University of Nottingham

School of Mathematical Sciences

New classes of nonassociative division algebras and MRD codes

Daniel Thompson

A thesis submitted to the University of Nottingham for the degree of

Doctor of Philosophy

October 2020

Abstract

In the first part of the thesis, we generalize a construction by J Sheekey that employs skew polynomials to obtain new nonassociative division algebras and maximum rank distance (MRD) codes. This construction contains Albert's twisted fields as special cases. As a byproduct, we obtain a class of nonassociative real division algebras of dimension four which has not been described in the literature so far in this form. We also obtain new MRD codes.

In the second part of the thesis, we study a general doubling process (similar to the one that can be used to construct the complex numbers from pairs of real numbers) to obtain new non-unital nonassociative algebras, starting with cyclic algebras. We investigate the automorphism groups of these algebras and when they are division algebras. In particular, we obtain a generalization of Dickson's commutative semifields.

We are using methods from nonassociative algebra throughout.

Acknowledgements

I would like to express my gratitude to my supervisor Susanne Pumplün for all her help and support over the past three years. Her guidance, knowledge and enthusiasm have been invaluable to my research. A special mention goes to John Sheekey at University College Dublin, whose insightful communications were invaluable in Chapter 3.

To all my friends I made during my time here, thank you for making my experience much more enjoyable and less stressful. In particular, thanks to Sammy and Ali, who had the privilege of living with me for a year, and to Adam, for being a sounding board for all my ideas and being an excellent travelling companion to conferences.

Finally, this thesis wouldn't have been possible without the constant patience and encouragement of Ellie, whose eternal support gave me the confidence and determination to carry on when times were difficult.

CONTENTS

1

INTRODUCTION

Division algebras over the real numbers and over finite fields have been widely studied over the last century. For the former, it is well-known that the dimension of a real division algebra must be 1, 2, 4 or 8 [34, 41] and a rough classification of real division algebra according to the isomorphism type of their derivation algebras was given by Benkart and Osborn [3]. Despite progress made towards classifying real division algebras, the classification of finite dimensional division algebras over a fixed base field is still an open problem in algebra. A general solution to this problem would be a massive undertaking at this time. One way to make progress towards a solution is a brute force approach: we find new division algebras and determine their structure. A useful method yielding new division algebras is the modification of pre-existing constructions to obtain large families of division algebras. This forms part of the motivation for the research done in this thesis and is a common theme that appears throughout.

Alternatively, finite division algebras (also known as semifields) have been investigated via a geometric approach through exploiting the connection between semifields and projective planes [37], see the survey by Lavrauw and Polverino in 2011 for a list of 28 such families [38], and exhaustive computer searches have lead to the classification of semifields of some relatively small orders [15, 16]. In recent years, there has been an increased focus on division algebras over $\mathbb{Q}$ and $\mathbb{Q}_p$ due to their applications to space-time coding [18, 27, 50, 52].

Fundamentally, a general coding theory requires both a set equipped with a distance metric and a closed subset of codewords. The most common example of this is a set of vectors with entries in $\mathbb{F}_2$ and a distance function defined by the Hamming metric [28]; other examples of codes include Gabidulin codes [23], Reed-Solomon codes [53] and LDPC codes [24]. Gabidulin codes, also known as *rank metric codes*, are defined by a subset $\mathcal{C} \subset M_{n\times m}(\mathbb{F}_q)$ equipped with a rank distance function:

$$d(A, B) = \operatorname{rank}(A - B)$$

for all $A, B \in M_{n\times m}(\mathbb{F}_q)$. It is well known that

$$|\mathcal{C}| \leq q^{n(m-d_{\mathcal{C}}+1)},$$

where $d_{\mathcal{C}}$ is the minimum distance of the code; a rank metric code attaining this bound is a *maximum rank distance code*. MRD codes have been studied due to their applications in data transmission, such as in random linear network coding (e.g. see [57]). Moreover, finite semifields appear as special cases of MRD codes, contributing to an increased focus in the research of both these areas over recent years.

Recently, skew polynomials have been successfully used in new constructions of division algebras (in particular semifields) and linear codes [2, 4, 5, 22, 44, 47, 48], in particular of space-time block codes (STBCs) and maximum rank distance (MRD) codes [49, 55, 56].

In the first half of this thesis, we generalize the construction presented in [56], where it was only considered mostly using finite fields. We consider this more generally over arbitrary fields in order to obtain division algebras and generalized MRD codes of matrices with entries both in a non-commutative algebra and a field. Our codes can be seen as generalizations of the classical and generalized Gabidulin codes constructed in [23], resp., [55]. Rank distance codes with entries from a noncommutative algebra have (to the best of the author's knowledge) never been previously considered. In addition to this, we obtain a large family of division algebras which include generalisations of Albert's twisted fields (as studied in [46]).

Let D be a finite-dimensional division algebra over its center C, and σ an automorphism of D of finite order n modulo inner automorphisms, i.e. $\sigma^n = i_u$ for some inner automorphism $i_u(z) = uzu^{-1}$, $u \in \mathrm{Fix}(\sigma)$. Let $R = D[t;\sigma]$ (which includes the case that $D = K$ is a cyclic field extension). For suitably chosen monic irreducible $f \in R = D[t;\sigma]$ with a bound in $C(R)$, we construct

both division algebras and MRD codes.

We consider the set

$$A = \{d_0 + d_1 t + \cdots + d_{lm-1} t^{lm-1} + \nu\rho(d_0)t^{lm} \mid d_i \in D\} \subset D[t;\sigma].$$

When $l = 1$, this can yield division algebras. In particular, when $l = 1$ and $\nu = 0$ we obtain Petit algebras, denoted S_f (as first discussed in [44] and subsequently named after the author). In every case, we relate A to a set of matrices in $M_k(\mathrm{Nuc}_r(S_f))$ and further explore how the rank of the matrices relate to the polynomials used in the construction.

We first give an overview of some results regarding the norm of a skew polynomial and subsequently employ these results to determine sufficient conditions to obtain division algebras and MRD codes, both when D is a cyclic algebra and K a field. We then determine the nuclei of the algebras we construct (more generally, the idealisers of the code) via spread sets. We apply the result to a worked example when K is cyclic extension of degree $\deg(f)$; in particular, 4-dimensional real division algebras are given as a special case.

We conclude with a brief look at the construction using a differential polynomial; when $\nu = 0$, we always obtain division algebras and MRD codes using this construction. The division algebras constructed when $\nu = 0$ are generalisations of Petit algebras as studied in [8]. To the best of the author's knowledge, the MRD codes we obtain have not been described in this way before and may be entirely new.

In the second half of this thesis, we present a generalised Cayley-Dickson doubling process and obtain a strong result regarding when we obtain division algebras. We consider one particular case of this doubling process, which is when we take a doubling of a field. As a special case of this, we obtain Dickson's commutative semifields, which motivates a generalisation of Dickson's commutative construction using a central simple algebra. Dickson's commutative division algebras [20] have been widely studied over finite fields as they yield a large class of proper finite semifields of even dimension: For any choice of

$c \in K \setminus K^2$ and $\sigma \in \mathrm{Aut}_F(K)$ not equal to the identity, $K \oplus K$ equipped with the multiplication

$$(u, v)(x, y) = (ux + c\sigma(vy), uy + vx)$$

is a division algebra over F when F is a finite field. This construction was additionally investigated in two papers by Burmester where K is a cyclic field extension of degree n over a field of characteristic not 2 [9, 10], producing $2n$-dimensional unital algebras over F. Further, Dickson [20] and Burmester gave a necessary and sufficient condition for when the algebras constructed this way are division algebras.

We explore this doubling process using a central simple algebra D/F. As D is not commutative, we have multiple options for a possible generalisation of the multiplication given in Dickson's construction. Clearly, the unital F-algebras we obtain this way are no longer commutative. This way we can now construct large families of new division algebras of dimensions $2\dim_{\mathbf{Q}}(D)$ over $\mathbf{Q}$, which most importantly have non-trivial nuclei, which might be used in future space-time block coding. This construction has now been published in Communications in Algebra [59].

Knuth recognised that Dickson's commutative division algebras also appear as a special case of another family of semifields [36]: A subalgebra L of a division algebra S is called a *weak nucleus* if $x(yz) - (xy)z = 0$, whenever two of x, y, z lie in L. Semifields which are quadratic over a weak nucleus are split into two cases; Case I semifields contain Dickson's construction as the only commutative semifields of this type. Due to this, Case I semifields are also called *generalized Dickson semifields*. Their construction is as follows: given a finite field $K = GF(p^n)$ for some odd prime p, define a multiplication on $K \oplus K$ by

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

for some automorphisms α, β, σ of K not all the identity automorphism and $c \in K \setminus K^2$. This construction produces a proper semifield containing p^{2n}

elements. Further work on semifields quadratic over a weak nucleus was done in [14, 25].

We introduce a doubling process which generalizes Knuth's construction in [36]: for a central simple associative algebra D/F or finite field extension K/F, we define a multiplication on the F-vector space $D \oplus D$ (resp. $K \oplus K$) as

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

for some $c \in D^\times$ and $\sigma_i \in \mathrm{Aut}_F(D)$ for $i = 1, 2, 3, 4$ (resp. $c \in K^\times$ and $\sigma_i \in \mathrm{Aut}_F(K)$). This yields an algebra of dimension $2\dim_F(D)$ or $2[K : F]$ over F. Over finite fields, we show this construction is the same as the one presented in [36] and yields examples of some Hughes-Kleinfeld, Knuth and Sandler semifields (for example, see [17]). Hughes-Kleinfeld, Knuth and Sandler semifield constructions were studied over arbitrary base fields in [7]. The contents of this section has now appeared in Communications in Mathematics [60].

2

PRELIMINARY RESULTS AND DEFINITIONS

2.1 NONASSOCIATIVE DIVISION ALGEBRAS

In the following sections, we always let F be a field. We will define an F-algebra A as a finite dimensional F-vector space equipped with a (not necessarily associative) bilinear map $A \times A \to A$ which is the multiplication of the algebra. A is a *division algebra* if for all nonzero $a \in A$ the maps $L_a : A \to A$, $x \mapsto ax$, and $R_a : A \to A$, $x \mapsto xa$, are bijective maps. As A is finite dimensional, A is a division algebra if and only if there are no zero divisors [54]. Finite division algebras are also called *(finite) semifields* in the literature.

For all $x, y, z \in A$, the *associator of* x, y, z is given by

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

Define the left, middle and right nuclei respectively as

$$\mathrm{Nuc}_l(A) = \{a \in A \mid [a, y, z] = 0 \text{ for all } y, z \in A\},$$

$$\mathrm{Nuc}_m(A) = \{a \in A \mid [x, a, z] = 0 \text{ for all } x, z \in A\},$$

$$\mathrm{Nuc}_l(A) = \{a \in A \mid [x, y, a] = 0 \text{ for all } x, y \in A\}.$$

It is easily checked that these are all subalgebras of A. The intersection of the left, middle and right nuclei is called the *nucleus of* A and is denoted

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

For two algebras A and B, any isomorphism $f : A \to B$ maps $\mathrm{Nuc}(A)$ isomorphically onto $\mathrm{Nuc}(B)$. Similar, define the *commutator of* A as

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

The intersection of the nucleus and commutator of A yields the *center of* A and is denoted $Z(A)$. Every division ring is a division algebra over its center.

2.1.1 *Nondegenerate forms*

Let F have characteristic 0 or $\text{char}(d) > d$. A *d-linear form* over F is an F-multilinear map $\theta : A \times ... \times A \to F$ (d copies) such that $\theta(x_1, x_2, ..., x_d)$ is invariant under all permutations of its variables. Define a *form of degree d* over F as a map $N : A \to F$ such that $N(ax) = a^d N(x)$ for all $a \in F$, $x \in A$ and such that the map $\theta : A \times ... \times A \to F$ defined by

$$\theta(x_1, x_2, ..., x_d) = \frac{1}{d!} \sum_{1 \leq i_1 < ... < i_l \leq d} (-1)^{d-1} N(x_{i_1} + ... + x_{i_l})$$

$(1 \leq l \leq d)$ is a d-linear form over F.

A form $N : A \to F$ of degree d is called *multiplicative* if $N(xy) = N(x)N(y)$ for all $x, y \in A$ and *nondegenerate* if we have $N(x) = 0$ if and only if $x = 0$. Note that if $N : A \to F$ is a nondegenerate multiplicative form and A is a unital algebra, it follows that $N(1_A) = 1_F$. Every central simple algebra of degree d admits a uniquely determined nondegenerate multiplicative form of degree d, called the *norm* of the algebra [35].

2.1.2 *Isotopes*

Denote the set of algebra structures on an F-vector space V by $Alg(V)$. Given $A \in Alg(V)$, write xAy for the product of $x, y \in V$ in the algebra (if not clear from the context which multiplication is used).
For $f, g, h \in Gl(V)$ define the algebra $A^{(f,g,h)}$, called an *isotope* of A, as V with the multiplication

$$xA^{(f,g,h)}y = h(f(x)g(y)) \quad x, y \in V.$$

If $f = g$ and $h = f^{-1}$, then $A^{(f,g,h)}$ is isomorphic to A.

Remark 2.1.1. In general, properties such as a multiplicative identity or commutativity are not preserved under isotopy. For example, we could define a multiplication on $\mathbb{C}$ by

$$x * y = x\overline{y}$$

for all $x, y \in \mathbb{C}$, so $(\mathbb{C}, *) = \mathbb{C}^{(\mathrm{id},^-,\mathrm{id})}$. However unlike the complex numbers, $\mathbb{C}^{(\mathrm{id},^-,\mathrm{id})}$ is neither commutative nor unital.

2.2 MAXIMUM RANK DISTANCE CODES

Let K be a field. A rank-metric code is a set $\mathcal{C} \subset M_{n\times m}(K)$ equipped with a rank distance function

$$d(A, B) = \mathrm{rank}(A - B).$$

Define the *minimum distance* of $\mathcal{C}$ as

$$d_{\mathcal{C}} = \min\{d(A, B) \mid A, B \in \mathcal{C}, A \neq B\}.$$

For some subfield $L \subset K$, we say that $\mathcal{C}$ is L-linear if $A + B \in \mathcal{C}$ and $\lambda A \in \mathcal{C}$ for all $A, B \in \mathcal{C}$ and $\lambda \in L$.

Such a code must satisfy a Singleton-like bound: suppose $\mathcal{C}$ is L-linear, then

$$\dim_L(\mathcal{C}) \leq n(m - d_{\mathcal{C}} + 1)[K : L].$$

If K is a finite field, then this becomes

$$|\mathcal{C}| \leq |K|^{n(m-d_{\mathcal{C}}+1)}$$

(see [43, Theorem 2]). If $\mathcal{C}$ attains the Singleton-like bound, we say that $\mathcal{C}$ is a *maximum rank distance code* or an MRD-code. Over finite fields, MRD codes were found to exist over every finite field [19]; these codes were rediscovered by Gabidulin [23] independently. Due to this, they are often called *Gabidulin codes*. In this thesis, we only consider rank-metric codes constructed with square matrices; for ease of notation, the set of $n \times n$ matrices with entries in K is denoted $M_n(K)$.

More generally, we would like to define MRD codes with matrices in $M_n(B)$ for $B \subset \mathrm{Nuc}_r(A)$ a subalgebra of a finite-dimensional division algebra A, such that A is free of finite rank as a right B-module. If B is not a field, more care is needed to ensure the distance between elements is well defined.

Definition 2.2.1. Let $A \in M_n(B)$. The *column rank of a matrix* A is the dimension of the right B-module generated by the columns of A; similarly, define the row rank of A as the dimension of the right B-module generated by the rows of A.

When B is not a field, column rank and row rank do not always coincide. Using the definition of column rank, we can define the distance between the elements $X, Y \in \mathcal{C}$ as $d(X,Y) = \text{colrank}(X-Y)$ and a minimum distance of $\mathcal{C}$ as

$$d_{\mathcal{C}} = \min\{\text{colrank}(X-Y) \mid X, Y \in \mathcal{C}, X \neq Y\}.$$

Such a code must also satisfy a Singleton-like bound:

Theorem 2.2.2. *[43, Theorem 2 for finite fields] Let $\mathcal{C} \subset M_n(B)$ be a rank-distance code with minimum distance d. Then $dim_B(\mathcal{C}) \leq n(n-d+1)$.*

Proof. Delete $d-1$ columns from all codewords in $\mathcal{C}$. Then all codewords in $\mathcal{C}$ are distinct: suppose $A, B \in \mathcal{C}$ are such that they are equal when $d-1$ columns are deleted. Then A and B only differ by at most $d-1$ columns, so $\text{colrank}(A-B) \leq d-1 < d$. This contradicts the minimum distance of $\mathcal{C}$. Hence the deletion of $d-1$ columns does not change the size of $\mathcal{C}$.
As this image of $\mathcal{C}$ lies in $M_{n\times(n-d+1)}(B)$, it follows that

$$\dim_B(\mathcal{C}) \leq n(n-d+1.)$$

□

If $\mathcal{C}$ attains this bound, we can rewrite this Singleton-like bound to determine that any MRD-code has minimum distance

$$d_{\mathcal{C}} = n - \frac{1}{n}\dim_B(\mathcal{C}) + 1.$$

We can now define our generalisation of maximum rank distance codes.

Definition 2.2.3. Let $\mathcal{C} \subset M_n(B)$ be an additively closed subset, where $B \subset \text{Nuc}_r(A)$ a subalgebra of a finite-dimensional division algebra A, such that A is free of finite rank as a right B-module. Define the distance between elements

$X, Y \in \mathcal{C}$ as $d(X,Y) = \text{colrank}(X-Y)$ and let $d_{\mathcal{C}}$ be the minimum distance of $\mathcal{C}$. If

$$d_{\mathcal{C}} = n - \frac{1}{n}\dim_B(\mathcal{C}) + 1,$$

then $\mathcal{C}$ is a *(generalised) MRD code*.

Note that this new definition contains the traditional MRD codes as the special case when B is a field. In this thesis, when we refer to MRD codes we refer to this more general definition.

2.2.1 *Constructing codes from division algebras*

Let F be a field and A an F-algebra. For all $a \in A$, the left multiplication $L_a : A \to A$, $x \to ax$, is an F-linear map and the set $\{L_a \,|\, a \in A\}$ is an F-vector subspace of the associative algebra $\text{End}_F(A)$. Consider

$$L : A \to \text{End}_F(A), a \mapsto L_a.$$

If A is a finite-dimensional division algebra then L is injective: $L_a = L_b$ implies $ax = bx$ for all $x \in A$, hence $(a-b)x = 0$ for all x which yields $a = b$. After a choice of an F-basis for A, we can embed $\text{End}_F(A)$ into the algebra $\text{Mat}_n(F)$. This way we get an embedding $\lambda : A \to M_n(F), a \mapsto L_a \mapsto M_a$ of vector spaces, where M_a is the matrix representing L_a.

(Contrary to the situation for associative division algebras, this only embeds the vector space A into the vector space $M_n(F)$, the algebra structure of A is disregarded here, so this is not a left regular representation.)

Since A is a finite-dimensional division algebra, all non-zero elements of A are invertible, hence all L_a with $a \neq 0$ are bijective and so all non-zero matrices in $\lambda(A)$ have non-zero determinant. If we use the set $\lambda(A)$ to define a space-time block code (STBC), then the difference of two distinct elements of $\lambda(A)$ will also lie in $\lambda(A)$, hence have non-zero determinant. The linear codebook $\lambda(A)$ is thus *fully diverse*, because the rank of the difference of two distinct codewords is maximal.

Borrowing the terminology of semifields, on the other hand, the *spread set* of a finite-dimensional division algebra A over F of dimension n is also defined as the set

$$\mathcal{C} = \mathcal{C}(A) = \lambda(A) = \{L_a : a \in A\} \subseteq \mathrm{End}_F(A).$$

For all $0 \neq a \in A$, L_a is a bijective endomorphism, since A is a division algebra. Moreover, $\mathcal{C}$ is a F-subvector space of $\mathrm{End}_F(A)$. Given an F-basis of A, each L_a can be represented by a matrix $M_a \in M_n(F)$ computed with respect to that basis, so that we obtain the *matrix spread set* of A,

$$\mathcal{C} = \mathcal{C}(A) = \{M_a : a \in A\} \subseteq M_n(F)$$

of invertible matrices, where the difference of any two elements in it will again be an invertible matrix, hence of maximum rank. This yields a linear MRD code in $M_n(F)$.

This idea is not new: For space-time block coding, usually finite-dimensional associative division algebras are considered as a vector space over some subalgebra B (usually a subfield K) of an associative algebra A. Given a finite-dimensional nonassociative F-algebra A with a subalgebra B, this is not always possible, and we will need the following additional assumptions: Let B be a subalgebra of A.

We need A to be a right B-module, i.e. we need

$$x(cd) = (xc)d \text{ for all } x \in A, c, d \in B.$$

This is satisfied if $B \subset \mathrm{Nuc}_r(A)$. We also need A to be a right B-module of finite rank.

Moreover, we need that $L_a \in \mathrm{End}_B(A)$. Now $L_a \in \mathrm{End}_B(A)$ is the same as $L_a(x\alpha) = L_a(x)\alpha$ for all $\alpha \in B$, $a, x \in A$, that means we need $a(x\alpha) = (ax)\alpha$ for all $\alpha \in B$, $a, x \in A$. This is satisfied if $B \subset \mathrm{Nuc}_r(A)$. Then

$$L : A \to \mathrm{End}_B(A), a \mapsto L_a$$

is a well-defined F-linear map.

So assume that $B = \mathrm{Nuc}_r(A)$ and consider A as a right B-module. It is free of rank k. After a choice of a B-basis for A, we can embed the right B-module $\mathrm{End}_B(A)$ into the module $M_r(B)$. Thus we get a well-defined embedding

$$\lambda : A \to M_r(B), a \mapsto L_a \mapsto M_a$$

of F-vector spaces. Obviously, we have $X \pm Y \in \lambda(A)$ for all $X, Y \in \lambda(A)$. Thus we have constructed a linear codebook/ matrix spread set. Its elements correspond to invertible endomorphisms.

2.2.2 *Example*

(cf. [50])

Let L/F_0 be a cyclic Galois field extension of degree n with $\mathrm{Gal}(L/F_0) = \langle\sigma\rangle$, and F/F_0 be a cyclic Galois field extension of degree m with $\mathrm{Gal}(F/F_0) = \langle\tau\rangle$. Let L and F be linearly disjoint over F_0 and let $K = L \otimes_{F_0} F = L \cdot F$ be the composite of L and F over F_0, with Galois group $\mathrm{Gal}(K/F_0) = \langle\sigma\rangle \times \langle\tau\rangle$, where σ and τ are canonically extended to K.

In the following, let $(L/F_0, \sigma, c)$ and $(F/F_0, \tau, d)$ be two cyclic algebras over F_0, i.e. $c \in L^\times$ and $d \in F^\times$. Suppose that $D = (L/F_0, \sigma, c) \otimes_{F_0} F = (K/F, \sigma, c)$ is an associative cyclic division algebra of degree d.

For $x = x_0 + ex_1 + e^2x_2 + \cdots + e^{d-1}x_{d-1} \in D$ ($x_i \in K$, $1 \leq i \leq d$), and $\tau \in \mathrm{Aut}(K)$, $L = \mathrm{Fix}(\tau)$, define the L-linear map $\widetilde{\tau} : D \to D$ via

$$\widetilde{\tau}(x) = \tau(x_0) + e\tau(x_1) + e^2\tau(x_2) + \cdots + e^{d-1}\tau(x_{d-1}).$$

If $c \in L$ then

$$\widetilde{\tau}(xy) = \widetilde{\tau}(x)\widetilde{\tau}(y) \text{ and } \lambda(\widetilde{\tau}(x)) = \tau(\lambda(x))$$

for all $x, y \in D$, where for any matrix $X = \lambda(x)$ representing left multiplication with x, $\tau(X)$ means applying τ to each entry of the matrix.

Then for $f(t) = t^m - d \in R = D[t; \widetilde{\tau}^{-1}]$,

$$S_f \cong (L/F_0, \sigma, c) \otimes_{F_0} (F/F_0, \tau, d).$$

S_f is an associative algebra if and only if $d \in F_0^\times$ and $c \in F_0^\times$. K is a subfield of S_f of degree mn over F_0 and $K = L \otimes_{F_0} F \subset \mathrm{Nuc}(S_f)$.

Let $\{1, e, e^2, \ldots, e^{n-1}\}$ be the standard basis of the L-vector space D_0 and $\{1, f, f^2, \ldots, f^{m-1}\}$ be the standard basis of the F-vector space D_1. S_f is a K-vector space with basis

$$\{1 \otimes 1, e \otimes 1, \ldots, e^{n-1} \otimes 1, 1 \otimes f, e \otimes f, \ldots, e^{n-1} \otimes f^{m-1}\}.$$

Identify

$$S_f = K \oplus eK \oplus \cdots \oplus e^{n-1}K \oplus fK \oplus efK \oplus \cdots \oplus e^{n-1}f^{m-1}K.$$

An element in $\lambda(S_f)$ has the form

$$\begin{bmatrix} Y_0 & d\tau(Y_{n-1}) & d\tau^2(Y_{n-2}) & \ldots & d\tau^{m-1}(Y_1) \\ Y_1 & \tau(Y_0) & d\tau^2(Y_{n-1}) & \ldots & d\tau^{m-1}(Y_2) \\ \vdots & & \vdots & & \vdots \\ Y_{n-2} & \tau(Y_{n-3}) & \tau^2(Y_{n-4}) & \ldots & d\tau^{m-1}(Y_{n-1}) \\ Y_{n-1} & \tau(Y_{n-2}) & \tau^2(Y_{n-3}) & \ldots & \tau^{m-1}(Y_0) \end{bmatrix} \tag{1}$$

with $\lambda(d) \in \lambda(D)$, $Y_i \in \lambda(D)$. That means, $Y_i \in \mathrm{Mat}_n(K)$, and when the entries in Y_i are restricted to elements in L, $Y_i \in \lambda((L/F_0, \sigma, c))$ (multiplication with d in the upper right triangle of the matrix means simply scalar multiplication with d). If f is irreducible, the set $\lambda(S_f)$ is a linear MRD code of invertible matrices in $M_{mn}(K)$. It is clearly linear by construction. Since all matrices are invertible, it has minimum rank distance n (and is a fully diverse STBC).

When is f irreducible? For this we have the following result:

Theorem 2.2.4. *[50] Let $(F/F_0, \tau, d)$ be a nonassociative cyclic algebra of degree m. Let $D_0 = (L/F_0, \sigma, c)$ be an associative cyclic algebra over F_0 of degree n, such that $D = D_0 \otimes_{F_0} F = (K/F, \sigma, c)$ is a division algebra.*

Assume m is prime and in case $m \neq 2, 3$, additionally that F_0 contains a primitive mth root of unity. Then

$$(L/F_0, \sigma, c) \otimes_{F_0} (F/F_0, \tau, d)$$

is a division algebra if and only if

$$d \neq z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{m-1}(z)$$

for all $z \in D$.

3

A CONSTRUCTION OF NEW DIVISION ALGEBRAS AND MRD-CODES EMPLOYING SKEW POLYNOMIAL RINGS

3.1 SKEW POLYNOMIAL RINGS

3.1.1 *Definitions*

Let D be an associative division ring with centre C and σ be an automorphism of D of finite order n modulo inner automorphisms and δ a σ-derivation. We recall some definitions:

Definition 3.1.1. An automorphism $\sigma \in \mathrm{Aut}(D)$ has *finite order modulo inner automorphisms* if there exists some $n \in \mathbb{N}$ and $u \in D^\times$ such that $\sigma^n(x) = uxu^{-1}$ for all $x \in D$. Without loss of generality, we may assume that $u \in \mathrm{Fix}(\sigma)$.

When $D = C$ (in other words, when D is a field), there are no non-identity inner automorphisms so this definition collapses to considering automorphisms with finite order.

Definition 3.1.2. Let $\sigma \in \mathrm{Aut}(D)$. Then $\delta : D \to D$ is a *σ-derivation* if $\delta(xy) = \delta(x)y + \sigma(x)\delta(y)$ for all $x, y \in D$. If σ is the identity automorphism, we see tat this is the standard definition of a derivation of D.

The *skew polynomial ring* $R = D[t; \sigma; \delta]$ is the set of polynomials

$$a_0 + a_1 t + \cdots + a_s t^s + \ldots$$

with $a_i \in D$, where addition is defined term-wise and multiplication by

$$ta = \sigma(a)t + \delta(a)$$

for all $a \in D$. For $f = a_0 + a_1 t + \cdots + a_s t^s$ with $a_n \neq 0$ define $\deg(f) = s$ and put $\deg(0) = -\infty$. Then $\deg(fg) = \deg(f) + \deg(g)$. If $\delta = 0$, we refer to this algebra as a *twisted polynomial rings*; alternatively, if $\sigma = id$, we call this a *differential polynomial ring*. When it is clear from the context, we will simply denote these algebras as $D[t; \sigma]$ and $D[t; \delta]$ respectively.

An element $f \in R$ is *irreducible* in R if it is not a unit and it has no proper factors, i.e if there do not exist $g, h \in R$ with $\deg(g), \deg(h) < \deg(f)$ such that $f = gh$.

R is a left and right principal ideal domain and there is a right division algorithm in R: for all $g, f \in R$, $g \neq 0$, there exist unique $r, q \in R$ with $\deg(r) < \deg(f)$, such that $g = qf + r$ [33, p. 3 and Prop. 1.1.14]. This makes R a right Euclidean domain. The terminology used here is the one used by Petit [44] and Lavrauw and Sheekey [39]; it is different from Jacobson's, who calls this a left division algorithm.

Unlike standard polynomial rings, it is clear that R is non-commutative; in fact, R is commutative if and only if $\sigma = id$ and $\delta = 0$. Let $R = D[t; \sigma]$ and define $F = C \cap \mathrm{Fix}(\sigma)$. Then R has center

$$Z(R) = F[u^{-1}t^n] = \{\sum_{i=0}^{k} a_i (u^{-1}t^n)^i \mid a_i \in F\} \cong F[x]$$

[33, Theorem 1.1.22].

Similarly, let $R = D[t; \delta]$ where C is a field of characteristic p (we allow $D = C$).

Definition 3.1.3. Let δ be a derivation of D. Then the subring of D fixed by δ is denoted $\mathrm{Const}(\delta) = \{c \in D \mid \delta(c) = 0\}$. Additionally, we call δ an *inner derivation* if there exists some $a \in D$ such that $\delta(x) = ax - xa$ for all $x \in D$; in this case, δ is denoted id_a.

Suppose δ is a derivation of D, such that $\delta|_C$ is algebraic with minimum polynomial

$$g(t) = t^{p^e} + c_1 t^{p^{e-1}} + \cdots + c_e t \in F[t]$$

of degree p^e, where $F = \mathrm{Const}(\delta) \cap C$. Then $g(\delta) = id_{d_0}$ is an inner derivation of D (specifically, $id_{d_0}(x) = d_0 x - x d_0$ for all $x \in D$). W.l.o.g. we choose $d_0 \in \mathrm{Const}(\delta)$, so that $\delta(d_0) = 0$ [33, Lemma 1.5.3]. Then R has center

$$Z(R) = F[x] = \{\sum_{i=0}^{k} a_i (g(t) - d_0)^i \mid a_i \in F\}$$

with $x = g(t) - d_0$. The two-sided $f \in D[t;\delta]$ are of the form $f(t) = uc(t)$ with $u \in D$ and $c(t) \in Z(R)$ [33, Theorem 1.1.32].

3.1.2 *Petit algebras*

Let $f \in R = D[t;\sigma;\delta]$ of degree m and $\mathrm{mod}_r f$ denote the remainder of right division by f. There is a canonical map between skew polynomials of degree less than m and the elements of the right R-module $R/Rf = D[t;\sigma;\delta]/D[t;\sigma;\delta]f$. Moreover,

$$R_m = \{g \in D[t;\sigma;\delta] \,|\, \deg(g) < m\}$$

together with the usual addition and the multiplication

$$g \circ h = \begin{cases} gh \text{ if } \deg(g) + \deg(h) < m, \\ gh \bmod_r f \text{ if } \deg(g) + \deg(h) \geq m, \end{cases}$$

is a unital nonassociative ring denoted S_f. We will usually drop the $\circ$ notation and simply use juxtaposition for multiplication in S_f. These algebras were first introduced by Petit [44] and as such are called *Petit algebras*. We review some of the properties of these algebras:

Theorem 3.1.4. *[44, 58]*

1. *If S_f is not associative, then*

$$\mathrm{Nuc}_l(S_f) = \mathrm{Nuc}_m(S_f) = D,$$

   and

$$\mathrm{Nuc}_r(S_f) = \{g \in R \,|\, \deg(g) < m \text{ and } fg \in Rf\}.$$

2. *S_f is associative if and only if f is right invariant; that is, Rf is a two-sided ideal of R.*

3. $\mathrm{Comm}(S_f) = \{\sum_{i=0}^{m-1} c_i t^i \,|\, \forall i, c_i \in \mathrm{Fix}(\sigma) \text{ and } dc_i = c_i\sigma^i(d) \text{ for all } d \in D\}$.

As a result of this, the right nucleus of S_f is precisely equal to the *eigenring* of f.

3.2 THE RIGHT NUCLEUS OF PETIT ALGEBRAS

3.2.1 *The right nucleus for irreducible $f \in D[t;\sigma]$*

Unless stated otherwise, let D be an associative division algebra with center C (we allow $D = C$ so the following section also applies to $K[t;\sigma]$ where K is a field). Let σ be an automorphism of D of finite order n modulo inner automorphisms, such that $\sigma^n = i_u$ for some inner automorphism $i_u(z) = uzu^{-1}$. Recall that we may choose $u \in \mathrm{Fix}(\sigma)$ without loss of generality. We also assume that n is the order of $\sigma|_C$. Define $R = D[t;\sigma]$ and $F = C \cap \mathrm{Fix}(\sigma)$; as $\sigma|_C$ has order n, it follows that $[C : F] = n$.

Definition 3.2.1. A polynomial $f(t) \in R$ is *bounded* if there exists a nonzero polynomial $f^* \in R$ such that Rf^* is the largest two-sided ideal of R contained in Rf. The polynomial f^* is uniquely determined by f up to scalar multiplication by nonzero elements of D and is called the *bound* of f.

In our case, every $f \in R$ is bounded as D is a finite dimension central simple algebra over C and σ has finite order modulo inner automorphisms [12, Theorem 4].

Definition 3.2.2. Let $f, g \in R$. The *greatest common right divisor* of f and g is denoted by $(f,g)_r$ and defined as $Rf + Rg = R.(f,g)_r$ (for example, see [26, p.3]).

If $(f,t)_r = 1$, then the bound lies in the centre of R [26, Lemma 2.11].

3.2.2 *The minimal central left multiple of $f \in D[t;\sigma]$*

Definition 3.2.3. For any bounded $f \in R = D[t;\sigma]$ with a bound in $Z(R)$, we define the *minimal central left multiple of f in R* to be the unique polynomial of

minimal degree $h = mzlm(f) \in Z(R) = F[u^{-1}t^n]$ such that $h(t) = \hat{h}(u^{-1}t^n)$ for some monic $\hat{h}(x) \in F[x]$ and such that $h = gf$ for some $g \in R$.

It seems clear from the above definition that the minimal central left multiple is also a bound of f. We check that the above definition makes sense and our claim about uniqueness is true:

Lemma 3.2.4. *Let $f \in R = D[t;\sigma]$ be bounded. If $(f,t)_r = 1$, then the minimal central left multiple exists and is unique. Additionally, the bound is equal to the minimal central left multiple up to a scalar multiple from D.*

Proof. Let f^* be a bound of f. By definition, f^* is unique up to scalar multiplication by elements in $D^\times$ and Rf^* is the (unique) largest two-sided ideal of R contained in the left ideal Rf. The assumption that $(f,t)_r = 1$ implies that $f^* \in Z(R)$ [26, Lemma 2.11]) thus f^* is the unique minimal central left multiple of f up to some scalar. □

From now on we assume that $(f,t)_r = 1$ and that f is bounded. Note that $(f,t)_r = 1$ is equivalent to f having a non-zero constant term. If f is irreducible and monic, we can relate the assumption that $(f,t)_r = 1$ to the minimal central left multiple of f:

Lemma 3.2.5. *For irreducible monic $f \in R$, the following statements are equivalent:*
(i) $(f,t)_r = 1$,
(ii) $f(t) \neq t$,
(iii) if $h(t) = \hat{h}(u^{-1}t^n)$ denotes the minimal central left multiple of f, then $\hat{h}(x) \neq x$.

Proof. (i) $\iff$ (ii): If $(f,t)_r \neq 1$, then f has non-zero constant term. If $\deg(f) \geq 2$, we can express $f = f't$ for some f' of degree at least one; this contradicts the irreducibility of f. Thus $\deg(f) = 1$ and thus $f = at$ for some $a \in D$. As f is monic, it follows that $f(t) = t$. The reverse direction is trivial. (ii) $\iff$ (iii): If $f(t) = t$, then $\hat{h}(u^{-1}t^n) = u^{-1}t^n$ is a central left multiple of f as $h(t) = (u^{-1}t^{n-1})t$. Further, $\deg(\hat{h}(x)) = 1$ so this must be the minimal

central left multiple of f. Conversely, suppose $h(u^{-1}t^n) = u^{-1}t^n$ is the minimal central multiple of some irreducible $f \in R$. If $n = 1$ and $\hat{h}(u^{-1}t^n) = u^{-1}t$ then it is clear that $f(t) = t$. So we assume $n > 1$. Then there exists some $g \in R$ such that

$$u^{-1}t^n = gf.$$

Comparing constant terms, we have $g_0 f_0 = 0$ where g_0 and f_0 are the constant terms of g and f respectively.

Suppose $f_0 \neq 0$. Then as D is a division algebra, we have $g_0 = 0$. In general, the coefficient of t^k is

$$\sum_{i+j=k} g_i \sigma^i(f_j).$$

Comparing coefficients to t^n, for all $k < n$ this sum must equal zero.

For $k = 1$, we have

$$\sum_{i+j=1} g_i \sigma^i(f_j) = g_1\sigma(f_0) + g_0 f_1 = 0.$$

As $g_0 = 0$ and $f_0 \neq 0$, this implies $g_1 = 0$. Inductively, suppose $g_k = g_{k-1} = ... = g_0 = 0$ for $k < n - 1$. Then

$$\sum_{i+j=k+1} g_i \sigma^i(f_j) = g_{k+1}\sigma^{k+1}(f_0) = 0 \implies g_{k+1} = 0.$$

Thus we conclude $g = g_n t^n$ for some $g_n \in D$, yielding $u^{-1}t^n = g_n t^n f$. Comparing degrees, it follows that $\deg(f) = 0$ which is a contradiction. So we must have $f_0 = 0$. As f is irreducible and monic, it follows that $f(t) = t$ as claimed. □

Proposition 3.2.6. *If f is irreducible and bounded in R, and $(f, t)_r = 1$, with minimal central left multiple $h(t) = \hat{h}(u^{-1}t^n)$. Then $\hat{h}(x)$ is irreducible in $F[x]$.*

Proof. By Lemma 3.2.4, the minimal central left multiple of f exists, so let $h = \hat{h}(u^{-1}t^n)$ be the minimal central left multiple of f. Suppose $\hat{h}$ is reducible in $F[u^{-1}t^n]$; that is, $h = h_1 h_2$ for some $h_i = \hat{h_i}(u^{-1}t^n) \in F[u^{-1}t^n]$, such that $0 < \deg(h_i) < \deg(h)$ for $i = 1, 2$. If f divides h_1 on the right, this contradicts the minimality of h. Moreover, as f is irreducible we conclude the greatest

common right divisor of f and h_1 is 1. As R is a right Euclidean domain, there exist $p, q \in R$ such that

$$pf + qh_1 = 1.$$

Multiplying everything by h_2, we obtain $pfh_2 + qh = h_2$. As f is a right divisor of h by definition, $h = rf$ for some $r \in R$. Noting that $h_2 = \hat{h_2}(u^{-1}t^n)$ lies in $Z(R)$, this yields

$$h_2 = ph_2f + qrf = (ph_2 + qr)f.$$

This implies that h_2 is a central left multiple of f of degree strictly less than h; this also contradicts the minimality of h. Thus we conclude that $\hat{h}(x)$ must be irreducible in $F[x]$. □

We say that two polynomials $f, g \in R$ are *similar* if $R/Rf \cong R/Rg$ as right R-modules. Employing a result from [11], we can relate similar irreducible polynomials to their minimal central left multiples:

Corollary 3.2.7. *Let f, g be bounded and irreducible in R such that $(f, t)_r = 1$ and $(g, t)_r = 1$. Then $mzlm(f) = mzlm(g)$ if and only if f, g are similar.*

Proof. If f is bounded and irreducible, all elements similar to f admit the same bound f^* [11, Corollary 2, p.9]. So the bound of g is f^*. Thus by Lemma 3.2.4, $mzlm(g) = f^* = mzlm(f)$. Conversely, suppose $mzlm(f) = mzlm(g)$. Then g is an irreducible divisor of $mzlm(f)$. As all irreducible factors of $mzlm(f)$ are similar, it follows that g is similar to f. □

In this section, we recall some results by Owen and Pumplün [42]:

Lemma 3.2.8. *Suppose that $h \in R$ is such that $h = \hat{h}(u^{-1}t^n)$ for some monic $\hat{h} \in F[x]$ with either $\hat{h}(x) = x$, or such that h has nonzero constant term. Then the quotient algebra R/Rh has center*

$$Z(R/Rh) \cong F[x]/(\hat{h}(x)).$$

Define $E_{\hat{h}} = F[x]/(\hat{h}(x))$. This is a commutative algebra over F of dimension $deg(\hat{h})$. If $\hat{h}$ is irreducible in $F[x]$, then $E_{\hat{h}}$ is a field extension of F of degree $deg(\hat{h})$.

Lemma 3.2.9. *Suppose that $h \in R$ is such that $h = \hat{h}(u^{-1}t^n)$ for some $\hat{h} \in F[x]$, $\hat{h}(x) \neq x$, and such that $\hat{h}$ is irreducible in $F[x]$. Then h generates a maximal two-sided ideal Rh in R.*

Proof. This is mentioned in [33, p. 16], we include a proof for the sake of the reader. Assume that there exists some $g \in R$, such that Rg is a two-sided ideal of R with $Rh \subsetneqq Rg$. Assume without loss of generality that $\deg(g) < \deg(h)$ (otherwise simply reduce g modulo h and use the ideal generated by $g \bmod_r h$ instead). Now $g(t) = \hat{g}(u^{-1}t^n)t^s$ for some $\hat{g} \in Z(R) \cong F[x]$, and some non-negative integer s, e.g. [44] or [33]. Since $Rh \subsetneqq Rg$, we have $h = ag$ for some $a \in R$. Moreover, $\hat{h}$ has nonzero constant term, so that t does not divide h, and so $s = 0$. Furthermore, since h and g lie in the center of R, a also lies in the center of R, i.e. there exists $\hat{a} \in Z(R) = F[u^{-1}t^n]$ such that $a = \hat{a}(u^{-1}t^n)$. It follows that $\hat{h}(x) = \hat{a}(x)\hat{g}(x)$. By assumption, $\hat{h}$ is irreducible in $F[x]$, and $Rg \neq Rh$. This forces $\hat{g} \in F$, i.e. $g \in F$. Hence $Rg = R$ and Rh is a maximal two-sided ideal of R. □

As h is the product of polynomials similar to f, intuition suggests a relation between R/Rh and the Petit algebra $S_f = R/Rf$:

Theorem 3.2.10. *[42] Let $f \in R = D[t;\sigma]$ be monic and irreducible of degree m such that $f(t) \neq t$, and let $h = \hat{h}(u^{-1}t^n)$ be its minimal central left multiple. Then $\mathrm{Nuc}_r(S_f)$ is a associative division algebra over $E_{\hat{h}} = F[x]/(\hat{h}(x))$ of degree $s = dn/k$, where k is the number of irreducible factors of h in R, and*

$$R/Rh \cong M_k(\mathrm{Nuc}_r(S_f)).$$

In particular, this means that $\deg(\hat{h}) = \frac{dm}{s}$ and $\deg(h) = km = \frac{dnm}{s}$, and

$$[\mathrm{Nuc}_r(S_f) : F] = s^2 \cdot \frac{dm}{s} = dms.$$

Moreover, s divides $gcd(dm, dn)$. If f is not right invariant, then $k > 1$ and $s \neq dn$.

We know that $[S_f : F] = [S_f : C][C : F] = d^2m \cdot n$. Since $\mathrm{Nuc}_r(S_f)$ is a subalgebra of S_f, comparing dimensions we obtain that

$$d^2mn = [S_f : F] = [S_f : \mathrm{Nuc}_r(S_f)] \cdot [\mathrm{Nuc}_r(S_f) : F] = k \cdot dms,$$

that is $[S_f : \mathrm{Nuc}_r(S_f)] = k$. If f is not right-invariant, then $k > 1$ and so we derive $s \neq dn$ looking at the degree of h.

Note that $\deg(h) = dnm$ is the largest possible degree of h.

Theorem 3.2.11. *[42] Let $f \in R = D[t;\sigma]$ be monic and irreducible of degree m such that $f(t) \neq t$. Let $h = \hat{h}(u^{-1}t^n)$ be its minimal central left multiple. Suppose that $gcd(m,n) = 1$. Then s divides d, and f is not right invariant unless $n = 1$. If d is prime then one of the following holds:*
(i) $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$, $dn = k$, $\deg(\hat{h}) = dm$ *and* $\deg(h) = dnm$. *In particular, then* $[\mathrm{Nuc}_r(S_f) : F] = dm$.
(ii) $\mathrm{Nuc}_r(S_f)$ *is a associative division algebra over* $E_{\hat{h}}$ *of degree* d, n *is the number of irreducible factors of* h *in* R, $\deg(h) = nm$, $\deg(\hat{h}) = m$ *and* $[\mathrm{Nuc}_r(S_f) : F] = d^2m$.

Theorem 3.2.12. *[42] Let $f \in R = D[t;\sigma]$ be monic and irreducible of degree m such that $f(t) \neq t$. Let $h = \hat{h}(u^{-1}t^n)$ be its minimal central left multiple. Suppose that $gcd(d,n) = 1$ and that f is not right invariant. Then $s = 1$, or $s \neq 1$ and s divides either d or n. Suppose additionally that d and n are prime. Then one of the following holds:*
(i) $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$, $dn = k$, $\deg(\hat{h}) = dm$ *and* $\deg(h) = dnm$. *In particular, then* $[\mathrm{Nuc}_r(S_f) : F] = dm$.
(ii) $\mathrm{Nuc}_r(S_f)$ *is a associative division algebra over* $E_{\hat{h}}$ *of degree* d, n *is the number of irreducible factors of* h *in* R, $\deg(h) = nm$, $\deg(\hat{h}) = m$ *and*

$$R/Rh \cong M_n(\mathrm{Nuc}_r(S_f)).$$

In particular, then $[\mathrm{Nuc}_r(S_f) : F] = d^2m$.
(iii) $\mathrm{Nuc}_r(S_f)$ *is a associative division algebra over* $E_{\hat{h}}$ *of degree* n, d *is the number of irreducible factors of* h *in* R, $\deg(\hat{h}) = dm/n$, $\deg(h) = dm$, *and* $[\mathrm{Nuc}_r(S_f) : F] = n^2/dm$.
Note that case (iii) cannot happen if n does not divide dm or if dm does not divide n^2.

Corollary 3.2.13. *[42] Suppose that $n = 1$, i.e. that σ is an inner automorphism of D, and that d is prime. Let $f \in R = D[t;\sigma]$ be monic and irreducible of*

degree m, $f(t) \neq t$, and let $h = \hat{h}(u^{-1}t)$ be its minimal central left multiple. Suppose that f is not right invariant. Then

$$\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}} = F[x]/(\hat{h}(x))$$

is a field extension of degree dm.

If $R = K[t;\sigma]$ for some finite field extension K/F, we obtain analogous results by setting $d = 1$.

3.2.3 *The minimal central left multiple of $f \in D[t;\delta]$*

Let $R = D[t;\delta]$ where C is a field of characteristic p (allowing $D = C$) and define $F = \mathrm{Const}(\delta) \cap C$. Let δ be a derivation of D such that $\delta|_C$ is algebraic with minimum polynomial

$$g(t) = t^{p^e} + c_1 t^{p^{e-1}} + \cdots + c_e t \in F[t],$$

so $g(\delta) = id_{d_0}$ is an inner derivation of D.

Similarly to Section 3.2.1, for every $f \in R = D[t;\delta]$ we define the *minimal central left multiple of f in R* to be the unique polynomial of minimal degree $h \in Z(R) \cong F[x]$ such that $h = gf$ for some $g \in R$, and such that $h(t) = \hat{h}(g(t) - d_0)$ for some monic $\hat{h}(x) \in F[x]$. As all polynomials in $D[t;\delta]$ are bounded, every $f \in R = D[t;\delta]$ has a unique minimal central left multiple: let f^* be a bound of f. Then Rf^* is the (unique) largest two-sided ideal of R contained in the left ideal Rf and $f^* \in Z(R)$ up to some invertible element in D. Thus f^* is the unique minimal central left multiple of f up to some scalar.

Proposition 3.2.14. *If f is irreducible in R with minimal central left multiple $h(t) = \hat{h}(g(t) - d_0)$, then $\hat{h}(x)$ is irreducible in $F[x]$.*

The proof is identical to the one of Proposition 3.2.6

Lemma 3.2.15. *[33, p. 16] Suppose that $h \in R$ is such that $h = \hat{h}(g(t) - d_0)$ for some $\hat{h} \in F[x]$, and such that $\hat{h}$ is irreducible in $F[x]$. Then h generates a maximal two-sided ideal Rh in R.*

Proposition 3.2.16. *[32, Proposition 4] Let* $h(t) = \hat{h}(g(t) - d_0) \in Z(R)$. *Then*

$$Z(R/Rh) \cong F[x]/F[x]\hat{h}(x).$$

Note that $\deg(h) = p^e \deg(\hat{h})$. We define $E_{\hat{h}} = F[x]/F[x]\hat{h}(x)$.

Let $f \in R = D[t;\delta]$ be a monic and irreducible polynomial of degree $m > 1$ and let $h(t) = \hat{h}(g(t) - d_0)$ be its minimal central left multiple.

Theorem 3.2.17. $\mathrm{Nuc}_r(S_f)$ *is a associative division algebra over* $E_{\hat{h}} = Z(R/Rh)$ *of degree* $s = dp^e/k$, *where* k *is the number of irreducible factors of* h *in* R, *and*

$$R/Rh \cong M_k(\mathrm{Nuc}_r(S_f)).$$

In particular, this means that $\deg(\hat{h}) = \frac{dm}{s}$ *and* $\deg(h) = km = \frac{dp^e m}{s}$, *and*

$$[\mathrm{Nuc}_r(S_f) : F] = s^2 \cdot \frac{dm}{s} = dms.$$

Moreover, s *divides* $gcd(dm, dp^e)$. *If* f *is not right invariant, then* $k > 1$ *and* $s \neq dp^e$.

Proof. Since f is bounded it has a minimal central left multiple h, S_f is free of finite rank as $\mathrm{Nuc}_r(S_f)$-module and the dimension of S_f over F is md^2p^e.

We have $h = gf$ for some $g \in R$ by the definition of h. Since R is a principal ideal domain, the irreducible factors h_i of any factorization $h = h_1 h_2 \cdots h_k$ of h into irreducible polynomials are all similar as polynomials. In particular, this means all irreducible factors of h have the same degree.

The minimal central left multiple h of an irreducible $f \in R$ is a two-sided maximal element in R in the terminology of [33]. Therefore R/Rh is a simple Artinian ring with $R/Rh \cong M_k(D_h)$, where $D_h \cong I(h_i)/Rh_i$ and $I(h_i) = \{g \in R : h_i g \in Rh_i\}$ is the idealiser of Rh_i [33, Theorem 1.2.19].

Since f is an irreducible divisor of h with $h = gf$ for some $g \in R$, we obtain that $h = h_1 h_2 \cdots h_{k-1} f$ for some irreducible polynomials $h_i \in R$ of degree m, $D_h \cong I(f)/Rf = \mathrm{Nuc}_r(S_f)$, and therefore

$$R/Rh \cong M_k(\mathrm{Nuc}_r(S_f)).$$

Since f is irreducible, $\mathrm{Nuc}_r(S_f)$ is a division algebra. In particular, here h has degree km, since all h_i are similar and thus have the same degree m as f. We know that R/Rh is a central simple algebra over its center $E_{\hat{h}}$ (which is a field) and so $\mathrm{Nuc}_r(S_f)$ is a associative division algebra over $E_{\hat{h}}$ of dimension s^2.

Comparing the dimensions of R/Rh and $M_k(\mathrm{Nuc}_r(S_f))$ over F it follows that

$$d^2\, p^{2e}\deg(\hat{h}) = k^2 s^2\, [E_{\hat{h}} : F],$$

so that $d^2\, p^{2e} = k^2 s^2$, that is $dp^e = ks$, so that $s = dp^e/k$.
Since $[E_{\hat{h}} : F] = \frac{dm}{s}$ we know that s divides dm. Since $k = \frac{dp^e}{s}$ we know that s divides dp^e. Furthermore, if we assume that f is not right invariant then S_f is not associative so $k > 1$, which implies $s \neq dp^e$. □

We know that $[S_f : F] = [S_f : C]p^e = d^2m \cdot p^e$. Since $\mathrm{Nuc}_r(S_f)$ is a subalgebra of S_f, comparing dimensions we obtain that

$$[S_f : \mathrm{Nuc}_r(S_f)] = k.$$

If f is not right-invariant, again $[S_f : \mathrm{Nuc}_r(S_f)] = k > 1$.

Theorem 3.2.18. *Suppose that $gcd(m, p^e) = 1$. Then s divides d, and f is not right invariant. If d is prime then one of the following holds:*
(i) $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$, $dp^e = k$, $\deg(\hat{h}) = dm$ *and* $\deg(h) = dp^e m$. *In particular, then* $[\mathrm{Nuc}_r(S_f) : F] = dm$.
(ii) $\mathrm{Nuc}_r(S_f)$ *is a associative division algebra over* $E_{\hat{h}}$ *of degree* d, p^e *is the number of irreducible factors of* h *in* R, $\deg(h) = p^e m$, $\deg(\hat{h}) = m$ *and* $[\mathrm{Nuc}_r(S_f) : F] = d^2 m$.

Proof. Since s divides $gcd(dm, dp^e)$ and we have $gcd(m, p^e) = 1$ by assumption, we know that s divides d. Moreover, then $k > 1$ as $k = dn/s$, thus f is not right invariant. Assume d is prime so that $s = 1$ or $s = d$. If $s = 1$ then we immediately get the assertion in (i), and $s = d$ yields (ii) using that $[\mathrm{Nuc}_r(S_f) : F] = [\mathrm{Nuc}_r(S_f) : E_{\hat{h}}][E_{\hat{h}} : F] = d^2 deg(\hat{h}) = d^2 p^e/p^e m = d^2 m$. □

Theorem 3.2.19. *Suppose that $gcd(d, p^e) = 1$ and that f is not right invariant. Then $s = 1$, or $s \neq 1$ and s divides either d or p^e.*

Suppose additionally that d is prime and $e = 1$. Then one of the following holds:
(i) $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$, $dp = k$, $\deg(\hat{h}) = dm$ *and* $\deg(h) = dpm$. *In particular, then* $[\mathrm{Nuc}_r(S_f) : F] = dm$.
(ii) $\mathrm{Nuc}_r(S_f)$ *is a associative division algebra over* $E_{\hat{h}}$ *of degree* d, p *is the number of irreducible factors of* h *in* R, $\deg(h) = pm$, $\deg(\hat{h}) = m$ *and*

$$R/Rh \cong M_k(\mathrm{Nuc}_r(S_f)).$$

In particular, then $[\mathrm{Nuc}_r(S_f) : F] = d^2m$.
(iii) $\mathrm{Nuc}_r(S_f)$ *is a associative division algebra over* $E_{\hat{h}}$ *of degree* p, d *is the number of irreducible factors of* h *in* R, $\deg(\hat{h}) = dm/p$, $\deg(h) = dm$, *and* $[\mathrm{Nuc}_r(S_f) : F] = p^2/dm$.
Note that case (iii) cannot happen if p *does not divide* dm *or if* dm *does not divide* p^2.

Proof. It is clear that $s = 1$, or $s \neq 1$ and s divides either d or p^e. Suppose additionally that d is prime, $e = 1$. Then the equation $dp = ks$ in the proof of Theorem 3.2.10, forces that either $s = 1$ and $k = pd$, or that $s \neq 1$ and then $d = k$ and $p = s$ (or resp., $d = s$ and $p = k$). As before, $s = 1$ yields (i).
If $d = s \neq 1$ and $p = k$ then this implies (ii) employing that $[\mathrm{Nuc}_r(S_f) : F] = [\mathrm{Nuc}_r(S_f) : E_{\hat{h}}][E_{\hat{h}} : F] = d^2 deg(\hat{h}) = d^2p/pm = d^2m$.
If $d = k$ and $p = s \neq 1$ then this implies (iii) using that $[\mathrm{Nuc}_r(S_f) : F] = [\mathrm{Nuc}_r(S_f) : E_{\hat{h}}][E_{\hat{h}} : F] = p^2 deg(\hat{h}) = p^2/dm$. In particular, this case means that $\deg(\hat{h}) = dm/p$, which forces n to divide dm, as well as $[\mathrm{Nuc}_r(S_f) : F] = p^2/dm$ which in turn forces dm to divide n^2. □

3.3 CONSTRUCTION OF DIVISION ALGEBRAS USING $f \in D[t;\sigma]$

Let D be an associative division algebra of degree d over its center $C = Z(D)$. As in previous sections, we allow the possibility that $d = 1$ and $D = C$ is a field. Let σ be an automorphism of D of finite order n modulo inner automorphisms

with $\sigma^n(z) = uzu^{-1}$ for some $u \in D^\times$, where we will assume without loss of generality that $u \in \mathrm{Fix}(\sigma)$. Then

$$Z(R) = F[u^{-1}t^n] \cong F[x]$$

by [33, Theorem 1.1.22] and n is the order of $\sigma|_C$. Every f is bounded.

Let $f \in R = D[t;\sigma]$ be an irreducible monic polynomial of degree m, such that $f(t) \neq t$. By Lemma 3.2.6, f has a minimal central left multiple $h = \hat{h}(u^{-1}t^n)$ which is irreducible in $F[x]$.

Furthermore, Rh is a maximal two-sided ideal of R and thus we can construct the associative quotient algebra $S_h = R/Rh$, which is simple over its centre $C(S_h) \cong E_{\hat{h}}$ by Lemma 3.2.8.

Lemma 3.3.1. *For each $z(t) = \hat{z}(u^{-1}t^n) \in F[u^{-1}t^n]$ with $\hat{z} \in F[x]$, we have $z \in Rf$ if and only if $z \in Rh$.*

Proof. As $h = gf$ for some $g \in R$, each $z \in Rh$ also lies in Rf.

Conversely, let $z(t) = \hat{z}(u^{-1}t^n) \in F[u^{-1}t^n]$ with $\hat{z} \in F[x]$ be such that $z \in Rf$. Using the Euclidean division algorithm in $F[x]$, there exist unique $\hat{q}(x), \hat{r}(x) \in F[x]$ such that

$$\hat{z} = \hat{q}\hat{h} + \hat{r},$$

where $\deg(\hat{r}) < \deg(\hat{h}) = s$ or $\hat{r} = 0$. If $\hat{r} \neq 0$, then $\hat{r} = \hat{z} - \hat{q}\hat{h}$, i.e. we found $q(t) = \hat{q}(u^{-1}t^n), r(t) = \hat{r}(u^{-1}t^n) \in F[u^{-1}t^n]$, such that

$$r(t) = z(t) - q(t)h(t) \in Rf.$$

Let $\hat{r'}(x) = r_0^{-1}\hat{r}(x) \in F[x]$, where $r_0 \in F^\times$ is the leading coefficient of $\hat{r}(x)$, then $r'(t) = \hat{r'}(u^{-1}t^n)$ is monic by definition.

As $r'(t) = \hat{r'}(u^{-1}t^n) \in Rf$, too, there exists $a(t) \in R$ such that $r'(t) = a(t)f(t)$. Thus, $r'(t) \in F[u^{-1}t^n]$ is a monic polynomial of degree less than s which is right divisible by f. This contradicts the definition of h as the minimal central left multiple of f. Thus we conclude that $r = 0$ and $z = qh \in Rh$, as required. □

Let

$$V_f = \{a + Rf : a \in R = D[t;\sigma]\} = R/Rf$$

be the R-module defined by factoring out the maximal left ideal Rf and let

$$E_f = \{z(t) + Rf : z(t) = \hat{z}(u^{-1}t^n) \in F[u^{-1}t^n]\} \subset V_f.$$

Together with the multiplication

$$(x + Rf) \circ (y + Rf) := (xy) + Rf$$

for all $x, y \in F[u^{-1}t^n]$, E_f becomes an F-algebra.

Lemma 3.3.2. *$E_f = (E_f, \circ)$ is a field and isomorphic to $E_{\hat{h}}$.*

Proof. Clearly, E_f is a commutative associative ring with identity $1 + Rf$; we only need to show that every non-zero element of E_f has an inverse in E_f. Let $z + Rf$ be a non-zero element of E_f. If $\deg(z) = 0$, then $z \in F^\times$ and $(z + Rf)^{-1} = z^{-1} + Rf$. So suppose $\deg(z) > 0$ and $z(t) = \hat{z}(u^{-1}t^n)$ for some $\hat{z}(x) \in F[x]$. By Lemma 3.3.1, $\hat{h}(x)$ does not divide $\hat{z}(x)$ in $F[x]$. Additionally, $\hat{h}$ is irreducible in $F[x]$ so $\hat{z}$ cannot divide $\hat{h}$ in $F[x]$. Thus the greatest common divisor of $\hat{z}$ and $\hat{h}$ in $F[x]$ must be some $k \in F^\times$ and that there exist some non-zero $\hat{q}, \hat{p} \in F[x]$ such that

$$\hat{z}\hat{p} + \hat{h}\hat{q} = k.$$

Let $p(t) = \hat{p}(u^{-1}t^n)$, then $zp - k \in Rh$. By Lemma 3.3.1, this implies $zp - k \in Rf$, that means $(z + Rf)(p + Rf) = k + Rf$, i.e. $(z + Rf)^{-1} = k^{-1}p + Rf$. It is clear that F is a subfield of E_f embedded via the map $F \longrightarrow F + Rf$, $k \mapsto k + Rf$ for all $k \in F$. Thus E_f is isomorphic to a field extension of F. Define a map $G : E_f \to E_{\hat{h}}$ by

$$G(z + Rf) = z + Rh$$

for all $z \in F[u^{-1}t^n]$.

Suppose $z + Rf = z' + Rf$. Then $z - z' \in Rf$ and $z - z' \in Rh$ by Lemma 3.3.1. Thus we obtain $z + Rh = z' + Rh$; that is, $G(z + Rf) = G(z' + Rf)$.

So G is well-defined. Additionally, for any $z + Rh \in E_{\hat{h}}$, it follows that $G(z + Rf) = z + Rh$. Thus G is surjective.

To check injectivity, we note that $G(x + Rh) = 0 + Rf$ if and only if $x \in Rf$. Again by Lemma 3.3.1, this implies $x \in Rh$ and so $x + Rh = 0 + Rh$. Furthermore, for all $x, y \in F[u^{-1}t^n]$ we have

$$G(x+Rf)+G(y+Rf) = (x+Rh)+(y+Rh) = (x+y)+Rh = G(x+y+Rf),$$

$$G(x+Rf)G(y+Rf) = (x+Rh)(y+Rh) = xy+Rh = G(xy+Rf),$$

yielding that G is an isomorphism of fields. □

Let $B = \mathrm{Nuc}_r(S_f)$. Then we have:

Proposition 3.3.3. *Let k be the number of irreducible factors of h. Then V_f is a right B-module of dimension k via the scalar multiplication given by $V_f \times B \longrightarrow V_f$,*

$$(a + Rf)(z + Rf) = az + Rf \in V_f$$

for all $z \in F[u^{-1}t^n]$ and $a \in R$. Thus, we can identify V_f with B^k via a canonical basis.

Proof. In order to show that the scalar multiplication is well-defined, suppose $a + Rf = a' + Rf$ and $z = z'$ for $a, a' \in R$ and $z, z' \in B$. Then there exists $u, v \in R$ such that $a' = a + uf$ and $z' = z + vf$ (as $B \subset R/Rf$), and we have

$$\begin{aligned}(a' + Rf)z' =& a'z' + Rf \\ =& (az + avf + ufz + ufvf) + Rf\end{aligned}$$

As $z \in B$, this implies $fz = z'f$ for some $z' \in R$ so $(az + avf + ufz + ufvf) + Rf = az + (av + uz' + ufv)f + Rf = az + Rf$. Thus it follows that $(a' + Rf)z' = (a + Rf)z$ as required.

The remaining properties we require for scalar multiplication such as distributivity follow from the multiplication in R. As V_f is a vector space of dimension d^2mn over F and B/F has dimension dms by Theorem 3.2.10 , it follows that V_f has

dimension $d^2mn/dms = dn/s = k$ over B, where k is the number of irreducible divisors of h in R. □

In the special case where $\deg(\hat{h}) = dm$, we see that

$$\mathrm{Nuc}_r(S_f) = E_{\hat{h}} \cong E_f$$

by Theorem 3.2.19. Under this assumption, h has exactly dn irreducible factors in R, yielding the following corollary:

Corollary 3.3.4. *Let* $\deg(\hat{h}) = dm$. *Then* V_f *is a right* E_f*-vector space of dimension* dn *via the scalar multiplication given by* $V_f \times E_f \longrightarrow V_f$,

$$(a + Rf)(z + Rf) = az + Rf \in V_f$$

for all $z \in F[u^{-1}t^n]$ *and* $a \in R$. *Thus, we can identify* V_f *with* E_f^{dn} *via a canonical basis.*

3.3.1 *The construction of* $S_{n,m,l}(\nu, \rho, f)$

For some $\nu \in D^\times$ and $\rho \in \mathrm{Aut}(D)$, define $F' = \mathrm{Fix}(\rho) \cap F$. We assume in the following that F/F' is finite-dimensional. Let k be the number of irreducible factors of $h(t)$ and s the degree of the right nucleus of S_f over $E_{\hat{h}}$. We assume f is not right-invariant which yields $k > 1$.

Let $l < k = dn/s$. Consider the set $S_{n,m,l}(\nu, \rho, f) = \{a + Rh \,|\, a \in A\} \subset R/Rh$, where

$$A = \{a_0 + a_1 t + \cdots + a_{lm-1}t^{lm-1} + \nu\rho(a_0)t^{lm} : a_i \in D\} \subset D[t;\sigma].$$

$S_{n,m,l}(\nu, \rho, f)$ is a vector space over F' of dimension $d^2nm[F : F']$. In particular, $S_{n,m,1}(\nu, \rho, f) = \{a + Rh \,|\, a \in A\}$, where

$$A = \{a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} + \nu\rho(a_0)t^{m} : a_i \in D\} \subset D[t;\sigma].$$

Remark 3.3.5. In [56], this construction over $\mathbb{F}_q$ is denoted by $S_{n,m,l}(\nu,\rho,h)$. Although this indicates that the set is a subspace of R/Rh, we change this notation in order to reflect the polynomial f used in the construction. This is because we are interested in expressing the multiplication of the algebras explicitly, whereas previous work only considers the multiplication via semifield spread sets.

Let L_a be the left multiplication map $L_a(b+Rf) = ab+Rf$ for $b+Rf \in V_f$. Note that L_a is B-linear, as we have $a(x\alpha) = (ax)\alpha$ for all $\alpha \in B = \mathrm{Nuc}_r(S_f)$, $a, x \in V_f$, and therefore $L_a(x\alpha) = L_a(x)\alpha$ for all $\alpha \in B$. Thus $L_a \in \mathrm{End}_B(V_f)$. Since $l < k = dn/s$, we have a well-defined map

$$L : S_{n,m,l}(\nu,\rho,f) \to \mathrm{End}_B(V_f),$$

$$a + Rh \mapsto L_a$$

To see that L is well-defined, let $a, a' \in A$ be such that $a + Rh = a' + Rh$. Suppose $a \neq a'$. Then $a + Rh = a' + Rh$ iff $a - a' \in Rh$ iff $a - a' = rh$ for some $r \in R$. As $a \neq a'$, it follows that $a - a' \neq 0$, so $r \neq 0$. Then taking degrees on both sides, we have $\deg(a-a') = \deg(rh) \geq \deg(h) = dmn$, but because we assumed a and a' to have degree less than or equal to lm, i.e. strictly less than $km = dmn/s$, this is a contradiction. So $a = a'$ and $L_a = L_{a'}$.

As $\mathrm{End}_B(V_f) \cong M_k(B)$, we can extend L to $M_k(B)$ as follows: define

$$L : S_{n,m,l}(\nu,\rho,f) \to \mathrm{End}_B(V_f) \to M_k(B),$$

$$a \mapsto L_a \mapsto M_a,$$

where M_a is the matrix associated to the left multiplication map L_a with respect to an B-basis of V_f.

For $l < k$, we denote the image of $S_{n,m,l}(\nu,\rho,f)$ in $M_k(B)$ by

$$\mathcal{C}(S) = \{M_a \mid a \in S_{n,m,l}(\nu,\rho,f)\}.$$

As the dimension of $\mathcal{C}$ as a right B-module is equal to

$$\dim_B(S_{n,m,l}(\nu,\rho,f)) = \frac{\dim_F(S_{n,m,l}(\nu,\rho,f))}{\dim_F(B)} = \frac{d^2nlmk}{d^2nm} = lk,$$

Theorem 2.2.2 implies the minimum distance of $\mathcal{C}$ as a rank-metric code satisfies

$$lk \leq k(k - d_{\mathcal{C}} + 1) \iff d_{\mathcal{C}} \leq k - l + 1;$$

moreover, $\mathcal{C}$ is an MRD-code in $M_k(B)$ if $d_{\mathcal{C}} = k - l + 1$.

3.3.2 *Division algebras over F'*

When $l = 1$, this construction can yield division algebras over F' via the set $S_{n,m,1}(\nu, \rho, f)$; the actual construction of these algebras may be viewed by two equivalent methods. Firstly, we directly define a multiplication on the F-vector space

$$R_m = \{g \in R : \deg(g) < m\}.$$

There is a natural bijection between R_m and A by $a(t) \mapsto a(t) + \nu\rho(a_0)t^m$ for all $a(t) = \sum_{i=0}^{m-1} a_i t^i \in R_m$. Define a multiplication $\circ : R_m \times R_m \to R_m$ by

$$a(t) \circ b(t) = (a(t) + \nu\rho(a_0)t^m)b(t) \mod_r(f).$$

In this way, $(R_m, \circ)$ can be viewed as a generalisation of Petit algebras [44] as setting $\nu = 0$ recovers the algebra S_f.

Example 3.3.6. Let $m = 1$, so $f(t) = t - c$ for some $c \in D$. For some $\nu \neq 0$ and $\rho \in \mathrm{Aut}(D)$, $S_{n,1,1}(\nu, \rho, f) = (D, \circ)$ has multiplication

$$\begin{aligned} x \circ y =& (x + \nu\rho(x)t)y) \bmod_r f \\ =& xy + \nu\rho(x)\sigma(y)t \bmod_r f \\ =& xy + \nu\rho(x)\sigma(y)c \end{aligned}$$

for all $x, y \in D$. If $R = K[t;\sigma]$ for some field extension K/F, this is precisely the multiplication of Albert's twisted semifields as given in [1]. If $R = D[t;\sigma]$ for a associative division algebra D/C, we obtain generalisations of Albert's twisted fields which were studied in [46].

Now suppose $x \circ y = 0$ for some non-zero $x, y \in R_1$. This occurs if and only if $xy = -\nu\rho(x)\sigma(y)c$. Taking norms of both sides and cancelling $N_{D/F'}(xy)$ from

both sides, we obtain that $N_{D/F'}(-\nu c) = 1$. Thus $S_{n,1,1}(\nu, \rho, f)$ is a division algebra if

$$N_{D/F'}(\nu c) \neq (-1)^{d^2 n[F:F']}.$$

Alternatively, we can use $\mathcal{C}(S) \subset M_k(B)$ to define a multiplication on B^m. As the dimension of D over F is d^2n and the dimension of B is d^2mn/k, there exists an F-vector space isomorphism between D^m and B^k. It follows that there similarly exists an isomorphism between $G : V_f \to B^k$ so, for each $a + Rf \in R/Rf$, there exists some $\underline{a} \in B^k$ such that $G(a + Rf) = \underline{a}$. Define $* : B^k \times B^k \to B^k$ by

$$\underline{a} * \underline{b} = M_a \cdot \underline{b}$$

for all $\underline{a}, \underline{b} \in B^k$, where $M_a \in \mathcal{C}(S)$ is the representation of the map $L_{a(t)+\nu\rho(a_0)t^m} \in End_B(V_f)$ induced by G. (Each $a \in R_m$ corresponds to a map $L_{a(t)+\nu\rho(a_0)t^m}$. As $End_B(V_f) \cong M_k(B)$ and $\dim(R_m) = \dim(\mathcal{C}(S))$, there is a canonical bijection between $L_{a(t)+\nu\rho(a_0)t^m}$ and M_a.) As M_a is a representation of the map $L_a \in \mathrm{End}_B(V_f)$, it follows that $(B^k, *)$ is isomorphic to R/Rf equipped with the multiplication $(a + Rf)(b + Rf) = L_{a(t)+\nu\rho(a_0)t^m}(b + Rf)$. Thus it follows that $(R_m, \circ)$ and $(B^k, *)$ are isomorphic algebras by construction.

3.3.3 *The rank of a matrix*

We recall the definition of rank of a matrix:

Definition 3.3.7. Let $A \in M_k(B)$. The *column rank of a matrix* A is the dimension of the right B-module generated by the columns of A; similarly, define the row rank of A as the dimension of the right B-module generated by the rows of A. When B is a field, row and column rank are always equal and is called the *rank of a matrix*.

A matrix in $M_k(B)$ has (column) rank at most k; any matrix which attains this bound is said to have attained *full (column) rank*. By definition of column rank, a matrix attains full column rank if and and only if its columns are linearly independent over B.

For any $M_a \in \mathcal{C}(S)$, suppose there exists some non-zero $\underline{x} \in B^k$ such that $M_a \cdot \underline{x} = \underline{0}$. Let $\underline{c_i} \in B^k$ be the column vectors of M_a and $x_i \in B$ be the entries of $\underline{x}$, then

$$M_a \cdot \underline{x} = 0 \iff \underline{c_1}x_1 + \cdots + \underline{c_k}x_k = 0.$$

As $\underline{x} \neq \underline{0}$, this implies there is a linear combination of the columns of M_a, i.e. M_a does not have full column rank. Conversely if we assume M_a does not have full column rank, there exists some non-zero $\underline{x} \in B^k$ such that $M_a \cdot \underline{x} = \underline{0}$. Hence $(B^k, *)$ is a division algebra if and only if every matrix in $\mathcal{C}(S)$ has full column rank.

Lemma 3.3.8. *Let R be a ring with no zero divisors. For all $h \in Z(R)$, every right divisor of h in R also divides h on the left.*

Proof. Suppose γ is a right divisor of h. Then $h = \delta\gamma$ for some $\delta \in R$. As h lies in the centre of R, we have $\delta h = h\delta = \delta\gamma\delta$. This rearranges to

$$0 = \delta h - \delta\gamma\delta = \delta(h - \gamma\delta).$$

As R contains no zero divisors and $\delta \neq 0$, it follows that $h = \gamma\delta$. □

Proposition 3.3.9. *Let $f \in D[t;\sigma]$ be irreducible and $\deg(\hat{h}) = km/n$. Let $B = \mathrm{Nuc}_r(S_f)$. For all $a + Rh \in R/Rh$, we have*

$$\dim_B(im(L_A)) = k^2 - \frac{k}{m}\deg(gcrd(a, \hat{h}(t^n))).$$

Moreover, the column rank of M_a is equal to $k - \frac{1}{m}\deg(gcrd(a, \hat{h}(t^n))$.

Proof. By Theorem 3.2.10, $R/Rh \cong M_k(B)$ as $E_{\hat{h}}$-algebras. Let $\Psi : R/Rh \to M_k(B)$, $\Psi(a + Rh) = M_a$, be such an isomorphism. For each $A \in M_k(B)$, define $\mathrm{Ann}_r(A) = \{N \in M_k(B) : AN = 0\}$. It is clear that $\mathrm{Ann}_r(A)$ is the kernel of the endomorphism $L_A : M_k(B) \to M_k(B)$ defined by

$$L_A : X \mapsto AX.$$

As B is associative, L_A is a right B-linear map: for all $b \in B$, $X \in M_k(B)$, $L_A(Xb) = A(Xb) = (AX)b = L_A(X)b$. By the Rank-Nullity Theorem for free right B-modules of finite rank [31, ch. IV, Cor. 2.14], it follows that

$$k^2 = \dim_B(im(L_A)) + \dim_B(\mathrm{Ann}_r(A)).$$

We conclude

$$\dim_B(im(L_A)) = k^2 - \dim_B(\mathrm{Ann}_r(A)).$$

Now for each $b+Rh$, $M_aM_b = 0$ if and only if $\Psi(a+Rh)\Psi(b+Rh) = 0$. As Ψ is multiplicative, this is true if and only if $\Psi((a+Rh)(b+Rh)) = 0$. Thus we conclude $(a+Rh)(b+Rh) = 0$. Hence it is clear that $\mathrm{Ann}_r(M_a) \cong \mathrm{Ann}_r(a)$, where

$$\mathrm{Ann}_r(a) = \{b+Rh \in R/Rh : (a+Rh)(b+Rh) = 0+Rh\},$$

so $\dim(\mathrm{Ann}_r(M_a)) = \dim(\mathrm{Ann}_r(a))$.

Let $\gamma = gcrd(a,h)$ so $h = \delta\gamma$ for some $\delta \in R$. As $h \in Z(R)$ and R is a domain, we also have $h = \gamma\delta$ by Lemma 3.3.8. Let $b \in R$ be the unique element such that $a = b\gamma$. Then $gcrd(b,\delta) = 1$, else γ is not the greatest common right divisor of a and h.

Let $v \in R$. By the left Euclidean division algorithm, there exist unique $u, w \in R$ such that $v = \delta u + w$ where $\deg(w) < \deg(\delta)$ and $gcld(w,\delta) = 1$. It follows that

$$\begin{aligned} av =& a\delta u + aw \\ =& b\gamma\delta u + b\gamma w \\ =& bhu + b\gamma w. \end{aligned}$$

Thus it follows that $av + Rh = b\gamma w + Rh$.

Suppose $b\gamma w \equiv 0 \bmod_r h$. As $gcrd(b,\delta) = 1$, there exist $c, d \in R$ such that $cb + d\delta = 1$ so

$$cb\gamma + d\delta\gamma = \gamma.$$

As $\delta\gamma = h$, this implies $cb\gamma \equiv \gamma \bmod_r h$. Hence

$$\gamma w \equiv cb\gamma w \equiv 0 \bmod_r h.$$

However, $\deg(w) < \deg(\delta)$ so $\deg(\gamma w) < \deg(\gamma\delta) = \deg(h)$; due to this, $\gamma w \equiv 0 \bmod_r h$ implies that $\gamma w = 0$. As $\gamma \neq 0$ and R is a domain, we conclude that $w = 0$.

Therefore, $(a+Rh)(v+Rh) = 0+Rh$ if and only if $v = \delta u$ where $\deg(u) < \deg(\gamma)$. As δ is uniquely defined by a and h, every element of $\mathrm{Ann}_r(a)$ is determined by $u \in R$ such that $\deg(u) < \deg(\gamma)$. Thus

$$\begin{aligned}\mathrm{Ann}_r(a) =& \{v+Rh \in R/Rh \,|,\ (a+Rh)(v+Rh) = 0+Rh\} \\ =& \{\delta u \,|\, u \in R, \deg(u) < \deg(\gamma)\} \\ \cong& R_{\deg\gamma}.\end{aligned}$$

As $\{1, t, \ldots, t^{\deg(\gamma)-1}\}$ is a D-basis for $R_{\deg\gamma}$, it follows that $\dim_D(\mathrm{Ann}_r(a)) = \deg(\gamma)$, so $\dim_F(\mathrm{Ann}_r(a)) = \deg(\gamma)d^2n$. Since $\dim_{E_{\hat{h}}}(B) = s^2 = d^2n^2/k^2$ and $[E_{\hat{h}} : F] = km/n$, we obtain $\dim_F(B) = d^2mn/k$. Hence we conclude that

$$\dim_B(\mathrm{Ann}_r(a)) = \frac{\deg(\gamma)d^2nk}{d^2mn} = \frac{\deg(\gamma)k}{m},$$

and so

$$\dim_B(im(L_A)) = k^2 - \dim_B(\mathrm{Ann}_r(A)) = k^2 - \frac{k}{m}\deg(\gamma).$$

Let $\underline{c_i}$ and $\underline{r_i}$ denote the columns and rows of A respectively and $\underline{x_i}$ denote the columns of X. Then computing the matrix using dot product notation we have

$$AX = \begin{pmatrix} \underline{r_1}\cdot\underline{x_1} & \cdots & \underline{r_1}\cdot\underline{x_k} \\ \vdots & \ddots & \vdots \\ \underline{r_k}\cdot\underline{x_1} & \cdots & \underline{r_k}\cdot\underline{x_k} \end{pmatrix}$$

The i^{th} column of AX is equal to

$$\begin{pmatrix} \underline{r_1}\cdot\underline{x_i} \\ \vdots \\ \underline{r_k}\cdot\underline{x_i} \end{pmatrix} = \underline{c_1}\lambda_1 + \cdots + \underline{c_k}\lambda_k$$

for some $\lambda_j \in B$. Hence the dimension of the B-vector space generated by the i^{th} column of AX is exactly the column rank of A. As there are k columns of AX, it follows that that $\dim_B(im(L_A)) = k \cdot \mathrm{colrank}(A)$. □

When $\deg(\hat{h}) = dm$, we recall that $B = \mathrm{Nuc}_r(S_f)$ is a field and we obtain the following corollary:

Corollary 3.3.10. *[56, Proposition 7 for finite fields] Let $f \in D[t;\sigma]$ and $\deg(\hat{h}) = dm$. For all $a + Rh \in R/Rh$, we have*

$$\operatorname{rank}(M_a) = dn - \frac{1}{m}\deg(gcrd(a, \hat{h}(t^n))).$$

As a result of this, $(B^k, *)$ is a division algebra if and only if there are no divisors of h in $S_{n,m,1}(\nu,\rho,f)$. More generally, $S_{n,m,l}(\nu,\rho,f)$ yields an MRD-code in $M_k(B)$ if and only if it contains no divisors of h of degree lm.

Theorem 3.3.11. $S_{n,m,l}(\nu,\rho,f) = \{a + Rh \,|\, a \in A\} \subset R/Rh$, *where*

$$A = \{a_0 + a_1 t + \cdots + a_{lm-1}t^{lm-1} + \nu\rho(a_0)t^{lm} : a_i \in D\}$$

yields an MRD-code if and only there are no elements $g \in S_{n,m,l}(\nu,\rho,f)$ of degree lm which can be written as $g = \prod_{i=1}^{l} f_i$, where f_i is similar to f for all i, i.e. there are no divisors of h of degree lm in A.

We can use the above Proposition 3.3.9 to determine some initial conditions to obtain division algebras:

Corollary 3.3.12. *Suppose that*

$$A = \{a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} + \nu\rho(a_0)t^{m} : a_i \in D\} \subset R.$$

Let f be an irreducible monic polynomial of degree m.
(i) If $a \in A$ is reducible, then a is not a left zero divisor in $(R_m, \circ)$.
(ii) If $\nu = 0$ then $(R_m, \circ)$ is a division algebra over F', which for $m \geq 2$ is a (unital) Petit algebra.
(iii) If A does not contain any polynomial similar to f, then $(R_m, \circ)$ is a division algebra over F'.

In order to find a more tractable condition to obtain division algebras and MRD codes, we must determine what the divisors of $h(t)$ look like. We follow two techniques to do this: firstly, we consider the technique used in [56] which employs semi-linear maps of R/Rf. The second method considers the norm map in $D(t;\sigma)$ as used in [13] to determine reducibility criteria for polynomials in $\mathbb{F}_q[t;\sigma]$. Both approaches were originally only considered for $\mathbb{F}_q[t;\sigma]$; we give generalisations to $D[t;\sigma]$, where D is a associative division algebra as assumed previously.

3.4 SEMI-LINEAR MAPS

Let $R = D[t;\sigma]$ with all assumptions on D as stated previously and $f \in R$ be a monic irreducible polynomial of degree m. Left multiplication by t defines a map

$$\phi_f : R/Rf \to R/Rf, \quad \phi_f(v) = tv \bmod_r f$$

for all $v \in R/Rf$. This is a *D-semi-linear map*, as

$$\phi_f(av) = \sigma(a)\phi_f(v)$$

for all $v \in R/Rf$, $a \in D$. Identify $R/Rf = D \oplus Dt \oplus \cdots \oplus Dt^{m-1}$ with the free left D-module D^m with the basis $\beta = \{1, t, \ldots, t^{m-1}\}$. In particular, this means we identify an m-tuple $(v_0, \ldots, v_{m-1}) = v_\beta$ with the polynomial $v = \sum_{i=0}^{m-1} v_i t^i$. Via our identification between R/Rf and D^m, we can view ϕ_f as a D-semi-linear map on D^m:

Lemma 3.4.1. *$\phi_f : D^m \to D^m$ is given by*

$$\begin{aligned}\phi_f(v_0, \ldots, v_{m-1}) =& (\sigma(v_0), \cdots, \sigma(v_{m-1})) \cdot \begin{pmatrix} 0 & 1 & \ldots & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & 1 \\ -a_0 & -a_1 & \ldots & -a_{m-2} & -a_{m-1} \end{pmatrix} \\ =& \sigma(v_\beta) \cdot C_f,\end{aligned}$$

where C_f is the companion matrix of f.

Proof. Let $v \in R/Rf$. Noting that $\phi_f(v) = \sum_{i=0}^{m-1} \sigma(v_i) t^{i+1} \bmod_r f$, we see that the only term of this sum that needs to be reduced modulo f is $\sigma(v_{m-1})t^m$. Upon right division by f, we obtain

$$\sigma(v_{m-1})t^m = -\sigma(v_{m-1})(a_0 + a_1 t + \cdots + a_{m-1}t^{m-1}) \bmod_r f.$$

Thus we can map $\sigma(v_{m-1})t^m$ to D^m via

$$\sigma(v_{m-1})t^m \mapsto (-\sigma(v_{m-1})a_0, -\sigma(v_{m-1})a_1, \ldots, -\sigma(v_{m-1})a_{m-1}).$$

It follows that

$$\phi_f(v) \mapsto (-\sigma(v_{m-1})a_0, \sigma(v_0) - \sigma(v_{m-1})a_1, \ldots, \sigma(v_{m-2}) - \sigma(v_{m-1})a_{m-1}).$$

Computing $\sigma(v_\beta) \cdot C_f$ yields exactly the same vector as required. □

Remark 3.4.2. We use the definition of the companion matrix as defined in [40, p. 4], which is transpose to the companion matrix used in [56]. Thus, the analogous result in [56] is

$$\phi_f(v_\beta^T) = C_f^T \cdot \sigma(v_\beta^T),$$

where v_β^T is a column vector of length m. When $f \in R = K[t;\sigma]$, it does not matter which of the two matrices we use for the definition of $\phi_f : K^m \to K^m$, as $C_f^T \cdot \sigma(v_\beta^T) = (\sigma(v_\beta) \cdot C_f)^T$, but for $R = D[t;\sigma]$, this is no longer true.

Remark 3.4.3. In [40, Corollary 1.9], the companion matrix of f is used to give an alternative description of the eigenring $\mathrm{End}_R(R/Rf)$ of the polynomial f, as we have

$$\mathrm{End}_R(R/Rf) \cong C_f^\sigma := \{B \in M_m(K) \mid C_f B = \sigma(B)C_f\}.$$

This holds even when we take $R = D[t;\sigma,\delta]$ by letting $C_f^{\sigma,\delta} = \{B \in M_m(D) \mid C_f B = \sigma(B)C_f + \delta(B)\}$.

Analogously, we may define an F-linear map

$$\phi_f^n : R/Rf \to R/Rf, \quad v \mapsto t^n v \bmod_r f$$

for all $v \in R$. By definition, it follows that $\phi_f^n = (\phi_f)^n$. Since

$$\phi_f^n(av) = \sigma^n(a)\phi_f(v) = uau^{-1}\phi_f(v),$$

this map is D-linear if $\sigma^n = id$. As with ϕ_f, we can view ϕ_f^n as a map on D^m:

Lemma 3.4.4. *$\phi_f^n : D^m \to D^m$ is given by*

$$\phi_f^n(v_\beta) = \sigma^n(v_\beta) \cdot \sigma^{n-1}(C_f) \cdots \sigma(C_f)C_f = \sigma^n(v_\beta) \cdot A_f,$$

where $\sigma(C_f)$ means that σ acts on each entry of $C_f \in M_m(D)$. If $\sigma^n = id$, ϕ_f^n is a D-linear map.

Proof. As $\phi_f^n = (\phi_f)^n$, this follows from our identification in Lemma 3.4.1. □

3.4.1 *The case for $K[t;\sigma]$*

We consider the special case when $d = 1$, i.e. $D[t;\sigma] = K[t;\sigma]$ for some field extension K/F. Much of this was done in [56] but we include the results for completion and comparison to the generalisation for $d > 1$. The work done previously in the literature assumed that K was a finite field but the proofs follow identically when we assume that $\deg(h) = mn$. This follows since the degree of h is always mn when K is a finite field.

Definition 3.4.5. Let E be a field. The *minimal polynomial* of a matrix $A \in M_n(E)$ is the polynomial $G(x) \in E[x]$ of lowest degree such that $G(A) = 0$. The *characteristic polynomial* of a matrix $A \in M_n(E)$ is defined as $\chi_A(x) = \det(xI - A)$.

Theorem 3.4.6. *(for finite fields K, cf. [56, Theorem 3]) The minimal central left multiple of f is given by $h(t) = \hat{h}(t^n)$, where $\hat{h}$ is equal to the minimal polynomial of the matrix A_f over F. If $\deg(h) = mn$, e.g. if n is prime or $gcd(m, n) = 1$, then the minimal polynomial of A_f is equal to the characteristic polynomial of A_f.*

Theorem 3.4.7. *(for finite fields K, cf. [56, Theorem 4]) If $\deg(h) = mn$, then*

$$N_{K/F}(a_0) = (-1)^{m(n-1)} h_0,$$

where a_0 and h_0 are the constant terms of f and h, respectively.

Theorem 3.4.8. *(for finite fields K, cf. [56, Theorem 5]) If $\deg(h) = mn$ and g is a monic divisor of $h(t) = \hat{h}(t^n)$ in R of degree ml, then*

$$N_{K/F}(g_0) = N_{K/F}(a_0)^l.$$

3.4.2 *The case for $D[t;\sigma]$*

For $d > 1$, D is non-commutative by definition so the determinant of A_f is not well-defined in $M_m(D)$. In order to generalise [56, Theorem 3], we restrict

D to a associative division algebra containing a maximal splitting field E and consider the *left regular representation* of D as follows:

If D is a central simple algebra of degree d and E is a subfield of D such that $[E : F] = d$, then E is a *splitting field* for D. Let $\{v_1, v_2, ..., v_d\}$ be a basis for D over E. By [33, Theorem 1.6.17], there exists a representation $\rho : D \to M_d(E)$ by writing

$$v_i a = \sum_{j=1}^{d} \rho_{ij}(a) v_j, \quad 1 \leq i \leq d,$$

where $\rho : D \longrightarrow M_d(E)$ is an F-vector space monomorphism. As D is associative, ρ is a multiplicative map.

Define $\widetilde{A_f} = \rho(A_f) \in M_m(M_d(E)) = M_{md}(E)$, where ρ is extended entry-wise to matrices in $M_m(D)$, i.e.

$$\widetilde{A_f} = \begin{pmatrix} \rho(a_{11}) & \dots & \rho(a_{1m}) \\ \rho(a_{21}) & \dots & \rho(a_{2m}) \\ \vdots & \ddots & \vdots \\ \rho(a_{m1}) & \dots & \rho(a_{mm}) \end{pmatrix}.$$

Unless stated otherwise, we will assume that D is a cyclic algebra $(E/C, \gamma, a)$ with $[E : C] = d$. In addition to this, we place restrictions on σ: let σ have finite order $n > 1$ and $\sigma \circ \gamma = \gamma \circ \sigma$. Note that the second assumption here implies that $\sigma_{|E} \in \mathrm{Aut}(E)$. These restrictions allow us to deduce some properties of the minimal polynomial of $\widetilde{A_f}$:

Lemma 3.4.9. *Suppose $\sigma_{|E} \in \mathrm{Aut}(E)$ and $\sigma \circ \gamma = \gamma \circ \sigma$. Then the minimal polynomial of $\widetilde{A_f}$ lies in $\mathrm{Fix}(\sigma)[x]$.*

Proof. Let $G \in E[x]$ be the minimal polynomial of $\widetilde{A_f}$ and $G' = \sigma(G)$. Then

$$0 = \sigma(G(\widetilde{A_f})) = G'(\sigma(\widetilde{A_f})),$$

where σ is extended entrywise to $M_{dn}(E)$. So G' is a polynomial identity for $\sigma(\widetilde{A_f})$.

Extend $\rho : D \to M_d(E)$ to $M_m(E)$ by applying ρ entry-wise. As $\rho(\sigma^i(C_f))$ is a $dm \times dm$ matrix partitioned into $d \times d$ blocks for $0 \leq i < n$, $\rho(\sigma(C_f))\rho(C_f)$

can be similarly partitioned into $d \times d$ blocks where the $(i,j)^{th}$ submatrix of $\rho(\sigma(C_f))\rho(C_f)$ is given by

$$C_{ij} = \sum_k A_{ik}B_{kj},$$

where A_{ik} is the $(i,k)^{th}$ submatrix of $\rho(\sigma(C_f))$ and B_{kj} is the $(k,j)^{th}$ submatrix of $\rho(C_f)$ [21, Theorem 1.9.6]. For all $1 \leq i,j,k \leq m$, $A_{ik} = \rho(a_{ik})$ and $B_{kj} = \rho(b_{kj})$ for some $a_{ik}, b_{jk} \in E$ so

$$A_{ik}B_{kj} = \rho(a_{ik})\rho(b_{kj}) = \rho(a_{ik}b_{kj})$$

as ρ is multiplicative when restricted to E (we note that a_{ik} lies in E as $\sigma_{|E} \in \mathrm{Aut}(E)$). As ρ is additive, it follows that $C_{ij} = \rho(\sum_k a_{ik}b_{kj})$. As this is true for each submatrix C_{ij} of $\rho(\sigma(C_f))\rho(C_f)$, it follows that $\rho(\sigma(C_f))\rho(C_f) = \rho(\sigma(C_f)C_f)$ and

$$\widetilde{A_f} = \rho(\sigma^{n-1}(C_f))...\rho(\sigma(C_f))\rho(C_f).$$

Note that $\sigma(A_f) = C_f\sigma^{n-1}(C_f)...\sigma(C_f)$, so $\sigma(\widetilde{A_f})\rho(C_f) = \rho(C_f)\widetilde{A_f}$.
By [6, Lemma 1, p.546], it follows that $det(\rho(C_f)) = det((-1)^m\rho(f_0)) \neq 0$ so we conclude $\rho(C_f)$ is invertible in $M_{md}(E)$. Thus $\sigma(\widetilde{A_f}) = \rho(C_f)\widetilde{A_f}\rho(C_f)^{-1}$, i.e. $\sigma(\widetilde{A_f})$ is similar to $\widetilde{A_f}$. Similar polynomials have the same minimal polynomial so it follows that G is the minimal polynomial of $\sigma(\widetilde{A_f})$. This implies that G must divide G'. But G' is monic and of the same degree as G, so this can only occur if $G' = G$. Hence G is fixed by σ. □

As a consequence, if $G \in C[x]$ then it follows that $G \in F[x]$. This is required to show that G is equal to the minimal central left multiple of f:

Theorem 3.4.10. *Suppose $\sigma_{|E} \in \mathrm{Aut}(E)$ and $\sigma \circ \gamma = \gamma \circ \sigma$. Let $f \in R$ be a monic polynomial of degree m such that $(f,t)_r = 1$. Then the following hold:*
(i) G is the polynomial of lowest degree such that $G(A_f) = 0$.
(ii) Let $\sigma^n = id$ and $G \in C[x]$. Then the minimal central left multiple $h(t) = \hat{h}(t^n)$ of f, $\hat{h}(x) \in F[x]$, satisfies that $\hat{h}(x)$ is equal to the minimal polynomial of the matrix $\widetilde{A_f}$.

Proof. Let $G = \sum_{i=0}^{k} G_i x^i$ be the minimal polynomial of $\widetilde{A_f}$; that is, G is the monic polynomial of lowest degree such that $G(\widetilde{A_f}) = 0$. By Lemma 3.4.9, we have $G \in F[x]$.

(i) As ρ is F-linear, this yields that

$$0 = G(\widetilde{A_f}) = G(\rho(A_f)) = \rho(G(A_f)),$$

which implies that $G(A_f) = 0$ as ρ is injective. So G annihilates A_f. Further G is the polynomial of lowest degree in $F[x]$ that anihilates A_f: Suppose $H(x) \in F[x]$ is such that $H(A_f) = 0$ and $\deg(H) < \deg(G)$. As ρ is F-linear, we have

$$0 = \rho(H(A_f)) = H(\rho(A_f)) = H(\widetilde{A_f}),$$

so H annihilates $\widetilde{A_f}$. This contradicts the minimality of G.

(ii) We know that $\phi_f^n(v) = \sigma^n(v_\beta) \cdot A_f$ by Lemma 3.4.4. Since $\sigma^n = id$, we get $\phi_f^n(v) = v_\beta \cdot A_f$, and

$$\begin{aligned} 0 =& v_\beta \cdot G(A_f) \\ =& \sum_{i=0}^{k} G_i (v_\beta \cdot (A_f)^i) \\ =& \sum_{i=0}^{k} G_i ((\phi_f^n)^i(v)) \\ =& G((\phi_f^n)(v)). \end{aligned}$$

Note that here $v_\beta \cdot A_f = \sigma^n(v_\beta) \cdot A_f = \phi_f^n(v)$ (where we identify v with v_β), because $\sigma^n = id$.

By identifying v_β with $v \in R/Rf$, we conclude that $G(t^n)v = 0 \bmod_r f$. Letting $v = 1$ yields $G(t^n) = 0 \bmod_r f$, so f divides $G(t^n)$ on the right in R. By the definition of minimal central left multiple and employing that $G(t^n) \in Z(R)$, this implies that $\hat{h}(x)$ divides $G(x)$ in $F[x]$.

Conversely, for all $v \in R/Rf$,

$$\begin{aligned} 0 =& v\hat{h}(t^n) \bmod_r f \\ =& \hat{h}(t^n)v \bmod_r f \\ =& \hat{h}(\phi_f^n)(v), \end{aligned}$$

so $v_\beta \cdot \hat{h}(A_f) = 0$ for all $v_\beta \in D^m$. Hence we have $\hat{h}(A_f) = 0$. As G is the minimal polynomial of A_f, we conclude that $G(x)$ divides $\hat{h}(x)$ in $F[x]$: suppose that a is the greatest common divisor of G and $\hat{h}$. Then there exist $p, q \in F[x]$ such that $a = Gp + \hat{h}q$, so

$$a(A_f) = G(A_f)p(A_f) + \hat{h}(A_f)q(A_f) = 0 + 0 = 0.$$

If $a \neq G$, it follows that $\deg(a) < \deg(G)$ which contradicts the minimality of G.

It follows that $\hat{h}(x) = G(x)$ as required. □

For the remainder of this section, we assume that $\sigma^n = id$, $\sigma_{|E} \in \mathrm{Aut}(E)$ and $\sigma \circ \gamma = \gamma \circ \sigma$. Note that if $\sigma_{|E} \notin \mathrm{Aut}(E)$, it would be impossible to have $\sigma \circ \gamma = \gamma \circ \sigma$ unless $\gamma = id$. In addition to these assumptions, we also must assume the minimal polynomial of A_f lies in $C[x]$ in order to employ Theorem 3.4.10.

Lemma 3.4.11. *Let $f \in R$ be a monic polynomial of degree m such that $(f,t)_r = 1$. If $\deg(\hat{h}) = dm$, then $\hat{h}(x) = p_{\widetilde{A_f}}(x) = det(xI - \widetilde{A_f})$, the characteristic polynomial of $\widetilde{A_f}$.*

Proof. By Theorem 3.4.10, the minimal polynomial polynomial of $\widetilde{A_f}$ is equal to $\hat{h}(x) \in F[x]$ under our assumptions. As the minimal polynomial divides the characteristic polynomial, it follows that $\hat{h}(x)$ divides $p_{\widetilde{A_f}}(x)$. Because both $\hat{h}$ and $p_{\widetilde{A_f}}$ are monic polynomials of degree dm in $F[x]$, we conclude that they must be equal. □

If we now consider D to be a cyclic algebra $(E/C, \gamma, a)$ and impose the restrictions stated above, we can compute the characteristic polynomial of A_f and so the minimal central left multiple of f:

Theorem 3.4.12. *Let $D = (E/C, \gamma, a)$ be a cyclic algebra over C of degree d. Let $f = \sum_{i=0}^{m} f_i t^i \in E[t;\sigma] \subset R$ be monic and irreducible, such that $(f,t)_r = 1$ and $\hat{h} = mclm(f)$ has degree dm. Then*

$$N_{E/F}(f_0) = (-1)^{dm(n-1)} h_0,$$

where f_0 and h_0 are the constant terms of f and h respectively.

Proof. As $\deg(\hat{h}) = dm$ and $G \in F[x]$ by Lemma 3.4.9, we have $\hat{h}(x) = \det(xI - \widetilde{A_f})$ by Lemma 3.4.11. Hence the constant term of $\hat{h}$ is equal to $\det(-\widetilde{A_f}) = (-1)^{dm}\det(\widetilde{A_f})$.
Let $\rho : D \to M_d(E)$ be left regular representation of D. As rho is multiplicative, it follows that

$$\widetilde{A_f} = \rho(A_f) = \rho(\sigma^{n-1}(C_f)) \dots \rho(C_f).$$

If we assume σ and γ commute, then $\rho(\sigma(C_f)) = \sigma(\rho(C_f))$ and thus

$$\det(\widetilde{A_f}) = \sigma^{n-1}(\det(\rho(C_f))) \dots \det(\rho(C_f)).$$

As $f_i \in E$, we may calculate $\det(\rho(C_f))$ by first evaluating the determinant with entries in $M_d(E)$, then evaluating the determinant of the resulting $d \times d$ matrix [6]. This yields

$$\det(\rho(C_f)) = \det((-1)^{m-1}\rho(-f_0)) = \det((-1)^m\rho(f_0)) = (-1)^{dm}\det(\rho(f_0)).$$

As $f_0 \in E$, $\rho(f_0) \in M_d(E)$ is a $d \times d$ diagonal matrix given by

$$\begin{pmatrix} f_0 & 0 & \dots & 0 \\ 0 & \gamma(f_0) & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \dots & \gamma^{d-1}(f_0) \end{pmatrix}$$

so $\det(\rho(C_f)) = (-1)^{dm}N_{E/C}(f_0)$. Thus it follows

$$\det(\widetilde{A_f}) = \sigma^{n-1}((-1)^{dm}N_{E/C}(f_0)) \dots (-1)^{dm}N_{E/C}(f_0) = (-1)^{dmn}N_{C/F}(N_{E/C}(f_0))$$

and we conclude that

$$h_0 = (-1)^{dm+dmn}N_{E/F}(f_0) = (-1)^{dm(n-1)}N_{E/F}(f_0).$$

□

Corollary 3.4.13. *Let $D = (E/C, \gamma, a)$ be a cyclic algebra over C of degree d.*

Let $f = \sum_{i=0}^{m} f_i t^i \in E[t;\sigma] \subset R$ *be monic and irreducible of degree* m*, such that* $(f,t)_r = 1$*. Let* $\deg(\hat{h}) = dm$ *and suppose that all the polynomials similar to* f *lie in* $E[t;\sigma]$*. If* g *is a monic divisor of* h *in* R *of degree* lm*, then*

$$N_{E/F}(g_0) = N_{E/F}(a_0)^l.$$

Proof. We know that $h(t) = \hat{h}(t^n)$, with $\hat{h}(x)$ irreducible in $F[x]$, since we assume that f is irreducible and $u = 1$. Thus h is a t.s.m. element in Jacobson's terminology. Therefore the irreducible factors $f_1(t), \ldots, f_k(t)$ of any decomposition of $h(t)$ into irreducibles are all similar, and in fact are all similar to f, as f must be one of them by the definition of h. Now $g(t)$ is a monic divisor of h. Thus we can decompose $g(t)$ into a product of irreducible factors and up to similarity the irreducible factors of g will be the same as suitably chosen irreducible factors of h by [33, Theorem 1.2.9.]. Hence w.l.o.g. $g = f_1 f_2 \cdots f_l$, where the f_i are irreducibles in R and f_i is similar to f for all $i = 1, 2, \ldots, l$ [33, Theorem 1.2.19]. Thus by Corollary 3.2.7, the minimal central left multiple of each f_i is equal to h. Since f is monic, we may assume w.l.o.g. that all f_i are monic.

By Theorem 3.4.12 and since all f_i lie in $E[t;\sigma]$ by our assumption, this implies that $N_{E/F}(f_i(0)) = (-1)^{dm(n-1)} h_0 = N_{E/F}(a_0)$. As the constant term of g is equal to $\prod_{i=1}^{l} f_i(0)$ and the norm is multiplicative, we see that

$$N_{E/F}(g_0) = \prod_{i=1}^{l} N_{E/F}(f_i(0)) = [(-1)^{dm(n-1)} h_0]^l = (-1)^{ldm(n-1)} h_0^l = N_{E/F}(a_0)^l.$$

□

Although we obtain a generalisation of [56, Theorem 3] for $D = (E/C, \gamma, a)$, we have to implement the restrictions $\sigma \neq id$, $\sigma^n = id$, and $\sigma \circ \gamma = \gamma \circ \sigma$. In addition to this, we must assume that the minimal polynomial of A_f lies in $C[x]$. These assumptions, particularly the final assumption about the minimal polynomial, mean that the above results could be difficult to use in general examples. Due to this, we consider another method of determining the reducibility of the minimal central left multiple of f.

3.5 USING THE NORM OF A POLYNOMIAL

We now consider using the norm of $f(t)$ in order to deduce reducibility criteria for the minimal central left multiple. The results in this section form part of [51].

Let $R = D[t;\sigma]$ and

$$D(t;\sigma) = \{f/g \mid f \in D[t;\sigma], g \in C(D[t;\sigma]), g \neq 0\}$$

be the ring of central quotients of $D[t;\sigma]$. Then $x = u^{-1}t^n$ is a commutative indeterminate over D. The center of $D(t;\sigma)$ is

$$C(D(t;\sigma)) = \mathrm{Quot}(C(D[t;\sigma])) = F(x),$$

where $\mathrm{Quot}(S)$ denotes the quotient field of an integral domain S. Note that $C(D(t;\sigma))$ is a field. The ring $D(x)$ of central quotients of $D[x]$ is a subring of $D(t;\sigma)$.

$D(t;\sigma)$ is a central simple $F(x)$-algebra, more precisely,

$$D(t;\sigma) \cong (D(x), \widetilde{\sigma}, ux)$$

is a cyclic generalized crossed product [29, Theorem 2.3]. Here, $\widetilde{\sigma}$ denotes the extension of σ to $D(x)$ that fixes x [29, Lemma 2.1.].

Note that when regarding $D(t;\sigma)$ as an $F(x)$-algebra, the choice of u is lost: x depends on u, and different choices of u lead to different actions of $F(x)$ on $D(t;\sigma)$. Here and in the following we thus assume that u is fixed and $x = u^{-1}t^n$.

The algebra $D(t;\sigma)$ has center $F(x)$ and $\deg(D(t;\sigma)) = dn$. In particular, as D is a division algebra then $D(t;\sigma)$ is also a division algebra [29, Theorem 2.2.]. The reduced norm N of $(D(x), \widetilde{\sigma}, ux)$ is a nondegenerate form of degree dn over $F(x)$.

3.5.1 *The norm of $f(t)$*

As with in Section 3.4, we assume D is a associative division algebra over C with a subfield E such that $[E : C] = d$.

Theorem 3.5.1. *Let $f \in D[t;\sigma]$. Then:*
(i) $N(f) \in F[x]$,
(ii) f divides $N(f)$.

The proof works similarly as the one of [33, Proposition 1.7.1]:

Proof. (i) We have $[C : F] = n$, $[D(x) : F(x)] = d^2n$, and $[(D(x), \widetilde{\sigma}, ut) : F(x)] = d^2n^2$. The set $\{1, t, \ldots, t^{n-1}\}$ generates $D[t;\sigma]$ over $D[x]$; since $C(D[t;\sigma]) = F[x] \subset D[x]$, the set $\{1, t, \ldots, t^{n-1}\}$ also generates $D(t;\sigma)$ over $D(x)$. Additionally, $(D(x), \widetilde{\sigma}, ut)$ is a central simple algebra of degree dn over $F(x)$ with subalgebra $D(x)$. We regard $(D(x), \widetilde{\sigma}, ut)$ as a left module over its noncommutative subalgebra $D(x)$.

Furthermore, we have $I_t|_{D(x)} = \sigma$, where I_t denotes the inner automorphism $I_t : f(x) \mapsto tf(x)t^{-1}$, σ denotes the extension of σ to $D(x)$ fixing x, and $D(x) \subset C_{D(t;\sigma)}(D(x))$. It therefore follows by [29, Lemma 1.27] that $\{1, t, \ldots, t^{n-1}\}$ is free over $D(x)$, thus

$$D(t;\sigma) = \bigoplus_{i=0}^{n-1} D(x)t^i.$$

Since

$$D[t;\sigma] = \bigoplus_{i=0}^{n-1} D[x]t^i,$$

and $t^n = ux$, every $f \in R \subset (D(x), \widetilde{\sigma}, ut)$ can be written as a linear combination of $1, t, \ldots, t^{n-1}$ with coefficients in $D[x]$. We therefore obtain a representation ρ of $(D(x), \widetilde{\sigma}, ut)$ by matrices in $M_n(D(x))$ by writing

$$t^i f(t) = \sum_{j=0}^{n-1} \rho_{ij}(f(t))t^j$$

for all $f \in R \subset (D(x), \widetilde{\sigma}, ut)$ and $0 \leq i, j \leq n-1$. Hence the matrix $\rho(f(t))$ has entries in $D[x]$ for every $f \in R$. Since D has a subfield E of degree d, we can regard D as a left module over E. Let $\{v_1, \ldots, v_d\}$ be a basis for D over $E(x)$.

Then $\{v_1, \ldots, v_d, v_1 t, \ldots, v_d t, \ldots v_d t^{n-1}\}$ is a basis of $(D(x), \widetilde{\sigma}, ut) = D(t;\sigma)$ as a left module over E and we now analogously obtain a representation ρ of $(D(x), \widetilde{\sigma}, ut)$ by matrices in $M_{dn}(E(x))$ with respect to that basis.

For $f(t) \in R$, the matrix $\rho(f(t))$ has entries in $E[x]$, therefore it follows that

$$N(f(t)) = \det(\rho(f(t))) \in E[x] \cap F(x) = F[x].$$

(ii) Similarly as in (i), it can be shown that all the coefficients of the characteristic polynomial of $\rho(f(t))$ are contained in $F[x]$ (cf. also [45, Proposition, p. 295]). Define the reduced adjoint of f as $f(t)^\sharp$ (as defined in [33, (1.6.12)]); by definition, $f(t)^\sharp \in R$. Since $N(f(t)) = f(t)f(t)^\sharp = f(t)^\sharp f(t)$, it follows that $f(t)$ divides $N(f)$ in R. □

Let $f \in R = D[t;\sigma]$ have degree m and bound f^*. Since $N(f) \in F[x] = Z(R)$ is a left multiple of f by Lemma 3.5.1, we know that the bound f^* divides $N(f)$ in R, so that $\deg(f^*) \leq \deg(N(f))$.

Theorem 3.5.2. *Let D be a division algebra which has a subfield E of degree d. Then for any $f \in D[t;\sigma]$ of degree m, $N(f)$ has degree dm.*

Proof. Write $m = kn + r$ for some $0 \leq r < n$. Substituting $t^n = ux$, we obtain $f(t) = P_0(x) + P_1(x)t + \cdots + P_{n-1}(x)t^{n-1} \in D[x][t;\sigma]$ where

$$P_i(x) = \begin{cases} a_i + \cdots + a_{i+kn}(ux)^k & \text{for } i \leq r, \\ a_i + \cdots + a_{i+(k-1)n}(ux)^{k-1} & \text{for } i > r. \end{cases}$$

Computing the left regular representation of $\rho : D[t;\sigma] \to M_n(D(x))$, we have

$$\rho(f(t)) = \begin{pmatrix} Q_{1,1}(x) & \cdots & Q_{1,n}(x) \\ \vdots & & \vdots \\ Q_{n,1}(x) & \cdots & Q_{n,n}(x) \end{pmatrix}$$

for some $Q_{i,j}(x) \in D[x]$ satisfying

$$t^{i-1} f = \sum_{j=1}^{n} Q_{ij}(x) t^{j-1}, \qquad 1 \leq i \leq n,$$

[33, Proposition 1.6.9]. Moreover, it follows that

$$\deg(Q_{i,j}) = \begin{cases} \deg(P_{j-i}) & \text{for } i \leq j, \\ \deg(P_{n+j-i}) + 1 & \text{for } i > j. \end{cases}$$

Comparing the above equation with the expressions for $P_i(x)$, it follows that

$$\deg(Q_{i,j}) \leq \begin{cases} k-1 & \text{for } i \leq j \text{ and } j-i > r, \\ k & \text{for } i \leq j \leq r+i \text{ or } j < i < n-r+j, \\ k+1 & \text{for } i > j \text{ and } i-j \geq n-r. \end{cases}$$

with $Q_{i,j}(x) = \sigma^{i-1}(a_m)u^k x^k + \dots$ for $j-i = r$ and $Q_{i,j}(x) = \sigma^{i-1}(a_m)u^{k+1}x^{k+1} + \dots$ for $i-j = n-r$.

This means the bottom left $r \times r$ minor of $\rho(f(t))$ has elements of degree at most $k+1$ in lower triangular entries (including the diagonal which attains this maximum degree) and the top right $n-r \times n-r$ minor of $\rho(f(t))$ has elements of degree at most $k-1$ in the upper triangular entries (excluding the diagonal which has elements of exactly degree k). Every other element of $\rho(f(t))$ has degree at most k.

As D has a subfield of degree d, there exists a left regular representation $\omega : D \to M_d(E)$ which extends to $D[x]$ by setting $\omega(x) = xId$. The $d \times d$ block matrices representing $Q_{i,j}(x)$ are inserted for every entry $Q_{i,j}(x)$ in $\rho(f(t))$ to obtain a representation for $D[t;\sigma]$ in $M_{dn}(E[x])$.

As ω is additive and $\omega(x)$ is a diagonal matrix, then

$$\omega(\sigma^j(g(x))) = \omega(\sigma^j(g_k)u^k)(xId)^k + \cdots + \omega(\sigma^j(g_0))$$

for any polynomial $g(x) = \sum_{i=0}^{k} g_i x^i \in D[x]$. As we are computing the determinant only to find the degree of $N(f(t))$, it is sufficient to only consider the term of highest degree in $Q_{i,j}(x)$ and ignore all terms of lower degree. We truncate $Q_{i,j}(x)$ at the highest term and apply ω to all the entries of the matrix. To determine the term of highest degree, we expand the determinant along the columns and consider only the portion of the determinant expansion which yields the maximum possible degree. As $\omega(a_m u^k) = \omega(a_m)\omega(u)^k$ is

invertible, there are no zero columns in $\omega(a_m u^k)$ so it is always possible to find an expansion of the matrix yielding the highest degree. Hence the degree of $N(f(t))$ is at most

$$dr(k+1) + d(n-r)k = d(kn+r) = dm.$$

We wish to show the coefficient of x^{dm} in $N(f(t))$ is non-zero. Following the expansion of $\omega \circ \rho(f(t))$ and ignoring any terms of degree less than dm, it follows that the coefficient of x^{dm} is equal to

$$\pm \det(\omega(a_m u^k))\det(\omega(\sigma(a_m u^k)) \cdots \det(\omega(\sigma^{n-r-1}(a_m u^k))\det(\omega(\sigma^{n-r}(a_m u^{k+1})) \cdots \det(\omega(\sigma^{n-1}(a_m u^{k+1})).$$

As σ is an automorphism, it follows that $\det(\omega(\sigma^i(a_m u^k)) \neq 0$ by our assumption on $\omega(a_m u^k)$. Thus it follows that the coefficient of x^{dm} is non-zero and

$$\deg(N(f(t)) = dm.$$

□

Example 3.5.3. We show the details of the above calculations for $d = 2$, $n = 3$ and $m = 7$; an actual computation of the matrix becomes difficult for arbitrary d, n, m. For $f(t) = a_0 + a_1 t + \cdots + a_7 t^7 \in D[t; \sigma]$, where we assume D has a subfield E of degree d, and $t^3 = ux$, it follows that $\rho(f(t))$ is equal to

$$\begin{pmatrix} a_0 + a_3ux + a_6u^2x^2 & a_1 + a_4ux + a_7u^2x^2 & a_2 + a_5ux \\ \sigma(a_2ux + a_5u^2x^2) & \sigma(a_0 + a_3ux + a_6u^2x^2) & \sigma(a_1 + a_4ux + a_7u^2x^2) \\ \sigma^2(a_1ux + a_4u^2x^2 + a_7u^3x^3) & \sigma^2(a_2ux + a_5u^2x^2) & \sigma^2(a_0 + a_3ux + a_6u^2x^2) \end{pmatrix}.$$

Truncating the polynomials in the matrix at the highest terms and applying $\omega : D \to M_2(E)$, we have

$$\begin{pmatrix} \omega(a_6u^2x^2) & \omega(a_7u^2x^2) & \omega(a_5ux) \\ \omega(\sigma(a_5u^2)x^2) & \omega(\sigma(a_6u^2)x^2) & \omega(\sigma(a_7u^2)x^2) \\ \omega(\sigma^2(a_7u^3)x^3) & \omega(\sigma^2(a_5u^2)x^2) & \omega(\sigma^2(a_6u^2)x^2) \end{pmatrix}$$

$$= \begin{pmatrix} a_{1,1}^{(1,1)}x^2 & a_{1,1}^{(1,2)}x^2 & a_{1,2}^{(1,1)}x^2 & a_{1,2}^{(1,2)}x^2 & a_{1,3}^{(1,1)}x & a_{1,3}^{(1,2)}x \\ a_{1,1}^{(2,1)}x^2 & a_{1,1}^{(2,2)}x^2 & a_{1,2}^{(2,1)}x^2 & a_{1,2}^{(2,2)}x^2 & a_{1,3}^{(2,1)}x & a_{1,3}^{(2,2)}x \\ a_{2,1}^{(1,1)}x^2 & a_{2,1}^{(1,2)}x^2 & a_{2,2}^{(1,1)}x^2 & a_{2,2}^{(1,2)}x^2 & a_{2,3}^{(1,1)}x^2 & a_{2,3}^{(1,2)}x^2 \\ a_{2,1}^{(2,1)}x^2 & a_{2,1}^{(2,2)}x^2 & a_{2,2}^{(2,1)}x^2 & a_{2,2}^{(2,2)}x^2 & a_{2,3}^{(2,1)}x^2 & a_{2,3}^{(2,2)}x^2 \\ a_{3,1}^{(1,1)}x^3 & a_{3,1}^{(1,2)}x^3 & a_{3,2}^{(1,1)}x^2 & a_{3,2}^{(1,2)}x^2 & a_{1,3}^{(1,1)}x^2 & a_{3,3}^{(1,2)}x^2 \\ a_{3,1}^{(2,1)}x^3 & a_{3,1}^{(2,2)}x^3 & a_{3,2}^{(2,1)}x^2 & a_{3,2}^{(2,2)}x^2 & a_{1,3}^{(2,1)}x^2 & a_{3,3}^{(2,2)}x^2 \end{pmatrix},$$

for some $a_{k,l}^{(i,j)} \in E$ for $i,j \in \{1,2\}$ and $k,l \in \{1,2,3\}$. Then the determinant of the above matrix is equal to

$$a_{3,1}^{(1,1)}x^3 \begin{vmatrix} a_{1,1}^{(1,2)}x^2 & a_{1,2}^{(1,1)}x^2 & a_{1,2}^{(1,2)}x^2 & a_{1,3}^{(1,1)}x & a_{1,3}^{(1,2)}x \\ a_{1,1}^{(2,2)}x^2 & a_{1,2}^{(2,1)}x^2 & a_{1,2}^{(2,2)}x^2 & a_{1,3}^{(2,1)}x & a_{1,3}^{(2,2)}x \\ a_{2,1}^{(1,2)}x^2 & a_{2,2}^{(1,1)}x^2 & a_{2,2}^{(1,2)}x^2 & a_{2,3}^{(1,1)}x^2 & a_{2,3}^{(1,2)}x^2 \\ a_{2,1}^{(2,2)}x^2 & a_{2,2}^{(2,1)}x^2 & a_{2,2}^{(2,2)}x^2 & a_{2,3}^{(2,1)}x^2 & a_{2,3}^{(2,2)}x^2 \\ a_{3,1}^{(2,2)}x^3 & a_{3,2}^{(2,1)}x^2 & a_{3,2}^{(2,2)}x^2 & a_{1,3}^{(2,1)}x^2 & a_{3,3}^{(2,2)}x^2 \end{vmatrix}$$

$$- a_{3,1}^{(2,1)}x^3 \begin{vmatrix} a_{1,1}^{(1,2)}x^2 & a_{1,2}^{(1,1)}x^2 & a_{1,2}^{(1,2)}x^2 & a_{1,3}^{(1,1)}x & a_{1,3}^{(1,2)}x \\ a_{1,1}^{(2,2)}x^2 & a_{1,2}^{(2,1)}x^2 & a_{1,2}^{(2,2)}x^2 & a_{1,3}^{(2,1)}x & a_{1,3}^{(2,2)}x \\ a_{2,1}^{(1,2)}x^2 & a_{2,2}^{(1,1)}x^2 & a_{2,2}^{(1,2)}x^2 & a_{2,3}^{(1,1)}x^2 & a_{2,3}^{(1,2)}x^2 \\ a_{2,1}^{(2,2)}x^2 & a_{2,2}^{(2,1)}x^2 & a_{2,2}^{(2,2)}x^2 & a_{2,3}^{(2,1)}x^2 & a_{2,3}^{(2,2)}x^2 \\ a_{3,1}^{(1,2)}x^3 & a_{3,2}^{(1,1)}x^2 & a_{3,2}^{(1,2)}x^2 & a_{1,3}^{(1,1)}x^2 & a_{3,3}^{(1,2)}x^2 \end{vmatrix} + \dots$$

where other terms of the expansion would yield terms of lower degree. Continuing

the expansion along the next column and only considering terms of highest degree, we obtain

$$a_{3,1}^{(1,1)}a_{3,1}^{(2,2)}x^6\begin{vmatrix} a_{1,2}^{(1,1)}x^2 & a_{1,2}^{(1,2)}x^2 & a_{1,3}^{(1,1)}x & a_{1,3}^{(1,2)}x \\ a_{1,2}^{(2,1)}x^2 & a_{1,2}^{(2,2)}x^2 & a_{1,3}^{(2,1)}x & a_{1,3}^{(2,2)}x \\ a_{2,2}^{(1,1)}x^2 & a_{2,2}^{(1,2)}x^2 & a_{2,3}^{(1,1)}x^2 & a_{2,3}^{(1,2)}x^2 \\ a_{2,2}^{(2,1)}x^2 & a_{2,2}^{(2,2)}x^2 & a_{2,3}^{(2,1)}x^2 & a_{2,3}^{(2,2)}x^2 \end{vmatrix}$$

$$-a_{3,1}^{(2,1)}a_{3,1}^{(1,2)}x^6\begin{vmatrix} a_{1,2}^{(1,1)}x^2 & a_{1,2}^{(1,2)}x^2 & a_{1,3}^{(1,1)}x & a_{1,3}^{(1,2)}x \\ a_{1,2}^{(2,1)}x^2 & a_{1,2}^{(2,2)}x^2 & a_{1,3}^{(2,1)}x & a_{1,3}^{(2,2)}x \\ a_{2,2}^{(1,1)}x^2 & a_{2,2}^{(1,2)}x^2 & a_{2,3}^{(1,1)}x^2 & a_{2,3}^{(1,2)}x^2 \\ a_{2,2}^{(2,1)}x^2 & a_{2,2}^{(2,2)}x^2 & a_{2,3}^{(2,1)}x^2 & a_{2,3}^{(2,2)}x^2 \end{vmatrix}+\dots$$

$$=(a_{3,1}^{(1,1)}a_{3,1}^{(2,2)}-a_{3,1}^{(2,1)}a_{3,1}^{(1,2)})x^6\begin{vmatrix} a_{1,2}^{(1,1)}x^2 & a_{1,2}^{(1,2)}x^2 & a_{1,3}^{(1,1)}x & a_{1,3}^{(1,2)}x \\ a_{1,2}^{(2,1)}x^2 & a_{1,2}^{(2,2)}x^2 & a_{1,3}^{(2,1)}x & a_{1,3}^{(2,2)}x \\ a_{2,2}^{(1,1)}x^2 & a_{2,2}^{(1,2)}x^2 & a_{2,3}^{(1,1)}x^2 & a_{2,3}^{(1,2)}x^2 \\ a_{2,2}^{(2,1)}x^2 & a_{2,2}^{(2,2)}x^2 & a_{2,3}^{(2,1)}x^2 & a_{2,3}^{(2,2)}x^2 \end{vmatrix}+\dots.$$

Comparing this to the matrix in terms of ω, it follows that this is equal to

$$\det(\omega(\sigma^2(a_7u^3))x^6\begin{vmatrix} \omega(a_7u^2x^2) & \omega(a_5ux) \\ \omega(\sigma(a_6u^2)x^2) & \omega(\sigma(a_7u^2)x^2) \end{vmatrix}+\dots.$$

Repeating this with the remaining block matrices, it follows that we have

$$N(f(t))=\det(\omega(\sigma^2(a_7u^3))\det(\omega(\sigma(a_7u^2))\det(\omega(a_7u^2))x^{14}+\text{ terms of lower degree.}$$

We can now relate the norm of f to its minimal central left multiple:

Corollary 3.5.4. *If* $\deg(h)=dmn$, *then* $\hat{h}(x)=\alpha N(f)$ *for some* $\alpha\in D^\times$, *where* α *is equal to*

$$\pm det(\omega(a_mu^k))\,det(\omega(\sigma(a_mu^k))\cdots det(\omega(\sigma^{n-r-1}(a_mu^k))\,det(\omega(\sigma^{n-r}(a_mu^{k+1}))\cdots det(\omega(\sigma^{n-1}(a_mu^{k+1})).$$

i.e. $N(f)$ *is equal to the bound of* f.

3.5.2 *Determining divisors of $N(f)$ in $D[t;\sigma]$*

We can use the method used in the proof of Theorem 3.5.2 to determine both the lead and constant term of $N(f(t))$ in some cases. For small d, n and m, we could compute the determinant of this matrix by hand for any D and polynomial f, given the representation $\omega : D \to M_d(E)$, as shown in Example 3.5.3. However, for larger examples the huge determinant calculations are too time-consuming to be practical. Instead, we restrict to a specific case D and $f \in R$ to obtain some more general results.

From now on, we assume that

$$D = (E/C, \gamma, a) \text{ is a cyclic algebra over } C \text{ of degree } d,$$

$$\sigma|_E \in \mathrm{Aut}(E) \text{ such that } \gamma \circ \sigma = \sigma \circ \gamma \text{ and } u \in E.$$

Then $\sigma|_E$ has order n. Write $m = kn + r$ for some $0 \leq r < n$.

Theorem 3.5.5. *For $f(t) = a_0 + a_1 t + \cdots + a_m t^m \in E[t;\sigma] \subset D[t;\sigma]$, we have*

$$N(f(t)) = N_{E/F}(a_0) + \cdots + (-1)^{dr(n-1)} N_{E/F}(a_m) N_{E/C}(u)^m x^{dm}.$$

Proof. The proof follows similarly to the proof of Theorem 3.5.2. As the entries of $\rho(f(t))$, $Q_{i,j}(x) \in D[x]$, are determined by the relation $t^{i-1} f = \sum_{j=1}^{n} Q_{ij}(x) t^{j-1}$, $1 \leq i \leq n$, it follows that

$$\rho(f(t)) = \begin{pmatrix} P_0(x) & P_1(x) & \cdots & P_{n-1}(x) \\ \sigma(P_{n-1}(x))ux & \sigma(P_0(x)) & \cdots & \sigma(P_{n-2}(x)) \\ \vdots & \ddots & & \vdots \\ \sigma^{n-m}(P_r(x))ux & & \ddots & \sigma^{n-m}(P_{r-1}(x)) \\ \vdots & & \ddots & \vdots \\ \sigma^{n-1}(P_1(x))ux & \sigma^{n-1}(P_2(x))ux & \cdots & \sigma^{n-1}(P_0(x)) \end{pmatrix},$$

where $P_i(x) \in E[x]$ for all i. Let $\{v_1, \ldots, v_d\}$ be a canonical basis for D as a left E-module. Then

$$\{v_1, \ldots, v_d, v_1 t, \ldots, v_d t, \ldots v_d t^{n-1}\}$$

is a basis of $(D(x), \widetilde{\sigma}, ut)$ as a left module over $E(x)$ and we now analogously obtain a representation ρ of $(D(x), \widetilde{\sigma}, ut)$ by matrices in $M_{dn}(E(x))$ with respect to that basis. This representation is given by an $nd \times nd$ matrix obtained as follows:

Let ω be the representation of A in $M_d(E)$ which is extended to a representation of $A[x]$ in $M_d(E[x])$ by setting $\omega(x) = xI_d$. The $d \times d$ block matrices representing the entries of $\rho(f(t))$ are inserted for every entry of the previous $n \times n$ matrix (cf. for instance [45, p. 298]) with σ extended to $M_d(E)$ by acting entry-wise. For all $a \in E$, the matrix $\omega(a) \in M_d(E)$ is a $d \times d$ diagonal matrix given by

$$\begin{pmatrix} a & 0 & \dots & 0 \\ 0 & \gamma(a) & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \dots & \gamma^{d-1}(a) \end{pmatrix}.$$

As a consequence, we note that $\omega(a_i x) = \omega(a_i)\omega(x) = \omega(a_i)(xI_d)$ and $\omega(a_i a_j) = \omega(a_i)\omega(a_j)$ for all $a_i, a_j \in E$. We extend ω to a representation of $M_n(D)$, where $\omega \circ \rho(f(t))$ is equal to

$$\begin{pmatrix} \omega(P_0(x)) & \omega(P_1(x)) & \cdots & \omega(P_{n-1}(x)) \\ \omega(\sigma(P_{n-1})(x))\omega(u)xId & \omega(\sigma(P_0(x))) & \cdots & \omega(P_{n-2}(x)) \\ \vdots & \ddots & & \vdots \\ \omega(\sigma^{n-m}(P_r(x)))\omega(u)xId & & \ddots & \omega(\sigma^{n-m}(P_{r-1}(x))) \\ \vdots & & \ddots & \vdots \\ \omega(\sigma^{n-1}(P_1(x)))\omega(u)xId & \omega(\sigma^{n-1}(P_2(x)))\omega(u)xId & \cdots & \omega(\sigma^{n-1}(P_0(x))) \end{pmatrix}.$$

Hence $\omega \circ \rho(f(t))$ is a $dn \times dn$ matrix in $M_{dn}(E[x])$.

As the $\omega(\sigma^j(P_i(x)))$ are pairwise commutative matrices, we may calculate the determinant of $\omega \circ \rho(f(t))$ by first evaluating the $n \times n$ determinant with entries in $M_d(E)$, then evaluating the resulting $d \times d$ matrix which has entries in E [6, Lemma 1, p. 546]. Thus we obtain $\det(\omega \circ \rho(f(t))) = \det(H)$, where

$$\begin{aligned} H =& \omega(P_0(x))\sigma(\omega(P_0(x)))\dots\sigma^{n-1}(\omega(P_0(x))) + \dots \\ &+ (-1)^{r(n-r)}\omega(P_r(x))\sigma(\omega(P_r(x)))\dots\sigma^{n}(\omega(P_r(x)))\omega(u)^r(xI_d)^r. \end{aligned}$$

As each $\omega(P_i(x))$ is a diagonal matrix in $M_d(E)$ for all $0 \leq i \leq n-1$, H is the diagonal matrix in $M_d(E)$ given by the entries

$$\begin{aligned} H_{ii} =& \gamma^{i-1}[P_0(x)\sigma(P_0(x))\dots\sigma^{n-1}(P_0(x)) + \dots \\ &+(-1)^{r(n-1)}P_r(x)\sigma(P_r(x))\dots\sigma^{n-1}(P_r(x))u^r]x^r. \end{aligned}$$

Hence

$$\begin{aligned} \det(H) = \prod_{i=1}^{d} & \gamma^{i-1}[P_0(x)\sigma(P_0(x))\dots\sigma^{n-1}(P_0(x)) + \dots \\ &+(-1)^{m(n-1)}P_r(x)\sigma(P_r(x))\dots\sigma^{n-1}(P_r(x))u^r x^r)]. \end{aligned}$$

We obtain the constant term of $N(f(t))$ by substituting $x = 0$. Thus the constant term equals

$$\prod_{i=1}^{d} \gamma^{i-1}(a_0\sigma(a_0)\dots\sigma^{n-1}(a_0)) = \prod_{i=1}^{n} \sigma^{i-1}(a_0\gamma(a_0)\dots\gamma^{d-1}(a_0)),$$

since γ commutes with σ. As $a_0 \in E$, this is equal to $\prod_{i=1}^{n} \sigma^{i-1}(N_{E/C}(a_0)) = N_{C/F}(N_{E/C}(a_0)) = N_{E/F}(a_0)$. Similarly, the leading term of $N(f(t))$ is given by the leading term of

$$\prod_{i=1}^{d} \gamma^{i-1}[(-1)^{r(n-1)}P_r(x)\sigma(P_r(x))\dots\sigma^{n-1}(P_r(x))u^r x^r],$$

which is given by

$$\begin{aligned} &\prod_{i=1}^{d} \gamma^{i-1}[(-1)^{r(n-1)}a_m\sigma(a_m)\dots\sigma^{n-1}(a_m)u^r(ux)^{kn}x^r)] \\ =&(-1)^{dr(n-1)}\left[\prod_{i=1}^{d} \gamma^{i-1}(a_m\sigma(a_m)\dots\sigma^{n-1}(a_m))\right] N_{E/C}(u)^{kn+r}x^{d(kn+r)} \end{aligned}$$

since $u \in E$. As σ and γ commute and $a_m \in E$, we can express this as

$$\begin{aligned} &(-1)^{dr(n-1)}\left[\prod_{i=1}^{n} \sigma^{i-1}(a_m\gamma(a_m)\dots\gamma^{d-1}(a_m))\right] N_{E/C}(u)^{kn+r}x^{d(kn+r)} \\ =&(-1)^{dr(n-1)}\left[\prod_{i=1}^{n} \sigma^{i-1}(N_{E/C}(a_m))\right] N_{E/C}(u)^{kn+r}x^{d(kn+r)} \\ =&(-1)^{dr(n-1)}N_{C/F}(N_{E/C}(a_m))N_{E/C}(u)^{kn+r}x^{d(kn+r)}. \end{aligned}$$

As $kn + r = m$, this implies the assertion. □

Remark 3.5.6. As $\sigma \circ \gamma = \gamma \circ \sigma$, it follows that

$$\sigma(N_{E/C}(u)) = \sigma(\prod_{i=1}^{d} \gamma^{i-1}(u)) = \prod_{i=1}^{d} \gamma^{i-1}(\sigma(u)).$$

Because $u \in \mathrm{Fix}(\sigma)$, we conclude that

$$\sigma(N_{E/C}(u)) = \prod_{i=1}^{d} \gamma^{i-1}(u) = N_{E/C}(u),$$

so $N_{E/C}(u) \in C \cap \mathrm{Fix}(\sigma) = F$. This confirms that $N(f(t)) \in F[x]$ in this case as expected.

Hence we obtain the following results:

Corollary 3.5.7. *Let $D = (E/C, \gamma, a)$ be a cyclic algebra over C of degree d such that $u \in E$ and $\gamma \circ \sigma = \sigma \circ \gamma$. Let $f(t) = a_0 + a_1 t + \cdots + a_m t^m \in E[t;\sigma] \subset D[t;\sigma]$ be a polynomial such that $(f,t)_r = 1$ and $\deg(h) = dmn$. Then*

$$N(f) = (-1)^{dr(n-1)} N_{E/F}(a_m) N_{E/C}(u)^m \hat{h}$$

and

$$N_{E/F}(a_0) = (-1)^{dr(n-1)} N_{E/F}(a_m) N_{E/C}(u)^m h_0,$$

where h_0 denotes the constant term of $\hat{h}$.

Corollary 3.5.8. *Let $D = (E/C, \gamma, a)$ be a cyclic algebra over C of degree d such that $u \in E$ and $\sigma \circ \gamma = \gamma \circ \sigma$. Let $f = \sum_{i=0}^{m} a_i t^i \in E[t;\sigma] \subset R$ be monic and irreducible of degree m, such that $(f,t)_r = 1$. Let $\deg(\hat{h}) = dm$ and suppose that all the polynomials similar to f lie in $E[t;\sigma]$. If g is a monic divisor of h in R of degree lm, then*

$$N_{E/F}(g_0) = N_{E/F}(a_0)^l = (-1)^{dr(n-1)l} N_{E/C}(u)^{lm} h_0^l.$$

We note that these are analogous conditions to the ones obtained via semi-linear maps; however, we no longer have to assume that $\sigma^n = id$. In addition to this, we were previously restricted by the intractable condition that the minimal polynomial of A_f must lie in $C[x]$. The method of using the norm of $D(t;\sigma)$ is significantly less restrictive and could even be used for any division algebra D with a maximal subfield E (not only for cyclic algebras), as shown in Example 3.5.3.

3.5.3 *The case for $K[t;\sigma]$*

This approach also recovers the results of Section 3.4.1 when $R = K[t;\sigma]$.

Theorem 3.5.9. *Let $f(t) = a_0 + a_1 t + \cdots + a_m t^m$ have degree m. Then*

$$N(f(t)) = N_{K/F}(a_0) + \cdots + (-1)^{m(n-1)} N_{K/F}(a_m) x^m.$$

This is the generalized and corrected version of [33, Proposition 1.7.1 (ii)], which stated $(-1)^{mn} N_{K/F}(a_m) x^m$ for the leading term, and also required $m < n$. Furthermore, our proof fixes a small mistake in the proof of [13, Lemma 2.1.15].

Proof. Write $f(t) = a_0 + a_1 t + \cdots + a_m t^m$ as $f(t) = P_0(x) + P_1(x)t + \cdots + P_{n-1}(x)t^{n-1}$ with $P_i(x) \in K[x]$. We can use verbatim the same proof as given in [13, Lemma 2.1.15] to obtain the matrix in $M_n(K[x])$ representing the left multiplication $\rho(f(t))$ with respect to the basis $1, t, \ldots, t^{n-1}$: we have

$$\rho(f(t)) = \begin{pmatrix} P_0 & X\sigma(P_{n-1}) & \cdots & & & X\sigma^{n-1}(P_1) \\ P_1 & \sigma(P_0) & \cdots & & \cdots & \\ \vdots & & \ddots & & & \vdots \\ & & & \ddots & & \\ & & & & \ddots & \\ \vdots & & & & \ddots & X\sigma^{n-1}(P_{n-1}) \\ P_{n-1} & & \cdots & & \cdots & \sigma^{n-1}(P_0) \end{pmatrix}.$$

Thus $N(f(t))$, which is the determinant of this matrix, has as constant term the constant term of $P_0(x)\sigma(P_0(x))\cdots\sigma^{n-1}(P_0(x))$, which is $a_0(x)\sigma(a_0(x))\cdots\sigma^{n-1}(a_0(x)) = N_{K/F}(a_0)$. There are unique integers k, r, $0 \le r \le n-1$, such that we can write m as $m = kn + r$. In the sum giving the determinant of this matrix, the term of highest degree is

$$(-1)^{m(n-1)} P_r(x)\sigma(P_r(x))\cdots\sigma^{n-r-1}(P_r(x))\sigma^{n-r}(P_r(x))\cdots\sigma^{n-1}(P_r(x))X^r.$$

It has degree $m = k(n-r) + (k+1)r = kn + r$ as polynomial in x. (The proof of [13, Lemma 2.1.15] forgot to include the factor $(-1)^{m(n-1)}$ here.) Therefore

$N(f(t))$ has as highest term the highest term of this sum. The highest term is thus given by $(-1)^{m(n-1)}a_m\sigma(a_m)\cdots\sigma^{n-1}(a_m) = (-1)^{m(n-1)}N_{K/F}(a_m)$. □

Corollary 3.5.10. *Let $f \in R$ be monic and irreducible of degree m such that $(f,t)_r = 1$ and $\deg(\hat{h}) = m$. If g is a monic divisor of h in R of degree lm, then*

$$N_{E/F}(g_0) = N_{E/F}(a_0)^l = (-1)^{m(n-1)l}N_{E/F}(a_m)^l h_0^l.$$

3.6 CONDITIONS TO OBTAIN DIVISION ALGEBRAS AND MRD CODES

We apply the results about the minimal central left multiple via the norm of $f(t)$ to determine some conditions to obtain division algebras.

3.6.1 *For $D[t;\sigma]$ where D is a cyclic algebra*

We recall when we obtain generalised maximum rank distance codes, as determined in Theorem 3.3.11.

Theorem 3.6.1 (Theorem 3.3.11)**.** *$S_{n,m,l}(\nu,\rho,f) = \{a + Rh \mid a \in A\} \subset R/Rh$, where*

$$A = \{a_0 + a_1 t + \cdots + a_{lm-1}t^{lm-1} + \nu\rho(a_0)t^{lm} : a_i \in D\}$$

yields an MRD-code if and only there are no elements $g \in S_{n,m,l}(\nu,\rho,f)$ of degree lm which can be written as $g = \prod_{i=1}^{l} f_i$, where f_i is similar to f for all i, i.e. there are no divisors of h of degree lm in A.

We note that this always holds if $\nu = 0$. When $\nu \neq 0$, the results obtained about divisors of h in the previous sections allow us to improve this statement. Using the results about the norm of $(D(x), \tilde{\sigma}, ux)$, we have the following:

Theorem 3.6.2. *(for $f \in K[t;\sigma]$, K a finite field, cf. [56, Theorem 7]) Let $D = (E/C, \gamma, a)$ be a cyclic division algebra over C of degree d such that $\sigma|_E \in \mathrm{Aut}(E)$ and $\gamma \circ \sigma = \sigma \circ \gamma$. Suppose that $\sigma^n(z) = u^{-1}zu$ with $u \in E$.*

Let $f(t) = a_0 + a_1 t + \cdots + t^m \in E[t;\sigma] \subset R = D[t;\sigma]$ *be monic irreducible,* $(f,t)_r = 1$*, and let the minimal central left multiple* h *of* f *have* $\deg(h) = dmn$*. Suppose that all monic* f_i *similar to* f *lie in* $E[t;\sigma]$*. Then the set*

$$S_{n,m,l}(\nu,\rho,f) = \{a + Rh \,|\, a \in A\} \subset R/Rh,$$

where

$$A = \{a_0 + a_1 t + \cdots + a_{lm-1}t^{lm-1} + \nu\rho(a_0)t^{lm} : a_i \in D\},$$

defines an F'*-linear MRD code in* $M_{dn}(E_{\hat{h}})$ *with minimum distance* $dn - l + 1$*,* $l < dn$*, if one of the following holds:*
(i) $\nu = 0$
(ii) $\nu \notin E$ *and* $\rho|_E \in \mathrm{Aut}(E)$*.*
(iii) $\nu \in E$*,* $\rho|_E \in \mathrm{Aut}(E)$ *and*

$$N_{E/F'}(\nu)N_{E/F'}(a_0)^l \neq 1.$$

This is equivalent to $N_{E/F'}(\nu)N_{F/F'}((-1)^{dlm(n-1)}N_{E/C}(u)^{lm}h_0^l) \neq 1$*.*

Note that our global assumption that $\sigma^n(z) = u^{-1}zu$ for all $z \in D$, so that $\sigma^n(e) = u^{-1}eu = e$ for all $e \in E$, forces $(\sigma|_E)^n = id$.

Proof. Let $\mathcal{C}$ be the code defined by $S_{n,m,l}(\nu,\rho,f)$. As A has dimension $d^2nml[F : F']$ over F', this implies that $\mathcal{C} \subset M_{dn}(E_{\hat{h}})$ has dimension $d^2nml[F : F']$ over F'. The Singleton-like bound implies that the largest possible minimum distance of $\mathcal{C}$ is equal to $dn - l + 1$, so $S_{n,m,l}(\nu,\rho,f)$ defines an MRD-code if the set A does not contain a divisor of h of degree lm.
Suppose that A contains a divisor g of h of degree lm. If $\nu = 0$, this is a contradiction as $\deg(g) \leq lm - 1$. So assume $\nu \neq 0$. Let $g_m t^m$ be the highest coefficient of g, so that $g_m^{-1}g$ is a monic divisor of h. Then $g_m^{-1}g = f_1 \ldots f_l$ for some irreducible $f_i \in D[t;\sigma]$ similar to f. Without loss of generality, we may assume all f_i are monic (as $g_m^{-1}g$ is monic). Additionally, as f_i are similar to f and all monic polynomials similar to f lies in $E[t;\sigma]$ by assumption, it follows that $g_m^{-1}g \in E[t;\sigma]$. Suppose $\nu \notin E$ and $\rho(E) \subset E$. Since the coefficients of the g_i all lie in E we have $g_m \neq \nu\rho(g_0)$ which yields a contradiction, and so

there is no divisor g of h in A.

Suppose that $\nu \in E^\times$ and $\rho(E) \subset E$. By Theorems 3.5.8 and since $g_m^{-1}g$ lies in $E[t;\sigma]$, this implies

$$N_{E/F}(g_m^{-1}g_0) = (-1)^{dlm(n-1)}N_{E/C}(u)^{lm}h_0^l = N_{E/F}(a_0)^l,$$

and in particular, that g_0 and g_m are both non-zero. Since $g \in A$, we also have $g_m = \nu\rho(g_0)$.

Suppose that $\nu \in E^\times$ and $\rho(E) \subset E$. Substituting $g_m = \nu\rho(g_0)$ into the above equation yields

$$N_{E/F}(g_0) = N_{E/F}(a_0)^l N_{E/F}(\nu\rho(g_0)).$$

Applying $N_{F/F'}$ to both sides implies that

$$N_{E/F'}(g_0) = N_{F/F'}(N_{E/F}(a_0)^l)N_{E/F'}(\nu\rho(g_0)).$$

Now $N_{E/F'}(\rho(g_0)) = N_{E/F'}(g_0)$, so we can cancel the non-zero term $N_{E/F'}(g_0)$ to obtain $1 = N_{E/F'}(a_0)^l N_{E/F'}(\nu)$. □

Corollary 3.6.3. *(for $f \in K[t;\sigma]$, K a finite field, cf. [56, Theorem 7]) Let $D = (E/C, \gamma, a)$ be a cyclic division algebra over C of degree d such that $\sigma|_E \in \mathrm{Aut}(E)$ and $\gamma \circ \sigma = \sigma \circ \gamma$. Suppose that $\sigma^n(z) = u^{-1}zu$ with $u \in E$.*

Let $f(t) = a_0 + a_1t + \cdots + t^m \in E[t;\sigma] \subset D[t;\sigma]$ be irreducible, $(f,t)_r = 1$, and let $\deg(h) = dmn$. Suppose that all monic f_i similar to f lie in $E[t;\sigma]$. Then $S_{n,m,1}(\nu,\rho,f)$ is a division algebra over F', if one of the following holds:
(i) $\nu = 0$.
(ii) $\nu \notin E$ and $\rho|_E \in \mathrm{Aut}(E)$.
(iii) $\nu \in E^\times$ and $\rho|_E \in \mathrm{Aut}(E)$, such that

$$N_{E/F'}(a_0)N_{E/F'}(\nu) \neq 1.$$

This is equivalent to $N_{E/F'}(\nu)N_{F/F'}((-1)^{dm(n-1)}N_{E/C}(u)^m h_0) \neq 1$.

This follows from Theorem 3.6.2 by setting $l = 1$.

3.6.2 *For $K[t;\sigma]$*

Theorem 3.6.4. *(for $f \in K[t;\sigma]$, K a finite field, cf. [56, Theorem 7]) Define $B = \mathrm{Nuc}_r(S_f)$. Then the set*

$$S_{n,m,l}(\nu,\rho,f) = \{a + Rh \,|\, a \in A\} \subset R/Rh,$$

where

$$A = \{a_0 + a_1 t + \cdots + a_{lm-1}t^{lm-1} + \nu\rho(a_0)t^{lm} : a_i \in K\}$$

defines an F'-linear MRD code in $M_k(B)$ with minimum distance $k-l+1$, $l<k$, if one of the following holds:
(i) $\nu = 0$.
(ii) $\deg(h) = mn$ *and* $\nu \in K$ *such that*

$$N_{K/F'}(\nu)N_{K/F'}(a_0)^l \neq 1.$$

In this case, the algebra $S(\nu,\rho,h)$ defines an F'-linear MRD-code in $M_n(E_{\hat{h}})$ with minimum distance $n-l+1$.

The proof follows analogously to Theorem 3.6.2, employing Theorem 3.5.10 to attain the result in (ii).

Corollary 3.6.5. *(for $f \in K[t;\sigma]$, K a finite field, cf. [56, Theorem 7]) Define $B = \mathrm{Nuc}_r(S_f)$. Then B is a division algebra and the algebra $S_{n,m,1}(\nu,\rho,f)$ is a division algebra if one of the following holds:*
(i) $\nu = 0$.
(ii) $\deg(h) = mn$ *and* $\nu \in K$ *such that*

$$N_{K/F'}(\nu) \neq 1/N_{K/F'}(a_0).$$

In this case, the algebra $S_{n,m,1}(\nu,\rho,f)$ defines an F'-linear MRD-code in $M_n(E_{\hat{h}})$ with minimum distance n.

3.7 NUCLEI AND CODE PARAMETERS

3.7.1 *Characterizing nuclei via spread sets*

Let $\mathcal{C} = \mathcal{C}(A) = \{L_a : a \in A\} \subseteq \mathrm{End}_F(A)$, where L_a is the left multiplication map in A, be the spread set of an F-algebra A. It is well-known that isotopic semifields have isomorphic nuclei. We define the *left*, respectively, *right idealisers* of $\mathcal{C}$ as

$$I_l(\mathcal{C}) = \{\Phi \in \mathrm{End}_F(A) : \Phi\mathcal{C} \subseteq \mathcal{C}\}, \text{ respectively, } I_r(\mathcal{C}) = \{\Phi \in \mathrm{End}_F(A) : \mathcal{C}\Phi \subseteq \mathcal{C}\}.$$

The *centraliser* of $\mathcal{C}$ is $C(\mathcal{C}) = \{\Phi \in \mathrm{End}_F(A) : \Phi M = M\Phi \quad \forall M \in \mathcal{C}\}$.

Lemma 3.7.1. *For a division algebra A over F, we have the following F-algebra isomorphisms:*
(i) $\mathrm{Nuc}_l(A) \cong \{L_a : a \in \mathrm{Nuc}_l(A)\} \subseteq \mathrm{End}_F(A)$,
(ii) $\mathrm{Nuc}_m(A) \cong \{L_a : a \in \mathrm{Nuc}_m(A)\} \subseteq \mathrm{End}_F(A)$,
(iii) $Z(A) \cong \{L_a : a \in Z(A)\} = \{R_a : a \in Z(A)\} \subseteq \mathrm{End}_F(A)$

This generalizes [56, Proposition 5].

Proof. Since A is a division algebra, $L : A \to \mathrm{End}_F(A)$, $a \mapsto L_a$, is injective.
(i) Restricting L to $\mathrm{Nuc}_l(A)$ yields an F-linear monomorphism with image $\{L_a : a \in \mathrm{Nuc}_l(A)\} \subseteq \mathrm{End}_F(A)$. For all $a, b \in \mathrm{Nuc}_l(A)$, $x \in A$,

$$L_{ab}(x) = (ab)x = a(bx) = L_a(L_b(x))$$

as $a \in \mathrm{Nuc}_l(A)$. Hence $L(ab) = L_{ab} = L_a \circ L_b = L(a)L(b)$, so L restricted to $\mathrm{Nuc}_l(A)$ is multiplicative. Thus $\mathrm{Nuc}_l(A) \cong \{L_a : a \in \mathrm{Nuc}_l(A)\}$. (ii) follows as (i) by restricting L to $\mathrm{Nuc}_m(A)$.
(iii) Restricting L to $Z(A)$ yields an F-linear monomorphism with image $\{L_a : a \in Z(A)\}$. As $a \in Z(A)$ commutes with all of A, it follows that $L_a = R_a$ for all $a \in C(A)$. Moreover, as $Z(A) \subset \mathrm{Nuc}_l(A)$ it follows that L restricted to $Z(A)$ is multiplicative by (i). Thus $Z(A) \cong \{L_a : a \in Z(A)\} = \{R_a : a \in Z(A)\}$. □

Lemma 3.7.2. *For a division algebra or unital algebra A over F,* $[\mathrm{Nuc}_r(A) : F] = [\{R_a : a \in \mathrm{Nuc}_r(A)\} : F]$.

Proof. Consider the map given by right multiplication with $a \in \mathrm{Nuc}_r(A)$, $R : \mathrm{Nuc}_r(A) \to \mathrm{End}_F(A)$, $R(a) = R_a$. This is an F-linear vector space homomorphism with image $\{R_a : a \in \mathrm{Nuc}_r(A)\} \subseteq \mathrm{End}_F(A)$. By our assumptions, it is injective. Thus $\mathrm{Nuc}_r(A) \cong \{R_a : a \in \mathrm{Nuc}_r(A)\}$ as F-vector spaces. □

Theorem 3.7.3. *(cf. [56, Proposition 5] for finite fields) Let A be a unital division algebra and $\mathcal{C}$ be the spread set of A. Let $\mathcal{C}^*$ be the the spread set associated to the opposite algebra A^{op}. Then*

$$\mathrm{Nuc}_l(A) \cong I_l(\mathcal{C}), \quad \mathrm{Nuc}_m(A) \cong I_r(\mathcal{C}), \quad \mathrm{Nuc}_r(A) \cong C(\mathcal{C}^*), \quad C(A) \cong I_l(\mathcal{C}) \cap C(\mathcal{C}).$$

The proof from [56] holds verbatim.

Let now $R = D[t; \sigma, \delta]$ and $f \in R$ be a monic irreducible polynomial of degree m. Suppose that D is a division algebra of degree d over its center C. Then the algebras $S = S_{n,m,l}(0, \rho, f)$ are unital Petit algebras, whose structure is already well known [44]. In this case, $\mathrm{Nuc}_l(S) = \mathrm{Nuc}_m(S) = D$, $\mathrm{Nuc}_r(S) = \{g \in R_m \mid fg \in Rf\}$ is the eigenspace of f, and if S is not associative then $Z(S) = \{d \in D \,|\, dg = gd \text{ for all } g \in S\}$. Moreover, we have $C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta) \subset Z(S)$.

The above results can now be applied to determine the nuclei and center of the algebras $S = S_{n,m,l}(\nu, \rho, f)$.

3.7.2 *Application to our construction*

Theorem 3.7.4. *Let $R = D[t; \sigma]$ and $\deg(h) = dmn$. Suppose $l \leq dn/2$, $n > 1$ and $lm > 2$. Let $S = S_{n,m,l}(\nu, \rho, f)$ and $\mathcal{C}$ be the image of S in $\mathrm{End}_{E_f}(V_f)$, that means the corresponding matrix code lies in $M_n(E_{\hat{h}})$. If $\nu \neq 0$, we have*
(i) $I_l(\mathcal{C}) \cong \{g_0 \in D : g_0\nu = \nu\rho(g_0)\} \subset D$ (in particular, $I_l(\mathcal{C}) \cong \mathrm{Fix}(\rho)$ if $\nu \in C$),
(ii) $I_r(\mathcal{C}) \cong \mathrm{Fix}(\rho^{-1} \circ \sigma^{lm}) \subset D$,

(iii) $C(\mathcal{C}) \cong E_{\hat{h}}$, $Z(\mathcal{C}) \cong F'$.
If $\nu = 0$, *we have*
(iv) $I_l(\mathcal{C}) \cong D$, $I_r(\mathcal{C}) \cong D$,
(v) $C(\mathcal{C}) \cong E_{\hat{h}}$, $Z(\mathcal{C}) \cong F$.

Much of the proof works identically to the proof of [56, Theorem 9]; we sketch the proof to highlight the main differences in this more general case. The $lm = 2$ case has to be considered separately, and we can only solve that when $F = \mathbb{R}$.

Proof. Let $\mathcal{C} = \{L_a \in \mathrm{End}_{E_f}(V_f) \,|\, a \in A \subset R/Rh\}$ be the image of $S_{n,m,l}(\nu, \rho, h)$ in $\mathrm{End}_{E_f}(V_f) \subset \mathrm{End}_F(V_f)$. In the following, we identify each element in $\mathrm{End}_F(V_f)$ with the element $g \in S$ that induces it.
Analogously to the proof of [56, Theorem 9], $\{g \in I_l(\mathcal{C}) : \deg(g) \leq lm\} = \{g_0 \in D : g_0\nu = \nu\rho(g_0)\}$. If $\nu = 0$, then $1 \in \mathcal{C}$ so $I_l(\mathcal{C}) \subset \mathcal{C}$ so all $g \in I_l(\mathcal{C})$ have degree at most lm.
Consider $\nu \neq 0$. To check there are no elements $g \in I_l(\mathcal{C})$ of degree higher than lm, we follow the approach of [56, Theorem 9] and consider $gt \bmod \hat{h}(u^{-1}t^n)$. Recalling $\deg(h) = dm$, we have $h(t) = (u^{-1}t^n)^{dm} + \cdots = u^{-dm}[t^n + h'_{dm-1}t^{(dm-1)n} + \cdots + h'_0]$ so

$$gt \bmod h(t) = \left(\sum_{i=0}^{dmn-1} g_{i-1}t^i\right) - g_{dmn-1}u^{dm}\left(\sum_{j=0}^{dm-1} h'_j t^{nj}\right).$$

As $g \in I_l(\mathcal{C})$, this implies $gt \bmod h \in \mathcal{C}$, so for all $i \in \{lm+1, \ldots, dmn-1\}$, we have

$$g_{i-1} = \begin{cases} 0 & \text{for } i \not\equiv 0 \bmod n \\ g_{dmn-1}u^{dm}h'_{i/n} & \text{for } i \equiv 0 \bmod n \end{cases} \tag{2}$$

where $h'_{i/n} = 0$ if i/n is not an integer. It suffices to show that $g_{dmn-1} = 0$ and thus $\deg(g) \leq lm - 1$. As $lm > 2$, this follows verbatim from [56, Theorem 9].

The same holds for $I_r(\mathcal{C})$ following Sheekey's proof with the appropriate amendments made for $D[t;\sigma]$. The results for $C(\mathcal{C})$ and $Z(\mathcal{C})$ hold verbatim from [56, Theorem 9]. □

Theorem 3.7.5. *Let $R = K[t;\sigma]$ and $\deg(h) = mn$. Suppose $l \leq n/2$, $n > 1$ and $lm > 2$. Let $S = S_{n,m,l}(\nu, \rho, f)$ with $\nu \neq 0$ and $\mathcal{C}$ be the image of S in $\mathrm{End}_{E_f}(V_f)$, so that the corresponding matrix code lies in $M_n(E_{\hat{h}})$. Then*
(i) $I_l(\mathcal{C}) \cong \mathrm{Fix}(\rho) \subset K$, $I_r(\mathcal{C}) \cong \mathrm{Fix}(\rho^{-1} \circ \sigma^{lm}) \subset K$,
(ii) $C(\mathcal{C}) \cong E_{\hat{h}}$, $Z(\mathcal{C}) \cong F'$.
If $\nu = 0$, we have
(iii) $I_l(\mathcal{C}) \cong K$, $I_r(\mathcal{C}) \cong K$,
(iv) $C(\mathcal{C}) \cong E_{\hat{h}}$, $Z(\mathcal{C}) \cong F$.

Again, the proof is analogous to the one of [56], Theorem 9. We note that it does not use the fact that for finite fields the right nucleus of S_f is $E_{\hat{h}}$. It only uses that R/Rh has center $E_{\hat{h}}$.

Theorems 3.7.4 and 3.7.5 generalize [56, Theorem 9], which was proved for finite fields only. The following results generalize [56, Corollary 1], which was proved for semifields, and follow as direct consequences of the above theorems:

Corollary 3.7.6. *Let $R = D[t;\sigma]$ and $\deg(h) = dmn$. Suppose $n > 1$, $m > 2$ and $S = S_{n,m,1}(\nu, \rho, f)$ with $\nu \neq 0$ be a division algebra. Then*
(i) $\mathrm{Nuc}_l(S) \cong \{g_0 \in D : g_0\nu = \nu\rho(g_0)\} \subset D$,
(ii) $\mathrm{Nuc}_m(S) \cong \mathrm{Fix}(\rho^{-1} \circ \sigma^m) \subset D$,
(iii) $Z(S) \cong \mathrm{Fix}(\rho) \cap F = F'$.
(iv) $\dim_{F'}\mathrm{Nuc}_r(S) = \dim_{F'}(E_{\hat{h}}) = \deg(\hat{h})[F : F'] = [F : F']dm$.

In particular, we have $\mathrm{Nuc}_l(S) = \mathrm{Fix}(\rho) \subset D$, if $\nu \in C$.

Corollary 3.7.7. *Let $R = K[t;\sigma]$ and $\deg(h) = mn$. Suppose that $n > 1$, $m > 2$ and that $S = S_{n,m,1}(\nu, \rho, f)$ is a division algebra with $\nu \neq 0$. Then*
(i) $\mathrm{Nuc}_l(S) \cong \mathrm{Fix}(\rho) \subset K$,
(ii) $\mathrm{Nuc}_m(S) \cong \mathrm{Fix}(\rho^{-1} \circ \sigma^m) \subset K$,
(iii) $Z(S) \cong \mathrm{Fix}(\rho) \cap F = F'$.
(iv) $\dim_{F'}\mathrm{Nuc}_r(S) = \dim_{F'}(E_{\hat{h}}) = \deg(\hat{h})[F : F'] = [F : F']m$.

3.8 EXAMPLES OF DIVISION ALGEBRAS AND MRD CODES

3.8.1 $K = F(\theta)$ *and* $f(t) = t^n - \theta$

Let $K = F(\theta)$ be an extension of prime degree n. Choose $f(t) = t^n - \theta$, then f is an irreducible polynomial in $K[t;\sigma]$. Note that we know the following:

- $f(t) = t^3 - \theta \in K[t;\sigma]$ is irreducible if and only if $\theta \neq \sigma^2(z)\sigma(z)z$ for all $z \in K$.
- Suppose F contains a primitive nth root of unity. Then $f(t) = t^n - \theta \in K[t;\sigma]$ is irreducible if and only if $\theta \neq \sigma^{n-1}(z)\cdots\sigma(z)z$ for all $z \in K$.

Define

$$h(t) = (t^n - \theta)(t^n - \sigma(\theta))\cdots(t^n - \sigma^{n-1}(\theta)) = (t^n)^n + \cdots + (-1)^n N_{K/F}(\theta).$$

As $t^n - \sigma^i(\theta) \in K[t^n]$, the factors of $h(t)$ are commutable and $h(t) \in K[t^n]$. Since

$$\sigma(h(t)) = (t^n - \sigma(\theta))\cdots(t^n - \sigma^{n-1}(\theta))(t^n - \theta) = h(t),$$

we know that $h(t) \in \mathrm{Fix}(\sigma)[t] = F[t]$ so $h(t) \in F[t] \cap K[t^n] = F[t^n] = Z(R)$. Hence $h(t) = \hat{h}(t^n)$ with $\hat{h}(x) = x^n + \cdots + (-1)^n N_{K/F}(\theta) \in F[x]$. As n is prime, the minimal central left multiple of f must have degree $\deg(f) = n$ in $F[x]$ by Theorem 3.2.10 (taking $d = 1$); thus indeed $h(t) = mclm(f)$ and hence $\hat{h}(x) = x^n + \cdots + (-1)^n N_{K/F}(\theta)$ is an irreducible polynomial in $F[x]$.

$E_f = \{z + Rf : z \in F[t^n]\}$ is generated (as a field) by

$$\{1+Rf, t^n+Rf, t^{2n}+Rf, \ldots, t^{n(n-1)}+Rf\} = \{1+Rf, \theta+Rf, \theta^2+Rf, \ldots, \theta^{n-1}+Rf\}$$

over F. As K is generated by $\{1, \theta, \ldots, \theta^{n-1}\}$, there is a canonical isomorphism $E_f \longrightarrow K$, $a + Rf \mapsto a$. It is clear that $\{1 + Rf, t + Rf, \ldots, t^{n-1} + Rf\}$ is an E_f-basis for V_f.

Let $a = a_0 + a_1 t + \cdots + a_{ln-1}t^{ln-1} + \nu\rho(a_0)t^{ln} \in S_{n,n,l}(\nu, \rho, f)$. In order to determine M_a, we consider how $L_{a_i t^i}$ acts on the basis elements of V_f. As left multiplication is distributive, i.e. $L_{a+b}(x) = L_a(x) + L_b(x)$, it follows that

$$L_a = \sum_{i=0}^{ln} L_{a_i t^i},$$

where $a_{ln} = \nu\rho(a_0)$. For each i, let $i = kn + i_0$ for some $i_0 < n$. Then the left multiplication map $L_{a_i t^i}$ acts on each basis element of V_f as follows:

$$\begin{aligned}
L_{a_i t^i}(1 + Rf) &= a_i t^{i_0}\theta^k + Rf = (t^{i_0} + Rf)(\sigma^{n-i_0}(a_i)\theta^k + Rf) \\
L_{a_i t^i}(t + Rf) &= a_i t^{i_0+1}\theta^k + Rf = (t^{i_0+1} + Rf)(\sigma^{n-i_0-1}(a_i)\theta^k + Rf) \\
&\vdots \qquad\qquad\qquad \vdots \\
L_{a_i t^i}(t^{n-i_0} + Rf) &= a_i t^{k(n+1)} + Rf = a_i\theta^{k+1} + Rf = (1 + Rf)(a_i\theta^{k+1} + Rf) \\
L_{a_i t^i}(t^{n-i_0+1} + Rf) &= a_i t^{k(n+1)+1} + Rf = a_i t\theta^{k+1} + Rf = (t + Rf)(\sigma(a_i)\theta^{k+1} + Rf) \\
&\vdots \qquad\qquad\qquad \vdots \\
L_{a_i t^i}(t^{n-1} + Rf) &= a_i t^{i_0-1}\theta^{k+1} + Rf = (t^{i_0-1} + Rf)(\sigma^{n-i_0+1}(a_i)\theta^{k+1} + Rf).
\end{aligned}$$

Thus we obtain a matrix representing $L_{a_i t^i}$, given by

$$M_{a_i t^i} = \begin{pmatrix}
0 & \cdots & 0 & \sigma^{n-i_0}(a_i)\theta^k & 0 & \cdots & 0 \\
0 & \cdots & 0 & 0 & \sigma^{n-(i_0+1)}(a_i)\theta^k & \cdots & 0 \\
\vdots & \ddots & & & & \ddots & \vdots \\
0 & & \ddots & & & & \sigma(a_i)\theta^k \\
a_i\theta^{k+1} & & & & \ddots & & 0 \\
0 & & & & & & \\
\vdots & \ddots & & & & \ddots & \vdots \\
0 & \cdots & \sigma^{n-(i_0-1)}(a_i)\theta^{k+1} & 0 & 0 & \cdots & 0
\end{pmatrix}.$$

As $M_a = \sum_{i=0}^{n} M_{a_i t^i}$, we obtain $M_a = (m_{i,j})_{i,j}$ where

$$m_{i,j} = \begin{cases}
[\sum_{p=0}^{l-1} \sigma^{n+1-i}(a_{pn})\theta^p] + \sigma^{n+1-i}(\nu\rho(a_0))\theta^l & \text{for } i = j, \\
[\sum_{p=0}^{l-1} \sigma^{n+1-i}(a_{pn+(i-j)})\theta^p] & \text{for } i > j, \\
[\sum_{p=1}^{l} \sigma^{n+1-i}(a_{pn+(i-j)})\theta^p] & \text{for } i < j.
\end{cases}$$

This yields $C(S) = \{M_a \mid a_k \in K \text{ for } k = 0, 1, \ldots, ln-1\} \subset M_n(K)$ as a matrix spread set of a $ln^2[F : F']$-dimensional F'-algebra. By Theorem 3.6.4, this yields an MRD code when

$$N_{K/F'}(\nu)N_{K/F'}(\theta)^l \neq 1.$$

If $l = 1$, we obtain $M_a = (m_{i,j})_{i,j}$ where

$$m_{i,j} = \begin{cases} \sigma^{n+1-i}(a_0) + \sigma^{n+1-i}(\nu\rho(a_0))\theta & \text{for } i = j, \\ \sigma^{n+1-i}(a_{i-j}) & \text{for } i > j, \\ \sigma^{n+1-i}(a_{n+i-j})\theta & \text{for } i < j. \end{cases}$$

The algebra associated to this spread set will be a division algebra if

$$N_{K/F'}(\theta)N_{K/F'}(\nu) \neq 1.$$

In particular, for $\nu = 0$ this condition is satisfied for any irreducible $f(t) = t^n - \theta$. This is the well known result that for every irreducible f the Petit algebra S_f is a division algebra and so are all its isotopes.

For $m, n > 2$, Corollary 3.7.7 yields

$$\mathrm{Nuc}_l(S) = \mathrm{Nuc}_m(S) = \mathrm{Fix}(\rho) \subset K,$$

$$C(S) = F', \quad \dim_{F'}\mathrm{Nuc}_r(S) = [F : F']m.$$

3.8.2 *Real division algebras of dimension 4*

Over a finite field F, all division algebras of dimension 4 over F which have F as their center and a nucleus of dimension 2 over F, can be constructed as algebras $S_{n,m,1}(\nu, \rho, f)$ for suitable parameters [56]. Let us now look at the division algebras we obtain with our construction over $\mathbb{R}$. Let $\hat{h}(x) = x^2 + b^2 \in \mathbb{R}[x]$. Then $h(t) = \hat{h}(t^2)$ is the minimal central left multiple of $f(t) = t^2 - bi \in \mathbb{C}[t; ^-]$, as $h(t) = t^4 + b^2 = (t^2 + bi)(t^2 - bi)$.

For all $b \in \mathbb{R}$, $f(t) = t^2 - bi$ is irreducible in $\mathbb{C}[t; ^-]$. For every irreducible $f(t) = t^2 - bi$, and $\nu \in \mathbb{C}$ such that $N_{\mathbb{C}/\mathbb{R}}(\nu) \neq \frac{1}{b^2}$, we obtain a four-dimensional

real division algebra $S = S_{2,2,1}(\nu, \rho, f)$ and an MRD code given by its matrix spread set

$$C(S) = \left\{ \begin{pmatrix} z_0 + \nu\rho(z_0)bi & z_1 bi \\ \overline{z_1} & \overline{z_0} + \overline{\nu\rho(z_0)}bi \end{pmatrix} \mid z_0, z_1 \in \mathbb{C} \right\},$$

where ρ is either the identity or the complex conjugation and $\nu \in \mathbb{C}$.

As mentioned in Theorem 3.7.2, [56, Theorem 9] cites results from the literature to deal with the case when $lm = 2$. These are only valid over finite fields, but we can extend Theorem 3.7.2 to $\mathbb{R}$:

Theorem 3.8.1. *Let $R = \mathbb{C}[t;^-]$ and $f(t) = t^2 - bi \in R$. Suppose $S = S_{2,2,1}(\nu, \rho, f)$ is a division algebra for some $\nu \neq 0$ and $\rho \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$. Then*
(i) $\mathrm{Nuc}_l(S) = \mathrm{Nuc}_m(S) = \mathrm{Fix}(\rho)$,
(ii) $Z(S) = \mathbb{R}$,
(iii) $\dim_{\mathbb{R}}(\mathrm{Nuc}_r(S)) = \dim_{\mathbb{R}}(\mathbb{R}[t^2]) = 2$.

Proof. Since $f(t) = t^2 - bi \in R$ we have $h(t) = t^4 + b^2 \in \mathbb{R}[t^2]$. Suppose $g + Rh \in I_l(\mathcal{C})$ for some $g(t) = g_0 + g_1 t + g_2 t^2 + g_3 t^3 \in R$. Then $ga \in S(\nu, \rho, f)$ for all $a \in S$. Direct and laborious computation yields $g_2 = 0$, $g_3 = -g_1\overline{\nu}$, and $\nu\rho(g_0 a_0 - b^2 g_1 \overline{\nu a_1}) = g_0 \nu\rho(a_0) + g_1 \overline{a_1}$. This is satisfied for all $a_0, a_1 \in \mathbb{C}$ if and only if $\nu\rho(g_0) = g_0\nu$ and $g_1 = \nu\rho(b^2 g_1 \overline{\nu})$.

Suppose $g_1 \neq 0$. Taking norms, we have

$$N_{\mathbb{C}/\mathbb{R}}(g_1) = N_{\mathbb{C}/\mathbb{R}}(\nu^2 b^2 g_1).$$

This simplifies to $N_{\mathbb{C}/\mathbb{R}}(\nu b)^2 = 1$. As $N_{\mathbb{C}/\mathbb{R}}(a) \geq 0$ for all $a \in \mathbb{C}$, it follows that $N_{\mathbb{C}/\mathbb{R}}(\nu b) = 1$; as S is a division algebra, this is a contradiction by Theorem 3.4.8. Hence $g_1 = 0$ so $g = g_0$ and it follows that $\mathrm{Nuc}_l(S) = \mathrm{Fix}(\rho)$.

The computations for $I_r(\mathcal{C})$ follow analogously and $Z(\mathcal{C})$ and $C(\mathcal{C})$ follow from the proof of [56, Theorem 4]. We obtain the final result on the nuclei using Theorem 3.7.3 to relate the idealisers and centraliser of $\mathcal{C}$ to the nuclei of the algebra S. □

If $\nu = 0$, then $N_{\mathbb{C}/\mathbb{R}}(\nu) = 0$ and we will obtain algebras isotopic to real Petit division algebras; this is true for any choice of irreducible $f(t) = t^2 - bi$. If $\nu \neq 0$, any choice of $f(t)$ also yields division algebras by Theorem 3.6.5.

For example, if we let $f(t) = t^2 - bi$ we obtain division algebras for all $\nu \in \mathbb{C}$ such that $N_{\mathbb{C}/\mathbb{R}}(\nu) \neq 1/b^2$.

If $\nu \neq 0$ and S is a division algebra, it follows that

$$\mathrm{Nuc}_l(S) = \mathrm{Nuc}_m(S) = \begin{cases} \mathbb{C}, \text{ if } \rho = id \\ \mathbb{R}, \text{ if } \rho = {}^- \end{cases}$$

$$C(S) = \mathbb{R},$$

$$\dim_{\mathbb{R}}(\mathrm{Nuc}_r(S)) = 2.$$

Since $\mathrm{Nuc}_r(S)$ is a two-dimensional division algebra over $\mathbb{R}$, it is an Albert isotope of $\mathbb{C}$ and can be found in the classification given in [30, Theorem 1]: $\mathbb{C}^{(^-,^-)}$, $\mathbb{C}^{(1+L(v)^-,^-)}$, $\mathbb{C}^{(^-,1+L(v)^-)}$, $\mathbb{C}^{(1+L(v)^-,1+L(w)^-)}$, with $v, w \in \mathbb{C}$ suitably chosen.

Note that the four-dimensional algebras in the first class are all isotopes of nonassociative quaternion algebras.

3.9 CONSTRUCTING ALGEBRAS USING $f \in D[t;\delta]$

We now briefly consider the same construction using differential polynomial rings. Let D be a finite-dimensional division algebra over its center C and C a field of characteristic p. Let $R = D[t;\delta]$, where δ is a derivation of D, such that $\delta|_C$ is algebraic with minimum polynomial $g(t) = t^{p^e} + c_1 t^{p^{e-1}} + \cdots + c_e t \in F[t]$ of degree p^e, with $F = C \cap \mathrm{Const}(\delta)$. Then $g(\delta) = id_{d_0}$ is an inner derivation of D. W.l.o.g. we choose $d_0 \in F$, so that $\delta(d_0) = 0$ [33, Lemma 1.5.3]. Then

$$C(D[t;\delta]) = F[x] = \{\sum_{i=0}^{k} a_i (g(t) - d_0)^i \mid a_i \in F\}$$

with $x = g(t) - d_0$. The two-sided $f \in D[t;\delta]$ are of the form $f(t) = uc(t)$ with $u \in D$ and $c(t) \in Z(R)$ [33, Theorem 1.1.32]. All polynomials $f \in R$ are bounded.

3.9.1 *The minimal central left multiple of $f \in D[t;\delta]$*

For every $f \in R = D[t;\sigma]$, the *minimal central left multiple of f in R* is defined to be the unique polynomial of minimal degree $h \in Z(R) = F[x]$ such that $h = gf$ for some $g \in R$, and such that $h(t) = \hat{h}(g(t) - d_0)$ for some monic $\hat{h}(x) \in F[x]$. For any $f \in R = D[t;\delta]$, the bound f^* is the unique minimal central left multiple of f up to some scalar.

Lemma 3.9.1. *Let $f \in R = D[t;\delta]$, then the minimal central left multiple of f exists and is unique. It is equal to f^* up to a scalar multiple in $D^\times$.*

Proof. Let f^* be a bound of f. Then f^* is unique up to scalar multiplication by elements in $D^\times$ and Rf^* is the largest two-sided ideal of R contained in the left ideal Rf. Since f^* is two-sided, we know that $f^*(t) = dc(t)$ for some $c(t) \in Z(R)$ and $d \in D^\times$. So assume w.l.o.g. that $f^* \in Z(R)$. The rest of the proof is identical to the one of Lemma 3.2.4. □

From now on let $f \in R = D[t;\delta]$ be a monic irreducible polynomial of degree m and let $h(t) = \hat{h}(g(t) - d_0)$ be its minimal central left multiple. Then $\hat{h}(x)$ is irreducible in $F[x]$ and h generates a maximal two-sided ideal Rh in R [33, p. 16]. We have

$$Z(R/Rh) \cong F[x]/F[x]\hat{h}(x)$$

[32, Proposition 4], $\deg(h) = p^e \deg(\hat{h})$, and define $E_{\hat{h}} = F[x]/F[x]\hat{h}(x)$. Recall that S_f is defined as the set $R_m = \{g \in D[t;\delta] \mid \deg(g) < m\}$ together with the usual addition and the multiplication

$$g \circ h = \begin{cases} gh \text{ if } \deg(g) + \deg(h) < m, \\ gh \bmod_r f \text{ if } \deg(g) + \deg(h) \geq m. \end{cases}$$

Theorem 3.9.2. *[42]* $\mathrm{Nuc}_r(S_f)$ *is a associative division algebra over $E_{\hat{h}} = Z(R/Rh)$ of degree $s = dp^e/k$, where k is the number of irreducible factors of h in R, and*

$$R/Rh \cong M_k(\mathrm{Nuc}_r(S_f)).$$

In particular, this means that $\deg(\hat{h}) = \frac{dm}{s}$, $\deg(h) = km = \frac{dp^e m}{s}$, *and*

$$[\mathrm{Nuc}_r(S_f) : F] = s^2 \cdot \frac{dm}{s} = dms.$$

Moreover, s *divides* $gcd(dm, dp^e)$. *If* f *is not right invariant, then* $k > 1$ *and* $s \neq dp^e$.

We know that $[S_f : F] = [S_f : C]p^e = d^2m \cdot p^e$. Since $\mathrm{Nuc}_r(S_f)$ is a subalgebra of S_f, comparing dimensions we obtain that $[S_f : \mathrm{Nuc}_r(S_f)] = k$. If f is not right-invariant, again $[S_f : \mathrm{Nuc}_r(S_f)] = k > 1$.

3.9.2 *The construction with* $f \in D[t;\delta]$

Define $B = \mathrm{Nuc}_r(S_f)$. As f is irreducible, $\hat{h}$ is irreducible. For each $z(t) = \hat{z}(g(t) - d_0) \in F[g(t) - d_0]$ with $\hat{z} \in F[x]$, we have $z \in Rf$ if and only if $z \in Rh$. Let

$$V_f = \{a + Rf \mid a \in R = D[t;\delta]\} = R/Rf$$

be the R-module defined by factoring out the maximal left ideal Rf and let

$$E_f = \{z(t) + Rf \mid z(t) = \hat{z}((g(t) - d_0)) \in F[(g(t) - d_0)]\}.$$

Together with the multiplication $(x + Rf) \circ (y + Rf) = (xy) + Rf$ for all $x, y \in F[(g(t) - d_0)]$, E_f is a field extension of F of degree $\deg(\hat{h})$ isomorphic to $E_{\hat{h}}$. Let k be the number of irreducible factors of h. Then V_f is a right B-module of dimension k via the scalar multiplication given by $V_f \times B \longrightarrow V_f$, $(a + Rf)(z + Rf) = az + Rf \in V_f$ for all $z \in F[(g(t) - d_0)]$ and $a \in R$. We identify V_f with B^k via a canonical basis.

Lemma 3.9.3. *For each* $z(t) = \hat{z}(g(t) - d_0) \in F[g(t) - d_0]$ *with* $\hat{z} \in F[x]$, *we have* $z \in Rf$ *if and only if* $z \in Rh$.

Lemma 3.9.4. $E_f = (E_f, \circ)$ *is a field and isomorphic to* $E_{\hat{h}}$. *Thus* E_f *is a field extension of degree* $\deg(\hat{h})$.

Proposition 3.9.5. *Let k be the number of irreducible factors of h. Then V_f is a right B-module of dimension k via the scalar multiplication given by $V_f \times B \longrightarrow V_f$,*

$$(a + Rf)(z + Rf) = az + Rf \in V_f$$

for all $z \in F[(g(t) - d_0)]$ and $a \in R$. Thus, we can identify V_f with B^k via a canonical basis.

All the proofs of the above results are identical to their analogues using $D[t;\sigma]$.

For some $\nu \in D^\times$ and $\rho \in \mathrm{Aut}(D)$, define $F' = \mathrm{Fix}(\rho) \cap F$. We assume from now on that F/F' is finite-dimensional. Let k be the number of irreducible factors of $h(t)$, and s the degree of the right nucleus of S_f over $E_{\hat{h}}$. We assume f is not right-invariant which yields $k > 1$.

Let $l < k = dp^e/s$. Define the set $S_{p^e,m,l}(\nu,\rho,f) = \{a + Rh \,|\, a \in A\} \subset R/Rh$, where

$$A = \{a_0 + a_1 t + \cdots + a_{lm-1}t^{lm-1} + \nu\rho(a_0)t^{lm} \,|\, a_i \in D\} \subset D[t;\delta].$$

$S_{p^e,m,l}(\nu,\rho,f)$ is a vector space over F' of dimension $d^2p^em[F:F']$. We identify each element of $S_{p^e,m,l}(\nu,\rho,f)$ with a map in $\mathrm{End}_B(V_f)$ as follows: For each $a \in S_{p^e,m,l}(\nu,\rho,f)$ let $L_a : V_f \to V_f$ be the left multiplication map $L_a(b + Rf) = ab + Rf$. L_a is a B-linear map. Let M_a be the matrix in $M_k(B)$ representing L_a with respect to an B-basis of V_f. As before, we will denote the image of $S = S_{p^e,m,l}(\nu,\rho,f)$ in $M_k(B)$ by

$$\mathcal{C}(S) = \{M_a \mid a \in S_{p^e,m,l}(\nu,\rho,f)\}.$$

For $l = 1$, this construction again yields algebras over F'. As with $D[t;\sigma]$, we can relate $S_{p^e,m,1}(\nu,\rho,f)$ to $R_m = \{g \in R \,|\, deg(g) < m\}$ endowed with the multiplication

$$a(t) \circ b(t) = (a(t) + \nu\rho(a_0)t^m)b(t) \mod_r(f).$$

Example 3.9.6. Let $R = D[t;\delta]$ and $f(t) = t + c$ for some $c \in D$. For some $\nu \neq 0$ and $\rho \in \mathrm{Aut}(D)$, $S_{p^e,1,1}(\nu,\rho,f) = (D,\circ)$ has multiplication

$$\begin{aligned} x \circ y =& (x + \nu\rho(x)t)y) \bmod_r f \\ =& xy + \nu\rho(x)yt + \nu\rho(x)\delta(y) \bmod_r f \\ =& xy + \nu\rho(x)(\delta(y) - yc) \end{aligned}$$

for all $x, y \in D$. Suppose $y \in F^\times$. As $F \subset \mathrm{Const}(\delta)$, it follows that $x \circ y = xy - \nu\rho(x)yc = (x - \nu\rho(x)c)y$ for all $x, y \in D$, Hence if $x = \nu\rho(x)c$ for some $x \in D$, $(D,\circ)$ is not a division algebra. Moreover, if $[D : F']$ is finite dimensional and $N_{D/F'}(\nu c) = 1$ then $(D,\circ)$ is not a division algebra. This gives us hope that there may be a analogous result to the one given in Example 3.3.6, i.e. $(D,\circ)$ is a division algebra if and only if $N_{D/F'}(\nu c) \neq 1$.

Proposition 3.9.7. *Let $f \in D[t;\delta]$ be irreducible and $\deg(h) = km$. Let $B = \mathrm{Nuc}_r(S_f)$. For all $a + Rh \in R/Rh$, we have*

$$\dim_B(im(L_A)) = k^2 - \frac{k}{m} deg(gcrd(a, \hat{h}(g(t) - d_0))).$$

Moreover, the column rank of M_a is equal to $k - \frac{1}{m} deg(gcrd(a, \hat{h}(g(t) - d_0))$.

Corollary 3.9.8. *Let $f \in D[t;\delta]$ and $\deg(h) = dmp^e$. For all $a + Rh \in R/Rh$, we have $rank(M_a) = dp^e - \frac{1}{m}\deg(gcrd(a, \hat{h}(g(t) - d_0)))$.*

The proofs are again analogous to the case where $R = D[t;\sigma]$. Consequently, we obtain the following result:

Theorem 3.9.9. *$S_{p^e,m,l}(\nu,\rho,f)$ is a division algebra if and only if there are no divisors of h in $S_{p^e,m,1}(\nu,\rho,f)$. More generally, $S_{p^e,m,l}(\nu,\rho,f)$ yields an MRD-code if and only if it contains no divisors of h of degree lm.*

Recall that for B a non-commutative division ring, we define MRD codes in $M_k(B)$ by $d(A,B) = \mathrm{colrank}(A - B)$ for all $A, B \in M_k(B)$. The above theorem can be rewritten equivalently into two cases:

Theorem 3.9.10. *$S_{p^e,m,l}(\nu,\rho,f)$ yields an MRD-code if and only there are no elements $g \in S_{p^e,m,l}(\nu,\rho,f)$ of degree lm which can be written as $g = \prod_{i=1}^{l} f_i$,*

where f_i is similar to f for all i. Thus if $\nu = 0$, $S_{p^e,m,l}(\nu,\rho,f)$ is an MRD code with minimum distance $k-l+1$.

Corollary 3.9.11. *Let f be an irreducible monic polynomial of degree m. Suppose that $A = \{a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} + \nu\rho(a_0)t^m : a_i \in D\} \subset R$.*
(i) If $a \in A$ is reducible, then a is not a left zero divisor of $S_{p^e,m,1}(\nu,\rho,f)$.
(ii) If $\nu = 0$ then $(R_m, \circ)$ is a division algebra over F', which for $m \geq 2$ is a (unital) Petit algebra.
(iii) If A does not contain any polynomial similar to f, then $(R_m, \circ)$ is a division algebra over F'.

3.9.3 *The norm of $f \in D[t;\delta]$*

Unless otherwise specified, let D be a associative division algebra over C with C a field of characteristic p. We also suppose D has a maximal subfield E of degree d and $R = D[t;\delta]$. Define the ring of central quotients of R as $D(t;\delta) = \{f/g \mid f \in R, g \in Z(R)\}$, with centre $C(D(t;\delta)) = \mathrm{Quot}(Z(R)) = F(x)$, where $x = g(t) = d_0$. Let $\tilde{\delta}$ be the extension of δ to $D(x)$ such that $\tilde{\delta} = id_{t|D(x)}$. Then $D(t;\delta)$ is a central simple $F(x)$-algebra, more precisely we have $D(t;\delta) \cong (D(x), \tilde{\delta}, d_0 + x)$, i.e. $D(t;\delta)$ is a generalized differential algebra.

Let N be the reduced norm of $D(t;\delta)$. For all $f \in R$, $N(f) \in F[x]$ and f divides $N(f)$. We give an analogue of Theorem 3.5.2 for $D[t;\delta]$:

Theorem 3.9.12. *Let D have a subfield E of degree d and let $\omega : D \to M_d(E)$ be the left regular representation of D. Then for any $f \in R$ of degree m,*

$$N(f) = \pm det(\omega(a_m))^{p^e} x^{dm} + \ldots$$

In particular, $N(f)$ has degree dm.

The proof follows analogously to the proof of Theorem 3.5.2.

Corollary 3.9.13. *Let $D = (E, \delta_0, a)$ be a differential algebra, $\delta|_E$ be a derivation on E, and let $f \in D[t;\delta]$ be monic with coefficients in E. Then $N(f(t)) = \pm x^{dm} + \dots$.*

Proof. Through direct computations of the left regular representation of D, we see that for each $a \in E$, $\omega(a)$ is a lower triangular matrix with each entry on the lead diagonal equal to a. Hence the result follows analogously to Theorem 3.5.5. □

As the bound of f has degree dm in $F[x]$, it follows that $N(f)$ is equal to the bound of f. Thus if $deg(\hat{h}) = dm$, we conclude that $\hat{h}(x) = \alpha N(f)$ for some $\alpha \in D^{\times}$.

3.9.4 *The norm of $f \in K[t;\delta]$*

Consider the special case where $d = 1$, i.e. $R = K[t;\delta]$ for some field extension K/F.

Theorem 3.9.14. *(i) For all $f \in R$ we have $N(f) \in F[x]$ and f divides $N(f)$. (ii) If $f(t) = a_0 + a_1 t + \cdots + a_m t^m \in R = K[t;\delta]$ has degree m, then*

$$N(f(t)) = (-1)^{m(p^e-1)} a_m^{p^e} x^m + \dots .$$

Proof. (i) By an analogous argument as given in the proof of Proposition 3.5.1, the set $\{1, t, \dots, t^{p^e-1}\}$ is a basis for $(K(x), \widetilde{\delta}, x)$ over $K(x)$. We obtain a representation ρ of A by matrices in $M_{p^e}(K[x])$ by writing

$$t^{i-1}a = \sum_{j=1}^{p^e} \rho_{ij}(a) t^{j-1}, \qquad 1 \le i \le p^e$$

for each $a \in R$, where $\rho_{ij}(a)$ is the $(i,j)^{\text{th}}$ entry of $\rho(a)$. Thus $\det(\rho(f(t))) \in K[x] \cap F(x) = F[x]$. This shows that $N(f) \in F[x]$ as claimed in [33, p.31]. Similarly, it can be shown that all the coefficients of the characteristic polynomial of $\rho(f(t))$ are contained in $F[x]$ (cf. also [45, Proposition, p. 295]) and thus $f(t)^\sharp \in R$ by [33, (1.6.12)]. Since $N(f(t)) = f(t)f(t)^\sharp = f(t)^\sharp f(t)$ [33,

(1.6.13)], it follows that $f(t)$ divides $N(f)$.

(ii) Write $m = kp^e + r$ for integers k, r with $0 \leq r < p^e$. Let $x = g(t) = t^{p^e} + g_0(t)$. Substituting $t^{p^e} = x - g_0(t)$, we obtain $f(t) = P_0(x) + P_1(x)t + \cdots + P_{p^e-1}(x)t^{p^e-1} \in K[x][t;\sigma]$ for some $P_i(x) \in K[x]$ with

$$\deg(P_i(x)) \leq \begin{cases} k & \text{for } i \leq r, \\ k-1 & \text{for } i > r. \end{cases}$$

and $P_r(x) = a_m X^k + \ldots$. We obtain the matrix

$$\rho(f(t)) = \begin{pmatrix} Q_{1,1}(x) & \cdots & Q_{1,p^e}(x) \\ \vdots & & \vdots \\ Q_{p^e,1}(x) & \cdots & Q_{p^e,p^e}(x) \end{pmatrix}$$

for some $Q_{i,j}(x) \in K[x]$, where

$$\deg(Q_{i,j}) = \begin{cases} \deg(P_{j-i}) & \text{for } i \leq j, \\ \deg(P_{p^e+j-i}) + 1 & \text{for } i > j. \end{cases}$$

Comparing the above equation with the expressions for $P_i(x)$, it follows that

$$\deg(Q_{i,j}) \leq \begin{cases} k-1 & \text{for } i \leq j \text{ and } j-i > r, \\ k & \text{for } i \leq j \leq m_0 + i \text{ or } j < i < p^e - r + j, \\ k+1 & \text{for } i > j \text{ and } i - j \geq p^e - r. \end{cases}$$

with $Q_{i,j}(x) = a_m x^k + \ldots$ for $j - i = r$ and $Q_{i,j}(x) = a_m x^{k+1} + \ldots$ for $i - j = p^e - r$.

This means the bottom left $r \times r$ minor of $\rho(f(t))$ has elements of degree at most $k+1$ in lower triangular entries (including the diagonal which attains this maximum degree) and the top right $p^e - r \times p^e - r$ minor of $\rho(f(t))$ has elements of degree at most $k-1$ in the upper triangular entries (excluding the diagonal which has elements of exactly degree k). Every other element of $\rho(f(t))$ has degree at most k.

We follow a similar technique as in Proposition 3.5.9. To determine the lead coefficient of $N(f(t)) = \det(\rho(f(t)))$, we see that the highest term of $\det(\rho(f(t)))$ is the leading term of

$$(-1)^{r(p^e-1)} \prod_{i=1}^{p^e-r} Q_{i,r+i} \cdot \prod_{i=p^e-r+1}^{p^e} Q_{i,r+i-p^e}.$$

By directly computing $t^{i-1}f(t) = \sum_{j=1}^{p^e} Q_{i,j}(x)t^{j-1}$, $\quad 1 \leq i \leq p^e$, we determine that for $1 \leq i \leq p^e - r$, $Q_{i,r+i}(x) = a_m x^k + \ldots$, and for $p^e - r + 1 \leq i \leq p^e$, $Q_{i,r+i-p^e}(x) = a_m x^{k+1} + \ldots$. Hence, we have

$$\begin{aligned} N(f(t)) &= (-1)^{r(p^e-1)} a_m^{p^e} X^{k(p^e-r)+(k+1)r} + \ldots \\ &= (-1)^{r(p^e-1)} a_m^{p^e} X^m + \ldots \end{aligned}$$

Now $m(p^e-1) = (kp^e + r)(p^e-1) = kp^e(p^e-1) + r(p^e-1)$. But $p^e(p^e-1)$ is always even, so $(-1)^{m(p^e-1)} = (-1)^{kp^e(p^e-1)}(-1)^{r(p^e-1)} = (-1)^{r(p^e-1)}$. $\square$

We note that this actually implies that $N(f(t)) = a_m^{p^e} x^m + \ldots$: if p is odd, $(-1)^{m(p^e-1)} = 1$. If p is even, we note that C has characteristic $p = 2$ so in fact $-1 = 1$.

Remark 3.9.15. The constant term in Theorem 3.9.14 is much more difficult to compute. With $R = K[t;\delta]$, consider the following examples:

1. Let $p^e = 5$, $f(t) = t^4 + a$ for some $a \in K^\times$, and $g(t) = t^5 + t$. Computing $\rho(f(t))$ yields

$$\begin{pmatrix} a & 0 & 0 & 0 & 1 \\ \delta(a) + x & a-1 & 0 & 0 & 0 \\ \delta^2(a) & 2\delta(a) + x & a-1 & 0 & 0 \\ \delta^3(a) & 3\delta^2(a) & 3\delta(a) + x & a-1 & 0 \\ \delta^4(a) & 4\delta^3(a) & 6\delta^2(a) & 4\delta(a) + x\text{‘} & a-1 \end{pmatrix}.$$

Setting $x = 0$ and taking the determinant of $\rho(f(t))$ gives the constant term of $N(f(t))$; in this case, we obtain that the constant term is equal to

$$\begin{aligned} &a^5 - 4a^4 + a^3[6 + \delta^4(a)] - a^2[4 + 3\delta^4(a) + 8\delta(a)\delta^3(a) + 6\delta^2(a)^2] \\ &+ a[1 + 3\delta^4(a) + 12\delta^2(a)^2 16\delta(a)\delta^3(a) + 36\delta(a)^2\delta^2(a)] \\ &- [\delta^4(a) + 8\delta(a)\delta^3(a) + 6\delta^2(a)^2 + 36\delta(a)^2\delta^2(a) + 24\delta(a)^4]. \end{aligned}$$

2. Let $p^e = 5$, $f(t) = t^5 + g_1 t + a$ for some $a \in K^\times$, and $g(t) = t^5 + g_1 t$. We see that $\rho(f(t))$ is a lower triangular matrix with determinant

$$N(f(t)) = (x + a)^5 = x^5 + 5ax^4 + 10a^2x^3 + 10a^3x^2 + 5a^4x + a^5,$$

so the constant term is simply a^5.

The second example above motivates a family of special cases where $N(f(t))$ can be easily computed in its entirety:

Proposition 3.9.16. *Let $R = K[t;\delta]$ with centre $F[x] \cong F[g(t)]$. For $f(t) = g(t) + a$ for some $a \in K$, $N(f(t)) = (x + a)^{p^e}$.*

Proof. Following the proof of Proposition 3.9.14, we substitute $x = g(t)$ so $f(t) = x + a \in K[x][t;\delta]$. Computing the left regular representation $\rho : K[t;\sigma] \to M_{p^e}(K[x])$, it follows that $\rho(f(t))$ is a lower triangular matrix where each diagonal entry is equal to $x + a$. As the determinant of a triangular matrix is the product of its diagonal entries, the result follows. □

3.9.5 *Obtaining division algebras and MRD codes*

Theorem 3.9.17. *$S_{p^e,m,l}(\nu,\rho,f)$ yields an MRD-code in $M_k(B)$ with minimum distance $k - l + 1$ if and only there are no divisors of h in $S_{p^e,m,l}(\nu,\rho,f)$. This occurs if:*
(i) $\nu = 0$,
(ii) there are no elements $g \in S_{p^e,m,l}(\nu,\rho,f)$ of degree lm which can be written as $g = \prod_{i=1}^{l} f_i$, where f_i is similar to f for all i.

Recall that when $l = 1$, this is the same as determining when $S_{p^e,m,1}(\nu, \rho, f)$ yields a division algebra.

Corollary 3.9.18. *$S_{p^e,m,l}(\nu, \rho, f)$ yields an MRD-code in $M_{dp^e}(E_{\hat{h}})$ with minimum distance $dp^e - l + 1$ if and only there are no divisors of h in $S_{p^e,m,l}(\nu, \rho, f)$. This occurs if:*
(i) $\nu = 0$,
(ii) there are no elements $g \in S_{p^e,m,l}(\nu, \rho, f)$ of degree lm which can be written as $g = \prod_{i=1}^{l} f_i$, where f_i is similar to f for all i.

As a consequence of this, $S_{p^e,m,l}(0, \rho, f)$ always yields an MRD-code in $M_k(B)$. When $\nu \neq 0$, we may consider $N(f(t)$ as before. There is more work to be done in this area, e.g. to determine the constant term of $N(f(t))$ in all cases, but small cases may be done via direct computation as shown above. However, we may generally say the following:

Proposition 3.9.19. *Let f be monic irreducible of degree m. If g is a divisor of h, then g is divisor of $N(f(t))$. Hence $S_{p^e,m,l}(\nu, \rho, f)$ yields an MRD-code if there are no divisors of $N(f(t))$ of degree lm in $S_{p^e,m,l}(\nu, \rho, f)$.*

Once a division algebra or MRD code is obtained, the nuclei of the algebras and the parameters of the codes still need to be calculated. This would form the focus of some future research, in order to determine whether the division algebras we obtain may be isomorphic to those obtained via some other method.

4

A GENERALISATION OF DICKSON'S DOUBLING PROCESS

4.1 A GENERALIZED CAYLEY-DICKSON DOUBLING PROCESS

In the second half of the thesis, we now consider a new family of constructions which arise from the following construction:

Definition 4.1.1. Let F be a field and S an F-vector space which becomes an F-algebra via the multiplications $*_i$, $i = 1, 2, 3, 4$. Define the generalized (orthogonal) Cayley-Dickson doubling $Cay(S, *_1, *_2, *_3, *_4) = S \oplus S$ via

$$(u, v)(u', v') = (u *_1 u' + v *_2 v', u *_3 v' + v *_4 u')$$

for all $u, u', v, v' \in S$.

Even in this generality, we can determine some properties about the algebras we obtain:

Lemma 4.1.2. *$A = Cay(S, *_1, *_2, *_3, *_4)$ has an identity element $1_A = (1_S, 0)$ if and only if 1_S is the identity element in $(S, *_1)$, a left identity in $(S, *_3)$, and a right identity in $(S, *_4)$.*

Proof. Suppose A has an identity element $1_A = (u, v)$. Then for all $x, y \in S$

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

which implies $u *_1 x + v *_2 y = x$ and $u *_3 y + v *_4 x = y$, and

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

which similarly implies $x *_1 u + y *_2 v = x$ and $x *_3 v + y *_4 u = y$.
If $x = 0$, this implies $v *_2 y = 0$ for all $y \in S$, so we must have $v = 0$. Thus we obtain

$$u *_1 x = x *_1 u = x$$

for all $x \in S$, so u is the identity element of $S = (S, *_1)$.
Further, we have $u *_3 y = y$ for all $y \in S$, so u is a left identity of $(S, *_3)$. Similarly we have $y *_4 u = y$ for all $y \in S$, so u is a right identity of $(S, *_4)$.
Conversely, suppose 1_S is the identity in $(S, *_1)$, a left identity in $(S, *_3)$, and a right identity in $(S, *_4)$ and define $1_A = (1_S, 0)$. Then we have

$$(1_S, 0)(u, v) = (1_S *_1 u, 1_S *_3 v) = (u, v)$$

and

$$(u, v)(1_S, 0) = (u *_1 1_S, v *_4 1_S) = (u, v),$$

so 1_A is a identity element in A. □

Definition 4.1.3. Let $f \in Gl(S)$ and S be an algebra with a nondegenerate multiplicative norm $N = N_S$. Then f is a *similarity* of N if, for all $u \in S$, $N(f(u)) = aN(u)$ for some $a \in F^\times$. If $a = 1$, f is called an *isometry* of N. Denote the set of similarities and isometries of N as $S(N)$ and $O(N)$, respectively.

Using similarities we can restrict our construction to simplify it. Let $S = (S*_1)$ be an associative unital division algebra with nondegenerate multiplicative norm $N = N_S$ and $(S, *_i) = (S, *_1)^{(f_i, g_i, h_i)}$ an isotope of $(S, *_1)$ such that f_i, g_i, h_i are similarities of N. So for all $u \in S$, we have $N(f_i(u)) = a_i N(u)$, $N(g_i(u)) = b_i N(u)$ and $N(h_i(u)) = c_i N(u)$ for some $a_i, b_i, c_i \in F^\times$, $i = 2, 3, 4$.

Lemma 4.1.4. *Let $S = (S, *_1)$ be an associative unital algebra and $(S, *_i) = (S, *_1)^{(f_i, g_i, h_i)}$ be isotopes of S such that f_i, g_i, h_i are similarities of N. If $A = Cay(S, *_1, *_2, *_3, *_4)$ has an identity, $a_3 b_3 c_3 = a_4 b_4 c_4 = 1_F$.*

Proof. Suppose $1_A = (1_S, 0)$ is an identity element in A. Then by Lemma 4.1.2 1_S is a left identity in $(S, *_3)$; that is, $1_S *_3 u = u$ for all $u \in S$. This can be expressed as

$$h_3(f_3(1_S) *_1 g_3(u)) = u$$

for all $u \in S$. Taking norms of both sides we have

$$a_3 b_3 c_3 N(u) = N(u)$$

for all $u \in S$. If we let $u = 1_S$, this yields $N(u) = 1_F$. Hence we obtain $a_3 b_3 c_3 = 1_F$.

Similarly, as 1_S is a right identity in $(S, *_4)$ we have $u *_4 1_S = u$ for all $u \in S$. This can be expressed as

$$h_4(f_4(u) *_1 g_4(1_S)) = u$$

for all $u \in S$. Taking norms of both sides we have

$$a_4 b_4 c_4 N(u) = N(u)$$

for all $u \in S$. If we let $u = 1_S$, we obtain $a_4 b_4 c_4 = 1_F$. □

Theorem 4.1.5. *Let $S = (S, *_1)$ be an associative unital division algebra with a nondegenerate norm $N = N_S$ of degree d and $(S, *_i) = (S, *_1)^{(f_i, g_i, h_i)}$ an isotope of $(S, *_1)$ such that f_i, g_i, h_i are similarities of N. So for all $u \in S$, we have $N(f_i(u)) = a_i N(u)$, $N(g_i(u)) = b_i N(u)$ and $N(h_i(u)) = c_i N(u)$ for some $a_i, b_i, c_i \in F^\times$, $i = 2, 3, 4$. Then $A = Cay(S, *_1, *_2, *_3, *_4)$ is a division algebra if*

$$a_2 a_3 b_2 b_3 c_2 c_3 a_4^{-1} b_4^{-1} c_4^{-1} \notin N(S^\times)^2.$$

Proof. Suppose

$$(0, 0) = (u, v)(u', v') = (u *_1 u' + v *_2 v', u *_3 v' + v *_4 u')$$

for some $u, v, u', v' \in S$ such that $(u, v) \neq (0, 0) \neq (u', v')$. This is equivalent to

$$u *_1 u' + v *_2 v' = 0, \tag{3}$$

$$u *_3 v' + v *_4 u' = 0. \tag{4}$$

Assume $v' = 0$. Then by (3), $u *_1 u' = 0$, so $u = 0$ or $u' = 0$ as $(S, *_1)$ is division. As $(u', v') \neq (0, 0)$, we must have $u' \neq 0$ so $u = 0$. Then by (4), $v *_4 u' = 0$ which implies $v = 0$ or $u' = 0$. This is a contradiction.
Assume $v' \neq 0$. By (4),

$$v *_4 u' = -u *_3 v'.$$

As $N(v') \neq 0$, we obtain that $N(v')^{-1} \in F$. Taking norms we have

$$\begin{aligned} &a_4b_4c_4N(v)N(u') = (-1)^d a_3b_3c_3N(u)N(v') \\ \implies &N(u) = (-1)^d a_3^{-1}b_3^{-1}c_3^{-1}a_4b_4c_4N(v)N(u')N(v')^{-1}. \end{aligned}$$

Similarly taking norms of (3), we obtain

$$N(u)N(u') = (-1)^d a_2b_2c_2N(v)N(v'). \tag{5}$$

Substituting our expression for $N(u)$ into (5), we have

$$\begin{aligned} 0 =&N(u)N(u') - (-1)^d a_2b_2c_2N(v)N(v') \\ =&(-1)^d(a_3^{-1}b_3^{-1}c_3^{-1}a_4b_4c_4N(v)N(u')N(v')^{-1})N(u') - (-1)^d a_2b_2c_2N(v)N(v') \\ =&(-1)^d N(v)[(N(u')N(v')^{-1})^2 - a_2b_2c_2a_3b_3c_3a_4^{-1}b_4^{-1}c_4^{-1}]. \end{aligned} \tag{6}$$

If $N(v) = 0$, it follows that $v = 0$ (as N is nondegenerate) so by (3) $u *_1 u' = 0$ implies $u' = 0$ (else $(u, v) = (0, 0)$). By (6),

$$a_2b_2c_2a_3b_3c_3a_4^{-1}b_4^{-1}c_4^{-1} = 0 \notin F^\times.$$

So $N(v) \neq 0$. Then $(N(u')N(v')^{-1})^2 = a_2b_2c_2a_3b_3c_3a_4^{-1}b_4^{-1}c_4^{-1}$. Hence $a_2b_2c_2a_3b_3c_3a_4^{-1}b_4^{-1}c_4^{-1} \in N(S^\times)^2$. □

Applying this result with Lemma 4.1.4 gives an immediate corollary.

Corollary 4.1.6. *Let $A = Cay(S*_1, *_2, *_3, *_4)$ be unital. Then A is a division algebra if $a_2b_2c_2 \notin N(S^\times)^2$.*

4.1.1 *Applying this construction to a field extension*

Let K be a finite separable field extension of F and N be the reduced norm of K/F. The similarities and isometries of N are given by

$$S(N) = K^{\times} \rtimes \mathrm{Aut}_F(K)$$

and

$$O(N) = ker(N) \rtimes \mathrm{Aut}_F(K),$$

respectively [62].

Using this classification of the similarities of N, for any field extension K we can easily construct all isotopes $K^{(f,g,h)}$ such that $f, g, h \in S(N)$. Define $(K, *) = K^{(f,g,h)}$ such that $f, g, h \in S(N)$. Then $f(x) = a\sigma(x)$, $g(x) = b\theta(x)$ and $h(x) = c\phi(x)$ for some $a, b, c \in K^{\times}$ and $\sigma, \theta, \phi \in \mathrm{Aut}_F(K)$. Hence the multiplication in $(K, *)$ can be written as

$$\begin{aligned} x * y =& h(f(x)g(y)) \\ =& c\phi(a\sigma(x)b\theta(y)) \\ =& c\phi(ab)\phi(\sigma(x)\theta(y)), \end{aligned}$$

where juxtaposition of elements indicates the usual multiplication in K.

Let $d = c\phi(ab)$, $\sigma_1 = \phi \circ \sigma$, and $\sigma_2 = \phi \circ \theta$. Then we can express the multiplication in $(K, *)$ as

$$x * y = d\sigma_1(x)\sigma_2(y)$$

for some $d \in K^{\times}$ and $\sigma_1, \sigma_2 \in \mathrm{Aut}_F(K)$.

Starting with an algebraic field extension, this means that we can write our generalised Cayley-Dickson doubling as follows:

Let $A = Cay(K, *_1, *_2, *_3, *_4)$ be the F-vector space $K \oplus K$ with the multiplication

$$(u, v)(x, y) = (ux + d_2\sigma_{21}(v)\sigma_{22}(y), d_3\sigma_{31}(u)\sigma_{32}(y) + d_4\sigma_{41}(v)\sigma_{42}(x))$$

for some $d_2, d_3, d_4 \in K^{\times}$ and $\sigma_{1i}, \sigma_{2i} \in \mathrm{Aut}_F(K)$ for $i = 2, 3, 4$.

This scenario covers all possible cases of our construction when doubling a finite separable field extension.

Proposition 4.1.7. *A is a division algebra if $N(d_2 d_3 d_4^{-1}) \notin N(K^\times)^2$.*

Proof. In $(K, *_i)$, we have $N(xy) = N(x *_i y) = N(d_i \sigma_{i1}(x)\sigma_{i2}(y))$ for all $x, y \in K$. As N is multiplicative, this implies $N(xy) = N(d_i)N(x)N(y)$ for all $x, y \in K$. Thus by Theorem 4.1.5, A is a division algebra if

$$N(d_2)N(d_3)N(d_4)^{-1} = N(d_2 d_3 d_4^{-1}) \notin N(K^\times)^2.$$

□

Lemma 4.1.8. *A is unital if and only if the multiplication in A can be written as*

$$(u, v)(x, y) = (ux + d_2\sigma_1(v)\sigma_2(y), \sigma_3(u)y + v\sigma_4(x))$$

for some $d_2 \in K^\times$ and $\sigma_i \in \mathrm{Aut}_F(K)$ for $i = 1, 2, 3, 4$.

Proof. Let 1_K be the multiplicative identity in K. Then 1_K is a left unit in $(K, *_3)$ if and only if we have $1_K *_3 x = x$ for all $x \in K$. That is,

$$d_3\sigma_{31}(1_K)\sigma_{32}(x) = x$$

for all $x \in K$. As $\sigma_{31}(1_K) = 1_K$, we must have $d_3\sigma_{32}(x) = x$ for all $x \in K$. If $x \in F$, then $\sigma_{32}(x) = x$, which implies $d_3 = 1$. Thus we conclude that $\sigma_{32}(x) = x$ for all $x \in K$, so $\sigma_{32} = id_K$.
Similarly, 1_K is a right unit in $(K, *_4)$ if and only if we have $x *_4 1_K = x$ for all $x \in K$. That is,

$$d_4\sigma_{41}(x)\sigma_{42}(1_K) = x$$

for all $x \in K$. As $\sigma_{42}(1_K) = 1_K$, we must have $d_4\sigma_{41}(x) = x$ for all $x \in K$. If $x \in F$, $\sigma_{41}(x) = x$, which implies $d_4 = 1$. Thus it follows that $\sigma_{41}(x) = x$ for all $x \in K$, so $\sigma_{41} = id_K$.
By Lemma 4.1.2, A is unital if and only if 1_K is a left unit in $(K, *_3)$ and a right unit in $(K, *_4)$, and so the result follows after relabelling the automorphisms.

□

In order to simplify our computations we will only consider unital algebras for the rest of this section. We will denote these unital algebras by

$$Cay(K, d_2, \sigma_1, \sigma_2, \sigma_3, \sigma_4).$$

Corollary 4.1.9. *Let $A = Cay(K, d_2, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$. Then A is a division algebra if $N(d_2) \notin N(K^\times)^2$.*

Proof. This follows as a consequence of Lemma 4.1.7 and Lemma 4.1.8. □

4.1.2 *Examples of semifields*

Let F be a finite field and let $A = Cay(K, d_2, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$. Under certain conditions, our construction gives examples of semifields which are discussed in the literature [17].

Example 4.1.10. Let $\sigma \in \mathrm{Aut}_F(K)$ and $\mu, \eta \in K^\times$. Knuth gave four multiplications on $K \oplus K$ in [36] which give semifields when $x\sigma(x) + \mu x - \eta = 0$ has no solutions in K. For elements $x, y, u, v \in K$, define the four multiplications on $K \oplus K$ as follows:

$$Kn_1 : (u, v)(x, y) = (ux + \eta\sigma(y)\sigma^{-1}(v), yu + v\sigma(x) + \mu\sigma(y)\sigma^{-1}(v)),$$

$$Kn_2 : (u, v)(x, y) = (ux + \eta\sigma^{-1}(y)\sigma^{-2}(v), yu + v\sigma(x) + \mu y\sigma^{-1}(v)),$$

$$Kn_3 : (u, v)(x, y) = (ux + \eta\sigma^{-1}(y)v, yu + v\sigma(x) + \mu yv),$$

$$HK : (u, v)(x, y) = (ux + \eta\sigma(y)v, yu + v\sigma(x) + \mu\sigma(y)v).$$

We refer to the semifields defined by the first three multiplications as *Knuth semifields* and the last multiplication as *Hughes-Kleinfeld semifields.*
Our generalised Cayley Dickson construction gives the subclass of each of these semifields where $\mu = 0$.

Example 4.1.11. Let $[K : F] = 2$ and let $c \in K \setminus K^2$. Let $\sigma_1 = \sigma_3 = \sigma \in \mathrm{Aut}_F(K)$ be a nontrivial automorphism and $\sigma_2 = \sigma_4 = id$. Then A is a *Sandler semifield* with multiplication given by

$$(u, v)(x, y) = (ux + c\sigma(v)y, \sigma(u)y + vx).$$

Generally, let σ be an automorphism of K which fixes a subfield F_0, with $[K : F_0] = m$. Sandler semifields are defined as an F-vector space with basis $1, \lambda, \lambda^2, ..., \lambda^{m-1}$ with multiplication defined by

$$(\lambda^i x)(\lambda^j y) = \lambda^i \lambda^j \sigma^j(x)y$$

for all $x, y \in K$. Further we have $\lambda^i\lambda^j = \lambda^{i+j}$ for $i + j < m$ and $\lambda^i\lambda^j = \lambda^{(i+j) mod\, m}\delta$ for $i + j \geq m$, where $\delta \in K$ is not a root of any polynomial of degree less than m over F_0. Our construction can only be used to construct Sandler semifields for $m = 2$; in fact, all Sandler semifields with $m = 2$ can be constructed this way.

Example 4.1.12. Let F have characteristic not 2. Let $d_2 \in K^\times \setminus K^2$, $\sigma_4 = id$ and $\sigma_1, \sigma_2, \sigma_3 \in \mathrm{Aut}_F(K)$ be not all the identity automorphism. Then A is a *generalised Dickson semifield* with multiplication given by

$$(u, v)(x, y) = (ux + d_2\sigma_1(v)\sigma_2(y), \sigma_3(u)y + vx)$$

for all $u, v, x, y \in K$[36]. Knuth also referred to these semfields as Case I semifields quadratic over a weak nucleus. All generalised Dickson semifields have this form and as such can be obtained by our doubling process. In the special case where $\sigma_1 = \sigma_2 = \sigma \in \mathrm{Aut}_F(K)$ is a nontrivial automorphism and $\sigma_3 = id$, A is a *commutative Dickson semifield* [20] with multiplication given by

$$(u, v)(x, y) = (ux + d_2\sigma(vy), uy + vx).$$

Hughes-Kleinfeld, Knuth and Sandler semifield constructions were studied over arbitrary base fields in [58]. Dickson's commutative semifield construction was introduced over finite fields in [20] and considered over any base field of characteristic not 2 when K is a finite cyclic extension in [9].

We use Dickson's construction of commutative semifields and Knuth's subsequent generalized semifields to motivate a new construction using central simple algebras. We will first consider Dickson's construction where K is an arbitrary

finite extension in Section 4.2 to expand the results given in [9, 10, 20] and further generalise this construction to central simple algebras in Section 4.3. This results of Sections 4.2 and 4.3 have now been published and can be found in [59]. Additionally, we consider Knuth's construction of Case I semifields extended to a doubling of central simple algebras in Section 4.4. This construction is the subject of [60].

4.2 A DOUBLING PROCESS USING FINITE FIELD EXTENSIONS

4.2.1 *The construction process*

Let K be a finite separable field extension of F of degree n. For some $c \in K^\times$ and $\sigma \in \mathrm{Aut}_F(K)$, we define a multiplication on the F-vector space $K \oplus K$ by

$$(u, v)(x, y) = (ux + c\sigma(vy), uy + vx)$$

for all $u, v, x, y \in K$. Under this multiplication, $K \oplus K$ is a unital nonassociative ring which we denote by $D(K, \sigma, c)$. Note that $D(K, id, c)$ is isomorphic to a quadratic field extension of K when $c \in K \setminus K^2$ and that $D(K, id, c) \cong K \times K$ when $c \in (K^\times)^2$. Due to this, we will only consider $\sigma \neq id$. Note that F is canonically embedded into $D(K, \sigma, c)$ via the map $F \mapsto F \oplus 0$. Similarly, we will denote any subalgebras of the form $E \oplus 0$ simply by E.

Clearly $D = D(K, \sigma, c)$ is commutative. Over finite fields, it is known that when $\sigma \neq id$, then $\mathrm{Nuc}_l(D) = \mathrm{Nuc}_r(D) = \mathrm{Fix}(\sigma)$ and $\mathrm{Nuc}_m(D) = K$ [17, p.126]. This is also true for any arbitrary field and is easily checked.

Theorem 4.2.1. *Let $D = D(K, \sigma, c)$ with $\sigma \in \mathrm{Aut}_F(K)$ a non-trivial automorphism. Then we have $\mathrm{Nuc}_l(D) = \mathrm{Nuc}_r(D) = \mathrm{Fix}(\sigma)$ and $\mathrm{Nuc}_m(D) = K$. In particular, this yields $\mathrm{Nuc}(D) = \mathrm{Fix}(\sigma)$ and $Z(D) = \mathrm{Fix}(\sigma)$.*

Clearly all subfields E of K are subalgebras of $D(K, \sigma, c)$. Additionally, if E is a subfield of K such that $c \in E^\times$ and $\sigma|_E \in \mathrm{Aut}_F(E)$, then $D(E, \sigma|_E, c)$ is a subalgebra of $D(K, \sigma, c)$. Moreover, if $L = \mathrm{Fix}(\sigma)$ and $c \in L^\times$, then $L \oplus L$

under the product of D is an associative subalgebra of $D(K, \sigma, c)$.

4.2.2 *Division algebras*

Dickson [20] gave a sufficient condition for $D(K, \sigma, c)$ to be a nonassociative division algebra when F is an infinite field and K/F is a cyclic extension. Burmester further showed this was also a necessary condition [9, Theorem 1]. If we assume $K/\mathrm{Fix}(\sigma)$ is cyclic, [9, Theorem 1] extends naturally to our construction:

Theorem 4.2.2. *Let F be an infinite field and $L = \mathrm{Fix}(\sigma)$. If $\mathrm{Aut}_L(K) = \langle\sigma\rangle$, then $D(K, \sigma, c)$ is a division algebra over F if and only if $N_{K/L}(c) \neq N_{K/L}(a^2)$ for all $a \in K$.*

The proof is analogous to the proof of [9, Theorem 1]. As it uses [1, Theorem 5, p.200], we require that F is not a finite field.

If $K/\mathrm{Fix}(\sigma)$ is not a cyclic extension, this result does not necessarily hold. However, we can directly compute a different necessary and sufficient condition for $D(K, \sigma, c)$ to be a division algebra:

Theorem 4.2.3. *$D(K, \sigma, c)$ is a division algebra if and only if*

$$c \neq r^2 s\sigma(s)^{-1}t^{-1}\sigma(t)^{-1}$$

for all $r, s, t \in K^\times$.

Proof. Suppose $D(K, \sigma, c)$ is not a division algebra. Then there exist nonzero elements $(u, v), (x, y) \in K \oplus K$ such that $(u, v)(x, y) = (0, 0)$. This is equivalent to the simultaneous equations

$$ux + c\sigma(vy) = 0, \tag{7}$$

$$uy + vx = 0. \tag{8}$$

If $v = 0$, (8) becomes $uy = 0$, so either $u = 0$ or $y = 0$. However, u must be non-zero, else $(u, v) = (0, 0)$ which is a contradiction, so we must have $y = 0$.

Additionally, (7) gives $ux = 0$. As u is non-zero, this implies $x = 0$ and so $(x, y) = (0, 0)$ which is again a contradiction.
So let $v \neq 0$. As K is a field, we have $v^{-1} \in K$ and hence we obtain $x = -uyv^{-1}$ from (8). Now if $y = 0$, this implies that $x = 0$ which contradicts the assumption that $(x, y) \neq (0, 0)$. Substituting this into (7), we get $-u^2yv^{-1} + c\sigma(vy) = 0$, which rearranges to give $c = u^2y\sigma(y)^{-1}v^{-1}\sigma(v)^{-1}$.
Conversely, suppose $c = r^2s\sigma(s)^{-1}t^{-1}\sigma(t)^{-1}$ for some $r, s, t \in K^\times$. Consider the elements (r, t) and $(-rst^{-1}, s)$. Both elements are nonzero but satisfy

$$(r,t)(-rst^{-1},s) = (-r^2st^{-1} + r^2s\sigma(s)^{-1}t^{-1}\sigma(t)^{-1}\sigma(ts), rs - rst^{-1}t) = (0,0).$$

Hence $D(K, \sigma, c)$ is not a division algebra. □

Corollary 4.2.4. *If $N_{K/F}(c) \neq N_{K/F}(a)^2$ for all $a \in K^\times$, then $D(K, \sigma, c)$ is a division algebra.*

Proof. Suppose $D(K, \sigma, c)$ is not a division algebra. By Theorem 4.2.3, there exists some $r, s, t \in K^\times$ such that $c = r^2s\sigma(s)^{-1}t^{-1}\sigma(t)^{-1}$. Taking norms of both sides of the equation we obtain $N_{K/F}(c) = N_{K/F}(r^2s\sigma(s)^{-1}t^{-1}\sigma(t)^{-1})$. As the norm is multiplicative and $N_{K/F}(x) = N_{K/F}(\sigma(x))$, this yields

$$N_{K/F}(c) = N_{K/F}(r^2)N_{K/F}(s)N_{K/F}(s^{-1})N_{K/F}(t^{-1})^2,$$

which simplifies to $N_{K/F}(c) = N_{K/F}((rt^{-1})^2) = N_{K/F}((rt^{-1}))^2$. □

We could also note that Corollary 4.2.4 follows as a corollary from Theorem 4.1.5.

Corollary 4.2.5. *If c is a square in K, then $D(K, \sigma, c)$ is not a division algebra.*

Proof. In the notation of Theorem 4.2.3, let $s = t = 1$. Then if $c = r^2$ for some $r \in K$, then $D(K, \sigma, c)$ is not a division algebra. □

Remark 4.2.6. (i) Let $F = \mathbb{R}$ and $K = \mathbb{C}$. As every element of $\mathbb{C}$ is a square, no real division algebras arise as a result of this construction.

(ii) Similarly if F is a finite field of characteristic 2, we also do not obtain any division algebras: again, every element is a square, so $D(K, \sigma, c)$ is not a division algebra by Corollary 4.2.5.

Although there are no real division algebras or division algebras over $\mathbb{F}_{2^q}$ for any $q \in \mathbb{N}$, it is easy to find large examples of division algebras over $\mathbb{Q}$ and $\mathbb{Q}_p$ using this construction. This is particularly relevant due to their use in space time block coding, as mentioned in the introduction of this thesis (see [52] for an example). We give some examples of rational and p-adic division algebras now:

Example 4.2.7. (i) Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{a})$ for some $a \in \mathbb{Q} \setminus \mathbb{Q}^2$. Then we obtain $N_{K/\mathbb{Q}}(x + y\sqrt{a}) = x^2 - y^2 a$ for all $x, y \in \mathbb{Q}$. If we let $c = y\sqrt{a}$ for any $y \in \mathbb{Q}^\times$, this yields $N_{K/\mathbb{Q}}(c) = -y^2 a \notin \mathbb{Q}^2$, so we conclude that $D(K, \sigma, c)$ is a division algebra of dimension 4 over $\mathbb{Q}$.

(ii) Let $F = \mathbb{Q}_p$ and $K = \mathbb{Q}_p(\alpha)$ be a quadratic field extension of $\mathbb{Q}_p$. Thus K is equal to one of $\mathbb{Q}_p(\sqrt{p})$, $\mathbb{Q}_p(\sqrt{u})$ or $\mathbb{Q}_p(\sqrt{up})$, where $u \in \mathbb{Z}_p \setminus \mathbb{Z}_p^2$. If $p \equiv 1 \pmod 4$, it follows that $-\alpha^2 \notin \mathbb{Q}_p^2$ and thus for all $y \in \mathbb{Q}_p$, we have $N_{K/\mathbb{Q}_p}(y\alpha) = -y^2\alpha^2 \notin \mathbb{Q}_p^2$. Hence, $D(K, \sigma, y\alpha)$ is a division algebra of dimension 4 over $\mathbb{Q}_p$.

Remark 4.2.8. If F is a finite field of odd characteristic, we can see that Corollary 4.2.5 is also a necessary condition for $D(K, \sigma, c)$ to be a division algebra. This was originally proved in [9, Theorem 1'] but can also be obtained as a consequence of Theorem 4.2.3:

If $F = \mathbb{F}_{p^s}$ and $K = \mathbb{F}_{p^r}$ is a finite extension of F, it is known that $\mathrm{Aut}_F(K)$ is cyclic of order r/s and is generated by ϕ^s, where ϕ is defined by the Frobenius automorphism $\phi(x) = x^p$ for all $x \in K$. Over a finite field of odd characteristic, we thus have

$$\sigma(x)x = \phi^t(x)x = x^{p^{st}}x = x^{p^{st}+1}$$

for some $t \in \mathbb{Z}$. As p is odd, $p^{st} + 1 = 2n$ for some $n \in \mathbb{Z}$ and so we can write $\sigma(x)x = x^{2n} = (x^n)^2$ for all $x \in K$. A similar argument shows that $\sigma(x)x^{-1}$ is

a square for all $x \in K$. Hence over finite fields of odd characteristic, Theorem 4.2.3 yields that $D = D(K, \sigma, c)$ is a division algebra if and only if c is not a square in K.

4.2.3 *Isomorphisms*

For the rest of the section, we will assume that F has characteristic not 2 unless stated otherwise and that $\sigma \in \mathrm{Aut}_F(K)$ is a non-trivial automorphism. Burmester [9] computed the isomorphisms of commutative Dickson algebras $D(K, \sigma, c)$ when K is a cyclic extension of F. The notation originally used in [9] differs from ours; for clarity, we rephrase his result in our notation:

Theorem 4.2.9 ([9], Theorem 2)**.** *Let K be a cyclic field of degree n over F and let $\mathrm{Aut}_F(K) = \langle\sigma\rangle$. Then $D(K, \sigma^i, c) \cong D(K, \sigma^j, d)$ if and only if $i = j$, and if there exists an integer $0 \leqslant k < n$ and an element $x \in K$ such that $d = x^2\sigma^k(c)$.*

In order to generalise this result, we first note the following two lemmas:

Lemma 4.2.10. *Let $D(K, \sigma, c)$ and $D(L, \phi, d)$ be two commutative Dickson algebras over F. If $\mathrm{Fix}(\sigma) \ncong \mathrm{Fix}(\phi)$, then $D(K, \sigma, c) \ncong D(L, \phi, d)$ for any choice of $c \in K^\times$ and $d \in L^\times$.*

Proof. Suppose $D(K, \sigma, c) \cong D(L, \phi, c)$. As any isomorphism must map the centre of $D(K, \sigma, c)$ to the centre of $D(L, \phi, c)$, this implies $\mathrm{Fix}(\sigma) \cong \mathrm{Fix}(\phi)$. □

Lemma 4.2.11. *Let $\sigma \in \mathrm{Aut}_F(K)$ and $\phi \in \mathrm{Aut}_F(L)$. If there exists an F-isomorphism $\tau : K \to L$ such that $\tau \circ \sigma = \phi \circ \tau$, then $\tau|_{\mathrm{Fix}(\sigma)}\colon \mathrm{Fix}(\sigma) \to \mathrm{Fix}(\phi)$ is an F-isomorphism.*

Proof. For all $x \in \mathrm{Fix}(\sigma)$, it follows that

$$\phi \circ \tau(x) = \tau \circ \sigma(x) = \tau(x),$$

so $\tau(x) \in \mathrm{Fix}(\phi)$. Hence we conclude that $im(\tau\mid_{\mathrm{Fix}(\sigma)}) \subseteq \mathrm{Fix}(\phi)$. To show that in fact $im(\tau\mid_{\mathrm{Fix}(\sigma)}) = \mathrm{Fix}(\phi)$, we note that for any $y \in \mathrm{Fix}(\phi)$ there exists $x \in K$ such that $\tau(x) = y$. As $\tau(x) \in \mathrm{Fix}(\phi)$, this implies $\tau \circ \sigma(x) = \phi \circ \tau(x) = \tau(x)$, thus $x \in \mathrm{Fix}(\sigma)$ and it follows that
$im(\tau\mid_{\mathrm{Fix}(\sigma)}) = \mathrm{Fix}(\phi)$. This is sufficient to show that $\tau\mid_{\mathrm{Fix}(\sigma)}$: $\mathrm{Fix}(\sigma) \to \mathrm{Fix}(\phi)$ is an F-isomorphism. □

Theorem 4.2.12. *Let K and L be two finite field extensions of F and $D = D(K, \sigma, c)$ and $D' = D(L, \phi, d)$ be two commutative Dickson algebras over F. Then $G : D \to D'$ is an isomorphism if and only if G has the form*

$$G(x, y) = (\tau(x), \tau(y)b)$$

for some F-isomorphism $\tau : K \to L$ such that:

(i) $\phi \circ \tau = \tau \circ \sigma$,

(ii) there exists $b \in L^\times$ such that $\tau(c) = d\phi(b^2)$, i.e. $\tau(c)d^{-1}$ is a square in $L^\times$.

Proof. Suppose $G : D \to D'$ is an F-isomorphism. Then G maps the middle nucleus of D to the middle nucleus of D', so we must have $K \cong L$. This means G restricted to K must be an isomorphism which maps K to L; that is, $G|_K = \tau : K \to L$ is an isomorphism of fields and we conclude $G(x, 0) = (\tau(x), 0)$ for all $x \in K$. Additionally, by Lemma 4.2.10 we see that $Z(D) \cong Z(D')$ under G. Thus, it follows that τ restricted to $\mathrm{Fix}(\sigma)$ must yield an isomorphism from $\mathrm{Fix}(\sigma)$ to $\mathrm{Fix}(\phi)$. Let $G(0, 1) = (a, b)$ for some $a, b \in L$. This implies

$$G(x, y) = G(x, 0) + G(0, 1)G(y, 0) = (\tau(x) + a\tau(y), \tau(y)b).$$

As G is multiplicative, it follows that $G((0, 1)^2) = G(0, 1)^2$ which holds if and only if $(a, b)(a, b) = (\tau(c), 0)$. From this, we obtain the equations $a^2 + d\phi(b^2) = \tau(c)$ and $2ab = 0$. As L does not have characteristic 2, this implies either $a = 0$ or $b = 0$. If $b = 0$, then $G(x, y) = (\tau(x) + \tau(y)a, 0)$ and so G is not surjective. This is a contradiction, as G is an isomorphism and hence is bijective

by definition. Thus we obtain $a = 0$ and $d\phi(b^2) = \tau(c)$.
Finally, as G is multiplicative this yields $G(u,v)G(x,y) = G((u,v)(x,y))$ for all $u, v, x, y \in K$. Computing both sides of this equation, we get

$$(\tau(ux) + d\phi(\tau(vy)b^2), \tau(uy)b + \tau(vx)b) = (\tau(ux + c\sigma(vy)), \tau(uy + vx)b)$$

for all $u, v, x, y \in K$, which implies $d\phi(\tau(vy)b^2) = \tau(c\sigma(vy))$. After substituting the condition $d\phi(b^2) = \tau(c)$, we are left with $\phi(\tau(vy)) = \tau(\sigma(vy))$ for all $v, y \in K$; that is, $\phi \circ \tau = \tau \circ \sigma$.
Conversely, let $G : K \oplus K \to L \oplus L$ be defined by $G(x,y) = (\tau(x), \tau(y)b)$ for some F-isomorphism $\tau : K \to L$ satisfying the conditions stated in the theorem above. It is easily checked that this is an F-linear bijective map between vector spaces. We only need to check that the map is multiplicative. Then we have $G(u,v)G(x,y) = G((u,v)(x,y))$ for all $u, v, x, y \in K$ if and only if it follows that $d\phi(\tau(vy)b^2) = \tau(c\sigma(vy))$. As $d\phi(b^2) = \tau(c)$ and $\phi \circ \tau = \tau \circ \sigma$, this is satisfied for all $v, y \in K$. Further, by Lemma 4.2.11 this certainly maps the centre of D to the centre of D'. Thus we conclude that $G : D \to D'$ is an F-algebra isomorphism. □

Corollary 4.2.13. *Let $D = D(K, \sigma, c)$ and $D' = D(K, \phi, d)$ be two commutative Dickson algebras over F. Then $G : D \to D'$ is an F-algebra isomorphism if and only if G has the form*

$$G(x,y) = (\tau(x), \tau(y)b)$$

for some $\tau \in \mathrm{Aut}_F(K)$ such that:

(i) $\phi \circ \tau = \tau \circ \sigma$,

(ii) there exists $b \in K^\times$ such that $\tau(c) = d\phi(b^2)$, i.e. $\tau(c)d^{-1}$ is a square in $K^\times$.

Corollary 4.2.14. *Suppose $\mathrm{Aut}_F(K)$ is an abelian group. If $\sigma \neq \phi$, then $D(K, \sigma, c) \ncong D(K, \phi, d)$ for any choice of $c, d \in K^\times$.*

Corollary 4.2.15. *For all $c \in K^\times$, we have $D(K,\sigma,c) \cong D(K,\tau\circ\sigma\circ\tau^{-1},\tau(c))$ for each $\tau \in \mathrm{Aut}_F(K)$ and $D(K,\sigma,c) \cong D(K,\sigma,\sigma(b^2)c)$ for each $b \in K^\times$.*

Proof. This is clear employing the isomorphisms $G(x,y) = (\tau(x),\tau(y))$ and $G(x,y) = (x,b^{-1}y)$, respectively. □

When K is a finite field of odd characteristic, $\tau(c)d^{-1}$ is a square if and only if either both c and d are squares or both are non-squares in K. Due to this, we obtain the following well-known result from Theorem 4.2.12:

Corollary 4.2.16 ([9], Theorem 2')**.** *Let F be a finite field of odd characteristic and K be a finite extension of degree n. Let $D = D(K,\sigma,c)$ and $D' = D(K,\phi,d)$ be division algebras. Then $D \cong D'$ if and only if $\sigma = \phi$. Hence up to isomorphism, there are exactly n commutative Dickson semifields of order p^{2n}.*

Over an arbitrary field however, it is possible that $D(K,\sigma,c) \ncong D(K,\sigma,d)$ for some $c,d \in K$ as we cannot guarantee that there exists $b \in K$ such that $\sigma(b)^2 = \tau(c)d^{-1}$. Let us now consider $F = \mathbb{Q}_p$ for $p \neq 2$ as an example. We employ the following well-known result, giving the proof for completion:

Lemma 4.2.17. *Let $K/\mathbb{Q}_p$ be a finite field extension for $p \neq 2$ with uniformizer $\pi \in \mathcal{O}_K$, where $\mathcal{O}_K$ is the valuation ring of K. Then $K^\times/(K^\times)^2 = \{1,u,\pi,u\pi\}$ for some $u \in \mathcal{O}_K \setminus \mathcal{O}_K^2$.*

Proof. Every element of $K^\times$ can be written as $u\pi^n$ for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}_K^\times$. Then $x \in K^\times$ is a square if and only if $x = u^2\pi^{2n}$ for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}_K^\times$. Thus we see that $K^\times/(K^\times)^2 \cong \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \times \mathbb{F}_2$. Note the residue field of $\mathcal{O}_K$ is the finite field $\mathbb{F}_{p^e}$ for some $e \in \mathbb{N}$. Thus it follows that $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \cong \mathbb{F}_{p^e}/(\mathbb{F}_{p^e})^2 \cong \mathbb{F}_2$, as p is an odd prime. Hence we conclude $K^\times/(K^\times)^2 \cong \mathbb{F}_2 \times \mathbb{F}_2$; a complete set of coset representatives is thus given by $\{1,u,\pi,u\pi\}$ for some $u \in \mathcal{O}_K \setminus \mathcal{O}_K^2$. □

Corollary 4.2.18. *For each finite field extension $K/\mathbb{Q}_p$ such that $\mathrm{Aut}_{\mathbb{Q}_p}(K)$ is an abelian group, there are at most $3\left|\mathrm{Aut}_{\mathbb{Q}_p}(K)\right|$ non-isomorphic commutative Dickson division algebras of the kind $D(K,\sigma,c)$.*

Proof. As in Corollary 4.2.16, we see that $D(K,\sigma,c) \cong D(K,\phi,d)$ if and only if $\sigma = \phi$ and there exists some $\tau \in \mathrm{Aut}_{\mathbb{Q}_p}(K)$ and $b \in K^\times$ such that $\tau(c)d^{-1} = \sigma(b^2)$. Such $b \in K$ exists if and only if $\tau(c)d^{-1}$ is a square in K. If we assume that $D(K,\sigma,c)$ and $D(K,\sigma,d)$ are division algebras, c,d are certainly not squares in K and so must lie in non-identity cosets of $K^\times/(K^\times)^2$. It is clear that $\tau(c)$ must lie in the same coset as c. Considering the images of $\tau(c)$ and d^{-1} in the quotient group $K^\times/(K^\times)^2$, it follows that $\tau(c)d^{-1}$ is a square in $K^\times$ if and only if c and d lie in the same coset of $K^\times/(K^\times)^2$. As there are 3 non-trivial cosets, we conclude there are at most $3\left|\mathrm{Aut}_{\mathbb{Q}_p}(K)\right|$ non-isomorphic commutative Dickson division algebras. □

We cannot say for certain that we attain this bound, as this would assume that there exists a suitable $c \in K^\times$ in each non-trivial coset of $K^\times/(K^\times)^2$ such that $D(K,\sigma,c)$ is a division algebra for each $\sigma \in \mathrm{Aut}_{\mathbb{Q}_p}(K)$. However, if we can find some $c \in K^\times$ that satisfies the conditions of Corollary 4.2.4 from each coset of $K^\times/(K^\times)^2$, this is sufficient to show that there are exactly $3\left|\mathrm{Aut}_{\mathbb{Q}_p}(K)\right|$ non-isomorphic commutative Dickson division algebras. For an arbitrary field F, we conclude the following analogously:

Corollary 4.2.19. *Suppose K/F is a finite field extension such that $\mathrm{Aut}_F(K)$ is an abelian group and there exists $c \in K^\times$ such that $N_{K/F}(c) \neq N_{K/F}(a^2)$ for all $a \in K$. Then there are at least $|\mathrm{Aut}_F(K)|$ non-isomorphic commutative Dickson division algebras over F of the form $D(K,\sigma,c)$.*

4.2.4 *Automorphisms*

The automorphisms of commutative Dickson algebras were computed in [9] when K is a finite cyclic field extension. We consider the subset

$$J(c) = \{\tau \in \mathrm{Aut}_F(K) \mid X^2 - \tau(c)c^{-1} = 0 \text{ has solutions in } K\} \subset \mathrm{Aut}_F(K),$$

introduced in [9].

Lemma 4.2.20. *$J(c)$ is a subgroup of $\mathrm{Aut}_F(K)$.*

Proof. Clearly the identity automorphism is contained in $J(c)$, as $0 = X^2 - cc^{-1} = X^2 - 1$ always has the solutions $X = \pm 1$.
Let $\tau, \phi \in J(c)$. Then $\tau(c)c^{-1} = a^2$ and $\phi(c)c^{-1} = b^2$ for some $a, b \in K^\times$. It follows that

$$\phi \circ \tau(c)c^{-1} = \phi(a^2c)c^{-1} = \phi(a^2)b^2cc^{-1},$$

so $X^2 - \phi \circ \tau(c)c^{-1} = 0$ has the solutions $X = \pm\phi(a)b$. This implies $\phi \circ \tau \in J(c)$. Finally, for each $\tau \in J(c)$ we have $\tau^{-1}(c)c^{-1} = \tau^{-1}(a^{-1})^2$, so $\tau^{-1} \in J(c)$. □

When K is a cyclic extension, there exist $2\,|J(c)|$ automorphisms of $D(K, \sigma, c)$:

Theorem 4.2.21. *(i) [[9], Theorem 3 in our notation] Let K be a cyclic extension of F. Then there exist $2\,|J(c)|$ automorphisms of $D(K, \sigma, c)$, each of which is given by*

$$G(x, y) = (\tau(x), \tau(y)b_i)$$

for each $\tau \in J(c)$, where $b_i \in K$ are such that $\sigma(b_i)$ are the two solutions of $X^2 - \tau(c)c^{-1} = 0$ for $i = 1, 2$.

(ii) [[9], Theorem 3' in our notation] Let F be a finite field of odd characteristic and K be a finite extension of degree n. Then there exists $2n$ automorphisms of $D = D(K, \sigma, c)$, each of which is given by

$$G(x, y) = (\tau(x), \tau(y)b_i)$$

for each $\tau \in \mathrm{Aut}_F(K)$, where $b_i \in K$ are such that $\sigma(b_i)$ are the two solutions of $X^2 - \tau(c)c^{-1} = 0$ for $i = 1, 2$.

We now compute the automorphisms when K is an arbitrary finite field extension. We continue to assume that $\sigma \neq id$.

Theorem 4.2.22. *All automorphisms $G : D(K, \sigma, c) \to D(K, \sigma, c)$ are of the form*

$$G(u, v) = (\tau(u), \tau(v)b)$$

for some $\tau \in \mathrm{Aut}_F(K)$ such that τ and σ commute and $b \in K^\times$ satisfying $\tau(c) = c\sigma(b^2)$. Further, all maps of this form with $\tau \in \mathrm{Aut}_F(K)$ and $b \in K^\times$ satisfying these conditions yield an automorphism of D.

Proof. Let $D = D(K, \sigma, c)$. Suppose that $G \in \mathrm{Aut}_F(D)$. As automorphisms preserve the nuclei of an algebra, G restricted to K must be an automorphism of K. As G is F-linear we obtain $F \subset \mathrm{Fix}(G|_K)$ and so in fact $G|_K \in \mathrm{Aut}_F(K)$. Let $G|_K = \tau \in \mathrm{Aut}_F(K)$, so we have $G(x, 0) = (\tau(x), 0)$ for all $x \in K$.
Let $G(0, 1) = (a, b)$ for some $a, b \in K$. Then we have

$$G(x, y) = G(x, 0) + G(0, 1)G(y, 0) + (\tau(x) + a\tau(y), \tau(y)b).$$

As G is multiplicative, we must also have $G((0, 1)^2) = G(0, 1)^2$ which holds if and only if

$$(a, b)(a, b) = (\tau(c), 0).$$

From this, we obtain the equations $a^2 + c\sigma(b^2) = \tau(c)$ and $2ab = 0$. As K does not have characteristic 2, this implies that either $a = 0$ or $b = 0$. If $b = 0$, then $G(x, y) = (\tau(x) + \tau(y)a, 0)$ and so G is not surjective. This is a contradiction, as G is an automorphism. Thus $a = 0$ and we obtain $c\sigma(b^2) = \tau(c)$.
Finally, as G is multiplicative we have $G(u, v)G(x, y) = G((u, v)(x, y))$ for all $u, v, x, y \in K$. Computing both sides of this equation, we get

$$(\tau(ux) + c\sigma(\tau(vy)b^2), \tau(uy)b + \tau(vx)b) = (\tau(ux + c\sigma(vy)), \tau(uy + vx)b)$$

for all $u, v, x, y \in K$, which implies that $c\sigma(\tau(vy)b^2) = \tau(c\sigma(vy))$. After substituting the condition $c\sigma(b^2) = \tau(c)$, we are left with $\sigma(\tau(vy)) = \tau(\sigma(vy))$ for all $v, y \in K$; that is, τ and σ must commute.
Conversely, let $G : D \to D$ be a map defined by $G(x, y) = (\tau(x), \tau(y)b)$ such that τ and σ commute and $\tau(c) = c\sigma(b^2)$. It is easily checked that G is F-linear, bijective, additive and multiplicative. Hence G is an F-algebra automorphism of D. □

Corollary 4.2.23. *There is a subgroup of* $\mathrm{Aut}_F(D)$ *isomorphic to*

$$\{\tau \in \mathrm{Aut}_F(K) \mid \tau(c) = c \text{ and } \tau \circ \sigma = \sigma \circ \tau\}.$$

Proof. By Theorem 4.2.22, all automorphisms of D are of the form $G(x, y) = (\tau(x), \tau(y)b)$, such that τ and σ commute and $b \in K^\times$ satisfies $\tau(c) = c\sigma(b^2)$. If we let $b = 1$, we obtain a subgroup of $\mathrm{Aut}_F(D)$ such that τ and σ commute and $\tau(c) = c$. □

The subset of $\mathrm{Aut}_F(K)$ containing all the automorphisms of K which commute with $\sigma \in \mathrm{Aut}_F(K)$ is called the *centralizer of* σ *in* $\mathrm{Aut}_F(K)$ and is denoted by

$$C(\sigma) = \{\tau \in \mathrm{Aut}_F(K) \mid \tau \circ \sigma = \sigma \circ \tau\}.$$

This subset forms a subgroup of $\mathrm{Aut}_F(K)$, so $J(c) \cap C(\sigma)$ is also a subgroup of $\mathrm{Aut}_F(K)$. We get the following generalisation of [9, Theorem 3]:

Theorem 4.2.24. *There are exactly* $2\,|J(c) \cap C(\sigma)|$ *automorphisms of* $D(K, \sigma, c)$*, each of which is given by*

$$G(x, y) = (\tau(x), \tau(y)b_i)$$

for each $\tau \in J(c) \cap C(\sigma)$*, where* $b_i \in K^\times$ *is chosen such that* $\sigma(b_i)$ *are the two solutions of* $X^2 - \tau(c)c^{-1} = 0$ *for* $i = 1, 2$.

Proof. By Theorem 4.2.22, G is an automorphism of $D(K, \sigma, c)$ if and only if $G(u, v) = (\tau(u), \tau(v)b)$ for some $\tau \in C(\sigma)$ and $b \in K^\times$ such that $\sigma(b)^2 = \tau(c)c^{-1}$. We can find such $b \in K^\times$ if and only if $\tau \in J(c)$. Denote the solutions of $X^2 - \tau(c)c^{-1} = 0$ by $\sigma(b_1)$ and $\sigma(b_2)$. Thus G is an automorphism of $D(K, \sigma, c)$ if and only if $G(u, v) = (\tau(u), \tau(v)b_i)$ for each $\tau \in J(c) \cap C(\sigma)$, where $b_i \in K$ are such that $\sigma(b_i)$ are the two solutions of $X^2 - \tau(c)c^{-1} = 0$ for $i = 1, 2$. □

Corollary 4.2.25. *If* $\mathrm{Aut}_F(K)$ *is abelian, then* $D(K, \sigma, c)$ *has exactly* $2\,|J(c)|$ *automorphisms.*

Proof. This follows immediately from Theorem 4.2.24 after noting that $C(\sigma) = \mathrm{Aut}_F(K)$. □

Corollary 4.2.26. *If $c \in F^\times$, then $D(K, \sigma, c)$ has exactly $2\,|C(\sigma)|$ automorphisms.*

Proof. As $c \in F^\times$, for all $\tau \in \mathrm{Aut}_F(K)$ we have

$$0 = X^2 - \tau(c)c^{-1} = X^2 - cc^{-1} = X^2 - 1,$$

which always has the solutions $X = \pm 1$. This yields $J(c) = \mathrm{Aut}_F(K)$. The result then follows from Theorem 4.2.24. □

As $J(c) \cap C(\sigma)$ forms a subgroup of $\mathrm{Aut}_F(K)$, we know that $|J(c) \cap C(\sigma)|$ must divide $|\mathrm{Aut}_F(K)|$. Due to this, we can easily determine the exact size of the automorphism group of $D(K, \sigma, c)$ in certain cases.

Corollary 4.2.27. *If K is a field extension of prime degree p over F, $J(c)$ is equal to either $\{id\}$ or $\mathrm{Aut}_F(K)$. Further, $|\mathrm{Aut}_F(D(K, \sigma, c))| \in \{2, 2p\}$.*

Proof. Let $[K : F] = p$ for some prime p. Then $\mathrm{Aut}_F(K)$ is necessarily cyclic and hence abelian. As $|\mathrm{Aut}_F(K)| = p$, we must have $|J(c)| \in \{1, p\}$ and so $J(c) = \{id\}$ or $J(c) = \mathrm{Aut}_F(K)$. The remainder of the result follows from Corollary 4.2.25. □

Corollary 4.2.28. *If $F = \mathbb{Q}_p$ for $p \neq 2$, then $J(c) = \mathrm{Aut}_{\mathbb{Q}_p}(K)$ and*

$$\left|\mathrm{Aut}_{\mathbb{Q}_p}(D(K, \sigma, c))\right| = 2\,|C(\sigma)|\,.$$

Proof. As $\tau(c)$ and c^{-1} clearly lie in the same coset of $K^\times/(K^\times)^2$, it follows that $\tau(c)c^{-1} \in K^2$ for all $\tau \in \mathrm{Aut}_{\mathbb{Q}_p}(K)$. We conclude that $J(c) = \mathrm{Aut}_{\mathbb{Q}_p}(K)$ and thus $\left|\mathrm{Aut}_{\mathbb{Q}_p}(D(K, \sigma, c))\right| = 2\,|C(\sigma)|$ by Theorem 4.2.24. □

Generally it is difficult to actually calculate $J(c)$, so we instead bound the size of $\mathrm{Aut}_F(D(K, \sigma, c))$. We already have an upper bound as a consequence of Theorem 4.2.22. All the elements of $\mathrm{Aut}_F(K)$ which act as the identity on c form a subgroup of $\mathrm{Aut}_F(K)$ called the *isotropy group of c*, denoted by

$$\mathrm{Aut}_F(K)_c = \{\tau \in \mathrm{Aut}_F(K) \mid \tau(c) = c\}.$$

By Corollary 4.2.23, there is a subgroup of $\mathrm{Aut}_F(D(K, \sigma, c))$ which is isomorphic to $C(\sigma) \cap \mathrm{Aut}_F(K)_c$. This allows us to bound the size of the automorphism group of $D(K, \sigma, c)$ from below:

Theorem 4.2.29. *There are between* $2\left|C(\sigma)\cap \mathrm{Aut}_F(K)_c\right|$ *and* $2\left|C(\sigma)\right|$ *automorphisms of* $D(K,\sigma,c)$.

Proof. It is clear that $J(c)\cap C(\sigma)$ is a subgroup of $C(\sigma)$. Each $\tau\in C(\sigma)$ can be used to construct at most 2 automorphisms of $D(K,\sigma,c)$ corresponding to the two possible solutions of $X^2-\tau(c)c^{-1}=0$, so we have $\left|\mathrm{Aut}_F(D(K,\sigma,c))\right|\leqslant 2\left|C(\sigma)\right|$.
Additionally, each $\tau\in C(\sigma)\cap \mathrm{Aut}_F(K)_c$ can be used to construct the maps $(x,y)\mapsto(\tau(x),\pm\tau(y))$. It follows from Theorem 4.2.22 that these are automorphisms of $D(K,\sigma,c)$, so $2\left|C(\sigma)\cap \mathrm{Aut}_F(K)_c\right|\leqslant\left|\mathrm{Aut}_F(D(K,\sigma,c))\right|$. □

Wene [61] derived an alternative description of the automorphism group of $D(K,\sigma,c)$ when K is a finite field, in terms of inner automorphisms. An automorphism θ of $D(K,\sigma,c)$ is an *inner automorphism* if there exists $m\in D(K,\sigma,c)$ with left inverse m_l^{-1} such that

$$\theta(x)=(m_l^{-1}x)m$$

for all $x\in D(K,\sigma,c)$. The proof given in [61, Theorem 18] holds verbatim for any finite field extension, yielding a sufficient condition for the existence of (nontrivial) inner automorphisms of a commutative Dickson algebra:

Theorem 4.2.30 ([61], Theorem 18)**.** *Let* $D(K,\sigma,c)$ *be a division algebra. Denote* $\lambda=(0,1)$. *Then*

$$\Phi(x,y)=[\lambda_l^{-1}(x,y)]\lambda=(\sigma(x),\sigma(y))$$

defines an inner automorphism of $D(K,\sigma,c)$ *if and only if* $\sigma(c)=c$.

4.2.5 *The group structure of* $\mathrm{Aut}_F(D)$

By Theorem 4.2.22, we know that all the $2\left|C(\sigma)\cap J(c)\right|$ automorphisms of D are of the form $G(u,v)=(\tau(u),\tau(v)b)$ for some $\tau\in C(\sigma)\cap J(c)$ and $b\in K^\times$ such that $\sigma(b)^2=\tau(c)c^{-1}$. Note that this final condition is equivalent to $b\in K^\times$ being a solution of

$$X^2-\sigma^{-1}(\tau(c)c^{-1})=0.$$

We will denote the solutions of this polynomial by $b_{\tau,1}$ and $b_{\tau,2}$. As the characteristic of F is not 2, it is clear that $b_{\tau,2} = -b_{\tau,1}$.

Lemma 4.2.31. *Let $b_{\tau,1}, b_{\tau,2}$ be the two solutions of $X^2 - \sigma^{-1}(\tau(c)c^{-1}) = 0$ and suppose $\tau^n = id$. Then $b_{\tau,i}\tau(b_{\tau,i})\tau^2(b_{\tau,i})...\tau^{n-1}(b_{\tau,i}) = \pm 1$.*
Moreover, if n is odd, we have $b_{\tau,i}\tau(b_{\tau,i})\tau^2(b_{\tau,i})...\tau^{n-1}(b_{\tau,i}) = 1$ for $i = 1$ or $i = 2$, but not both.

Proof. As in the proof of Lemma 4.2.20, if b_τ and b_ϕ are solutions of $X^2 - \sigma^{-1}(\tau(c)c^{-1}) = 0$ and $X^2 - \sigma^{-1}(\phi(c)c^{-1}) = 0$ respectively then the equation

$$X^2 - \sigma^{-1}(\phi \circ \tau(c)c^{-1}) = 0$$

has the solutions $X = \pm\phi(b_\tau)b_\phi$. Similarly the equation $X^2 - \sigma^{-1}(\tau^2(c)c^{-1}) = 0$ has the solutions $X = \pm\tau(b_\tau)b_\tau$, the equation $X^2 - \sigma^{-1}(\tau^3(c)c^{-1}) = 0$ has the solutions $X = \pm\tau(b_{\tau^2})b_\tau = \tau^2(b_\tau)\tau(b_\tau)b_\tau$, and so on. Hence we see that for $i = 1, 2$

$$b_{\tau,i}\tau(b_{\tau,i})\tau^2(b_{\tau,i})...\tau^{n-1}(b_{\tau,i})$$

is a solution of $X^2 - \sigma^{-1}(\tau^n(c)c^{-1}) = 0$. As $\tau^n = id$, we also conclude that the solutions of

$$0 = X^2 - \sigma^{-1}(\tau^n(c)c^{-1}) = X^2 - \sigma^{-1}(cc^{-1}) = X^2 - 1$$

are $X = \pm 1$ and so $b_{\tau,i}\tau(b_{\tau,i})\tau^2(b_{\tau,i})...\tau^{n-1}(b_{\tau,i}) = \pm 1$. As $b_{\tau,2} = -b_{\tau,1}$, we have

$$b_{\tau,2}\tau(b_{\tau,2})\tau^2(b_{\tau,2})...\tau^{n-1}(b_{\tau,2}) = (-1)^n b_{\tau,1}\tau(b_{\tau,1})\tau^2(b_{\tau,1})...\tau^{n-1}(b_{\tau,1}).$$

If n is odd, this implies that

$$b_{\tau,2}\tau(b_{\tau,2})\tau^2(b_{\tau,2})...\tau^{n-1}(b_{\tau,2}) = -b_{\tau,1}\tau(b_{\tau,1})\tau^2(b_{\tau,1})...\tau^{n-1}(b_{\tau,1})$$

and the result follows. □

Theorem 4.2.32. *For all $D(K, \sigma, c)$, we have*

$$\mathrm{Aut}_F(D(K, \sigma, c)) \cong (C(\sigma) \cap J(c)) \times \mathbb{F}_2.$$

Proof. As $C(\sigma) \cap J(c)$ is a finite group, there exists a minimal generating set $\{\tau_1, ..., \tau_m\}$. Let τ be an element of this generating set and let $b_{\tau,i}$ $(i = 1, 2)$ be the two roots of $X^2 - \sigma^{-1}(\tau(c)c^{-1})$. As $J(c)$ is a finite group, τ^n must be equal to the identity for some $n > 1$. By Lemma 4.2.31, this implies

$$b_{\tau,i}\tau(b_{\tau,i})\tau^2(b_{\tau,i})...\tau^{n-1}(b_{\tau,i}) = \pm 1$$

for $i = 1, 2$. If n is odd, relabel the roots such that $b_{\tau,1}$ satisfies

$$b_{\tau,1}\tau(b_{\tau,1})\tau^2(b_{\tau,1})...\tau^{n-1}(b_{\tau,1}) = 1$$

and $b_{\tau,2}$ satisfies

$$b_{\tau,2}\tau(b_{\tau,2})\tau^2(b_{\tau,2})...\tau^{n-1}(b_{\tau,2}) = -1.$$

Henceforth, we will denote $b_{\tau,1} = b_\tau$. Now let $\phi \in C(\sigma) \cap J(c)$. As $\{\tau_1, ..., \tau_m\}$ generates $C(\sigma) \cap J(c)$, ϕ can be expressed as a product of the τ_i. Due to this, we can construct the roots of $X^2 - \sigma^{-1}(\phi(c)c^{-1}) = 0$ from the b_{τ_i}. For example, if $\phi = \tau_i \circ \tau_j$ then we obtain

$$b_\phi = b_{\tau_i}\tau_i(b_{\tau_j}).$$

This method can be applied recursively to construct the roots of $X^2 - \sigma^{-1}(\tau(c)c^{-1}) = 0$ for all $\tau \in C(\sigma) \cap J(c)$.

We can now express all automorphisms of D in the form $G(u, v) = (\tau(u), \pm\tau(v)b_\tau)$ for some $\tau \in J(c) \cap C(\sigma)$ and b_τ as defined above. Define a map $\Phi : \mathrm{Aut}_F(D) \to (J(c) \cap C(\sigma)) \times \mathbb{F}_2$ by

$$\Phi(G) = (\tau, \pm 1).$$

This map is well-defined due to the careful labelling of roots of $X^2 - \sigma^{-1}(\tau(c)c^{-1}) = 0$. It is easy to see that it gives an isomorphism between groups. □

Corollary 4.2.33. *If $F = \mathbb{Q}_p$, then $\mathrm{Aut}_{\mathbb{Q}_p}(D(K, \sigma, c)) \cong C(\sigma) \times \mathbb{F}_2$.*

Proof. This follows from Corollary 4.2.28. □

Thus it is sufficient to consider the subgroups of $\mathrm{Aut}_F(K)$, $C(\sigma)$ and $J(c)$, in order to determine the structure of the automorphism groups of these algebras.

4.3 USING DICKSON'S DOUBLING PROCESS WITH CENTRAL SIMPLE ALGEBRAS

Let B be an associative division algebra over F. Let $\sigma \in \mathrm{Aut}_F(B)$ be a non-trival automorphism and $c \in B^\times$. As B is not commutative, we can generalise the classical Dickson multiplication on the F-vector space $B \oplus B$ in three ways:

- $(u, v) \circ (x, y) = (ux + c\sigma(vy), uy + vx)$,
- $(u, v) \circ (x, y) = (ux + \sigma(v)c\sigma(y), uy + vx)$,
- $(u, v) \circ (x, y) = (ux + \sigma(vy)c, uy + vx)$.

We denote the F-vector space $B \oplus B$ endowed with each of these multiplications by $D(B, \sigma, c)$, $D_m(B, \sigma, c)$ and $D_r(B, \sigma, c)$, respectively. If $c \in F^\times$, the three constructions are identical. All three constructions yield unital nonassociative algebras over F and are canonical generalisations of the commutative construction defined by Dickson.

Lemma 4.3.1. *(i) Let $D = D(B, \sigma, c)$ or $D = D_r(B, \sigma, c)$. Then* $\mathrm{Comm}(D) = F \oplus F$.

(ii) Let $D = D_m(B, \sigma, c)$. If $c \in F^\times$, then $\mathrm{Comm}(D) = F \oplus F$. *Otherwise,* $\mathrm{Comm}(D) = F$.

Proof. (i) We only show the proof for $D(B, \sigma, c)$ as the proof for $D_r(B, \sigma, c)$ follows identically. Let $(u, v) \in \mathrm{Comm}(D)$. Then for all $x \in B$, we have

$$(u, v)(x, 0) = (x, 0)(u, v).$$

This is equivalent to $ux = xu$ and $vx = xv$. This holds for all $x \in B$ if and only if both u and v lie in the centre of B. Hence $\mathrm{Comm}(D) \subseteq F \oplus F$. It is easily checked that all elements of $F \oplus F$ are contained in $\mathrm{Comm}(D)$. Hence $\mathrm{Comm}(D) = F \oplus F$.

(ii) Let $(u, v) \in \mathrm{Comm}(D)$. Then for all $x \in B$, we have $(u, v)(0, x) = (0, x)(u, v)$. This is equivalent to $\sigma(v)c\sigma(x) = \sigma(x)c\sigma(v)$ and $ux = xu$. The second equation implies that $u \in Z(B) = F$. If $c \notin F$, then the first equation is only satisfied for all $x \in B$ when $v = 0$, which yields $\mathrm{Comm}(D) = F$.
If $c \in F^\times$, we have $D_m(B, \sigma, c) = D(B, \sigma, c)$ and so by (i), we obtain that $\mathrm{Comm}(D) = F \oplus F$.

□

Theorem 4.3.2. *Let $D = D(B, \sigma, c)$. Then*

- $\mathrm{Nuc}_l(D) = \{k \in B \mid c\sigma(k) = kc\} \subset B$,
- $\mathrm{Nuc}_m(D) = B$,
- $\mathrm{Nuc}_r(D) = \mathrm{Fix}(\sigma)$.

In particular,

$$\mathrm{Nuc}(D) = \mathrm{Fix}(\sigma) \cap \{k \in B \mid c\sigma(k) = kc\} = \{k \in \mathrm{Fix}(\sigma) \mid ck = kc\}$$

and $Z(D) = F$.

Proof. We will show the proof for the left nucleus. The calculations for the middle and right nucleus are obtained similarly.
Suppose (k, l) lies in the left nucleus for some $k, l \in B$. Then for all $x \in B$, we must have

$$((k, l)(0, 1))(x, 0) = (k, l)((0, 1)(x, 0)).$$

Computing both sides of this it follows that

$$(c\sigma(l)x, kx) = (c\sigma(lx), kx).$$

As σ is a non-trivial automorphism of B, this is true for all $x \in B$ if and only if $l = 0$. Thus we only need to consider elements of the form $(k, 0)$ for $k \in B$. Now $(k, 0) \in \mathrm{Nuc}_l(D)$ if and only if we obtain

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

for all $u, v, x, y \in B$. Computing both sides of this, this yields

$$(kux + c\sigma(kvy), kuy + kvx) = (kux + kc\sigma(vy), kuy + kvx).$$

This is satisfied for all $u, v, x, y \in B$ if and only if $c\sigma(k) = kc$. Hence we have that

$$\mathrm{Nuc}_l(D) = \{(k, 0) \mid k \in B \text{ such that } c\sigma(k) = kc\}.$$

As the centre is the intersection of the nucleus and the commutator, this yields $Z(D) = (\mathrm{Fix}(\sigma) \cap \{k \in B \mid c\sigma(k) = kc\} \cap F) \oplus 0 = F \oplus 0$. □

Similarly, we can calculate the left, middle and right nuclei and centre of $D_r(B, \sigma, c)$ and $D_m(B, \sigma, c)$:

Theorem 4.3.3. *Let $D = D_r(B, \sigma, c)$. Then*

- $\mathrm{Nuc}_l(D) = \mathrm{Fix}(\sigma)$,
- $\mathrm{Nuc}_m(D) = B$,
- $\mathrm{Nuc}_r(D) = \{k \in B \mid c\sigma(k) = kc\} \subset B$.

In particular, $\mathrm{Nuc}(D) = \{k \in \mathrm{Fix}(\sigma) \mid ck = kc\}$ *and* $Z(D) = F$.

Theorem 4.3.4. *Let $D = D_m(B, \sigma, c)$. Then*

- $\mathrm{Nuc}_l(D) = \mathrm{Fix}(\sigma)$,
- $\mathrm{Nuc}_m(D) = \{k \in B \mid \sigma(k)c = c\sigma(k)\} \subset B$,
- $\mathrm{Nuc}_r(D) = \mathrm{Fix}(\sigma)$.

In particular, $\mathrm{Nuc}(D) = \{k \in \mathrm{Fix}(\sigma) \mid ck = kc\}$ *and* $Z(D) = F$.

Note that if $c \in F^\times$, the three algebras we obtain are identical as noted earlier. In this case, the left and right nuclei are equal to $\mathrm{Fix}(\sigma)$ and the middle nucleus is equal to B. However if $c \notin F$, we obtain at least 2 non-isomorphic algebras from the construction:

Corollary 4.3.5. *Let $c \in B \setminus F^\times$. Then*

- $D(B,\sigma,c) \ncong D_m(B,\sigma,c)$,
- $D_m(B,\sigma,c) \ncong D_r(B,\sigma,c)$.

If c does not commute with all elements of $\mathrm{Fix}(\sigma)$*, then* $D(B,\sigma,c) \ncong D_r(B,\sigma,c)$.

Proof. Since automorphisms preserve each of the left, middle and right nuclei, if $D(B,\sigma,c) \cong D_m(B,\sigma,c)$ this implies that $\{k \in B \mid \sigma(k)c = c\sigma(k)\} = B$. As $c \notin F$, we can find $k \in B$ such that $\sigma(k)$ does not commute with c so this is never true. An identical argument shows that $D_m(B,\sigma,c) \ncong D_r(B,\sigma,c)$. Finally, we see that $D(B,\sigma,c) \cong D_r(B,\sigma,c)$ occurs only if $\mathrm{Fix}(\sigma) = \{k \in B \mid kc = c\sigma(k)\}$. Let $x \in \mathrm{Fix}(\sigma)$. We have $x \in \{k \in B \mid kc = c\sigma(k)\}$ if and only if $cx = xc$.
Similarly, if we take an element $y \in \{k \in B \mid kc = c\sigma(k)\}$, it lies in $\mathrm{Fix}(\sigma)$ if and only if $cy = yc$. Thus the left nuclei of the two algebras are equal only when c commutes with all of $\mathrm{Fix}(\sigma)$. Otherwise, we must have $D(B,\sigma,c) \ncong D_r(B,\sigma,c)$. □

Similarly to the algebras we obtained from doubling a field extension, any F-subalgebra of B appears as a subalgebra of $D(B,\sigma,c)$, $D_m(B,\sigma,c)$ and $D_r(B,\sigma,c)$. Additionally, if $E \subset B$ is such that $c \in E^\times$ and $\sigma|_E \in \mathrm{Aut}_F(E)$, then $D(E,\sigma|_E,c)$ (resp. $D_m(E,\sigma|_E,c)$ and $D_r(E,\sigma|_E,c)$) is a subalgebra of $D(B,\sigma,c)$ (resp. $D_m(B,\sigma,c)$ and $D_r(B,\sigma,c)$). In particular, this yields the following:

Theorem 4.3.6. *If $c \in K^\times$ for some separable field extension K/F contained in B such that $\sigma|_K = \phi \in \mathrm{Aut}_F(K)$, then $D(K,\phi,c)$ is a commutative Dickson subalgebra of $D(B,\sigma,c)$, $D_m(B,\sigma,c)$ and $D_r(B,\sigma,c)$.*

Theorem 4.3.7. *(i) $D = D(B,\sigma,c)$ is a division algebra if and only if $c \neq rt^{-1}rs\sigma(s^{-1}t^{-1})$ for all $r,s,t \in B^\times$.*

(ii) $D_m(B,\sigma,c)$ is a division algebra if and only if $c \neq \sigma(t)^{-1}rt^{-1}rs\sigma(s)^{-1}$ for all $r,s,t \in B^\times$.

(iii) $D_r(B, \sigma, c)$ *is a division algebra if and only if* $c \neq \sigma(s^{-1}t^{-1})rt^{-1}rs$ *for all* $r, s, t \in B^\times$.

Proof. (i): Suppose that D is not a division algebra. Then there exist nonzero elements $(u, v), (x, y) \in B \oplus B$ such that $(u, v)(x, y) = (0, 0)$. This is equivalent to the simultaneous equations

$$ux + c\sigma(vy) = 0, \tag{9}$$

$$uy + vx = 0. \tag{10}$$

If $v = 0$, then (10) becomes $uy = 0$, so either $u = 0$ or $y = 0$. However, u must be nonzero, else $(u, v) = (0, 0)$ which is a contradiction, so we must have $y = 0$. Additionally, (9) gives $ux = 0$. As u is nonzero, this implies $x = 0$ and so $(x, y) = (0, 0)$ which is again a contradiction.

So let $v \neq 0$. As B is an associative division algebra, we have $v^{-1} \in B$ and hence we obtain

$$x = -v^{-1}uy$$

from (10). Now if $y = 0$, this implies that $x = 0$ which is a contradiction to $(x, y) \neq (0, 0)$. Substituting this into (9), we get

$$-uv^{-1}uy + c\sigma(vy) = 0,$$

which rearranges to give $c = uv^{-1}uy\sigma(y)^{-1}\sigma(v)^{-1}$.

Conversely, suppose $c = rt^{-1}rs\sigma(s)^{-1}\sigma(t)^{-1}$ for some $r, s, t \in K^\times$. Consider the elements (r, t) and $(-t^{-1}rs, s)$. Both elements are nonzero but satisfy

$$\begin{aligned}(r, t)(-t^{-1}rs, s) &= (-rt^{-1}rs + rt^{-1}rs\sigma(s)^{-1}\sigma(t)^{-1}\sigma(ts), rs - tt^{-1}rs)\\ &= (0, 0).\end{aligned}$$

Hence D is not a division algebra.

The proofs of (ii) and (iii) follow almost identically to (i). □

Corollary 4.3.8. *If* $c \in (B^\times)^2$, *then* $D(B, \sigma, c), D_m(B, \sigma, c)$, *and* $D_r(B, \sigma, c)$ *are not division algebras.*

Proof. This follows from setting $s = t = 1$ in Theorem 4.3.7. □

Corollary 4.3.9. *Let $N_{B/F} : B \to F$ be the nondegenerate multiplicative norm form on B. The algebras $D = D(B, \sigma, c)$, $D_m(B, \sigma, c)$, $D_r(B, \sigma, c)$ are division algebras if*

$$N_{B/F}(c) \neq N_{B/F}(a)^2$$

for all $a \in B$.

Proof. This follows analogously to Corollary 4.2.4. □

Example 4.3.10. (i) Let $F = \mathbb{Q}$ and $B = (a, b)$ be a quaternion division algebra over $\mathbb{Q}$ with $a, b > 0$. For all $x \in B^\times$, we see that $N_{B/\mathbb{Q}}(x)^2 > 0$; as a consequence, $D(B, \sigma, c)$ is a division algebra for any $c \in B^\times$ such that $N_{B/\mathbb{Q}}(c) < 0$. For example, if we pick $c = c_1 i + c_2 j$ for some $c_i \in \mathbb{Q}$ not both zero, then

$$N_{B/\mathbb{Q}}(c) = -c_1^2 a - c_2^2 b < 0,$$

so $D(B, \sigma, c)$ is a division algebra.

(ii) Let $F = \mathbb{Q}_p$ and $B = (u, p)$ be the unique quaternion division algebra over $\mathbb{Q}_p$ for some $u \in \mathbb{Z}_p \setminus (\mathbb{Z}_p)^2$ with basis $\{1, i, j, k\}$ where $i^2 = u$, $j^2 = p$ and $k = ij = -ji$. Then for all $c \in B$, it follows that

$$N_{B/\mathbb{Q}_p}(c) = x^2 - y^2 u - z^2 p + w^2 up$$

for some $x, y, z, w \in \mathbb{Q}_p$. As up is not a square in $\mathbb{Q}_p$, for any $c \in B$ such that $N_{B/\mathbb{Q}_p}(c) = w^2 up$ we conclude that $D(B, \sigma, c)$ is a division algebra over $\mathbb{Q}_p$.

4.3.1 *Isomorphisms*

The results and proofs from Section 4.2 regarding isomorphisms and automorphisms of commutative Dickson algebras generalise almost identically to $D(B, \sigma, c)$ and $D_r(B, \sigma, c)$, as the middle nuclei of these algebras are equal to B. First note the following result:

Lemma 4.3.11. *Let $D = D(B, \sigma, c)$, $D' = D(B', \phi, d)$ be two Dickson algebras over F. If there exists an F-isomorphism $\tau : B \to B'$ such that $\tau \circ \sigma = \phi \circ \tau$ and $\tau(c) = db^2$ for some $b \in F^\times$, then $\tau|_{\mathrm{Nuc}_l(D)}$: $\mathrm{Nuc}_l(D) \to \mathrm{Nuc}_l(D')$ is an F-isomorphism.*

Proof. As with the proof of Lemma 4.2.11, we only need to show that

$$\mathrm{Im}(\tau|_{\mathrm{Nuc}_l(D)}) = \mathrm{Nuc}_l(D').$$

First, consider $x \in \mathrm{Nuc}_l(D)$. It follows that x must satisfy $c\sigma(k) = kc$. Applying τ to both sides of the equation and substituting in the condition on $\tau(c)$, we obtain

$$db^2\tau(\sigma(k)) = \tau(k)db^2.$$

As $b \in F^\times$, we can cancel this from both sides. After substituting $\tau \circ \sigma = \phi \circ \tau$, this yields $d\phi(\tau(k)) = \tau(k)d$ and thus $\tau(k) \in \mathrm{Nuc}_l(D')$. Hence

$$\mathrm{Im}(\tau|_{\mathrm{Nuc}_l(D)}) \subseteq \mathrm{Nuc}_l(D').$$

In order to show equality, we follow an analogous process to the one in the proof of Lemma 4.2.11. □

It is clear that the above proof also holds when considering the right nucleus of $D_r(B, \sigma, c)$, as this is equal to the left nucleus of $D(B, \sigma, c)$. We will always assume that B, B' are central simple division algebras over F. We now give a proof of the generalisation of Theorem 4.2.12:

Theorem 4.3.12. *Let $D = D(B, \sigma, c)$ and $D' = D(B', \phi, d)$ be F-algebras. Then $G : D \to D'$ is an isomorphism if and only if G has the form*

$$G(x, y) = (\tau(x), \tau(y)b)$$

for some F-isomorphism $\tau : B \to B'$ such that $\phi \circ \tau = \tau \circ \sigma$ and $\tau(c) = db^2$ for some $b \in F^\times$.

Proof. Suppose $G : D \to D'$ is an F-isomorphism. Then G maps the middle nucleus of D to the middle nucleus of D', so by Theorem 4.3.2 this implies

$B \cong B'$. This means G restricted to B must be an isomorphism which maps to B'; that is, $G|_B = \tau : B \to B'$, so this yields $G(x,0) = (\tau(x),0)$ for all $x \in B$. Let $G(0,1) = (a,b)$ for some $a,b \in B'$. Then we have $G(x,y) = G(x,0) + G(0,1)G(y,0) = (\tau(x) + a\tau(y), \tau(y)b)$, and $G(x,y) = G(x,0) + G(y,0)G(0,1) = (\tau(x) + \tau(y)a, b\tau(y))$. This implies that $a,b \in Z(B') = F$.
As G is multiplicative, it follows that $G((0,1)^2) = G(0,1)^2$ which holds if and only if $(a,b)(a,b) = (\tau(c),0)$. From this, we obtain the equations

$$a^2 + d\phi(b^2) = \tau(c),\ ab + ba = 0.$$

Since we established that $a,b \in F$, this simplifies to $a^2 + db^2 = \tau(c)$ and $2ab = 0$. As F does not have characteristic 2, this implies that either $a = 0$ or $b = 0$. If $b = 0$, then $G(x,y) = (\tau(x) + \tau(y)a, 0)$ and so G is not surjective. This is a contradiction, as G is an isomorphism. Thus $a = 0$ and we obtain $db^2 = \tau(c)$.
Finally, as G is multiplicative it follows that $G(u,v)G(x,y) = G((u,v)(x,y))$ for all $u,v,x,y \in K$. Computing both sides of this equation, we get

$$(\tau(ux) + d\phi(\tau(v)b\tau(y)b), \tau(uy)b + \tau(v)b\tau(x)) = (\tau(ux + c\sigma(vy)), \tau(uy + vx)b)$$

for all $u,v,x,y \in K$. As $b \in F$, this implies $db^2\phi(\tau(vy)) = \tau(c\sigma(vy))$. After substituting the condition $\tau(c) = d\phi(b^2)$, we conclude $\phi \circ \tau = \tau \circ \sigma$.
Conversely, let $G : B \oplus B \to B' \oplus B'$ be defined by $G(x,y) = (\tau(x), \tau(y)b)$ for some F-isomorphism $\tau : B \to B'$ such that $\phi \circ \tau = \tau \circ \sigma$ and $\tau(c) = db^2$ for some $b \in F^\times$. By Lemma 4.2.11 and Lemma 4.3.11, we see that G maps the nuclei of D isomorphically to the nuclei of D'. Thus, it is easily checked that this G gives an F-algebra isomorphism from D to D'. □

Theorem 4.3.13. *Let $D = D_r(B,\sigma,c)$ and $D' = D_r(B',\phi,d)$ be F-algebras. Then $G : D \to D'$ is an isomorphism if and only if G has the form*

$$G(x,y) = (\tau(x), \tau(y)b)$$

for some F-isomorphism $\tau : B \to B'$ such that $\phi \circ \tau = \tau \circ \sigma$ and $\tau(c) = db^2$ for some $b \in F^\times$.

Proof. The proof is analogous to Theorem 4.3.12, as the middle nuclei of $D_r(B, \sigma, c)$ and $D_r(B', \phi, d)$ are equal to B and B' respectively. Due to this, we can construct the isomorphisms in the same way as in the previous proof. □

Corollary 4.3.14. *Let $D = D(B, \sigma, c)$ (resp. $D_r(B, \sigma, c)$) and $D' = D(B, \phi, d)$ (resp. $D_r(B, \phi, d)$) be F-algebras. Then $G : D \to D'$ is an isomorphism if and only if G has the form*

$$G(x, y) = (\tau(x), \tau(y)b)$$

for some F-isomorphism $\tau \in \mathrm{Aut}_F(B)$ such that $\phi \circ \tau = \tau \circ \sigma$ and $\tau(c) = db^2$ for some $b \in F^\times$.

Corollary 4.3.15. *If $c \in F^\times$ and $d \in B^\times \setminus F$, then $D(B, \sigma, c)$ is not isomorphic to any of $D(B, \sigma, d)$, $D_m(B, \sigma, d)$ or $D_r(B, \sigma, d)$.*

Proof. If $D(B, \sigma, c)$ is isomorphic to one of $D(B, \sigma, d)$ or $D_r(B, \sigma, d)$, by Corollary 4.3.14 there must exist some $b \in F^\times$ such that $c = db^2$. This implies $d = cb^{-2} \in F^\times$, which is a contradiction.
Finally, if $D_m(B, \sigma, d) \cong D(B, \sigma, c)$, then the middle nuclei of the two algebras must be isomorphic; that is, $B \cong \{k \in B \mid \sigma(k)d = d\sigma(k)\}$. This is satisfied if and only if $d \in F^\times$, contradicting our assumption. □

Note that we cannot use an analogous proof to the one in Theorem 4.3.12 to determine the isomorphisms of $D_m(B, \sigma, c)$, as the middle nucleus is not equal to B. We obtain some weaker results:

Lemma 4.3.16. *If $\mathrm{Fix}(\sigma) \ncong \mathrm{Fix}(\phi)$, then $D_m(B, \sigma, c) \ncong D_m(B', \phi, d)$ for any choice of $c \in B^\times$ and $d \in B'^\times$.*

Proof. If $D_m(B, \sigma, c) \cong D_m(B', \phi, d)$, the left nucleus of $D_m(B, \sigma, c)$ is mapped isomorphically to the left nucleus of $D_m(B', \phi, d)$. By Lemma 4.3.4, this implies $\mathrm{Fix}(\sigma) \cong \mathrm{Fix}(\phi)$. □

Theorem 4.3.17. *Let $D = D_m(B, \sigma, c)$ and $D' = D_m(B', \phi, d)$ be F-algebras. If $\tau : B \to B'$ is an F-isomorphism such that $\phi \circ \tau = \tau \circ \sigma$ and $\tau(c) = db^2$ for some $b \in F^\times$, there is an isomorphism $G : D \to D'$ given by $G(x, y) = (\tau(x), \tau(y)b)$ for all $x, y \in B$.*

Proof. Clearly this is an F-vector space isomorphism from $B \oplus B$ to $B' \oplus B'$ as it is additive, bijective and F-linear. To show this map is multiplicative and thus an F-algebra isomorphism, we consider $G(u,v)G(x,y) = G((u,v)(x,y))$. This is equivalent the equations

$$\tau(u)\tau(x) + \phi(\tau(v)b)d\phi(\tau(y)b) = \tau(ux + \sigma(v)c\sigma(y)),$$
$$\tau(u)\tau(y)b + \tau(v)b\tau(x) = \tau(uy + vx)b.$$

As $b \in F^\times$, this is equivalent to simply considering

$$\phi(\tau(v))db^2\phi(\tau(y)) = \tau(\sigma(v))\tau(c)\tau(\sigma(y)).$$

Substituting $\tau(c) = db^2$, we conclude that this is satisfied for all $v, y \in B$ as we assumed $\phi \circ \tau = \tau \circ \sigma$. Hence $G : D \to D'$ is a F-algebra isomorphism. □

4.3.2 *Automorphisms*

Theorem 4.3.18. *Let $D = D(B,\sigma,c)$ (resp. $D = D_r(B,\sigma,c)$). All automorphisms $G : D \to D$ are of the form*

$$G(u,v) = (\tau(u), \tau(v)b)$$

for some $\tau \in \mathrm{Aut}_F(B)$ such that $\tau \in C(\sigma)$ and $b \in F^\times$ satisfying $\tau(c) = cb^2$. Further, all maps of this form with $\tau \in \mathrm{Aut}_F(B)$ and $b \in F^\times$ satisfying these conditions yield automorphisms of D.

Proof. Suppose that $G : D \to D$ is an F-automorphism. Then G restricts to an automorphism of the middle nucleus of D. This means that G restricted to B must be an automorphism of B; that is, $G\,|_B = \tau \in \mathrm{Aut}_F(B)$, so we have $G(x,0) = (\tau(x), 0)$ for all $x \in B$.
Let $G(0,1) = (a,b)$ for some $a, b \in B$. Then we have

$$G(x,y) = G(x,0) + G(0,1)G(y,0) = (\tau(x) + a\tau(y), \tau(y)b),$$

and $G(x,y) = G(x,0) + G(y,0)G(0,1) = (\tau(x) + \tau(y)a, b\tau(y))$. This implies that $a, b \in Z(B') = F$.

As G is multiplicative, we must also have $G((0,1)^2) = G(0,1)^2$ which holds if and only if $(a,b)(a,b) = (\tau(c),0)$. From this, we obtain the equations $a^2 + c\phi(b^2) = \tau(c)$ and $ab + ba = 0$. Since we have $a, b \in F$, this simplifies to $a^2 + cb^2 = \tau(c)$ and $2ab = 0$. As F does not have characteristic 2, this implies either $a = 0$ or $b = 0$. If $b = 0$, then $G(x,y) = (\tau(x) + \tau(y)a, 0)$ and so G is not surjective. This is a contradiction, as G is an automorphism. Thus we conclude $a = 0$ and $cb^2 = \tau(c)$.

Finally, as G is multiplicative we have $G(u,v)G(x,y) = G((u,v)(x,y))$ for all $u, v, x, y \in K$. When $D = D(B, \sigma, c)$, this yields

$$(\tau(ux) + c\sigma(\tau(v)b\tau(y)b), \tau(uy)b + \tau(v)b\tau(x)) = (\tau(ux + c\sigma(vy)), \tau(uy + vx)b)$$

for all $u, v, x, y \in K$. As $b \in F$, this implies we must have $cb^2\sigma(\tau(vy)) = \tau(c\sigma(vy))$. After substituting the condition $\tau(c) = c\phi(b^2)$, we get $\sigma \circ \tau = \tau \circ \sigma$. This follows almost identically for $D_r(B, \sigma, c)$.

Conversely, let $G : B \oplus B \to B \oplus B$ be defined by $G(x,y) = (\tau(x), \tau(y)b)$ for some F-automorphism $\tau : B \to B$ such that $\sigma \circ \tau = \tau \circ \sigma$ and $\tau(c) = cb^2$ for some $b \in F^\times$. It is easily checked that this in fact gives an F-algebra automorphism of D. □

Corollary 4.3.19. *Let $D = D(B, \sigma, c)$ (resp. $D = D_r(B, \sigma, c)$). There is a subgroup of $\mathrm{Aut}_F(D)$ isomorphic to*

$$\{\tau \in \mathrm{Aut}_F(B) \mid \tau(c) = c \text{ and } \tau \circ \sigma = \sigma \circ \tau\}.$$

In order to describe the number of automorphisms of $D(B, \sigma, c)$ and $D_r(B, \sigma, c)$, we introduce a slightly different version of the group $J(c)$:

$$J_F(c) = \{\tau \in \mathrm{Aut}_F(B) \mid X^2 - \tau(c)c^{-1} = 0 \text{ has solutions in } F\} \subset \mathrm{Aut}_F(B).$$

Similarly to $J(c)$, this forms a subgroup of $\mathrm{Aut}_F(B)$. The proof of this follows identically to the proof of Theorem 4.2.20.

Theorem 4.3.20. *There are exactly $2\,|J_F(c) \cap C(\sigma)|$ automorphisms of $D(B, \sigma, c)$ (respectively $D_r(B, \sigma, c)$), each of which is given by the automorphisms $G(x,y) = (\tau(x), \tau(y)b_i)$ for each $\tau \in J_F(c) \cap C(\sigma)$, where $b_i \in F$ are the two solutions of $X^2 - \tau(c)c^{-1} = 0$ for $i = 1, 2$.*

Proof. The proof follows analogously to the proof of Theorem 4.2.24, apart from requiring that $b_i \in F^\times$. This is due to the constraints determined in Theorem 4.3.18. □

Corollary 4.3.21. *If $c \in F^\times$, then there are exactly $2\,|C(\sigma)|$ automorphisms of $D(B, \sigma, c)$, each of which is given by the automorphisms $G(x, y) = (\tau(x), \pm\tau(y))$ for each $\tau \in C(\sigma)$.*

Proof. This follows similarly to Corollary 4.2.26. □

An integral part of the proof given in Theorem 4.3.18 is that one of the nuclei of these algebras must be equal to B and so any automorphism of $D(B, \sigma, c)$ must restrict to an automorphism of B. For $D_m(B, \sigma, c)$ with $c \notin F^\times$, B is not equal to any of the nuclei so we cannot make this deduction. However, if we assume that an automorphism of $D_m(B, \sigma, c)$ restricts to an automorphism of B, then it must be of the same form as the automorphisms of the other Dickson algebras:

Theorem 4.3.22. *Let $D = D_m(B, \sigma, c)$ and suppose G is an automorphism which restricts to an automorphism of B. Then*

$$G(u, v) = (\tau(u), \tau(v)b)$$

for some $\tau \in \mathrm{Aut}_F(B)$ such that $\tau \in C(\sigma)$ and $b \in F^\times$ satisfying $\tau(c) = cb^2$.

Proof. The proof follows analogously to Theorem 4.3.18 as G restricts to an automorphism of B. □

4.4 GENERALIZED DICKSON ALGEBRAS

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

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

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

Theorem 4.4.1. *(i) If $N_{D/F}(c) \neq N_{D/F}(a)^2$ for all $a \in D^\times$, then*

$\mathrm{Cay}(D, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$ *is a division algebra.*

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

This follows analogously to Theorem 4.1.5.

Remark 4.4.2. If $F = \mathbb{F}_{p^s}$ and $K = \mathbb{F}_{p^r}$ is a finite extension of F, then $\mathrm{Aut}_F(K)$ is cyclic of order r/s and is generated by ϕ^s, where ϕ is defined by the Frobenius automorphism $\phi(x) = x^p$ for all $x \in K$. Then $A = \mathrm{Cay}(K, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$ is a division algebra if and only if c is not a square in K. The proof of this is analogous to the one given in [36, p. 53].

Although it appears that we obtain some additional semifields from the doubling process that were not considered in [36], we show that this is not the case:

Theorem 4.4.3. *Let D and D' be two central simple F-algebras (respectively, K and L finite field extensions of F) and $g, h : D \to D'$ be two F-algebra isomorphisms. Let $A_D = \mathrm{Cay}(D, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$ and $B_{D'} = \mathrm{Cay}(D', g(c)b^2, \phi_1, \phi_2, \phi_3, \phi_4)$ for some $b \in F^\times$ (resp. $A_K = \mathrm{Cay}(K, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$ and $B_L = \mathrm{Cay}(L, g(c)\phi_1(b)\phi_2(b), \phi_1, \phi_2, \phi_3, \phi_4)$ for some $b \in K^\times$). If*

$$\phi_i = g \circ \sigma_i \circ h^{-1} \text{ for } i = 1, 2, \tag{11}$$

$$\phi_i = h \circ \sigma_i \circ g^{-1} \text{ for } i = 3, 4, \tag{12}$$

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

Proof. We show the proof in the central simple algebra case. It follows analogously when we take field extensions K and L. Clearly G is F-linear, additive and bijective. It only remains to show that G is multiplicative; that is, $G((u,v)(x,y)) = G(u,v)G(x,y)$ for all $u,v,x,y \in D$. First we have

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

It similarly follows that

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

By (11) and (12), we obtain equality and thus G is an F-algebra isomorphism.

□

Corollary 4.4.4. *Let* $g, h \in \mathrm{Aut}_F(D)$ *(resp.* $\mathrm{Aut}_F(K)$*) and* $b \in F^\times$ *(resp.* $b \in K^\times$*). Let* $B_D = \mathrm{Cay}(D, g(c)b^2, \phi_1, \phi_2, \phi_3, \phi_4)$
(resp. $B_K = \mathrm{Cay}(K, g(c)\phi_1(b)\phi_2(b), \phi_1, \phi_2, \phi_3, \phi_4)$ *for some* $b \in K^\times$*). If*

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

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

Corollary 4.4.5. *Every generalised Dickson algebra* $A_D = \mathrm{Cay}(D, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$ *is isomorphic to an algebra of the form* $\mathrm{Cay}(D, c, \sigma_1', \sigma_2', \sigma_3', id)$ *(analogously for the algebras* A_K*).*

Proof. Consider the map $G : D \oplus D \to D \oplus D$ defined by $G(u, v) = (u, \sigma_4^{-1}(v))$. By Theorem 4.4.3, this yields the isomorphism

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

□

This confirms that when K is a finite field, every algebra obtained from this construction is isomorphic to a generalized Dickson semifield. Thus, for finite fields the results given in [36] can be translated across to this construction via the isomorphism given in Corollary 4.4.5. This motivates the investigation of analogue results for the construction with both an associative division algebra D/F and a finite field extension K/F in the following sections, which have not been considered previously.

4.4.1 *Commutator and nuclei*

Unless otherwise stated, we will write $A_D = \mathrm{Cay}(D, c, \sigma_1, \sigma_2, \sigma_3, id)$ and $A_K = \mathrm{Cay}(K, c, \sigma_1, \sigma_2, \sigma_3, id)$ without loss of generality; if $\sigma_4 \neq id$, we may use Corollary 4.4.5 to obtain an isomorphic algebra $\mathrm{Cay}(D, c, \sigma_1', \sigma_2', \sigma_3', id)$.

Proposition 4.4.6. *If $\sigma_1 = \sigma_2$ and $\sigma_3 = id$, $\mathrm{Comm}(A_D) = F \oplus F$ and A_K is commutative. Otherwise, $\mathrm{Comm}(A_D) = F \oplus S$, where $S = \{v \in D \mid yv = v\sigma_1^{-1} \circ \sigma_2(y)$ and $\sigma_3(y)v = vy\}$, and $\mathrm{Comm}(A_K) = \mathrm{Fix}(\sigma_3) \oplus 0 \subseteq K$.*

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

$$ux + c\sigma_1(v)\sigma_2(y) = xu + c\sigma_1(y)\sigma_2(v), \tag{13}$$

$$\sigma_3(u)y + vx = \sigma_3(x)v + yu, \tag{14}$$

for all $x, y \in D$. If $y = 0$ and $x \neq 0$, the first equation implies $u \in Z(D) = F$; if $x = 0$ and $y \neq 0$, we must have $v \in D$ satisfies $\sigma_1(v)\sigma_2(y) = \sigma_1(y)\sigma_2(v)$.

If we let $y \in F$, then we have $\sigma_1(v) = \sigma_2(v)$. If we use this condition in (13), we see that $v \in D$ must satisfy $yv = v\sigma_1^{-1} \circ \sigma_2(y)$ for all $y \in D$. Under these assumptions on u and v, (13) is satisfied for all $x, y \in D$. Similar deduction yields that (14) is satisfied for all $x, y \in D$ if and only if $\sigma_3(x)v = vx$. □

Remark 4.4.7. If $\mathrm{Comm}(A_K) \not\subseteq K$, then $\sigma_1 = \sigma_2$ and $\sigma_3 = \sigma_4 = id$ by Lemma 4.4.6. Hence, every such algebra is isomorphic to the generalisation of commutative Dickson algebras as defined in [59].

Proposition 4.4.8. *(i) Suppose that at least one of the following holds:*

- $\sigma_2 \neq id$,
- $\sigma_1 \neq \sigma_2 \circ \sigma_3$,
- $\sigma_1 \neq \sigma_3 \circ \sigma_2$.

Then $\mathrm{Nuc}_l(A_D) = \{(x, 0) \in D \oplus D \mid \sigma_1 \circ \sigma_3(x) = c^{-1}xc\} \subseteq D \oplus 0$ *and* $\mathrm{Nuc}_l(A_K) = \mathrm{Fix}(\sigma_1 \circ \sigma_3) \oplus 0 \subseteq K \oplus 0$.

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

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

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

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

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

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

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

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

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

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

The associator is linear in each component, so we have $[(k,m),(u,v),(x,y)] = [(k,0),(u,v),(x,y)] + [(0,m),(u,v),(x,y)]$. It is clear that is $(k,0),(0,m) \in \mathrm{Nuc}_l(A_D)$, then $(k,m) \in \mathrm{Nuc}_l(A_D)$. Conversely, suppose $(k,m) \in \mathrm{Nuc}_l(A_D)$. As $[(k,m),(u,v),(x,y)] = 0$ is satisfied for all $u,v,x,y \in D$, we consider $x = u = 0$; from this, we obtain $c\sigma_1(\sigma_3(k)v)\sigma_2(y) = kc\sigma_1(v)\sigma_2(y)$ must be satisfied for all $v,y \in D$. Comparing this with the computations for $((k,0)(u,v))(x,y) = (k,0)((u,v)(x,y))$, we see that these conditions are identical. So $(k,m) \in \mathrm{Nuc}_l(A_D)$ implies $(k,0) \in \mathrm{Nuc}_l(A_D)$. As $[(0,m),(u,v),(x,y)] = [(k,m),(u,v),(x,y)] - [(k,0),(u,v),(x,y)]$ and $\mathrm{Nuc}_l(A_D)$ is closed under addition, it is clear that $(0,m) \in \mathrm{Nuc}_l(A_D)$. Thus it follows that (k,m) lies in the left nucleus if and only if $(k,0)$ and $(0,m)$ are both also in the left nucleus. Thus to show that there are no other elements in the left nucleus, it suffices to check that there are no elements of the form $(0,m)$, $m \in D$, in $\mathrm{Nuc}_l(A_D)$.

If $(0,m) \in \mathrm{Nuc}_l(A_D)$, then for all $u,v,x,y \in D$ we have $((0,m)(u,v))(x,y) = (0,m)((u,v)(x,y))$. This holds for all $u,v,x,y \in D$ if and only if

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

$$\sigma_3(c\sigma_1(m)\sigma_2(v))y = mc\sigma_1(v)\sigma_2(y).$$

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

additional conditions that $\sigma_1 = \sigma_3 \circ \sigma_2$ and $\sigma_2 = id$. Under these assumptions, we see that there may exist some $m \neq 0$ such that $((0,m)(u,v))(x,y) = (0,m)((u,v)(x,y))$ for all $u,v,x,y \in D$.

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

□

Corollary 4.4.9. *A_K is associative if and only if $A_K = \mathrm{Cay}(K, c, \sigma, id, \sigma, id)$ for some $\sigma \in \mathrm{Aut}_F(K)$ such that $\sigma^2 = id$ and $c \in \mathrm{Fix}(\sigma)$. That is, A_K is a quaternion algebra over $\mathrm{Fix}(\sigma)$.*

As the center of A is defined as $Z(A) = \mathrm{Comm}(A) \cap \mathrm{Nuc}_l(A) \cap \mathrm{Nuc}_m(A) \cap \mathrm{Nuc}_r(A)$, we see that $Z(A_K) \subseteq K$ unless $\sigma_1 = \sigma_2 = \sigma$ and $\sigma_3 = \sigma_4 = \sigma^{-1}$. If $A_K = \mathrm{Cay}(K, c, \sigma, \sigma, \sigma^{-1}, \sigma^{-1})$ for some $\sigma \in \mathrm{Aut}_F(K)$, then A_K is a commutative, associative algebra.

4.4.2 *Isomorphisms*

In certain cases, the maps defined in Theorem 4.4.3 and Corollary 4.4.4 are the only possible isomorphisms between two algebras constructed via our generalised Cayley-Dickson doubling:

Theorem 4.4.10. *Let $A_K = \mathrm{Cay}(K, c, \sigma_1, \sigma_2, \sigma_3, id)$ and $B_L = \mathrm{Cay}(L, c', \phi_1, \phi_2, \phi_3, id)$. Suppose that $G : A_K \to B_L$ is an isomorphism that restricts to an isomorphism $g : K \to L$. Then G is of the form $G(x,y) = (g(x), g(y)b)$ such that $\phi_i \circ g = g \circ \sigma_i$ for $i = 1,2,3$ and some $b \in L^\times$ such that $g(c) = c'\phi_1(b)\phi_2(b)$.*

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

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

and

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

It follows that either $\phi_3 \circ g \circ \sigma_3^{-1} = g$ or $b = 0$. However, if $b = 0$ this would imply that G was not surjective, which is a contradiction to the assumption that G is an isomorphism. Thus it follows that $\phi_3 \circ g \circ \sigma_3^{-1} = g$. Additionally, we have either $g \circ \sigma_3^{-1} = g$ or $a = 0$.
Consider $G((0,1)^2) = G(0,1)^2$. This gives $(a^2 + c'\phi_1(b)\phi_2(b), \phi_3(a)b + ba) = (g(c),0)$. As we have established that $b \neq 0$, this implies that $\phi_3(a) = -a$. If $a \neq 0$, we obtain $g \circ \sigma_3^{-1} = g$. Substituting this into the condition $\phi_3 \circ g \circ \sigma_3^{-1} = g$, we conclude that $\phi_3 = id$. This contradicts $\phi_3(a) = -a$. Thus we must in fact have $a = 0$ and $G(x,y) = (g(x), g(y)b)$ where $\phi_3 \circ g = g \circ \sigma_3$ and $g(c) = c'\phi_1(b)\phi_2(b)$. Computing $G(u,v)G(x,y) = G((u,v)(x,y))$ gives the remaining conditions. □

As the isomorphism defined in Corollary 4.4.5 restricts to an automorphism of K, Corollary 4.4.5 can be employed in conjugation with the above result to determine isomorphisms when $\sigma_4 \neq id$ or $\phi_4 \neq id$. The proof of Theorem 4.4.10 does not hold when we consider the algebras A_D, as we rely heavily on the commutativity of K.

Corollary 4.4.11. *Suppose that $G : A_K \to B_K$ is an isomorphism that restricts to an automorphism g of K. Then G is of the form $G(x,y) =$*

$(g(x), g(y)b)$ *such that* $\phi_i \circ g = g \circ \sigma_i$ *for* $i = 1, 2, 3$ *and some* $b \in K^\times$ *such that* $g(c) = c'\phi_1(b)\phi_2(b)$.

If $\mathrm{Nuc}_l(A) = \mathrm{Nuc}_l(B) = K$, all isomorphisms from $A \to B$ must restrict to an automorphism of K; similar considerations are true for restrictions to the middle and right nuclei. It follows that we can determine precisely when two such algebras are isomorphic by Corollary 4.4.11.

Corollary 4.4.12. *Suppose that* $G : A_K \to B_K$ *is an isomorphism that restricts to an automorphism of* K. *If* K *is a separable extension of* F, *we must have* $N_{K/F}(cc'^{-1}) = N_{K/F}(b^2)$ *for some* $b \in K^\times$.

Proof. Suppose $G : A_K \to B_K$ is an isomorphism that restricts to an automorphism of K. By Theorem 4.4.11, we have $g(c) = c'\phi_1(b)\phi_2(b)$. Applying norms to both side, we obtain

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

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

Example 4.4.13. Let $F = \mathbb{Q}_p$ $(p \neq 2)$ and K be a separable extension of $\mathbb{Q}_p$. It is well known that $(\mathbb{Q}_p^\times)^2/\mathbb{Q}_p = \{[1], [u], [p], [up]\}$ for some $u \in \mathbb{Z}_p \setminus \mathbb{Z}_p^2$. If $N_{K/F}(c)$ and $N_{K/F}(c')$ do not lie in the same coset of $(\mathbb{Q}_p^\times)^2/\mathbb{Q}_p$, there does not exist an isomorphism that restricts to K such that $\mathrm{Cay}(K, c, \sigma_1, \sigma_2, \sigma_3, \sigma_4) \cong \mathrm{Cay}(K, c', \phi_1, \phi_2, \phi_3, \phi_4)$ by Corollary 4.4.12.

4.4.3 *Automorphisms*

Theorem 4.4.14. *Let* $g \in \mathrm{Aut}_F(D)$ *(resp.* $\mathrm{Aut}_F(K)$*) such that* g *commutes with* $\sigma_1, \sigma_2, \sigma_3$ *and let* $b \in F^\times$ *(resp.* $b \in K^\times$*) such that* $g(c) = b^2c$ *(resp.* $g(c) = \sigma_1(b)\sigma_2(b)c$*). Then the map* $G : A \to A$ *defined by* $G(u, v) = (g(u), g(v)b)$ *is an automorphism of* A_D *(resp.* A_K*).*

This is easily checked via some long calculations.

Theorem 4.4.15. *Suppose that at least one of* $\mathrm{Nuc}_l(A_K)$, $\mathrm{Nuc}_m(A_K)$, $\mathrm{Nuc}_r(A_K)$ *is equal to* K. *Then* $G : A_K \to A_K$ *is an automorphism of* A_K *if and only if* G *has the form stated in Theorem 4.4.14.*

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

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

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

and also

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

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

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

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

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

Finally we consider $G(u, v)G(x, y) = G((u, v)(x, y))$ for all $u, v, x, y \in K$. We obtain $(g(u), g(v)b)(g(x), g(y)b) = (g(uv + c\sigma_1(v)\sigma_2(y)), g(\sigma_3(u)y + vx)b)$ which gives the equations

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

As $g \circ \sigma_3 = \sigma_3 \circ g$, the second equation holds for all $u, v, x, y \in K$. Substituting $g(c) = c\sigma_1(b)\sigma_2(b)$ into the first equation, we obtain $\sigma_1(g(v))\sigma_2(g(y)) = g(\sigma_1(v))g(\sigma_2(y))$ for all $v, y \in K$. This implies $\sigma_1 \circ g = g \circ \sigma_1$ and $\sigma_2 \circ g = g \circ \sigma_2$. Hence if G is an automorphism of A we must have $G(u, v) = (g(u), g(v)b)$ for some $g \in \mathrm{Aut}_F(K)$ such that $g \circ f = f \circ g$ for $f = \sigma_1, \sigma_2, \sigma_3$ and some $b \in K^\times$ such that $g(c) = \sigma_1(b)\sigma_2(b)c$. □

Corollary 4.4.16. *Suppose that at least one of* $\mathrm{Nuc}_l(A_K)$, $\mathrm{Nuc}_m(A_K)$, $\mathrm{Nuc}_r(A_K)$ *is equal to* K *and* $\mathrm{Aut}_F(K) = \langle\sigma\rangle$. *Then* $G : A_K \to A_K$ *is an automorphism of* A_K *if and only if* $G(u, v) = (\sigma^i(u), \sigma^i(v)b)$ *for some* $i \in \mathbb{Z}$ *and* $b \in K^\times$ *satisfying* $\sigma^i(c) = c\sigma^{\alpha_2}(b)\sigma^{\beta_2}(b)$.

In the case when doubling an associative division algebra, we obtain a partial generalisation of Theorem 4.4.15. Recall that we assume $A_D = \mathrm{Cay}(D, c, \sigma_1, \sigma_2, \sigma_3, id)$.

Lemma 4.4.17. *Let* $G \in \mathrm{Aut}(A_D)$ *be such that* $G\,|_D = g \in \mathrm{Aut}_F(D)$. *Then there must exist some* $a, b \in D$, $b \neq 0$, *such that for all* $y \in D$,

$$ag(y) = g \circ \sigma_3^{-1}(y)a,$$

$$bg(y) = \sigma_3 \circ g \circ \sigma_3^{-1}(y)b.$$

Proof. Suppose $G\,|_D = g \in \mathrm{Aut}_F(D)$. Then for all $x \in D$, we obtain $G(x,0) = (g(x),0)$. Let $G(0,1) = (a,b)$ for some $a,b \in D$. It now follows that

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

and also

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

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

Theorem 4.4.18. *Let $G \in \mathrm{Aut}(A_D)$ be such that $G\,|_D = g \in \mathrm{Aut}_F(D)$. If $\sigma_3 = id$, then $G : A_D \to A_D$ must have the form as stated in Theorem 4.4.14.*

Proof. Suppose $G|_D = g \in \mathrm{Aut}_F(D)$. Substituting $\sigma_3 = id$ into Lemma 4.4.17, we see that $G(0,1) = (a,b)$ for some $a,b \in D$ such that

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

This is satisfied for all $y \in D$ if and only if $a,b \in F$ and so $G(x,y) = (g(x) + g(y)a, g(y)b)$. The remainder of this proof follows almost exactly the same to Theorem 4.4.15:

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

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

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

Finally we consider $G(u,v)G(x,y) = G((u,v)(x,y))$ for all $u,v,x,y \in D$. We obtain $(g(u), g(v)b)(g(x), g(y)b) = (g(uv + c\sigma_1(v)\sigma_2(y)), g(uy + vx)b)$, which gives the equations

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

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

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

BIBLIOGRAPHY

[1] A. A. Albert. *Modern higher algebra*. Courier Dover Publications, 2018.

[2] D. Augot, P. Loidreau, and G. Robert. "Generalized Gabidulin codes over fields of any characteristic". In: *Designs, Codes and Cryptography* 86.8 (2018), pp. 1807–1848.

[3] G.M. Benkart and J. Marshall Osborn. "The derivation algebra of a real division algebra". In: *American Journal of Mathematics* 103.6 (1981), pp. 1135–1150.

[4] D. Boucher and F. Ulmer. "Linear codes using skew polynomials with automorphisms and derivations". In: *Designs, codes and cryptography* 70.3 (2014), pp. 405–431.

[5] M. Boulagouaz and A. Leroy. "(σ, δ)-codes." In: *Advances in Mathematics of Communications* 7.4 (2013), pp. 463–474.

[6] Bourbaki. *Elements of Mathematics*. Hermann, 1971.

[7] C. Brown, S. Pumplün, and A. Steele. "Automorphisms and isomorphisms of Jha-Johnson semifields obtained from skew polynomial rings". In: *Communications in Algebra* 46.10 (2018), pp. 4561–4576.

[8] Christian Brown. "Petit Algebras and their Automorphisms". PhD thesis. Un, 2018. arXiv: `1806.00822 [math.RA]`.

[9] M.V.D. Burmester. "On the commutative non-associative division algebras of even order of LE Dickson". In: *Rend. Mat. Appl* 21 (1962), pp. 143–166.

[10] M.V.D. Burmester. "On the non-unicity of translation planes over division algebras". In: *Archiv der Mathematik* 15.1 (1964), pp. 364–370.

[11] J. Carcanague. "Idéaux bilatères d'un anneau de polynomes non commutatifs sur un corps". In: *Journal of Algebra* 18.1 (1971), pp. 1–18.

[12] J Carcanague. “Quelques resultats sur les anneaux de Ore”. In: *CR Acad. Sci. Paris Sr. AB* 269 (1969), A749–A752.

[13] X. Caruso and J. Le Borgne. “A new faster algorithm for factoring skew polynomials over finite fields”. In: *Journal of Symbolic Computation* 79 (2017), pp. 411–443.

[14] S. D. Cohen and M. J. Ganley. “Commutative semifields, two dimensional over their middle nuclei”. In: *Journal of Algebra* 75.2 (1982), pp. 373–385.

[15] E. F. Combarro, J. Ranilla, and I. F. Rúa. “Classification of semifields of order 64”. In: *Journal of Algebra* 322.11 (2009), pp. 4011–4029.

[16] E. F. Combarro, I. F. Rùa, and J. Ranilla. “Finite semifields with 74 elements”. In: *International Journal of Computer Mathematics* 89.13-14 (2012), pp. 1865–1878.

[17] M. Cordero and G. P. Wene. “A survey of finite semifields”. In: *Discrete Mathematics* 208 (1999), pp. 125–137.

[18] A. Deajim and D. Grant. “Space time codes and non-associative division algebras arising from elliptic curves”. In: *Contemp. Math* 463 (2008), pp. 29–44.

[19] P. Delsarte. “Bilinear forms over a finite field, with applications to coding theory”. In: *Journal of combinatorial theory, Series A* 25.3 (1978), pp. 226–241.

[20] L. E. Dickson. “On commutative linear algebras in which division is always uniquely possible”. In: *Transactions of the American Mathematical Society* 7.4 (1906), pp. 514–522.

[21] H. W. Eves. *Elementary matrix theory*. Courier Corporation, 1980.

[22] N. Fogarty and H. Gluesing-Luerssen. “A circulant approach to skew-constacyclic codes”. In: *Finite Fields and Their Applications* 35 (2015), pp. 92–114.

[23] E. M. Gabidulin. “Theory of codes with maximum rank distance”. In: *Problemy Peredachi Informatsii* 21.1 (1985), pp. 3–16.

[24] R. Gallager. “Low-density parity-check codes”. In: *IRE Transactions on Information Theory* 8.1 (1962), pp. 21–28.

[25] M. J. Ganley. “Central weak nucleus semifields”. In: *European Journal of Combinatorics* 2.4 (1981), pp. 339–347.

[26] J. Gómez-Torrecillas, F.J. Lobillo, and G. Navarro. “Computing the bound of an Ore polynomial. Applications to factorization”. In: *Journal of Symbolic Computation* 92 (2019), pp. 269–297.

[27] D. Grant and M. K. Varanasi. “The equivalence of space-time codes and codes defined over finite fields and Galois rings”. In: *Advances in Mathematics of Communications* 2.2 (2008), p. 131.

[28] R. W. Hamming. “Error detecting and error correcting codes”. In: *The Bell system technical journal* 29.2 (1950), pp. 147–160.

[29] T. Hanke. “A direct approach to noncrossed product division algebras”. In: *arXiv:1109.1580* (2011).

[30] M. Hübner and H. P. Petersson. “Two-dimensional real division algebras revisited.” In: *Beiträge zur Algebra und Geometrie* 45.1 (2004), pp. 29–36.

[31] T. W. Hungerford. *Algebra*. 1980.

[32] S. Ikehata. “Purely inseparable ring extensions and Azumaya algebras”. In: *Mathematical Journal of Okayama University* 41.1 (1999).

[33] N. Jacobson. *Finite-dimensional division algebras over fields*. Springer Science & Business Media, 2009.

[34] M. Kervaire. “Non-parallelizability of the n-sphere for $n > 7$”. In: *Proc. Nat. Acad. Sci 44* (1958), pp. 280–283.

[35] M. Knus et al. *The book of involutions*. Vol. 44. American Mathematical Soc., 1998.

[36] D. E. Knuth. “Finite semifields and projective planes”. PhD thesis. California Institute of Technology, 1963.

[37] M. Lavrauw. “Finite semifields and nonsingular tensors”. In: *Designs, codes and cryptography* 68.1-3 (2013), pp. 205–227.

[38] M. Lavrauw and O. Polverino. “Finite semifields”. In: *Current research topics in Galois Geometry* (2011), pp. 131–160.

[39] M. Lavrauw and J. Sheekey. “Semifields from skew polynomial rings”. In: *Advances in Geometry* 13.4 (2013), pp. 583–604.

[40] A. Leroy. “Noncommutative polynomial maps”. In: *Journal of Algebra and its Applications* 11.04 (2012), p. 1250076.

[41] J. Milnor and R. Bott. “On the parallelizability of the spheres”. In: *Bull. AMS 64* (1958), pp. 87–89.

[42] A. Owen and S. Pumplün. “The eigenspaces of twisted polynomials over cyclic field extensions”. In: *arXiv:1909.07728* (2019).

[43] S.B. Pai and B. S. Rajan. “A Singleton bound for generalized Ferrers diagram rank metric codes”. In: *arXiv:1506.05558* (2015).

[44] J. Petit. “Sur certains quasi-corps généralisant un type d’anneau-quotient”. In: *Séminaire Dubreil. Algèbre et théorie des nombres* 20.2 (1966), pp. 1–18.

[45] R. Pierce. *Associative Algebras*. Vol. 88. Springer-Verlag, 1982.

[46] S. Pumplün. “Albert’s twisted field construction using division algebras with a multiplicative norm”. In: *arXiv:1504.00188* (2015).

[47] S. Pumplün. “Finite nonassociative algebras obtained from skew polynomials and possible applications to (f, σ, δ)-codes”. In: *Advances in Mathematics of Communications* 3 (11 2017), pp. 615–634.

[48] S. Pumplün. “How to obtain lattices from (f, σ, δ)-codes via a generalization of Construction A”. In: *Applicable Algebra in Engineering, Communication and Computing* 29.4 (2018), pp. 313–333.

[49] S. Pumplün. “Quotients of orders in algebras obtained from skew polynomials with applications to coding theory”. In: *Communications in Algebra* 46.11 (2018), pp. 5053–5072.

[50] S. Pumplün and A. Steele. “The nonassociative algebras used to build fast-decodable space-time block codes”. In: *Advances in Mathematics of Communications* 9 (2015), p. 449.

[51] S. Pumplün and D. Thompson. “The norm of a skew polynomial”. In: *arXiv:2006.10418* (2020).

[52] S. Pumplün and T. Unger. “Space-time block codes from nonassociative division algebras”. In: *Advances in Mathematics of Communications* 5 (2011), p. 449.

[53] I. S. Reed and G. Solomon. “Polynomial codes over certain finite fields”. In: *Journal of the society for industrial and applied mathematics* 8.2 (1960), pp. 300–304.

[54] R. D. Schafer. *An introduction to nonassociative algebras*. Dover Publications, 1995.

[55] J. Sheekey. “A new family of linear maximum rank distance codes”. In: *Advances in Mathematics of Communications* 10.3 (2016), p. 475.

[56] J. Sheekey. “New semifields and new MRD codes from skew polynomial rings”. In: *Journal of the London Mathematical Society* 101.1 (2020), pp. 432–456.

[57] D. Silva and R. Kschischang F. R a.nd Koetter. “A rank-metric approach to error control in random network coding”. In: *IEEE Transactions on Information Theory* 54.9 (2008), pp. 3951–3967.

[58] A. Steele. “Automorphism groups of some finite semifields”. In: *arXiv:1305.5121* (2013).

[59] D. Thompson. “A generalization of Dickson’s commutative division algebras”. In: *Communications in Algebra* (2020), pp. 1–11.

[60] D. Thompson. “Division algebras that generalize Dickson semifields”. In: *Communications in Mathematics* 28 (2020), pp. 89–101.

[61] G. P. Wene. “Inner automorphisms of finite semifields”. In: *Note di Matematica* 29 (2010), pp. 231–242.

[62] A. Wesolowski. “Automorphism and similarity groups of forms determined by the characteristic polynomial”. In: *Communications in Algebra* 27.7 (1999), pp. 3109–3116.