CLASSES OF NONASSOCIATIVE ALGEBRAS CARRYING MAPS OF DEGREE n WITH INTERESTING PROPERTIES

S. PUMPLÜN AND A. STEELE

ABSTRACT. We discuss classes of algebras which carry a map of degree n into one of their subalgebras. Some of these maps permit some weak type of (Jordan) composition and can be viewed as generalizations of a norm form. For instance, several classes of algebras recently obtained carry what we call a semi-multiplicative map. Their elements satisfy a polynomial identity over one of their subalgebras, thus behaving similar to algebras with norm forms.

INTRODUCTION

Certain division algebras recently studied in the context of space-time block codes, cf. [Pu-U], [S-Pu-O], possess a map of degree n into some subalgebra which displays some interesting properties, more precisely, it behaves similar to the norm of a central simple associative or an octonion algebra.

While trying to find constructions of nonassociative algebras which could be useful for space-time block coding, we then came across some more examples. In this note, we take a closer look at this phenomenon.

We first consider certain finite-dimensional algebras A over a field F containing a subalgebra D with multiplicative norm N_D of degree n, which permit a map $M_A : A \mapsto D$ of degree n such that $M_A(ax) = M_A(xa) = N_D(a)M_A(x)$ for all $a \in D$, $x \in A$. We call such a map M_A *semi-multiplicative*. Semi-multiplicative maps of degree n exist on nonassociative cyclic algebras of dimension n^2 which were first studied by Sandler [S] over finite fields, and more recently, over arbitrary base fields, by Steele in his PhD thesis [St1, 2]. Semi-multiplicative quadratic maps appear when generalizing classical constructions of Hurwitz algebras.

On algebras which can be considered as generalizations of the first Tits construction, we find cubic maps which allow some sort of Jordan composition.

The contents of the paper are as follows: After introducing our terminology in Section 1, Section 2 deals with some general properties of semi-multiplicative maps. In Section 3, algebras with semi-multiplicative maps $M_A : A \to D$ into some subalgebra D are constructed employing both a generalized Cayley-Dickson doubling process and the generalization of a construction for octonion algebras out of quadratic étale algebras and hermitian forms [T]. These algebras also carry a bijective map $^- : A \mapsto A$ satisfying $M_A(x)1_A = x\bar{x}$ for all $x \in A$. Moreover, for some of these algebras, the identity $x^2 - T_A(x) + M_A(x)1_A = 0$ is satisfied for

Date: 25.4.2013.

1991 *Mathematics Subject Classification.* Primary: 17A35.

Key words and phrases. Division algebras, multiplicative maps, composition algebras.

all $x \in A$, where $T_A(x) = M_A(1_A, x)$. We also consider the weaker notion of a left or right semi-multiplicative map.

Semi-multiplicative maps of degree n on nonassociative cyclic algebras are considered in Section 4. These semi-multiplicative maps of degree 3 induce quadratic and linear maps which are shown to display certain identities similar to those which the corresponding ones for cubic algebras satisfy. Section 5 looks at a possible generalization of the first Tits construction which leads to a unital algebra with a cubic map satisfying some sort of a generalized Jordan composition. In Section 6, some other classes of algebras are discussed which carry left or right semi-multiplicative maps.

1. Preliminaries

1.1. **Nonassociative algebras.** Let F be a field. By an "F-algebra" we mean a finite dimensional nonassociative algebra over F. A nonassociative algebra $A \neq 0$ 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 is measured by the *associator* $[x, y, z] = (xy)z - x(yz)$. $\mathrm{Nuc}_l(A) = \{x \in A \,|\, [x, A, A] = 0\}$ is the *left nucleus*, $\mathrm{Nuc}_m(A) = \{x \in A \,|\, [A, x, A] = 0\}$ is *middle nucleus* and $\mathrm{Nuc}_r(A) = \{x \in A \,|\, [A, A, x] = 0\}$ the *right nucleus* of A. Their intersection $\mathrm{Nuc}(A) = \{x \in A \,|\, [x, A, A] = [A, x, A] = [A, A, x] = 0\}$ is called the *nucleus* of A. An anti-automorphism $\sigma : A \mapsto A$ of period 2 is called an *involution* on A.

1.2. A *map of degree* d over F is a map $M : V \mapsto W$ between two finite-dimensional vector spaces V and W over F such that $M(av) = a^d M(v)$ for all $a \in F$, $v \in V$ and such that the map $M : V \times \cdots \times V \mapsto W$ defined by

$$M(v_1, \dots, v_d) = \sum_{1 \leq i_1 < \cdots < i_l \leq d} (-1)^{d-l} M(v_{i_1} + \cdots + v_{i_l})$$

$(1 \leq l \leq d)$ is a d-linear map over F, i.e., $M : V \times \cdots \times V \mapsto W$ (d-copies) is an F-multilinear map where $M(v_1, \dots, v_d)$ is invariant under all permutations of its variables.

A map $\varphi : V \mapsto F$ of degree n is called a *form of degree n over F*. A form of degree d is called *nondegenerate* if $v = 0$ is the only vector such that $\varphi(v, v_2, \dots, v_d) = 0$ for all $v_i \in V$.

A nondegenerate form $\varphi(x_1, \dots, x_n)$ of degree d in n variables *is multiplicative* if $\varphi(x)\varphi(y) = \varphi(z)$ where x, y are systems of n indeterminates and where each z_l is a bilinear form in x, y with coefficients in F. In this case the vector space $V = F^n$ admits a bilinear map $V \times V \to V$ which can be viewed as the multiplicative structure of a nonassociative F-algebra $A = V$ and so $\varphi(vw) = \varphi(v)\varphi(w)$ for all $v, w \in V$.

1.3. Composition algebras. An algebra A is called a *composition algebra* over F if it admits a multiplicative quadratic form $N \colon A \mapsto F$. The form N is unique [KMRT, p. 454 ff.]. It is called the *norm* of A and we also write $N = N_A$. A unital composition algebra is called a *Hurwitz algebra*. Hurwitz algebras are quadratic alternative and $N(1_A) = 1$. Hurwitz algebras exist only in dimensions 1, 2, 4 or 8. Those of dimension 2 are exactly the quadratic étale F-algebras, those of dimension 4 exactly the well-known quaternion algebras.

The ones of dimension 8 are called *octonion algebras*. The conjugation $\overline{x} = T_A(x)1_A - x$ of a Hurwitz algebra A is a scalar involution, called the *standard involution* of A, where $T_A\colon A \mapsto F$, $T_A(x) = N_A(1_A, x)$, is the *trace* of A.

2. Semi-multiplicative maps

2.1. Let A be an algebra over F containing a subalgebra D. Suppose we can define a map

$$M_A : A \mapsto D$$

on A of degree n. Then M is called *left semi-multiplicative* if

$$M_A(ax) = M_A(a)M_A(x) \text{ for all } a \in D, x \in A$$

and *right semi-multiplicative* if

$$M_A(xa) = M_A(a)M_A(x) \text{ for all } a \in D, x \in A.$$

M is called *semi-multiplicative* if it is left and right semi-multiplicative.

By linearization we show:

Lemma 1. *(i) If M is left semi-multiplicative then the multilinear map $M : A\times\cdots\times A \mapsto D$ satsifies*

$$M_A(au_1, \ldots, au_n) = M_A(a)M_A(u_1, \ldots, u_n)$$

for all $a \in D$, $u_1, \ldots, u_n \in A$.
(ii) If M is right semi-multiplicative then the multilinear map $M : A\times\cdots\times A \mapsto D$ satsifies

$$M_A(u_1a, \ldots, u_na) = M_A(a)M_A(u_1, \ldots, u_n)$$

for all $a \in D$, $u_1, \ldots, u_n \in A$.

Assuming additionally that $M_A(a) \in F$ for all $a \in D$, it is elementary to see that in both cases $M_A|_D$ is multiplicative: $M_A(ab) = M_A(ab) = M_A(a)M_A(b)$ for all $a, b \in D$.

2.2. Quadratic case. In this section, let A be an algebra over F and D a proper subalgebra of A. Let $M_A : A \mapsto D$ be a quadratic map and $M_A : A \times A \mapsto D$, $M_A(x, y) = M_A(x + y) - M_A(x) - M_A(y)$ its associated symmetric bilinear map. If A is unital, define two F-linear maps $T_A : A \mapsto D$ and $^- : A \mapsto A$ by

$$T_A(x) = M_A(1_A, x), \quad \overline{x} = T_A(x)1_A - x.$$

Lemma 2. *(i) If M_A is left semi-multiplicative then*

$$M_A(au, bv) + M_A(bu, av) = M_A(a, b)M_A(u, v)$$

for all $a, b \in D, u, v \in A$. In particular, if A is unital, then

$$M_A(a, bv) + M_A(b, av) = M_A(a, b)T_A(v),$$

$$M_A(au, v) + M_A(u, av) = T_D(a)M_A(u, v)$$

for all $a, b \in D, u, v \in A$.
(ii) If M_A is right semi-multiplicative then

$$M_A(ua, vb) + M_A(ub, va) = M_A(a, b)M_A(u, v)$$

for all $a, b \in D, u, v \in A$. In particular, if A is unital, then

$$M_A(a, vb) + M_A(b, va) = M_A(a, b)T_A(v),$$

$$M_A(ua, v) + M_A(u, va) = T_A(a)M_A(u, v)$$

for all $a, b \in D, u, v \in A$.

We conclude that if M_A is semi-multiplicative, then

$$M_A(au, av) = M_A(ua, va)$$

and

$$M_A(au, bv) + M_A(bu, av) = M_A(ua, vb) + M_A(ub, va) \text{ for all } a, b \in D, u, v \in A.$$

Lemma 3. *Suppose $x \in A$ satisfies $\overline{x}x = M_A(x)$ then*

$$x^2 - T_A(x)x - x = 0,$$

similarly if $x \in A$ satisfies $x\overline{x} = M_A(x)$ then

$$x^2 - xT_A(x) - x = 0.$$

The proof is trivial.

Define the F-subvector space

$$A^\perp = \{x \in A \,|\, M_A(x, A) = 0\}$$

and let

$$R(M) = \{x \in A^\perp \,|\, M_A(x) = 0\}.$$

Lemma 4. *(a) If M_A is non-trivial then for every field extension L of F, $A^\perp \otimes L = (A \otimes L)^\perp$.*
(b) Let $a \in A$ such that $N_D(a) \in F^\times$.
(i) Suppose that $D \subset \mathrm{Nuc}_l(A)$ or $D \subset \mathrm{Nuc}_m(A)$. If M is left semi-multiplicative then $A^\perp$ is a left ideal in A.
(ii) Suppose that $D \subset \mathrm{Nuc}_r(A)$ or $D \subset \mathrm{Nuc}_m(A)$. If M is right semi-multiplicative then $A^\perp$ is a right ideal in A.
(c) If F has characteristic 0 or odd characteristic, $A^\perp = R(A)$.

Proof. (a) is trivial.
(b) (i) Define the F-vector space homomorphisms $\Gamma : A \mapsto A \mapsto A/A^\perp, \quad x \mapsto ax \mapsto ax + A^\perp$ and $\Psi : A \mapsto A \mapsto A/A^\perp, \quad x \mapsto xa \mapsto ax + A^\perp$. We have $w \in \ker(\Gamma)$ iff $aw \in A^\perp$, hence $M_A(aw, y) = 0$ for all $y \in A$, which implies $M_A(aw, ay') = N(a)M_A(w, y') = 0$ for all $y' \in A$ ($y' = \frac{1}{a}ay$), that is $M_A(w, y') = 0$ for all $y' \in A$ and thus $w \in A^\perp$. Conversely, let $y \in A^\perp$, then $M_A(y, z) = 0$ and hence $N_D(a)M_A(y, z) = 0$ for all $z \in A$. This implies that $M_A(ay, az) = M_A(ay, z') = 0$ for all $z' \in A$ ($z' = \frac{1}{a}az$) and therefore $ay \in A^\perp$, i.e. $\Gamma(y) = ay + A^\perp \in \ker(\Gamma)$.
(ii) is proved analogously.
(c) If F has odd characteristic, we have $\frac{1}{2}M_A(x, x) = M_A(x)$ and hence $M_A(x) = 0$ for all $x \in A^\perp$, so $A^\perp \subset R(A) = \{x \in A^\perp \,|,\ M_A(x) = 0\} = \{x \in A^\perp \,|,\ M_A(x, x) = 0\}$ and $A^\perp = R(A)$. □

We say the quadratic map M_A on A is *nondegenerate* if $M_A(x,y)=0$ for all $y\in A$ implies $x=0$. For a subspace D of A, we denote by $D^\perp$ the subspace

$$D^\perp=\{x\in A\mid M_A(x,a)=0 \text{ for all } a\in D\}.$$

Theorem 5. *Let F have characteristic not 2 and let A be a unital algebra over F with a proper unital subalgebra D of A such that $M_A:A\to D$ is a nondegenerate, semi-multiplicative quadratic map which restricts to a nondegenerate quadratic map on D. Suppose further that $M_A(x,a)\in F$ for all $x\in A$, $a\in D$. Then A has the F-vector space decomposition*

$$A=D\oplus D^\perp.$$

Moreover, A contains the direct sum subspace

$$K:=D\oplus Dz,$$

where $z\in A^\perp$ and for $a+bz\in K$ we have

$$M_A(a+bz)=M_A(a)-dM_A(b),$$

for some $d\in D\setminus\{0\}$ and

$$\overline{a+bz}=\overline{a}-bz.$$

Proof. The assumptions $M_A(x,a)\in F$ for all $a\in D$ and char $F\neq 2$ imply that

$$M_A(a)=\frac{1}{2}M_A(a,a)\in F,$$

for all $a\in D$, so $M_A|_D$ is a multiplicative, nondegenerate quadratic form on D. Denote the dual space of D by D^*, then nondegeneracy of $M_A|_D$ and finite-dimensionality of D gives an F-vector space isomorphism

$$a\mapsto M_A(a,\_)|_D:D\to D^*,$$

for all $a\in D$. For all $x\in A$, the restriction of the map $M_A(x,\_)$ to the subalgebra D is also a linear functional by our assumption that $M_A(x,a)\in F$ for all $a\in D$, hence there exists a $d_x\in D$ with

$$M_A(x,\_)|_D=M_A(d_x,\_)|_A.$$

Setting $x'=x-d_x$ gives $M_A(x',a)=0$ for all $a\in D$ and hence the decomposition $x=d_x+x'\in D\oplus D^\perp$ for all $x\in A$. $D^\perp\neq 0$ since D is proper and by nondegeneracy

$$0\neq M_A(D^\perp,A)=M_A(D^\perp,D\oplus D^\perp)=M_A(D^\perp,D^\perp).$$

Therefore, there exist $z,z'\in D^\perp$ with $M_A(z,z')\neq 0$. Suppose $M_A(z,z)=M_A(z',z')=0$, then

$$M_A(z+z',z+z')=M_A(z,z)+M_A(z',z')+2M_Z(z,z')\neq 0,$$

since char $F\neq 2$. This implies there exists an anisotropic vector $z\in D^\perp$ say, $M_A(z)=:-d\in D\setminus\{0\}$. We claim that $Dz\subseteq D^\perp$ so the subspace $K=D+Dz$ is direct. This follows from the fact that $T_A(a)=M_A(a,1)\in F$ and so by Lemma 2:

$$M_A(az,b)=M_A(z,T_A(a)b)-M_A(z,ab)=M_A(z,\overline{a}b)=0,$$

for all $a, b \in D$, since z is orthogonal to D. For a typical element $a + bz \in K$ we have

$$M_A(a + bz) = M_A(a) + M_A(a, bz) + M_A(bz) = M_A(a) - dM_A(b),$$

since bz is orthogonal to D and M_A is semi-multiplicative. Furthermore, $T_A(bz) = M_A(bz, 1) = 0$ since $1 \in D$. Therefore,

$$\overline{a + bz} = T_A(a + bz) - a + bz = T_A(a) - a + T_A(bz) - bz = \overline{a} - bz.$$

□

2.3. Cubic case. In this section, let A be an F-algebra, D a proper subalgebra of A and

$$M_A : A \to D$$

a cubic map. The trilinear map $M_A : A \times A \times A \to D$ given by

$$M_A(x, y, z) = M_A(x + y + z) - M_A(x + y) - M_A(x + z) - M_A(y + z) + M_A(x) + M_A(y) + M_A(z),$$

for all $x, y, z \in A$, is symmetric in all three variables. If $1/6 \in F^{\times}$ then $M_A(x) = 1/6M_A(x, x, x)$. If M_A is left semi-multiplicative then

$$M_A(a, a, a)M_A(x, x, x) = M_A(ax, ax, ax),$$

for all $a \in D$ and $x \in A$ and if M_A is left semi-multiplicative then

$$M_A(a, a, a)M_A(x, x, x) = M_A(xa, xa, xa),$$

for all $a \in D$ and $x \in A$. By linearisation we obtain

Lemma 6. *Let $M_A : A \to D$ be a cubic map*
(i) If M_A is left semi-multiplicative then

$$\begin{aligned} M_A(a, b, c)M_A(x, y, z) = {} & M_A(ax, by, cz) + M_A(ax, cy, bz) \\ & + M_A(bx, ay, cz) + M_A(bx, cy, az) \\ & + M_A(cx, ay, bz) + M_A(cx, by, az), \end{aligned}$$

for all $a, b, c \in D$, $x, y, z \in A$.
(ii) If M_A is right semi-multiplicative then

$$\begin{aligned} M_A(a, b, c)M_A(x, y, z) = {} & M_A(xa, yb, zc) + M_A(xa, yc, zb) \\ & + M_A(xb, ya, zc) + M_A(xb, yc, za) \\ & + M_A(xc, ya, zb) + M_A(xc, yb, za), \end{aligned}$$

for all $a, b, c \in D$, $x, y, z \in A$.

Suppose from now on that A is unital and that F is not of characteristic 2 or 3. Define the linear map $T_A : A \to D$ and the quadratic map $S_A : A \to D$ by

$$T_A(x) := \frac{1}{2}M_A(x, 1, 1), \qquad S_A(x) := \frac{1}{2}M_A(x, x, 1),$$

for all $x \in A$. Then

$$T_A(1) = S_A(1) = 3. \tag{1}$$

If M_A is left semi-multiplicative then putting $b = c = 1$ in Lemma 6 yields

$$M_A(ax, y, z) + M_A(x, ay, z) + M_A(x, y, az) = T_A(a)M_A(x, y, z), \tag{2}$$

for all $a \in D$ and $x, y, z \in A$. Similarly, if M_A is right semi-multiplicative then

$$M_A(xa, y, z) + M_A(x, ya, z) + M_A(x, y, za) = T_A(a)M_A(x, y, z), \tag{3}$$

for all $a \in D$ and $x, y, z \in A$ and if M_A is semi-multiplicative then

$$M_A([a, x], y, z) + M_A(x, [a, y], z) + M_A(x, y, [a, z]) = 0, \tag{4}$$

for all $a \in D$ and $x, y, z \in A$, where $[a, x] = ax - xa$ denotes the commutator of a and x.

Define a bilinear map $T_A : A \times A \to D$ by

$$T_A(x, y) := T_A(x)T_A(y) = M_A(x, y, 1),$$

for all $x, y \in A$. If M_A is left semi-multiplicative then putting $y = z = 1$ into equation (2) gives us

$$M_A(ax, 1, 1) + M_A(a, x, 1) + M_A(x, 1, a) = T_A(a)M_A(x, 1, 1),$$

for all $a \in D$ and $x \in A$. We rearrange to get

$$T_A(ax) = T_A(a)T_A(x) - M_A(x, a, 1) = T_A(a, x).$$

Similarly, if M_A is right semi-multiplicative then

$$T_A(xa) = T_A(a, x),$$

for all $a \in D$ and $x \in A$. It follows that

$$T_A(1, x) = T_A(x, 1) = T_A(x), \tag{5}$$

for all $x \in A$. We may also bilinearize the quadratic map S_A to get

$$S_A : A \times A \to D : \quad S_A(x, y) = S_A(x + y) - S_A(x) - S_A(y) = M_A(x, y, 1),$$

for all $x, y \in A$. Comparing with the definition of $T_A(x, y)$ we obtain

$$S_A(x, y) = M_A(x, y, 1) = M_A(1, x, y) = T_A(x)T_A(y) - T_A(x, y), \tag{6}$$

for all $x, y \in A$.

We define a quadratic map $\sharp : A \to A$ by $x^\sharp = x^2 - T_A(x)x + S_A(x)1$. Its linearization is

$$x \sharp y = (x + y)^\sharp - x^\sharp - y^\sharp.$$

Hence if F is not of characteristic 2,

$$x^\sharp = 1/2(x \sharp x).$$

Proposition 7. *For all $y \in A$, $1 \sharp y = T_A(y)1 - y$.*

Proof. Calculating directly from the linearized sharp map we obtain:

$$\begin{aligned}1\sharp y &= (1+y)^\sharp - 1^\sharp - y^\sharp\\ &= (1+y)^2 - T_A(1+y)(1+y) + S(1+y)\\ &\quad - 1 + T_A(1)1 - S_A(1)1 - y^2 + T_A(y)y - S_A(y).\end{aligned}$$

Expanding this and using (1) we get

$$1\sharp y = -y - T_A(y) + S_A(1+y) - S_A(1) - S_A(y) = S_A(1,y) - y - T_A(y),$$

but equations (6) and (5) imply that

$$S_A(1,y) = T_A(1)T_A(y) - T(1,y) = 3T_A(y) - T_A(y).$$

We conclude that

$$1\sharp y = T_A(y) - y.$$

□

Proposition 8. *Suppose every element $x \in A$ satisfies $x^\sharp x = M_A(x)1$. Then:*
(i) Every element $x \in A$ satisfies the equation

$$x^2 x - T_A(x)x^2 + S_A(x)x - M_A(x)1 = 0.$$

(ii) If M_A is isotropic then A has zero divisors.

The proof is trivial.

2.4. Non-unital division algebras with left and right semi-multiplicative maps. We close this section with the easy observation that isotopes of algebras with semi-multiplicative maps yield examples of algebras with left or right semi-multiplicative maps: Let A be an algebra together with a semi-multiplicative map $M_A : A \mapsto D$ of degree n, where D is a subalgebra of A with a multiplicative form N of degree n. Let V be the underlying vector space of A and $F, G, H \in \mathrm{Gl}(V)$. Suppose that $M_A(G(x)) = M_A(x)$ and $M_A(H(x)) = M_A(x)$ for all $x \in A$ and $F|_D \in O(N_D)$. Take the isotope $A^{(F,G,H)}$ of A with multiplication defined via

$$x * y = H(F(x)G(y))$$

for all $x, y \in A$. Then for

$$M_A(a * x) = M_A(H(F(a)G(x))) = M_A(F(a)G(x)) = N(F(a))M_A(G(x)) = N(a)M_A(x)$$

for all $x \in A$, $a \in D$, and M_A on $A^{(F,G,H)}$ is left semi-multiplicative.

If we take the isotope $A^{(G,F,H)}$ of A with

$$x * y = H(G(x)F(y))$$

for all $x, y \in A$ then for

$$M_A(x * a) = M_A(G(x)F(a)) = N(F(a))M_A(G(x)) = N(a)M_A(x)$$

for all $x \in A$ $a \in D$. So M_A is right semi-multiplicative on $A^{(G,F,H)}$.

Suppose that additionally $G|_D \in O(N_D)$. Then M_A is semi-multiplicative on $A^{(G,G,H)}$.

3. Unital algebras with semi-multiplicative quadratic maps

3.1. A generalized Cayley-Dickson doubling. Let B be a unital algebra over F together with a multiplicative quadratic form $N_B : B \mapsto F$ and D be one of the following:
(i) a Hurwitz algebra over F with canonical involution $^- : D \mapsto D$, norm N_D and trace T_D.
(ii) a unital algebra over F together with a semi-multiplicative quadratic map $M_D : D \mapsto B$ where B is a subalgebra of D. We have $T_D(x) = M_D(1_D, x)$ and $^- : D \mapsto D$, $\bar{x} = T_D(x)1_D - x$ defined as before.

Let $d \in D$ be an invertible element. The F-vector space $A = D \oplus D$ can be made into an algebra over F via the multiplications

(1) $$(u,v)(u',v') = (uu' + d(\bar{v'}v), v'u + v\bar{u'})$$
(2) $$(u,v)(u',v') = (uu' + \bar{v'}(dv), v'u + v\bar{u'})$$
or
(3) $$(u,v)(u',v') = (uu' + (\bar{v'}v)d, v'u + v\bar{u'})$$

for $u, u', v, v' \in D$. The unit element of the new algebra A is given by $1_A = (1_D, 0)$ in each case. Note that D is a subalgebra of A.

A is called the *Cayley-Dickson doubling of D (with element d placed on the left hand side, in the middle*, or *on the right hand side)* and denoted by $\mathrm{Cay}(D, d)$ for multiplication (1), by $\mathrm{Cay}_m(D, d)$ for multiplication (2) and by $\mathrm{Cay}_r(D, d)$ for multiplication (3).

For D quadratic étale, the algebras obtained this way are either quaternion algebras (iff $d \in F^\times$) or the nonassociative quaternion algebras introduced in [W], see also [As-Pu] (iff $d \in D \setminus F$). For D a quaternion algebra, we obtain either octonion algebras (iff $d \in F^\times$) or the algebras treated in [Pu1] (iff $d \in D \setminus F$). If D is a separable quadratic field extension or a quaternion division algebra then A is a division algebra for any choice of $d \in D \setminus F$ [Pu1, Theorem 6].

3.2. From now on, let D be a unital algebra over F together with a semi-multiplicative quadratic map $M_D : D \mapsto B$ where B is a subalgebra of D. Let $A = \mathrm{Cay}(D, d)$, $A = \mathrm{Cay}_m(D, d)$ or $A = \mathrm{Cay}_r(D, d)$. Define $M_A : A \mapsto D$,

$$M_A((u, v)) = M_D(u) - dM_D(v)$$

for all $(u, v) \in A$ and $T_A : A \mapsto D$ and $^- : A \mapsto A$ by

$$T_A(x) = M_A(1_A, x), \quad \overline{x} = T_A(x)1_A - x.$$

Proposition 9. *(i) M_A is an F-quadratic map such that*

$$M_A((a, 0)(u, v)) = M_A((u, v)(a, 0)) = N_{B/F}(a)M_A((u, v))$$

for all $a \in B$, $(u, v) \in A$.
(ii) For all $x = (u, v), y = (u', v') \in A$, the associated bilinear map $M_A : A \times A \mapsto D$ is given by

$$M_A(x, y) = M_D(u, u') - dM_D(v, v').$$

(iii) $T_A : A \mapsto F$, $T_A(x) = T_D(u)$ *for* $x = (u, v) \in A$, *is* F*-linear and* $\overline{(u, v)} = (\bar{u}, -v)$.
(iv)

$$M_A(a, bx) + M_A(b, ax) = M_A(a, xb) + M_A(b, xa) = M_D(a, b)T_A(v) \in B$$

for all $x \in A$, $a, b \in B$.
(v) $M_A(\bar{x}) = M_A(x)$ *and* $M_A(x)1_A = \bar{x}x = x\bar{x}$ *for all* $x \in A$.
(vi) If $d \notin F$ *then* $M_A(x) = 0$ *if and only* $x = 0$.
(vii) If D *is unital and* $A = \mathrm{Cay}(D, d)$ *or* $\mathrm{Cay}_r(D, d)$, *then*

$$x^2 - T_A(x)x + M_A(x)1_A = 0$$

for all $x \in A$.

Proof. (i) The fact that M_A is quadratic is straightforward. For all $a \in B$, $(u, v) \in A$,

$$M_A((a, 0)(u, v)) = M_A((au, va)) = M_D(au) - dM_D(va).$$

Since M_D is semi-multiplicative, thus

$$M_A((a, 0)(u, v)) = N_B(a)(M_D(u) - dM_D(v)) = N_B(a)M_A((u, v))$$

and similarly,

$$M_A((u, v)(a, 0)) = M_A((ua, av)) = M_D(ua) - dM_D(av) = N_B(a)(M_D(u) - dM_D(v)) = N_B(a)M_A((u, v)).$$

(ii), (iii), (v) and (vi) are trivial calculations.
(iv) follows by linearization from (i).
(vii) follows directly from (v) and Lemma 3. □

Corollary 10. *(i) If* $d \in B$, $M_A : A \mapsto B$ *is a semi-multiplicative quadratic map, such that* $M_A|_B = N_B$ *is a multiplicative quadratic form.*
(ii) If $M_A(x)^{-1} \in \mathrm{Nuc}_l(A)$ *then* x *has the left inverse* $M_A(x)^{-1}\bar{x}$, *if* $M_A(x)^{-1} \in \mathrm{Nuc}_r(A)$ *then* x *has the right inverse* $\bar{x}M_A(x)^{-1}$,
(iii) If $M_A(x) = \alpha \in F^\times$ *then* $x \in A^\times$ *with inverse* $\alpha^{-1}\bar{x}$.

3.3. Let C be a Hurwitz algebra over F. Let $A_0 = C$ and define a *repeated generalized Cayley-Dickson doubling* of A_0 inductively by

$$A_{i+1} = \mathrm{Cay}(A_i, d_i), \quad A_{i+1} = \mathrm{Cay}_m(A_i, d_i) \text{ or } A_{i+1} = \mathrm{Cay}_r(A_i, d_i)$$

with $d_i \in A_i$ for all i, $i \geq 0$.

Define $M_0 = N_C$ and $M_{i+1} : A_{i+1} \mapsto A_i$,

$$M_{i+1}((u, v)) = M_i(u) - d_i M_i(v)$$

for all $(u, v) \in A$ and $T_{i+1} : A_{i+1} \mapsto A_{i+1}$ and $^- : A_{i+1} \mapsto A_{i+1}$ by

$$T_{i+1}(x) = M_{i+1}(1, x), \quad \overline{x} = T_{i+1}(x)1 - x.$$

A simple proof by induction yields:

Corollary 11. *Let C be a Hurwitz algebra over F and A_i a repeated generalized Cayley-Dickson doubling of C.*
(i) A_{i+1} carries an F-quadratic map $M_{i+1} : A_{i+1} \mapsto A_i$, $Mi+1((u,v)) = M_i(u) - d_i M_i(v)$ such that

$$Mi+1((a,0)(u,v)) = Mi+1((u,v)(a,0)) = N_C(a)Mi+1((u,v))$$

for all $a \in C$, $(u,v) \in Ai+1$.
(ii) For all $x = (u,v), y = (u',v') \in Ai+1$, the associated bilinear map $M_{i+1} : A_{i+1} \times A_{i+1} \mapsto A_i$ is given by

$$M_{i+1}(x,y) = M_i(u,u') - d_i M_i(v,v')$$

(iii)

$$M_{i+1}(a,bx) + M_{i+1}(b,ax) = M_{i+1}(a,xb) + M_{i+1}(b,xa) = N_C(a,b)T_{i+1}(v) \in B$$

for all $x \in A_{i+1}$, $a,b \in C$.
(iv) $T_{i+1} : A_{i+1} \mapsto F$, $T_{i+1}(x) = T_C(u)$ for $x = (u,v) \in A_{i+1}$, is F-linear and $\overline{(u,v)} = (\bar{u}, -v)$ is a bijective map of order two.
(v) $M_{i+1}(\bar{x}) = M_{i+1}(x)$, $M_{i+1}(x)1_{A_{i+1}} = \bar{x}x = x\bar{x}$ and $x\bar{y} + y\bar{x} = M_{i+1}(x,y)1_{A_{i+1}}$ for all $x \in A_{i+1}$.
(vi) If $d_i \notin F$ and $M_i(u) = 0$ if and only if $u = 0$, then $M_{i+1}(x) = 0$ if and only $x = 0$
(vii) If for all $j \leq i$, $A_{j+1} = \mathrm{Cay}(A_j, d_j)$ or $A_{j+1} = \mathrm{Cay}_r(A_j, d_j)$, then

$$x^2 - T_{i+1}(x)x + M_{i+1}(x)1_{A_{i+1}} = 0$$

for all $x \in A_{i+1}$, $a,b \in C$.

Several known unital algebras carry a semi-multiplicative quadratic map:

Example 12. (i) Let $A = \mathrm{Cay}(K,d)$, $d \in K \setminus F$, be a nonassociative quaternion algebra. Then $M_A : A \mapsto K$, $M_A((u,v)) = N_{K/F}(u) - dN_{K/F}(v)$ is a semi-multiplicative quadratic map. Here, $T_A : A \mapsto F$, $T_A(x) = T_{K/F}(u)$ for $x = (u,v) \in A$, and

$$x^2 - T_A(x)x + M_A(x)1_A = 0$$

for all $x \in A$.
(ii) Let D be a quaternion algebra over F and A be either $\mathrm{Cay}(D,d)$, $\mathrm{Cay}_m(D,d)$ or $\mathrm{Cay}_r(D,d)$, $d \in D \setminus F$. Then $M : A \mapsto D$, $M_A((u,v)) = N_D(u) - dN_D(v)$ is a semi-multiplicative quadratic map. Here, $T_A : A \mapsto F$, $T_A(x) = T_D(u)$ for $x = (u,v) \in A$. For $\mathrm{Cay}(D,d)$ or $\mathrm{Cay}_r(D,d)$,

$$x^2 - T_A(x)x + M_A(x)1_A = 0$$

for all $x \in A$.
(iii) Let us double the nonassociative quaternion algebra $D = \mathrm{Cay}(K,c)$ over F which possesses the semi-multiplicative quadratic map $M_D((u,v)) = N_K(u) - cN_K(v)$ and $^- : D \mapsto D$, $(u,v) \mapsto (\bar{u}, -v)$. I.e., let A be either $\mathrm{Cay}(D,d)$, $\mathrm{Cay}_m(D,d)$ or $\mathrm{Cay}_r(D,d)$, $d \in D \setminus F$. Then $M_A((u,v)) = M_D(u) - dM_D(v)$ is a semi-multiplicative quadratic map. If $A = \mathrm{Cay}(D,d)$ or $\mathrm{Cay}_r(D,d)$, then

$$x^2 - T_A(x)x + M_A(x)1_A = 0$$

for all $x \in A$.

3.4. There is another way to construct eight-dimensional unital algebras with a semi-multiplicative map: Let S be a quadratic étale F-algebra with canonical involution $^{-}$. Let (P,h) be a ternary nondegenerate $^{-}$-hermitian space (P a projective S-module) such that $\bigwedge^3(P,h) \cong \langle 1 \rangle$. Choose an isomorphism $\alpha : \bigwedge^3(P,h) \mapsto \langle 1 \rangle$ and define a cross product $\times_\alpha : P \times P \mapsto P$ via

$$h(u \times_\alpha v, w) = \alpha(u \wedge v \wedge w)$$

as in [T, p. 5122]. Choose $c \in S \setminus F$. The F-vector space $A = S \oplus P$ becomes a unital F-algebra denoted by $\mathrm{Cay}(S,P,ch,\times_\alpha)$ via the multiplication

$$(a,u)(b,v) = (ab - ch(v,u), va + u\bar{b} + v \times_\alpha u),$$

for all $a, b \in S$, $u, v \in P$. For $c \in F^\times$, $\mathrm{Cay}(S,P,ch,\times_\alpha)$ is an octonion algebra with norm $N((a,u)) = n_S(a) + ch(u,u)$ and the construction is independent of the choice of the isomorphism α, so that we may simply write $\mathrm{Cay}(S,P,ch)$. Any octonion algebra over F can be constructed like this.

If $C = \mathrm{Cay}(S,P,h) = \mathrm{Cay}(S,P,h,\times_\alpha)$ is an octonion division algebra over F, then $\mathrm{Cay}(S,P,dh) := \mathrm{Cay}(S,P,dh,\times_\alpha)$ is a division algebras over F, for any choice of $d \in S \setminus F$ [Pu2, Theorem 9].

Proposition 13. *Let K be a quadratic étale algebra of F, $A = \mathrm{Cay}(S,P,h)$ an octonion algebra and $A = \mathrm{Cay}(S,P,dh)$, $d \in S \setminus F$. Define the quadratic map $M_A : A \mapsto S$,*

$$M_A((a,u)) = N_{S/F}(a) - dh(u,u).$$

(i) M_A is semi-multiplicative:

$$M_A((a,0)(b,v)) = M_A((b,v)(a,0)) = N_{S/F}(a)M_A((b,v))$$

for all $a \in S$, $(b,v) \in A$.
(ii) For all $x = (a,u), y = (b,v) \in A$, the associated bilinear map $M_A : A \times A \mapsto S$ is given by

$$M_A(x,y) = N_{S/F}(a,b) - dh(u,v).$$

(iii) $T_A : A \mapsto F$, $T_A(x) = T_S(a)$ for $x = (a,u) \in A$ and $\overline{(a,u)} = (\bar{a}, -u)$ is a bijective F-linear map of order two.
(iv) $M_A(a,bx) + M_A(b,ax) = M_A(a,xb) + M_A(b,xa) = N_{S/F}(a,b)T_A(v) \in S$ for all $x \in A$, $a, b \in S$.
(v) $M_A(\bar{x}) = M_A(x)$, $M_A(x)1_A = \bar{x}x = x\bar{x}$ and $x\bar{y} + y\bar{x} = M_A(x,y)1_A$ for all $x \in A$.
(vi) If $d \notin F$ then $M_A(x) = 0$ if and only $x = 0$.
(vii) $x^2 - T_A(x)x + M_A(x)1_A = 0$ for all $x \in A$, $a, b \in S$.

Proof. The proof is straightforward calculation, in particular, we have

$$M_A((a,0)(b,v)) = M_A((ab,av))$$
$$= N_S(ab) - dh(av,av) = N_S(a)(N_S(b) - da\bar{a}h(v,v)) = N_S(a)M_A((b,v))$$

and

$$M_A((b,v)(a,0)) = M_A((ab,av))$$
$$= N_S(ab) - dh(av,av) = N_S(a)(N_S(b) - da\bar{a}h(v,v)) = N_S(a)M_A((b,v)).$$

Furthermore, for $x = (a,u)$,

$$x^2 - M_A(1,x)x + M_A(x)1 = (a^2 - ch(u,u) - N(1,u)u + N(u)1 - cN(u), uT(u) - T(u)u) = (0,0).$$

□

Corollary 14. *Let $A = \mathrm{Cay}(D,d)$ or $A = \mathrm{Cay}_r(D,d)$ with D either a quadratic étale or a quaternion algebra, or let $A = \mathrm{Cay}(S,P,dh)$ as in Proposition 8. Then*

$$x^2 - (x+\bar{x})x + (x\bar{x})1 = 0$$

for all $x \in A$.

4. A Semi-Multiplicative Map for Nonassociative Cyclic Algebras

4.1. Nonassociative cyclic algebras of degree n. The proofs of the following results will be published in [St1, 2]. Let $G = \mathbb{Z}/n\mathbb{Z} = \langle \sigma \rangle$ and let L be a Galois G-algebra over F. Pick $a \in L \setminus F$ and define $(L/F,\sigma,a)$ to be the free L-module of rank n

$$(L/F,\sigma,a) = \bigoplus_{i=0}^{n-1} Lz^i$$

with basis $\{1 := z^0, z, \dots, z^{n-1}\}$, where the z^i are formal symbols. We define a multiplication on two elements lz^i and mz^j for $l,m \in L, 0 \le i,j, < n$, by

$$(lz^i)(mz^j) = \begin{cases} l\sigma^i(m)z^{i+j} & \text{if } i+j<n \\ l\sigma^i(m)az^{(i+j)-n} & \text{if } i+j \ge n \end{cases}$$

and then extend it linearly to all of $(L/F,\sigma,a)$. The above algebra is called a *nonassociative cyclic algebra of degree* n. For $n=2$ this is a nonassociative quaternion algebra.

It should be noted that these algebras are not of degree n themselves. The 'degree n' in the name refers only to the field extension used to construct the algebra.

If L/F is a cyclic field extension of degree n then if the elements $\{1,a,\dots,a^{n-1}\}$ are linearly independent over F, A is a division algebra. In particular, $A = (L/F,\sigma,a)$ is a division algebra for all cyclic field extensions L/F of prime degree p.

Let $A = (L/F,\sigma,a)$ be a nonassociative cyclic algebra of degree n. Consider it as a left L-vector space with basis $\{1,z,\dots,z^{n-1}\}$. The map $R_x : y \mapsto yx$ of right multiplication by an element $x \in A$ for all $y \in A$, is a vector space homomorphism. Write R_x for the matrix of right multiplication by x with respect to the basis $\{1,z,\dots,z^{n-1}\}$:

$$R_x = \begin{pmatrix} x_0 & x_1 & x_2 & \cdots & x_{n-1} \\ a\sigma(x_{n-1}) & \sigma(x_0) & \sigma(x_1) & \cdots & \sigma(x_{n-2}) \\ a\sigma^2(x_{n-2}) & a\sigma^2(x_{n-1}) & \sigma^2(x_0) & \cdots & \sigma^2(x_{n-3}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a\sigma^{n-1}(x_1) & a\sigma^{n-1}(x_2) & a\sigma^{n-1}(x_3) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix},$$

for $x = x_0 + x_1 z + \cdots + x_{n-1} z^{n-1}, x_i \in L$. We define a map $M_A : A \to L$ by

$$M_A(x) = \det(R_x)$$

for all $x \in A$. This is similar to the definition of the reduced norm of an associative cyclic algebra. However, M_A is not multiplicative since the map $x \mapsto R_x$ is not an F-algebra homomorphism.

Proposition 15. *(i) If $l \in L$ is considered as an element of A then $M_A(l) = N_L(l)$.*
(ii) If $x \in A$ and $l \in L$ then

$$M_A(lx) = N_L(l) M_A(x).$$

4.2. Isometries of M_A. A bijective linear map $f : A \to A$ such that $M_A(f(x)) = M_A(x)$ for all $x \in A$ is called an *isometry* of M_A.

The map

$$x \mapsto x_0 + x_1 l z + x_2 l \sigma(l) z^2 + \cdots + x_{n-1} l \sigma(l) \dots \sigma^{n-2}(l) z^{n-1}$$

for some $l \in L$ such that $N_L(l) = 1$, is an automorphism of A. We can write this map as

$$\varphi_m(x) = x_0 + x_1 m \sigma(m)^{-1} z + \cdots + x_{n-1} m \sigma^{n-1}(m) z^{n-1}$$

for some $m \in L$ [St1, 2]. Define the F-linear maps

$$\sigma_A^j : A \to A, \qquad \sum_{i=0}^{n-1} x_i z^i \mapsto \sum_{i=0}^{n-1} \sigma^j(x_i) z^i$$

for all $j = 0, \dots, n-1$. We obtain:

Proposition 16. *(i) $M_A(\varphi_m(x)) = M_A(x)$ for all $x \in A$.*
(ii) $M_A(\sigma_A^j(x)) = M_A(x)$ for all $x \in A$.

Not all automorphisms of A are isometries of M_A. If there exists an element $l \in L$ such that $\sigma^j(a) = N_L(l) a$ for some $j \in \{1, \dots, n-1\}$ then the map

$$\theta_l^j(x_0 + x_1 z + \cdots + x_{n-1} z^{n-1}) =$$

$$\sigma^j(x_0) + \sigma^j(x_1) l z + \sigma^j(x_2) l \sigma(l) z^2 + \cdots + \sigma^j(x_{n-1}) l \sigma(l) \dots \sigma^{n-2}(l) z^{n-1}$$

is an automorphism and we still get:

Theorem 17. *For all $x \in A$ we have*

$$M_A(\theta_l^j(x)) = \sigma^j(M_A(x)).$$

4.3. Some Identities for the Degree 3 Case. (The proofs are given in [St1, 2].)

Let F be a field of characteristic not 2 and 3 and let $A = (L/F, \sigma, a)$ be a cubic nonassociative cyclic algebra. Let x, y, w be three elements of A of the form

$$x = x_0 + x_1 z + x_2 z^2$$

$$y = y_0 + y_1 z + y_2 z^2$$

$$x = w_0 + w_1 z + w_2 z^2$$

for $x_i, y_i, w_i \in L$. Let $N_L : L \to F$ be the field norm and $T_L : L \to F$ the field trace. Explicitly, we have

$$M_A(x) = N_L(x_0) + aN_L(x_1) + a^2N_L(x_2) - aTr_L(x_0\sigma(x_1)\sigma^2(x_2)).$$

Linearize this to get a map $M_A : A \times A \mapsto L, (x, y) \to M_A(x; y)$,

$$M_A(x; y) = N_L(x_0; y_0) + aN_L(x_1, y_1) + a^2N_L(x_2, y_2) - af(x; y)$$

which is quadratic in x and linear in y, where

$$N_L(x_i; y_i) = x_i\sigma(x_i)\sigma^2(y_i) + x_i\sigma(y_i)\sigma^2(x_i) + y_i\sigma(x_i)\sigma^2(x_i)$$

and

$$f(x; y) = T_L(x_0\sigma(x_1)\sigma^2(y_2)) + T_L(x_0\sigma(y_1)\sigma^2(x_2)) + T_L(y_0\sigma(x_1)\sigma^2(x_2)).$$

We get the full linearization $M_A : A \times A \times A \mapsto L$, $(x, y, w) \to M_A(x, y, w)$ by

$$\begin{aligned} M_A(x, y, w) &= M_A(x + w; y) - M_A(x; y) - M_A(w; y) \\ &= N_L(x_0, y_0, w_0) + aN_L(x_1, y_1, w_1) + a^2N_L(x_2, y_2, w_2) \\ &- af(x, y, w), \end{aligned}$$

where

$$\begin{aligned} N_L(x_i, y_i, w_i) &= x_i\sigma(y_i)\sigma^2(w_i) + x_i\sigma(w_i)\sigma^2(y_i) + y_i\sigma(x_i)\sigma^2(w_i) \\ &= +y_i\sigma(w_i)\sigma^2(x_i) + w_i\sigma(x_i)\sigma^2(y_i) + w_i\sigma(y_i)\sigma^2(x_i) \end{aligned}$$

and

$$\begin{aligned} f(x, y, w) &= T_L(x_0\sigma(y_1)\sigma^2(w_2)) + T_L(x_0\sigma(w_1)\sigma^2(y_2)) \\ &+ T_L(y_0\sigma(x_1)\sigma^2(w_2)) + T_L(y_0\sigma(w_1)\sigma^2(x_2)) \\ &+ T_L(w_0\sigma(x_1)\sigma^2(y_2)) + T_L(w_0\sigma(y_1)\sigma^2(w_2)). \end{aligned}$$

$M_A(x, y, w)$ is a 3-linear map. We define a linear map $T_A : A \mapsto L$,

$$T_A(x) = M_A(1; x) = T_L(x_0),$$

with bilinearization

$$\begin{aligned} T_A(x, y) &= T_A(x)T_A(y) - N_A(1, x, y) \\ &= T_L(x_0y_0) + aT_L(\sigma(x_1)\sigma^2(y_2)) + aT_L(\sigma(y_1)\sigma^2(x_2)) \end{aligned}$$

and a quadratic map $S_A : A \mapsto L$,

$$S_A(x) = M_A(x; 1) = T_L(x_0)\sigma(x_0) - aT_L(x_1\sigma(x_2))$$

with linearization

$$S_A(x, y) = M_A(x, y, 1) = T_L(x_0\sigma(y_0)) + T_L(y_0\sigma(x_0)) - aT_L(x_1\sigma(y_2)) - aT_L(y_1\sigma(x_2)).$$

Then

$$T_A(1) = S_A(1) = 3,$$
$$T_A(1, y) = T_A(y),$$
$$S_A(x, y) = T_A(x)T_A(y) - T_A(x, y).$$

We define a quadratic map $\sharp : A \to A$ by

$$x^\sharp = x^2 - T_A(x)x + S_A(x)1.$$

Explicitly, we have

$$x^\sharp = \sigma(x_0)\sigma^2(x_0) - a\sigma(x_1)\sigma^2(x_2) + (ax_2\sigma^2(x_2) - \sigma^2(x_0)x_1)z + x_1\sigma(x_1) - \sigma(x_0)x_2)z^2$$

and its linearization $x\sharp y = (x+y)^\sharp - x^\sharp - y^\sharp$ satisfies

$$x^\sharp = 1/2(x\sharp x).$$

By Proposition 7, $1\sharp y = T_A(y) - y$ for all $y \in A$. Suppose that $x \in L$. Then for all $y \in A$,

$$T_A(x^\sharp, y) = M_A(x; y)$$

[St1, Proposition 6.7, St2].

Proposition 18. *(cf. [St1, Proposition 6.7, 6.8, 6.9])*
(i) For all $x \in L$, $x\sharp y = \sigma(x_0)\sigma^2(y_0) + \sigma(y_0)\sigma^2(x_0) - \sigma^2(x_0)y_1z - \sigma(x_0)y_2z^2$,
(ii) $T_A(x\sharp y) = S_A(x, y)$ *for all* $y \in A$.
(iii) If $y \in L$ *then*

$$T_A(x\sharp y, w) = T_A(x, y\sharp w) = M_A(x, y, w)$$

for all $w \in A$.
(iv) Every element $x \in A$ *satisfies* $x^\sharp x = M_A(x)1$.

From Proposition 8 we deduce that every element $x \in A$ satisfies the equation

$$x^2x - T(x)x^2 + S(x)x - M(x)1 = 0.$$

5. Semi-multiplicativity for a quadratic U-operator

Let A be an associative F-algebra equipped with a multiplicative cubic norm structure, i.e. A possesses a multiplicative cubic form $N_A : A \to F$ and a linear trace form $T_A : A \to F$. This gives rise to a bilinear trace $T_A : A \times A \to F, (x, y) \mapsto T_A(x, y) := T_A(xy)$. We also have an adjoint $\sharp : A \to A, x \mapsto x^\sharp$, a quadratic map which bilinearizes to

$$(x, y) \mapsto x\sharp y = (x+y)^\sharp - x^\sharp - y^\sharp.$$

Moreover, the following relations hold in all scalar extensions:

$$N_A(1) = 1, \tag{7}$$

$$1^\sharp = 1, \tag{8}$$

$$1\sharp x = T_A(x)1 - x, \tag{9}$$

$$T_A(x^\sharp, y) = (\partial_y N_A)(x), \tag{10}$$

$$x^{\sharp\sharp} = N_A(x)x, \tag{11}$$

$$(xy)^\sharp = y^\sharp x^\sharp. \tag{12}$$

We refer the reader to [McC2] for these and the various other identities that hold in this set-up. In particular, the bilinear Jordan product $x \circ y = xy + yx$ for all $x, y \in A$ can be written as

$$x \circ y = x\sharp y + T_A(x)y + T_A(y)x - (T_A(x)T_A(y) - T_A(x, y))1,$$

and the norm N_A satisfies the relation

$$N_A(x^\sharp) = N_A(x)^2. \tag{13}$$

We now generalize the first Tits construction of A as follows: pick an invertible element $\mu \in A^\times$. Define the F-vector space

$$Trip(A, N_A) := A_0 \oplus A_1 \oplus A_2,$$

where each summand is a copy of the algebra A. Identifing A with A_0 we define a cubic map $M : Trip(A, N_A) \to A$ by

$$M((x_0, x_1, x_2)) = N_A(x_0) + \mu N_A(x_1) + \mu^{-1} N_A(x_2) - T_A(x_0x_1x_2)$$

for all $x_i \in A$. This map satisfies $M((x_0, 0, 0)) = N_A(x_0)$, so M restricted to A is N_A. We also extend the adjoint map by defining $\sharp : Trip(A, N_A) \to Trip(A, N_A)$,

$$x^\sharp = (x_0^\sharp - x_1x_2, \mu^{-1}x_2^\sharp - x_0x_1, \mu x_1^\sharp - x_2x_0),$$

for $x = (x_0, x_1, x_2), x_i \in A$. This linearizes to

$$x\sharp y = (x_0\sharp y_0 - x_1y_2 - y_1x_2, \mu^{-1}(x_2\sharp y_2) - x_0y_1 - y_0x_1, \mu(x_1\sharp y_1) - x_2y_0 - y_2x_0)$$

for $y = (y_0, y_1, y_2), y_i \in A$. The trace forms are extended to $Trip(A, N_A)$ via

$$T(x, y) = T_A(x_0y_0) + T_A(x_1y_2) + T_A(y_1x_2),$$

$$T(x) = T_A(x_0),$$

for x and y as above. We define a multiplication $\circ$ on $Trip(A, N_A)$ by putting

$$x \circ y := x\sharp y + T(x)y + T(y)x - (T(x)T(y) - T(x, y))1$$

for all $x, y \in A$. For $x_0 \in A$, write $\overline{x_0} = T_A(x_0) - x_0$, then a quick calculation shows that the multiplication can be written as

$$x \circ y = (x_0 \circ y_0 + \overline{x_1y_2} + \overline{x_2y_1}, \overline{x_0}y_1 + \overline{y_0}x_1 + \mu^{-1}(x_2 \times y_2), \overline{x_0}y_2 + \overline{y_0}x_2 + \mu(x_1 \times y_1)).$$

The multiplication thus canonically extends the one obtained for the classical first Tits construction. $Trip(A, N_A)$ is a unital F-algebra which contains A as a subalgebra.

The intermediate quadratic form $S_A : A \to F$ is defined by $S_A(x_0) = N_A(x; 1)$. This linearizes to a map $S_A(x, y) : A \times A \to F$, moreover we have $S_A(x_0) = T_A(x_0^\sharp)$ for all $x_0 \in A$.

Proposition 19. *Extending S_A to $Trip(A, N_A)$ by defining $S(x) := M(x; 1)$, we have $S(x) = T(x^\sharp)$ and the linearization $S(x, y)$ satisfies*

$$S(x, y) = T(x)T(y) - T(x, y),$$

for all $y \in Trip(A, N_A)$.

Proof. Let $x = (x_0, x_1, x_2)$ and $y = (y_0, y_1, y_2)$ for $x_i, y_i \in A$ then explicitly we have

$$M(x;y) = N_A(x_0;y_0)+\mu N_A(x_1;y_1)+\mu^{-1}N_A(x_2;y_2)-T_A(x_0x_1y_2)-T_A(x_0y_1x_2)-T_A(y_0x_1x_2),$$

and hence

$$S(x) := M(x;1) = N_A(x_0;1) - T_A(x_1x_2) = S_A(x_0) - T_A(x_1x_2).$$

On the other hand

$$T(x^\sharp) = T_A(x_0^\sharp - x_1x_2) = T_A(x_0^\sharp) - T_A(x_1x_2) = S_A(x_0) - T_A(x_1x_2) = S(x),$$

as required. In A we have the relation $S_A(x_0, y_0) = T_A(x_0)T_A(y_0) - T_A(x_0, y_0)$ for all $x_0, y_0 \in A$. Linearizing $S(x)$ gives

$$\begin{aligned} S(x, y) &= S_A(x_0, y_0) - T_A(x_1y_2) - T_A(y_1x_2) \\ &= T_A(x_0)T_A(y_0) - T_A(x_0, y_0) - T_A(x_1y_2) - T_A(y_1x_2) \\ &= T(x)T(y) - T(x, y), \end{aligned}$$

using the definitions of $T_A(x_i)$ and $T_A(x_i, y_i)$ and the fact that $T_A(x_0, y_0) = T_A(x_0y_0)$. □

Lemma 20. *Let $x = (x_0, x_1, x_2) \in Trip(A, N_A), x_i \in A$. Then $x\sharp 1 = T(x) - x$.*

Proof. From the definition of $\sharp$, we get

$$x\sharp 1 = (x_0\sharp 1, -x_1, -x_2) = T(x) - x,$$

using the relation $x_0\sharp 1 = T_A(x_0) - x_0$ on A. □

For all $x \in Trip(A, N_A)$ define the operator $U_x : Trip(A, N_A) \to Trip(A, N_A)$ by

$$U_x y = T(x, y)x - x^\sharp \sharp y,$$

for all $y \in Trip(A, N_A)$.

Theorem 21. *Consider $x \in A$ embedded as $(x, 0, 0) \in Trip(A, N_A)$, then for all $y \in Trip(A, N_A)$ we have*

$$M(U_x y) = N_A(x)^2 M(y).$$

Proof. Using the definitions of U_x and the sharp mapping given above it is straightforward to check that when $x \in A$ we get

$$U_x y = (T_A(x, y_0)x - x^\sharp \sharp y_0, x^\sharp y_1, y_2x^\sharp),$$

for $y = (y_0, y_1, y_2)$. The first term $T_A(x, y_0)x - x^\sharp \sharp y_0$ is just $U_x y_0$ where the U-operator is now restricted to A. Hence we have

$$\begin{aligned} M(U_x y) &= M(T_A(x, y_0)x - x^\sharp \sharp y_0, x^\sharp y_1, y_2x^\sharp) \\ &= N_A(U_x y_0) + \mu N_A(x^\sharp y_1) + \mu^{-1}N_A(y_2x^\sharp) - T_A((U_x y_0)(x^\sharp y_1)(y_0x^\sharp)). \end{aligned}$$

Now since A is a classical cubic norm structure we know that $N_A(U_x y_0) = N_A(x)^2 N_A(y)$. By (13) and the multiplicativity of N_A, we see $N_A(x^\sharp y_1) = N_A(x)^2 N_A(y_1)$ and similarly $N_A(y_2x^\sharp) = N_A(x)^2 N_A(y_2)$ so if we can show that

$$T_A((U_x y_0)(x^\sharp y_1)(y_0x^\sharp)) = N_A(x)^2 T_A(y_0y_1y_2),$$

then we are done. We can prove this identity by considering a classical Tits construction over A, say $J = J(A, 1)$ for example. If we look at the U-operator in $J(A, 1)$ of the same elements x and y above (J is the same vector space as $Trip(A, N_A)$) we see

$$U_x y = (T_A(x, y_0)x - x^\sharp \sharp y_0, x^\sharp y_1, y_2 x^\sharp),$$

as before. Since J does satisfy the equation $N_A(U_x y) = N_A(x)^2 N_A(y)$ for all $x, y \in J$ we have

$$\begin{aligned} &N_A(U_x y_0) + \mu N_A(x^\sharp y_1) + \mu^{-1} N_A(y_2 x^\sharp) - T_A((U_x y_0)(x^\sharp y_1)(y_0 x^\sharp)) \\ &= N_A(x)^2 (N_A(y_0) + N_A(y_1) + N_A(y_2) - T_A(y_0 y_1 y_2)). \end{aligned}$$

We can cancel the terms we know are equal to leave

$$T_A((U_x y_0)(x^\sharp y_1)(y_0 x^\sharp)) = N_A(x)^2 T_A(y_0 y_1 y_2),$$

as required. □

6. Examples of unital algebras with left or right semi-multiplicative quadratic maps

In this section we construct an algebra $HK(L, \sigma, \eta, \mu)$ with a quadratic map M_{HK} satisfying $M_{HK}(bx) = M_{HK}(b)M_{HK}(x)$ for all $x \in HK$ and all b belonging to a certain subalgebra of HK. This algebra fails to satisfy $M_{HK}(xb) = M_{HK}(x)M_{HK}(b)$. We also construct an algebra Kn with a map M_{Kn} satisfying a right semi-multiplicative property but not a left semi-multiplicative property. These algebras are based on constructions of finite semifields given by Hughes and Kleinfeld [HK] and Knuth [Kn].

Definition 1 (HK)**.** Let L/F be a separable field extension of degree n. Let σ be a nontrivial automorphism of L and $\eta, \mu \in L^\times$. Endow the F-vector space $HK(L, \sigma, \eta, \mu) = L \oplus L$ with the multiplication

$$(x, y)(u, v) = (xu + \eta\sigma(v)y, vx + y\sigma(u) + \mu\sigma(v)y),$$

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

$HK(L, \sigma, \eta, \mu)$ is a unital, $2n$-dimensional F-algebra. It is a division algebra if an only if the equation

$$w\sigma(w) + \mu w - \eta$$

has no solutions in L [HK]. The multiplication in HK may be written as

$$(x, y)(u, v) = (x, y) \begin{pmatrix} u & v \\ \eta\sigma(v) & \sigma(u) + \mu\sigma(v) \end{pmatrix},$$

for all $x, y, u, v \in L$. We use this to define a quadratic map $M_{HK} : HK \to L$,

$$M_{HK}(x, y) = det \begin{pmatrix} x & y \\ \eta\sigma(y) & \sigma(x) + \mu\sigma(y) \end{pmatrix}$$

for $(x, y) \in HK$.

Explicitly, we can write

$$M_{HK}(x, y) = x\sigma(x) + \mu x\sigma(y) - \eta y\sigma(y)$$

for all $(x, y) \in HK$.

Proposition 22. *The map M_{HK} satisfies $M_{HK}((l,0)(x,y)) = M_{HK}(l,0)M_{HK}(x,y)$ for all $l, x, y \in L$.*

Proof.

$$\begin{aligned} M_{HK}((l,0)(x,y)) &= M_{HK}((lx, ly)) \\ &= lx\sigma(lx) + \mu lx\sigma(ly) - \eta ly\sigma(ly) \\ &= l\sigma(l)(x\sigma(x) + \mu x\sigma(y) - y\sigma(y)) \\ &= M_{HK}((l,0))M_{HK}((x,y)). \end{aligned}$$

□

Hence if we identify L with the subspace $L \oplus 0$, we can think of M_{HK} as a left semi-multiplicative map. In general, the identity $M_{HK}((x,y)(l,0)) = M_{HK}(x,y)M_{HK}(l,0)$ is not satisfied so M_{HK} is not right semi-multiplicative.

Definition 2 (Kn)**.** Let L/F be a separable field extension of degree n. Let σ be a nontrivial automorphism of L and let $\eta, \mu \in L^\times$. Endow the F-vector space $Kn(L, \sigma, \eta, \mu) = L \oplus L$ with the multiplication

$$(x, y)(u, v) = (xu + \eta\sigma^{-1}(v)y, vx + y\sigma(u) + \mu vy),$$

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

$Kn(L, \sigma, \eta, \mu)$ is a unital $2n$-dimensional F-algebra. It is a division algebra if an only if the equation

$$w\sigma(w) + \mu w - \eta$$

has no solutions in L. (The sufficiency of this condition was proved in [Kn] for L a finite field and easily extends to infinite fields. Conversely $(\eta, w)(w, 1) = (0, 0)$ if w is a root of the above equation.) We may write the multiplication in Kn as

$$(x, y)(u, v) = (x, y)\begin{pmatrix} u & v \\ \eta\sigma^{-1}(v) & \sigma(u) + \mu v \end{pmatrix}.$$

If we define $M_{Kn} : Kn \to L$ by

$$M_{Kn}((x, y)) = det\begin{pmatrix} x & y \\ \eta\sigma^{-1}(y) & \sigma(x) + \mu y \end{pmatrix},$$

explicitly this is

$$M_{Kn}((x, y)) = x\sigma(x) + \mu xy - \eta y\sigma^{-1}(y).$$

A similar calculation to that in Proposition 22 yields

Proposition 23. *$M_{Kn}((x,y)(l,0)) = M_{Kn}(x,y)M_{Kn}(l,0)$ for all $l, x, y \in L$.*

Therefore if we identify L with the subalgebra $L \oplus 0$ of Kn, then M_{Kn} is a right semi-multiplicative map. However, it is not left semi-multiplicative in general.

References

[As-Pu] Astier, V., Pumplün, S., *Nonassociative quaternion algebras over rings.* Israel J. Math. 155, 125 – 147, 2006.

[HK] Hughes, D. R., Kleinfeld, E., *Seminuclear Extensions of Galois Fields.* American Journal of Mathematics, Vol. 82, (3), (1960), pp 389–392.

[KMRT] Knus, M.A., Merkurjev, A., Rost, M., Tignol, J.-P., “The Book of Involutions”, AMS Coll. Publications, Vol.44 (1998).

[Kn] Knuth, D. E., *Finite Semifields and Projective Planes.* Journal of Algebra, (2), (1965), pp 182–217.

[McC1] McCrimmon, K., “A Taste of Jordan Algebras”. Universitext, Springer Verlag, New York 2004.

[McC2] McCrimmon, K., *The Freudenthal-Springer-Tits constructions of exceptional Jordan algebras*, Trans. Amer. Math. Soc 139 (1969), 495-510.

[Pu1] Pumplün, S., *How to obtain division algebras from a generalized Cayley-Dickson doubling process.* Submitted.

[Pu2] Pumplün, S., *A construction method for some real division algebras with* $su(3)$ *as derivation algebra.* Israel J. Math. 191, Part A (2012), 307 - 335.

[Pu-U] Pumplün, S., Unger, T., *Space-time block codes from nonassociative division algebras.* Advances in Mathematics of Communications 5 (3), 609-629.

[S] Sandler, R., *Autotopism groups of some finite nonassociative algebras.* AMS J. Math. 84 (2) (1962), 239 - 264.

[Sch] Schafer, R. D., *Forms permitting composition.* Adv. Math. 4 (1970), 127 – 148.

[St1] Steele, A., *Nonassociative Cyclic Algebras.* To appear in Israel J. Math., available at http://molle.fernuni-hagen.de/~loos/jordan/archive/nonassoc_cyclic/index.html.

[St2] Steele, A., *Some new classes of algebras.* PhD Thesis, University of Nottingham, in preparation.

[S-Pu-O] Steele, A., Pumplün, S., Oggier, F., *MIDO space-time codes from associative and non-associative cyclic algebras.* Information Theory Workshop (ITW) 2012 IEEE (2012), 192-196.

[T] Thakur, M. L., *Cayley algebra bundles on* $\mathbb{A}^2_K$ *revisited*, Comm. Algebra 23(13) (1995), 5119-5130.

[W] Waterhouse, W.C., *Nonassociative quaternion algebras.* Algebras, Groups and Geometries 4, pp. 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

E-mail address: pmxas4@nottingham.ac.uk

School of Mathematical Sciences, University of Nottingham, University Park, Nottingham NG7 2RD, United Kingdom