $(a_1, y)_{v_2} = (a_2, y)_{v_2}$ that $(a_1, y)_{v_2} = 0$, hence $(a_1, x)_{v_2} = (a_1, b_1)_{v_2} = 2/3$.

For $v \neq v_1$, v_2, we consider four cases, according to the relation between a_1 and a_2 in the group of cube classes:

- if $a_1 \in F_v^{\times 3}$, then clearly $(a_1, x)_v = 0$.
- if $a_1 \equiv a_2 \bmod F_v^{\times 3}$, then $(a_1, x)_v = 0$ as for $v = v_1$ above.
- if $a_1 \equiv a_2^{-1} \bmod F_v^{\times 3}$, then $(a_1, x)_v = (a_1, b_1)_v$ as for $v = v_2$ above, hence $(a_1, x)_v = 0$.
- if $a_2 \in F_v^{\times 3}$, then $(a_1, x)_v = 0$ follows from $(a_1, x) = (a_2, x^{-1})$.

Thus, the invariants of (a_1, x) are:

$$(a_1, x)_{v_2} = 2/3, \quad \text{and} \quad (a_1, x)_v = 0 \quad \text{for } v \neq v_2,$$

a contradiction to the reciprocity law.

Jean-Pierre Tignol, June 1996.

References

[1] H. P. Petersson and M. L. Racine, *An elementary approach to the Serre-Rost invariant of Albert algebras*, Indag. Mathem., N.S. **7** (1996), no. 3, 343–365.

NWF I - Mathematik, Universität Regensburg, D-93040 Regensburg, Germany
E-mail address: markus.rost@mathematik.uni-regensburg.de
URL: http://www.physik.uni-regensburg.de/~rom03516