Some New Classes of Division Algebras and Potential Applications to Space-Time Block Coding

Andrew Steele, M.Sci.

Thesis submitted to the University of Nottingham
for the degree of Doctor of Philosophy

October 2013

Abstract

In this thesis we study some new classes of nonassociative division algebras. First we introduce a generalisation of both associative cyclic algebras and of Waterhouse's nonassociative quaternions. An important aspect of these algebras is the simplicity of their construction, which is a modification of the classical definition of associative cyclic algebras. By taking the parameter used in the classical definition from a larger field, we lose the property of associativity but gain many new examples of division algebras. This idea is also applied to obtain a generalisation of the first Tits construction.

We go on to study constructions of Menichetti, Knuth, and Hughes and Kleinfeld, which have previously only been considered over finite fields. We extend these definitions to infinite fields and get new examples of division algebras, including some over the real numbers.

Recently, both associative and nonassociative division algebras have been applied to the theory of space-time block coding. We explore this connection and show how the algebras studied in this thesis can be used to construct space-time block codes.

Acknowledgements

I would like to express my sincere thanks to my supervisor, Susanne Pumplün, for her constant help and guidance during the past three years. At times when I felt I was not making progress, her words of encouragement gave me the confidence and determination to carry on.

A special mention should go to Prof. Holger Petersson, whose insightful questions at a workshop in Madrid, and his subsequent communications were the inspiration for Chapter 5.

To all the friends I have made during my time here, thank-you for making this a much more enjoyable experience. In particular, to Iain Foulger and Thomas Oliver, who I have had the privilege of living with for the past two years, thank-you for putting up with me!

Finally, I would like to thank my parents who have continually supported and encouraged me throughout my studies.

Contents

Chapter 1

Introduction

Hamilton introduced quaternion algebras in 1843 as a 4-dimensional real vector space with basis $\{1, i, j, k\}$ and multiplication defined by the famous formula

$$i^2 = j^2 = k^2 = ijk = -1.$$

This classical construction, denoted $\mathbb{H}$ in honour of Hamilton, is familiar to all algebraists. However, the most elegant construction method of quaternion algebras is perhaps that of a Cayley-Dickson doubling of a quadratic separable field extension. This goes as follows: let F be a field and let L be a quadratic separable extension of F with non-trivial automorphism, $x \mapsto \sigma(x)$. Pick a nonzero scalar $\lambda \in F$ and define the F-vector space

$$\mathrm{Cay}(L/F, \lambda) := L \oplus L.$$

The bilinear product

$$(x, y)(u, v) = (xu + \lambda y\sigma(v), xv + y\sigma(u)),$$

for all $x, y, u, v \in L$, gives $\mathrm{Cay}(L/F, \lambda)$ the structure of an F-algebra. Quaternion algebras are associative, central simple and can be applied to many areas of mathematics and physics.

Nonassociative quaternions were first discovered by Dickson [18] in 1935. However, it was Waterhouse, in [56], who first carried out a systematic study

of these algebras. He showed that they could be built by using the same construction for a quadratic separable field extension L of F but taking the element a from $L \setminus F$ instead. These new algebras are nonassociative, but for every choice of $a \in L \setminus F$, they are division algebras. Comparing this to the associative case, where $\mathrm{Cay}(L/F, \lambda)$ is a division algebra if and only if λ is not the norm of any element $l \in L$, we see that it is much easier to find examples of division algebras using Waterhouse's construction. For example, over the real numbers, $\mathbb{H}$ is the only associative quaternion division algebra up to isomorphism; however, there are infinitely many nonisomorphic, nonassociative quaternion division algebras.

The classification of all division algebras over a fixed base field is one of the major open problems in algebra and, in particular, the classification question for real division algebras is an area of much active research (see [14] for a nice reference on current progress). More recently, both associative and nonassociative division algebras over number fields have become important in the context of space-time block coding (see [51] and [47], for example), thus highlighting the importance of this problem. A complete solution of the classification question is a massive and seemingly intractable problem at the current time. One way to attack it is to find new classes of division algebras and try to find patterns and structure in them. The above example shows us that by a simple modification of a well-known construction, we get new examples of division algebras. This theme reoccurs throughout the thesis.

In the next chapter we will introduce the necessary preliminaries and notations used throughout. Recall that if F is a field and L is a cyclic field extension of F of degree n then we can form the cyclic algebra $(L/F, \sigma, a)$ of degree n, where σ is the generator of the Galois group of L/F and a is some nonzero scalar in F (see [30, §30.A.]). The properties of these central simple associative algebras are well known (see [30] or [44, Ch 15]).

A priori, it is not straightforward to determine whether a given cyclic algebra is a division algebra, or if there even exist any cyclic division algebras

over a given field. For example, there do not exist any cyclic division algebras over finite fields. In Chapter 3 we generalise both nonassociative quaternion algebras and associative cyclic algebras of degree n to what we call *nonassociative cyclic algebras of degree n*. We define nonassociative cyclic algebras by imitating the classical definition, but now taking $a \in L \setminus F$. We show that if the elements $1, a, a^2, \ldots a^{n-1}$ are linearly independent over F, where n is the degree of L/F, then the resulting nonassociative cyclic algebra is division (loc. cit. Theorem 3.2.10). To ensure this we simply choose a such that it belongs to no proper subfield of L. In particular, if L/F is of prime degree, every choice of $a \in L \setminus F$ yields a division algebra. We study these algebras in some detail and prove results concerning their automorphisms and derivations. We also look at their subalgebras and study them in detail for nonassociative cyclic algebras of degree 4 (i.e., when L/F is a field extension of degree 4). The contents of this chapter will be published in the Israel Journal of Mathematics [53].

Recall that a multiplicative form of degree n on an F-algebra A is a homogeneous polynomial map $N : A \to F$ of degree n such that $N(xy) = N(x)N(y)$ for all $x, y \in A$. The most common examples of multiplicative forms are the field norm of a finite field extension and the reduced norm of a central simple algebra. In Chapter 4 we introduce the concept of *semi-multiplicative maps*. These can be thought of as a generalisation of multiplicative forms. We consider maps $M_A : A \to D$, where D is some subalgebra of A, such that M_A satisfies $M_A(dx) = M_A(d)M_A(x)$ for all $d \in D$ and $x \in A$. It can be shown that a nonassociative cyclic algebra of degree n possesses a semi-multiplicative map which motivated our study of these objects. In particular, we look at the quadratic and the cubic case in detail and prove several results about them which are analogus to known results for quadratic and cubic multiplicative forms.

The first Tits construction is intimately linked with cubic algebras and in particular, can be used to construct an Albert algebra from a central

simple algebra of degree 3. We consider a generalisation of this in Chapter 5. Our generalised first Tits construction possesses a map which satisfies some kind of Jordan semi-multiplicativity and is analogous to the cubic map on a classical first Tits construction.

In Chapter 6 we construct nonassociative cyclic algebras over finite fields. In fact, this special case was studied already by Sandler in [48] and was generalised in [40] and [25], again over finite fields. Although these constructions are well known to those who work with finite division algebras, they have not received much attention outside of this area. By a famous theorem of Wedderburn [35], any associative division algebras over a finite field is, again, a finite field. However, if we drop the condition of associativity then there are many examples of finite division algebras. These are called *semifields* in the literature and surveys can be found in [13], [27] and [34]. Traditionally, semifields are studied in the context of finite geometries due to their connections with projective planes. In fact, every proper semifield coordinatizes a non-Desarguesian projective plane and two semifields coordinatize the same projective plane if and only if they are *isotopic* [3]. Because of this, semifields are usually classified up to isotopy rather than up to isomorphism. In this chapter we study them as algebraic objects in their own right. By using the results found in the more general context of Chapter 3, we are able to determine the automorphism groups of these semifields. We also consider the question of how many nonisomorphic semifields of this type exist given a finite field F and a finite extension L/F.

In Chapters 7 and 8 we look at other well-known constructions of finite semifields and generalise these to algebras over general fields. In particular, we look at the the constructions of Menichetti, Hughes-Kleinfeld and Knuth. We obtain results about their automorphisms, which we can then apply to gain new insights about the automorphism groups of some classical semifield constructions.

In the final chapter, we highlight the connection between the nonassociative division algebras we built and space-time block codes. This connection has received some attention recently from coding theorists and we briefly look at how the constructions defined in the previous chapters can be used for space-time block codes.

Chapter 2

Preliminaries

2.1 Nonassociative Algebras

Throughout, let F be a field. By an F-algebra A, we mean a finite-dimensional F-vector space equipped with a (not necessarily associative) bilinear map $A \times A \to A$ which is the multiplication of the algebra. The *associator* of $x, y, z \in A$ is defined to be

$$[x, y, z] := (xy)z - x(yz).$$

The *nucleus* of A is then defined to be the set

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

This is an associative subalgebra of A (which may be zero) and we have $(xy)z = x(yz)$ if one of x, y or z belongs to $Nuc(A)$. One can define the left, right and middle nuclei denoted $Nuc_l(A), Nuc_r(A)$ and $Nuc_m(A)$ respectively, as the set of elements whose corresponding associator vanishes, for example the left nucleus is given as $Nuc_l A := \{x \in A : [x, A, A] = 0\}$. It follows from this that the nucleus is the intersection of the left, right and middle nuclei. The *commuter* of A is the set of elements which commute with every other element,

$$Comm(A) := \{x \in A \mid xy = yx \text{ for all } y \in A\}.$$

The *centre* is then given by the intersection of $Nuc(A)$ and $Comm(A)$ and is denoted $Z(A)$. A is called *unital* if there exists a unique element, denoted 1_A or simply 1 if the context is clear, such that $1x = x1 = x$ for all $x \in A$. We will always assume that homomorphisms between two unital F-algebras, A and B, send 1_A to 1_B. Any isomorphism $f : A \to B$, maps the nucleus of A isomorphically onto the nucleus of B.

An F-algebra A is called a *division algebra* if the maps $L_x : y \mapsto xy$ and $R_x : y \mapsto yx$ are bijective for all nonzero $x \in A$. Since we are working with finite-dimensional vector spaces, this is equivalent to the condition that A contains no nontrivial zero divisors ([49]). A *derivation* of an F-algebra A is a F-linear map $\delta : A \to A$, which satisfies the Leibniz rule:

$$\delta(xy) = \delta(x)y + x\delta(y),$$

for all $x, y \in A$.

2.2 Cyclic Algebras

In this section we recall an important class of associative, central simple algebras known as cyclic algebras.

Definition 2.2.1. Let L/F be a cyclic field extension of degree n with Galois group generated by the automorphism σ. Pick a nonzero element $a \in F^\times$ and define the L-vector space

$$(L/F, \sigma, a) := L \oplus Lz \oplus \cdots \oplus Lz^{n-1},$$

where $\{1, z, \ldots, z^{n-1}\}$ is called the *standard basis* of $(L/F, \sigma, a)$. We give $(L/F, \sigma, a)$ the structure of an F-algebra by defining an associative product via the rules

$$zl = \sigma(l)z \quad \text{and} \quad z^n = a,$$

for all $l \in L$. We call $(L/F, \sigma, a)$ a *cyclic algebra of degree* n.

Remark 2.2.2. Cyclic algebras can be defined more generally using an étale F-algebra L instead of a cyclic field extension (see [30, §19 & §30], for example). However, since we will be concerned with finding division algebras throughout this thesis, we will only consider the case where L is a field extension.

Cyclic algebras play an important role in the theory of central simple algebras and a more in-depth discussion on them can be found in many textbooks, for example [19, §10] or [44, Ch. 15]. In particular, we recall the following well-known results (see [32, §14]).

Theorem 2.2.3 (Albert)**.** *If L/F is a field extension of prime degree then $(L/F, \sigma, a)$ is a division algebra if and only if $a \notin N_{L/F}(L^\times)$.*

Theorem 2.2.4 (Wedderburn)**.** *If L/F is a field extension of degree n and the order of a in $F/N_{L/F}(L^\times)$ is n then $(L/F, \sigma, a)$ is a division algebra.*

2.3 The Cayley-Dickson Process

Suppose that L/F is a separable quadratic extension. Applying Definition 2.2.1 to L/F yields a quaternion algebra. As mentioned in the introduction, the Cayley-Dickson doubling process is a very elegant method for constructing quaternion algebras. In fact, the Cayley-Dickson process can be applied to any unital algebra with an involution and can be used to construct all composition algebras over a field of characteristic not 2. We briefly give the details here.

Let A be a unital F-algebra. An *involution* on A is a map $\sigma : A \to A$ satisfying the following conditions:

(i) $\sigma(x + y) = \sigma(x) + \sigma(y)$,

(ii) $\sigma(xy) = \sigma(y)\sigma(x)$,

(iii) $\sigma(\sigma(x)) = x$,

for all $x, y \in A$. A is called a *composition algebra* if there exists a nondegenerate quadratic form N_A on A such that

$$N_A(1_A) = 1 \quad \text{and} \quad N_A(xy) = N_A(x)N_A(y),$$

for all $x, y \in A$. The quadratic form N_A is said to *permit composition*.

Definition 2.3.1 (The Cayley-Dickson Process)**.** Let A be a unital algebra over a field F and let σ be an involution of A. By picking a scalar $\lambda \in F^\times$, we may form a new unital F-algebra called the *Cayley-Dickson doubling of* A and denoted $\mathrm{Cay}(A, \lambda)$, by setting

$$\mathrm{Cay}(A, \lambda) := A \oplus A,$$

and defining multiplication by

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

for all $x, y, u, v \in A$. We extend the involution on A to $\mathrm{Cay}(A, \lambda)$ by setting

$$\sigma(x, y) := (\sigma(x), -y),$$

for all $x, y \in A$. If the involution on A is such that the norm $N_A(x) := x\sigma(x) \in F1$ and trace $Tr_A(x) := x + \sigma(x) \in F1$, then we can extend these maps to $\mathrm{Cay}(A, \lambda)$ by setting

$$N(x, y) := N_A(x) - \lambda N_A(y) \in F1, \quad \text{and} \quad Tr(x, y) := Tr_A(x) \in F1,$$

for all $x, y \in A$. The algebra $\mathrm{Cay}(A, \lambda)$ is clearly twice the dimension of A and has unit $1 = (1, 0)$. It also contains A as a subalgebra. If A is an associative composition algebra then $\mathrm{Cay}(A, \lambda)$ is a composition algebra, but it is not necessarily associative.

Remark 2.3.2. If A is a quadratic separable field extension of F and σ is the non-trivial automorphism of A then, by choosing the basis $1 = (1, 0)$ and $z = (0, 1)$ of $\mathrm{Cay}(A, \lambda)$, it is easy to see that $\mathrm{Cay}(A, \lambda)$ is the cyclic algebra $(A/F, \sigma, \lambda)$ of degree 2, i.e., a quaternion algebra.

Example 2.3.3. Let F be a field of characteristic not 2. We assume that the involution σ is the trivial map, $x \mapsto x$, on F. Picking $\lambda_1 \in F$ and setting $L := \mathrm{Cay}(F, \lambda_1)$, we see that L is a 2-dimensional F algebra, which is a field if λ_1 is not a square in F, otherwise, L is said to be *split* and is isomorphic to $F \times F$. Choosing another scalar $\lambda_2 \in F$ and repeating the process we get $Q := \mathrm{Cay}(L, \lambda_2)$. This is a quaternion algebra and is division if L is a field and $\lambda_2 \neq N_L(x)$ for any $x \in L$. If $\lambda_2 = N_L(x)$ for some $x \in L$, then Q is a *split quaternion algebra*, i.e., it is isomorphic to $\mathrm{Mat}_2(F)$. We can repeat the process again with another scalar $\lambda_3 \in F$ to get $O := \mathrm{Cay}(Q, \lambda_3)$, which is an octonion algebra. Octonion algebras are not associative but they are alternative, i.e., $(xx)y = x(xy)$ and $y(xx) = (yx)x$ for all $x, y \in O$. O is a division algebra if Q is division and $\lambda_3 \neq N_Q(q)$ for any $q \in Q$, otherwise it is also called *split*. Each of these algebras is a composition algebra with the quadratic form inherited in the Cayley-Dickson process.

One can repeatedly apply the Cayley-Dickson process to get an infinite sequence of algebras, each twice the dimension of the previous one. However, after applying the process to an octonion algebra, the quadratic form on the resulting algebra no longer permits composition. It is a remarkable fact that *all* composition algebras over a field F of characteristic unequal to 2, can be constructed using the Cayley-Dickson process in this manner and, therefore, composition algebras can only be of dimensions 1,2,4 or 8. For more details on the Cayley-Dickson process and composition algebras, we refer the reader to [30, §33].

2.4 The First Tits Construction

In Jacobson's book [23], the author mentions two constructions for cubic Jordan algebras, communicated to him by Jacques Tits. The so-called first and second Tits constructions can be used to construct all degree-3 Jordan algebras over fields. The first Tits construction can be thought of as analogous to the Cayley-Dickson process and we give a generalisation of it in Chapter

5.

Let F be a field of characteristic not 2. A *Jordan algebra*, J, over F is an algebra with bilinear product denoted $x \bullet y$, satisfying

$$x \bullet y = y \bullet x,$$
$$(x^2 \bullet y) \bullet x = x^2 \bullet (y \bullet x),$$

for all $x, y \in J$. For an associative algebra A over F, we denote by A^+ the algebra which has the same vector-space structure as A, but with new product

$$x \bullet y := \frac{1}{2}(xy + yx),$$

for all $x, y \in A$. This product satisfies the two identities above and, therefore, A^+ is a Jordan algebra.

Any Jordan algebra J, which is a subalgebra of A^+, for some associative algebra A, is called a *special* Jordan algebra, otherwise J is called *exceptional*. It turns out that the only exceptional Jordan algebras are the 27-dimensional Albert algebras. The details of this fact are not relevant to this work, however, for an excellent historical survey and introduction to Jordan algebras we refer the reader to McCrimmon's book [38]. For the purposes of this thesis, the following definition will suffice.

Definition 2.4.1. An *Albert Algebra* is a 27-dimensional, exceptional Jordan algebra.

Albert algebras can be built from certain 9-dimensional, associative cubic algebras via the first Tits construction in a similar manner to how octonion algebras can be built from quaternion algebras via the Cayley-Dickson process.

Definition 2.4.2. Let A be a unital associative algebra over a field F of characteristic not 2 or 3. A *cubic norm form* on A is a map $N_A : A \to F$ such that $N_A(\alpha x) = \alpha^3 N_A(x)$ for all $\alpha \in F$ and $x \in A$, and $N_A(1_A) = 1_F$, where 1_A and 1_F are the units in A and F respectively. We define linearisations

$N_A(x;y)$ of the norm map by the directional derivative

$$N_A(x;y) := \partial_y N_A|_x,$$

in the direction of y, evaluated at x. This map is quadratic in x and linear in y and linearises to the trilinear map

$$N_A(x,y,z) := N_A(x+z;y) - N_A(x;y) - N_A(z;y),$$

for all $x, y, z \in A$. $N_A(x,y,z)$ is symmetric in all three variables.

The main ingredient of the first Tits construction is an associative algebra with a cubic norm form. We also require that the algebra be of degree 3. This definition is as follows.

Definition 2.4.3. Let A be a unital associative algebra with a cubic norm form N_A. We define

$$\begin{aligned} Tr_A(x) &:= N_A(1;x), \\ Tr_A(x,y) &:= T_A(x)T_A(y) - N_A(1,x,y), \\ S_A(x) &:= N_A(x;1), \end{aligned}$$

for all $x, y \in A$. Since $N_A(1) = 1$, we have $Tr_A(1) = S_A(1) = 3$. We also define an *adjoint* map, $\sharp : A \to A$, by

$$x^\sharp := x^2 - Tr_A(x)x + S_A(x)1,$$

for all $x \in A$. We say A is *of degree 3* over F if the following identities hold in all scalar extensions.

$$\begin{aligned} x^3 - Tr_A(x)x^2 + S_A(x) - N_A(x)1 &= 0, \\ Tr_A(x^\sharp, y) &= N_A(x;y), \\ Tr_A(x,y) &= T_A(xy), \end{aligned}$$

for all $x, y \in A$.

As a consequence (see [38, §II.4.5]) these algebras satisfy the *adjoint identity*:

$$(x^\sharp)^\sharp = N_A(x)x.$$

The first Tits Construction can be defined in an explicit manner as follows: let F be a field of characteristic not 2 or 3 and let A be an associative F-algebra of degree 3 with cubic norm form N_A. Pick an invertible scalar $\mu \in F^\times$. Define

$$J(A, \mu) := A \oplus A \oplus A,$$

with multiplication given by

$$\begin{aligned}(x_0, x_1, x_2) \bullet (y_0, y_1, y_2) = (&x_0 \bullet y_0 + \overline{x_1 y_2} + \overline{x_2 y_1}, \\ &\overline{x_0} y_1 + \overline{y_0} x_1 + \mu^{-1}(x_2 \times y_2), \\ &\overline{x_0} y_2 + \overline{y_0} x_2 + \mu(x_1 \times y_1)),\end{aligned} \tag{2.1}$$

where

$$\begin{aligned} x \bullet y &= \frac{1}{2}(xy + yx), \\ \overline{x} &= \frac{1}{2}(Tr_A(x) - x), \end{aligned}$$

and

$$x \times y = x \bullet y - \frac{1}{2} Tr_A(x) y - \frac{1}{2} Tr_A(y) x + \frac{1}{2}(Tr_A(x) Tr_A(y) - Tr_A(x \bullet y)),$$

for all $x, y, x_i, y_i \in A$ ([30, §39] or [42, p. 15]).

The resulting algebra $J = J(A, \mu)$ is a Jordan algebra of dimension $3n$, where $n = \dim_F A$. Given any central simple algebra A of degree 3 and any scalar $\mu \in F^\times$, the first Tits construction $J = J(A, \mu)$ is a 27-dimensional Jordan algebra. It can be shown to be exceptional and, therefore, J is an Albert algebra. For more details on these constructions and their significance in Jordan theory see [23, Ch. IX §12] or [38, §II.4].

2.5 Nonassociative Quaternion Algebras

In this section we will define the construction which was the inspiration for this thesis. Although nonassociative quaternions were studied by Dickson [18] and later by Althoen, Hansen and Kugler [4] over the reals, the first

systematic study of them was by Waterhouse in [56]. Waterhouse gave the following definition of a nonassociative quaternion algebra.

Definition 2.5.1. An *nonassociative quaternion algebra* is a unital, 4-dimensional F-algebra whose nucleus is equal to a quadratic separable field extension L/F.

Starting from this definition, Waterhouse was able to give a more explicit characterisation of these algebras.

Theorem 2.5.2. *Let F be a field and L/F be a quadratic separable field extension of F with non-trivial automorphism σ. Nonassociative quaternion algebras are precisely the algebras which have the vector-space structure*

$$L \oplus Lz,$$

and multiplication defined by

$$(x_0 + x_1 z)(y_0 + y_1 z) = (x_0 y_0 + a x_1 \sigma(y_1)) + (x_0 y_1 + x_1 \sigma(y_0))z, \qquad (2.2)$$

for all $x_i, y_i \in L$ and where $a \in L \setminus F$.

This characterisation is almost identical to the definition of the Cayley-Dickson doubling process for a quadratic separable field extension used to construct an associative quaternion algebra. The only difference here is that the element a in the definition of multiplication belongs to the larger field L, rather than to F. We will thus denote the nonassociative quaternion algebra built from the field extension L/F with multiplication given by (2.2) by $(L/F, \sigma, a)$. For reference we recall the main facts about nonassociative quaternion algebras; all proofs can be found in [56].

Theorem 2.5.3. *Let L/F be a quadratic separable field extension with non-trivial automorphism σ. For all $a \in L \setminus F$, the nonassociative quaternion algebra $(L/F, \sigma, a)$ is a division algebra.*

Theorem 2.5.4. *Let $A = (L/F, \sigma, a)$ and $B = (L'/F, \sigma', b)$ be nonassociative quaternion algebras over F. Then*

(i) $A \cong B$ *only if* $L \cong L'$.

(ii) If $L = L'$ *then* $A \cong B$ *if and only if* $a = N_{L/F}(l)b$ *or* $\sigma(a) = N_{L/F}(l)b$ *for some* $l \in L$. *Every* $l \in L$ *yields a unique isomorphism from* A *to* B *given by*

$$x_0 + x_1 z \mapsto x_0 + x_1 l z \quad \text{or} \quad x_0 + x_1 z \mapsto \sigma(x_0) + \sigma(x_1) l z.$$

Corollary 2.5.5. *Let* $A = (L/F, \sigma, a)$ *be a nonassociative quaternion algebra. For every* $l \in L$ *such that* $N_{L/F}(l) = 1$, *the map*

$$x_0 + x_1 z \mapsto x_0 + x_1 l z$$

is an automorphism of A. *These are the only automorphisms of* A *unless there exists an element* $l' \in L$, *such that* $\sigma(a) = N_{L/F}(l')a$. *In this case the map*

$$x_0 + x_1 z \mapsto \sigma(x_0) + \sigma(x_1) l' z$$

is also an automorphism.

Theorem 2.5.6. *Let* $A = (L/F, \sigma, a)$ *be a nonassociative quaternion algebra. The derivations of* A *consist of all maps of the form*

$$\delta(x_0 + x_1 z) = c x_1 z,$$

where $c \in L$ *is such that* $c + \sigma(c) = 0$.

Chapter 3

Nonassociative Cyclic Algebras

The construction of nonassociative quaternion algebras, mentioned at the end of Chapter 2, has two obvious generalisations. Firstly, since octonion algebras can be constructed using the Cayley-Dickson process in a similar manner to quaternion algebras, one could double an associative quaternion algebra Q but now take the scalar λ, used in the Cayley-Dickson process, to be an element of Q outside of F. This generalisation has been studied by Pumplün in [45] and gives new examples of division algebras, including some over the reals.

On the other hand, quaternion algebras are cyclic algebras of degree 2 so modifying the construction of cyclic algebras given in Chapter 2, Definition 2.2.1, is another possible generalisation of Waterhouse's work. In this chapter we do just that, defining nonassociative cyclic algebras.

3.1 Cubic Nonassociative Cyclic Algebras

Let L/F be a cubic cyclic field extension with Galois group $\{\mathrm{Id}, \sigma, \sigma^2\}$. Pick an element $a \in L \setminus F$ and define the cubic *nonassociative cyclic algebra* $(L/F, \sigma, a)$ to be the 3-dimensional, left L-vector space

$$(L/F, \sigma, a) := L1 \oplus Lz \oplus Lz^2$$

with basis $1, z, z^2$. For two elements $x = x_0+x_1z+x_2z^2$ and $y = y_0+y_1z+y_2z^2$ of $(L/F, \sigma, a)$, their product xy is defined by

$$\begin{aligned} xy = &(x_0y_0 + x_1\sigma(y_2)a + x_2\sigma^2(y_1)a) \\ &+ (x_0y_1 + x_1\sigma(y_0) + x_2\sigma^2(y_2)a)z \\ &+ (x_0y_2 + x_1\sigma(y_1) + x_2\sigma^2(y_0))z^2. \end{aligned}$$

$(L/F, \sigma, a)$ is a nine-dimensional, unital F-algebra with unit 1_L.

Note that from this definition we get

$$zl = \sigma(l)z \text{ for all } l \in L,$$

$$z^2z = a$$

and

$$zz^2 = a.$$

In particular, z^3 is well defined and hence all conditions defining the multiplication in classical cyclic algebras also hold in this setting.

However, this multiplication is not associative, in fact it is not even fourth-power associative. For example

$$(zz^2)z = z^3z = az,$$

but on the other hand

$$z(z^2z) = zz^3 = za = \sigma(a)z.$$

These two expressions are not equal since $\sigma(a) \neq a$.

Proposition 3.1.1. *Let $A = (L/F, \sigma, a)$ be a cubic nonassociative cyclic algebra. Then $Nuc_l(A) = Nuc_r(A) = Nuc_m(A) = L$, hence $Nuc(A) = L$.*

Proof. Here we show $Nuc_r(A) = L$, the other equalities are proved similarly. Let $x = x_0 + x_1z + x_2z^2$ and $y = y_0 + y_1z + y_2z^2$ be elements of A and let $l \in L$. From the definition of multiplication in A we can see

$$\begin{aligned} (xy)l = &(x_0y_0l + x_1\sigma(y_2)al + x_2\sigma^2(y_1)al) \\ &+ (x_0y_1\sigma(l) + x_1\sigma(y_0)\sigma(l) + x_2\sigma^2(y_2)a\sigma(l))z \\ &+ (x_0y_2\sigma^2(l) + x_1\sigma(y_1)\sigma^2(l) + x_2\sigma^2(y_0)\sigma^2(l))z^2, \end{aligned}$$

whereas $yl = y_0l + y_1\sigma(l)z + y_2\sigma^2(l)z^2$, so

$$\begin{aligned} x(yl) = &(x_0y_0l + x_1\sigma(y_2\sigma^2(l))a + x_2\sigma^2(y_1\sigma(l))a) \\ &+ (x_0y_1\sigma(l) + x_1\sigma(y_0l) + x_2\sigma^2(y_2\sigma^2(l))a)z \\ &+ (x_0y_2\sigma^2(l) + x_1\sigma(y_1\sigma(l)) + x_2\sigma^2(y_0l))z^2. \end{aligned}$$

Multiplying out the powers of σ shows that $(xy)l = x(yl)$ for all $x, y \in A$ and $l \in L$. Hence $L \subseteq Nuc_r(A)$.

Conversely, suppose that $x = x_0 + x_1z + x_2z^2 \in Nuc_r(A)$. Then we should have $(zz^2)x = z(z^2x)$, however

$$(zz^2)x = ax = ax_0 + ax_1z + ax_2z^2,$$

whereas

$$\begin{aligned} z(z^2x) &= z(\sigma^2(x_0)z^2 + \sigma^2(x_1)a + \sigma^2(x_2)az \\ &= x_0a + x_1\sigma(a)z + x_2\sigma(a)z^2. \end{aligned}$$

If we compare coefficients we see that these two expressions can only be equal if $x_1 = x_2 = 0$ since $a \neq \sigma(a)$. In other words $x = x_0 \in L$. Hence $Nuc_r(A) \subseteq L$ and so $Nuc_r(A) = L$.

□

Proposition 3.1.2. *Let $A = (L/F, \sigma, a)$ be a cubic nonassociative cyclic algebra, then $Comm(A) = F$. Hence $Z(A) = F$.*

Proof. Let $x = x_0 + x_1z + x_2z^2 \in A$ and let $k \in F$. Then

$$\begin{aligned} xk &= x_0k + x_1\sigma(k)z + x_2\sigma^2(k)z^2 \\ &= kx_0 + kx_1z + kx_2z^2 = kx \end{aligned}$$

since $\sigma(k) = k$ for all $k \in F$. Therefore $F \subseteq Comm(A)$.

Conversely, suppose $x \in Comm(A)$ and let $l \in L \setminus F$ be nonzero. We should have $xl = lx$, however,

$$lx = lx_0 + lx_1z + lx_2z^2,$$

whereas

$$xl = x_0 l + x_1 \sigma(l) z + x_2 \sigma^2(l) z^2.$$

For the same reasons as in the proof of the previous proposition, this shows that $x_1 = x_2 = 0$ and hence $x = x_0 \in L$. Moreover, we should also have $x_0 z = z x_0 = \sigma(x_0) z$, but this is true if and only if $x_0 \in F$. Therefore $Comm(A) \subseteq F$ so we get the first claim. The center of A, being the intersection of $Comm(A)$ and $Nuc(A)$, is also F. □

Our main result is the following:

Theorem 3.1.3. *For any $a \in L \setminus F$ the cubic nonassociative cyclic algebra $(L/F, \sigma, a)$ is a division algebra.*

Proof. Write an element $x_0 + x_1 z + x_2 z^2 \in (L/F, \sigma, a)$, with $x_i \in L$, as (x_0, x_1, x_2). Then it is easy to see that the multiplication $(x_0, x_1, x_2)(y_0, y_1, y_2)$ can be described by

$$(x_0, x_1, x_2) \begin{pmatrix} y_0 & y_1 & y_2 \\ a\sigma(y_2) & \sigma(y_0) & \sigma(y_1) \\ a\sigma^2(y_1) & a\sigma^2(y_2) & \sigma^2(y_0) \end{pmatrix},$$

where this product is ordinary matrix multiplication. Denote the 3×3 matrix given above by R_y where y is the element (y_0, y_1, y_2).

Suppose

$$xy = (x_0, x_1, x_2)(y_0, y_1, y_2) = 0$$

for some nonzero x and y in $(L/F, \sigma, a)$, i.e.

$$(x_0, x_1, x_2) \begin{pmatrix} y_0 & y_1 & y_2 \\ a\sigma(y_2) & \sigma(y_0) & \sigma(y_1) \\ a\sigma^2(y_1) & a\sigma^2(y_2) & \sigma^2(y_0) \end{pmatrix} = (0, 0, 0).$$

Elementary linear algebra tells us that if $\mathrm{Det}(R_y) \neq 0$ then this implies $x_0 = x_1 = x_2 = 0$. Now

$$\mathrm{Det}(R_y) = N_{L/F}(y_0) + a N_{L/F}(y_1) + a^2 N_{L/F}(y_2) - a Tr_{L/F}(y_0 \sigma(y_1) \sigma^2(y_2)),$$

where $N_{L/F}$ and $Tr_{L/F}$ are the field norm and trace, respectively. The elements $1, a$ and a^2 are linearly independent over F and all norms and traces belong to F, so if $\mathrm{Det}(R_y) = 0$ then $N_{L/F}(y_0) = N_{L/F}(y_2) = 0$. This implies that $y_0 = y_2 = 0$ since field norms are anisotropic. In turn, this gives $y_1 = 0$ and so $y = 0$. We conclude that $(L/F, \sigma, a)$ contains no zero divisors.

□

We can also classify these algebras up to isomorphism.

Proposition 3.1.4. *Let $A = (L/F, \sigma, a) = L \oplus Lz \oplus Lz^2$ and $B = (L'/F, \sigma', b)$ $= L' \oplus L'u \oplus L'u^2$ be cubic nonassociative cyclic algebras over F. Then*

(i) $A \cong B$ only if $L \cong L'$.

(ii) If $L = L'$ then $A \cong B$ if and only if $\sigma^i(a) = N_{L/F}(l)b$ for some $i \in \{0, 1, 2\}$ and $l \in L$. Every $l \in L$ yields a unique isomorphism from A to B given by

$$(x_0 + x_1 z + x_2 z^2) \mapsto (\sigma^i(x_0) + \sigma^i(x_1) lu + \sigma^i(x_2) l\sigma(l) u^2).$$

Proof. The first claim is clear since any isomorphism must preserve the nucleus. For (ii), let $f : A \to B$ be an isomorphism. We must have $f(L) = L$ so $f|_L$ is an F-automorphism and hence $f|_L \in \{\mathrm{Id}, \sigma, \sigma^2\}$. Suppose that $f|_L = \sigma^i$ for $i \in \{0, 1, 2\}$, and $f(z) = l_0 + l_1 u + l_2 u^2$ for some $l_i \in L$. Then, for every $m \in L$, we have

$$f(z)f(m) = l_0\sigma^i(m) + l_1\sigma^{i+1}(m)u + l_2\sigma^{i+2}(m)u^2,$$

where the indices of σ are read modulo 3. Also we get

$$\begin{aligned} f(zm) &= f(\sigma(m)z) \\ &= \sigma^{i+1}(m)l_0 + \sigma^{i+1}(m)l_1 u + \sigma^{i+1}(m)l_2 u^2, \end{aligned}$$

where indices are read modulo 3 as well. Comparing coefficients we see that $f(z)f(m) = f(zm)$ for all $m \in L$ if and only if $l_0 = l_2 = 0$. Hence $f(z) = lz$ for some $l \in L$. Finally, we get that

$$\sigma^i(a) = f(a) = f(z^3) = (lu)^3 = l\sigma(l)\sigma^2(l)u^3 = N_{L/F}(l)b.$$

For ease of notation when showing these maps give isomorphisms we will assume $f|_L = \mathrm{Id}$ so $f(x_0 + x_1 z + x_2 z^2) = (x_0 + x_1 lu + x_2 l\sigma(l)u^2)$. The other maps are exactly the same except with the appropriate power of σ inserted. It is clear that such maps are bijective and F-linear. Suppose $x = x_0 + x_1 z + x_2 z^2$ and $y = y_0 + y_1 z + y_2 z^2$ are elements of A. Then using the definition of the multiplication we have

$$\begin{aligned} f(xy) = &(x_0y_0 + x_1\sigma(y_2)a + x_2\sigma^2(y_1)a) \\ &+ (x_0y_1 + x_1\sigma(y_0) + x_2\sigma^2(y_2)a)lu \\ &+ (x_0y_2 + x_1\sigma(y_1) + x_2\sigma^2(y_0))l\sigma(l)u^2. \end{aligned}$$

Similarly, we calculate

$$\begin{aligned} f(x)f(y) &= (x_0 + x_1lu + x_2l\sigma(l)u^2)(y_0 + y_1lu + y_2l\sigma(l)u^2) \\ &= (x_0y_0 + x_1l\sigma(y_2)\sigma(l)\sigma^2(l)b + x_2l\sigma(l)\sigma^2(y_1)\sigma^2(l)b) \\ &+ (x_0y_1l + x_1l\sigma(y_0) + x_2l\sigma(l)\sigma^2(y_2)\sigma^2(l)lb)u \\ &+ (x_0y_2l\sigma(l) + x_1l\sigma(y_1)\sigma(l) + x_2l\sigma(l)\sigma^2(y_0))u^2 \\ &= (x_0y_0 + x_1\sigma(y_2)N_{L/F}(l)b + x_2\sigma^2(y_1)N_{L/F}(l)b) \\ &+ (x_0y_1 + x_1\sigma(y_0) + x_2\sigma^2(y_2)N_{L/F}(l)b)lu \\ &+ (x_0y_2 + x_1\sigma(y_1) + x_2\sigma^2(y_0))l\sigma(l)u^2. \end{aligned}$$

Hence $f(xy) = f(x)f(y)$ since $a = N_{L/F}(l)b$. □

Corollary 3.1.5. *Let $A = (L/F, \sigma, a)$ be a cubic nonassociative cyclic algebra. For every $l \in L$ such that $N_{L/F}(l) = 1$, the map*

$$(x_0 + x_1 z + x_2 z^2) \mapsto (x_0 + x_1 lz + x_2 l\sigma(l)z^2)$$

is an automorphism of A. These are the only automorphisms of A unless there exists an element $l' \in L$, such that $\sigma^i(a) = N_{L/F}(l')a$ for $i = 1$ or 2. In this case the map

$$(x_0 + x_1 z + x_2 z^2) \mapsto (\sigma^i(x_0) + \sigma^i(x_1)l'z + \sigma^i(x_2)l'\sigma(l')z^2)$$

is also an automorphism.

Proof. An automorphism f of A can have three possible actions on the field L; either $f|_L = \mathrm{Id}$, $f|_L = \sigma$ or $f|_L = \sigma^2$. If $f|_L = \mathrm{Id}$, then by Proposition 3.1.4, $a = N_{L/F}(l)a$ for some $l \in L$, whence $N_{L/F}(l) = 1$. If $f|_L$ is either of the other two possibilities then Proposition 3.1.4 again gives the required condition. □

Corollary 3.1.6. *Consider $N_{L/F}$ as a group homomorphism from $L^\times$ to $F^\times$. Then $\mathrm{Ker}(N_{L/K})$ is isomorphic to a subgroup of the automorphism group of $(L/F, \sigma, a)$.*

Recall that a derivation of an F-algebra A is an F-linear map δ which satisfies the Leibniz rule:

$$\delta(xy) = \delta(x)y + x\delta(y),$$

for all $x, y \in A$. If A is an associative algebra then for any $c \in A$, the map

$$\delta_c : x \mapsto cx - xc,$$

for all $x \in A$, is a derivation. The set of all such maps forms an important subclass of derivations of A known as *inner derivations*. If A is not associative then the map δ_c is not necessarily a derivation. However, the following lemma shows one case in which it is.

Lemma 3.1.7. *Let A be a nonassociative F-algebra and suppose that $c \in Nuc(A)$. The map δ_c is a derivation of A.*

Proof. For $x, y \in A$, we have

$$\begin{aligned}
\delta_c(xy) &= c(xy) - (xy)c \\
&= (cx)y - x(yc) \\
&= (cx)y - (xc)y + x(cy) - x(yc) \\
&= \delta_c(x)y + x\delta_c(y),
\end{aligned}$$

as required. □

Theorem 3.1.8. *Let $A = (L/F, \sigma, a)$ be a cubic nonassociative cyclic algebra and let $c \in L$. The map*

$$x_0 + x_1 z + x_2 z^2 \mapsto (c - \sigma(c))x_1 z + (c - \sigma^2(c))x_2 z^2$$

is a derivation of A. If F is not of characteristic 2, these are all the derivations.

Proof. It is easy to see that

$$x_0 + x_1 z + x_2 z^2 \mapsto (c - \sigma(c))x_1 z + (c - \sigma^2(c))x_2 z^2$$

is simply the map $\delta_c(x) = cx - xc$ which is a derivation for this algebra by the previous lemma. For the second claim, suppose char$F \neq 2$. Let $A = (L/F, \sigma, a)$ be a cubic nonassociative cyclic algebra and let δ be a derivation of A. Suppose that $\delta(l) = l_0 + l_1 z + l_2 z^2$ for every $l \in L$. We claim that $l_0 = 0$: suppose also that $\delta(m) = m_0 + m_1 z + m_2 z^2$. Then consider the map δ' sending each $l \in L$ to the first component of $\delta(l)$, i.e., l_0 in this case. Then

$$\begin{aligned}\delta(lm) &= l\delta(m) + \delta(l)m \\ &= lm_0 + lm_1 z + lm_2 z^2 + l_0 m + l_1 \sigma(m) z + l_2 \sigma^2(m) z^2.\end{aligned}$$

Hence

$$\delta'(lm) = lm_0 + l_0 m = l\delta'(m) + \delta'(l)m.$$

So δ' is an F-derivation of the separable F-algebra L. It is known that all derivations of separable algebras are inner ([21]) and since L is a commutative algebra this means that δ' must be zero. So

$$\delta(l) = l_1 z + l_2 z^2, \tag{3.1}$$

for all $l \in L$. Now let

$$\delta(a) = sz + tz^2 \tag{3.2}$$

and suppose that

$$\delta(z) = u + vz + wz^2. \tag{3.3}$$

Then $\delta(z^2) = z\delta(z) + \delta(z)z$ and we get

$$\delta(z^2) = (w + \sigma(w))a + (u + \sigma(u))z + (v + \sigma(v))z^2. \tag{3.4}$$

In A we have $a = z^3 = z^2z = zz^2$, so again using the Leibniz property of derivations: $\delta(z^2z) = z^2\delta(z) + \delta(z^2)z$ and $\delta(zz^2) = z\delta(z^2) + \delta(z)z^2$, we obtain

$$\begin{aligned}\delta(z^2z) =&(v + \sigma(v) + \sigma^2(v))a + (w + \sigma(w) + \sigma^2(w))az \\ &+ (u + \sigma(u) + \sigma^2(u))z^2,\end{aligned} \tag{3.5}$$

whereas

$$\begin{aligned}\delta(zz^2) =&(v + \sigma(v) + \sigma^2(v))a + (wa + (\sigma(w) + \sigma^2(w))\sigma(a))z \\ &+ (u + \sigma(u) + \sigma^2(u))z^2.\end{aligned} \tag{3.6}$$

Comparing the z terms of (3.5) and (3.6) gives

$$wa + (\sigma(w) + \sigma^2(w))a = wa + (\sigma(w) + \sigma^2(w))\sigma(a).$$

Since $a \neq \sigma(a)$, this implies $\sigma(w) + \sigma^2(w) = 0$. Applying $N_{L/F}$ we get that $N_{L/F}(w) = -N_{L/F}(w)$ and, since F has characteristic unequal to 2, we must have $w = 0$. If Tr denotes the field trace from L to F, then comparing with (3.2) shows that $s = 0$ and $Tr(v)a = 0$, which means $Tr(v) = 0$. Comparing the z^2 terms of (3.2) and (3.5) tells us that $t = Tr(u)$, therefore we have the identities

$$\begin{aligned}\delta(a) &= tz^2 = Tr(u)z^2, \\ \delta(z) &= u + vz, \\ \delta(z^2) &= (u + \sigma(u))z + (v + \sigma(v))z^2.\end{aligned}$$

Using these simplifications we calculate

$$\delta(az) = a(u + Tr(u)) + avz. \tag{3.7}$$

Then, using this and the fact $\delta((az)z^2) = az\delta(z^2) + \delta(az)z^2$, yields

$$\delta((az)z^2) = a^2(Tr(v)) + (aTr(u) + aTr(u))z^2. \tag{3.8}$$

On the other hand, we know $\delta((az)z^2) = \delta(a(zz^2)) = \delta(aa) = a\delta(a) + \delta(a)a$, so

$$\delta((az)z^2) = \delta(aa) = (aTr(u) + \sigma^2(a)Tr(u))z^2. \tag{3.9}$$

Comparing the z^2 term of (3.8) and (3.9) shows that $aTr(u) = \sigma^2(a)Tr(u)$, which implies that $Tr(u) = 0$ and hence $\delta(a) = Tr(u)z^2 = 0$. Now $\delta(a) = 0$ implies that $\delta(l) = 0$ for all $l \in L$, since by (3.1) we may assume $\delta(l) = l_1 z + l_2 z^2$. Consider

$$\delta(al) = \delta(a)l + a\delta(l) = 0 + al_1 z + al_2 z^2$$

whereas

$$\delta(la) = \delta(l)a + l\delta(a) = l_1\sigma(a)z + l_2\sigma^2(a)z^2 + 0.$$

Since a and l commute, these should be equal, thus $l_1 = l_2 = 0$ so $\delta(l) = 0$ for all $l \in L$. In particular, $\delta(\sigma(a)) = 0$. Then

$$\delta(za) = \delta(z)a + z\delta(a) = ua + v\sigma(a)z + 0,$$

however,

$$\delta(\sigma(a)z) = \delta(\sigma(a))z + \sigma(a)\delta(z) = 0 + \sigma(a)u + \sigma(a)vz.$$

Comparing terms shows us that $u = 0$ and we conclude $\delta(z) = vz$ and $\delta(z^2) = (v + \sigma(v))z^2$. Hence

$$\delta(x_0 + x_1 z + x_2 z^2) = x_1 vz + x_2(v + \sigma(v))z^2.$$

Finally, to see that this map is of the form described in the theorem recall that any v of trace zero is of the form $c - \sigma(c)$ for some $c \in L$, then

$$v + \sigma(v) = c - \sigma(c) + \sigma(c) - \sigma^2(c) = c - \sigma^2(c)$$

as required. □

3.2 General Nonassociative Cyclic Algebras

A natural generalisation for the above construction is to consider cyclic field extensions of higher degree and define a nonassociative cyclic algebra of degree n. Let L/F be a cyclic field extension of degree n with Galois group generated by the automorphism σ. Pick an element $a \in L \setminus F$ and define $(L/F, \sigma, a)$ to be the n-dimensional left L-vector space

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

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

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

and then extend it linearly to all of $(L/F, \sigma, a)$. We say that the above algebra is a *nonassociative cyclic algebra of degree* n.

Remarks 3.2.1. (i) The definition of the multiplication implies that

$$zl = \sigma(l)z$$

for all $l \in L$. Moreover, for all i, j such that $i + j = n$, we have

$$z^i z^j = a.$$

Putting $z^n := a$ gives us the two conditions which define the multiplication in the classical case.

(ii) When $n = 2$ this construction is simply that of a nonassociative quaternion algebra and when $n = 3$ the definition is the same as in the cubic case from the previous section.

(iii) A nonassociative cyclic algebra of degree n is not $(n+1)$th power associative since $(z^{n-1}z)z = az$ and $z(z^{n-1}z) = za = \sigma(a)z$, which are not equal since $a \in L \setminus F$.

(iv) 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.

Let $A := (L/F, \sigma, a)$ be a nonassociative cyclic algebra of degree n. The calculation of the nuclei is slightly different than in the cubic case and, in fact, the size of the left nucleus depends on whether a belongs to a proper subfield of L or not.

Proposition 3.2.2. *For any $a \in L \setminus F$, $Nuc_r(A) = Nuc_m(A) = L$.*

Proof. We begin with $Nuc_r(A)$. By the distributivity of the multiplication in A is is enough to check associativity for elements xz^i and yz^j and l where x, y and $l \in L$ and $0 \leq i, j \leq n-1$. We have

$$((xz^i)(yz^j))l = \begin{cases} x\sigma^i(y)\sigma^{i+j}(l)z^{i+j} & \text{if } i+j < n \\ x\sigma^i(y)a\sigma^{(i+j)-n}(l)z^{(i+j)-n} & \text{if } i+j \geq n, \end{cases}$$

whereas

$$(xz^i)((yz^j)l) = (xz^i)(y\sigma^j(l)z^j) = \begin{cases} x\sigma^i(y)\sigma^{i+j}(l)z^{i+j} & \text{if } i+j < n \\ x\sigma^i(y)\sigma^{(i+j)-n}(l)az^{(i+j)-n} & \text{if } i+j \geq n. \end{cases}$$

These are both equal so $L \subseteq Nuc_r(A)$.

Conversely, let $w = \sum_{i=0}^{n-1} w_i z^i$ be an element of the right nucleus and suppose that $w_k \neq 0$ for some $k \geq 1$. Then the z^kth term of the associator $[z, z^{n-1}, w]$ is

$$\begin{aligned}(zz^{n-1})w_kz^k - z(z^{n-1}w_kz^k) &= aw_kz^k - z(\sigma^{n-1}(w_k)a)z^{k-1} \\ &= (aw_k - w_k\sigma(a))z^k,\end{aligned}$$

which is nonzero since $\sigma(a) \neq a$ for all $a \in L \setminus F$. Hence we must have $w_i = 0$ for all $1 \leq i \leq n-1$. Therefore $w = w_0 \in L$.

For the middle nucleus we again consider elements xz^i and yz^j in A and $l \in L$ where $0 \leq i, j \leq n-1$. We have

$$((xz^i)l)(yz^j) = (x\sigma^i(l)z^i)(yz^j) = \begin{cases} (x\sigma^i(l)\sigma^i(y)z^{i+j}) = & \text{if } i+j < n \\ x\sigma^i(l)\sigma^i(y)az^{(i+j)-n} & \text{if } i+j \geq n. \end{cases}$$

whereas

$$(xz^i)(l(yz^j)) = (xz^i)(lyz^j) = \begin{cases} x\sigma^i(ly)z^{i+j} & \text{if } i+j < n \\ x\sigma^i(ly)az^{(i+j)-n} & \text{if } i+j \geq n. \end{cases}$$

These are both equal so $L \subseteq Nuc_m(A)$.

Conversely, let $w = \sum_{i=0}^{n-1} w_i z^i$ be an element of the middle nucleus and suppose that $w_k \neq 0$ for some $k \geq 1$. If $k \neq n-1$ then the z term of the associator $[z, w, z^{n-k}]$ will be

$$\begin{aligned}(zw_kz^k)z^{n-k} - z(w_kz^kz^{n-k}) &= (\sigma(w_k)z^{k+1})z^{n-k} - z(w_ka) \\ &= \sigma(w_k)az - \sigma(w_k)\sigma(a)z.\end{aligned}$$

On the other hand, if $k = n-1$ then the z term of the associator $[z, w, z^{n-k}] = [z, w, z]$ will be

$$\begin{aligned}(zw_{n-1}z^{n-1})z - z(w_{n-1}z^{n-1}z) &= (\sigma(w_{n-1})a)z - z(w_{n-1}a) \\ &= \sigma(w_{n-1})az - \sigma(w_{n-1})\sigma(a)z.\end{aligned}$$

In either case this will be nonzero since $\sigma(a) \neq a$ for all $a \in L \setminus F$. Hence we must have $w_i = 0$ for all $1 \leq i \leq n-1$. Therefore $w = w_0 \in L$. □

The left nucleus of a nonassociative cyclic algebra depends on the choice of $a \in L \setminus F$. Recall that by the definition of $(L/F, \sigma, a)$ we cannot have $a \in F$. However, a may belong to some proper subfield $E \subset L$. In this case there exists a proper subgroup G_E of $Gal(L/F)$ such that for all $\tau \in G_E$ we have $\tau(a) = a$. Since $Gal(L/F)$ is a cyclic group, the subgroup G_E is generated by some power of the generator of $Gal(L/F)$. If the generator of $Gal(L/F)$ is σ then denote the generator of G_E by σ^s where $2 \leq s \leq n-1$.

Proposition 3.2.3. *Let $A = (L/F, \sigma, a)$ then*

$$Nuc_l(A) = L \oplus Lz^s \oplus Lz^{2s} \oplus \cdots \oplus Lz^{n-s}$$

where s is such that a is invariant under the subgroup $\langle \sigma^s \rangle$ of $Gal(L/F)$, i.e., $\sigma^{ks}(a) = a$ for all $k \in \mathbb{Z}$.

Proof. Again we check associativity for elements wz^m, xz^i and yz^j where $m = ks$, so $\sigma^m(a) = a$, and $0 \leq m, i, j \leq n-1$. We have

$$wz^m((xz^i)(yz^j)) = \begin{cases} wz^m(x\sigma^i(y)z^{i+j}) & \text{if } i+j < n \\ wz^m(x\sigma^i(y)az^{(i+j)-n}) & \text{if } i+j \geq n \end{cases}$$

$$= \begin{cases} w\sigma^m(x)\sigma^{i+m}(y)z^{i+j+m} & \text{if } i+j+m < n \\ w\sigma^m(x)\sigma^{i+m}(y)az^{(i+j+m)-n} & \text{if } n \leq i+j+m < 2n \\ w\sigma^m(x)\sigma^{i+m}(y)a^2z^{(i+j+m)-2n} & \text{if } i+j+m \geq 2n, \end{cases}$$

whereas

$$((wz^m)(xz^i))(yz^j) = \begin{cases} (w\sigma^m(x)z^{m+i})yz^j) & \text{if } m+i < n \\ (w\sigma^m(x)az^{(m+i)-n})yz^j) & \text{if } m+i \geq n \end{cases}$$

$$= \begin{cases} w\sigma^m(x)\sigma^{m+i}(y)z^{i+j+m} & \text{if } i+j+m < n \\ w\sigma^m(x)\sigma^{m+i}(y)az^{(i+j+m)-n} & \text{if } n \leq i+j+m < 2n \\ w\sigma^m(x)\sigma^{m+i}(y)a^2z^{(i+j+m)-2n} & \text{if } i+j+m \geq 2n. \end{cases}$$

In any of the cases these terms are equal, so we have the inclusion

$$L \oplus Lz^s \oplus Lz^{2s} \oplus \cdots \oplus Lz^{n-s} \subseteq Nuc_l(A).$$

Conversely, let $w = \sum_{i=0}^{n-1} w_i z^i$ be an element of the left nucleus and suppose that $w_k \neq 0$ for some k which is not a multiple of s. Then we have $\sigma^k(a) \neq a$. The z^k term of the associator $[w, z^{n-k}, z^k]$ is

$$\begin{aligned}((w_kz^k)z^{n-k})z^k - w_kz^k(z^kz^{n-k}) &= w_kaz^k - w_kz^k(a) \\ &= w_kaz^k - w_k\sigma^k(a)z^k\end{aligned}$$

which is not zero since $\sigma^k(a) \neq a$. Thus the left nucleus of A contains only the terms mentioned in the proposition. □

Corollary 3.2.4. *Let $A = (L/F, \sigma, a)$ and suppose that a belongs to no proper subfield of L. Then $Nuc_l(A) = L$.*

Proof. Since a belongs to no proper subfield of L, the subgroup G of $Gal(L/F)$ such that $\tau(a) = a$ for all $\tau \in G$ is trivial. The result now follows from above. □

Corollary 3.2.5. *Let $A = (L/F, \sigma, a)$ where L/F is a cyclic field extension of prime degree. Then $Nuc_l(A) = L$.*

Proof. Since L/F is prime, there are no proper intermediate subfields of L and F. □

Corollary 3.2.6. *For all $a \in L \setminus F$, $Nuc((L/F, \sigma, a)) = L$.*

Proof. The nucleus is the intersection of the left, middle and right nuclei so, by the above propositions, it is always equal to L. □

Similarly, we can calculate the centre of a nonassociative cyclic algebra of degree n.

Proposition 3.2.7. *Let A be a nonassociative cyclic algebra $(L/F, \sigma, a)$ of degree n. Then $Comm(A) = F$ and hence $Z(A) = F$.*

Proof. Since $\sigma(k) = k$ for all $k \in F$, we have

$$(\sum_{i=0}^{n-1} x_i z^i)k = (\sum_{i=0}^{n-1} x_i \sigma^i(k) z^i) = (\sum_{i=0}^{n-1} x_i k z^i) = k(\sum_{i=0}^{n-1} x_i z^i),$$

i.e., $xk = kx$ for all $x \in A$ and $k \in F$. Therefore $F \subseteq Comm(A)$. For the reverse inclusion, pick an element $l \in L$ which does not belong to any intermediate field extensions of L and F. Then $\sigma^i(l) \neq l$ for all $1 \leq i \leq n-1$. Suppose $x = \sum_{i=0}^{n-1} x_i z^i \in Comm(A)$. Then we have

$$lx = \sum_{i=0}^{n-1} l x_i z^i,$$

whereas

$$xl = \sum_{i=0}^{n-1} x_i \sigma^i(l) z^i.$$

These are equal if and only if $x_i = 0$ for all $1 \leq i \leq n-1$ so $x = x_0 \in L$. Moreover, we must have

$$xz = x_0 z = z x_0 = \sigma(x_0) z$$

but this can only happen if $x_0 \in F$. Hence $Comm(A) = F$. □

We also can determine when two nonassociative cyclic algebras are isomorphic. Recall that the field norm, $N_{L/F} : L \to F$, in the case of cyclic field extensions of degree n is given by $N_{L/F}(l) = \Pi_{i=0}^{n-1} \sigma(l)$.

Proposition 3.2.8. *Let $A = (L/F, \sigma, a)$ and $B = (L'/F, \sigma', b)$ be nonassociative cyclic algebras over F. Then*

(i) $A \cong B$ only if $L \cong L'$.

(ii) If $L = L'$ then $A \cong B$ if and only if $\sigma^i(a) = N_{L/F}(l)b$ for some $l \in L$ and $0 \leq i < n$ and . Every $l \in L$ yields a unique isomorphism from A to B given by

$$\sum_{j=0}^{n-1} x_j z^j \mapsto \sum_{j=0}^{n-1} \sigma^i(x_j) l \ldots \sigma^{j-1}(l) u^j.$$

Proof. Part (i) is clear since isomorphisms preserve the nucleus. For (ii), let $A = \bigoplus_{i=0}^{n-1} L z^i$ and $B = \bigoplus_{i=0}^{n-1} L u^i$ and suppose $f : A \to B$ is an isomorphism. First note that f must map the subspace Lz^0 isomorphically to the subspace Lu^0 since it must preserve the nucleus. Hence $f|_L$ is an F-automorphism so it is of the form σ^i for some $0 \leq i < n$. Also the subspace Lz is mapped to the subspace Lu since suppose $f(z) = \sum_{j=0}^{n-1} l_j u^i$, then

$$f(zm) = f(\sigma(m)z) = \sigma^{i+1}(m) \sum_{j=0}^{n-1} l_j u^j,$$

whereas

$$f(z)f(m) = (\sum_{j=0}^{n-1} l_j u^j)\sigma^i(m) = \sum_{j=0}^{n-1} l_j \sigma^{i+j}(m) u^j,$$

for all $m \in L$. However, these two expressions are only equal whenever $j = 1$, so $l_j = 0$ for all $j \neq 1$ in order for equality to hold. Hence $f(z) = lu$ for some $l \in L$. Finally, we see that

$$\sigma^i(a) = f(a) = f(z^n) = (lz)^n = l\sigma(l)\dots\sigma^{n-1}(l)u^n = N_{L/F}(l)b$$

as required.

Conversely, it is easy to check that if $\sigma^i(a) = N_{L/F}(l)b$, then the map

$$f : \sum_{j=0}^{n-1} x_j z^j \mapsto \sum_{j=0}^{n-1} \sigma^i(x_j) l \dots \sigma^{j-1}(l) u^j,$$

is an isomorphism from A to B. To show this we assume $f|_L = \mathrm{Id}$ (as the other cases are similar). We show that multiplication is preserved for monomials xz^j and yz^j since general elements are sums of these monomials and f is clearly linear. We have

$$\begin{aligned} f(xz^i)f(yz^j) &= (xl\dots\sigma^{i-1}(l)u^i)(yl\dots\sigma^{j-1}(l)u^j) \\ &= xl\dots\sigma^{i-1}(l)\sigma^i(y)\sigma^i(l)\dots\sigma^{i+j-1}(l)u^{i+j}, \end{aligned}$$

if $i + j < n$, or

$$x\sigma^i(y)N_{L/F}(l)l\sigma(l)\dots\sigma^{i+j-n-1}(l)bu^{i+j-n},$$

if $i + j \geq n$. On the other hand

$$\begin{aligned} f(xz^iyz^j) &= f(x\sigma^i(y)z^{i+j}) \\ &= x\sigma^i(y)l\dots\sigma^{i+j-1}(l)u^{i+j} \end{aligned}$$

if $i + j < n$. If $i + j \geq n$ then

$$\begin{aligned} f(xz^iyz^j) &= f(x\sigma^i(y)az^{i+j-n}) \\ &= x\sigma^i(y)al\dots\sigma^{i+j-n-1}(l)u^{i+j-n}. \end{aligned}$$

In either case, since $a = N_{L/F}(l)b$, products are preserved by f so it is an isomorphism. □

Corollary 3.2.9. *Let $A = (L/F, \sigma, a)$ be a nonassociative cyclic algebra of degree n. For all $l \in L$ such that $N_{L/F}(l) = 1$, the map*

$$\sum_{i=0}^{n-1} x_i z^i \mapsto \sum_{i=0}^{n-1} x_i l\sigma(l) \dots \sigma^{i-1}(l) z^i,$$

is an automorphism of A. These maps are the only automorphisms of A unless there exists an element $l' \in L$ such that $\sigma^i(a) = N_{L/F}(l')a$ for some $i = 1, \dots, n-1$.

The proof is exactly the same as in the cubic case (Corollary 3.1.5). Again this corollary implies that the kernel of the norm map is isomorphic to a subgroup of $Aut(L/F, \sigma, a)$.

Theorem 3.2.10. *Let $A = (L/F, \sigma, a)$ be a nonassociative cyclic algebra of degree n. If the elements $1, a, \dots, a^{n-1}$ are linearly independent over F, then A is a division algebra.*

Proof. We write an element $x_0 + x_1 z + \cdots + x_{n-1} z^{n-1} \in A$ as the n-tuple $(x_0, x_1, \dots, x_{n-1})$. The multiplication of elements $(x_0, \dots, x_{n-1})$ and $(y_0, \dots, y_{n-1})$ in A is given by the matrix multiplication

$$(x_0, \dots, x_{n-1}) \begin{pmatrix} y_0 & y_1 & y_2 & \cdots & y_{n-1} \\ a\sigma(y_{n-1}) & \sigma(y_0) & \sigma(y_1) & \cdots & \sigma(y_{n-2}) \\ a\sigma^2(y_{n-2}) & a\sigma^2(y_{n-1}) & \sigma^2(y_0) & \cdots & \sigma^2(y_{n-3}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a\sigma^{n-1}(y_1) & a\sigma^{n-1}(y_2) & a\sigma^{n-1}(y_3) & \cdots & \sigma^{n-1}(y_0) \end{pmatrix}.$$

Now the proof follows the same argument as in Theorem 3.1.3. Suppose that

$$(x_0, \dots, x_{n-1})(y_0, \dots, y_{n-1}) = (0, \dots, 0)$$

in A. Denoting the above $n \times n$ matrix by R_y, we see that if $\mathrm{Det}(R_y)$ is non zero then the only solution is $(x_0, \dots, x_{n-1}) = (0, \dots, 0)$. It is a well-known fact that if we were to replace the element a in R_y by an element $a' \in F$ then the determinant would also be an element of F. It follows that the

determinant of R_y is a polynomial in a with coefficients in F. It is easy to see that the highest power of a in the determinant is $n-1$, in fact, the coefficient of a^{n-1} will be $\pm N_{L/F}(y_{n-1})$. Since $1, a, \ldots, a^{n-1}$ are linearly independent, it follows that if the determinant of this matrix is zero then all coefficients of a in the determinant must be zero. In particular, $N_{L/F}(y_{n-1}) = 0$ since this is the only coefficient of the a^{n-1} term. It is also easy to check that the only constant term (i.e., without a power of a) will be the product of the elements on the main diagonal of the matrix, which is $N_{L/F}(y_0)$. Since the norm is an anisotropic form, this implies y_0 and y_{n-1} are both zero. Hence, if $\mathrm{Det}(R_y) = 0$, we have

$$R_y = \begin{pmatrix} 0 & y_1 & y_2 & \cdots & 0 \\ 0 & 0 & \sigma(y_1) & \cdots & \sigma(y_{n-2}) \\ a\sigma^2(y_{n-2}) & 0 & 0 & \cdots & \sigma^2(y_{n-3}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a\sigma^{n-1}(y_1) & a\sigma^{n-1}(y_2) & a\sigma^{n-1}(y_3) & \cdots & 0 \end{pmatrix}.$$

The only remaining coefficient for a^{n-2} must be $\pm N_{L/F}(y_{n-2})$, so, by the linear independence of the a^i, this must also be zero, which means y_{n-2} is zero. If we continue in this manner, calculating the coefficients of the a^i, we get that $N_{L/F}(y_i) = 0$ for all i which, in turn, implies that $y_i = 0$ for each i. Hence $\mathrm{Det}(R_y) = 0$ if and only if $(y_0, \ldots, y_{n-1}) = (0, \ldots, 0)$ and so A contains no nontrivial zero divisors. □

Corollary 3.2.11. *Let $A = (L/F, \sigma, a)$ be a nonassociative cyclic algebra of prime degree p. Then A is a division algebra.*

Proof. Consider the proper field extension $F(a)$, we have that

$$[L : F] = [L : F(a)][F(a) : F].$$

Since $[L : F]$ is prime we must have $F(a) = L$, hence $1, a, a^2, \ldots, a^{p-1}$ are linearly independent over F. □

Proposition 3.2.12. *Let $A = (L/F, \sigma, a)$ be a nonassociative cyclic algebra of degree n. For every element $c \in L$, the map*

$$\sum_{i=0}^{n-1} x_i z^i \mapsto \sum_{i=1}^{n-1} (c - \sigma^i(c)) x_i z^i$$

is an F-derivation of A.

Proof. As in Theorem 3.1.8, these are just the inner derivations of the form

$$x \mapsto cx - xc,$$

which are derivations since $c \in Nuc(A)$. □

At this point we briefly discuss the algebras constructed by Sandler [48] which are mentioned in the introduction. We will give a full exposition of the finite field case in Chapter 6. Let $A := (L/F, \sigma, a)$ be a nonassociative cyclic algebra of degree n. We want to consider the opposite algebra A^{op}. This algebra has the same vector space structure as A but with a new multiplication given by

$$x \circ y = yx,$$

where juxtaposition is used to denote the multiplication in A. We also consider the following algebra, originally constructed by Sandler over finite fields [48].

Definition 3.2.13. Let L/F be a cyclic field extension of degree n with Galois group generated by σ. Pick a nonzero element $a \in L \setminus F$. We consider the L-vector space with basis $\{1, z, \ldots, z^{n-1}\}$

$$\Omega_{L,a,\sigma} := L \oplus zL \oplus \cdots \oplus z^{n-1}L.$$

Endow this with a multiplication, $*$, given as follows

$$(z^i x) * (z^j y) = \begin{cases} z^{i+j}\sigma^j(x)y & \text{if } i+j < n \\ z^{(i+j)-n} a \sigma^j(x) y & \text{if } i+j \geq n \end{cases}$$

for $x, y \in L$ and extend this linearly to all of $\Omega_{L,a,\sigma}$.

To avoid confusion with our definition of a nonassociative cyclic algebra $(L/F, \sigma, a)$, we use the notation $\Omega_{L,a,\sigma}$ for this algebra.

Proposition 3.2.14. *Let $A = (L/F, \sigma, a)$. Then $A^{op} \cong \Omega_{L,a,\sigma}$.*

Proof. Define the map

$$f : A^{op} \to \Omega_{L,a,\sigma}$$

by

$$\sum_{i=0}^{n-1} x_i z^i \mapsto \sum_{i=0}^{n-1} z^i x_i.$$

This is clearly a vector space isomorphism. We show that f respects the multiplication of elements xz^i and yz^j in A^{op} where $0 \leq i, j \leq n-1$, then, since f is linear, this will show that f is an algebra isomorphism.

$$\begin{aligned} f(xz^i \circ yz^i) = f((yz^j)(xz^i)) &= \begin{cases} f(y\sigma^j(x)z^{i+j}) & \text{if } i+j < n \\ f(y\sigma^j(x)az^{(i+j)-n}) & \text{if } i+j \geq n \end{cases} \\ &= \begin{cases} z^{i+j}y\sigma^j(x) & \text{if } i+j < n \\ z^{(i+j)-n}y\sigma^j(x)a & \text{if } i+j \geq n \end{cases} \\ &= (z^i x) * (z^j y) \\ &= f(xz^i) * f(yz^j) \end{aligned}$$

as required. □

Remark 3.2.15. It appears there is a mistake in [48, Theorem 1] of Sandler's paper where he claims that the middle nucleus of his algebra will be strictly bigger than L if a belongs to a proper subfield of L. However, since Sandler's algebras are isomorphic to A^{op} for A a nonassociative cyclic algebra, and since $Nuc_m(A) = Nuc_m(A^{op})$ for any algebra A, Proposition 3.2.2 implies that the middle nucleus of Sandler's algebras will always be L.

The question arises of whether $(L/F, \sigma, a)^{op}$ is isomorphic to $(L/F, \sigma, b)$ for any $b \in L^\times$. It turns out that this happens only in the case of nonassociative quaternion algebras.

Proposition 3.2.16. *Let $A := (L/F, \sigma, a)$ be a nonassociative quaternion algebra, i.e., L/F is a quadratic extension and σ is the nontrivial automorphism on L. Then $A \cong A^{op}$.*

Proof. An isomorphism $f : A \to A^{op}$ is simply an anti-automorphism of A, so $f(xy) = f(y)f(x)$ for all $x, y \in A$. We claim that the map

$$f : A \to A \qquad x_0 + x_1 z \mapsto x_0 + \sigma(x_1)z,$$

is an anti-automorphism. To see this, let $x_0 + x_1 z$ and $y_0 + y_1 z$ be elements of A. Then

$$\begin{aligned} f((x_0 + x_1 z)(y_0 + y_1 z)) &= f(x_0 y_0 + x_1 \sigma(y_1)a + (x_0 y_1 + x_1 \sigma(y_0))z) \\ &= x_0 y_0 + x_1 \sigma(y_1)a + (\sigma(x_0 y_1) + \sigma(x_1)y_0)z, \end{aligned}$$

and

$$\begin{aligned} f(y_0 + y_1 z)f(x_0 + x_1 z) &= (y_0 + \sigma(y_1)z)(x_0 + \sigma(x_1)z) \\ &= y_0 x_0 + \sigma(y_1)x_1 a + (y_0 \sigma(x_1) + \sigma(y_1)\sigma(x_0))z. \end{aligned}$$

So f is the required map. □

For a nonassociative cyclic algebra of degree $n > 2$, the opposite algebra $(L/F, \sigma, a)$ is *not* isomorphic to $(L/F, \sigma, b)$ for any $b \in L$. To prove this we use the following definition and lemma.

Definition 3.2.17. Let A be a nonassociative algebra and let n be a positive integer. An element $x \in A$ is said to be *nth power associative* if x^j is well-defined for all $j \leq n$, i.e., the product of j copies of x always gives the same result, no matter which order we bracket them, for all $j \leq n$.

Note that every element in an algebra A is first and second power associative.

Lemma 3.2.18. *Let $f : A \to B$ be an algebra homomorphism or anti-homomorphism. If $x \in A$ is nth power associative in A then $f(x)$ is nth power associative in B.*

Proof. For $n = 3$ we have

$$(f(x)f(x))f(x) = f((xx)x) = f(x(xx)) = f(x)(f(x)f(x))$$

for a homomorphism f and for an anti-homomorphism we have

$$(f(x)f(x))f(x) = f(x(xx)) = f((xx)x) = f(x)(f(x)f(x)).$$

Now suppose $x \in A$ is nth power associative and that $f(x)^i$ is well-defined for all $i < n$. Then for all $0 < i, j, k < n$ such that $i + j + k = n$, we have

$$0 = f(0) = f([x^i, x^j, x^k]) = [f(x)^i, f(x)^j, f(x)^k]$$

for a homomorphism f and

$$0 = f(0) = f([x^i, x^j, x^k]) = [f(x)^k, f(x)^j, f(x)^i]$$

for an anti-homomorphism f. This shows that $f(x)^n$ is well-defined. □

Theorem 3.2.19. *Let $A = (L/F, \sigma, a)$ be a nonassociative cyclic algebra of degree $n \geq 3$. Then A^{op} is not isomorphic to a nonassociative cyclic algebra $(L/F, \sigma, b)$ for any $b \in L \setminus F$.*

Proof. Let

$$B = (L/F, \sigma, b) = \sum_{i=0}^{n-1} Lu^i$$

and suppose $f : A^{op} \to B$ is an isomorphism. Since isomorphisms must preserve the nucleus we have $f(L) = L$ so $f|_L \in Gal(L/F)$, say $f|_L = \sigma^k$. Now suppose

$$f(z) = l_0 + l_1u + l_2u^2 + \cdots + l_{n-1}u^{n-1}.$$

Let $\circ$ denote the multiplication in A^{op}, i.e., $x \circ y = yx$ for all $x, y \in A$, and pick $m \in L$ such that m does not belong to any proper subfield of L. Then

$$\begin{aligned} f(m)f(z) &= \sigma^k(m)(l_0 + l_1u + \cdots + l_{n-1}u^{n+1}) \\ &= \sigma^k(m)l_0 + \sigma^k(m)l_1u + \cdots + \sigma^k(m)l_{n-1}u^{n-1}, \end{aligned}$$

whereas

$$\begin{aligned} f(m \circ z) &= f(zm) = f(\sigma(m)z) = f(z \circ \sigma(m)) \\ &= (l_0 + l_1 u + \cdots + l_{n-1}u^{n+1})\sigma^{k+1}(m) \\ &= l_0\sigma^{k+1}(m) + l_1\sigma^{k+2}(m)u + \cdots + l_{n-1}\sigma^{(k+1)+(n-1)}(m)u^{n-1}, \end{aligned}$$

where powers of σ are read modulo n. Since m does not belong to a proper subfield of L, the elements $\sigma^i(m)$, for $i = 0, \ldots, n-1$, are all distinct. The two expressions above are only equal at the $(n-1)$th term and so $l_i = 0$ for all $0 \leq i \leq n-2$. Therefore $f(z) = lu^{n-1}$ for some $l \in L^\times$. Now the element $z \in A$ is nth power associative, in particular, it is third power associative, however, the element $lu^{n-1} = f(z)$ is not. We have

$$(lu^{n-1}lu^{n-1})lu^{n-1} = (l\sigma^{n-1}(l)au^{n-2})lu^{n-1} = l\sigma^{n-1}(l)\sigma^{n-2}(l)a^2u^{n-3},$$

however,

$$lu^{n-1}(lu^{n-1}lu^{n-1}) = lu^{n-1}(l\sigma^{n-1}(l)au^{n-2}) = l\sigma^{n-1}(l)\sigma^{n-2}(l)a\sigma^{n-1}(a)u^{n-3}.$$

These two are not the same since $a \neq \sigma^{n-1}(a)$. Hence f cannot be an isomorphism. □

3.3 Nonassociative Cyclic Algebras of Degree 4

One might hope that the construction of nonassociative cyclic algebras of degree n will always give division algebras for any choice of $a \in L \setminus F$. However, we can easily get a counter example of degree 4.

Example 3.3.1. Let F be a field containing a primitive fourth root of unity, denoted i, and let ω be a root of the irreducible polynomial $x^4 - c$ for some $c \in F^\times$. Then the field extension $L = F(\omega)$ is a cyclic field extension of degree 4 with Galois group $G = \langle\sigma\rangle$. We note the following explicit calculations of the automorphism σ:

$$\sigma(\omega) = i\omega, \quad \sigma^2(\omega) = -\omega, \quad \sigma(\omega^2) = -\omega^2, \quad \sigma^2(\omega^2) = \omega^2.$$

Let $a = -\omega^2/c \in L \setminus F$ and consider the nonassociative cyclic algebra $A = (L/F, \sigma, a)$. We claim that A contains zero divisors. Consider elements $x = \omega + \omega^2 z^2$ and $y = \omega z + \omega^2 z^3$. These are nonzero elements of A and

$$xy = (\omega^2 + \omega^2\sigma^2(\omega^2)a)z + (\omega^3 + \omega^2\sigma^2(\omega))z^3 = 0.$$

In this section we want to look at certain subalgebras of nonassociative cyclic algebras. It is clear that a nonassociative cyclic algebra $(L/F, \sigma, a)$ contains both L and F as subalgebras. In the case that L/F is a field extension of prime degree, we suspect that these are all subalgebras, but this remains an open question. The most interesting examples of subalgebras occur when the degree of the field extension L/F is not prime. We introduce the following notation.

Let L/F be a cyclic field extension of degree n and suppose that $n = st$ for some integers $1 < s, t < n$. If $G = Gal(L/F) = \langle\sigma\rangle$, then denote by G_s the subgroup of G generated by σ^s. Furthermore, denote the fixed field of G_s by E_s, so we have a tower of fields:

$$F \subset E_s \subset L.$$

Theorem 3.3.2. *Let $A = (L/F, \sigma, a)$ be a nonassociative cyclic algebra over F of degree n where $n = st$. A contains $A_s := (L/E_s, \sigma^s, a)$ as a subalgebra where A_s is viewed as an F-algebra. It is an associative subalgebra if $a \in E_s$ and it is a nonassociative subalgebra if $a \in L \setminus E_s$.*

Proof. First note that if $a \in E_s$ then A_s is an associative cyclic algebra over E_s, and if $a \in L/E_s$ then A_s is a nonassociative cyclic algebra. It can be easily checked that the linear subspace

$$S := L \oplus Lz^s \oplus Lz^{2s} \oplus \cdots \oplus Lz^{(t-1)s}$$

of A, together with the multiplication inherited from A, is a subalgebra of A. Moreover, it has the same vector space structure as the algebra A_s defined

above. Consider a product of monomials lz^{is} and mz^{js} in S for some $l, m \in L$ and $0 \leq i, j \leq t-1$. This is

$$(lz^{is})(mz^{js}) = \begin{cases} l\sigma^{is}(m)z^{(i+j)s} & \text{if } i+j < t \\ l\sigma^{is}(m)az^{(i+j-t)s} & \text{if } i+j \geq t, \end{cases}$$

which is clearly the same as the multiplication in A_s. □

Remark 3.3.3. An obvious analogue of this result also holds when we have an associative central simple cyclic algebra of degree $n = st$.

Let $A = (L/F, \sigma, a)$ be a nonassociative cyclic algebra over F of degree $n = st$. If $a \in E_s$ then we may also consider the vector space

$$A|_{E_s} := E_s \oplus E_s z \oplus \cdots \oplus E_s z^{n-1},$$

endowed with the multiplication of A restricted to $A|_{E_s}$. With this multiplication it becomes a subalgebra of A. We will study this subalgebra in the case where $n = 4$.

For the remainder of this chapter let L/F be a cyclic field extension of degree 4 with $Gal(L/F) = \langle\sigma\rangle$. Set $G = G_2 = \langle\sigma^2\rangle$ and $E = E_2 = \text{Fix}(G)$. Then

$$A = (L/F, \sigma, a) = L \oplus Lz \oplus Lz^2 \oplus Lz^3$$

where $a \in E$ and

$$A|_E := E \oplus Ez \oplus Ez^2 \oplus Ez^3.$$

This is an eight-dimensional algebra over F. Elements are of the form $x_0 + x_1 z + x_2 z^2 + x_3 z^3$ for $x_i \in E$ and multiplication is now given by

$$\begin{aligned} xy &= (x_0 + x_1 z + x_2 z^2 + x_3 z^3)(y_0 + y_1 z + y_2 z^2 + y_3 z^3) \\ &= x_0 y_0 + x_1 \sigma(y_3) a + x_2 y_2 a + x_3 \sigma(y_1) a \\ &+ (x_0 y_1 + x_1 \sigma(y_0) + x_2 y_3 a + x_3 \sigma(y_2) a) z \\ &+ (x_0 y_2 + x_1 \sigma(y_1) + x_2 y_0 + x_3 \sigma(y_3) a) z^2 \\ &+ (x_0 y_3 + x_1 \sigma(y_2) + x_2 y_1 + x_3 \sigma(y_0)) z^3, \end{aligned} \tag{3.10}$$

since σ^2 acts trivially on E and $\sigma|_E = \sigma^3|_E$.

Proposition 3.3.4. *(i)* $Nuc(A|_E) = E$.

(ii) $Comm(A|_E) = F \oplus Fz^2$.

Proof. Clearly $E \subset Nuc(A|_E)$ since $E \subset Nuc(A)$. Conversely, suppose

$$n = n_0 + n_1 z + n_2 z^2 + n_3 z^3 \in Nuc(A|_E)$$

for some $n_i \in E$. Calculating the associator $[z, z^3, n]$, we have

$$(zz^3)(n_0 + n_1 z + n_2 z^2 + n_3 z^3) = an_0 + an_1 z + an_2 z^2 + an_3 z^3,$$

on the one hand, whereas

$$\begin{aligned} &z(z^3(n_0 + n_1 z + n_2 z^2 + n_3 z^3)) \\ &= z(\sigma^3(n_0)z^3 + \sigma^3(n_1)a + \sigma^3(n_2)az + \sigma^3(n_3)az^2) \\ &= n_0 a + n_1\sigma(a)z + n_2\sigma(a)z^2 + n_3\sigma(a)z^3. \end{aligned}$$

Hence $n_1 = n_2 = n_3 = 0$. For the second claim, it is routine to check from Equation (3.10) that $F \oplus Fz^2 \subseteq Comm(A|_E)$. Conversely, if $x = x_0 + x_1 z + x_2 z^2 + x_3 z^3 \in Comm(A|_E)$ then, for all $l \in L$ we have $lx = xl$ which implies that $x_1 = x_3 = 0$. Moreover, $zx = xz$ implies that x_0, x_2 must be in F. □

Notice that $A|_E$ contains within it the linear subspace $E \oplus Ez^2$. A routine verification tells us that, under the multiplication inherited from A, this is a quadratic étale E-algebra, which is a field if a is not a square in E. It turns out that $A|_E$ can be built out of two copies of its subalgebra $E \oplus Ez^2$ as follows: denote $B := E \oplus Ez^2$. On B we define two maps

$$\sigma : B \to B; \quad b_0 + b_1 z^2 \mapsto \sigma(b_0) + \sigma(b_1)z^2$$

and

$$\psi_a : B \to B; \quad b_0 + b_1 z^2 \mapsto \sigma(b_1)a + \sigma(b_0)z^2.$$

We can now define a new algebra.

Definition 3.3.5. On the F-vector space

$$B \oplus Bz$$

we define a multiplication

$$(u + vz)(s + tz) = (us + v\psi_a(t)) + (ut + v\sigma(s))z,$$

for all $u, v, s, t \in B$. With this multiplication the vector space becomes an F-algebra which we denote $\mathrm{Doub}(B, \psi_a, \sigma)$.

Proposition 3.3.6. $A|_E = \mathrm{Doub}(B, \psi_a, \sigma)$.

Proof. Consider the elements:

$$\begin{aligned} u &= x_0 + x_2 z^2, \\ v &= x_1 + x_3 z^2, \\ s &= y_0 + y_2 z^2, \\ t &= y_1 + y_3 z^2. \end{aligned}$$

The strangely numbered indices allow us to compare with the multiplication in (3.10) above. First we calculate $us + v\psi_a(t)$, this is

$$\begin{aligned} &(x_0 + x_2 z^2)(y_0 + y_2 z^2) + (x_1 + x_3 z^2)(\sigma(y_3)a + \sigma(y_1)z^2) \\ &= (x_0 y_0 + x_2 y_2 a) + (x_0 y_2 + x_2 y_0)z^2 \\ &+ (x_1\sigma(y_3)a + x_3\sigma(y_1)a) + (x_1\sigma(y_1) + x_3\sigma(y_3)a)z^2. \end{aligned}$$

Similarly computing the second term $ut + v\sigma(s)$ gives

$$\begin{aligned} &(x_0 + x_2 z^2)(y_1 + y_3 z^2) + (x_1 + x_3 z^2)(\sigma(y_0) + \sigma(y_2)z^2) \\ &= (x_0 y_1 + x_2 y_3 a) + (x_0 y_3 + x_2 y_1)z^2 \\ &+ (x_1\sigma(y_0) + x_3\sigma(y_2)a) + (x_1\sigma(y_2) + x_3\sigma(y_0))z^2. \end{aligned}$$

Now combining the two terms and comparing with the equation (3.10) above we see that the multiplication for

$$(us + v\psi_a(t)) + (ut + v\sigma(s))z$$

in $\mathrm{Doub}(B, \psi_a, \sigma)$ is the same as the multiplication

$$(x_0 + x_1 z + x_2 z^2 + x_3 z^3)(y_0 + y_1 z + y_2 z^2 + y_3 z^3)$$

in $A|_E$. □

Theorem 3.3.7. *$A|_E$ is a division algebra if and only if a is not a square in E.*

Proof. If a is a square in E then the subalgebra $E \oplus Ez^2$ is split and $A|_E$ contains zero divisors. If a is not a square then $E \oplus Ez^2$ is a field which we denote by B. In view of the previous proposition, we show that $\mathrm{Doub}(B, \psi_a, \sigma)$ does not contain zero divisors. Suppose

$$(u + vz)(s + tz) = 0,$$

where $u + vz \neq 0 \neq s + tz$. Then

$$us + v\psi_a(t) = 0 \tag{3.11}$$

and

$$ut + v\sigma(s) = 0. \tag{3.12}$$

We may assume that $s \neq 0$ since otherwise a quick check of the above equations implies that either $u + vz = 0$ or $s + tz = 0$. Similarly we have $v \neq 0$. Then, from (3.11), we get

$$u = -v\psi_a(t)s^{-1}.$$

Putting this into (3.12) yields

$$v\psi_a(t)ts^{-1} = v\sigma(s).$$

Since $v \neq 0$, we multiply by v^{-1} and rearrange to leave

$$t\psi_a(t) = s\sigma(s).$$

Now, if $t = t_0 + t_1 z^2$ and $s = s_0 + s_1 z^2$ are elements of B, then

$$\begin{aligned} s\sigma(s) &= (s_0 + s_1 z^2)(\sigma(s_0) + \sigma(s_1) z^2) \\ &= (N_{E/F}(s_0) + N_{E/F}(s_1)a) + Tr_{E/F}(s_0\sigma(s_1))z^2 \end{aligned}$$

and

$$\begin{aligned} t\psi_a(t) &= (t_0 + t_1 z^2)(\sigma(t_1)a + \sigma(t_0) z^2) \\ &= Tr_{E/F}(t_0\sigma(t_1))a + (N_{E/F}(t_0) + N_{E/F}(t_1)a)z^2, \end{aligned}$$

where $N_{E/F} : x \mapsto x\sigma(x)$ and $Tr_{E/F} : x \mapsto x + \sigma(x)$ are the norm and trace maps from $E \to F$. Comparing the first term of each equation we get

$$N_{E/F}(s_0) + (N_{E/F}(s_1) - Tr_{E/F}(t_0\sigma(t_1)))a = 0,$$

which implies that $s_0 = 0$, since $1, a$ are linearly independent over F. Similarly, looking at the z^2 term in each equation shows

$$Tr_{E/F}(s_0\sigma(s_1)) - N_{E/F}(t_0) - N_{E/F}(t_1)a = 0 - N_{E/F}(t_0) - N_{E/F}(t_1)a = 0,$$

and hence $t_0 = t_1 = 0$. Finally, this gives that $s_1 = 0$ which is a contradiction of our assumption. □

It also turns out that if $a \in E$, then the cyclic algebra $(L/F, \sigma, a)$ can be viewed as a similar doubling of the (associative) quaternion subalgebra A_2, defined in Theorem 3.3.2.

Definition 3.3.8. Let $A = (L/F, \sigma, a)$ be a nonassociative cyclic algebra of degree 4, where a belongs to an intermediate subfield of L and F of degree 2. Let $A_2 = (L/E, \sigma^2, a)$ be the associative quaternion subalgebra of A with vector space decomposition

$$A_2 = L \oplus Lz^2.$$

Define maps on A_2

$$\sigma : A_2 \to A_2, \quad x_0 + x_1 z^2 \mapsto \sigma(x_0) + \sigma(x_1) z^2$$

and

$$\psi_a : A_2 \to A_2, \quad x_0 + x_1 z^2 \mapsto \sigma(x_1)a + \sigma(x_0)z^2.$$

On the F-vector space

$$A_2 \oplus A_2 z$$

we define a multiplication

$$(u + vz)(s + tz) = (us + v\psi_a(t)) + (ut + v\sigma(s))z,$$

for all $u, v, s, t \in A_2$. We call this $\mathrm{Doub}(A_2, \sigma, \psi_a)$.

A routine calculation, similar to the proof of Proposition 3.3.5, yields the following result.

Proposition 3.3.9. $\mathrm{Doub}(A_2, \sigma, \psi_a) = (L/F, \sigma, a)$.

Remark 3.3.10. Note that because $a \in E$ we have $a = \sigma^2(a)$. This fact ensures that the multiplication in $\mathrm{Doub}(A_2, \sigma, \psi_a)$ is the same as that in $(L/F, \sigma, a)$. In the case that $a \in L \setminus E$, the cyclic algebra $(L/F, \sigma, a)$ cannot be represented by this doubling process.

If we assume that A_2 is a division algebra, i.e. $a \neq l\sigma^2(l)$ for all $l \in L$, then we can try the same trick as in Theorem 3.3.7 to check if $(L/F, \sigma, a)$ is a division algebra. Suppose that we have zero divisors

$$(u + vz)(s + tz) = 0.$$

Then we get the equations

$$us + v\psi_a(t) = 0,$$

and

$$ut + v\sigma(s) = 0.$$

Rearranging (and being more careful because of the noncommutative multiplication in A_2) we arrive at the equation

$$\psi_a(t)s^{-1}t = \sigma(s). \tag{3.13}$$

Hence, if Equation 3.13 does not hold for all nonzero s and t, then $(L/F, \sigma, a)$ is a division algebra. To study this further we consider A_2 as an eight-dimensional F-algebra and define a multiplicative norm form $N_{A_2/F}$ on A_2 by

$$N_{A_2/F}(u) = N_{E/F}N_{A_2/E}(u) \tag{3.14}$$

for all $u \in A_2$. In (3.14), $N_{A_2/E}$ is the quaternion norm on A_2 defined by

$$N_{A_2/E}(u_0 + u_1 z^2) = N_{L/E}(u_0) - aN_{L/E}(u_1),$$

for all $u = u_0 + u_1 z^2 \in A_2$ and where

$$N_{L/E} : L \to E; \quad l \mapsto l\sigma^2(l), \tag{3.15}$$

for all $l \in L$ and

$$N_{E/F} : E \to F; \quad m \mapsto m\sigma(m), \tag{3.16}$$

for all $m \in E$. Note that

$$N_{E/F}(N_{L/E}(l)) = N_{L/F}(l), \tag{3.17}$$

for all $l \in L$. The map $N_{A_2/F}$ is clearly a multiplicative, anisotropic map since it is a composition of two multiplicative, anisotropic norm maps.

Lemma 3.3.11. *For all $u \in A_2$, $N_{A_2/F}(\psi_a(u)) = N_{E/F}(a)N_{A_2/F}(\sigma(u))$.*

Proof. If $u = u_0 + u_1 z^2$ then $\psi_a(u) = \sigma(u_1)a + \sigma(u_0)z^2$ and $\sigma(u) = \sigma(u_0) + \sigma(u_1)z^2$. Hence

$$\begin{aligned} N_{A_2/E}(\psi_a(u)) &= N_{L/E}(\sigma(u_1)a) - aN_{L/E}(\sigma(u_0)) \\ &= -a\big(N_{L/E}(\sigma(u_0)) - aN_{L/E}(\sigma(u_1))\big) \\ &= -aN_{A_2/E}(\sigma(u)). \end{aligned}$$

Therefore

$$\begin{aligned} N_{A_2/F}(\psi_a(u)) &= N_{E/F}N_{A_2/E}(\psi_a(u)) \\ &= N_{E/F}\big(-aN_{A_2/E}(\sigma(u))\big) \\ &= N_{E/F}(a)N_{A_2/F}(\sigma(u)), \end{aligned}$$

as required. □

In general $N_{A_2/F}(u) \neq N_{A_2/F}(\sigma(u))$, however, in the case where $a \in F^\times$ (so $(L/F, \sigma, a)$ is associative), they are equal.

Lemma 3.3.12. *Let $a \in F^\times$ and let $A = (L/F, \sigma, a)$ be an associative cyclic algebra of degree 4 with quaternion subalgebra A_2. Then $N_{A_2/F}(u) = N_{A_2/F}(\sigma(u))$ for all $u \in A_2$.*

Proof. Let $u = u_0 + u_1 z^2 \in A_2$. We have

$$\begin{aligned} N_{A_2/F}(u) &= N_{E/F}\big(N_{A_2/E}(u_0 + u_1 z^2)\big) \\ &= N_{E/F}\big(N_{L/E}(u_0) - aN_{L/E}(u_1)\big) \\ &= N_{E/F}\big(N_{L/E}(u_0)\big) + N_{E/F}\big(aN_{L/E}(u_1)\big) \\ &\quad - N_{L/E}(u_0)\sigma(a)\sigma\big(N_{L/E}(u_1)\big) \\ &\quad - \sigma\big(N_{L/E}(u_0)\big)aN_{L/E}(u_1). \end{aligned}$$

Also

$$\begin{aligned} N_{A_2/F}(\sigma(u)) &= N_{E/F}\big(N_{A_2/E}(\sigma(u_0) + \sigma(u_1)z^2)\big) \\ &= N_{E/F}\big(N_{L/E}(\sigma(u_0)) - aN_{L/E}(\sigma(u_1))\big) \\ &= N_{E/F}\big(N_{L/E}(\sigma(u_0))\big) + N_{E/F}\big(aN_{L/E}(\sigma(u_1))\big) \\ &\quad - N_{L/E}(\sigma(u_0))\sigma(a)\sigma\big(N_{L/E}(\sigma(u_1))\big) \\ &\quad - \sigma\big(N_{L/E}(\sigma(u_0))\big)aN_{L/E}(\sigma(u_1)). \end{aligned}$$

A quick check using equations (3.15)-(3.17) and the fact that $\sigma(a) = a$ shows that these two expressions are equal. □

Lemma 3.3.13. *Let L/F be a cyclic field extension of degree 4 with $Gal(L/F) = \langle\sigma\rangle$ and let E be the intermediate field of L and F corresponding to the subgroup $\{1, \sigma^2\}$. If $a \in F^\times$ is such that $a^2 \notin N_{L/F}(L^\times)$ then*

(i) $a \notin N_{L/F}(L^\times)$.

(ii) $a \notin N_{L/E}(L^\times)$.

(iii) $a \neq \pm N_{E/F}(m)$ *for any* $m \in E$.

Proof. (i) If $a = N_{L/F}(l)$ for some non-zero $l \in L$ then

$$a^2 = N_{L/F}(l)^2 = N_{L/F}(l^2),$$

which is a contradiction of our hypothesis.
(ii) Suppose $a \in N_{L/E}(L^\times)$, then $a = l\sigma^2(l)$ for some $l \in L^\times$. This implies

$$a^2 = a\sigma(a) = l\sigma^2(l)\sigma(l)\sigma^3(l) = N_{L/F}(l).$$

(iii) Similarly if $a = \pm m\sigma(m)$ for some $m \in E$ then

$$a^2 = m\sigma(m)m\sigma(m) = m\sigma(m)\sigma^2(m)\sigma^3(m) = N_{L/F}(m).$$

□

Theorem 3.3.14. *Let $A = (L/F, \sigma, a)$ be an associative cyclic algebra of degree 4. If $a^2 \notin N_{L/F}(L^\times)$ then A is a division algebra.*

Proof. By Lemma 3.3.13, $a^2 \notin N_{L/F}(L^\times)$ implies $a \notin N_{L/E}(L^\times)$ and so the quaternion subalgebra A_2 is a division algebra. We consider A as the doubling $\mathrm{Doub}(A_2, \psi_a, \sigma)$. Suppose A has zero divisors, say

$$(u + vz)(s + tz) = 0,$$

for some $u, v, s, t \in A_2$. This then reduces to Equation (3.13) above

$$\psi_a(t)s^{-1}t = \sigma(s).$$

Applying the norm $N_{A_2/F}$ to both sides gives

$$N_{A_2/F}(\psi_a(t))N_{A_2/F}(s^{-1})N_{A_2/F}(t) = N_{A_2/F}(\sigma(s))$$

since $N_{A_2/F}$ is multiplicative. Using Lemma 3.3.11 we see

$$N_{E/F}(a)N_{A_2/F}(\sigma(t))N_{A_2/F}(s^{-1})N_{A_2/F}(t) = N_{A_2/F}(\sigma(s)).$$

Lemma 3.3.12 and the fact that $N_{E/F}(a) = a^2$ then implies that

$$a^2 N_{A_2/F}(t^2) = N_{A_2/F}(s^2).$$

If $t = 0$, then s must also equal zero since $N_{A_2/F}$ is anisotropic. If $t \neq 0$ then

$$a^2 = N_{A_2/F}(s^2)N_{A_2/F}(t^2)^{-1} = N_{A_2/F}(st^{-1})^2,$$

and so

$$a = \pm N_{A_2/F}(st^{-1}).$$

Recalling that $N_{A_2/F} = N_{E/F}(N_{A_2/E})$ gives

$$a = \pm N_{E/F}(m),$$

for $m = N_{A_2/E}(st^{-1}) \in E^\times$, but this is a contradiction of our hypothesis that $a^2 \notin N_{L/F}(L^\times)$ by Lemma 3.3.13. □

Remark 3.3.15. The condition in the above Theorem is equivalent to that in the Theorem of Wedderburn (cf. Theorem 2.2.4). Suppose that $a = N_{L/F}(l)$ for some $l \in L$, then $a^2 = N_{L/F}(l)^2 = N_{L/F}(l^2)$. Similarly, if $a^3 = N_{L/F}(l)$, then

$$N_{L/F}(a)a^2 = a^4a^2 = a^6 = N_{L/F}(l)^2 = N_{L/F}(l^2),$$

and so $a^2 = N_{L/F}(l^2)N_{L/F}(a^{-1})$. Both cases contradict the hypothesis that a^2 is not the norm of some element of L.

Chapter 4

Semi-Multiplicative Maps

4.1 Preliminaries and Basic Properties

In this section we introduce the concept of a *semi-multiplicative map* of degree n and give some properties of quadratic and cubic semi-multiplicative maps. A nonassociative cyclic algebra of degree n possesses a semi-multiplicative map of degree n and these will be studied in the next sections. This chapter is part of a joint work with Pumplün [46].

Let $M : V \to W$ be a map between two finite-dimensional F-vector spaces, V and W. M is said to be of degree n if $M(\lambda v) = \lambda^n M(v)$ for all $\lambda \in F$, $v \in V$ and the map $M : V \times \cdots \times V \mapsto W$ defined by

$$M(v_1, \ldots, v_n) = \sum_{1 \leq i_1 < \cdots < i_l \leq n} (-1)^{n-l} M(v_{i_1} + \cdots + v_{i_l}), \tag{4.1}$$

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

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

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

By linearisation we show:

Lemma 4.1.1. *(i) If M_A is left semi-multiplicative then the multilinear map $M_A : A \times \cdots \times A \mapsto D$ satisfies*

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

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

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

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

Proof. This follows directly from (4.1) and the definition of semi-multiplicativity. □

If, in addition, we assume that $M_A(a) \in F$ for all $a \in D$, then the restriction of M_A to the subalgebra D (denoted M_D) is a multiplicative form since

$$M_D(ab) = M_A(ab) = M_A(a)M_A(b) = M_D(a)M_D(b),$$

for all $a, b \in D$.

4.1.1 Quadratic case

Unless stated otherwise, let A be an algebra over F containing a subalgebra D, together with a quadratic map $M_A : A \mapsto D$ and associated symmetric bilinear map $M_A : A \times A \mapsto D$, $M_A(x, y) = M_A(x + y) - M_A(x) - M_A(y)$. If A is unital, define two F-linear maps $T_A : A \mapsto D$ and $^- : A \mapsto A$ by

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

Lemma 4.1.2. *Let $M_A : A \mapsto D$ be a quadratic map.*
(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

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

and

$$M_A(au, v) + M_A(u, av) = T_D(a)M_A(u, v) \text{ for all } a, b \in D, u, v \in A.$$

(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

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

and

$$M_A(ua, v) + M_A(u, va) = T_A(a)M_A(u, v) \text{ for all } a, b \in D, u, v \in A.$$

Proof. If M_A is left semi-multiplicative then by, Lemma 4.1.1,

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

for all $a \in D, u, v \in A$. It follows that

$$\begin{aligned} M_A(a,b)M_A(u,v) &= M_A(a+b)M_A(u,v) - M_A(a)M_A(u,v) \\ &\quad - M_A(b)M_A(u,v) \\ &= M_A((a+b)u,(a+b)v) - M_A(au,av) - M_A(bu,bv) \\ &= M_A(au,bv) + M_A(bu,av), \end{aligned}$$

as required. If A is unital, then setting $u = 1$ (resp. $b = 1$) gives the second (resp. third) identity. The proof is similar in the case that M_A is right semi-multiplicative. □

Corollary 4.1.3. *If M_A is semi-multiplicative then*

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

and

$$M_A(au,bv) + M_A(bu,av) = M_A(ua,vb) + M_A(ub,va)$$

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

Lemma 4.1.4. *If an element $x \in A$ satisfies $\overline{x}x = M_A(x)$ then it also satisfies the equation*

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

Similarly, if $x \in A$ satisfies $x\overline{x} = M_A(x)$ then it also satisfies

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

Proof. The proof follows easily from the definition $\overline{x} = T_A(x) - x$. □

Example 4.1.5. Let L/F be a quadratic separable field extension with non-trivial automorphism σ and let $a \in L \setminus F$. On the nonassociative quaternion algebra $Q = (L/F, \sigma, a)$, define a quadratic map, $M_Q : Q \to L$, as follows: for $x = x_0 + x_1 z \in Q, x_0, x_1 \in L$, set

$$M_Q(x) := N_{L/F}(x_0) - aN_{L/F}(x_1),$$

where $N_{L/F}$ is the field norm of L. Then M_Q is a semi-multiplicative map and every element $x \in Q$ satisfies the equation

$$x^2 - T_Q(x)x + M_Q(x) = 0.$$

Proof. An element $l \in L$ is identified with the element $l + 0z \in Q$. Thus $M_Q(l) = N_{L/F}(l)$ and, if $x = x_0 + x_1 z \in Q$ then,

$$\begin{aligned} M_Q(lx) = M_Q(lx_0 + lx_1 z) &= N_{L/F}(lx_0) - aN_{L/F}(lx_1) \\ &= N_{L/F}(l)(N_{L/F}(x_0) - aN_{L/F}(x_1)) \\ &= M_Q(l)M_Q(x). \end{aligned}$$

It is shown similarly that $M_Q(xl) = M_Q(l)M_Q(x)$, so M_Q is semi-multiplicative. The linearisation of the field norm $N_{L/F}$ is

$$N_{L/F}(x_0, y_0) = x_0\sigma(y_0) + y_0\sigma(x_0),$$

for $x_0, y_0 \in L$, and hence

$$M_Q(x, y) = N_{L/F}(x_0, y_0) - aN_{L/F}(x_1, y_1),$$

where $y = y_0 + y_1 z \in Q$. Thus $T_Q(x) = N_{L/F}(1, x_0) = Tr_{L/F}(x_0)$, where $Tr_{L/F}$ is the field trace of L. We also see that

$$\overline{x} = T_Q(x) - x = \sigma(x_0) - x_1 z,$$

and therefore

$$\begin{aligned} \overline{x}x &= (\sigma(x_0) - x_1 z)(x_0 + x_1 z) \\ &= (\sigma(x_0)x_0 - x_1\sigma(x_1)a) + (\sigma(x_0)x_1 - x_1\sigma(x_0))z \\ &= M_Q(x). \end{aligned}$$

□

Remark 4.1.6. The map M_Q defined above bears a striking resemblance to the reduced norm map of an associative quaternion algebra. In the next section, we will define a map for nonassociative cyclic algebras of degree n, which can be thought of as an analogue of the reduced norm map for associative cyclic algebras of degree n.

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 4.1.7. *Let A be a unital algebra over a field of characteristic not 2 and let D be a proper finite-dimensional, unital subalgebra 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 $x \in A$ and $a \in D$. 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 $z \in D^\perp$ 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 $x \in A$. Now $D^\perp \neq 0$ 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 4.1.2:

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

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,

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

□

Remark 4.1.8. The previous theorem, which is a generalisation of a well-known result for multiplicative quadratic forms (cf. [24, §7.6, Lemma 3]), shows that nonassociative quaternion algebras are a good prototypical example of algebras carrying a nondegenerate, quadratic semi-multiplicative map.

4.1.2 Cubic case

Let A be an F-algebra, D a 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

$$\begin{aligned} M_A(x,y,z) = {} & M_A(x+y+z) - M_A(x+y) - M_A(x+z) - M_A(y+z) \\ & + M_A(x) + M_A(y) + M_A(z), \end{aligned}$$

for all $x, y, z \in A$, is symmetric in all three variables. If $1/6 \in F^\times$ then $M_A(x) = 1/6 M_A(x,x,x)$. 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 right 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 the following lemma.

Lemma 4.1.9. *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 $a, b, c \in D$ and all $x, y, z \in A$.
(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 $a, b, c \in D$ and all $x, y, z \in A$.

Proof. The proof is similar to that of Lemma 4.1.2. □

Suppose that A is unital and that F is not of characteristic 2 or 3. We define a linear map $T_A : A \to D$ and a 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 $x \in A$. It is easy to see that

$$T_A(1) = S_A(1) = 3. \tag{4.2}$$

If M_A is left semi-multiplicative then putting $b = c = 1$ in Lemma 4.1.9 yields

$$M_A(ax, y, z) + M_A(x, ay, z) + M_A(x, y, az) = T_A(a)M_A(x, y, z), \tag{4.3}$$

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

$$M_A(xa, y, z) + M_A(x, ya, z) + M_A(x, y, za) = T_A(a)M_A(x, y, z), \tag{4.4}$$

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

$$M_A([a, x], y, z) + M_A(x, [a, y], z) + M_A(x, y, [a, z]) = 0, \tag{4.5}$$

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

$$T_A(x, y) := T_A(x)T_A(y) - M_A(x, y, 1), \tag{4.6}$$

for all $x, y \in A$. If M_A is left semi-multiplicative then putting $y = z = 1$ into equation (4.3) 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

$$T_A(1, x) = T_A(x, 1) = T_A(x), \tag{4.7}$$

for all $x \in A$. We may also bilinearise 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 $T_A(x, y)$ in (4.6) we obtain

$$S_A(x, y) = M_A(x, y, 1) = M_A(1, x, y) = T_A(x)T_A(y) - T_A(x, y), \tag{4.8}$$

for all $x, y \in A$.

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

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

and hence,

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

Proposition 4.1.10. *For all $y \in A$, $1 \sharp y = T_A(y) - y$.*

Proof. Calculating directly from the linearised 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 (4.2) 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 (4.8) and (4.7) 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 4.1.11. *Suppose every element $x \in A$ satisfies $x^\sharp x = M_A(x)$. Then:*
(i) Every element $x \in A$ satisfies the equation

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

Proof. The proof is clear from the definition of $\sharp : A \to A$. □

4.2 A Semi-Multiplicative Map for Nonassociative Cyclic Algebras

In the classical theory of associative algebras, the reduced norm of a central simple algebra of degree n is a multiplicative form of degree n. In this section we define an analogous map for a nonassociative cyclic algebra. Although this map is not multiplicative, it is semi-multiplicative of degree n.

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

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

for $x = x_0 + x_1z + \cdots + x_{n-1}z^{n-1}, x_i \in L$. We define a map $M_A : A \to L$ by

$$M_A(x) := \mathrm{Det}(R_x)$$

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

Proposition 4.2.1. *$M_A(x)$ is a polynomial in a of degree $n-1$ with coefficients in F.*

Proof. It is clear that $M_A(x)$ is a polynomial in a of degree $n-1$ with coefficients in L. To show that they actually belong to F we consider a matrix R_x^t with entries in $L[t,t^{-1}]$ given by

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

for $x = x_0 + x_1 z + \cdots + x_{n-1}z^{n-1}$, with $x_i \in L$. We extend the automorphism σ to $L[t,t^{-1}]$ by setting $\sigma(t) = t$. We also define the map $\sigma_A : A \to A$ by

$$\sigma_A(x_0 + x_1 z + \cdots + x_{n-1}z^{n-1}) = \sigma(x_0) + \sigma(x_1)z + \cdots + \sigma(x_{n-1})z^{n-1}.$$

Clearly we have

$$\mathrm{Det}(R^t_{\sigma_A(x)}) = \sigma(\mathrm{Det}(R_x^t)).$$

On the other hand it is easy to check that

$$R_x^t = \begin{pmatrix} 0 & 0 & \cdots & 0 & t^{-1} \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} R^t_{\sigma_A(x)} \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ t & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Hence $\mathrm{Det}(R_x^t) = \mathrm{Det}(R^t_{\sigma_A(x)})$. This shows that the coefficients of t in $\mathrm{Det}(R_x^t)$ are invariant under σ so they must belong to F. Therefore the coefficients of a in $\mathrm{Det}(R_x) = M_A(x)$ also belong to F. □

Proposition 4.2.2. *If $l \in L$ is considered as an element of A then $M_A(l) = N_{L/F}(l)$.*

Proof. If l is considered as an element of A, it is written as $l = l + 0z + \cdots + 0z^{n-1}$. Hence

$$R_l = \begin{pmatrix} l & 0 & \cdots & 0 \\ 0 & \sigma(l) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma^{n-1}(l) \end{pmatrix}.$$

□

Proposition 4.2.3. *If $x \in A$ and $l \in L$ then*

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

Proof. For $x = x_0 + x_1 z + \cdots + x_{n-1}z^{n-1}$ with $x_i \in L$, we have

$$lx = lx_0 + lx_1 z + \cdots + lx_{n-1}z^{n-1},$$

and, therefore,

$$R_{lx} = \begin{pmatrix} lx_0 & lx_1 & \cdots & lx_{n-1} \\ a\sigma(lx_{n-1}) & \sigma(lx_0) & \cdots & \sigma(lx_{n-2}) \\ \vdots & \vdots & \ddots & \vdots \\ a\sigma^{n-1}(lx_1) & a\sigma^{n-1}(lx_2) & \cdots & \sigma^{n-1}(lx_0) \end{pmatrix}$$

$$= \begin{pmatrix} l & 0 & \cdots & 0 \\ 0 & \sigma(l) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma^{n-1}(l) \end{pmatrix} \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ a\sigma(x_{n-1}) & \sigma(x_0) & \cdots & \sigma(x_{n-2}) \\ \vdots & \vdots & \ddots & \vdots \\ a\sigma^{n-1}(x_1) & a\sigma^{n-1}(x_2) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}$$

$$= R_l R_x.$$

Similarly, it is easy to check that $R_{xl} = R_x R_l$ and so

$$M_A(xl) = M_A(x)M_A(l) = M_A(l)M_A(x)$$

since $M_A(x)$ belongs to a commutative subfield of A for all x. □

We recall that for $x = x_0 + x_1 z + \cdots x_{n-1} z^{n-1}$, the map

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

for some $l \in L$ such that $N_{L/F}(l) = 1$, is an automorphism of A. Using the following lemma we can write this map as

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

for some $m \in L$ and we denote the map by φ_m.

Lemma 4.2.4. *Let L/F be a cyclic field extension of degree n. If $l \in L$ is such that $N_{L/F}(l) = 1$ then for all $k \in \{0, 1, \ldots, n-1\}$*

$$l\sigma(l) \ldots \sigma^k(l) = m\sigma^{k+1}(m)^{-1}$$

for some $m \in L$.

Proof. The case $k = 0$ is Hilbert's Theorem 90 and, by induction,

$$\begin{aligned} l\sigma(l) \ldots \sigma^{k-1}(l)\sigma^k(l) &= m\sigma^k(m)^{-1}\sigma^k(m\sigma(m)^{-1}) \\ &= m\sigma^k(m)^{-1}\sigma^k(m)\sigma^{k+1}(m)^{-1} \\ &= m\sigma^{k+1}(m)^{-1}. \end{aligned}$$

□

Proposition 4.2.5. *$M_A(\varphi_m(x)) = M_A(x)$ for all $x \in A$.*

Proof. If R_m is the matrix

$$R_m = \begin{pmatrix} m & 0 & \cdots & 0 \\ 0 & \sigma(m) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma^{n-1}(m) \end{pmatrix}$$

then $R_m^{-1} = R_{m^{-1}}$ and it is easy to check that

$$R_{\varphi_m(x)} = R_m R_x R_m^{-1},$$

so the result follows. □

We 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 $j = 0, \ldots, n-1$. We saw in the proof of Proposition 4.2.1 that

$$R_x = A R_{\sigma_A(x)} B$$

where

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & a^{-1} \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

and

$$B = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ a & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

In fact we have $B = A^{-1}$ and so $R_{\sigma_A(x)} = A R_x A^{-1}$. It follows that

$$R_{\sigma_A^j(x)} = A^j R_x A^{-j}$$

hence we also have $M_A(\sigma_A^j(x)) = M_A(x)$ for all $x \in A$.

Not all automorphisms of A satisfy the property in Proposition 4.2.5. Recall from Corollary 3.2.9 that, if there exists an element $l \in L$ such that $\sigma^j(a) = N_{L/F}(l)a$ for some $j \in \{1, \ldots, n-1\}$, then the map θ_l^j which sends $x_0 + x_1 z + \cdots + x_{n-1} z^{n-1}$ to

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

is an automorphism. For ease of notation, we define

$$l_0 = 1; \qquad l_i = l_{i-1} \sigma^{i-1}(l),$$

for $1 \leq i \leq n-1$. Therefore we can write

$$\theta_l^j(\sum_{i=0}^{n-1} x_i z^i) = \sum_{i=0}^{n-1} \sigma^j(x_i) l_i z^i.$$

Theorem 4.2.6. *For all $x \in A$ we have*

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

Proof. To simplify notation we will only show the case $j = 1$ since the other cases are completely similar. First extend the automorphism σ to $\mathrm{Mat}_n(L)$ by applying it component-wise on matrix entries. If we have

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

then

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

and so $\sigma(M_A(x)) = \mathrm{Det}(\sigma(R_x))$. Now θ_l^1 maps $x_0 + x_1 z + \cdots + x_{n-1} z^{n-1}$ to

$$\sigma(x_0) + \sigma(x_1) l_1 z + \sigma(x_2) l_2 z^2 + \cdots + \sigma(x_{n-1}) l_{n-1} z^{n-1}$$

and so

$$R_{\theta_l^1(x)} = \begin{pmatrix} \sigma(x_0) & \sigma(x_1)l_1 & \cdots & \sigma(x_{n-1})l_{n-1} \\ a\sigma^2(x_{n-1})\sigma(l_{n-1}) & \sigma^2(x_0) & \cdots & \sigma^2(x_{n-2})\sigma(l_{n-2}) \\ \vdots & \vdots & \ddots & \vdots \\ ax_1\sigma^{n-1}(l_1) & ax_2\sigma^{n-1}(l_2) & \cdots & x_0 \end{pmatrix}.$$

From the definition of θ_l^1 we know that $\sigma(a) = N_{L/F}(l)a$. Also notice that

$$\begin{aligned} l_i N_{L/F}(l)^{-1} &= l\sigma(l) \ldots \sigma_{i-1}(l) N_{L/F}(l)^{-1} \\ &= \left(\sigma^i(l) \ldots \sigma^{n-1}(l)\right)^{-1} \\ &= \sigma^i(l_{n-i})^{-1}, \end{aligned}$$

for all $1 \leq i \leq n-1$. Replacing a by $\sigma(a)N_{L/F}(l)^{-1}$, we get

$$\begin{pmatrix} \sigma(x_0) & \sigma(x_1)l_1 & \cdots & \sigma(x_{n-1})l_{n-1} \\ \sigma(a)\sigma^2(x_{n-1})l_1^{-1} & \sigma^2(x_0) & \cdots & \sigma^2(x_{n-2})\sigma(l_{n-2}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma(a)x_1l_{n-1}^{-1} & \sigma(a)x_2\sigma(l_{n-2})^{-1} & \cdots & x_0 \end{pmatrix}.$$

Let M_l be the matrix

$$\begin{pmatrix} l\sigma(l)\ldots\sigma^{n-2}(l) & 0 & \cdots & 0 \\ 0 & \sigma(l)\ldots\sigma^{n-2}(l) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

then its inverse is

$$(M_l)^{-1} = \begin{pmatrix} l^{-1}\sigma(l)^{-1}\ldots\sigma^{n-2}(l)^{-1} & 0 & \cdots & 0 \\ 0 & \sigma(l)^{-1}\ldots\sigma^{n-2}(l)^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Moreover, it is straightforward to check that

$$R_{\theta_l^1(x)} = M_l\sigma(R_x)(M_l)^{-1}.$$

Hence $M_A(\theta_m^1(x)) = \sigma(M_A(x))$. □

4.3 Some Identities for the Degree 3 Case

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

$$x = x_0 + x_1z + x_2z^2,$$
$$y = y_0 + y_1z + y_2z^2,$$
$$w = w_0 + w_1z + w_2z^2,$$

for $x_i, y_i, w_i \in L$. Explicitly we have

$$M_A(x) = N_{L/F}(x_0) + aN_{L/F}(x_1) + a^2N_{L/F}(x_2) - aTr_{L/F}(x_0\sigma(x_1)\sigma^2(x_2)).$$

We can linearise this to get a map $M_A(x;y)$ which is quadratic in x and linear in y:

$$M_A(x;y) = N_{L/F}(x_0;y_0) + aN_{L/F}(x_1,y_1) + a^2N_{L/F}(x_2,y_2) - af(x;y),$$

where

$$N_{L/F}(x_i;y_i) = x_i\sigma(x_i)\sigma^2(y_i) + x_i\sigma(y_i)\sigma^2(x_i) + y_i\sigma(x_i)\sigma^2(x_i)$$

and

$$\begin{aligned} f(x;y) = {} & Tr_{L/F}(x_0\sigma(x_1)\sigma^2(y_2)) + Tr_{L/F}(x_0\sigma(y_1)\sigma^2(x_2)) \\ & + Tr_{L/F}(y_0\sigma(x_1)\sigma^2(x_2)). \end{aligned}$$

We can get the full linearisation $M_A(x,y,w)$ by

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

where

$$\begin{aligned} N_{L/F}(x_i,y_i,w_i) = {} & x_i\sigma(y_i)\sigma^2(w_i) + x_i\sigma(w_i)\sigma^2(y_i) + y_i\sigma(x_i)\sigma^2(w_i) \\ & + y_i\sigma(w_i)\sigma^2(x_i) + w_i\sigma(x_i)\sigma^2(y_i) + w_i\sigma(y_i)\sigma^2(x_i) \end{aligned}$$

and

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

The map $M_A(x,y,w)$ is symmetric in all three variables. Since A is unital, we have the maps T_A and S_A defined in Section 4.1.2:

$$T_A(x) := M_A(1;x) = Tr_{L/F}(x_0),$$

and

$$S_A(x) := M_A(x;1) = Tr_{L/F}(x_0)\sigma(x_0) - aTr_{L/F}(x_1\sigma(x_2)).$$

The linearisation of T_A is

$$\begin{aligned} T_A(x,y) :&= T_A(x)T_A(y) - M_A(1,x,y) \\ &= Tr_{L/F}(x_0y_0) + aTr_{L/F}(\sigma(x_1)\sigma^2(y_2)) + aTr_{L/F}(\sigma(y_1)\sigma^2(x_2)) \end{aligned}$$

and the linearisation of S_A is given by

$$\begin{aligned} S_A(x,y) := M_A(x,y,1) = Tr_{L/F}(x_0\sigma(y_0)) + Tr_{L/F}(y_0\sigma(x_0)) \\ - aTr_{L/F}(x_1\sigma(y_2)) - aTr_{L/F}(y_1\sigma(x_2)). \end{aligned}$$

From Equations (4.2), (4.7) and (4.8), respectively, we have

$$\begin{aligned} T_A(1) &= S_A(1) = 3, \\ T_A(1,y) &= T_A(y), \\ S_A(x,y) &= T_A(x)T_A(y) - T_A(x,y). \end{aligned}$$

We also have the quadratic sharp map, $x^\sharp = x^2 - T_A(x)x + S_A(x)$. Explicitly, this is

$$\begin{aligned} x^\sharp = \sigma(x_0)\sigma^2(x_0) - a\sigma(x_1)\sigma^2(x_2) \\ + (ax_2\sigma^2(x_2) - \sigma^2(x_0)x_1)z \\ + (x_1\sigma(x_1) - \sigma(x_0)x_2)z^2 \end{aligned}$$

and its linearisation is

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

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

Proposition 4.3.1. *Suppose that $x \in L$. Then*

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

(ii) $x\sharp y = \sigma(x_0)\sigma^2(y_0) + \sigma(y_0)\sigma^2(x_0) - \sigma^2(x_0)y_1 z - \sigma(x_0)y_2 z^2$,

(iii) $1\sharp y = T_A(y)1 - y$,

(iv) $T_A(x\sharp y) = S_A(x, y)$

for all $y \in A$.

Proof. (i) For $x = x_0 + 0z + 0z^2 \in L$ we have $T_A(x, y) = Tr_{L/F}(x_0 y_0)$ for all $y \in A$, and $x^\sharp = \sigma(x_0)\sigma^2(x_0)$. Hence

$$T_A(x^\sharp, y) = Tr_{L/F}(\sigma(x_0)\sigma^2(x_0)y_0) = M_A(x, y).$$

(ii) is a straightforward calculation and (iii) and (iv) follow directly from (ii) and the definitions. □

Proposition 4.3.2. *If either* x *or* y *belong to* L *then*

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

for all $w \in A$.

Proof. It suffices to show that if $x \in L$ then $T_A(x\sharp y, w) = M_A(x, y, w)$, since $x\sharp y = y\sharp x$ implies that

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

whenever $y \in L$. Suppose $x \in L$, then by the previous proposition and the definition of T_A we have

$$\begin{aligned} T_A(x\sharp y, w) &= Tr_{L/F}(\sigma(x_0)\sigma^2(y_0)w_0 + \sigma(y_0)\sigma^2(x_0)w_0) \\ &\quad - aTr_{L/F}(x_0\sigma(y_1)\sigma^2(w_2)) - aTr_{L/F}(x_0\sigma(w_1)\sigma^2(y_2)) \\ &= M_A(x, y, w). \end{aligned}$$

The calculation is similar for $y \in L$. □

Theorem 4.3.3. *Every element* $x \in A$ *satisfies* $x^\sharp x = M_A(x)$.

Proof. The proof is a straightforward calculation. Calculating the first component of $x^\sharp x$, i.e., the term with no z. This is

$$\begin{aligned}
&\sigma(x_0)\sigma^2(x_0)x_0 - a\sigma(x_1)\sigma^2(x_2)x_0 + x_2\sigma^2(x_2)a\sigma(x_2)a \\
&- \sigma^2(x_0)x_1\sigma(x_2)a + x_1\sigma(x_1)\sigma^2(x_1)a - \sigma(x_0)x_2\sigma(x_1)a \\
&= N_L(x_0) + aN_L(x_1) + a^2N_L(x_2) - aTr_L(x_0\sigma(x_1)\sigma^2(x_2)) \\
&= M_A(x).
\end{aligned}$$

On the other hand the z component of $x^\sharp x$ is

$$\begin{aligned}
&\sigma(x_0)\sigma^2(x_0)x_1 - a\sigma(x_1)\sigma^2(x_2)x_1 + x_2\sigma^2(x_2)a\sigma(x_0) \\
&- \sigma^2(x_0)x_1\sigma(x_0) + x_1\sigma(x_1)\sigma^2(x_2)a - \sigma(x_0)x_2\sigma^2(x_2)a
\end{aligned}$$

which is equal to zero. Similarly, the z^2 term of $x^\sharp x$ is

$$\begin{aligned}
&\sigma(x_0)\sigma^2(x_0)x_2 - a\sigma(x_1)\sigma^2(x_2)x_2 + x_2\sigma^2(x_2)a\sigma(x_1) \\
&- \sigma^2(x_0)x_1\sigma(x_1) + x_1\sigma(x_1)\sigma^2(x_0)a - \sigma(x_0)x_2\sigma^2(x_0)a
\end{aligned}$$

which is also zero. □

Corollary 4.3.4. *Every element $x \in A$ satisfies an equation*

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

Proof. This follows from the previous theorem and the definition of $x^\sharp$. □

Chapter 5

Generalised First Tits Construction

We now look at a possible generalisation of the first Tits construction. This generalisation exhibits some interesting properties and its construction fits in nicely with the theme of this thesis. The contents of this chapter were inspired by a private communication with Petersson [43].

5.1 The Classical Construction Using Cubic Norms

In this section, we will give a slightly different definition of the first Tits construction to that in Chapter 2, Section 4, this time using the cubic norm form on an associative algebra of degree 3. This definition can also be found in McCrimmon's book ([38, Ch II.4]) but we will give the main details here. Since there are quite a lot of identities associated with cubic forms, we will recall the important ones here for ease of reference.

Let F be a field of characteristic not 2 or 3 and let A be a unital, associative F-algebra of degree 3, equipped with a cubic norm form N_A. We recall

the linearisation $N_A(x;y)$ given by the directional derivative

$$N_A(x;y) := \partial_y N_A|_x,$$

in the direction of y, evaluated at x. This map is quadratic in x and linear in y and linearises to the trilinear map

$$N_A(x,y,z) := N_A(x+z;y) - N_A(x;y) - N_A(z;y),$$

for all $x, y, z \in A$. $N_A(x,y,z)$ is symmetric in all three variables. We also have the associated maps

$$\begin{aligned} Tr_A(x) &:= N_A(1;x), \\ Tr_A(x,y) &:= T_A(x)T_A(y) - N_A(1,x,y), \\ S_A(x) &:= N_A(x;1), \\ S_A(x,y) &:= S_A(x+y) - S_A(x) - S_A(y) = N_A(x,y,1), \end{aligned}$$

for all $x, y \in A$, and the adjoint map, $\sharp : A \to A$, given by

$$x^\sharp := x^2 - Tr_A(x)x + S_A(x)1,$$

for all $x \in A$. The following identities hold in all scalar extensions.

$$\begin{aligned} x^3 - T_A(x)x^2 + S_A(x) - N_A(x)1 &= 0, \\ T_A(x^\sharp, y) &= N_A(x;y), \\ T_A(x,y) &= T_A(xy), \\ (x^\sharp)^\sharp &= N_A(x)x, \\ (xy)^\sharp &= y^\sharp x^\sharp, \\ N_A(x^\sharp) &= N_A(x)^2. \end{aligned}$$

for all $x, y \in A$. The adjoint map is a quadratic map which bilinearises to

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

The unit element of A, denoted 1_A, satisfies

$$1_A^\sharp = 1_A, \quad \text{and} \quad 1_A \times x = T_A(x)1_A - x,$$

for all $x \in A$. A quadratic U-operator can be defined as

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

with linearisation

$$U_{x,y} := U_{x+y} - U_x - U_y,$$

for all $x, y \in A$. We can then define a bilinear product on A in terms of the U-operator:

$$x \circ y := U_{x,y} 1_A.$$

A routine, but tedious, verification shows that $x \circ y = xy + yx$, for all $x, y \in A$. Therefore, the F-vector space structure of A endowed with the multiplication $x \bullet y := \frac{1}{2}(x \circ y)$ is, in fact, the Jordan algebra A^+. The norm of A permits Jordan composition on the U-operator, i.e.,

$$N_A(U_x y) = N_A(x)^2 N_A(y),$$

for all $x, y \in A$.

Remark 5.1.1. In fact, Jordan algebras can be defined over commutative rings using a quadratic U-operator instead of the usual bilinear product. When the ground ring contains $1/2$, these *quadratic* Jordan algebras are equivalent to those defined by the bilinear product. This quadratic theory was developed by McCrimmon in [37] and gives a characteristic-free approach to Jordan algebras.

Given the above ingredients, the first Tits construction proceeds as follows: we pick an element $\mu \in F^\times$ and define the F-vector space

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

where each component A_i is a copy of A. By identifying A with the first component A_0, we can extend the unit element, norm and adjoint of A to J as follows

$$\begin{aligned} 1 &= (1_A, 0, 0), \\ N(x) &:= N_A(x_0) + \mu N_A(x_1) + \mu^{-1} N_A(x_2) - T_A(x_0 x_1 x_2), \\ x^\sharp &:= (x_0^\sharp - x_1 x_2, \mu^{-1} x_2^\sharp - x_0 x_1, \mu x_1^\sharp - x_2 x_0), \end{aligned}$$

for $x = (x_0, x_1, x_2) \in J, x_i \in A$. This gives rise to a linearised trace

$$\begin{aligned} T(x, y) &= T_A(x_0 y_0) + T_A(x_1 y_2) + T_A(y_1 x_2), \\ T(x) &:= T(x, 1) = T_A(x_0), \end{aligned}$$

for $y = (y_0, y_1, y_2) \in J$. The quadratic sharp map linearises to

$$\begin{aligned} x \times y = \big(&x_0 \times y_0 - x_1 y_2 - y_1 x_2, \mu^{-1}(x_2 \times y_2) - x_0 y_1 - y_0 x_1, \\ &\mu(x_1 \times y_1) - x_2 y_0 - y_2 x_0\big). \end{aligned}$$

We can then introduce a quadratic U-operator on J defined by

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

for all $x, y \in J$. This allows us to define a bilinear product on J by $x \circ y := U_{x,y}1$. A routine calculation shows that

$$\begin{aligned} x \circ y = \big(&x_0 \circ y_0 + \overline{x_1 y_2} + \overline{x_2 y_1}, \\ &\overline{x_0} y_1 + \overline{y_0} x_1 + \mu^{-1}(x_2 \times y_2), \\ &\overline{x_0} y_2 + \overline{y_0} x_2 + \mu(x_1 \times y_1)\big), \end{aligned}$$

where $\overline{x} := T_A(x) - x$. Setting $x \bullet y = \frac{1}{2}(x \circ y)$, we see that this agrees with the definition of multiplication in Chapter 2, Equation (2.1).

5.2 The Generalised Construction

Following the approach in the previous section, we generalise the first Tits construction. Let A be an associative algebra of degree 3 with cubic norm N_A and pick an invertible element $\mu \in A^\times$ rather than in $F^\times$. Define the following vector-space over F:

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

where each component A_i is a copy of A. As before, we identify A with A_0 above and define a map $M : P \to A$ by

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

for $x_i \in A$. This map satisfies $M((x_0, 0, 0)) = N_A(x_0)$ so we may say that the restriction of M to A is N_A. We can also extend the adjoint map by defining

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

for $x = (x_0, x_1, x_2), x_i \in A$. This yields the linearised sharp and trace maps on P:

$$\begin{aligned} x \times y = \big(&x_0 \times y_0 - x_1y_2 - y_1x_2, \mu^{-1}(x_2 \times y_2) - x_0y_1 - y_0x_1, \\ &\mu(x_1 \times y_1) - x_2y_0 - y_2x_0\big), \\ T(x, y) = &\, T_A(x_0y_0) + T_A(x_1y_2) + T_A(y_1x_2), \\ T(x) = &\, T_A(x_0), \end{aligned}$$

for $(x_0, x_1, x_2), (y_0, y_1, y_2) \in P$. We define a multiplication, denoted $\circ$, on $P(A, N_A, \mu)$ by putting

$$x \circ y := x \times y + T(x)y + T(y)x - (T(x)T(y) - T(x, y))1, \tag{5.1}$$

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

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

for $x = (x_0, x_1, x_2)$ and $y = (y_0, y_1, y_2)$, which is similar to the bilinear product in the classical first Tits construction.

Remark 5.2.1. If, in the definition of the map $\sharp : P \to P$, we change the position of μ and μ^{-1}, this will make a difference in the bilinear product if A is noncommutative and μ does not belong to the centre of A. For example, if we define

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

and follow through with this definition of $\sharp$, we would arrive at the following definition of the multiplication:

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

We have the intermediate form $S_A : A \to F$ defined by $S_A(x_0) = N_A(x; 1)$, which is quadratic. This linearises 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 $x_0 \in A$ ([38, ch II.4]).

Proposition 5.2.2. *If we extend the map S_A to $P(A, N_A, \mu)$ by defining $S(x) := M(x; 1)$, we have $S(x) = T(x^\sharp)$ and the linearisation $S(x, y)$ satisfies*

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

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

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

$$\begin{aligned} M(x; y) = &N_A(x_0; y_0) + \mu N_A(x_1; y_1) + \mu^{-1} N_A(x_2; y_2) \\ &- T_A(x_0 x_1 y_2) - T_A(x_0 y_1 x_2) - T_A(y_0 x_1 x_2), \end{aligned}$$

and hence

$$S(x) = M(x; 1) = N_A(x_0; 1) - T_A(x_1 x_2) = S_A(x_0) - T_A(x_1 x_2).$$

On the other hand

$$\begin{aligned} T(x^\sharp) &= T_A(x_0^\sharp - x_1 x_2) = T_A(x_0^\sharp) - T_A(x_1 x_2) \\ &= S_A(x_0) - T_A(x_1 x_2) = S(x), \end{aligned}$$

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 $x_0, y_0 \in A$. Therefore, linearising $S(x)$ gives

$$\begin{aligned} S(x, y) &= S_A(x_0, y_0) - T_A(x_1 y_2) - T_A(y_1 x_2) \\ &= T_A(x_0)T_A(y_0) - T_A(x_0, y_0) - T_A(x_1 y_2) - T_A(y_1 x_2) \\ &= T(x)T(y) - T(x, y), \end{aligned}$$

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

Lemma 5.2.3. *Let $x = (x_0, x_1, x_2) \in P(A, N_A, \mu), x_i \in A$. Then $x \times 1 = T(x) - x$.*

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

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

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

Proposition 5.2.4. *For all $x \in P(A, N_A, \mu)$ define the quadratic operator $U_x : P(A, N_A, \mu) \to P(A, N_A, \mu)$ by*

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

for all $y \in P(A, N_A, \mu)$. Then $x \circ y = U_{x,y}1$.

Proof. First we calculate

$$\begin{aligned} U_x 1 &= T(x, 1)x - x^\sharp \times 1 \\ &= T(x)x - (T(x^\sharp) - x^\sharp) \\ &= T(x)x - S(x) + x^\sharp, \end{aligned}$$

using Lemma 5.2.3 and Proposition 5.2.2. Linearising then gives

$$\begin{aligned} U_{x,y}1 &= U_{x+y}1 - U_x 1 - U_y 1 \\ &= T(x+y)(x+y) - S(x+y) + (x+y)^\sharp \\ &\quad - T(x)x + S(x) - x^\sharp - T(y)y + S(y) - y^\sharp \\ &= T(x)y + T(y)x - S(x, y) + x \times y, \end{aligned}$$

using the linearisations of $S(x)$ and $x^\sharp$. This expression is equal to that for $x \circ y$ in (5.1), since $S(x, y) = T(x)T(y) - T(x, y)$ by Proposition 5.2.2. □

Theorem 5.2.5. *Consider $x \in A$ as an element of $P(A, N_A, \mu)$, i.e., $x = (x, 0, 0)$, then for all $y \in P(A, N_A, \mu)$ 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

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

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

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

Now since A is a classical cubic norm structure we know that $N_A(U_x y_0) = N_A(x)^2 N_A(y_0)$ and also $N_A(x^\sharp y_1) = N_A(x)^2 N_A(y_1)$ and similarly $N_A(y_2 x^\sharp) = N_A(x)^2 N_A(y_2)$ so if we can show that

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

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

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

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. □

Chapter 6

Finite Semifields

6.1 Preliminaries

In this chapter we explore the construction of a nonassociative cyclic algebra over a finite field. This construction was previously discovered by Sandler in [48], where it was studied in the context of *finite semifields*. During the preparation of this thesis, some results overlapping with this chapter were published in [15], [16] and [26]. However, most of them treat these algebras in the more general setting of semilinear transformations or skew-polynomial rings, whereas the results obtained here are straight corollaries from the previously developed theory.

A finite semifield is a finite set S with two operations, addition and multiplication, which satisfy the following axioms:

1. $(S, +)$ is a group with identity 0.
2. If a and b are elements of S with $ab = 0$ then $a = 0$ or $b = 0$.
3. Distributivity holds: $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b, c \in S$.
4. There is a multiplicative identity 1: $a1 = 1a = a$ for all $a \in S$.

It can be shown that semifields posses a vector space structure over some prime field $F = \mathbb{F}_p$, so the number of elements in a finite semifield S is p^n where n is the dimension of S over F. This implies that a semifield is simply a unital division algebra with finitely many elements. A famous theorem of Wedderburn [35] states that every finite, associative division algebra is a finite field. Hence, any finite semifield is necessarily either a finite field or it is *not* associative, i.e., there exist elements $a, b, c \in S$ such that $(ab)c \neq a(bc)$. A semifield which is not a finite field is called a *proper semifield*. The number of elements in a semifield S is called the *order* of S. For a survey of results on finite semifields we refer the reader to [13] or [27].

Due to their connections with projective geometries, semifields are usually classified up to *isotopy*. In fact, every proper semifield coordinatizes a non-Desarguesian projective plane and two semifields coordinatize the same projective plane if and only if they are isotopic [3]. Two semifields, S_1, S_2, are isotopic if there exist linear bijections $f, g, h : S_1 \to S_2$, such that

$$f(x * y) = g(x) \circ h(y),$$

where $*$ and $\circ$ denote the multiplications in S_1 and S_2 respectively. The concept of isotopy was introduced by Albert in [2] and plays an important role in the theory of nonassociative structures.

Finite semifields have also found applications in coding theory [12], [28], [20] and combinatorics and graph theory [36]. In [57], Wene mentions that little is known about automorphisms of finite semifields, however, he mentions partial determinations by Dickson [17], Menichetti [39, 41], Kleinfeld [29], Knuth [31] and Burmester [11]. In this chapter, we look at finite extensions L/F of prime degree and compute the automorphism groups and isomorphism classes of Sandler's semifields in this case. The methods used are purely algebraic and rely heavily on the results from Chapter 3.

6.2 Semifields from Nonassociative Cyclic Algebras

Given a field F and a cyclic extension L of degree r, it is always possible to construct a nonassociative cyclic algebra of degree r which is division. To do this, simply pick an element $a \in L$ which does not belong to any proper subfield of L. Then $1, a, a^2, \ldots, a^{r-1}$ are linearly independent over F and, by Theorem 3.2.10, $(L/F, \sigma, a)$ is a division algebra. In particular, this is true even if F is a finite field. Throughout this chapter we let $\mathbb{F}_q$ denote the finite field with q elements.

Theorem 6.2.1. *Let q be a prime power, i.e., $q = p^n$ for some prime p and $n \geq 1$, and let r be an integer strictly bigger than 1. There exists a finite semifield of order q^{r^2} with nucleus $\mathbb{F}_{q^r}$ and center $\mathbb{F}_q$.*

Proof. Let $F = \mathbb{F}_q$ then by the above paragraph we can construct a nonassociative cyclic algebra of degree r over F which will be a division algebra. This is done by taking a field extension $L = \mathbb{F}_{q^r}$ of degree r over F and forming the algebra $A = (L/F, \sigma, a)$, where $a \in L$ does not belong to a proper subfield of L. The semifield A has nucleus L by Corollary 3.2.6, and centre F by Proposition 3.2.7. □

Remark 6.2.2. There may be many non-isomorphic finite semifields of order q^{r^2} arising from nonassociative cyclic algebras. For example, if r is a prime number, then by Corollary 3.2.11 any choice of $a \in L \setminus F$ will yield a division algebra. Also, two semifields of the same order can have very different structures, for example, consider $q = 2$ and $r = 4$ in Theorem 6.2.1. Then we can form a semifield with $q^{r^2} = 2^{16}$ elements which has nucleus $\mathbb{F}_{2^4}$ and center $\mathbb{F}_2$. We can also construct a finite semifield with 2^{16} elements by letting $q = 16$ and $r = 2$. In this case the nucleus will be $\mathbb{F}_{2^8}$ and the center will be $\mathbb{F}_{16}$. In fact, this shows that the two semifields mentioned are not even isotopic since isotopic semifields have isomorphic nuclei (see [10], for example).

If L/F is a cyclic extension of prime degree then any choice of $a \in L \setminus F$ will give a finite semifield of the form $(L/F, \sigma, a)$, however when the degree of the extension is not prime, the choice of a making $(L/F, \sigma, a)$ a semifield becomes more limited.

Theorem 6.2.3. *Let F be a finite field and let L/F be a cyclic extension of degree r. Then $(L/F, \sigma, a)$ is a finite semifield if and only if a does not belong to a proper subfield of L.*

Proof. Suppose a does not belong to any proper subfield of L. Then the elements $1, a, a^2, \ldots, a^{r-1}$ are linearly independent over F, otherwise the field extension $F(a) \subseteq L$ would have degree strictly less than r, contradicting the hypothesis. Theorem 3.2.10 implies that $(L/F, \sigma, a)$ is a semifield. Conversely, let $a \in E$ where

$$F \subsetneqq E \subsetneqq L,$$

and suppose that $A = (L/F, \sigma, a)$ is a semifield. The left, right and middle nuclei of A are associative subalgebras of a finite division algebra, hence by Wedderburn's Theorem, they are finite fields. However, by Proposition 3.2.3,

$$Nuc_l(A) = L \oplus Lz^s \oplus Lz^{2s} \oplus \cdots \oplus Lz^{r-s},$$

where σ^s is the generator of the Galois group of the fixed field of E. This is a noncommutative subalgebra, thus giving us a contradiction. □

Given a prime power q and an prime r, the natural question arises of how many non-isomorphic semifields of order q^{r^2} can be constructed in this manner. In order to answer this question we frequently make use of Proposition 3.2.8 which states $(L/F, \sigma, a) \cong (L/F, \sigma, b)$ iff $\sigma^i(a) = N_{L/F}(l)b$ for some $0 \leq i \leq r-1$ and some $l \in L^\times$. For ease of notation, we will denote $(L/F, \sigma, a)$ by A_a when F and L are clear.

Example 6.2.4. Let $F = \mathbb{F}_2$ and let $L = \mathbb{F}_4$, then we can write

$$L = \{0, 1, T, 1 + T\}$$

where $T^2 + T + 1 = 0$. For the algebra A_a we can either choose $a = T$ or $a = 1+T$, both choices will give a division algebra since L is a field extension of prime degree. We also know that $A_a \cong A_b$ if and only if $\sigma(a) = N_{L/F}(l)b$, but since we are working with finite fields the norm map

$$N_{L/F} : L^\times \to F^\times$$

is surjective, so $N_{L/F}(l) = 1$ for all $l \in L^\times$. The statement then reduces to $A_a \cong A_b$ if and only if $\sigma(a) = b$. Now

$$\sigma(T) = T^2 = 1 + T.$$

Therefore $A_T \cong A_{1+T}$ so, up to isomorphism, there is only one semifield that can be constructed as a nonassociative cyclic algebra from the field F and the extension L.

This semifield is well known and was one of the first examples of semifields of order 16 (for example see [31, §2.2]). The fact that the norm map is surjective for finite field extensions of finite fields allows us to restate the condition from Proposition 3.2.8 as follows.

Corollary 6.2.5. *Let F be a finite field and L a finite extension of F. If $A_a := (L/F, \sigma, a)$ and $A_b := (L/F, \sigma, b)$ are two nonassociative cyclic algebras, then $A_a \cong A_b$ iff $\sigma^i(a) = kb$ for some $0 \leq i \leq r-1$ and some $k \in F^\times$.*

We recall a simple lemma concerning when a finite field contains certain roots of unity.

Lemma 6.2.6. *Let $F = \mathbb{F}_q$ where q is a prime power and let r be a prime number. F contains a primitive rth root of unity if and only if r divides $q-1$.*

Proof. The group $F^\times$ is cyclic and hence it contains a subgroup of order r if and only if r divides $|F^\times| = q - 1$. Since r is prime the elements of this subgroup will be the rth roots of unity. □

It is well known that if F contains a primitive rth root of unity and L is a cyclic field extension of F of degree r (where r is prime to the characteristic of F) then $L = F(\omega)$, where ω is a root of the irreducible polynomial $x^r - c$ for some $c \in F^\times$ (see [33, §VI.6]).

Lemma 6.2.7. *Let r be a prime number and let F be a field of characteristic not r such that F contains a primitive rth root of unity. Let $L = F(\omega)$ be a cyclic field extension of F with Galois group $\langle\sigma\rangle$. The eigenvalues of the automorphisms σ^i are precisely the rth roots of unity. Moreover the only possible eigenvectors are scalar multiples of the elements ω^i for $0 \leq i \leq r-1$.*

Proof. Let the elements $1, \omega, \ldots, \omega^{r-1}$ be a basis for L/F. The action of σ on ω is given by

$$\sigma(\omega) = \zeta\omega,$$

where ζ is a primitive rth root of unity. Hence

$$\sigma^i(\omega) = \zeta^i\omega$$

and

$$\sigma^i(\omega^j) = \sigma^i(\omega)^j = \zeta^{ij}\omega^j,$$

for all $0 \leq i, j, \leq r-1$. So the rth roots of unity are indeed eigenvalues for the automorphisms σ^i with eigenvectors ω^j. Now suppose that k is another eigenvalue for σ^i, i.e., $\sigma^i(x) = kx$ for some $x \in L^\times$. Applying the norm map to both sides gives

$$N_{L/F}(\sigma^i(x)) = N_{L/F}(kx) = k^r N_{L/F}(x).$$

However, $N_{L/F}(\sigma^i(x)) = N_{L/F}(x)$ for all i, which implies that $k^r = 1$, i.e., k is an rth root of unity and $k = \zeta^j$ for some $0 \leq j \leq r-1$. With our chosen basis of L/F the matrix of the automorphism σ^i is

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta^i & 0 & \cdots & 0 \\ 0 & 0 & \zeta^{2i} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \zeta^{(r-1)i} \end{pmatrix}.$$

The equation $\sigma^i(x) = \zeta^j x$ in matrix form becomes

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta^i & 0 & \cdots & 0 \\ 0 & 0 & \zeta^{2i} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \zeta^{(r-1)i} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{r-1} \end{pmatrix} = \zeta^j \Big(x_0, x_1, x_2, \ldots, x_{r-1}\Big)^T,$$

where $x = (x_0, x_1, \ldots, x_{r-1})$ is written as an r-tuple with respect to our F-basis. This gives

$$\Big(x_0, \zeta^i x_1, \zeta^{2i} x_2, \ldots, \zeta^{(r-1)i} x_{r-1}\Big) = \Big(\zeta^j x_0, \zeta^j x_1, \zeta^j x_2, \ldots, \zeta^j x_{r-1}\Big),$$

which implies that all the x_k are zero except for one, say x_{k_0}, where k_0 is such that $k_0 i = j \bmod r$. Hence $x = x_{k_0}\omega^{k_0}$, as required. □

Define an equivalence relation on the set $L \setminus F$ by

$$a \sim b \text{ if and only if } (L/F, \sigma, a) \cong (L/F, \sigma, b).$$

We wish to know how many distinct equivalence classes there are in $L \setminus F$ for a given finite field F and extension L of prime degree.

Theorem 6.2.8. *Let $F = \mathbb{F}_q$ and let L be an extension of F of degree r where r is prime and q is a prime power. If r divides $q-1$ then there are*

$$r - 1 + \frac{q^r - q - (q-1)(r-1)}{r(q-1)}$$

equivalence classes of the above equivalence relation. If r does not divide $q-1$ then there are precisely

$$\frac{q^r - q}{r(q-1)}$$

equivalence classes.

Proof. In the case of the semifields defined above, we are looking for elements $a \in L \setminus F$ with $\sigma^i(a) = ka$. Note that $k = 1$ is not relevant for this case since $\sigma^i(a) = a$ if and only if $a \in F$. For each $a \in L \setminus F$ we have

$$(L/F, \sigma, a) \cong (L/F, \sigma, \sigma^i(a))$$

for $0 \leq i \leq r-1$ and

$$(L/F, \sigma, a) \cong (L/F, \sigma, ka)$$

for $k \in F^\times$. If the elements $k\sigma^i(a)$, for $0 \leq i \leq r-1$ and $k \in F^\times$, are all distinct then there are precisely $r(q-1)$ elements in the equivalence class of a. If they are not all distinct then $\sigma^i(a) = ka$ for some i and some $k \in F^\times$. We saw in the proof of Lemma 6.2.7 that if $\sigma^i(a) = ka$ then k is an rth root of unity. We cannot have $k = 1$ so k is a primitive rth root of unity. From Lemma 6.2.6, this happens if and only if r divides $q-1$. Hence, if r does not divide $q-1$ then, from the $q^r - q$ elements in $L \setminus F$, we get

$$\frac{q^r - q}{r(q-1)}$$

equivalence classes. On the other hand, if r does divide $q-1$ then F contains the primitive rth roots of unity and so we may write L as

$$F[T]/(T^r - c)$$

for some $c \in F^\times$. Lemma 6.2.7 tells us that the only elements $a \in L \setminus F$ with $\sigma^i(a) = ka$ are the elements T^j for $1 \leq j \leq r-1$ and scalar multiples of these. Moreover, for each T^j we have $\sigma^i(T^j) = \zeta^{ij}T^j$ and $\zeta^{ij} \in F$ so there are only $q-1$ distinct elements in the equivalence class of each T^j. Hence the $(q-1)(r-1)$ elements kT^j ($k \in F^\times$ and $1 \leq j \leq r-1$) form exactly $r-1$ equivalence classes. Since these are all the elements in $L \setminus F$ that are eigenvectors for the automorphisms σ^i we can deduce that the remaining $q^r - q - (q-1)(r-1)$ elements will form

$$\frac{q^r - q - (q-1)(r-1)}{r(q-1)}$$

equivalence classes. In total we have

$$r - 1 + \frac{q^r - q - (q-1)(r-1)}{r(q-1)}$$

equivalence classes. □

Corollary 6.2.9. *Let $F = \mathbb{F}_q$ and let L be an extension of F of degree r where r is prime and q is a prime power. If r divides $q-1$ then there are*

$$r - 1 + \frac{q^r - q - (q-1)(r-1)}{r(q-1)}$$

non-isomorphic semifields arising from the construction $(L/F, \sigma, a)$. If r does not divide $q-1$ then there are precisely

$$\frac{q^r - q}{r(q-1)}$$

non-isomorphic semifields arising from a nonassociative cyclic algebra of degree r over the field F.

6.3 Automorphisms

Recall from Corollary 3.2.9 that the automorphisms of $(L/F, \sigma, a)$ are given by

$$\sum_{i=0}^{n-1} x_i z^i \mapsto \sum_{i=0}^{n-1} x_i l \sigma(l) \dots \sigma^{i-1}(l) z^i$$

where for some $l \in L$ with $N_{L/F}(l) = 1$. These are all the automorphisms unless there exists an $l' \in L$ such that $\sigma^i(a) = N_{L/F}(l')a$, in which case

$$\sum_{i=0}^{n-1} x_i z^i \mapsto \sum_{i=0}^{n-1} \sigma^i(x_i) l' \sigma(l') \dots \sigma^{i-1}(l') z^i$$

is also an automorphism. Hence the automorphisms of $(L/F, \sigma, a)$ also depend on the existence of elements $k \in F^\times$ such that $\sigma^i(a) = ka$. However, it is clear that the kernel of the norm map $N_{L/F}$ will be isomorphic to a subgroup of the automorphism group of the semifield. We give a proof of the following well-known fact.

Proposition 6.3.1. *Let $F = \mathbb{F}_q$ and let L be an extension of F of degree r, so $L = \mathbb{F}_{q^r}$. The kernel of the norm map $N_{L/F}$ is a cyclic subgroup of order $s = \frac{q^r-1}{q-1}$. Moreover, for each $k \in F^\times$, there are exactly s elements $x \in L$ such that $N_{L/F}(x) = k$.*

Proof. Any subgroup of $L^\times$ is cyclic so all that remains is to work out the number of elements in $\mathrm{Ker}(N_{L/F})$. Explicitly, the norm of an element $x \in L$ is given by

$$N_{L/F}(x) = xx^q x^{q^2} \dots x^{q^{r-1}} = x^{1+q+\dots+q^{r-1}} = x^s.$$

Hence the equation

$$N_{L/F}(x) = x^s = 1,$$

has at most s solutions. Conversely, the group $L^\times$ is cyclic of order $q^n - 1$ so it contains a subgroup order s. Therefore there are at least s elements in $L^\times$ satisfying $x^s = 1$.

For the second claim, let x_i, $1 \leq i \leq s$, be the s elements with norm 1. Fix a nonzero $k \in F^\times$. By the surjectivity of $N_{L/F}$, there exists a $y_k \in L$ such that $N_{L/F}(y_k) = k$. The s elements $y_k x_i$ are distinct, and

$$N_{L/F}(y_k x_i) = N_{L/F}(y_k) N_{L/F}(x_i) = k1.$$

Thus we have at least s elements with norm k for each $k \in F^\times$. Since there are $q-1$ such elements $k \in F^\times$, the $s(q-1) = q^r - 1$ elements $y_k x_i$, for $k \in F$ and $1 \leq i \leq s$, cover all elements of $L^\times$. Therefore, there are exactly s elements of norm k for each $k \in F^\times$. □

Corollary 6.3.2. *Let $F = \mathbb{F}_q$ and let L be an extension of F of prime degree r. If r does not divide $q-1$ then for all $a \in L \setminus F$, $Aut((L/F, \sigma, a)) \cong \mathbb{Z}/s\mathbb{Z}$ where $s = \frac{q^r-1}{q-1}$.*

Proof. All automorphisms of $(L/F, \sigma, a)$ correspond to elements of $\mathrm{Ker}(N_{L/F})$ unless there exists a $k \in F^\times$ with $\sigma^i(a) = ka$ for some $1 \leq i \leq r-1$. It was shown in the proof of Lemma 6.2.7 that any such k is a primitive rth root of unity which cannot happen in F by Lemma 6.2.6. The result now follows from the previous proposition. □

Consider now the case where F and L are as above but r does divide $q-1$. Since F contains all rth roots of unity we may write

$$L = F[T]/(T^r - c)$$

for some $c \in F^\times$. Define the set

$$S := \{\lambda T^j \mid 1 \leq j \leq r-1, \lambda \in F^\times\} \subset L.$$

Corollary 6.3.3. *Let F and L be as above with*

$$L = F[T]/(T^r - c).$$

Then for all $a \in L \setminus (F \cup S)$, $Aut((L/F, \sigma, a)) \cong \mathbb{Z}/s\mathbb{Z}$ where $s = \frac{q^r-1}{q-1}$. If $a \in S$ then $Aut((L/F, \sigma, a))$ is a group of order

$$r\frac{q^r-1}{q-1}.$$

Proof. Lemma 6.2.7 states that the only elements $a \in L \setminus F$ with $\sigma^i(a) = ka$ for some $1 \leq i \leq r-1$ and some $k \in F$ are the elements of S, hence the first claim follows. Now suppose $a = \lambda T^j \in S$. For each $i \in \{0, \ldots, r-1\}$ there exists a unique rth root of unity ζ_i, such that $\sigma^i(a) = \zeta_i a$ (note $\zeta_0 = 1$). There are exactly $\frac{q^r-1}{q-1}$ elements $l \in L$ with $N_{L/F}(l) = \zeta_i$ and each of these elements correspond to a unique automorphism. Therefore, in total we have

$$r\frac{q^r-1}{q-1}$$

automorphisms. □

Example 6.3.4. Let $F = \mathbb{F}_3$ and $L = \mathbb{F}_9$ where

$$L = F[T]/(T^2 - 2) = \{0, 1, 2, T, 2T, T+1, T+2, 2T+1, 2T+2\}.$$

There are two nonisomorphic Sandler semifields for L/F. These are $A_T := (L/F, \sigma, T)$ and $A_{T+1} := (L/F, \sigma, T+1)$. Moreover, $Aut(A_{T+1})$ is the cyclic group of order 4, whereas $Aut(A_T)$ is isomorphic to the group of quaternion units.

Proof. From Corollary 6.2.9, we see that there are 2 nonisomorphic semifields of order 81 arising from the construction $(L/F, \sigma, a)$ and Lemma 6.2.7 implies that two such nonisomorphic semifields are $(L/F, \sigma, T)$ and $(L/F, \sigma, T+1)$.

Denote these two semifields by A_T and A_{T+1} respectively. Now Corollary 6.3.3 tells us that the automorphism group of A_{T+1} is the cyclic group of order 4. However, the automorphism group of A_T is a group of order 8. To calculate what this group is we introduce the following notation.

Let $l \in L$ be such that $N_{L/F}(l) = 1$. Denote by φ_l the automorphism of A_T given by

$$\varphi_l(x_0 + x_1 z) = x_0 + x_1 l z$$

for all $x = x_0 + x_1 z \in A_T$. Now let $m \in L$ be such that $\sigma(T) = N_{L/F}(m)T$. Denote by θ_m the automorphism of A_T given by

$$\theta_m(x_0 + x_1 z) = \sigma(x_0) + \sigma(x_1) m z.$$

Since $\sigma(T) = T^3 = 2T$, we require all those $m \in L$ with $N_{L/F}(m) = 2$. A quick calculation shows that these are:

$$m \in \{1 + T, 1 + 2T, 2 + T, 1 + 2T\}.$$

Moreover, the subset of L consisting of elements with norm 1 is

$$\{1, 2, T, 2T\}.$$

Hence using the above notation the automorphism group will be

$$Aut(A_T) = \{\varphi_1, \varphi_2, \varphi_T, \varphi_{2T}, \theta_{1+T}, \theta_{1+2T}, \theta_{2+T}, \theta_{2+2T}\}.$$

It is easy to check that this is a non-abelian group of order eight, also it has one element of order two, namely φ_2 and the rest of the (non-identity) elements are of order four. The classification of small groups then implies that $Aut(A_T) \cong \mathcal{Q}$, the group of quaternion units. □

Theorem 6.3.5. *Let $F = \mathbb{F}_q$ be a field of characteristic not 2 and let L be a quadratic extension of F. For $a \in L \setminus F$ put $A_a := (L/F, \sigma, a)$. Then $Aut(A_a)$ is the cyclic group of order $q + 1$ or the dicyclic group of order $2q + 2$*

Proof. Write $L = F[T]/(T^2 - c)$ for some $c \in F^\times$. If $a = kT$ for some nonzero $k \in F$ then we know from Corollary 6.3.3 that $Aut(A_a)$ is of order $2(q + 1)$,

otherwise $Aut(A_a)$ is the cyclic group of order $q+1$. We may assume that $a = T$ since $A_a \cong A_{ka}$ for all nonzero $k \in F$. Since $\sigma(T) = -T$ we have the following automorphisms:

$$\varphi_{l_i} : A_a \to A_a : \qquad x_0 + x_1 z \mapsto x_0 + x_1 l_i z,$$

for $x_0 + x_1 z \in A_a$ and $l_i \in L$ such that $N_{L/F}(l_i) = 1$. There are precisely $q+1$ such maps. We also have the automorphisms

$$\theta_{m_j} : A_a \to A_a : \qquad x_0 + x_1 z \mapsto \sigma(x_0) + \sigma(x_1) m_i z$$

for all $m_j \in L$ such that $N_{L/F}(m_j) = -1$. Again, there are precisely $q+1$ such maps. We note the following relations between the automorphisms:

$$\varphi_{l_i} \circ \varphi_{l_j} = \varphi_{l_i l_j}, \qquad \varphi_{l_i} \circ \theta_{m_j} = \theta_{l_i m_j},$$

$$\theta_{m_i} \circ \varphi_{l_j}, = \theta_{m_i \sigma(l_j)} \qquad \theta_{m_i} \circ \theta_{m_j} = \varphi_{m_i \sigma(m_j)}.$$

Recall that we can describe the dicyclic group of order $4n$, denoted Dic_n, by the following presentation:

$$\mathrm{Dic}_n = \langle x, y \mid y^{2n} = 1, x^2 = y^n, x^{-1} y x = y^{-1} \rangle.$$

We claim that $Aut(A_a) \cong \mathrm{Dic}_n$ for $n = (q+1)/2$. First note that the group $\mathrm{Ker}(N_{L/F}) = \{l_i \mid N_{L/F}(l_i) = 1\}$ is cyclic, so pick $l_0 \in \mathrm{Ker}(N_{L/F})$ which generates it as a group. Also pick any m_0 such that $N_{L/F}(m_0) = -1$, then the map

$$\varphi_{l_0} \mapsto y, \qquad \theta_{m_0} \mapsto x$$

is an isomorphism from $Aut(A_a) \to \mathrm{Dic}_q$. Clearly we have

$$(\varphi_{l_0})^{2n} = \varphi_{(l_0)^{2n}} = \varphi_1 = \mathrm{Id}_{A_a}.$$

From this it follows that $(\varphi_{l_0})^n = \varphi_{-1}$ and so

$$(\theta_{m_0})^2 = \varphi_{N_{L/F}(m_0)} = \varphi_{-1} = (\varphi_{l_0})^n.$$

Finally, note that $(\theta_{m_0})^{-1} = \theta_{m_j}$ where m_j is such that $m_j \sigma(m_0) = 1$ and $(\varphi_{l_0})^{-1} = \varphi_{\sigma(l_0)}$. Hence

$$(\theta_{m_0})^{-1} \circ \varphi_{l_0} \circ \theta_{m_0} = \varphi_{m_j \sigma(l_0) \sigma(m_0)} = \varphi_{\sigma(l_0)} = (\varphi_{l_0})^{-1}.$$

□

Chapter 7

Menichetti's Construction

7.1 Introduction

We will next look at some well-know finite semifields and apply the construction method to more general, infinite fields. This chapter will be concerned with a construction of Menichetti [40], which he defines over finite fields in order to generalise the semifields constructed by Sandler in [48]. We will generalise Menichetti's method to general Galois field extensions of degree 3 and 4. In particular, we will define an algebra using a biquadratic field extension, which is a situation that does not occur over finite fields.

These algebras also have potential applications to space-time block coding, which will be studied in more detail in Chapter 9. Good space-time block codes (STBC's) consist of infinite subspaces of invertible matrices whose entries are elements of some number field. The matrices defined in the construction of these algebras are ideal candidates for STBC's and this area of coding theory provides a good motivation for extending Menichetti's construction to infinite fields.

We briefly outline the idea behind Menichetti's construction here, the details will be given in the next sections. Let $F = \mathbb{F}_q$ be a finite field and let L be an extension of F of degree n with generating Galois automorphism σ. Consider the n^2-dimensional F-vector space $V := L \oplus \cdots \oplus L$ (n-copies of L)

and let $M : V \to \mathrm{Mat}_{n\times n}(L)$ be an F-vector space homomorphism such that

$$M(1, 0, \ldots, 0) = I_n,$$

where I_n is the $n \times n$ identity matrix, and for $y = (y_0, y_1, \ldots, y_{n-1}) \in V$, the first row of the matrix $M(y)$ is the row vector y. With these ingredients we can define a bilinear multiplication on V for two elements $x = (x_0, \ldots, x_{n-1})$ and $y = (y_0, \ldots, y_{n-1})$, by setting

$$xy := xM(y).$$

The two conditions imposed on M above ensure that this multiplication gives V the structure of a unital F-algebra with unit $1_V = (1, 0, \ldots, 0)$ since

$$x1_V = xI_n = x$$

and

$$1_V y = (1, 0, \ldots, 0)(y, *, \ldots, *)^T = y,$$

where $*$ denotes any of the remaining row vectors in $M(y)$.

If we can guarantee that the matrix $M(y)$ has nonzero determinant for all nonzero $y \in V$ then, by basic linear algebra, the system of equations $xM(y)$ has no non-trivial solutions. It follows that V, with the multiplication defined above, contains no non-trivial zero divisors and, therefore, it is a division algebra. Menichetti defines the map M by sending a vector $y = (y_0, \ldots, y_{n-1})$ to a matrix whose entries are all conjugates of the elements y_i under the field automorphism σ, along with certain parameters $a_0, \ldots, a_{n-1} \in L$. The entries are arranged in such a way so that the determinant of $M(y)$ is a polynomial in the a_i with coefficients in F. The parameters a_i can then be carefully chosen to ensure the matrix has nonzero determinant. Full details of how this is done for extensions of degree 3 and degree 4 will be given in the next sections.

7.2 Cubic Field Extensions

In Waterhouse's paper [56], he shows that every four-dimensional, unital algebra over a field F, which has nucleus equal to a quadratic separable field extension of F, is a nonassociative quaternion algebra. This mimics the situation for central simple associative algebras where every four-dimensional associative central simple algebra over F is a quaternion algebra. One may ask if every nine-dimensional, unital algebra over F with nucleus equal to a cubic separable field extension is equal to a nonassociative cyclic algebra of degree 3? Such a result would again mimic the situation for nine-dimensional central simple associative algebras, all of which are cubic cyclic algebras. The answer in this case is no. We give a construction of a nine-dimensional algebra with nucleus equal to a cubic separable field extension of F. This algebra resembles a nonassociative cyclic algebra but it can be shown that is not isomorphic to any nonassociative cyclic algebra.

Let F be a field, L a cubic separable extension of F and let $a, b, c \in L^\times$. For all triples $(y_0, y_1, y_2) \in L^3$ define the matrix:

$$M(y_0, y_1, y_2) := \begin{pmatrix} y_0 & y_1 & y_2 \\ ca^{-1}\sigma(y_2) & \sigma(y_0) & ba^{-1}\sigma(y_1) \\ ca^{-1}\sigma^2(y_1) & cb^{-1}\sigma^2(y_2) & \sigma^2(y_0) \end{pmatrix}.$$

We can define a multiplication on the F-vector space $L^3 = L \oplus L \oplus L$ by

$$(x_0, x_1, x_2)(y_0, y_1, y_2) = (x_0, x_1, x_2)M(y_0, y_1, y_2),$$

for all $x_i, y_i \in L$. This gives L^3 the structure of an F-algebra which we denote by $(L/F, a, b, c)$. We will introduce the symbols $z := (0, 1, 0)$ and $z^2 := (0, 0, 1)$. Thus a general element of $(L/F, a, b, c)$ can be written as $x_0 + x_1 z + x_2 z^2$ where $x_i \in L$. We also have the following identities:

$$zz = ba^{-1}z^2, \quad z^2 z = zz^2 = ca^{-1}, \quad z^2 z^2 = ca^{-1}z.$$

Putting $a = b = 1$ gives a cyclic algebra, $(L/F, \sigma, c)$, which is associative or nonassociative depending on the position of $c \in L$. The next theorem follows from basic linear algebra.

Theorem 7.2.1. *The algebra $(L/F, a, b, c)$ is a division algebra if $M(x_0, x_1, x_2) \neq 0$ for all $(x_0, x_1, x_2) \neq (0, 0, 0)$.*

We give a few examples of when this occurs.

Example 7.2.2. Let $d \in L \setminus F$. The following are all division algebras:

1. $(L/F, 1, 1, d)$.
2. $(L/F, 1, d, d)$.
3. $(L/F, d, 1, d)$.
4. $(L/F, d, 1, 1)$.
5. $(L/F, d, d, 1)$.

Proof. For all $x \in L$, let $N(x) = N_{L/F}(x)$ denote the field norm of x and $T(x) = T_{L/F}(x)$ denote the field trace of x. For all $x_0, x_1, x_2 \in L$ the determinant of $M(x_0, x_1, x_2)$ is

$$N(x_0) + cba^{-1}b^{-1}N(x_1) + c^2a^{-1}b^{-1}N(x_2) - ca^{-1}T(x_0\sigma(x_1)\sigma^2(x_2)).$$

Considering, for example, $(L/F, 1, d, d)$ the determinant becomes

$$N(x_0) + d^2N(x_1) + dN(x_2) - dT(x_0\sigma(x_1)\sigma^2(x_2)).$$

Since L/F is a cubic field extension, $1, d, d^2$ are linearly independent over F. Using this, it is easy to check that if the above determinant is zero then each of x_0, x_1, x_2 must equal zero. A similar argument shows the other algebras are division. □

We now look at the explicit multiplication in each of the algebras in the above example. Let $x = x_0 + x_1z + x_2z^2$ and $y = y_0 + y_1z + y_2z^2$, where $x_i, y_i \in L$, then the multiplication in $(L/F, a, b, c)$ is given by

$$\begin{aligned} xy = &(x_0y_0 + ca^{-1}x_1\sigma(y_2) + ca^{-1}x_2\sigma^2(y_1)) \\ &+ (x_0y_1 + x_1\sigma(y_0) + cb^{-1}x_2\sigma^2(y_2))z \\ &+ (x_0y_2 + ba^{-1}x_1\sigma(y_1) + x_2\sigma^2(y_0))z^2. \end{aligned}$$

It is easy to see that the multiplication for $(L/F, 1, 1, d)$ is the same as the multiplication for a cubic nonassociative cyclic algebra which we denote by $(L/F, \sigma, d) =: A$.

In the second example, $(L/F, 1, d, d)$, the multiplication becomes

$$\begin{aligned} xy = &(x_0y_0 + dx_1\sigma(y_2) + dx_2\sigma^2(y_1)) \\ &+ (x_0y_1 + x_1\sigma(y_0) + x_2\sigma^2(y_2))z \\ &+ (x_0y_2 + dx_1\sigma(y_1) + x_2\sigma^2(y_0))z^2. \end{aligned}$$

To simplify notation we will denote this algebra by (A_1, d).

The third example, $(L/F, d, 1, d)$, yields the multiplication

$$\begin{aligned} xy = &(x_0y_0 + x_1\sigma(y_2) + x_2\sigma^2(y_1)) \\ &+ (x_0y_1 + x_1\sigma(y_0) + dx_2\sigma^2(y_2))z \\ &+ (x_0y_2 + d^{-1}x_1\sigma(y_1) + x_2\sigma^2(y_0))z^2. \end{aligned}$$

We will denote this algebra by (A_2, d).

Using these notations we can see that for examples (4) and (5) we have

$$\begin{aligned} (L/F, d, 1, 1) &= (A_1, d^{-1}) \\ (L/F, d, d, 1) &= (L/F, \sigma, d^{-1}). \end{aligned}$$

Thus it suffices to study the algebras (A_1, d) and (A_2, d). It turns out that the first one is already familiar to us.

Proposition 7.2.3. *For all $d \in L \setminus F$, $(A_1, d) \cong (L/F, \sigma^2, d)$.*

Proof. The map

$$\begin{aligned} \varphi : (L/F, \sigma^2, d) &\to (A_1, d) \\ x_0 + x_1z + x_2z^2 &\mapsto x_0 + x_2z + x_1z^2, \end{aligned}$$

is easily shown to be an isomorphism. □

Remark 7.2.4. Consider the definition of (A_2, d) but with the element d taken in F. One can check that this is an associative, central simple algebra over F. By the classical theory this must be a cyclic algebra. In fact, we can show that $(A_2, d) \cong (L/F, \sigma, d^{-1})$ for all $d \in F^\times$, via the map

$$x_0 + x_1 z + x_2 z^2 \mapsto x_0 + x_1 z + d x_2 z^2.$$

When the element $d \in L \setminus F$, the situation is different.

Proposition 7.2.5. *For all $d \in L \setminus F$, the nucleus of (A_2, d) is equal to L.*

Proof. We will show that L is equal to the middle nucleus of (A_2, d), it is shown similarly that L is equal to the left and right nuclei. First L is contained in the middle nucleus since for all $x = x_0 + x_1 z + x_2 z^2$ and $y = y_0 + y_1 z + y_2 z^2$ in (A_2, d) and $l \in L$ we have

$$\begin{aligned} x(ly) &= (x_0 + x_1 z + x_2 z^2)(l y_0 + l y_1 z + l y_2 z^2) \\ &= (x_0 l y_0 + x_1 \sigma(l y_2) + x_2 \sigma^2(l y_1)) \\ &+ (x_0 l y_1 + x_1 \sigma(l y_0) + d x_2 \sigma^2(l y_2)) z \\ &+ (x_0 l y_2 + d^{-1} x_1 \sigma(l y_1) + x_2 \sigma^2(l y_0)) z^2. \end{aligned}$$

On the other hand, we have

$$\begin{aligned} (xl)y &= (x_0 l + x_1 \sigma(l) z + x_2 \sigma^2(l) z^2)(y_0 + y_1 z + y_2 z^2) \\ &= (x_0 l y_0 + x_1 \sigma(l)\sigma(y_2) + x_2 \sigma^2(l)\sigma^2(y_1)) \\ &+ (x_0 l y_1 + x_1 \sigma(l)\sigma(y_0) + d x_2 \sigma^2(l)\sigma^2(y_2)) z \\ &+ (x_0 l y_2 + d^{-1} x_1 \sigma(l)\sigma(y_1) + x_2 \sigma^2(l)\sigma(y_0)) z^2. \end{aligned}$$

These expressions are clearly the same.

For the reverse inclusion, suppose that $n = n_0 + n_1 z + n_2 z^2$ is an element of the middle nucleus of (A_2, d) for some $n_i \in L$. We calculate

$$\begin{aligned} (z(n_0 + n_1 z + n_2 z^2))z &= (\sigma(n_0) z + \sigma(n_1) d^{-1} z^2 + \sigma(n_2)) z \\ &= \sigma(n_0) d^{-1} z^2 + \sigma(n_1) d^{-1} + \sigma(n_2) z. \end{aligned}$$

However, we see that

$$\begin{aligned} z((n_0 + n_1 z + n_2 z^2)z) &= z(n_0 z + n_1 d^{-1} z^2 + n_2) \\ &= \sigma(n_0) d^{-1} z^2 + \sigma(n_1)\sigma(d^{-1}) + \sigma(n_2) z. \end{aligned}$$

These expressions are only equal if $n_1 = 0$. A similar calculation of the associator $[z^2, n, z^2]$ shows that $n_2 = 0$ as well. We conclude that $n \in L$. $\square$

Proposition 7.2.6. *For $d \in L \setminus F$, the algebra (A_2, d) is not isomorphic to $(L/F, \sigma, a)$ or $(L/F, \sigma^2, a)$ for any $a \in L$.*

Proof. Let $A = (L/F, \sigma, a)$ and $A_2 = (A_2, d)$ and suppose that $f : A \to A_2$ is an isomorphism. To avoid confusion we denote the multiplication in A by $\circ$ and in A_2 by $*$. We note the following identities:

$$z \circ z = z^2, z^2 \circ z = z \circ z^2 = a, z^2 \circ z^2 = az,$$

$$z * z = d^{-1} z^2, z^2 * z = z * z^2 = 1, z^2 * z^2 = dz.$$

Since $Nuc(A) = Nuc(A_2) = L$ we must have $f(L) = L$ and hence $f|_L = \sigma^i$ for some $i \in \mathbb{Z}/3\mathbb{Z}$. Suppose that $f(z) = l_0 + l_1 z + l_2 z^2$ for some $l_i \in L$. Then for every $m \in L$ we have

$$f(z) * f(m) = l_0 \sigma^i(m) + l_1 \sigma^{i+1}(m) z + l_2 \sigma^{i+2}(m) z^2,$$

where the indices of σ are read modulo 3. Also we get

$$\begin{aligned} f(z \circ m) &= f(\sigma(m) \circ z) \\ &= \sigma^{i+1}(m) l_0 + \sigma^{i+1}(m) l_1 z + \sigma^{i+1}(m) l_2 z^2. \end{aligned}$$

Comparing coefficients we see that $f(z) * f(m) = f(z \circ m)$ for all m if and only if $l_0 = l_2 = 0$. Hence $f(z) = lz$ for some $l \in L$. It follows from this that

$$f(z^2) = f(z \circ z) = f(z) * f(z) = lz * lz = l\sigma(l) d^{-1} z^2.$$

Since $z^2 \circ z = z \circ z^2 = a$, we calculate the image of a under f in two different ways. Firstly we have

$$f(z^2 \circ z) = f(z^2) * f(z) = l\sigma(l) d^{-1} z^2 * lz = l\sigma(l)\sigma^2(l) d^{-1}.$$

On the other hand,

$$f(z \circ z^2) = f(z) * f(z^2) = lz * l\sigma(l)d^{-1}z^2 = l\sigma(l)\sigma^2(l)\sigma(d^{-1}).$$

These two expressions are not equal since $d^{-1} \neq \sigma(d^{-1})$. A similar argument shows that A_2 is not isomorphic to $(L/F, \sigma^2, a)$ for any $a \in L$ either. The main difference in this case is that any isomorphism, $f : (L/F, \sigma^2, a) \to A_2$, must map z onto lz^2 for some $l \in L$. □

We may also consider the isomorphism question for the algebra (A_2, d) (cf. Proposition 3.1.4).

Proposition 7.2.7. *Let L/F be a cubic, cyclic field extension and let (A_2, d) and (A_2, d') be two algebras as defined above with $d, d' \in L\backslash F$. Then $(A_2, d) \cong (A_2, d')$ if and only if $d' = \sigma^i(d)N_{L/F}(l)$ for some $i \in \{0, 1, 2\}$ and $l \in L$. Every such $l \in L$ yields a unique isomorphism from (A_2, d) to (A_2, d') given by*

$$(x_0 + x_1z + x_2z^2) \mapsto (\sigma^i(x_0) + \sigma^i(x_1)lz + \sigma^i(x_2)\sigma^2(l)^{-1}z^2).$$

Proof. The proof is similar to that of Proposition 3.1.4 in Chapter 2 so we will only highlight the main differences here. Suppose $\varphi : (A_2, d) \to (A_2, d')$ is an isomorphism. As in the proof of Proposition 3.1.4, we must have $\varphi|_L = \sigma^i \in Gal(L/F)$ and $\varphi(z) = lz$ for some $l \in L$. Now, in (A_2, d) we have $(zz)z = (d^{-1}z^2)z = d^{-1}$ and hence

$$\sigma^i(d^{-1}) = \varphi(d^{-1}) = \varphi((zz)z) = ((lz)(lz))(lz) = d'^{-1}l\sigma(l)\sigma^2(l).$$

Rearranging gives $d' = \sigma^i(d)N_{L/F}(l)$. Finally, since $zz = d^{-1}z^2$ in (A_2, d), we have $z^2 = d(zz)$ and so

$$\varphi(z^2) = \varphi(d(zz)) = \sigma^i(d)((lz)(lz)) = \sigma^i(d)d'^{-1}l\sigma(l)z^2 = \sigma^2(l)^{-1}z^2,$$

by the condition $d' = \sigma^i(d)l\sigma(l)\sigma^2(l)$. This gives us the map φ explicitly.

Conversely, it is routine to verify that such a map is indeed an isomorphism. □

Corollary 7.2.8. *Let L/F be a cubic, cyclic field extension. Every $l \in L$ with $N_{L/F}(l) = 1$ yields an automorphism of (A_2, d) given by*

$$x_0 + x_1 z + x_2 z^2 \mapsto x_0 + x_1 l z + x_2 \sigma^2(l)^{-1} z^2,$$

for all $x_0 + x_1 z + x_2 z^2 \in (A_2, d)$. These are all such automorphisms unless there exists an element $l' \in L$ with $d = \sigma^i(d) N_{L/F}(l')$. In this case the map

$$x_0 + x_1 z + x_2 z^2 \mapsto \sigma^i(x_0) + \sigma^i(x_1) l + \sigma^i(x_2) \sigma^2(l)^{-1} z^2$$

is also an automorphism of (A_2, d).

Since the conditions for two algebras (A_2, d) and (A_2, d') to be isomorphic are the same as the conditions for two nonassociative cyclic algebras $(L/F, \sigma, d)$ and $(L/F, \sigma, d')$ to be isomorphic, we can apply the results from Chapter 6 when we consider the algebra (A_2, d) over a finite field.

Corollary 7.2.9 (cf. Corollary 6.2.9)**.** *Let $F = \mathbb{F}_q$ where q is a prime power and let L be a cubic extension of F. If 3 divides $q - 1$ then there are*

$$\frac{q^2 + q + 4}{3}$$

non-isomorphic semifields arising from the construction (A_2, d). If 3 does not divide $q - 1$ then there are precisely

$$\frac{q^2 + q}{3}$$

non-isomorphic semifields arising from the construction (A_2, d).

Corollary 7.2.10 (cf. Corollary 6.3.3)**.** *Let L be a cubic extension of a finite field $F = \mathbb{F}_q$ where q is a prime power. If 3 does not divide $q - 1$ then for all $d \in L \setminus F$, $Aut((A_2, d)) \cong \mathbb{Z}/s\mathbb{Z}$ where $s = q^2 + q + 1$. If 3 does divide $q - 1$ then the automorphism group is either isomorphic to $\mathbb{Z}/s\mathbb{Z}$ or is a group of order $3(q^2 + q + 1)$.*

7.3 Cyclic Field Extensions of Degree 4

Let F be a field and L a cyclic extension of F of degree 4 with Galois group generated by the automorphism σ. Pick nonzero elements $a, b, c, d \in L$. For all 4-tuples $(x_0, x_1, x_2, x_3) \in L^4$ we consider the matrix $M(x_0, x_1, x_2, x_3)$ defined by

$$\begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ da^{-1}\sigma(x_3) & \sigma(x_0) & ba^{-1}\sigma(x_1) & ca^{-1}\sigma(x_2) \\ cda^{-1}b^{-1}\sigma^2(x_2) & db^{-1}\sigma^2(x_3) & \sigma^2(x_0) & ca^{-1}\sigma^2(x_1) \\ da^{-1}\sigma^3(x_1) & db^{-1}\sigma^3(x_2) & dc^{-1}\sigma^3(x_3) & \sigma^3(x_0) \end{pmatrix}.$$

Proposition 7.3.1. *The determinant of $M(x_0, x_1, x_2, x_3)$ is of the form*

$$\sum_i a^{n_{i1}} b^{n_{i2}} c^{n_{i3}} d^{n_{i4}} f_i(x_0, x_1, x_2, x_3),$$

where the n_{ij} are integers and the f_i are functions which take values in F.

Proof. A routine, but tedious, calculation shows that

$$\begin{aligned} \mathrm{Det}(M(x_0, x_1, x_2, x_3)) = {} & N_{L/F}(x_0) - \frac{bcd}{a^3} N_{L/F}(x_1) + \frac{c^2d^2}{a^2b^2} N_{L/F}(x_2) \\ & - \frac{d^3}{abc} N_{L/F}(x_3) + \frac{cd}{a^2} Tr_{L/F}(x_0\sigma(x_1)\sigma^2(x_1)\sigma^3(x_2)) \\ & - \frac{d}{a} Tr_{L/F}(x_0\sigma(x_0)\sigma^2(x_1)\sigma^3(x_3)) \\ & + \frac{d^2}{ab} Tr_{L/F}(x_0\sigma(x_2)\sigma^2(x_3)\sigma^3(x_3)) \\ & + \frac{cd^2}{a^2b} Tr_{L/F}(x_1\sigma(x_2)\sigma^2(x_2)\sigma^3(x_3)) \\ & - \frac{cd}{ab} Tr_{F_0/F}(x_0\sigma^2(x_0)\sigma(x_2)\sigma^3(x_2)) \\ & + \frac{d^2}{a^2} Tr_{F_0/F}(x_1\sigma^2(x_1)\sigma(x_3)\sigma^3(x_3)), \end{aligned} \tag{7.1}$$

where F_0 is the intermediate field of L and F fixed by σ^2. □

Remark 7.3.2. In [40], Menichetti proves this using clever matrix manipulations to show that $\mathrm{Det}(M(x_0, x_1, x_2, x_3)) = \mathrm{Det}(M(\sigma(x_0), \sigma(x_1), \sigma(x_2), \sigma(x_3))$

and thus deduces that the determinant of the matrix is of the desired form. Here, we prefer the more explicit approach as it proves to be more useful for our purposes.

On the vector space $L^4 = L \oplus L \oplus L \oplus L$, we define a product by

$$(x_0, x_1, x_2, x_3)(y_0, y_1, y_2, y_3) = (x_0, x_1, x_2, x_3)M(y_0, y_1, y_2, y_3),$$

for all $x_i, y_i \in L$. This gives L^4 the structure of an F-algebra, which we denote by $(L/F, a, b, c, d)$. As before, we introduce the symbols $z = (0, 1, 0, 0), z^2 = (0, 0, 1, 0)$ and $z^3 = (0, 0, 0, 1)$, so we may write an element $(x_0, x_1, x_2, x_3) \in (L/F, a, b, c, d)$ as $x_0 + x_1 z + x_2 z^2 + x_3 z^3$. Multiplication can be expressed as

$$\begin{aligned} xy &= (x_0 + x_1 z + x_2 z^2 + x_3 z^3)(y_0 + y_1 z + y_2 z^2 + y_3 z^3) \\ &= x_0 y_0 + da^{-1} x_1 \sigma(y_3) + cda^{-1} b^{-1} x_2 \sigma^2(y_2) + da^{-1} x_3 \sigma^3(y_1) \\ &+ (x_0 y_1 + x_1 \sigma(y_0) + db^{-1} x_2 \sigma^2(y_3) + db^{-1} x_3 \sigma^3(y_2)) z \\ &+ (x_0 y_2 + ba^{-1} x_1 \sigma(y_1) + x_2 \sigma^2(y_0) + dc^{-1} x_3 \sigma^3(y_3)) z^2 \\ &+ (x_0 y_3 + ca^{-1} x_1 \sigma(y_2) + ca^{-1} x_2 \sigma^2(y_1) + x_3 \sigma^3(y_0)) z^3. \end{aligned}$$

Example 7.3.3. Let $a = b = c = 1$, then $(L/F, 1, 1, 1, d)$ is a cyclic algebra of degree 4 which is associative if $d \in F$ and nonassociative if $d \in L \setminus F$.

Proposition 7.3.4. *If the matrix $M(x_0, x_1, x_2, x_3)$ has nonzero determinant for all $(0, 0, 0, 0) \neq (x_0, x_1, x_2, x_3) \in L^4$, then $(L/F, a, b, c, d)$ is a division algebra.*

Proof. Due to the definition of the multiplication in $(L/F, a, b, c, d)$, this follows from basic linear algebra. □

Example 7.3.5. Pick $d \in L$ such that $1, d, d^2, d^3$ are linearly independent over F. The following are division algebras.

- $(L/F, d, 1, 1, 1)$,
- $(L/F, 1, d, 1, 1)$,

- $(L/F, 1, 1, d, 1)$,
- $(L/F, 1, 1, 1, d)$,
- $(L/F, d, d, d, 1)$,
- $(L/F, d, d, 1, d)$,
- $(L/F, d, 1, d, d)$,
- $(L/F, 1, d, d, d)$.

Proof. As an example, we will show that $(L/F, d, d, d, 1)$ is a division algebra. The other cases are proved similarly. From the previous proposition, we know that if the determinant of the matrix of right multiplication $M(x_0, x_1, x_2, x_3)$ is nonzero for all nonzero $(x_0, x_1, x_2, x_3) \in L^4$, then the algebra will be division. We can easily check this condition by putting our chosen parameters into the explicit formulation for $\mathrm{Det}(M(x_0, x_1, x_2, x_3))$ in (7.1). We see that the determinant is a polynomial of degree 3 in $1/d$ with coefficients in F. Since $1, d, d^2, d^3$ are linearly independent over F, so are $1, 1/d, 1/d^2, 1/d^3$. Moreover, the only constant term (i.e.. without a factor of $1/d$) is $N_{L/F}(x_0)$ and the only term with a factor of $1/d^3$ is $-N_{L/F}(x_3)$. Hence if $\mathrm{Det}(M(x_0, x_1, x_2, x_3)) = 0$, we would have $x_0 = x_3 = 0$. Putting this back into (7.1), we see that the only remaining coefficient of $1/d$ is $-N_{L/F}(x_1)$ and the only remaining coefficient of $1/d^2$ is $N_{L/F}(x_2)$, so these must be zero also, implying that $x_1 = x_2 = 0$. □

Example 7.3.6 (Menichetti)**.** Let $a = 1, c = b, d = bb'$ and suppose that $b = k_0 + k_2 b'$ where $k_0, k_1 \in F$ with $k_0 \neq 0$. The matrix $M = M(x_0, x_1, x_2, x_3)$ now becomes

$$M = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ bb'\sigma(x_3) & \sigma(x_0) & b\sigma(x_1) & b\sigma(x_2) \\ bb'\sigma^2(x_2) & b'\sigma^2(x_3) & \sigma^2(x_0) & b\sigma^2(x_1) \\ bb'\sigma^3(x_1) & b'\sigma^3(x_2) & b'\sigma^3(x_3) & \sigma^3(x_0) \end{pmatrix}.$$

We can see that $\mathrm{Det}(M)$ is a polynomial of the form

$$f_0(x_0,x_1,x_2,x_3) + bb' f_1(x_0,x_1,x_2,x_3) + \\ + bb'^2 f_2(x_0,x_1,x_2,x_3) + bb'^3 f_3(x_0,x_1,x_2,x_3),$$

where the f_i are functions which take values in F. Suppose we choose b, b' such that $1, bb', bb'^2, bb'^3$ are linearly independent over F and suppose that $\mathrm{Det}(M) = 0$. Expanding the determinant along the first column of M shows that $f_0(x_0,x_1,x_2,x_3) = N_{L/F}(x_0)$. We must, therefore, have $x_0 = 0$. Putting this into F, we can then check that the expansion of the determinant becomes

$$bb'(k_0^2 N_{L/F}(x_1) + b'[\ldots]) + \ldots$$

and $k_0^2 N_{L/F}(x_1)$ is the only nonzero coefficient of the term bb'. Since $k_0 \neq 0$ we must have $x_1 = 0$. Repeating this process, we find that $x_2 = x_3 = 0$ and so the matrix M has zero determinant only if and only if $x_0 = x_1 = x_2 = x_3 = 0$.

The elements $1, bb', bb'^2, bb'^3$ can be chosen to be linearly independent as follows: pick b' such that $\{1, b', b'^2, b'^3\}$ is a basis for L/F and write

$$1, bb' = k_0 b' + k_1 b'^2, bb'^2 = k_0 b'^2 + k_1 b'^3, bb'^3 = k_0 b'^3 + k_0 b'^4.$$

If $b'^4 = \lambda_0 + \lambda_1 b' + \lambda_2 b'^2 + \lambda_3 b'^3$, then $1, bb', bb'^2, bb'^3$ will be linearly independent over F if the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & k_0 & k_1 & 0 \\ 0 & 0 & k_0 & k_1 \\ k_1\lambda_0 & k_1\lambda_1 & k_1\lambda_2 & k_0 + k_1\lambda_3 \end{pmatrix},$$

has nonzero determinant, i.e., if

$$k_0^3 + k_0^2 k_1 \lambda_3 - k_0 k_1^2 \lambda_2 + k_2 \lambda_1 \neq 0.$$

7.4 Biquadratic Field Extensions

In [40], Menichetti only considers this construction over finite fields where all extensions are cyclic. In our more general situation, over infinite fields,

we may encounter non-cyclic field extensions, for example, biquadratic extensions. Let L/F be such a biquadratic field extension, i.e.,

$$L = F(\sqrt{u}, \sqrt{v}),$$

where u, v and uv are square-free elements of F. Then

$$Gal(L/F) = \{1, \sigma, \tau, \sigma\tau\},$$

where σ and τ are defined by

$$\sigma(\sqrt{u}) = \sqrt{u}, \quad \sigma(\sqrt{v}) = -\sqrt{v},$$

$$\tau(\sqrt{u}) = -\sqrt{u}, \quad \tau(\sqrt{v}) = \sqrt{v}.$$

We pick nonzero elements $a, b, c, d \in L$ and define the matrix $M(x_0, x_1, x_2, x_3)$ to be

$$\begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ da^{-1}\sigma(x_3) & \sigma(x_0) & ba^{-1}\sigma(x_1) & ca^{-1}\sigma(x_2) \\ cda^{-1}b^{-1}\tau(x_2) & db^{-1}\tau(x_3) & \tau(x_0) & ca^{-1}\tau(x_1) \\ da^{-1}\sigma^3(x_1) & db^{-1}\sigma\tau(x_2) & dc^{-1}\sigma\tau(x_3) & \sigma\tau(x_0) \end{pmatrix},$$

for every 4-tuple $(x_0, x_1, x_2, x_3) \in L^4$.

Proposition 7.4.1. *The determinant of the matrix $M(x_0, x_1, x_2, x_3)$ is a polynomial of the form*

$$\sum_i a^{n_{i1}} b^{n_{i2}} c^{n_{i3}} d^{n_{i4}} g_i(x_0, x_1, x_2, x_3),$$

where n_{ij} are integers and the g_i are functions which take values in F.

Proof. Calculating the determinant explicitly we have

$$\begin{aligned}\mathrm{Det}(M(x_0,x_1,x_2,x_3)) &= N_{L/F}(x_0) - \frac{bcd}{a^3}N_{L/F}(x_1) + \frac{c^2d^2}{a^2b^2}N_{L/F}(x_2)\\ &- \frac{d^3}{abc}N_{L/F}(x_3) + \frac{cd}{a^2}Tr_{L/F}(x_0\sigma(x_1)\tau(x_1)\sigma\tau(x_2))\\ &- \frac{d}{a}Tr_{L/F}(x_0\sigma(x_0)\tau(x_1)\sigma\tau(x_3))\\ &+ \frac{d^2}{ab}Tr_{L/F}(x_0\sigma(x_2)\tau(x_3)\sigma\tau(x_3))\\ &+ \frac{cd^2}{a^2b}Tr_{L/F}(x_1\sigma(x_2)\tau(x_2)\sigma\tau(x_3))\\ &- \frac{cd}{ab}Tr_{F_0/F}(x_0\tau(x_0)\sigma(x_2)\sigma\tau(x_2))\\ &+ \frac{d^2}{a^2}Tr_{F_0/F}(x_1\tau(x_1)\sigma(x_3)\sigma\tau(x_3)),\end{aligned} \tag{7.2}$$

where $F_0 = F(\sqrt{v})$ is the intermediate field of L and F fixed by τ. □

On the vector space $L^4 = L \oplus L \oplus L \oplus L$, we define a product by

$$(x_0,x_1,x_2,x_3)(y_0,y_1,y_2,y_3) = (x_0,x_1,x_2,x_3)M(y_0,y_1,y_2,y_3),$$

for all $x_i, y_i \in L$. This gives L^4 the structure of an F-algebra, which we denote by $(L/F,a,b,c,d)$. As before, we introduce the symbols $z = (0,1,0,0), z^2 = (0,0,1,0)$ and $z^3 = (0,0,0,1)$, so we may write an element $(x_0,x_1,x_2,x_3) \in (L/F,a,b,c,d)$ as $x_0 + x_1z + x_2z^2 + x_3z^3$. Multiplication can be expressed as

$$\begin{aligned}xy &= (x_0 + x_1z + x_2z^2 + x_3z^3)(y_0 + y_1z + y_2z^2 + y_3z^3)\\ &= x_0y_0 + da^{-1}x_1\sigma(y_3) + cda^{-1}b^{-1}x_2\tau(y_2) + da^{-1}x_3\sigma\tau(y_1)\\ &+ (x_0y_1 + x_1\sigma(y_0) + db^{-1}x_2\tau(y_3) + db^{-1}x_3\sigma\tau(y_2))z\\ &+ (x_0y_2 + ba^{-1}x_1\sigma(y_1) + x_2\tau(y_0) + dc^{-1}x_3\sigma\tau(y_3))z^2\\ &+ (x_0y_3 + ca^{-1}x_1\sigma(y_2) + ca^{-1}x_2\tau(y_1) + x_3\sigma\tau(y_0))z^3.\end{aligned}$$

Proposition 7.4.2. *If the matrix $M(x_0,x_1,x_2,x_3)$ has nonzero determinant for all $(0,0,0,0) \neq (x_0,x_1,x_2,x_3) \in L^4$, then $(L/F,a,b,c,d)$ is a division algebra.*

Proof. Due to the definition of the multiplication in $(L/F, a, b, c, d)$, this follows from basic linear algebra. □

Example 7.4.3. Pick $d \in L$ such that $1, d, d^2, d^3$ are linearly independent over F. The following are division algebras.

- $(L/F, d, 1, 1, 1)$,
- $(L/F, 1, d, 1, 1)$,
- $(L/F, 1, 1, d, 1)$,
- $(L/F, 1, 1, 1, d)$,
- $(L/F, d, d, d, 1)$,
- $(L/F, d, d, 1, d)$,
- $(L/F, d, 1, d, d)$,
- $(L/F, 1, d, d, d)$.

The proof that these are division algebras is exactly the same as in Example 7.3.5.

Chapter 8

Hughes-Kleinfeld and Knuth Constructions

In this chapter we look at some other well-known constructions for finite semifields, namely one of Hughes and Kleinfeld, and a few given by Knuth. We apply the constructions to more general fields and investigate the resulting algebras. In particular, these constructions yield division algebras over the real numbers. In [22], Hughes and Kleinfeld gave a construction of a finite semifield which is quadratic over a finite field L contained in the right and middle nucleus. In a closing remark of the paper they mention that this construction will also work over general fields and gives (infinite) division algebras. However, they do not study the situation over infinite fields since this construction does not classify those algebras quadratic over such a field L as it does in the finite case.

In his thesis, [31], Knuth considered three similar constructions of finite semifields. These three along with the Hughes-Kleinfeld semifield are some of the best-known finite semifields and have been studied in a variety of contexts (e.g. [5], [57]) but always over finite fields. Here we look at these four constructions over general fields. We show that they give a simple construction for division algebras. Under certain conditions they each possess different combinations of left, right and middle nuclei and so they are mu-

tually non-isomorphic. Automorphisms of these algebras are studied and in specific cases we determine the automorphism group.

8.1 Definition

Let F be a field and let L be a Galois field extension of F. We consider four multiplications on the F-vector space $L \oplus L$. Pick elements η and μ of L and a nontrivial automorphism $\sigma \in Gal(L/F)$. For elements $x, y, u, v \in L$ the four multiplications are given as follows:

$$Kn_1 : (x,y) \circ (u,v) = (xu + \eta\sigma^{-2}(y)\sigma(v), xv + y\sigma(u) + \mu\sigma^{-1}(y)\sigma(v)),$$

$$Kn_2 : (x,y) \circ (u,v) = (xu + \eta\sigma^{-2}(y)\sigma^{-1}(v), xv + y\sigma(u) + \mu\sigma^{-1}(y)v),$$

$$Kn_3 : (x,y) \circ (u,v) = (xu + \eta y\sigma^{-1}(v), xv + y\sigma(u) + \mu yv),$$

$$HK : (x,y) \circ (u,v) = (xu + \eta y\sigma(v), xv + y\sigma(u) + \mu y\sigma(v)).$$

We will denote the vector-space $L \oplus L$ endowed with each of the above multiplications by $Kn_1(L, \sigma, \eta, \mu), Kn_2(L, \sigma, \eta, \mu), Kn_3(L, \sigma, \eta, \mu)$ and $HK(L, \sigma, \eta, \mu)$, respectively. This notation reflects the fact that the first three are the constructions defined by Knuth and the last one is the construction defined by Hughes-Kleinfeld. If it is clear from the context or irrelevant to the discussion we may omit some or all of the parameters. Each of Kn_1, Kn_2, Kn_3 and HK is a unital F-algebra with unit element $(1, 0)$. They also contain $L \oplus 0$ as a subalgebra, which we identify with the field L.

Theorem 8.1.1 ([22], [31]). *If L is a finite field and if the equation*

$$w\sigma(w) + \mu w - \eta \tag{8.1}$$

has no solutions in L, then each of the above algebras is a division algebra.

Thus we get four constructions for finite semifields. As Hughes and Kleinfeld mentioned in their paper, if L/F is any separable field extension and Equation (8.1) has no solutions then $HK(L, \sigma, \eta, \mu)$ is a division algebra. In fact, this is true for all of the above algebras.

Theorem 8.1.2. *Let L/F be any separable field extension. The algebras Kn_1, Kn_2, Kn_3 and HK are all division algebras if and only if Equation (8.1) has no solutions in L.*

Proof. We prove the sufficiency for Kn_1 since the other cases are similar. Suppose that Kn_1 contains zero divisors. That is

$$(x, y) \circ (u, v) = (xu + \eta\sigma^{-2}(y)\sigma(v), xv + y\sigma(u) + \mu\sigma^{-1}(y)\sigma(v)) = (0, 0),$$

for some $(x, y) \neq (0, 0) \neq (u, v)$. We may assume that none of x, y, u, v are zero since otherwise a quick check would reveal that we must either have $(x, y) = (0, 0)$ or $(u, v) = (0, 0)$. Thus each of their inverses in L exist. We have the following equations:

$$\begin{aligned} xu + \eta\sigma^{-2}(y)\sigma(v) &= 0, \\ xv + y\sigma(u) + \mu\sigma^{-1}(y)\sigma(v) &= 0. \end{aligned}$$

The first equation implies that there exists an element $z \in L^\times$ such that

$$u = z\sigma^{-2}(y), \qquad x = -\eta\sigma(v)z^{-1}.$$

Plugging this into the second equation gives

$$-\eta\sigma(v)z^{-1}v + y\sigma(z)\sigma^{-1}(y) + \mu\sigma^{-1}(y)\sigma(v) = 0.$$

Multiplying through by z and setting $w = z\sigma^{-1}(y)v^{-1}$ yields

$$\sigma(v)v(-\eta + w\sigma(w) + \mu w) = 0.$$

Since $v \neq 0$ we must have $w\sigma(w) + \mu w - \eta = 0$ which is a contradiction of our hypothesis. For necessity, notice that if w is a nonzero solution to Equation (8.1) then

$$(-\eta, \sigma(w)) \circ (\sigma^{-1}(w), 1) = (0, 0),$$

for both Kn_1 and Kn_2 and

$$(-\eta, w) \circ (w, 1) = (0, 0),$$

for both Kn_3 and HK. Hence all algebras contain nontrivial zero divisors. If $w = 0$ is a solution to Equation (8.1) then we must have $\eta = 0$. If $\mu \neq 0$ then $w = -\sigma^{-1}(\mu)$ is also a solution and is nonzero so the previous paragraph applies. If $\mu = 0$ then the multiplication on each algebra becomes

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

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

$$(0, 1) \circ (0, 1) = (0, 0)$$

and so each algebra has nontrivial zero divisors in this case. □

By the previous theorem, if $\eta = 0$ then the algebras Kn_1, Kn_2, Kn_3 and HK are never division, so we shall assume that $\eta \neq 0$ from now on.

8.2 Nuclei

In this section we calculate some of the nuclei of the algebras Kn_1, Kn_2, Kn_3 and HK and show that no two of them possess the same combination of left, right and middle nuclei unless $\sigma^2 = \mathrm{Id}$ and $\mu = 0$. If both $\sigma^2 = \mathrm{Id}$ and $\mu = 0$ then the multiplication for each algebra is the same:

$$(x, y) \circ (u, v) = (xu + \eta y\sigma(v), xv + y\sigma(u)).$$

In this case σ is of order two in $Gal(L/F)$ and as such L has a subfield E such that $[L : E] = 2$ and $Gal(L/E) = \{\mathrm{Id}, \sigma\}$. Hence, the multiplication given above defines a quaternion algebra over E which is associative if $\eta \in E$ and nonassociative if $\eta \in L \setminus E$. The structure of these is well known in the associative case and the nonassociative case is covered in Chapter 3, so we will assume from now on that either $\sigma^2 \neq \mathrm{Id}$ or $\mu \neq 0$.

Proposition 8.2.1. *Suppose that either $\sigma^2 \neq \mathrm{Id}$ or that $\mu \neq 0$.*
(i) L is equal to the middle and right nucleus of $Kn_2(L, \sigma, \eta, \mu)$ but is not contained in the left nucleus.
(ii) L is equal to the left and right nucleus of $Kn_3(L, \sigma, \eta, \mu)$ but is not contained in the middle nucleus.
(iii) L is equal to the left and middle nucleus of $HK(L, \sigma, \eta, \mu)$ but is not contained in the right nucleus.
(iv) L is not contained in the left, right or middle nucleus of $Kn_1(L, \sigma, \eta, \mu)$.

Proof. This time we will only prove (i), the other cases are similar. We will also drop the circle notation for multiplication and denote it simply by juxtaposition: $(x, y) \circ (u, v) = (x, y)(u, v)$. To show L is contained in the middle nucleus we let $l \in L$ and calculate

$$\begin{aligned}((x, y)(l, 0))(u, v) &= (xl, y\sigma(l))(u, v) \\ &= \big(xlu + \eta\sigma^{-2}(y)\sigma^{-1}(l)\sigma^{-1}(v), \\ &\qquad xlv + y\sigma(l)\sigma(u) + \mu\sigma^{-1}(y)lv\big).\end{aligned}$$

On the other hand,

$$\begin{aligned}(x, y)((l, 0)(u, v)) &= (x, y)(lu, lv) \\ &= (xlu + \eta\sigma^{-2}(y)\sigma^{-1}(lv), xlv + y\sigma(lu) + \mu\sigma^{-1}(y)lv).\end{aligned}$$

These two expressions are the same hence $L \subseteq Nuc_m(Kn_2)$. To show that there are no other elements in the middle nucleus of Kn_2 it suffices to check that no elements of the form $(0, m), m \in L$, belong to the middle nucleus. This is because the associator is linear:

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

If $(0, m) \in Nuc_m(Kn_2)$ then for all $v \in L$ we should have

$$[(0, v), (0, m), (0, 1)] = (0, 0),$$

however, calculating directly we get

$$\begin{aligned}&((0,v)(0,m))(0,1) - (0,v)((0,m)(0,1)) = \\ &(\eta\sigma^{-2}(\mu)\sigma^{-3}(v)\sigma^{-2}(m),\ \ \eta\sigma^{-2}(v)\sigma^{-1}(m) + \mu\sigma^{-1}(\mu)\sigma^{-2}(v)\sigma^{-1}(m)) \\ &- (\eta\sigma^{-2}(v)\sigma^{-1}(\mu)\sigma^{-2}(m),\ \ v\sigma(\eta)\sigma^{-1}(m) + \mu\sigma^{-1}(v)\mu\sigma^{-1}(m)) = 0.\end{aligned}$$

If $\mu \neq 0$ then looking at the first term gives

$$\sigma^{-2}(\mu)\sigma^{-3}(v) = \sigma^{-2}(v)\sigma^{-1}(\mu)$$

for all $v \in L$ which can't hold. If $\mu = 0$ then, by hypothesis, we must have $\sigma^2 \neq \mathrm{Id}$ and looking at the second term gives the equation

$$\eta\sigma^{-2}(v) = v\sigma(\eta),$$

which again can't hold for all $v \in L$. A similar calculation shows that the right nucleus is also equal to L. To show that L is not contained in the left nucleus we check

$$\begin{aligned}((l,0)(x,y))(u,v) &= (lx,ly)(u,v) \\ &= (lxu + \eta\sigma^{-2}(ly)\sigma^{-1}(v), lxv + ly\sigma(u) + \mu\sigma^{-1}(ly)v),\end{aligned}$$

whereas

$$\begin{aligned}(l,0)((x,y)(u,v)) &= (l,0)(xu + \eta\sigma^{-2}(y)\sigma^{-1}(v), xv + y\sigma(u) + \mu\sigma^{-1}(y)v) \\ &= (lxu + l\eta\sigma^{-2}(y)\sigma^{-1}(v), lxv + ly\sigma(u) + l\mu\sigma^{-1}(y)v).\end{aligned}$$

These equations are not equal for all $l \in L$ unless $\sigma^2 = \mathrm{Id}$ and $\mu = 0$. □

Remark 8.2.2. In their paper [22], Hughes and Kleinfeld show that the right and middle nuclei of their algebra are equal to L. This is because they use a slightly different definition of multiplication to us. They consider the product

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

for all $x, y, u, v \in L$. It is easily checked that this multiplication gives the opposite algebra HK^{op}, which explains the swap of right and left nucleus.

Corollary 8.2.3. *The algebras Kn_1, Kn_2, Kn_3 and HK are mutually non-isomorphic unless $\sigma^2 = \mathrm{Id}$ and $\mu = 0$, in which case they are the same algebra.*

Proof. Since isomorphisms must preserve each of the left, right and middle nuclei, the first claim holds when either $\sigma^2 \neq \mathrm{Id}$ or $\mu \neq 0$. On the other hand if both $\sigma^2 = \mathrm{Id}$ and $\mu = 0$ the the definition of multiplication in each algebra is exactly the same. □

8.3 Automorphisms

In this section we describe all automorphisms for the algebras HK, Kn_2 and Kn_3. We also exhibit some automorphisms for the algebra Kn_1.

Proposition 8.3.1. *Let $A = HK(L, \sigma, \eta, \mu)$. All automorphisms of A are of the form*

$$(x, y) \mapsto (\tau(x), \tau(y)b),$$

where $\tau \in Gal(L/F)$ commutes with σ and $b \in L^\times$ is such that

$$\eta b\sigma(b) = \tau(\eta) \text{ and } \mu\sigma(b) = \tau(\mu).$$

Proof. Let $\varphi : A \to A$ be an automorphism. Since $Nuc_l(A) = L$ and isomorphisms preserve left, right and middle nuclei, we must have $\varphi(L) = L$. Hence $\varphi|_L = \tau \in Gal(L/F)$. We can write any element (x, y) of HK as

$$(x, y) = (x, 0) + (y, 0)(0, 1).$$

Since $\varphi((x, 0)) = (\tau(x), 0)$ for all $x \in L$, it remains to determine $\varphi((0, 1))$. Suppose $\varphi((0, 1)) = (a, b)$ for some $a, b \in L$, thus we can write

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

For all $m \in L$ we must have

$$\varphi((0,1)(m,0)) = \varphi((0,1))\varphi((m,0)).$$

On the one hand we have

$$\varphi((0,1)(m,0)) = \varphi((0,\sigma(m)) = (\tau(\sigma(m))a, \tau(\sigma(m))b),$$

whereas the right hand side becomes

$$(a,b)(\tau(m),0) = (\tau(m)a, \sigma(\tau(m))b).$$

Since $\sigma \neq \mathrm{Id}$, this implies that $a = 0$ and that τ and σ commute. Finally, we have $(0,1)(0,1) = (\eta,\mu)$ and so $\varphi((0,1)(0,1)) = (\tau(\eta), \tau(\mu)b)$. However,

$$\varphi((0,1))\varphi((0,1)) = (0,b)(0,b) = (\eta b\sigma(b), \mu b\sigma(b)),$$

and so we arrive at the conditions $\eta b\sigma(b) = \tau(\eta)$ and $\mu\sigma(b) = \tau(\mu)$.

Conversely, suppose $b \in L$ satisfies the conditions mentioned in the proposition. Then for all $x, y, u, v \in L$, we have

$$\begin{aligned}
\varphi((x,y))\varphi((u,v)) &= (\tau(x), \tau(y)b)(\tau(u), \tau(v)b) \\
&= \big(\tau(x)\tau(u) + \eta\tau(y)b\sigma(\tau(v)b), \\
&\qquad \tau(x)\tau(v)b + \tau(y)b\sigma(\tau(u)) + \mu\tau(y)b\sigma(\tau(v)b)\big) \\
&= \big(\tau(xu) + \tau(\eta y\sigma(v)), \tau(xv) + \tau(y\sigma(u)) + \tau(\mu y\sigma(v))b\big) \\
&= \varphi\big((x,y)(u,v)\big).
\end{aligned}$$

□

Proposition 8.3.2. *Let $A = Kn_2(L,\sigma,\eta,\mu)$. All automorphisms of A are of the form*

$$(x,y) \mapsto (\tau(x), \tau(y)b),$$

where $\tau \in Gal(L/F)$ commutes with σ and $b \in L^\times$ is such that

$$\eta\sigma^{-2}(b)\sigma^{-1}(b) = \tau(\eta) \text{ and } \mu\sigma^{-1}(b) = \tau(\mu).$$

Proof. By Proposition 8.2.1, $Nuc_m(A) = L$, so any automorphism $\varphi : A \to A$ must restrict to an automorphism of L/F, say $\varphi|_L = \tau \in Gal(L/F)$. Following the proof of Proposition 8.3.1, we deduce that

$$\varphi(x, y) = (\tau(x), \tau(y)b),$$

for all $(x, y) \in A$ and some $b \in L$. Now $(0, 1)(0, 1) = (\eta, \mu)$ and, therefore, $\varphi((0, 1)(0, 1)) = (\tau(\eta), \tau(\mu)b)$. However,

$$\varphi((0, 1))\varphi((0, 1)) = (0, b)(0, b) = (\eta\sigma^{-2}(b)\sigma^{-1}(b), \mu\sigma^{-1}(b)b),$$

and so $\eta\sigma^{-2}(b)\sigma^{-1}(b) = \tau(\eta)$ and $\mu\sigma^{-1}(b) = \tau(\mu)$.

It is a routine calculation, similar to that in Proposition 8.3.1, to show that such maps are indeed automorphisms. □

Proposition 8.3.3. *Let $A = Kn_3(L, \sigma, \eta, \mu)$. All automorphisms of A are of the form*

$$(x, y) \mapsto (\tau(x), \tau(y)b),$$

where $\tau \in Gal(L/F)$ commutes with σ and $b \in L^\times$ is such that

$$\eta b\sigma^{-1}(b) = \tau(\eta) \text{ and } \mu b = \tau(\mu).$$

Proof. In this case $Nuc_l(A) = L$ so, again using the same argument as in Proposition 8.3.1, we conclude that any automorphism $\varphi : A \to A$ is of the form

$$(x, y) \mapsto (\tau(x), \tau(y)b),$$

for $(x, y) \in A$ and some $b \in L$. To determine what conditions b must satisfy, we calculate $\varphi((0, 1)(0, 1)) = (\tau(\eta), \tau(\mu)b)$ and

$$\varphi((0, 1))\varphi((0, 1)) = (0, b)(0, b) = (\eta b\sigma^{-1}(b), \mu b^2).$$

Therefore $\eta b\sigma^{-1}(b) = \tau(\eta)$ and $\mu b = \tau(\mu)$. As before, it is routine to verify that such maps are automorphisms of A. □

The key part in these three proofs is the fact that either the left, right or middle nucleus of HK, Kn_2 and Kn_3 is equal to L. From this we deduce that any automorphism of the algebra must restrict to an automorphism of L. For Kn_1, L is not contained in any of the nuclei so we cannot make this deduction. However, if we assume that an automorphism of Kn_1 restricts to an automorphism of L, then it must be of a similar form to the above maps.

Proposition 8.3.4. *Let $A = Kn_1(L, \sigma, \eta, \mu)$ and suppose φ is an automorphism of A which restricts to an automorphism of L: $\varphi|_L = \tau \in Gal(L/F)$. Then, for all $(x, y) \in A$*

$$\varphi((x, y)) = (\tau(x), \tau(y)b),$$

where $\eta\sigma^{-2}(b)\sigma(b) = \tau(\eta)$ and $\mu\sigma^{-1}(b)\sigma(b) = \tau(\mu)b$.

Proof. Assuming that $\varphi|_L = \tau \in Gal(L/F)$ allows us to deduce that

$$\varphi((x, y)) = (\tau(x), \tau(y)b),$$

for all $(x, y) \in A$ and some $b \in L$. In Kn_1 we have $\varphi((0, 1)(0, 1)) = (\tau(\eta), \tau(\mu)b)$ and

$$\varphi((0, 1))\varphi((0, 1)) = (0, b)(0, b) = (\eta\sigma(b)\sigma^{-2}(b), \mu\sigma^{-1}(b)\sigma(b)).$$

Therefore $\eta\sigma^{-2}(b)\sigma(b) = \tau(\eta)$ and $\mu\sigma^{-1}(b)\sigma(b) = \tau(\mu)b$. □

Whenever $\mu \neq 0$, there are very few automorphisms for each of these algebras, in many cases there are fewer automorphisms than of L/F. The exact size of the automorphism group depends on the position of the elements η and μ within L.

Proposition 8.3.5. *Let $G = Gal(L/F)$ and let $C_G(\sigma)$ be the centraliser of σ in G. If A is one of the algebras $HK(L, \sigma, \eta, \mu), Kn_2(L, \sigma, \eta, \mu)$ or $Kn_3(L, \sigma, \eta, \mu)$ where $\mu \neq 0$, then the automorphism group of A is isomorphic to the subgroup of $C_G(\sigma)$ which fixes the element $\mu\sigma(\mu)\sigma(\eta)^{-1}$, i.e.,*

$$Aut(A) \cong \{\tau \in C_G(\sigma) \mid \tau\left(\frac{\mu\sigma(\mu)}{\sigma(\eta)}\right) = \frac{\mu\sigma(\mu)}{\sigma(\eta)}\}.$$

Proof. Suppose $A = HK(L, \sigma, \eta, \mu)$ and denote by φ_τ^b the automorphism of A

$$(x, y) \mapsto (\tau(x), \tau(y)b),$$

for all $(x, y) \in A$. From Proposition 8.3.1 we know that $\tau \in C_G(\sigma)$ and $\mu\sigma(b) = \tau(\mu)$. Since $\mu \neq 0$, the element $b \in L$ is determined completely by the action of τ on μ so we may drop the superscript b in φ_τ^b and write φ_τ. We also have the equation $\eta b\sigma(b) = \tau(\eta)$ defining φ_τ. Substituting in $b = \sigma^{-1}(\tau(\mu))\sigma^{-1}(\mu)^{-1}$ and rearranging gives

$$\sigma(\eta)\tau(\mu)\sigma(\tau(\mu)) = \sigma(\tau(\eta))\mu\sigma(\mu).$$

Since σ and τ commute, we can rearrange this further to get

$$\tau\left(\frac{\mu\sigma(\mu)}{\sigma(\eta)}\right) = \frac{\mu\sigma(\mu)}{\sigma(\eta)}.$$

Consider two such automorphisms φ_{τ_1} and φ_{τ_2} of A. Then

$$\varphi_{\tau_i}(x, y) = (\tau_i(x), \tau_i(y)b_i),$$

for all $(x, y) \in A$ and $b_i \in L$ satisfies

$$\eta b_i\sigma(b_i) = \tau_i(\eta) \text{ and } \mu\sigma(b_i) = \tau_i(\mu).$$

We see that

$$\varphi_{\tau_1} \circ \varphi_{\tau_2}(x, y) = \big(\tau_1\tau_2(x), \tau_1\tau_2(y)\tau_1(b_2)b_1\big),$$

so we need to show that $b := \tau_1(b_2)b_1$ satisfies the required properties for the automorphism $\varphi_{\tau_1\tau_2}$ namely

$$\eta b\sigma(b) = \tau_1\tau_2(\eta) \text{ and } \mu\sigma(b) = \tau_1\tau_2(\mu).$$

Firstly, we have that

$$\begin{aligned}
\tau_1\tau_2(\eta) = \tau_1(\eta b_2\sigma(b_2)) &= \tau_1(\eta)\tau_1(b_2)\tau_1\sigma(b_2) \\
&= \eta b_1\sigma(b_1)\tau(b_2)\tau_1\sigma(b_2) \\
&= \eta\tau_1(b_2)b_1\sigma(\tau_1(b_2)b_1) \\
&= \eta b\sigma(b).
\end{aligned}$$

Similar reasoning shows that

$$\tau_1\tau_2(\mu) = \tau_1(\mu\sigma(b_2)) = \tau_1(\mu)\sigma(\tau_1(b_2)) = \mu\sigma(b_1)\sigma(\tau_1(b_2)) = \mu\sigma(b).$$

Therefore $\varphi_{\tau_1} \circ \varphi_{\tau_2} = \varphi_{\tau_1\tau_2}$ and the map $\varphi_\tau \mapsto \tau$ is the required isomorphism. □

Corollary 8.3.6. *Let L/F be a quadratic, separable field extension and suppose A is one of the algebras $HK(L, \sigma, \eta, \mu)$, $Kn_2(L, \sigma, \eta, \mu)$ or $Kn_3(L, \sigma, \eta, \mu)$ where $\mu \neq 0$, then the automorphism group of A is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ if $\eta \in F$. Otherwise $Aut(A)$ is trivial.*

Proof. Since L/F is quadratic, σ is the nontrivial automorphism of L/F. By the previous Proposition, we can have at most two possible automorphisms of A: φ_{Id} and φ_σ. Moreover, $\varphi_\sigma \in Aut(A)$ if and only if

$$\sigma\left(\frac{\mu\sigma(\mu)}{\sigma(\eta)}\right) = \frac{\mu\sigma(\mu)}{\sigma(\eta)}.$$

Now $\mu\sigma(\mu) \in F^\times$ for all $\mu \in L^\times$, so this condition is equivalent to

$$\sigma\left(\frac{1}{\sigma(\eta)}\right) = \frac{1}{\sigma(\eta)}$$

i.e. $\eta = \sigma(\eta)$. This happens if and only if $\eta \in F$. □

8.4 A Semi-multiplicative Map for HK and Kn_3

In this section we will look at a map $M_{HK} : HK \to L$ which satisfies the property $M_{HK}((l, 0)(x, y)) = M_{HK}(l, 0)M_{HK}(x, y)$ for all $l, x, y \in L$. First notice that the multiplication in HK can be written in the following way:

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

If we denote the 2×2 matrix above by $R_{(u,v)}$ for all $(u, v) \in HK$, then we can define the map

$$M_{HK} : HK \to L$$

by

$$M_{HK}((u, v)) = \mathrm{Det}(R_{(u,v)}).$$

Proposition 8.4.1. *For all $l, x, y \in L$, the map M satisfies*

$$M_{HK}((l, 0)(x, y)) = M_{HK}((l, 0))M_{HK}((x, y)).$$

Proof. Explicitly we have

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

Therefore we get

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

□

In general, the map M_{HK} is not multiplicative, nor does it satisfy the property

$$M_{HK}((x, y)(l, 0)) = M_{HK}((x, y))M_{HK}((l, 0))$$

for all $l, x, y \in L$. Hence, M_{HK} is a left semi-multiplicative map which is not right semi-multiplicative.

Similarly, we may consider the multiplication in Kn_3 as follows:

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

If we define $M_{Kn_3} : Kn_3 \to L$ by

$$M_{Kn_3}((x, y)) = \mathrm{Det} \begin{pmatrix} x & y \\ \eta\sigma^{-1}(y) & \sigma(x) + \mu y \end{pmatrix},$$

explicitly this is

$$M_{Kn_3}((x,y)) = x\sigma(x) + \mu xy - \eta y\sigma^{-1}(y).$$

Then we get

$$\begin{aligned} M_{Kn_3}((x,y)(l,0)) &= M_{Kn_3}((xl, y\sigma(l))) \\ &= xl\sigma(xl) + \mu xly\sigma(l) + \eta y\sigma(l)\sigma^{-1}(y\sigma(l)) \\ &= (x\sigma(x) + \mu xy + y\sigma^{-1}(y))l\sigma(l) \\ &= M_{Kn_3}((x,y))M_{Kn_3}((l,0)). \end{aligned}$$

Therefore M_{Kn_3} is a right semi-multiplicative map which is not left semi-multiplicative.

8.5 Constructions for Noncommutative Algebras

In this section we generalise the above constructions to a doubling process which starts with an associative (but possibly noncommutative) F-algebra D. In this case we need to put some additional restrictions on the elements η and μ and we use a scalar involution of D rather than an automorphism. In the case where D is a quaternion algebra, these constructions can be thought of as a generalisation of octonion algebras. Recall that a scalar involution on D is an involution $^- : D \to D$, such that

$$x\overline{x} = \overline{x}x \in F.$$

Let D be an associative F-algebra with scalar involution, denoted $^-$, and pick elements $\eta, \mu \in F^\times$. On the vector-space $D \oplus D$ we can define the following

multiplications:

$$Kn_1 : (x,y) \circ (u,v) = (xu + \eta\bar{v}y, vx + y\bar{u} + \mu\bar{v}\bar{y}),$$

$$Kn_2 : (x,y) \circ (u,v) = (xu + \eta\bar{v}y, vx + y\bar{u} + \mu v\bar{y}),$$

$$Kn_3 : (x,y) \circ (u,v) = (xu + \eta\bar{v}y, vx + y\bar{u} + \mu vy),$$

$$HK : (x,y) \circ (u,v) = (xu + \eta\bar{v}y, vx + y\bar{u} + \mu\bar{v}y),$$

for all $x, y, u, v \in D$. As before we will denote the resulting algebras by $Kn_1(D, ^-, \eta, \mu), Kn_2(D, ^-, \eta, \mu), Kn_3(D, ^-, \eta, \mu)$ and $HK(D, ^-, \eta, \mu)$ respectively and we may omit some or all of these parameters when they are irrelevant to the discussion. Each of these is a unital F-algebra of dimension $2n$, where $n = \dim_F D$ and they each contain D as a subalgebra. If D is a quadratic separable field extension then these algebras are special cases of those defined in Section 2.

Theorem 8.5.1. *Suppose D is a division algebra. If the equation*

$$w^2 + \mu w - \eta$$

has no solutions in F, then each of $Kn_1(D, ^-, \eta, \mu), Kn_2(D, ^-, \eta, \mu)$, $Kn_3(D, ^-, \eta, \mu)$ and $HK(D, ^-, \eta, \mu)$ is a division algebra.

Proof. We will prove this for Kn_1. We suppose that

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

for some nonzero $(x,y), (u,v) \in Kn_1$. For the same reasons as mentioned at the beginning of the proof of Theorem 8.1.2, we may assume that x, y, u and v are all non zero and, since D is an associative division algebra, their inverses exist. From the definition of multiplication in Kn_1 we get the equations

$$xu + \eta\bar{v}y = 0, \tag{8.2}$$

and

$$vx + u\bar{u} + \mu\bar{v}\bar{y}. \tag{8.3}$$

From equation (8.2) we have $u = -x^{-1}\eta\bar{v}y$. Setting $z = -x^{-1}\eta\bar{v}$, we can write

$$u = zy \qquad \text{and} \qquad x = -\eta\bar{v}z^{-1}.$$

Substituting these into equation (8.3) gives us

$$-\eta v\bar{v}z^{-1} + y\bar{y}\bar{z} + \mu\bar{v}\bar{y} = 0.$$

Multiplying through on the right by z and on the left by $(v\bar{v})^{-1}$ yields

$$-\eta + (v\bar{v})^{-1}y\bar{y}\bar{z}z + \mu v^{-1}\bar{y}z.$$

Setting $w = v^{-1}\bar{y}z$ shows that

$$w\bar{w} + \mu w - \eta = 0,$$

and so, if this equation has no solutions in D, then Kn_1 has no zero divisors. However, notice that if w is not an element of F, then we cannot have

$$w\bar{w} + \mu w - \eta = 0,$$

since $w\bar{w}, \mu, \eta \in F$, so we only have to make sure this equation has no solutions in F. This is the same as requiring

$$w^2 + \mu w - \eta \neq 0,$$

for all $w \in F$. □

Chapter 9

Applications to Coding Theory

In this chapter we give an application of nonassociative algebras for the construction of Space-Time Block Codes (STBC's). STBC's are used in wireless communication to send data between multiple antennas, which helps to improve the reliability of the data transfer. The *codewords* for an STBC are represented by $n \times n$ matrices with complex entries. We then require that the *codebook*, i.e., the collection of all codewords, be *fully diverse*. This amounts to the condition that for any two distinct matrices in the codebook, say $A, B \in \mathrm{Mat}_n(\mathbb{C})$, we have $\mathrm{Det}(A - B) \neq 0$. Once we have a fully diverse codebook, we may then require some additional properties from the matrices that will affect the performance of the code.

In the seminal work by Sethuraman, Rajan and Shashidhar [51], a connection was made between central simple division algebras and fully diverse STBC's. If D is a central simple algebra of degree n then there exists a so-called *splitting representation* $\lambda : D \to \mathrm{Mat}_n(L)$, where L is a subfield of D. Since D is simple, this map is injective and, furthermore, if D is a division algebra, then $\mathrm{Im}(\lambda) \subset \mathrm{Mat}_n(L)$ only consists of invertible matrices and the zero matrix.

For more information on this see [9] or [50] for a general overview or for implementations of codes from central simple division algebras see [55], [7] or [8], to name but a few.

9.1 Codes from Nonassociative Algebras

In [47] the authors construct STBC's from a nonassociative quaternion algebra. Although nonassociative quaternions do not admit a splitting representation, there does exist an injective L-vector space homomorphism $\lambda : D \to \mathrm{Mat}_2(L)$, where $D := (L/F, \sigma, a)$ is a nonassociative quaternion algebra and L is the maximal subfield of D. This is done as follows: for $y = y_0 + y_1 z \in D$, $y_i \in L$, the map λ is defined by

$$\lambda(y) = \begin{bmatrix} y_0 & y_1 \\ a\sigma(y_1) & \sigma(y_0) \end{bmatrix}.$$

The matrix $\lambda(y)$ can be viewed as the matrix of right multiplication by the element y in D with respect to the basis $\{1, z\}$ of D as a left L-vector space. In fact, if we represent elements of D by tuples (y_0, y_1) then for another element $x = (x_0, x_1) \in D$ we have

$$xy = x\lambda(y).$$

It follows from elementary linear algebra that the matrix $\lambda(y)$ has nonzero determinant for all nonzero $y \in D$ since, otherwise, the system of linear equations $(x_0, x_1)\lambda(y) = (0, 0)$ has a nontrivial solution (x_0, x_1), which contradicts the fact that D contains no zero divisors. Thus, the set $\{\lambda(y) \mid 0 \neq y \in D\}$ is a fully diverse STBC.

We can extend this idea using nonassociative cyclic algebras of degree n in the obvious way.

Definition 9.1.1. Let $(L/F, \sigma, a)$ be a nonassociative cyclic algebra. For an element $y = y_0 + y_1 z + \cdots y_{n-1} z^{n-1} \in (L/F, \sigma, a)$, where each $y_i \in L$, we define $\lambda(y)$ to be the matrix

$$\begin{bmatrix} y_0 & y_1 & y_2 & \cdots & y_{n-1} \\ a\sigma(y_{n-1}) & \sigma(y_0) & \sigma(y_1) & \cdots & \sigma(y_{n-2}) \\ a\sigma^2(y_{n-2}) & a\sigma^2(y_{n-1}) & \sigma^2(y_0) & \cdots & \sigma^2(y_{n-3}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a\sigma^{n-1}(y_1) & a\sigma^{n-1}(y_2) & a\sigma^{n-1}(y_3) & \cdots & \sigma^{n-1}(y_0) \end{bmatrix}.$$

Theorem 9.1.2. *Let $D = (L/F, \sigma, a)$ be a nonassociative cyclic division algebra. The set*

$$\{\lambda(y) \mid 0 \neq y \in D\},$$

is a fully diverse STBC.

Proof. As in the proof of Theorem 3.2.10 in Chapter 3, we consider the matrix $\lambda(y)$ as the matrix of right multiplication by y in D, i.e., writing elements of D as n-tuples, we can express the product in D by the matrix multiplication

$$xy = x\lambda(y),$$

for all $x, y \in D$. Since D is division, a similar argument to that given above implies $\lambda(y)$ has nonzero determinant whenever $y \neq 0$. □

Codes from nonassociative cyclic algebras of degree 4 have successfully been constructed in a joint work with Oggier and Pumplün [54] using cyclic extensions of number fields. For example, $\mathbb{Q}(\zeta_5)/\mathbb{Q}$, where ζ_5 is a primitive 5th root of unity, is a cyclic extension of degree 4. Picking $a \in \mathbb{Q}(\zeta_5)$ such that $1, a, a^2, a^3$ are linearly independent over $\mathbb{Q}$, yields a nonassociative cyclic division algebra $(\mathbb{Q}(\zeta_5)/\mathbb{Q}, \sigma, a)$. The element a is chosen carefully to ensure the resulting STBC satisfies other desirable properties, for example, fast-decodability.

Following the proof of Theorem 9.1.2, we are able to give a more general method of constructing fully diverse STBC's from nonassociative division algebras. In particular, this method can be applied to several of the algebras studied in this thesis.

Suppose that $(A, \bullet)$ is a division algebra over F with multiplication denoted by $\bullet$ and such that A has a decomposition as a left (resp. right) n-dimensional L-vector space, where L is some subfield of A. We write

$$A = L \oplus L \oplus \cdots \oplus L,$$

as an L-vector space. Let $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1})$ be two elements of A written with respect to the L-vector space decomposition,

where $x_i, y_i \in L$. Furthermore, suppose that multiplication by the element y on the right (resp. by the element x on the left) in A can be represented by the matrix multiplication

$$x \bullet y = xM_r(y) \quad (\text{resp. } x \bullet y = (M_l(x)y^T)^T),$$

where $M_r(y)$ (resp. $M_l(x)$) is an $n \times n$ matrix with entries of L. It follows that the set of matrices $M_r(y)$ for nonzero $y \in A$ (resp. $M_l(x)$ for nonzero $x \in A$) forms a fully diverse STBC. A nonassociative cyclic algebra of degree n fits into this situation.

Example 9.1.3. Let $A = \Omega_{L,a,\sigma}$ be the algebra defined by Sandler in [48]. It was shown in Proposition 3.2.14 that A is isomorphic to the opposite algebra of the nonassociative cyclic algebra $(L/F, \sigma, a)$. A is a right L-vector space:

$$A = L \oplus zL \oplus \cdots \oplus z^{n-1}L,$$

and if we write the elements of A as row vectors, i.e., $x = (x_0, \ldots, x_{n-1}), y = (y_0, \ldots, y_{n-1})$, where $x_i, y_i \in L$, we can express the multiplication in A as the matrix product

$$xy = (M_l(x)y^T)^T,$$

where $M_l(x)$ is the $n \times n$ matrix

$$\begin{bmatrix} x_0 & a\sigma(x_{n-1}) & \ldots & a\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \ldots & a\sigma^{n-1}(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \ldots & \sigma^{n-1}(x_0) \end{bmatrix}.$$

Remark 9.1.4. An associative cyclic algebra $(L/F, \sigma, a), a \in F^\times$, is often defined as a right K-vector space with the appropriate multiplication. When this definition is adopted in the coding theory literature, the STBC's which arise from cyclic division algebras consist of matrices of the form $M_l(x)$ given above, except with a now being an element of $F^\times$.

Example 9.1.5 (Menichetti's Construction)**.** Following the examples in Chapter 7, we can construct several different 3×3 and 4×4 STBC's. In the 3×3 case, we have a cubic cyclic field extension L/F and seek elements $a, b, c \in L$ such that the matrix

$$\begin{bmatrix} x_0 & x_1 & x_2 \\ ca^{-1}\sigma(x_2) & \sigma(x_0) & ba^{-1}\sigma(x_1) \\ ca^{-1}\sigma^2(x_1) & cb^{-1}\sigma^2(x_2) & \sigma^2(x_0) \end{bmatrix},$$

has nonzero determinant for all $(0,0,0) \neq (y_0, y_1, y_2) \in L^3$. For example, (see Example 7.2.2) we could choose $a = c \in L \setminus F$ and $b = 1$. Our codebook coming from the algebra $(L/F, c, 1, c)$ consists of all matrices of the form

$$\begin{bmatrix} x_0 & x_1 & x_2 \\ \sigma(x_2) & \sigma(x_0) & c^{-1}\sigma(x_1) \\ \sigma^2(x_1) & c\sigma^2(x_2) & \sigma^2(x_0) \end{bmatrix}.$$

Similarly, following Example 7.3.5, we can take L/F to be a cyclic field extension of degree 4 and get a fully diverse codebook consisting of matrices of the form

$$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ d\sigma(x_3) & \sigma(x_0) & d\sigma(x_1) & d\sigma(x_2) \\ d\sigma^2(x_2) & \sigma^2(x_3) & \sigma^2(x_0) & d\sigma^2(x_1) \\ d\sigma^3(x_1) & \sigma^3(x_2) & \sigma^3(x_3) & \sigma^3(x_0) \end{bmatrix},$$

coming from the algebra $(L/F, 1, d, d, d)$, where $d \in L$ is such that $1, d, d^2, d^3$ are linearly independent over F.

Alternatively, we could take L/F to be a biquadratic field extension and, following Example 7.4.3, get a fully diverse codebook consisting of matrices of the form

$$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ a^{-1}\sigma(x_3) & \sigma(x_0) & a^{-1}\sigma(x_1) & a^{-1}\sigma(x_2) \\ a^{-1}\tau(x_2) & \tau(x_3) & \tau(x_0) & a^{-1}\tau(x_1) \\ a^{-1}\sigma^3(x_1) & \sigma\tau(x_2) & \sigma\tau(x_3) & \sigma\tau(x_0) \end{bmatrix},$$

coming from the algebra $(L/F, a, 1, 1, 1)$, where $a \in L$ is such that $1, a, a^2, a^3$ are linearly independent over F.

We will also construct 2 fully-diverse 2×2 STBC's based on the constructions of Hughes-Kleinfeld and Knuth given in Chapter 8. We briefly recall the definitions here.

Definition 9.1.6. 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

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

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. The multiplication in HK may be written as

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

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

If the algebra HK is division, then the matrix on the right hand side of the above equation will have nonzero determinant for all $(u, v) \neq 0$. Thus we get a fully diverse codebook of matrices of the form

$$\begin{bmatrix} u & v \\ \eta\sigma(v) & \sigma(u) + \mu\sigma(v) \end{bmatrix},$$

for all $u, v \in L$, where $\mu, \eta \in L$ are such that the equation

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

has no roots in L.

Our second example is based on a construction of Knuth.

Definition 9.1.7. 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 $Kn_3(L, \sigma, \eta, \mu) = L \oplus L$ with the multiplication

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

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

$Kn_3(L, \sigma, \eta, \mu)$ 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.

We may write the multiplication in Kn_3 as

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

As before, if Kn_3 is a division algebra then we will get a fully diverse codebook consisting of the matrices

$$\begin{bmatrix} u & v \\ \eta\sigma^{-1}(v) & \sigma(u) + \mu v \end{bmatrix},$$

for $u, v \in L$ and $\mu, \eta \in L$ such that the equation

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

has no roots in L.

Remark 9.1.8. Suppose that L/F is a quadratic extension, $\eta \in F$ and $\mu = 0$. As noted in Section 2 of Chapter 8, the algebras HK and Kn_3 are quaternion algebras in this case. Two of the best performing STBC's known are the Alamouti code [1] and the Golden code [6], both of which are based on quaternion algebras. We remark that, if $\mu \neq 0$, then the extra term $\mu\sigma(v)$ (resp. μv) in the bottom right entry of the codes defined above will most likely have an adverse effect on their performance. However, we include these codes for the sake of completeness and leave it to the coding theory experts to determine how well they actually perform.

9.2 An Iterated Code Construction

In this section we show how to construct a new nonassociative algebra using copies of an associative cyclic division algebra $D = (K/F, \sigma, \gamma)$. This is inspired by a nonassociative algebra constructed in [52], which is used to construct STBC's. In certain special cases this construction yields the STBC's that arise from (associative or nonassociative) cyclic division algebras and, therefore, can be thought of as a generalisation of these codes.

We will use the notation defined below throughout the remainder of the section. Let F and L be fields and let K be a cyclic extension of both F and L such that

1. $Gal(K/F) = \langle \sigma \rangle$ and $[K : F] = m$,
2. $Gal(K/L) = \langle \tau \rangle$ and $[K : L] = n$,
3. σ and τ commute: $\sigma\tau = \tau\sigma$.

Let $D = (K/F, \sigma, \gamma)$ be an associative cyclic division algebra of degree m with standard basis $\{1, e, \ldots, e^{m-1}\}$ and some suitable element $\gamma \in F \cap L$, i.e.,

$$D := K \oplus Ke \oplus \cdots \oplus Ke^{m-1},$$

with multiplication defined by the rules

$$ek = \sigma(k)e, \qquad \text{and} \quad e^m = \gamma,$$

for all $k \in K$.

For $x = x_0 + x_1 e + x_2 e^2 + \cdots + x_{m-1}e^{m-1} \in D$, define the L-linear map $\widetilde{\tau} : D \to D$ via

$$\widetilde{\tau}(x) = \tau(x_0) + \tau(x_1)e + \tau(x_2)e^2 + \cdots + \tau(x_{m-1})e^{m-1}.$$

The maps $\widetilde{\tau}^i$, for $2 \leq i \leq n-1$ are defined analogously.

Definition 9.2.1. Pick $d \in D^\times$ and define the left D-module

$$It^n(D, \tau, d) = D \oplus Df \oplus Df^2 \oplus \cdots \oplus Df^{n-1}.$$

Multiplication on $It^n(D, \tau, d)$ is defined by the rules

$$(xf^i)(yf^j) = \begin{cases} x\widetilde{\tau}^i(y)f^{i+j} & \text{if } i+j < n \\ x\widetilde{\tau}^i(y)df^{(i+j)-n} & \text{if } i+j \geq n, \end{cases}$$

for all $x, y \in D$.

Remarks 9.2.2.

1. Our assumption that γ is also an element of L implies that $\widetilde{\tau}$ is multiplicative on D: $\widetilde{\tau}(xy) = \widetilde{\tau}(x)\widetilde{\tau}(y)$ for all $x, y \in D$.

2. The fact that $\tau(\gamma) = \gamma$ also implies that $\lambda(\widetilde{\tau}(x)) = \tau(\lambda(x))$ for all $x \in D$, where $\lambda(x)$ is the splitting representation of D.

3. In general, $It^n(D, \tau, d)$ is a nonassociative, unital algebra with unit 1_D. It contains D as an associative subalgebra.

We can represent multiplication in $It^n(D, \tau, d)$ by a particular matrix multiplication. For an element $y = y_0 + y_1 f + y_2 f^2 + \cdots + y_{n-1} f^{n-1} \in It^n(D, \tau, d)$, where $y_i \in D$, we define the $n \times n$ matrix

$$M(y) = \begin{bmatrix} y_0 & y_1 & y_2 & \cdots & y_{n-1} \\ \widetilde{\tau}(y_{n-1})d & \widetilde{\tau}(y_0) & \widetilde{\tau}(y_1) & \cdots & \widetilde{\tau}(y_{n-2}) \\ \widetilde{\tau}^2(y_{m-2})d & \widetilde{\tau}^2(y_{n-1})d & \widetilde{\tau}^2(y_0) & \cdots & \widetilde{\tau}^2(y_{n-3}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \widetilde{\tau}^{n-1}(y_1)d & \widetilde{\tau}^{n-1}(y_2)d & \widetilde{\tau}^{n-1}(y_3)d & \cdots & \widetilde{\tau}^{n-1}(y_0) \end{bmatrix}$$

with entries in D. If we represent $x = x_0 + x_1 f + \cdots x_{n-1} f^{n-1} \in It^n(D, \tau, d)$ as a row vector $(x_0, x_1, \ldots, x_{n-1})$, where each $x_i \in D$, then we can write the product of two elements, $x, y \in It^n(D, \tau, d)$ as the matrix multiplication

$$xy = xM(y).$$

Since D is a left K-vector space of dimension m, $It^n(D, \tau, d)$ is a left K-vector space of dimension mn. If $\{1, e, \ldots, e^{m-1}\}$ is the standard basis for D, then

$$\{1, e, \ldots, e^{m-1}, f, ef, \ldots, e^{m-1}f^{n-1}\}$$

is a basis for $It^n(D, \tau, d)$ as a left K-vector space. Taking this into consideration, we write elements in $It^n(D, \tau, d)$ as row vectors of length mn with entries in K. We can now express the product of two elements $x, y \in It^n(D, \tau, d)$ by the matrix multiplication

$$xy = x\lambda(M(y)),$$

where $\lambda(M(y))$ is the $mn \times mn$ matrix defined by taking the splitting representation of each entry in the matrix $M(y)$. By the previous remark, we can write the matrix $\lambda(M(y))$ as

$$\lambda(M(y)) = \begin{bmatrix} \lambda(y_0) & \lambda(y_1) & \cdots & \lambda(y_{n-1}) \\ \tau(\lambda(y_{n-1}))\lambda(d) & \tau(\lambda(y_0)) & \cdots & \tau(\lambda(y_{n-2})) \\ \vdots & \vdots & \ddots & \vdots \\ \tau^{n-1}(\lambda(y_1))\lambda(d) & \tau^{n-1}(\lambda(y_2))\lambda(d) & \cdots & \tau^{n-1}(\lambda(y_0)) \end{bmatrix} \quad (9.1)$$

with $y_i \in D$.

Definition 9.2.3. Let $y = y_0 + y_1 f + \cdots + y_{n-1} f^{n-1}$ be an element of the algebra $It^n(D, \tau, d)$. We call the $mn \times mn$ matrix $\lambda(M(y))$ the *matrix of right multiplication* by the element y.

Because the matrices $\lambda(M(y))$ can be used to define multiplication in $It^n(D, \tau, d)$, we get the following, more general, version of Theorem 2 in [52].

Theorem 9.2.4. *Let $A = It^n(D, \tau, d)$ and let $y \in A$ be nonzero. If y is not a right zero divisor in A, then the matrix of right multiplication by y, $\lambda(M(y))$ has nonzero determinant. In particular, if $C \subseteq A$ is a linear subset of A such that every $y \in C$ is not a right zero divisor, then*

$$\mathcal{C} := \{\lambda(M(y)) \mid 0 \neq y \in C\}$$

forms a fully diverse, linear space-time block code.

Proof. Suppose $\lambda(M(y))$ is a singular matrix. Then the system of mn linear equations

$$(x_0, \ldots, x_{mn-1})\lambda(M(y)) = 0$$

has a non-trivial solution $(x_0, \ldots, x_{mn-1}) \in K^{mn}$ which contradicts the assumption that y is not a right zero divisor in A. $\square$

In general it is difficult to determine whether $It^n(D, \tau, d)$ is a division algebra or not. However, we can show that there exist linear subspaces which consist of elements that are not right zero divisors. First, we require the following lemma.

Lemma 9.2.5. *Let $D := (K/F, \sigma, \gamma)$ be an associative cyclic division algebra such that $\gamma \in L$ and let $A = It^n(D, \tau, d)$. Then D is contained in the middle nucleus of A.*

Proof. By linearity of multiplication, we only need to show that

$$((xf^i)y)zf^j = xf^i(y(zf^j)),$$

for all $x, y, z \in D$ and all integers $0 \leq i, j \leq n-1$. A straightforward calculation shows that these are equal if and only if $\widetilde{\tau}(x)\widetilde{\tau}(y) = \widetilde{\tau}(xy)$ for all $x, y \in D$. This is true if and only if $\tau(\gamma) = \gamma$. $\square$

Theorem 9.2.6. *Let $D = (K/F, \sigma, \gamma)$ be an associative cyclic division algebra of degree m such that $\gamma \in L$ and let $A = It^n(D, \tau, d)$. If $d \neq \widetilde{\tau}^{n-1}(z)\widetilde{\tau}^{n-2}(z)\ldots\widetilde{\tau}(z)z$ for all $z \in D$, then all elements in A of the form $y = y_0 + y_1 f$ are not right zero divisors.*

Proof. Suppose that

$$(x_0 + x_1 f + \cdots + x_{n-1}f^{n-1})(y_0 + y_1 f) = 0,$$

where $x_i, y_i \in D$ and at least one of the $x_i \neq 0$. We may assume that y_0 and y_1 are both nonzero since, otherwise, it is straightforward to see that this leads to a contradiction. Because D is contained in the middle nucleus of A, we can rewrite this as

$$(x_0' + x_1' f + \cdots x_{n-1}' f^{n-1})(y_0' + f) = 0,$$

where $y_0' = y_1^{-1} y_0$ and

$$x_i' = x_i \widetilde{\tau}^i(y_1),$$

for all $i = 0 \dots n-1$. Since the elements f^i are linearly independent over A, we have the equations

$$x_0' y_0' + x_{n-1}' d = 0 \tag{9.2}$$

$$x_i' \widetilde{\tau}(y_0') + x_{i-1}' = 0 \quad \text{for all } 1 \leq i \leq n-1. \tag{9.3}$$

Since $y_0' \neq 0$, equations (9.2) and (9.3) imply that $x_i' \neq 0$ for all $i = 0 \dots n-1$. Therefore, solving equation (9.3), we get

$$x_0' = (-1)^{n-1} x_{n-1}' \widetilde{\tau}^{n-1}(y_0') \dots \widetilde{\tau}(y_0').$$

Putting this into equation (9.2) yields

$$(-1)^{n-1} x_{n-1}' \big(\widetilde{\tau}^{n-1}(y_0') \dots \widetilde{\tau}(y_0') y_0' + d \big) = 0.$$

It follows that

$$\widetilde{\tau}^{n-1}(y_0') \dots \widetilde{\tau}(y_0') y_0' = (-1)^n d,$$

since $x_{n-1} \neq 0$. Setting $z = -y_0'$ now gives the desired contradiction. □

Corollary 9.2.7. *Let $D = (K/F, \sigma, \gamma)$ be an associative cyclic division algebra of degree m such that $\gamma \in L$ and let $A = It^n(D, \tau, d)$. If $d \neq \widetilde{\tau}^{n-1}(z)\widetilde{\tau}^{n-2}(z) \dots \widetilde{\tau}(z) z$ for all $z \in D$, then the set*

$$\{\lambda(M(y)) \mid 0 \neq y = y_0 + y_1 f \in A\}$$

is a fully diverse STBC, it consists of all matrices of the form

$$\lambda(M(y)) = \begin{bmatrix} \lambda(y_0) & \lambda(y_1) & 0 & \cdots & 0 \\ 0 & \tau(\lambda(y_0)) & \tau(\lambda(y_1)) & \cdots & 0 \\ 0 & 0 & \tau^2(\lambda(y_0)) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \tau^{n-1}(\lambda(y_1))\lambda(d) & 0 & 0 & \cdots & \tau^{n-1}(\lambda(y_0)) \end{bmatrix}.$$

9.2.1 Special Case: $n = 2$

If $n = 2$ in Definition 9.2.1, we have $A = It^2(D, \tau, d) = D \oplus Df$ for some cyclic division algebra D. If $d \neq \widetilde{\tau}(z)z$ for all $z \in D$, then, by Theorem 9.2.6, A contains no right zero divisors. It follows that A contains no left zero divisors either and is a division algebra. We consider a space-time block code consisting of the matrices of right multiplication by elements in A, i.e., matrices of the form

$$\begin{bmatrix} \lambda(y_0) & \lambda(y_1) \\ \tau(\lambda(y_1))\lambda(d) & \tau(\lambda(y_0)) \end{bmatrix},$$

where $y_0, y_1 \in D$.

Example 9.2.8. Suppose that D is a quaternion division algebra and let $d = d_0 + d_1 e \in D$ be such that $d \neq \widetilde{\tau}(z)z$ for all $z \in D$. Let $x = x_0 + x_1 e, y = y_0 + y_1 e \in D^\times$, where $x_i, y_i \in K$. Then

$$\lambda(x) = \begin{bmatrix} x_0 & x_1 \\ \sigma(x_1)\gamma & \sigma(x_0) \end{bmatrix},$$

and $\lambda(y)$, $\lambda(d)$ look similar, mutatis mutandis. The matrix of right multiplication by the element $x + yf \in A = It^2(D, \tau, d)$ is

$$\begin{bmatrix} \lambda(x) & \lambda(y) \\ \tau(\lambda(y))\lambda(d) & \tau(\lambda(x)) \end{bmatrix}.$$

Notice that the matrix multiplication in the bottom left block of this matrix is explicitly

$$\begin{aligned} \tau(\lambda(y))\lambda(d) &= \begin{bmatrix} \tau(y_0)d_0 + \tau(y_1)\gamma\sigma(d_1) & \tau(y_0)d_1 + \tau(y_1)\sigma(d_0) \\ (\sigma\tau(y_1)d_0 + \sigma\tau(y_0)\sigma(d_1))\gamma & \sigma\tau(y_1)\gamma d_1 + \sigma\tau(y_0)\sigma(d_0) \end{bmatrix} \\ &= \begin{bmatrix} u_1 & u_2 \\ u_3 & u_4 \end{bmatrix}. \end{aligned}$$

Thus, the 4×4 matrix of right multiplication by $x + yf$ is given by

$$\begin{bmatrix} x_0 & x_1 & y_0 & y_1 \\ \sigma(x_1)\gamma & \sigma(x_0) & \sigma(y_1)\gamma & \sigma(y_0) \\ u_1 & u_3 & \tau(x_0) & \tau(x_1) \\ u_2 & u_4 & \tau(\sigma(x_1))\gamma & \tau(\sigma(x_0)) \end{bmatrix},$$

where u_i, defined above, are the entries of the matrix $\tau(\lambda(y))\lambda(d)$.

To simplify the matrix, we restrict the element d to the field K, i.e. $d = d_0 + 0e$ above. In this case $\lambda(d) = \text{diag}[d_0, \sigma(d_0)]$. The matrix of right multiplication now becomes

$$\begin{bmatrix} x_0 & x_1 & y_0 & y_1 \\ \sigma(x_1)\gamma & \sigma(x_0) & \sigma(y_1)\gamma & \sigma(y_0) \\ \tau(y_0)d_0 & \tau(y_1)\sigma(d_0) & \tau(x_0) & \tau(x_1) \\ \sigma\tau(y_1)\gamma d_0 & \sigma(d_0)\sigma\tau(y_0) & \tau(\sigma(x_1))\gamma & \tau(\sigma(x_0)) \end{bmatrix}.$$

Similarly, we can consider $d = 0 + d_0 e$. In this case the matrix of right multiplication by $x + yf$ is

$$\begin{bmatrix} x_0 & x_1 & y_0 & y_1 \\ \sigma(x_1\gamma) & \sigma(x_0) & \sigma(y_1)\gamma & \sigma(y_0) \\ \tau(y_1)\gamma\sigma(d_0) & \tau(y_0)d_0 & \tau(x_0) & \tau(x_1) \\ \sigma\tau(y_0)\gamma\sigma(d_0) & \sigma\tau(y_1)\gamma d_0 & \tau(\sigma(x_1))\gamma & \tau(\sigma(x_0)) \end{bmatrix}.$$

Example 9.2.9. Suppose that $D = (K/F, \sigma, \gamma)$ is a cyclic division algebra of degree 3 and let $d \in K$. Let $x = x_0 + x_1 e + x_2 e^2, y = y_0 + y_1 e + y_2 e^2 \in D$ where each $x_i, y_i \in K$. Then

$$\lambda(x) = \begin{bmatrix} x_0 & x_1 & x_2 \\ \sigma(x_2)\gamma & \sigma(x_0) & \sigma(x_1) \\ \sigma^2(x_1)\gamma & \gamma\sigma^2(x_2) & \sigma^2(x_0) \end{bmatrix},$$

and similarly for $\lambda(y)$. We have $\lambda(d) = \text{diag}[d, \sigma(d), \sigma^2(d)]$. For the element $x + yf \in It^2(D, \tau, d) = A$, the 6×6 right multiplication matrix is given by

$$\begin{bmatrix} x_0 & x_1 & x_2 & y_0 & y_1 & y_2 \\ \sigma(x_2)\gamma & \sigma(x_0) & \sigma(x_1) & \sigma(y_2)\gamma & \sigma(y_0) & \sigma(y_1) \\ \sigma^2(x_1)\gamma & \sigma^2(x_2)\gamma & \sigma^2(x_0) & \sigma^2(y_1)\gamma & \sigma^2(y_2)\gamma & \sigma^2(y_0) \\ \tau(y_0)d & \tau(y_1)\sigma(d) & \tau(y_2)\sigma^2(d) & \tau(x_0) & \tau(x_1) & \tau(x_2) \\ \tau\sigma(y_2)\gamma d & \tau\sigma(y_0)\sigma(d) & \tau\sigma(y_1)\sigma^2(d) & \tau\sigma(x_2)\gamma & \tau\sigma(x_0) & \tau\sigma(x_1) \\ \tau\sigma^2(y_1)\gamma d & \tau\sigma^2(y_2)\gamma\sigma(d) & \tau\sigma^2(y_0)\sigma^2(d) & \tau\sigma^2(x_1)\gamma & \tau\sigma^2(x_2)\gamma & \tau\sigma^2(x_0) \end{bmatrix}.$$

9.2.2 Special case: $m = 1$

Suppose now that $K = F$ in Definition 9.2.1. By a slight abuse of notation we take our division algebra D to be the field K itself and the splitting representation to be the identity on K. Let L be as before, so that K/L is a cyclic field extension of degree n with Galois group generated by the automorphism τ. For some element $d \in K$, we may form the algebra

$$It^n(K, \tau, d) = K \oplus Kf \oplus \cdots \oplus Kf^{n-1}$$

with the same multiplication as given in Definition 9.2.1. Then $It^n(K, \tau, d)$ is the cyclic algebra $(K/L, \tau, d)$ which is associative if $d \in L$ and nonassociative if $d \notin L$. For an element $x = x_0 + x_1 f + \cdots + x_{n-1} f^{n-1} \in It^n(K, \tau, d)$, the right multiplication matrix of x is

$$\begin{bmatrix} x_0 & x_1 & \dots & x_{n-1} \\ \tau(x_{n-1})d & \tau(x_0) & \dots & \tau(x_{n-2}) \\ \vdots & \vdots & \ddots & \vdots \\ \tau^{n-1}(x_1)d & \tau^{n-1}(x_2)d & \dots & \tau^{n-1}(x_0) \end{bmatrix}.$$

Since conditions are known for $It^n(K, \tau, d) = (K/L, \tau, d)$ to be a division algebra, we get a more general result than in Theorem 9.2.6 above.

Theorem 9.2.10. *Let $A = It^n(K, \tau, d)$. If $d \in L^\times$ and $d^s \neq N_{K/L}(k)$ for all $k \in K$ and all $1 \leq s \leq n-1$, then A is a division algebra. If $d \in K \setminus L$ and is such that $1, d, d^2, \ldots, d^{n-1}$ are linearly independent over L, then A is a division algebra. In particular, if n is prime, then A is division for any choice of $d \in K \setminus L$.*

Proof. When $d \in L$, $A = (K/L, \tau, d)$ is an associative cyclic algebra and this result is well known. When $d \in K \setminus L$, $A = (K/L, \tau, d)$ is a nonassociative cyclic algebra and the proof is given in Chapter 3. □

Bibliography

[1] S. M. Alamouti. A simple transmitter diversity scheme for wireless communications. *IEEE J. Sel. Areas Commun*, pages 1451–1458, 1998.

[2] A. A. Albert. Non-associative algebras. I. Fundamental concepts and isotopy. *Ann. of Math. (2)*, 43:685–707, 1942.

[3] A. A. Albert. Finite division algebras and finite planes. In *Proc. Sympos. Appl. Math., Vol. 10*, pages 53–70. American Mathematical Society, Providence, R.I., 1960.

[4] S. C. Althoen, K. D. Hansen, and L. D. Kugler. **C**-associative algebras of dimension 4 over **R**. *Algebras Groups Geom.*, 3(3):329–360, 1986.

[5] S. Ball and M. Lavrauw. On the Hughes-Kleinfeld and Knuth's semifields two-dimensional over a weak nucleus. *Des. Codes Cryptogr.*, 44(1-3):63–67, 2007.

[6] J.C. Belfiore, G. Rekaya, and E. Viterbo. The Golden code: a 2×2 full-rate space-time code with nonvanishing determinants. *IEEE Trans. Inform. Theory*, 51(4):1432–1436, 2005.

[7] G. Berhuy and F. Oggier. Space-time codes from crossed product algebras of degree 4. In *Applied algebra, algebraic algorithms and error-correcting codes*, volume 4851 of *Lecture Notes in Comput. Sci.*, pages 90–99. Springer, Berlin, 2007.

[8] G. Berhuy and F. Oggier. On the existence of perfect space-time codes. *IEEE Trans. Inform. Theory*, 55(5):2078–2082, 2009.

[9] G. Berhuy and F. Oggier. *An introduction to central simple algebras and their applications to wireless communication*, volume 191 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2013.

[10] R. H. Bruck. Contributions to the theory of loops. *Trans. Amer. Math. Soc.*, 60:245–354, 1946.

[11] M. V. D. Burmester. On the commutative non-associative division algebras of even order of L. E. Dickson. *Rend. Mat. e Appl. (5)*, 21:143–166, 1962.

[12] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel. Z_4-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. *Proc. London Math. Soc. (3)*, 75(2):436–480, 1997.

[13] M. Cordero and G. P. Wene. A survey of finite semifields. *Discrete Math.*, 208/209:125–137, 1999. Combinatorics (Assisi, 1996).

[14] E. Darpö. Some modern developments in the theory of real division algebras. *Proc. Est. Acad. Sci.*, 59(1):53–59, 2010.

[15] U. Dempwolff. On irreducible semilinear transformations. *Forum Math.*, 22(6):1193–1206, 2010.

[16] U. Dempwolff. Autotopism groups of cyclic semifield planes. *J. Algebraic Combin.*, 34(4):641–669, 2011.

[17] L. E. Dickson. Linear algebras in which division is always uniquely possible. *Trans. Amer. Math. Soc.*, 7(3):370–390, 1906.

[18] L. E. Dickson. Linear algebras with associativity not assumed. *Duke Math. J.*, 1(2):113–125, 1935.

[19] P. K. Draxl. *Skew fields*, volume 81 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1983.

[20] S. González, C. Martínez, and I. F. Rúa. Symplectic spread-based generalized Kerdock codes. *Des. Codes Cryptogr.*, 42(2):213–226, 2007.

[21] G. Hochschild. On the cohomology theory for associative algebras. *Ann. of Math. (2)*, 47:568–579, 1946.

[22] D. R. Hughes and E. Kleinfeld. Seminuclear extensions of Galois fields. *Amer. J. Math.*, 82:389–392, 1960.

[23] N. Jacobson. *Structure and representations of Jordan algebras*. American Mathematical Society Colloquium Publications, Vol. XXXIX. American Mathematical Society, Providence, R.I., 1968.

[24] N. Jacobson. *Basic algebra. I*. W. H. Freeman and Company, New York, second edition, 1985.

[25] V. Jha and N. L. Johnson. An analog of the Albert-Knuth theorem on the orders of finite semifields, and a complete solution to Cofman's subplane problem. *Algebras Groups Geom.*, 6(1):1–35, 1989.

[26] N. L. Johnson, G. Marino, O. Polverino, and R. Trombetti. On a generalization of cyclic semifields. *J. Algebraic Combin.*, 29(1):1–34, 2009.

[27] W. M. Kantor. Finite semifields. In *Finite geometries, groups, and computation*, pages 103–114. Walter de Gruyter GmbH & Co. KG, Berlin, 2006.

[28] W. M. Kantor and M. E. Williams. Symplectic semifield planes and $\mathbb{Z}_4$-linear codes. *Trans. Amer. Math. Soc.*, 356(3):895–938, 2004.

[29] E. Kleinfeld. Techniques for enumerating Veblen-Wedderburn systems. *J. Assoc. Comput. Mach.*, 7:330–337, 1960.

[30] M. A. Knus, A. Merkurjev, M. Rost, and J. P. Tignol. *The book of involutions*, volume 44 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1998.

[31] D. E. Knuth. *Finite semifields and projective planes*. ProQuest LLC, Ann Arbor, MI, 1963. Thesis (Ph.D.)–California Institute of Technology.

[32] T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.

[33] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[34] M. Lavrauw and O. Polverino. *Finite Semifields*. Chapter 6 in Current Research Topics in Galois Geometry. NOVA Academic Publishers, 2011.

[35] J. H. Maclagan-Wedderburn. A theorem on finite algebras. *Trans. Amer. Math. Soc.*, 6(3):349–352, 1905.

[36] J. P. May, D. Saunders, and Z. Wan. Efficient matrix rank computation with application to the study of strongly regular graphs. In *ISSAC 2007*, pages 277–284. ACM, New York, 2007.

[37] K. McCrimmon. A general theory of Jordan rings. *Proc. Nat. Acad. Sci. U.S.A.*, 56:1072–1079, 1966.

[38] K. McCrimmon. *A taste of Jordan algebras*. Universitext. Springer-Verlag, New York, 2004.

[39] G. Menichetti. Algebre tridimensionali su un campo di Galois. *Ann. Mat. Pura Appl. (4)*, 97:283–301, 1973.

[40] G. Menichetti. Sopra una classe di quasicorpi distributivi di ordine finito. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8)*, 59(5):339–348, 1975.

[41] G. Menichetti. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field. *J. Algebra*, 47(2):400–410, 1977.

[42] R. Parimala, R. Sridharan, and Maneesh L. Thakur. Tits' constructions of Jordan algebras and F_4 bundles on the plane. *Compositio Math.*, 119(1):13–40, 1999.

[43] H.P. Petersson. Comments on a generalised tits construction. *Private Communication*, 2011.

[44] R. S. Pierce. *Associative algebras*, volume 88 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982. Studies in the History of Modern Science, 9.

[45] S. Pumplün. How to obtain division algebras from twisted Cayley-Dickson doublings. *Comm. Algebra*, 40(8):2989–3009, 2012.

[46] S. Pumplün and A. Steele. Algebras carrying maps of degree n. 2012. Available online at `http://molle.fernuni-hagen.de/~loos/jordan/index.html`.

[47] S. Pumplün and T. Unger. Space-time block codes from nonassociative division algebras. *Adv. Math. Commun.*, 5(3):449–471, 2011.

[48] R. Sandler. Autotopism groups of some finite non-associative algebras. *Amer. J. Math.*, 84:239–264, 1962.

[49] R. D. Schafer. *An introduction to nonassociative algebras*. Dover Publications Inc., New York, 1995. Corrected reprint of the 1966 original.

[50] B. A. Sethuraman. Division algebras and wireless communication. *Notices Amer. Math. Soc.*, 57(11):1432–1439, 2010.

[51] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar. Full-diversity, high-rate space-time block codes from division algebras. *IEEE Trans. Inform. Theory*, 49(10):2596–2616, 2003.

[52] K.P. Srinath and B.S. Rajan. Fast-decodable MIDO codes with large coding gain. 2013. Available online at `http://arxiv.org/abs/1208.1593`.

[53] A. Steele. Nonassociative cyclic algebras. *To appear in Israel J. Math.*, 2012. Available online at `http://molle.fernuni-hagen.de/~loos/jordan/index.html`.

[54] A. Steele, S. Pumplün, and F. Oggier. MIDO space-time codes from associative and nonassociative cyclic algebras. *Proc. IEEE Information Theory Workshop (ITW) 2012, Lausanne, Switzerland (In Press.)*, pages 192–196, 2012.

[55] R. Vehkalahti, C. Hollanti, and F. Oggier. Fast-decodable asymmetric space-time codes from division algebras. *IEEE Trans. Inform. Theory*, 58(4):2362–2385, 2012.

[56] W. C. Waterhouse. Nonassociative quarternion algebras. *Algebras Groups Geom.*, 4(3):365–378, 1987.

[57] G. P. Wene. Inner automorphisms of finite semifields. *Note Mat.*, 29(suppl. 1):231–242, 2009.