University of Nottingham

School of Mathematical Sciences

Petit Algebras and their Automorphisms

Christian Brown

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

Doctor of Philosophy

September 2017

Acknowledgements

I would like to express my sincere gratitude to my supervisor Susanne Pumplün for all her help, guidance and enthusiasm throughout the last three years. When times were difficult and progress was slow, she gave me the support I needed to carry on and this thesis would not have been possible without her.

My thanks also go to Esther and my parents, for their continuing love and support.

Preface

First introduced by Ore [51] in 1933, skew polynomial rings are one of the earliest examples in the theory of noncommutative algebra. A skew polynomial ring $R = D[t;\sigma,\delta]$ consists of a unital associative ring D, an injective endomorphism σ of D, a left σ-derivation δ of D, and an indeterminate t satisfying the commutation rule $ta = \sigma(a)t + \delta(a)$ for all $a \in D$. Since their introduction, skew polynomial rings have been extensively studied, and their properties are well understood (see for instance [16, Chapter 2] and [32, Chapter 1]).

We now assume D is a division ring. In this case, it is well-known R possesses a right division algorithm, that is, for all $f(t), g(t) \in R$ with $f(t) \neq 0$ there exist unique $q(t), r(t) \in R$ with $\deg(r(t)) < \deg(f(t))$ such that $g(t) = q(t)f(t) + r(t)$. The existence of this right division algorithm allows us to construct a class of nonassociative algebras following a little known paper by Petit [52]: Let $f(t) \in R$ be of degree $m \geq 2$ and consider the additive subgroup $R_m = \{g \in R \mid \deg(g) < m\}$ of R. Then R_m together with the multiplication $a \circ b = ab \ \mathrm{mod}_r f$ yields a nonassociative algebra $S_f = (R_m, \circ)$ over $F = \{c \in D \mid c \circ h = h \circ c \text{ for all } h \in S_f\}$. Here the juxtaposition ab denotes multiplication in R, and $\mathrm{mod}_r f$ denotes the remainder after right division by $f(t)$. We call these algebras Petit algebras and also denote them R/Rf when we wish to make clear the ring R is used in their construction. After their introduction by Petit in 1967, these algebras were largely ignored until Wene [66] and more recently Lavrauw and Sheekey [44] studied them in the context of finite semifields. Earlier in 1906, the algebra S_f with $f(t) = t^2 - i \in \mathbb{C}[t;^-]$, $^-$ complex conjugation, appeared as the first example of a nonassociative division algebra in a paper by L.E. Dickson [18]. The structure of this thesis is as follows:

In Chapter 1 we state the necessary definitions and notations. We describe the construction of Petit algebras and discuss how this relates to other known constructions of algebras. For example, if D is a finite-dimensional central division algebra over a field C, $\sigma|_C$ is an automorphism of finite order m and $f(t) = t^m - a \in D[t;\sigma]$, $a \in \mathrm{Fix}(\sigma)^\times$, is right invariant, then the associative algebra $S_f = D[t;\sigma]/D[t;\sigma]f$ is called a generalised cyclic algebra and denoted (D, σ, a) [32, §1.4]. This happens to be the quotient algebra.

A unital finite nonassociative division ring is called a semifield in the literature. It is well-known that every associative semifield is in fact a field, however, there are many examples of semifields which are not associative. These are called proper semifields. An important example of semifields which appear throughout this thesis are Jha-Johnson semifields (also called cyclic semifields) [33], which generalise the Hughes-Kleinfeld and Sandler semifields. In a recent paper, Lavrauw and Sheekey proved that if K is a finite field, σ is an automorphism of K and $f(t) \in K[t;\sigma]$ is irreducible, then S_f is a Jha-Johnson semifield [44, Theorem 15]. While each Jha-Johnson semifield is isotopic to some algebra S_f [44, Theorem 16], it is not itself necessarily isomorphic to such an algebra S_f. In this thesis we will focus on those Jha-Johnson semifields which arise from Petit's algebra construction.

In Chapter 2 we will move on to study the properties of Petit algebras, and prove results concerning their nuclei, center, eigenring, zero divisors and associativity. We pay particular attention to the question of when Petit algebras are division algebras, and show this is closely related to whether the polynomial $f(t) \in R$ used in their construction is irreducible. Indeed, we will prove $f(t)$ is irreducible if and only if S_f is a (right) division algebra (Theorems 2.20 and 2.26). We will also show that when σ is not surjective and $f(t)$ is irreducible, then S_f is a right but not left division algebra (Corollary 2.24 and Example 2.25).

The connection between $f(t)$ being irreducible and S_f being a (right) division algebra motivates the study of irreducibility criteria in skew polynomial rings in Chapter 3. The results we obtain, in conjunction with Theorems 2.20 and 2.26, immediately yield criteria for some Petit algebras to be (right) division algebras.

Irreducibility and factorisation in skew polynomial rings have been investigated before and algorithms for factoring skew polynomials over finite fields and $\mathbb{F}_q(y)$ have appeared already in [13], [14], [22], [24] and [46]. We also mention the papers of Churchill and Zhang [15], and Granja, Martinez and Rodriguez [26], which employ valuation theory to obtain an analogue of the Eisenstein criteria for skew polynomial rings. The methods we use in Chapter 3, however, are purely algebraic and build upon the ideas of Lam and Leroy [40, Lemma 2.4], Jacobson [32, §1.3] and Petit [52, (17), (18), (19)].

In Chapter 4 we investigate isomorphisms between Petit algebras S_f and S_g, with $f(t), g(t) \in R = D[t;\sigma,\delta]$ and σ an automorphism of D. We apply these results to study in detail the automorphism group of Petit algebras in Chapter 5, focussing on the case where S_f is a nonassociative cyclic algebra in Chapter 6. Many of the results appearing in Chapter's 5 and 6 recently appeared in [11].

One of the main motivations for studying automorphisms of Petit algebras comes from the question how the automorphism groups of Jha-Johnson semifields look like. We are also motivated by a question by Hering [28]: Given a finite group G, does there exist a semifield such that G is a subgroup of its automorphism group?

It is well-known that two semifields coordinatize the same Desarguesian projective plane if and only if they are isotopic, hence semifields are usually classified up to isotopy rather than up to isomorphism and in many cases their automorphism group is not known. We apply our results to obtain information on the automorphism groups of some Jha-Johnson semifields in Section 5.3, and in the special case where S_f is a nonassociative cyclic algebra over a finite field in Section 6.2. In particular, we completely determine the automorphism group of a nonassociative cyclic algebra of prime degree over a finite field (Theorem 6.19): it is either a cyclic group, a dicyclic group, or the semidirect product of two cyclic groups.

Next we look at a generalisation of Petit's algebra construction using the skew polynomial ring $S[t;\sigma,\delta]$, where S is any associative unital ring, σ is an injective endomorphism of S, and δ is a left σ-derivation of S. While $S[t;\sigma,\delta]$ is in general not right Euclidean (unless S is a division ring), we are still able to right divide by polynomials $f(t) \in S[t;\sigma,\delta]$ whose leading coefficient is invertible (Theorem 7.1). Therefore, when $f(t)$ has an invertible leading coefficient, it is possible to define the same algebra construction. We briefly study some of the properties of these algebras including their center, zero divisors and nuclei.

Recall that a central simple algebra A of degree n over a field F is a G-crossed product algebra if it contains a maximal subfield M (i.e. $[M:F]=n$) that is a Galois extension of F with Galois group G. Moreover, we say A is a solvable G-crossed product algebra if $G=\mathrm{Gal}(M/F)$ is a solvable group. In Chapter 8, we revisit a result on the structure of solvable crossed product algebras, due to both Petit [52, §7] and a careful reading of Albert [1, p. 186]. We write up a proof of Albert's result using generalised cyclic algebras following the approach of Petit. We note that none of Petit's results are proved in [52, §7]. To do this we extend the definition of classical generalised cyclic algebras (D,σ,d) to where D need not be a division algebra. More specifically, we show a G-crossed product algebra is solvable if and only if it can be constructed as a finite chain of generalised cyclic algebras satisfying certain conditions. We describe how the structure of the solvable group, that is its chain of normal subgroups, relates to the structure of the crossed product algebra. We also generalise [52, §7] to central simple algebras which need neither be crossed product or division algebras.

We finish the Chapter by giving a recipe for constructing central division algebras containing a given finite abelian Galois field extension by forming a chain of generalised cyclic algebras. This generalises a result by Albert [1, p. 186], see also [32, Theorem 2.9.55], in which $G = \mathbb{Z}_2 \times \mathbb{Z}_2$.

CONTENTS

1

PRELIMINARIES

1.1 SOME BASIC DEFINITIONS

Let F be a field. An **algebra** A over F is an F-vector space together with a bilinear map $A \times A \to A, (x, y) \mapsto xy$, which we call the **multiplication** of A. A is **associative** if the associative law $(xy)z = x(yz)$ holds for all $x, y, z \in A$. Our algebras are **nonassociative** in the sense that we do not assume this law and we call algebras in which the associative law fails **not associative**. A is called **unital** if it contains a multiplicative identity 1. We assume throughout this thesis that our algebras are unital without explicitly saying so. Given an algebra A, the **opposite algebra** A^{op} is the algebra with the same elements and addition operator as A, but where multiplication is performed in the reverse order.

We say an algebra $0 \neq A$ is a **left** (resp. **right**) **division algebra**, if the left multiplication $L_a : x \mapsto ax$ (resp. the right multiplication $R_a : x \mapsto xa$) is bijective for all $0 \neq a \in A$ and A is a **division algebra** if it is both a left and a right division algebra. A finite-dimensional algebra is a division algebra if and only if it has no non-trivial zero divisors [60, p. 12], that is $ab = 0$ implies $a = 0$ or $b = 0$ for all $a, b \in A$. Finite division algebras are also called **finite semifields** in the literature.

The **associator** of three elements of an algebra A is defined to be $[x, y, z] = (xy)z - x(yz)$. We then define the **left nucleus** to be $\mathrm{Nuc}_l(A) = \{x \in A \mid [x, A, A] = 0\}$, the **middle nucleus** to be $\mathrm{Nuc}_m(A) = \{x \in A \mid [A, x, A] =$

$0\}$ and the **right nucleus** to be $\mathrm{Nuc}_r(A) = \{x \in A \mid [A, A, x] = 0\}$; their intersection $\mathrm{Nuc}(A) = \{x \in A \mid [A, A, x] = [A, x, A] = [x, A, A] = 0\}$ is the **nucleus** of A. $\mathrm{Nuc}(A)$, $\mathrm{Nuc}_l(A)$, $\mathrm{Nuc}_m(A)$ and $\mathrm{Nuc}_r(A)$ are all associative subalgebras of A. The **commutator** of A is the set of all elements which commute with every other element,

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

The **center** of A is $\mathrm{Cent}(A) = \mathrm{Nuc}(A) \cap \mathrm{Comm}(A)$.

If D is an associative division ring, an automorphism $\sigma : D \to D$ is called an **inner automorphism** if $\sigma = I_u : x \mapsto uxu^{-1}$ for some $u \in D^\times$. The **inner order** of an automorphism σ of D, is the smallest positive integer n such that σ^n is an inner automorphism. If no such n exists we say σ has **infinite inner order**.

A **left (right) principal ideal domain** is a domain R such that every left (right) ideal in R is of the form Rf (fR) for some $f \in R$. We say R is a **principal ideal domain**, if it is both a left and a right principal ideal domain.

Let R be a left principal ideal domain and $0 \neq a, b \in R$. Then there exists $d \in R$ such that $Ra + Rb = Rd$. This implies $a = c_1 d$ and $b = c_2 d$ for some $c_1, c_2 \in R$, so d is a right factor of both a and b. We denote this by writing $d|_r a$ and $d|_r b$. In addition, if $e|_r a$ and $e|_r b$, then $Ra \subset Re$, $Rb \subset Re$, hence $Rd \subset Re$ and so $e|_r d$. Therefore we call d a **right greatest common divisor** of a and b. Furthermore, there exists $g \in R$ such that $Ra \cap Rb = Rg$. Then $a|_r g$ and $b|_r g$. Moreover, if $a|_r n$ and $b|_r n$ then $Rn \subset Rg$ and so $g|_r n$. We call g the **least common left multiple** of a and b.

The **field norm** $N_{K/F} : K \to F$ of a finite Galois field extension K/F is given by

$$N_{K/F}(k) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(k).$$

In particular, if K/F is a cyclic Galois field extension of degree m with Galois group generated by σ, then the field norm has the form

$$N_{K/F}(k) = k\sigma(k) \cdots \sigma^{m-1}(k).$$

1.2 SKEW POLYNOMIAL RINGS

Let D be an associative ring, σ be an injective endomorphism of D and δ be a **left σ-derivation** of D, i.e. $\delta : D \to D$ is an additive map and satisfies

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b,$$

for all $a, b \in D$, in particular $\delta(1) = 0$. Furthermore, an easy induction yields

$$\delta(a^n) = \sum_{i=0}^{n-1} \sigma(a)^i \delta(a) a^{n-1-i}, \tag{1.1}$$

for all $a \in D$, $n \in \mathbb{N}$ [25, Lemma 1.1]. The set $\mathrm{Const}(\delta) = \{d \in D \mid \delta(d) = 0\}$ of **δ-constants** forms a subring of D, moreover if D is a division ring, this is a division subring of D [32, p. 7].

The following definition is due to Ore [51]:

Definition. *The **skew polynomial ring** $R = D[t;\sigma,\delta]$ is the set of left polynomials $a_0 + a_1t + a_2t^2 + \ldots + a_mt^m$ with $a_i \in D$, where addition is defined term-wise, and multiplication by $ta = \sigma(a)t + \delta(a)$.*

This multiplication makes R into an associative ring [32, p. 2-3]. If $\delta = 0$, then $D[t;\sigma,0] = D[t;\sigma]$ is called a **twisted polynomial ring**, and if σ is the identity map, then $D[t;\mathrm{id},\delta] = D[t;\delta]$ is called a **differential polynomial ring**. For the special case that $\delta = 0$ and $\sigma = \mathrm{id}$, we obtain the usual left polynomial ring $D[t] = D[t;\mathrm{id},0]$. Skew polynomial rings are also called Ore extensions in the literature and their properties are well understood. For a thorough introduction to skew polynomial rings see for example [16, Chapter 2], [32, Chapter 1] and [51].

We briefly mention some definitions and properties of skew polynomials which will be useful to us: The associative and distributive laws in $R = D[t;\sigma,\delta]$ yield

$$t^n b = \sum_{j=0}^{n} S_{n,j}(b)t^j, \quad n \geq 0, \tag{1.2}$$

and

$$(bt^n)(ct^m) = \sum_{j=0}^{n} b(S_{n,j}(c))t^{j+m}, \tag{1.3}$$

for all $b, c \in D$, where the maps $S_{n,j} : D \to D$ are defined by the recursion formula

$$S_{n,j} = \delta S_{n-1,j} + \sigma S_{n-1,j-1}, \tag{1.4}$$

with $S_{0,0} = \mathrm{id}_D$, $S_{1,0} = \delta$, $S_{1,1} = \sigma$ and $S_{n,0} = \delta^n$ [32, p. 2]. This means $S_{n,j}$ is the sum of all monomials in σ and δ that are of degree j in σ and of degree $n - j$ in δ. In particular $S_{n,n} = \sigma^n$ and if $\delta = 0$ then $S_{n,j} = 0$ for $n \neq j$.

We say $f(t) \in R$ is **right invariant** if Rf is a two-sided ideal in R, $f(t)$ is **left invariant** if fR is a two-sided ideal in R, and $f(t)$ is **invariant** if it is both right and left invariant. We define the **degree** of a polynomial $f(t) = a_m t^m + \ldots + a_1 t + a_0 \in R$ with $a_m \neq 0$ to be $\deg(f(t)) = m$ and $\deg(0) = -\infty$. We call a_m the **leading coefficient** of $f(t)$. Then $\deg(g(t)h(t)) \leq \deg(g(t)) + \deg(h(t))$ for all $g(t), h(t) \in R$, with equality if D is a domain. This implies that when D is a domain, $D[t; \sigma, \delta]$ is also a domain.

Henceforth we assume D is a division ring and remark that every endomorphism of D is necessarily injective. Then $R = D[t; \sigma, \delta]$ is a left principal ideal domain and there is a **right division algorithm** in R [32, p. 3]. That is, for all $f(t), g(t) \in R$ with $f(t) \neq 0$ there exist unique $r(t), q(t) \in R$ with $\deg(r(t)) < \deg(f(t))$, such that $g(t) = q(t)f(t) + r(t)$. Here $r(t)$ is the remainder after right division by $f(t)$, and if $r(t) = 0$ we say $f(t)$ **right divides** $g(t)$ and write $f(t)|_r g(t)$. A polynomial $f(t) \in R$ is **irreducible** if it is not a unit and has no proper factors, i.e. there do not exist $g(t), h(t) \in R$ with $\deg(g(t))$, $\deg(h(t)) < \deg(f(t))$ such that $f(t) = g(t)h(t)$. Two non-zero $f(t), g(t) \in R$ are **similar** if there exist unique $h, q, u \in R$ such that $1 = hf + qg$ and $u'f = gu$ for some $u' \in R$. Notice if $f(t)$ is similar to $g(t)$ then $\deg(f(t)) = \deg(g(t))$ [32, p. 14].

If σ is a ring automorphism, then R is also a right principal ideal domain, (hence a principal ideal domain) [32, Proposition 1.1.14], and there exists a left division algorithm in R [32, p. 3 and Proposition 1.1.14]. In this case any right invariant polynomial $f(t)$ is invariant [32, p. 6], furthermore we can also view R as the set of right polynomials with multiplication defined by $at = t\sigma^{-1}(a) - \delta(\sigma^{-1}(a))$ for all $a \in D$ [32, (1.1.15)].

1.3 PETIT'S ALGEBRA CONSTRUCTION

In this Section, we describe the construction of a family of nonassociative algebras S_f built using skew polynomial rings. These algebras will be the focus of study of this thesis. They were first introduced in 1966 by Petit [52], [53], and laregly ignored until Wene [66] and more recently Lavrauw and Sheekey [44] studied them in the context of semifields.

Let D be an associative division ring with center C, σ be an endomorphism of D and δ be a left σ-derivation of D.

Definition (Petit [52]). *Let $f(t) \in R = D[t;\sigma,\delta]$ be of degree m and*

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

Define a multiplication $\circ$ on R_m by $a \circ b = ab \bmod_r f$, where the juxtaposition ab denotes multiplication in R, and $\bmod_r f$ denotes the remainder after right division by $f(t)$. Then $S_f = (R_m, \circ)$ is a nonassociative algebra over $F = \{c \in D \mid c \circ h = h \circ c \text{ for all } h \in S_f\}$. We also call the algebras S_f ***Petit algebras*** *and denote them by R/Rf if we want to make it clear which ring R is used in the construction.*

W.l.o.g., we may assume $f(t)$ is monic, since the algebras S_f and S_{df} are equal for all $d \in D^\times$. We obtain the following straightforward observations:

Remarks. *(i) If $f(t)$ is right invariant, then S_f is the associative quotient algebra obtained by factoring out the two-sided ideal Rf.*

(ii) *If* $\deg(g(t)) + \deg(h(t)) < m$, *then the multiplication* $g \circ h$ *is the usual multiplication of polynomials in* R.

(iii) *If* $\deg(f(t)) = 1$ *then* $R_1 = D$ *and* $S_f \cong D$. *We will assume throughout this thesis that* $\deg(f(t)) \geq 2$.

Note that F is a subfield of D [52, (7)]. It is straightforward to see that $F = C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$. Indeed, if $c \in F$ then $c \in D$ and $c \circ h = h \circ c$ for all $h \in S_f$, in particular this means $c \in C$. Furthermore, we have $c \circ t = t \circ c$ so that $ct = \sigma(c)t + \delta(c)$, hence $\sigma(c) = c$ and $\delta(c) = 0$ and thus $F \subset C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$.

Conversely, if $c \in C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$ and $h = \sum_{i=0}^{m-1} h_i t^i \in S_f$, then

$$hc = \sum_{i=0}^{m-1} h_i t^i c = \sum_{i=0}^{m-1} h_i \sum_{j=0}^{i} S_{i,j}(c) t^j = \sum_{i=0}^{m-1} h_i c t^i = \sum_{i=0}^{m-1} c h_i t^i = ch,$$

because $S_{i,j}(c) = 0$ for $i \neq j$ and $S_{i,i}(c) = \sigma^i(c) = c$. Therefore $c \in F$ as required. In the special case where D is commutative and $\delta = 0$ then $F = \mathrm{Fix}(\sigma)$.

Examples 1.1. (i) *Let* $f(t) = t^m - a \in D[t;\sigma]$ *where* $a \neq 0$. *Then the multiplication in* S_f *is given by*

$$(bt^i) \circ (ct^j) = \begin{cases} b\sigma^i(c)t^{i+j} & \text{if } i+j < m, \\ b\sigma^i(c)\sigma^{i+j-m}(a)t^{i+j-m} & \text{if } i+j \geq m, \end{cases}$$

for all $b, c \in D$ *and* $i, j \in \{0, \ldots, m-1\}$, *then linearly extended.*

(ii) *Let* $f(t) = t^2 - a_1 t - a_0 \in D[t;\sigma]$. *Then multiplication in* S_f *is given by*

$$(x + yt) \circ (u + vt) = \big(xu + y\sigma(v)a_0\big) + \big(xv + y\sigma(u) + y\sigma(v)a_1\big)t,$$

for all $x, y, u, v \in D$. *By identifying* $x + yt = (x, y)$ *and* $u + vt = (u, v)$, *the multiplication in* S_f *can also be written as*

$$(x + yt) \circ (u + vt) = (x, y) \begin{pmatrix} u & v \\ \sigma(v)a_0 & \sigma(u) + \sigma(v)a_1 \end{pmatrix}.$$

(iii) Let $f(t) = t^2 - a \in D[t;\sigma,\delta]$, then multiplication in S_f is given by

$$(x + yt) \circ (u + vt) = (x, y) \begin{pmatrix} u & v \\ \sigma(v)a + \delta(u) & \sigma(u) + \delta(v) \end{pmatrix},$$

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

When σ is an automorphism there is also a left division algorithm in R and can define a second algebra construction: Let $f(t) \in R$ be of degree m and denote by $\mathrm{mod}_l f$ the remainder after left division by $f(t)$. Then R_m together with the multiplication $a \ {}_f{\circ}\ b = ab \ \mathrm{mod}_l f$, becomes a nonassociative algebra ${}_fS$ over F, also denoted R/fR. It suffices to study the algebras S_f, as every algebra ${}_fS$ is the opposite algebra of some Petit algebra:

Proposition 1.2. *([52, (1)]). Suppose $\sigma \in \mathrm{Aut}(D)$ and $f(t) \in D[t;\sigma,\delta]$. The canonical anti-isomorphism*

$$\psi : D[t;\sigma,\delta] \to D^{\mathrm{op}}[t;\sigma^{-1}, -\delta\sigma^{-1}], \ \sum_{i=0}^{n} a_i t^i \mapsto \sum_{i=0}^{n} \Big(\sum_{j=0}^{i} S_{n,j}(a_i) \Big) t^i,$$

between the skew polynomial rings $D[t;\sigma,\delta]$ and $D^{\mathrm{op}}[t;\sigma^{-1}, -\delta\sigma^{-1}]$, induces an anti-isomorphism between $S_f = D[t;\sigma,\delta]/D[t;\sigma,\delta]f$, and

$${}_{\psi(f)}S = D^{\mathrm{op}}[t;\sigma^{-1}, -\delta\sigma^{-1}]/\psi(f) D^{\mathrm{op}}[t;\sigma^{-1}, -\delta\sigma^{-1}].$$

1.4 RELATION OF S_f TO OTHER KNOWN CONSTRUCTIONS

We now show connections between Petit algebras and some other known constructions of algebras.

1.4.1 *Nonassociative Cyclic Algebras*

Let K/F be a cyclic Galois field extension of degree m with $\mathrm{Gal}(K/F) = \langle \sigma \rangle$ and $f(t) = t^m - a \in K[t;\sigma]$. Then

$$A = (K/F, \sigma, a) = K[t;\sigma]/K[t;\sigma]f(t)$$

is called a **nonassociative cyclic algebra of degree** m over F. The multiplication in A is associative if and only if $a \in F$, in which case A is a classical associative cyclic algebra over F.

Nonassociative cyclic algebras were studied in detail by Steele in his Ph.D. thesis [64]. We remark that our definition of nonassociative cyclic algebras yields the opposite algebras to the ones studied by Steele in [64]. Moreover, if K is a finite field, then A is an example of a Sandler semifield [58].

Nonassociative cyclic algebras of degree 2 are **nonassociative quaternion algebras**. These algebras were first studied in 1935 by Dickson [19] and subsequently by Althoen, Hansen and Kugler [2] over $\mathbb{R}$, however, the first systematic study was carried out by Waterhouse [65].

Classical associative quaternion algebras of characteristic not 2 are precisely associative cyclic algebras of degree 2. That is, they have the form $(K/F, \sigma, a)$ where K/F is a quadratic separable field extension with non-trivial automorphism σ, $\mathrm{char}(F) \neq 2$ and $a \in F^{\times}$. Thus the only difference in defining nonassociative quaternion algebras, is that the element a belongs to the larger field K.

1.4.2 *(Nonassociative) Generalised Cyclic Algebras*

Let D be an associative division algebra of degree n over its center C and σ be an automorphism of D such that $\sigma|_C$ has finite order m and fixed field $F = C \cap \mathrm{Fix}(\sigma)$. A **nonassociative generalised cyclic algebra** of degree mn, is an algebra $S_f = D[t;\sigma]/D[t;\sigma]f(t)$ over F with $f(t) = t^m - a \in D[t;\sigma]$, $a \in D^{\times}$. We denote this algebra (D, σ, a) and note that it has dimension n^2m^2 over F. Note that when $D = K$ is a field, and K/F is a cyclic field extension with Galois group generated by σ, we obtain the nonassociative cyclic algebra $(K/F, \sigma, a)$.

In the special case where $f(t) = t^m - a \in D[t;\sigma]$, $d \in F^{\times}$, then $f(t)$ is invariant and (D, σ, a) is the associative **generalised cyclic algebra** defined by Jacobson [32, p. 19].

1.4.3 *(Nonassociative) Generalised Differential Algebras*

Let C be a field of characteristic p and D be an associative central division algebra over C of degree n. Suppose δ is a derivation of D such that $\delta|_C$ is algebraic, that is there exists a p-polynomial

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

where $F = C \cap \mathrm{Const}(\delta)$ such that $g(\delta) = 0$. Suppose $g(t)$ is chosen with minimal e, $d \in D$ and $f(t) = g(t) - d \in D[t;\delta]$, then the algebra $S_f = D[t;\delta]/D[t;\delta]f(t)$ is called a **(nonassociative) generalised differential algebra** and also denoted (D,δ,d) [56]. (D,δ,d) is a nonassociative algebra over F of dimension $p^{2e}n^2$, moreover (D,δ,d) is associative if and only if $d \in F$.

When $d \in F$, then (D,δ,d) is central simple over F and is called the **generalised differential extension** of D in [32, p. 23].

For the remainder of this Section we consider examples of finite-dimensional division algebras over finite fields. These are called (finite) semifields in the literature.

1.4.4 *Hughes-Kleinfeld and Knuth Semifields*

Let K be a finite field and σ be a non-trivial automorphism of K. Choose $a_0, a_1 \in K$ such that the equation $w\sigma(w) + a_1 w - a_0 = 0$ has no solution $w \in K$. In [35, p. 215], Knuth defined four classes of semifields two-dimensional over K with unit element $(1,0)$. Their multiplications are defined by

$$\text{(K1)}: (x,y)(u,v) = \big(xu + a_0\sigma^{-2}(y)\sigma(v),\ xv + y\sigma(u) + a_1\sigma^{-1}(y)\sigma(v)\big),$$
$$\text{(K2)}: (x,y)(u,v) = \big(xu + a_0\sigma^{-2}(y)\sigma^{-1}(v),\ xv + y\sigma(u) + a_1\sigma^{-1}(y)v\big),$$
$$\text{(K3)}: (x,y)(u,v) = \big(xu + a_0 y\sigma^{-1}(v),\ xv + y\sigma(u) + a_1 yv\big),$$
$$\text{(K4)}: (x,y)(u,v) = \big(xu + a_0 y\sigma(v),\ xv + y\sigma(u) + a_1 y\sigma(v)\big).$$

The class of semifields defined by the multiplication (K4) were first discovered by Hughes and Kleinfeld [29] and are called **Hughes-Kleinfeld semifields**.

The classes of semifields defined by the multiplications (K2) and (K4) can be obtained using Petit's construction:

Theorem 1.3. *([61, Theorem 5.15]). Let $f(t) = t^2 - a_1 t - a_0 \in K[t;\sigma]$ where $w\sigma(w) + a_1 w - a_0 \neq 0$ for all $w \in K$.*

(i) ${}_fS$ is isomorphic to the semifield $(K2)$.

(ii) S_f is isomorphic to the semifield $(K4)$.

There is a small mistake in [61, p. 63 (5.1) and (5.2)] where the multiplication of two elements of S_f is stated incorrectly. We give the full proof to avoid confusion.

Proof. (i) The multiplication in ${}_fS$ is given by

$$\begin{aligned}(x+yt)\ {}_f\circ(u+vt) &= xu + xvt + y\sigma(u)t + t^2\sigma^{-2}(y)\sigma^{-1}(v)\\ &= xu + xvt + y\sigma(u)t + (a_1t + a_0)\sigma^{-2}(y)\sigma^{-1}(v)\\ &= xu + xvt + y\sigma(u)t + a_1\sigma^{-1}(y)vt + a_0\sigma^{-2}(y)\sigma^{-1}(v)\\ &= \big(xu + a_0\sigma^{-2}(y)\sigma^{-1}(v)\big) + \big(xv + y\sigma(u) + a_1\sigma^{-1}(y)v\big)t,\end{aligned}$$

for all $x, y, u, v \in K$. Therefore the map $\psi : {}_fS \to$ (K2), $x + yt \mapsto (x, y)$ can easily be seen to be an isomorphism.

(ii) The multiplication in S_f is given by

$$\begin{aligned}(x+yt)\circ(u+vt) &= xu + xvt + y\sigma(u)t + y\sigma(v)t^2\\ &= xu + xvt + y\sigma(u)t + y\sigma(v)(a_1t + a_0)\\ &= \big(xu + y\sigma(v)a_0\big) + \big(xv + y\sigma(u) + y\sigma(v)a_1\big)t,\end{aligned}$$

for all $x, y, u, v \in K$. Therefore the map $\phi : S_f \to$ (K4), $x + yt \mapsto (x, y)$ can readily be seen to be an isomorphism.

□

1.4.5 *Jha-Johnson Semifields*

Jha-Johnson semifields, also called cyclic semifields, are built using irreducible semilinear transformations and generalise the Sandler and Hughes-Kleinfield semifields.

Definition. *Let K be a field. An additive map $T : V \to V$ on a vector space $V = K^m$ is called a **semilinear transformation** if there exists $\sigma \in \mathrm{Aut}(K)$ such that $T(\lambda v) = \sigma(\lambda)T(v)$, for all $\lambda \in K, v \in V$. The set of invertible semilinear transformations on V forms a group called the **general semilinear group** and is denoted by $\Gamma L(V)$. An element $T \in \Gamma L(V)$ is said to be **irreducible**, if the only T-invariant subspaces of V are V and $\{0\}$.*

Suppose now K is a finite field.

Definition ([33])**.** *Let $T \in \Gamma L(V)$ be irreducible and fix a K-basis $\{e_0, \dots, e_{m-1}\}$ of V. Define a multiplication $\cdot$ on V by*

$$a \cdot b = a(T)b = \sum_{i=0}^{m-1} a_i T^i(b),$$

*where $a = \sum_{i=0}^{m-1} a_i e_i$. Then $\mathbb{S}_T = (V, \cdot)$ defines a **Jha-Johnson semifield**.*

Let $L_{t,f}$ denote the semilinear transformation $v \mapsto tv \ \mathrm{mod}_r f$.

Theorem 1.4. *([44, Theorems 15 and 16]). If σ is an automorphism of K and $f(t) \in K[t;\sigma]$ is irreducible then $S_f \cong \mathbb{S}_{L_{t,f}}$. Conversely, if T is any irreducible element of $\Gamma L(V)$ with automorphism σ, $\mathbb{S}_T$ is isotopic to S_f for some irreducible $f(t) \in K[t;\sigma]$.*

This means that every Petit algebra S_f with $f(t) \in K[t;\sigma]$ irreducible is a Jha-Johnson semifield, and every Jha-Johnson semifield is isotopic to some S_f.

2

THE STRUCTURE OF PETIT ALGEBRAS

In the following, let D be an associative division ring with center C, σ be an endomorphism of D, δ be a left σ-derivation of D and $f(t) \in R = D[t;\sigma,\delta]$. Recall S_f is a nonassociative algebra over $F = C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$.

2.1 SOME STRUCTURE THEORY

In this Section we investigate the structure theory of Petit algebras. We begin by summarising some of the structure results stated by Petit in [52]:

Theorem 2.1. *([52, (2), (5), (1), (14), (15)]). Let $f(t) \in R$ be of degree m.*

(i) If S_f is not associative then

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

and

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

(ii) The powers of t are associative if and only if $t^m \circ t = t \circ t^m$ if and only if $t \in \mathrm{Nuc}_r(S_f)$.

(iii) S_f is associative if and only if $f(t)$ is right invariant.

(iv) Suppose $\delta = 0$, then $\mathrm{Comm}(S_f)$ contains the set

$$\Big\{ \sum_{i=0}^{m-1} c_i t^i \mid c_i \in \mathrm{Fix}(\sigma) \text{ and } dc_i = c_i \sigma^i(d) \text{ for all } d \in D,\ i = 0, \ldots, m-1 \Big\}. \tag{2.1}$$

If t is left invertible the two sets are equal.

(v) *Suppose $\delta = 0$ and $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in D[t;\sigma]$. Then $f(t)$ is right invariant if and only if $\sigma^m(z)a_i = a_i\sigma^i(z)$ and $\sigma(a_i) = a_i$ for all $z \in D$, $i \in \{0, \ldots, m-1\}$.*

The nuclei of S_f were also calculated for special cases by Dempwolff in [17, Proposition 3.3].

Remark. *([55, Remark 9]). If $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in D[t;\sigma]$, then t is left invertible is equivalent to $a_0 \neq 0$. Indeed, if $a_0 = 0$ and there exists $g(t) \in R_m$ and $q(t) \in R$ such that $g(t)t = q(t)f(t) + 1$, then the left side of the equation has constant term 0, while the right hand side has constant term 1, a contradiction.*

Conversely, if $a_0 \neq 0$ then defining $g(t) = a_0^{-1}t^{m-1} - \sum_{i=0}^{m-2} a_0^{-1}a_{i+1}t^i$, we conclude $g(t)t = a_0^{-1}f(t) + 1$, therefore $g(t) \circ t = 1$ and t is left invertible in S_f.

Corollary 2.2. *Suppose $\sigma \in \mathrm{Aut}(D)$ is such that $\sigma|_C$ has order at least m or infinite order, $f(t) \in D[t;\sigma]$ has degree m and $t \in S_f$ is left invertible. Then* $\mathrm{Comm}(S_f) = F = C \cap \mathrm{Fix}(\sigma)$.

Proof. $\mathrm{Comm}(S_f)$ is equal to the set (2.1) by Theorem 2.1(iv), in particular $F = C \cap \mathrm{Fix}(\sigma) \subseteq \mathrm{Comm}(S_f)$. Let now $\sum_{i=0}^{m-1} c_i t^i \in \mathrm{Comm}(S_f)$ and suppose, for contradiction, $c_j \neq 0$ for some $j \in \{1, \ldots, m-1\}$. Then $bc_j = c_j\sigma^j(b)$ for all $b \in D$, thus $(b - \sigma^j(b))c_j = 0$ for all $b \in C$ and so $b - \sigma^j(b) = 0$ for all $b \in C$, a contradiction since $\sigma|_C$ has order $\geq m$. Therefore $\sum_{i=0}^{m-1} c_i t^i = c_0$ and $c_0 \in F$ by (2.1). □

Proposition 2.3. *Let L be a division subring of D such that $\sigma|_L$ is an endomorphism of L and $\delta|_L$ is a $\sigma|_L$-derivation of L. If $f(t) \in L[t;\sigma|_L,\delta|_L]$ then $L[t;\sigma|_L,\delta|_L]/L[t;\sigma|_L,\delta|_L]f(t)$ is a subring of $S_f = D[t;\sigma,\delta]/D[t;\sigma,\delta]f(t)$.*

Proof. Clearly $L[t;\sigma|_L,\delta|_L]/L[t;\sigma|_L,\delta|_L]f(t)$ is a subset of S_f and is a ring in its own right. Additionally $L[t;\sigma|_L,\delta|_L]/L[t;\sigma|_L,\delta|_L]f(t)$ inherits the multiplication in S_f by the uniqueness of right division in $L[t;\sigma|_L,\delta|_L]$ and in $D[t;\sigma,\delta]$. □

Given $f(t) \in R = D[t;\sigma,\delta]$ of degree m, the **idealizer** $I(f) = \{g \in R \mid fg \in Rf\}$ is the largest subalgebra of R in which Rf is a two-sided ideal. We then define the **eigenring** of $f(t)$ as the quotient $E(f) = I(f)/Rf$. Therefore the eigenring

$$E(f) = \{g \in R \mid \deg(g) < m \text{ and } fg \in Rf\}$$

is equal to the right nucleus $\mathrm{Nuc}_r(S_f)$ by Theorem 2.1(i), which as the right nucleus, is an associative subalgebra of S_f. By Theorem 2.1(i) we obtain:

Corollary 2.4. *Let $f(t) \in R$.*

(i) $E(f) = S_f$ if and only if $f(t)$ is right invariant if and only if S_f is associative.

(ii) If $f(t)$ is not right invariant then $\mathrm{Cent}(S_f) = F$.

Proof. (i) If $f(t)$ is not right invariant then $E(f) = \mathrm{Nuc}_r(S_f) \neq S_f$ by Theorem 2.1(i). On the other hand if $f(t)$ is right invariant, then Rf is a two-sided ideal, hence $f|_r fg$ for all $g \in R_m$ and so $E(f) = S_f$.

(ii) We have

$$\begin{aligned}\mathrm{Cent}(S_f) &= \mathrm{Comm}(S_f) \cap \mathrm{Nuc}(S_f) = \mathrm{Comm}(S_f) \cap D \cap E(f)\\ &= F \cap E(f) = F,\end{aligned}$$

by Theorem 2.1.

□

Example 2.5. *If K is a finite field, σ is an automorphism of K and $f(t) \in K[t;\sigma]$ is irreducible of degree m, then*

$$E(f) = \{u \bmod_r f \mid u \in \mathrm{Cent}(K[t;\sigma])\} \cong \mathbb{F}_{q^m}$$

by [44, p. 9].

Theorem 2.6. *Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in D[t;\sigma,\delta]$ be such that $f(t)$ is not right invariant and $a_j \in \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$ for all $j \in \{0,\dots,m-1\}$. Then the set*

$$\Big\{ \sum_{i=0}^{m-1} k_i t^i \mid k_i \in F = C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta) \Big\}, \tag{2.2}$$

is contained in $\mathrm{Nuc}_r(S_f)$.

Proof. Clearly $F \subseteq \mathrm{Nuc}_r(S_f)$, therefore if we can show $t \in \mathrm{Nuc}_r(S_f)$, then (2.2) is contained in $\mathrm{Nuc}_r(S_f)$. To this end, we calculate

$$t^m \circ t = \Big(\sum_{i=0}^{m-1} a_i t^i\Big) \circ t = \sum_{i=0}^{m-2} a_i t^{i+1} + a_{m-1} \sum_{i=0}^{m-1} a_i t^i,$$

and

$$\begin{aligned} t \circ t^m &= t \circ \Big(\sum_{i=0}^{m-1} a_i t^i\Big) = t \circ a_{m-1} t^{m-1} + t \circ \sum_{i=0}^{m-2} a_i t^i \\ &= \big(\sigma(a_{m-1})t + \delta(a_{m-1})\big) \circ t^{m-1} + \sum_{i=0}^{m-2} \big(\sigma(a_i)t + \delta(a_i)\big) t^i \\ &= a_{m-1} \sum_{i=0}^{m-1} a_i t^i \ + \ \sum_{i=0}^{m-2} a_i t^{i+1}, \end{aligned}$$

since $a_0, a_1, \ldots, a_{m-1} \in \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$. Therefore $t^m \circ t = t \circ t^m$, which yields $t \in \mathrm{Nuc}_r(S_f)$ by Theorem 2.1(ii). $\square$

If we assume additionally $a_j \in C$ in Theorem 2.6, i.e. we assume $f(t) \in F[t]$, then we obtain:

Corollary 2.7. *Let $f(t) \in F[t] = F[t;\sigma,\delta] \subset D[t;\sigma,\delta]$ be of degree m and not right invariant. Then the set* (2.2) *is a commutative subalgebra of* $\mathrm{Nuc}_r(S_f)$. *Here* (2.2) *equals $F[t]/F[t]f(t)$. Furthermore, if $f(t)$ is irreducible in $F[t]$, the set* (2.2) *is a field.*

Proof. S_f contains the commutative subalgebra $F[t]/F[t]f(t)$ which is isomorphic to (2.2) because $f(t) \in F[t]$. Now, (2.2) is contained in $\mathrm{Nuc}_r(S_f)$ by Theorem 2.6 and thus if $f(t)$ is irreducible in $F[t]$, then $F[t]/F[t]f(t)$ is a field. $\square$

When $\sigma = \mathrm{id}$, Corollary 2.7 is precisely [56, Proposition 2].

Remark. *Suppose K is a finite field, σ is an automorphism of K and $F = \mathrm{Fix}(\sigma)$. If $f(t) \in F[t] \subset K[t;\sigma]$ is irreducible and not right invariant, then* (2.2) *is equal to* $\mathrm{Nuc}_r(S_f)$ *[66, Theorem 3.2].*

2.2 SO-CALLED RIGHT SEMI-INVARIANT POLYNOMIALS

As in the previous Section, suppose D is a division ring with center C, σ is an endomorphism of D, δ is a left σ-derivation of D and $f(t) \in R = D[t;\sigma,\delta]$. We now investigate conditions for D to be contained in the right nucleus of S_f, therefore either S_f is associative or $\mathrm{Nuc}(S_f) = D$ by Theorem 2.1(i). We do this by looking at so-called right semi-invariant polynomials:

Definition. *([39], [42]). A polynomial $f(t) \in R$ is called **right semi-invariant** if $f(t)D \subseteq Df(t)$. Similarly, $f(t)$ is **left semi-invariant** if $Df(t) \subseteq f(t)D$.*

We have $f(t)$ is right semi-invariant if and only if $df(t)$ is right semi-invariant for all $d \in D^\times$ [39, p. 8]. For this reason it suffices to only consider monic $f(t)$. Furthermore, if σ is an automorphism, then $f(t)$ is right semi-invariant if and only if it is left semi-invariant if and only if $f(t)D = Df(t)$ [39, Proposition 2.7].

For a thorough background on right semi-invariant polynomials we refer the reader to [39] and [42]. Our interest in right semi-invariant polynomials stems from the following result:

Theorem 2.8. *$f(t) \in R$ is right semi-invariant if and only if $D \subseteq \mathrm{Nuc}_r(S_f)$. In particular, if $f(t)$ is right semi-invariant, then either $\mathrm{Nuc}(S_f) = D$ or S_f is associative.*

Proof. If $f(t) \in R$ is right semi-invariant, $f(t)D \subseteq Df(t) \subseteq Rf(t)$ and hence $D \subseteq E(f) = \mathrm{Nuc}_r(S_f)$. Conversely, if $D \subseteq \mathrm{Nuc}_r(S_f) = E(f)$ then for all $d \in D$, there exists $q(t) \in R$ such that $f(t)d = q(t)f(t)$. Comparing degrees, we see $q(t) \in D$ and thus $f(t)D \subseteq Df(t)$.

The second assertion follows by Theorem 2.1(i). $\square$

The following result on the existence of a non-constant right semi-invariant polynomial is due to Lemonnier [45]:

Proposition 2.9. *([45, (9.21)]). Suppose σ is an automorphism of D, then the following are equivalent:*

(i) *There exists a non-constant right semi-invariant polynomial in R.*

(ii) *R is not simple.*

(iii) *There exist $b_0, \dots, b_n \in D$ with $b_n \neq 0$ such that $b_0 \delta_{c,\theta} + \sum_{i=1}^{n} b_i \delta^i = 0$, where θ is an endomorphism of D and $\delta_{c,\theta}$ denotes the θ-derivation of D sending $x \in D$ to $cx - \theta(x)c$.*

Combining Theorem 2.8 and Proposition 2.9 we conclude:

Corollary 2.10. *Suppose σ is an automorphism of D and R is simple. Then there are no nonassociative algebras S_f with $D \subseteq \mathrm{Nuc}_r(S_f)$. In particular there are no nonassociative algebras S_f with $D \subseteq \mathrm{Nuc}(S_f)$.*

Proof. R is not simple if and only if there exists a non-constant right semi-invariant polynomial in R by Proposition 2.9, and hence the assertion follows by Theorem 2.8. □

Theorem 2.8 allows us to rephrase some of the results on semi-invariant polynomials in [39] and [42], in terms of the right nucleus of S_f:

Theorem 2.11. *([39, Lemma 2.2, Corollary 2.12, Propositions 2.3 and 2.4], [42, Corollary 2.6]). Let $f(t) = \sum_{i=0}^{m} a_i t^i \in R$ be monic of degree m.*

(i) *$D \subseteq \mathrm{Nuc}_r(S_f)$ if and only if $f(t)c = \sigma^m(c) f(t)$ for all $c \in D$, if and only if*
$$\sigma^m(c) a_j = \sum_{i=j}^{m} a_i S_{i,j}(c) \tag{2.3}$$
for all $c \in D$ and $j \in \{0, \dots, m-1\}$, where $S_{i,j}$ is defined as in (1.4).

(ii) *Suppose σ is an automorphism of D of infinite inner order. Then $D \subseteq \mathrm{Nuc}_r(S_f)$ implies S_f is associative.*

(iii) *Suppose $\delta = 0$. Then $D \subseteq \mathrm{Nuc}_r(S_f)$ if and only if*
$$\sigma^m(c) = a_j \sigma^j(c) a_j^{-1} \tag{2.4}$$
for all $c \in D$ and all $j \in \{0, \dots, m-1\}$ with $a_j \neq 0$. Furthermore, S_f is associative if and only if $f(t)$ satisfies (2.4) and $a_j \in \mathrm{Fix}(\sigma)$ for all $j \in \{0, \dots, m-1\}$.

(iv) Suppose $\delta = 0$ *and* σ *is an automorphism of* D *of finite inner order* k*, i.e.* $\sigma^k = I_u$ *for some* $u \in D^\times$*. The polynomials* $g(t) \in D[t;\sigma]$ *such that* $D \subseteq \mathrm{Nuc}_r(S_g)$ *are precisely those of the form*

$$b\sum_{j=0}^{n} c_j u^{n-j} t^{jk}, \tag{2.5}$$

where $n \in \mathbb{N}$*,* $c_n = 1$*,* $c_j \in C$ *and* $b \in D^\times$*. Furthermore,* S_g *is associative if and only if* $g(t)$ *has the form* (2.5) *and* $c_j u^{n-j} \in \mathrm{Fix}(\sigma)$ *for all* $j \in \{0, \ldots, n\}$*.*

(v) Suppose $\sigma = \mathrm{id}$*. Then* $D \subseteq \mathrm{Nuc}_r(S_f)$ *is equivalent to*

$$ca_j = \sum_{i=j}^{m} \binom{i}{j} a_i \delta^{i-j}(c), \tag{2.6}$$

for all $c \in D$*,* $j \in \{0, \ldots, m-1\}$*. Furthermore,* S_f *is associative if and only if* $f(t)$ *satisfies* (2.6) *and* $a_j \in \mathrm{Const}(\delta)$ *for all* $j \in \{0, \ldots, m-1\}$*.*

Theorem 2.11(iii) provides us with an alternate proof of [64, Corollary 3.2.6] about the nucleus of nonassociative cyclic algebras:

Corollary 2.12. *([64, Corollary 3.2.6]). Let* $A = (K/F, \sigma, a)$ *be a nonassociative cyclic algebra of degree* m *for some* $a \in K \setminus F$*. Then* $\mathrm{Nuc}(A) = K$*.*

Proof. Notice $A = K[t;\sigma]/K[t;\sigma](t^m - a)$ and $t^m - a$ is right semi-invariant by Theorem 2.11(iii). Hence $K \subseteq \mathrm{Nuc}_r(A)$ by Theorem 2.8 since A is not associative. □

Let L be a division subring of D. Then we can look for conditions for $L \subseteq \mathrm{Nuc}_r(S_f)$ by generalising the definition of right semi-invariant polynomials as follows: We say $f(t) \in D[t;\sigma,\delta]$ L**-weak semi-invariant** if $f(t)L \subseteq Df(t)$. Clearly any right semi-invariant polynomial is also L-weak semi-invariant for every division subring L of D. Moreover we obtain:

Proposition 2.13. $f(t)$ *is* L*-weak semi-invariant if and only if* $L \subseteq E(f) = \mathrm{Nuc}_r(S_f)$*. If* $f(t)$ *is* L*-weak semi-invariant but not right invariant, then* $L \subseteq \mathrm{Nuc}(S_f) \subseteq D$*.*

Proof. If $f(t) \in R$ is L-weak semi-invariant, $f(t)L \subseteq Df(t) \subseteq Rf(t)$ and hence $L \subseteq E(f)$. Conversely, if $L \subseteq E(f)$ then for all $l \in L$, there exists $q(t) \in R$ such that $f(t)l = q(t)f(t)$. Comparing degrees, we see $q(t) \in D$ and thus $f(t)L \subseteq Df(t)$.

Hence if $f(t)$ is L-weak semi-invariant but not right invariant, then

$$L \subseteq \mathrm{Nuc}(S_f) = E(f) \cap D \subseteq D$$

by Theorem 2.1, which yields the second assertion. □

Example 2.14. *Let K be a field, σ be a non-trivial automorphism of K, $L = \mathrm{Fix}(\sigma^j)$ be the fixed field of σ^j for some $j > 1$ and $f(t) = \sum_{i=0}^{n} a_i t^{ij} \in K[t;\sigma]$. Then*

$$f(t)l = \sum_{i=0}^{n} a_i t^{ij} l = \sum_{i=0}^{n} a_i \sigma^{ij}(l) t^{ij} = \sum_{i=0}^{n} a_i l t^{ij} = l f(t),$$

for all $l \in L$ and hence $f(t)L \subseteq Lf(t)$. In particular, $f(t)$ is L-weak semi-invariant.

It turns out that results similar to Theorem 2.11(i), (iii) and (v) also hold for L-weak semi-invariant polynomials:

Proposition 2.15. *Let $f(t) = \sum_{i=0}^{m} a_i t^i \in D[t;\sigma,\delta]$ be monic of degree m and L be a division subring of D.*

(i) $f(t)$ is L-weak semi-invariant if and only if $f(t)c = \sigma^m(c)f(t)$ for all $c \in L$, if and only if

$$\sigma^m(c)a_j = \sum_{i=j}^{m} a_i S_{i,j}(c) \tag{2.7}$$

for all $c \in L$, $j \in \{0, \dots, m-1\}$.

(ii) Suppose $\delta = 0$. Then $f(t)$ is L-weak semi-invariant if and only if $\sigma^m(c)a_j = a_j \sigma^j(c)$ for all $c \in L$, $j \in \{0, \dots, m-1\}$.

(iii) Suppose $\sigma = \mathrm{id}$. Then $f(t)$ is L-weak semi-invariant if and only if

$$ca_j = \sum_{i=j}^{m} \binom{i}{j} a_i \delta^{i-j}(c) \tag{2.8}$$

for all $c \in L$, $j \in \{0, \dots, m-1\}$.

Proof. (i) We have

$$f(t)c = \sum_{i=0}^{m} a_i t^i c = \sum_{i=0}^{m} a_i \sum_{j=0}^{i} S_{i,j}(c) t^j = \sum_{j=0}^{m} \sum_{i=j}^{m} a_i S_{i,j}(c) t^j \tag{2.9}$$

for all $c \in L$, hence the t^m coefficient of $f(t)c$ is $S_{m,m}(c) = \sigma^m(c)$, and so $f(t)$ is L-weak semi-invariant if and only if $f(t)c = \sigma^m(c) f(t)$ for all $c \in L$. Comparing the t^j coefficient of (2.9) and $\sigma^m(c)f(t)$ for all $j \in \{0, \ldots, m-1\}$ yields (2.7).

(ii) When $\delta = 0$, $S_{i,j} = 0$ unless $i = j$ in which case $S_{j,j} = \sigma^j$. Therefore (2.7) simplifies to $\sigma^m(c)a_j = a_j \sigma^j(c)$ for all $c \in L$, $j \in \{0, \ldots, m-1\}$.

(iii) When $\sigma = \mathrm{id}$ we have

$$t^i c = \sum_{j=0}^{i} \binom{i}{j} \delta^{i-j}(c)$$

for all $c \in D$ by [32, (1.1.26)] and thus

$$f(t)c = \sum_{i=0}^{m} a_i t^i c = \sum_{i=0}^{m} a_i \sum_{j=0}^{i} \binom{i}{j} \delta^{i-j}(c) t^j = \sum_{j=0}^{m} \sum_{i=j}^{m} \binom{i}{j} a_i \delta^{i-j}(c) t^j \tag{2.10}$$

for all $c \in L$. Furthermore $f(t)$ is L-weak semi-invariant is equivalent to $f(t)c = cf(t)$ for all $c \in L$ by (i). Comparing the t^j coefficient of (2.10) and $cf(t) = \sum_{i=0}^{m} c a_i t^i$ for all $c \in L$, $j \in \{0, \ldots, m-1\}$ yields (2.8).

□

2.3 WHEN ARE PETIT ALGEBRAS DIVISION ALGEBRAS?

In this Section we look at conditions for Petit algebras to be right or left division algebras. This is closely linked to whether the polynomial $f(t)$ used in their construction is irreducible.

Given $f(t) \in R = D[t;\sigma,\delta]$, recall S_f is a **right** (resp. **left**) **division algebra**, if the right multiplication $R_a : S_f \to S_f,\ x \mapsto x \circ a$, (resp. the left multiplication $L_a : S_f \to S_f,\ x \mapsto a \circ x$), is bijective for all $0 \neq a \in S_f$.

Furthermore S_f is a **division algebra** if it is both a right and a left division algebra. If S_f is finite-dimensional over F, then S_f is a division algebra if and only if it has no zero divisors [60, p. 12].

We say $f(t) \in R$ is **bounded** if there exists $0 \neq f^* \in R$ such that $Rf^* = f^*R$ is the largest two-sided ideal of R contained in Rf. The element f^* is determined by f up to multiplication on the left by elements of $D^\times$.

The link between factors of $f(t)$ and zero divisors in the eigenring $E(f)$ is well-known:

Proposition 2.16. *Let $f(t) \in R$.*

(i) ([23, Proposition 4]). If $f(t)$ is irreducible then $E(f)$ has no non-trivial zero divisors.

(ii) ([23, Proposition 4]). Suppose σ is an automorphism and $f(t)$ is bounded. Then $f(t)$ is irreducible if and only if $E(f)$ has no non-trivial zero divisors.

(iii) ([22, Theorem 3.3]). If $D = \mathbb{F}$ is a finite field and $\delta = 0$, all polynomials are bounded and hence $f(t)$ is irreducible if and only if $E(f)$ is a finite field.

In general, the statement $f(t)$ is irreducible if and only if $E(f)$ has no non-trivial zero divisors is not true. Examples of reducible skew polynomials whose eigenrings are division algebras are given in [23, Example 3] and [62]. We prove the following result, stated but not proved by Petit in [52, p. 13-07]:

Proposition 2.17. *If $f(t) \in R$ is irreducible then $E(f)$ is a division ring.*

Proof. Let $\mathrm{End}_R(R/Rf)$ denote the endomorphism ring of the left R-module R/Rf, that is $\mathrm{End}_R(R/Rf)$ consists of all maps $\phi : R/Rf \to R/Rf$ such that $\phi(rh + r'h') = r\phi(h) + r'\phi(h')$ for all $r, r' \in R$, $h, h' \in R/Rf$.

Now $f(t)$ irreducible implies R/Rf is a simple left R-module [23, p. 15], therefore $\mathrm{End}_R(R/Rf)$ is an associative division ring by Schur's Lemma [38, p. 33]. Finally $E(f)$ is isomorphic to the ring $\mathrm{End}_R(R/Rf)$ [23, p. 18-19] and thus $E(f)$ is also an associative division ring. $\square$

We now look at conditions for S_f to be a right division algebra.

Lemma 2.18. *If $f(t) \in R$ is reducible, then S_f contains zero divisors. In particular, S_f is neither a left nor right division algebra.*

Proof. Suppose $f(t) = g(t)h(t)$ for some $g(t), h(t) \in R$ with $\deg(g(t))$, $\deg(h(t)) < \deg(f(t))$, then $g(t) \circ h(t) = g(t)h(t) \bmod_r f = 0$. □

Notice S_f is a free left D-module of finite rank $m = \deg(f(t))$ and let $0 \neq a \in S_f$. Then $R_a(y+z) = (y+z) \circ a = (y \circ a) + (z \circ a) = R_a(y) + R_a(z)$ and

$$R_a(k \circ z) = (k \circ z) \circ a = k \circ (z \circ a) = k \circ R_a(z),$$

for all $k \in D$, $y, z \in S_f$, since either S_f is associative or has left nucleus equal to D by Theorem 2.1. Thus R_a is left D-linear. We will require the following well-known Rank-Nullity Theorem:

Theorem 2.19. *(See for example [30, Chapter IV, Corollary 2.14]). Let S be a free left (resp. right) D-module of finite rank m and $\phi : S \to S$ be a left (resp. right) D-linear map. Then*

$$\dim(\mathrm{Ker}(\phi)) + \dim(\mathrm{Im}(\phi)) = m,$$

in particular, ϕ is injective if and only if it is surjective.

Theorem 2.20. *([52, (6)]). Let $f(t) \in R$ have degree m and $0 \neq a \in S_f$. Then R_a is bijective is equivalent to 1 being a right greatest common divisor of $f(t)$ and a. In particular, $f(t)$ is irreducible if and only if S_f is a right division algebra.*

Proof. Let $0 \neq a \in S_f$. Since S_f is a free left D-module of finite rank m and R_a is left D-linear, the Rank-Nullity Theorem 2.19 implies R_a is bijective if and only if it is injective which is equivalent to $\mathrm{Ker}(R_a) = \{0\}$. Now $R_a(z) = z \circ a = 0$ is equivalent to $za \in Rf$, which means we can write

$$\mathrm{Ker}(R_a) = \{z \in R_m \mid za \in Rf\}.$$

Furthermore, R is a left principal ideal domain, which implies $za \in Rf$ if and only if $za \in Ra \cap Rf = Rg = Rha$, where $g = ha$ is the least common left multiple of a and f. Therefore $za \in Rf$ is equivalent to $z \in Rh$, and hence $\mathrm{Ker}(R_a) \neq \{0\}$, if and only if there exists a polynomial of degree strictly less than m in Rh, which is equivalent to $\deg(h) \leq m-1$.

Let $b \in R$ be a right greatest common divisor of a and f. Then

$$\deg(f) + \deg(a) = \deg(g) + \deg(b) = \deg(ha) + \deg(b),$$

by [32, Proposition 1.3.1], and so $\deg(b) = \deg(f) - \deg(h)$. Thus $\deg(h) \leq m-1$ if and only if $\deg(b) \geq 1$, so we conclude $\mathrm{Ker}(R_a) = \{0\}$ if and only if $\deg(b) = 0$, if and only if 1 is a right greatest common divisor of $f(t)$ and a. In particular, this implies S_f is a right division algebra if and only if R_a is bijective for all $0 \neq a \in S_f$, if and only if 1 is a right greatest common divisor of $f(t)$ and a for all $0 \neq a \in S_f$, if and only if $f(t)$ is irreducible. □

We wish to determine when S_f is also a left division algebra, hence when it is a division algebra.

Proposition 2.21. *If $f(t) \in R$ is right invariant, then $f(t)$ is irreducible if and only if S_f is a division algebra.*

Proof. Suppose $f(t)$ is right invariant so that S_f is associative by Theorem 2.1. If $f(t)$ is reducible then S_f is not a division algebra by Lemma 2.18. Conversely, if $f(t)$ is irreducible the maps R_b are bijective for all $0 \neq b \in S_f$ by Theorem 2.20. This implies the maps L_b are also bijective for all $0 \neq b \in S_f$ by [12, Lemma 1B], and so S_f is a division algebra. □

Lemma 2.22. *If $f(t)$ is irreducible then L_a is injective for all $0 \neq a \in S_f$.*

Proof. If $f(t)$ is irreducible then $L_a(z) = a \circ z = R_z(a) = 0$ is impossible for $0 \neq z \in S_f$, as R_z is injective by Theorem 2.20. Thus L_a is also injective. □

In general L_a is neither left nor right D-linear. Therefore, when $f(t)$ is irreducible we cannot apply the Rank-Nullity Theorem to conclude L_a is surjective, as we did for R_a in the proof of Theorem 2.20. In fact, the following Theorem shows that L_a may not be surjective even if $f(t)$ is irreducible:

Theorem 2.23. *Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in D[t;\sigma]$ where $a_0 \neq 0$. Then for every $j \in \{1, \ldots, m-1\}$, L_{t^j} is surjective if and only if σ is surjective. In particular, if σ is not surjective then S_f is not a left division algebra.*

Proof. We first prove the result for $j = 1$: Given $z = \sum_{i=0}^{m-1} z_i t^i \in S_f$, we have

$$\begin{aligned} L_t(z) = t \circ z &= \sum_{i=0}^{m-2} \sigma(z_i) t^{i+1} + \sigma(z_{m-1}) t \circ t^{m-1} \\ &= \sum_{i=1}^{m-1} \sigma(z_{i-1}) t^i + \sigma(z_{m-1}) \sum_{i=0}^{m-1} a_i t^i. \end{aligned} \tag{2.11}$$

($\Rightarrow$) Suppose L_t is surjective, then given any $b \in D$ there exists $z \in S_f$ such that $t \circ z = b$. The t^0-coefficient of $L_t(z)$ is $\sigma(z_{m-1})a_0$ by (2.11), and thus for all $b \in D$ there exists $z_{m-1} \in D$ such that $\sigma(z_{m-1})a_0 = b$. Therefore σ is surjective.

($\Leftarrow$) Suppose σ is surjective and let $g = \sum_{i=0}^{m-1} g_i t^i \in S_f$. Define

$$z_{m-1} = \sigma^{-1}(g_0 a_0^{-1}),\ z_{i-1} = \sigma^{-1}(g_i) - z_{m-1}\sigma^{-1}(a_i)$$

for all $i \in \{1, \ldots, m-1\}$. Then

$$L_t(z) = \sigma(z_{m-1})a_0 + \sum_{i=1}^{m-1} \big(\sigma(z_{i-1}) + \sigma(z_{m-1}a_i)\big) t^i = \sum_{i=0}^{m-1} g_i t^i = g,$$

by (2.11), which implies L_t is surjective.

Hence L_t surjective is equivalent to σ surjective. To prove the result for all $j \in \{1, \ldots, m-1\}$ we show that

$$L_{t^j} = L_t^j, \tag{2.12}$$

for all $j \in \{1, \ldots, m-1\}$, then it follows σ is surjective if and only if L_t is surjective if and only if $L_t^j = L_{t^j}$ is surjective. In the special case when $D = \mathbb{F}_q$ is a finite field, σ is an automorphism and $f(t)$ is monic and irreducible, the equality (2.12) is proven in [44, p. 12]. A similar proof also works more generally in our context: suppose inductively that $L_{t^j} = L_t^j$ for some $j \in$

$\{1, \ldots, m-2\}$. Then $L_t^j(b) = t^j b \bmod_r f$ for all $b \in R_m$. Let $L_t^j(b) = b'$ so that $t^j b = qf + b'$ for some $q \in R$. We have

$$\begin{aligned} L_t^{j+1}(b) &= L_t(L_t^j(b)) = L_t(b') = L_t(t^j b - qf) = t \circ (t^j b - qf) \\ &= (t^{j+1} b - tqf) \bmod_r f = t^{j+1} b \bmod_r f = L_{t^{j+1}}(b), \end{aligned}$$

hence (2.12) follows by induction. □

We can use Theorems 2.20 and 2.23 to find examples of Petit algebras which are right but not left division algebras:

Corollary 2.24. *Suppose σ is not surjective and $f(t) \in D[t;\sigma]$ is irreducible. Then S_f is a right division algebra but not a left division algebra.*

Example 2.25. *Let K be a field, y be an indeterminate and define $\sigma : K(y) \to K(y)$ by $\sigma|_K = \mathrm{id}$ and $\sigma(y) = y^2$. Then σ is an injective but not surjective endomorphism of $K(y)$ [7, p. 123]. For $a(y) \in K[y]$ denote by $\deg_y(a(y))$ the degree of $a(y)$ as a polynomial in y.*

Let $f(t) = t^2 - a(y) \in K(y)[t;\sigma]$ where $0 \neq a(y) \in K[y]$ is such that $3 \nmid \deg_y(a(y))$. We will show later in Corollary 3.7 that $f(t)$ is irreducible in $K(y)[t;\sigma]$, hence S_f is a right, but not a left division algebra by Corollary 2.24.

The following result was stated but not proved by Petit [52, (7)]:

Theorem 2.26. *([52, (7)]). Let $f(t) \in D[t;\sigma,\delta]$ be such that S_f is a finite-dimensional F-vector space or a right $\mathrm{Nuc}_r(S_f)$-module, which is free of finite rank. Then S_f is a division algebra if and only if $f(t)$ is irreducible.*

Proof. When S_f is associative the assertion follows by Proposition 2.21 so suppose S_f is not associative. If $f(t)$ is reducible, S_f is not a division algebra by Lemma 2.18. Conversely, suppose $f(t)$ is irreducible so that S_f is a right division algebra by Theorem 2.20. Let $0 \neq a \in S_f$ be arbitrary, then L_a is injective for all $0 \neq a \in S_f$ by Lemma 2.22. We prove L_a is surjective, hence S_f is also a left division algebra:

(i) Suppose S_f is a finite-dimensional F-vector space. Then since $F \subseteq \mathrm{Nuc}(S_f)$, we have

$$L_a(k \circ z) = a \circ (k \circ z) = (a \circ k) \circ z = (k \circ a) \circ z = k \circ (a \circ z) = k \circ L_a(z)$$

and

$$L_a(z \circ k) = a \circ (z \circ k) = (a \circ z) \circ k = L_a(z) \circ k,$$

for all $k \in F$, $z \in S_f$. Therefore L_a is F-linear, and thus L_a is surjective by the Rank-Nullity Theorem 2.19.

(ii) Suppose S_f is a free right $\mathrm{Nuc}_r(S_f)$-module of finite rank, then $E(f)$ is a division ring by Proposition 2.17. Furthermore, we have

$$L_a(z \circ k) = a \circ (z \circ k) = (a \circ z) \circ k = L_a(z) \circ k$$

for all $k \in \mathrm{Nuc}_r(S_f)$, $z \in S_f$ and so L_a is right $\mathrm{Nuc}_r(S_f)$-linear. Therefore L_a is surjective by the Rank-Nullity Theorem 2.19.

□

Theorem 2.27. *Let σ be an automorphism of D, L be a division subring of D such that D is a free right L-module of finite rank, and $f(t) \in D[t;\sigma,\delta]$ be L-weak semi-invariant. Then S_f is a division algebra if and only if $f(t)$ is irreducible. In particular if σ is an automorphism of D and $f(t)$ is right semi-invariant then S_f is a division algebra if and only if $f(t)$ is irreducible.*

Proof. If $f(t)$ is reducible then S_f is not a division algebra by Lemma 2.18. Conversely, suppose $f(t)$ is irreducible. Then S_f is a right division algebra by Theorem 2.20 so we are left to show S_f is also a left division algebra. Let $0 \neq a \in S_f$ be arbitrary and recall L_a is injective by Lemma 2.22. Since $f(t)$ is L-weak semi-invariant, $L \subseteq \mathrm{Nuc}_r(S_f)$ which implies

$$L_a(z \circ \lambda) = a \circ (z \circ \lambda) = (a \circ z) \circ \lambda = L_a(z) \circ \lambda,$$

for all $z \in S_f$, $\lambda \in L$. Hence L_a is right L-linear.

S_f is a free right D-module of rank $m = \deg(f)$ because σ is an automorphism. Since D is a free right L-module of finite rank then also S_f is a free right L-module of finite rank. Thus the Rank-Nullity Theorem 2.19 implies L_a is bijective as required. $\square$

2.4 SEMI-MULTIPLICATIVE MAPS

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

$$M(v_1, \ldots, v_m) = \sum_{1 \leq i_1 < \cdots < i_l \leq m} (-1)^{m-l} M(v_{i_1} + \ldots + v_{i_l}),$$

$(1 \leq l \leq m)$ is m-linear over F. A map $M : V \to F$ of degree m is called a ***form of degree*** *m over F.*

Definition. *Consider a finite-dimensional nonassociative algebra A over a field F containing a subalgebra D. A map $M : A \to D$ of degree m is called* ***left semi-multiplicative*** *if $M(dg) = M(d)M(g)$, for all $d \in D$, $g \in A$.* ***Right semi-multiplicative*** *maps are defined similarly.*

As before let D be a division ring with center C, σ be an endomorphism of D, δ be a left σ-derivation of D, and $f(t) \in D[t;\sigma,\delta]$ be of degree m. In his Ph.D. thesis [64, §4.2], Steele defined and studied a left semi-multiplicative map on nonassociative cyclic algebras. In this Section, we show that when D is commutative and S_f is finite-dimensional over $F = C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$, then we can similarly define a left semi-multiplicative map M_f for S_f.

In the classical theory of associative central simple algebras of degree n, the reduced norm is a multiplicative form of degree n. The maps M_f can be seen as a generalisation of the reduced norm.

Consider S_f as a free left D-module of rank $m = \deg(f(t))$ with basis $\{1, t, \ldots, t^{m-1}\}$, and recall the right multiplication $R_g : S_f \to S_f$, $h \mapsto h \circ g$ is left D-linear for all $0 \neq g \in S_f$ by the argument on page 22. Define

$$\lambda : S_f \to \mathrm{End}_D(S_f),\ g \mapsto R_g,$$

which induces a map

$$\lambda : S_f \to \mathrm{Mat}_m(D),\ g \mapsto W_g,$$

where $W_g \in \mathrm{Mat}_m(D)$ is the matrix representing R_g with respect to the basis $\{1, t, \ldots, t^{m-1}\}$. If we represent $h = h_0 + h_1 t + \ldots + h_{m-1}t^{m-1} \in S_f$ as the row vector $(h_0, h_1, \ldots, h_{m-1})$ with entries in D, then we can write the product of two elements in S_f as $h \circ g = hW_g$.

When D is commutative, define $M_f : S_f \to D$ by $M_f(g) = \det(W_g)$. Notice this definition does not make sense unless D is commutative, otherwise W_g is a matrix with entries in the noncommutative ring D, and as such we cannot take its determinant.

Proposition 2.28. *Suppose $f(t)$ is right invariant, i.e. S_f is associative, then $W_g W_h = W_{g \circ h}$ for all $g, h \in S_f$. In particular, if D is commutative then M_f is multiplicative.*

Proof. We have

$$yW_{g\circ h} = y \circ (g \circ h) = (y \circ g) \circ h = (yW_g)W_h = y(W_g W_h)$$

for all $y, g, h \in S_f$, where we have used the associativity in S_f and the associativity of matrix multiplication. This means $W_g W_h = W_{g\circ h}$ for all $g, h \in S_f$. If D is commutative, then

$$M_f(g \circ h) = \det(W_{g\circ h}) = \det(W_g W_h) = \det(W_g)\det(W_h) = M_f(g)M_f(h)$$

for all $g, h \in S_f$, therefore M_f is multiplicative. □

In general, $W_{g\circ h} \neq W_g W_h$ for $g, h \in S_f$ unless S_f is associative since the map $g \mapsto W_g$ is not an F-algebra homomorphism. Nevertheless we obtain:

Proposition 2.29. *$W_d W_g = W_{d\circ g}$ for all $d \in D$, $g \in S_f$. In particular, if D is commutative and S_f is finite-dimensional over F, then M_f is left semi-multiplicative.*

Proof. Consider $d \in D$ as an element of S_f so that $d = d + 0t + \ldots + 0t^{m-1}$. When S_f is associative the assertion follows by Proposition 2.28, otherwise $D = \mathrm{Nuc}_m(S_f)$ by Theorem 2.1 and so

$$yW_{d\circ g} = y \circ (d \circ g) = (y \circ d) \circ g = (yW_d)W_g = y(W_d W_g)$$

for all $d \in D$, $y, g \in S_f$. Thus $W_d W_g = W_{d \circ g}$.

If D is commutative and S_f is finite-dimensional over F, then

$$M_f(d \circ g) = \det(W_{d \circ g}) = \det(W_d W_g) = \det(W_d)\det(W_g) = M_f(d) M_f(g)$$

for all $d \in D$, $g \in S_f$ and so M_f is left semi-multiplicative. □

Examples 2.30. *(i) Let $f(t) = t^2 - a_1 t - a_0 \in D[t;\sigma,\delta]$. Given $g = g_0 + g_1 t \in S_f$ with $g_0, g_1 \in D$, the matrix W_g has the form*

$$\begin{pmatrix} g_0 & g_1 \\ \sigma(g_1)a_0 + \delta(g_0) & \sigma(g_0) + \sigma(g_1)a_1 + \delta(g_1) \end{pmatrix}.$$

(ii) Let $f(t) = t^m - a \in D[t;\sigma]$, then given $g = g_0 + g_1 t + \ldots + g_{m-1}t^{m-1} \in S_f$, $g_i \in D$, the matrix W_g has the form

$$W_g = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{m-1} \\ \sigma(g_{m-1})a & \sigma(g_0) & \sigma(g_1) & \cdots & \sigma(g_{m-2}) \\ \sigma^2(g_{m-2})a & \sigma^2(g_{m-1})\sigma(a) & \sigma^2(g_0) & \cdots & \sigma^2(g_{m-3}) \\ \sigma^3(g_{m-3})a & \sigma^3(g_{m-2})\sigma(a) & \sigma^3(g_{m-1})\sigma^2(a) & \cdots & \sigma^3(g_{m-4}) \\ \vdots & \vdots & \vdots & & \vdots \\ \sigma^{m-1}(g_1)a & \sigma^{m-1}(g_2)\sigma(a) & \sigma^{m-1}(g_3)\sigma^2(a) & \cdots & \sigma^{m-1}(g_0) \end{pmatrix}.$$

In other words, $W_g = (W_{ij})_{i,j=0,\ldots,m-1}$, where

$$W_{ij} = \begin{cases} \sigma^i(g_{j-i}) & \text{if } i \leq j, \\ \sigma^i(g_{m-i+j})\sigma^j(a) & \text{if } i > j. \end{cases}$$

If D is a finite field, the matrix W_g is the (σ, a)-circulant matrix M_a^σ in [21]. In this case, Proposition 2.29 is [21, Remark 3.2(b)].

We now look at the connection between M_f and zero divisors in S_f:

Theorem 2.31. *Suppose D is commutative.*

(i) Let $0 \neq g \in S_f$. If g is not a right zero divisor in S_f then $M_f(g) \neq 0$.

(ii) S_f has no non-trivial zero divisors if and only if $M_f(g) \neq 0$ for all $0 \neq g \in S_f$, if and only if S_f is a right division algebra.

(iii) *If S_f is a finite-dimensional left F-vector space or a free of finite rank right* $\mathrm{Nuc}_r(S_f)$*-module, then S_f is a division algebra is equivalent to $M_f(g) \neq 0$ for all $0 \neq g \in S_f$.*

Proof. (i) If W_g is a singular matrix, then the equation

$$h \circ g = (h_0, \dots, h_{m-1})W_g = 0,$$

has a non-trivial solution $(h_0, \dots, h_{m-1}) \in D^m$, contradicting the assumption that g is not a right zero divisor in S_f.

(ii) Suppose $M_f(g) \neq 0$ for all $0 \neq g \in S_f$. If $g, h \in S_f$ are non-zero and $h \circ g = hW_g = 0$ then $h = 0W_g^{-1} = 0$, a contradiction. Hence S_f has no non-trivial zero divisors. Conversely, if S_f has no non-trivial zero divisors then $M_f(g) \neq 0$ for all $0 \neq g \in S_f$ by (i).

Additionally, S_f contains no non-trivial zero divisors if and only if the right multiplication map $R_g : S_f \to S_f,\ x \mapsto x \circ g$ is injective for all non-zero $g \in S_f$, if and only if S_f is a right division algebra by the proof of Theorem 2.20.

(iii) Follows from (ii) and Theorem 2.26.

□

3

IRREDUCIBILITY CRITERIA IN SKEW POLYNOMIAL RINGS

Let D be a division ring with center C, σ be an endomorphism of D and δ be a left σ-derivation. Throughout this Chapter we assume without loss of generality $f(t) \in R = D[t;\sigma,\delta]$ is monic.

In Section 2.3, we saw that whether S_f is a division algebra or not is closely linked to whether the polynomial $f(t)$ used in its construction is irreducible. For instance, S_f is a right division algebra if and only if $f(t)$ is irreducible by Theorem 2.20. This motivates the study of factorisation and irreducibility of skew polynomials which we do in the present Chapter. The results we obtain, in conjunction with Theorems 2.20 and 2.26, yield criteria for some Petit algebras to be (right) division algebras.

It is well-known that a skew polynomial can always be factored as a product of irreducible skew polynomials. This factorisation is in general not unique, however, the degrees of the factors are unique up to permutation:

Theorem 3.1. *([51, Theorem 1]). Every non-zero polynomial $f(t) \in R$ factorises as $f(t) = f_1(t) \cdots f_n(t)$ where $f_i(t) \in R$ is irreducible for all $i \in \{1, \ldots, n\}$. Furthermore, if $f(t) = g_1(t) \cdots g_s(t)$ is any other factorisation of $f(t)$ as a product of irreducible $g_i \in R$, then $s = n$ and there exists a permutation $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that f_i is similar to $g_{\pi(i)}$. In particular, f_i and $g_{\pi(i)}$ have the same degree for all $i \in \{1, \ldots, n\}$.*

We first restrict our attention to the case where $\delta = 0$.

3.1 IRREDUCIBILITY CRITERIA IN $R = D[t;\sigma]$

Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R = D[t;\sigma]$. In order to study when $f(t)$ is irreducible, we first determine the remainder after dividing $f(t)$ on the right by $(t-b)$, $b \in D$. By [32, p. 15] we have the identity

$$\begin{aligned} &t^i - \sigma^{i-1}(b)\sigma^{i-2}(b)\cdots b \\ &\quad = \Big(t^{i-1} + \sigma^{i-1}(b)t^{i-2} + \ldots + \sigma^{i-1}(b)\cdots\sigma(b)\Big)(t-b), \end{aligned} \tag{3.1}$$

for all $i \in \mathbb{N}$. Multiplying (3.1) on the left by a_i and summing over i yields

$$f(t) = q(t)(t-b) + N_m(b) - \sum_{i=0}^{m-1} a_i N_i(b),$$

for some $q(t) \in R$, where $N_i(b) = \sigma^{i-1}(b)\cdots\sigma(b)b$ for $i > 0$ and $N_0(b) = 1$. Therefore the remainder after dividing $f(t)$ on the right by $(t-b)$ is $N_m(b) - \sum_{i=0}^{m-1} a_i N_i(b)$, and we conclude:

Proposition 3.2. *([32, p. 16]).* $(t-b)|_r f(t)$ *is equivalent to*

$$a_m N_m(b) - \sum_{i=0}^{m-1} a_i N_i(b) = 0.$$

When σ is an automorphism of D, we can also determine the remainder after dividing $f(t)$ on the left by $(t-b)$, $b \in D$: Similarly to (3.1) we have the identity

$$\begin{aligned} t^i - b\sigma^{-1}(b)\cdots\sigma^{1-i}(b) &= (t-b)\Big(t^{i-1} + \sigma^{-1}(b)t^{i-2} \\ &\quad + \sigma^{-1}(b)\sigma^{-2}(b)t^{i-3} + \ldots + \sigma^{-1}(b)\sigma^{-2}(b)\cdots\sigma^{1-i}(b)\Big) \end{aligned} \tag{3.2}$$

for all $i \in \mathbb{N}$. Multiplying (3.2) on the right by $\sigma^{-i}(a_i)$, and using $a_i t^i = t^i \sigma^{-i}(a_i)$ gives

$$\begin{aligned} &a_i t^i - b\sigma^{-1}(b)\cdots\sigma^{1-i}(b)\sigma^{-i}(a_i) \\ &= (t-b)\Big(t^{i-1} + \sigma^{-1}(b)t^{i-2} + \ldots + \sigma^{-1}(b)\sigma^{-2}(b)\cdots\sigma^{1-i}(b)\Big)\sigma^{-i}(a_i). \end{aligned}$$

Summing over i, we obtain

$$f(t) = (t-b)q(t) + M_m(b) - \sum_{i=0}^{m-1} M_i(b)\sigma^{-i}(a_i),$$

for some $q(t) \in R$ where $M_i(b)$ are defined by $M_0(b) = 1$, $M_1(b) = b$ and $M_i(b) = b\sigma^{-1}(b) \cdots \sigma^{1-i}(b)$ for $i \geq 2$. We immediately conclude:

Proposition 3.3. *Suppose σ is an automorphism of D. Then $(t-b)|_l f(t)$ if and only if $M_m(b) - \sum_{i=0}^{m-1} M_i(b)\sigma^{-i}(a_i) = 0$.*

A careful reading of Propositions 3.2 and 3.3 yields the following:

Corollary 3.4. *Suppose σ is an automorphism and $f(t) = t^m - a \in D[t;\sigma]$. Then $f(t)$ has a left linear divisor if and only if it has a right linear divisor.*

Proof. Let $b \in D$, then $(t-b)|_r f(t)$ is equivalent to $\sigma^{m-1}(b) \cdots \sigma(b)b = a$ by Proposition 3.2, if and only if $c\sigma^{-1}(c) \cdots \sigma^{1-m}(c) = a$ where $c = \sigma^{m-1}(b)$, if and only if $(t-c)|_l f(t)$ by Proposition 3.3. □

Using Propositions 3.2 and 3.3 we obtain criteria for some skew polynomials of degree two or three to be irreducible. The following was stated but not proven by Petit in [52, (17), (18)]:

Theorem 3.5. *(i) Suppose σ is an endomorphism of D. Then $f(t) = t^2 - a_1 t - a_0 \in D[t;\sigma]$ is irreducible if and only if*

$$\sigma(b)b - a_1 b - a_0 \neq 0,$$

for all $b \in D$.

(ii) Suppose σ is an automorphism. Then $f(t) = t^3 - a_2 t^2 - a_1 t - a_0 \in D[t;\sigma]$ is irreducible if and only if

$$\sigma^2(b)\sigma(b)b - \sigma^2(b)\sigma(b)a_2 - \sigma^2(b)\sigma(a_1) - \sigma^2(a_0) \neq 0,$$

and

$$\sigma^2(b)\sigma(b)b - a_2\sigma(b)b - a_1 b - a_0 \neq 0,$$

for all $b \in D$.

Proof. (i) Since $\deg(f(t)) = 2$, we have $f(t)$ is irreducible if and only if $(t-b) \nmid_r f(t)$ for all $b \in D$, if and only if

$$N_2(b) - a_1 N_1(b) - a_0 N_0(b) = \sigma(b)b - a_1 b - a_0 \neq 0,$$

for all $b \in D$ by Proposition 3.2.

(ii) Here $\deg(f(t)) = 3$ and so $f(t)$ is irreducible if and only if $(t-b) \nmid_r f(t)$ and $(t-b) \nmid_l f(t)$ for all $b \in D$, if and only if

$$\sigma^2(b)\sigma(b)b - a_2\sigma(b)b - a_1 b - a_0 \neq 0,$$

and

$$b\sigma^{-1}(b)\sigma^{-2}(b) - b\sigma^{-1}(b)\sigma^{-2}(a_2) - b\sigma^{-1}(a_1) - a_0 \neq 0, \qquad (3.3)$$

for all $b \in D$ by Propositions 3.2 and 3.3. Applying σ^2 to (3.3) we obtain the assertion.

□

When $f(t)$ has the form $f(t) = t^3 - a \in D[t;\sigma]$, we obtain the following simplification of Theorem 3.5(ii):

Corollary 3.6. *Suppose σ is an automorphism of D, then $f(t) = t^3 - a \in D[t;\sigma]$ is irreducible is equivalent to $\sigma^2(b)\sigma(b)b \neq a$ for all $b \in D$.*

Proof. Recall $f(t)$ has a right linear divisor if and only if it has a left linear divisor by Corollary 3.4. Therefore $f(t)$ is irreducible if and only if $(t-b) \nmid_r f(t)$ for all $b \in D$, if and only if $\sigma^2(b)\sigma(b)b \neq a$ for all $b \in D$ by Proposition 3.2. □

Corollary 3.7. *Let K be a field, y be an indeterminate and define $\sigma : K(y) \to K(y)$ by $\sigma|_K = \mathrm{id}$ and $\sigma(y) = y^2$. For $a(y) \in K[y]$ denote by $\deg_y(a(y))$ the degree of $a(y)$ as a polynomial in y. Let $f(t) = t^2 - a(y) \in K(y)[t;\sigma]$ where $0 \neq a(y) \in K[y]$ is such that $3 \nmid \deg_y(a(y))$. Then $f(t)$ is irreducible in $K(y)[t;\sigma]$.*

Proof. Note that σ is an injective but not surjective endomorphism of $K(y)$ by [7, p. 123]. We have $f(t)$ is irreducible is equivalent to $\sigma(b(y))b(y) \neq a(y)$ for all $b(y) \in K(y)$ by Theorem 3.5. Given $0 \neq b(y) \in K(y)$, write $b(y) = c(y)/d(y)$ for some non zero $c(y), d(y) \in K[y]$.

If $\sigma(b(y))b(y) \notin K[y]$ then $\sigma(b(y))b(y) \neq a(y)$ because $a(y) \in K[y]$. Conversely suppose $\sigma(b(y))b(y) \in K[y]$ and let $c(y) = \sum_{i=0}^{l} \lambda_i y^i$, $d(y) =$

$\sum_{j=0}^{n} \mu_j y^j$ for some $\lambda_i, \mu_j \in K$ with $\lambda_l, \mu_n \neq 0$. Then $\sigma(c(y)) = \sum_{i=0}^{l} \lambda_i y^{2i}$, $\sigma(d(y)) = \sum_{j=0}^{n} \mu_j y^{2j}$, and so

$$\sigma(b(y))b(y) = \frac{\sigma(c(y))c(y)}{\sigma(d(y))d(y)} = \frac{\sum_{i=0}^{l} \lambda_i y^{2i} \sum_{k=0}^{l} \lambda_k y^k}{\sum_{j=0}^{n} \mu_j y^{2j} \sum_{s=0}^{n} \mu_s y^s} = \frac{\sum_{i=0}^{l} \sum_{k=0}^{l} \lambda_i \lambda_k y^{2i+k}}{\sum_{j=0}^{n} \sum_{s=0}^{n} \mu_j \mu_s y^{2j+s}}.$$

This means $\deg_y\big(\sigma(b(y))b(y)\big) = 3l - 3n$ is a multiple of 3, thus if $3 \nmid \deg_y(a(y))$ then $\sigma(b(y))b(y) \neq a(y)$ and $f(t)$ is irreducible. $\square$

Consider the field extension $\mathbb{C}/\mathbb{R}$ where $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\}$ and σ denotes complex conjugation. By [54, Corollary 6], any non-constant $g(t) \in \mathbb{C}[t;\sigma]$ decomposes into a product of linear and irreducible quadratic skew polynomials, in particular, every polynomial of degree ≥ 3 is reducible. As a Corollary of Theorem 3.5(i) we now give some irreducibility criteria for $f(t) \in \mathbb{C}[t;\sigma]$ of degree 2:

Corollary 3.8. *(i) Let $f(t) = t^2 - a \in \mathbb{C}[t;\sigma]$, then $f(t)$ is irreducible if and only if $a \in \mathbb{C} \setminus \mathbb{R}$ or $a \in \mathbb{R}^- = \{r \in \mathbb{R} \mid r < 0\}$.*

(ii) [5, Corollary 2.6] Let $f(t) = t^2 - a_1 t - a_0 \in \mathbb{C}[t;\sigma]$ with $a_0, a_1 \in \mathbb{R}$, then $f(t)$ is irreducible in $\mathbb{C}[t;\sigma]$ if and only if $a_1^2 + 4a_0 < 0$ if and only if $f(t)$ is irreducible in $\mathbb{R}[t]$. Moreover, if $f(t)$ is reducible, then the factorisation of $f(t)$ into monic linear polynomials is unique when $a_1 \neq 0$, whereas $f(t)$ factors an infinite number of ways into monic linear factors when $a_1 = 0$.

(iii) Let $f(t) = t^2 - a_1 t - a_0 \in \mathbb{C}[t;\sigma]$ where $a_0 \in \mathbb{R}$ and $a_1 = \lambda + \mu i$ for some $\lambda, \mu \in \mathbb{R}^\times$. Then $f(t)$ is irreducible if and only if $a_0 < -(\lambda^2 + \mu^2)/4$. In particular, if $a_0 \geq 0$ then $f(t)$ is reducible.

Proof. (i) We have $f(t)$ is reducible is equivalent to $\sigma(b)b = a$ for some $b = c + di \in \mathbb{C}$ by Theorem 3.5, which is equivalent to $c^2 + d^2 = a$ for some $c, d \in \mathbb{R}$. Therefore if $0 > a \in \mathbb{R}$ or $a \in \mathbb{C} \setminus \mathbb{R}$, then $f(t)$ must be irreducible. On the other hand, if $0 < a \in \mathbb{R}$ then setting $b = \sqrt{a}$ gives $\sigma(b)b = b^2 = a$ as required.

(iii) We have $f(t)$ is reducible if and only if $\sigma(b)b - a_1 b - a_0 = 0$ for some $b = c + di \in \mathbb{C}$ by Theorem 3.5, if and only if

$$c^2 + d^2 - \lambda c + \mu d - a_0 - (\lambda d + \mu c)i = 0,$$

if and only if $c^2 + d^2 - \lambda c + \mu d - a_0 = 0$ and $\lambda d + \mu c = 0$ for some $c, d \in \mathbb{R}$. Therefore $f(t)$ is reducible if and only if

$$\Big(1 + \frac{\mu^2}{\lambda^2}\Big)c^2 + \Big(-\lambda - \frac{\mu^2}{\lambda}\Big)c - a_0 = 0,$$

for some $c \in \mathbb{R}$, if and only if

$$\Big(-\lambda - \frac{\mu^2}{\lambda}\Big)^2 + 4a_0\Big(1 + \frac{\mu^2}{\lambda^2}\Big) \geq 0,$$

if and only if $a_0 \geq -(\lambda^2 + \mu^2)/4$.

□

Lemma 3.9. *Let $f(t) \in R = D[t;\sigma]$ and suppose $f(t) = q(t)g(t)$ for some $q(t), g(t) \in R$. Then $f(bt) = q(bt)g(bt)$ for all $b \in F = C \cap \mathrm{Fix}(\sigma)$.*

Proof. Write $q(t) = \sum_{i=0}^{l} q_i t^i,\ g(t) = \sum_{j=0}^{n} g_j t^j$, then

$$f(t) = q(t)g(t) = \sum_{i=0}^{l}\sum_{j=0}^{n} q_i t^i g_j t^j = \sum_{i=0}^{l}\sum_{j=0}^{n} q_i \sigma^i(g_j) t^{i+j},$$

and so

$$\begin{aligned} q(bt)g(bt) &= \sum_{i=0}^{l} q_i (bt)^i \sum_{j=0}^{n} g_j (bt)^j = \sum_{i=0}^{l}\sum_{j=0}^{n} q_i \sigma^i(g_j) b^{i+j} t^{i+j} \\ &= \sum_{i=0}^{l}\sum_{j=0}^{n} q_i \sigma^i(g_j)(bt)^{i+j} = f(bt), \end{aligned}$$

for all $b \in F$. □

The following result was stated as Exercise by Bourbaki in [9, p. 344] and proven in the special case where σ is an automorphism of order m in [16, Proposition 3.7.5]:

Theorem 3.10. *Let σ be an endomorphism of D, $f(t) = t^m - a \in R = D[t;\sigma]$ and suppose $F = C \cap \mathrm{Fix}(\sigma)$ contains a primitive m^{th} root of unity. If $g(t) \in R$ is a monic irreducible polynomial dividing $f(t)$ on the right, then the degree d of $g(t)$ divides m and $f(t)$ is the product of m/d polynomials of degree d.*

Proof. Let $g(t) \in R$ be a monic irreducible polynomial of degree d dividing $f(t)$ on the right, and $\omega \in F$ be a primitive m^{th} root of unity.

Define $g_i(t) = g(\omega^i t)$ for all $i \in \{0, \ldots, m-1\}$. Then $\bigcap_{i=0}^{m-1} Rg_i(t)$ is an ideal of R, and since R is a left principle ideal domain, we have

$$Rh(t) = \bigcap_{i=0}^{m-1} Rg_i(t), \tag{3.4}$$

for a suitably chosen $h(t) \in R$. Furthermore, we may assume $h(t)$ is monic, otherwise if $h(t)$ has leading coefficient $d \in D^\times$, then $Rh(t) = R(d^{-1}h(t))$.

We show $f(t) \in Rh(t)$: As $g(t)$ right divides $f(t)$, we can write $f(t) = q(t)g(t)$ for some $q(t) \in R$. In addition, we have $(\omega t)^i = \omega^i t^i$ for all $i \in \{0, \ldots, m-1\}$ because $\omega \in F$, therefore

$$f(\omega^i t) = \omega^{mi} t^m - a = t^m - a = f(t) = q(\omega^i t) g(\omega^i t),$$

by Lemma 3.9 and so $g_i(t)$ right divides $f(t)$ for all $i \in \{0, \ldots, m-1\}$. This means

$$f(t) \in \bigcap_{i=0}^{m-1} Rg_i(t) = Rh(t),$$

in particular, $Rh(t)$ is not the zero ideal.

We next show $h(\omega^i t) = h(t)$ for all $i \in \{0, \ldots, m-1\}$: For simplicity we only do this for $i = 1$, the other cases are similar. Notice $h(t) \in \bigcap_{j=0}^{m-1} Rg_j(t)$ by (3.4) and thus there exists $q_0(t), \ldots, q_{m-1}(t) \in R$ such that $h(t) = q_j(t) g_j(t)$, for all $j \in \{0, \ldots, m-1\}$. Therefore

$$h(\omega t) = q_{m-1}(\omega t) g_{m-1}(\omega t) = q_{m-1}(\omega t) g_0(t),$$

and

$$h(\omega t) = q_j(\omega t) g_j(\omega t) = q_j(\omega t) g_{j+1}(t) \in Rg_{j+1}(t),$$

for all $j \in \{0, \ldots, m-2\}$ by Lemma 3.9, which implies

$$h(\omega t) \in \bigcap_{j=0}^{m-1} Rg_j(t) = Rh(t).$$

As a result $h(\omega t) = k(t)h(t)$ for some $k(t) \in R$, and by comparing degrees, we conclude $0 \neq k(t) = k \in D$. Suppose $h(t)$ has degree l and write

$$h(t) = a_0 + \ldots + a_{l-1}t^{l-1} + t^l, \ a_j \in D,$$

here $Rg(t) \supseteq Rh(t)$ and $f(t) \in Rh(t)$ which yields $\deg(g(t)) = d \leq l \leq m$. Since $h(\omega t) = kh(t)$, we have $kt^l = (\omega t)^l = \left(\prod_{j=0}^{l-1} \sigma^j(\omega)\right)t^l = \omega^l t^l$ which implies $k = \omega^l$. Clearly, the coefficients a_j must be zero for all $j \in \{1, \ldots, l-1\}$, otherwise $a_j(\omega t)^j = ka_j t^j = \omega^l a_j t^j$ giving $\omega^j = \omega^l$, a contradiction as ω is a primitive m^{th} root of unity. This means $h(t) = t^l + a_0$, and with

$$\omega^l t^l + a_0 = h(\omega t) = kh(t) = \omega^l(t^l + a_0) = \omega^l t^l + \omega^l a_0,$$

we obtain $\omega^l = 1$. This implies $l = m$ and $k = \omega^m = 1$, hence $h(\omega t) = h(t)$.

We next prove $h(t) = f(t)$: Now $f(t) \in Rh(t)$ implies $f(t) = t^m - a = p(t)(t^m + a_0)$ for some $p \in R$. Comparing degrees we see $p \in D^\times$, thus $t^m - a = p(t^m + a_0) = pt^m + pa_0$ which yields $p = 1$, $a_0 = -a$ and $f(t) = h(t)$.

Finally, $\bigcap_{i=0}^{m-1} Rg_i(t) = Rf(t)$ is equivalent to $f(t)$ being the least common left multiple of the $g_i(t)$, $i \in \{0, \ldots, m-1\}$ [32, p. 10]. As a result, we can write

$$f(t) = q_{i_r}(t)q_{i_{r-1}}(t) \cdots q_{i_1}(t),$$

by [51, p. 496], where $i_1 = 0 < i_2 < \ldots < i_r \leq m-1$ and each $q_{i_s}(t) \in R$ is similar to $g_{i_s}(t)$. Similar polynomials have the same degree [32, p. 14] so $r = m/d$, and $f(t)$ factorises into m/d irreducible polynomials of degree d. $\square$

Theorem 3.10 implies the following result, which improves [52, (19)] by making $\sigma^{m-1}(a) \neq \sigma^{m-1}(b) \cdots \sigma(b)b$ for all $b \in D$ a superfluous condition:

Theorem 3.11. *Suppose m is prime, σ is an endomorphism of D and F contains a primitive m^{th} root of unity. Then $f(t) = t^m - a \in D[t;\sigma]$ is irreducible if and only if it has no right linear divisors, if and only if*

$$a \neq \sigma^{m-1}(b) \cdots \sigma(b)b$$

for all $b \in D$.

Proof. Let $g(t) \in D[t;\sigma]$ be an irreducible polynomial of degree d dividing $f(t)$ on the right. Without loss of generality $g(t)$ is monic, otherwise if $g(t)$ has leading coefficient $c \in D^\times$, then $c^{-1}g(t)$ is monic and also right divides $f(t)$. Thus d divides m by Theorem 3.10 and since m is prime, either $d = m$, in which case $g(t) = f(t)$, or $d = 1$, which means $f(t)$ can be written as a product of m linear factors. Therefore $f(t)$ is irreducible if and only if $(t-b) \nmid_r f(t)$ for all $b \in D$, if and only if $a \neq \sigma^{m-1}(b) \cdots \sigma(b)b$, for all $b \in D$ by Proposition 3.2. $\square$

Lemma 3.12. *Let K be a field, y be an indeterminate, and σ be the automorphism of $K(y)$ such that $\sigma|_K = \mathrm{id}$ and $\sigma(y) = qy$ for some $1 \neq q \in K^\times$. Let $b(y) \in K(y)$ and write $b(y) = c(y)/d(y)$ for some $c(y), d(y) \in K[y]$ with $d(y) \neq 0$. Then $\sigma^j(b(y)) = c(q^j y)/d(q^j y)$ for all $j \in \mathbb{N}$.*

Proof. Write $c(y) = \lambda_0 + \lambda_1 y + \ldots + \lambda_l y^l$ and $d(y) = \mu_0 + \mu_1 y + \ldots + \mu_n y^n$ for some $\lambda_i, \mu_j \in K$, then

$$\begin{aligned}\sigma^j(b(y)) &= \frac{\sigma^j(c(y))}{\sigma^j(d(y))} = \frac{\sigma^j(\lambda_0) + \sigma^j(\lambda_1 y) + \ldots + \sigma^j(\lambda_l y^l)}{\sigma^j(\mu_0) + \sigma^j(\mu_1 y) + \ldots + \sigma^j(\mu_n y^n)} \\ &= \frac{\lambda_0 + \lambda_1 \sigma^j(y) + \ldots + \lambda_l \sigma^j(y^l)}{\mu_0 + \mu_1 \sigma^j(y) + \ldots + \mu_n \sigma^j(y^n)} = \frac{\lambda_0 + \lambda_1 q^j y + \ldots + \lambda_l (q^j y)^l}{\mu_0 + \mu_1 q^j y + \ldots + \mu_n (q^j y)^n} = b(q^j y).\end{aligned}$$

$\square$

For $a(y) \in K[y]$ denote $\deg_y(a(y))$ the degree of $a(y)$ as a polynomial in y.

Corollary 3.13. *Let $K(y)$ and σ be as in Lemma 3.12. Suppose m is prime, K contains a primitive m^{th} root of unity, and $f(t) = t^m - a(y) \in K(y)[t;\sigma]$ where $0 \neq a(y) \in K[y]$ is such that $m \nmid \deg_y(a(y))$. Then $f(t)$ is irreducible in $K(y)[t;\sigma]$.*

Proof. We have $f(t)$ is irreducible if and only if

$$N_m(b(y)) = \sigma^{m-1}(b(y)) \cdots \sigma(b(y))b(y) \neq a(y)$$

for all $b(y) \in K(y)$ by Theorem 3.11. Given $b(y) \in K(y)$, write $b(y) = c(y)/d(y)$ for some $c(y), d(y) \in K[y]$ with $d(y) \neq 0$, then

$$N_m(b(y)) = \frac{c(q^{m-1}y) \cdots c(qy)c(y)}{d(q^{m-1}y) \cdots d(qy)d(y)}$$

by Lemma 3.12. If $N_m(y) \notin K[y]$, we immediately conclude $N_m(b(y)) \neq a(y)$ because $a(y) \in K[y]$. Conversely if $N_m(b(y)) \in K[y]$, then

$$\deg_y(N_m(b(y))) = m\deg_y(c(y)) - m\deg_y(d(y))$$

for all $0 \neq b(y) \in K(y)$. Therefore $\deg_y(N_m(b(y)))$ is a multiple of m, thus $N_m(b(y)) \neq a(y)$ for all $b(y) \in K(y)$, and so $f(t)$ is irreducible. □

Recall $N_{K/F}(K^\times) \subseteq F^\times$ for any finite field extension K/F, therefore we obtain the following Corollary of Theorem's 3.5 and 3.11:

Corollary 3.14. *Let K/F be a cyclic Galois field extension of degree m with* $\mathrm{Gal}(K/F) = \langle\sigma\rangle$.

(i) If $m = 2$ then $f(t) = t^2 - a \in K[t;\sigma]$ is irreducible for all $a \in K \setminus F$.

(ii) If $m = 3$ then $f(t) = t^3 - a \in K[t;\sigma]$ is irreducible for all $a \in K \setminus F$.

(iii) If m is prime and F contains a primitive m^{th} root of unity then $f(t) = t^m - a \in K[t;\sigma]$ is irreducible for all $a \in K \setminus F$.

Proof. We have $\sigma^{m-1}(b) \cdots \sigma(b)b = N_{K/F}(b) \in F$, for all $b \in K$, hence the result follows by Corollary 3.6 and Theorems 3.5 and 3.11. □

Recently in [5, Theorem 3.1], it was shown that in the special case where K is an algebraically closed field and σ is an automorphism of K of order $n \geq 2$, that every non-constant reducible skew polynomial in $K[t;\sigma]$ can be written as a product of irreducible skew polynomials of degree less than or equal to n. Notice that in this case, the Artin-Schreier Theorem implies $\mathrm{char}(K) = 0$ and $n = 2$ [38, p. 242]. Therefore we can immediately improve [5, Theorem 3.1] to the following:

Theorem 3.15. *Let K be an algebraically closed field and σ be an automorphism of K of order $n \geq 2$. Then* $\mathrm{char}(K) = 0$*, $n = 2$ and every non-constant reducible skew polynomial in $K[t;\sigma]$ can be written as a product of linear and irreducible quadratic skew polynomials.*

We now extend some of our previous arguments to find criteria for skew polynomials of degree 4 to be irreducible. We will see that the conditions for $f(t)$ to be irreducible become complicated when $f(t)$ has degree 4.

Suppose σ is an automorphism of D and $f(t) = t^4 - a_3t^3 - a_2t^2 - a_1t - a_0 \in R = D[t;\sigma]$. Then either $f(t)$ is irreducible, $f(t)$ is divisible by a linear factor from the right, from the left, or $f(t) = g(t)h(t)$ for some $g(t), h(t) \in R$ of degree 2. In Propositions 3.2 and 3.3 we computed the remainders after dividing $f(t)$ by a linear polynomial on the right and the left. In order to obtain irreducibility criteria for $f(t)$, we wish to find the remainder after dividing $f(t)$ by $t^2 - ct - d$, $(c, d \in D)$ on the right. To do this we use the identities

$$t^2 = (t^2 - ct - d) + (ct + d), \tag{3.5}$$

$$t^3 = (t + \sigma(c))\big(t^2 - ct - d\big) + \big(\sigma(d) + \sigma(c)c\big)t + \sigma(c)d, \tag{3.6}$$

and

$$\begin{aligned} t^4 = {} & \big(t^2 + \sigma^2(c)t + \sigma^2(d) + \sigma^2(c)\sigma(c)\big)\big(t^2 - ct - d\big) \\ & + \big(\sigma^2(c)\sigma(c)c + \sigma^2(d)c + \sigma^2(c)\sigma(d)\big)t + \sigma^2(d)d + \sigma^2(c)\sigma(c)d. \end{aligned} \tag{3.7}$$

If we define

$$M_0(c,d)(t) = 1,\ M_1(c,d)(t) = t,\ M_2(c,d)(t) = ct + d$$

$$M_3(c,d)(t) = \big(\sigma(d) + \sigma(c)c\big)t + \sigma(c)d,$$

$$M_4(c,d)(t) = \big(\sigma^2(c)\sigma(c)c + \sigma^2(d)c + \sigma^2(c)\sigma(d)\big)t + \sigma^2(d)d + \sigma^2(c)\sigma(c)d,$$

then multiplying (3.5), (3.6) and (3.7) on the left by a_i and summing over i yields

$$f(t) = q(t)\big(t^2 - ct - d\big) + M_4(c,d)(t) - \sum_{i=0}^{3} a_i M_i(c,d)(t)$$

for some $q(t) \in R$. This means the remainder after dividing $f(t)$ on the right by $(t^2 - ct - d)$ is

$$M_4(c,d)(t) - \sum_{i=0}^{3} a_i M_i(c,d)(t),$$

which evidently implies:

Proposition 3.16. *$(t^2 - ct - d)|_r f(t)$ is equivalent to*

$$\sigma^2(c)\sigma(c)c + \sigma^2(d)c + \sigma^2(c)\sigma(d) - a_3\big(\sigma(d) + \sigma(c)c\big) - a_2c - a_1 = 0,$$

and

$$\sigma^2(d)d + \sigma^2(c)\sigma(c)d - a_3\sigma(c)d - a_2d - a_0 = 0.$$

Together Propositions 3.2, 3.3 and 3.16 yield:

Theorem 3.17. *$f(t)$ is irreducible if and only if*

$$\sigma^3(b)\sigma^2(b)\sigma(b)b + a_3\sigma^2(b)\sigma(b)b + a_2\sigma(b)b + a_1b + a_0 \neq 0, \tag{3.8}$$

and

$$\begin{aligned}&\sigma^3(b)\sigma^2(b)\sigma(b)b + \sigma^3(b)\sigma^2(b)\sigma(b)a_3\\ &+\sigma^3(b)\sigma^2(b)\sigma(a_2) + \sigma^3(b)\sigma^2(a_1) + \sigma^3(a_0) \neq 0,\end{aligned} \tag{3.9}$$

for all $b \in D$, and for every $c, d \in D$, we have

$$\sigma^2(c)\sigma(c)c + \sigma^2(d)c + \sigma^2(c)\sigma(d) + a_3(\sigma(d) + \sigma(c)c) + a_2c + a_1 \neq 0, \tag{3.10}$$

or

$$\sigma^2(d)d + \sigma^2(c)\sigma(c)d + a_3\sigma(c)d + a_2d + a_0 \neq 0. \tag{3.11}$$

i.e., $f(t)$ is irreducible if and only if (3.8) *and* (3.9) *and (*(3.10) *or* (3.11)*) holds.*

Proof. $f(t)$ is irreducible if and only if $(t-b) \nmid_r f(t)$ for all $b \in D$, $(t-b) \nmid_l f(t)$ for all $b \in D$ and $(t^2 - ct - d) \nmid_r f(t)$ for all $c, d \in D$. Therefore the result follows from Propositions 3.2, 3.3 and 3.16. □

We briefly consider the special case where $f(t)$ has the form $f(t) = t^4 - a \in R$:

Lemma 3.18. *Let $f(t) = t^4 - a \in R$. Suppose $(t-b)|_r f(t)$, then*

$$f(t) = (t + \sigma^3(b))(t^2 + \sigma^2(b)\sigma(b))(t-b),$$

and

$$f(t) = (t^2 + \sigma^3(b)\sigma^2(b))(t + \sigma(b))(t-b),$$

are factorisations of $f(t)$. In particular $(t+\sigma(b))(t-b) = t^2 - \sigma(b)b$ also right divides $f(t)$.

Proof. Multiplying out these factorisations gives $t^4 - \sigma^3(b)\sigma^2(b)\sigma(b)b$ which is equal to $f(t)$ by Proposition 3.2. □

Lemma 3.18 implies that if $f(t) = t^4 - a$ has a right linear divisor then it also has a right quadratic divisor. Therefore in this case Theorem 3.17 simplifies to:

Theorem 3.19. *$f(t) = t^4 - a \in R$ is reducible if and only if*

$$\sigma^2(c)\sigma(c)c + \sigma^2(d)c + \sigma^2(c)\sigma(d) = 0 \quad \text{and} \quad \sigma^2(d)d + \sigma^2(c)\sigma(c)d = a,$$

for some $c, d \in D$.

Proof. Recall $f(t)$ has a right linear divisor if and only if it has a left linear divisor by Corollary 3.4. Moreover if $f(t)$ has a right linear divisor then it also has a quadratic right divisor by Lemma 3.18, therefore $f(t)$ is reducible if and only if $(t^2 - ct - d)|_r f(t)$ for some $c, d \in D$. The result now follows from Proposition 3.16. □

3.2 IRREDUCIBILITY CRITERIA IN SKEW POLYNOMIAL RINGS OVER FINITE FIELDS

Let $K = \mathbb{F}_{p^h}$ be a finite field of order p^h for some prime p and σ be a non-trivial $\mathbb{F}_p$-automorphism of K. This means $\sigma : K \to K,\ k \mapsto k^{p^r}$, for some $r \in \{1, \ldots, h-1\}$ is a power of the Frobenius automorphism. Here σ has order $n = h/\gcd(r,h)$. Algorithms for efficiently factorising polynomials in $K[t;\sigma]$ exist, see [22] or more recently [14], however our methods are purely algebraic and employ the previously developed theory. All of our previous results from Section 3.1 hold in $K[t;\sigma]$. In this Section we focus on polynomials of the form $f(t) = t^m - a \in K[t;\sigma]$.

We will require the following well-known result:

Lemma 3.20. $\gcd(p^h - 1, p^r - 1) = p^{\gcd(h,r)} - 1$.

Proof. Let $d = \gcd(r, h)$ so that $h = dn$. We have

$$p^h - 1 = (p^d - 1)(p^{d(n-1)} + \ldots + p^d + 1),$$

therefore $p^h - 1$ is divisible by $p^d - 1$. A similar argument shows $(p^d - 1)|(p^r - 1)$. Suppose that c is a common divisor of $p^h - 1$ and $p^r - 1$, this means $p^h \equiv p^r \equiv 1 \bmod (c)$. Write $d = hx + ry$ for some integers x, y, then we have

$$p^d = p^{hx+ry} = (p^h)^x (p^r)^y \equiv 1 \bmod (c)$$

which implies $c|(p^d - 1)$ and hence $p^d - 1 = \gcd(p^h - 1, p^r - 1)$. □

Given $k \in K^\times$, we have $k \in \mathrm{Fix}(\sigma)$ if and only if $k^{p^r - 1} = 1$, if and only if k is a $(p^r - 1)^{\text{th}}$ root of unity. It is well-known there are $\gcd(p^r - 1, p^h - 1)$ such roots of unity in K, see for example [36, Proposition II.2.1], thus

$$|\mathrm{Fix}(\sigma)| = \gcd(p^r - 1, p^h - 1) + 1 = p^{\gcd(r,h)}$$

by Lemma 3.20 and so $\mathrm{Fix}(\sigma) \cong \mathbb{F}_q$ where $q = p^{\gcd(r,h)}$.

Proposition 3.21. *(i) Suppose $n \in \{2, 3\}$, then $f(t) = t^n - a \in K[t;\sigma]$ is irreducible if and only if $a \in K \setminus \mathrm{Fix}(\sigma)$. In particular there are precisely $p^h - q$ irreducible polynomials in $K[t;\sigma]$ of the form $t^n - a$ for some $a \in K$.*

(ii) Suppose n is a prime and $n|(q - 1)$. Then $f(t) = t^n - a \in K[t;\sigma]$ is irreducible if and only if $a \in K \setminus \mathrm{Fix}(\sigma)$. In particular there are precisely $p^h - q$ irreducible polynomials in $K[t;\sigma]$ of the form $t^n - a$ for some $a \in K$.

Proof. Here σ has order n and $K/\mathrm{Fix}(\sigma)$ is a cyclic Galois field extension of degree n with Galois group generated by σ.

(i) $f(t)$ is irreducible if and only if $\prod_{l=0}^{n-1} \sigma^l(b) = N_{K/\mathrm{Fix}(\sigma)}(b) \neq a$ for all $b \in K$ by Theorem 3.5 or Corollary 3.6, where $N_{K/\mathrm{Fix}(\sigma)}$ is the field norm. It is well-known that as K is a finite field, $N_{K/\mathrm{Fix}(\sigma)} : K^\times \to \mathrm{Fix}(\sigma)^\times$ is surjective and so $f(t)$ is irreducible if and only if $a \notin \mathrm{Fix}(\sigma)$. There are $p^h - q$ elements in $K \setminus \mathrm{Fix}(\sigma)$, hence there are precisely $p^h - q$ irreducible polynomials of the form $t^n - a$ for some $a \in K$.

(ii) Notice $\mathrm{Fix}(\sigma) \cong \mathbb{F}_q$ contains a primitive n^{th} root of unity because $n|(q-1)$ [36, Proposition II.2.1]. The rest of the proof is similar to (i) but using Theorem 3.11.

□

Let $a, b \in K$ and recall $(t-b)|_r(t^m - a)$ is equivalent to

$$a = \sigma^{m-1}(b) \cdots \sigma(b) b = b^s$$

by Proposition 3.2 where $s = \sum_{j=0}^{m-1} p^{rj} = (p^{mr} - 1)/(p^r - 1)$. Suppose z is a **primitive element** of K, that is z generates the multiplicative group $K^\times$. Writing $b = z^l$ for some $l \in \mathbb{Z}$ yields $(t-b)|_r(t^m - a)$ if and only if $a = z^{ls}$. This implies the following:

Proposition 3.22. *Let $f(t) = t^m - a \in K[t;\sigma]$ and write $a \in K$ as $a = z^u$ for some $u \in \{0, \ldots, p^h - 2\}$.*

(i) $(t-b) \nmid_r f(t)$ for all $b \in K$ if and only if $u \notin \mathbb{Z}s \bmod (p^h - 1)$.

(ii) If $m \in \{2, 3\}$ then $f(t)$ is irreducible if and only if $u \notin \mathbb{Z}s \bmod (p^h - 1)$.

(iii) Suppose m is a prime divisor of $(q-1)$, then $f(t)$ is irreducible if and only if $u \notin \mathbb{Z}s \bmod (p^h - 1)$.

Proof. (i) $(t-b) \nmid_r f(t)$ for all $b \in K$ if and only if $a = z^u \neq z^{ls}$ for all $l \in \mathbb{Z}$, if and only if $u \notin \mathbb{Z}s \bmod (p^h - 1)$.

(ii) $f(t)$ has a left linear divisor if and only if it has a right linear divisor by Corollary 3.4. Therefore if $m \in \{2, 3\}$ then $f(t)$ is irreducible if and only if $(t-b) \nmid_r f(t)$ for all $b \in K$ and so the assertion follows by (i).

(iii) If m is a prime divisor of $(q-1)$ then $\mathrm{Fix}(\sigma) \cong \mathbb{F}_q$ contains a primitive m^{th} root of unity. Therefore the result follows by (i) and Theorem 3.11. □

Corollary 3.23. *(i) There exists $a \in K$ such that $(t-b) \nmid_r (t^m - a)$ for all $b \in K$ if and only if* $\gcd(s, p^h - 1) > 1$.

(ii) [52, (22)] Suppose $m \in \{2,3\}$ or m is a prime divisor of $(q-1)$. Then there exists $a \in K^\times$ such that $t^m - a \in K[t;\sigma]$ is irreducible if and only if $\gcd(s, p^h - 1) > 1$.

Proof. There exists $u \in \{0, \ldots, p^h - 2\}$ such that $u \notin \mathbb{Z}s \bmod (p^h - 1)$, if and only if s does not generate $\mathbb{Z}_{p^h-1}$, if and only if $\gcd(s, p^h - 1) > 1$. Hence the result follows by Proposition 3.22. □

When $p \equiv 1 \bmod m$, it becomes simpler to apply Corollary 3.23:

Corollary 3.24. *Suppose $p \equiv 1 \bmod m$.*

(i) There exists $a \in K$ such that $(t-b) \nmid_r (t^m - a)$ for all $b \in K$.

(ii) If p is an odd prime, then there exists $a \in K^\times$ such that $t^2 - a \in K[t;\sigma]$ is irreducible.

(iii) If $m = 3$, then there exists $a \in K^\times$ such that $t^3 - a \in K[t;\sigma]$ is irreducible.

(iv) Suppose m is a prime divisor of $(q-1)$, then there exists $a \in K^\times$ such that $t^m - a \in K[t;\sigma]$ is irreducible.

Proof. We have

$$s \bmod m = \sum_{i=0}^{m-1} (p^{ri} \bmod m) \bmod m = (\sum_{i=0}^{m-1} 1) \bmod m = 0,$$

and $p^h \equiv 1 \bmod m$. This means $m | s$ and $m | (p^h - 1)$, therefore $\gcd(s, p^h - 1) \geq m$ and so the assertion follows by Corollary 3.23. □

3.3 IRREDUCIBILITY CRITERIA IN $R = D[t;\sigma,\delta]$

Let D be a division ring with center C, σ be an endomorphism of D and δ be a left σ-derivation of D. In this Section we investigate irreducibility criteria in $R = D[t;\sigma,\delta]$ generalising some of our results from Section 3.1.

Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ and define a sequence of maps $N_i : D \to D,\ i \geq 0$, recursively by

$$N_{i+1}(b) = \sigma(N_i(b))b + \delta(N_i(b)),\ N_0(b) = 1,$$

e.g. $N_0(b) = 1,\ N_1(b) = b,\ N_2(b) = \sigma(b)b + \delta(b), \ldots$

Let $r \in D$ be the unique remainder after right division of $f(t)$ by $(t-b)$, then

$$r = N_m(b) - \sum_{i=0}^{m-1} a_i N_i(b),$$

by [40, Lemma 2.4]. This evidently implies:

Proposition 3.25. *$(t-b)|_r f(t)$ is equivalent to $N_m(b) - \sum_{i=0}^{m-1} a_i N_i(b) = 0$.*

Now suppose σ is an automorphism of D. We wish to find the remainder after left division of $f(t)$ by $(t-b)$. Define a sequence of maps $M_i : D \to D$, $i \geq 0$, recursively by

$$M_{i+1}(b) = b\sigma^{-1}(M_i(b)) - \delta(\sigma^{-1}(M_i(b))),\ M_0(b) = 1,$$

for example $M_0(b) = 1,\ M_1(b) = b,\ M_2(b) = b\sigma^{-1}(b) - \delta(\sigma^{-1}(b))$, ...

Recall from page 5 that since σ is an automorphism, we can also view R as a right polynomial ring. In particular this means we can write $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ in the form $f(t) = t^m - \sum_{i=0}^{m-1} t^i a_i'$ for some uniquely determined $a_i' \in D$.

Proposition 3.26. *$(t-b)|_l f(t)$ is equivalent to $M_m(b) - \sum_{i=0}^{m-1} M_i(b) a_i' = 0$. In particular, $(t-b)|_l (t^m - a)$ if and only if $M_m(b) \neq a$.*

Proof. We first show $t^n - M_n(b) \in (t-b)R$ for all $b \in D$ and $n \geq 0$: If $n = 0$ then $t^0 - M_0(b) = 1 - 1 = 0 \in (t-b)R$ as required. Suppose inductively $t^n - M_n(b) \in (t-b)R$ for some $n \geq 0$, then

$$\begin{aligned}
&t^{n+1} - M_{n+1}(b) = t^{n+1} - b\sigma^{-1}(M_n(b)) + \delta(\sigma^{-1}(M_n(b))) \\
&= t^{n+1} + (t-b)\sigma^{-1}(M_n(b)) - t\sigma^{-1}(M_n(b)) + \delta(\sigma^{-1}(M_n(b))) \\
&= t^{n+1} + (t-b)\sigma^{-1}(M_n(b)) - M_n(b)t - \delta(\sigma^{-1}(M_n(b))) + \delta(\sigma^{-1}(M_n(b))) \\
&= (t-b)\sigma^{-1}(M_n(b)) + (t^n - M_n(b))t \in (t-b)R,
\end{aligned}$$

as $t^n - M_n(b) \in (t-b)R$. Therefore $t^n - M_n(b) \in (t-b)R$ for all $b \in D$, $n \geq 0$ by induction.

As a result, there exists $q_i(t) \in R$ such that $t^i = (t-b)q_i(t) + M_i(b)$, for all $i \in \{0, \ldots, m\}$. Multiplying on the right by a'_i and summing over i yields

$$f(t) = (t-b)q(t) + M_m(b) - \sum_{i=0}^{m-1} M_i(b)a'_i,$$

for some $q(t) \in R$. □

Using Propositions 3.25 and 3.26 we obtain criteria for skew polynomials of degree 2 and 3 to be irreducible:

Theorem 3.27. *(i) Suppose σ is an endomorphism of D, then $f(t) = t^2 - a_1t - a_0 \in R$ is irreducible if and only if $\sigma(b)b + \delta(b) - a_1b - a_0 \neq 0$ for all $b \in D$.*

(ii) Suppose σ is an automorphism of D and $f(t) = t^3 - a_2t^2 - a_1t - a_0 \in R$. Write $f(t) = t^3 - t^2a'_2 - ta'_1 - a'_0$ for some unique $a'_0, a'_1, a'_2 \in D$, then $f(t)$ is irreducible if and only if

$$N_m(b) - \sum_{i=0}^{2} a_iN_i(b) \neq 0, \tag{3.12}$$

and

$$M_m(b) - \sum_{i=0}^{2} M_i(b)a'_i \neq 0, \tag{3.13}$$

for all $b \in D$.

Proof. (i) We have $f(t)$ is irreducible if and only if it has no right linear factors, if and only if

$$N_2(b) - a_1 N_1(b) - a_0 N_0(b) = \sigma(b)b + \delta(b) - a_1 b - a_0 \neq 0,$$

for all $b \in D$ by Proposition 3.25.

(ii) We have $f(t)$ is irreducible if and only if it has no left or right linear factors, if and only if (3.12) and (3.13) hold for all $b \in D$ by Propositions 3.25 and 3.26.

□

We now prove an analogous result to Theorem 3.11:

Theorem 3.28. *Suppose σ is an endomorphism of D, m is prime,* $\mathrm{Char}(D) \neq m$ *and $C \cap \mathrm{Fix}(\sigma)$ contains a primitive m^{th} root of unity ω. Then $f(t) = t^m - a \in R$ is irreducible if and only if $N_m(b) \neq a$ for all $b \in D$.*

Proof. Recall

$$\delta(b^n) = \sum_{i=0}^{n-1} \sigma(b)^i \delta(b) b^{n-1-i},$$

for all $b \in D$, $n \geq 1$ by (1.1) and so

$$0 = \delta(1) = \delta(\omega^m) = \sum_{i=0}^{m-1} \sigma(\omega)^i \delta(\omega)\omega^{m-1-i} = \sum_{i=0}^{m-1} \omega^i \delta(\omega)\omega^{m-1-i}$$
$$= \sum_{i=0}^{m-1} \delta(\omega)\omega^{m-1} = \delta(\omega)\omega^{m-1} m,$$

where we have used $\omega \in C \cap \mathrm{Fix}(\sigma)$. Therefore $\omega \in \mathrm{Const}(\delta)$ because $\mathrm{Char}(D) \neq m$, hence also $\omega^i \in \mathrm{Const}(\delta)$ and so $(\omega t)^i = \omega^i t^i$ for all $i \in \{1, \ldots, m\}$. Furthermore if $b \in D$, then $(t - b) \nmid_r f(t)$ is equivalent to $N_m(b) \neq a$ by Proposition 3.25. The proof now follows exactly as in Theorem's 3.10 and 3.5. □

Setting $m = 3$ and $\sigma = \mathrm{id}$ in Theorem 3.28 yields:

Corollary 3.29. *Suppose* $\mathrm{Char}(D) \neq 3$, $\sigma = \mathrm{id}$ *and C contains a primitive 3^{rd} root of unity. Then $f(t) = t^3 - a \in D[t;\delta]$ is irreducible if and only if*

$$N_3(b) = b^3 + 2\delta(b)b + b\delta(b) + \delta^2(b) \neq a,$$

for all $b \in D$.

3.4 IRREDUCIBILITY CRITERIA IN $D[t;\delta]$ WHERE $\mathrm{Char}(D)=p$

Suppose $\mathrm{Char}(D) = p \neq 0$, $\sigma = \mathrm{id}$ and

$$f(t) = t^{p^e} - a_1 t^{p^{e-1}} - \ldots - a_e t - d \in D[t;\delta].$$

In $D[t;\delta]$ we have the equalities

$$(t-b)^p = t^p - V_p(b), \qquad V_p(b) = b^p + \delta^{p-1}(b) + * \in D, \tag{3.14}$$

for all $b \in D$, with $*$ a sum of commutators of $b, \delta(b), \ldots, \delta^{p-2}(b)$ [32, p. 17-18]. E.g. $V_2(b) = b^2 + \delta(b)$ and $V_3(b) = b^3 + \delta^2(b) + \delta(b)b - b\delta(b)$. In particular, if D is commutative or b commutes with all of its derivatives, then $* = 0$ and the formula simplifies to

$$V_p(b) = b^p + \delta^{p-1}(b). \tag{3.15}$$

We can iterate (3.14) to obtain

$$(t-b)^{p^i} = t^{p^i} - V_{p^i}(b), \tag{3.16}$$

for all $i \in \mathbb{N}$ where $V_{p^i}(b) = V_p^i(b) = V_p(V_p(\cdots(V_p(b))\cdots))$. We thus have $a_i t^{p^i} = a_i(t-b)^{p^i} + a_i V_{p^i}(b)$ and by summing over i we conclude:

Proposition 3.30. *([32, Proposition 1.3.25]). $(t-b)|_r f(t)$ is equivalent to*

$$V_{p^e}(b) - a_1 V_{p^{e-1}}(b) - \ldots - a_e b - d = 0. \tag{3.17}$$

Looking instead at left division of $f(t)$ by a linear polynomial gives:

Proposition 3.31. *$(t-b)|_l f(t)$ is equivalent to*

$$V_{p^e}(b) - \big(V_{p^{e-1}}(b)a_1 - \delta^{p^{e-1}}(a_1)\big) - \ldots - \big(V_p(b)a_{e-1} - \delta^p(a_{e-1})\big) \\ - (ba_e - \delta(a_e)) - d = 0.$$

Proof. We have $t^{p^k}a = (t-b)^{p^k}a + V_{p^k}(b)a$, for all $a, b \in D$ and $k \geq 1$ by (3.16). Moreover, iterating the relation $ta = at + \delta(a)$ yields

$$t^{p^k}a = \sum_{i=0}^{p^k} \binom{p^k}{i} \delta^{p^k-i}(a)t^i,$$

for all $a \in D$, $k \geq 1$ [32, (1.1.26)]. This implies $t^{p^k}a = \delta^{p^k}(a) + at^{p^k}$ for all $a \in D$, $k \geq 1$ because $\binom{p^k}{i} = 0$ for all $i \in \{1, \dots, p^k - 1\}$. Therefore

$$at^{p^k} = (t-b)^{p^k}a + V_{p^k}(b)a - \delta^{p^k}(a),$$

and hence

$$\begin{aligned} f(t) &= t^{p^e} - a_1 t^{p^{e-1}} - \ldots - a_e t - d \\ &= (t-b)q(t) + V_{p^e}(b) - \big(V_{p^{e-1}}(b)a_1 - \delta^{p^{e-1}}(a_1)\big) \\ &\qquad - \ldots - \big(V_p(b)a_{e-1} - \delta^p(a_{e-1})\big) - ba_e + \delta(a_e) - d. \end{aligned}$$

□

Corollary 3.32. *Suppose* $\mathrm{Char}(D) = p \neq 0$ *and* $f(t) = t^p - a_1 t - a_0 \in D[t;\delta]$, *where* $a_1 \in C \cap \mathrm{Const}(\delta)$. *Then* $(t-b)|_r f(t)$ *if and only if* $(t-b)|_l f(t)$.

Proof. Recall $(t-b)|_r f(t)$ if and only if $V_p(b) - a_1 b - a_0 = 0$ by Proposition 3.30, and $(t-b)|_l f(t)$ if and only if $V_p(b) - ba_1 + \delta(a_1) - a_0 = 0$ by Proposition 3.31. When $a_1 \in C \cap \mathrm{Const}(\delta)$, these two conditions are equivalent. □

When $p = 3$, Propositions 3.30 and 3.31 yield the following:

Corollary 3.33. *Let* $\mathrm{Char}(D) = 3$ *and* $f(t) = t^3 - a_1 t - a_0 \in D[t;\delta]$.

(i) $f(t)$ *is irreducible if and only if*

$$V_3(b) - a_1 b - a_0 \neq 0 \ \ \textit{and} \ \ V_3(b) - ba_1 + \delta(a_1) - a_0 \neq 0,$$

for all $b \in D$.

(ii) Let $a_1 \in C \cap \mathrm{Const}(\delta)$, *then* $f(t)$ *is irreducible if and only if* $V_3(b) - a_1 b - a_0 \neq 0$ *for all* $b \in D$.

(iii) Suppose D is commutative, then $f(t)$ is irreducible if and only if

$$b^3 + \delta^2(b) - a_1 b - a_0 \neq 0 \text{ and } b^3 + \delta^2(b) - ba_1 + \delta(a_1) - a_0 \neq 0,$$

for all $b \in D$.

Proof. Notice $f(t)$ is irreducible if and only if $(t-b) \nmid_r f(t)$ and $(t-b) \nmid_l f(t)$ for all $b \in D$ and thus (i) follows by Propositions 3.30 and 3.31. (ii) follows from (i) and Corollary 3.32 and (iii) follows from (i) and (3.15). □

Proposition 3.34. *Suppose* $\mathrm{Char}(D) = p \neq 0$*, D is commutative and δ is a non-trivial derivation of D such that $\delta^p = 0$. Let $f(t) = t^p - a \in D[t;\delta]$ where $a \notin \mathrm{Const}(\delta)$, then*

(i) $(t-b) \nmid_r f(t)$ and $(t-b) \nmid_l f(t)$ for all $b \in D$.

(ii) If $p = 3$ then $f(t)$ is irreducible.

Proof. (i) Recall $(t-b)|_r f(t)$ is equivalent to $(t-b)|_l f(t)$ by Corollary 3.32, and that $(t-b)|_r f(t)$ if and only if $V_p(b) = a$ if and only if $b^p + \delta^{p-1}(b) = a$ by Proposition 3.30. Now $b^p \in \mathrm{Const}(\delta)$ for all $b \in D$ as D is commutative [37, p. 60], also $\delta^{p-1}(b) \in \mathrm{Const}(\delta)$ as $\delta^p = 0$. Therefore if $a \notin \mathrm{Const}(\delta)$ then $b^p + \delta^{p-1}(b) \neq a$ for all $b \in D$.

(ii) If $p = 3$, then $f(t)$ is irreducible if and only if $(t-b) \nmid_r f(t)$ and $(t-b) \nmid_l f(t)$ for all $b \in D$, hence the assertion follows by (i).

□

When $f(t)$ has the form $f(t) = t^p - t - a \in D[t;\delta]$, we have:

Theorem 3.35. *([3, Lemmas 4 and 6]). For any $a \in D$, the polynomial $f(t) = t^p - t - a \in D[t;\delta]$ is either a product of commuting linear factors or irreducible. Furthermore, $f(t)$ is irreducible if and only if $V_p(b) - b - a \neq 0$, for all $b \in D$. In particular, if D is commutative then $f(t)$ is irreducible if and only if*

$$b^p + \delta^{p-1}(b) - b - a \neq 0,$$

for all $b \in D$.

4

ISOMORPHISMS BETWEEN PETIT ALGEBRAS

We now investigate isomorphisms between some Petit Algebras. The results we obtain in this Chapter will then be applied in Chapter 5 to study the automorphism groups of Petit algebras.

Let D be an associative division ring with center C, σ be an automorphism of D and δ be a left σ-derivation of D. Suppose D', C', σ' and δ' are defined similarly. Let $f(t) \in R = D[t;\sigma,\delta]$, $g(t) \in R' = D'[t;\sigma',\delta']$, and recall $S_f = R/Rf$ is an algebra over $F = C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$ and $S_g = R'/R'g$ is an algebra over $F' = C' \cap \mathrm{Fix}(\sigma') \cap \mathrm{Const}(\delta')$. Denote by $\circ_f$ the multiplication in S_f and by $\circ_g$ the multiplication in S_g. If $f(t)$ and $g(t)$ are not right invariant and $F = F'$, we have the following necessary conditions for S_f to be F-isomorphic to S_g:

Proposition 4.1. *Suppose $f(t)$, $g(t)$ are not right invariant, $F = F'$ and S_f is F-isomorphic to S_g. Then*

(i) $D \cong D'$.

(ii) $\mathrm{Nuc}_r(S_f) \cong \mathrm{Nuc}_r(S_g)$.

(iii) *S_f is a division algebra if and only if S_g is a division algebra.*

(iv) *If S_f is a finite-dimensional left F-vector space, then* $\deg(f(t)) = \deg(g(t))$.

Proof. (i) We have $\mathrm{Nuc}_l(S_f) = D$ and $\mathrm{Nuc}_l(S_g) = D'$ by Theorem 2.1(i) because S_f and S_g are not associative. Any isomorphism preserves the left nucleus and so $D \cong D'$.

(ii) Any isomorphism also preserves the right nucleus, thus $\mathrm{Nuc}_r(S_f) \cong \mathrm{Nuc}_r(S_g)$.

(iii) Let $L_{a,f} : S_f \to S_f,\ x \mapsto a \circ_f x$ denote the left multiplication in S_f and $L_{b,g} : S_g \to S_g,\ x \mapsto b \circ_g x$ the left multiplication in S_g. Similarly denote the right multiplication maps $R_{a,f}$ and $R_{b,g}$. Suppose $\phi : S_f \to S_g$ is an F-isomorphism and S_f is a division algebra, so that $L_{a,f}$ and $R_{a,f}$ are bijective for all non-zero $a \in S_f$. Furthermore we have

$$L_{b,g}(x) = \phi(L_{\phi^{-1}(b),f}(\phi^{-1}(x))) \text{ and } R_{b,g}(x) = \phi(R_{\phi^{-1}(b),f}(\phi^{-1}(x))),$$

for all $x \in S_g$, $0 \neq b \in S_g$. These imply $L_{b,g}$ and $R_{b,g}$ are bijective for all non-zero $b \in S_g$ because $\phi, \phi^{-1}, L_{\phi^{-1}(b),f}$ and $R_{\phi^{-1}(b),f}$ are all bijective, hence S_g is a division algebra. The reverse implication is proven analogously.

(iv) S_f and S_g must have the same dimension as left F-vector spaces, and since $D \cong D'$, this implies $\deg(f(t)) = \deg(g(t))$.

$\square$

4.1 AUTOMORPHISMS OF $R = D[t;\sigma,\delta]$

Henceforth we assume $D = D'$, $\sigma = \sigma'$, $\delta = \delta'$ and $f(t), g(t) \in R = D[t;\sigma,\delta]$ have degree m. Automorphisms of R can be used to define isomorphisms between Petit algebras:

Theorem 4.2. *Let Θ be an F-automorphism of R. Given $f(t) \in R$, define $g(t) = l\Theta(f(t)) \in R$ for some $l \in D^\times$. Then Θ induces an F-isomorphism $S_f \cong S_g$.*

Proof. $\Theta(t)$ has degree 1 by the argument in [41, p. 4], therefore Θ preserves the degree of elements of R and thus $\Theta|_{R_m} : R_m \to R_m$ is well defined, hence bijective and F-linear. Let $a, b \in R_m$, then there exist unique

$q(t), r(t) \in R$ with $\deg(r(t)) < m$ such that $ab = q(t)f(t) + r(t)$. We have

$$\begin{aligned}\Theta(a \circ_f b) &= \Theta(ab - qf) = \Theta(a)\Theta(b) - \Theta(q)\Theta(f) \\ &= \Theta(a)\Theta(b) - \Theta(q)l^{-1}l\Theta(f) = \Theta(a) \circ_g \Theta(b),\end{aligned}$$

and so $\Theta|_{R_m} : S_f \to S_g$ is an F-isomorphism between algebras. □

When $D = K$ is a finite field and $f(t) \in K[t;\sigma]$ is irreducible, then [44, Theorem 7] states that an automorphism Θ of $K[t;\sigma]$ restricts to an isomorphism between S_f and $S_{\Theta(f)}$. Therefore Theorem 4.2 is a generalisation of [44, Theorem 7].

In order to employ Theorem 4.2, we first investigate what the automorphisms of R look like: Given $\tau \in \mathrm{Aut}_F(D)$ and $p(t) \in R$, the map

$$\Theta : R \to R,\ \sum_{i=0}^{n} b_i t^i \mapsto \sum_{i=0}^{n} \tau(b_i) p(t)^i,$$

is an F-homomorphism if and only if

$$p(t)\tau(b) = \tau(\sigma(b))p(t) + \tau(\delta(b)), \tag{4.1}$$

for all $b \in D$ by [41, p. 4]. Furthermore, by a simple degree argument we see Θ is injective if and only if $p(t)$ has degree ≥ 1, and Θ is bijective if and only if $p(t)$ has degree $= 1$ [41, p. 4]. Therefore, by (4.1) we conclude:

Proposition 4.3. *Let $c \in D$, $d \in D^\times$, then*

$$\Theta_{\tau,c,d} : R \to R,\ \sum_{i=0}^{n} b_i t^i \mapsto \sum_{i=0}^{n} \tau(b_i)(c + dt)^i, \tag{4.2}$$

is an F-automorphism of R if and only if

$$c\tau(b) + d\delta(\tau(b)) = \tau(\sigma(b))c + \tau(\delta(b)), \tag{4.3}$$

and

$$d\sigma(\tau(b)) = \tau(\sigma(b))d, \tag{4.4}$$

for all $b \in D$.

Proof. Let $p(t) = c + dt$, then $\Theta_{\tau,c,d} : R \to R$ is bijective because $p(t)$ has degree 1, furthermore $\Theta_{\tau,c,d}$ is an F-automorphism if and only if

$$(c+dt)\tau(b) = c\tau(b) + d\sigma(\tau(b))t + d\delta(\tau(b)) = \tau(\sigma(b))(c+dt) + \tau(\delta(b)),$$

by (4.1). Comparing the coefficients of t^0 and t yields (4.3) and (4.4) as required. □

Looking closely at the conditions (4.3) and (4.4) yields the following:

Corollary 4.4. *(i) Suppose $c \in D$, $d \in D^\times$. Then $\Theta_{\mathrm{id},c,d}$ is an F-automorphism of R if and only if $d \in C^\times$ and*

$$cb + d\delta(b) = \sigma(b)c + \delta(b)$$

for all $b \in D$.

(ii) $\Theta_{\tau,0,1}$ is an F-automorphism of R if and only if $\sigma \circ \tau = \tau \circ \sigma$ and $\delta \circ \tau = \tau \circ \delta$.

(iii) Let $c \in D$, then $\Theta_{\tau,c,1}$ is an F-automorphism of R if and only if $\sigma \circ \tau = \tau \circ \sigma$ and

$$c\tau(b) + \delta(\tau(b)) = \tau(\sigma(b))c + \tau(\delta(b)), \tag{4.5}$$

for all $b \in D$.

(iv) Suppose $c \in D^\times, 1 \neq d \in C^\times$ and δ is the inner σ-derivation

$$\delta : D \to D,\ b \mapsto c(1-d)^{-1}b - \sigma(b)c(1-d)^{-1}. \tag{4.6}$$

Then $\Theta_{\mathrm{id},c,d}$ is an F-automorphism of R.

Proof. (ii) and (iii) follow immediately from (4.3) and (4.4).

(i) Setting $\tau = \mathrm{id}$ in (4.4) yields $d\sigma(b) = \sigma(b)d$ for all $b \in D$, which is equivalent to $d \in C^\times$. The result follows by setting $\tau = \mathrm{id}$ in (4.3).

(iv) If δ has the form (4.6) and $\tau = \mathrm{id}$, then

$$cb + d\delta(b) = cb + d\big(c(1-d)^{-1}b - \sigma(b)c(1-d)^{-1}\big)$$

$$= (1-d)^{-1}\big(cb(1-d) + dcb - d\sigma(b)c\big) = (1-d)^{-1}(cb - d\sigma(b)c)$$
$$= (1-d)^{-1}\big(\sigma(b)c(1-d) + cb - \sigma(b)c\big) = \sigma(b)c + \delta(b),$$

and $d\sigma(b) = \sigma(b)d$, for all $b \in D$ because $d \in C^{\times}$. Therefore $\Theta_{\mathrm{id},c,d}$ is an F-automorphism of R by Proposition 4.3.

□

We can use Theorem 4.2 together with Proposition 4.3 and Corollary 4.4, to find isomorphisms between some Petit algebras:

Corollary 4.5. *Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$.*

(i) Suppose $\tau \in \mathrm{Aut}_F(D)$ and $c \in D$, $d \in D^{\times}$ are such that (4.3) and (4.4) hold for all $b \in D$. Let $g(t) = (c+dt)^m - \sum_{i=0}^{m-1} \tau(a_i)(c+dt)^i \in R$, then $S_f \cong S_g$.

(ii) Suppose $\tau \in \mathrm{Aut}_F(D)$ is such that $\sigma \circ \tau = \tau \circ \sigma$ and $\delta \circ \tau = \tau \circ \delta$ and define $g(t) = t^m - \sum_{i=0}^{m-1} \tau(a_i)t^i \in R$, then $S_f \cong S_g$.

(iii) Suppose $\tau \in \mathrm{Aut}_F(D)$ and $c \in D$ are such that $\sigma \circ \tau = \tau \circ \sigma$ and (4.5) holds for all $b \in D$. If $g(t) = (c+t)^m - \sum_{i=0}^{m-1} \tau(a_i)(c+t)^i \in R$, then $S_f \cong S_g$.

(iv) Suppose δ is the inner σ-derivation given by (4.6) for some $c \in D^{\times}, 1 \neq d \in C^{\times}$. If $g(t) = (c+dt)^m - \sum_{i=0}^{m-1} a_i(c+dt)^i \in R$, then $S_f \cong S_g$.

Proof. In (i), (ii), (iii) and (iv) the maps $\Theta_{\tau,c,d}$, $\Theta_{\tau,0,1}$, $\Theta_{\tau,c,1}$ and $\Theta_{\mathrm{id},c,d}$ resp. are F-automorphisms of R by Proposition 4.3 and Corollary 4.4. Applying these automorphisms to $f(t)$ gives $g(t)$ in each case, thus the assertion follows by Theorem 4.2. □

4.2 isomorphisms between S_f and S_g when $f(t), g(t) \in D[t;\delta]$

Let D be an associative division ring with center C, δ be a derivation of D and $F = C \cap \mathrm{Const}(\delta)$. We briefly look into the isomorphisms between some Petit algebras S_f and S_g in the special case where $f(t), g(t) \in R = D[t;\delta]$. Here Proposition 4.3 becomes:

Corollary 4.6. *Let $c, d \in D$ and $\tau \in \mathrm{Aut}_F(D)$, then the map $\Theta_{\tau,c,d}$ defined by (4.2) is an F-automorphism of R, if and only if $d \in C^\times$ and*

$$c\tau(b) + d\delta(\tau(b)) = \tau(b)c + \tau(\delta(b)). \tag{4.7}$$

In particular, if $c \in C$ then $\Theta_{\tau,c,1}$ is an F-automorphism if and only if $\delta \circ \tau = \tau \circ \delta$.

Proof. With $\sigma = \mathrm{id}$, (4.4) becomes $d\tau(b) = \tau(b)d$ for all $b \in D$, i.e. $d \in C$. Finally, setting $\sigma = \mathrm{id}$ in (4.3) yields (4.7), hence the result follows by Proposition 4.3. □

Recall from (3.14) that when D has characteristic $p \neq 0$, we have

$$(t-b)^p = t^p - V_p(b),\ V_p(b) = b^p + \delta^{p-1}(b) + *$$

for all $b \in D$, where $*$ is a sum of commutators of $b, \delta(b), \ldots, \delta^{p-2}(b)$. An iteration yields $(t-b)^{p^e} = t^{p^e} - V_{p^e}(b)$, for all $b \in D$ with $V_{p^e}(b) = V_p^e(b) = V_p(\ldots(V_p(b)\ldots)$. We use Corollary 4.6, together with Theorem 4.2 to obtain sufficient conditions for some Petit algebras to be isomorphic:

Corollary 4.7. *(a) Suppose D has arbitrary characteristic and $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R = D[t;\delta]$.*

- *(i) Let $\tau \in \mathrm{Aut}_F(D)$ and $g(t) = (t-c)^m - \sum_{i=0}^{m-1} \tau(a_i)(t-c)^i \in R$ for some $c \in C$. If $\tau \circ \delta = \delta \circ \tau$, then $S_f \cong S_g$.*
- *(ii) Let $g(t) = (t-c)^m - \sum_{i=0}^{m-1} a_i(t-c)^i \in R$ for some $c \in C$, then $S_f \cong S_g$.*

(b) Suppose $\mathrm{Char}(D) = p \neq 0$ and $f(t) = t^{p^e} + a_1 t^{p^{e-1}} + \ldots + a_e t + d \in R$.

- *(i) Let $\tau \in \mathrm{Aut}_F(D)$. If $\tau \circ \delta = \delta \circ \tau$ and*

$$\begin{aligned} g(t) = t^{p^e} &+ \tau(a_1)t^{p^{e-1}} + \ldots + \tau(a_e)t + \tau(d) - V_{p^e}(c) \\ &- \tau(a_1)V_{p^{e-1}}(c) - \ldots - \tau(a_e)c \in R \end{aligned}$$

for some $c \in C$, then $S_f \cong S_g$.

(ii) Let

$$g(t) = f(t) - V_{p^e}(c) - a_1 V_{p^{e-1}}(c) - \ldots - a_e c \in R$$

for some $c \in C$, then $S_f \cong S_g$.

Proof. (i) The maps $\Theta_{\tau,-c,1}$ are automorphisms of R for all $c \in C$ by Corollary 4.6. In (a) we have $g(t) = \Theta_{\tau,-c,1}(f(t))$ and so $S_f \cong S_g$ by Theorem 4.2.

In (b), since $\mathrm{Char}(D) = p \neq 0$, we have

$$\begin{aligned}\Theta_{\tau,-c,1}(f(t)) &= (t-c)^{p^e} + \tau(a_1)(t-c)^{p^{e-1}} + \ldots + \tau(a_e)(t-c) + \tau(d)\\ &= t^{p^e} - V_{p^e}(c) + \tau(a_1)\big(t^{p^{e-1}} - V_{p^{e-1}}(c)\big) + \ldots + \tau(a_e)(t-c) + \tau(d)\\ &= g(t),\end{aligned}$$

and hence $S_f \cong S_g$ by Theorem 4.2.

(ii) follows from (i) by setting $\tau = \mathrm{id}$.

□

4.3 ISOMORPHISMS BETWEEN S_f AND S_g WHEN $f(t), g(t) \in D[t;\sigma]$

Let D be an associative division ring with center C and σ be an automorphism of D. Suppose $\delta = 0$ so that

$$f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i, \; g(t) = t^m - \sum_{i=0}^{m-1} b_i t^i \in R = D[t;\sigma],$$

then S_f and S_g are nonassociative algebras over $F = C \cap \mathrm{Fix}(\sigma)$. Throughout this Section, if we assume σ has order $\geq m-1$, we include infinite order. We begin by looking at the automorphisms of R. Here Proposition 4.3 becomes:

Corollary 4.8. *Let $c \in D$, $d \in D^\times$ and $\tau \in \mathrm{Aut}_F(D)$. Then $\Theta_{\tau,c,d}$ is an F-automorphism of R if and only if $c\tau(b) = \tau(\sigma(b))c$ and $d\sigma(\tau(b)) = \tau(\sigma(b))d$ for all $b \in D$. In particular, if $\sigma \circ \tau = \tau \circ \sigma$ then $\Theta_{\tau,0,d}$ is an F-automorphism if and only if $d \in C^\times$.*

We employ Corollary 4.8, together with Theorem 4.2, to find sufficient conditions for S_f and S_g to be F-isomorphic. When $f(t)$ and $g(t)$ are not right invariant, σ commutes with all F-automorphisms of D, and $\sigma|_C$ has order at least $m-1$, these conditions are also necessary:

Theorem 4.9. *(i) Suppose there exists $k \in C^\times$ such that*

$$a_i = \Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big) b_i, \tag{4.8}$$

for all $i \in \{0, \dots, m-1\}$. Then $S_f \cong S_g$. Furthermore, for every such $k \in C^\times$ the maps $Q_{\mathrm{id},k} : S_f \to S_g$,

$$Q_{\mathrm{id},k} : \sum_{i=0}^{m-1} x_i t^i \mapsto x_0 + \sum_{i=1}^{m-1} x_i \big(\prod_{l=0}^{i-1} \sigma^l(k)\big) t^i, \tag{4.9}$$

are F-isomorphisms between S_f and S_g.

(ii) Suppose there exists $\tau \in \mathrm{Aut}_F(D)$ and $k \in C^\times$ such that σ commutes with τ and

$$\tau(a_i) = \Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big) b_i, \tag{4.10}$$

for all $i \in \{0, \dots, m-1\}$. Then $S_f \cong S_g$. Furthermore, for every such τ and k the maps $Q_{\tau,k} : S_f \to S_g$,

$$Q_{\tau,k} : \sum_{i=0}^{m-1} x_i t^i \mapsto \tau(x_0) + \sum_{i=1}^{m-1} \tau(x_i) \big(\prod_{l=0}^{i-1} \sigma^l(k)\big) t^i, \tag{4.11}$$

are F-isomorphisms between S_f and S_g.

(iii) Suppose $f(t)$, $g(t)$ are not right invariant, $\sigma|_C$ has order at least $m-1$, and σ commutes with all F-automorphisms of D. Then $S_f \cong S_g$ if and only if there exists $\tau \in \mathrm{Aut}_F(D)$ and $k \in C^\times$ such that (4.10) *holds for all $i \in \{0, \dots, m-1\}$. Every such τ and k gives rise to an F-isomorphism $Q_{\tau,k} : S_f \to S_g$ and these are the only F-isomorphisms between S_f and S_g.*

Proof. (i) Recall $\Theta_{\mathrm{id},0,k}$ is an F-automorphism of R by Corollary 4.8, moreover

$$\Theta_{\mathrm{id},0,k}(f(t)) = (kt)^m - \sum_{i=0}^{m-1} a_i (kt)^i$$

$$= (\prod_{l=0}^{m-1} \sigma^l(k))t^m - a_0 - \sum_{i=1}^{m-1} a_i(\prod_{l=0}^{i-1} \sigma^l(k))t^i$$
$$= (\prod_{l=0}^{m-1} \sigma^l(k))\Big(t^m - \sum_{i=0}^{m-1} b_i t^i\Big) = (\prod_{l=0}^{m-1} \sigma^l(k))g(t),$$

by (4.8) and thus $\Theta_{\mathrm{id},0,k}$ restricts to an isomorphism between S_f and S_g by Theorem 4.2. This restriction is $Q_{\mathrm{id},k}$ by a straightforward calculation.

(ii) The proof is similar to (i) using that $\Theta_{\tau,0,k} \in \mathrm{Aut}_F(R)$ by Corollary 4.8.

(iii) We are left to prove that $S_f \cong S_g$ implies there exists $\tau \in \mathrm{Aut}_F(D)$ and $k \in C^\times$ such that (4.10) holds for all $i \in \{0, \dots, m-1\}$, and that all F-isomorphisms between S_f and S_g have the form $Q_{\tau,k}$ where τ and k satisfy (4.10).

Suppose $S_f \cong S_g$ and let $Q : S_f \to S_g$ be an F-isomorphism. $f(t)$ and $g(t)$ are not right invariant which is equivalent to S_f and S_g not being associative, therefore $\mathrm{Nuc}_l(S_f) = \mathrm{Nuc}_l(S_g) = D$ by Theorem 2.1(i). Since any isomorphism preserves the left nucleus, $Q(D) = D$ and so $Q|_D = \tau$ for some $\tau \in \mathrm{Aut}_F(D)$. Suppose $Q(t) = \sum_{i=0}^{m-1} k_i t^i$ for some $k_i \in D$, then we have

$$Q(t \circ_f z) = Q(t) \circ_g Q(z) = \Big(\sum_{i=0}^{m-1} k_i t^i\Big) \circ_g \tau(z) = \sum_{i=0}^{m-1} k_i \sigma^i(\tau(z))t^i, \tag{4.12}$$

and

$$Q(t \circ_f z) = Q(\sigma(z)t) = \sum_{i=0}^{m-1} \tau(\sigma(z))k_i t^i \tag{4.13}$$

for all $z \in D$. Comparing the coefficients of t^i in (4.12) and (4.13) we obtain

$$k_i \sigma^i(\tau(z)) = k_i \tau(\sigma^i(z)) = \tau(\sigma(z))k_i, \tag{4.14}$$

for all $i \in \{0, \dots m-1\}$ and all $z \in D$ as σ and τ commute. In particular

$$k_i \tau(\sigma^i(z)) = k_i \tau(\sigma(z)),$$

for all $i \in \{0, \dots m-1\}$ and all $z \in C$. This means

$$k_i \tau\big(\sigma^i(z) - \sigma(z)\big) = 0,$$

for all $i \in \{0, \dots m-1\}$ and all $z \in C$, i.e. $k_i = 0$ or $\sigma|_C = \sigma^i|_C$ for all $i \in \{0, \dots, m-1\}$. Now, $\sigma|_C$ has order at least $m-1$ or infinite order which means $\sigma^i|_C \neq \sigma|_C$ for all $1 \neq i \in \{0, \dots, m-1\}$ and thus $k_i = 0$ for all $1 \neq i \in \{0, \dots, m-1\}$. Therefore $Q(t) = kt$ for some $k \in D^\times$ such that $k\tau(\sigma(z)) = \tau(\sigma(z))k$ for all $z \in D$ by (4.14). Hence $k \in C^\times$.

Furthermore, we have

$$Q(zt^i) = Q(z) \circ_g Q(t)^i = \tau(z)(kt)^i = \tau(z)\Big(\prod_{l=0}^{i-1} \sigma^l(k)\Big)t^i,$$

for all $i \in \{1, \dots, m-1\}$ and all $z \in D$. Thus Q has the form

$$Q_{\tau,k} : \sum_{i=0}^{m-1} x_i t^i \mapsto \tau(x_0) + \sum_{i=1}^{m-1} \tau(x_i)\big(\prod_{l=0}^{i-1} \sigma^l(k)\big)t^i,$$

for some $k \in C^\times$. Moreover, with $t^m = t \circ_f t^{m-1}$, also

$$\begin{aligned} Q(t^m) &= Q\big(\sum_{i=0}^{m-1} a_i t^i\big) = \sum_{i=0}^{m-1} Q(a_i) \circ_g Q(t)^i \\ &= \tau(a_0) + \sum_{i=1}^{m-1} \tau(a_i)\big(\prod_{l=0}^{i-1} \sigma^l(k)\big)t^i, \end{aligned} \tag{4.15}$$

and $Q(t \circ_f t^{m-1}) = Q(t) \circ_g Q(t)^{m-1}$, i.e.

$$Q(t^m) = Q(t) \circ_g Q(t)^{m-1} = \Big(\prod_{l=0}^{m-1} \sigma^l(k)\Big)t^m = \Big(\prod_{l=0}^{m-1} \sigma^l(k)\Big) \sum_{i=0}^{m-1} b_i t^i. \tag{4.16}$$

Comparing (4.15) and (4.16) gives $\tau(a_i) = \Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big)b_i$, for all $i \in \{0, \dots, m-1\}$, and hence Q has the form $Q_{\tau,k}$ where $\tau \in \mathrm{Aut}_F(D)$ and $k \in C^\times$ satisfy (4.10).

□

Remark. *Suppose $D = \mathbb{F}_{p^n}$ is a finite field of order p^n, $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n},\ k \mapsto k^p$ is the Frobenius automorphism and $f(t), g(t) \in \mathbb{F}_{p^n}[t;\sigma]$ are irreducible of degree $m \in \{2, 3\}$. Then S_f and S_g are isomorphic semifields if and only if there exists $\tau \in$*

$\mathrm{Aut}(\mathbb{F}_{p^n})$ and $k \in \mathbb{F}_{p^n}^\times$ are such that (4.10) holds for all $i \in \{0, \ldots, m-1\}$ by [66, Theorems 4.2 and 5.4]. Therefore Theorem 4.9(iii) can be seen as a generalisation of [66, Theorems 4.2 and 5.4].

We obtain the following Corollaries of Theorem 4.9:

Corollary 4.10. *Let $f(t) = t^m - a \in R$ and define $g(t) = t^m - k^m a \in R$ for some $k \in F^\times$. Then $S_f \cong S_g$.*

Proof. We have $\left(\prod_{l=0}^{m-1} \sigma^l(k)\right) a = k^m a$ and so $S_f \cong S_g$ by Theorem 4.9(i). $\square$

We next take a closer look at the equation (4.10) to obtain necessary conditions for some S_f and S_g to be isomorphic.

Corollary 4.11. *Suppose $f(t)$ and $g(t)$ are not right invariant, σ commutes with all F-automorphisms of D and $\sigma|_C$ has order at least $m-1$. If $S_f \cong S_g$ then $a_i = 0$ is equivalent to $b_i = 0$ for all $i \in \{0, \ldots, m-1\}$.*

Proof. If $a_i \neq b_i$ then $\tau(a_i) \neq \left(\prod_{l=i}^{m-1} \sigma^l(k)\right) b_i$ for all $\tau \in \mathrm{Aut}_F(D)$ and all $k \in C^\times$ and so $S_f \not\cong S_g$ by Theorem 4.9(iii), a contradiction. $\square$

Now suppose C/F is a proper field extension of finite degree, D is finite-dimensional as an algebra over C, and D is also finite-dimensional when considered as an algebra over F. Let $N_{D/C}$ denote the norm of D considered as an algebra over C, $N_{D/F}$ the norm of D considered as an algebra over F and $N_{C/F}$ be the norm of the field extension C/F. We have $N_{D/F}(z) = N_{C/F}(N_{D/C}(z))$ and $N_{D/F}(\tau(z)) = N_{D/F}(z)$, for all $\tau \in \mathrm{Aut}_F(D)$ and all $z \in D$ [47, p. 547, 548].

Corollary 4.12. *Suppose $f(t)$ and $g(t)$ are not right invariant, σ commutes with all F-automorphisms of D and $\sigma|_C$ has order at least $m-1$.*

(i) If $b_0 \neq 0$ and $N_{D/F}(a_0 b_0^{-1}) \notin F^{\times m}$ then $S_f \not\cong S_g$.

(ii) If there exists $i \in \{0, \ldots, m-1\}$ such that $b_i \neq 0$ and $N_{D/F}(a_i b_i^{-1}) \notin F^{\times(m-i)}$ then $S_f \not\cong S_g$.

Proof. We prove (ii) since setting $i = 0$ in (ii) yields (i). Suppose, for a contradiction, that $S_f \cong S_g$. Then there exists $\tau \in \mathrm{Aut}_F(D)$ and $k \in C^\times$ such that $\tau(a_i) = \Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big) b_i$ by Theorem 4.9(iii). Applying $N_{D/F}$ we obtain

$$N_{D/F}(\tau(a_i)) = N_{D/F}(a_i) = N_{D/F}\big(\big(\prod_{l=i}^{m-1} \sigma^l(k)\big) b_i\big) = N_{D/F}(k)^{m-i} N_{D/F}(b_i).$$

This implies $N_{D/F}(a_i b_i^{-1}) = N_{D/F}(k)^{m-i}$ by the multiplicity of the norm, but here $N_{D/F}(k)^{m-i} \in F^{\times(m-i)}$, a contradiction. $\square$

In [64], isomorphisms between two nonassociative cyclic algebras were briefly investigated. We show Theorem 4.9(iii) specialises to [64, Proposition 3.2.8] and [64, Corollary 6.2.5].

Let K/F be a cyclic Galois field extension of degree m with $\mathrm{Gal}(K/F) = \langle \sigma \rangle$ and $a, b \in K \setminus F$. Then Theorem 4.9(iii) shows when the nonassociative cyclic algebras $(K/F, \sigma, a)$ and $(K/F, \sigma, b)$ are isomorphic:

Corollary 4.13. *([64, Proposition 3.2.8]).* $(K/F, \sigma, a) \cong (K/F, \sigma, b)$ *if and only if there exists* $k \in K^\times$ *and* $j \in \{0, \dots, m-1\}$ *such that* $\sigma^j(a) = \big(\prod_{l=0}^{m-1} \sigma^l(k)\big) b = N_{K/F}(k) b$.

Now suppose additionally K and F are finite fields. It is well-known that the norm $N_{K/F} : K^\times \to F^\times$ is surjective for finite extensions of finite fields and so by Corollary 4.13, we conclude:

Corollary 4.14. *([64, Corollary 6.2.5]).* $(K/F, \sigma, a) \cong (K/F, \sigma, b)$ *if and only if* $\sigma^j(a) = kb$ *for some* $j \in \{0, \dots, m-1\}$ *and some* $k \in F^\times$.

5

AUTOMORPHISMS OF PETIT ALGEBRAS

Let D be an associative division ring with center C, σ be a ring automorphism of D, δ be a left σ-derivation of D and $f(t) \in R = D[t;\sigma,\delta]$. Here S_f is a nonassociative algebra over $F = C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$. Since $S_f = S_{df}$ for all $d \in D^\times$ we assume w.l.o.g. that $f(t)$ is monic, otherwise, if $f(t)$ has leading coefficient $d \in D^\times$, then consider $d^{-1}f(t)$. In this Chapter we study the automorphism groups of Petit algebras building upon our results in Chapter 4. We obtain partial results in the most general case where σ is not necessarily the identity and δ is not necessarily 0, however, most of our attention is given to the cases where $f(t)$ is either a differential or twisted polynomial (see Sections 5.1 and 5.2 respectively). Later in Chapter 6 we go on to study the automorphism groups of nonassociative cyclic algebras.

If $f(t) \in R$ is not right invariant, then S_f is not associative and any automorphism of S_f extends automorphisms of $\mathrm{Nuc}_l(S_f)$, $\mathrm{Nuc}_m(S_f)$ and $\mathrm{Nuc}_r(S_f)$ because the nuclei are invariant under automorphisms. Since $\mathrm{Nuc}_l(S_f) = \mathrm{Nuc}_m(S_f) = D$ and $\mathrm{Nuc}_r(S_f) = E(f)$ by Theorem 2.1, we conclude:

Lemma 5.1. *If $f(t) \in R$ is not right invariant, any F-automorphism of S_f extends an F-automorphism of D and an F-automorphism of $E(f)$.*

By Theorem 4.2, automorphisms $\Theta : R \to R$ induce isomorphisms between S_f and $S_{\Theta(f(t))}$. This means if $\Theta(f(t)) = lf(t)$ for some $l \in D^\times$, then Θ induces an isomorphism $S_f \cong S_{l\Theta(f(t))} = S_f$, i.e. Θ induces an automorphism of S_f:

Theorem 5.2. *If Θ is an F-automorphism of R and $\Theta(f(t)) = lf(t)$ for some $l \in D^\times$, then $\Theta(b \circ c) = \Theta(b) \circ \Theta(c)$ for all $b, c \in S_f$, i.e. Θ induces an F-automorphism of S_f.*

Theorem 5.2 allows us to find automorphisms of Petit algebras which are induced by automorphisms of R, later focusing on the special cases where R is a differential or twisted polynomial ring. More generally, when σ is not necessarily the identity, and δ is not necessarily 0, we can still use Theorem 5.2 to obtain non-trivial automorphisms of S_f for some quadratic $f(t)$:

Proposition 5.3. *Suppose $1 \neq d \in C^\times$ is such that $d\sigma(d) = 1$ and δ is the inner σ-derivation given by*

$$\delta : D \to D,\ b \mapsto c(1-d)^{-1}b - \sigma(b)c(1-d)^{-1},$$

for some $c \in D^\times$. If $f(t) = t^2 - (c - d\sigma(c))(1-d)^{-1}t - a \in R$, then the map

$$H_{\mathrm{id},c,d} : S_f \to S_f,\ x_0 + x_1 t \mapsto x_0 + x_1(c + dt),$$

is a non-trivial F-automorphism of S_f. Moreover, if additionally d is a primitive n^{th} root of unity for some $n > 1$, then $\langle H_{\mathrm{id},c,d}\rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(S_f)$ of order n.

Proof. Recall

$$\Theta : R \to R,\ \sum_{i=0}^{n} b_i t^i \mapsto \sum_{i=0}^{n} b_i (c + dt)^i,$$

is an F-automorphism by Corollary 4.4. We have

$$\begin{aligned}
\Theta(f(t)) &= (c+dt)^2 - (c - d\sigma(c))(1-d)^{-1}(c+dt) - a \\
&= d\sigma(d)t^2 + \Big(cd + d\sigma(c) + d\delta(d) - (c - d\sigma(c))(1-d)^{-1}d\Big)t \\
&\qquad + \Big(c^2 + d\delta(c) - (c - d\sigma(c))(1-d)^{-1}c - a\Big) \\
&= t^2 - (c - d\sigma(c))(1-d)^{-1}t - a = f(t),
\end{aligned}$$

where we have used that $d\sigma(d) = 1$, hence the first assertion follows by Theorem 5.2.

To prove the final assertion we first show $H^n_{\mathrm{id},c,d}$ has the form

$$H^n_{\mathrm{id},c,d}(x_0 + x_1 t) = x_0 + x_1 c(1-d^n)(1-d)^{-1} + x_1 d^n t, \tag{5.1}$$

for all $n \in \mathbb{N}$ by induction: For $n = 1$ we have

$$x_0 + x_1 c(1-d^n)(1-d)^{-1} + x_1 d^n t = x_0 + x_1 c + x_1 dt = H_{\mathrm{id},c,d}(x_0 + x_1 t)$$

as required. Assume as induction hypothesis that (5.1) holds for some $n \geq 1$, then

$$\begin{aligned}
{H_{\mathrm{id},c,d}}^{n+1}(x_0 + x_1 t) &= H_{\mathrm{id},c,d}\big(H^n_{\mathrm{id},c,d}(x_0 + x_1 t)\big) \\
&= H_{\mathrm{id},c,d}\big(x_0 + x_1 c(1-d^n)(1-d)^{-1} + x_1 d^n t\big) \\
&= x_0 + x_1 c(1-d^n)(1-d)^{-1} + x_1 d^n (c + dt) \\
&= x_0 + x_1 c \sum_{j=0}^{n-1} d^j + x_1 c d^n + x_1 d^{n+1} t = x_0 + x_1 c \sum_{j=0}^{n} d^j + x_1 d^{n+1} t \\
&= x_0 + x_1 c(1-d^{n+1})(1-d)^{-1} + x_1 d^{n+1} t,
\end{aligned}$$

and thus (5.1) holds by induction. In particular (5.1) implies $H^n_{\mathrm{id},c,d} = \mathrm{id}$ if and only if $d^n = 1$, therefore if d is a primitive n^{th} root of unity, $\langle H_{\mathrm{id},c,d} \rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(S_f)$ of order n. $\square$

Setting $d = -1$ in Proposition 5.3 gives:

Corollary 5.4. *Suppose* $\mathrm{Char}(D) \neq 2$ *and δ is the inner σ-derivation given by*

$$\delta : D \to D, \ b \mapsto \frac{c}{2} b - \sigma(b) \frac{c}{2},$$

for some $c \in D^\times$. Then for

$$f(t) = t^2 - \frac{1}{2}(c + \sigma(c))t - a \in R,$$

the map $H_{\mathrm{id},c,-1}$ is an F-automorphism of S_f. Moreover $\{\mathrm{id}, H_{\mathrm{id},c,-1}\}$ is a subgroup of $\mathrm{Aut}_F(S_f)$.

Example 5.5. *Suppose $K = F(i)$ is a quadratic separable extension of F with non-trivial automorphism σ and let δ be the inner σ-derivation*

$$\delta : K \to K,\ b \mapsto \frac{c}{1-i}(b - \sigma(b)),$$

for some $c \in K$. Then $i\sigma(i) = -i^2 = 1$ and i is a primitive 4^{th} root of unity, so for

$$f(t) = t^2 - \frac{c - i\sigma(c)}{1-i}t - a \in K[t;\sigma,\delta],$$

the map $H_{\mathrm{id},c,i}$ is an automorphism of S_f of order 4 by Proposition 5.3.

Proposition 5.6. *Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in F[t] = F[t;\sigma,\delta] \subset R$, then for all $\tau \in \mathrm{Aut}_F(D)$ such that $\sigma \circ \tau = \tau \circ \sigma$ and $\delta \circ \tau = \tau \circ \delta$, the maps*

$$H_{\tau,0,1} : S_f \to S_f,\ \sum_{i=0}^{m-1} b_i t^i \mapsto \sum_{i=0}^{m-1} \tau(b_i) t^i,$$

are F-automorphisms of S_f.

Proof. Let $\tau \in \mathrm{Aut}_F(D)$, then

$$\Theta : R \to R,\ \sum_{i=0}^{n} b_i t^i \mapsto \sum_{i=0}^{n} \tau(b_i) t^i,$$

is an F-automorphism if and only if $\sigma \circ \tau = \tau \circ \sigma$ and $\delta \circ \tau = \tau \circ \delta$ by Corollary 4.4. If all the coefficients of $f(t)$ are contained in F, a straightforward computation yields $\Theta(f(t)) = f(t)$, hence $H_{\tau,0,1} \in \mathrm{Aut}_F(S_f)$ by Theorem 5.2. $\square$

Given a nonassociative F-algebra A, an element $0 \neq c \in A$ has a **left inverse** $c_l \in A$ if $R_c(c_l) = c_l c = 1$, and a **right inverse** $c_r \in A$ if $L_c(c_r) = cc_r = 1$. We say c is **invertible** if it has both a left and a right inverse. In [68, p. 233] the definition of inner automorphisms of associative algebras is generalised to finite nonassociative division algebras, also called finite semifields. We can generalise this definition further to arbitrary nonassociative algebras:

Definition. *An automorphism $G \in \mathrm{Aut}_F(A)$ is an* ***inner automorphism*** *if there is an element $0 \neq c \in A$ with left inverse c_l, such that $G(x) = (c_l x)c$ for all $x \in A$.*

Equivalently, an automorphism G is inner if there is an element $0 \neq c \in A$ with left inverse c_l, such that $G(x) = R_c(L_{c_l}(x))$ for all $x \in A$.

When A is a finite semifield, every non-zero element of A is left invertible and our definition reduces to the definition of inner automorphisms given in [68]. Given an inner automorphism $G \in \mathrm{Aut}_F(A)$ and some $H \in \mathrm{Aut}_F(A)$ then a straightforward calculation shows $H^{-1} \circ G \circ H$ is the inner automorphism $A \to A,\ x \mapsto \big(H^{-1}(c_l)x\big)H^{-1}(c)$.

If $c \in \mathrm{Nuc}(A)$ is invertible, then $c_l = c_r$ as $\mathrm{Nuc}(A)$ is an associative algebra. We denote this element c^{-1}. Let G_c denote the map $G_c : A \to A,\ x \mapsto (c^{-1}x)c$ for all invertible $c \in \mathrm{Nuc}(A)$.

We remark that if $c \in D$ and $f(t) \in D[t;\sigma,\delta]$ is not right invariant, then multiplying $1 = c_l c$ on the right by c_r and using $c \in \mathrm{Nuc}_m(S_f)$ yields $c_r = (c_l c)c_r = c_l(cc_r) = c_l = c^{-1}$.

Proposition 5.7. *$Q = \{G_c \mid c \in \mathrm{Nuc}(A)$ is invertible$\}$ is a subgroup of $\mathrm{Aut}_F(A)$ consisting of inner automorphisms.*

Proof. We have

$$\begin{aligned} G_c(x)G_c(y) &= \big((c^{-1}x)c\big)\big((c^{-1}y)c\big) = (c^{-1}x)[c((c^{-1}y)c)] = (c^{-1}x)[[cc^{-1}y]c] \\ &= (c^{-1}x)(yc) = \big((c^{-1}x)y\big)c = (c^{-1}(xy))c = G_c(xy), \end{aligned}$$

for all $x, y \in A$, where we have used $c^{-1} \in \mathrm{Nuc}(A)$. Hence G_c is multiplicative. Now G_c is clearly bijective and F-linear, and so the maps G_c are F-automorphisms of A for all invertible $c \in \mathrm{Nuc}(A)$.

We now prove Q is a subgroup of $\mathrm{Aut}_F(A)$: Clearly $\mathrm{id}_A = G_1 \in Q$. Let $G_c, G_d \in Q$ for some invertible $c, d \in \mathrm{Nuc}(A)$, then

$$G_d(G_c(x)) = \big(d^{-1}((c^{-1}x)c)\big)d = (d^{-1}c^{-1}x)cd = (cd)^{-1}xcd = G_{cd}(x)$$

for all $x \in A$ and so Q is closed under composition. Finally $G_c \circ G_{c^{-1}} = G_1 = \mathrm{id}$, therefore Q is also closed under inverses since $c^{-1} \in \mathrm{Nuc}(A)$. Thus Q is a subgroup of $\mathrm{Aut}_F(A)$. □

In the case where A is a finite semifield, Proposition 5.7 was proven in [68, 2 Lemma]. By Proposition 5.7 we conclude:

Corollary 5.8. *Given $f(t) \in R = D[t;\sigma,\delta]$, the maps $G_c(x) = (c^{-1} \circ x) \circ c$ are inner automorphisms of S_f for all invertible $c \in \mathrm{Nuc}(S_f)$. In particular, if $f(t)$ is right semi-invariant the maps G_c are inner automorphisms of S_f for all $c \in D^\times$.*

Proof. The first assertion follows immediately from Proposition 5.7. We have $f(t) \in R$ is right semi-invariant is equivalent to $D \subseteq \mathrm{Nuc}_r(S_f)$ by Theorem 2.8, thus either S_f is associative or $\mathrm{Nuc}(S_f) = D \cap \mathrm{Nuc}_r(S_f) = D$. Therefore the maps G_c are inner automorphisms of S_f for all $c \in D^\times$. □

5.1 AUTOMORPHISMS OF S_f, $f(t) \in R = D[t;\delta]$

Now suppose D is an associative division ring of characteristic $p \neq 0$ and center C, $\sigma = \mathrm{id}$ and $0 \neq \delta$ is a derivation of D. In this Section we investigate the automorphisms of S_f in the special case where

$$f(t) = t^{p^e} + a_1 t^{p^{e-1}} + \ldots + a_e t + d \in R = D[t;\delta].$$

Here S_f is a nonassociative algebra over $F = C \cap \mathrm{Const}(\delta)$.

Recall from (3.14) that as D has characteristic p, we can write $(t-b)^p = t^p - V_p(b)$, where $V_p(b) = b^p + \delta^{p-1}(b) + *$ for all $b \in D$, with $*$ a sum of commutators of $b, \delta(b), \ldots, \delta^{p-2}(b)$. In particular, if $b \in C$ then $* = 0$ and $V_p(b) = b^p + \delta^{p-1}(b)$. An iteration yields $(t-b)^{p^e} = t^{p^e} - V_{p^e}(b)$, for all $b \in D$ with $V_{p^e}(b) = V_p^e(b) = V_p(\ldots(V_p(b)\ldots)$.

The automorphisms of R are described in Corollary 4.6. Together with Theorem 5.2, this leads us to the following result, which generalises [56, Proposition 7] in which $\tau = \mathrm{id}$:

Corollary 5.9. *Suppose $\tau \in \mathrm{Aut}_F(D)$ commutes with δ and*

$$f(t) = t^{p^e} + a_1 t^{p^{e-1}} + \ldots + a_e t + d \in R,$$

where $a_1, \ldots, a_e \in \mathrm{Fix}(\tau)$. Then for any $b \in C$ such that

$$V_{p^e}(b) + a_1 V_{p^{e-1}}(b) + \ldots + a_e b + d = \tau(d), \tag{5.2}$$

the map

$$H_{\tau,-b,1} : S_f \to S_f, \ \sum_{i=0}^{p^e-1} x_i t^i \mapsto \sum_{i=0}^{p^e-1} \tau(x_i)(t-b)^i, \tag{5.3}$$

is an F-automorphism of S_f.

Proof. The map

$$\Theta : R \to R, \ \sum_{i=0}^{n} b_i t^i \mapsto \sum_{i=0}^{n} \tau(b_i)(t-b)^i,$$

is an F-automorphism for all $b \in C$ by Corollary 4.6. Furthermore, a close inspection of the proof of Corollary 4.7 shows $\Theta(f(t)) = f(t)$ if and only if (5.2) holds, thus the assertion follows by Theorem 5.2. □

Let $f(t) = t^p - t - d \in R$, then $H_{\tau,-b,1} \in \mathrm{Aut}_F(S_f)$ for all $b \in C$, $\tau \in \mathrm{Aut}_F(D)$ such that $\tau \circ \delta = \delta \circ \tau$ and

$$\tau(d) = b - V_p(b) + d = b + d - b^p - \delta^{p-1}(b)$$

by Corollary 5.9. In addition, if $f(t)$ is not right invariant, δ commutes with all F-automorphisms of D and $F \subsetneq C$, these are the only F-automorphisms of S_f:

Theorem 5.10. *Let $f(t) = t^p - t - d \in R$. Then for all $\tau \in \mathrm{Aut}_F(D)$ and $b \in C$ such that τ commutes with δ and*

$$\tau(d) = b + d - b^p - \delta^{p-1}(b), \tag{5.4}$$

the maps $H_{\tau,-b,1}$ given by (5.3) *are F-automorphisms of S_f. Moreover, if $f(t)$ is not right invariant, δ commutes with all F-automorphisms of D and $F \subsetneq C$, these are all the automorphisms of S_f.*

Proof. Suppose $f(t)$ is not right invariant, $F \subsetneq C$ and $H \in \mathrm{Aut}_F(S_f)$. By Corollary 5.9 we are left to show H has the form $H_{\tau,-b,1}$ for some $\tau \in \mathrm{Aut}_F(D)$ and $b \in C$ satisfying (5.4).

Since $f(t)$ is not right invariant, S_f is not associative and $\mathrm{Nuc}_l(S_f) = D$ by Theorem 2.1. Any automorphism of S_f must preserve the left nucleus, thus

$H(D) = D$ and so $H|_D = \tau$ for some $\tau \in \mathrm{Aut}_F(D)$. Write $H(t) = \sum_{i=0}^{p-1} b_i t^i$ for some $b_i \in D$, then we have

$$H(t \circ z) = H(t) \circ H(z) = \sum_{i=0}^{p-1} b_i t^i \circ \tau(z) = \sum_{i=0}^{p-1} \sum_{j=0}^{i} \binom{i}{j} b_i \delta^{i-j}(\tau(z)) t^j, \quad (5.5)$$

and

$$H(t \circ z) = H(zt + \delta(z)) = \tau(z) \sum_{i=0}^{p-1} b_i t^i + \tau(\delta(z)), \quad (5.6)$$

for all $z \in D$. Comparing the coefficients of t^{p-2} in (5.5) and (5.6) we obtain

$$\tau(z) b_{p-2} = b_{p-2}\tau(z) + \binom{p-1}{p-2} b_{p-1} \delta(\tau(z)),$$

for all $z \in D$. In particular,

$$\binom{p-1}{p-2} b_{p-1} \delta(\tau(z)) = 0,$$

for all $z \in C$, therefore $b_{p-1} = 0$ since $\binom{p-1}{p-2} \neq 0$ and $\delta(\tau(z)) = \tau(\delta(z)) \neq 0$ for all $z \in C$ with $z \notin \mathrm{Const}(\delta)$. Such a z exists because $F \subsetneq C$.

Similarly, looking in turn at the coefficients of $t^{p-3}, \ldots, t^2, t$ in (5.5) and (5.6) yields $b_{p-1} = b_{p-2} = \ldots = b_2 = 0$, and comparing the coefficients of t^0 in (5.5) and (5.6) we get

$$\tau(z) b_0 + \tau(\delta(z)) = b_0 \tau(z) + b_1 \delta(\tau(z)), \quad (5.7)$$

for all $z \in D$. In particular, this means $\tau(\delta(z)) = b_1 \tau(\delta(z))$ for all $z \in C$ since τ and δ commute. Hence $b_1 = 1$ as $F \subsetneq C$. We conclude $\tau(z) b_0 = b_0 \tau(z)$ for all $z \in D$ by (5.7), thus $b_0 \in C$ and so $H(t) = t - b$ for some $b \in C$.

We now show H has the form (5.3): We have

$$H(z \circ t^i) = H(z) \circ H(t)^i = \tau(z)(t-b)^i,$$

for all $i \in \{1, \ldots, m-1\}$, $z \in D$, and so H has the form $H_{\tau,-b,1}$ for some $b \in C$. Moreover, with $t^p = t \circ t^{p-1}$, also

$$H(t^p) = H(t+d) = t - b + \tau(d), \quad (5.8)$$

and $H(t \circ t^{p-1}) = H(t) \circ H(t)^{p-1}$, i.e.

$$\begin{aligned} H(t^p) &= H(t) \circ H(t)^{p-1} = (t-b)^p \bmod_r f \\ &= t^p - V_p(b) \bmod_r f = t + d - V_p(b). \end{aligned} \tag{5.9}$$

Comparing (5.8) and (5.9) gives

$$\tau(d) = d - V_p(b) + b = b + d - b^p - \delta^{p-1}(b), \tag{5.10}$$

and thus H has the form $H_{\tau,-b,1}$, where $\tau \in \mathrm{Aut}_F(D)$ and $b \in C$ satisfy (5.10). $\square$

When $f(t) = t^p - t - d \in R$, we see $H_{\mathrm{id},-1,1} \in \mathrm{Aut}_F(S_f)$ by Theorem 5.10. Additionally, a straightforward calculation shows $H^i_{\mathrm{id},-1,1}(t) = t - i$ for all $i \in \mathbb{N}$, therefore since $\mathrm{Char}(D) = p$, we have $H^i_{\mathrm{id},-1,1} \neq \mathrm{id}$ for all $i \in \{1, \dots, p-1\}$. Furthermore

$$\Theta : R \to R : \sum_{i=0}^{n} b_i t^i \mapsto \sum_{i=0}^{n} b_i (t-1)^i$$

is an automorphism of order p [3, p. 90], thus $\langle H_{\mathrm{id},-1,1} \rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(S_f)$ of order p [56, Lemma 9].

Notice the equation (5.4) in Theorem 5.10 is remarkably similar to (3.17) in Proposition 3.30. Comparing them yields a connection between the automorphisms of S_f and factors of certain differential polynomials:

Proposition 5.11. *Let $\tau \in \mathrm{Aut}_F(D)$, $f(t) = t^p - t - d \in R$ and $g(t) = t^p - t - (d - \tau(d)) \in R$.*

(i) Suppose τ commutes with δ. If $b \in C^\times$ is such that $(t-b)|_r g(t)$, then $H_{\tau,-b,1} \in \mathrm{Aut}_F(S_f)$.

(ii) Given $b \in C^\times$, if $(t-b)|_r(t^p - t)$ then $H_{\mathrm{id},-b,1} \in \mathrm{Aut}_F(S_f)$.

(iii) Suppose $f(t)$ is not right invariant, δ commutes with all F-automorphisms of D and $F \subsetneq C$. Then $H_{\tau,-b,1} \in \mathrm{Aut}_F(S_f)$ if and only if $b \in C^\times$ and $(t-b)|_r g(t)$. In particular, if $b \in C^\times$ then $H_{\mathrm{id},-b,1} \in \mathrm{Aut}_F(S_f)$ if and only if $(t-b)|_r(t^p - t)$.

(iv) *Suppose $f(t)$ is not right invariant, δ commutes with all F-automorphisms of D and $F \subsetneq C$. If $g(t)$ is irreducible then $H_{\tau,-b,1} \notin \mathrm{Aut}_F(S_f)$ for all $b \in C^\times$.*

Proof. (i) We have $(t-b)|_r g(t)$ is equivalent to $V_p(b) - b - d + \tau(d) = 0$ by Proposition 3.30. As τ commutes with δ and $b \in C^\times$, this yields $H_{\tau,-b,1} \in \mathrm{Aut}_F(S_f)$ by Theorem 5.10.

(ii) follows by setting $\tau = \mathrm{id}$ in (i).

(iii) If $f(t)$ is not right invariant and $F \subsetneq C$, then $H_{\tau,-b,1} \in \mathrm{Aut}_F(S_f)$ if and only if τ commutes with δ, $b \in C^\times$ and $\tau(d) = b - V_p(b) + d$ by Theorem 5.10. Now $(t-b)|_r g(t)$ is equivalent to $V_p(b) - b - d + \tau(d) = 0$ by Proposition 3.30 and the assertion follows.

(iv) If $g(t)$ is irreducible then in particular, $(t-b) \nmid_r g(t)$ for all $b \in C^\times$ and the assertion follows by (iii).

□

5.2 AUTOMORPHISMS OF S_f, $f(t) \in R = D[t;\sigma]$

Now suppose D is an associative division ring with center C, $\mathrm{Char}(D)$ is arbitrary, σ is a non-trivial automorphism of D and $f(t) \in R = D[t;\sigma]$. Thus S_f is a nonassociative algebra over $F = C \cap \mathrm{Fix}(\sigma)$. Throughout this Section, if we assume σ has order $\geq m-1$ we include infinite order. From Theorem 4.9 we obtain:

Theorem 5.12. *Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$.*

(i) *For every $k \in C^\times$ such that*

$$a_i = \Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big) a_i, \tag{5.11}$$

for all $i \in \{0, \ldots, m-1\}$, the maps

$$H_{\mathrm{id},k} : \sum_{i=0}^{m-1} x_i t^i \mapsto x_0 + \sum_{i=1}^{m-1} x_i \big(\prod_{l=0}^{i-1} \sigma^l(k)\big) t^i, \tag{5.12}$$

are F-automorphisms of S_f. Furthermore

$$\{H_{\mathrm{id},k} \mid k \in K^\times \textit{ satisfies } (5.11) \textit{ for all } i \in \{0,\dots,m-1\}\}$$

is a subgroup of $\mathrm{Aut}_F(S_f)$.

(ii) *For every $\tau \in \mathrm{Aut}_F(D)$ and $k \in C^\times$ such that τ commutes with σ and*

$$\tau(a_i) = \Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big) a_i, \tag{5.13}$$

for all $i \in \{0,\dots,m-1\}$, the maps

$$H_{\tau,k} : \sum_{i=0}^{m-1} x_i t^i \mapsto \tau(x_0) + \sum_{i=1}^{m-1} \tau(x_i)\big(\prod_{l=0}^{i-1} \sigma^l(k)\big) t^i, \tag{5.14}$$

are F-automorphisms of S_f. Moreover

$$\{H_{\tau,k} \mid \tau \in \mathrm{Aut}_F(D),\ \tau\circ\sigma = \sigma\circ\tau,\ k \in K^\times \textit{ satisfies } (5.13) \textit{ for all } i\}$$

is a subgroup of $\mathrm{Aut}_F(S_f)$.

(iii) *Suppose $f(t)$ is not right invariant, σ commutes with all F-automorphisms of D and $\sigma|_C$ has order at least $m-1$. A map $H : S_f \to S_f$ is an F-automorphism of S_f if and only if H has the form $H_{\tau,k}$, where $\tau \in \mathrm{Aut}_F(D)$ and $k \in C^\times$ are such that* (5.13) *holds for all $i \in \{0,\dots,m-1\}$.*

Proof. Note that the inverse of $H_{\tau,k}$ is $H_{\tau^{-1},\tau^{-1}(k^{-1})}$ and $H_{\tau,k} \circ H_{\rho,b} = H_{\tau\rho,\tau(b)k}$. The rest of the proof is trivial using Theorem 4.9.

□

The automorphisms $H_{\tau,k}$ in Theorem 5.12 are restrictions of automorphisms

$$\Theta : R \to R,\ \sum_{i=0}^{n} b_i t^i \mapsto \sum_{i=0}^{n} \tau(b_i)(kt)^i,$$

by the proof of Theorem 4.9. If $f(t)$ is not right invariant, σ commutes with all F-automorphisms of D and $\sigma|_C$ has order at least $m-1$, then Theorem 5.12(iii) shows that all F-automorphisms of S_f are restrictions of automorphisms of R. Conversely, when $\sigma|_C$ has order $< m-1$ and σ commutes with all F-automorphisms of D, the automorphisms $H_{\tau,k}$ are restrictions of automorphisms of R and form a subgroup of $\mathrm{Aut}_F(S_f)$. Moreover we have:

Proposition 5.13. *Suppose $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ is not right invariant, σ commutes with all F-automorphisms of D and $\sigma|_C$ has order $n < m-1$. Let $H \in \mathrm{Aut}_F(S_f)$ and $N = \mathrm{Nuc}_r(S_f)$. Then $H|_D = \tau$ for some $\tau \in \mathrm{Aut}_F(D)$, $H_N \in \mathrm{Aut}_F(N)$ and $H(t) = g(t)$ with*

$$g(t) = k_1 t + k_{1+n} t^{1+n} + k_{1+2n} t^{1+2n} + \ldots + k_{1+sn} t^{1+sn}, \tag{5.15}$$

for some $k_{1+ln} \in D$.

Proof. Let $H : S_f \to S_f$ be an automorphism. Then $H|_N \in \mathrm{Aut}_F(N)$ and $H|_D = \tau$ for some $\tau \in \mathrm{Aut}_F(D)$ by Lemma 5.1.

Suppose $H(t) = \sum_{i=0}^{m-1} k_i t^i$ for some $k_i \in D$. Comparing the coefficients of t in $H(t \circ z) = H(t) \circ H(z) = H(\sigma(z)t)$ we obtain $k_i = 0$ or $\sigma^i(z) = \sigma(z)$, for all $i \in \{0, \ldots, m-1\}$ and all $z \in C$. Now, since $\sigma|_C$ has order $n < m-1$, $\sigma^i(z) = \sigma(z)$ for all $z \in C$ if and only if $i = 1 + nl$ for some $l \in \mathbb{Z}$. Therefore $k_i = 0$ for every $i \neq 1 + nl$, $l \in \mathbb{N} \cup \{0\}$, $i \in \{0, \ldots, m-1\}$ and hence $H(t)$ has the form (5.15) for some s with $sn < m-1$. □

Suppose σ commutes with all F-automorphisms of D and $\sigma|_C$ has order at least $m-1$, then the automorphism groups of S_f for $f(t) = t^m - a \in R$ not right invariant, are essential to understanding the automorphism groups of all the algebras S_g, as for all nonassociative S_g with $g(t) = t^m - \sum_{i=0}^{m-1} b_i t^i \in R$ and $b_0 = a$, $\mathrm{Aut}_F(S_g)$ is a subgroup of $\mathrm{Aut}_F(S_f)$:

Theorem 5.14. *Suppose σ commutes with all F-automorphisms of D and $\sigma|_C$ has order at least $m-1$. Let $g(t) = t^m - \sum_{i=0}^{m-1} b_i t^i \in R$ not be right invariant.*

(i) If $f(t) = t^m - b_0 \in R$ is not right invariant, then $\mathrm{Aut}_F(S_g)$ is a subgroup of $\mathrm{Aut}_F(S_f)$.

(ii) If $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ is not right invariant and $a_j \in \{0, b_j\}$ for all $j \in \{0, \ldots, m-1\}$, then $\mathrm{Aut}_F(S_g)$ is a subgroup of $\mathrm{Aut}_F(S_f)$.

If additionally all automorphisms of S_g are extensions of the identity, i.e. have the form $H_{\mathrm{id},k}$ for some $k \in C^\times$, then $\mathrm{Aut}_F(S_g)$ is a normal subgroup of $\mathrm{Aut}_F(S_f)$.

Proof. (i) Let $H \in \mathrm{Aut}_F(S_g)$, then H has the form $H_{\tau,k}$ where $\tau \in \mathrm{Aut}_F(D)$ and $k \in C^\times$ satisfy $\tau(b_i) = \big(\prod_{l=i}^{m-1} \sigma^l(k)\big) b_i$ for all $i \in \{0,\dots,m-1\}$ by Theorem 5.12(iii). In particular, $\tau(b_0) = \Big(\prod_{l=0}^{m-1} \sigma^l(k)\Big) b_0$, thus $H_{\tau,k}$ is also an automorphism of S_f, again by Theorem 5.12(iii). Therefore $\mathrm{Aut}_F(S_g) \leq \mathrm{Aut}_F(S_f)$.

Suppose additionally that all automorphisms of S_g are extensions of the identity. Let $H_{\rho,k} \in \mathrm{Aut}_F(S_f)$, $H_{\mathrm{id},z} \in \mathrm{Aut}_F(S_g)$ for some $\rho \in \mathrm{Aut}_F(D)$ and $k, z \in C^\times$. The inverse of $H_{\rho,k}$ is $H_{\rho^{-1},\rho^{-1}(k^{-1})}$, furthermore

$$\begin{aligned}
&H_{\rho,k}\Big(H_{\mathrm{id},z}\Big(H_{\rho^{-1},\rho^{-1}(k^{-1})}\Big(\sum_{i=0}^{m-1} x_i t^i\Big)\Big)\Big)\\
&\quad = H_{\rho,k}\Big(H_{\mathrm{id},z}\Big(\rho^{-1}(x_0) + \sum_{i=1}^{m-1} \rho^{-1}(x_i)\big(\prod_{l=0}^{i-1} \sigma^l(\rho^{-1}(k^{-1}))\big)t^i\Big)\Big)\\
&\quad = H_{\rho,k}\Big(\rho^{-1}(x_0) + \sum_{i=1}^{m-1} \rho^{-1}(x_i)\big(\prod_{l=0}^{i-1} \sigma^l(\rho^{-1}(k^{-1}))\big)\big(\prod_{l=0}^{i-1} \sigma^l(z)\big)t^i\Big)\\
&\quad = x_0 + \sum_{i=1}^{m-1} x_i\big(\prod_{l=0}^{i-1} \rho(\sigma^l(z))\big)t^i = x_0 + \sum_{i=1}^{m-1} x_i\big(\prod_{l=0}^{i-1} \sigma^l(\rho(z))\big)t^i\\
&\quad = H_{\mathrm{id},\rho(z)}\Big(\sum_{i=0}^{m-1} x_i t^i\Big),
\end{aligned}$$

because σ and ρ commute. Therefore if we show $H_{\mathrm{id},\rho(z)} \in \mathrm{Aut}_F(S_g)$, then indeed $\mathrm{Aut}_F(S_g)$ is a normal subgroup of $\mathrm{Aut}_F(S_f)$.

As $H_{\mathrm{id},z} \in \mathrm{Aut}_F(S_g)$, Theorem 5.12(iii) implies $\prod_{l=i}^{m-1} \sigma^l(z) = 1$, for all $i \in \{0,\dots,m-1\}$ such that $b_i \neq 0$. Applying ρ and using that σ and ρ commute, we obtain

$$\rho(1) = 1 = \rho\Big(\prod_{l=i}^{m-1} \sigma^l(z)\Big) = \prod_{l=i}^{m-1} \sigma^l(\rho(z)),$$

for all $i \in \{0,\dots,m-1\}$ such that $b_i \neq 0$. Thus

$$b_i = \Big(\prod_{l=i}^{m-1} \sigma^l(\rho(z))\Big) b_i,$$

for all $i \in \{0,\dots,m-1\}$ and hence $H_{\mathrm{id},\rho(z)} \in \mathrm{Aut}_F(S_g)$ by Theorem 5.12.

(ii) The proof is analogous to (i).

$\square$

5.2.1 *Cyclic Subgroups of* $\mathrm{Aut}_F(S_f)$

We now give some conditions for $\mathrm{Aut}_F(S_f)$ to have cyclic subgroups of certain order. In the special case when the coefficients of $f(t)$ are contained in F we obtain the following:

Proposition 5.15. *Let* $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in F[t;\sigma] \subseteq R$.

(i) If σ has finite order n, then $\langle H_{\sigma,1} \rangle \cong \mathbb{Z}/n\mathbb{Z}$ is a subgroup of $\mathrm{Aut}_F(S_f)$.

(ii) Suppose $D = K$ is a cyclic Galois field extension of F of prime degree m, $\mathrm{Gal}(K/F) = \langle \sigma \rangle$*, $a_0 \neq 0$ and not all $a_1, \dots, a_{m-1}$ are zero. Then* $\mathrm{Aut}_F(S_f) = \langle H_{\sigma,1} \rangle \cong \mathbb{Z}/m\mathbb{Z}$.

Proof. (i) Since $a_i \in F$, we have $\sigma(a_i) = a_i = \Big(\prod_{l=i}^{m-1} \sigma^l(1)\Big) a_i$, for all $i \in \{0, \dots, m-1\}$ and so $H_{\sigma,1} \in \mathrm{Aut}_F(S_f)$ by Theorem 5.12(ii). Furthermore, $H_{\sigma^j,1} \circ H_{\sigma^l,1} = H_{\sigma^{l+j},1}$ and $H_{\sigma^n,1} = H_{\mathrm{id},1}$, hence $\langle H_{\sigma,1} \rangle = \{H_{\mathrm{id},1}, H_{\sigma,1}, \dots, H_{\sigma^{n-1},1}\} \cong \mathbb{Z}/n\mathbb{Z}$ is a cyclic subgroup of order n.

(ii) The automorphisms of S_f are exactly the maps $H_{\sigma^j,k}$ for some $j \in \{0, \dots, m-1\}$ and $k \in K^\times$ such that

$$\sigma^j(a_i) = a_i = \Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big) a_i, \tag{5.16}$$

for all $i \in \{0, \dots, m-1\}$ by Theorem 5.12(iii). The maps $H_{\sigma^j,1}$ are therefore automorphisms of S_f for all $j \in \{0, \dots, m-1\}$. We show that these are all the automorphisms of S_f: We have $N_{K/F}(k) = 1$ because $a_0 \neq 0$, hence by Hilbert's Theorem 90, there exists $\alpha \in K$ such that $k = \sigma(\alpha)/\alpha$. Let $q \in \{1, \dots, m-1\}$ be such that $a_q \neq 0$, then

$$1 = \prod_{l=q}^{m-1} \sigma^l(k) = \prod_{l=q}^{m-1} \sigma^l\Big(\frac{\sigma(\alpha)}{\alpha}\Big) = \frac{\prod_{l=q+1}^{m} \sigma^l(\alpha)}{\prod_{l=q}^{m-1} \sigma^l(\alpha)} = \frac{\alpha}{\sigma^q(\alpha)},$$

by (5.16). This means $\alpha \in \mathrm{Fix}(\sigma^q) = F$ as m is prime. Therefore $k = \sigma(\alpha)/\alpha = \alpha/\alpha = 1$ as required.

$\square$

If F contains a primitive n^{th} root of unity for some $n \geq 2$, then there exist algebras S_f whose automorphism groups contain a cyclic subgroup of order n:

Theorem 5.16. *Let $f(t) = t^m - a \in R$. If $n|m$ and F contains a primitive n^{th} root of unity ω, then $\mathrm{Aut}_F(S_f)$ contains a cyclic subgroup of order n generated by $H_{\mathrm{id},\omega}$.*

Proof. We have $\omega\sigma(\omega)\cdots\sigma^{m-1}(\omega) = \omega^m = 1$ and thus $H_{\mathrm{id},\omega} \in \mathrm{Aut}_F(S_f)$ by Theorem 5.12(i). Notice H_{id,ω^j} is not the identity automorphism for all $j \in \{1, \dots, n-1\}$ and that $H_{\mathrm{id},\omega^n} = H_{\mathrm{id},1}$ is the identity. Furthermore

$$\begin{aligned} H_{\mathrm{id},\omega^j}\Big(H_{\mathrm{id},\omega^l}\Big(\sum_{i=0}^{m-1} x_i t^i\Big)\Big) &= H_{\mathrm{id},\omega^j}\Big(\sum_{i=0}^{m-1} x_i \omega^{li} t^i\Big) = \sum_{i=0}^{m-1} x_i \omega^{li}\omega^{ji} t^i \\ &= H_{\mathrm{id},\omega^{j+l}}\Big(\sum_{i=0}^{m-1} x_i t^i\Big), \end{aligned}$$

thus $H_{\mathrm{id},\omega^j} \circ H_{\mathrm{id},\omega^l} = H_{\mathrm{id},\omega^{j+l}}$ for all $j, l \in \{0, \dots, n-1\}$. This implies $\langle H_{\mathrm{id},\omega}\rangle = \{H_{\mathrm{id},1}, H_{\mathrm{id},\omega}, \dots, H_{\mathrm{id},\omega^{n-1}}\}$ is a cyclic subgroup. $\square$

Proposition 5.17. *Suppose F contains a primitive n^{th} root of unity ω and let $f(t) = t^{nm} - \sum_{i=0}^{m-1} a_{in} t^{in} \in R$. Then $\mathrm{Aut}_F(S_f)$ contains a cyclic subgroup of order n generated by $H_{\mathrm{id},\omega}$.*

Proof. We have

$$\Big(\prod_{l=in}^{nm-1} \sigma^l(\omega)\Big) a_{in} = \omega^{mn-in} a_{in} = a_{in},$$

for all $i \in \{0, \dots, m-1\}$ which implies $H_{\mathrm{id},\omega} \in \mathrm{Aut}_F(S_f)$ by Theorem 5.12(i). The rest of the proof is similar to Theorem 5.16. $\square$

F contains a primitive 2^{nd} root of unity whenever $\mathrm{Char}(F) \neq 2$, namely -1. Therefore setting $n = 2$ in Proposition 5.17 yields:

Corollary 5.18. *If $\mathrm{Char}(F) \neq 2$ and $f(t) = t^{2m} - \sum_{i=0}^{m-1} a_{2i} t^{2i} \in R$, then $\{H_{\mathrm{id},1}, H_{\mathrm{id},-1}\}$ is a subgroup of $\mathrm{Aut}_F(S_f)$ of order 2.*

5.2.2 Inner Automorphisms

In this subsection we consider the case where $\sigma|_C$ has finite order m, and look at the inner automorphisms of S_f.

Proposition 5.19. *Suppose $\sigma|_C$ has finite order m and $f(t) = t^m - a \in R$. Then the maps*

$$G_c : S_f \to S_f,\ \sum_{i=0}^{m-1} x_i t^i \mapsto \sum_{i=0}^{m-1} x_i c^{-1}\sigma^i(c) t^i,$$

are inner automorphisms for all $c \in C^\times$. Furthermore, $\{G_c \mid c \in C^\times\}$ is a non-trivial subgroup of $\mathrm{Aut}_F(S_f)$.

Proof. Let $c \in C^\times$, then $\prod_{l=0}^{i-1} \sigma^l\big(c^{-1}\sigma(c)\big) = c^{-1}\sigma^i(c)$ for all $i \geq 1$, thus $G_c = H_{\mathrm{id},k}$ where $k = c^{-1}\sigma(c)$. Moreover, we have

$$\prod_{l=0}^{m-1} \sigma^l(c^{-1}\sigma(c)) = c^{-1}\sigma^m(c) = c^{-1}c = 1,$$

and hence $G_c = H_{\mathrm{id},k} \in \mathrm{Aut}_F(S_f)$ by Theorem 5.12(i). A simple calculation shows $G_c\Big(\sum_{i=0}^{m-1} x_i t^i\Big) = \Big(c^{-1}\sum_{i=0}^{m-1} x_i t^i\Big)c$, and so G_c are inner automorphisms for all $c \in C^\times$.

A straightforward calculation shows $G_c \circ G_d = G_{cd}$ for all $c, d \in C^\times$, therefore $\{G_c \mid c \in C^\times\}$ is closed under composition. Additionally, we have $G_1 = \mathrm{id}_{S_f}$ and $G_c \circ G_{c^{-1}} = G_1$, hence $\{G_c \mid c \in C^\times\}$ forms a subgroup of $\mathrm{Aut}_F(S_f)$. Finally, G_c is not the identity for all $c \in C \setminus F$ which yields the assertion. □

Example 5.20. *We use the same set-up as in Hanke [27, p. 200]: Let $K = \mathbb{Q}(\alpha)$ where α is a root of $x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$. Then $K/\mathbb{Q}$ is a cyclic Galois field extension of degree* 3*, its Galois group is generated by $\tilde{\sigma} : \alpha \mapsto \alpha^2 - \alpha + 1$. Let also $L = K(\beta)$ where β is a root of $x^3 + (\alpha - 2)x^2 - (\alpha + 1)x + 1 \in K[x]$. Then L/K is a cyclic Galois field extension of degree* 3 *and there is $\tau \in \mathrm{Gal}(L/K)$ with $\tau(\beta) = \beta^2 + (\alpha - 2)\beta - \alpha$. Define $\pi = \alpha^2 + 2\alpha - 1 \in K$, then $D = (L/K, \tau, 2\pi)$ is an associative cyclic division algebra of degree* 3 *and $\tilde{\sigma}$ extends to an automorphism σ of D.*

Suppose $f(t) = t^3 - a \in D[t;\sigma]$ *and note that* $\mathrm{Cent}(D) = K$ *and* $\sigma|_K = \tilde{\sigma}$ *has order* 3*. Therefore* $\{G_c \mid c \in K^\times\}$ *is a non-trivial subgroup of* $\mathrm{Aut}_F(S_f)$ *consisting of inner automorphisms by Proposition 5.19.*

Corollary 5.21. *Suppose* $\sigma|_C$ *has finite order* m *and* $f(t) = t^m - a \in R$*. Let* $c \in C^\times$ *and suppose there exists* $j \in \mathbb{N}$ *such that* $c^j \in F$*. Let* j *be minimal. Then* $\langle G_c \rangle \cong \mathbb{Z}/j\mathbb{Z}$ *is a cyclic subgroup of* $\mathrm{Aut}_F(S_f)$ *consisting of inner automorphisms.*

Proof. The maps $G_c, G_{c^2}, \ldots$ are all automorphisms of S_f by Proposition 5.19, furthermore a straightforward calculation shows $G_{c^i} \circ G_{c^l} = G_{c^{i+l}}$ for all $i, l \in \mathbb{N}$. Notice $G_c^j = G_{c^j}$ is the identity automorphism if and only if $c^j \in F$, then by the minimality of j we conclude $\langle G_c \rangle = \{G_c, G_{c^2}, \ldots, G_{c^{j-1}}, \mathrm{id}\}$ is a cyclic subgroup. □

If D is finite-dimensional over C, then since $\sigma|_C$ has finite order m, σ has inner order m by the Skolem-Noether Theorem. That is σ^m is an inner automorphism $I_u : x \mapsto u^{-1}xu$ for some $u \in D^\times$, where we can choose $u \in D^\times$ such that $\sigma(u) = u$ [32, Theorem 1.1.22]. Given $f(t) = \sum_{j=0}^{n} a_j u^{n-j} t^{jm} \in D[t;\sigma]$ such that $a_n = 1$ and $a_j \in C$, then $f(t)$ is right semi-invariant by Theorem 2.11. Therefore as a direct consequence of Corollary 5.8, we obtain:

Corollary 5.22. *Suppose* σ *and* m *are as above, and let* $f(t) = \sum_{j=0}^{n} a_j u^{n-j} t^{jm} \in R$ *where* $a_n = 1$ *and* $a_j \in C$*. Then the maps*

$$G_c : S_f \to S_f, \ \sum_{i=0}^{mn-1} x_i t^i \mapsto \sum_{i=0}^{mn-1} c^{-1} x_i \sigma^i(c) t^i,$$

are inner automorphisms for all $c \in D^\times$*.*

5.2.3 *Necessary Conditions for* $H_{\tau,k} \in \mathrm{Aut}_F(S_f)$

We next take a closer look at the equality (5.13), to obtain necessary conditions for $\tau \in \mathrm{Aut}_F(D)$ to extend to $H_{\tau,k} \in \mathrm{Aut}_F(S_f)$. The more non-zero coefficients $f(t)$ has the more restrictive these conditions become.

Proposition 5.23. *Let $\sigma, \tau \in \mathrm{Aut}_F(D)$ and $k \in C^\times$ be such that (5.13) holds for all $i \in \{0, \dots, m-1\}$, i.e. $\tau(a_i) = \big(\prod_{l=i}^{m-1} \sigma^l(k)\big) a_i$ for all $i \in \{0, \dots, m-1\}$.*

(i) If $a_{m-1} \neq 0$ then

$$\tau(a_i) = \Big(\prod_{l=i}^{m-1} \sigma^{l-m+1}\big(\tau(a_{m-1})a_{m-1}^{-1}\big)\Big) a_i$$

for all $i \in \{0, \dots, m-1\}$.

(ii) If two consecutive $a_s, a_{s+1} \in \mathrm{Fix}(\tau)^\times$ then $k = 1$.

(iii) If $a_{m-1} \in \mathrm{Fix}(\tau)^\times$ then $k = 1$.

(iv) If there is $i \in \{0, \dots, m-1\}$ such that $a_i \in \mathrm{Fix}(\tau)^\times$ then $1 = \prod_{l=i}^{m-1} \sigma^l(k)$.

Proof. (i) Since $a_{m-1} \neq 0$, (5.13) implies $\tau(a_{m-1}) = \sigma^{m-1}(k) a_{m-1}$, hence $k = \sigma^{-m+1}\big(\tau(a_{m-1})a_{m-1}^{-1}\big)$. Subbing this back into (5.13) yields the assertion.

(ii) If there are two consecutive $a_s, a_{s+1} \in \mathrm{Fix}(\tau)^\times$, then by (5.13) we conclude $\prod_{l=s}^{m-1} \sigma^l(k) = 1 = \prod_{l=s+1}^{m-1} \sigma^l(k)$, thus cancelling gives $\sigma^s(k) = 1$, i.e. $k = 1$.

The proof of (iii) and (iv) is similar to [11, Proposition 9], but we need not assume D is a field:

(iii) Since $a_{m-1} \in \mathrm{Fix}(\tau)^\times$, (5.13) yields $\tau(a_{m-1}) = a_{m-1} = \sigma^{m-1}(k) a_{m-1}$, thus $\sigma^{m-1}(k) = 1$ and so $k = 1$.

(iv) We have $\tau(a_i) = a_i = \prod_{l=i}^{m-1} \sigma^l(k) a_i$ by (5.13), hence $1 = \prod_{l=i}^{m-1} \sigma^l(k)$. □

The condition (5.13) heavily restricts the choice of available k to $k = 1$ in many cases. Therefore in many instances we conclude $\mathrm{Aut}_F(S_f)$ is isomorphic to a subgroup of $\mathrm{Aut}_F(D)$ or is trivial:

Corollary 5.24. *Suppose $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ is not right invariant, σ commutes with all F-automorphisms of D and σ has order at least $m-1$. Suppose also that one of the following holds:*

(i) $a_{m-1} \neq 0$ *and there exists* $j \in \{0, \dots, m-2\}$ *such that*

$$\tau(a_j) \neq \Big(\prod_{l=j}^{m-1} \sigma^{l-m+1}\big(\tau(a_{m-1})a_{m-1}^{-1}\big)\Big) a_j,$$

for all $\mathrm{id} \neq \tau \in \mathrm{Aut}_F(D)$.

(ii) $a_{m-1} \in F^\times$ *and for all* $\mathrm{id} \neq \tau \in \mathrm{Aut}_F(D)$ *there exists* $j \in \{0, \dots, m-2\}$ *such that* $a_j \notin \mathrm{Fix}(\tau)$.

(iii) There are two consecutive $a_s, a_{s+1} \in F^\times$ *and for all* $\mathrm{id} \neq \tau \in \mathrm{Aut}_F(D)$ *there exists* $j \in \{0, \dots, m-1\}$ *such that* $a_j \notin \mathrm{Fix}(\tau)$.

Then $\mathrm{Aut}_F(S_f)$ *is trivial.*

Proof. Suppose $H \in \mathrm{Aut}_F(S_f)$, then $H = H_{\tau,k}$ for some $\tau \in \mathrm{Aut}_F(D)$ and $k \in C^\times$ satisfying (5.13) by Theorem 5.12.

(i) We have $\tau = \mathrm{id}$ by Proposition 5.23(i), therefore (5.13) implies $a_{m-1} = \sigma^{m-1}(k)a_{m-1}$. This means $k = 1$ and $H = H_{\mathrm{id},1}$ is trivial.

(ii) We have $k = 1$ by Proposition 5.23(iii), therefore (5.13) implies $\tau(a_i) = a_i$ for all $i \in \{0, \dots, m-1\}$ and thus $\tau = \mathrm{id}$. Therefore $H = H_{\mathrm{id},1}$ and $\mathrm{Aut}_F(S_f)$ is trivial.

(iii) Proposition 5.23(ii) yields $k = 1$, therefore by (5.13) we have $\tau(a_i) = a_i$ for all $i \in \{0, \dots, m-1\}$, hence $\tau = \mathrm{id}$ and $H = H_{\mathrm{id},1}$.

□

Denote by $\mathrm{Cent}_{\mathrm{Aut}(D)}(\sigma)$ the centralizer of σ in $\mathrm{Aut}_F(D)$. If the coefficients of $f(t)$ are all in F, we have:

Proposition 5.25. *Let* $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in F[t] = F[t;\sigma] \subset R$.

(i) $\{H_{\tau,1} \mid \tau \in \mathrm{Cent}_{\mathrm{Aut}(D)}(\sigma)\} \cong \mathrm{Cent}_{\mathrm{Aut}(D)}(\sigma)$ *is a subgroup of* $\mathrm{Aut}_F(S_f)$.

(ii) Suppose $f(t)$ *is not right invariant,* σ *commutes with all* F*-automorphisms of* D, $a_{m-1} \neq 0$ *and* $\sigma|_C$ *has order at least* $m-1$. *Then*

$$\mathrm{Aut}_F(S_f) = \{H_{\tau,1} \mid \tau \in \mathrm{Aut}_F(D)\} \cong \mathrm{Aut}_F(D).$$

Proof. (i) We have $\tau(a_i) = a_i = \Big(\prod_{l=i}^{m-1} \sigma^l(1)\Big)a_i$, for all $i \in \{0,\ldots,m-1\}$, $\tau \in \mathrm{Cent}_{\mathrm{Aut}(D)}(\sigma)$, therefore $\{H_{\tau,1} \mid \tau \in \mathrm{Cent}_{\mathrm{Aut}(D)}(\sigma)\}$ is a subset of $\mathrm{Aut}_F(S_f)$ by Theorem 5.12(ii). Furthermore, $H_{\tau,1} \circ H_{\rho,1} = H_{\tau\rho,1}$ for all $\tau,\rho \in \mathrm{Cent}_{\mathrm{Aut}(D)}(\sigma)$, hence $\{H_{\tau,1} \mid \tau \in \mathrm{Cent}_{\mathrm{Aut}(D)}(\sigma)\}$ is a subgroup of $\mathrm{Aut}_F(S_f)$ because $\mathrm{Cent}_{\mathrm{Aut}(D)}(\sigma)$ is a group.

(ii) In this case we prove the subgroup in (i) is all of $\mathrm{Aut}_F(S_f)$: Let $H \in \mathrm{Aut}_F(S_f)$, then H has the form $H_{\tau,k}$ for some $\tau \in \mathrm{Aut}_F(D)$, $k \in C^\times$ such that $\tau(a_i) = a_i = \Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big)a_i$, for all $i \in \{0,\ldots,m-1\}$ by Theorem 5.12(iii). In particular, $a_{m-1} = \sigma^{m-1}(k)a_{m-1}$ which implies $k = 1$ since $a_{m-1} \neq 0$. Thus $H = H_{\tau,1}$ as required.

□

Now suppose C/F is a proper field extension of finite degree, and D is finite-dimensional as an algebra over C and over F. Let $N_{D/C}$ denote the norm of D considered as an algebra over C, $N_{D/F}$ denote the norm of D considered as an algebra over F, and $N_{C/F}$ denote the norm of the field extension C/F. Recall $N_{D/F}(z) = N_{C/F}(N_{D/C}(z))$ for all $z \in D$ [31, §7.4] and $N_{D/F}(\tau(z)) = N_{D/F}(z)$ for all $\tau \in \mathrm{Aut}_F(D)$ and all $z \in D$ [47, p. 547]. Applying $N_{D/C}$ to (5.13) yields a necessary condition for $H_{\tau,k}$ to be an automorphism of S_f:

Proposition 5.26. *Suppose σ commutes with all F-automorphisms of D, $\sigma|_C$ has order at least $m-1$ and $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in D[t;\sigma]$ is not right invariant. If $H_{\tau,k} \in \mathrm{Aut}_F(S_f)$, then $N_{C/F}(k)$ is a $[D:C](m-i)$th root of unity for all $i \in \{0,\ldots,m-1\}$ such that $a_i \neq 0$. In particular, if D is commutative and $a_0 \neq 0$ then $N_{C/F}(k)$ is an mth root of unity.*

Proof. Applying $N_{D/F}$ to (5.13) we obtain

$$\begin{aligned} N_{D/F}(\tau(a_i)) = N_{D/F}(a_i) &= N_{D/F}\Big(\Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big)a_i\Big) \\ &= N_{D/F}(k)^{m-i} N_{D/F}(a_i) = N_{C/F}(k)^{[D:C](m-i)} N_{D/F}(a_i), \end{aligned}$$

for all $i \in \{0, \dots, m-1\}$ since $N_{D/F}(k) = N_{C/F}(N_{D/C}(k)) = N_{C/F}(k)^{[D:C]}$ for all $k \in C^\times$. This yields $N_{C/F}(k)^{[D:C](m-i)} = 1$ or $a_i = 0$ for every $i \in \{0, \dots, m-1\}$. □

5.2.4 *Connections Between Automorphisms of S_f, $f(t) = t^m - a \in D[t;\sigma]$, and Factors of Skew Polynomials*

Suppose D is an associative division ring with center C, σ is a non-trivial ring automorphism of D and $f(t) = t^m - a \in R = D[t;\sigma]$. We compare Theorem 5.12 and Proposition 3.2 to obtain connections between the automorphisms of S_f and factors of certain skew polynomials:

Proposition 5.27. *(i) Suppose $\tau \in \mathrm{Aut}_F(D)$ commutes with σ and $k \in C^\times$, then $H_{\tau,k} \in \mathrm{Aut}_F(S_f)$ if $(t-k)|_r(t^m - \tau(a)a^{-1})$.*

(ii) Suppose $(t-k)|_r(t^m - 1)$ for some $k \in C^\times$, then $H_{\mathrm{id},k} \in \mathrm{Aut}_F(S_f)$.

(iii) Suppose $f(t)$ is not right invariant, σ commutes with all F-automorphisms of D and $\sigma|_C$ has order at least $m-1$. If $k \in C^\times$ and $\tau \in \mathrm{Aut}_F(D)$, then $H_{\tau,k} \in \mathrm{Aut}_F(S_f)$ if and only if $(t-k)|_r(t^m - \tau(a)a^{-1})$. In particular, $H_{\mathrm{id},k} \in \mathrm{Aut}_F(S_f)$ if and only if $(t-k)|_r(t^m - 1)$.

Proof. (i) If $(t-k)|_r(t^m - \tau(a)a^{-1})$ then $\prod_{l=0}^{m-1} \sigma^l(k) = \tau(a)a^{-1}$ by Proposition 3.2, thus $H_{\tau,k} \in \mathrm{Aut}_F(S_f)$ by Theorem 5.12(i).

(ii) follows by setting $\tau = \mathrm{id}$ in (i).

(iii) If $(t-k)|_r(t^m - \tau(a)a^{-1})$ then $H_{\tau,k} \in \mathrm{Aut}_F(S_f)$ by (i). Conversely if $H_{\tau,k} \in \mathrm{Aut}_F(S_f)$, then $\tau(a) = \big(\prod_{l=0}^{m-1} \sigma^l(k)\big)a$ by Theorem 5.12(iii), and thus $(t-k)|_r(t^m - \tau(a)a^{-1})$ by Proposition 3.2.

□

When D is commutative, Proposition 5.27 shows there is an injective map between the monic linear right divisors of $t^m - 1$ in R and the automorphisms of S_f of the form $H_{\mathrm{id},k}$. If additionally $f(t)$ is not right invariant, σ

commutes with all F-automorphisms of D and σ has order at least $m-1$, then there is a bijection between the monic linear right divisors of $t^m - 1$ in R and the automorphisms of S_f of the form $H_{\mathrm{id},k}$.

Corollary 5.28. *Suppose σ commutes with all F-automorphisms of D, $f(t)$ is not right invariant, and $\sigma|_C$ has order at least $m-1$.*

(i) If all F-automorphisms of S_f have the form $H_{\mathrm{id},k}$ for some $k \in C^\times$, then $(t-b) \nmid_r (t^m - \tau(a)a^{-1})$, for all $\mathrm{id} \neq \tau \in \mathrm{Aut}_F(D)$, $b \in C^\times$. In addition, if D is commutative, m is prime and $\mathrm{Fix}(\sigma)$ contains a primitive m^{th} root of unity, then $t^m - \tau(a)a^{-1} \in R$ is irreducible for all $\mathrm{id} \neq \tau \in \mathrm{Aut}_F(D)$.

(ii) If $t^m - \tau(a)a^{-1} \in R$ is irreducible for all $\mathrm{id} \neq \tau \in \mathrm{Aut}_F(D)$, then

$$\mathrm{Aut}_F(S_f) = \Big\{ H_{\mathrm{id},k} \mid k \in C^\times \text{ such that } \prod_{l=0}^{m-1} \sigma^l(k) = 1 \Big\}.$$

Proof. (i) The first assertion follows immediately from Proposition 5.27. If D is commutative this means $(t-b) \nmid_r (t^m - \tau(a)a^{-1})$ for all $b \in D^\times$ and all $\mathrm{id} \neq \tau \in \mathrm{Aut}_F(D)$. If also $\mathrm{Fix}(\sigma)$ contains a primitive m^{th} root of unity, then $t^m - \tau(a)a^{-1} \in R$ is irreducible for all $\mathrm{id} \neq \tau \in \mathrm{Aut}_F(D)$ by Theorem 3.11.

(ii) Suppose $t^m - \tau(a)a^{-1} \in R$ is irreducible for all $\mathrm{id} \neq \tau \in \mathrm{Aut}_F(D)$, then in particular, $(t-b) \nmid_r (t^m - \tau(a)a^{-1})$ for all $b \in C^\times$, $\mathrm{id} \neq \tau \in \mathrm{Aut}_F(D)$. Therefore $H_{\tau,b} \notin \mathrm{Aut}_F(S_f)$ for all $b \in C^\times$, and all $\mathrm{id} \neq \tau \in \mathrm{Aut}_F(D)$ by Proposition 5.27 and so

$$\mathrm{Aut}_F(S_f) = \Big\{ H_{\mathrm{id},k} \mid k \in C^\times \text{ such that } \prod_{l=0}^{m-1} \sigma^l(k) = 1 \Big\}$$

by Theorem 5.12.

□

5.3 AUTOMORPHISMS OF JHA-JOHNSON SEMIFIELDS OBTAINED FROM SKEW POLYNOMIAL RINGS

In this Section we study the automorphism groups of the Jha-Johnson semifields which arise from Petit's algebra construction. Let $K = \mathbb{F}_{p^h}$ be a finite field of order p^h for some prime p and σ be a non-trivial $\mathbb{F}_p$-automorphism of K, i.e. $\sigma : K \to K$, $k \mapsto k^{p^r}$ for some $r \in \{1, \dots, h-1\}$ is a power of the Frobenius automorphism. Notice that $F = \mathrm{Fix}(\sigma) \cong \mathbb{F}_q$ where $q = p^{\gcd(r,h)}$, σ has order $n = h/\gcd(r,h)$, and σ commutes with all $\mathbb{F}_q$-automorphisms of K.

Suppose $f(t) \in R = K[t;\sigma]$ is monic and irreducible, so that S_f is a Jha-Johnson semifield [44, Theorem 15] (see Theorem 1.4). Recall that when $f(t) = t^m - a \in K[t;\sigma]$ is irreducible, $a \in K \setminus F$ and $n \geq m$, then S_f is called a Sandler semifield [58]. The automorphism groups of Sandler semifields are particularly relevant as for all Jha-Johnson semifields S_g with $g(t) = t^m - \sum_{i=0}^{m-1} b_i t^i \in K[t;\sigma]$ irreducible and $b_0 = a$, $\mathrm{Aut}_F(S_g)$ is a subgroup of $\mathrm{Aut}_F(S_f)$ by Theorem 5.14. We study the automorphisms of Sandler semifields in Section 5.3.1. When $m = n$, Sandler semifields are precisely the nonassociative cyclic algebras over F, and their automorphism groups are studied in detail in Chapter 6.

We remark that the results in this Section hold more generally when $f(t) \in R$ is not necessarily irreducible, here S_f is a nonassociative algebra over F, but S_f is not a semifield unless $f(t)$ is irreducible (Theorem 2.26).

Theorem 5.12 becomes:

Theorem 5.29. *Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in K[t;\sigma]$ and define $s_i = (p^{rm} - p^{ri})/(p^r - 1)$.*

(i) Suppose $k \in K^\times$ is an s_ith root of unity for all $i \in \{0, \dots, m-1\}$ with $a_i \neq 0$. Then $H_{\mathrm{id},k} \in \mathrm{Aut}_F(S_f)$.

(ii) Suppose $k \in K^\times$ and $j \in \{0, \dots, n-1\}$ are such that $\sigma^j(a_i) = k^{s_i} a_i$ for all $i \in \{0, \dots, m-1\}$, then $H_{\sigma^j,k} \in \mathrm{Aut}_F(S_f)$.

(iii) Suppose $f(t)$ is not right invariant and $n \geq m-1$. Then $H \in \mathrm{Aut}_F(S_f)$ if and only if $H = H_{\sigma^j,k}$ for some $k \in K^\times$, $j \in \{0,\dots,n-1\}$ such that $\sigma^j(a_i) = k^{s_i} a_i$ for all $i \in \{0,\dots,m-1\}$.

Proof. (i) We have

$$\Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big) a_i = \Big(\prod_{l=i}^{m-1} k^{p^{rl}}\Big) a_i = k^{s_i} a_i = a_i,$$

for all $i \in \{0,\dots,m-1\}$ and thus $H_{\mathrm{id},k} \in \mathrm{Aut}_F(S_f)$ by Theorem 5.12(i).

(ii) Similarly to (i) we have

$$\Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big) a_i = \Big(\prod_{l=i}^{m-1} k^{p^{rl}}\Big) a_i = k^{s_i} a_i = \sigma^j(a_i)$$

for all $i \in \{0,\dots,m-1\}$, and thus $H_{\sigma^j,k} \in \mathrm{Aut}_F(S_f)$ by Theorem 5.12(ii).

(iii) follows by (ii) and Theorem 5.12(iii).

□

As a direct consequence of Theorem 5.14, we have:

Corollary 5.30. *Let $n \geq m-1$ and $g(t) = t^m - \sum_{i=0}^{m-1} b_i t^i \in R$ not be right invariant.*

(i) If $f(t) = t^m - b_0 \in R$ is not right invariant then $\mathrm{Aut}_F(S_g)$ is a subgroup of $\mathrm{Aut}_F(S_f)$.

(ii) If $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ is not right invariant and $a_j \in \{0, b_j\}$ for all $j \in \{0,\dots,m-1\}$, then $\mathrm{Aut}_F(S_g)$ is a subgroup of $\mathrm{Aut}_F(S_f)$.

Proposition 5.15 becomes:

Corollary 5.31. *Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in F[t;\sigma] \subseteq K[t;\sigma]$. Then $\langle H_{\sigma,1}\rangle \cong \mathbb{Z}/n\mathbb{Z}$ is a cyclic subgroup of $\mathrm{Aut}_F(S_f)$.*

The Hughes-Kleinfeld semifields can be written in the form S_f for irreducible $f(t) \in K[t;\sigma]$ of degree 2 by Theorem 1.3. Setting $m = 2$ in Theorem 5.29 gives a description of the automorphisms of Hughes Kleinfeld semifields. In particular we obtain [64, Proposition 8.3.1] and [64, Corollary 8.3.6] as straightforward corollaries of Theorem 5.12(iii).

5.3.1 *Automorphisms of Sandler Semifields*

In this Subsection we study the automorphism group of S_f when $f(t) = t^m - a \in K[t;\sigma]$. In particular, when $a \in K \setminus F$ and σ has order $n \geq m$ this yields results on the automorphisms of Sandler semifields. Let

$$s = \frac{p^{rm} - 1}{p^r - 1}.$$

Theorem 5.29 implies:

Corollary 5.32. *Let $f(t) = t^m - a \in K[t;\sigma]$.*

(i) The set $\{H_{\mathrm{id},k} \mid k \in K,\ k^s = 1\}$ is a cyclic subgroup of $\mathrm{Aut}_F(S_f)$ of order $\gcd(s, p^h - 1)$.

(ii) If $p \equiv 1 \bmod m$, then there are at least m automorphisms of S_f of the form $H_{\mathrm{id},k}$. In particular, $\mathrm{Aut}_F(S_f)$ is not trivial.

(iii) Suppose h is even and at least one of r, m are even. If $p \equiv -1 \bmod m$, then there are at least m automorphisms of S_f of the form $H_{\mathrm{id},k}$. In particular, $\mathrm{Aut}_F(S_f)$ is not trivial.

(iv) Suppose p is an odd prime and $m = 2$. Then $\mathrm{Aut}_F(S_f)$ is not trivial.

Proof. (i) If $k \in K^\times$ is an s^{th} root of unity then $H_{\mathrm{id},k} \in \mathrm{Aut}_F(S_f)$ by Theorem 5.29(i). Moreover a straightforward calculation shows $H_{\mathrm{id},k} \circ H_{\mathrm{id},l} = H_{\mathrm{id},kl} \in \{H_{\mathrm{id},k} \mid k^s = 1\}$ for all s^{th} roots of unity $k, l \in K^\times$. This means $\{H_{\mathrm{id},k} \mid k^s = 1\}$ is isomorphic to the cyclic subgroup of $K^\times$ consisting of all s^{th} roots of unity. There are precisely $\gcd(s, p^h - 1)$ s^{th} roots of unity in K by [36, Proposition II.2.1] which yields the assertion.

(ii) We have $\gcd(s, p^h - 1) \geq m$ by the proof of Corollary 3.24, therefore there are at least m automorphisms of S_f of the form $H_{\mathrm{id},k}$ by (i).

(iii) We have $p^h \equiv (-1)^h \bmod m \equiv 1 \bmod m$ because h is even. If r is even then $p^r \equiv 1 \bmod m$ and

$$s \bmod m \equiv \Big(\sum_{i=0}^{m-1} (p^{ri} \bmod m) \Big) \bmod m \equiv \big(\sum_{i=0}^{m-1} 1 \big) \bmod m \equiv 0 \bmod m.$$

On the other hand, if r is odd then m must be even, therefore $p^r \equiv -1 \bmod m$ and

$$\begin{aligned} s \bmod m &\equiv \Big(\sum_{i=0}^{m-1} (p^{ri} \bmod m) \Big) \bmod m \\ &\equiv \big(\sum_{i=0}^{m-1} (-1)^i \big) \bmod m \equiv 0 \bmod m. \end{aligned}$$

In either case, $m | (p^h - 1)$ and $m | s$. Hence $\gcd(s, p^h - 1) \geq m$, so there are at least m automorphisms of S_f of the form $H_{\mathrm{id},k}$ by (i).

(iv) p is odd so $p \equiv 1 \bmod 2$ and the result follows by (ii).

□

Corollary 5.32(i) implies that if $\mathrm{Aut}_F(S_f)$ is trivial for a single $f(t) = t^m - a \in K[t;\sigma]$, then all $t^m - c \in K[t;\sigma]$, $c \in K$, are reducible: Indeed if $\mathrm{Aut}_F(S_f)$ is trivial then $\gcd(s, p^h - 1) = 1$ by Corollary 5.32(i), and so $t^m - c \in K[t;\sigma]$ is reducible for all $c \in K$ by Corollary 3.23.

Proposition 5.33. *Let $f(t) = t^m - a \in K[t;\sigma]$.*

(i) If $c \in K^\times$ is a $(p^{rm} - 1)$ root of unity, then the map

$$G_c : S_f \to S_f, \ \sum_{i=0}^{m-1} x_i t^i \mapsto \Big(c^{-1} \sum_{i=0}^{m-1} x_i t^i \Big) c,$$

is an inner automorphism of S_f.

(ii) If $p^{\gcd(rm,h)} - p^{\gcd(r,h)} > 0$, then there exists a non-trivial inner automorphism of S_f of the form G_c for some $c \in K^\times$ which is a $(p^{rm} - 1)$ root of unity, but not a $(p^r - 1)$ root of unity.

Proof. Let $k = c^{p^r - 1}$.

(i) We have $k^{(p^{rm}-1)/(p^r-1)} = 1$ and so $H_{\mathrm{id},k} \in \mathrm{Aut}_F(S_f)$ by Theorem 5.29(i). Furthermore

$$H_{\mathrm{id},k}\big(\sum_{i=0}^{m-1} x_i t^i \big) = x_0 + \sum_{i=1}^{m-1} x_i \Big(\prod_{l=0}^{i-1} \sigma^l(k) \Big) t^i = x_0 + \sum_{i=1}^{m-1} x_i \Big(\prod_{l=0}^{i-1} k^{p^{rl}} \Big) t^i$$

$$= x_0 + x_1 kt + \sum_{i=2}^{m-1} x_i k^{(p^{ri}-1)/(p^r-1)} t^i = \sum_{i=0}^{m-1} x_i c^{-1} \sigma^i(c) t^i$$
$$= \Big(c^{-1} \sum_{i=0}^{m-1} x_i t^i\Big) c,$$

so we conclude $H_{\mathrm{id},k} = G_c$ is an inner automorphism.

(ii) Notice $H_{\mathrm{id},k}$ is the identity if and only if $k = 1$, i.e. if and only if c is a $(p^r - 1)$th root of unity. Moreover every $(p^r - 1)$th root of unity c is also a $(p^{rm} - 1)$th root of unity because $(p^r - 1)|(p^{rm} - 1)$. Therefore if the number of $(p^{rm} - 1)$ roots of unity in K is strictly greater than the number of $(p^r - 1)$ roots of unity, then there exists a non-trivial automorphism of S_f of the form G_c for some $c \in K^\times$ which is a $(p^{rm} - 1)$ root of unity, but not a $(p^r - 1)$ root of unity.

Finally, the number of $(p^{rm} - 1)$ roots of unity in K is strictly greater than the number of $(p^r - 1)$ roots of unity if and only if

$$\gcd(p^{rm} - 1, p^h - 1) - \gcd(p^r - 1, p^h - 1) > 0,$$

if and only if

$$p^{\gcd(rm,h)} - 1 - (p^{\gcd(r,h)} - 1) = p^{\gcd(rm,h)} - p^{\gcd(r,h)} > 0$$

by Lemma 3.20.

□

When K contains a primitive $(p^{rm} - 1)^{\text{th}}$ primitive root of unity, Proposition 5.33 leads to:

Corollary 5.34. *Suppose $f(t) = t^m - a \in K[t;\sigma]$ and $(rm)|h$, then K contains a primitive $(p^{rm} - 1)$ root of unity c and $\mathrm{Aut}_F(S_f)$ contains a cyclic subgroup of inner automorphisms of order $(p^{rm} - 1)/(p^r - 1)$ generated by G_c.*

Proof. K contains a primitive $(p^{rm} - 1)$ root of unity if and only if $(p^{rm} - 1)|(p^h - 1)$ by [36, Proposition II.2.1], if and only if

$$p^{rm} - 1 = \gcd(p^{rm} - 1, p^h - 1) = p^{\gcd(rm,h)} - 1$$

by Lemma 3.20, if and only if $rm = \gcd(rm, h)$ if and only if $(rm)|h$. Let $c \in K^\times$ be a primitive $(p^{rm} - 1)$ root of unity, then G_c is a non-trivial inner automorphism of S_f by Proposition 5.33. Additionally, notice $k = c^{p^r - 1}$ is a primitive $(p^{rm} - 1)/(p^r - 1)$ root of unity and $G_c = H_{\mathrm{id},k}$ by the proof of Proposition 5.33. Thus $\langle G_c \rangle = \{G_c, G_{c^2}, \ldots, \mathrm{id}\}$ is a cyclic subgroup of $\mathrm{Aut}_F(S_f)$ of order $(p^{rm} - 1)/(p^r - 1)$. $\square$

Proposition 5.35. *Let $f(t) = t^m - a \in K[t;\sigma]$ and $l \in \mathbb{N}$ be such that $l|m$ and $l|(p^{\gcd(r,h)} - 1)$. Then F contains a primitive l^{th} root of unity ω and $\mathrm{Aut}_F(S_f)$ contains a cyclic subgroup of order l generated by $H_{\mathrm{id},\omega}$.*

Proof. F contains a primitive l^{th} root of unity is equivalent to $l|(p^{\gcd(r,h)} - 1)$, so the result follows by Theorem 5.16. $\square$

6

AUTOMORPHISMS OF NONASSOCIATIVE CYCLIC ALGEBRAS

Throughout this Chapter, let K/F be a cyclic Galois field extension of degree m with $\mathrm{Gal}(K/F) = \langle \sigma \rangle$, and

$$A = (K/F, \sigma, a) = K[t;\sigma]/K[t;\sigma](t^m - a)$$

be a nonassociative cyclic algebra of degree m for some $a \in K \setminus F$. Here A is not associative by Theorem 2.1(v).

In this Chapter we investigate the automorphisms of nonassociative cyclic algebras using results in Chapter 5 and those by Steele in [64, §6.3].

In particular, we will prove there always exist non-trivial inner automorphisms of a nonassociative cyclic algebra and find conditions for all automorphisms to be inner. These conditions are closely related to whether or not the field F contains a primitive m^{th} root of unity. We pay special attention to the case where K/F is an extension of finite fields in Section 6.2, and we completely determine the automorphism group of nonassociative cyclic algebras of prime degree different from $\mathrm{Char}(F)$.

The field norm $N_{K/F} : K \to F$ is given by $N_{K/F}(k) = \prod_{l=0}^{m-1} \sigma^l(k)$. Recall Hilbert's Theorem 90, which states $N_{K/F}(b) = 1$ if and only if $b = \sigma(c)c^{-1}$ for some $c \in K^\times$, thus $\mathrm{Ker}(N_{K/F}) = \Delta^\sigma(1)$, where $\Delta^\sigma(l) = \{\sigma(c)lc^{-1} \mid c \in K^\times\}$ is the **σ-conjugacy class** of $l \in K^\times$ [40].

In this case Theorem 5.12(iii) immediately becomes:

Corollary 6.1. *([64, Corollary 3.2.9]). A map $H : A \to A$ is an F-automorphism of A if and only if $H = H_{\sigma^j,k}$ for some $j \in \{0, \ldots, m-1\}$ and $k \in K^\times$ such that $\sigma^j(a) = N_{K/F}(k)a$, where $H_{\sigma^j,k}$ is defined as in* (5.14).

Corollary 6.1 leads us to the following Theorem on the inner automorphisms of nonassociative cyclic algebras:

Theorem 6.2. *(i) The maps*

$$G_c : A \to A,\ \sum_{i=0}^{m-1} x_i t^i \mapsto \sum_{i=0}^{m-1} x_i c^{-1} \sigma^i(c) t^i, \tag{6.1}$$

are inner automorphisms for all $c \in K^\times$.

(ii) Let $c \in K^\times$, then $G_c = H_{\mathrm{id},k}$ where $k = c^{-1}\sigma(c)$. Furthermore every $H_{\mathrm{id},l} \in \mathrm{Aut}_F(A)$ is inner and can be written in the form G_c for some $c \in K^\times$.

(iii) Let $c, d \in K^\times$, then $G_c = G_d$ if and only if $c^{-1}\sigma(c) = d^{-1}\sigma(d)$.

(iv) There exists a non-trivial inner automorphism of A. Therefore the automorphism group of A is not trivial.

(v) $N = \{G_c \mid c \in K^\times\} \cong \mathrm{Ker}(N_{K/F})$ is an abelian normal subgroup of $\mathrm{Aut}_F(A)$. In particular, $H \circ G_c \circ H^{-1}$ is inner for all $c \in K^\times$ and all $H \in \mathrm{Aut}_F(A)$.

(vi) If $\sigma^j(a)a^{-1} \notin N_{K/F}(K^\times)$ for all $j \in \{1, \ldots, m-1\}$ then

$$\mathrm{Aut}_F(A) = \{G_c \mid c \in K^\times\} \cong \mathrm{Ker}(N_{K/F}),$$

and all automorphisms of A are inner. In particular, $\mathrm{Aut}_F(A)$ is abelian.

(vii) Let $c \in K \setminus F$ and suppose there exists $j \in \mathbb{N}$ such that $c^j \in F^\times$. Let j be minimal. Then $\langle G_c \rangle \cong \mathbb{Z}/j\mathbb{Z}$ is a cyclic subgroup of $\mathrm{Aut}_F(A)$.

Proof. (i) A straightforward calculation shows

$$G_c\Big(\sum_{i=0}^{m-1} x_i t^i\Big) = \Big(c^{-1} \sum_{i=0}^{m-1} x_i t^i\Big) c,$$

for all $c \in K^\times$. Furthermore, $D = \mathrm{Nuc}(A)$ by Corollary 2.12 and hence G_c are inner automorphisms by Corollary 5.8.

(ii) If $k = c^{-1}\sigma(c)$, then

$$H_{\mathrm{id},k}\big(\sum_{i=0}^{m-1} x_i t^i\big) = x_0 + \sum_{i=1}^{m-1} x_i \Big(\prod_{l=0}^{i-1} \sigma^l(k)\Big) t^i$$
$$= x_0 + \sum_{i=1}^{m-1} x_i c^{-1} \sigma^i(c) t^i = G_c\big(\sum_{i=0}^{m-1} x_i t^i\big),$$

and thus $G_c = H_{\mathrm{id},k}$. Suppose $H_{\mathrm{id},l} \in \mathrm{Aut}_F(A)$ for some $l \in K^\times$, then $N_{K/F}(l) = 1$ by Corollary 6.1 and so there exists $c \in K^\times$ such that $l = c^{-1}\sigma(c)$ by Hilbert 90. This means $H_{\mathrm{id},l} = G_c$ by the above calculation.

(iii) Let $k = c^{-1}\sigma(c)$ and $l = d^{-1}\sigma(d)$, so that $G_c = H_{\mathrm{id},k}$ and $G_d = H_{\mathrm{id},l}$ by (ii). Therefore $G_c = G_d$ if and only if $H_{\mathrm{id},k} = H_{\mathrm{id},l}$ if and only if $k = l$.

(iv) G_c is a non-trivial inner automorphism of A for all $c \in K \setminus F$.

(v) Note $N = \{H_{\mathrm{id},k} \mid k \in \mathrm{Ker}(N_{K/F})\}$ by (ii) and Corollary 6.1 and N is a subgroup of $\mathrm{Aut}_F(A)$ by Theorem 5.12(i). Furthermore, a straightforward calculation shows $G_c \circ G_d = G_{cd} = G_{dc} = G_d \circ G_c$, for all $c, d \in K^\times$, i.e. N is abelian. We are left to prove N is a normal subgroup of $\mathrm{Aut}_F(A)$: Let $c \in K^\times$ and $H \in \mathrm{Aut}_F(A)$. Then $H = H_{\sigma^j,k}$ for some $j \in \{0, \ldots, m-1\}$, $k \in K^\times$ such that $\sigma^j(a) = N_{K/F}(k)a$ by Corollary 6.1. Additionally the inverse of $H_{\sigma^j,k}$ is $H_{\sigma^{-j},\sigma^{-j}(k^{-1})}$, and we have

$$H_{\sigma^j,k}\Big(G_c\Big(H^{-1}_{\sigma^j,k}\big(\sum_{i=0}^{m-1} x_i t^i\big)\Big)\Big)$$
$$= H_{\sigma^j,k}\Big(G_c\Big(\sigma^{-j}(x_0) + \sum_{i=1}^{m-1} \sigma^{-j}(x_i)\big(\prod_{l=0}^{i-1} \sigma^{l-j}(k^{-1})\big) t^i\Big)\Big)$$
$$= H_{\sigma^j,k}\Big(\sigma^{-j}(x_0) + \sum_{i=1}^{m-1} \sigma^{-j}(x_i)\big(\prod_{l=0}^{i-1} \sigma^{l-j}(k^{-1})\big) c^{-1}\sigma^i(c) t^i\Big)$$
$$= x_0 + \sum_{i=1}^{m-1} x_i \big(\prod_{l=0}^{i-1} \sigma^l(k^{-1})\big) \sigma^j(c^{-1}) \sigma^{i+j}(c) \big(\prod_{l=0}^{i-1} \sigma^l(k)\big) t^i$$
$$= x_0 + \sum_{i=1}^{m-1} x_i \sigma^j(c^{-1}) \sigma^{j+i}(c) t^i = G_{\sigma^j(c)}\Big(\sum_{i=0}^{m-1} x_i t^i\Big),$$

hence $H_{\sigma^j,k} \circ G_c \circ H^{-1}_{\sigma^j,k} = G_{\sigma^j(c)} \in N$ which yields the assertion.

(vi) Here $\mathrm{Aut}_F(A) = \{H_{\mathrm{id},k} \mid k \in \mathrm{Ker}(N_{K/F})\}$ by Corollary 6.1 and hence the result follows by (ii) and (iii).

(vii) This is just Corollary 5.21.

□

In some instances, $\mathrm{Aut}_F(A)$ is a non-abelian group:

Proposition 6.3. *Suppose $H_{\sigma^j,k} \in \mathrm{Aut}_F(A)$ for some $j \in \{1,\dots,m-1\}$ and $k \in K^\times$. If there exists $c \in K^\times$ and $i \in \{1,\dots,m-1\}$ such that $c^{-1}\sigma^i(c) \notin \mathrm{Fix}(\sigma^j)$, then $\mathrm{Aut}_F(A)$ is a non-abelian group.*

Proof. We have

$$H_{\sigma^j,k}(G_c(t^i)) = H_{\sigma^j,k}\big(c^{-1}\sigma^i(c)t^i\big) = \sigma^j\big(c^{-1}\sigma^i(c)\big)\Big(\prod_{l=0}^{i-1}\sigma^l(k)\Big)t^i,$$

and

$$G_c(H_{\sigma^j,k}(t^i)) = G_c\Big(\Big(\prod_{l=0}^{i-1}\sigma^l(k)\Big)t^i\Big) = \Big(\prod_{l=0}^{i-1}\sigma^l(k)\Big)c^{-1}\sigma^i(c)t^i,$$

for all $i \in \{1,\dots,m-1\}$. Thus if there exists $i \in \{1,\dots,m-1\}$ such that $c^{-1}\sigma^i(c) \notin \mathrm{Fix}(\sigma^j)$, then $G_c \circ H_{\sigma^j,k} \neq H_{\sigma^j,k} \circ G_c$ and $\mathrm{Aut}_F(A)$ is not abelian.

□

We now take a closer look at the inner automorphisms in the case where F does not contain certain primitive roots of unity:

Theorem 6.4. *Suppose $a \in K^\times$ does not lie in any proper subfield of K and F does not contain a non-trivial m^{th} root of unity. Then*

$$\mathrm{Aut}_F(A) = \{G_c \mid c \in K^\times\} \cong \mathrm{Ker}(N_{K/F}),$$

and all automorphisms of A are inner.

Proof. We first prove every automorphism of A has the form $H_{\mathrm{id},k}$, then

$$\mathrm{Aut}_F(A) = \{G_c \mid c \in K^\times\} \cong \mathrm{Ker}(N_{K/F}),$$

by Theorem 6.2 and all automorphisms of A are inner. Suppose, for a contradiction, that there exists $j \in \{1, \dots, m-1\}$ and $k \in K^\times$ such that $H_{\sigma^j,k} \in \mathrm{Aut}_F(A)$. This implies $H^2_{\sigma^j,k} = H_{\sigma^j,k} \circ H_{\sigma^j,k} \in \mathrm{Aut}_F(A)$, and

$$H^2_{\sigma^j,k}\Big(\sum_{i=0}^{m-1} x_i t^i\Big) = \sigma^{2j}(x_0) + \sum_{i=1}^{m-1} \sigma^{2j}(x_i)\Big(\prod_{q=0}^{i-1} \sigma^{j+q}(k)\sigma^q(k)\Big)t^i. \tag{6.2}$$

Now $H^2_{\sigma^j,k}$ must have the form $H_{\sigma^{2j},l}$ for some $l \in K^\times$ by Corollary 6.1, and comparing (5.14) and (6.2) yields $l = k\sigma^j(k)$. Similarly, $H^3_{\sigma^j,k} = H_{\sigma^{3j},s} \in \mathrm{Aut}_F(A)$ where $s = k\sigma^j(k)\sigma^{2j}(k)$. Continuing in this manner we conclude the maps $H_{\sigma^j,k}, H_{\sigma^{2j},l}, H_{\sigma^{3j},s}, \dots$ are all F-automorphisms of A, therefore

$$\begin{aligned} \sigma^j(a) &= N_{K/F}(k)a, \\ \sigma^{2j}(a) &= N_{K/F}(k\sigma^j(k))a = N_{K/F}(k)^2 a, \\ &\ \vdots \qquad\qquad \vdots \\ a = \sigma^{nj}(a) &= N_{K/F}(k)^n a, \end{aligned} \tag{6.3}$$

by Corollary 6.1, where $n = m/\mathrm{gcd}(j, m)$ is the order of σ^j.

Note that $\sigma^{ij}(a) \neq a$ for all $i \in \{1, \dots, n-1\}$ since a is not contained in any proper subfield of K. Therefore $N_{K/F}(k)^n = 1$ and $N_{K/F}(k)^i \neq 1$ for all $i \in \{1, \dots, n-1\}$ by (6.3), i.e. $N_{K/F}(k)$ is a primitive n^{th} root of unity, thus also an m^{th} root of unity, a contradiction. □

Example 6.5. *Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\theta)$ where θ is a root of $T(y) = y^3 + y^2 - 2y - 1 \in F[y]$. Then K/F is a cubic cyclic Galois field extension, its Galois group is generated by σ where $\sigma(\theta) = -\theta^2 - \theta + 1$ [27, p. 199]. Suppose $A = (K/F, \sigma, a)$ for some $a \in K \setminus F$. As F does not contain a non-trivial 3^{rd} root of unity, Theorem 6.4 implies $\mathrm{Aut}_F(A) = \{G_c \mid c \in K^\times\} \cong \mathrm{Ker}(N_{K/F})$, and all automorphisms of A are inner.*

We now investigate the automorphisms of A in the case when F contains a primitive m^{th} root of unity. It is well-known that if F contains a primitive m^{th} root of unity and K/F is cyclic of degree m (where m and $\mathrm{Char}(F)$ are coprime), then $K = F(d)$ where d is a root of the irreducible polynomial $x^m - e \in F[x]$ for some $e \in F^\times$ [43, §VI.6].

Lemma 6.6. *Suppose F contains a primitive m^{th} root of unity and either F has characteristic 0 or $\gcd(\mathrm{char}(F), m) = 1$. Write $K = F(d)$ where d is a root of the irreducible polynomial $x^m - e$ for some $e \in F^\times$. Then $\sigma^j(\lambda d^i) = \omega^{ij}\lambda d^i$, for all $\lambda \in F$ and $i, j \in \{0, \ldots, m-1\}$ with $\omega \in F^\times$ a primitive m^{th} root of unity. Furthermore, if m is prime then λd^i are the only possible eigenvectors of σ^j.*

Proof. When m is prime this is [64, Lemma 6.2.7]. We are left to prove the first assertion when m is not necessarily prime, this is similar to the first part of the proof of [64, Lemma 6.2.7]: We have $\sigma(d^m) = \sigma(e) = e = d^m$, therefore the action of σ on d is given by $\sigma(d) = \omega d$ where ω is a primitive m^{th} root of unity. Thus $\sigma^j(d) = \omega^j d$ and $\sigma^j(d^i) = \omega^{ij} d^i$ for all $i, j \in \{0, \ldots, m-1\}$. □

When m is prime, Corollary 6.1 and Lemma 6.6 yield:

Proposition 6.7. *Suppose m is prime, F has characteristic not m and contains a primitive m^{th} root of unity. Write $K = F(d)$ where d is a root of the irreducible polynomial $x^m - e \in F[x]$ for some $e \in F^\times$.*

(i) If $a \neq \lambda d^i$ for all $\lambda \in F^\times$, $i \in \{1, \ldots, m-1\}$ then $\mathrm{Aut}_F(A) \cong \mathrm{Ker}(N_{K/F})$ and all automorphisms of A are inner.

(ii) Suppose $a = \lambda d^i$ for some $\lambda \in F^\times$, $i \in \{1, \ldots, m-1\}$. If there exists $j \in \{1, \ldots, m-1\}$ and $k \in K^\times$ such that $N_{K/F}(k) = \omega^{ij}$ where $\omega \in F^\times$ is the primitive m^{th} root of unity satisfying $\sigma(d) = \omega d$, then $\langle H_{\sigma^j,k} \rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(A)$ of order m^2. Otherwise $\mathrm{Aut}_F(A) \cong \mathrm{Ker}(N_{K/F})$ and all automorphisms of A are inner.

Proof. (i) If $a \neq \lambda d^i$ for all $\lambda \in F^\times$, $i \in \{1, \ldots, m-1\}$ then $\sigma^j(a) \neq la$ for all $l \in F^\times$, $j \in \{1, \ldots, m-1\}$ by Lemma 6.6. In particular, this means $\sigma^j(a) \neq N_{K/F}(k)a$ for all $k \in K^\times$ and so $H_{\sigma^j,k}$ is not an automorphism of A for all $j \in \{1, \ldots, m-1\}$, $k \in K^\times$ by Corollary 6.1. Therefore $\mathrm{Aut}_F(A) = \{H_{\mathrm{id},k} \mid N_{K/F}(k) = 1\}$ again by Corollary 6.1 and $\mathrm{Aut}_F(A) = \{G_c \mid c \in K^\times\} \cong \ker(N_{K/F})$ by Theorem 6.2, hence all automorphisms of A are inner.

(ii) Suppose there exists $j \in \{1, \ldots, m-1\}$ and $k \in K$ such that $N_{K/F}(k) = \omega^{ij}$ where $\omega \in F^\times$ is a primitive m^{th} root of unity. Then

$$\sigma^j(a) = \omega^{ij} a = N_{K/F}(k)a,$$

by Lemma 6.6 which implies $H_{\sigma^j,k} \in \mathrm{Aut}_F(A)$ by Corollary 6.1. Since m is prime, σ^j has order m, and $H_{\sigma^j,k} \circ \ldots \circ H_{\sigma^j,k}$ (m-times) becomes $H_{\mathrm{id},b}$ where $b = \omega^{ij} = N_{K/F}(k)$. As b is a primitive m^{th} root of unity, $H_{\mathrm{id},b}$ has order m so the subgroup generated by $H_{\sigma^j,k}$ has order m^2.

On the other hand, if $N_{K/F}(k) \neq \omega^{ij}$ for all $k \in K^\times$, $j \in \{1, \ldots, m-1\}$, then $\sigma^j(a) \neq N_{K/F}(k)a$ for all $k \in K^\times$, $j \in \{1, \ldots, m-1\}$ by Lemma 6.6, and hence $H_{\sigma^j,k} \notin \mathrm{Aut}_F(A)$ for all $j \in \{1, \ldots, m-1\}$, $k \in K^\times$ by Corollary 6.1. Therefore $\mathrm{Aut}_F(A) = \{G_c \mid c \in K^\times\} \cong \ker(N_{K/F})$ by Theorem 6.2.

□

6.1 AUTOMORPHISMS OF NONASSOCIATIVE QUATERNION ALGEBRAS

We now study the automorphisms of nonassociative cyclic algebras of degree 2, i.e. nonassociative quaternion algebras. Suppose $\mathrm{Char}(F) \neq 2$, K/F is a quadratic separable field extension with non-trivial automorphism σ, and write $K = F(\sqrt{b})$ for some $b \in K^\times$. Let $A = (K/F, \sigma, a)$, $a \in K \setminus F$, be a nonassociative quaternion algebra.

Theorem 6.8. *(i) A map H is an automorphism of A if and only if $H = H_{\sigma^j,k}$ for some $j \in \{0, 1\}$ and $k \in K^\times$ such that $\sigma^j(a) = N_{K/F}(k)a$.*

(ii) The map $H_{\mathrm{id},c^{-1}\sigma(c)} = G_c$ defined as in (6.1) is an inner automorphism of A for all $c \in K^\times$. Moreover every automorphism of A of the form $H_{\mathrm{id},k}$ can also be written in the form G_c for some $c \in K^\times$.

(iii) G_c is not trivial if and only if $c \in K \setminus F$. In particular there exists a non-trivial inner automorphism of A.

(iv) $\{G_c \mid c \in K^\times\}$ *are the only inner automorphisms of* A.

Proof. (i), (ii) and (iii) follow immediately from Corollary 6.1 and Theorem 6.2. The proof of (iv) is similar to [67, Lemmas 2 and 3] with $\alpha = \mathrm{id}$:

Suppose, for a contradiction, that $\{G_c \mid c \in K^\times\}$ are not the only inner automorphisms of A. This means there exists an element $0 \neq r + st \in A$ with left inverse $u + vt$, such that $s \neq 0$ and

$$H : A \to A,\ x_0 + x_1 t \mapsto [(u + vt) \circ (x_0 + x_1 t)] \circ (r + st),$$

is an automorphism. We have

$$1 = (u + vt) \circ (r + st) = ur + v\sigma(s)a + \big(us + v\sigma(r)\big)t, \tag{6.4}$$

and comparing the coefficients of t in (6.4) yields

$$us + v\sigma(r) = 0. \tag{6.5}$$

Any automorphism must preserve the left nucleus, so $H(K) = K$ and $H|_K = \sigma^j$ for some $j \in \{0, 1\}$. This implies

$$\begin{aligned} H(k) &= [(u + vt) \circ k] \circ (r + st) = (uk + v\sigma(k)t) \circ (r + st) \\ &= ukr + v\sigma(k)\sigma(s)a + (uks + v\sigma(k)\sigma(r))t = \sigma^j(k) \end{aligned}$$

for all $k \in K$, in particular

$$kus + \sigma(k)v\sigma(r) = 0. \tag{6.6}$$

Therefore $kus = \sigma(k)us$ for all $k \in K$ by (6.5), (6.6), hence $u = 0$ since $s \neq 0$ and σ is not trivial. Furthermore $v\sigma(r) = 0$ by (6.5) which means $r = 0$ because σ is injective and $v \neq 0$. Now A is a division algebra by Corollary 3.14 and Theorem 2.26 (see also [65, p. 369]), moreover

$$\frac{1}{\sigma(s)a} t \circ st = 1,$$

and so the left inverse of st is unique and equal to $(1/(\sigma(s)a))t$. We conclude H has the form

$$H(x_0 + x_1 t) = \Big[\frac{1}{\sigma(s)a} t \circ (x_0 + x_1 t)\Big] \circ st = \Big(\frac{\sigma(x_0)}{\sigma(s)a} t + \frac{\sigma(x_1)}{\sigma(s)}\Big) \circ st$$

$$= \sigma(x_0) + \frac{\sigma(x_1)s}{\sigma(s)}t,$$

that is $H = H_{\sigma,b}$ where $b = \sigma(s)^{-1}s$, and

$$\sigma(a) = \sigma(s)^{-1}s\sigma^2(s)^{-1}\sigma(s)a = s\sigma^2(s)^{-1}a = ss^{-1}a = a$$

by Corollary 6.1, a contradiction because $a \in K \setminus F$. □

Theorem 6.8(i) is also proven by Waterhouse in [65, p. 370-371]. Setting $m = 2$ in Theorem 6.2(vi) and Proposition 6.7(i) yields:

Corollary 6.9. *(i) If $a = \lambda_0 + \lambda_1\sqrt{b}$ for some $\lambda_0, \lambda_1 \in F^\times$, then $\mathrm{Aut}_F(A) = \{G_c \mid c \in K^\times\} \cong \mathrm{Ker}(N_{K/F})$ and all automorphisms of A are inner.*

(ii) If $a = \lambda\sqrt{b}$ for some $\lambda \in F^\times$ and $N_{K/F}(k) \neq -1$ for all $k \in K^\times$, then $\mathrm{Aut}_F(A) = \{G_c \mid c \in K^\times\} \cong \mathrm{Ker}(N_{K/F})$ and all automorphisms of A are inner.

Proof. (i) $-1 \in F^\times$ is a primitive 2^{nd} root of unity so the result follows by Proposition 6.7(i).

(ii) We have $\sigma(a)a^{-1} = -aa^{-1} = -1$ so the assertion follows by Theorem 6.2(vi).

□

Example 6.10. *Consider the nonassociative quaternion algebra $A = (\mathbb{C}/\mathbb{R}, \sigma, a)$ where $a \in \mathbb{C} \setminus \mathbb{R}$ and σ denotes complex conjugation. Given $k = k_0 + k_1 i \in \mathbb{C}$, $k_0, k_1 \in \mathbb{R}$, we have*

$$N_{\mathbb{C}/\mathbb{R}}(k) = k\sigma(k) = (k_0 + k_1 i)(k_0 - k_1 i) = k_0^2 + k_1^2 \neq -1,$$

and so $\mathrm{Aut}_{\mathbb{R}}(A) = \{G_c \mid c \in \mathbb{C}^\times\} \cong \mathrm{Ker}(N_{\mathbb{C}/\mathbb{R}})$ by Corollary 6.9. Now since $\mathrm{Ker}(N_{\mathbb{C}/\mathbb{R}}) = \{k_0 + k_1 i \in \mathbb{C} \mid k_0^2 + k_1^2 = 1\}$, we conclude $\mathrm{Aut}_{\mathbb{R}}(A)$ is isomorphic to the unit circle in $\mathbb{C}$.

Recall the **dicyclic group** of order $4l$ has the presentation

$$\mathrm{Dic}_l = \langle x, y \mid y^{2l} = 1,\ x^2 = y^l,\ x^{-1}yx = y^{-1}\rangle. \tag{6.7}$$

The **semidirect product** $\mathbb{Z}/s\mathbb{Z} \rtimes \mathbb{Z}/n\mathbb{Z}$ between cyclic groups $\mathbb{Z}/s\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ corresponds to a choice of integer l such that $l^n \equiv 1 \bmod s$. It can be described by the presentation

$$\mathbb{Z}/s\mathbb{Z} \rtimes_l \mathbb{Z}/n\mathbb{Z} = \langle x, y \mid x^s = 1,\ y^n = 1,\ yxy^{-1} = x^l \rangle. \tag{6.8}$$

Theorem 6.11. *Let $a = \lambda\sqrt{b}$ for some $\lambda \in F^\times$ and suppose there exists $k \in K^\times$ such that $N_{K/F}(k) = -1$. For every $c \in K \setminus F$ for which there exists a positive integer j such that $c^j \in F^\times$, pick the smallest such j.*

(i) If j is even then $\mathrm{Aut}_F(A)$ contains a subgroup isomorphic to the dicyclic group of order $2j$.

(ii) If j is odd then $\mathrm{Aut}_F(A)$ contains a subgroup isomorphic to the semidirect product $\mathbb{Z}/j\mathbb{Z} \rtimes_{j-1} \mathbb{Z}/4\mathbb{Z}$.

Proof. Since $\sigma(a) = -a = N_{K/F}(k)a$, $H_{\sigma,k} \in \mathrm{Aut}_F(A)$ by Corollary 6.1. $\langle G_c \rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(A)$ of order j by Theorem 6.2, furthermore, a straightforward calculation shows that

$$\langle H_{\sigma,k} \rangle = \{H_{\sigma,k}, H_{\mathrm{id},-1}, H_{\sigma,-k}, H_{\mathrm{id},1}\}. \tag{6.9}$$

(i) Suppose j is even and write $j = 2l$. We prove first that $G_{c^l} = H_{\mathrm{id},-1}$. Write $c^l = \lambda + \mu\sqrt{b}$ for some $\lambda, \mu \in F$. Then

$$c^j = c^{2l} = \lambda^2 + \mu^2 b + 2\lambda\mu\sqrt{b} \in F,$$

which implies $2\lambda\mu = 0$, i.e. $\lambda = 0$ or $\mu = 0$. By the minimality of j, $c^l \notin F$ thus $\lambda = 0$ and hence $c^l = \mu\sqrt{b}$. We have

$$\begin{aligned} G_{c^l}(x_0 + x_1 t) &= x_0 + x_1(\mu\sqrt{b})^{-1}\sigma(\mu\sqrt{b})t = x_0 + x_1\mu^{-1}b^{-1}\sqrt{b}(-\mu\sqrt{b})t \\ &= x_0 - x_1 t = H_{\mathrm{id},-1}(x_0 + x_1 t), \end{aligned}$$

that is $G_{c^l} = H_{\mathrm{id},-1}$.

Next we prove $(H_{\sigma,k})^{-1} \circ G_c \circ H_{\sigma,k} = G_c^{-1}$: Simple calculations show $(H_{\sigma,k})^{-1} = H_{\sigma,-k}$ and $G_c^{-1} = G_{\sigma(c)}$. Furthermore

$$H_{\sigma,-k}\big(G_c\big(H_{\sigma,k}(x_0 + x_1 t)\big)\big) = H_{\sigma,-k}\big(G_c\big(\sigma(x_0) + \sigma(x_1)kt\big)\big)$$

$$\begin{aligned} &= H_{\sigma,-k}\big(\sigma(x_0) + \sigma(x_1)kc^{-1}\sigma(c)t\big) \\ &= x_0 - x_1\sigma(k)\sigma(c^{-1})ckt \\ &= x_0 + x_1\sigma(c^{-1})ct = G_{\sigma(c)}\big(x_0 + x_1 t\big), \end{aligned}$$

that is $(H_{\sigma,k})^{-1} \circ G_c \circ H_{\sigma,k} = G_c^{-1}$.

We conclude $H_{\sigma,k}^2 = H_{\mathrm{id},-1} = G_{c^l} = G_c^l$, $G_c^{2l} = \mathrm{id}$ and $(H_{\sigma,k})^{-1} \circ G_c \circ H_{\sigma,k} = G_c^{-1}$, hence $\langle H_{\sigma,k}, G_c \rangle$ has the presentation (6.7) as required.

(ii) Suppose j is odd, then $\langle G_c \rangle$ is cyclic of order j so does not contain $H_{\mathrm{id},-1}$, because $H_{\mathrm{id},-1}$ has order 2. This implies $\langle H_{\sigma,k} \rangle \cap \langle G_c \rangle = \{\mathrm{id}\}$ by (6.9). Furthermore, $(H_{\sigma,k})^{-1} \circ G_c \circ H_{\sigma,k} = G_c^{-1} = G_c^{j-1} = G_{c^{j-1}}$, similarly to the argument in (i). Notice that

$$(j-1)^4 = j^4 - 4j^3 + 6j^2 - 4j + 1 \equiv 1 \bmod (j),$$

thus $\mathrm{Aut}_F(A)$ contains the subgroup

$$\langle G_c \rangle \rtimes_{j-1} \langle H_{\sigma,k} \rangle \cong \mathbb{Z}/j\mathbb{Z} \rtimes_{j-1} \mathbb{Z}/4\mathbb{Z}$$

as required.

$\square$

In particular if we choose $c = \sqrt{b}$ in Theorem 6.11 then clearly $j = 2$ which means $\mathrm{Aut}_F(A)$ contains the dicyclic group of order 4, which is the cyclic group of order 4:

Corollary 6.12. *If $a = \lambda\sqrt{b}$ for some $\lambda \in F^\times$ and there exists $k \in K^\times$ such that $k\sigma(k) = -1$ then $\mathrm{Aut}_F(A)$ contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z}$.*

Examples 6.13. *(i) Suppose $F = \mathbb{Q}(i)$, $K = F(\sqrt{-3})$ and $\sigma : K \to K$ is the F-automorphism sending $\sqrt{-3}$ to $-\sqrt{-3}$. Let $A = (K/F, \sigma, \lambda\sqrt{-3})$ for some $\lambda \in F^\times$, $c = 1 + \sqrt{-3} \in K$, and notice $i\sigma(i) = i^2 = -1$. We have $c^2 = -2 + 2\sqrt{-3}$ and $c^3 = -8$ so that $c, c^2 \in K \setminus F$ and $c^3 \in F$. This means $\mathrm{Aut}_F(A)$ contains a subgroup isomorphic to the semidirect product $\mathbb{Z}/3\mathbb{Z} \rtimes_2 \mathbb{Z}/4\mathbb{Z}$ by Theorem 6.11.*

(ii) *Suppose $F = \mathbb{Q}(i)$, $K = F(\sqrt{-1/12})$ and $\sigma : K \to K$ the F-automorphism sending $\sqrt{-1/12}$ to $-\sqrt{-1/12}$. Let*

$$A = (K/F, \sigma, \lambda\sqrt{-1/12})$$

for some $\lambda \in F^\times$, $c = 1 + 2\sqrt{-1/12} \in K$ and notice $i\sigma(i) = i^2 = -1$. Then

$$c^2 = \frac{2}{3} + \frac{2i}{\sqrt{3}}, \quad c^3 = \frac{8i}{3\sqrt{3}}, \quad c^4 = \frac{-8}{9} + \frac{8i}{3\sqrt{3}},$$
$$c^5 = \frac{-16}{9} + \frac{16i}{9\sqrt{3}} \quad \text{and} \quad c^6 = \frac{-64}{27}.$$

Hence $c, c^2, c^3, c^4, c^5 \in K \setminus F$ and $c^6 \in F$. Therefore $\mathrm{Aut}_F(A)$ contains the dicyclic group of order 12 by Theorem 6.11.

(iii) *Suppose $F = \mathbb{Q}(i)(\sqrt{5})$, $K = F\big(\sqrt{2\sqrt{5}-5}\big)$ and $\sigma : K \to K$ is the F-automorphism sending $\sqrt{2\sqrt{5}-5}$ to $-\sqrt{2\sqrt{5}-5}$. Let*

$$A = (K/F, \sigma, \lambda\sqrt{2\sqrt{5}-5})$$

for some $\lambda \in F^\times$, $c = 1 + \sqrt{2\sqrt{5}-5} \in K$ and notice $i\sigma(i) = i^2 = -1$. Then

$$\begin{aligned}
c^2 &= -4 + 2\sqrt{5} + 2\sqrt{2\sqrt{5}-5} \in K \setminus F,\\
c^3 &= -14 + 6\sqrt{5} - 2\sqrt{2\sqrt{5}-5} + 2\sqrt{5}\sqrt{2\sqrt{5}-5} \in K \setminus F,\\
c^4 &= 16 - 8\sqrt{5} - 16\sqrt{2\sqrt{5}-5} + 8\sqrt{5}\sqrt{2\sqrt{5}-5} \in K \setminus F,\\
c^5 &= 176 - 80\sqrt{5} \in F,
\end{aligned}$$

so we conclude $\mathrm{Aut}_F(A)$ contains a subgroup isomorphic to the semidirect product $\mathbb{Z}/5\mathbb{Z} \rtimes_4 \mathbb{Z}/4\mathbb{Z}$ by Theorem 6.11.

6.2 AUTOMORPHISMS OF NONASSOCIATIVE CYCLIC ALGEBRAS OVER FINITE FIELDS

In [64, p. 88-92], the automorphisms of nonassociative cyclic algebras over finite fields were briefly investigated. In this Section we continue this investigation. In particular, we completely determine the automorphism group of nonassociative cyclic algebras of prime degree p where $\mathrm{Char}(F) \neq p$, this was done only for $p = 2$ in [64].

Let now $F = \mathbb{F}_q$ be a finite field of order q and $K = \mathbb{F}_{q^m}$ for some $m \geq 2$. Then K/F is a cyclic Galois extension of degree m, say $\mathrm{Gal}(K/F) = \langle \sigma \rangle$. Suppose $A = (K/F, \sigma, a)$ is a nonassociative cyclic algebra for some $a \in K \setminus F$. Let α be a primitive element of K, i.e. $K^\times = \langle \alpha \rangle$. We recall the well-known fact that since K and F are finite fields, the field norm $N_{K/F} : K^\times \to F^\times$ is surjective. Therefore by Corollary 6.1, the problem of finding for which $j \in \{0, \ldots, m-1\}$ there exists $H_{\sigma^j,k} \in \mathrm{Aut}_F(A)$ for some $k \in K^\times$, reduces to finding which $j \in \{0, \ldots, m-1\}$ exist such that $\sigma^j(a)a^{-1} \in F^\times$.

Let $s = (q^m - 1)/(q-1)$ and notice $s = \sum_{i=0}^{m-1} q^i$.

Lemma 6.14. *([64, Proposition 6.3.1]). For every $b \in F^\times$ there are precisely s elements $k \in K^\times$ such that $N_{K/F}(k) = b$. Furthermore, $\mathrm{Ker}(N_{K/F}) \cong \mathbb{Z}/s\mathbb{Z}$ is a cyclic subgroup of the multiplicative group $K^\times$.*

If $\gcd(m, q-1) = 1$ then F does not contain a non-trivial m^{th} root of unity by [36, p. 42]. Therefore Theorems 6.2 and 6.4 become:

Theorem 6.15. *(i) $\langle G_\alpha \rangle$ is a cyclic normal subgroup of $\mathrm{Aut}_F(A)$ of order s. Moreover every automorphism of A of the form $H_{\mathrm{id},k}$ for some $k \in K^\times$, is contained in $\langle G_\alpha \rangle$.*

(ii) All automorphisms contained in $\langle G_\alpha \rangle$ are inner, and if $m = 2$ these are all the inner automorphisms of A.

(iii) If $\gcd(m, q-1) = 1$ and a is not contained in any proper subfield of K, then $\mathrm{Aut}_F(A) = \langle G_\alpha \rangle$ is a cyclic group of order s and all automorphisms of A are inner.

Proof. (i) If $K^\times = \langle \alpha \rangle$ then $F^\times = \langle \alpha^s \rangle$ by [50, p. 303]. This means $\alpha^s \in F^\times$ but $\alpha^j \notin F$ for all $j \in \{1, \ldots, s-1\}$ which implies $\langle G_\alpha \rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(A)$ of order s by Theorem 6.2. Since $\mathrm{Ker}(N_{K/F}) \cong \mathbb{Z}/s\mathbb{Z}$ by Lemma 6.14, every automorphism $H_{\mathrm{id},k}$ is contained in $\langle G_\alpha \rangle$ by Theorem 6.2.

(ii) follows by (i) and Theorem 6.2 and (iii) follows by (i) and Theorem 6.4.

$\square$

Lemma 6.16. *Suppose $m|(q-1)$, then $m|s$.*

Proof. We prove first

$$(q-1)|\Big(\big(\sum_{i=0}^{m-1} q^i\big) - m\Big) \tag{6.10}$$

for all $m \geq 2$ by induction: Clearly (6.10) holds for $m = 2$. Suppose (6.10) holds for some $m \geq 2$, then

$$\big(\sum_{i=0}^{m} q^i\big) - (m+1) = \big(\sum_{i=0}^{m-1} q^i\big) - m + q^m - 1 = \big(\sum_{i=0}^{m-1} q^i\big) - m + \big(\sum_{i=0}^{m-1} q^i\big)(q-1). \tag{6.11}$$

Now, $(q-1)|\Big(\big(\sum_{i=0}^{m-1} q^i\big) - m\Big)$ by induction hypothesis, thus $(q-1)$ divides (6.11) which implies (6.10) holds by induction. In particular since $m|(q-1)$, (6.10) yields

$$m|\Big(\big(\sum_{i=0}^{m-1} q^i\big) - m\Big),$$

therefore m divides $\big(\sum_{i=0}^{m-1} q^i\big) - m + m = s$ as required. $\square$

Lemma 6.17. *Suppose $m|(q-1)$.*

(i) If m is odd then $m^2 \nmid (ls)$ for all $l \in \{1, \ldots, m-1\}$.

(i) If $(q-1)/m$ is even then $m^2 \nmid (ls)$ for all $l \in \{1, \ldots, m-1\}$.

Proof. Write $q = 1 + rm$ for some $r \in \mathbb{N}$, then

$$\begin{aligned} q^j = (1+rm)^j = \sum_{i=0}^{j} \binom{j}{i} (rm)^i &\equiv \sum_{i=0}^{1} \binom{j}{i} (rm)^i \bmod (m^2) \\ &\equiv (1 + jrm) \bmod (m^2) \end{aligned}$$

for all $j \geq 1$. Therefore

$$ls = l \sum_{j=0}^{m-1} q^j \equiv l\big(1 + \sum_{j=1}^{m-1} (1 + jrm)\big) \bmod (m^2)$$

$$\equiv \Big(lm + lrm\frac{(m-1)m}{2}\Big) \bmod (m^2),$$

for all $l \in \{1, \ldots, m-1\}$. If m is odd or $r = (q-1)/m$ is even, then

$$\frac{lr(m-1)}{2} \in \mathbb{Z}$$

and so

$$lrm\frac{(m-1)m}{2} \bmod (m^2) \equiv 0$$

for all $l \in \{1, \ldots, m-1\}$. This means

$$ls \equiv lm \bmod (m^2) \not\equiv 0 \bmod (m^2),$$

that is, $m^2 \nmid (ls)$ for all $l \in \{1, \ldots, m-1\}$. □

Theorem 6.18. *Suppose* $\gcd(\mathrm{Char}(F), m) = 1$ *and* $m|(q-1)$. *Then we can write* $K = F(d)$ *where* d *is a root of the irreducible polynomial* $x^m - e \in F[x]$ *as in Lemma 6.6. Let* $A = (K/F, \sigma, \lambda d^i)$ *for some* $i \in \{1, \ldots, m-1\}$, $\lambda \in F^\times$. *If* m *is odd or* $(q-1)/m$ *is even, then* $\mathrm{Aut}_F(A)$ *is a group of order* ms *and contains a subgroup isomorphic to the semidirect product of cyclic groups*

$$\mathbb{Z}/\Big(\frac{s}{m}\Big)\mathbb{Z} \rtimes_q \mathbb{Z}/(m\mu)\mathbb{Z}, \tag{6.12}$$

where $\mu = m/\gcd(i, m)$. *Moreover if* i *and* m *are coprime, then*

$$\mathrm{Aut}_F(A) \cong \mathbb{Z}/\Big(\frac{s}{m}\Big)\mathbb{Z} \rtimes_q \mathbb{Z}/(m^2)\mathbb{Z}. \tag{6.13}$$

Proof. Let $\tau : K \to K,\ k \mapsto k^q$, then $\tau^j(\lambda d^i) = \omega^{ij}\lambda d^i$, for all $j \in \{0, \ldots, m-1\}$ where $\omega \in F^\times$ is a primitive m^{th} root of unity by Lemma 6.6. As τ generates $\mathrm{Gal}(K/F)$, the automorphisms of A are precisely the maps $H_{\tau^j,k}$, where $j \in \{0, \ldots, m-1\}$ and $k \in K^\times$ are such that $\tau^j(\lambda d^i) = N_{K/F}(k)\lambda d^i$ by Corollary 6.1. Moreover there are exactly s elements $k \in K^\times$ with $N_{K/F}(k) = \omega^{ij}$ by Lemma 6.14, and each of these elements corresponds to a unique automorphism of A. Therefore $\mathrm{Aut}_F(A)$ is a group of order ms.

Choose $k \in K^\times$ such that $N_{K/F}(k) = \omega^i$ so that $H_{\tau,k} \in \mathrm{Aut}_F(A)$. As τ has order m, $H_{\tau,k} \circ \ldots \circ H_{\tau,k}$ (m-times) becomes $H_{\mathrm{id},b}$ where $b = \omega^i = N_{K/F}(k)$. Notice ω^i is a primitive μ^{th} root of unity where $\mu = m/\gcd(i, m)$, therefore

$H_{\mathrm{id},b}$ has order μ, and thus the subgroup of $\mathrm{Aut}_F(A)$ generated by $H_{\tau,k}$ has order $m\mu$.

$\langle G_\alpha \rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(A)$ of order s by Theorem 6.15 where α is a primitive element of K. Furthermore, $m|s$ by Lemma 6.16 and so $\langle G_{\alpha^m} \rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(A)$ of order s/m. We will prove $\mathrm{Aut}_F(A)$ contains the semidirect product $\langle G_{\alpha^m} \rangle \rtimes_q \langle H_{\tau,k} \rangle$, by showing it can be written in the presentation (6.8):

The inverse of $H_{\tau,k}$ in $\mathrm{Aut}_F(A)$ is $H_{\tau^{-1},\tau^{-1}(k^{-1})}$ and so

$$\begin{aligned}
&H_{\tau,k}\Big(G_{\alpha^m}\Big(H_{\tau,k}^{-1}\Big(\sum_{j=0}^{m-1} x_j t^j\Big)\Big)\Big)\\
&\quad= H_{\tau,k}\Big(G_{\alpha^m}\Big(\tau^{-1}(x_0) + \sum_{j=1}^{m-1} \tau^{-1}(x_j)\Big(\prod_{l=0}^{j-1}\sigma^l(\tau^{-1}(k^{-1}))\Big)t^j\Big)\Big)\\
&\quad= H_{\tau,k}\Big(\tau^{-1}(x_0) + \sum_{j=1}^{m-1} \tau^{-1}(x_j)\Big(\prod_{l=0}^{j-1}\sigma^l(\tau^{-1}(k^{-1}))\Big)\alpha^{-m}\sigma^j(\alpha^m)t^j\Big)\\
&\quad= x_0 + \sum_{j=1}^{m-1} x_j\tau(\alpha^{-m})\tau(\sigma^j(\alpha^m))t^j = x_0 + \sum_{j=1}^{m-1} x_j\tau(\alpha^{-m})\sigma^j(\tau(\alpha^m))t^j\\
&\quad= G_{\tau(\alpha^m)}\Big(\sum_{j=0}^{m-1} x_j t^j\Big) = G_{\alpha^{mq}}\Big(\sum_{j=0}^{m-1} x_j t^j\Big),
\end{aligned}$$

that is $H_{\tau,k} \circ G_{\alpha^m} \circ H_{\tau,k}^{-1} = G_{\alpha^{mq}} = (G_{\alpha^m})^q$.

Notice $q^m = qs - s + 1$, i.e. $q^m \equiv 1 \bmod (s)$, and so $q^{m\mu} \equiv 1 \bmod (s)$. Then $m|s$ by Lemma 6.16, hence $q^{m\mu} \equiv 1 \bmod (s/m)$. In order to prove $\mathrm{Aut}_F(A)$ contains $\langle G_{\alpha^m} \rangle \rtimes_q \langle H_{\tau,k} \rangle$, we are left to show that $\langle H_{\tau,k} \rangle \cap \langle G_{\alpha^m} \rangle = \{\mathrm{id}\}$.

Suppose, for a contradiction, that $\langle H_{\tau,k} \rangle \cap \langle G_{\alpha^m} \rangle \neq \{\mathrm{id}\}$. Then $H_{\mathrm{id},\omega^l} \in \langle G_{\alpha^m} \rangle$ for some $l \in \{1, \dots, m-1\}$. Therefore $\langle G_{\alpha^m} \rangle$ contains a subgroup of order $m/\gcd(l,m)$ generated by H_{id,ω^l} and so $(m/\gcd(l,m))|(s/m)$. This means $m^2|(s\gcd(l,m))$, a contradiction by Lemma 6.17.

Therefore $\mathrm{Aut}_F(A)$ contains the subgroup

$$\langle G_{\alpha^m} \rangle \rtimes_q \langle H_{\tau,k} \rangle \cong \mathbb{Z}/\Big(\frac{s}{m}\Big)\mathbb{Z} \rtimes_q \mathbb{Z}/(m\mu)\mathbb{Z}.$$

If $\gcd(i,m) = 1$ this subgroup has order ms and since $|\mathrm{Aut}_F(A)| = ms$, this is all of $\mathrm{Aut}_F(A)$. $\square$

We can completely determine the automorphism group of nonassociative cyclic algebras of prime degree m different from $\mathrm{Char}(F)$. If F does not contain a primitive m^{th} root of unity, i.e. if $m \nmid (q-1)$, then $\mathrm{Aut}_F(A) = \langle G_\alpha \rangle \cong \mathbb{Z}/s\mathbb{Z}$ by Theorem 6.15(iii), and all automorphisms of A are inner. Otherwise we have:

Theorem 6.19. *Suppose m is prime and $m|(q-1)$. Then we can write $K = F(d)$ where d is a root of the irreducible polynomial $x^m - e \in F[x]$ as in Lemma 6.6. Let $A = (K/F, \sigma, a)$ for some $a \in K \setminus F$.*

(i) If $a \neq \lambda d^i$ for any $i \in \{0, \ldots, m-1\}$, $\lambda \in F^\times$, then $\mathrm{Aut}_F(A) = \langle G_\alpha \rangle \cong \mathbb{Z}/s\mathbb{Z}$ and all automorphisms of A are inner.

(ii) ([64, Theorem 6.3.5]). If $m = 2$ and $a = \lambda d$ for some $\lambda \in F^\times$, then $\mathrm{Aut}_F(A)$ is the dicyclic group of order $2q+2$.

(iii) If $m > 2$ and $a = \lambda d^i$ for some $i \in \{1, \ldots, m-1\}$, $\lambda \in F^\times$, then

$$\mathrm{Aut}_F(A) \cong \mathbb{Z}/\left(\frac{s}{m}\right)\mathbb{Z} \rtimes_q \mathbb{Z}/(m^2)\mathbb{Z}.$$

Proof. (i) This is [64, Corollary 6.3.3] together with Theorem 6.15(i).

(iii) follows immediately from Theorem 6.18.

□

7

GENERALISATION OF THE S_f CONSTRUCTION

Until now, we have studied the construction $S_f = D[t;\sigma,\delta]/D[t;\sigma,\delta]f$ in the case where D is an associative division ring. In this Chapter we generalise this construction using the skew polynomial ring $S[t;\sigma,\delta]$, where S is any associative unital ring, σ is an injective endomorphism of S and δ is a σ-derivation of S. While $S[t;\sigma,\delta]$ is in general neither left nor right Euclidean (unless S is a division ring), we are still able to right divide by polynomials $f(t) \in S[t;\sigma,\delta]$ whose leading coefficient is a unit. Moreover, if σ is an automorphism we are also able to left divide by such $f(t)$. Therefore, when $f(t)$ has an invertible leading coefficient, it is possible to generalise the construction of the algebras S_f to this setting.

In the following, let S be a unital associative ring, σ be an injective endomorphism of S and δ be a left σ-derivation of S. An element $0 \neq b \in S$ is called **right-invertible** if there exists $b_r \in S$ such that $bb_r = 1$, and **left-invertible** if there exists $b_l \in S$ such that $b_l b = 1$. An element b which is both left and right invertible is called **invertible** (or a **unit**), and $b_l = b_r$ is called the **inverse** of b and denoted b^{-1} [38, p. 4]. We say a non-zero ring is a **domain** if it has no non-trivial zero divisors. A commutative domain is called an **integral domain**.

Recall from (1.4) that $S_{n,j}$ denotes the sum of all monomials in σ and δ that are of degree j in σ and degree $n-j$ in δ. The equality

$$(bt^n)(ct^m) = \sum_{j=0}^{n} b(S_{n,j}(c))t^{j+m}, \tag{1.3}$$

for all $b, c \in S$, holds more generally for S any unital associative ring by [8, p. 4].

The degree function satisfies

$$\deg\big(g(t)h(t)\big) \leq \deg(g(t)) + \deg(h(t)) \tag{7.1}$$

for all $g(t), h(t) \in S[t;\sigma,\delta]$. In general (7.1) is not an equality unless S is a domain, or $g(t)$ has an invertible leading coefficient, or $h(t)$ has an invertible leading coefficient:

Indeed, if S is a domain this is [23, p. 12], and the equality in (7.1) implies $S[t;\sigma,\delta]$ is also a domain. Suppose now S is not necessarily a domain, $g(t)$ has degree l and leading coefficient g_l and $h(t)$ has degree n and leading coefficient h_n. If h_n is invertible then $\sigma^l(h_n)$ is also invertible and

$$g(t)h(t) = g_l\sigma^l(h_n)t^{l+n} + \text{ lower degree terms}.$$

Here $g_l\sigma^l(h_n) \neq 0$ since invertible elements are not zero divisors. Similarly, if g_l is invertible then $g_l\sigma^l(h_n) \neq 0$. In either case (7.1) is an equality.

$S[t;\sigma,\delta]$ is in general neither left nor right Euclidean, nor a left or right principal ideal domain. Nevertheless, we can still perform right division by a polynomial whose leading coefficient is a unit. Additionally, when σ is an automorphism we can also left divide by such a polynomial. When $\delta = 0$ and $\sigma \in \mathrm{Aut}(S)$ this was proven for special cases of S, for instance in [20, p. 4], [34, p. 4] and [48, p. 391]:

Theorem 7.1. *Let $f(t) = a_m t^m - \sum_{i=0}^{m-1} a_i t^i \in R = S[t;\sigma,\delta]$ and suppose a_m is invertible.*

(i) *For all $g(t) \in R$, there exists uniquely determined $r(t), q(t) \in R$ with $\deg(r(t)) < m$, such that $g(t) = q(t)f(t) + r(t)$.*

(ii) *Suppose additionally σ is an automorphism of S. Then for all $g(t) \in R$, there exists uniquely determined $r(t), q(t) \in R$ with $\deg(r(t)) < m$, such that $g(t) = f(t)q(t) + r(t)$.*

Proof. Let $g(t) = \sum_{i=0}^{l} g_i t^i \in R$ have degree l.

(i) Suppose $l < m$, then $g(t) = 0q(t) + g(t)$. Moreover, we have

$$\deg(q(t)f(t)) = \deg(q(t)) + \deg(f(t)) \geq m,$$

for all $0 \neq q(t) \in R$ as $f(t)$ has an invertible leading coefficient. Therefore if $g(t) = q(t)f(t) + r(t)$ then $q(t) = 0$ and so $r(t) = g(t)$ as required.

Now suppose $l \geq m$, then

$$\begin{aligned}
g(t) - g_l\sigma^{l-m}(a_m^{-1})t^{l-m}f(t) &= g(t) - g_l\sigma^{l-m}(a_m^{-1})t^{l-m}\Big(a_m t^m - \sum_{i=0}^{m-1} a_i t^i\Big) \\
&= g(t) - g_l\sigma^{l-m}(a_m^{-1})t^{l-m}a_m t^m + \sum_{i=0}^{m-1} g_l\sigma^{l-m}(a_m^{-1})t^{l-m}a_i t^i \\
&= g(t) - g_l\sigma^{l-m}(a_m^{-1})\Big(\sum_{j=0}^{l-m} S_{l-m,j}(a_m)t^j\Big)t^m \\
&\quad + \sum_{i=0}^{m-1} g_l\sigma^{l-m}(a_m^{-1})\Big(\sum_{j=0}^{l-m} S_{l-m,j}(a_i)t^j\Big)t^i \\
&= g(t) - g_l\sigma^{l-m}(a_m^{-1})S_{l-m,l-m}(a_m)t^l \\
&\quad - g_l\sigma^{l-m}(a_m^{-1}) \sum_{0\leq j\leq l-m-1} S_{l-m,j}(a_m)t^{j+m} \\
&\quad + \sum_{i=0}^{m-1}\sum_{j=0}^{l-m} g_l\sigma^{l-m}(a_m^{-1})S_{l-m,j}(a_i)t^{i+j} \\
&= g(t) - g_l\sigma^{l-m}(a_m^{-1})\sigma^{l-m}(a_m)t^l \\
&\quad - \sum_{0\leq j\leq l-m-1} g_l\sigma^{l-m}(a_m^{-1})S_{l-m,j}(a_m)t^{j+m} \\
&\quad + \sum_{i=0}^{m-1}\sum_{j=0}^{l-m} g_l\sigma^{l-m}(a_m^{-1})S_{l-m,j}(a_i)t^{i+j}
\end{aligned}$$

$$= g(t) - g_l t^l - \sum_{0 \le j \le l-m-1} g_l \sigma^{l-m}(a_m^{-1}) S_{l-m,j}(a_m) t^{j+m} + \sum_{i=0}^{m-1} \sum_{j=0}^{l-m} g_l \sigma^{l-m}(a_m^{-1}) S_{l-m,j}(a_i) t^{i+j},$$

where we have used $S_{l-m,l-m}(a_m) = \sigma^{l-m}(a_m)$. Hence the polynomial $g(t) - g_l \sigma^{l-m}(a_m^{-1}) t^{l-m} f(t)$ has degree $< l$ and by iteration of this argument, we find $q(t), r(t) \in R$ with $\deg(r(t)) < m$, such that $g(t) = q(t)f(t) + r(t)$.

We now prove uniqueness of $r(t)$ and $q(t)$. Suppose

$$g(t) = q_1(t)f(t) + r_1(t) = q_2(t)f(t) + r_2(t),$$

and so $\big(q_1(t) - q_2(t)\big)f(t) = r_2(t) - r_1(t)$. If $q_1(t) - q_2(t) \neq 0$, then the left hand side of the equation has degree $\geq m$ since $f(t)$ has an invertible leading coefficient, while the right hand side has degree $< m$. Thus $q_1(t) = q_2(t)$ and so $r_1(t) = r_2(t)$.

(ii) If we assume σ is an automorphism, then (ii) is proven similarly to (i) by showing $g(t) - f(t)\sigma^{-m}(a_m^{-1})\sigma^{-m}(g_l)t^{l-m}$ has degree $< l$ and iterating this argument. Uniqueness is proven analogously to (i).

$\square$

Let $\mathrm{mod}_r f$ denote the remainder after right division by $f(t)$. Since remainders are uniquely determined by Theorem 7.1(i), the skew polynomials of degree $< m$ canonically represent the elements of the left $S[t;\sigma,\delta]$-module $S[t;\sigma,\delta]/S[t;\sigma,\delta]f$. Similarly, when σ is an automorphism, the skew polynomials of degree $< m$ canonically represent the elements of the right $S[t;\sigma,\delta]$-module $S[t;\sigma,\delta]/fS[t;\sigma,\delta]$.

Definition. *Let $f(t) \in R = S[t;\sigma,\delta]$ be of degree m with invertible leading coefficient $a_m \in S$ and $R_m = \{g(t) \in R \mid deg(g(t)) < m\}$.*

(i) Then R_m together with the multiplication $g \circ h = gh \ \mathrm{mod}_r f$, becomes a unital nonassociative ring $S_f = (R_m, \circ)$, also denoted R/Rf.

(ii) Suppose additionally σ is an automorphism and let $\mathrm{mod}_l f$ *denote the remainder after left division by $f(t)$. Then R_m together with the multiplication $g\,{}_f\!\circ h = gh \,\mathrm{mod}_l f$, becomes a unital nonassociative ring ${}_fS = (R_m, {}_f\!\circ)$, also denoted R/fR.*

S_f and ${}_fS$ are unital nonassociative algebras over

$$S_0 = \{c \in S \mid c \circ h = h \circ c \text{ for all } h \in S_f\} = \mathrm{Comm}(S_f) \cap S,$$

which is a commutative subring of S. If S is a division ring then this construction is precisely Petit's algebra construction given in Chapter 1.

Remarks. *(i) Let $g(t), h(t) \in R_m$ be such that $\deg(g(t)h(t)) < m$. Then the multiplication $g \circ h$ is the same as that in R.*

(ii) S_f is associative if and only if $f(t)$ is right invariant [55, Theorem 4(ii)].

(iii) We have $qf + r = (qd^{-1})(df) + r$, for all $q, r \in R$, and all invertible $d \in S$. It follows that $S_f = S_{df}$ for all invertible $d \in S$.

(iv) If $\deg(f(t)) = m = 1$ then $R_m = S$ and $S_f \cong S$.

Henceforth suppose $\deg(f(t)) = m \geq 2$. We may assume w.l.o.g. again that $f(t)$ is monic. Similarly to Proposition 1.2, it suffices to only consider the algebras S_f since we still have following anti-isomorphism:

Proposition 7.2. *([55, Proposition 3]). Let $f(t) \in S[t;\sigma,\delta]$ where $\sigma \in \mathrm{Aut}(S)$ and $f(t)$ has invertible leading coefficient. The canonical anti-isomorphism*

$$\psi : S[t;\sigma,\delta] \to S^{\mathrm{op}}[t;\sigma^{-1}, -\delta\sigma^{-1}], \quad \sum_{i=0}^{n} b_i t^i \mapsto \sum_{i=0}^{n} \Big(\sum_{j=0}^{i} S_{n,j}(b_i) \Big) t^i,$$

between the skew polynomial rings $S[t;\sigma,\delta]$ and $S^{\mathrm{op}}[t;\sigma^{-1}, -\delta\sigma^{-1}]$, induces an anti-isomorphism between the rings $S_f = S[t;\sigma,\delta]/S[t;\sigma,\delta]f$, and

$${}_{\psi(f)}S = S^{\mathrm{op}}[t;\sigma^{-1}, -\delta\sigma^{-1}]/\psi(f)S^{\mathrm{op}}[t;\sigma^{-1}, -\delta\sigma^{-1}].$$

We now take a closer look at S_f in the special case where $\delta = 0$.

Proposition 7.3. *Suppose $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R = S[t;\sigma]$. If $\sigma^m(z)a_i = a_i\sigma^i(z)$ and $\sigma(a_i) = a_i$ for all $z \in S$, $i \in \{0,\dots,m-1\}$, then $f(t)$ is right invariant and S_f is associative.*

Proof. We have

$$\begin{aligned} f(t)zt^j &= t^m z t^j - \sum_{i=0}^{m-1} a_i t^i z t^j = \sigma^m(z)t^{m+j} - \sum_{i=0}^{m-1} a_i \sigma^i(z) t^{i+j} \\ &= \sigma^m(z)t^j t^m - \sum_{i=0}^{m-1} \sigma^m(z) a_i t^j t^i = \sigma^m(z)t^j t^m - \sum_{i=0}^{m-1} \sigma^m(z) t^j a_i t^i \\ &= \sigma^m(z) t^j f(t) \in Rf, \end{aligned}$$

for all $z \in S$, $j \in \{0,\dots,m-1\}$ since $t^j a_i = \sigma^j(a_i)t^j = a_i t^j$ and $\sigma^m(z)a_i = a_i\sigma^i(z)$. Therefore by distributivity $fR \subseteq Rf$. This implies $bfc \in Rf$ for all $b,c \in R$, thus Rf is a two-sided ideal and so S_f is associative by [55, Theorem 4(ii)]. $\square$

Proposition 7.4. *Suppose $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in S[t;\sigma]$.*

(i) ([55, Theorem 8]). $\mathrm{Comm}(S_f)$ *contains the set*

$$\Big\{ \sum_{i=0}^{m-1} c_i t^i \mid c_i \in \mathrm{Fix}(\sigma) \text{ and } bc_i = c_i\sigma^i(b) \text{ for all } b \in S \Big\}. \tag{7.2}$$

(ii) If S is a domain and $a_0 \neq 0$ the two sets are equal.

(iii) If a_0 is invertible the two sets are equal.

Proof. (ii) Let $c = \sum_{i=0}^{m-1} c_i t^i \in \mathrm{Comm}(S_f)$, then in particular

$$t \circ c = t \circ \Big(\sum_{i=0}^{m-1} c_i t^i \Big) = \sum_{i=0}^{m-2} \sigma(c_i) t^{i+1} + \sigma(c_{m-1}) \sum_{i=0}^{m-1} a_i t^i, \tag{7.3}$$

and

$$c \circ t = \Big(\sum_{i=0}^{m-1} c_i t^i \Big) \circ t = \sum_{i=0}^{m-2} c_i t^{i+1} + c_{m-1} \sum_{i=0}^{m-1} a_i t^i, \tag{7.4}$$

must be equal. Comparing the t^0 coefficient in (7.3) and (7.4) yields

$$(\sigma(c_{m-1}) - c_{m-1})a_0 = 0, \tag{7.5}$$

which implies $c_{m-1} \in \mathrm{Fix}(\sigma)$ because S is a domain and $a_0 \neq 0$. Comparing the t^j coefficients in (7.3) and (7.4) gives

$$\sigma(c_{j-1}) + \sigma(c_{m-1})a_j = c_{j-1} + c_{m-1}a_j,$$

for all $j \in \{1, \dots, m-1\}$, hence $c_{j-1} \in \mathrm{Fix}(\sigma)$ for all $j \in \{1, \dots, m-1\}$ because $c_{m-1} \in \mathrm{Fix}(\sigma)$.

Since $c \in \mathrm{Comm}(S_f)$ we also have $b \circ c = c \circ b$ for all $b \in S$. As a result

$$b \circ c = \sum_{i=0}^{m-1} bc_i t^i, \tag{7.6}$$

and

$$c \circ b = \sum_{i=0}^{m-1} c_i t^i b = \sum_{i=0}^{m-1} c_i \sigma^i(b) t^i \tag{7.7}$$

must be equal. Comparing the coefficients of the powers of t in (7.6) and (7.7) yields $bc_i = c_i\sigma^i(b)$ for all $b \in S$, $i \in \{0, \dots, m-1\}$ as required.

(iii) The proof is similar to (ii), but (7.5) implies $c_{m-1} \in \mathrm{Fix}(\sigma)$ because a_0 is invertible, hence not a zero divisor.

□

Corollary 7.5. *Suppose S is a central simple algebra over a field C and $\sigma \in \mathrm{Aut}(S)$ is such that $\sigma|_C$ has order at least m. Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in S[t;\sigma]$ where $a_0 \in S$ is invertible. Then* $\mathrm{Comm}(S_f) = C \cap \mathrm{Fix}(\sigma)$.

Proof. $\mathrm{Comm}(S_f)$ is equal to the set (7.2) by Proposition 7.4, in particular $C \cap \mathrm{Fix}(\sigma) \subseteq \mathrm{Comm}(S_f)$.

Let $\sum_{i=0}^{m-1} c_i t^i \in \mathrm{Comm}(S_f)$ and suppose, for contradiction, $c_j \neq 0$ for some $j \in \{1, \dots, m-1\}$. Then $bc_j = c_j\sigma^j(b)$ for all $b \in S$, in particular $(b - \sigma^j(b))c_j = 0$ for all $b \in C$. We have $0 \neq b - \sigma^j(b)$ for some $b \in C$ since $\sigma|_C$ has order $\geq m$. Moreover $b - \sigma^j(b) \in C$, therefore it is invertible and hence $(b - \sigma^j(b))c_j \neq 0$ for some $b \in C$ because invertible elements are not zero divisors, a contradiction. Thus $\sum_{i=0}^{m-1} c_i t^i = c_0 \in C \cap \mathrm{Fix}(\sigma)$ by (7.2). □

7.1 WHEN DOES S_f CONTAIN ZERO DIVISORS?

We investigate when the algebras S_f contain zero divisors. If the ring S contains zero divisors then clearly so does S_f, therefore we only consider the case where S is a domain. Furthermore, if $f(t) = g(t)h(t)$ for some $g(t), h(t) \in R_m$, then $g(t) \circ h(t) = 0$ and so S_f contains zero divisors.

When S is commutative, i.e. an integral domain, it is well-known that we can associate to S its field of fractions $D \supseteq S$, so that every element of D has the form rs^{-1} for some $r \in S$, $0 \neq s \in S$. On the other hand, if S is a noncommutative domain then we cannot necessarily associate such a "right division ring of fractions" unless S is a so-called right Ore domain:

Definition. *A **right Ore domain** S is a domain such that $aS \cap bS \neq \{0\}$ for all $0 \neq a, b \in S$. The **ring of right fractions** of S is a division ring D containing S, such that every element of D is of the form rs^{-1} for some $r \in S$ and $0 \neq s \in S$.*

Any integral domain is a right Ore domain; its right ring of fractions is equal to its quotient field.

Let now S be a right Ore domain with ring of right fractions D, σ be an injective endomorphism of S and δ be a σ-derivation of S. Then σ and δ extend uniquely to D by setting

$$\sigma(rs^{-1}) = \sigma(r)\sigma(s)^{-1} \text{ and } \delta(rs^{-1}) = \delta(r)s^{-1} - \sigma(rs^{-1})\delta(s)s^{-1}, \qquad (7.8)$$

for all $r \in S$, $0 \neq s \in S$ by [25, Lemma 1.3]. We conclude:

Theorem 7.6. *Let $f(t) \in S[t;\sigma,\delta]$ have invertible leading coefficient and extend σ and δ to D as in (7.8). If $f(t)$ is irreducible in $D[t;\sigma,\delta]$ then $S_f = S[t;\sigma,\delta]/S[t;\sigma,\delta]f(t)$ contains no zero divisors.*

Proof. If $f(t)$ is irreducible in $D[t;\sigma,\delta]$, then $D[t;\sigma,\delta]/D[t;\sigma,\delta]f$ is a right division algebra by Theorem 2.20, therefore it contains no zero divisors. $S_f = S[t;\sigma,\delta]/S[t;\sigma,\delta]f$ is contained in $D[t;\sigma,\delta]/D[t;\sigma,\delta]f$, so also contains no zero divisors. $\square$

Let K be a field and y be an indeterminate. Then $K[y]$ is an integral domain which is not a division algebra. Given $a(y) \in K[y]$, denote $\deg_y(a(y))$ the degree of $a(y)$ as a polynomial in y. We obtain the following Corollaries of Theorem 7.6 using Corollaries 3.7 and 3.13 in Chapter 3:

Corollary 7.7. *Define the injective endomorphism $\sigma : K[y] \to K[y]$ by $\sigma|_K = \mathrm{id}$ and $\sigma(y) = y^2$. If $f(t) = t^2 - a(y) \in K[y][t;\sigma]$ where $0 \neq a(y) \in K[y]$ is such that $3 \nmid \deg_y(a(y))$, then S_f contains no zero divisors. Here S_f is an infinite-dimensional algebra over $S_0 = \mathrm{Fix}(\sigma) = K$.*

Proof. Extend σ to an endomorphism of $K(y)$, the field of fractions of $K[y]$ as in (7.8). Then $f(t)$ is irreducible in $K(y)[t;\sigma]$ by Corollary 3.7 and hence S_f contains no zero divisors by Theorem 7.6. □

Corollary 7.8. *Let σ be the automorphism of $K[y]$ defined by $\sigma|_K = \mathrm{id}$ and $\sigma(y) = qy$ for some $1 \neq q \in K^\times$. Suppose m is prime, K contains a primitive m^{th} root of unity and $f(t) = t^m - a(y) \in K[y][t;\sigma]$ where $0 \neq a(y) \in K[y]$ is such that $m \nmid \deg_y(a(y))$. Then S_f contains no zero divisors.*

Proof. Extend σ to an automorphism of $K(y)$ as in (7.8). Then $f(t)$ is irreducible in $K(y)[t;\sigma]$ by Corollary 3.13, which implies S_f contains no zero divisors by Theorem 7.6. □

Remark. *Consider the set-up in Corollary 7.8. If q is not a root of unity then $\sigma(y^i) = q^i y^i \neq y^i$ for all $i > 1$, therefore S_f is an infinite-dimensional algebra over $S_0 = \mathrm{Fix}(\sigma) = K$.*

Otherwise q is a primitive n^{th} root of unity for some $n \in \mathbb{N}$, then $\sigma(y^i) = q^i y^i = y^i$ if and only if $i = ln$ for some positive integer l. Thus S_f is an algebra over $S_0 = \mathrm{Fix}(\sigma) = K[y^n]$, and since $K[y]$ is finite-dimensional over $K[y^n]$, S_f is also finite-dimensional over $K[y^n]$.

7.2 THE NUCLEUS

In this Section we study the nuclei of S_f, generalising some of our results from Chapter 2.

Theorem 7.9. *Let $f(t) \in R = S[t;\sigma,\delta]$ be of degree m. Then*

$$S \subseteq \mathrm{Nuc}_l(S_f)\ ,\ S \subseteq \mathrm{Nuc}_m(S_f)$$

and

$$\mathrm{Nuc}_r(S_f) = \{u \in R_m \mid fu \in Rf\} = E(f).$$

Proof. Let $b,c,d \in R_m$ and write $bc = q_1 f + r_1$ and $cd = q_2 f + r_2$ for some uniquely determined $q_1, q_2, r_1, r_2 \in R$ with $\deg(r_1(t))$, $\deg(r_2(t)) < m$. This means $b \circ c = bc - q_1 f$ and $c \circ d = cd - q_2 f$. We have

$$(b \circ c) \circ d = (bc - q_1 f) \circ d = (bc - q_1 f)d \ \mathrm{mod}_r f = (bcd - q_1 fd) \ \mathrm{mod}_r f,$$

and

$$b \circ (c \circ d) = b \circ (cd - q_2 f) = b(cd - q_2 f) \ \mathrm{mod}_r f = bcd \ \mathrm{mod}_r f,$$

and hence $(b \circ c) \circ d = b \circ (c \circ d)$ if and only if $q_1 fd \ \mathrm{mod}_r f = 0$ if and only if $q_1 fd \in Rf$.

(i) If $b \in S$ then

$$\deg(bc) \leq \deg(b) + \deg(c) \leq \deg(c) < m, \tag{7.9}$$

but here $bc = q_1 f + r_1$ also means $q_1 = 0$, otherwise $\deg(q_1 f + r_1) \geq m$ as $f(t)$ has invertible leading coefficient, contradicting (7.9). Hence $q_1 fd \ \mathrm{mod}_r f = 0$ which implies $b \in \mathrm{Nuc}_l(S_f)$.

(ii) $S \subseteq \mathrm{Nuc}_m(S_f)$ is proven similarly to (i).

(iii) If $d \in E(f)$ then $fd \in Rf$ and thus $q_1 fd \in Rf$ for all $q_1 \in R$. This implies $d \in \mathrm{Nuc}_r(S_f)$ and $E(f) \subseteq \mathrm{Nuc}_r(S_f)$.

To prove the opposite inclusion, let now $d \in \mathrm{Nuc}_r(S_f)$ and choose $b(t), c(t) \in R$ with invertible leading coefficients b_l and c_n respectively such that $\deg(b(t)) + \deg(c(t)) = m$, so that $\deg(b(t)c(t)) = m$. We have $\deg(q_1(t)f(t)) = \deg(q_1(t)) + m$, but using that $b(t)c(t) = q_1(t)f(t) + r_1(t)$, we conclude $\deg(q_1(t)) = 0$, so $q_1(t) = q_1 \in S$ is non-zero. If $\deg(b(t)) = l$ then the leading coefficient of $b(t)c(t)$ is $b_l \sigma^l(c_n)$

and the leading coefficient of $q_1 f(t)$ is q_1. Therefore $q_1 = b_l \sigma^l(c_n)$ is invertible in S, being a product of invertible elements of S. Since $d \in \mathrm{Nuc}_r(S_f)$ implies $q_1 f d \in Rf$, this yields $fd \in Rf$.

□

By Theorem 7.9(iii) we immediately conclude:

Corollary 7.10. *$E(f) = S_f$ if and only if S_f is associative.*

Proof. $\mathrm{Nuc}_r(S_f) = S_f$ if and only if S_f is associative so the result follows by Theorem 7.9(iii). □

The following generalises [52, (5)]:

Proposition 7.11. *Let $f(t) \in R = S[t;\sigma,\delta]$ be of degree m. The powers of t are associative if and only if $t \circ t^m = t^m \circ t$ if and only if $t \in \mathrm{Nuc}_r(S_f)$.*

Proof. Let $t \in \mathrm{Nuc}_r(S_f)$. Then also $t, \ldots, t^{m-1} \in \mathrm{Nuc}_r(S_f)$ giving $[t^i, t^j, t^k] = 0$ for all $i, j, k < m$, i.e. the powers of t are associative. In particular $(t \circ t^{m-1}) \circ t = t \circ (t^{m-1} \circ t)$, that is $t^m \circ t = t \circ t^m$. We are left to prove $t^m \circ t = t \circ t^m$ implies $t \in \mathrm{Nuc}_r(S_f)$. Suppose $t^m \circ t = t \circ t^m$, then

$$t^m \circ t = (t^m - f(t)) \circ t = \big(t^{m+1} - f(t)t\big) \bmod_r f, \tag{7.10}$$

and

$$t \circ t^m = t \circ (t^m - f(t)) = \big(t^{m+1} - tf(t)\big) \bmod_r f = t^{m+1} \bmod_r f, \tag{7.11}$$

are equal. Comparing (7.10) and (7.11) yields $f(t)t \bmod_r f = 0$, hence $f(t)t \in Rf$. This means $t \in \mathrm{Nuc}_r(S_f)$ by Theorem 7.9. □

When $\delta = 0$ and S is a domain, then either S_f is associative or S_f has left and middle nuclei equal to S:

Theorem 7.12. *Let S be a domain and $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in S[t;\sigma]$. If S_f is not associative then $\mathrm{Nuc}_l(S_f) = \mathrm{Nuc}_m(S_f) = S$.*

Proof. We have $S \subseteq \mathrm{Nuc}_l(S_f)$ and $S \subseteq \mathrm{Nuc}_m(S_f)$ by Theorem 7.9. Suppose S_f is not associative.

(i) We prove $\mathrm{Nuc}_l(S_f) \subseteq S$:

Suppose first that $\sigma(a_i) = a_i$ for all $i \in \{0, \dots, m-1\}$. Let $0 \neq p = \sum_{i=0}^{m-1} p_i t^i \in \mathrm{Nuc}_l(S_f)$ be arbitrary and $j \in \{0, \dots, m-1\}$ be maximal such that $p_j \neq 0$. Suppose towards a contradiction $j > 0$. Then

$$\begin{aligned}(p \circ t^{m-j}) \circ c &= \Big(\sum_{i=0}^{j} p_i t^i \circ t^{m-j}\Big) \circ c = \Big(\sum_{i=0}^{j-1} p_i t^{i+m-j} + p_j \sum_{i=0}^{m-1} a_i t^i\Big) \circ c \\ &= \sum_{i=0}^{j-1} p_i \sigma^{i+m-j}(c) t^{i+m-j} + \sum_{i=0}^{m-1} p_j a_i \sigma^i(c) t^i,\end{aligned}$$

and

$$\begin{aligned}p \circ (t^{m-j} \circ c) &= \sum_{i=0}^{j} p_i t^i \circ \sigma^{m-j}(c) t^{m-j} \\ &= \sum_{i=0}^{j-1} p_i \sigma^{i+m-j}(c) t^{i+m-j} + \sum_{i=0}^{m-1} p_j \sigma^m(c) a_i t^i,\end{aligned}$$

must be equal for all $c \in S$. Comparing the coefficients of t^i yields

$$p_j(a_i \sigma^i(c) - \sigma^m(c) a_i) = 0$$

for all $c \in S$, $i \in \{0, \dots, m-1\}$, thus $a_i \sigma^i(c) - \sigma^m(c) a_i = 0$ since S is a domain and $p_j \neq 0$. This implies S_f is associative by Proposition 7.3, a contradiction. Thus $p = p_0 \in S$.

Now suppose $a_l \notin \mathrm{Fix}(\sigma)$ for some $l \in \{0, \dots, m-1\}$. As before let $0 \neq p = \sum_{i=0}^{m-1} p_i t^i \in \mathrm{Nuc}_l(S_f)$ be arbitrary and $j \in \{0, \dots, m-1\}$ be maximal such that $p_j \neq 0$. Suppose towards a contradiction $j > 0$.

If $j = 1$ then

$$\begin{aligned}(p \circ t^{m-1}) \circ t &= \Big(p_0 t^{m-1} + p_1 \sum_{i=0}^{m-1} a_i t^i\Big) \circ t \\ &= p_0 \sum_{i=0}^{m-1} a_i t^i + \sum_{i=0}^{m-2} p_1 a_i t^{i+1} + p_1 a_{m-1} \sum_{i=0}^{m-1} a_i t^i\end{aligned}$$

and

$$p \circ (t^{m-1} \circ t) = p_0 \sum_{i=0}^{m-1} a_i t^i + p_1 \sum_{i=0}^{m-2} \sigma(a_i) t^{i+1} + p_1 \sigma(a_{m-1}) \sum_{i=0}^{m-1} a_i t^i$$

must be equal. Comparing the coefficients of t^0 yields

$$p_1 a_{m-1} a_0 = p_1 \sigma(a_{m-1}) a_0, \tag{7.12}$$

and comparing the coefficients of t^i yields

$$p_1 a_{i-1} + p_1 a_{m-1} a_i = p_1 \sigma(a_{i-1}) + p_1 \sigma(a_{m-1}) a_i, \tag{7.13}$$

for all $i \in \{1, \dots, m-1\}$.

If $a_{m-1} \in \mathrm{Fix}(\sigma)$ then (7.13) implies $p_1(a_{i-1} - \sigma(a_{i-1})) = 0$, that is $a_i \in \mathrm{Fix}(\sigma)$ for all $i \in \{0, \dots, m-2\}$ because S is a domain and $p_1 \neq 0$, a contradiction since $a_l \notin \mathrm{Fix}(\sigma)$. Therefore $a_{m-1} \notin \mathrm{Fix}(\sigma)$. Let $k \in \{0, \dots, m-1\}$ be minimal such that $a_k \neq 0$. If $k = 0$ then $p_1 = 0$ by (7.12) as S is a domain, a contradiction. Otherwise (7.13) implies $p_1(a_{m-1} - \sigma(a_{m-1}))a_k = 0$, therefore $p_1 = 0$ as S is a domain and $a_{m-1} \notin \mathrm{Fix}(\sigma)$, a contradiction.

Suppose now $j \geq 2$, then

$$\begin{aligned}(p \circ t^{m-j}) \circ t &= \Big(\sum_{i=0}^{j-1} p_i t^{i+m-j} + p_j \sum_{i=0}^{m-1} a_i t^i \Big) \circ t \\ &= \sum_{i=0}^{j-2} p_i t^{i+m-j+1} + p_{j-1} \sum_{i=0}^{m-1} a_i t^i + p_j \sum_{i=0}^{m-2} a_i t^{i+1} + p_j a_{m-1} \sum_{i=0}^{m-1} a_i t^i\end{aligned}$$

and

$$\begin{aligned}p \circ (t^{m-j} \circ t) &= \sum_{i=0}^{j} p_i t^i \circ t^{m-j+1} \\ &= \sum_{i=0}^{j-2} p_i t^{i+m-j+1} + p_{j-1} \sum_{i=0}^{m-1} a_i t^i + p_j \sum_{i=0}^{m-2} \sigma(a_i) t^{i+1} + p_j \sigma(a_{m-1}) \sum_{i=0}^{m-1} a_i t^i\end{aligned}$$

must be equal. Comparing them gives

$$p_j a_{m-1} a_0 = p_j \sigma(a_{m-1}) a_0, \tag{7.14}$$

and

$$p_j a_{i-1} + p_j a_{m-1} a_i = p_j \sigma(a_{i-1}) + p_j \sigma(a_{m-1}) a_i. \tag{7.15}$$

This yields a contradiction similar to the $j = 1$ case. Therefore $p = p_0 \in S$ and so $\mathrm{Nuc}_l(S_f) \subseteq S$.

(ii) The proof that $\mathrm{Nuc}_m(S_f) \subseteq S$ is similar to (i), but we look at $(t^{m-j} \circ p) \circ c = t^{m-j} \circ (p \circ c)$ and $(t^{m-j} \circ p) \circ t = t^{m-j} \circ (p \circ t)$ instead.

$\square$

When S is a domain and δ is not necessarily 0, we can prove a similar result to Theorem 7.12 for polynomials of degree 2:

Proposition 7.13. *Let S be a domain and $f(t) = t^2 - a_1 t - a_0 \in S[t;\sigma,\delta]$ be such that one of the following holds:*

(i) $a_1 \in \mathrm{Fix}(\sigma)$ *and* $a_0 \notin \mathrm{Const}(\delta)$.

(ii) $a_1 \in \mathrm{Fix}(\sigma)$, $a_0 \in \mathrm{Fix}(\sigma)$ *and* $a_1 \notin \mathrm{Const}(\delta)$.

(iii) $a_1 \in \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$ *and* $a_0 \notin \mathrm{Fix}(\sigma)$.

(iv) $a_1 \notin \mathrm{Fix}(\sigma)$ *and* $a_0 \in \mathrm{Const}(\delta)$.

(v) $a_1 \notin \mathrm{Fix}(\sigma)$, $a_0 \in \mathrm{Fix}(\sigma)$ *and* $a_1 \in \mathrm{Const}(\delta)$.

Then $\mathrm{Nuc}_l(S_f) = \mathrm{Nuc}_m(S_f) = S$.

Proof. Recall $S \subseteq \mathrm{Nuc}_l(S_f)$ by Theorem 7.9. We prove the reverse inclusion: Suppose $p = p_0 + p_1 t \in \mathrm{Nuc}_l(S_f)$ for some $p_0, p_1 \in S$, then

$$\begin{aligned}(p \circ t) \circ t &= (p_0 t + p_1(a_1 t + a_0)) \circ t \\ &= p_0(a_1 t + a_0) + p_1 a_1 (a_1 t + a_0) + p_1 a_0 t \\ &= p_0 a_0 + p_1 a_1 a_0 + \big(p_0 a_1 + p_1 a_1^2 + p_1 a_0\big) t,\end{aligned}$$

and

$$p \circ (t \circ t) = (p_0 + p_1 t) \circ (a_1 t + a_0)$$

$$
\begin{aligned}
&= p_0a_1t + p_0a_0 + p_1(\sigma(a_0)t + \delta(a_0)) + p_1(\sigma(a_1)t + \delta(a_1)) \circ t \\
&= p_0a_1t + p_0a_0 + p_1\sigma(a_0)t + p_1\delta(a_0) + p_1\sigma(a_1)(a_1t + a_0) + p_1\delta(a_1)t \\
&= p_0a_0 + p_1\sigma(a_1)a_0 + p_1\delta(a_0) + \big(p_0a_1 + p_1\sigma(a_1)a_1 + p_1\delta(a_1) + p_1\sigma(a_0)\big)t,
\end{aligned}
$$

must be equal. Comparing the coefficients of t yields

$$p_1a_1a_0 = p_1\sigma(a_1)a_0 + p_1\delta(a_0), \tag{7.16}$$

and

$$p_1a_1^2 + p_1a_0 = p_1\sigma(a_1)a_1 + p_1\sigma(a_0) + p_1\delta(a_1). \tag{7.17}$$

It is a straightforward exercise to check using (7.16) and (7.17) that in each of our five cases we must have $p_1 = 0$ so $p = p_0 \in S$.

We prove $S \subseteq \mathrm{Nuc}_m(S_f)$ similarly but consider instead $(t \circ p) \circ t = t \circ (p \circ t)$. $\square$

8

SOLVABLE CROSSED PRODUCT ALGEBRAS AND APPLICATIONS TO G-ADMISSIBLE GROUPS

In this Chapter, we show that for every finite-dimensional central simple algebra A over a field F, which contains a maximal subfield M with non-trivial $G = \mathrm{Aut}_F(M)$, then G is solvable if and only if A contains a finite chain of subalgebras, which are generalised cyclic algebras over their centers, satisfying certain conditions. This chain of subalgebras is closely related to a normal series of G which exists when G is solvable. In particular, we obtain that a crossed product algebra is solvable if and only if it has such a chain.

Recall from Section 1.4.2, that when D is a finite-dimensional central division algebra over C, $\sigma|_C$ has finite order m and $f(t) = t^m - a \in D[t;\sigma]$, $d \in \mathrm{Fix}(\sigma)^\times$ is right invariant, the associative quotient algebra $D[t;\sigma]/D[t;\sigma]f$ is also called a generalised cyclic algebra and denoted (D, σ, a). For this Chapter, we extend the definition of a generalised cyclic algebra, to where we do not require D be a division algebra:

Definition. *Let S be a finite dimensional central simple algebra of degree n over C and $\sigma \in \mathrm{Aut}(S)$ be such that $\sigma|_C$ has finite order m. We define the* ***generalised cyclic algebra*** *(S, σ, a) to be the associative algebra of the form $S_f = S[t;\sigma]/S[t;\sigma]f$ where $f(t) = t^m - a \in S[t;\sigma]$, $a \in \mathrm{Fix}(\sigma)^\times$ is right invariant. (S, σ, a) is a central simple algebra over $F = \mathrm{Fix}(\sigma) \cap C$ of degree mn [10, p. 4].*

Definition. *Let F be a field and A be a central simple algebra over F of degree n. A is called a G-**crossed product algebra** or **crossed product algebra** if it* *contains a field extension M/F which is Galois of degree n with Galois group $G = \mathrm{Gal}(M/F)$.*

Equivalently we can define a (G)-crossed product algebra $(M, G, \mathfrak{a})$ over F via factor sets starting with a finite Galois field extension as follows: Suppose M/F is a finite Galois field extension of degree n with Galois group G and $\{a_{\sigma,\tau} \mid \sigma, \tau \in G\}$ is a set of elements of $M^\times$ such that

$$a_{\sigma,\tau} a_{\sigma\tau,\rho} = a_{\sigma,\tau\rho} \sigma(a_{\tau,\rho}), \tag{8.1}$$

for all $\sigma, \tau, \rho \in G$. Then a map $\mathfrak{a} : G \times G \to M^\times$, $(\sigma, \tau) \mapsto a_{\sigma,\tau}$, is called a ***factor set*** *or* ***2-cocycle*** *of G.*

An associative multiplication is defined on the F-vector space $\bigoplus_{\sigma \in G} M x_\sigma$ by

$$x_\sigma m = \sigma(m) x_\sigma, \tag{8.2}$$

$$x_\sigma x_\tau = a_{\sigma,\tau} x_{\sigma\tau}, \tag{8.3}$$

for all $m \in M$, $\sigma, \tau \in G$. This way $\bigoplus_{\sigma \in G} M x_\sigma$ becomes an associative central simple F-algebra that contains a maximal subfield isomorphic to M. This algebra is denoted $(M, G, \mathfrak{a})$ and is called a G-crossed product algebra over F. If G is solvable then A is also called a ***solvable G-crossed product algebra*** *over F.*

8.1 CROSSED PRODUCT SUBALGEBRAS OF CENTRAL SIMPLE ALGEBRAS

Let M/F be a field extension of degree n and $G = \mathrm{Aut}_F(M)$ be the group of automorphisms of M which fix the elements of F. Let A be a central simple algebra of degree n over F and suppose M is contained in A, this makes M a maximal subfield of A [6, Lemma 15.1]. Such maximal subfields do not always exist for a general central simple algebra [6, Remark 15.4], however they always exists for example when A is a division algebra [6, Corollary 15.6]. We denote by $A^\times$ the set of invertible elements of A, and for a subset B in A, denote $\mathrm{Cent}_A(B)$ the centralizer of B in A.

Some of the results in this Chapter, namely Lemma 8.3, Corollary 8.4 and Theorems 8.1, 8.7, are stated for central division algebras A over F by Petit in [52, §7], and none of them are proved there. The following generalises [52, (27)] to central simple algebras with a maximal subfield M as above. The result was before only stated for division algebras and also not in terms of crossed product algebras:

Theorem 8.1. *(i) A contains a subalgebra $M(G)$ which is a crossed product algebra $(M, G, \mathfrak{a})$ of degree $|G|$ over* $\mathrm{Fix}(G)$ *with maximal subfield M.*

(ii) A is equal to $M(G)$ if and only if M is a Galois extension of F. In this case A is a G-crossed product algebra over F.

(iii) For any subgroup H of G, there is an F-subalgebra $M(H)$ of both $M(G)$ and A, which is a H-crossed product algebra of degree $|H|$ over $\mathrm{Fix}(H)$ *with maximal subfield M.*

Proof. (i) Define $M(G) = \mathrm{Cent}_A(\mathrm{Fix}(G))$, then $M(G)$ is a central simple algebra over $\mathrm{Fix}(G)$ by the Centralizer Theorem for central simple algebras [6, Theorem III.5.1]. Furthermore, since M is a maximal subfield of $M(G)$ and $M/\mathrm{Fix}(G)$ is a Galois field extension with Galois group G, we conclude $M(G)$ is a G-crossed product algebra.

(ii) Notice $[M : F] = n$, A has dimension n^2 over F, and $M(G)$ has a basis $\{x_\sigma | \sigma \in G\}$ as a vector space over M. If M is not a Galois extension of F, then $|G| < n$ and thus $\{x_\sigma \mid \sigma \in G\}$ cannot be a set of generators for A as a vector space over M. Conversely, if M/F is a Galois extension, then $|G| = n$ and since $\{x_\sigma \mid \sigma \in G\}$ is linearly independent over M, counting dimensions yields $M(G) = A$. The rest of the assertion is trivial.

(iii) For any subgroup H of G, let $M(H) = \mathrm{Cent}_A(\mathrm{Fix}(H))$. Since $\mathrm{Fix}(G) \subseteq \mathrm{Fix}(H)$, we have $M(H) = \mathrm{Cent}_A(\mathrm{Fix}(H))$ is contained in $M(G) = \mathrm{Cent}_A(\mathrm{Fix}(G))$ The proof now follows exactly as in (i).

□

Remark. *When A has prime degree over F and M/F is not a Galois extension then $M(G) = M$: $M(G)$ is a simple subalgebra of A by Theorem 8.1(i), therefore* $\dim_F(M(G))$ *divides* $\dim_F(A) = n^2$ *by the Centralizer Theorem for central simple algebras [6, Theorem III.5.1]. Now $M(G)$ contains M and $M(G)$ is equal to A if and only if M/F is a Galois extension by Theorem 8.1(ii). As n is prime and M/F is not Galois, this means $M(G) = M$.*

A close look at the proof of Theorem 8.1 yields the following observations:

Lemma 8.2. *(i) Given any subgroup H of G, $M(H)$ is a H-crossed product algebra over its center with $M(H) = (M, H, \mathfrak{a}_H)$, where $\mathfrak{a}_H$ denotes the factor set of the G-crossed product algebra $M(G) = (M, G, \mathfrak{a})$ restricted to the elements of H.*

(ii) For any subgroup H of G, $M(H)$ is the centralizer of $\mathrm{Fix}(H)$ *in A.*

The following generalises [52, (26)] to any central simple algebra A with a maximal subfield M as above. Again it was previously only stated and not proved for central division algebras:

Lemma 8.3. *(i) For any $\sigma \in G$ there exists $x_\sigma \in A^\times$ such that the inner automorphism*

$$I_{x_\sigma} : A \to A,\ y \mapsto x_\sigma y x_\sigma^{-1}$$

restricted to M is σ.

(ii) Given any $\sigma \in G$, we have $\{x \in A^\times \mid I_x|_M = \sigma\} = M^\times x_\sigma$.

(iii) The set of cosets $\{M^\times x_\sigma \mid \sigma \in G\}$ with multiplication given by

$$M^\times x_\sigma M^\times x_\tau = M^\times x_{\sigma\tau},$$

is a group isomorphic to G, where σ and $M^\times x_\sigma$ correspond under this isomorphism.

Proof. A contains the G-crossed product algebra $M(G)$ by Theorem 8.1, thus (i) and (iii) follows from (8.2) and (8.3). For (ii) we have

$$I_{mx_\sigma}(y) = (mx_\sigma)y(mx_\sigma)^{-1} = (mx_\sigma)y(x_\sigma^{-1}m^{-1}) = m\sigma(y)m^{-1} = \sigma(y)$$

for all $m, y \in M^\times$, and thus $M^\times x_\sigma \subset \{x \in A^\times \mid I_x|_M = \sigma\}$.

Suppose $u \in \{x \in A^\times \mid I_x|_M = \sigma\}$. Then as u and x_σ are invertible, we can write $u = vx_\sigma$ for some $v \in A^\times$. We are left to prove that $v \in M^\times$. We have

$$\sigma(y) = I_u(y) = (vx_\sigma)y(vx_\sigma)^{-1} = vx_\sigma y x_\sigma^{-1} v^{-1} = v\sigma(y)v^{-1},$$

for all $y \in M$, and so $\sigma(y)v = v\sigma(y)$ for all $y \in M$, that is $mv = vm$ for all $m \in M$ since σ is bijective. Therefore v is contained in the centralizer of M in A, which is equal to M because M is a maximal subfield of A.

□

The following generalises [52, (28)]:

Corollary 8.4. *If H is a cyclic subgroup of G of order $h > 1$ generated by σ, then there exists $c \in \mathrm{Fix}(\sigma)^\times$ such that*

$$M(H) \cong (M/\mathrm{Fix}(\sigma), \sigma, c) = M[t;\sigma]/M[t;\sigma](t^h - c),$$

is a cyclic algebra of degree h over $\mathrm{Fix}(\sigma)$.

Proof. $M(H)$ is a H-crossed product algebra of degree h over $\mathrm{Fix}(\sigma)$ by Theorem 8.1. Moreover H is a cyclic group and so $M(H)$ is a cyclic algebra of degree h over $\mathrm{Fix}(\sigma)$ (see for example [57, p. 49]). This means there exists $c \in \mathrm{Fix}(\sigma)^\times$ such that $M(H) \cong (M/\mathrm{Fix}(\sigma), \sigma, c)$. □

In particular, we conclude that if a central division algebra A over F contains a maximal subfield M and non-trivial $\sigma \in \mathrm{Aut}_F(M)$ of order h, then it contains a cyclic division algebra of degree h, (though not necessarily with center F). This is the case even if A is a noncrossed product (i.e. if A is not a crossed product algebra):

Theorem 8.5. *([10, Theorem 4]). Let A be a central division algebra of degree n over F with maximal subfield M and non-trivial $\sigma \in \mathrm{Aut}_F(M)$ of order h. Then A contains a cyclic division algebra $(M/\mathrm{Fix}(\sigma), \sigma, c)$ of degree h over* $\mathrm{Fix}(\sigma)$ *as a subalgebra.*

Proof. This follows immediately from Corollary 8.4. □

It is well-known that a central division algebra of prime degree over F is a cyclic algebra if and only if it contains a cyclic subalgebra of prime degree (though not necessarily with center F) [49, p. 2]. Together with Theorem 8.5 this yields the following:

Corollary 8.6. *([10, Corollary 6]). Let A be a central division algebra over F of prime degree p. Then either A is a cyclic algebra or each of its maximal subfields M has trivial automorphism group $\mathrm{Aut}_F(M)$.*

Proof. Suppose $G = \mathrm{Aut}_F(M)$ is non-trivial, then there exists a non-trivial $\sigma \in \mathrm{Aut}_F(M)$ of finite order h. Thus A contains a cyclic division algebra of degree h over $\mathrm{Fix}(\sigma)$ as a subalgebra. Looking at the possible intermediate field extensions of M/F yields $[M : \mathrm{Fix}(\sigma)]$ is either 1 or p. Since G is not trivial, $[M : \mathrm{Fix}(\sigma)] = h = p$, thus A contains a cyclic subalgebra of prime degree and so is itself a cyclic algebra. □

8.2 CENTRAL SIMPLE ALGEBRAS CONTAINING A MAXIMAL SUBFIELD M WITH SOLVABLE F-AUTOMORPHISM GROUP

Suppose G is a finite solvable group, then there exists a chain of subgroups

$$\{1\} = G_0 < G_1 < \ldots < G_k = G, \tag{8.4}$$

such that G_j is normal in G_{j+1} and G_{j+1}/G_j is cyclic of prime order q_j for all $j \in \{0, \ldots, k-1\}$, i.e.

$$G_{j+1}/G_j = \{G_j, G_j\sigma_{j+1}, \ldots\}, \tag{8.5}$$

for some $\sigma_{j+1} \in G_{j+1}$. Theorem 8.1, Corollary 8.4 and Lemma 8.3 lead us to the following generalisation of [52, (29)]. As before, the result was previously only stated (and not proved) for central division algebras over F, and also without the connection to crossed product algebras:

Theorem 8.7. *Let M/F be a field extension of degree n with non-trivial solvable $G = \mathrm{Aut}_F(M)$, and A be a central simple algebra of degree n over F with maximal subfield M. Then there exists a chain of subalgebras*

$$M = A_0 \subset A_1 \subset \ldots \subset A_k = M(G) \subseteq A, \tag{8.6}$$

of A which are G_i-crossed product algebras over $Z_i = \mathrm{Fix}(G_i)$, and where

$$A_{i+1} \cong A_i[t_i; \tau_i] / A_i[t_i; \tau_i](t_i^{q_i} - c_i), \tag{8.7}$$

for all $i \in \{0, \ldots, k-1\}$, such that

(i) *q_i is the prime order of the factor group G_{i+1}/G_i in the chain* (8.4),

(ii) *τ_i is an F-automorphism of A_i of inner order q_i which restricts to $\sigma_{i+1} \in G_{i+1}$ which generates G_{i+1}/G_i, and*

(iii) *$c_i \in \mathrm{Fix}(\tau_i)$ is invertible.*

Note that the inclusion $M(G) \subseteq A$ in (8.6) is an equality if and only if M/F is a Galois extension by Theorem 8.1. In this case A is a solvable G-crossed product algebra.

Proof. Define $A_i = M(G_i)$ for all $i \in \{1, \ldots, k\}$. A_i is a G_i-crossed product algebra over $\mathrm{Fix}(G_i)$ by Theorem 8.1.

$G_1/G_0 \cong G_1$ is a cyclic subgroup of G of prime order q_0 generated by some $\sigma_1 \in G$. Let $\tau_0 = \sigma_1$, then there exists $c_0 \in \mathrm{Fix}(\tau_0)^\times$ such that $A_1 = M(G_1)$ is F-isomorphic to

$$M[t_0; \tau_0] / M[t_0; \tau_0](t_0^{q_0} - c_0),$$

by Corollary 8.4, which is a cyclic algebra of prime degree q_0 over $\mathrm{Fix}(\tau_0)$.

Now $G_1 \triangleleft G_2$ and G_2/G_1 is cyclic of prime order q_1 with

$$G_2/G_1 = \{(G_1\sigma_2)^i \mid i \in \mathbb{Z}\} = \{G_1, G_1\sigma_2, \ldots, G_1\sigma_2^{q_1-1}\}, \tag{8.8}$$

for some $\sigma_2 \in G_2$. Hence we can write $G_2 = \{h\sigma_2^i \mid h \in G_1, 0 \leq i \leq q_1 - 1\}$ and thus the crossed product algebra $A_2 = M(G_2)$ has a basis

$$\{x_{h\sigma_2^j} \mid h \in G_1,\ 0 \leq j \leq q_1 - 1\},$$

as an M-vector space. Recall $M^\times x_{h\sigma_2^j} = M^\times x_h x_{\sigma_2^j} = M^\times x_h x_{\sigma_2}^j$ for all $h \in G_1$ by Lemma 8.3, and $\{1, x_{\sigma_2}, \ldots, x_{\sigma_2}^{q_1-1}\}$ is a basis for A_2 as a left A_1-module, i.e.

$$A_2 = A_1 + A_1 x_{\sigma_2} + \ldots + A_1 x_{\sigma_2}^{q_1-1}. \tag{8.9}$$

We have $G_2 G_1 = G_1 G_2$ as G_1 is normal in G_2 and so for every $h \in G_1$, we get $\sigma_2 h = h' \sigma_2$ for some $h' \in G_1$. Choose the basis $\{x_h \mid h \in G_1\}$ of A_1 as a vector space over M. By (8.3) we obtain

$$x_{\sigma_2} x_h = a_{\sigma_2,h} x_{\sigma_2 h} = a_{\sigma_2,h} x_{h'\sigma_2} = a_{\sigma_2,h} (a_{h',\sigma_2})^{-1} x_{h'} x_{\sigma_2}. \tag{8.10}$$

Recall $x_{\sigma_2} \in A^\times$ by Lemma 8.3. The inner automorphism

$$\tau_1 : A \to A, \ z \mapsto x_{\sigma_2} z x_{\sigma_2}^{-1}$$

restricts to σ_2 on M. Moreover,

$$\begin{aligned} \tau_1(x_h) &= x_{\sigma_2} x_h x_{\sigma_2}^{-1} = a_{\sigma_2,h} (a_{h',\sigma_2})^{-1} x_{h'} x_{\sigma_2} x_{\sigma_2}^{-1} \\ &= a_{\sigma_2,h} (a_{h',\sigma_2})^{-1} x_{h'} \in A_1, \end{aligned} \tag{8.11}$$

for all $h \in G_1$, i.e. $\tau_1|_{A_1}(y) \in A_1$ for all $y \in A_1$ and so $\tau_1|_{A_1}$ is an F-automorphism of A_1. Furthermore, $x_{\sigma_2} x_h = \tau_1|_{A_1}(x_h) x_{\sigma_2}$, for all $h \in G_1$ by (8.10), (8.11), and

$$x_{\sigma_2} m = \sigma_2(m) x_{\sigma_2} = \tau_1|_{A_1}(m) x_{\sigma_2},$$

for all $m \in M$. We conclude that

$$x_{\sigma_2} y = \tau_1|_{A_1}(y) x_{\sigma_2} \tag{8.12}$$

for all $y \in A_1$ by distributivity. Define $c_1 = x_{\sigma_2}^{q_1}$, then $\sigma_2^{q_1} \in G_1$ by (8.8) which implies $c_1 \in A_1$. Furthermore c_1 is invertible since x_{σ_2} is invertible. Also, $\tau_1|_{A_1}(c_1) = x_{\sigma_2} x_{\sigma_2}^{q_1} x_{\sigma_2}^{-1} = c_1$ which means $c_1 \in \mathrm{Fix}(\tau_1|_{A_1})^\times$. Since

$$x_{\sigma_2^{-q_1}} x_{\sigma_2^{q_1}} = a_{\sigma_2^{-q_1}, \sigma_2^{q_1}} x_{\mathrm{id}} \in M^\times,$$

it follows that $c_1^{-1} = x_{\sigma_2^{q_1}}^{-1} \in M^\times x_{\sigma_2^{-q_1}} \in A_1$ as $\sigma_2^{-q_1} \in G_1$. Hence $\tau_1|_{A_1}$ has inner order q_1, as indeed $(\tau_1|_{A_1})^{q_1} : A_1 \to A_1, z \mapsto c_1 z c_1^{-1}$, is an inner automorphism.

Consider the algebra

$$B_2 = A_1[t_1; \tau_1|_{A_1}] / A_1[t_1; \tau_1|_{A_1}](t_1^{q_1} - c_1)$$

with center

$$\mathrm{Cent}(B_2) \supset \{b \in A_1 \mid bh = hb \text{ for all } h \in B_2\} = \mathrm{Cent}(A_1) \cap \mathrm{Fix}(\tau_1) \supset F.$$

Now, using (8.9) and (8.12), the map

$$\phi : A_2 \to B_2, \; yx_{\sigma_2}^i \mapsto yt_1^i \qquad (y \in A_1),$$

can readily be seen to be an isomorphism between F-algebras. Indeed, it is clearly bijective and F-linear. In addition, we have

$$\begin{aligned}
\phi\big((yx_{\sigma_2}^i)(zx_{\sigma_2}^j)\big) &= \phi\big(y\tau_1|_{A_1}^i(z)x_{\sigma_2}^i x_{\sigma_2}^j\big) \\
&= \begin{cases} \phi\big(y\tau_1|_{A_1}^i(z)x_{\sigma_2}^{i+j}\big) & \text{if } i+j < q_1, \\ \phi\big(y\tau_1|_{A_1}^i(z)x_{\sigma_2}^{q_1} x_{\sigma_2}^{i+j-q_1}\big) & \text{if } i+j \geq q_1, \end{cases} \\
&= \begin{cases} y\tau_1|_{A_1}^i(z)t^{i+j} & \text{if } i+j < q_1, \\ y\tau_1|_{A_1}^i(z)c_1 t^{i+j-q_1} & \text{if } i+j \geq q_1, \end{cases}
\end{aligned}$$

by (8.12), and

$$\begin{aligned}
\phi(yx_{\sigma_2}^i) \circ \phi(zx_{\sigma_2}^j) = (yt^i) \circ (zt^j) &= \begin{cases} y\tau_1|_{A_1}^i(z)t^{i+j} & \text{if } i+j < q_1, \\ y\tau_1|_{A_1}^i(z)t^{i+j-q_1}c_1 & \text{if } i+j \geq q_1, \end{cases} \\
&= \begin{cases} y\tau_1|_{A_1}^i(z)t^{i+j} & \text{if } i+j < q_1, \\ y\tau_1|_{A_1}^i(z)c_1 t^{i+j-q_1} & \text{if } i+j \geq q_1, \end{cases}
\end{aligned}$$

for all $y, z \in A_1$, $i, j \in \{0, \dots, q_1 - 1\}$. By distributivity we conclude ϕ is also multiplicative, thus an isomorphism between F-algebras. Continuing in this manner for $G_2 \lhd G_3$ etc. yields the assertion. $\square$

Remarks. *(i) If A is a division algebra, the algebras A_i in Theorem 8.7 are also division algebras, being subalgebras of the finite-dimensional algebra A.*

(iii) The algebras A_i in Theorem 8.7 are associative being subalgebras of the associative algebra A. Therefore $t_i^{q_i} - c_i \in A_i[t_i;\tau_i]$ are right invariant for all $i \in \{0, \dots, k-1\}$ by [55, Theorem 4].

We obtain the following straightforward observations about Theorem 8.7:

Corollary 8.8. *Let M/F be a field extension of degree n with non-trivial solvable $G = \mathrm{Aut}_F(M)$, and A be a central simple algebra of degree n over F with maximal subfield M. Consider the algebras $A_i = M(G_i)$ as in Theorem 8.7.*

(i) $A_i = \mathrm{Cent}_A(\mathrm{Fix}(G_i))$ for all $i \in \{0, \dots, k-1\}$.

(ii) A_i is a crossed product algebra over $Z_i = \mathrm{Fix}(G_i)$ of degree $|G_i| = \prod_{l=0}^{i-1} q_l$ for all $i \in \{1, \dots, k-1\}$.

(iii) $M = Z_0 \supset \dots \supset Z_{k-1} \supset Z_k \supset F$.

(iv) Z_{i-1}/Z_i has prime degree q_{i-1} for all $i \in \{1, \dots, k\}$.

(v) M/Z_i is a Galois field extension and M is a maximal subfield of A_i for all $i \in \{0, \dots, k\}$.

(vi) [10, Corollary 10] A_i is a generalised cyclic algebra over Z_i for all $i \in \{0, \dots, k\}$.

(vii) A contains the cyclic algebra

$$(M/\mathrm{Fix}(\sigma_1), \sigma_1, c_0) \cong M[t_0;\sigma_1]/M[t_0;\sigma_1](t_0^{q_0} - c_0),$$

of prime degree q_0 over $\mathrm{Fix}(\sigma_1)$.

Proof. (i) This is Lemma 8.2.

(ii) A_i has degree $[M : \mathrm{Fix}(G_i)]$ which is equal to $|G_i|$ by the Fundamental Theorem of Galois Theory.

(iii) Follows from the fact that $\{1\} = G_0 \leq G_1 \leq \dots \leq G_k = G$ and $Z_i = \mathrm{Fix}(G_i)$.

(iv) We have $n = [M : F] = [M : Z_i][Z_i : F] = |G_i|[Z_i : F]$ for all i by the Fundamental Theorem of Galois Theory, therefore

$$[Z_{i-1} : Z_i] = \frac{[Z_{i-1} : F]}{[Z_i : F]} = \frac{|G_i|}{|G_{i-1}|} = q_{i-1},$$

for all $i \in \{1, \dots, k\}$ as required.

(v) $M/\mathrm{Fix}(G_i)$ is a Galois field extension with Galois group G_i by Galois Theory. The rest of the assertion is trivial by Theorem 8.7.

(vii) $G_1 = \langle \sigma_1 \rangle$ is a cyclic subgroup of G of order q_0, therefore the result follows by Corollary 8.4.

□

Corollary 8.9. *([10, Corollaries 9, 11]). Let A be a central division algebra over F containing a maximal subfield M with non-trivial solvable $G = \mathrm{Aut}_F(M)$.*

(i) There is a non-central element $t_0 \in A$ such that $t_0^{q_0} \in \mathrm{Fix}(\sigma_1)^\times$ and $t_0^m \notin \mathrm{Fix}(\sigma_1)$ for all $m \in \{1, \dots, q_0 - 1\}$.

(ii) A contains a chain of generalised cyclic division algebras A_i over intermediate fields $Z_i = \mathrm{Fix}(G_i)$ of M/F as in (8.6).

Our next result generalises [53, (9)] and characterises all the algebras with a maximal subfield M/F that have a non-trivial solvable automorphism group $G = \mathrm{Aut}_F(M)$:

Theorem 8.10. *Let M/F be a field extension of degree n with non-trivial $G = \mathrm{Aut}_F(M)$, and A be a central simple algebra of degree n over F containing M. Then G is solvable if there exists a chain of subalgebras*

$$M = A_0 \subset A_1 \subset \dots \subset A_k \subseteq A \tag{8.13}$$

of A which all have maximal subfield M, where A_k is a G-crossed product algebra over $\mathrm{Fix}(G)$, and where

$$A_{i+1} \cong A_i[t_i; \tau_i]/A_i[t_i; \tau_i](t_i^{q_i} - c_i), \tag{8.14}$$

for all $i \in \{0, \dots, k-1\}$, with *(i)* q_i *a prime,*

(ii) τ_i *an F-automorphism of* A_i *of inner order* q_i *which restricts to an automorphism* $\sigma_{i+1} \in G$*, and*

(iii) $c_i \in \mathrm{Fix}(\tau_i)^\times$.

Proof. Suppose there exists a chain of algebras A_i, $i \in \{0, \ldots, k\}$ satisfying the above assumptions. Put $G_k = G$. Each A_i has center $Z_i = Z_{i-1} \cap \mathrm{Fix}(\tau_{i-1})$ by Corollary 7.5, so that by induction

$$Z_i = \mathrm{Fix}(\tau_0) \cap \mathrm{Fix}(\tau_1) \cap \cdots \cap \mathrm{Fix}(\tau_{i-1}) \supset F,$$

in particular $Z_i \subseteq M$.

M/Z_i is a Galois extension contained in A_i: Let H_i be the subgroup of G generated by $\sigma_1, \ldots, \sigma_i$, $i \in \{1, \ldots, k\}$. Then

$$\begin{aligned} Z_i &= \mathrm{Fix}(\tau_0) \cap \mathrm{Fix}(\tau_1) \cap \cdots \cap \mathrm{Fix}(\tau_{i-1}) \\ &= M \cap \mathrm{Fix}(\tau_0) \cap \mathrm{Fix}(\tau_1) \cap \cdots \cap \mathrm{Fix}(\tau_{i-1}) \\ &= \mathrm{Fix}(\sigma_1) \cap \cdots \cap \mathrm{Fix}(\sigma_i) = \mathrm{Fix}(H_i), \end{aligned}$$

so M/Z_i is a Galois field extension by Galois theory. Put $G_i = \mathrm{Gal}(M/Z_i)$, then each A_i is a G_i-crossed product algebra. In particular, G_i is a subgroup of G_{i+1}.

We use induction to prove that each G_i, thus G, is a solvable group. For $i = 1$,

$$A_1 \cong M[t_0; \sigma_1]/M[t_0; \sigma_1](t_0^{q_0} - c_0)$$

is a cyclic algebra of degree q_0 over $\mathrm{Fix}(\sigma_1)$. $G_1 = \langle \sigma_1 \rangle$ is a cyclic group of prime order q_0 and therefore solvable.

We assume as induction hypothesis that if there exists a chain

$$M = A_0 \subset \ldots \subset A_j$$

of algebras such that (8.14) holds for all $i \in \{0, \ldots, j-1\}$, $j \geq 1$, then G_j is solvable. For the induction step we take a chain of algebras $M = A_0 \subset \ldots \subset A_j \subset A_{j+1}$,

$$A_{i+1} \cong A_i[t_i; \tau_i]/A_i[t_i; \tau_i](t_i^{q_i} - c_i)$$

where τ_i is an automorphism of A_i of inner order q_i which induces an automorphism $\sigma_{i+1} \in G$, $c_i \in \mathrm{Fix}(\tau_i)$ is invertible and q_i is prime, for all $i \in \{0, \dots, j\}$. By the induction hypothesis, G_j is a solvable group.

We show that G_{j+1} is solvable: t_j is an invertible element of

$$A_{j+1} \cong A_j[t_j; \tau_j] / A_j[t_j; \tau_j](t_j^{q_j} - c_j),$$

with inverse $c_j^{-1} t_j^{q_j - 1}$. A_j is a G_j-crossed product algebra over Z_j with maximal subfield M. The F-automorphism τ_j on A_j satisfies $t_j l = \tau_j(l) t_j$ for all $l \in A_j$ which implies the inner automorphism

$$I_{t_j} : A \to A,\ d \mapsto t_j d t_j^{-1}$$

restricts to τ_j on A_j and so also restricts to σ_{j+1} on M.

For any $\sigma \in G$ there exists an invertible $x_\sigma \in A$ such that the inner automorphism

$$I_{x_\sigma} : A \to A,\ y \mapsto x_\sigma y x_\sigma^{-1}$$

restricted to M is σ by Lemma 8.3. Hence we have $x_{\sigma_{j+1}} = t_j$ with $x_{\sigma_{j+1}}$ as defined in Lemma 8.3. We know that $\{1, t_j, \dots, {t_j}^{q_j - 1}\}$ is a basis for A_{j+1} as a left A_j-module. By (8.3) we have $x_{\sigma_{j+1}^2} = a_1 {t_j}^2$, $x_{\sigma_{j+1}^3} = a_2 {t_j}^3, \dots$ for suitable $a_i \in M^\times$, so that w.l.o.g. $\{1, x_{\sigma_{j+1}}, \dots, x_{\sigma_{j+1}^{q_j - 1}}\}$ is a basis for A_{j+1} as a left A_j-module.

Since A_j is a G_j-crossed product algebra, it has $\{x_\rho \mid \rho \in G_j\}$ as M-basis, and hence A_{j+1} has basis

$$\{x_\rho x_{\sigma_{j+1}^i} \mid \rho \in G_j,\ 0 \leq i \leq q_j - 1\}$$

as a vector space over M.

Additionally, $x_\rho x_{\sigma_{j+1}^i} \in M^\times x_{\rho \sigma_{j+1}^i}$ by Lemma 8.3 (iii) and thus A_{j+1} has the M-basis

$$\{x_{\rho \sigma_{j+1}^i} \mid \rho \in G_j,\ 0 \leq i \leq q_j - 1\}.$$

Now A_{j+1} is a G_{j+1}-crossed product algebra and thus also has the M-basis $\{x_\sigma \mid \sigma \in G_{j+1}\}$. We use these two basis to show that $G_{j+1} = G_j \langle \sigma_{j+1} \rangle$: Write

$$x_{\rho \sigma_{j+1}^i} = \sum_{\sigma \in G_{j+1}} m_\sigma x_\sigma$$

for some $m_\sigma \in M$, not all zero. Then

$$x_{\rho\sigma_{j+1}^i} m = \sum_{\sigma \in G_{j+1}} m_\sigma x_\sigma m = \sum_{\sigma \in G_{j+1}} m_\sigma \sigma(m) x_\sigma,$$

and

$$x_{\rho\sigma_{j+1}^i} m = \rho\sigma_{j+1}^i(m) x_{\rho\sigma_{j+1}^i} = \rho\sigma_{j+1}^i(m) \sum_{\sigma \in G_{j+1}} m_\sigma x_\sigma,$$

for all $m \in M$. Let $\sigma \in G_{j+1}$ be such that $m_\sigma \neq 0$, then in particular

$$m_\sigma \sigma(m) x_\sigma = \rho\sigma_{j+1}^i(m) m_\sigma x_\sigma,$$

for all $m \in M$, that is $\sigma = \rho\sigma_{j+1}^i$. This means that $\{\rho\sigma_{j+1}^i \mid \rho \in G_j,\ 0 \leq i \leq q_j - 1\} \subseteq G_{j+1}$. Both sets have the same size so must be equal and we conclude $G_{j+1} = G_j \langle \sigma_{j+1} \rangle$.

Finally we prove G_j is a normal subgroup of G_{j+1}: the inner automorphism $I_{x_{\sigma_{j+1}}}$ restricts to the F-automorphism τ_j of A_j. In particular, this implies $x_{\sigma_{j+1}} x_\rho x_{\sigma_{j+1}}^{-1} \in A_j$, for all $\rho \in G_j$. Furthermore,

$$x_{\sigma_{j+1}\rho\sigma_{j+1}^{-1}} \in M^\times x_{\sigma_{j+1}} x_\rho x_{\sigma_{j+1}^{-1}} = M^\times x_{\sigma_{j+1}} x_\rho x_{\sigma_{j+1}}^{-1} \subset A_j,$$

for all $\rho \in G_j$ by Lemma 8.3.

Hence $\sigma_{j+1}\rho\sigma_{j+1}^{-1} \in G_j$ because A_j is a G_j-crossed product algebra. Similarly, we see $\sigma_{j+1}^r \rho \sigma_{j+1}^{-r} \in G_j$ for all $r \in \mathbb{N}$. Let $g \in G_{j+1}$ be arbitrary and write $g = h\sigma_{j+1}^r$ for some $h \in G_j$, $r \in \{0, \ldots, q_j - 1\}$ which we can do because $G_{j+1} = G_j \langle \sigma_{j+1} \rangle$. Then

$$g\rho g^{-1} = (h\sigma_{j+1}^r)\rho(h\sigma_{j+1}^r)^{-1} = h(\sigma_{j+1}^r \rho \sigma_{j+1}^{-r})h^{-1} \in G_j,$$

for all $\rho \in G_j$ so G_j is indeed normal.

It is well-known that a group G is solvable if and only if given a normal subgroup H of G, both H and G/H are solvable. It is clear now that G_{j+1}/G_j is cyclic and hence solvable, which implies G_{j+1} is solvable as required. □

8.3 SOLVABLE CROSSED PRODUCT ALGEBRAS

We now focus on the case when M/F is a Galois field extension:

Suppose M/F is a finite Galois field extension of degree n and A is a central simple algebra of degree n over F with maximal subfield M. i.e. now A is a G-crossed product algebra where $G = \mathrm{Gal}(M/F)$. We obtain the following as a special case of Theorem 8.7 and Corollary 8.8:

Theorem 8.11. *Let A be a G-crossed product algebra of degree n over F with maximal subfield M such that $M/F$is a Galois field extension of degree n with non-trivial solvable $G = \mathrm{Gal}(M/F)$. Then there exists a chain of subalgebras*

$$M = A_0 \subset A_1 \subset \ldots \subset A_k = M(G) = A$$

of A which are generalised cyclic algebras

$$A_{i+1} \cong A_i[t_i;\tau_i]/A_i[t_i;\tau_i](t_i^{q_i} - c_i),$$

of degree $\prod_{l=0}^{i-1} q_l$ over $Z_i = \mathrm{Fix}(G_i)$ for all $i \in \{0,\ldots,k-1\}$, such that

(i) *q_i a prime,*

(ii) *τ_i an F-automorphism of A_i of inner order q_i which restricts to an automorphism $\sigma_{i+1} \in G$,*

(iii) *$c_i \in \mathrm{Fix}(\tau_i)^\times$, and*

(iv) *Z_i/Z_{i-1} has prime degree q_{i-1} and A_i is the centralizer of $\mathrm{Fix}(G_i)$ in A.*

Theorem 8.12. *In the set-up of Theorem 8.11, A is a division algebra if and only if*

$$b\tau_i(b)\cdots\tau_i^{q_i-1}(b) \neq c_i, \tag{8.15}$$

for all $b \in A_i$, for all $i \in \{0,\ldots,k-1\}$.

Proof. Suppose $A_k = A$ is a division algebra, then every subalgebra of A must also be a division algebra as A is finite-dimensional. Therefore A_i are division algebras for all $i \in \{0,\ldots,k\}$. In particular this means

$t_j^{q_j} - c_j \in A_j[t_j; \tau_j]$ are irreducible by Theorem 2.26, thus (8.15) holds for all $b \in A_i$ by [32, Theorem 1.3.16].

Conversely suppose (8.15) holds for all $b \in A_i$, for all $i \in \{0, \ldots, k-1\}$. We prove by induction that A_j is a division algebra for all $j \in \{0, \ldots, k\}$, then in particular $A = A_k$ is a division algebra:

Clearly $A_0 = M$ is a field so in particular is a division algebra. Assume as induction hypothesis A_j is a division algebra for some $j \in \{0, \ldots, k-1\}$. By the proof of Theorem 8.7, $\tau_j^{q_j}$ is the inner automorphism $z \mapsto c_j z c_j^{-1}$ on A_j and τ_j has inner order q_j. Then $A_{j+1} \cong A_j[t_j; \tau_j]/A_j[t_j; \tau_j](t_j^{q_j} - c_j)$ is a division algebra if and only if $t_j^{q_j} - c_j \in A_j[t_j; \tau_j]$ is irreducible, if and only if

$$b\tau_j(b) \cdots \tau_j^{q_j - 1}(b) \neq c_j,$$

for all $b \in A_j$ by [32, Theorem 1.3.16]. Thus A_i is a division algebra for all $i \in \{0, \ldots, k\}$ by induction. $\square$

The following result follows immediately from Theorem 8.10:

Corollary 8.13. *Let A be a G-crossed product algebra of degree n over F with maximal subfield M such that M/F is a Galois field extension of degree n with non-trivial $G = \mathrm{Gal}(M/F)$. Then G is solvable if there exists a chain of subalgebras*

$$M = A_0 \subset A_1 \subset \ldots \subset A_k = A$$

of A which all have maximal subfield M, and are generalised cyclic algebras

$$A_{i+1} \cong A_i[t_i; \tau_i]/A_i[t_i; \tau_i](t_i^{q_i} - c_i),$$

over their centers for all $i \in \{0, \ldots, k-1\}$, where q_i a prime, τ_i an F-automorphism of A_i of inner order q_i which restricts to an automorphism $\sigma_{i+1} \in G$, and $c_i \in \mathrm{Fix}(\tau_i)^{\times}$.

Remark. *Let M/F be a finite Galois field extension with non-trivial solvable Galois group G and A be a solvable crossed product algebra over F with maximal* *subfield M. Careful reading of [1, p. 182-187] shows that Albert constructs the same chain of algebras*

$$A_{i+1} = A_i[t_i;\tau_i]/A_i[t_i;\tau_i](t_i^{q_i} - c_i)$$

inside a solvable crossed product A as we do in Theorem 8.11. However they are not explicitly identified as quotient algebras of skew polynomial rings. We also obtain the converse of Albert's statement in Corollary 8.13. Furthermore, neither Theorems 8.7, 8.10, nor Corollaries 8.8 and 8.9 require M/F to be a Galois field extension, unlike Albert's result which requires M/F to be Galois.

8.4 SOME APPLICATIONS TO G-ADMISSIBLE GROUPS

The following definition is due to Schacher [59]:

Definition. *A finite group G is called **admissible** over a field F, if there exists a G-crossed product division algebra over F.*

Suppose G is a finite solvable group, then we have a chain of normal subgroups $\{1\} = G_0 \leq \ldots \leq G_k = G$, such that $G_j \triangleleft G_{j+1}$ and G_{j+1}/G_j is cyclic of prime order q_j for all $j \in \{0, \ldots, k-1\}$. If G is admissible over F, then Theorem 8.7 implies that the subgroups G_i of G in the chain, are admissible over suitable intermediate fields of M/F:

Theorem 8.14. *Suppose G is a finite solvable group which is admissible over a field F. Then each G_i is admissible over the intermediate field $Z_i = \mathrm{Fix}(G_i)$ of M/F. Furthermore $[Z_i : F] = \prod_{j=i}^{k-1} q_j$ for all $i \in \{1, \ldots, k\}$. In particular G_{k-1} is admissible over $Z_{k-1} = \mathrm{Fix}(G_{k-1})$ which has prime degree q_{k-1} over F.*

Proof. As G is F-admissible there exists a G-crossed product division algebra D over F. By Theorem 8.11, there also exists a chain of G_i-crossed product division algebras A_i over Z_i with maximal subfield M, and M/Z_i is a Galois field extension with $G_i = \mathrm{Gal}(M/Z_i)$. This means G_i is Z_i-admissible. $\square$

Example 8.15. *Let $G = \mathbf{S_4}$, then G is $\mathbb{Q}$-admissible [59, Theorem 7.1], so there exists a finite-dimensional associative central division algebra D over $\mathbb{Q}$, with maximal subfield M such that $M/\mathbb{Q}$ is a finite Galois field extension and* $\mathrm{Gal}(M/\mathbb{Q}) = G$. *Furthermore, G is a finite solvable group, indeed we have the subnormal series*

$$\{\mathrm{id}\} \lhd \langle(12)(34)\rangle \lhd \mathbf{K} \lhd \mathbf{A_4} \lhd \mathbf{S_4},$$

where $\mathbf{K}$ is the Klein four-group and $\mathbf{A_4}$ is the alternating group. We have

$$\mathbf{S_4}/\mathbf{A_4} \cong \mathbb{Z}/2\mathbb{Z}, \ \mathbf{A_4}/\mathbf{K} \cong \mathbb{Z}/3\mathbb{Z},$$

$$\mathbf{K}/\langle(12)(34)\rangle \cong \mathbb{Z}/2\mathbb{Z} \quad \textit{and} \quad \langle(12)(34)\rangle/\{\mathrm{id}\} \cong \mathbb{Z}/2\mathbb{Z}.$$

By Theorem 8.11, there exists a corresponding chain of division algebras

$$M = A_0 \subset A_1 \subset A_2 \subset A_3 \subset A_4 = D$$

over $\mathbb{Q}$, such that

$$A_{i+1} \cong A_i[t_i;\tau_i]/A_i[t_i;\tau_i](t_i^{q_i} - c_i),$$

for all $i \in \{0,1,2,3\}$, where τ_i is an automorphism of A_i, whose restriction to M is $\sigma_{i+1} \in G$, $c_i \in \mathrm{Fix}(\tau_i)^\times$ and τ_i has inner order $2,2,3,2$ for $i = 0,1,2,3$ respectively. Moreover $q_0 = q_1 = q_3 = 2$ and $q_2 = 3$, and A_i has degree $\prod_{l=0}^{i-1} q_l$ over its center Z_i for all $i \in \{1,2,3,4\}$ by Corollary 8.8. In addition, by Theorem 8.14 we conclude:

(i) $\mathbf{A_4}$ *is admissible over Z_3, where $Z_3 \subset M$ is a quadratic field extension of $\mathbb{Q}$.*

(ii) $\mathbf{K}$ *is admissible over $Z_2 \subset M$, where Z_2 is a simple field extension of Z_3 of degree $q_2 = 3$. Therefore Z_2 is a simple field extension of $\mathbb{Q}$ of degree $q_2q_3 = 6$ as any finite field extension of $\mathbb{Q}$ is simple.*

(iii) $\langle(12)(34)\rangle$ *is admissible over $Z_1 \subset M$, where Z_1 is a simple field extension of Z_2 of degree $q_1 = 2$. Therefore Z_1 is a simple extension of $\mathbb{Q}$ of degree $q_1q_2q_3 = 12$.*

Schacher proved that for every finite group G, there exists an algebraic number field F such that G is admissible over F [59, Theorem 9.1]. Combining this with Theorem 8.11 we obtain:

Corollary 8.16. *Let G be a finite solvable group. Then there exists an algebraic number field F and a G-crossed product division algebra D over F. Furthermore, there exists a chain of crossed product division algebras*

$$M = A_0 \subset A_1 \subset \ldots \subset A_k = D$$

over F, such that

$$A_{i+1} \cong A_i[t_i; \tau_i] / A_i[t_i; \tau_i](t_i^{q_i} - c_i),$$

for all $i \in \{0, \ldots, k-1\}$, and satisfying

(i) q_i is the prime order of the factor group G_{i+1}/G_i in the subnormal series (8.4) *which exists because G is solvable,*

(ii) τ_i is an automorphism of A_i of inner order q_i which restricts to $\sigma_i \in G$ on M,

(iii) $c_i \in \mathrm{Fix}(\tau_i)$ is invertible.

Proof. Such a field F and division algebra D exist by [59, Theorem 9.1]. The assertion then follows by Theorem 8.11. □

In [63, Theorem 1], Sonn proved that a finite solvable group is admissible over $\mathbb{Q}$ if and only if all its Sylow subgroups are metacyclic, i.e. if every Sylow subgroup H of G has a cyclic normal subgroup N, such that H/N is also cyclic. Combining this with Theorem 8.11 yields:

Corollary 8.17. *Let G be a finite solvable group such that all its Sylow subgroups are metacyclic. Then there exists a G-crossed product division algebra D over $\mathbb{Q}$, and a chain of crossed product division algebras*

$$M = A_0 \subset A_1 \subset \ldots \subset A_k = D$$

over $\mathbb{Q}$, such that

$$A_{i+1} \cong A_i[t_i; \tau_i] / A_i[t_i; \tau_i](t_i^{q_i} - c_i),$$

for all $i \in \{0, \ldots, k-1\}$, such that

(i) q_i is the prime order of the factor group G_{i+1}/G_i in the subnormal series (8.4) *which exists because G is solvable,*

(ii) τ_i *is an automorphism of* A_i *of inner order* q_i *which restricts to* $\sigma_i \in G$ *on* M*,*

(iii) $c_i \in \mathrm{Fix}(\tau_i)$ *is invertible.*

Proof. Such a division algebra D exists by [63, Theorem 1]. The assertion then follows by Theorem 8.11. □

8.5 HOW TO CONSTRUCT CROSSED PRODUCT DIVISION ALGEBRAS CONTAINING A GIVEN ABELIAN GALOIS FIELD EXTENSION AS A MAXIMAL SUBFIELD

Let M/F be a Galois field extension of degree n with abelian Galois group $G = \mathrm{Gal}(M/F)$. We now show how to canonically construct crossed product division algebras of degree n over F containing M as a subfield. This generalises a result by Albert in which $n = 4$ and $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ [1, p. 186], cf. also [32, Theorem 2.9.55]: For $n = 4$ every central division algebra containing a quartic abelian extension M with Galois group $\mathbb{Z}_2 \times \mathbb{Z}_2$ can be obtained this way [1, p. 186], that means as a generalised cyclic algebra (D, τ, c) with D a quaternion algebra over its center.

Another way to construct such a crossed product algebra is via generic algebras, using a process going back to Amitsur and Saltman [4], described also in [32, §4.6].

As G is a finite abelian group, we have a chain of subgroups

$$\{1\} = G_0 \leq \ldots \leq G_k = G,$$

such that $G_j \triangleleft G_{j+1}$ and G_{j+1}/G_j is cyclic of prime order $q_j > 1$ for all $j \in \{0, \ldots, k-1\}$. We use this chain to construct the algebras we want:

$G_1 = \langle \sigma_1 \rangle$ is cyclic of prime order $q_0 > 1$ for some $\sigma_1 \in G$. Let $\tau_0 = \sigma_1$. Choose any $c_0 \in F^\times$ that satisfies $z\tau_0(z) \cdots \tau_0^{q_0-1}(z) \neq c_0$ for all $z \in M$ and define $f(t_0) = t_0^{q_0} - c_0 \in M[t_0; \tau_0]$. Since τ_0 has order q_0, we have $\tau_0^{q_0}(z)c_0 =$

$zc_0 = c_0 z$ for all $z \in M$, and so $f(t_0)$ is right invariant by Theorem 2.1. Therefore we see that

$$A_1 = M[t_0; \tau_0]/M[t_0; \tau_0](t_0^{q_0} - c_0)$$

is an associative algebra which is cyclic of degree q_0 over $\text{Fix}(\tau_0)$. Moreover, $f(t_0)$ is irreducible by [32, Theorem 2.6.20(i)] and therefore A_1 is a division algebra.

Now G_2/G_1 is cyclic of prime order q_1, say $G_2/G_1 = \{\sigma_2^i G_1 \mid i \in \mathbb{Z}\}$ for some $\sigma_2 \in G_2$ where $\sigma_2^{q_1} \in G_1$. As $\sigma_2^{q_1} \in G_1$ we have $\sigma_2^{q_1} = \sigma_1^{\mu}$ for some $\mu \in \{0, \ldots, q_0 - 1\}$. Define $c_1 = l_1 t_0^{\mu}$ for some $l_1 \in F^{\times}$ and define the map

$$\tau_1 : A_1 \to A_1, \ \sum_{i=0}^{q_0-1} m_i t_0^i \mapsto \sum_{i=0}^{q_0-1} \sigma_2(m_i) t_0^i,$$

which is an automorphism of A_1 by a straightforward calculation.

Denote the multiplication in A_1 by $\circ$. Then

$$\tau_1(c_1) = \sigma_2(l_1) t_0^{\mu} = l_1 t_0^{\mu} = c_1.$$

We have

$$\tau_1^{q_1}\Big(\sum_{i=0}^{q_0-1} m_i t_0^i\Big) \circ c_1 = \sum_{i=0}^{q_0-1} \sigma_2^{q_1}(m_i) t_0^i \circ l_1 t_0^{\mu} = \sum_{i=0}^{q_0-1} l_1 \sigma_1^{\mu}(m_i) t_0^i \circ t_0^{\mu}$$

and

$$c_1 \circ \sum_{i=0}^{q_0-1} m_i t_0^i = l_1 t_0^{\mu} \circ \sum_{i=0}^{q_0-1} m_i t_0^i = \sum_{i=0}^{q_0-1} l_1 \sigma_1^{\mu}(m_i) t_0^{\mu} \circ t_0^i$$

for all $m_i \in M$. Hence $\tau_1^{q_1}(z) \circ c_1 = c_1 \circ z$ for all $z \in A_1$ and $\tau_1(c_1) = c_1$, thus $f(t_1) = t_1^{q_1} - c_1 \in A_1[t_1; \tau_1]$ is right invariant by Proposition 7.3 and

$$A_2 = A_1[t_1; \tau_1]/A_1[t_1; \tau_1](t_1^{q_1} - c_1)$$

is a finite-dimensional associative algebra over

$$\text{Comm}(A_2) \cap A_1 = \text{Fix}(\tau_1) \cap \text{Cent}(A_1) = \text{Fix}(\tau_1) \cap \text{Fix}(\tau_0) \supset F$$

by Proposition 7.4(iii).

Again, G_3/G_2 is cyclic of prime order q_2, say $G_3/G_2 = \{\sigma_3^i G_2 \mid i \in \mathbb{Z}\}$ for some $\sigma_3 \in G$ with $\sigma_3^{q_2} \in G_2$. Write $\sigma_3^{q_2} = \sigma_2^{\lambda_1}\sigma_1^{\lambda_0}$ for some $\lambda_1 \in \{0, \dots, q_1 - 1\}$ and $\lambda_0 \in \{0, \dots, q_0 - 1\}$. The map

$$H_{\sigma_3} : A_1 \to A_1, \sum_{i=0}^{q_0-1} m_i t_0^i \mapsto \sum_{i=0}^{q_0-1} \sigma_3(m_i) t_0^i,$$

is an automorphism of A_1 by a straightforward calculation. Define

$$\tau_2 : A_2 \to A_2, \sum_{i=0}^{q_1-1} x_i t_1^i \mapsto \sum_{i=0}^{q_1-1} H_{\sigma_3}(x_i) t_1^i \ (x_i \in A_1).$$

Then a straightforward calculation using that H_{σ_3} commutes with τ_1 and $H_{\sigma_3}(c_1) = c_1$ shows that τ_2 is an automorphism of A_2. Define $c_2 = l_2 t_0^{\lambda_0} t_1^{\lambda_1}$ for some $l_2 \in F^\times$. Denote the multiplication in A_i by $\circ_{A_i}$ and let $x_i = \sum_{j=0}^{q_0-1} y_{ij} t_0^j \in A_1$, $y_{ij} \in M$, $i \in \{0, \dots, q_1 - 1\}$. Then

$$\tau_2(c_2) = \tau_2(l_2 t_0^{\lambda_0} t_1^{\lambda_1}) = H_{\sigma_3}(l_2 t_0^{\lambda_0}) t_1^{\lambda_1} = l_2 t_0^{\lambda_0} t_1^{\lambda_1} = c_2.$$

Furthermore we have

$$\begin{aligned}
\tau_2^{q_2}\Big(\sum_{i=0}^{q_1-1} x_i t_1^i\Big) \circ_{A_2} c_2 &= \sum_{i=0}^{q_1-1} H_{\sigma_3}^{q_2}(x_i) t_1^i \circ_{A_2} l_2 t_0^{\lambda_0} t_1^{\lambda_1} \\
&= \sum_{i=0}^{q_1-1}\sum_{j=0}^{q_0-1} \sigma_3^{q_2}(y_{ij}) t_0^j t_1^i \circ_{A_2} l_2 t_0^{\lambda_0} t_1^{\lambda_1} \\
&= \sum_{i=0}^{q_1-1}\sum_{j=0}^{q_0-1} \sigma_2^{\lambda_1}(\sigma_1^{\lambda_0}(y_{ij})) t_0^j t_1^i \circ_{A_2} l_2 t_0^{\lambda_0} t_1^{\lambda_1} \\
&= \sum_{i=0}^{q_1-1} \Big(\sum_{j=0}^{q_0-1} \sigma_2^{\lambda_1}(\sigma_1^{\lambda_0}(y_{ij})) t_0^j \circ_{A_1} \tau_1^i(l_2 t_0^{\lambda_0})\Big) t_1^i \circ_{A_2} t_1^{\lambda_1} \\
&= \sum_{i=0}^{q_1-1} \Big(\sum_{j=0}^{q_0-1} l_2 \sigma_2^{\lambda_1}(\sigma_1^{\lambda_0}(y_{ij})) t_0^j \circ_{A_1} t_0^{\lambda_0}\Big) t_1^i \circ_{A_2} t_1^{\lambda_1},
\end{aligned}$$

and

$$\begin{aligned}
c_2 \circ_{A_2} \sum_{i=0}^{q_1-1} x_i t_1^i = l_2 t_0^{\lambda_0} t_1^{\lambda_1} \circ_{A_2} \sum_{i=0}^{q_1-1} x_i t_1^i &= \sum_{i=0}^{q_1-1} \big(l_2 t_0^{\lambda_0} \circ_{A_1} \tau_1^{\lambda_1}(x_i)\big) t_1^{\lambda_1} \circ_{A_2} t_1^i \\
&= \sum_{i=0}^{q_1-1}\sum_{j=0}^{q_0-1} \big(l_2 t_0^{\lambda_0} \circ_{A_1} \sigma_2^{\lambda_1}(y_{ij}) t_0^j\big) t_1^{\lambda_1} \circ_{A_2} t_1^i
\end{aligned}$$

$$= \sum_{i=0}^{q_1-1} \Big(\sum_{j=0}^{q_0-1} l_2 \sigma_1^{\lambda_0}(\sigma_2^{\lambda_1}(y_{ij})) t_0^{\lambda_0} \circ_{A_1} t_0^j \Big) t_1^{\lambda_1} \circ_{A_2} t_1^i.$$

Hence $\tau_2^{q_2}(z) \circ_{A_2} c_2 = c_2 \circ_{A_2} z$ for all $z \in A_2$ and $\tau_2(c_2) = c_2$, therefore $f(t_2) = t_2^{q_2} - c_2 \in A_2[t_2;\tau_2]$ is right invariant by Proposition 7.3 and thus

$$A_3 = A_2[t_2;\tau_2]/A_2[t_2;\tau_2](t_2^{q_2} - c_2)$$

is a finite-dimensional associative algebra over

$$\mathrm{Comm}(A_3) \cap A_2 = \mathrm{Fix}(\tau_2) \cap \mathrm{Cent}(A_2) = \mathrm{Fix}(\tau_0) \cap \mathrm{Fix}(\tau_1) \cap \mathrm{Fix}(\tau_2) \supset F$$

by Proposition 7.4(iii). Continuing in this manner we obtain a chain $M = A_0 \subset \ldots \subset A_k$ of finite-dimensional associative algebras

$$A_{i+1} = A_i[t_i;\tau_i]/A_i[t_i;\tau_i](t_i^{q_i} - c_i)$$

over

$$\mathrm{Fix}(\tau_i) \cap \mathrm{Cent}(A_i) = \mathrm{Fix}(\tau_0) \cap \mathrm{Fix}(\tau_1) \cap \cdots \cap \mathrm{Fix}(\tau_i) \supset F,$$

for all $i \in \{0, \ldots, k-1\}$, where $\tau_0 = \sigma_1$ and τ_i restricts to σ_{i+1} on M for all $i \in \{0, \ldots, k-1\}$. Moreover,

$$[A_i : M] = [A_i : A_{i-1}] \cdots [A_1 : M] = \prod_{l=0}^{i-1} q_l$$

hence

$$[A_k : F] = \Big(\prod_{l=0}^{k-1} q_l\Big) n = n^2,$$

and A_k contains M as a subfield.

Let us furthermore assume that each c_i above, $i \in \{0, \ldots, k-1\}$, is successively chosen such that

$$z\tau_i(z) \cdots \tau_i^{q_i-1}(z) \neq c_i \tag{8.16}$$

for all $z \in A_i$, then using that τ_i has inner order q_i and $f(t_i) = t_i^{q_i} - c_i \in A_i[t_i;\tau_i]$ is an irreducible twisted polynomial, we conclude A_{i+1} is a division algebra by [32, Theorem 1.3.16].

Lemma 8.18. *For all $i \in \{0, \ldots, k-1\}$, $\tau_i : A_i \to A_i$ has inner order q_i.*

Proof. The automorphism $\tau_0 = \sigma_1 : M \to M$ has inner order q_0.

Fix $i \in \{1, \dots, k-1\}$. A_i is finite-dimensional over F, so it is also finite-dimensional over its center $\mathrm{Cent}(A_i) \supset F$. Recall that $\tau_i^{q_i}(z)c_i = c_i z$ for all $z \in A_i$, in particular $\tau_i^{q_i}|_{\mathrm{Cent}(A_i)} = id$. As q_i is prime this means either $\tau_i|_{\mathrm{Cent}(A_i)} = id$ or $\tau_i|_{\mathrm{Cent}(A_i)}$ has order $q_i > 1$.

Assume that $\tau_i|_{\mathrm{Cent}(A_i)} = id$, then τ_i is an inner automorphism of A_i by the Theorem of Skolem-Noether, say $\tau_i(z) = uzu^{-1}$ for some invertible $u \in A_i$, for all $z \in A_i$. In particular $\tau_i(m) = \sigma_{i+1}(m) = umu^{-1}$ for all $m \in M$. Write $u = \sum_{j=0}^{q_{i-1}-1} u_j t_{i-1}^j$ for some $u_j \in A_{i-1}$, thus

$$\begin{aligned}\sigma_{i+1}(m)u = \sigma_{i+1}(m)\sum_{j=0}^{q_{i-1}-1} u_j t_{i-1}^j &= \sum_{j=0}^{q_{i-1}-1} u_j t_{i-1}^j m \\ &= \sum_{j=0}^{q_{i-1}-1} u_j \tau_{i-1}^j(m) t_{i-1}^j = \sum_{j=0}^{q_{i-1}-1} u_j \sigma_i^j(m) t_{i-1}^j.\end{aligned}$$

for all $m \in M$. Choose η_i with $u_{\eta_i} \neq 0$ then

$$\sigma_{i+1}(m)u_{\eta_i} = u_{\eta_i}\sigma_i^{\eta_i}(m), \tag{8.17}$$

for all $m \in M$.

If $i = 1$ we are done. If $i \geq 2$ then we can also write $u_{\eta_i} = \sum_{l=0}^{q_{i-2}-1} w_l t_{i-2}^l$ for some $w_l \in A_{i-2}$, therefore (8.17) yields

$$\begin{aligned}\sigma_{i+1}(m)\sum_{l=0}^{q_{i-2}-1} w_l t_{i-2}^l = \sum_{l=0}^{q_{i-2}-1} w_l t_{i-2}^l \sigma_i^{\eta_i}(m) &= \sum_{l=0}^{q_{i-2}-1} w_l \tau_{i-2}^l(\sigma_i^{\eta_i}(m)) t_{i-2}^l \\ &= \sum_{l=0}^{q_{i-2}-1} w_l \sigma_{i-1}^l(\sigma_i^{\eta_i}(m)) t_{i-2}^l,\end{aligned}$$

for all $m \in M$. Choose η_{i-1} with $w_{\eta_{i-1}} \neq 0$, then

$$\sigma_{i+1}(m)w_{\eta_{i-1}} = w_{\eta_{i-1}}\sigma_{i-1}^{\eta_{i-1}}(\sigma_i^{\eta_i}(m)),$$

for all $m \in M$.

Continuing in this manner we see that there exists $s \in M^\times$ such that

$$\sigma_{i+1}(m)s = s\sigma_1^{\eta_1}(\sigma_2^{\eta_2}(\cdots(\sigma_i^{\eta_i}(m)\cdots),$$

for all $m \in M$, hence

$$\sigma_{i+1}(m) = \sigma_1^{\eta_1}(\sigma_2^{\eta_2}(\cdots(\sigma_i^{\eta_i}(m)\cdots),$$

for all $m \in M$ where $\eta_j \in \{0, \dots, q_{j-1} - 1\}$ for all $j \in \{1, \dots, i\}$. But $\sigma_{i+1} \notin G_i$ and thus

$$\sigma_{i+1} \neq \sigma_1^{\eta_1} \circ \sigma_2^{\eta_2} \circ \cdots \circ \sigma_i^{\eta_i},$$

a contradiction.

It follows that $\tau_i|_{\mathrm{Cent}(A_i)}$ has order $q_i > 1$. By the Skolem-Noether Theorem the kernel of the restriction map $\mathrm{Aut}(A_i) \to \mathrm{Aut}(\mathrm{Cent}(A_i))$ is the group of inner automorphisms of A_i, and so τ_i has inner order q_i. □

Proposition 8.19. $\mathrm{Cent}(A_k) = F$.

Proof. $F \subset \mathrm{Cent}(A_k)$ by construction. Let now

$$z = z_0 + z_1 t_{k-1} + \ldots + z_{q_{k-1}-1} t_{k-1}^{q_{k-1}-1} \in \mathrm{Cent}(A_k)$$

where $z_i \in A_{k-1}$. Then z commutes with all $l \in A_{k-1}$, hence $lz_i = z_i \tau_{k-1}^i(l)$ for all $i \in \{0, \dots, q_{k-1} - 1\}$. This implies $z_0 \in \mathrm{Cent}(A_{k-1})$ and $z_i = 0$ for all $i \in \{1, \dots, q_{k-1} - 1\}$, otherwise z_i is invertible and τ_{k-1}^i is inner, a contradiction by Lemma 8.18. Thus $z = z_0 \in \mathrm{Cent}(A_{k-1})$. A similar argument shows $z \in \mathrm{Cent}(A_{k-1})$ and continuing in this manner we conclude $z \in M = \mathrm{Cent}(A_0)$.

Suppose, for a contradiction, that $z \notin F$. Then $\rho(z) \neq z$ for some $\rho \in G$. Since the σ_{i+1} were chosen so that they generate the cyclic factor groups G_{i+1}/G_i, we can write $\rho = \sigma_1^{i_0} \circ \sigma_2^{i_1} \circ \cdots \circ \sigma_k^{i_{k-1}}$ for some $i_s \in \{0, \dots, q_s - 1\}$. We have

$$\begin{aligned} t_0^{i_0} t_1^{i_1} \cdots t_{k-1}^{i_{k-1}} z &= \sigma_1^{i_0}(\sigma_2^{i_1}(\cdots(\sigma_k^{i_{k-1}}(z)\cdots) t_0^{i_0} t_1^{i_1} \cdots t_{k-1}^{i_{k-1}} \\ &= \rho(z) t_0^{i_0} t_1^{i_1} \cdots t_{k-1}^{i_{k-1}} \neq z t_0^{i_0} t_1^{i_1} \cdots t_{k-1}^{i_{k-1}}, \end{aligned}$$

contradicting that $z \in \mathrm{Cent}(A_k)$. Therefore $\mathrm{Cent}(A_k) \subset F$. □

This yields a recipe for constructing a G-crossed product division algebra $A = A_k$ over F with maximal subfield M provided it is possible to find suitable c_i's satisfying (8.16).

BIBLIOGRAPHY

[1] A. A. Albert. *Structure of algebras*, volume 24. American Mathematical Soc., 1939.

[2] S. C. Althoen, K. D. Hansen, and L. D. Kugler. $\mathbb{C}$-associative algebras of dimension 4 over $\mathbb{R}$. *Algebras, Groups and Geometries*, 3:329–360, 1986.

[3] A. Amitsur. Non-commutative cyclic fields. *Duke Math. J*, 21:87–105, 1954.

[4] S. Amitsur and D. Saltman. Generic abelian crossed products and p-algebras. *Journal of Algebra*, 51(1):76–87, 1978.

[5] J. Bergen, M. Giesbrecht, P. N. Shivakumar, and Y. Zhang. Factorizations for difference operators. *Advances in Difference Equations*, 2015(1):1–6, 2015.

[6] G. Berhuy and F. Oggier. *An introduction to central simple algebras and their applications to wireless communication*, volume 191. American Mathematical Society, 2013.

[7] A. J. Berrick and M. E. Keating. *An Introduction to Rings and Modules: with K-theory in view*, volume 65. Cambridge University Press, 2000.

[8] M. Boulagouaz and A. Leroy. (σ, δ)-codes. *Adv. Math. Commun. 7(4)*, 2013.

[9] N. Bourbaki. *Éléments de mathématique: Fasc. XXIII. Algèbre; Chapitre 8, Modules et anneaux semi-simples*. Hermann, 1973.

[10] C. Brown and S. Pumplün. Solvable crossed product algebras revisited. *arXiv preprint arXiv:1702.04605*, 2017.

[11] C. Brown and S. umplün. The automorphisms of Petit's algebras. *Communications in Algebra*, 46(2):834–849, 2018.

[12] R. H. Bruck. Contributions to the theory of loops. *Transactions of the American Mathematical Society*, 60(2):245–354, 1946.

[13] X. Caruso and J. L. Borgne. Some algorithms for skew polynomials over finite fields. *arXiv preprint arXiv:1212.3582*, 2012.

[14] X. Caruso and J. Le Borgne. A new faster algorithm for factoring skew polynomials over finite fields. *Journal of Symbolic Computation*, 79:411–443, 2017.

[15] R. C. Churchill and Y. Zhang. Irreducibility criteria for skew polynomials. *Journal of Algebra*, 322(11):3797–3822, 2009.

[16] P. M. Cohn. *Skew Fields: Theory of General Division Rings*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1995.

[17] U. Dempwolff. Autotopism groups of cyclic semifield planes. *Journal of Algebraic Combinatorics*, 34(4):641–669, 2011.

[18] L. E. Dickson. On commutative linear algebras in which division is always uniquely possible. *Transactions of the American Mathematical Society*, 7(4):514–522, 1906.

[19] L. E. Dickson. Linear algebras with associativity not assumed. *Duke Mathematical Journal*, 1(2):113–125, 1935.

[20] J. Ducoat and F. Oggier. On skew polynomial codes and lattices from quotients of cyclic division algebras. *Advances in Mathematics of Communications*, 10(1):79–94, 2016.

[21] N. Fogarty and H. Gluesing-Luerssen. A circulant approach to skew-constacyclic codes. *Finite Fields and Their Applications*, 35:92–114, 2015.

[22] M. Giesbrecht. Factoring in skew-polynomial rings over finite fields. *Journal of Symbolic Computation*, 26(4):463–486, 1998.

[23] J. Gómez-Torrecillas. Basic module theory over non-commutative rings with computational aspects of operator algebras. In *Algebraic and Algorithmic Aspects of Differential and Integral Operators*, pages 23–82. Springer, 2014.

[24] J. Gomez-Torrecillas, F. Lobillo, and G. Navarro. Computing the bound of an Ore polynomial. Applications to factorization. *arXiv preprint arXiv:1307.5529*, 2013.

[25] K. Goodearl. Prime ideals in skew polynomial rings and quantized Weyl algebras. *Journal of Algebra*, 150(2):324–377, 1992.

[26] Á. Granja, M. C. Martínez, and C. Rodríguez. Real valuations on skew polynomial rings. *Algebras and Representation Theory*, 17(5):1413–1436, 2014.

[27] T. Hanke. A twisted Laurent series ring that is a noncrossed product. *Israel Journal of Mathematics*, 150(1):199–203, 2005.

[28] C. Hering. Fibrations in free modules. *Notes Soc. Mat, Chile (NS) X*, pages 11–16, 1991.

[29] D. Hughes and E. Kleinfeld. Seminuclear extensions of Galois fields. *American Journal of Mathematics*, pages 389–392, 1960.

[30] T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980.

[31] N. Jacobson. *Basic Algebra. I, 2nd ed.* W. H. Freeman and Company, New York, 1985.

[32] N. Jacobson. *Finite-dimensional division algebras over fields*, volume 233. Springer, 1996.

[33] V. Jha and N. Johnson. An analog of the Albert-Knuth theorem on the orders of finite semifields, and a complete solution to Cofman's subplane problem. *Algebras Groups Geom*, 6(1):1–35, 1989.

[34] S. Jitman, S. Ling, and P. Udomkavanich. Skew constacyclic codes over finite chain rings. *arXiv preprint arXiv:1008.0327*, 2010.

[35] D. E. Knuth. Finite semifields and projective planes. *Journal of Algebra*, 2(2):182–217, 1965.

[36] N. Koblitz. *A course in number theory and cryptography*, volume 114. Springer Science & Business Media, 1994.

[37] E. R. Kolchin. *Differential algebra & algebraic groups*, volume 54. Academic press, 1973.

[38] T.-Y. Lam. *A first course in noncommutative rings*. Springer-Verlag New York, 2nd edition, 2001.

[39] T.-Y. Lam and A. Leroy. Algebraic conjugacy classes and skew polynomial rings. In *Perspectives in ring theory*, pages 153–203. Springer, 1988.

[40] T.-Y. Lam and A. Leroy. Vandermonde and Wronskian matrices over division rings. *Journal of Algebra*, 119(2):308–336, 1988.

[41] T.-Y. Lam and A. Leroy. Homomorphisms between Ore extensions. *Comtemporary Mathematics*, 124:83–110, 1992.

[42] T.-Y. Lam, A. Leroy, H. Leung, and J. Matczuk. Invariant and semi-invariant polynomials in skew polynomial rings. *Israel Math. Conf. Proc*, 1:247–261, 1989.

[43] S. Lang. Algebra, revised third edition. *Graduate Texts in Mathematics*, 2002.

[44] M. Lavrauw and J. Sheekey. Semifields from skew polynomial rings. *Advances in Geometry*, 13(4):583–604, 2013.

[45] B. Lemonnier. *Dimension de Krull et codeviations, quelques applications en theorie des modules*. PhD thesis, Poitiers, 1984.

[46] A. Leroy. Noncommutative polynomial maps. *Journal of Algebra and its Applications*, 11(04):1250076, 2012.

[47] B. A. Magurn. *An algebraic introduction to K-theory*, volume 87. Cambridge University Press, 2002.

[48] B. R. McDonald. *Finite rings with identity*, volume 28. Marcel Dekker Incorporated, 1974.

[49] M. Motiee. A note on the existence of cyclic algebras in division algebras. *Communications in Algebra*, 45(10):4396–4399, 2017.

[50] W. K. Nicholson. *Introduction to abstract algebra*. John Wiley & Sons, 2012.

[51] O. Ore. Theory of non-commutative polynomials. *Annals of mathematics*, pages 480–508, 1933.

[52] J.-C. Petit. Sur certains quasi-corps généralisant un type d'anneau-quotient. *Séminaire Dubreil. Algèbre et théorie des nombres*, 20(2):1–18, 1966-1967.

[53] J.-C. Petit. Sur les quasi-corps distributifs à base monogéne. *CR Acad. Sci. Paris Sér AB*, 266:A402–A404, 1968.

[54] S. Pumplün. Factoring skew polynomials over Hamilton's quaternion algebra and the complex numbers. *Journal of Algebra*, 427:20–29, 2015.

[55] S. Pumplün. Finite nonassociative algebras obtained from skew polynomials and possible applications to (f,σ,δ)-codes. *To appear in Advances in Mathematics of Communications. Online at arXiv:1507.01491[cs.IT]*, 2016.

[56] S. Pumplün. Nonassociative differential extensions of characteristic p. *Results in Mathematics, DOI 10.1007/s00025-017-0656-x*, 2017.

[57] D. J. Saltman. *Lectures on division algebras*, volume 94. American Mathematical Soc., 1999.

[58] R. Sandler. Autotopism groups of some finite non-associative algebras. *American Journal of Mathematics*, pages 239–264, 1962.

[59] M. M. Schacher. Subfields of division rings, I. *Journal of Algebra*, 9(4):451–477, 1968.

[60] R. D. Schafer. *An introduction to nonassociative algebras*, volume 22. Courier Dover Publications, 1966.

[61] J. Sheekey. *On rank problems for subspaces of matrices over finite fields*. PhD thesis, University College Dublin, 2011.

[62] M. F. Singer. Testing reducibility of linear differential operators: a group theoretic perspective. *Applicable Algebra in Engineering, Communication and Computing*, 7(2):77–104, 1996.

[63] J. Sonn. $\mathbb{Q}$-admissibility of solvable groups. *Journal of Algebra*, 84(2):411–419, 1983.

[64] A. Steele. *Some new classes of division algebras and potential applications to space time block coding*. PhD thesis, University of Nottingham, 2013.

[65] W. C. Waterhouse. Nonassociative quarternion algebras. *Algebras, Groups and Geometries*, 1987.

[66] G. Wene. Finite semifields three-dimensional over the left nuclei. *Lecture Notes in Pure and Applied Mathematics*, pages 447–456, 2000.

[67] G. Wene. Automorphisms of type I semifields quadratic over a weak nucleus. *Algebras Groups Geom*, 23(4):375—-386, 2006.

[68] G. Wene. Inner automorphisms of finite semifields. *Note di Matematica*, 29(suppl_1):231–242, 2010.