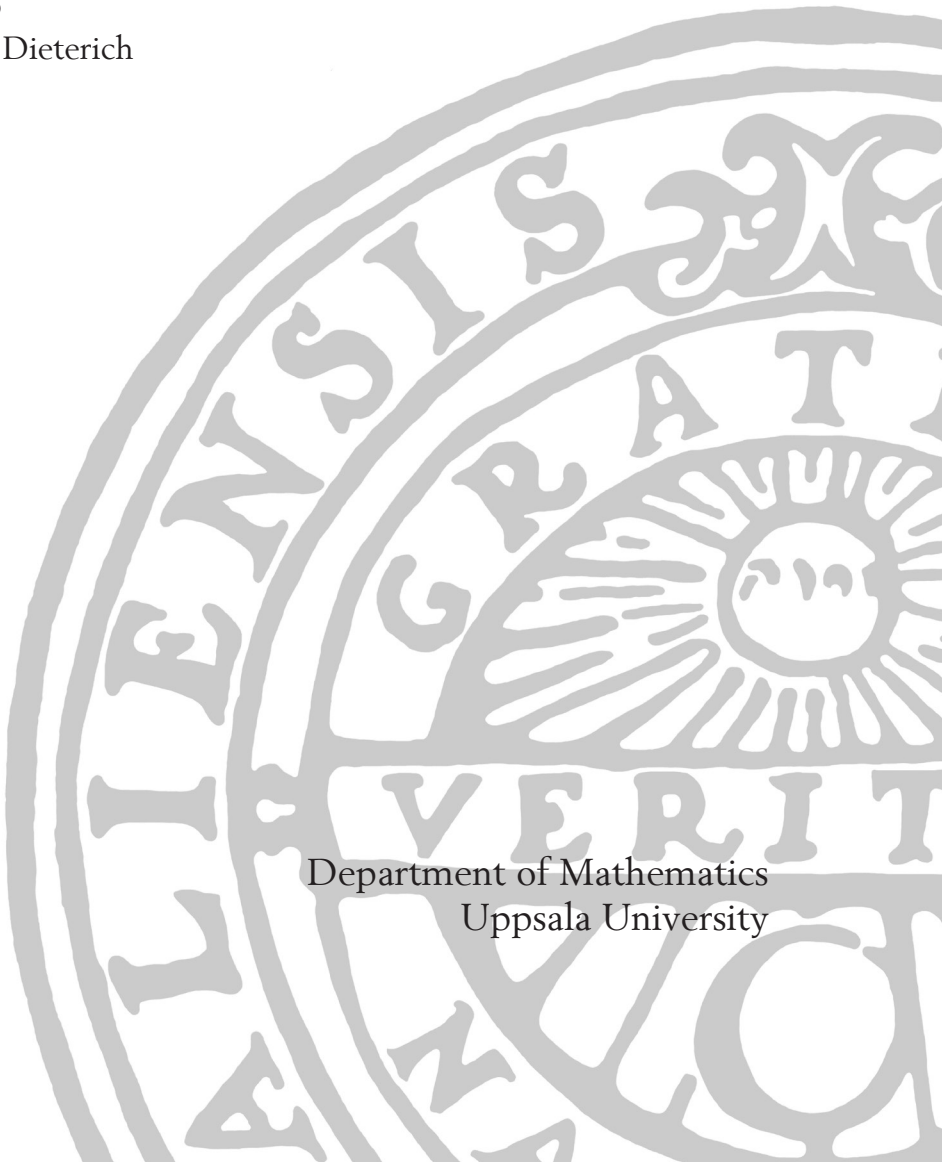
UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2015:18

On four-dimensional unital division algebras over finite fields

Anders Lindqvist

Examensarbete i matematik, 15 hp
Handledare och examinator: Ernst Dieterich
Juni 2015



Department of Mathematics
Uppsala University

On four-dimensional unital division algebras over finite fields

Anders Lindqvist

2015

Abstract

A division algebra over a field F is a nonzero F-algebra A in which division is possible, in the sense that all left and right multiplication operators by nonzero elements are invertible. For finite-dimensional A this is equivalent to A having no zero divisors. A is called unital if it has a unity element e such that $ex = x = xe$ for every x in A. In this paper we admit as ground field any finite field $k := \mathbb{F}_q$ where q is an odd prime power greater than 3, and study the class of division algebras $\mathcal{D}_4^{1*}(k) \subset \mathcal{D}_4^1(k)$ which is obtained by putting restraints on the automorphism group and left nucleus of the four-dimensional unital division algebras over k. We eventually arrive at the concept of *admissible structure constants*, which will allow a an exhaustive construction of $\mathcal{D}_4^{1*}(k)$, that depends on two parameters in k.

Keywords - Division algebra, finite field, Klein's four-group, left nucleus.

Acknowledgements

The work with this thesis would not have been possible without the help and patience of my supervisor Ernst Dieterich, to whom I owe my gratitude.

I would also like to thank my family and all my friends here in Uppsala, who have provided not only distractions but also motivation and encouragement when I needed it. Thank you.

Ille terrarum mihi praeter omnes angulus ridet.

-Horace

Uppsala, June 2015
Anders Lindqvist

Contents

1 Introduction

This Bachelor thesis is an elaborate version of the interesting but extremely tersely written paper [1] by M. Bani-Ata et al. which originates in the following question.

Given a finite group G and a finite field $k := \mathbb{F}_q$ for some prime power q, is there a division algebra over k such that $G \lesssim \mathrm{Aut}(A)$? The notation $G_1 \lesssim G_2$ has the meaning G_1 *is isomorphic to a subgroup of* G_2.

Bani-Ata took interest in studying this problem for Klein's four-group and showed in [2] that there exists such division algebras for q being a power of 2, and in [3] the same for q being an odd prime power greater than 3. We will consider the latter case and in particular study the division algebras also satisfying that $\mathbb{F}_{q^2}$ is contained in its left nucleus, with the aim to provide an exhaustive construction of this class of division algebras.

2 Preliminaries

2.1 Division algebras

The objects of interest in this paper are algebras. An algebra A over a field F, or an F-algebra, is a vector space over F with a multiplication $A \times A \to A, (a, b) \mapsto ab$ that is bilinear, i.e. such that the following holds.

1. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in A$
2. $t(ab) = (ta)b = a(tb)$ for all $t \in F$ and $a, b \in A$

and we will denote the class of algebras over a field F by $\mathcal{A}(F)$. The n-dimensional algebras over F are denoted $\mathcal{A}_n(F)$. An algebra A is called *unital* when there is a unity element $e \in A$ such

that $ea = a = ae$ for every $a \in A$. The class of n-dimensional unital algebras over the field F is denoted $\mathcal{A}_n^1(F)$.

When A is an algebra over some field F, define for every $a \in A$ the left and right multiplication operator of a

$$L_a : A \to A,\ x \mapsto ax$$
$$R_a : A \to A,\ x \mapsto xa.$$

Following from the definition of an algebra, obviously we have that R_a and L_a, for any $a \in A$, are F-linear and have the following properties

(i) $R_a(e) = a = L_a(e)\, \forall a \in A$.
(ii) $R_a + R_b = R_{a+b}$ and $L_a + L_b = L_{a+b}\, \forall a, b \in A$.
(iii) $R_e = L_e$ is the identity operator.
(iv) $tR_a(x) = R_{ta}(x)$ and $tL_a(x) = L_{ta}(x)\, \forall a, x \in A$ and $t \in F$.

We will with these tools lay a foundation to the following sections by defining a division algebra.

Definition 1. *A nonzero algebra A is called a* division algebra *if R_a and L_a are invertible for every $a \in A \setminus \{0\}$.*

Remark 1. *For finite-dimensional algebras the division property is equivalent to the non-existence of zero divisors in A, i.e. $xy = 0$ only if $x = 0$ or $y = 0$.*

The class of division algebras over F is denoted $\mathcal{D}(F)$.

Definition 2. *The left, middle and right nucleus of an algebra A is defined in the following way, respectively.*
$N_l(A) = \{a \in A : (ax)y = a(xy)\ \forall x, y \in A\}$
$N_m(A) = \{a \in A : (xa)y = x(ay)\ \forall x, y \in A\}$
$N_r(A) = \{a \in A : (xy)a = x(ya)\ \forall x, y \in A\}$

Observe that 0 is an element in each of these sets, so the nuclei are always nonempty. If A is unital, then the unity element is also an element of each nucleus of A. We will in particular study the left nucleus, which we denote by $\mathrm{N}(A)$ for a given algebra A, and in fact we see that for any unital F-algebra A, we have that $F \subseteq \mathrm{N}(A)$, where we canonically identify F with Fe. A nucleus may be interpreted as a degree of associativity for some given algebra.

Proposition 1. *Suppose that $A \in \mathcal{A}(F)$, for some field F. Then $\mathrm{N}(A)$ is a subalgebra of A.*

Proof. Begin by showing that $\mathrm{N}(A)$ is a subspace of A.
$0 \in \mathrm{N}(A)$ is obvious. For $a, b \in \mathrm{N}(A), \lambda \in F$ we have, by using the bilinearity property of A, $(\lambda a)(xy) = \lambda(a(xy)) = \lambda((ax)y) = (\lambda(ax))y = ((\lambda a)x)y$ so $\lambda a \in \mathrm{N}(A)$ and $(a+b)(xy) = a(xy) + b(xy) = (ax)y + (bx)y = (ax+bx)y = ((a+b)x)y$ so $a+b \in \mathrm{N}(A)$ and it follows that $\mathrm{N}(A)$ is a supspace of A.

Now we prove $a, b \in \mathrm{N}(A) \Rightarrow ab \in \mathrm{N}(A)$. If this holds, then $\mathrm{N}(A)$ is a subalgebra of A, finishing the proof. Let $a, b \in \mathrm{N}(A)$. Then $((ab)x)y = a(bx)y = a(b(xy)) = (ab)(xy)$ and hence $ab \in \mathrm{N}(A)$.

□

Remark 2. *Let F be a finite field and assume that $A \in \mathcal{D}^1(F)$ is finite-dimensional. Then $\mathrm{N}(A) \subseteq A$ has no zero divisors, so $\mathrm{N}(A) \in \mathcal{D}^1(F)$, and it is then a finite skew field. Following from Wedderburn's theorem, $\mathrm{N}(A)$ is a finite field.*

Definition 3. *The automorphism group $\mathrm{Aut}(A)$ of an algebra A is*

$$\mathrm{Aut}(A) := \{\phi \in \mathrm{GL}(A) | \phi(xy) = \phi(x)\phi(y)\, \forall x, y \in A\}.$$

Remark 3. *The automorphism group of an algebra A is equal to* $\{\phi \in \mathrm{GL}(A) | \phi \mathrm{R}_a \phi^{-1} = \mathrm{R}_{\phi(a)} \, \forall a \in A\}$ *since*

$$\begin{aligned} \phi(xy) = \phi(x)\phi(y) &\Leftrightarrow \phi \mathrm{R}_y(x) = \mathrm{R}_{\phi(y)}\phi(x) \\ &\Leftrightarrow \phi \mathrm{R}_y(x)\phi^{-1}(x) = \mathrm{R}_{\phi(y)}(x). \end{aligned}$$

We now make the observation that any automorphism $\sigma \in \mathrm{Aut}(A)$ will leave the nucleus invariant. Since σ is bijective it is sufficient to show that $\sigma(a) \in \mathrm{N}(A)$ for any $a \in \mathrm{N}(A)$. Let $a \in \mathrm{N}(A)$ and $x, y \in A$. Denote $x' := \sigma^{-1}(x), y' := \sigma^{-1}(y)$. Then

$$\begin{aligned} &(\sigma(a)x)y = (\sigma(a)\sigma(x'))\sigma(y') = \sigma(ax')\sigma(y') = \sigma((ax')y') = \\ &= \sigma(a(x'y')) = \sigma(a)\sigma(x'y') = \sigma(a)(\sigma(x')\sigma(y')) = \sigma(a)(xy) \end{aligned}$$

so $\sigma(a) \in \mathrm{N}(A)$ for any $a \in \mathrm{N}(A)$ and then $\sigma(\mathrm{N}(A)) = \mathrm{N}(A)$.

For the remainder of this paper, let $q > 3$ be an odd prime power. We will be interested in studying four-dimensional unital division algebras over the finite field $k := \mathbb{F}_q$ having the following properties:

1. $\mathrm{C}_2 \times \mathrm{C}_2 \lesssim \mathrm{Aut}(A)$
2. $\ell := \mathbb{F}_{q^2} \subseteq \mathrm{N}(A)$, where we canonically identify ℓ with ℓe.

The class of such algebras will be denoted $\mathcal{D}_4^{1*}(k)$.

2.2 The finite fields k and ℓ

The reader is assumed to know that for any given prime power p^m there exists exactly one field of this order, up to isomorphism. We will in this section study some properties of the finite fields k and ℓ which prove to be useful when studying $\mathcal{D}_4^{1*}(k)$. The field extension $k \subset \ell$ is a Galois extension of degree 2, whose Galois group consists of the identity map and the Frobenius automorphism

$$\mathrm{Fr} : \ell \to \ell,\ a \mapsto a^q$$

which we for simplicity will denote with a bar: $\mathrm{Fr}(a) = \overline{a}$. In particular we have $\overline{a+b} = \overline{a} + \overline{b}$ and $\overline{ab} = \bar{a}\bar{b}$ for any $a, b \in \ell$. Also $\overline{\overline{a}} = a$ for every $a \in \ell$.

Lemma 1. *Let $a \in \ell$. Then the following holds.*

$$\overline{a} = a \Leftrightarrow a \in k$$

Proof. $\overline{a} = a \Rightarrow a \in k$ is a consequence of a being in the fixed field of $\mathrm{Gal}(\ell/k)$, which is k. $a \in k \Rightarrow \overline{a} = a$ follows directly when $a = 0$. When $a \neq 0$, then a is in the multiplicative group of k, which has order $q - 1$. It follows from Lagrange's theorem that the order of a divides $q - 1$ and then $\overline{a} = a$.

□

Lemma 2. *Let $a, b, c, d \in \ell$. If $ax + b\overline{x} = cx + d\overline{x}$ holds for all $x \in \ell$, then $a = c$ and $b = d$.*

Proof. We assign the value 1 to x in order to obtain

$$a + b = c + d$$

and the value $x = z - \overline{z}$ for some $z \in \ell \setminus k$, for which it holds that $\overline{x} = \overline{z} - z = -x$ and we get

$$(a - b)x = (c - d)x$$

equivalent to $a - b = c - d$, since otherwise $x = 0$ or $x = 1$, both cases implying $\overline{x} = x$, leading to $x \in k$, contradicting our choice of x. By adding this equation to $a+b = c+d$ we get that $2a = 2c$ from which it follows that $a = c$ since the characteristic of ℓ is not equal to two. By substituting this into $a + b = c + d$ we easily see that $b = d$, concluding the proof.

□

Lemma 3. *For every $x \in k$ the following holds.*

(i) x has a square root in ℓ.
(ii) there is some $y \in \ell$ such that $x = y\overline{y}$.

Proof. The multiplicative group $\ell \setminus \{0\}$ is generated by an element $\alpha \in \ell \setminus \{0\}$ which has the order $q^2 - 1$. Now consider the element $\alpha\overline{\alpha} = \alpha^{q+1}$ which is in $k \setminus \{0\}$ since it is fixed by the Frobenius automorphism, so its order divides $q - 1$. In fact, it is equal to $q-1$ since any order $m < q-1$ would imply that $(\alpha^{q+1})^m = 1$ i.e. that $q^2 - 1$ divides $(q + 1)m < (q + 1)(q - 1) = q^2 - 1$ leading to a contradiction. Denote $\beta := \alpha^{q+1}$. Then we may conclude that β generates $k \setminus \{0\}$ and

$$k = \{0\} \cup \langle\beta\rangle = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^{q-2}\}$$
$$\ell = \{0\} \cup \langle\alpha\rangle = \{0\} \cup \{1, \alpha, \alpha^2, \cdots \alpha^{q^2-2}\}.$$

To show (i), consider the function $\gamma : \ell \to \ell, x \mapsto x^2$ and we wish to show that $k \subset \gamma(\ell)$. We have

$$\gamma(\ell) = \{0\} \cup \langle\alpha^2\rangle = \{0\} \cup \{1, \alpha^2, \alpha^4, \ldots, \alpha^{2(q^2-2)}\}$$

that is, the image of γ contains every even power of α. Since q is odd, it follows straightforward that $m(q + 1)$ is even for every m, so $(\alpha^{q+1})^m = \beta^m \in \gamma(\ell)$ and then $k \subset \gamma(\ell)$.

To show (ii), consider the function $\sigma : \ell \to k, x \mapsto x\overline{x}$ which we will show is surjective. $x\overline{x}$ is fixed under the Frobenius automorphism so it follows from Lemma 1 that it is in k for every x, so σ is well-defined. Since $\gamma(0) = 0$ and any nonzero element in ℓ may be written as α^i, for which we will have $\gamma(\alpha^i) = (\alpha^{q+1})^i = \beta^i \in k \setminus \{0\}$, we find that the first $q-1$ powers of α in ℓ will be mapped by γ onto k, and it follows that $\gamma(\ell) = k$.

□

Remark 4. *We will, for any* $x = \alpha^{i(q+1)} \in k \setminus \{0\}$ *have*

$$\sqrt{x} = \alpha^{\frac{i(q+1)}{2}} \in \ell$$

with $\alpha \in \ell$ *being a generator of* $\ell \setminus \{0\}$ *as in the proof above.* x *has exactly one other root, namely* $-\sqrt{x} = (p-1)\sqrt{x}$.

3 A as a two-dimensional vector space over ℓ

In this section we will consider a division algebra $A \in \mathcal{D}_4^{1*}(k)$ and in detail study the right multiplication operator R_a for arbitrary $a \in A$. We will find that the restrictions put on the automorphism group and nucleus of A will let us consider A as a two-dimensional vector space over ℓ. This in turn will allow us to uniquely determine R_a by a few elements in k.

Proposition 2. *If* $A \in \mathcal{D}_4^{1*}(k)$, *then* $N(A) = \ell$.

Proof. Since $N(A)$ is a subalgebra of A, it is a finite field as stated in Remark 2, so $N(A) = \mathbb{F}_{q^m}$ for some $1 \leq m \leq 4$. We also have that $\ell \subseteq N(A)$, so either $\ell \cong N(A)$ or $\mathbb{F}_{q^4} \cong N(A)$. The aim of this proof will be to show that $\mathbb{F}_{q^4} \cong N(A)$ leads to a contradiction, leaving the desired result.

Suppose that $\mathbb{F}_{q^4} \cong N(A)$. It follows, due to the order of A, that $A = N(A) \cong \mathbb{F}_{q^4}$. That is, A is a finite field. Every automorphism on A is k-linear and fixes the unity element, so $\sigma(x) = x\sigma(e) = ex = x$ for any $x \in k$ and $\sigma \in \mathrm{Aut}(A)$, so $\mathrm{Aut}(A) = \mathrm{Gal}(\mathbb{F}_{q^4}/k)$, which is cyclic and generated by the Frobenius automorphism on $\mathbb{F}_{q^4}$:

$$\mathrm{Aut}(A) = \langle \mathrm{Fr} \rangle \cong \mathrm{C}_4$$

reaching a contradiction since $\mathrm{C}_2 \times \mathrm{C}_2 \lesssim \mathrm{Aut}(A)$.

□

We have shown that the nucleus of $A \in \mathcal{D}_4^{1*}(k)$ is equal to ℓ, and hence the condition $a(bx) = (ab)x$ for any $a, b \in \ell$, $x \in A$ is fulfilled, so A is also a vector space over ℓ. The other axioms of vector spaces are fulfilled by A being a unital algebra. As a vector space over ℓ, A is two-dimensional and has some basis $\underline{b} = (b_1, b_2)$ with $b_1, b_2 \in A$.

Remark 5. *A is a vector space over ℓ, but not an ℓ-algebra since $t(ab) = (ta)b$ is shown to hold for any $t \in \ell$ and $a, b \in A$, but $t(ab) = a(tb)$ does not hold in general.*

3.1 The automorphism group of A

Proposition 3. $\mathrm{Aut}(A) < \Gamma\mathrm{L}(2, q^2)$ with $\Gamma\mathrm{L}(2, q^2) :=$

$$\{\zeta : (x, y) \mapsto (\sigma(x)\,\sigma(y))\mathrm{M} : \sigma \in \mathrm{Aut}(\ell), \mathrm{M} \in \mathrm{GL}(2, q^2)\}.$$

Proof. Consider any $\gamma \in \mathrm{Aut}(A)$. Let $a \in A$ with $a = xb_1 + yb_2$ and $x, y \in k$. We have $\gamma(b_1) = b_{11}b_1 + b_{12}b_2, \gamma(b_2) = b_{21}b_1 + b_{22}b_2$ for some $b_{11}, b_{12}, b_{21}, b_{22} \in \ell$. Then

$$\begin{gathered}\gamma(a) = \gamma(xb_1+yb_2) = \gamma(xb_1)+\gamma(yb_2) = \gamma(x)\gamma(b_1)+\gamma(y)\gamma(b_2) = \\ = \gamma(x)(b_{11}b_1 + b_{12}b_2) + \gamma(y)(b_{21}b_1 + b_{22}b_2) = \\ (\gamma(x)b_{11} + \gamma(y)b_{21})b_1 + (\gamma(x)b_{12} + \gamma(y)b_{22}))b_2\end{gathered}$$

As γ leaves $\mathrm{N}(A) = \ell$ invariant, γ induces an automorphism on ℓ which we denote by $\sigma \in \mathrm{Aut}(\ell)$. Then

$$\begin{gathered}(\gamma(a))_{\underline{b}} = (\sigma(x)b_{11} + \sigma(y)b_{21}, \sigma(x)b_{12} + \sigma(y)b_{22})) = \\ (\sigma(x)\,\sigma(y))\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}\end{gathered}$$

with $M = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in \mathrm{GL}(2, q^2)$ because otherwise $\det(M) = b_{11}b_{22} - b_{12}b_{21} = 0$, eqiuivalent to $b_{11}b_{22} = b_{12}b_{21}$, which implies $\frac{b_{11}}{b_{21}} = \frac{b_{12}}{b_{22}} = t$ for some $t \in \ell$ and then $b_1 = tb_2$, i.e. b_1 and b_2 are linearly dependent, which is not the case since they form a basis in A. We have shown that $\gamma \in \Gamma\mathrm{L}(2, q^2)$ for any $\gamma \in \mathrm{Aut}(A)$ and hence $\mathrm{Aut}(A) < \Gamma\mathrm{L}(2, q^2)$.

□

We will use $b_1 = e \in \ell$ as the first basis element and then the other must be chosen in $A \setminus \ell$. It is assumed that we have $E \cong \mathrm{C}_2 \times \mathrm{C}_2 \lesssim \mathrm{Aut}(A)$, which suggests that there are two elements in the automorphism group that will generate E. We will in the following result present two such automorphisms.

Lemma 4. *There is a second basis element $b_2 \in A$ such that the maps $T : \ell \times \ell \to \ell \times \ell$, $\varphi : \ell \times \ell \to \ell \times \ell$ with*

$$T(x, y) = (x, -y),\ \varphi(x, y) = (\overline{x}, \overline{y})$$

are generators of $E < \mathrm{Aut}(A)$.

Proof. First, for T, φ to be generators of E, we demand that $T^2 = \mathbb{1} = \varphi^2$ and $T\varphi = \varphi T$. $T^2 = \mathbb{1}$ is obvious. For φ^2 we get $\varphi^2(x, y) = (\overline{\overline{x}}, \overline{\overline{y}}) = (x, y)$, so $\varphi^2 = \mathbb{1}$ and from the fact that q is odd it follows that for all $x, y \in \ell$, $T\varphi(x, y) = T(\overline{x}, \overline{y}) = (\overline{x}, -\overline{y}) = \varphi(x, -y) = \varphi T(x, y)$ and hence $T\varphi = \varphi T$.

Secondly, we need to show that there exists a b_2 such that T and φ are automorphisms. Let $E = \{\mathbb{1}, \alpha, \beta, \gamma\}$ where $\alpha\beta = \gamma = \beta\alpha$. Bani-Ata showed in [4] that E acts freely on A, i.e. there exist a k-basis $\underline{a} = \{a_{\mathbb{1}}, a_\alpha, a_\beta, a_\gamma\}$ in A such that

$$\epsilon(a_\delta) = a_{\epsilon\delta}\ \forall \epsilon, \delta \in E.$$

Using this basis of A we will now determine the eigenspaces for 1 and -1 of α and β. The matrix representation of each automorphism $\epsilon \in E$ is on the form

$$(\epsilon)_{\underline{a}} = \begin{pmatrix} (\epsilon(a_{\mathbb{1}}))_{\underline{a}} \\ (\epsilon(a_\alpha))_{\underline{a}} \\ (\epsilon(a_\beta))_{\underline{a}} \\ (\epsilon(a_\gamma))_{\underline{a}} \end{pmatrix}$$

so we get

$$(\alpha)_{\underline{a}} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \; (\beta)_{\underline{a}} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

and by recalling from linear algebra that the eigenspace for λ of some operator with the matrix M is equal to the nullspace of $M - \lambda I_4$ we find that, in the basis $\underline{a}$,

$$\mathrm{Eg}_\alpha(1) = k \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \oplus k \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \; \mathrm{Eg}_\alpha(-1) = k \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \oplus k \begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \end{pmatrix}$$

$$\mathrm{Eg}_\beta(1) = k \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \oplus k \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \; \mathrm{Eg}_\beta(-1) = k \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \oplus k \begin{pmatrix} 0 \\ -1 \\ 0 \\ 1 \end{pmatrix}$$

Now set

$$S_1 = \mathrm{Eg}_\alpha(1) \cap \mathrm{Eg}_\beta(1), \; S_2 = \mathrm{Eg}_\alpha(1) \cap \mathrm{Eg}_\beta(-1)$$
$$S_3 = \mathrm{Eg}_\alpha(-1) \cap \mathrm{Eg}_\beta(1), \; S_4 = \mathrm{Eg}_\alpha(-1) \cap \mathrm{Eg}_\beta(-1)$$

and we find

$$S_1 = k\begin{pmatrix}1\\1\\1\\1\end{pmatrix},\ S_2 = k\begin{pmatrix}-1\\-1\\1\\1\end{pmatrix},\ S_3 = k\begin{pmatrix}-1\\1\\-1\\1\end{pmatrix},\ S_4 = k\begin{pmatrix}-1\\1\\1\\-1\end{pmatrix}$$

and then $A = S_1 \oplus S_2 \oplus S_3 \oplus S_4$ as a kE-module. Now choose $\underline{s} = (s_1, s_2, s_3, s_4)$ by taking an $s_i \in S_i$ for every $1 \leq i \leq 4$. Then $\underline{s}$ is a new k-basis in A, for which it holds that

$$(\mathbb{1})_{\underline{s}} = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\ (\alpha)_{\underline{s}} = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&-1&0\\0&0&0&-1\end{pmatrix}$$

$$(\beta)_{\underline{s}} = \begin{pmatrix}1&0&0&0\\0&-1&0&0\\0&0&1&0\\0&0&0&-1\end{pmatrix},\ (\gamma)_{\underline{s}} = \begin{pmatrix}1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&1\end{pmatrix}$$

The k-linear subspaces $k \subset l \subset A$ are kE-submodules. We have that $k = ke \subset S_1$ since e is fixed by every automorphism and in particular α and β. From $\dim_k(k) = \dim_k(S_1)$ it now follows that $k = ke = S_1$, and thus we may choose $s_1 = e$. From Maschke's theorem (p. 383 of [5], thm. 7.4) and Krull-Schmidt's theorem (p. 349 of [5], thm. 8.10) it follows that $\ell = S_1 \oplus S_i$ for some $i \in \{2, 3, 4\}$. Thus we have

$$A = S_1 \oplus S_i \oplus S_j \oplus S_k = \ell b_1 \oplus S_j \oplus S_k$$

where $\{i, j, k\} = \{2, 3, 4\}$ and now we set $(b_1, b_2) := (s_1, s_j) = (e, s_j)$ which is ℓ-linearly independent, and hence an ℓ-basis in A.

Moreover, $\ell b_2 = \ell s_j = ks_j \oplus ks_k$, since $ks_j = kb_2 \subset \ell b_2$ are kE-submodules, and then Maschke's Theorem and Krull-Schmidt's Theorem imply that $\ell b_2 = S_j \oplus S_k = ks_j \oplus ks_k$.

Now, denote the automorphism induced by $\sigma \in \mathrm{Aut}(A)$ on $\ell \times \ell$ with $\hat{\sigma}$. If we have $i = 2$ then $(b_1, b_2) = (e, s_3)$ with $\alpha_\ell = \mathbb{1}_\ell$ and $\alpha(b_2) = -b_2$. We also find that $\beta_\ell = \mathrm{Fr}$ (as it is not the identity), $\beta(b_2) = b_2$ and recall from the proof of Proposition 3 that we have

$$\hat{\alpha}(x,y) = (\alpha_\ell(x), \alpha_\ell(y)) \begin{pmatrix} (\alpha(e))_{\underline{b}} \\ (\alpha(b_2))_{\underline{b}} \end{pmatrix} =$$

$$= (x,y) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = (x,-y) = T(x,y)$$

$$\hat{\beta}(x,y) = (\beta_\ell(x), \beta\ell(y)) \begin{pmatrix} (\beta(b_1))_{\underline{b}} \\ (\beta(b_2))_{\underline{b}} \end{pmatrix} =$$

$$= (\overline{x}, \overline{y}) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = (\overline{x}, \overline{y}) = \varphi(x,y)$$

and similarly it can be shown that when $i = 3$ we get that $\hat{\beta} = T$ and $\hat{\alpha} = \varphi$. For $i = 4$ it holds that $\hat{\gamma} = T$ and $\hat{\alpha} = \varphi$, so in any of these cases it holds that we can select $(b_1, b_2) = (e, b_2)$ such that T and φ are automorphisms generating E.

□

3.2 The right multiplication operator

For a given element $a = xe + yb_2 \in A$ the operator R_a is represented in the ℓ-basis $\underline{b} = \{e, b_2\}$ by a matrix

$$R_{(x,y)} = \begin{pmatrix} R_{(x,y)}(1) \\ R_{(x,y)}(b_2) \end{pmatrix} = \begin{pmatrix} x & y \\ f(x,y) & g(x,y) \end{pmatrix}$$

for some k-linear maps $f, g : \ell \times \ell \to \ell$. The linearity is a direct consequence of the properties (ii) and (iv) of the right multiplication operator, described in section 2.1. To reveal more information about the operator, we will need the following lemma.

Lemma 5. *For any k-linear map $f : \ell \times \ell \to \ell$ there are uniquely determined $a_0, a_1, a_2, a_3 \in \ell$ such that*

$$f(x,y) = a_0x + a_1\bar{x} + a_2y + a_3\bar{y}.$$

Proof. Since f is a map from a four-dimensional vector space over k into a two-dimensional vector space over k, and k is of order q, we have that there are exactly q^8 different such maps. Note that for any $\mathbf{a} = (a_0, a_1, a_2, a_3)$ with $a_i \in \ell$ for $1 \leq i \leq 4$ we have that the map

$$f_{\mathbf{a}} : (x,y) \mapsto a_0x + a_1\bar{x} + a_2y + a_3\bar{y}$$

obviously is k -linear.

We will now prove that any two different choices of quadruples will lead to different maps. Take $\mathbf{a} = (a_0, a_1, a_2, a_4)$,
$\mathbf{b} = (b_0, b_1, b_2, b_3)$ with $a_i \in \ell$ and $b_i \in \ell$ for $1 \leq i \leq 4$ and assume that $f_{\mathbf{a}} = f_{\mathbf{b}}$, i.e. that

$$a_0x + a_1\overline{x} + a_2y + a_3\overline{y} = b_0x + b_1\overline{x} + b_2y + b_3\overline{y}$$

for all $(x,y) \in \ell \times \ell$. For $x = 0$, the equality $a_2y + a_3\overline{y} = b_2y + b_3\overline{y}$ holds for every $y \in \ell$ and for $y = 0$ we get that

$a_0x + a_1\overline{x} = b_0x + b_1\overline{x}$ holds for every $x \in \ell$. It now follows from Lemma 2 that $a_0 = b_0, a_1 = b_1, a_2 = b_2, a_3 = b_3$. Since two quadruples are equal when their correpsponding maps are, we may conclude that different quadruples cannot lead to equal maps. Since the number of possible quadruples of elements in ℓ are q^8 we may conclude that any k-linear map from $\ell \times \ell$ to ℓ may be uniquely determined in this way.

□

This result directly allows us to uniquely describe the matrix $R_{(x,y)}$ using only eight elements of ℓ. It will however prove to be even more powerful than that; we will in the next result reduce the number of elements to three, and demand that they are in k.

Proposition 4. *For a division algebra $A \in \mathcal{D}_1^{4^*}(k)$ the following holds.*

(i) The matrix $R_{(x,y)}$ is invertible for any $(x, y) \neq (0, 0)$.

(ii) There are $a_2, a_3, b_0, b_1 \in k$ such that $b_0 + b_1 = 1$ and

$$R_{(x,y)} = \begin{pmatrix} x & y \\ a_2y + a_3\overline{y} & b_0x + b_1\overline{x} \end{pmatrix}$$

for any $(x, y) \in \ell \times \ell$.

Proof. The invertability of the matrix follows from the fact that it represents the right multiplication operator which for $(x, y) \neq (0, 0)$ is invertible.

For the second part, we notice that T and ϕ are automorphisms on $\ell \times \ell$, and in particular $TR_vT^{-1} = R_{T(v)}$ and T is represented by the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. By Lemma 5, there are elements $a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3 \in k$ such that

$$R_{(x,y)} = \begin{pmatrix} x & y \\ a_0x + a_1\overline{x} + a_2y + a_3\overline{y} & b_0x + b_1\overline{x} + b_2y + b_3\overline{y} \end{pmatrix} = \\ = \begin{pmatrix} x & y \\ f(x,y) & g(x,y) \end{pmatrix}$$

and we have that

$$R_{T(x,y)} = R_{(x,-y)} = \begin{pmatrix} x & -y \\ f(x,-y) & g(x,-y) \end{pmatrix} = TR_{(x,y)}T^{-1} = \\ = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} x & y \\ f(x,y) & g(x,y) \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} x & -y \\ -f(x,y) & g(x,y) \end{pmatrix}$$

so $-f(x,y) = f(x,-y)$ and $g(x,-y) = g(x,y)$, and since the functions are uniquely determined by $a_0, \ldots, b_3$ we get

$$-a_0x - a_1\overline{x} - a_2y - a_3\overline{x} = a_0x + a_1\overline{x} - a_2y - a_3\overline{y} \\ b_0x + b_1\overline{x} - b_2y - b_3\overline{y} = b_0x + b_1\overline{x} + b_2y + b_3\overline{y}$$

from which it follows that $2a_0x + 2a_1\overline{x} = 0$, $2b_2y + 2b_3\overline{y} = 0$ and then $a_0x + a_1\overline{x} = 0, b_2y + b_3\overline{y} = 0$ for every $(x,y) \in \ell \times \ell$, since the characteristic of ℓ is not equal to 2. But $0x + 0\overline{x} = 0 = 0y + 0\overline{y}$ so it follows from Lemma 2 that $a_0 = a_1 = b_2 = b_3 = 0$. Now we study the operator $R_{(\overline{x},\overline{y})}$. We directly get that it is represented by the matrix

$$R_{\phi(x,y)} = R_{(\overline{x},\overline{y})} = \begin{pmatrix} \overline{x} & \overline{y} \\ f(\overline{x},\overline{y}) & g(\overline{x},\overline{y}) \end{pmatrix}$$

but we may also determine the matrix row-wise by applying $R_{(x,y)}$ to each of the basis vectors

$$R_{\phi(x,y)} = \begin{pmatrix} (e(\overline{x}e + \overline{y}b_2))_{\underline{b}} \\ (b_2(\overline{x}e + \overline{y}b_2))_{\underline{b}} \end{pmatrix}$$

and we obviously get the first row $(\overline{x} \;\; \overline{y})$. For the second row, we make the observation that ϕ maps $(b_2)_{\underline{b}} = (0,1)$ to itself, and see that $b_2(\overline{x}e + \overline{y}b_2) = \phi(b_2)\phi(xe + yb_2) = \phi(b_2(xe + yb_2)) = \phi(R_{(x,y)}(b_2))$ but $R_{(x,y)}(b_2)$ is defined to be $(f(x,y) \;\; g(x,y))$ so the second row will be $(\overline{f(x,y)} \;\; \overline{g(x,y)})$.

Then we have

$$\begin{pmatrix} \overline{x} & \overline{y} \\ \overline{f(x,y)} & \overline{g(x,y)} \end{pmatrix} = \begin{pmatrix} \overline{x} & \overline{y} \\ f(\overline{x},\overline{y}) & g(\overline{x},\overline{y}) \end{pmatrix}$$

from which it follows that $f(\overline{x},\overline{y}) = \overline{f(x,y)}$, $g(\overline{x},\overline{y}) = \overline{g(x,y)}$. That is,

$$a_2\overline{y} + a_3 y = \overline{a_2 y + a_3\overline{y}} = \overline{a_2}\overline{y} + \overline{a_3} y$$
$$b_0\overline{x} + b_1 x = \overline{b_0 x + b_1\overline{x}} = \overline{b_0}\overline{x} + \overline{b_1} x$$

and from Lemma 2 it then follows that a_2, a_3, b_0, b_1 are all fixed under the Frobenius automorphism, and hence they are in k, according to Lemma 1. In conclusion we have

$$\mathbb{1} = R_{(1,0)} = \begin{pmatrix} 1 & 0 \\ 0 & b_0 + b_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

so $b_0 + b_1 = 1$.

□

The right multiplication operator might now be written

$$R_{(x,y)} = \begin{pmatrix} x & y \\ a_2 y + a_3 \overline{y} & x + b_1(\overline{x} - x) \end{pmatrix}$$

which allows us to uniquely define the operator by a triple of elements from k. In the next section we will introduce the concept of admissible structure constants which will be used to identify divison algebras in $\mathcal{D}_4^{1*}(k)$ with triples in k^3.

4 Admissible structure constants

For elements $a_2, a_3, b_1 \in k$ we define $A(a_2, a_3, b_1)$ to be the 4-dimensional k-algebra isomorphic to $\ell \times \ell$ with multiplication

$$(a,b)(x,y) = R_{(x,y)}(a,b) = (a,b)\begin{pmatrix} x & y \\ a_2 y + a_3 \bar{y} & x + b_1(\bar{x} - x) \end{pmatrix}$$

Definition 4. *The triple* $(a_2, a_3, b_1) \in k^3$ *is called a triple of* admissible structure constants *if* $A(a_2, a_3, b_1)$ *is a division algebra. The set of all triples of admissible strucure constants will be denoted* $\mathcal{S} \subset k^3$.

Let $r(x,y) := b_0 x^2 - a_2 y^2 + b_1 x\overline{x} - a_3 y\overline{y}$ denote the determinant of the matrix $R_{(x,y)}$. From the definition of division algebras it follows that $r(x,y) \neq 0 \, \forall (x,y) \neq (0,0)$ exactly when (a_2, a_3, b_1) is a triple of admissible structure constants and $b_0 = 1 - b_1$.

Lemma 6. *Let* $(a_2, a_3, b_1) \in \mathcal{S}$. *If we set* $b_0 = 1 - b_1$, *the elements* a_2 *and* b_0 *are nonzero and we may then make the substitution* $u := \sqrt{b_0}x$, $v := \sqrt{a_2}y$ *to get*

$$r(x,y) = u^2 - v^2 + \frac{b_1}{\sqrt{b_0}\overline{\sqrt{b_0}}} u\overline{u} - \frac{a_3}{\sqrt{a_2}\overline{\sqrt{a_2}}} v\overline{v}.$$

Proof. Assume that $a_2 = 0$, then $r(1, y) = b_0 + b_1 - a_3 y\overline{y}$ and we have that $r(0, 1) = a_2 + a_3 = a_3 \neq 0$. Since $\frac{b_0+b_1}{a_3} \in k$ it follows from Lemma 3 that there is some $y \in \ell$ with $\frac{b_0+b_1}{a_3} = y\overline{y}$, and then $r(1, y) = 0$ for this y, reaching a contradiction. Likewise, we will by taking $r(x, 1)$ and assuming that $b_0 = 0$ find an x such that $r(x, 1) = 0$. Hence a_2, b_0 are nonzero. As shown in Lemma 3 they have a square root which will be nonzero so the above expression is well-defined and obtained straightforward from the given substitution. □

Lemma 7. *Let $a, b \in k$. Then the following are equivalent.*

(i) $h(x, y) := x^2 - y^2 + ax\overline{x} + by\overline{y} \neq 0 \, \forall (x, y) \neq (0, 0)$

(ii) $a = b \neq 0$ *and* $1 - a^2$ *is not a square in* k.

Proof. See [1], the proof of Proposition 1. □

5 Main results

The goal of this section is to further reduce the number of elements in k that are needed to fully determine a division algebra over k, by presenting a method of finding every triple of admissible structure constants. This is presented as our main result. Denote the set of squares in k by k_{sq}.

Theorem 1. *Let* $\mathcal{R} = \{(a_2, b_0) \in k^* \times k^* | 2b_0 - 1 \notin k_{\text{sq}}\}$ *and define the map*

$$\varphi : \mathcal{R} \to k^3,\ (a_2, b_0) \mapsto (a_2, \frac{1-b_0}{\sqrt{b_0}\overline{\sqrt{b_0}}}\sqrt{a_2}\overline{\sqrt{a_2}}, 1-b_0).$$

Then $\varphi(\mathcal{R}) = \mathcal{S}$.

Proof. We begin by showing $\varphi(\mathcal{R}) \subseteq \mathcal{S}$. Assume that we have some $(a_2, b_0) \in \mathcal{R}$ and define $b_1 := 1 - b_0, a_3 = -\frac{1-b_0}{\sqrt{b_0}\overline{\sqrt{b_0}}}\sqrt{a_2}\overline{\sqrt{a_2}}$ and $a := \frac{1-b_0}{\sqrt{b_o}\overline{\sqrt{b_0}}} =: b$. Then

$$1-a^2 = 1-\frac{(1-b_0)^2}{(\sqrt{b_0}\overline{\sqrt{b_0}})^2} = 1-\frac{1-2b_0+b_0^2}{b_0\overline{\sqrt{b_0}}^2} = 1-\frac{1-2b_0+b_0^2}{b_0\overline{b_0}} =$$
$$= 1 - \frac{1-2b_0+b_0^2}{b_0^2} = \frac{b_0^2-1+2b_0-b_0^2}{b_0^2} = \frac{2b_0-1}{b_0^2}$$

and since $2b_0 - 1$ is not a square in k, while b_0^2 is, it follows that $1 - a^2 \notin (k)_{sq}$. Lemma 7 now grants that

$$h(u, v) = u^2 - v^2 + au\overline{u} + bv\overline{v} \neq 0\, \forall (u, v) \neq (0, 0)$$

and by substituting $x := \frac{u}{\sqrt{b_0}}, y := \frac{v}{\sqrt{a_2}}$ we obtain

$$h(u,v) = b_0x^2 - a_2y^2 + \frac{1-b_0}{\sqrt{b_0}\overline{\sqrt{b_0}}}\sqrt{b_0}\overline{\sqrt{b_0}}x\overline{x} + \frac{1-b_0}{\sqrt{b_o}\overline{\sqrt{b_0}}}\sqrt{a_2}\overline{\sqrt{a_2}}y\overline{y}$$
$$= b_0x^2 - a_2y^2 + b_1x\overline{x} - a_3y\overline{y} = r(x,y) \neq 0 \,\forall (u,v) \neq (0,0)$$

and whenever $(u,v) \neq (0,0)$ it also holds that $(x,y) \neq (0,0)$ so in fact we have $r(x,y) \neq 0 \ \forall (x,y) \neq (0,0)$ and then $\varphi(a_2,b_0) \in \mathcal{S}$ for every $(a_2,b_0) \in \mathcal{R}$, i.e. $\varphi(\mathcal{R}) \subseteq \mathcal{S}$.

Now show that $\mathcal{S} \subseteq \varphi(\mathcal{R})$. Take some $(a_2,a_3,b_1) \in \mathcal{S}$. The substitution stated in Lemma 6 gives us that

$$r(x,y) = u^2 - v^2 + \frac{b_1}{\sqrt{b_0}\overline{\sqrt{b_0}}}u\overline{u} - \frac{a_3}{\sqrt{a_2}\overline{\sqrt{a_2}}}v\overline{v} \neq 0 \,\forall (x,y) \neq (0,0)$$

where $u := \sqrt{b_0}x, v := \sqrt{a_2}y$. From Lemma 7 it follows that $a = b \neq 0$ and $1 - a^2 \notin (k)_{sq}$ where $a = \frac{b_1}{\sqrt{b_0}\overline{\sqrt{b_0}}}$. So $1 - a^2 = \frac{2b_0 - 1}{b_0^2}$ by the same argument as above, and then $2b_0 - 1 \notin (k)_{sq}$. We also see, by taking $b = -\frac{a_3}{\sqrt{a_2}\overline{\sqrt{a_2}}}$, since $a = b$ that
$a_3 = -\frac{b_1}{\sqrt{b_0}\overline{\sqrt{b_0}}}\sqrt{a_2}\overline{\sqrt{a_2}} = -\frac{1-b_0}{\sqrt{b_0}\overline{\sqrt{b_0}}}\sqrt{a_2}\overline{\sqrt{a_2}}$ and as shown in the proof of Lemma 6, $a_2 \neq 0 \neq b_0$ so $(a_2,b_0) \in \mathcal{R}$ and $\varphi(a_2,b_0) = (a_2,a_3,b_1)$. It follows that $\mathcal{S} \subseteq \varphi(\mathcal{R})$ and we may conclude $\varphi(\mathcal{R}) = \mathcal{S}$, finishing the proof.

□

The following result is a direct consequence of the steps taken in sections 3 and 4.

Corollary 1. *If $A \in \mathcal{D}_4^{1*}(k)$, then $A \cong A(a_2,a_3,b_1)$ for some $(a_2,a_3,b_1) \in \mathcal{S}$.*

References

[1] Bani-Ata, M., Aldhafeeri, S., Belgacem, F., Laila, M. : *On four-dimensional unital division algebras over finite fields*, Algebr. Represent. Theor. 2014

[2] Bani-Ata, M.: *The semifields of order q^4, q is a power of 2.* Commun. Algebra **36** (09), 3347-3352 (2008)

[3] Bani-Ata, M., Neumann, A., Rawashdeh, A., Hering, C.: *On the existence of semifields of prime power order admitting free automorphism groups.* J. Geom. **86**(2006)

[4] Bani-Ata, M.: *Semifields as free modules.* Q. J. Math. **62**(1), 1-6 (2011)

[5] Grillet, P. A.: *Abstract Algebra (Graduate texts in Mathematics)*, 2nd edition, Springer Science + Business Media LLC, 2007.