International Journal of Mathematics and
Computer Science, **17**(2022), no. 3, 1211–1218

On composition algebras and their automorphism groups

Mashhour Bani-Ata[1], **Ra'ed Al-Nouty**[2],
Khaled Ali Ahmad Kasasbeh[3]

[1]Department of Mathematics
The Public Authority for Applied Education and Training
Adailiyah, Kuwait

[2]Department of Mathematics
Hashemite University,
Zarqa, Jordan

[3] Department of Mathematics
Aljahra, Kuwait

email: mashhour_ibrahim@yahoo.com, ghalebit@yahoo.com,
kkkald_81@yahoo.com

(Received February 22, 2022, Accepted April 4, 2022)

Abstract

The purpose of this article is to investigate composition algebras over fields $\mathbb{F}_q = GF(q)$, $q = p^m$, p prime, and in particular the Cayley-Dickson numbers, also called octaves, and their automorphism groups $G_2(q)$.

1 Introduction

We are only assuming composition algebras over finite fields. It turns out that there is a quite few of them. A composition Algebra A is an algebra (not necessarily associative) over a finite filed $\mathbb{F}$ with unit element e, equipped

Key words and phrases: Composition Algebra, Cayley-Dickson Algebra, automorphism groups.
AMS (MOS) Subject Classifications: 17A75.
Mashhour Bani-Ata is the corresponding author.
ISSN 1814-0432, 2022, http://ijmcs.future-in-tech.net

with a non-degenerate quadratic form Q such that $Q(xy) = Q(x)Q(y)$ for all $x, y \in A$, where $Q : A \to \mathbb{F}$ such that $Q(\lambda x) = \lambda^2 Q(x)$ for all $x \in A$, $\lambda \in \mathbb{F}$, associated with a bilinear map $(x, y) = Q(x + y) - Q(x) - Q(y)$. The possible dimensions of A are $1, 2, 4, 8$. There is a unique composition algebra of dimension 8, called the Cayley-Dickson algebra. There exist 2 algebras of dimension $2, 4$ depending whether the form Q has a maximal Witt-index or not. The Witt-index$= max\{dimW \mid W \leq V \ , \ Q(w) = 0 \ \forall w \in W\}$, where V is a vector space over $\mathbb{F}_q$. We know that Witt-index$= \frac{1}{2}dimV$ or $\frac{1}{2}dimV - 1$, in other words, for dimension 2,4, we have 2 types of quadratic forms, for each such form, there is a unique algebra. Hence for dimension 8, the form Q must have Witt-index 4 and there exists a unique algebra for such form. The automorphism group $G_2(q)$ of the Cayley Dickson algebra A consists of all $g \in GL(A)$ such that $Q(x^g) = Q(x)$ for all $x \in A$ and $x^g \circ y^g = (x \circ y)^g$. From understanding the Cayley-Dickson algebra we also get information on elements of p-order in $G_2(q)$; i. e., if r is a prime, $r \neq p$, $o(g) = r$, $g \in G_2(q)$, then $C_A(g)$ the centralizer of g in A is a subalgebra of A of dim $2, 4$, and if $dimC_A(g) = 2$, then $C_{G_2(q)}(g) = SL(3, g)$ as we will prove later . For more information about composition algebras one may refer to [2], [3], [4] and [5].

Examples: We give examples of composition algebras with a quadratic form Q.

1. $A = \mathbb{F}_q$, $x \circ y = xy$, $Q(x) = x^2$, $\forall x, y \in \mathbb{F}_{q^2}$ and $dimA = 1$.

2. $A = \mathbb{F}_q \times \mathbb{F}_q = \{(x, y) \mid x, y \in \mathbb{F}_q\}$.
   Define $(a, b) \circ (x, y) = (ax, by)$, $\forall a, b, x, y \in \mathbb{F}_q$ and $Q : A \to \mathbb{F}_q$ by $Q(x, y) = xy$. Then $Q((a, b) \circ (x, y)) = Q(ax, by) = axby = Q(a, b) \cdot Q(x, y)$ and $dimA = 2$.

3. $A = \mathbb{F}_{q^2}$, define $x \circ y = xy$ (field multiplication), $x, y \in \mathbb{F}_q$, and define $Q(x) = x\overline{x}$, where $\overline{x} = x^q$, then $Q(x \circ y) = Q(xy) = (xy)(xy)^q = (xy)^{q+1} = x^{q+1}y^{q+1} = Q(x) \cdot Q(y)$ and $dim_{\mathbb{F}_q}A = 2$.

4. (a) Let $A = \left\{ \begin{bmatrix} a & b \\ -\overline{b} & \overline{a} \end{bmatrix} \mid a, b \in \mathbb{F}_q \ , \ \overline{b} = b^q \right\}$, $dim_{\mathbb{F}_q}A = 4$.

   (b) or $A = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b \in \mathbb{F}_q \right\}$

   Let $M, N \in A$, define $M \circ N = MN$ (matrix multiplication), and the quadratic form $Q : A \to \mathbb{F}_q$ by $Q(M) = det(M)$. A is closed under matrix multiplication, So A is an algebra. For the classification of composition algebras of dimension 4, see [1, 3].

5. Let A be the Cayley-Dikson algebra, over $\mathbb{F}_q$ and let $G = G_2(q)$ be its automorphism group; i.e., A is a non associative algebra of dimension eight over $\mathbb{F}_q$ with unit element e and equipped with a non-degenerate quadratic from Q such that $Q(xy) = Q(x)Q(y)$ for all $x, y \in A$. The associated bilinear form in denoted by $(,)$. The group $G = \{g \in GL(A) | e^g = e,\ Q(x^g) = Q(x),\ (x,y)^g = x^g y^g\ \forall x, y \in A\}$.

In particular, $G \leq O^+(8,q)$ the orthogonal group corresponding to Q, fixing e. So $G \leq O(7,q)$ acting on $A/\langle e\rangle = e^\perp$.

For the composition algebra $A = \mathbb{F}_q \times \mathbb{F}_q$, $\mathrm{Aut}(A) \cong Z_{q-1}$ consisting of all mappings : $(x,y) \to (x^t, x^{t-1})$, $t \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

If $A = \mathbb{F}_{q^2}$, then $Aut(A) = Z_{q+1}$ consisting of all mappings $x \to x^t$, $t \in \mathbb{F}_{q^2}$ with $t^{q+1} = 1$.

If $A = Mat(2 \times 2, \mathbb{F}_q)$, then $Aut(A) = PGL(2,q)$ and it is induced by the mappings $M \to M^g$, $g \in GL(2,q)$.

If $A = \left\{ \begin{bmatrix} a & b \\ -\overline{b} & \overline{a} \end{bmatrix} \mid a, b \in \mathbb{F}_{q^2} \right\}$, then $Aut(A) = PGL(2,q^2)$ induced by the mappings $M \to g^t M \overline{g}$, $M \in A$, $g \in U(2, \mathbb{F}_{q^2})$.

2 Properties of composition algebras

Let A be a composition algebra over a commutative groundfield K, which have a non-degenerate quadratic form Q; that is to say, forms satisfying $Q(a) = 0$ and $(x,a) = 0$ for all $a \in A$ implies $a = 0$, if the characteristic $\chi_K \neq 2$, then $(x,a) = 0$ for all $x \in A$ implies $Q(a) = 0$.

Properties :

(2.1) $(x,x) = 2Q(x),\ Q(e) = 1.$

(2.2) $Q(a)(x,y) = (ax, ay) = (xa, ya).$

(2.3) $(a,b)(x,y) = (ax, by) + (bx, ay).$

(2.4) Define $\overline{a} = (a,e)e - a,\ a \in A$, Then $\overline{\overline{a}} = a,\ Q(a) = Q(\overline{a}).$

(2.5) $(ax, y) = (x, \overline{a}y).$

(2.6) $a\overline{a} = Q(a)e$ or $a^2 - (a,e)a + Q(a)e = 0.$

(2.7) $ab + ba - (a,e)b - (b,e)a + (a,b)e = 0.$

(2.8) $\overline{ab} = \overline{a}\overline{b}.$

(2.9) $a(\overline{a}b) = \overline{a}(ab) = (b\overline{a})a = (ba)\overline{a} = Q(a)b.$

(2.10) If $a \neq 0,\ b \neq 0$ and $ab = 0$, then $Q(a) = Q(b) = 0$.

For these properties see [5].

3 Cayley-Dickson algebra

In (2.4[5]), it has been proved that for a Cayley-Dickson algebra A, there is a base $x_i, y_i,\ i = 0, 1, 2, 3$ of A such that among other relations the following holds:

$$Q\left(\sum_{i=0}^{3} \lambda_i x_i + \sum_{i=0}^{3} M_i y_i\right) = \sum_{i=0}^{3} \lambda_i M_i$$

$$\begin{cases} e = x_0 + y_0,\ (x_0)^2 = x_0,\ (y_0)^2 = y_0 \\ x_0 x_i = x_i,\ y_0 x_i = y_i \\ x_1 x_2 = y_3,\ x_2 x_3 = y_1,\ x_3 x_1 = y_2 \\ y_1 y_2 = x_3,\ y_2 y_3 = x_1,\ y_3 y_1 = x_2 \qquad (*) \\ x_i y_j = -g_{ij} x_0,\ y_i x_j = -g_{ij} y_0 \\ (y_i)^2 = (x_i)^2 = 0 \\ x_i x_0 = y_i y_0 = 0,\ x_i y_0 = x_i,\ y_i x_0 = y_i,\ y_0 x_i = y_i,\ y_0 x_i = x_0 y_i = 0 \\ x_0 y_0 = y_0 x_0 = 0 \ \ for \ \ i = 1, 2, 3. \end{cases}$$

Remark 3.1: Let A be a Cayley-Dickson algebra and $G = Aut(A)$. Let r be a prime, $r \neq p,\ g \in G$ with $o(g) = r$ where $o(g)$ is the order of g. Then by Maschke's Theorem, $A = C_A(g) \oplus [A, g]$, where $C_A(g) = \{a \in A \mid a^g = a\}$, $[A, g] = \{a - a^g \mid a \in A\}$.

This means that $C_A(g)$ and $[A, g]$ are orthogonal, $\dim C_A(g)$ is even, as $r \neq p$ and g preserves Q. It is obvious that $B = C_A(g)$ is closed under multiplication as g is an automorphism. So B is then a non-degenerate proper subalgebra of A.

Proposition 3.2: For a fixed $a \in A$, define the mapping $\alpha_a : A \to A$ by $\alpha_a : x \to ax$, $\forall x \in A$. If $Q(a) \neq 0$, then α is injective.

Proof: By (1.4[5]), we have $\overline{a}(ax) = Q(a)x$. If $ax = 0$, it follows that $\overline{a}(ax) = 0 = Q(a)x$. This implies $x = 0$ as $Q(a) \neq 0$. Hence the claim.

Proposition 3.3: Let $a \in A$, $a \neq 0$ and $Q(a) = 0$, Then $\dim aA = \frac{1}{2} \dim A$.

Proof: Let $\alpha_a : A \to A$ be the map as defined above. Then consider the space $im(\alpha) = \{ax \mid x \in A\}$. In particular $im(\alpha)$ is totaly singular as $Q(ax) = Q(a)Q(x) = 0$. Hence $im(\alpha) \subseteq im(\alpha)^{\perp}$, which implies $\dim im(\alpha) \leq \frac{1}{2} \dim A$. Also $\ker(\alpha) = \{x \mid ax = 0\} \subseteq \ker(\alpha)^{\perp}$ as if $0 \neq x \in \ker(\alpha)$,

then $ax = 0$ and hence by Property (2.10), $Q(x) = 0$. From this it follows that $\dim \ker(\alpha) \leq \frac{1}{2} \dim A$. As $\dim A = \dim im(\alpha) + \dim \ker(\alpha)$, then $\dim aA = \frac{1}{2} \dim A$.

Corollary 3.4: If Q has isotropic points (i. e., there exists $0 \neq a \in A$, such that $Q(a) = 0$). Then $\dim A$ must be even and Q is of Witt-index$= \frac{1}{2} \dim A$ as for $aA,\ a \neq 0,\ Q(a) = 0$, is a maximal totally singular subspace.

4 Classification of composition algebras of dimension 2,4

(a) $\dim B = 2$.

Case 1: Let $B = \langle e, a \rangle$, where $0 \neq a \in B$ with $Q(a) = 0$. As Q is non-degenerate, it follows $(e, a) \neq 0$ as otherwise $a \perp B$ and $Q(a) = 0$ implies that $a = 0$, a contradiction. So we can assume $(e, a) = 1$ and we replace a by $b = \frac{1}{(e,a)}a$, this implies $(e, b) = \frac{1}{e,a}(e, a) = 1$ with $Q(b) = 0$. So without loss of generality one can assume $(e, a) = 1$ with $Q(a) = 0$. Form property(2.6), $a^2 = (a, e)a - Q(a)e = a$, If $b = e - a$ then $Q(b) = Q(e) - (e, a) + a(-a) = 1 - 1 = 0$ and $b^2 = (e - a)(e - a) = e - a - a + a^2 = e - a = b$. So we see that $a^2 = a,\ b^2 = b,\ e = a + b,\ Q(a) = Q(b) = 0$. This implies $B = \mathbb{F}_q \oplus \mathbb{F}_q$.

Case 2: [1] Consider the Cayley-Dickson algebra A over $\mathbb{F}_{q^2}$. A contains a basis $x_i, y_i,\ i = 0, 1, 2, 3$ satisfying the relations $(*)$. Consider the $\mathbb{F}_q$ subspace $A_0 \leq A$ generated by all elements $ax_i + a^q y_i$ for $i = 0, 1, 2, 3$ and $a \in \mathbb{F}_{q^2}$. Then clearly $\dim_{\mathbb{F}_q} B = 8$. From the relations $(*)$ it follows that

$$(ax_0 + a^q y_0)(bx_1 + b^q y_i) = (ab)x_i + (ab)^q y_i$$
$$(ax_i + a^q y_0)(bx_i + b^q y_i) = -(ab^q + x_0 + a^q b y_0) \text{ for } i > 0$$
$$(ax_0 + a^q y_i)(bx_{i+1} + b^q y_{i+1}) = a^q b^q x_{i+2} + (ab)y_{i+2} \text{ for } i > 0$$

Hence A_0 is an 8-dimensional composition algebra over $\mathbb{F}_q$ and is therefore isomorphic to the Cayley-Dickson algebra over $\mathbb{F}_q$. A_0 contains the anisotropic subspace $B = \{ax_0 + a^q y_0 \mid a \in \mathbb{F}_q\} \cong \mathbb{F}_{q^2}$, as $Q(ax_0 + a^q y_0) = aa^q$.

(b) $\dim B = 4$.

There are exactly 3 isomorphic types of non-degenerate subalgebras B where $\dim B = 4$. These subalgebras B are isomorphic to the ring 2×2 matrices over $\mathbb{F}_q$[5].

Theorem 4.1: Let A be the Cayley-Dickson algebra with base x_i, y_i , $i = 0, 1, 2, 3$, and let G be $Aut(A)$. Then the centralizer $C_G\langle x_0, y_0\rangle$ of $\langle x_0, y_0\rangle$ is isomorphic $SL_3(q)$ and the normalizer $N_G(\langle x_0, y_0\rangle)$ is isomorphic to $SL_3(q)\cdot 2$.

Proof: Let $B = \langle x_0, y_0\rangle$ be a non-degenerate hyperbolic subalgebra of A, and let $h \in C(B)$ and $\langle x_1, x_2, x_3\rangle^h = \langle x_1, x_2, x_3\rangle$ and $\langle y_1, y_2, y_3\rangle^h = \langle y_1, y_2, y_3\rangle$. As $x_ix_{i+1} = y_{i+2}$ and $y_iy_{i+1} = y_{i+2}$ from relations $(*)$, then it follows that h acts faithfully on $\langle x_1, x_2, x_3\rangle = \langle y_1, y_2, y_3\rangle$. So, let $x_i^h = \sum_{j=1}^{3} g_{ij}x_j$, and as $x_1x_2 = y_3$, $x_2x_3 = y_1$, $x_3x_1 = y_2$, one obtains $y_3^h = (x_1x_2)^h = x_1^h x_2^h = (\sum_{j=1}^{3} g_{1j}x_j)(\sum_{j=1}^{3} g_{2j}x_j) = \sum_{i,j=1}^{3} g_{1i}g_{2j}x_ix_j = \sum_{i\neq j} g_{1i}g_{2j}x_ix_j$ as $x_i^2 = 0$, $i = 1, 2, 3$ and $x_{ix_j} = -x_{j_i}$, $i \neq j$, by relations (*).

$$\begin{aligned} &= \sum_{i<j}(g_{1i}g_{2i} - g_{1j}g_{2i})x_ix_j \\ &= (g_{11}g_{22} - g_{12}g_{21})x_1x_2 + (g_{12}g_{23} - g_{13}g_{22})x_2x_3 + (g_{13}g_{21} - g_{11}g_{23})x_3x_1 \\ &= (g_{11}g_{23} - g_{13}g_{22})y_1 + (g_{13}g_{21} - g_{11}g_{23})y_2 + (g_{11}g_{22} - g_{12}g_{21})y_3 \end{aligned}$$

$$\begin{aligned} y_1^h &= (x_2x_3)^h = \sum_{i<j}(g_{2i}g_{3i} - g_{2j}g_{3i})x_{ij} \\ &= (g_{21}g_{32} - g_{22}g_{31})x_1x_2 + (g_{22}g_{33} - g_{23}g_{32})x_2x_3 + (g_{23}g_{31} - g_{21}g_{33})x_3x_1 \\ &= (g_{21}g_{32} - g_{22}g_{31})y_3 + (g_{22}g_{33} - g_{23}g_{32})y_1 + (g_{23}g_{31} - g_{21}g_{33})y_2 \end{aligned}$$

and

$$\begin{aligned} y_2^h &= (x_3x_1)^h = \sum_{i<j}(g_{3i}g_{3j} - g_{3j}g_{1i})x_ix_j \\ &= (g_{31}g_{12} - g_{32}g_{11})x_1x_2 + (g_{32}g_{13} - g_{33}g_{12})x_2x_3 + (g_{33}g_{11} - g_{31}g_{13})x_3x_1 \\ &= (g_{31}g_{12} - g_{32}g_{11})y_3 + (g_{32}g_{13} - g_{33}g_{12})y_1 + (g_{32}g_{13} - g_{33}g_{12})y_2 \end{aligned}$$

In a matrix form, h can be represented by:

	x_0	y_0	x_1	x_2	x_3	y_1	y_2	y_3
x_0	1							
y_0		1						
x_1								
x_2				g				
x_3								
y_1								
y_2							g^*	
y_3								

where g is the matrix of h with respect to $\langle x_1, x_2, x_3\rangle$, and g^* is the matrix of h with respect to $\langle y_1, y_2, y_3\rangle$.

$$\begin{aligned} -x_0 &= (x_3y_3)^h = x_3^h y_3^h \\ \text{So one obtains} \quad &= (g_{31}x_1 + g_{32}x_2 + g_{33}x_3[(g_{12}g_{23} - g_{13}g_{22})y_1 + (g_{13}g_{21} - g_{12}g_{31})y_2 + (g_{11}g_{22} - g_{12}g \\ &= -deg(g)x_0 \end{aligned}$$

This implies $det(g) = 1$. By simple computations one can see $g.g^* = det(g)I$. Hence $g^* = (g^t)^{-1}$. This implies that $C_G(B) = SL_3(q)$. The map σ on A defined by

$$\sigma(x_0) = y_0,\ \sigma(y_0) = x_0,\ \sigma(x_i) = y_i,\ \sigma(y_i) = x_i,\ i = 1, 2, 3,$$

is an automorphism of order 2 and can be represented by the matrix

	x_0	y_0	x_1	x_2	x_3	y_1	y_2	y_3
x_0		1						
y_0	1							
x_1								
x_2				0		I		
x_3								
y_1								
y_2				I		0		
y_3								

and $N_G(B) = \langle C_G(B), \sigma\rangle SL_3(q) \cdot 2$. Hence the claim.

Note that the above result was mentioned in [1] and a sketch of the proof was given. Here we give a detailed proof.

Theorem 4.2: (a) Let t be an element of G of prime order $r \neq p$. Then $A = C_A(t) \oplus [A, t]$ and $C_A(t)$ is a nontrivial nondegenerate subalgebra of A.

(b) There exist exactly 3 isomorphism classes of nontrivial nondegenerate

subalgebras of A, and G acts transitively on the sets of pairwise isomorphic nontrivial nondegenerate subalgebras. If B is a nontrivial nondegenerate subalgebra of A, then one of the following holds.

(1) $\dim B = 4$, B is isomorphic to the ring of 2×2 matrices over $\mathbb{F}_q$, $C_G(B) \cong SL(2,q)$, and $N_G(B) \cong SO^+(4,q)$.
(2) $\dim B = 2$ and B is hyperbolic. Then $B \cong \mathbb{F}_q \times \mathbb{F}_q$, $C_G(B) \cong SL(3,q)$, and $N(B) \cong SL(3,q).2$.
(3) $\dim B = 2$ and B is anisotropic. Then $B \cong \mathbb{F}_{q^2}$, $C_G(B) \cong SU(3,q^2)$,and $N(B) \cong SU(3,q^2).2$.

Proof. See [1]

References

[1] Mashhour I. M. Al Ali, A. Neumann, Ch. Hering, On the B-injectors of groups with components of small rank, *Communications in Algebra*, **27,** no. 6, (2005), 2853–2886.

[2] H. S. M. Coxeter, Integral Cayley numbers, Duke Math. J., **13,** (1946), 561–578.

[3] N. Jacobson, Composition algebras and their automorphisms, *Rend. Circ. Mat. Palermo II*, tomo VIII, (1958), 55–80.

[4] K. Mahler, On ideals in the Cayley-Dickson algebra, Proc. Royal Irish Acad., **48,** A5, (1942).

[5] F. Van Der Blij, T. A. Springer, The arithmetics of octaves and of the group G_2, *Indagationes Mathematica*, **21**, (1959), 406–418.