ISRAEL JOURNAL OF MATHEMATICS **129** (2002), 175–187

GENERATORS OF CENTRAL SIMPLE p-ALGEBRAS OF DEGREE 3*

BY

UZI VISHNE

Institute of Mathematics, The Hebrew University of Jerusalem
Givat Ram, Jerusalem 91904, Israel
e-mail: vishne@math.huji.ac.il

ABSTRACT

We discuss standard pairs of generators of cyclic division p-algebras of degree p, and prove for $p = 3$ that any two Artin–Schreier elements are connected by a chain of standard pairs. This result has immediate applications to the presentations of such algebras.

1. Introduction

Let Q be a quaternion algebra over a field F. It is well known (for example, see [2, Lemma 6.3]) that if $Q = (a, b) = (a', b')$ are two presentations of Q, then there is some $c \in F$ such that

$$(a, b) = (a, c) = (a', c) = (a', b').$$

Recently, a similar result for cyclic division algebras of degree 3 was proved by M. Rost [6]. If $A = (a, b)_3 = (a', b')_3$ are two presentations of A (where the base field contains 3-roots of unity), then there exist elements c, d, e in the base field such that

$$(a, b)_3 \cong (a, c)_3 \cong (d, c)_3 \cong (d, e)_3 \cong (a', e)_3 \cong (a', b')_3.$$

Chains of this form were also studied, in a more general context, in [4].

* The research was done while the author held a post-doctoral position at UCL, Louvain-la-Neuve, Belgium.

Received November 20, 2000 and in revised form May 3, 2001

If the degree of a central simple algebra is a power of the characteristic p of the base field, it is called a p-**algebra**. Standard generators of cyclic p-algebras of degree p were studied in the author's dissertation [8, Chap. 1, Sec. 4]. Theorem 4.16 there is, in a sense, a chain lemma for arbitrary p, but it requires tensoring by matrices.

In Section 2 we describe the basic properties of standard pairs of generators and related definitions are given. We define distance between Artin–Schreier elements, and state the main result, Theorem 2.6, and the applications to presentations of cyclic p-algebras.

We study short chains of pairs for $p = 3$ in Section 3, and this is applied in Section 4 to prove Theorem 2.6. Some large subgraphs of the graph of standard pairs of generators are given in Section 5.

ACKNOWLEDGEMENT: I am indebted to Prof. J.-P. Tignol for pointing out references [4] and [6] and for his kind hospitality during my stay at UCL.

2. Standard generators of cyclic p-algebras of degree p

Let F be a field of characteristic p, and A a central simple cyclic algebra of degree p over F (that is, $\dim_F A = p^2$). By Wedderburn's structure theorem, A is either a division algebra, or the algebra of $p \times p$ matrices over F. The basic structure theory of p-algebras is given in [1], cf. also [5].

It is known that A can be given the following presentation, where $a, b \in F$, $b \neq 0$:

$$A = F[x, y| \quad x^p - x = a, \quad y^p = b, \quad yxy^{-1} = x + 1].$$

We call such x, y a **standard pair of generators**. Let

$$\begin{aligned} \mathrm{X}_A =& \{x \in A : \quad x^p - x \in F, \quad [F[x] : F] = p\}, \\ \mathrm{Y}_A =& \{y \in A : \quad y^p \in F^*, \quad [F[y] : F] = p\} \end{aligned}$$

be the possible components of a standard pair of generators. The elements of X_A are called **Artin–Schreier elements** of A; every cyclic subfield of A contains such an element.

Remark 2.1: If $x, y \in A$ satisfy $yxy^{-1} = x + 1$, then x, y form a standard pair of generators, that is, $A = F[x, y]$, $x^p - x = a$ and $y^p = b$ for some $a, b \in F$.

Proof: We first show that x, y generate A. Indeed, $F[x]$ is a separable extension of dimension p over F (with an automorphism $x \mapsto x+1$ induced by y). Note that $[y^i, x] = y^i x - xy^i = iy^i$. Now suppose $f_0 + f_1 y + \cdots + f_{p-1} y^{p-1} = 0$ for $f_i \in F[x]$.

Applying the derivation by x, we get $0 = f_1 y + 2f_2 y^2 + \cdots + (p-1)f_{p-1}y^{p-1}$. Repeating this, we get $0 = f_1 y + 2^j f_2 y^2 + \cdots + (p-1)^j f_{p-1}y^{p-1}$ for every $j = 1, \ldots, p-1$. Since the Vandermonde matrix of $0, \ldots, p-1$ is invertible, we get that $f_i y^i = 0$; but y is invertible, so that $f_i = 0$. It follows that $\sum F[x]y^i$ has dimension p^2 over F, and is thus equal to A.

Now, from the assumption it readily follows that $a = x^p - x$ and $b = y^p$ commute with x, y and are thus central, so x, y form a standard pair of generators. ∎

Now let

$$\mathrm{XY}_A = \{(x,y) \in \mathrm{X}_A \times \mathrm{Y}_A : \quad yxy^{-1} = x+1\}.$$

XY_A may by viewed as a bipartite graph, where the vertices are the elements of X_A and Y_A, and there is an edge connecting x and y iff $(x,y) \in \mathrm{XY}_A$. For an element to be in X_A or in Y_A depends on the characteristic polynomial, so we have $p-1$ (non-linear) equations for each set. It follows that X_A and Y_A are (p^2-p+1)-dimensional varieties over F, and $\mathrm{XY}_A \subseteq \mathrm{X}_A \times \mathrm{Y}_A$ is a (p^2+1)-dimensional subvariety (as seen from Remark 2.3). In a sense, we study the geometry of XY_A.

Note that there are no isolated points on the graph:

Remark 2.2:

(i) For every $x \in \mathrm{X}_A$ there is some $y \in A$ such that $(x,y) \in \mathrm{XY}_A$.

(ii) Likewise for every $y \in \mathrm{Y}_A$, there is some $x \in A$ such that $(x,y) \in \mathrm{XY}_A$.

Proof: (i) It is easy to see that $F[x]$ is either a subfield of dimension p of A, or isomorphic to the split ring $F^{\times p} = F \times \cdots \times F$. In both cases the automorphism induced by $x \mapsto x+1$ is inner (Skolem–Noether theorem, or the generalization to maximal separable commutative subalgebras in [3]), say induced by y. Then $F[x,y] = A$ by Remark 2.1.

(ii) This is [1, Theorem IV.17]. ∎

Two elements z, z' of $\mathrm{X}_A \cup \mathrm{Y}_A$ are said to be **at distance** $t/2$ if there is a chain of elements $z = z_0, z_1, \ldots, z_t = z' \in \mathrm{X}_A \cup \mathrm{Y}_A$ such that, for every $i = 1, \ldots, t$, the couple z_{i-1}, z_i is a standard pair of generators. We take half of the usual distance in the graph XY_A, since we are sometimes more interested in the induced patterns on X_A or Y_A. We denote this situation by saying that $z \longleftrightarrow z_1 \longleftrightarrow \cdots \longleftrightarrow z_{t-1} \longleftrightarrow z'$ is a chain, where necessarily elements of X_A and Y_A interchange. We write X_A and Y_A in appropriate places in the chain to state existence of appropriate elements. For example, elements $x, x' \in \mathrm{X}_A$ are at distance 2 iff there is a chain $x \longleftrightarrow \mathrm{Y}_A \longleftrightarrow \mathrm{X}_A \longleftrightarrow \mathrm{Y}_A \longleftrightarrow x'$.

Let (x, y) be a standard pair of generators. The neighborhood of x, y is described in the following remark.

Remark 2.3:

(i) The elements forming a standard pair of generators with x are of the form λy, where $\lambda \in F[x]^*$.

(ii) The elements forming a standard pair of generators with y are of the form $\mu + x$, where $\mu \in F[y]$.

Proof: (i) $y_1 x y_1^{-1} = x + 1$ iff $y_1 y^{-1} \in C_A(F[x]) = F[x]$, and $y_1 y^{-1}$ is invertible since y, y_1 are.

(ii) $y x_1 y^{-1} = x_1 + 1$ iff $x_1 - x \in C_A(F[y]) = F[y]$. ∎

In particular, if $x \in \mathrm{X}_A$, then $x + \alpha \in \mathrm{X}_A$ for every $\alpha \in F$, and likewise for $y \in \mathrm{Y}_A$, $\beta y \in Y$ for every $\beta \in F^*$. We have

Remark 2.4: The actions of F^+ and F^* on X_A and Y_A, respectively, define equivalence relations.

In particular, if x, y form a standard pair of generators, $x' \equiv x$, and $y' \equiv y$, then x', y' also form a standard pair of generators.

The next proposition shows that there is essentially only one path connecting every two elements at distance 1.

Proposition 2.5: *Let $x, x' \in \mathrm{X}_A$ and $y, y' \in \mathrm{Y}_A$. If (x, y), (x, y'), (x', y) and (x', y') are all standard pairs of generators, then $x' \equiv x$ or $y' \equiv y$.*

Proof: By Remark 2.3, $\mu = x' - x \in F[y] \cap F[y']$, and $\lambda = y' y^{-1} \in F[x]$. Now $\lambda \mu \lambda^{-1} = \mu$, so that λ and μ commute. If A is a division ring, then we are done (as μ commutes with y, λ, so either $\mu \in F$ or $\lambda \in F$), but for the general case, write $\lambda = \sum \alpha_i x^i$ and $\mu = \sum \beta_j y^j$. Then compute $0 = [\mu, \lambda] = \sum \alpha_i \beta_j ((x+j)^i - x^i) y^j$, and compare the upper monomials with respect to y and x. We get a contradiction unless λ or μ are central. ∎

The main result of this paper is the following

Theorem 2.6: *Let F be a field of characteristic $p = 3$, and let A be a (cyclic) division algebra of degree p over F.*

Then every two elements $x, z \in \mathrm{X}_A$ are at distance at most 3.

The proof is given in Section 4. This theorem can be reformulated in terms of presentations of algebras. Recall that for $a, b \in F$, $[a, b)_p$ denotes the p-algebra

$$[a, b)_p = F[x, y| \quad x^p - x = a, \quad y^p = b, \quad yxy^{-1} = x + 1].$$

COROLLARY 2.7: *Suppose $[a,b)_3 \cong [a',b')_3$ are two presentations of the same division algebra. Then there exist $a_1, a_2 \in F$ and $b_1, b_2, b_3 \in F^*$ such that*

$$[a,b) \cong [a,b_1) \cong [a_1,b_1) \cong [a_1,b_2) \cong [a_2,b_2) \cong [a_2,b_3) \cong [a',b_3) \cong [a',b').$$

One remark is in order concerning the split case. If $[a,b)_p \cong [a',b')_p$ are two presentations of $M_p(F)$, then

$$[a,b) \cong [0,b) \cong [0,b') \cong [a',b'),$$

so for a split algebra Corollary 2.7 holds, in a stronger form and for arbitrary p.

3. Elements at distance $1\frac{1}{2}$

Let A be a cyclic division p-algebra of degree p over F, where from now on we assume $p = \operatorname{char} F = 3$.

Fix a standard pair of generators $x, y \in A$, and set $\gamma = y^3 \in F$. In this section we classify the elements $u \in \mathrm{Y}_A$ which are at distance $1\frac{1}{2}$ from x, that is, elements for which there exists a chain

$$y \longleftrightarrow x \longleftrightarrow \mathrm{Y}_A \longleftrightarrow \mathrm{X}_A \longleftrightarrow u.$$

We denote by Tr the reduced trace map of A, and by tr the trace map of the extension $F[x]/F$. The action of y by conjugation on $F[x]$ is denoted by σ, and the notation $\mathrm{N}(\lambda)$ is preserved for the norm of elements in $F[x]$. Since $A = F[x,y] = \sum F[x]y^j$, we can write every $u \in A$ in the form $u = \lambda_0 + \lambda_1 y + \lambda_2 y^2$ for unique $\lambda_0, \lambda_1, \lambda_2 \in F[x]$. Set $\eta = \lambda_1 \cdot \sigma\lambda_2$.

REMARK 3.1: *Assuming $u \notin F$, we have that $u \in \mathrm{Y}_A$ iff $\mathrm{Tr}(u) = \mathrm{Tr}(u^2) = 0$. As $\mathrm{Tr}(\lambda y) = \mathrm{Tr}(\lambda y^2) = 0$ for every $\lambda \in F[x]$, a simple computation yields the following conditions, equivalent to $u \in Y_A$:*

$$\mathrm{tr}(\lambda_0) = 0, \tag{1}$$

$$\gamma\,\mathrm{tr}(\eta) = \mathrm{tr}(\lambda_0^2). \tag{2}$$

Under these assumptions, one can compute that $u^3 = \mathrm{N}(\lambda_0) + \gamma\,\mathrm{N}(\lambda_1) + \gamma^2\,\mathrm{N}(\lambda_2)$.

LEMMA 3.2: *The element u is at distance $1\frac{1}{2}$ from x if and only if the following equations have a solution with $f_1, f_2 \in F$, $\lambda \in F[x]^*$:*

$$f_1\gamma(\lambda \cdot \sigma\lambda_2 - \sigma^2\lambda \cdot \lambda_2) + f_2\gamma \cdot \sigma\lambda \cdot (\lambda \cdot \sigma^2\lambda_1 - \sigma^2\lambda \cdot \lambda_1) = -\lambda_0, \tag{3}$$

$$f_1(\sigma\lambda_0 - \lambda_0) + f_2\gamma(\sigma\lambda \cdot \sigma^2\lambda_2 - \sigma^2\lambda \cdot \lambda_2) = 0, \tag{4}$$

$$f_1(\lambda \cdot \sigma\lambda_1 - \sigma\lambda \cdot \lambda_1) + f_2 \cdot \lambda \cdot \sigma\lambda \cdot (\sigma^2\lambda_0 - \lambda_0) = \lambda_2. \tag{5}$$

Proof: The elements x,u are at distance $1\frac{1}{2}$ iff there are some $y' \in \mathrm{Y}_A$ and $x' \in \mathrm{X}_A$ such that $x \longleftrightarrow y' \longleftrightarrow x' \longleftrightarrow u$ form a chain. By Lemma 2.3, we can write $y' = \lambda y$ for some $\lambda \in F[x]$, and then $x' - x \in F[\lambda y]$. Thus $x' = x + f_0 + f_1\lambda y + f_2(\lambda y)^2$ for some $f_0, f_1, f_2 \in F$, and by Remark 2.4 we may take $f_0 = 0$. The only remaining condition is that $ux' - x'u = u$, and comparing coefficients of y in both sides, we get Equations (3)–(5). ∎

Let $K = F[x]$ be a cyclic extension of dimension 3 of F, as before. The following facts are easily checked.

REMARK 3.3: (i) *For every* $\alpha_0, \alpha_1, \alpha_2 \in F$, *we have that*

$$\mathrm{tr}_{K/F}(\alpha_0 + \alpha_1 x + \alpha_2 x^2) = -\alpha_2.$$

(ii) *For every* $\phi \in K$, *if* $\mathrm{tr}_{K/F}\,\phi = \mathrm{tr}_{K/F}\,\phi^2 = 0$, *then* $\phi \in F$.

(iii) *The map* $(\sigma - 1) : K \to K$ *defined by* $(\sigma - 1)a = \sigma(a) - a$ *is onto the subspace* $\{\phi \in K : \mathrm{tr}_{K/F}\,\phi = 0\}$.

(iv) $\mathrm{tr}_{K/F}\,\phi = 0$ *iff* $(\sigma - 1)\phi \in F$.

Proof: (i) follows since the minimal polynomial of x is of the form $x^3 - x - \theta = 0$. (ii) and (iii) follow trivially from (i), and (iv) follows since for every $\phi \in K$ we have that $(\sigma - 1)^2\phi = (\sigma^2 + \sigma + 1)\phi$. ∎

PROPOSITION 3.4: *Assume* $u = \lambda_0 + \lambda_1 y + \lambda_2 y^2$ *as before, and* $\lambda_0 \in F$. *Then* u *is at distance* $1\frac{1}{2}$ *from* x *if and only if the following holds:*

(a) $\lambda_2 = 0$, **or**

(b) $\lambda_2 \neq 0$, $\lambda_1 \neq 0$ *and* $\eta \notin F$, **or**

(c) $\lambda_2 \neq 0$, $\lambda_1 \neq 0$, $\eta \in F$, *and* $\lambda_0\,\mathrm{N}(\lambda_1) = \eta^2\gamma$.

These conditions may look a little less random in light of the following observation: assuming $\lambda_0 \in F$, we have that $\eta \in F$ iff $F[u] = F[\lambda_1 y]$. If this is the case, then $u^2 \in F + F(\lambda_1 y)^2$ iff $\lambda_0\,\mathrm{N}(\lambda_1) = \eta^2\gamma$.

Proof: **Case 1:** $\lambda_2 = 0$. We must have $\lambda_1 \neq 0$, for otherwise $u = \lambda_0 \in F[x]$ would be separable. If $\lambda_0 = 0$, then by Remark 2.3 (i) we have the chain $y \longleftrightarrow x \longleftrightarrow y \longleftrightarrow x \longleftrightarrow \lambda_1 y = u$. Otherwise, choose $f_1 = 0$. Substituting, we find that Equations (4) and (5) are satisfied, and Equation (3) becomes

$$f_2\gamma\left(\sigma^2\left(\frac{\lambda_1}{\lambda}\right) - \frac{\lambda_1}{\lambda}\right) \cdot \mathrm{N}(\lambda) = -\lambda_0,$$

which can be solved by choosing $\lambda = x^{-1}\lambda_1$ and $f_2 = \theta\lambda_0/\gamma\,\mathrm{N}(\lambda_1)$, where $\theta = \mathrm{N}(x) \in F$. This results in the chain

$$x \longleftrightarrow y' = x^{-1}\lambda_1 y \longleftrightarrow x + \lambda_0 {y'}^{-1} \longleftrightarrow u.$$

Case 2: $\lambda_2 \neq 0$. If $\lambda_1 = 0$, then equation (5) has no solution. Thus we assume $\lambda_1 \neq 0$. In particular, $\eta = \lambda_1 \cdot \sigma\lambda_2 \neq 0$.

Case 2.1: $\eta \notin F$. Choose $f_2 = 0$ and $f_1 = 1$. Then Equation (4) vanishes, and substituting $\lambda_2 = \sigma^2\eta/\sigma^2\lambda_1$, Equations (3) and (5) become

$$\begin{aligned} \eta\lambda/\lambda_1 - \sigma^2(\eta\lambda/\lambda_1) &= -\lambda_0/\gamma, \\ \lambda/\lambda_1 - \sigma(\lambda/\lambda_1) &= \sigma^2(\eta)/\,\mathrm{N}(\lambda_1), \end{aligned}$$

which is solved by

$$\lambda = \frac{\lambda_2 \cdot \sigma^2(\lambda_2) - \gamma^{-1}\lambda_0\lambda_1}{\sigma(\eta) - \eta}.$$

This satisfies $\lambda \neq 0$, for otherwise $\gamma\,\mathrm{N}(\lambda_2) = \lambda_0\eta$, contrary to the assumption $\eta \notin F$. Then we have the following chain: $x \longleftrightarrow \lambda y \longleftrightarrow x + \lambda y \longleftrightarrow u$.

Case 2.2: $\eta \in F$. We cannot have $f_2 \neq 0$, for then Equation (4) will force $\lambda/\lambda_1 \in F$, and from Equation (5) we then get $\eta = 0$, contrary to the assumption $\lambda_2 \neq 0$. Thus we have $f_2 = 0$, and the equations become

$$f_1\left(\sigma\Big(\frac{\lambda}{\lambda_1}\Big) - \frac{\lambda}{\lambda_1}\right) = \frac{-\lambda_0}{\gamma\eta} = \frac{-\sigma^2(\eta)}{\mathrm{N}(\lambda_1)},$$

for which, by Remark 3.3 (iii), there is a solution λ iff $\lambda_0\,\mathrm{N}(\lambda_1) = \gamma\eta^2$. Indeed we can take $f_1 = 1$ and $\lambda = -\lambda_2\sigma(\lambda_1)^{-1}x$, and the resulting chain is $x \longleftrightarrow \lambda y \longleftrightarrow x + \lambda y \longleftrightarrow u$ ∎

COROLLARY 3.5: *Let $x \in \mathrm{X}_A$; then x and $-x$ are at distance at least* 3.

Proof: Choose y such that $(x, y) \in \mathrm{XY}_A$. We show that there is no chain $y \longleftrightarrow x \longleftrightarrow \mathrm{Y}_A \longleftrightarrow \mathrm{X}_A \longleftrightarrow u \longleftrightarrow -x \longleftrightarrow y^2$. Every appropriate u is, by Remark 2.3 (i), of the form $u = \lambda y^2$ for some $\lambda \in F[-x] = F[x]$, and then the completion is impossible by the last proposition. ∎

COROLLARY 3.6: *For every $y \in \mathrm{Y}_A$, the distance between y and y^2 is at least* 3.

Proof: Otherwise, there is a chain

$$y \longleftrightarrow x' \longleftrightarrow \mathrm{Y}_A \longleftrightarrow \mathrm{X}_A \longleftrightarrow y^2,$$

but since $-x', y^2$ form a standard pair of generators, it follows that the distance between x' and $-x'$ is at most 2, contrary to the former corollary. ∎

For the rest of the section we no longer assume $\lambda_0 \in F$. Let $b = \sigma(\lambda_0) - \lambda_0$; then $b \in F$ by Equation (1) and Remark 3.3 (iv). Moreover, since $\operatorname{tr}(\lambda_0) = 0$, we have that $\lambda_0 = a + bx$ for $a \in F$.

PROPOSITION 3.7: *Let x, y form a standard pair of generators and $u = \lambda_0 + \lambda_1 y + \lambda_2 y^2 \in \mathrm{Y}_A$ where $\lambda_0 = a + bx$ and $\eta = \lambda_1 \cdot \sigma\lambda_2$ as above. If $\lambda_0 \notin F$ and $\gamma(\sigma^2\eta - \eta) = b\lambda_0$, then u is at distance $1\frac{1}{2}$ from x.*

Proof: Set $x' = x - b^{-1}\lambda_2 y^2$ and $y' = \lambda_2 \cdot \sigma^2\lambda_2 \cdot y$. Then the first two pairs in the chain

$$x \longleftrightarrow y' \longleftrightarrow x' \longleftrightarrow u$$

follow from Remark 2.3. For the third pair, compute that

$$ux' - x'u = \gamma b^{-1}(\sigma^2\eta - \eta) + \lambda_1 y + \lambda_2 y^2,$$

which equals u by the assumption. ∎

Note that the assumption $\gamma(\sigma^2\eta - \eta) = b\lambda_0$ implies (but is not implied by) Equation (2).

The following remark is given as a counterpart for Proposition 3.4, and is not needed later.

REMARK 3.8: *Assume $u = \lambda_0 + \lambda_1 y + \lambda_2 y^2$ as before, and $\lambda_0 \notin F$. Then there exist homogeneous quadratic forms Q_I, Q_{II} in two variables over F, explicitly stated in the proof, such that u is at distance $1\frac{1}{2}$ from x if and only there are $g, f_1 \in F$ such that*

$$Q_I(g, f_1) = 0,$$
$$Q_{II}(g, f_1) \neq 0.$$

Proof: Since $\lambda_0 \notin F$, by Remark 3.3 (ii) we have that $\operatorname{tr}\lambda_0^2 \neq 0$, so by Equation (2), $\eta \neq 0$ and thus also $\lambda_1, \lambda_2 \neq 0$. Moreover, Equation (4) has no solution with $f_2 = 0$, so we may assume $f_2 \neq 0$.

We write

$$\lambda = \frac{g + f_1 \cdot \sigma^2\lambda_0}{f_2\gamma \cdot \sigma\lambda_2} \tag{6}$$

for $g \in K$. Then Equation (4) is equivalent to $g \in F$, and we assume this is the case. Recall that by Lemma 3.2 we need to solve Equations (3)–(5) with

$f_1, f_2 \in F$ and $\lambda \in K$, so this now becomes solving Equations (3) and (5) with $f_1, f_2, g \in F$, $f_2 \neq 0$. Write $\lambda_0 = a + bx$ with $a, b \in F$. Note that from Equation (2) and Remark 3.3 (i), we get that $\gamma \operatorname{tr}(\eta) = \operatorname{tr}(\lambda_0^2) = -b^2$.

Denote by

$$\begin{aligned} Q_0(s,t) = {} & (\sigma^2\eta - \eta)s^2 + (\sigma^2\lambda_0 \cdot \eta - \sigma\lambda_0 \cdot \sigma^2\eta)st \\ & + (\gamma b \operatorname{N}(\lambda_2) + \lambda_0(\sigma^2\lambda_0 \cdot \sigma^2\eta - \sigma\lambda_0 \cdot \eta))t^2, \\ Q_2(s,t) = {} & -bs^2 + (\gamma(\sigma\eta - \eta) + b \cdot \sigma\lambda_0)st \\ & + (\gamma(\sigma^2\lambda_0 \cdot \sigma\eta - \lambda_0\eta) - b\lambda_0 \cdot \sigma^2\lambda_0)t^2 \end{aligned}$$

the two quadratic forms in s, t over K.

Substituting (6) in Equations (3) and (5), multiplying by $f_2\gamma \operatorname{N}(\lambda_2)$ in the first case and by $f_2\gamma^2 \cdot \sigma\lambda_2 \cdot \sigma^2\lambda_2$ in the second case, we get the following system of equations, in the variables $g, f_1 \in F$, $f_2 \in F^*$:

$$Q_0(g, f_1) = -\lambda_0 f_2 \gamma \operatorname{N}(\lambda_2) \tag{7}$$

$$Q_2(g, f_1) = f_2\gamma^2 \operatorname{N}(\lambda_2). \tag{8}$$

It can be checked that Q_2 is actually a quadratic form over F. Q_0, however, is not defined over F (the coefficient $\sigma^2\eta - \eta \notin F$, for otherwise we would have $b^2 = \gamma \operatorname{tr}\eta = 0$ by Remark 3.3 (iv)).

Fortunately we have that $\operatorname{tr} Q_0 = 0$, so by Remark 3.3 (i), the coefficients of Q_0 lie in the two-dimensional F-space $F + F\lambda_0 \subset K$. Write

$$Q_0 = Q_I + \lambda_0 Q_{II}$$

for the respective components. Then we can compute $Q_{II} = \frac{1}{b}(\sigma(Q_0) - Q_0)$ to be

$$\begin{aligned} Q_{II}(s,t) = {} & -\operatorname{tr}(\eta)/b \cdot s^2 + \operatorname{tr}(\lambda_0 \cdot \sigma\eta)/b \cdot st \\ & - \operatorname{tr}(\lambda_0 \cdot \eta \cdot \sigma\lambda_0)/b \cdot t^2 \end{aligned}$$

and so $Q_I = Q_0 - \lambda_0 Q_{II}$ is

$$\begin{aligned} Q_I(s,t) = {} & (\sigma^2\eta - \eta - b\lambda_0/\gamma)s^2 + (\sigma^2\lambda_0 \cdot \sigma^2\eta - \sigma\lambda_0 \cdot \eta + b\lambda_0^2/\gamma)st \\ & + (\gamma b \operatorname{N}(\lambda_2) - b \operatorname{N}(\lambda_0)/\gamma)t^2. \end{aligned}$$

It may not be so obvious, but one can check that Q_I is indeed defined over F.

Using this decomposition, Equation (7) now becomes

$$Q_I(g, f_1) = 0, \tag{9}$$

$$Q_{II}(g, f_1) = -f_2\gamma \operatorname{N}(\lambda_2). \tag{10}$$

Again this is not immediate, but one can compute that $Q_2 = -\gamma Q_{I\!I}$. Thus solving Equations (7) and (8) is equivalent to solving Equations (9) and (10). Recall that we only assumed $f_2 \neq 0$, so all we have to do is find a zero of Q_I which is not a zero of $Q_{I\!I}$, as claimed. ∎

EXAMPLE 3.9: *Suppose $\gamma(\sigma^2\eta - \eta) = b\lambda_0$ as in Proposition 3.7. The coefficient $-\operatorname{tr}(\eta)/b = b/\gamma$ of s^2 in the form $Q_{I\!I}(s,t)$ is nonzero, so if we substitute $f_1 = 0$ and $g = 1$ in $Q_I, Q_{I\!I}$ we get $Q_I(1,0) = \sigma^2\eta - \eta - b\lambda_0/\gamma = 0$ and $Q_{I\!I}(1,0) = -\operatorname{tr}(\eta)/b \neq 0$. By Remark 3.8, u is at distance $1\frac{1}{2}$ from x, in accordance with the above-mentioned proposition.*

4. A Proof of Theorem 2.6

Let A be a division p-algebra of degree $p = 3$. We are given two elements $x, z \in \mathrm{X}_A$, and wish to find a chain

$$x \longleftrightarrow \mathrm{Y}_A \longleftrightarrow \mathrm{X}_A \longleftrightarrow \mathrm{Y}_A \longleftrightarrow \mathrm{X}_A \longleftrightarrow \mathrm{Y}_A \longleftrightarrow z.$$

Choose (using Remark 2.2 (i)) elements y, u such that x, y and z, u are standard pairs of generators. For x, y, u we use the notations of the previous section: σ is the action of conjugation by y on $F[x]$, $\mathrm{N}(\lambda)$ is preserved for the norm of elements in $F[x]$, $u = \lambda_0 + \lambda_1 y + \lambda_2 y^2$ for $\lambda_0, \lambda_1, \lambda_2 \in F[x]$, and $\eta = \lambda_1 \cdot \sigma\lambda_2$. Also $b = \sigma\lambda_0 - \lambda_0$, and $\lambda_0 = a + bx$ for $a, b \in F$. Similarly, whenever we specify an element u', the same notation is used: $u' = \lambda'_0 + \lambda'_1 y + \lambda'_2 y^2$, $\eta' = \lambda'_1 \cdot \sigma\lambda'_2$, and $\lambda'_0 = a' + b'x$.

REMARK 4.1: *For every $\alpha \in F$ we have that $u + \alpha$ is at distance $1\frac{1}{2}$ from z.*

Proof: Case 1 of Proposition 3.4 (with z, u in place of x, y and $u + \alpha$ in place of u) gives the chain

$$u + \alpha \longleftrightarrow z + \alpha u^{-1} z \longleftrightarrow z^{-1} u \longleftrightarrow z \longleftrightarrow u. \qquad ∎$$

Proof of Theorem 2.6: **Case 1:** $\lambda_0 \in F$. Note that $\operatorname{tr}(\eta) = 0$ by Equation (2). If $\lambda_2 = 0$, then we have the chain

$$y \longleftrightarrow x \longleftrightarrow \mathrm{Y}_A \longleftrightarrow \mathrm{X}_A \longleftrightarrow u \longleftrightarrow z$$

by Proposition 3.4. So we assume $\lambda_2 \neq 0$.

Case 1.1: $\lambda_1 = 0$. Then $u = \lambda_0 + \lambda_2 y^2$. Set

$$\tilde{z} = -x - \frac{\lambda_0 x}{\gamma \cdot \sigma\lambda_2} y,$$

and check that $\tilde{z}, u$ form a standard pair of generators. Compute that

$$\tilde{z}u = \lambda_0 x - \frac{\lambda_0^2 x}{\gamma\cdot\sigma\lambda_2}y - x\lambda_2 y^2,$$

and set $u' = \tilde{z}u$. Then for u' we have $b' = \sigma(\lambda_0 x) - \lambda_0 x = \lambda_0$, $a' = \lambda_0' - b'x = 0$, and $\eta' = \lambda_1'\cdot\sigma\lambda_2' = \frac{1}{\gamma}\lambda_0^2(x+x^2)$.

Case 1.1.1: $\lambda_0 \neq 0$ (so that $\lambda_0' \notin F$). Compute that $\gamma(\sigma^2\eta' - \eta') = x\lambda_0^2 = b'\lambda_0'$, so by Proposition 3.7, u' is at distance $1\frac{1}{2}$ from x, and we have the following chain:

$$y \longleftrightarrow x \longleftrightarrow \mathrm{Y}_A \longleftrightarrow \mathrm{X}_A \longleftrightarrow u' \longleftrightarrow \tilde{z} \longleftrightarrow u \longleftrightarrow z.$$

Case 1.1.2: $\lambda_0 = 0$. Then $u = \lambda_2 y^2$ and thus $-x+u, u$ form a standard pair of generators. Choose $u' = (-x+u)u = (\gamma\lambda_2\cdot\sigma^2\lambda_2)y - (x\lambda_2)y^2$, so that we have $\lambda_0' = 0$, $\lambda_2' \neq 0$, $\lambda_1' \neq 0$, and $\eta' = \lambda_1'\cdot\sigma\lambda_2' = -\gamma\,\mathrm{N}(\lambda_2)\sigma(x) \notin F$. By Case (b) of Proposition 3.4, u' is at distance $1\frac{1}{2}$ from x, and the resulting chain is

$$y \longleftrightarrow x \longleftrightarrow \lambda y \longleftrightarrow x + \lambda y \longleftrightarrow u' \longleftrightarrow -x + \lambda_2 y^2 \longleftrightarrow \lambda_2 y^2 = u \longleftrightarrow z$$

for $\lambda = -x(x-1)/\gamma\cdot\sigma\lambda_2$.

Case 1.2: $\lambda_1 \neq 0$. If $\lambda_2 = 0$, or $\lambda_2 \neq 0$ but $\eta \notin F$, there is a chain

$$y \longleftrightarrow x \longleftrightarrow \mathrm{Y}_A \longleftrightarrow \mathrm{X}_A \longleftrightarrow u \longleftrightarrow z$$

by Proposition 3.4. So suppose $\lambda_2 \neq 0$, and $\eta \in F^*$. Choose

$$\alpha = \frac{\gamma\eta^2}{\mathrm{N}(\lambda_1)} - \lambda_0;$$

then for $u' = u + \alpha$ we have that $\lambda_1' = \lambda_1 \neq 0$, $\lambda_2' = \lambda_2 \neq 0$, $\lambda_0' = \alpha + \lambda_0 \in F$, and $\eta' = \eta$. But now we have $\lambda_0'\,\mathrm{N}(\lambda_1') = \eta'^2\gamma$, so from Case (c) of Proposition 3.4 and Remark 4.1, we get the chain

$$y \longleftrightarrow x \longleftrightarrow \lambda y \longleftrightarrow x + \lambda y \longleftrightarrow u' \longleftrightarrow z + \alpha u^{-1}z \longleftrightarrow z^{-1}u \longleftrightarrow z \longleftrightarrow u$$

where $\lambda = -x\lambda_2/\sigma\lambda_1$.

Case 2: $\lambda_0 \notin F$. In view of Remark 4.1, it is enough to show that there is some $\alpha \in F$ such that $x, u + \alpha$ are at distance $1\frac{1}{2}$. Recall that $\lambda_0 = a + bx$ where $a, b \in F$, so by Equation (2) we also have $\gamma\eta = \eta_0 + \eta_1 x + b^2x^2$ for $\eta_0, \eta_1 \in F$. Choose $\alpha = b - a - \eta_1/b$; then for $u' = u + \alpha$ we have that $\eta' = \eta$, and $\gamma(\sigma^2\eta - \eta) = b^2(x+1) - \eta_1 = b\lambda_0 + b\alpha = b\lambda_0'$. By Proposition 3.7 we thus have the chain

$$x \longleftrightarrow \lambda_2\cdot\sigma^2\lambda_2\cdot y \longleftrightarrow x - b^{-1}\lambda_2 y^2 \longleftrightarrow u' \longleftrightarrow z + \alpha u^{-1}z \longleftrightarrow z^{-1}u \longleftrightarrow z,$$

and we are done. ∎

5. The geometry of XY_A

Let A be a division algebra of degree 3 over a field F of characteristic $p = 3$. In this section we describe some properties of the graph XY_A and the graphs induced on X_A and Y_A, and present some special subgraphs. It seems reasonable to slightly alter the notation for this purpose.

Recall the equivalence relations defined in Remark 2.4. In this section we let X_A,Y_A denote the sets of equivalence classes (rather than the sets of points, as done previously). Again, XY_A is the bipartite graph whose vertices are $\mathrm{X}_A \cup \mathrm{Y}_A$, with an edge connecting the classes $[x], [y]$ iff x, y are a standard pair of generators. We view X_A and Y_A as subgraphs of XY_A, where two points $x, x' \in \mathrm{X}_A$ are connected iff there is some $y \in \mathrm{Y}_A$ such that $(x, y), (x', y) \in \mathrm{XY}_A$, and similarly for Y_A. Thus the distance induced by XY_A on X_A and Y_A is the usual distance in graphs.

Theorem 2.6 bounds the diameter of X_A to be ≤ 3, and this bound is shown to be exact in Corollary 3.5. Applying Remark 2.2, we see that the diameter of Y_A is bounded by 4. A lower bound of 3 is given by Corollary 3.6

Fix some $y \in \mathrm{Y}_A$. The elements $x \in \mathrm{X}_A$ connected to y are at distance 1 from one another, so they form a complete subgraph in X_A. The same thing happens in Y_A around every $x \in \mathrm{X}_A$.

Subgraphs of XY_A are more interesting. Proposition 2.5 shows that X_A and Y_A are simple graphs (i.e., there are no multiple paths between neighbors). It follows that XY_A does not contain squares. Let x, y be a fixed standard pair of generators, and let $\gamma = y^3$. Set $\tilde{y} = \gamma + y - y^2$ and $\tilde{x} = x + xy$. Then we get the following hexagon:

$$\begin{tikzcd}
 & xy \arrow[r, leftrightarrow] & \tilde{x} \arrow[dr, leftrightarrow] & \\
x \arrow[ur, leftrightarrow] \arrow[dr, leftrightarrow] & & & xy + \tilde{y} \\
 & y \arrow[r, leftrightarrow] & x + \gamma - \tilde{y} \arrow[ur, leftrightarrow] &
\end{tikzcd}$$

This can be generalized, to the following:

$$\begin{tikzcd}
x \arrow[dr, leftrightarrow] \arrow[dd, leftrightarrow] & & & \\
 & xy + \alpha y \arrow[dr, leftrightarrow] & & \\
y \arrow[dd, leftrightarrow] & & \tilde{x} + \alpha y \arrow[r, leftrightarrow] & \tilde{y} \\
 & xy + \tilde{y} + \alpha y \arrow[ur, leftrightarrow] & & \\
x + \gamma - \tilde{y} \arrow[ur, leftrightarrow] & & &
\end{tikzcd}$$

For every $\alpha \in F$, this figure is a triangle in X_A, together with the corresponding triangle in Y_A. As α varies, the complex is rotated along the fixed axis

$x \longleftrightarrow y \longleftrightarrow x+\gamma-\tilde{y}$, with all the heads of the resulting triangles connected to a single point $\tilde{y}$. In particular, we get infinitely many different chains of length $1\frac{1}{2}$ connecting x and $\tilde{y}$. It also shows a point (x) connected to a star (the points $\{\tilde{x}+ay\}$ around $\tilde{y}$) but not to its center, and other similar phenomenon.

References

[1] A. A. Albert, *Structure of Algebras*, American Mathematical Society Colloquium Publications, Vol. XXIV, American Mathematical Society, Providence, RI, 1961.

[2] S. Amitsur, L. H. Rowen and J.-P. Tignol, *Division algebras of degree* 4 *and* 8 *with involution*, Israel Journal of Mathematics **33** (1979), 133–148.

[3] S. U. Chase, *Two results on central simple algebras*, Communications in Algebra **12** (1984), 2279–2289.

[4] W. Fischer, *On Twisted Cyclic Algebras and the Chain Equivalence of Kummer Elements*, Doctoral Dissertation, Regensburg University, Germany, July 1999.

[5] N. Jacobson, *Finite Dimensional Division Algebras over Fields*, Springer, Berlin, 1996.

[6] M. Rost, *The chain lemma for Kummer elements of degree* 3, Comptes Rendus de l'Académie des Sciences, Paris, Série I **328** (1999), 185–190.

[7] L. H. Rowen, *Ring Theory*, Academic Press, New York, 1988.

[8] U. Vishne, *Central Simple Algebras*, Doctoral Dissertation, Bar-Ilan University, Israel, July 2000.