sciendo

Communications in Mathematics 28 (2020) 89–102
DOI: 10.2478/cm-2020-0012

Division algebras that generalize Dickson semifields

Daniel Thompson

Abstract. We generalize Knuth's construction of Case I semifields quadratic over a weak nucleus, also known as generalized Dickson semifields, by doubling of central simple algebras. We thus obtain division algebras of dimension $2s^2$ by doubling central division algebras of degree s. Results on isomorphisms and automorphisms of these algebras are obtained in certain cases.

1 Introduction

The commutative division algebras constructed by Dickson [6] yield proper semifields of even dimension over finite fields. They have been subsequently studied in many papers, for example in [2], [3], [8], [12]. Knuth recognised that Dickson's commutative division algebras also appear as a special case of another family of semifields [10]: A subalgebra L of a division algebra S is called a *weak nucleus* if $x(yz) - (xy)z = 0$, whenever two of x, y, z lie in L. Semifields which are quadratic over a weak nucleus are split into two cases; Case I semifields contain Dickson's construction as the only commutative semifields of this type. Due to this, Case I semifields are also called *generalized Dickson semifields*. Their construction is as follows: given a finite field $K = GF(p^n)$ for some odd prime p, define a multiplication on $K \oplus K$ by

$$(u, v)(x, y) = (uv + c\alpha(v)\beta(y), \sigma(u)y + vx),$$

for some automorphisms α, β, σ of K not all the identity automorphism and $c \in K \setminus K^2$. This construction produces a proper semifield containing p^{2n} elements. Further work on semifields quadratic over a weak nucleus was done in [7] and [4].

In this paper, we define a doubling process which generalizes Knuth's construction in [10]: for a central simple associative algebra D/F or finite field extension

2020 MSC: 17A35, 17A36, 17A60
Key words: Nonassociative algebras, division algebras, automorphisms
Affiliation: School of Mathematical Science, University of Nottingham, Nottingham NG7 2QL, United Kingdom
E-mail: daniel.thompson1@nottingham.ac.uk

K/F, we define a multiplication on the F-vector space $D \oplus D$ (resp. $K \oplus K$) as

$$(u, v)(x, y) = (ux + c\sigma_1(v)\sigma_2(y), \sigma_3(u)y + v\sigma_4(x))$$

for some $c \in D^\times$ and $\sigma_i \in \mathrm{Aut}_F(D)$ for $i = 1, 2, 3, 4$ (resp. $c \in K^\times$ and $\sigma_i \in \mathrm{Aut}_F(K)$). This yields an algebra of dimension $2 \dim_F(D)$ or $2[K : F]$ over F. Over finite fields, we show this construction is the same as the one presented in [10] and yields examples of some Hughes-Kleinfeld, Knuth and Sandler semifields (for example, see [5]). Hughes-Kleinfeld, Knuth and Sandler semifield constructions were studied over arbitrary base fields in [1]. Dickson's commutative semifield construction was introduced over finite fields in [6] and considered over any base field of characteristic not 2 when K is a finite cyclic extension in [2]. This was generalized to a doubling of any finite field extension and central simple algebras in [12]. The construction described in [10] has never been considered as a doubling of central simple algebras.

After preliminary results and definitions, we define a doubling process for both a central simple algebra D/F and a finite field extension K/F; we recover the multiplication used in Knuth's construction of generalized Dickson semifields when $\sigma_4 = \mathrm{id}$. Further, we show that it is sufficient to only consider the case where $\sigma_4 = \mathrm{id}$. We find criteria for them to be division algebras. We then determine the nucleus and commutator of these algebras and examine both isomorphisms and automorphisms. The results of this paper are part of the author's PhD thesis written under the supervision of Dr S. Pumplün.

2 Definitions and preliminary results

In this paper, let F be a field. We define an F-algebra A as a finite dimensional F-vector space equipped with a (not necessarily associative) bilinear map $A \times A \to A$ which is the multiplication of the algebra. A is a *division algebra* if for all nonzero $a \in A$ the maps $L_a \colon A \to A$, $x \mapsto ax$, and $R_a \colon A \to A$, $x \mapsto xa$, are bijective maps. As A is finite dimensional, A is a division algebra if and only if there are no zero divisors [11].

The *associator* of $x, y, z \in A$ is defined to be $[x, y, z] := (xy)z - x(yz)$. Define the *left, middle* and *right nuclei* of A as

$$\mathrm{Nuc}_l(A) := \{x \in A : [x, A, A] = 0\},$$
$$\mathrm{Nuc}_m(A) := \{x \in A : [A, x, A] = 0\},$$

and

$$\mathrm{Nuc}_r(A) := \{x \in A : [A, A, x] = 0\}.$$

The left, middle and right nuclei are associative subalgebras of A. Their intersection

$$\mathrm{Nuc}(A) := \{x \in A : [x, A, A] = [A, x, A] = [A, A, x] = 0\}$$

is the *nucleus* of A. The *commutator* of A is the set of elements which commute with every other element,

$$\mathrm{Comm}(A) := \{x \in A : xy = yx, \forall y \in A\}.$$

The *center* of A is given by the intersection of $\mathrm{Nuc}(A)$ and $\mathrm{Comm}(A)$,

$$Z(A) := \{x \in \mathrm{Nuc}(A) : xy = yx, \forall y \in A\}.$$

For two algebras A and B, any isomorphism $f\colon A \to B$ maps $\mathrm{Nuc}_l(A)$ isomorphically onto $\mathrm{Nuc}_l(B)$ (similarly for the middle and right nuclei).

An algebra A is *unital* if there exists an element $1_A \in A$ such that

$$x1_A = 1_A x = x$$

for all $x \in A$. A *central simple* algebra over F is an algebra A such that $Z(A) = F$ and A has no two-sided ideals except $\{0\}$ and A. Every central simple F-algebra A has dimension n^2 over F for some $n \in \mathbb{N}$; we call n the *degree* of A.

A form $N\colon A \to F$ is called *multiplicative* if

$$N(xy) = N(x)N(y)$$

for all $x, y \in A$ and *nondegenerate* if we have $N(x) = 0$ if and only if $x = 0$. Note that if $N\colon A \to F$ is a nondegenerate multiplicative form and A is a unital algebra, it follows that $N(1_A) = 1_F$. We assume that N is invariant under automorphisms of A. Every central simple algebra admits a uniquely determined nondegenerate multiplicative form, called the *norm* of the algebra [9].

3 A doubling process which generalizes Knuth's construction

Let D be a central simple associative division algebra of degree n over F with nondegenerate multiplicative norm form $N_{D/F}\colon D \to F$. Given $\sigma_i \in \mathrm{Aut}_F(D)$ for $i = 1, 2, 3, 4$ and $c \in D^\times$, define a multiplication on the F-vector space $D \oplus D$ by

$$(u, v)(x, y) = (ux + c\sigma_1(v)\sigma_2(y), \sigma_3(u)y + v\sigma_4(x)).$$

We denote the F-vector space endowed with this multiplication by

$$\mathrm{Cay}(D, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4).$$

We can also define an analogous multiplication on $K \oplus K$ for a finite field extension K/F for some $c \in K^\times$ and $\sigma_i \in \mathrm{Aut}_F(K)$. We similarly denote these algebras by $\mathrm{Cay}(K, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$. This yields unital F-algebras of dimension $2\dim_F(D)$ and $2[K : F]$ respectively. When $\sigma_4 = \mathrm{id}$, our multiplication is identical to the one used in the construction of generalized Dickson semifields. For every subalgebra $E \subseteq D$ such that $c \in E^\times$ and $\sigma_i|_E = \phi_i \in \mathrm{Aut}_F(E)$ for $i = 1, 2, 3, 4$, it is clear that $\mathrm{Cay}(E, c, \phi_1, \phi_2, \phi_3, \phi_4)$ is a subalgebra of $\mathrm{Cay}(D, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$.

Theorem 1. *(i) If $N_{D/F}(c) \neq N_{D/F}(a)^2$ for all $a \in D^\times$, then*

$$\mathrm{Cay}(D, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$$

is a division algebra.

(ii) If K is separable over F and $N_{K/F}(c) \neq N_{K/F}(a)^2$ for all $a \in K^\times$, then $\mathrm{Cay}(K, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$ is a division algebra.

Proof. (i) Suppose $(0,0) = (u,v)(x,y)$ for some $u,v,x,y \in D$ such that

$$(u,v) \neq (0,0) \neq (x,y)\,.$$

This is equivalent to

$$ux + c\sigma_1(v)\sigma_2(y) = 0\,, \tag{1}$$
$$\sigma_3(u)y + v\sigma_4(x) = 0\,. \tag{2}$$

Assume $y = 0$. Then by (1), $ux = 0$, so $u = 0$ or $x = 0$ as D is a division algebra. As $(x,y) \neq (0,0)$, we must have $x \neq 0$ so $u = 0$. Then by (2), $v\sigma_4(x) = 0$ which implies $v = 0$ or $x = 0$. This is a contradiction, thus it follows that $y \neq 0$. By (2), $v\sigma_4(x) = -\sigma_3(u)y$. Let $N = N_{D/F}\colon D \to F$. Taking norms of both sides, we have

$$\begin{aligned} &N(v)N(x) = (-1)^n N(u)N(y) \\ \implies &N(u) = (-1)^n N(v)N(x)N(y)^{-1}, \end{aligned} \tag{3}$$

since $y \neq 0$. Similarly, taking norms of (1) yields

$$N(c)N(\sigma_1(v))N(\sigma_2(y)) = N(-1)N(u)N(x)\,,$$

which rearranges to

$$(-1)^n N(u)N(x) - N(c)N(v)N(y) = 0\,.$$

Using this and (3) implies

$$\begin{aligned} 0 &= (-1)^n N(u)N(x) - N(c)N(v)N(y) \\ &= ((-1)^{2n} N(v)N(x)N(y)^{-1})N(x) - N(c)N(v)N(y) \\ &= N(v)N(y)\big[(N(x)N(y)^{-1})^2 - N(c)\big]. \end{aligned} \tag{4}$$

If $N(v) = 0$, then $v = 0$ so by (1) $ux = 0$ implies $x = 0$ (else $(u,v) = (0,0)$). Thus (4) implies $N(c) = 0 \notin F^\times$, which cannot happen as $c \neq 0$. Thus we must have $N(v) \neq 0$ and $(N(x)N(y)^{-1})^2 = N(c)$. Hence, if $N(c) \neq N(a)^2$ for all $a \in D$ there cannot exist any zero divisors in A, so A is a division algebra.

(ii) The proof follows analogously as in (i); we require K to be separable over F so that $N_{K/F}(\sigma(x)) = N_{K/F}(x)$ for all $\sigma \in \mathrm{Aut}_F(K)$ and $x \in K$. □

Remark 1. If $F = \mathbb{F}_{p^s}$ and $K = \mathbb{F}_{p^r}$ is a finite extension of F, then $\mathrm{Aut}_F(K)$ is cyclic of order r/s and is generated by ϕ^s, where ϕ is defined by the Frobenius automorphism $\phi(x) = x^p$ for all $x \in K$. Then $A = \mathrm{Cay}(K, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$ is a division algebra if and only if c is not a square in K. The proof of this is analogous to the one given in [10, p. 53].

Although it appears that we obtain some additional finite semifields from the doubling process that were not considered in [10], we show that this is not the case:

Theorem 2. *Let D and D' be two central simple F-algebras (respectively, K and L finite field extensions of F) and $g, h\colon D \to D'$ be two F-algebra isomorphisms. Let*

$$A_D = \mathrm{Cay}(D, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4) \quad \text{and} \quad B_{D'} = \mathrm{Cay}(D', g(c)b^2, \phi_1, \phi_2, \phi_3, \phi_4)$$

for some $b \in F^\times$ (resp.

$$A_K = \mathrm{Cay}(K, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4) \quad \text{and} \quad B_L = \mathrm{Cay}(L, g(c)\phi_1(b)\phi_2(b), \phi_1, \phi_2, \phi_3, \phi_4)$$

for some $b \in K^\times$). If

$$\phi_i = \begin{cases} g \circ \sigma_i \circ h^{-1} & \text{for } i = 1, 2, \\ h \circ \sigma_i \circ g^{-1} & \text{for } i = 3, 4, \end{cases} \tag{5}$$

then the map $G\colon A \to B$, $G(u, v) = (g(u), h(v)b^{-1})$ defines an F-algebra isomorphism.

Proof. We show the proof in the central simple algebra case. It follows analogously when we take field extensions K and L. Clearly G is F-linear, additive and bijective. It only remains to show that G is multiplicative; that is,

$$G((u, v)(x, y)) = G(u, v)G(x, y)$$

for all $u, v, x, y \in D$. First we have

$$\begin{aligned} G(u, v)G(x, y) &= (g(u), h(v)b^{-1})(g(x), h(y)b^{-1}) \\ &= \big(g(u)g(x) + g(c)b^2\phi_1(h(v)b^{-1})\phi_2(h(y)b^{-1}), \phi_3(g(u))h(y)b^{-1} \\ &\quad + h(v)b^{-1}\phi_4(g(x))\big) \\ &= \big(g(ux) + g(c)\phi_1(h(v))\phi_2(h(y)), [\phi_3(g(u))h(y) + h(v)\phi_4(g(x))]b^{-1}\big). \end{aligned}$$

It similarly follows that

$$\begin{aligned} G((u, v)(x, y)) &= G(ux + c\sigma_1(v)\sigma_2(y), \sigma_3(u)y + v\sigma_4(x)) \\ &= (g(ux + c\sigma_1(v)\sigma_2(y)), h(\sigma_3(u)y + v\sigma_4(x))b^{-1}) \\ &= (g(ux) + g(c)g(\sigma_1(v))g(\sigma_2(y)), [h(\sigma_3(u))h(y) + h(v)h(\sigma_4(x))]b^{-1}). \end{aligned}$$

By (5), we obtain equality and thus G is an F-algebra isomorphism. □

Corollary 1. *Let $g, h \in \mathrm{Aut}_F(D)$ (resp. $\mathrm{Aut}_F(K)$) and $b \in F^\times$ (resp. $b \in K^\times$). Let*

$$B_D = \mathrm{Cay}(D, g(c)b^2, \phi_1, \phi_2, \phi_3, \phi_4)$$

(resp. $B_K = \mathrm{Cay}(K, g(c)\phi_1(b)\phi_2(b), \phi_1, \phi_2, \phi_3, \phi_4)$ for some $b \in K^\times$). If

$$\phi_i = \begin{cases} g \circ \sigma_i \circ h^{-1} & \text{for } i = 1, 2, \\ h \circ \sigma_i \circ g^{-1} & \text{for } i = 3, 4, \end{cases}$$

then the map $G\colon A \to B$, $G(u, v) = (g(u), h(v)b^{-1})$ defines an F-algebra isomorphism.

Corollary 2. *Every generalised Dickson algebra* $A_D = \mathrm{Cay}(D, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$ *is isomorphic to an algebra of the form* $\mathrm{Cay}(D, c, \sigma_1', \sigma_2', \sigma_3', \mathrm{id})$ *(analogously for the algebras* A_K*).*

Proof. Consider the map $G\colon D \oplus D \to D \oplus D$ defined by $G(u, v) = (u, \sigma_4^{-1}(v))$. By Theorem 2, this yields the isomorphism

$$\mathrm{Cay}(D, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4) \cong \mathrm{Cay}(D, c, \sigma_1 \circ \sigma_4, \sigma_2 \circ \sigma_4, \sigma_4^{-1} \circ \sigma_3, \mathrm{id})\,. \qquad \square$$

This confirms that when K is a finite field, every algebra obtained from this construction is isomorphic to a generalized Dickson semifield. Thus, for finite fields the results given in [10] can be translated across to this construction via the isomorphism given in Corollary 2. This motivates the investigation of analogue results for the construction with both a central simple algebra D/F and a finite field extension K/F, which have not been considered previously.

3.1 Commutator and nuclei

Unless otherwise stated, we will write

$$A_D = \mathrm{Cay}(D, c, \sigma_1, \sigma_2, \sigma_3, \mathrm{id}) \quad \text{and} \quad A_K = \mathrm{Cay}(K, c, \sigma_1, \sigma_2, \sigma_3, \mathrm{id})$$

without loss of generality; if $\sigma_4 \neq \mathrm{id}$, we may use Corollary 2 to obtain an isomorphic algebra $\mathrm{Cay}(D, c, \sigma_1', \sigma_2', \sigma_3', \mathrm{id})$.

Proposition 1. *If* $\sigma_1 = \sigma_2$ *and* $\sigma_3 = \mathrm{id}$, $\mathrm{Comm}(A_D) = F \oplus F$ *and* A_K *is commutative. Otherwise,* $\mathrm{Comm}(A_D) = F \oplus S$*, where*

$$S = \{v \in D : yv = v\sigma_1^{-1} \circ \sigma_2(y) \text{ and } \sigma_3(y)v = vy\}\,,$$

and $\mathrm{Comm}(A_K) = \mathrm{Fix}(\sigma_3) \oplus 0 \subseteq K$.

Proof. We compute this only for A_D as the computations for A_K follow analogously. By definition, $(u, v) \in \mathrm{Comm}(A_D)$ if and only if for all $x, y \in D$,

$$(u, v)(x, y) = (x, y)(u, v)\,.$$

This is equivalent to

$$ux + c\sigma_1(v)\sigma_2(y) = xu + c\sigma_1(y)\sigma_2(v), \tag{6}$$

$$\sigma_3(u)y + vx = \sigma_3(x)v + yu, \tag{7}$$

for all $x, y \in D$. If $y = 0$ and $x \neq 0$, the first equation implies $u \in Z(D) = F$; if $x = 0$ and $y \neq 0$, we must have $v \in D$ satisfies $\sigma_1(v)\sigma_2(y) = \sigma_1(y)\sigma_2(v)$. If we let $y \in F$, then we have $\sigma_1(v) = \sigma_2(v)$. If we use this condition in (6), we see that $v \in D$ must satisfy $yv = v\sigma_1^{-1} \circ \sigma_2(y)$ for all $y \in D$. Under these assumptions on u and v, (6) is satisfied for all $x, y \in D$. Similar deduction yields that (7) is satisfied for all $x, y \in D$ if and only if $\sigma_3(x)v = vx$. $\square$

Remark 2. If $\mathrm{Comm}(A_D) \neq F$ or $\mathrm{Comm}(A_K) \not\subseteq K$, then $\sigma_1 = \sigma_2$ and $\sigma_3 = \sigma_4 = \mathrm{id}$ by Lemma 1. Hence, every such algebra is isomorphic to the generalisation of commutative Dickson algebras as defined in [12].

Proposition 2. *(i) Suppose that at least one of the following holds:*

- $\sigma_2 \neq \mathrm{id}$,
- $\sigma_1 \neq \sigma_2 \circ \sigma_3$,
- $\sigma_1 \neq \sigma_3 \circ \sigma_2$.

Then

$$\mathrm{Nuc}_l(A_D) = \{(x,0) \in D \oplus D : \sigma_1 \circ \sigma_3(x) = c^{-1}xc\} \subseteq D \oplus 0$$

and

$$\mathrm{Nuc}_l(A_K) = \mathrm{Fix}(\sigma_1 \circ \sigma_3) \oplus 0 \subseteq K \oplus 0\,.$$

(ii) Suppose that at least one of the following holds:

- *there exists some $x \in D$ (resp. K) such that $\sigma_1 \circ \sigma_3(x) \neq c^{-1}xc$,*
- *$\sigma_2 \neq \mathrm{id}$,*
- *for all $v \in D$, there exists some $x \in D$ (resp. K) such that*

$$\sigma_3(c)\sigma_3(\sigma_1(x))\sigma_3(\sigma_2(v)) \neq xc\sigma_1(v)\,.$$

Then $\mathrm{Nuc}_m(A) = \mathrm{Fix}(\sigma_3^{-1} \circ \sigma_2^{-1} \circ \sigma_1) \oplus 0$ for both $A = A_D$ and $A = A_K$.

(iii) Suppose that at least one of the following holds:

- *there exists some $x \in D$ (resp. K) such that $\sigma_1 \circ \sigma_3(x) \neq c^{-1}xc$,*
- *$\sigma_1 \neq \sigma_2 \circ \sigma_3$,*
- *for all $y \in D$, there exists some $x, x' \in D$ (resp. K) such that*

$$\sigma_3(c)\sigma_3(\sigma_1(x))x'y \neq xcx'\sigma_2(y)\,.$$

Then $\mathrm{Nuc}_r(A) = \mathrm{Fix}(\sigma_2) \oplus 0$ for both $A = A_D$ and $A = A_K$.

Proof. (i) First consider all elements of the form $(k,0)$ for $k \in D$. Then $(k,0) \in \mathrm{Nuc}_l(A_D)$ if and only if we have $((k,0)(u,v))(x,y) = (k,0)((u,v)(x,y))$ for all $u,v,x,y \in D$. Computing this directly, we obtain the equations

$$\begin{aligned} kux + c\sigma_1(\sigma_3(k)v)\sigma_2(y) &= kux + kc\sigma_1(v)\sigma_2(y)\,,\\ \sigma_3(ku)y + \sigma_3(k)vx &= \sigma_3(k)\sigma_3(u)y + \sigma_3(k)vx\,. \end{aligned}$$

These hold for all $u,v,x,y \in D$ if and only if $c\sigma_1 \circ \sigma_3(k) = kc$, i.e. we have $\sigma_1 \circ \sigma_3(k) = c^{-1}kc$. The same calculations yield that this holds for all $u,v,x,y \in D$ if and only if $\sigma_1 \circ \sigma_3(k) = k$.

The associator is linear in each component, so we have

$$[(k,m),(u,v),(x,y)] = [(k,0),(u,v),(x,y)] + [(0,m),(u,v),(x,y)]\,.$$

It is clear that is

$$(k,0),(0,m) \in \mathrm{Nuc}_l(A_D)\,,$$

then $(k,m) \in \mathrm{Nuc}_l(A_D)$. Conversely, suppose

$$(k,m) \in \mathrm{Nuc}_l(A_D)\,.$$

As $[(k,m),(u,v),(x,y)] = 0$ is satisfied for all $u,v,x,y \in D$, we consider $x = u = 0$; from this, we obtain $c\sigma_1(\sigma_3(k)v)\sigma_2(y) = kc\sigma_1(v)\sigma_2(y)$ must be satisfied for all $v,y \in D$. Comparing this with the computations for

$$((k,0)(u,v))(x,y) = (k,0)((u,v)(x,y))\,,$$

we see that these conditions are identical. So $(k,m) \in \mathrm{Nuc}_l(A_D)$ implies $(k,0) \in \mathrm{Nuc}_l(A_D)$. As

$$[(0,m),(u,v),(x,y)] = [(k,m),(u,v),(x,y)] - [(k,0),(u,v),(x,y)]$$

and $\mathrm{Nuc}_l(A_D)$ is closed under addition, it is clear that $(0,m) \in \mathrm{Nuc}_l(A_D)$. Thus it follows that (k,m) lies in the left nucleus if and only if $(k,0)$ and $(0,m)$ are both also in the left nucleus. Thus to show that there are no other elements in the left nucleus, it suffices to check that there are no elements of the form $(0,m)$, $m \in D$, in $\mathrm{Nuc}_l(A_D)$.

If $(0,m) \in \mathrm{Nuc}_l(A_D)$, then for all $u,v,x,y \in D$ we have

$$((0,m)(u,v))(x,y) = (0,m)((u,v)(x,y))\,.$$

This holds for all $u,v,x,y \in D$ if and only if

$$c\sigma_1(m)[\sigma_2(v)x + \sigma_1(u)\sigma_2(y)] = c\sigma_1(m)[\sigma_2(v)\sigma_2(x) + \sigma_2(\sigma_3(u))\sigma_2(y)]\,,$$
$$\sigma_3(c\sigma_1(m)\sigma_2(v))y = mc\sigma_1(v)\sigma_2(y)\,.$$

When $m = 0$, this is satisfied for all $u,v,x,y \in D$. If $m \neq 0$, we consider various elements of D in order to determine some conditions on the σ_i. For example, substituting $v = x = 0$ and $y = 1$ yields that $\sigma_1(u) = \sigma_2(\sigma_3(u))$ for all $u \in D$; i.e. $\sigma_1 = \sigma_2 \circ \sigma_3$. Via other similar choices of u,v,x and y, we obtain the additional conditions that $\sigma_1 = \sigma_3 \circ \sigma_2$ and $\sigma_2 = \mathrm{id}$. Under these assumptions, we see that there may exist some $m \neq 0$ such that

$$((0,m)(u,v))(x,y) = (0,m)((u,v)(x,y))$$

for all $u,v,x,y \in D$.

(ii) and (iii) follow analogously: we first determine all elements of the form $(k,0)$ in $\mathrm{Nuc}_m(A)$ and $\mathrm{Nuc}_r(A)$ respectively. As the associator is linear in the each component, it then suffices to look at the elements of the form $(0,m)$. As in (i), we determine these conditions by considering various elements of D. □

Corollary 3. *A_K is associative if and only if $A_K = \mathrm{Cay}(K, c, \sigma, \mathrm{id}, \sigma, \mathrm{id})$ for some $\sigma \in \mathrm{Aut}_F(K)$ such that $\sigma^2 = \mathrm{id}$ and $c \in \mathrm{Fix}(\sigma)$. That is, A_K is a quaternion algebra over $\mathrm{Fix}(\sigma)$.*

As the center of A is defined as

$$Z(A) = \mathrm{Comm}(A) \cap \mathrm{Nuc}_l(A) \cap \mathrm{Nuc}_m(A) \cap \mathrm{Nuc}_r(A)\,,$$

we see that $Z(A_K) \subseteq K$ unless $\sigma_1 = \sigma_2 = \sigma$ and $\sigma_3 = \sigma_4 = \sigma^{-1}$. If

$$A_K = \mathrm{Cay}(K, c, \sigma, \sigma, \sigma^{-1}, \sigma^{-1})$$

for some $\sigma \in \mathrm{Aut}_F(K)$, then A_K is a commutative, associative algebra.

3.2 Isomorphisms

In certain cases, the maps defined in Theorem 2 and Corollary 1 are the only possible isomorphisms between two algebras constructed via our generalised Cayley-Dickson doubling:

Theorem 3. *Let $A_K = \mathrm{Cay}(K, c, \sigma_1, \sigma_2, \sigma_3, \mathrm{id})$ and $B_L = \mathrm{Cay}(L, c', \phi_1, \phi_2, \phi_3, \mathrm{id})$. Suppose that $G\colon A_K \to B_L$ is an isomorphism that restricts to an isomorphism $g\colon K \to L$. Then G is of the form $G(x, y) = (g(x), g(y)b)$ such that $\phi_i \circ g = g \circ \sigma_i$ for $i = 1, 2, 3$ and some $b \in L^\times$ such that $g(c) = c'\phi_1(b)\phi_2(b)$.*

Proof. Suppose G is an isomorphism from A_K to B_L such that $G|_K = g\colon K \to L$ is an isomorphism. Then for all $x \in K$, we have $G(x, 0) = (g(x), 0)$. Let $G(0, 1) = (a, b)$ for some $a, b \in L$. As G is multiplicative, this yields

$$\begin{aligned} G(x, y) &= G(x, 0) + G(\sigma_3^{-1}(y), 0)G(0, 1) \\ &= (g(x), 0) + (g(\sigma_3^{-1}(y)), 0)(a, b) \\ &= (g(x) + g(\sigma_3^{-1}(y))a, \phi_3(g(\sigma_3^{-1}(y)))b), \end{aligned}$$

and

$$\begin{aligned} G(x, y) &= G(x, 0) + G(0, 1)G(y, 0) \\ &= (g(x), 0) + (a, b)(g(y), 0) \\ &= (g(x) + g(y)a, bg(y)). \end{aligned}$$

It follows that either $\phi_3 \circ g \circ \sigma_3^{-1} = g$ or $b = 0$. However, if $b = 0$ this would imply that G was not surjective, which is a contradiction to the assumption that G is an isomorphism. Thus it follows that $\phi_3 \circ g \circ \sigma_3^{-1} = g$. Additionally, we have either $g \circ \sigma_3^{-1} = g$ or $a = 0$.

Consider $G((0, 1)^2) = G(0, 1)^2$. This gives

$$(a^2 + c'\phi_1(b)\phi_2(b), \phi_3(a)b + ba) = (g(c), 0)\,.$$

As we have established that $b \neq 0$, this implies that $\phi_3(a) = -a$. If $a \neq 0$, we obtain $g \circ \sigma_3^{-1} = g$. Substituting this into the condition $\phi_3 \circ g \circ \sigma_3^{-1} = g$, we conclude that $\phi_3 = \mathrm{id}$. This contradicts $\phi_3(a) = -a$. Thus we must in fact have $a = 0$ and $G(x, y) = (g(x), g(y)b)$ where $\phi_3 \circ g = g \circ \sigma_3$ and $g(c) = c'\phi_1(b)\phi_2(b)$. Computing $G(u, v)G(x, y) = G((u, v)(x, y))$ gives the remaining conditions. □

As the isomorphism defined in Corollary 2 restricts to an automorphism of K, Corollary 2 can be employed in conjugation with the above result to determine isomorphisms when $\sigma_4 \neq \mathrm{id}$ or $\phi_4 \neq \mathrm{id}$. The proof of Theorem 3 does not hold when we consider the algebras A_D, as we rely heavily on the commutativity of K.

Corollary 4. *Suppose that $G\colon A_K \to B_K$ is an isomorphism that restricts to an automorphism g of K. Then G is of the form $G(x,y) = (g(x), g(y)b)$ such that $\phi_i \circ g = g \circ \sigma_i$ for $i = 1,2,3$ and some $b \in K^\times$ such that $g(c) = c'\phi_1(b)\phi_2(b)$.*

If $\mathrm{Nuc}_l(A) = \mathrm{Nuc}_l(B) = K$, all isomorphisms from $A \to B$ must restrict to an automorphism of K; similar considerations are true for restrictions to the middle and right nuclei. It follows that we can determine precisely when two such algebras are isomorphic by Corollary 4.

Corollary 5. *Suppose that $G\colon A_K \to B_K$ is an isomorphism that restricts to an automorphism of K. If K is a separable extension of F, we must have $N_{K/F}(cc'^{-1}) = N_{K/F}(b^2)$ for some $b \in K^\times$.*

Proof. Suppose $G\colon A_K \to B_K$ is an isomorphism that restricts to an automorphism of K. By Theorem 4, we have $g(c) = c'\phi_1(b)\phi_2(b)$. Applying norms to both side, we obtain

$$N_{K/F}(g(c)) = N_{K/F}(c'\phi_1(b)\phi_2(b)).$$

As K is a separable extension of F, it follows that $N_{K/F}(g(x)) = N_{K/F}(x)$ for all $x \in K$, $g \in \mathrm{Aut}_F(K)$. This yields $N_{K/F}(c) = N_{K/F}(c'b^2)$. As $c' \in K^\times$ and $N_{K/F}$ is multiplicative, we conclude that $N_{K/F}(cc'^{-1}) = N_{K/F}(b^2)$. □

Example 1. Let $F = \mathbb{Q}_p$ ($p \neq 2$) and K be a separable extension of $\mathbb{Q}_p$. It is well known that $(\mathbb{Q}_p^\times)^2/\mathbb{Q}_p = \{[1],[u],[p],[up]\}$ for some $u \in \mathbb{Z}_p \setminus \mathbb{Z}_p^2$. If $N_{K/F}(c)$ and $N_{K/F}(c')$ do not lie in the same coset of $(\mathbb{Q}_p^\times)^2/\mathbb{Q}_p$, there does not exist an isomorphism that restricts to K such that

$$\mathrm{Cay}(K, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4) \cong \mathrm{Cay}(K, c', \phi_1, \phi_2, \phi_3, \phi_4)$$

by Corollary 5.

3.3 Automorphisms

Theorem 4. *Let $g \in \mathrm{Aut}_F(D)$ (resp. $\mathrm{Aut}_F(K)$) such that g commutes with σ_1, σ_2, σ_3 and let $b \in F^\times$ (resp. $b \in K^\times$) such that $g(c) = b^2c$ (resp. $g(c) = \sigma_1(b)\sigma_2(b)c$). Then the map $G\colon A \to A$ defined by $G(u,v) = (g(u), g(v)b)$ is an automorphism of A_D (resp. A_K).*

This is easily checked via some long calculations.

Theorem 5. *Suppose that at least one of $\mathrm{Nuc}_l(A_K)$, $\mathrm{Nuc}_m(A_K)$, $\mathrm{Nuc}_r(A_K)$ is equal to K. Then $G\colon A_K \to A_K$ is an automorphism of A_K if and only if G has the form stated in Theorem 4.*

Proof. Let $A = A_K$. Suppose $G \in \mathrm{Aut}_F(A)$ and $\mathrm{Nuc}_l(A) = K$. As automorphisms preserve the nuclei of an algebra, G restricted to $\mathrm{Nuc}_l(A)$ must be an automorphism of K; that is, $G|_K = g \in \mathrm{Aut}_F(K)$ and so we have $G(x,0) = (g(x),0)$ for all $x \in K$.

If $\mathrm{Nuc}_l(A) \neq K$, by our assumptions one of $\mathrm{Nuc}_m(A)$ or $\mathrm{Nuc}_r(A)$ are equal to K. In either case, we can use an identical argument by restricting G to $\mathrm{Nuc}_m(A)$ or $\mathrm{Nuc}_r(A)$ respectively. As automorphisms preserve the nuclei of an algebra, G restricted to $\mathrm{Nuc}_m(A)$ (respectively $\mathrm{Nuc}_r(A)$) must be an automorphism of K. Let $G(0,1) = (a,b)$ for some $a, b \in K$. Then

$$\begin{aligned} G(x,y) &= G(x,0) + G(\sigma_3^{-1}(y),0)G(0,1) \\ &= (g(x) + g \circ \sigma_3^{-1}(y)a, \sigma_3 \circ g \circ \sigma_3^{-1}(y)b), \end{aligned}$$

and also

$$\begin{aligned} G(x,y) &= G(x,0) + G(0,1)G(y,0) \\ &= (g(x) + g(y)a, g(y)b) \end{aligned}$$

for all $x, y \in K$. Hence we must have $g \circ \sigma_3^{-1}(y)a = g(y)a$ for all $y \in K$, which implies either $\sigma_3 = \mathrm{id}$ or $a = 0$. Additionally we have $\sigma_3 \circ g \circ \sigma_3^{-1}(y)b = g(y)b$. If $b = 0$, this would imply $G(x,y) = (g(x) + g(y)a, 0)$, which is a contradiction as it implies G is not surjective. Thus we must in fact have $\sigma_3 \circ g \circ \sigma_3^{-1}(y) = g(y)$ for all $y \in K$.

Now we consider $G((0,1)^2) = G(0,1)^2$. This gives $(a,b)(a,b) = (g(c),0)$, which implies

$$\begin{aligned} a^2 + c\sigma_1(b)\sigma_2(b) &= g(c), \\ \sigma_3(a)b + ba &= 0. \end{aligned}$$

If $\sigma_3 \neq \mathrm{id}$, we already know that $a = 0$. On the other hand if $\sigma_3 = \mathrm{id}$, we obtain $2ab = 0$. As K has characteristic not 2 and $b \neq 0$, this implies $a = 0$. In either case, we obtain $c\sigma_1(b)\sigma_2(b) = g(c)$ and $G(u,v) = (g(u), g(v)b)$ with $\sigma_3 \circ g = g \circ \sigma_3$.

Finally we consider $G(u,v)G(x,y) = G((u,v)(x,y))$ for all $u, v, x, y \in K$. We obtain

$$(g(u), g(v)b)(g(x), g(y)b) = \big(g(uv + c\sigma_1(v)\sigma_2(y)), g(\sigma_3(u)y + vx)b\big)$$

which gives the equations

$$\begin{aligned} c\sigma_1(g(v)b)\sigma_2(g(y)b) &= g(c)g(\sigma_1(v)\sigma_2(y)), \\ \sigma_3(g(u))g(y)b + g(y)g(x)b &= g(\sigma_3(u)y + vx)b. \end{aligned}$$

As $g \circ \sigma_3 = \sigma_3 \circ g$, the second equation holds for all $u, v, x, y \in K$. Substituting $g(c) = c\sigma_1(b)\sigma_2(b)$ into the first equation, we obtain

$$\sigma_1(g(v))\sigma_2(g(y)) = g(\sigma_1(v))g(\sigma_2(y))$$

for all $v, y \in K$. This implies $\sigma_1 \circ g = g \circ \sigma_1$ and $\sigma_2 \circ g = g \circ \sigma_2$. Hence if G is an automorphism of A we must have $G(u,v) = (g(u), g(v)b)$ for some $g \in \mathrm{Aut}_F(K)$ such that $g \circ f = f \circ g$ for $f = \sigma_1, \sigma_2, \sigma_3$ and some $b \in K^\times$ such that

$$g(c) = \sigma_1(b)\sigma_2(b)c\,. \qquad \square$$

Corollary 6. *Suppose that at least one of* $\mathrm{Nuc}_l(A_K), \mathrm{Nuc}_m(A_K), \mathrm{Nuc}_r(A_K)$ *is equal to* K *and* $\mathrm{Aut}_F(K) = \langle\sigma\rangle$. *Then* $G\colon A_K \to A_K$ *is an automorphism of* A_K *if and only if* $G(u,v) = (\sigma^i(u), \sigma^i(v)b)$ *for some* $i \in \mathbb{Z}$ *and* $b \in K^\times$ *satisfying*

$$\sigma^i(c) = c\sigma^{\alpha_2}(b)\sigma^{\beta_2}(b)\,.$$

In the case when doubling a central simple algebra, we obtain a partial generalisation of Theorem 5. Recall that we assume $A_D = \mathrm{Cay}(D, c, \sigma_1, \sigma_2, \sigma_3, \mathrm{id})$.

Lemma 1. *Let* $G \in \mathrm{Aut}(A_D)$ *be such that* $G|_D = g \in \mathrm{Aut}_F(D)$. *Then there must exist some* $a, b \in D$, $b \neq 0$, *such that for all* $y \in D$,

$$\begin{aligned} ag(y) &= g \circ \sigma_3^{-1}(y)a\,,\\ bg(y) &= \sigma_3 \circ g \circ \sigma_3^{-1}(y)b\,. \end{aligned}$$

Proof. Suppose $G|_D = g \in \mathrm{Aut}_F(D)$. Then for all $x \in D$, we obtain

$$G(x,0) = (g(x), 0)\,.$$

Let $G(0,1) = (a,b)$ for some $a, b \in D$. It now follows that

$$\begin{aligned} G(x,y) &= G(x,0) + G(\sigma_3^{-1}(y),0)G(0,1)\\ &= (g(x) + g \circ \sigma_3^{-1}(y)a, \sigma_3 \circ g \circ \sigma_3^{-1}(y)b)\,, \end{aligned}$$

and also

$$\begin{aligned} G(x,y) &= G(x,0) + G(0,1)G(y,0)\\ &= (g(x) + ag(y), bg(y))\,. \end{aligned}$$

Setting these two equivalent expressions for $G(x,y)$ equal to each other yields the result. Note that if $b = 0$, G would no longer be surjective, which would contradict our assumption that $G \in \mathrm{Aut}(A_D)$. □

Theorem 6. *Let* $G \in \mathrm{Aut}(A_D)$ *be such that* $G|_D = g \in \mathrm{Aut}_F(D)$. *If* $\sigma_3 = \mathrm{id}$, *then* $G\colon A_D \to A_D$ *must have the form as stated in Theorem 4.*

Proof. Suppose $G|_D = g \in \mathrm{Aut}_F(D)$. Substituting $\sigma_3 = \mathrm{id}$ into Lemma 1, we see that $G(0,1) = (a,b)$ for some $a, b \in D$ such that

$$ag(y) = g(y)a, \quad bg(y) = g(y)b.$$

This is satisfied for all $y \in D$ if and only if $a, b \in F$ and so

$$G(x,y) = (g(x) + g(y)a, g(y)b)\,.$$

The remainder of this proof follows almost exactly the same to Theorem 5:

Now we consider $G((0,1)^2) = G(0,1)^2$. This gives $(a,b)(a,b) = (g(c),0)$, which implies

$$\begin{aligned} a^2 + c\sigma_1(b)\sigma_2(b) &= g(c)\\ ab + ba &= 0\,. \end{aligned}$$

As $a, b \in F$, the second equation is equivalent to $2ab = 0$. As F has characteristic not 2, this implies $a = 0$ or $b = 0$. If $b = 0$, G would not be surjective, which contradicts our assumption that G is an isomorphism. Thus we must have $a = 0$ and so we obtain $g(c) = cb^2$ and $G(u, v) = (g(u), g(v)b)$.

Finally we consider $G(u, v)G(x, y) = G((u, v)(x, y))$ for all $u, v, x, y \in D$. We obtain

$$(g(u), g(v)b)(g(x), g(y)b) = \big(g(uv + c\sigma_1(v)\sigma_2(y)), g(uy + vx)b\big)\,,$$

which gives the equations

$$\begin{aligned} c\sigma_1(g(v)b)\sigma_2(g(y)b) &= g(c)g(\sigma_1(v)\sigma_2(y)), \\ g(u)g(y)b + g(y)g(x)b &= g(uy + vx)b. \end{aligned}$$

After substituting $cb^2 = g(c)$, we conclude that this is satisfied for all $x, y, u, v \in D$ if and only if we have $\sigma_1 \circ g = g \circ \sigma_1$ and $\sigma_2 \circ g = g \circ \sigma_2$. □

For $\sigma_4 \neq \mathrm{id}$, this is equivalent to assuming that $\sigma_3 = \sigma_4$.

References

[1] C. Brown, S. Pumplün: The automorphisms of Petit's algebras. *Communications in Algebra* 46 (2) (2018) 834–849.

[2] M.V.D. Burmester: On the commutative non-associative division algebras of even order of LE Dickson. *Rendiconti di Matematica e delle sue Applicazioni. Serie V* 21 (1962) 143–166.

[3] M.V.D. Burmester: On the non-unicity of translation planes over division algebras. *Archiv der Mathematik* 15 (1) (1964) 364–370.

[4] S.D. Cohen, M.J. Ganley: Commutative semifields, two dimensional over their middle nuclei. *Journal of Algebra* 75 (2) (1982) 373–385.

[5] M. Cordero, G.P. Wene: A survey of finite semifields. *Discrete Mathematics* 208 (1999) 125–137.

[6] L.E. Dickson: On commutative linear algebras in which division is always uniquely possible. *Transactions of the American Mathematical Society* 7 (4) (1906) 514–522.

[7] M.J. Ganley: Central weak nucleus semifields. *European Journal of Combinatorics* 2 (4) (1981) 339–347.

[8] A. Hui, Y.K. Tai, P.P.W. Wong: On the autotopism group of the commutative Dickson semifield K and the stabilizer of the Ganley unital embedded in the semifield plane $\Pi(K)$. *Innovations in Incidence Geometry: Algebraic, Topological and Combinatorial* 14 (1) (2015) 27–42.

[9] M. Knus, A. Merkurjev, M. Rost, J. Tignol: *The book of involutions.* American Mathematical Soc. (1998).

[10] D.E. Knuth: Finite semifields and projective planes. Dissertation (Ph.D.), California Institute of Technology. (1963).

[11] R.D. Schafer: *An introduction to nonassociative algebras.* Dover Publications (1995).

[12] D. Thompson: A generalisation of Dickson's commutative division algebras. *Communications in Algebra* 48 (9) (2020) 3922–3932.

Received: 4 June 2019
Accepted for publication: 23 January 2020
Communicated by: Ivan Kaygorodov