

HOW TO OBTAIN DIVISION ALGEBRAS FROM TWISTED CAYLEY-DICKSON DOUBLINGS

S. PUMPLÜN

ABSTRACT. We change the order of the factors in the classical Cayley-Dickson doubling process and investigate the eight-dimensional algebras obtained when doubling a quaternion algebra using this twisted multiplication. We also allow the scalar c used in the doubling process to be an invertible element in the quaternion algebra. By changing the place of c inside the multiplication we then obtain different families of algebras. We give conditions when these algebras are division over a given base field.

1. INTRODUCTION

In this paper, we study families of unital eight-dimensional algebras over a field F . To obtain these families, we permute the factors inside the multiplication obtained by the Cayley-Dickson doubling process. Moreover, we allow the scalar c used in the doubling process to be an invertible element in the quaternion algebra D we double. The idea of constructing algebras by choosing the scalar in the Cayley-Dickson doubling outside of F was already employed in [Al-H-K], [W], [As-Pu] and [Pu]. All our algebras contain quaternion algebras as subalgebras and have a nonassociative quaternion subalgebra if there is a separable quadratic field extension $L \subset D$ such that $c \in L \setminus F$.

The types of algebras we study are thus modified Cayley-Dickson doublings of a quaternion algebra D . We call them *twisted Dickson algebras*. The base-free approach makes it easy to describe them. Depending on whether c lies in F or not, they have different structures. If $c \in D^\times \setminus F$ then A is not third power-associative, i.e. the equation $uu^2 = u^2u$ is not true for all $u \in A$. Different placements of c inside the product yield different families of algebras. A is a division algebra if D is a division algebra and if $N_{D/F}(c) \notin N_{D/F}(D^\times)^2$. If $c \in F^\times$, we obtain division algebras if the quaternion algebra D used in the doubling process is a division algebra and $c \notin \pm N_{D/F}(D^\times)$. We thus get division algebras over suitable fields. However, our algebras are not division algebras if $F = \mathbb{R}$. Properties and isomorphisms of some of these algebras are studied. We conclude with an outlook on how to use twisted Cayley-Dickson doublings to obtain sixteen-dimensional division algebras.

There has always been an interest in real division algebras, cf. for instance [B-O1, 2], [R], [Do-Z1, 2], [M-B],[K], [D-D-H], [B-B-O], [D1, 2], [C-V-K-R], [J-P] and [Die], to name just a few. Our motivation to search for classes of division algebras over fields other than the reals is their potential use in space-time block coding. Space-time coding is used for reliable

Date: 18.7.2010.

1991 Mathematics Subject Classification. Primary: 17A35.

Key words and phrases. Cayley-Dickson doubling, division algebra.

high rate transmission over wireless digital channels with multiple antennas at both the transmitter and receiver ends. From the mathematical point of view, designing space-times codes means to design families of $n \times n$ matrices over the complex numbers using the left representation of an algebra. Central simple associative division algebras over number fields, in particular cyclic division algebras, have been used highly successfully to systematically build space-time block codes (cf. for instance [E-S-K], [S-R-S], [H-L-R-V], [Be-Og1, 2, 3], [O-R-B-V]). These codes, made of $n \times n$ matrices over the complex numbers, display excellent performance if measured by error probability.

Nonassociative division algebras over number fields can be used in code design and thus become interesting in this setting as well [Pu-U].

2. PRELIMINARIES

2.1. Nonassociative algebras. Let F be a field. By “ F -algebra” we mean a finite dimensional unital nonassociative algebra over F .

A nonassociative algebra A is called a *division algebra* if for any $a \in A$, $a \neq 0$, the left multiplication with a , $L_a(x) = ax$, and the right multiplication with a , $R_a(x) = xa$, are bijective. A is a division algebra if and only if A has no zero divisors [Sch, pp. 15, 16].

For an F -algebra A , associativity in A is measured by the *associator* $[x, y, z] = (xy)z - x(yz)$. The *left nucleus* of A is defined as $N_l(A) = \{x \in A \mid [x, A, A] = 0\}$, the *middle nucleus* of A is defined as $N_m(A) = \{x \in A \mid [A, x, A] = 0\}$ and the *right nucleus* of A is defined as $N_r(A) = \{x \in A \mid [A, A, x] = 0\}$. Their intersection $N(A) = \{x \in A \mid [x, A, A] = [A, x, A] = [A, A, x] = 0\}$ is the *nucleus* of A . The nucleus is an associative subalgebra of A (it may be zero), and $x(yz) = (xy)z$ whenever one of the elements x, y, z is in $N(A)$.

The *commuter* of A is defined as $\text{Comm}(A) = \{x \in A \mid xy = yx \text{ for all } y \in A\}$ and the *center* of A is $\text{C}(A) = \{x \in A \mid x \in \text{Nuc}(A) \text{ and } xy = yx \text{ for all } y \in A\}$.

Recall that over a field F of characteristic 2, we can define the quaternion algebra $[a, b]$ via $[a, b] = \langle i, j \mid i^2 + i = a, j^2 = b, ij = ji + j \rangle$ with $a \in F$ and $b \in F^\times$. Obviously, $[a, b] = \text{Cay}(L, b)$ with $L = F(i)$ where $i^2 + i = a$ is a separable quadratic field extension [S, p. 314].

Let S be a quadratic étale algebra over F (i.e., a separable quadratic F -algebra in the sense of [Knu, p. 4]) with canonical involution $\sigma: S \rightarrow S$, also written as $\sigma = \bar{}$, and with nondegenerate norm $N_{S/F}: S \rightarrow F$, $N_{S/F}(s) = s\bar{s} = \bar{s}s$. With the diagonal action of F , $F \times F$ is a quadratic étale algebra with canonical involution $(x, y) \mapsto (y, x)$. A quadratic étale algebra S which is isomorphic to the algebra $F \times F$ is called *split*.

2.2. Nonassociative quaternion division algebras. Let F be a field. A *nonassociative quaternion algebra* is a four-dimensional unital F -algebra A whose nucleus is a separable quadratic field extension of F . Let S be a quadratic étale algebra over F with canonical involution $\sigma = \bar{}$. For every $b \in S \setminus F$, the vector space

$$\text{Cay}(S, b) = S \oplus S$$

becomes a nonassociative quaternion algebra over F with unit element $(1, 0)$ and nucleus S under the multiplication

$$(u, v)(u', v') = (uu' + b\bar{v}'v, v'u + v\bar{u}')$$

for $u, u', v, v' \in S$. Given any nonassociative quaternion algebra A over F with nucleus S , there exists an element $b \in S \setminus F$ such that $A \cong \text{Cay}(S, b)$ [As-Pu, Lemma 1].

Nonassociative quaternion algebras are neither power-associative nor quadratic. $\text{Cay}(S, b)$ is a division algebra if and only if S is a separable quadratic field extension of F [W, p. 369]. Two nonassociative quaternion algebras $A = \text{Cay}(K, b)$ and $A' = \text{Cay}(L, c)$ can only be isomorphic if $L \cong K$. Moreover,

$$\text{Cay}(K, b) \cong \text{Cay}(K, c) \text{ iff } g(b) = N_{K/F}(d)c$$

for some automorphism $g \in \text{Aut}(K)$ and some non-zero $d \in K$ [W].

Nonassociative quaternion division algebras canonically appeared as the most interesting case in the classification of the algebras of dimension 4 over F which contain a separable field extension K of F in their nucleus [W] (see also Althoen-Hansen-Kugler [Al-H-K] for $F = \mathbb{R}$). They were first discovered by Dickson [Di] in 1935 and Albert [A] in 1942 as early examples of real division algebras.

2.3. The Cayley-Dickson doubling process. Let D be a quaternion algebra over F . Let $\sigma = \bar{\cdot} : D \rightarrow D$ be the canonical involution of D . Let $c \in D$ be an invertible element. Then the eight-dimensional F -vector space $A = D \oplus D$ can be made into a unital algebra over F via the multiplication

$$(u, v)(u', v') = (uu' + c\bar{v}'v, v'u + v\bar{u}')$$

for $u, u', v, v' \in D$. The unit element is given by $1 = (1, 0)$.

A is called the *Cayley-Dickson doubling of D (with scalar c)* and denoted by $\text{Cay}(D, c)$. An algebra obtained from a Cayley-Dickson doubling of D with a scalar $c \in F^\times$ is an octonion algebra. If $c \in D^\times$ is not contained in F , we also distinguish between the other two possible multiplications

$$(u, v)(u', v') = (uu' + \bar{v}'cv, v'u + v\bar{u}')$$

resp.

$$(u, v)(u', v') = (uu' + \bar{v}'vc, v'u + v\bar{u}')$$

on $D \oplus D$ and denote the corresponding algebras by $\text{Cay}_m(D, c)$, resp. $\text{Cay}_r(D, c)$. $\text{Cay}(D, c)$, $\text{Cay}_m(D, c)$ and $\text{Cay}_r(D, c)$ are called *Dickson algebras* over F and were studied in [Pu]. Dickson algebras are not third power-associative. The Cayley-Dickson doubling $\text{Cay}(D, c)$, resp. $\text{Cay}_m(D, c)$ or $\text{Cay}_r(D, c)$, of a quaternion division algebra D is a division algebra with nucleus, commutator and center F , for any choice of invertible $c \in D$ not in F [Pu].

3. TWISTED CAYLEY-DICKSON DOUBLINGS

Let D be a noncommutative unital algebra over F with an involution $\sigma = \bar{\cdot} : D \rightarrow D$. Let $c \in D$ be an invertible element. The F -vector space $D \oplus D$ can be made into a unital algebra A over F by modifying the multiplication which is used in the Cayley-Dickson doubling of

D . Since D is not commutative, we have the several possibilities. Each such algebra is denoted by $\text{Cay}_t(D, c)$ with $t = t(i)$, $t = t(i, j)$ or $t = (i, j, k)$ depending on which and how many of the four products appearing in the multiplication of the Cayley-Dickson doubling have been permuted, e.g:

$A = \text{Cay}_{t(1)}(D, c)$ has multiplication

$$(u, v)(u', v') = (u'u + c(\overline{v'}v), v'u + v\overline{u'}),$$

$A = \text{Cay}_{t(1,2)}(D, c)$ has multiplication

$$(u, v)(u', v') = (u'u + c(v\overline{v'}), v'u + v\overline{u'}),$$

$A = \text{Cay}_{t(1,2,3,4)}(D, c)$ has multiplication

$$(u, v)(u', v') = (u'u + c(v\overline{v'}), uv' + \overline{u'}v),$$

where $u, u', v, v' \in D$. An algebra obtained from such a modified Cayley-Dickson doubling of D with a scalar $c \in D^\times$ is called a *twisted Dickson algebra* over F .

We can immediately say that for $c \in F^\times$,

$$\text{Cay}_{t(1,4)}(D, c) = \text{Cay}_{t(2,3)}(D^{\text{op}}, c), \quad \text{Cay}_{t(1,3)}(D, c) = \text{Cay}_{t(2,4)}(D^{\text{op}}, c),$$

$$\text{Cay}_{t(1,2)}(D, c) = \text{Cay}_{t(3,4)}(D^{\text{op}}, c), \quad \text{Cay}_{t(1,2,3)}(D, c) = \text{Cay}_{t(4)}(D^{\text{op}}, c),$$

$$\text{Cay}_{t(1,2,4)}(D, c) = \text{Cay}_{t(3)}(D^{\text{op}}, c), \quad \text{Cay}_{t(1,3,4)}(D, c) = \text{Cay}_{t(2)}(D^{\text{op}}, c),$$

$$\text{Cay}_{t(1)}(D, c) = \text{Cay}_{t(2,3,4)}(D^{\text{op}}, c),$$

so unless $c \in D^\times \setminus F$, it suffices to study the algebras $\text{Cay}_{t(2,3)}(D, c)$, $\text{Cay}_{t(2,4)}(D, c)$, $\text{Cay}_{t(3,4)}(D, c)$, $\text{Cay}_{t(2,3,4)}(D, c)$, $\text{Cay}_{t(2)}(D, c)$ and $\text{Cay}_{t(3)}(D, c)$.

If $c \in D^\times \setminus F$, we can change the place of c inside the multiplication to obtain more families of algebras. For instance,

${}_r\text{Cay}_{t(1)}(D, c)$ has multiplication

$$(u, v)(u', v') = (u'u + (\overline{v'}v)c, v'u + v\overline{u'}),$$

${}_r\text{Cay}_{t(1,2)}(D, c)$ has multiplication

$$(u, v)(u', v') = (u'u + (v\overline{v'})c, v'u + v\overline{u'}),$$

for $u, u', v, v' \in D$, and so on. Each such algebra is denoted by ${}_r\text{Cay}_t(D, c)$ with $t = t(i)$, $t = t(i, j)$ or $t = (i, j, k)$ depending on which and how many of the four factors have been permuted. Moreover, we can place c in the middle and define, for instance:

${}_m\text{Cay}_{t(1)}(D, c)$ has multiplication

$$(u, v)(u', v') = (u'u + \overline{v'}(cv), v'u + v\overline{u'}),$$

${}_m\text{Cay}_{t(1,2)}(D, c)$ has multiplication

$$(u, v)(u', v') = (u'u + v(c\overline{v'}), v'u + v\overline{u'}),$$

for $u, u', v, v' \in D$. Each such algebra is denoted by ${}_m\text{Cay}_t(D, c)$ with $t = t(i)$, $t = t(i, j)$ or $t = (i, j, k)$ depending on which and how many of the four factors have been permuted.

Each of the algebras $\text{Cay}_t(D, c)$, ${}_m\text{Cay}_t(D, c)$, ${}_r\text{Cay}_t(D, c)$ has unit element $1 = (1, 0)$. If D is associative, we can omit the parentheses in the first term. If D is not associative, for each case there are two more possible ways to put the parentheses in the second term which only becomes relevant when we construct algebras of dimension 16.

Remark 1. Let $A = \text{Cay}_t(D, c)$, $A = {}_r\text{Cay}_t(D, c)$ or $A = {}_m\text{Cay}_t(D, c)$.

- (i) D is a subalgebra of A for $t = t(i)$, $i = 2, 3, 4$, $t = t(i, j)$, $i, j \in \{2, 3, 4\}$ and $t = t(2, 3, 4)$.
- (ii) D^{op} is a subalgebra of A for $t = t(1)$, $t = t(1, j)$ and $j \in \{2, 3, 4\}$ and $t = t(1, j, k)$, $j, k \in \{2, 3, 4\}$, $j \neq k$.
- (iii) If there is a unital subalgebra (B, σ) of (D, σ) with involution such that $c \in B^\times$ then the twisted Dickson algebra $\text{Cay}_t(B, c)$ (resp., ${}_r\text{Cay}_t(B, c)$ or ${}_m\text{Cay}_t(B, c)$) is a subalgebra of A .

If $B = K$ is a separable quadratic field extension and $c \in F^\times$ then $\text{Cay}(K, c)$ is a quaternion subalgebra. If $c \in K \setminus F$, it is a nonassociative quaternion subalgebra.

- (iv) If $c \in D^\times \setminus F$ and $\sigma(c) \neq c$ then A is not third power-associative: Suppose $A = \text{Cay}_t(D, c)$ (the other cases are proved analogously). For $l = (0, 1)$ we have $l^2 = (c, 0)$ and $ll^2 = (0, \sigma(c))$ while $l^2l = (0, c)$, hence A is not power-associative. Every quadratic unital algebra is clearly power-associative, so A is also not quadratic.

In this paper we will mainly focus on the case that D is a quaternion algebra over F , $c \in D^\times$, and study the corresponding eight-dimensional twisted Dickson algebras. Unless stated otherwise, let D be a quaternion algebra over F with canonical involution $\bar{} : D \rightarrow D$.

Remark 2. The algebras $\text{Cay}_{t(2,3)}(D, c)$ could be viewed as a generalization of a nonassociative quaternion algebra. Their multiplication corresponds to the one given for a nonassociative quaternion algebra in [W]. Since $\text{Cay}_{t(1,2,3,4)}(D, c) = \text{Cay}(D^{\text{op}}, c)$, ${}_m\text{Cay}_{t(1,2,3,4)}(D, c) = \text{Cay}_m(D^{\text{op}}, c)$, and ${}_r\text{Cay}_{t(1,2,3,4)}(D, c) = \text{Cay}(D^{\text{op}}, c)$, the algebras $\text{Cay}_{t(1,2,3,4)}(D, c)$, ${}_m\text{Cay}_{t(1,2,3,4)}(D, c)$ and ${}_r\text{Cay}_{t(1,2,3,4)}(D, c)$, with D a quaternion algebra, were already treated in [Pu] and are division algebras for all choices of $c \in D^\times \setminus F$, if D is a division algebra.

Theorem 3. *Let D be a quaternion division algebra. The twisted Cayley-Dickson doubling $\text{Cay}_t(D, c)$, ${}_m\text{Cay}_t(D, c)$, resp. ${}_r\text{Cay}_t(D, c)$ is a division algebra for any choice of $c \in D^\times$ such that $N_{D/F}(c) \notin N_{D/F}(D^\times)^2$.*

Note that this is never the case for $F = \mathbb{R}$.

Proof. We show that $A = \text{Cay}_{t(2,3)}(D, c)$ has no zero divisors: suppose

$$(0, 0) = (r, s)(u, v) = (ru + cs\bar{v}, rv + s\bar{u})$$

for $r, s, u, v \in D$. This is equivalent to

$$ru + cs\bar{v} = 0 \text{ and } rv + s\bar{u} = 0.$$

Assume $s = 0$, then $ru = 0$ and $rv = 0$. Hence either $r = 0$ and so $(r, s) = 0$ or $r \neq 0$ and $u = v = 0$.

So let $s \neq 0$. Then $s \in D^\times$ and $s\bar{u} = -rv$ yields $u = -\bar{v}\bar{r}\bar{s}^{-1}$ and substituted in to the first equation this gives $-r\bar{v}\bar{r}\bar{s}^{-1} + cs\bar{v} = 0$. It follows that

$$(*) \quad cs\bar{v} = r\bar{v}\bar{r}\bar{s}^{-1}$$

and applying the norm $N_{D/F}$ we obtain that

$$N_{D/F}(c)N_{D/F}(s)^2N_{D/F}(v) = N_{D/F}(r)^2N_{D/F}(v).$$

If $v = 0$ then $ru = 0$ and $s\bar{u} = 0$, thus $u = 0$ and $(u, v) = 0$. If $v \neq 0$ then $N_{D/F}(v) \neq 0$ and we get $N_{D/F}(c) = N_{D/F}(\frac{r}{s})^2$, a contradiction to our initial assumption that $N_{D/F}(c) \notin N_{D/F}(D^\times)^2$, unless $r = 0$. However, if $r = 0$ (and $s \neq 0$ as assumed above) then the initial two equalities give $u = 0$ and $v = 0$, so that $(u, v) = (0, 0)$.

The proof is analogous for all twisted algebras of the type $\text{Cay}_t(D, c)$: for the other multiplications, the order of the factors in $(*)$ changes, which however does not affect the proof.

The proof for the other algebras is analogous to the one for $A = \text{Cay}_t(D, c)$, since the different placement of c in the first equation is not relevant in the different steps. \square

Corollary 4. *Let D be a quaternion division algebra.*

(i) *Let $c \in D^\times \setminus F$ and $A = \text{Cay}_t(D, c)$, $A = {}_m\text{Cay}_t(D, c)$ or $A = {}_r\text{Cay}_t(D, c)$. If $N_{D/F}(c) \notin F^{\times 2}$, then A is a division algebra.*

(ii) *$\text{Cay}_t(D, c)$ is a division algebra for any choice of $c \in F^\times$ such that $c \notin \pm N_{D/F}(D^\times)$.*

Note that $c \notin \pm N_{D/F}(D^\times)$ is never the case for $F = \mathbb{Q}$ [L, Theorem 1.4, p. 378].

Example 5. Let $F = \mathbb{Q}$ and $D = (a, b)_{\mathbb{Q}}$ a division algebra.

Suppose $a, b > 0$. Then for every $c = x_1i + x_2j$ with $(x_1, x_2) \neq (0, 0)$ we know that $N_{D/F}(c) = -(ax_1^2 + bx_2^2) < 0$ is not a square in \mathbb{Q} , thus $\text{Cay}_t(D, c)$, ${}_m\text{Cay}_t(D, c)$ and ${}_r\text{Cay}_t(D, c)$ are division algebras over \mathbb{Q} for any choice of t .

For $a, b < 0$, D is always a division algebra and $\text{Cay}_t(D, c)$, ${}_m\text{Cay}_t(D, c)$ and ${}_r\text{Cay}_t(D, c)$ are division algebras for any t and all $c = x_0 + x_1i + x_2j + x_3k$, such that the positive rational number $N_{D/\mathbb{Q}}(c) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$ is not a square in \mathbb{Q} .

If $D = (-1, p)_{\mathbb{Q}}$, $p \not\equiv 1(4)$ an odd prime, D is a division algebra and we may for instance choose $c = x_2i + x_3k$ with $x_2, x_3 \in \mathbb{Q}$, $(x_1, x_2) \neq (0, 0)$. Then $N_{D/\mathbb{Q}}(c) = -p(x_2^2 + x_3^2) < 0$, hence $\text{Cay}_t(D, c)$, ${}_m\text{Cay}_t(D, c)$ and ${}_r\text{Cay}_t(D, c)$ are division algebras for any choice of t .

If $D = (-2, p)_{\mathbb{Q}}$, $p \equiv 1, 3(8)$ an odd prime, D is a division algebra and we may again choose $c = x_2i + x_3k$ with $x_2, x_3 \in \mathbb{Q}$, $(x_1, x_2) \neq (0, 0)$. Then $N_{D/\mathbb{Q}}(c) = -(px_2^2 + 2px_3^2) < 0$, hence $\text{Cay}_t(D, c)$, ${}_m\text{Cay}_t(D, c)$ and ${}_r\text{Cay}_t(D, c)$ are division algebras for any choice of t .

We obtain the following more general rule:

Lemma 6. *Let F be an ordered field such that -1 is not a square and $(a, b)_F$ a division algebra over F with $a < 0$ and $b > 0$. Then $\text{Cay}_t(D, c)$, ${}_m\text{Cay}_t(D, c)$ and ${}_r\text{Cay}_t(D, c)$ are division algebras for any choice of t , for every $c = x_2i + x_3k \in D$ with $(x_1, x_2) \neq (0, 0)$.*

Proof. We have $N_{D/F}(c) = -b(x_2^2 - ax_3^2) < 0$. \square

Remark 7. Let $D = (a, b)_F$ be a division algebra. For $e \in F^\times$, $\text{Cay}(D, e)$ is an octonion division algebra over F if and only if $e \notin N_{D/F}(D^\times)$. So let $c \in F$ then $c \notin \pm N_{D/F}(D^\times)$ iff $\text{Cay}(F, a, b, -c)$ and $\text{Cay}(F, a, b, c)$ are octonion division algebras.

Lemma 8. Let $A = \text{Cay}_t(D, c)$, $A =_m \text{Cay}_t(D, c)$ or $A =_r \text{Cay}_t(D, c)$ be a twisted Dickson algebra and $c \in D^\times$. Then $\text{Comm}(A) = F$.

Proof. Let $A = \text{Cay}_t(D, c)$. Let us consider the classical Cayley-Dickson doubling as a reference point: For $C = \text{Cay}(D, c)$ we have $(u, v) \in \text{Comm}(C)$ iff $(u, v)(r, s) = (r, s)(u, v)$ for all $r, s \in D$ iff

$$(1) \quad ru + c\bar{v}s = ur + c\bar{s}v \text{ and } (2) \quad vr + s\bar{u} = su + v\bar{r}$$

for all $r, s \in D$. Now let $A = \text{Cay}_t(D, c)$, so we have to twist the components in the above multiplication and thus in (1) and (2) accordingly. Nonetheless, for $s = 0$ we will always get $ru = ur$ for all $r \in D$, therefore $u \in F$. For $u \in F$, (1) yields

$$(1') \quad c\bar{v}s = c\bar{s}v$$

if the second term in the multiplication was left unchanged and

$$(1') \quad c\bar{s}v = c\bar{v}s$$

otherwise. Both times, $s = 1$ implies that $v \in F$ as well. Now for $v \in F$, (2) yields

$$(2') \quad vr = v\bar{r}$$

if the fourth term in the multiplication was left unchanged and

$$(2') \quad rv = \bar{r}v$$

otherwise, both times implying that $v = 0$. Obviously, $F \subset \text{Comm}(A)$, so we have proved the assertion.

For $A =_m \text{Cay}_t(D, c)$ or $A =_r \text{Cay}_t(D, c)$ again consider the classical Cayley-Dickson doubling as a reference point: For $C = \text{Cay}(D, c)$ we have $(u, v) \in \text{Comm}(C)$ iff $(u, v)(r, s) = (r, s)(u, v)$ for all $r, s \in D$ iff

$$(1) \quad ru + c\bar{v}s = ur + c\bar{s}v \text{ and } (2) \quad vr + s\bar{u} = su + v\bar{r}$$

for all $r, s \in D$. Now we have to twist the components in the above multiplication and thus in (1) and (2) accordingly and also adjust the placement of c . Nonetheless, for $s = 0$ we will always get $ru = ur$ for all $r \in D$, therefore $u \in F$. For $u \in F$, (1) yields

$$(1') \quad \bar{v}cs = \bar{s}cv \text{ resp. } \quad \bar{v}sc = \bar{s}vc$$

if the second term in the multiplication was left unchanged and

$$(1') \quad s\bar{c}v = v\bar{c}s \text{ resp. } \quad s\bar{v}c = v\bar{s}c$$

otherwise. Both times, $s = 1$ implies that $v \in F$ as well. Now for $v \in F$, (2) yields

$$(2') \quad vr = v\bar{r}$$

if the fourth term in the multiplication was left unchanged and

$$(2') \quad rv = \bar{r}v$$

otherwise, both times implying that $v = 0$. Obviously, $F \subset \text{Comm}(A)$, so we have proved the assertion. \square

4. PROPERTIES IF $t = t(1)$, $t = t(2)$, $t = t(1, 2)$, $t = t(3, 4)$, $t = t(1, 3, 4)$ OR $t = t(2, 3, 4)$.

We have a closer look at eighteen of our families. In this section, let

$$A = \text{Cay}_t(D, c), \quad A = {}_m\text{Cay}_t(D, c) \text{ or } A = {}_r\text{Cay}_t(D, c)$$

where D is a quaternion division algebra and $c \in D^\times \setminus F$. Unless explicitly stated otherwise, in this section we assume that

$$t = t(1), t = t(2), t = t(1, 2), t = t(3, 4), t = t(1, 3, 4) \text{ or } t = t(2, 3, 4).$$

Theorem 9. *D is the only quaternion subalgebra of A .*

Proof. Let $A = \text{Cay}_t(D, c)$. We distinguish two cases.

(i) Let F have characteristic not 2. Suppose there is a quaternion subalgebra $B = (e, f)_F$ in A . Then there is an element $X \in A$, $X = (u, v)$ with $u, v \in D$ such that $X^2 = e \in F^\times$ and an element $Y \in A$, $Y = (w, z)$ with $w, z \in D$ such that $Y^2 = f \in F^\times$ and $XY + YX = 0$. The first equation would be equivalent to

$$(1) \quad u^2 + cN_{D/F}(v) = e \text{ and } (2) \quad vu + v\sigma(u) = 0$$

if we were looking at the classical doubling process. The twisted versions will obviously switch around the order of the corresponding factors. This, however, will not affect equation (1). Thus in all cases we have that if $v = 0$, then $u^2 = e$ and $X = (u, 0) \in (D, 0)$.

Now if $t = t(1)$, $t = t(2)$, or $t = t(1, 2)$, equation (2) stays as above, too, and the same proof as in [Pu, Theorem 6] implies the assertion (we repeat it here for the sake of the reader): if $v \neq 0$ then v is invertible and $\sigma(u) = -u$. This implies $u^2 = -N_{D/F}(u)$, thus $e + N_{D/F}(u) = cN_{D/F}(v)$ i.e. $N_{D/F}(v^{-1})(e + N_{D/F}(u)) = c$ which is a contradiction since the right hand side lies in D and not in F , while the left hand side lies in F .

Analogously, the second equation implies $w^2 = f$ and $Y = (w, 0)$, $w \in D$. Hence $(0, 0) = XY + YX = (uw + wu, 0)$ means $uw + wu = 0$ and so the standard basis $1, X = u, Y = w, XY = uw$ for the quaternion algebra $(e, f)_F$ lies in D and we obtain $D = (e, f)_F$.

If $t = t(3, 4)$, $t = t(1, 3, 4)$, $t = t(2, 3, 4)$, equation (2) stays changes to

$$(2') \quad uv + \sigma(u)v = 0.$$

Hence if $v \neq 0$ then v is invertible and $\sigma(u) = -u$ and again the same proof as in [Pu, Theorem 6] implies the assertion.

(ii) Let F have characteristic 2. Suppose there is a quaternion subalgebra $B = [e, f]$ in A . Then there is an element $X \in A$, $X = (u, v)$ with $u, v \in D$ such that $X^2 + X = e \in F$ and an element $Y \in A$, $Y = (w, z)$ with $w, z \in D$ such that $Y^2 = f \in F^\times$ and $XY = YX + Y$. Analogously as in the above proof, the second equation $Y^2 = f \in F^\times$ implies $w^2 = f$ and $Y = (w, 0)$, $w \in D$, if $t = t(1)$, $t = t(2)$, $t = t(1, 2)$, $t = t(3, 4)$, $t = t(1, 3, 4)$, or $t = t(2, 3, 4)$.

The first equation implies

$$(3) \quad u^2 + cN_{D/F}(v) + u = e \text{ and } (4) \quad vu + v\sigma(u) + v = 0$$

if we were looking at the classical and not at a twisted doubling process. The twisted versions will obviously switch around the order of the corresponding factors in (4). Equation (3) is not affected. Now if $t = t(1)$, $t = t(2)$ or $t = t(1, 2)$, equation (4) stays the same, too, and the same proof as in [Pu, Theorem 6] implies the assertion (we repeat it for the sake of completeness): If $v \neq 0$ then v is invertible and $\sigma(u) + u + 1 = 0$. This implies $u = -(\sigma(u) + 1)$, thus $\sigma(u^2) + \sigma(u) + cN_{D/F}(v) = e$ i.e. we get $\sigma(u^2 + u) + cN_{D/F}(v) = u^2 + u + cN_{D/F}(v)$ which yields $\sigma(u^2 + u) = u^2 + u$. Hence $u^2 + u \in F$. This implies that $cN_{D/F}(v) = e - (u^2 + u) \in F$, a contradiction.

If $t = t(3, 4)$, $t = t(1, 3, 4)$, or $t = t(2, 3, 4)$, equation (4) changes to

$$(4') \quad uv + \sigma(u)v + v = 0.$$

Thus if $v \neq 0$ then v is invertible and $\sigma(u) + u + 1 = 0$. This implies $u = -(\sigma(u) + 1)$, thus the same contradiction that plugged into (3) we obtain that $cN_{D/F}(v) = e - (u^2 + u) \in F$.

Hence $v = 0$ which implies $u^2 + u = e$ and $X = (u, 0) \in D$. Now $XY = YX + Y$ means $uw = wu + w$ and the standard basis $1, X = u, Y = w$ for the quaternion algebra $[e, f]$ lies in D . We obtain $D = [e, f]$.

The proofs for the other algebras are analogous. \square

Theorem 10. *If $c \in D^\times \setminus F$ is contained in a separable quadratic field extension L of F and $\text{Cay}(K, e)$ is a nonassociative quaternion subalgebra of A , then $K = L$ and there is $z \in D^\times$ such that $e = cN_{D/F}(z)$.*

If $c \in D^\times \setminus F$ is instead contained in a purely inseparable quadratic field extension K of F , then A has no nonassociative quaternion subalgebras.

If $\text{Cay}(K', e)$ is a subalgebra of A , where K' is a purely inseparable quadratic field extension of F , then $K' = K$.

Proof. Suppose that $\text{Cay}(K, e)$ is a nonassociative quaternion subalgebra of $A = \text{Cay}_t(D, c)$.

(i) Let F have characteristic not 2 and let $K = F(\sqrt{f})$. Then there is an element $Y \in A$, $Y = (w, z)$ with $w, z \in D$ such that $Y^2 = f \in F^\times$. As in the proof of Theorem 9, this implies $Y = (w, 0)$ and $w^2 = f$, $w \in D$, so $(K, 0) \subset (D, 0)$.

There also is an element $Z = (w, z) \in A$, $w, z \in D$, such that $Z^2 = (e, 0)$ and $(x, 0)(w, z) = (w, z)(\sigma(x), 0)$ for all $x \in K$. This is equivalent to

$$(5)w^2 + cN(z) = e, \quad (6) \quad z(w + \sigma(w)) = 0 \quad \text{and} \quad (7) \quad xw = w\sigma(x)$$

for all $x \in K$ if we look at the classical and not at a twisted doubling process. The twisted versions will switch around the order of the corresponding factors in (6) and (7), while (5) remains the same, so that we alternatively deal with the equations

$$(6') \quad (w + \sigma(w))z = 0 \quad \text{and/or} \quad (7') \quad wx = \sigma(x)w$$

for all $x \in K$.

If $z = 0$ then $w^2 = e \in K$. Write $D = \text{Cay}(K, b)$ for a suitable $b \in F^\times$, then $w = x_0 + jx_1$ with $j^2 = b$ and $w^2 = e$ implies that $x_1 = 0$ or $\sigma(x_0) = -x_0$. The latter implies the contradiction that $w^2 = x_0^2 + \sigma(x_1)x_1b = -N_{K/F}(x_0) + N_{K/F}(x_1)b = e \in F$, hence we get $x_1 = 0$. Thus $w \in K^\times$ and $Z = (w, 0)$ which again yields a contradiction, since we also

require equation (7) respectively (7') to hold.

Therefore $z \neq 0$ and thus $\sigma(w) = -w$. The first equation yields $-N_{D/F}(w) + cN_{D/F}(z) = e \in K \setminus F$. Since $N_{D/F}(z) \neq 0$ the left-hand side of the equation is an element of $L \setminus F$, hence $L = K$. Now $xw = w\sigma(x)$ means $xw = -\sigma(w)\sigma(x) = \sigma(wx)$, therefore $xw \in F$ for all $x \in K$, and the same conclusion follows if we have (7') instead. For $x = 1$ we obtain $w \in F$, a contradiction to the requirement that $\sigma(w) = -w$, unless $w = 0$. We conclude that the first equation implies that $c\bar{z}z = e$.

By 2.2,

$$\text{Cay}(L, cN_{D/F}(z)) \cong \text{Cay}(L, c) \text{ iff } N_{D/F}(z)g(c) = N_{L/F}(d)c$$

for an automorphism $g \in \text{Aut}(L)$ and a non-zero $d \in L$, so if we know that there is $d \in L$ such that $N_{L/F}(d) = N_{D/F}(z)$ then the nonassociative quaternion algebra $\text{Cay}(L, c)$ in A is unique up to isomorphism.

(ii) Let F have characteristic 2. K is a separable quadratic field extension of F . Hence there is an element $X = (w, z) \in A$, $w, z \in D$, such that $X^2 + X = f \in F^\times$. As in the proof of Theorem 3 this implies $X = (w, 0)$ and $w^2 + w = f$, $w \in D$, so $K \subset (D, 0)$.

There also is an element $Z = (w, z) \in A$ such that $Z^2 = (e, 0)$ and $(x, 0)(w, z) = (w, z)(\sigma(x), 0)$ for all $x \in K$. The rest of the assertion follows analogously as in (i).

If c lies in a purely inseparable quadratic field extension, however, the conclusion that $-N_{D/F}(w) + cN_{D/F}(z) = e \in K \setminus F$, with the left-hand side a non-zero element of L , hence $L = K$, yields a contradiction. Thus in this case A has no nonassociative quaternion subalgebras.

If $\text{Cay}(K', e)$ is a subalgebra of A , where K' is a purely inseparable quadratic field extension of F , it follows that $K' = K$.

The statements are proved analogously for the other algebras. \square

We choose the algebras $A = \text{Cay}_{t(2,3)}(D, c)$ and $A = \text{Cay}_{t(2,3,4)}(D, c)$ to investigate their nuclei.

Lemma 11. *Let $A = \text{Cay}_{t(2,3)}(D, c)$.*

(i) *Let $c \in F^\times$. Then $\text{Nuc}_l(A) = \{(w, 0) \mid w \in D\} \cong D$, $\text{Nuc}_m(A) = F \oplus F$ and $\text{Nuc}_r(A) = F \oplus F$.*

(ii) *Let $c \in D^\times \setminus F$. Then $K \subset \text{Nuc}_l(A) = \{(w, 0) \mid w \in D \text{ and } wc = cw\}$, where K is a quadratic field extension of F contained in D with $c \in K$, $\text{Nuc}_m(A) = F$ and $\text{Nuc}_r(A) = F \oplus F$.*

(iii) *$\text{Nuc}(A) = F$ and $C(A) = F$.*

Proof. (i) and (ii) are proved together: We have

$$(w, z)((r, s)(u, v)) = (wru + wcs\bar{v} + cz\bar{v}\bar{r} + czu\bar{s}, wrv + ws\bar{u} + z\bar{u}\bar{r} + zv\bar{s}\bar{c})$$

and

$$((w, z)(r, s))(u, v) = (wru + cz\bar{s}u + cws\bar{v} + cz\bar{r}\bar{v}, wrv + cz\bar{s}u + ws\bar{u} + z\bar{r}\bar{u}).$$

$(w, z) \in \text{Nuc}_l(A)$ iff for all $u, v, r, s \in D$, $(w, z)((r, s)(u, v)) = ((w, z)(r, s))(u, v)$. I.e., iff

$$wcs\bar{v} + cz\bar{v}\bar{r} + czu\bar{s} = cz\bar{s}u + cws\bar{v} + cz\bar{r}\bar{v}$$

and

$$ws\bar{u} + z\bar{u}\bar{r} + zv\bar{s}\bar{c} = cz\bar{s}v + ws\bar{u} + z\bar{r}\bar{u}.$$

For $s = 1$ and $v = 0$ this yields $z = 0$ so $(w, z) \in \text{Nuc}_l(A)$ iff $z = 0$ and for all $u, v, r, s \in D$, $wcs\bar{v} = cws\bar{v}$. Thus $(wc - cw)s\bar{v} = 0$ for all $s, v \in D$ and for $s = v = 1$, $wc = cw$. If $c \in F^\times$, this holds for all $w \in D$. If $c \notin F$, it holds for all $w \in K$, where K is a quadratic subfield of D containing F .

A straightforward calculation as the above shows that if $(r, s) \in \text{Nuc}_m(A)$ then $r, s \in F$. Thus the equivalence $(r, s) \in \text{Nuc}_m(A)$ iff $(w, z)((r, s)(u, v)) = ((w, z)(r, s))(u, v)$ for all $u, v, w, z \in D$ becomes

$$wc\bar{v}s = cw\bar{v}s \text{ and } zv\bar{c}s = czvs,$$

which is equivalent to $(wc - cw)\bar{v}s = 0$ and $(zv\bar{c} - czv)s = 0$ for all $v, w, z \in D$. Suppose $c \in F^\times$, then this is satisfied for all $v, w, z \in D$ and so $\text{Nuc}_m(A) = F \oplus F$. If $c \notin F$ then we obtain for $v = 1$: $(wc - cw)s = 0$ and $(z\bar{c} - cz)s = 0$ for all $w, z \in D$. Since $c \notin \text{Comm}(D) = F$, $(wc - cw) \neq 0$ for some w , hence $s = 0$.

$(u, v) \in \text{Nuc}_r(A)$ iff $(w, z)((r, s)(u, v)) = ((w, z)(r, s))(u, v)$ for all $r, s, w, z \in D$ implies $v \in F$ for $s = z = 1$ and $w = 0$. With $v \in F$ it is equivalent to

$$wcsv + czu\bar{s} = cz\bar{s}u + cwsv$$

and

$$z\bar{u}\bar{r} + z\bar{s}\bar{c}v = cz\bar{s}v + z\bar{r}\bar{u}.$$

For $r = 0$ and $s = z = 1$ we get $v = 0$ if $c \notin F$. This implies $u \in F$.

Suppose now that $c \in F^\times$. Then an easy calculation also shows that $u \in F$.

(iv) is obvious now. □

Note that $A = \text{Cay}_{t(2,3)}(D, c)$ can be viewed as a right K -vector space for all $c \in D^\times$ and any quadratic subfield K in D and since $L \subset \text{Nuc}_l(A)$ for all $c \in L \subset D^\times$ it can be used in the design of space-time block codes.

Lemma 12. *Let $A = \text{Cay}_{t(2,3,4)}(D, c)$ be a twisted Dickson algebra.*

(i) $\text{Nuc}_l(A) = \{(w, 0) \mid w \in F\} \cong F$,

(ii) if $c \in F^\times$ or if D is division and $c \in D^\times \setminus F$, then $\text{Nuc}_m(A) = \{(w, 0) \mid w \in F\} \cong F$,

(iii) $\text{Nuc}_r(A) = \{(w, 0) \mid w \in F\} \cong F$.

(iv) $C(A) = F$.

Proof. (i) We have

$$(w, z)((r, s)(u, v)) = (wru + wcs\bar{v} + cz\bar{v}\bar{r} + cz\bar{s}u, wrv + w\bar{u}s + \bar{u}\bar{r}z + v\bar{s}\bar{c}z)$$

and

$$((w, z)(r, s))(u, v) = (wru + cz\bar{s}u + cws\bar{v} + c\bar{r}z\bar{v}, wrv + cz\bar{s}v + \bar{u}ws + \bar{u}\bar{r}z).$$

$(w, z) \in \text{Nuc}_l(A)$ iff for all $u, v, r, s \in D$, $(w, z)((r, s)(u, v)) = ((w, z)(r, s))(u, v)$. I.e., iff

$$wcs\bar{v} + cz\bar{v}\bar{r} + cz\bar{s}u = cz\bar{s}u + cws\bar{v} + c\bar{r}z\bar{v}$$

and

$$w\bar{u}s + v\bar{s}\bar{c}z = cz\bar{s}v + \bar{u}ws.$$

For $s = 0$ and $v = 1$ the first equation yields $z \in F$. Now the second equation with $z \in F$, $s = 1$ and $v = 0$ yields $w \in F$. For $z, w \in F$, the first equation is always satisfied, the second yields $zv\bar{s}\bar{c} = zc\bar{s}v$ for all $s, v \in D$. Suppose $c \in D^\times \setminus F$. Then this gives $z(\bar{c} - c) = 0$, hence $z = 0$ for $s = v = 1$.

If $c \in F^\times$, the first equation yields $z = 0$.

(iii) A straightforward calculation as the above shows that if $(r, s) \in \text{Nuc}_m(A)$ then $r \in F$. Thus the equivalence $(r, s) \in \text{Nuc}_m(A)$ iff $((w, z)((r, s)(u, v)) = ((w, z)(r, s))(u, v)$ for all $u, v, w, z \in D$ becomes

$$w\bar{u}s + v\bar{s}\bar{c}z = cz\bar{s}v + \bar{u}ws \text{ and } wcs\bar{v} = cws\bar{v}.$$

If $c \in F^\times$, the second equation with $w = 0, z = 1$ yields $s \in F$ and then with $v = 0$ immediately $s = 0$. So suppose $c \in D^\times \setminus F$. Then the second equation with $v = 0$ gives $s = 0$ if D is a division algebra.

(iv) is similar. □

As a direct consequence of the Lemmas 11 (i), (ii) and 12 we obtain:

Corollary 13. *For all quaternion algebras B, D over F and elements $c \in D^\times, b \in B^\times$,*

$$\text{Cay}_{t(2,3)}(D, c) \not\cong \text{Cay}_{t(2,3,4)}(B, b)$$

and

$$\text{Cay}_{t(2,3)}(D, c)^{op} \not\cong \text{Cay}_{t(2,3,4)}(B, b).$$

Computing the nuclei also for the other algebras is one possibility to see if the algebras within two families are isomorphic or not. We omit this here to keep the paper within reasonable length.

5. ISOMORPHISMS

5.1. Let B and D be two quaternion algebras over F and $g : D \rightarrow B$ an algebra isomorphism. Let $m \in F^\times$. Then the map

$$(u, v) \rightarrow (g(u), m^{-1}g(v))$$

induces the following algebra isomorphisms:

$$\begin{aligned} \text{Cay}_t(D, c) &\cong \text{Cay}_t(B, m^2g(c)), \\ {}_r\text{Cay}_t(D, c) &\cong {}_r\text{Cay}_t(B, m^2g(c)), \\ {}_m\text{Cay}_t(D, c) &\cong {}_m\text{Cay}_t(B, m^2g(c)). \end{aligned}$$

For $D = B$, $g(u) = aua^{-1}$ for a suitable $a \in D^\times$ by the Theorem of Skolem-Noether [KMRT, (1.4), p. 4], therefore

$$\begin{aligned} \text{Cay}_t(D, c) &\cong \text{Cay}_t(D, m^2aca^{-1}), \\ {}_r\text{Cay}_t(D, c) &\cong {}_r\text{Cay}_t(D, m^2aca^{-1}), \\ {}_m\text{Cay}_t(D, c) &\cong {}_m\text{Cay}_t(D, m^2aca^{-1}). \end{aligned}$$

Example 14. For $\text{char } F \neq 2$ and $c = c_0 + c_1i + c_2j + c_3k \in D^\times \setminus F$,

$$\begin{aligned}\text{Cay}_t((a, b)_F, c) &\cong \text{Cay}_t((e^2a, f^2b)_F, c_0 + ec_1i + fc_2j + efc_3k), \\ {}_m\text{Cay}_t((a, b)_F, c) &\cong {}_m\text{Cay}_t((e^2a, f^2b)_F, c_0 + ec_1i + fc_2j + efc_3k), \\ {}_r\text{Cay}_t((a, b)_F, c) &\cong {}_r\text{Cay}_t((e^2a, f^2b)_F, c_0 + ec_1i + fc_2j + efc_3k),\end{aligned}$$

since $(a, b)_F \cong (e^2a, f^2b)_F$ via $g(i) = ei, g(j) = fj$ for $e, f \in F^\times$ and

$$\begin{aligned}\text{Cay}_t((a, b)_F, c) &\cong \text{Cay}_t((b, a)_F, c_0 + abc_2i + abc_1j + a^2b^2c_3k), \\ {}_m\text{Cay}_t((a, b)_F, c) &\cong {}_m\text{Cay}_t((e^2a, f^2b)_F, c_0 + ec_1i + fc_2j + efc_3k), \\ {}_r\text{Cay}_t((a, b)_F, c) &\cong {}_r\text{Cay}_t((e^2a, f^2b)_F, c_0 + ec_1i + fc_2j + efc_3k),\end{aligned}$$

since $(a, b)_F \cong (b, a)_F$ via $g(i) = abj, g(j) = abi$.

For $\text{char } F = 2$, $D = \text{Cay}(L, b) = [a, b]$ for some separable quadratic field extension L/F and $c = m + nj \in D = \text{Cay}(L, b)$ invertible, $m, n \in L$,

$$\begin{aligned}\text{Cay}_t(D, m + nj) &\cong \text{Cay}_t(D, m + fnj), \\ {}_m\text{Cay}_t(D, m + nj) &\cong {}_m\text{Cay}_t(D, m + fnj), \\ {}_r\text{Cay}_t(D, m + nj) &\cong {}_r\text{Cay}_t(D, m + fnj),\end{aligned}$$

for all $f \in F^\times$, since $D = \text{Cay}(L, b) \cong \text{Cay}(L, f^2b)$ via $g(w, z) = (w, fz)$ for $f \in F^\times$.

We focus again on $t = t(1)$, $t = t(2)$, $t = t(1, 2)$, $t = t(3, 4)$, $t = t(1, 3, 4)$ or $t = t(2, 3, 4)$.

Theorem 15. Let D and B be two quaternion division algebras.

(a) Suppose and $c \in D^\times \setminus F$, $d \in B^\times \setminus F$, $t = t(1)$, $t = t(2)$, $t = t(1, 2)$, $t = t(3, 4)$, $t = t(1, 3, 4)$ or $t = t(2, 3, 4)$ and that one of the following holds:

- (i) $\text{Cay}_t(D, c)$ and $\text{Cay}_t(B, d)$ are two division algebras such that $\text{Cay}_t(D, c) \cong \text{Cay}_t(B, d)$.
- (ii) ${}_r\text{Cay}_t(D, c)$ and ${}_r\text{Cay}_t(B, d)$ are two division algebras such that ${}_r\text{Cay}_t(D, c) \cong_r \text{Cay}_t(B, d)$.
- (iii) ${}_m\text{Cay}_t(D, c)$ and ${}_m\text{Cay}_t(B, d)$ are two division algebras such that ${}_m\text{Cay}_t(D, c) \cong {}_m\text{Cay}_t(B, d)$. Then $D \cong B$ and either both c and d lie in two isomorphic separable quadratic field extensions or they both lie in two isomorphic purely inseparable quadratic field extensions contained in D , resp. B . If $c \in L$ and $d \in L'$ lie in two isomorphic separable quadratic field extensions L and L' then there is an element $s \in D^\times$ such that

$$g(c) = N_{D/F}(s)d$$

with $g : L \rightarrow L'$ an isomorphism.

(b) Let $c, d \in F^\times$. If $\text{Cay}_{t(2,3)}(D, c) \cong \text{Cay}_{t(2,3)}(B, d)$ then D and B are isomorphic.

Proof. (a) Every isomorphism maps a quaternion subalgebra of $\text{Cay}(D, c)$ to a quaternion subalgebra of $\text{Cay}(B, d)$, hence $D \cong B$ in (i), (ii), (iii) by Theorem 9.

By Theorem 10, both $c \in D^\times$ and $d \in B^\times$ either both lie in two separable isomorphic quadratic field extensions contained in D , resp. B (in which case both algebras have a nonassociative quaternion subalgebra) or both lie in two isomorphic purely inseparable quadratic field extensions contained in D , resp. B (in which case both algebras have no nonassociative quaternion subalgebra).

Let us look at (i). Suppose both $c \in D^\times$ and $d \in B^\times$ lie in two separable quadratic

field extensions $L \subset D$ resp. $L' \subset B$. Then the isomorphism $\text{Cay}(D, c) \cong \text{Cay}(B, d)$ implies that $L \cong L'$ and that there are $z \in D^\times$, $z' \in B^\times$ such that $\text{Cay}(L, cN_{D/F}(z)) \cong \text{Cay}(L', dN_{B/F}(z'))$ (Theorem 10). Now

$$\text{Cay}(L, cN_{D/F}(z)) \cong \text{Cay}(L', dN_{B/F}(z')) \text{ implies } g(cN_{D/F}(z)) = N_{L'/F}(e')dN_{B/F}(z')$$

with $g : L \rightarrow L'$ an isomorphism and some non-zero $e' \in L'$, i.e.

$$N_{D/F}(z)g(c) = N_{B/F}(z')N_{L'/F}(e')d.$$

Since $D \cong B$ and $L \cong L'$, there is an element $t \in D^\times$ such that $N_{D/F}(t) = N_{B/F}(z')N_{L'/F}(e')$ and an element $s \in D^\times$ such that

$$g(c) = N_{D/F}(s)d.$$

If both $c \in D^\times$ and $d \in B^\times$ lie in a purely inseparable quadratic field extension $K \subset D$ resp. $K' \subset B$ then the isomorphism $\text{Cay}(D, c) \cong \text{Cay}(B, d)$ implies that $K \cong K'$ by Theorem 10.

The proof is the same for (ii) and (iii).

(b) Any isomorphism maps the left nucleus of $\text{Cay}_{t(2,3)}(D, c)$ onto the left nucleus of $\text{Cay}_{t(2,3)}(B, d)$, hence $D \cong B$ by Lemma 11. \square

For the rest of this section, let D be a quaternion division algebra and suppose that $c, d \in D^\times \setminus F$.

Lemma 16. *Let $G : \text{Cay}_t(D, c) \rightarrow \text{Cay}_t(D, d)$, $G :_m \text{Cay}_t(D, c) \rightarrow_m \text{Cay}_t(D, d)$ or $G :_r \text{Cay}_t(D, c) \rightarrow_r \text{Cay}_t(D, d)$ be an algebra isomorphism. Suppose $G((0, 1)) = (0, s)$ with $s \in D^\times$, i.e. that G maps Dl to Dl' . Then there is $a \in D^\times$ such that:*

- (i) $dN_{D/F}(s) = aca^{-1}$ if $G : \text{Cay}_t(D, c) \rightarrow \text{Cay}_t(D, d)$ or $G :_r \text{Cay}_t(D, c) \rightarrow_r \text{Cay}_t(D, d)$,
 - (ii) $\sigma(s)ds = aca^{-1}$ if $G :_m \text{Cay}_t(D, c) \rightarrow_m \text{Cay}_t(D, d)$ and $t = t(1)$, $t(3, 4)$, or $t(1, 3, 4)$
 - (iii) $sd\sigma(s) = aca^{-1}$ if $G :_m \text{Cay}_t(D, c) \rightarrow_m \text{Cay}_t(D, d)$ and $t = t(1, 2)$, $t(2)$ or $t(2, 3, 4)$.
- Moreover,

$$G((u, v)) = (aua^{-1}, sava^{-1})$$

if $t = t(1)$, $t = t(2)$ or $t = t(1, 2)$ and

$$G((u, v)) = (aua^{-1}, ava^{-1}s)$$

if $t = t(3, 4)$, $t = t(1, 3, 4)$ or $t = t(2, 3, 4)$.

Proof. By the uniqueness of the quaternion algebra D , we have $G((D, 0)) = (D, 0)$, so that $G((u, 0)) = (aua^{-1}, 0)$ for some $a \in D^\times$. In particular, we get $(aca^{-1}, 0) = G((c, 0)) = G((0, 1)(0, 1)) = G((0, 1))G((0, 1))$. If $G((0, 1)) = (0, s)$ with $s \in D^\times$ then $G((0, v)) = G((v, 0))G((0, 1)) = (ava^{-1}, 0)(0, s) = (0, sava^{-1})$, so that

$$G((u, v)) = (aua^{-1}, sava^{-1})$$

if $t = t(1)$, $t = t(2)$ or $t = t(1, 2)$ and $G((0, v)) = G((v, 0))G((0, 1)) = (ava^{-1}, 0)(0, s) = (0, sava^{-1})$, so that

$$G((u, v)) = (aua^{-1}, ava^{-1}s)$$

else. Moreover, we have $(aca^{-1}, 0) = (0, s)(0, s) = (d\sigma(s)s, 0)$ and thus

$$dN_{D/F}(s) = aca^{-1}$$

if $G : \text{Cay}_t(D, c) \rightarrow \text{Cay}_t(D, d)$ or $G :_r \text{Cay}_t(D, c) \rightarrow_r \text{Cay}_t(D, d)$ and $(aca^{-1}, 0) = (0, s)(0, s) = (\sigma(s)ds, 0)$ and thus

$$\sigma(s)ds = aca^{-1}$$

if $G :_m \text{Cay}_t(D, c) \rightarrow_m \text{Cay}_t(D, d)$ and $t = t(1)$, $t(3, 4)$, or $t(1, 3, 4)$ or $(aca^{-1}, 0) = (0, s)(0, s) = (sd\sigma(s), 0)$ and thus

$$sd\sigma(s) = aca^{-1}$$

if $t = t(1, 2)$, $t(2)$ or $t(2, 3, 4)$. □

Theorem 17. (a) Suppose $t = t(2)$, $t = t(1, 2)$, $t = t(3, 4)$ or $t = t(1, 3, 4)$. Then $\text{Cay}_t(D, c) \cong \text{Cay}_t(D, d)$ if and only if there are $a \in D^\times$, $m \in F^\times$, such that $d = m^2aca^{-1}$. The isomorphisms are then given by the maps

$$G((u, v)) = (aua^{-1}, m^{-1}ava^{-1}).$$

Suppose $t = t(1)$ or $t = t(2, 3, 4)$. Then $\text{Cay}_t(D, c) \cong \text{Cay}_t(D, d)$ if and only if there are $a, s \in D^\times$ such that $dN_{D/F}(s) = c$. The isomorphisms are then given by the maps

$$G((u, v)) = (aua^{-1}, sava^{-1})$$

if $t = t(1)$ and by

$$G((u, v)) = (aua^{-1}, ava^{-1}s)$$

if $t = t(2, 3, 4)$.

(b) Suppose $t = t(2)$, $t = t(1, 2)$, $t = t(3, 4)$ or $t = t(1, 3, 4)$. Then ${}_r\text{Cay}_t(D, c) \cong {}_r\text{Cay}_t(D, d)$ if and only if there are $a \in D^\times$, $m \in F^\times$, such that $d = m^2aca^{-1}$. The isomorphisms are then given by the maps

$$G((u, v)) = (aua^{-1}, m^{-1}ava^{-1}).$$

Suppose $t = t(1)$ or $t = t(2, 3, 4)$. Then ${}_r\text{Cay}_t(D, c) \cong {}_r\text{Cay}_t(D, d)$ if and only if there are $a, s \in D^\times$ such that $dN_{D/F}(s) = c$. The isomorphisms are then given by the maps

$$G((u, v)) = (aua^{-1}, sava^{-1})$$

$t = t(1)$ and by

$$G((u, v)) = (aua^{-1}, ava^{-1}s)$$

if $t = t(2, 3, 4)$.

Proof. (a) Let $G : \text{Cay}_t(D, c) \rightarrow \text{Cay}_t(D, d)$ be an algebra isomorphism which maps Dl to Dl' . Since G is multiplicative we have

$$(1) \quad G((u, v)(u', v')) = G(u, v)G(u', v').$$

For $t = t(1)$, equation (1) is equivalent to

$$(2) \quad ac\bar{v}'va^{-1} = d\bar{a}^{-1}\bar{v}'va^{-1}N(a)N(s),$$

$$(3) \quad sav\bar{u}'a^{-1} = zav\bar{u}'\bar{a}N(a)^{-1}$$

for all $u, u', v, v' \in D$. Using that $dN_{L/F}(s) = aca^{-1}$ by Lemma 16, both equations are true for all $a, z \in D^\times$ with $dN_{D/F}(s) = aca^{-1}$, they are the same as if we use the classical Cayley-Dickson doubling, cf. [Pu, Theorem 14].

For $t(2)$ or $t(1, 2)$, only the first equation changes and becomes

$$(2) \quad acv\bar{v}'a^{-1} = dsav\bar{v}'\bar{a}\bar{s}N(a)^{-1}$$

for all $u, u', v, v' \in D$. This is equivalent to

$$v\bar{v}' = a^{-1}\bar{s}^{-1}av\bar{v}'\bar{a}\bar{s}N(a)^{-1},$$

i.e.

$$av\bar{v}'a^{-1} = \bar{s}^{-1}(av\bar{v}'a^{-1})\bar{s},$$

for all $u, u', v, v' \in D$ and implies that $sw = ws$ for all $w \in D$, hence $s \in \text{Comm}(D) = F$. This makes (1) true. Put $m = s^{-1}$.

Let $t = t(3, 4)$ or $t = t(1, 3, 4)$. Equation (1) is then equivalent to

- (2) $ac\bar{v}'va^{-1} = d\bar{s}\bar{a}^{-1}\bar{v}'\bar{a}ava^{-1}s$ and
- (3) $a\bar{u}'va^{-1}s = \bar{a}^{-1}\bar{u}'va^{-1}zN(a)$

for all $u, u', v, v' \in D$. Equation (3) is always true. With $d\bar{s} = aca^{-1}s^{-1}$, (2) is the same as

$$\bar{v}'va^{-1} = a^{-1}s^{-1}\bar{a}^{-1}\bar{v}'va^{-1}sN(a)$$

for all $u, u', v, v' \in D$. This is equivalent to

$$w = a^{-1}s^{-1}\bar{a}^{-1}wsN(a)$$

for all $w \in D$, i.e. to

$$s(\bar{a}^{-1}w) = (\bar{a}^{-1}w)s$$

for all $w \in D$ and we conclude that we need $s \in \text{Comm}(D) = F$ in order for (1) to hold.

For $t = t(2, 3, 4)$, equation (1) is equivalent to

- (2) $acv\bar{v}'a^{-1} = dava^{-1}s\bar{s}\bar{a}^{-1}\bar{v}'\bar{a}$ and
- (3) $a\bar{u}'va^{-1}s = \bar{a}^{-1}\bar{u}'va^{-1}zN(a)$

for all $u, u', v, v' \in D$. (3) is always true. Using that $dN_{L/F}(s) = aca^{-1}$, (2) is equivalent to

$$v\bar{v}'a^{-1} = v\bar{v}'a^{-1}$$

and thus also true for all $a, s \in D^\times$ with $dN_{L/F}(s) = aca^{-1}$.

It remains to show that for $G : \text{Cay}_t(D, c) \rightarrow \text{Cay}_t(D, d)$ indeed $G((0, 1)) = (0, s)$. Suppose that $G((0, 1)) = (t, s)$ with $t, s \in D$ and $t \neq 0$. Then $(aca^{-1}, 0) = G((c, 0)) = G((0, 1))G((0, 1)) = (t, s)(t, s) = (t^2 + d\sigma(s)s, s(t + \sigma(t)))$ implies that

$$t^2 + d\sigma(s)s = 0 \text{ and } s(t + \sigma(t)) = 0.$$

If $s = 0$ then $t \neq 0$ and G is not injective, since $G((0, 1)) = (t, 0) = G((a^{-1}ta, 0))$. Thus $s \neq 0$ and $\sigma(t) = -t$.

Assume $t = t(2)$. G is multiplicative, hence we have

$$G((0, v)) = G((v, 0))G((0, 1)) = (ava^{-1}, 0)(t, s) = (ava^{-1}t, sava^{-1})$$

and

$$G((u, v)) = G((u, 0)) + G((v, 0)) = (aua^{-1} + ava^{-1}t, sava^{-1})$$

for all $u, v \in D$. Use $G((u, v)(u', v')) = G((u, v))G((u', v'))$: The first entry yields

$$\begin{aligned} (aua^{-1} + ava^{-1}t)(au'a^{-1} + av'a^{-1}t) + c(sava^{-1})(\sigma(a^{-1}\sigma(v)\sigma(a)\sigma(s))) \\ = auu'a^{-1} + acv\sigma(v')a^{-1} + a(v'u + v\sigma(u'))a^{-1}t \end{aligned}$$

for all $u, v, u', v' \in D$. Put $v = 0$ to obtain $uv'a^{-1}t = v'ua^{-1}t$ and since $t \neq 0$ thus $uv' = v'u$ for all $u, v' \in D$, a contradiction.

Assume $t = t(1)$. G is multiplicative, hence we have

$$G((0, v)) = G((v, 0))G((0, 1)) = (ava^{-1}, 0)(t, s) = (tava^{-1}, sava^{-1})$$

and

$$G((u, v)) = G((u, 0)) + G((v, 0)) = (aua^{-1} + tava^{-1}, sava^{-1})$$

for all $u, v \in D$. Use $G((u, v)(u', v')) = G((u, v))G((u', v'))$: The first entry yields

$$\begin{aligned} & (aua^{-1} + tava^{-1})(au'a^{-1} + tav'a^{-1}) + c(\sigma(a^{-1}\sigma(v)\sigma(a)\sigma(s)))(sava^{-1}) \\ & = auu'a^{-1} + ac\sigma(v')va^{-1} + ta(v'u + v\sigma(u'))a^{-1} \end{aligned}$$

for all $u, v, u', v' \in D$. Put $v = 0$ to obtain

$$aua^{-1}tav' = tav'u.$$

for all $u, v' \in D$, for $v' = 1$, thus $u(a^{-1}ta) = (a^{-1}ta)u$ for all $u, v' \in D$, hence $a^{-1}ta \in F^\times$ so that $t \in F^\times$, implying $uv' = v'u$ for all $u, v' \in D$, a contradiction.

Assume $t = t(1, 2)$. G is multiplicative, hence we have

$$G((0, v)) = G((v, 0))G((0, 1)) = (ava^{-1}, 0)(t, s) = (tava^{-1}, sava^{-1})$$

and

$$G((u, v)) = G((u, 0)) + G((v, 0)) = (aua^{-1} + tava^{-1}, sava^{-1})$$

for all $u, v \in D$. Use $G((u, v)(u', v')) = G((u, v))G((u', v'))$: The first entry yields

$$\begin{aligned} & (au'a^{-1} + tav'a^{-1})(aua^{-1} + tava^{-1}) + c(sava^{-1})(\sigma(a^{-1}\sigma(v)\sigma(a)\sigma(s))) \\ & = au'u'a^{-1} + acv\sigma(v')a^{-1} + ta(v'u + v\sigma(u'))a^{-1} \end{aligned}$$

for all $u, v, u', v' \in D$. Put $v = 0$ to obtain $tav'u = tav'u$ for all $u, v' \in D$, thus $v'u = v'u$ for all $u, v' \in D$ since $t \neq 0$, a contradiction.

The proof for the other cases works analogously. To prove that $t = 0$ it suffices again to look at the first equation above.

(b) Let $G : {}_r\text{Cay}_t(D, c) \rightarrow {}_r\text{Cay}_t(D, d)$ be an algebra isomorphism which maps Dl to Dl' . Since G is multiplicative we have

$$(1) \quad G((u, v)(u', v')) = G(u, v)G(u', v').$$

An analogous proof as the one for $t = t(1)$, $t = t(2)$ or $t = t(1, 2)$ in Proposition (a) also works for $G : {}_r\text{Cay}_t(D, c) \rightarrow {}_r\text{Cay}_t(D, d)$. Next let $t = t(3, 4)$ or $t = t(1, 3, 4)$. Then equation (1) is equivalent to

$$(2) \quad a\bar{v}'vca^{-1} = \bar{s}\bar{a}^{-1}\bar{v}'\bar{a}ava^{-1}sd \text{ and}$$

$$(3) \quad a\bar{u}'va^{-1}s = \bar{a}^{-1}\bar{u}'va^{-1}sN(a)$$

for all $u, u', v, v' \in D$. Equation (3) is true. With $dN_{D/F}(s) = aca^{-1}$, (2) is the same as

$$a\bar{v}'v = \bar{s}\bar{a}^{-1}\bar{v}'va^{-1}\bar{s}^{-1}aN_{D/F}(a),$$

for all $u, u', v, v' \in D$, i.e. to $w\bar{z} = \bar{z}w$ for all $w \in D$ implying $s \in F^\times$.

Let $t = t(2, 3, 4)$. Then equation (1) is equivalent to two equations (2') and (3') as before, with equation (3') being equation (3) in (a), so always true. Equation (2') is

$$avv'ca^{-1} = ava^{-1}s\bar{s}a^{-1}\bar{v}'\bar{a}d$$

and holds for all $a, s \in D^\times$ with $dN_{D/F}(s) = aca^{-1}$. The remaining assertions now follows analogously as in (a). The converse is now a straightforward calculation in all cases. \square

Corollary 18. *Let $A = \text{Cay}_t(D, c)$ or $A = {}_r\text{Cay}_t(D, c)$.*

(i) *Suppose $t = t(2)$, $t = t(1, 2)$, $t = t(3, 4)$ or $t = t(1, 3, 4)$. The automorphisms of A are given by the maps*

$$G((u, v)) = (aua^{-1}, m^{-1}ava^{-1})$$

where $a \in D^\times$, $m \in F^\times$, such that $ca = m^2ac$.

(ii) *Suppose $t = t(1)$ or $t = t(2, 3, 4)$. The automorphisms of A are given by the maps*

$$G((u, v)) = (aua^{-1}, sava^{-1})$$

if $t = t(1)$ and by

$$G((u, v)) = (aua^{-1}, ava^{-1}s)$$

if $t = t(2, 3, 4)$, with $a, s \in D^\times$ such that $N_{D/F}(s) = 1$.

Corollary 19. *Let B, D be two quaternion division algebras, $c, d \in D^\times \setminus F$. Let s, t be elements of $\{t(1), t(2), t(1, 2), t(3, 4), t(1, 3, 4), t(2, 3, 4)\}$.*

(i) *If $\text{Cay}_t(D, c) \cong_r \text{Cay}_s(B, d)$ then $B \cong D$.*

(ii) *If ${}_m\text{Cay}_t(D, c) \cong \text{Cay}_s(B, d)$ then $B \cong D$.*

(iii) *If $\text{Cay}_t(D, c) \cong_r \text{Cay}_s(B, d)$ then $B \cong D$.*

Moreover, the isomorphisms imply either both c and d lie in two isomorphic separable quadratic field extensions L and L' or they both lie in two isomorphic purely inseparable quadratic field extensions K and K' .

This follows from the above results. Concerning the question if there are isomorphisms between the different classes of twisted Cayley-Dickson doublings, we conjecture that given a quaternion division algebra D , $c, d \in D^\times \setminus F$, and s, t elements of $\{t(1), t(2), t(1, 2), t(3, 4), t(1, 3, 4), t(2, 3, 4)\}$, it can be shown that

$$\text{Cay}_t(D, c) \not\cong_r \text{Cay}_s(D, d),$$

$${}_m\text{Cay}_t(D, c) \not\cong \text{Cay}_s(D, d)$$

and

$${}_m\text{Cay}_t(D, c) \not\cong_r \text{Cay}_s(D, d).$$

The proof should work analogously to the one of Theorem 17.

6. DIVISION ALGEBRAS OF DIMENSION 16

We briefly point out that we can also obtain results on division algebras of dimension 16:

Theorem 20. *Let C be an octonion division algebra over F with canonical involution $\sigma = -$. Let $A = \text{Cay}_t(C, c)$, $A =_m \text{Cay}_t(C, c)$ or $A =_r \text{Cay}_t(C, c)$.*

- (i) *A is a division algebra for any choice of $c \in C^\times \setminus F$ such that $N_{C/F}(c) \notin N_{C/F}(C^\times)^2$.*
- (ii) *A is a division algebra for any choice of $c \in C^\times \setminus F$ such that $N_{C/F}(c) \notin F^{\times 2}$.*
- (iii) *A is a division algebra for any choice of $c \in F^\times$ such that $c \notin \pm N_{C/F}(C^\times)$.*

Proof. (i) and (iii): We show that $A = \text{Cay}_{t(2,3)}(C, c)$ has no zero divisors: suppose

$$(0, 0) = (r, s)(u, v) = (ru + c(s\bar{v}), rv + s\bar{u})$$

for $r, s, u, v \in C$. This is equivalent to

$$ru + c(s\bar{v}) = 0 \text{ and } rv + s\bar{u} = 0.$$

Assume $s = 0$, then $ru = 0$ and $rv = 0$. Hence either $r = 0$ and so $(r, s) = 0$ or $r \neq 0$ and $u = v = 0$ (this is the same for all possible t).

So let $s \neq 0$. Then $s \in C^\times$ and $s\bar{u} = -rv$. Thus $u\bar{s} = -\bar{v}\bar{r}$, $(u\bar{s})\bar{s} = u\bar{s}^2 = (-\bar{v}\bar{r})\bar{s}$ (since A is flexible), thus $u = -\frac{1}{N(s)^2}((\bar{v}\bar{r})\bar{s})s^2$ plugged into $ru + c(s\bar{v}) = 0$ implies that

$$\frac{1}{N(s)^2}r((\bar{v}\bar{r})\bar{s})s^2 = c(s\bar{v}).$$

Applying the norm $N_{D/F}$ we obtain that

$$N(r)^2N(v) = N(c)N(s)^2N(v).$$

If $v = 0$ then $ru = 0$ and $s\bar{u} = 0$, thus $u = 0$ and $(u, v) = 0$. If $v \neq 0$ then $N_{D/F}(v) \neq 0$ and $N_{D/F}(c) = N_{D/F}(\frac{r}{s})^2$, a contradiction to our initial assumption that $c \in C^\times \setminus F$ and $N_{C/F}(c) \notin N_{C/F}(C^\times)^2$, resp. $c \in F^\times$ such that $c \notin \pm N_{C/F}(C^\times)$, unless $r = 0$. However, if $r = 0$ (and $s \neq 0$ as assumed above) then the initial two equalities give $u = 0$ and $v = 0$, so that $(u, v) = (0, 0)$.

The other cases (i.e., different t) are treated similarly, the argument remains the same.

The proof for $A =_m \text{Cay}_t(C, c)$ and $A =_r \text{Cay}_t(C, c)$ is along the same lines, the placement of c is not relevant for the argument.

(ii) follows from (i). □

Example 21. Let $F = \mathbb{Q}$ and $C = \text{Cay}(\mathbb{Q}, a, b, e)$ an octonion algebra.

For all $a, b, e < 0$, C is a division algebra and $\text{Cay}_t(C, c)$, $_m \text{Cay}_t(C, c)$ and $_r \text{Cay}_t(D, c)$ are division algebras for all t and all $c = x_0 + x_1i + x_2j + x_3k + x_4l + x_5il + x_6jl + x_7kl$, such that the positive rational number

$$N_{D/F}(c) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 - ex_4^2 + aex_5^2 + bex_6^2 - abex_7^2$$

is not a square. E.g., let $C = \text{Cay}(\mathbb{Q}, -1, -1, -1)$. If c is not a sum of 8 squares then $\text{Cay}_t(C, c)$, $_m \text{Cay}_t(C, c)$ and $_r \text{Cay}_t(D, c)$ are division algebras for all t .

The structure of these algebras remains similar as well, for instance:

Theorem 22. *Let F have characteristic not 2 and let C be an octonion division algebra, $c \in C \setminus F$ invertible. Let $t = t(1)$, $t = t(2)$, $t = t(1, 2)$, $t = t(3, 4)$, $t = t(1, 3, 4)$ or $t = t(2, 3, 4)$. Then C is the only octonion subalgebra of the algebras $A = \text{Cay}_t(C, c)$, respectively $A = {}_r\text{Cay}_t(C, c)$.*

If there is a quaternion algebra D such that the Dickson algebra $\text{Cay}(D, d)$ is a subalgebra of $\text{Cay}(C, c)$, respectively $\text{Cay}_r(D, d)$ of $\text{Cay}_r(C, c)$, then D is a subalgebra of C , $c \in D$, and there is $z \in C^\times$ such that $d = cN_{C/F}(z)$.

The proof is analogous to the one of Theorems 9 and 10.

Corollary 23. *Let F have characteristic not 2 and let C, H be two octonion division algebras, $c \in C \setminus F$, $d \in H \setminus F$. Let $t = t(1)$, $t = t(2)$, $t = t(1, 2)$, $t = t(3, 4)$, $t = t(1, 3, 4)$ or $t = t(2, 3, 4)$. If $\text{Cay}_t(C, c) \cong \text{Cay}_t(H, d)$ or ${}_r\text{Cay}_t(C, c) \cong_r \text{Cay}_t(H, d)$ then $C \cong H$.*

REFERENCES

- [A] Albert, A. A., *On the power-associativity of rings*. Summa Braziliensis Mathematicae 2, 21 – 33, 1948.
- [Al-H-K] Althoen, C., Hansen, K. D., Kugler, L. D., *\mathbb{C} -Associative algebras of dimension 4 over \mathbb{R}* . Algebras, Groups and Geometries 3, pp. 329 – 360, 1986.
- [As-Pu] Astier, V., Pumplün, S., *Nonassociative quaternion algebras over rings*. Israel J. Math. 155, 125 – 147, 2006.
- [B-B-O] Benkart, G. M., Britten, D. J., Osborn, J. M., *Real flexible division algebras*. Canad. J. of Math. 34 (3), 550 – 588, 1982.
- [B-O1] Benkart, G. M., Osborn, J. M., *The derivation algebra of a real division algebra*. Amer. J. of Math. 103 (6), 1135 – 1150, 1981.
- [B-O2] Benkart, G. M., Osborn, J. M., *An investigation of real division algebras using derivations*. Pacific J of Math. 96 (2), 265 – 300, 1981.
- [Be-Og1] G. Berhuy, F. Oggier, *On the existence of perfect space-time codes*. Transactions on Information Theory 55 (5) May 2009, 2078 – 2082.
- [Be-Og2] G. Berhuy, F. Oggier, *Introduction to central simple algebras and their applications to wireless communication*.
<http://www.foutier.ujf-grenoble.fr/~berhuy/fichiers/BOCSA.pdf>
- [Be-Og3] G. Berhuy, F. Oggier, *Space-time codes from crossed product algebras of degree 4*. S. Boztaş and H.F. Lu (Eds.), AAEECC 2007, LNCS 4851, pp. 90 – 99, 2007.
- [C-V-K-R] Cuenca Mira, J. A., De Los Santos Villodres, R., Kaidi, A., Rochdi, A., *Real quadratic flexible division algebras*. Linear Algebra and its Appl. 290, 1 – 22, 1999.
- [D-D-H] Darpö, E., Dieterich, E., Herschend, M., *In which dimensions does a division algebra over a given ground field exist?* Enseign. Math. 51 (3 – 4), 255 – 263, 2005.
- [Di] Dickson, L. E., *Linear Algebras with associativity not assumed*. Duke Math. J. 1, 113 – 125, 1935.
- [Die] Dieterich, E., *Power-associative division algebras*. Algebras and Modules, II (Geiranger, 1996), 134 – 144, CMS Conference Proc., Amer. Math. Soc., Providence, RI, 1998.
- [Do-Z1] Dokovich, D.Z., Zhao, K., *Real homogeneous algebras as truncated division algebras and their automorphism groups*. Algebra Colloq. 11 (1), 11 – 20, 2004.
- [Do-Z2] Dokovich, D.Z., Zhao, K., *Real division algebras with large automorphism group*. J. Algebra 282, 758 – 796, 2004.
- [J-P] Jiménez-Gestal, C., Pérez-Izquierdo, J. M., *Ternary derivations of finite-dimensional real division algebras*. Linear Algebra Appl. 428, 2192 – 2219, 2008.
- [E-S-K] P. Elia, A. Sethuraman, P. V. Kumar, *Perfect space-time codes with minimum and non-minimum delay for any number of antennas*. Proc. Wirelss Com 2005, International Conference on Wireless Networks, Communications and Mobile Computing.

- [H-L-R-V] C. Hollanti, J. Lahtonen, K. Rauto, R. Vehkalahti, *Optimal lattices for MIMO codes from division algebras*. IEEE International Symposium on Information Theory, July 9 - 14, 2006, Seattle, USA, 783 – 787.
- [K] Kervaire, M., *Non-parallelizability of the n -sphere for $n > 7$* . Proc. Nat. Acad. Sci. 44, 280 – 283, 1958.
- [L] Lam, T.Y., "Quadratic forms over fields". Graduate studies in Mathematics, Vol. 67, AMS Providence, Rhode Island, 2005.
- [M-B] Milnor, J., Bott, R., *On the parallelizability of the spheres*. Bull. AMS 64, 87 – 89, 1958.
- [O-R-B-V] F. Oggier, G. Rekaya, J.-C. Belfiore, E. Viterbo, *Perfect space-time block codes*. IEEE Trans. on Information Theory 32 (9), pp. 3885–3902, Sept. 2006.
- [Pu] Pumplün, S. *How to obtain division algebras out of a generalized Cayley-Dickson process*. Preprint on arXiv:math.RA/0906.5374, 2009.
- [Pu-U] Pumplün, S., Unger, T. *Space-time block codes from nonassociative division algebras*. Preprint on arxiv:1006.2348v1[cs.IT], 2010.
- [R] Rochdi, A., *Étude des algèbres réelles de Jordan noncommutatives, de division, de dimension 8, dont l'algèbre de Lie des dérivations n'est triviale*. J. Algebra 178, 843 – 871, 1995.
- [Sch] R.D. Schafer, "An introduction to nonassociative algebras", Dover Publ., Inc., New York, 1995.
- [S] Scharlau, W., "Quadratic and Hermitian Forms." Springer-Verlag, Berlin-Heidelberg-New York, 1985.
- [S-R-S] B. A. Sethuraman, B. S. Rajan, V. Sashidhar, *Full diversity, high rate space time block codes from division algebras*. IEEE Trans. Inf. Theory 49, pp. 2596 – 2616, Oct. 2003.
- [W] Waterhouse, W.C., *Nonassociative quaternion algebras*. Algebras, Groups and Geometries 4, 365 – 378, 1987.

E-mail address: susanne.pumpluen@nottingham.ac.uk

SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITY OF NOTTINGHAM, UNIVERSITY PARK, NOTTINGHAM NG7 2RD, UNITED KINGDOM