UNIVERSITY OF NOTTINGHAM

SCHOOL OF MATHEMATICAL SCIENCES

On the Right Nucleus of Petit Algebras

Adam Owen

A thesis submitted to the University of Nottingham for the degree of DOCTOR OF PHILOSOPHY

August 2021

Abstract

Let D be division algebra over its center C, let σ be an endormorphism of D, let δ be a left σ-derivation of D, and let $R = D[t; \sigma, \delta]$ be a skew polynomial ring. We study the structure of a class of nonassociative algebras, denoted by S_f, whose construction canonically generalises that of the associative quotient algebras R/Rf where $f \in R$ is right-invariant.

We determine the structure of the right nucleus of S_f when the polynomial f is bounded and not right invariant and either $\delta = 0$, or $\sigma = \mathrm{id}_D$. As a by-product, we obtain a new proof on the size of the right nuclei of the cyclic (Petit) semifields $\mathbb{S}_f$.

We look at subalgebras of the right nucleus of S_f, generalising several of Petit's results [Pet66] and introduce the notion of semi-invariant elements of the coefficient ring D. The set of semi-invariant elements is shown to be equal to the nucleus of S_f when f is not right-invariant. Moreover, we compute the right nucleus of S_f for certain f.

In the final chapter of this thesis we introduce and study a special class of polynomials in R called generalised A-polynomials. In a differential polynomial ring over a field of characteristic zero, A-polynomials were originally introduced by Amitsur [Ami54]. We find examples of polynomials whose eigenring is a central simple algebra over the field $C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$.

Acknowledgements

My full and sincere gratitude goes out to my supervisor Susanne Pumplün. You have been a wonderful mentor for the last three and a half years and your infinite patience and wisdom got me through the highs and lows of this process.

Thank you to Dan for being an excellent travel companion to conferences, coffee shops, and bars, and for always having time to listen to my ramblings.

I would also like to extend my thanks to John Sheekey and José Gómez-Torrecillas whose correspondence proved to be extremely helpful.

Finally, I would like to say a special thank you to Holly and my parents for putting up with me and the maths and for your unconditional love and support.

Introduction

Let D be a unital associative ring, let σ and δ be an injective endomorphism and a left σ-derivation of D, respectively, and let $R = D[t; \sigma, \delta]$ be a skew polynomial ring in the single indeterminate t. The ring R was introduced by Ore in 1933 [Ore33]. Since then it has been widely studied and its properties are well understood as a result (e.g. see [MRS01] and [GWJ04] for surveys). We exclusively consider the case that D is a unital associative division ring, in which case any endomorphism of D is necessarily injective.

Ore showed that R possesses a right division algorithm, that is for any given skew polynomials $f, g \in R$ (with $f \neq 0$), there exists a unique quotient $q \in R$, and a unique remainder $r \in R$, such that $\deg(r) < \deg(f)$ and $g = qf + r$. Consequently, every left ideal of R is principal, i.e. has the form Rg for some $g \in R$. Moreover, if σ is an automorphism, then R also possesses the analogous left division algorithm, hence every right ideal of R is also principal, i.e. of the form gR for some $g \in R$, and R is a principal ideal domain [Jac09]. We note that what we call a right division algorithm, Jacobson calls left and vice versa.

For each skew polynomial $f \in R$ of degree $m \geq 1$, the eigenring of f

is defined by the set

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

which is an associative algebra, and if f is an irreducible polynomial, then $\mathcal{E}(f)$ is a division algebra. For bounded polynomials $f \in R$ the irreducible factors of f in the ring R are in one to one correspondence with the nontrivial zero divisors in $\mathcal{E}(f)$, in particular if f is bounded and $\mathcal{E}(f)$ is a division algebra, then f is irreducible [GT12, GTLN13]. Therefore the eigenring of a skew polynomial f often appears whenever a factorisation of f in R is investigated.

In 1966 Petit introduced a new class of unital nonassociative algebras, whose construction canonically generalises the construction of the associative quotient algebras R/Rf when factoring by a right-invariant (i.e. two-sided) polynomial $f \in R$ in [Pet66]. Let $f \in R$ have degree $m \geq 1$ and consider the additive subgroup

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

of R. When endowed with the multiplication

$$g \circ h = gh \bmod_r f,$$

where $\bmod_r f$ denotes the remainder upon right division by f in R, R_m forms a unital nonassociative algebra over the field $F = C(D) \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$. These so-called *Petit algebras* are denoted by S_f where f is the polynomial used in the construction, or often by R/Rf due to the R-module structure of S_f. Petit algebras were studied in detail in [Pet66] and more recently in [Bro18], [BP18] for example, and in [LS13], [She18]

over fields of characteristic $p > 0$ (in which case $\delta = 0$ w.l.o.g.). Petit's method can be used to construct unital nonassociative division algebras, for example the Petit algebra S_f with $f(t) = t^2 - i \in \mathbb{C}[t; \bar{}]$, where $\bar{}$ denotes complex conjugation, was described earlier by Dickson and forms the earliest example of a nonassociative division algebra [Dic06].

Constructions of codes via classical algebraic methods are well known. In recent years, the nonassociative algebras S_f have been employed in the construction of space-time block codes, (f, σ, δ)-codes, and wire tap codes, to name a few, when S_f is an algebra over a number field (e.g. [Pum15a, Pum15b, BO13, DO15b, DO15a, OS12]. In particular, we note their use in the construction of fast-decodable fully diverse space-time block codes in [PS15a, PS15b, SPO12], due to the fact that the right nucleus of S_f is large. This motivates our investigation into the structure of $\mathrm{Nuc}_r(S_f)$ from a purely algebraic point of view, since a better understanding of the algebras S_f and their nuclei may lead to new developments in coding theory.

For f of degree at least 2, Petit showed that the eigenring of f is equal to the right nucleus of S_f [Pet66]. Thus we are able to analyse the structure of the nonassociative algebra S_f and its right nucleus via classical methods from the theory of R-modules and the theory of associative algebras. Alternatively, one may say that this identification of the right nucleus of S_f as the eigenring of f allows us to take the novel approach to investigate the structure of the eigenring of f in the context of nonassociative algebras.

The structure of this thesis is as follows:

Chapter 1 introduces the necessary notation, definitions and background theory used throughout. In particular, we recall some properties of the skew polynomial ring R, recount the theory of bounded polynomials in R, and describe Petit's construction of the algebras S_f. In Chapter 2, we focus on the case that $R = D[t;\sigma]$, where σ is an automorphism of D of finite inner order n. For any bounded skew polynomial $f \in R$ such that its bound f^* is a maximal two-sided element of R, i.e. the left ideal Rf^* is a two-sided maximal ideal, the ring $A = R/Rf^*$ is a simple Artinian ring, hence the left A-module R/Rf is semisimple, i.e. is the direct sum of simple modules. Motivated by this we employ methods from the Artin-Wedderburn theory of semisimple Artinian rings and algebras (e.g. [Lan04]), and Jacobson's theory of noncommutative principal ideal domains [Jac43], to study both the A-module and R-module structure of S_f. Moreover, the endomorphism ring $\mathrm{End}_R(R/Rf)$ is known to be equal to the eigenring of f (e.g. [GTLN13]), hence we obtain a description of the right nucleus of the Petit algebra S_f via classical methods.

Chapter 3 follows the same format as Chapter 2, however, this time we employ the classical methods described above in order to analyse the module structure of S_f when $R = D[t;\delta]$ for δ an inner derivation of D (when $\mathrm{Char}(D) = 0$) or an algebraic derivation of D of finite degree (when $\mathrm{Char}(D) = p > 0$). Chapter 4 consists of a generalisation of the results of Chapters 2 and 3, under the assumption that f^* completely factorises into a product of irreducibles in the center of R, which are not equal to one another up to scalar multiplication by elements in $D^\times$. We focus here on the case $R = D[t;\sigma]$, however, the results of Chapter 4 also hold analogously in the case $R = D[t;\delta]$. We discard the case $R = D[t;\sigma,\delta]$ in Chapters 2 through 4, since we require that D has finite degree as a central division algebra over C, hence R is either a twisted

polynomial ring or a differential polynomial ring [Jac09, Theorem 1.1.21].

Moving on, we study the algebraic properties of S_f and its nuclei. We introduce the notion of (right) semi-invariant elements in the coefficient ring D with respect to a skew polynomial $f \in R$. An element $c \in D$ is *(right) semi-invariant* with respect to $f \in R$ if $fc \in Rf$. We show that the set of such elements $L = L^{(\sigma,\delta,f)}$ is equal to $\mathrm{Nuc}(S_f)$ whenever f is not right-invariant, and if f is right-invariant, then $L = D$. Moreover, we determine sufficient conditions for the indeterminate t and its powers to lie in the right nucleus of S_f, and we generalise Petit's result [Pet66, (16)] providing necessary and sufficient conditions for t to lie in $\mathrm{Nuc}_r(S_f)$ when $R = D[t;\sigma]$. We make use of these new structural results to generate subalgebras of the right nucleus. In the special case $f(t) = t^m - a \in D[t;\sigma]$ we show that $f(t)$ is right-invariant in $L[t;\sigma]$ and that $\mathrm{Nuc}_r(S_f)$ is equal to the associative quotient algebra $L[t;\sigma]/L[t;\sigma]f(t)$.

The eigenring appears implicitly in classical papers by Amitsur [Ami53, Ami54, Ami55], wherein Amitsur shows that any central simple algebra that is split by some field K is isomorphic to the eigenring of some skew polynomial in $K[t;\delta]$, where (K,δ) is a suitable differential field. Any such polynomial is called an *A-polynomial*, however, the property of being an A-polynomial has been somewhat ignored since its introduction. Motivated by Amitsur's work we introduce the notion of *generalised A-polynomials* in $R = D[t;\sigma,\delta]$ in Chapter 7. These are non-constant polynomials in R whose eigenrings are central simple algebras over F. We utilise the results of the previous chapters to provide necessary and sufficient conditions of $f \in R$ to be a generalised A-polynomial in a variety of special cases.

Contents

Chapter 1

Preliminaries and Notation

Although we have tried to make this thesis as comprehensive as possible, we assume that the reader has some knowledge of the basic theory of rings, modules over rings, and algebras over fields, as well as some elementary linear algebra, and the Galois theory of fields.

1.1 Modules, Endomorphism Rings and Annihilators

Let R denote a unital, associative ring and M and M' be left R-modules. Throughout this thesis, all rings and modules are assumed to be unital and we take R-module to mean a left R-module, unless stated otherwise[1].

The set of R-module homomorphisms from M to M' forms an abelian group under addition of maps, denoted by $\mathrm{Hom}_R(M, M')$. In fact, the set of endomorphisms of M is a ring with multiplication defined by the composition of maps, and is denoted by $\mathrm{End}_R(M)$. The structure of $\mathrm{End}_R(M)$ encodes many of the properties of the module M, for example,

[1] All of the notions/results in this section apply analogously if we replace all left R-modules with right R-modules, via symmetric arguments.

Schur's Lemma states that if M is a simple R-module, then $\mathrm{End}_R(M)$ is a division ring, see for example [AW12, pg. 396].

It will be useful to recall some of the basic properties of $\mathrm{End}_R(M)$, especially when M is a direct sum of finitely many left R-modules, or when M is a simple left R-module.

Lemma 1. *[SH04, Exercise 6.7.2] Suppose that $M \cong M'$. Then $\mathrm{End}_R(M) \cong \mathrm{End}_R(M')$.*

Lemma 2. *[SH04, Lemma 6.7.5] Let $M_1, M_2, \ldots, M_k, M_1', M_2', \ldots, M_l'$ be left R-modules, and let $M = M_1 \oplus M_2 \oplus \cdots \oplus M_k$ and $M' = M_1' \oplus M_2' \oplus \cdots \oplus M_l'$.*

(i) $\mathrm{Hom}_R(M, M') \cong \begin{pmatrix} \mathrm{Hom}_R(M_1, M_1') & \cdots & \mathrm{Hom}_R(M_k, M_1') \\ \vdots & \ddots & \vdots \\ \mathrm{Hom}_R(M_1, M_l') & \cdots & \mathrm{Hom}_r(M_k, M_l') \end{pmatrix}$ *as Abelian groups.*

(ii) If $M_1 = M_2 = \cdots = M_k$, then

$$\mathrm{End}_R(M) = \mathrm{End}_R(M_1^{\oplus k}) \cong M_k(\mathrm{End}_R(M_1))$$

as rings.

Lemma 3. *Let $S_1, S_2, \ldots, S_k$ be mutually non-isomorphic simple left R-modules.*

(i) If $i \neq j$, then

$$\mathrm{Hom}_R(S_i, S_j) = 0.$$

(ii) If $i \neq j$ and $m, n \in \mathbb{N}$, then

$$\mathrm{Hom}_R(S_i^{\oplus m}, S_j^{\oplus n}) = 0.$$

(iii) Let $m_1, m_2, \ldots, m_k \in \mathbb{N}$, then

$$\mathrm{End}_R(\bigoplus_{i=1}^{k} S_i^{\oplus m_i}) \cong \bigoplus_{i=1}^{k} \mathrm{End}_R(S_i^{\oplus m_i}).$$

Proof. (i) Let $\phi \in \mathrm{Hom}_R(S_i, S_j)$ be a nonzero map. Since $\ker(\phi)$ is a submodule of S_i, $\ker(\phi) = 0$ (as S_i is simple). Similarly, $\mathrm{im}(\phi)$ is a submodule of S_j, thus we are forced to take $\mathrm{im}(\phi) = S_j$. Hence ϕ is a bijection, i.e. $S_i \cong S_j$. This is a contradiction, and so $\phi = 0$. Therefore $\mathrm{Hom}_R(S_i, S_j) = 0$ as claimed.

(ii) By Lemma 2,

$$\mathrm{Hom}_R(S_i^{\oplus m}, S_j^{\oplus n}) \cong \begin{pmatrix} \mathrm{Hom}_R(S_i, S_j) & \cdots & \mathrm{Hom}_R(S_i, S_j) \\ \vdots & \ddots & \vdots \\ \mathrm{Hom}_R(S_i, S_j) & \cdots & \mathrm{Hom}_R(S_i, S_j) \end{pmatrix},$$

is the ring of $m \times n$ matrices with entries in $\mathrm{Hom}_R(S_i, S_j)$; and by (i), $\mathrm{Hom}_R(S_i, S_j) = 0$. We conclude that $\mathrm{Hom}_R(S_i^{\oplus m}, S_j^{\oplus n}) = 0$.

(iii) By Lemma 2,

$$\mathrm{End}_R(\bigoplus_{i=1}^{k} S_i^{\oplus m_i}) \cong \begin{pmatrix} \mathrm{Hom}_R(S_1^{\oplus m_1}, S_1^{\oplus m_1}) & \cdots & \mathrm{Hom}_R(S_k^{\oplus m_k}, S_1^{\oplus m_1}) \\ \vdots & \ddots & \vdots \\ \mathrm{Hom}_R(S_1^{\oplus m_1}, S_k^{\oplus m_k}) & \cdots & \mathrm{Hom}_R(S_k^{\oplus m_k}, S_k^{\oplus m_k}) \end{pmatrix}.$$

By (ii) and the fact that $\mathrm{End}_R(S_i^{\oplus m_i}) = \mathrm{Hom}_R(S_i^{\oplus m_i}, S_i^{\oplus m_i})$, this

becomes

$$\mathrm{End}_R(\bigoplus_{i=1}^{k} S_i^{\oplus m_i}) \cong \begin{pmatrix} \mathrm{End}_R(S_1^{\oplus m_1}) & 0 & \cdots & 0 \\ 0 & \mathrm{End}_R(S_2^{\oplus m_2}) & \cdots & \vdots \\ \vdots & \cdots & \ddots & 0 \\ 0 & \cdots & 0 & \mathrm{End}_R(S_k^{\oplus m_k}) \end{pmatrix}$$
$$\cong \bigoplus_{i=1}^{k} \mathrm{End}_R(S_i^{\oplus m_i}).$$

□

Let N be a subset of M. The annihilator of N is defined by $\mathrm{Ann}_R(N) = \{r \in R : ra = 0, \forall a \in N\}$, and it is a left ideal of R. If N is a submodule of M, then $\mathrm{Ann}_R(N)$ is a two-sided ideal of R. In particular, the annihilator $M^0 = \mathrm{Ann}_R(M)$ is a two-sided ideal of R. For lack of a proper reference, a proof of the following well known result is included.

Lemma 4. *If I is a two-sided ideal of R contained in M^0, then M is also an R/I-module, and*

$$\mathrm{End}_R(M) = \mathrm{End}_{R/I}(M).$$

In particular M is an R/M^0-module and

$$\mathrm{End}_R(M) = \mathrm{End}_{R/M^0}(M).$$

Proof. Let $\cdot : R \times M \longrightarrow M$ denote the action of R on M. It is well known that we can view the left R-module M as a left R/I-module via a new action $\star_I : R/I \times M \longrightarrow M$, defined by

$$\overline{r} \star_I m = (r + I) \star_I m = r \cdot m \tag{1.1}$$

where $\overline{r}$ denotes the coset $r + I$ for any $r \in R$.

Let ϕ be an endomorphism of M. Then ϕ is R-linear if and only if

$$r \cdot \phi(m) = \phi(r \cdot m)$$

for all $m \in M$, and all $r \in R$, which is true if and only if

$$\overline{r} \star_I \phi(m) = \phi(\overline{r} \star_I m)$$

for all $m \in M$ and all $\overline{r} \in R/I$ by (1.1). We conclude that ϕ is R-linear if and only if ϕ is R/I-linear, hence $\mathrm{End}_R(M) = \mathrm{End}_{R/I}(M)$. The second claim follows by choosing $I = M^0$. □

1.2 Nonassociative Algebras and Associative Central Simple Algebras

Let F be a field and A be a vector space over F. We call A a *(nonassociative) algebra* over F (alternatively an *F-algebra*) if there exists a bilinear map $A \times A \longrightarrow A$, $(a, b) \mapsto ab$ which we call the *multiplication* of A. We assume throughout that any F-algebra A is *unital*, i.e. there exists a multiplicative identity $1 \in A$ such that $1a = a1 = a$ for all $a \in A$.

The *associator* of A is the bracket $[x, y, z] = (xy)z - x(yz)$. If $[x, y, z] = 0$ for all elements $x, y, z \in A$, then A is an *associative* algebra. We define the *left nucleus* of A by $\mathrm{Nuc}_l(A) = \{x \in A : [x, A, A] = 0\}$, the *middle nucleus* of A by $\mathrm{Nuc}_m(A) = \{x \in A : [A, x, A] = 0\}$, and the *right nucleus* of A by $\mathrm{Nuc}_r(A) = \{x \in A : [A, A, x] = 0\}$. The intersection $\mathrm{Nuc}(A) = \mathrm{Nuc}_l(A) \cap \mathrm{Nuc}_m(A) \cap \mathrm{Nuc}_r(A)$ is called the *nucleus* of A, and

the sets $\mathrm{Nuc}_l(A)$, $\mathrm{Nuc}_m(A)$, $\mathrm{Nuc}_r(A)$, and $\mathrm{Nuc}(A)$ are associative subalgebras of A.

The *commutator bracket* on A is defined by $[x, y] = xy - yx$ for all $x, y \in A$. Let $B \subset A$ be a nonempty subset of A, then the *centraliser of B in A* is the set $\mathrm{Cent_A}(B) = \{x \in A : [x, y] = 0 \text{ for all } y \in B\}$. We call the centraliser of A in A the *commutator* of A, and write $\mathrm{Comm}(A) = \mathrm{Cent_A}(A)$. The intersection $\mathrm{C}(A) = \mathrm{Comm}(A) \cap \mathrm{Nuc}(A)$ consisting of all elements in A which both commute and associate with all others is called the *center* of A. The center of any algebra A is an associative, unital, commutative subalgebra of A containing the field F, since we can identify F with $F1 \subseteq \mathrm{C}(A)$.

For $a \in A$ we define the *left (resp. right) multiplication map* $L_a : A \longrightarrow A$ (resp. $R_a : A \longrightarrow A$) by $L_a(x) = ax$ (resp. $R_a(x) = xa$) for all $x \in A$. For $a \neq 0$, if L_a (resp. R_a) is bijective, then a is called *left (resp. right) invertible*, and when a is both left and right invertible then a is said to be *invertible*. When all nonzero elements in A are left (resp., right) invertible, then A is called a *left (resp., right) division algebra*. We call A a *division algebra* if it is both a left and right division algebra. If A has finite dimension over F, then A is a division algebra if and only if A has no non-trivial zero divisors. Unital nonassociative division algebras with a finite number of elements are also known as *(finite) semifields*.

An algebra A is called *simple* if it contains no proper nontrivial two-sided ideals. If A is a unital simple F-algebra, then $\mathrm{C}(A)$ is a field extension of F, and we may regard A as an algebra over $C(A)$. If additionally $[A : C(A)]$ is finite, then we call A a *central simple algebra* over $C(A)$. Any division ring D contains no nontrivial two-sided

ideals other than itself, and additionally if D is assumed to be unital, then its center $\mathrm{C}(D)$ is a field. Thus any unital division ring D such that $[D : C(D)] < \infty$ is a central simple algebra over $C(D)$. In this case, D is also called a *central division algebra* over $C(D)$ (e.g. [Alb52]). It is well known that if A is an associative central simple algebra over $C(A)$, then $[A : C(A)]$ is equal to the square of a positive integer, and $A \cong M_k(D)$ for k a positive integer. Moreover, then D is an associative central division algebra over $C(A)$, with D unique up to isomorphism. The *degree* of A is $\deg(A) = \sqrt{[A : C(A)]}$, and the *index* of A is $\mathrm{ind}(A) = \sqrt{[D : C(A)]} = \deg(D)$ (e.g. [Bou03, Chapter VIII]). When referring to a central simple algebra in this thesis, we assume that it is associative unless otherwise stated.

1.3 Skew Polynomial Rings

Let D be a unital, associative division algebra over its center C, let σ be an endomorphism of D, and let δ be a left σ-derivation of D, i.e. δ is an additive map on D satisfying the Leibniz product rule

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

for all $x, y \in D$. An element $a \in D$ is said to be *fixed* by σ if it satisfies $\sigma(a) = a$, and the set $\mathrm{Fix}(\sigma)$ of such elements is a division subring of D. If σ is an automorphism, then σ is said to be an *inner automorphism* if there exists $u \in D^\times$ such that $\sigma(a) = uau^{-1}$ for all $a \in D$, otherwise σ is said to be an *outer automorphism*. For $u \in D^\times$ we write ι_u to denote the inner automorphism of D defined by $a \mapsto uau^{-1}$. If there exists $n \in \mathbb{Z}^+$ such that $\sigma^n = \iota_u$ for some $u \in D^\times$, and σ^i is an outer automorphism for $1 \leq i < n$, then σ is said to have *finite inner order* n. If no such

integer n exists, then σ is said to have *infinite inner order*. We say that $a \in D$ is a *δ-constant* if $\delta(a) = 0$. The set of all δ-constants also forms a division subring of D denoted by $\mathrm{Const}(\delta)$. The derivation δ is said to be an *inner derivation* if there exists $c \in D$ such that $\delta(a) = [c, a] = ca - ac$ for all $a \in D$, otherwise δ is called an *outer derivation*. For $c \in D$, δ_c denotes the inner derivation of D defined by $\delta_c(a) = [c, a]$ for all $a \in D$.

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

$$a_m t^m + a_{m-1} t^{m-1} + \cdots + a_1 t + a_0$$

in the indeterminate t, with coefficients $a_i \in D$, endowed with term-wise addition, and multiplication defined by

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

for all $a \in D$. Under this addition and multiplication, R forms a unital, associative ring. A simple induction yields

$$(at^j)(bt^k) = \sum_{i=0}^{j} a\Delta_{j,i}(b)t^{i+k}$$

for all $a, b \in D$ and $j, k \in \mathbb{N}$, where the maps $\Delta_{j,i} : D \longrightarrow D$ are defined recursively by the relation

$$\Delta_{j,i} = \delta(\Delta_{j-1,i}) + \sigma(\Delta_{j-1,i-1})$$

with $\Delta_{0,0} = \mathrm{id}_D$, $\Delta_{1,0} = \delta$, and $\Delta_{1,1} = \sigma$. If $\delta = 0$, then R is called a *twisted polynomial ring*, denoted $R = D[t; \sigma]$, and we have $\Delta_{j,i} = 0$ for $j \neq i$, and $\Delta_{j,j} = \sigma^j$. If $\sigma = \mathrm{id}_D$, then R is called a *differential polynomial ring*, denoted $R = D[t; \delta]$, and $\Delta_{j,i} = \binom{j}{i}\delta^{j-i}$. Finally, if both $\sigma = \mathrm{id}$ and

$\delta = 0$, then $R = D[t]$ is the ring of left polynomials with coefficients in D, and $\Delta_{j,i} = 0$ for all $i \neq j$, and $\Delta_{j,j} = \mathrm{id}_D$; in particular $ta = at$ for all $a \in D$.

We refer the reader to [MRS01], [GWJ04], or [Ore33] for an introduction to the theory of skew polynomial rings.

For $f(t) = a_m t^m + a_{m-1} t^{m-1} + \cdots + a_1 t + a_0$ with $a_m \neq 0$, the *degree* of f, denoted by $\deg(f)$, is m, and by convention $\deg(0) = -\infty$. In the particular case that $a_m = 1$, we call f *monic*. The degree of polynomials in R satisfies $\deg(fg) = \deg(f) + \deg(g)$ and $\deg(f+g) \leq \max(\deg(f), \deg(g))$ for all $f, g \in R$. A polynomial $f \in R$ is called *reducible* if $f = gh$ for some $g, h \in R$ such that $\deg(g), \deg(h) < \deg(f)$, otherwise we call f *irreducible*. A polynomial $f \in R$ is called *right (resp. left) invariant* if $fR \subseteq Rf$ (resp. $Rf \subseteq fR$), i.e. Rf (resp. fR) is a two-sided ideal of R. We call f *invariant* if it is both right and left invariant.

The ring $R = D[t; \sigma, \delta]$ is a left Euclidean domain, and as such there is a right Euclidean division algorithm in R: for any $f, g \in R$ with $f \neq 0$, then there exist unique polynomials $q, r \in R$ such that

$$g = qf + r,$$

with $\deg(r) < \deg(f)$. As a result R is a left principal ideal domain. If σ is an automorphism of R, then R is also a right Euclidean domain, hence there is also a left Euclidean division algorithm in R, and R is also a right principal ideal domain, i.e. R is a principal ideal domain. Henceforth we write PID to mean principal ideal domain, and left (resp. right) PID to mean left (resp. right) principal ideal domain.

Now, since R is a left PID, every left ideal of R is generated by a single skew polynomial in R, that is, for any left ideal I, there exists a polynomial $f \in R$, such that $I = Rf$. The *left idealiser* of a polynomial f in R is defined by the set

$$\mathcal{I}(f) = \{g \in R : fg \in Rf\},$$

which is the largest subring of R within which Rf is a two-sided ideal. We define the *eigenring* of f to be the associative quotient ring

$$\mathcal{E}(f) = \frac{\mathcal{I}(f)}{Rf} = \{g \in R : \deg(g) < m \text{ and } fg \in Rf\}.$$

A nonzero skew polynomial $f \in R$ is said to be *bounded* if there exists another nonzero skew polynomial $f^\star \in R$, called a *bound* of f, such that $Rf^\star$ is the unique largest two-sided ideal of R contained in the left ideal Rf. Equivalently, a nonzero polynomial in $f \in R$ is said to be bounded, if there exists a right-invariant polynomial $f^\star \in R$, which is called a bound of f, such that

$$Rf^\star = \mathrm{Ann}_R(R/Rf) \neq \{0\}.$$

Recall that the annihilator $\mathrm{Ann}_R(R/Rf)$ of the left R-module R/Rf is always a two-sided ideal of R. When the skew polynomial f is bounded, it is well known that nontrivial zero divisors in the eigenspace of f are in one-to-one correspondence with proper right factors of f in R:

Theorem 5. *[GT12, Lemma 3, Proposition 4] Let $f \in R$ have positive degree. Then the following are satisfied:*

(i) If f is bounded and σ is an automorphism of D, then f is irreducible

if and only if $\mathcal{E}(f)$ has no non-trivial zero divisors.

(ii) Each non-trivial zero divisor q of f in $\mathcal{E}(f)$ gives a proper factor $\operatorname{gcrd}(q, f)$ *of f.*

Carcanague determines sufficient conditions for all non-zero polynomials in the skew polynomial ring R to be bounded [Car69, Theorem IV]. The following result appears in [BP18, Proposition 21], and is an immediate Corollary to [Car69, Theorem IV]:

Proposition 6. *[BP18, Proposition 21] If σ is an automorphism of D, and $R = D[t; \sigma, \delta]$, then the following are equivalent:*

(1) R has finite rank over its center;

(2) D has finite rank over the field $F_0 = C \cap \operatorname{Fix}(\sigma) \cap \operatorname{Const}(\delta)$.

Moreover, if (1) and (2) are satisfied, then all non-zero polynomials in R are bounded, and if f is irreducible, then S_f is a division algebra.

For $\sigma = \mathrm{id}$, this is [Pum18, Proposition 3]. In many cases, the skew polynomial ring $R = D[t; \sigma, \delta]$ is isomorphic to either a twisted polynomial ring, or a differential polynomial ring. In fact, if D has finite dimension as an algebra over its center C, then $R = D[t; \sigma, \delta]$ is either a twisted polynomial ring or a differential polynomial ring [Jac09, Theorem 1.1.21]. In many parts of this thesis, we will require D to be finite dimensional over $F_0 = C \cap \operatorname{Fix}(\sigma) \cap \operatorname{Const}(\delta)$, so that all polynomials in $R = D[t; \sigma, \delta]$ are bounded; in this case, it is necessary that $[D : C]$ be finite. Hence, in many places we lose no generality when we examine the special cases $R = D[t; \sigma]$ and $R = D[t; \delta]$ separately.

We obtain the following Corollary to Proposition 6, describing special cases for which all non-zero polynomials in R are bounded:

Corollary 7. *Let D be a central division algebra over C of degree d.*

(i) If σ has finite inner order, then all non-zero polynomials in $R = D[t;\sigma]$ are bounded.

(ii) If D has characteristic zero, and δ is an inner derivation, then all non-zero polynomials in $R = D[t;\delta]$ are bounded.

(iii) If D has prime characteristic, and $\delta|_C$ is algebraic, then all non-zero polynomials in $R = D[t;\delta]$ are bounded.

Proof. We refer the reader to Sections 1.4 and 1.5 of [Jac09], in which Jacobson shows that D has finite dimension as an F-vector space, hence finite rank as an F-module in cases (i)-(iii). The result follows immediately by Proposition 6. □

Since any bound $f^\star$ of a non-zero polynomial f in R is a right-invariant polynomial in R, we recall some results which determine the right-invariant polynomials in R, when R is either a twisted polynomial ring, or a differential polynomial ring.

Independently, Jacobson [Jac09] and Petit [Pet66] determine the right-invariant polynomials in $R = D[t;\sigma]$ and the center of R:

Proposition 8. *([Pet66, (15)], [Jac09, Theorem 1.1.22])*

(i) The polynomial $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in D[t;\sigma]$ is right-invariant in $D[t;\sigma]$ if and only if $a_i \in \mathrm{Fix}(\sigma)$ and $\sigma^m(c)a_i = a_i\sigma^i(c)$ for all $i \in \{0,1,\ldots,m-1\}$ and for all $c \in D$.

(ii) $f(t)$ is right-invariant in $D[t;\sigma]$ if and only if $f(t) = ag(t)t^s$ for some $a \in D^\times$, $g(t) \in C(R)$ and integer $s \geq 0$.

(iii) If no non-zero power of σ is an inner automorphism then $C(R) = F$.

(iv) If σ has finite inner order n with $\sigma^n = \iota_u$ for some $u \in D^\times$, then $C(R)$ is equal to the set of polynomials of the form

$$\gamma_0 + \gamma_1 u^{-1} t^n + \gamma_2 u^{-2} t^{2n} + \cdots + \gamma_s u^{-s} t^{sn}$$

for some $s \in \mathbb{N} \cup \{0\}$ and $\gamma_i \in F$ such that $\gamma_i u^{-i} \in \mathrm{Fix}(\sigma)$. Moreover, if n is also the order of $\sigma|_C$, then u can be taken from $\mathrm{Fix}(\sigma)$, and

$$C(R) = F[u^{-1}t^n].$$

The last situation holds if $[D : C] < \infty$.

Also, Amitsur [Jac09, Theorem 1.1.32] determines the right-invariant polynomials in $R = D[t; \delta]$ and its center:

Theorem 9. *[Jac43, Theorem 1.1.32]*

(i) The right-invariant polynomials of $R = D[t; \delta]$ are the elements $ap(t)$ where $a \in D$ and $q(t) \in C(R)$.

(ii) For D of characteristic zero, the following are satisfied:

(a) If $\delta = \delta_c$ for some $c \in D^\times$, then

$$C(R) = F[t - c]$$

which is isomorphic to $F[x]$ under the map fixing elements of F and sending $t - c$ to x.

(b) If δ is an outer derivation, then $C(R) = F$.

(iii) If D has prime characteristic p, then the following are satisfied:

(a) If $\delta|_C$ is algebraic with minimum polynomial

$$g(t) = t^{p^e} + \gamma_1 t^{p^{e-1}} + \cdots + \gamma_e t \in F[t]$$

such that $g(\delta) = \delta_c$ *for some* $c \in D^\times$*, then*

$$C(R) = F[g(t) - c]$$

which is isomorphic to $F[x]$ *under the map fixing elements of* F *and sending* $g(t) - c$ *to* x*.*

(b) If $\delta|_C$ *is transcendental, then* $C(R) = F$*.*

1.4 Petit Algebras

This section is dedicated to a construction of nonassociative algebras obtained from a skew polynomial ring R, which generalises the construction of the associative quotient algebras of R obtained from factoring R by a two-sided principal ideal.

Let $R = D[t; \sigma, \delta]$ be a skew polynomial ring, and let $f \in R$ have positive degree m. The skew polynomials of degree less than m canonically represent the elements of the right R-module R/Rf. Moreover, the set of skew polynomials of degree less than m

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

endowed with the usual term-wise addition, and the multiplication defined by

$$g \circ_f h = \begin{cases} gh, & \text{if } \deg(g) + \deg(h) < m \\ gh \bmod_{\mathrm{r}} f, & \text{if } \deg(g) + \deg(h) \geq m \end{cases}$$

where $\bmod_{\mathrm{r}} f$ denotes the remainder on right division by f, is a unital, nonassociative ring S_f, which we also denote by R/Rf. When the con-

text is clear we will use $\circ$, or simply juxtaposition in place of $\circ_f$ for the multiplication in S_f. The ring S_f has the structure of a unital, nonassociative algebra over its subfield $F = \{a \in D : ag = ga \text{ for all } g \in S_f\} = \mathrm{Comm}(S_f) \cap D$. We remark that S_f is a free left D-module of finite rank with basis $t^0 = 1, t^1 = t, t^2, \ldots, t^{m-1}$, and S_f is associative if and only if f is right-invariant in R, in which case S_f is equal to the associative quotient algebra $R/(f)$. The algebras S_f were first introduced in 1966 by Petit, hence they are known as Petit algebras [Pet66]. The skew polynomials f and df yield isomorphic Petit algebras for any $d \in D^\times$, and if $\deg(f) = 1$, then $S_f \cong D$.

It can be easily shown that the field $F = \mathrm{Comm}(S_f) \cap D$ is equal to the subfield $C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$ of D, i.e.

$$F = \mathrm{Comm}(S_f) \cap D = C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta).$$

To see this, suppose that $a \in F \subseteq D$, so that $ga = ag$ for all $g \in S_f$. In particular $ab = ba$ for all $b \in D$, and $at = ta$. That is, $a \in C$, and

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

which yields $\sigma(a) = a$ and $\delta(a) = 0$. Therefore $a \in C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$. On the other hand, if $a \in C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$, then $\Delta_{j,i}(a) = 0$, and $\Delta_{j,j}(a) = a$ for any non-negative integers i, j, such that $i < j$. So for any $g(t) = \sum_{j=0}^{m-1} g_j t^j \in S_f$ we have

$$ga = (\sum_{j=0}^{m-1} g_j t^j)a = \sum_{j=0}^{m-1} g_j \sum_{i=0}^{j} \Delta_{j,i}(a) t^i = \sum_{i=0}^{m-1} g_j a t^j = a \sum_{i=0}^{m-1} g_j t^j = ag,$$

i.e. $a \in F$. Hence $F = C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$.

In [Pet66], Petit determines the right, middle, and left nuclei of S_f and provides equivalent conditions for the indeterminant t to be contained in the right nucleus of S_f:

Theorem 10. *[Pet66, (2),(5)] Let $f \in R$ have degree $m > 1$.*

(i) The right nucleus of S_f is equal to the eigenring of f, that is

$$\mathrm{Nuc}_r(S_f) = \mathcal{E}(f).$$

(ii) If f is not right-invariant, then the left and middle nuclei of S_f are equal to D, that is

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

(iii) $ft \in Rf$ if and only if $t \in \mathrm{Nuc}_r(S_f)$ if and only if $t \circ_f t^m = t^m \circ_f t$ if and only if the powers of t are associative.

Remark. *We note here that for $f \in R$ of degree 1, i.e. $f(t) = t - a$ for some $a \in D$, the right nucleus is $\mathrm{Nuc}_r(S_f) = D$, as $S_f \cong D$, however, the eigenring of f is given by*

$$\mathcal{E}(f) = \{b \in D : \sigma(b)a = ab - \delta(b)\},$$

which is not equal to D in general. For instance, if D is commutative and $\delta = 0$, then the eigenring of f is

$$\mathcal{E}(f) = \{b \in D : \sigma(b) = b\} = \mathrm{Fix}(\sigma),$$

which is not equal to D when σ is not the identity map. Hence Theorem

10 does not apply for $\deg(f) = 1$.

Chapter 2

The Eigenring of $f \in D[t;\sigma]$

2.1 The Minimal Central Left Multiple of $f \in D[t;\sigma]$

Throughout this chapter, unless stated otherwise, let D be a central division algebra over C of degree d, let σ be an automorphism of D of finite order n modulo inner automorphisms with $\sigma^n = \iota_u$, and let $f \in R = D[t;\sigma]$ be a monic, non-constant polynomial of degree $m \geq 1$. Then D has finite dimension d^2n over the field $F = C \cap \mathrm{Fix}(\sigma)$. Recall that R has center

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

and that all non-constant polynomials in R are bounded. We define the minimal central left multiple of f to be the polynomial $h(t) = \hat{h}(u^{-1}t^n)$ where $\hat{h} \in F[x]$ is a monic polynomial of minimal degree such that f right divides h in R. In the following we use the notation h and $\hat{h}$ for the minimal central left multiple of f.

We begin by providing some results on the minimal central left multiple of $f \in D[t;\sigma]$, and the relationship between irreducible factors of h

in R and irreducible factors of f in R.

Given a bound f^* of f, it is straightforward to determine the minimal central left multiple of f:

Proposition 11. *Let $f \in R$ be a non-constant polynomial with a given bound $f^* = ac(t)t^r$ where $a \in D^\times$, $c(t) = \hat{c}(u^{-1}t^n)$ for some monic polynomial $\hat{c} \in F[x]$, and some $r \in \{0, 1, \ldots, n-1\}$.*

(i) If $r = 0$, then

$$h(t) = a^{-1}f^* = c(t),$$

i.e. $\hat{h}(x) = \hat{c}(x)$.

(ii) If $r \neq 0$, then

$$h(t) = pf^* = c(t)u^{-1}t^n,$$

where $p(t) = u^{-1}\sigma^{n-s}(a^{-1})t^{n-r} \in R$, i.e. $\hat{h}(x) = \hat{c}(x)x$.

Proof. (i) If $r = 0$, then $f^* = ac(t)$ is a central left multiple of f, and if c' is any other central left multiple of f, then c' has degree greater than or equal to that of f^*, or else Rc' is a two-sided ideal of R contained in Rf that is not contained in Rf^*, which contradicts the definition of the bound of f. Hence f^* is a central left multiple of f of minimal degree. Now $f^* = bh(t) = b\hat{h}(u^{-1}t^n)$ for some $b \in D^\times$, i.e.

$$a\hat{c}(x) = b\hat{h}(x).$$

Comparing lead coefficients on both sides yields $a = b$, i.e. $h(t) = a^{-1}f^* = c(t)$ as claimed.

(ii) If $0 < r < n-1$, then the polynomial

$$u^{-1}\sigma^{n-r}(a^{-1})t^{n-r}f^*$$

is clearly a left multiple of f, because f^* is a left multiple of f. Now, since $c(t)$ commutes with all polynomials in R (in particular, with powers of t and elements of D) we have that:

$$\begin{aligned} u^{-1}\sigma^{n-r}(a^{-1})t^{n-s}f^* &= (u^{-1}\sigma^{n-r}(a^{-1})t^{n-r})(ac(t)t^r) \\ &= u^{-1}\sigma^{n-r}(a^{-1})\sigma^{n-r}(a)c(t)t^n \\ &= c(t)u^{-1}t^n. \end{aligned}$$

Therefore the polynomial pf^* with $p(t) = u^{-1}\sigma^{n-r}(a^{-1})t^{n-r}$ is a central left multiple of f, that is also monic as polynomial in $F[x]$ when we make the identification $x = u^{-1}t^n$. Hence in order to confirm that pf^* is the *minimal* central left multiple of f, we need only show that there is no central left multiple of f of strictly lower degree. To this end suppose for a contradiction that e is a central left multiple of f of degree less than that of pf^*. Since the degree of e is a multiple of n, it has degree at most $\deg(pf^*) - n$, and since $\deg(pf^*) = \deg(f^*) + n - r$, we have the following inequalities

$$\deg(e) \leq \deg(f^*) - r < \deg(f^*)$$

as $r > 0$. Therefore Re is a two-sided ideal of R contained in Rf, but $Re \nsubseteq Rf^*$, which is a contradiction, since f^* is a bound of f. Hence pf^* achieves minimal degree for a central left multiple of f and the result follows immediately. □

As we have already seen, all non-constant polynomials in R have

a uniquely determined bound (unique up to left multiplication by an element of $D^\times$), hence the preceding result guarantees that any non-constant polynomial has a uniquely determined minimal central left multiple which is a multiple of its bound.

We note that in the notation of Proposition 11, if $(f,t)_r = 1$ then $r = 0$, and f^* is equal to $ah(t)$, i.e. f^* is central up to left multiplication by an element in $D^\times$.

Proposition 12. *Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$, and let f have minimal central left multiple $h(t) = \hat{h}(u^{-1}t^n)$ for some monic polynomial $\hat{h} \in F[x]$ with constant coefficient h_0.*

(i) The following are equivalent:

(a) $a_0 \neq 0$,

(b) $(f,t)_r = 1$,

(c) $h_0 \neq 0$,

(d) $(h,t)_r = 1$.

(ii) If the equivalent conditions of (i) are satisfied, then $f(t) \neq t$, and $\hat{h}(x) \neq x$.

Proof. (i) Clearly, (a) is equivalent to (b), and (c) is equivalent to (d), therefore we need only show that $(a)/(b)$ implies $(c)/(d)$ and vice versa. Firstly, we show that $(c) \Rightarrow (b)$ via the contrapositive. So suppose that $(f,t)_r \neq 1$, then we must have that $(f,t)_r = t$ since 1 and t are the only monic right divisors of t. Then t right divides f, i.e. $f = pt$ for some $p \in R$, and so $h = gf = (gp)t$ for some $g \in R$. We conclude that $(h,t)_r \neq 1$.

Finally, to show that $(b) \Rightarrow (c)$, suppose that $(f,t)_r = 1$, and suppose for

a contradiction that $(h,t)_r \neq 1$. Then $h = qt$ for some $q \in R$. Since t is a proper two-sided divisor of h in R, there exists a proper factorisation of f in R of the form $f = ab$ where $b = (f,t)_r$, and a is bounded [GTLN13, Proposition 5.1]. However, $b = (f,t)_r = 1$ by assumption, which is a contradiction, $b = 1$ is not a proper factor of f. Hence we conclude that (b) and (c) are equivalent.

(ii) Now assume that the equivalent conditions of (i) are satisfied. Immediately we obtain $f(t) \neq t$ (else $a_0 = 0$). Moreover if $\hat{h}(x) = x$, then $h_0 = 0$ thus (ii) follows via the contrapositive. □

Corollary 13. *Let $f = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ be irreducible, and let f have minimal central left multiple $h(t) = \hat{h}(u^{-1}t^n)$ for some monic, irreducible $\hat{h} \in F[x]$ with constant coefficient h_0. Then the following are equivalent:*

(1) $a_0 \neq 0$,

(2) $(f,t)_r = 1$

(3) $h_0 = 0$,

(4) $(h,t)_r = 1$,

(5) $\hat{h}(x) \neq x$,

(6) $f(t) \neq t$.

Proof. By Proposition 12, (1) - (4) are equivalent, and the equivalent conditions (1) - (4) imply (5) and (6). To complete the proof, we show that (5) implies (6), and that (6) implies (2).

(5) ⇒ (6)

We show that (5) ⇒ (6) by proving the contrapositive, i.e. if $f(t) = t$, then $\hat{h}(x) = x$.

Suppose that $f(t) = t$, and let $g(t) = u^{-1}t^{n-1}$, then

$$g(t)f(t) = (u^{-1}t^{n-1})t$$

is a monic polynomial of minimal positive degree in the commutative polynomial ring $F[u^{-1}t^n]$. Therefore we must have

$$h(t) = \hat{h}(u^{-1}t^n) = u^{-1}t^n$$

by definition of the minimal central left multiple of f, and we conclude that $\hat{h}(x) = x$.

(6) $\Rightarrow$ (2)

Finally, suppose that $f(t) \neq t$. As f is assumed to be a monic, irreducible polynomial in R, we must have either $(f,t)_r = f$ or $(f,t)_r = 1$. If $(f,t)_r = f$ then, by definition of the greatest common right divisor, $t = pf$ for some $p \in R$. Since both t and f are monic, irreducible polynomials we are forced to take $p = 1$, and $f = t$, a contradiction. Hence we are left with $(f,t)_r = 1$. □

Lemma 14. *(for finite fields this is [Gie98]) Suppose that $h \in R$ is such that $h = \hat{h}(u^{-1}t^n)$ for some monic $\hat{h} \in F[x]$ and either $\hat{h}(x) = x$, or h has nonzero constant term. Then the quotient algebra R/Rh has center*

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

Proof. Since $\hat{h}(u^{-1}t^n) \in C(R)$, Rh is a two-sided ideal in R. If $\hat{h}(x) = x$, then a direct calculation shows that $C(R/Rh) = F[x]/(x) = F$.

So suppose that $\hat{h}(x) \neq x$, and h has nonzero constant term h_0. Let $\phi : R \longrightarrow R/Rh$, $\phi(a) = a + Rh$. If $a \in C(R)$, then $(a + Rh)(b + Rh) =$

$(b + Rh)(a + Rh)$ for any $b \in R$, and so $a + Rh = \phi(a) \in C(R/Rh)$. Therefore $\phi(C(R)) \subset C(R/Rh)$.

Now let $\bar{a} \in C(R/Rh)$, then $\bar{a} = a + Rh$ for some $a \in R$ such that $\deg(a) < \deg(h) = mn$, and $(a + Rh)(b + Rh) = (b + Rh)(a + Rh)$ for all $b \in R$, which is equivalent to $ab + Rh = ba + Rh$ for all $b \in R$. This means that for all $b \in R$, we have

$$ab = ba + r_b h \tag{2.1}$$

for some $r_b \in R$.

As (2.1) is satisfied for all $b \in R$, let $b \in D$ and suppose $r_b \neq 0$. By comparing degrees on both sides of Equation (2.1), we obtain

$$\deg(ab) = \deg(ba + r_b h) \Leftrightarrow \deg(a) = \deg(r_b h).$$

This is a contradiction; thus we conclude $r_b = 0$ and $ab = ba$, i.e. a commutes with all elements of D. Now suppose that $b = t$. Assume for a contradiction that $r_t \notin D$, so $\deg(r_t) \geq 1$. Comparing degrees yields

$$\deg(at) = \deg(ta + r_t h) \Rightarrow \deg(a) + 1 = \deg(r_t h) \geq \deg(h) + 1,$$

which is a contradiction, thus $r_t \in D$. Comparing constant terms on both sides of (2.1), we see that $r_t h_0 = 0$, where h_0 is the constant term of h. This implies that either $r_t = 0$ or $h_0 = 0$. Since $h_0 \neq 0$ this forces $r_t = 0$, and $at = ta$, i.e. a commutes with t, and therefore by induction, also with t^j. Thus $a \in C(R)$. Hence for all $\bar{a} \in C(R/Rh)$, there exists $a \in C(R)$ such that $\bar{a} = \phi(a) \in \phi(C(R))$, and so $C(R/Rh) = \phi(C(R))$.

Due to this, any element $\bar{a} \in \phi(C(R))$ can be written in the form $\bar{a} = a + Rh$ for some $a \in C(R) \cong F[x]$, where $\deg(a) < \deg(h)$. Moreover, $\phi(C(R))$ inherits the multiplication of R/Rh. Define a map from $\phi(C(R))$

to $F[x]/(\hat{h}(x))$ which fixes elements of F and maps $u^{-1}t^n + Rh$ to $x + (\hat{h}(x))$. This yields an F-algebra isomorphism and thus $C(R/Rh) \cong F[x]/(\hat{h}(x))$. □

2.2 The Eigenring of $f \in D[t;\sigma]$ for $\hat{h}$ Irreducible

Recall that D is a central division algebra of finite degree d over C, and σ is an automorphism of D of finite inner order n, with $\sigma^n = \iota_u$ for $u \in D^\times$. In the following, let $f \in R = D[t;\sigma]$ be monic of degree m with minimal central left multiple $h(t) = \hat{h}(u^{-1}t^n)$, where $\hat{h}$ is a monic polynomial in $F[x]$. In this section, we determine the structure of the eigenring of f, if $\hat{h}(x)$ is irreducible in $F[x]$.

Lemma 15. *[Jac43, Theorem 13] Let f be irreducible in R such that $(f,t)_r = 1$. Then $\hat{h}(x)$ is irreducible in $F[x]$.*

Proof. Suppose that $\hat{h} = \hat{a}\hat{b}$ for some $\hat{a}, \hat{b} \in F[x]$, with $\deg(\hat{a}), \deg(\hat{b}) < \deg(\hat{h})$. If f divides $\hat{a}(u^{-1}t^n)$ on the right, then $\hat{a}(u^{-1}t^n)$ is a left multiple of f of degree less than $\hat{h}(u^{-1}t^n)$, contradicting the minimality of h. Therefore f does not divide $\hat{a}(u^{-1}t^n)$. Since f is irreducible, we have that $(f, \hat{a}(u^{-1}t^n))_r = 1$, and since R is a right Euclidean domain, there exist $p, q \in R$ such that

$$pf + q\hat{a}(u^{-1}t^n) = 1.$$

Multiplying through by $\hat{b}(u^{-1}t^n)$ on the right gives

$$pf\hat{b}(u^{-1}t^n) + q\hat{a}(u^{-1}t^n)\hat{b}(u^{-1}t^n) = \hat{b}(u^{-1}t^n).$$

Since f right divides $\hat{h}(u^{-1}t^n)$ there exists $g \in R$ such that $\hat{h}(u^{-1}t^n) =$

$\hat{a}(u^{-1}t^n)\hat{b}(u^{-1}t^n) = g(t)f(t)$, therefore we get

$$(p\hat{b}(u^{-1}t^n) + qg)f = \hat{b}(u^{-1}t^n).$$

That is, $\hat{b}(u^{-1}t^n)$ is a left multiple of f, and since $\deg(\hat{b}) < \deg(\hat{h})$, $\hat{b}$ is a left multiple of f of degree less than $\hat{h}$, contradicting the minimality of h. Hence $\hat{h}$ is irreducible in $F[x]$. □

Although the converse to Lemma 15 is false in general, Gomez-Torrecillas et al [GTLN13] give sufficient conditions for which it holds true. Note that $\deg(h) = mnd$ is the largest possible degree of h. We rephrase the original statement of [GTLN13, Proposition 4.1] to suit our theory since the authors did not recognise $\mathcal{E}(f)$ as the right nucleus of the nonassociative algebra S_f.

Proposition 16. *[GTLN13, Proposition 4.1] Let $f \in R$ have degree $m > 1$ and satisfy $(f,t)_r = 1$. If $\deg(h) = mnd$ and $\hat{h}$ is irreducible in $F[x]$, then f is irreducible and $\mathrm{Nuc}_r(S_f) \cong F[x]/(\hat{h}(x))$.*

If the minimal central left multiple of f is irreducible as a polynomial in $F[x]$, then the irreducible factors in any factorisation of f in R are mutually similar:

Lemma 17. *Let $f \in R$ satisfy $(f,t)_r = 1$, and let $\hat{h}(x)$ be irreducible in $F[x]$. Then all irreducible factors of f are similar to all irreducible factors of h. In particular, all irreducible factors of f are mutually similar to each other.*

Proof. In the language of [Jac09, Theorem 1.2.19], $h(t)$ is a two-sided maximal element of R, hence any factorisation $h(t) = h_1(t)\cdots h_k(t)$ into irreducible polynomials in R is unique up to similarity of polynomials,

and $h_i \sim h_j$ for all i, j. Let $f(t) = f_1(t) \cdots f_l(t)$ for f_i irreducible polynomials in R. Then, by definition of the minimal central left multiple

$$h_1(t)h_2(t) \cdots h_k(t) = p(t)f_1(t)f_2(t) \cdots f_l(t)$$

for some $p \in R$. Since the decomposition of h is unique up to similarity, for each $i \in \{1, \ldots, l\}$, there must exist $j \in \{1, \ldots, k\}$ such that $f_i \sim h_j$. Finally, as $h_i \sim h_j$ for all i, j, we conclude that $f_i \sim f_j$ for all i, j. □

Define $E_{\hat{h}} = F[x]/(\hat{h}(x))$. This is a commutative, associative algebra over F of dimension $\deg(\hat{h})$. If $\hat{h}$ is irreducible in $F[x]$, then $E_{\hat{h}}$ is a field extension of F of degree $\deg(\hat{h})$. We first consider the case that f has degree at least 2 and that f is irreducible in R, which is a sufficient condition for $\hat{h}$ to be irreducible in $F[x]$ by Lemma 15. We show that $\mathrm{Nuc}_r(S_f)$ is a central division algebra of degree $s = dn/k$ over a field extension $E_{\hat{h}}$ of F determined by h, where k is the number of irreducible factors in any factorisation of h into irreducible polynomials in R.

After we have explored some special cases, we loosen the restriction that f is irreducible in R, instead assuming only that $\hat{h}$ is irreducible in $F[x]$. We show that $\mathrm{Nuc}_r(S_f)$ is a central simple algebra of degree $s = ldn/k$ over the same field extension $E_{\hat{h}}$ of F, with k as above, and l the number of irreducible factors in any factorisation of f into irreducible polynomials in R.

Lemma 18. *[Jac09, p. 16] Suppose that $h \in R$ is such that $h(t) = \hat{h}(u^{-1}t^n)$ for some $\hat{h} \in F[x]$, $\hat{h}(x) \neq x$, and such that $\hat{h}$ is irreducible in $F[x]$. Then h generates a maximal two-sided ideal Rh in R.*

Let $f(t) = t - a \in R$ for some $a \in D$. Then the F-algebra S_f is equal to the associative ring D, hence $\mathrm{Nuc}_r(S_f) = D$. Moreover for any $b \in D$,

it can be easily seen that fb lies in Rf if and only if $\sigma(b)a = ab$. Thus the eigenring $\mathcal{E}(f)$ is equal to $\{b \in D : \sigma(b)a = ab\}$. In particular, if $a \in C$ then $\mathcal{E}(f) = \mathrm{Fix}(\sigma)$ and if $\sigma = \mathrm{id}$, then $\mathcal{E}(f) = \mathrm{Cent}_D(a)$. Henceforth, for the rest of the chapter, unless stated otherwise, we assume that f has degree $m > 1$, in which case $\mathrm{Nuc}_r(S_f) = \mathcal{E}(f)$.

Theorem 19. *Let $f \in R = D[t;\sigma]$ be irreducible of degree $m > 1$. Then $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}} = F[x]/(\hat{h}(x))$ of degree $s = dn/k$, where k is the number of irreducible factors of h in R, and*

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

This means that $\deg(\hat{h}) = \frac{md}{s}$, $\deg(h) = \frac{mnd}{s}$, *and*

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

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

Proof. The minimal central left multiple h of f is a two-sided maximal element in R in the terminology of [Jac09], and $h = gf$ for some $g \in R$ by the definition of h. Since R is a principal ideal domain, the irreducible factors h_i of any factorization $h = h_1 h_2 \cdots h_k$ of h into irreducible polynomials are all similar as polynomials. This implies that all irreducible factors of h have the same degree.

Moreover, R/Rh is a simple Artinian ring with $R/Rh \cong M_k(D_h)$, where $D_h \cong \mathcal{I}(h_i)/Rh_i$ and $\mathcal{I}(h_i) = \{g \in R : h_i g \in Rh_i\}$ is the idealiser of Rh_i [Jac09, Theorem 1.2.19].

Since f is an irreducible divisor of h with $h = gf$ for some $g \in R$, we thus obtain that $h = h_1 h_2 \cdots h_{k-1} f$ for some irreducible polynomials

$h_i \in R$ of degree m, $D_h \cong \mathcal{I}(f)/Rf = \mathcal{E}(f)$, and therefore

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

since the eigenring of f is equal to the right nucleus of S_f when f has degree at least 2. In particular, here h has degree km and since f is irreducible, $\mathrm{Nuc}_r(S_f)$ is a division algebra. Now R/Rh is a central simple algebra over $E_{\hat{h}}$ and so $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}}$ of dimension s^2. Comparing the dimensions of R/Rh and $M_k(\mathrm{Nuc}_r(S_f))$ over F it follows that $d^2n\deg(h) = d^2n^2\deg(\hat{h}) = k^2s^2\deg(\hat{h})$, so that we get $d^2n^2 = k^2s^2$, that is $dn = ks$. In particular, this implies that $\deg(h) = \frac{dnm}{s}$ and $\deg(\hat{h}) = \frac{dm}{s}$. Moreover

$$[\mathrm{Nuc}_r(S_f) : F] = [\mathrm{Nuc}_r(S_f) : E_{\hat{h}}][E_{\hat{h}} : F] = s^2\deg(\hat{h}) = \frac{dms^2}{s} = dms.$$

Now since $\mathrm{Nuc}_r(S_f)$ is a subalgebra of S_f we have

$$[S_f : F] = [S_f : \mathrm{Nuc}_r(S_f)][\mathrm{Nuc}_r(S_f) : F] = d^2mn. \tag{2.2}$$

Substituting $dn = ks$ and $[\mathrm{Nuc}_r(S_f) : F] = dms$ into Equation (3.2) we obtain the equality $[S_f : \mathrm{Nuc}_r(S_f)] = k$. If f is not right-invariant, then $k > 1$ and so we derive $s \neq dn$ looking at the degree of h. More precisely, for f of degree $m > 1$, f being not right-invariant is equivalent to S_f being not associative which in turn is equivalent to $k > 1$. □

Remark. *If we consider the degree one polynomial $f = t - a$ for some $a \in D^\times$, then an analogous proof to the one of Theorem 19 yields* $\deg(h) = \frac{nd}{s}$, $\deg(\hat{h}) = \frac{d}{s}$ *and that $\mathcal{E}(f)$ is a central division algebra over F of degree s contained in D. In particular s divides d. Recall that for f of degree one,* $\mathrm{Nuc}_r(S_f)$ *is not necessarily equal to the eigenring of f.*

Now that we have dealt with the right nucleus of f for f an irreducible polynomial in R, we turn our attention to the more general setting with f not necessarily irreducible in R, but with $\hat{h}$ an irreducible polynomial in $F[x]$. Note that this setting includes the previous case that $f \in R$ is irreducible, which corresponds to the case $l = 1$ in the following result (Theorem 20).

Theorem 20. *Let $f \in R$ satisfy $(f,t)_r = 1$, and suppose that $\hat{h}(x)$ is irreducible in $F[x]$. Then f is the product of $l \geq 1$ irreducible polynomials in R all of which are mutually similar to each other, and*

$$R/Rh \cong M_k(\mathcal{E}(g))$$

where $g \in R$ is any irreducible divisor of h in R. If $\deg(g) = r \geq 1$, then $m = rl$, $\mathcal{E}(g)$ is a central division algebra over $E_{\hat{h}} = F[x]/(\hat{h}(x))$ of degree $s' = dn/k$, where k is the number of irreducible factors of h, and

$$\mathrm{Nuc}_r(S_f) \cong M_l(\mathcal{E}(g)).$$

In particular, $\mathrm{Nuc}_r(S_f)$ is a central simple algebra over $E_{\hat{h}}$ of degree $s = ls'$, $\deg(\hat{h}) = \frac{rd}{s'} = \frac{md}{s}$, $\deg(h) = \frac{rnd}{s'} = \frac{mnd}{s}$, and

$$[\mathrm{Nuc}_r(S_f) : F] = l^2 rds' = mds.$$

In particular s' divides $\gcd(rd, dn)$, and s divides $\gcd(md, dn)$.

Proof. Since $\hat{h}$ is irreducible in $F[x]$, h is a two-sided maximal element of R in the language of [Jac09], and $h = pf$ for some $p \in R$ by the definition of the minimal central left multiple. Since R is a principal ideal domain, the irreducible factors h_i of any factorisation $h = h_1 h_2 \cdots h_k$ of h in R

into irreducible polynomials are all similar as polynomials. In particular, $R/Rh_i \cong R/Rh_j$ for all i, j, and all irreducible factors of h have the same degree.

Moreover, R/Rh is a simple Artinian ring with $R/Rh \cong M_k(\mathcal{E}(g))$, where $g \in R$ is an irreducible polynomial similar to h_i for all i, and $\mathcal{E}(g)$ denotes the eigenring of g in R [Jac09, Theorem 1.2.19].

Let $A = R/Rh$, and suppose that $f = f_1 f_2 \cdots f_l$ where $f_i \in R$ are irreducible polynomials. Then $f_i \sim f_j$ for any i, j, and each of the polynomials g_i has minimal central left multiple h [GTLN13, Proposition 5.2]. Any left A-module is isomorphic to a direct sum of simple left A-modules, and any two simple left A-modules are isomorphic [Jac43, Theorem 25]. It follows that

$$R/Rf \cong R/Rf_1 \oplus R/Rf_2 \oplus \cdots \oplus R/Rf_l$$

as left A-modules (e.g. see [GTLN13, Corollary 4.7]). Since $R/Rf_i \cong R/Rg$ for g any irreducible factor of h, we have

$$R/Rf \cong (R/Rg)^{\oplus l},$$

as left A-modules. By Lemmas 1 and 2, we obtain

$$\mathrm{End}_A(R/Rf) \cong \mathrm{End}_A((R/Rg)^{\oplus l}) \cong M_l(\mathrm{End}_A(R/Rg)),$$

as rings. Since h is a bound of both f and g, the two-sided ideal Rh is equal to $\mathrm{Ann}_R(R/Rf)$ and to $\mathrm{Ann}_R(R/Rg)$ [Jac43, pg. 38]. Hence $\mathrm{End}_R(R/Rf) = \mathrm{End}_A(R/Rf)$ and $\mathrm{End}_R(R/Rg) = \mathrm{End}_A(R/Rg)$, by

Lemma 4, and

$$\mathrm{End}_R(R/Rf) \cong M_l(\mathrm{End}_R(R/Rg)).$$

Finally, for any $p \in R$, the eigenring $\mathcal{E}(p)$ is isomorphic to $\mathrm{End}_R(R/Rp)$, therefore

$$\mathcal{E}(f) \cong M_l(\mathcal{E}(g)).$$

Suppose that $\deg(g) = r \geq 1$ for g any irreducible factor of h in R. Then $f = f_1 f_2 \cdots f_l$ for $f_i \in R$ irreducible, implies that $\deg(f_i) = r$, and

$$m = \deg(f) = \sum_{i=1}^{l} \deg(f_i) = rl.$$

Now since g is irreducible of degree r with minimal central left multiple $h(t) = \hat{h}(u^{-1}t^n)$, $\mathcal{E}(g)$ is a central division algebra over $E_{\hat{h}}$ of degree $s' = dn/k$, where k is the number of irreducible divisors of h in R, $\deg(\hat{h}) = \frac{rd}{s'} = \frac{md}{ls'}$ and $\deg(h) = \frac{rdn}{s'} = \frac{mdn}{ls'}$ by Theorem 19. Finally, since

$$\mathcal{E}(f) \cong M_l(\mathcal{E}(g)),$$

$\mathcal{E}(f)$ is a central simple algebra over $E_{\hat{h}}$ of degree $s = ls'$, and

$$[\mathcal{E}(f) : F] = s^2 \deg(\hat{h}) = mds.$$

□

An immediate Corollary to Theorem 20 is:

Corollary 21. *Under the assumptions of Theorem 20*

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

In Theorem 20, in the particular case that $\deg(g) = 1$, f is the product of m linear polynomials in R which are all mutually similar to each other, $\mathrm{Nuc}_r(S_f)$ is a central simple algebra over $E_{\hat{h}}$ of degree ms, and s divides d. We obtain the following result as a Corollary to Theorem 20:

Corollary 22. *Suppose that* $(f,t)_r = 1$, *that* $\gcd(m,n) = 1$ *and that* $\hat{h}$ *is irreducible in* $F[x]$. *Then* s *divides* d, *and* f *is not right-invariant unless* $n = 1$ *and* $s = d$. *Additionally, if we suppose that* d *is prime, then one of the following holds:*

(1) f *is irreducible and* $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ *is a field extension of* F *of degree* md.

(2) f *is irreducible and* $\mathrm{Nuc}_r(S_f)$ *is a central division algebra over* $E_{\hat{h}}$ *of degree* d, $\deg(\hat{h}) = m$, *and* $[\mathrm{Nuc}_r(S_f) : F] = d^2m$.

(3) f *is the product of* d *irreducible polynomials in* R *of degree* $\frac{m}{d}$, *all of which are mutually similar to each other. Moreover*

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

is a central simple algebra over $E_{\hat{h}}$ *of degree* d, $\deg(\hat{h}) = m$, *and* $[\mathrm{Nuc}_r(S_f) : F] = d^2m$.

Proof. Since $\gcd(dm, dn) = \gcd(m,n)d = d$, s divides d by Theorem 20. Moreover, f is right-invariant if and only if $[S_f : F] = [\mathrm{Nuc}_r(S_f) : F]$, i.e. if and only $d^2mn = dms$. This yields $s = d$ and $n = 1$ since $s \leq d$.
Now suppose additionally that d is prime. Then s dividing d means that $s = 1$ or $s = d$. If $s = 1$, then $\deg(h) = mnd$ and we obtain (1) by Proposition 16.
On the other hand if $s = d$, then there are two possible scenarios; either $l = 1$ in which case f satisfies (2), or $l = d$ in which case we obtain case (3), both following Theorem 20. □

Note that in Corollary 22, if d does not divide m (e.g. if d is greater than m), then (3) cannot occur. Also if $n = 1$ and f is not right-invariant, then f must satisfy (1).

Now we consider some certain special cases of Theorems 19 and 20.

What if σ is an inner automorphism?

Suppose now that $\sigma = \iota_u$ for some $u \in D^\times$ (i.e. σ has finite inner order $n = 1$). Then we have that $C \subseteq \mathrm{Fix}(\sigma)$, i.e. $F = C \cap \mathrm{Fix}(\sigma) = C$, and

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

under the map which fixes elements of C and sends $u^{-1}t$ to x. Then f has minimal central left multiple $h(t) = \hat{h}(t^n)$ for some $\hat{h} \in C[x]$. We obtain the following results as Corollaries to Theorem 19:

Corollary 23. *Let f be irreducible. Then:*
(i) $\mathrm{Nuc}_r(S_f)$ *is a central division algebra over* $E_{\hat{h}} = C[x]/(\hat{h}(x))$ *of degree* $s = d/k$*, where k is the number of irreducible factors of h in R, and*

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

This means that $\deg(\hat{h}) = \frac{md}{s}$, $\deg(h) = \frac{md}{s}$, *s divides d and*

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

(ii) If d is prime and f not right-invariant, then

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

is a field extension and $[\mathrm{Nuc}_r(S_f) : C] = md$, $\deg(\hat{h}) = md$, *and* $\deg(h) = md$.

Proof. (i) We note that

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

and that $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}}$ of dimension s^2 by an identical proof of Theorem 19. Now comparing the dimensions of R/Rh and $M_k(\mathrm{Nuc}_r(S_f))$ over F it follows that $d^2 \deg(h) = d^2 \deg(\hat{h}) = k^2 s^2 \deg(\hat{h})$, so that we get $d^2 = k^2 s^2$, that is $d = ks$. In particular, this implies that $\deg(h) = \deg(\hat{h}) = \frac{md}{s}$.
(ii) If d is prime and f not right-invariant, then in the above proof $d = ks$ forces $s = 1$, so that here $R/Rh \cong M_k(E_{\hat{h}})$, $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ and $\deg(h) = \deg(\hat{h}) = md$. □

Corollary 24. *Let $d = pq$ for p and q prime, and f be irreducible and not right-invariant. Then $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ is a field extension of C of degree md, or $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}}$ of degree q (resp., p), and $[\mathrm{Nuc}_r(S_f) : C] = mdq^2$ (resp., $= mdp^2$).*

Proof. (i) Since f is not right-invariant, we note that $k > 1$. If $d = pq$ then the equation $d = ks$ in the proof of Corollary 23 (i) forces either that $s = 1$ and $k = d$, hence that $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$, or that $s \neq 1$ and then w.l.o.g. that $k = p$ and $s = q$, so that here $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}}$ of degree q, $\deg(h) = \deg(\hat{h}) = mp$, and $[\mathrm{Nuc}_r(S_f) : C] = mds = mpq^2$. □

This observation generalizes as follows by induction:

Corollary 25. *Let $d = p_1 \cdots p_l$ be the prime decomposition of d, and f be irreducible and not right-invariant. Then $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ is a field extension of C of degree md, or $\mathrm{Nuc}_r(S_f)$ is a central division algebra*

over $E_{\hat{h}}$ *of degree* $q = q_1 \cdots q_r$, *with* $q_i \in \{p_1, \ldots, p_l\}$, *and*

$$[\mathrm{Nuc}_r(S_f) : C] = mpq^2,$$

where $p = \frac{d}{q_1 \cdots q_r} = \frac{d}{q}$.

Again, we next turn our attention to the more general setting that $f \in R$ is reducible polynomial of degree $m > 1$ such that $(f,t)_r = 1$ with minimal central left multiple $h(t) = \hat{h}(u^{-1}t^n)$ for some monic, irreducible polynomial $\hat{h}(x) \in C[x]$. The following results are Corollaries to Theorem 20.

Corollary 26. *The polynomial* f *is the product of* $l \geq 1$ *irreducible polynomials in* R *all of which are mutually similar to each other, and*

$$R/Rh \cong M_k(\mathcal{E}(g))$$

where $g \in R$ *is any irreducible divisor of* h *in* R.

(i) Suppose that $\deg(g) = r \geq 1$. *Then* $m = rl$, $\mathcal{E}(g)$ *is a central division algebra over* $E_{\hat{h}} = C[x]/(\hat{h}(x))$ *of degree* $s' = d/k$, *where* k *is the number of irreducible factors of* h, *and*

$$\mathrm{Nuc}_r(S_f) \cong M_l(\mathcal{E}(g)).$$

In particular, $\mathrm{Nuc}_r(S_f)$ *is a central simple algebra over* $E_{\hat{h}}$ *of degree* $s = ls'$, $\deg(\hat{h}) = \frac{rd}{s'} = \frac{md}{s}$, $\deg(h) = \frac{rd}{s'} = \frac{md}{s}$, *and*

$$[\mathrm{Nuc}_r(S_f) : C] = l^2 rds' = mds.$$

In particular l, s' *and* s *all divide* d, *and* l *divides* k.

(ii) If $\gcd(d,m) = 1$*, then* f *is irreducible, and* $\mathrm{Nuc}_r(S_f)$ *is a central division algebra over* $E_{\hat{h}}$ *of degree* $s = d/k$*, and* $\deg(\hat{h}) = \deg(h) = \frac{md}{s}$.

(iii) If d *is prime, and* f *is not right-invariant, then* f *is irreducible and*

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

is a field extension of F *of degree* md.

In Corollary 26 (i), if $\deg(g) = 1$, then f is the product of m linear polynomials in R which are all mutually similar to each other, and $\mathrm{Nuc}_r(S_f)$ is a central simple algebra over $E_{\hat{h}}$ of degree md/k.

What if D is a field?

Now suppose that $D = K$ for K a cyclic Galois field extension of $F = \mathrm{Fix}(\sigma)$ of degree n with Galois group $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Then σ has order n, and $R = K[t;\sigma]$ has center

$$C(R) = F[t^n]$$

which is isomorphic to $F[x]$ under the map which fixes elements of F and sends t^n to x. Also f has minimal central left multiple $h(t) = \hat{h}(t^n)$ for $\hat{h} \in F[x]$. We obtain the following results as corollaries to Theorem 19:

Theorem 27. *Let* f *be irreducible, then:*
(i) $\mathrm{Nuc}_r(S_f)$ *is a central division algebra over* $E_{\hat{h}} = F[x]/(\hat{h}(x))$ *of degree* $s = n/k$*, where* k *is the number of irreducible factors of* h*, and*

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

In particular, this means that $\deg(\hat{h}) = \frac{m}{s}$, $\deg(h) = \frac{nm}{s}$, *and*

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

Moreover, s *divides* m *and* n.

(ii) If $\gcd(m,n) = 1$, *or* n *is prime and* f *not right-invariant, then*

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

In particular, then $[\mathrm{Nuc}_r(S_f) : F] = m$, $\deg(\hat{h}) = m$, *and* $\deg(h) = mn$.

Proof. (i) We note that

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

and that $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}}$ of dimension s^2 by an identical proof of Theorem 19. Now comparing the dimensions of R/Rh and $M_k(\mathrm{Nuc}_r(S_f))$ over F it follows that $n\deg(h) = n^2\deg(\hat{h}) = k^2s^2\deg(\hat{h})$, so that we get $n^2 = k^2s^2$, that is $n = ks$. In particular, this implies that $\deg(h) = nm/s$ and $\deg(\hat{h}) = \frac{m}{s}$.
(ii) If n is prime then in the above proof $n = ks$ forces $s = 1$, so that here $R/Rh \cong M_k(E_{\hat{h}})$, $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ and $\deg(h) = mn$. □

Remark. *As a byproduct of Theorem 27, we obtain [LS13, Lemma 4]. This is due to the fact that* $E_{\hat{h}}$ *in the proof of (i) is a finite extension of the field* F, *and so for* $F = \mathbb{F}_q$ *a finite base field, the only central division algebra over* $E_{\hat{h}}$ *is itself, i.e.* $s = 1$. *In this case* $[\mathrm{Nuc}_r(S_f) : \mathbb{F}_q] = m$, *hence* $|\mathrm{Nuc}_r(S_f)| = q^m$.

Corollary 28. *Let* $n = pq$ *for* p *and* q *prime. Let* f *be irreducible and not right-invariant.*

(i) $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ *is a field extension of* F *of degree* m, *or* $\mathrm{Nuc}_r(S_f)$ *is a*

central division algebra over $E_{\hat{h}}$ of prime degree q (resp., p), $[\mathrm{Nuc}_r(S_f) : F] = qm$ (resp., $= pm$), and q (resp., p) divides m.
(ii) If $\gcd(m,n) = 1$, then $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ is a field extension of F of degree m.

This observation generalizes as follows by induction:

Corollary 29. *Let f be irreducible and not right-invariant.*
(i) $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ is a field extension of F of degree m, or $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}}$ of degree $q_1 \cdots q_r$, with $q_i \in \{p_1, \ldots, p_l\}$, $[\mathrm{Nuc}_r(S_f) : F] = q_1 \cdots q_r m$, and $q_1 \cdots q_r$ divides m.
(ii) If $\gcd(m,n) = 1$ (i.e., m is not divisible by any set of prime factors of n), then $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ is a field extension of F of degree m.

Corollary 30. *Let f be irreducible. Suppose that m is prime. Then f is not right-invariant and one of the following holds:*
(i) $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$, $[\mathrm{Nuc}_r(S_f) : F] = m$, and $\deg(h) = mn$.
(ii) $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $F = E_{\hat{h}}$ of prime degree m, $[\mathrm{Nuc}_r(S_f) : F] = m^2$, and m divides n. This case occurs when $\hat{h}(x) = x - a \in F[x]$, i.e. when $h(t) = t^n - a$.

We therefore found examples of polynomials $f \in R$ whose eigenspace is a central simple algebra over F. Thus for any splitting field L of $\mathrm{Nuc}_r(S_f)$ of degree m, the polynomial f in case (ii) of Theorem 27 will be reducible in $L[t;\sigma]$.

Corollary 31. *Suppose that n is prime or that $\gcd(m,n) = 1$, and let $f \in F[t] \subset K[t;\sigma]$ be irreducible and not right-invariant. Then $\mathrm{Nuc}_r(S_f) \cong F[t]/(f(t))$.*

Proof. If f is irreducible in $K[t;\sigma]$, then $F[t]/(f(t))$ is a subfield of the right nucleus of degree m [BP18, Proposition 2], hence must be all of the right nucleus, since that has dimension m due to our assumptions (Theorem 27 (ii), Corollary 29 (ii)). □

Theorem 32. *Suppose that $\hat{h}(x)$ is irreducible in $F[x]$. Then:*

(i) f is the product of $l \geq 1$ irreducible polynomials in R all of which are mutually similar to each other, and

$$R/Rh \cong M_k(\mathcal{E}(g))$$

where $g \in R$ is any irreducible divisor of h in R. If $\deg(g) = r \geq 1$, then $m = rl$, $\mathcal{E}(g)$ is a central division algebra over $E_{\hat{h}} = F[x]/(\hat{h}(x))$ of degree $s' = n/k$, where k is the number of irreducible factors of h, and

$$\mathrm{Nuc}_r(S_f) \cong M_l(\mathcal{E}(g)).$$

In particular, $\mathrm{Nuc}_r(S_f)$ is a central simple algebra over $E_{\hat{h}}$ of degree $s = ls'$, $\deg(\hat{h}) = \frac{r}{s'} = \frac{m}{s}$, $\deg(h) = \frac{rn}{s'} = \frac{mn}{s}$, and

$$[\mathrm{Nuc}_r(S_f) : F] = l^2 r s' = ms.$$

In particular s' divides $\gcd(r,n)$, s divides $\gcd(m,n)$ and l divides $\gcd(m,n)$.

(ii) If m is prime, then one of the following holds:

(a) $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ is a field extension of F of prime degree m,

(b) $\mathrm{Nuc}_r(S_f)$ is a central division algebra over F of prime degree m,

(c) $\mathrm{Nuc}_r(S_f) \cong M_m(F)$ is a central simple algebra over F of prime degree m.

(iii) If $\gcd(m,n) = 1$, or n is prime and f not right-invariant, then f is irreducible and

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

is a field extension of F of degree $\deg(\hat{h}) = m$, and $\deg(h) = mn$.

Proof. This result corresponds to the special case that $d = 1$ in Theorem 20, and the corollaries that follow it. □

Remark. *Let K/F be a cyclic Galois extension of degree n with Galois group $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ and let $f \in R$ be monic. If $(f,t)_r = 1$, then the minimal central left multiple of f is equal to the minimal polynomial of the matrix $A_f = C_f C_f^{\sigma} \cdots C_f^{\sigma^{n-1}}$ over F, where C_f is the companion matrix of f [She18, Section 3.4].*

Chapter 3

The Eigenring of $f \in D[t;\delta]$

Let D be a central division algebra of finite degree d over its center C. We now investigate the dimension of the right nucleus of S_f for $f \in R = D[t;\delta]$ monic of degree m. Similarly to Chapter 2, if $f(t) = t - a$ for some $a \in D$, then it can be easily seen that $\mathrm{Nuc}_r(S_f) = D$ as the F-algebra S_f is equal to the associative ring D. Moreover, for any $b \in D$, $fb \in Rf$ if and only if $\delta(b) = ab - ba$. Therefore the eigenring $\mathcal{E}(f)$ is equal to $\{b \in D : \delta(b) = [a, b]\}$. Hence for the rest of the chapter, unless explicitly stated otherwise, we assume that $m > 1$. Since the center of R depends on the characteristic of D, we split our investigation into the cases $\mathrm{Char}(C) = 0$, and $\mathrm{Char}(C) = p$ prime.

3.1 Zero Characteristic

In the following, let $\mathrm{Char}(D) = 0$. Let δ be a derivation of D, and recall that $F = C \cap \mathrm{Const}(\delta)$. Recall that δ is said to be an inner derivation of D if there exists $c \in D$ such that $\delta(a) = [c, a] = ca - ac$ for all $a \in D$, otherwise it is called an outer derivation of D. If δ is an outer derivation, then $R = D[t;\delta]$ is a simple ring and $\mathrm{C}(R) = F$ (Amitsur, cf. [Jac09, Theorem 1.1.32]). In this case there are no non-constant

bounded polynomials in R. Henceforth we assume that $\delta = \delta_c$ is the inner derivation of D defined by $\delta(a) = ca - ac$ for $c \in D^\times$. Note that here $\mathrm{Const}(\delta) = \mathrm{Cent}_D(c)$ is the centraliser of c in D, since $\delta_c(a) = 0$ if and only if $ca = ac$. Since $C \subseteq \mathrm{Cent}_D(c)$, we have $F = C \cap \mathrm{Const}(\delta) = C$. Every polynomial in $R = D[t;\delta]$ is bounded (Corollary 7). Again, we define the *minimal central left multiple* of a polynomial $f \in R$ to be the monic polynomial $h(t) = \hat{h}(t-c)$ for some $\hat{h} \in F[x]$ of minimal degree, such that $h = gf$ for some $g \in R$.

Every polynomial f in R has a unique minimal central left multiple $h(t)$, and for any bound f^* of f, $h(t) = af^*$ for some nonzero scalar a in $D^\times$. We note that $f^* \in C(R)$ for all $f \in R$ by [Jac09, Theorem 1.1.32], and so we need not assume that $(f,t)_r = 1$ as in the case $R = D[t;\sigma]$.

Lemma 33. *Let $f \in R$ have degree $m \geq 1$. Then the following are satisfied.*

(i) Every $f \in R = D[t;\delta]$ has a unique minimal central left multiple, which is a bound of f.

(ii) [Jac43, Theorem 13] If f is irreducible in R, then $\hat{h}$ is irreducible in $F[x]$.

(iii) [Jac09] The quotient algebra R/Rh has center

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

(iv) Suppose that $\hat{h}$ is irreducible in $F[x]$.

(a) [Jac43, Theorem 13] h generates a maximal two sided ideal in R.

(b) *All irreducible factors of f are similar to all irreducible factors of h in R. In particular, all irreducible factors of f are mutually similar to each other.*

Proof. (i) follows directly from Theorem 10, and (ii), (iii), (iv)(a), and (iv)(b) follow from identical arguments to those of Lemmas 15, 14, 18, and 17, respectively. □

Define $E_{\hat{h}} = F[x]/(\hat{h}(x))$. This is a commutative algebra over F of dimension $\deg(\hat{h})$. If $\hat{h}$ is irreducible in $F[x]$, then $E_{\hat{h}}$ is a field extension of F of degree equal to the degree of $\hat{h}$ in $F[x]$. Gomez-Torrecillas et al. show that the converse of Lemma 33 (ii) holds when h achieves the maximum possible degree mnd:

Proposition 34. *[GTLN13, Proposition 4.1] Let f have degree $m \geq 1$. If $\deg(h) = md$ and $\hat{h}$ is irreducible in $F[x]$, then f is irreducible and $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$.*

Again, we first consider the case that f is irreducible in R, which is a sufficient condition for $\hat{h}$ to be irreducible in $F[x]$ by Lemma 33 (ii). We show that $\mathrm{Nuc}_r(S_f)$ is a central division algebra of degree $s = d/k$ over a field extension $E_{\hat{h}}$ of F determined by h, where k is the number of irreducible factors in any complete factorisation of h in R.

After we have explored some special cases, we loosen the restriction that f is irreducible in R, instead assuming only that $\hat{h}$ is irreducible in $F[x]$. We note that this setting includes the previous one that f is irreducible as a special case. We obtain that $\mathrm{Nuc}_r(S_f)$ is a central simple algebra of degree $s = ldn/k$ over the same field extension $E_{\hat{h}}$ of F, with k as above, and l the number of irreducible factors in any complete factorisation of f in R.

Theorem 35. *Let f be irreducible.*
(i) $\mathrm{Nuc}_r(S_f)$ *is a central division algebra over* $E_{\hat{h}} = F[x]/(\hat{h}(x))$ *of degree* $s = d/k$*, where* k *is the number of irreducible factors of* h *in* R*, and*

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

In particular, this means that $\deg(\hat{h}) = \frac{md}{s}$, $\deg(h) = \frac{md}{s}$*, and*

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

Moreover, s *divides* d*.*
(ii) If d *is prime and* f *not right-invariant, then*

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

In particular, then $[\mathrm{Nuc}_r(S_f) : F] = md$*,* $\deg(\hat{h}) = md$*, and* $\deg(h) = md$*.*

Proof. (i) The first part of the proof of (i) may be taken verbatim to be the first part of the proof of Theorem 19. Comparing the dimensions of R/Rh and $M_k(\mathrm{Nuc}_r(S_f))$ over F it follows that $d^2 \deg(h) = d^2 \deg(\hat{h}) = k^2 s^2 \deg(\hat{h})$, so that we get $d^2 = k^2 s^2$, that is $d = ks$. In particular, this implies that $\deg(h) = \frac{dm}{s}$ and $\deg(\hat{h}) = \frac{dm}{s}$. Moreover

$$[\mathrm{Nuc}_r(S_f) : F] = [\mathrm{Nuc}_r(S_f) : E_{\hat{h}}][E_{\hat{h}} : F] = s^2 \deg(\hat{h}) = \frac{dms^2}{s} = dms.$$

Now since $\mathrm{Nuc}_r(S_f)$ is a subalgebra of S_f we have

$$[S_f : F] = [S_f : \mathrm{Nuc}_r(S_f)][\mathrm{Nuc}_r(S_f) : F] = d^2 m. \tag{3.1}$$

Substituting $d = ks$ and $[\mathrm{Nuc}_r(S_f) : F] = dms$ into Equation (3.2) we

obtain the equality $[S_f : \mathrm{Nuc}_r(S_f)] = k$. If f is not right-invariant, then $k > 1$ and so we derive $s \neq d$ looking at the degree of h. More precisely, for f of degree $m > 1$, f being not right-invariant is equivalent to S_f being not associative which in turn is equivalent to $k > 1$.
(ii) If d is prime then $d = ks$ forces $s = 1$, as $k = 1$ implies that f is right-invariant, so that here $R/Rh \cong M_k(E_{\hat{h}})$, $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ and $\deg(h) = md$. □

Corollary 36. *Let $d = pq$ for primes p and q and suppose that f is irreducible and not right-invariant. Then $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ is a field extension of C of degree md, or $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}}$ of degree q (resp. p), and*

$$[\mathrm{Nuc}_r(S_f) : C] = mpq^2 \ (resp.\, mqp^2).$$

Proof. If $s = 1$, then $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ is a field extension of C of degree md. Suppose that $s \neq 1$. Since s divides $d = pq$, we have w.l.o.g. $s = q$. Then $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}}$ of degree q, and

$$[\mathrm{Nuc}_r(S_f) : C] = mds = mpq^2.$$

□

Corollary 36 generalises by induction as follows:

Corollary 37. *Let $d = p_1 \cdots p_l$ be the prime decomposition of n and suppose that f is irreducible and not right-invariant. Then $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ is a field extension of C of degree md, or $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}}$ of degree $q = p_1 \cdots p_r$, where $r < l$, and if $p = \frac{d}{q} = p_{r+1} \cdots p_l$, then*

$$[\mathrm{Nuc}_r(S_f) : C] = mpq^2.$$

Theorem 38. *(i) Suppose that $\hat{h}(x)$ is irreducible in $F[x]$. Then f is the product of $l \geq 1$ irreducible polynomials in R all of which are mutually similar to each other, and*

$$R/Rh \cong M_k(\mathcal{E}(g))$$

where $g \in R$ is any irreducible divisor of h in R. If $\deg(g) = r \geq 1$, then $m = rl$, $\mathcal{E}(g)$ is a central division algebra over $E_{\hat{h}} = F[x]/(\hat{h}(x))$ of degree $s' = d/k$, where k is the number of irreducible factors of h, and

$$\mathrm{Nuc}_r(S_f) \cong M_l(\mathcal{E}(g)).$$

In particular, $\mathrm{Nuc}_r(S_f)$ is a central simple algebra over $E_{\hat{h}}$ of degree $s = ls'$, $\deg(\hat{h}) = \frac{rd}{s'} = \frac{md}{s}$, $\deg(h) = \frac{rd}{s'} = \frac{md}{s}$, and

$$[\mathrm{Nuc}_r(S_f) : F] = l^2 rds' = mds.$$

In particular s', s, and l divide d.
(ii) If d is prime and f not right-invariant, then

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

In particular, then $[\mathrm{Nuc}_r(S_f) : F] = md$, $\deg(\hat{h}) = md$, and $\deg(h) = md$.

Proof. (i) Once again, we can take the first part of the proof (i) verbatim from the proof of Theorem 20. Now since g is irreducible of degree r with minimal central left multiple $h(t) = \hat{h}(u^{-1}t^n)$, $\mathcal{E}(g)$ is a central division algebra over $E_{\hat{h}}$ of degree $s' = d/k$, where k is the number of irreducible divisors of h in R, $\deg(\hat{h}) = \frac{rd}{s'} = \frac{md}{ls'}$ and $\deg(h) = \frac{rd}{s'} = \frac{md}{ls'}$

by Theorem 19. Finally, since

$$\mathcal{E}(f) \cong M_l(\mathcal{E}(g)),$$

$\mathcal{E}(f)$ is a central simple algebra over $E_{\hat{h}}$ of degree $s = ls'$, and

$$[\mathcal{E}(f) : F] = s^2 \deg(\hat{h}) = mds.$$

(ii) Suppose that d is prime and f not right-invariant. As s divides d, we are forced to take $s = 1$ (else $s = d$ and $[\mathrm{Nuc}_r(S_f) : F] = d^2 m$, i.e. f is right-invariant). The result follows immediately. □

3.2 Prime Characteristic

In this section, let $\mathrm{Char}(C) = p > 0$. Let δ be a derivation of D, such that $\delta|_C$ is algebraic with minimum polynomial

$$g(t) = t^{p^e} + \gamma_1 t^{p^{e-1}} + \gamma_2 t^{p^{e-2}} + \cdots + \gamma_{e-1} t^p + \gamma_e t \in F[t],$$

such that $g(\delta) = \delta_c$ is the inner derivation defined by $c \in D^\times$. Then we have $[C : F] = p^e$ for $F = C \cap \mathrm{Const}(\delta)$. Then R has dimension $d^2 p^e$ over F and every polynomial in R is bounded (Corollary 7). Recall that the two-sided elements of R are the elements $uq(t)$ where $u \in D$ and $q(t) \in C(R)$, and $C(R) = F[g(t) - c]$, which is isomorphic to $F[x]$ under the map fixing elements of F and sending $g(t) - c$ to x [Jac09, Theorem 1.1.32]. Again we define the *minimal central left multiple* of a polynomial $f \in R$ to be the monic polynomial $h(t) = \hat{h}(g(t) - c)$ for some $\hat{h} \in F[x]$ of minimal degree, such that $h = gf$ for some $g \in R$.

Lemma 39. *(i) f has a unique minimal central left multiple, which is*

a bound of f.

(ii) [Jac43, Theorem 13] If f is irreducible, then $\hat{h}$ is irreducible in $F[x]$.

(iii) [Jac09] The quotient algebra R/Rh has center

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

(iv) Suppose that $\hat{h}$ is irreducible in $F[x]$.

(a) [Jac43, Theorem 13] h generates a maximal two sided ideal in R.

(b) All irreducible factors of f are similar to all irreducible factors of h in R. In particular, all irreducible factors of f are mutually similar to each other.

Proof. This is identical to the proof of Lemma 33. □

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

Theorem 40. *Let f be irreducible. Then $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}} = F[x]/(\hat{h}(x))$ of degree $s = dp^e/k$, where k is the number of irreducible factors of h in R, and*

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

In particular, this means that $\deg(\hat{h}) = \frac{md}{s}$, $\deg(h) = \frac{mdp^e}{s}$, and

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

Moreover, s divides $\gcd(dm, dp^e)$.

Proof. The first part of this proof can be taken verbatim to be the first part of the proof of Theorem 19. Comparing the dimensions of R/Rh and $M_k(\mathrm{Nuc}_r(S_f))$ over F it follows that $d^2p^e \deg(h) = d^2p^{2e} \deg(\hat{h}) = k^2s^2 \deg(\hat{h})$, so that we get $d^2p^{2e} = k^2s^2$, that is $dp^e = ks$. In particular, this implies that $\deg(h) = \frac{dmp^e}{s}$ and $\deg(\hat{h}) = \frac{dm}{s}$. Moreover

$$[\mathrm{Nuc}_r(S_f) : F] = [\mathrm{Nuc}_r(S_f) : E_{\hat{h}}][E_{\hat{h}} : F] = s^2 \deg(\hat{h}) = \frac{dms^2}{s} = dms.$$

Now since $\mathrm{Nuc}_r(S_f)$ is a subalgebra of S_f we have

$$[S_f : F] = [S_f : \mathrm{Nuc}_r(S_f)][\mathrm{Nuc}_r(S_f) : F] = d^2mp^e. \tag{3.2}$$

Substituting $dp^e = ks$ and $[\mathrm{Nuc}_r(S_f) : F] = dms$ into Equation (3.2) we obtain the equality $[S_f : \mathrm{Nuc}_r(S_f)] = k$. If f is not right-invariant, then $k > 1$ and so we derive $s \neq dp^e$ looking at the degree of h. More precisely, for f of degree $m > 1$, f being not right-invariant is equivalent to S_f being not associative which in turn is equivalent to $k > 1$. □

Corollary 41. *Let f be irreducible. If $\gcd(m, p^e) = 1$, then s divides d, and f is not right-invariant. Additionally, if d is prime, then one of the following holds:*

(i) $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ *is a field extension of F of degree md.*

(ii) $\mathrm{Nuc}_r(S_f)$ *is a central division algebra over $E_{\hat{h}}$ of degree d,* $\deg(h) = mp^e$, $\deg(h) = m$, *and* $[\mathrm{Nuc}_r(S_f) : F] = md^2$.

Proof. Since $\gcd(m, p^e) = 1$, $\gcd(dm, dp^e) = d$. Hence s divides d by Theorem 40, and we have

$$[\mathrm{Nuc}_r(S_f) : F] = mds \leq md^2 < md^2p^e = [S_f : F],$$

i.e. f is not right-invariant. Additionally, if we suppose that d is prime,

then s dividing d implies that $s = 1$ or $s = d$. (i) follows by considering $s = 1$ and (ii) follows from $s = d$. □

The following result partially answers a question by Amitsur, who asked when the right nucleus of a polynomial is a central simple algebra.

Theorem 42. *Suppose that* $\gcd(d, p^e) = 1$ *and that* f *is not right-invariant. Then* $s = 1$*, or* $s \neq 1$ *and* s *divides either* d *or* p^e*.*
Suppose additionally that d *is prime and* $e = 1$*. Then one of the following holds:*
(i) $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$*,* $dp = k$*,* $\deg(\hat{h}) = dm$ *and* $\deg(h) = dpm$*. In particular, then* $[\mathrm{Nuc}_r(S_f) : F] = dm$*.*
(ii) $\mathrm{Nuc}_r(S_f)$ *is a central division algebra over* $E_{\hat{h}}$ *of degree* d*,* p *is the number of irreducible factors of* h *in* R*,* $\deg(h) = pm$*,* $\deg(\hat{h}) = m$ *and*

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

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

Proof. It is clear that $s = 1$, or else $s \neq 1$ and s divides either d or p^e. Suppose additionally that d is prime, $e = 1$. Then the equation $dp = ks$ forces that either $s = 1$ and $k = pd$, or that $s \neq 1$ and then $d = k$ and $p = s$ (or resp., $d = s$ and $p = k$). As before, $s = 1$ yields (i).
If $d = s \neq 1$ and $p = k$ then this implies (ii) employing that $[\mathrm{Nuc}_r(S_f) : F] = [\mathrm{Nuc}_r(S_f) : E_{\hat{h}}][E_{\hat{h}} : F] = d^2\deg(\hat{h}) = d^2m$.
If $d = k$ and $p = s \neq 1$ then this implies (iii) using that $[\mathrm{Nuc}_r(S_f) :$

$F] = [\mathrm{Nuc}_r(S_f) : E_{\hat{h}}][E_{\hat{h}} : F] = p^2\deg(\hat{h}) = p^2/dm$. In particular, this case means that $\deg(\hat{h}) = dm/p$, which forces n to divide dm, as well as $[\mathrm{Nuc}_r(S_f) : F] = p^2/dm$ which in turn forces dm to divide n^2. □

Theorem 43. *Suppose that $\hat{h}$ is irreducible in $F[x]$. Then f is the product of $l \geq 1$ irreducible polynomials in R all of which are mutually similar to each other, and*

$$R/Rh \cong M_k(\mathcal{E}(g))$$

where $g \in R$ is any irreducible divisor of h in R. If $\deg(g) = r \geq 1$, then $m = rl$, $\mathcal{E}(g)$ is a central division algebra over $E_{\hat{h}} = F[x]/(\hat{h}(x))$ of degree $s' = dp^e/k$, where k is the number of irreducible factors of h, and

$$\mathrm{Nuc}_r(S_f) \cong M_l(\mathcal{E}(g)).$$

In particular, $\mathrm{Nuc}_r(S_f)$ is a central simple algebra over $E_{\hat{h}}$ of degree $s = ls'$, $\deg(\hat{h}) = \frac{rd}{s'} = \frac{md}{s}$, $\deg(h) = \frac{rdp^e}{s'} = \frac{mdp^e}{s}$, and

$$[\mathrm{Nuc}_r(S_f) : F] = l^2rds' = mds.$$

In particular s', s, and l divide $\gcd(dp^e, dm)$.

Proof. The first part of this proof is identical to the first part of the proof of Theorem 20. Now since g is irreducible of degree r with minimal central left multiple $h(t) = \hat{h}(u^{-1}t^n)$, $\mathcal{E}(g)$ is a central division algebra over $E_{\hat{h}}$ of degree $s' = dp^e/k$, where k is the number of irreducible divisors of h in R, $\deg(\hat{h}) = \frac{rd}{s'} = \frac{md}{ls'}$ and $\deg(h) = \frac{rdp^e}{s'} = \frac{mdp^e}{ls'}$ by Theorem 19. Finally, since

$$\mathcal{E}(f) \cong M_l(\mathcal{E}(g)),$$

$\mathcal{E}(f)$ is a central simple algebra over $E_{\hat{h}}$ of degree $s = ls'$, and

$$[\mathcal{E}(f) : F] = s^2 \deg(\hat{h}) = mds.$$

□

Corollary 44. *Let $f \in R$ be reducible (i.e. $l \geq 2$) and suppose that $\hat{h}(x)$ is irreducible in $F[x]$. If $\gcd(m, p^e) = 1$ (i.e. p does not divide m), then s divides d. If d is prime and not equal to p, then f is not right-invariant and has d irreducible factors in any factorisation into irreducible polynomials in R, each of which has degree $r = m/d$. Moreover*

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

is a central simple algebra over $E_{\hat{h}}$ of degree d, $\deg(\hat{h}) = m$, $\deg(h) = mp^e$, and $[\mathrm{Nuc}_r(S_f) : F] = md^2$.

Proof. Suppose that d is a prime not equal to p. Since l divides d by Theorem 43, we are forced to take $l = d$. Also by Theorem 43, $s = ds'$ divides d, and we are forced to take $s' = 1$ and $s = d$. Therefore f is not right-invariant, as $[\mathrm{Nuc}_r(S_f) : F] = md^2 < [S_f : F]$, and the rest follows immediately from Theorem 43 by applying $s = d$.

□

Proposition 45. *Suppose that $\hat{h}$ is irreducible in $F[x]$. If d divides p and $\gcd(m, p^e) = 1$, then f is irreducible.*

Proof. First we note that l divides $\gcd(dm, dp^e)$ in the notation of Theorem 42. Since $\gcd(m, p^e) = 1$ by assumption, we must have that l divides d, and so l must also divide the prime p. Hence $l = 1$ or $l = p$. Suppose that $l = p$, then p divides m (since l divides m by Theorem 42), which contradicts our assumption that $\gcd(m, p^e) = 1$. We conclude that l must be equal to 1, i.e. that f is irreducible. □

What if $D = K$ is a Field of Prime Characteristic?

Let K be a field with $\mathrm{Char}(K) = p > 0$. Let δ be an algebraic derivation of K with minimum polynomial

$$g(t) = t^{p^e} + \gamma_1 t^{p^{e-1}} + \gamma_2 t^{p^{e-2}} + \cdots + \gamma_{e-1} t^p + \gamma_e t \in F[t]$$

such that $g(\delta) = 0$ where $F = \mathrm{Const}(\delta)$. If $R = K[t; \delta]$ then

$$C(R) = F[g(t)] \cong F[x].$$

We note that in this setting the results Lemma 39 through to Corollary 44 hold analogously, with $D = K$, $g(\delta) = 0$, and $d = 1$. Note that

$$S_f = K[t; \delta]/K[t; \delta]f(t)$$

is a nonassociative algebra over F of dimension mp^e. In this setting f has minimal central left multiple $h(t) = \hat{h}(g(t))$ for some $\hat{h} \in F[x]$.

Theorem 46. *Let f be irreducible. Then $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}} = F[x]/(\hat{h}(x))$ of degree $s = p^e/k$, where k is the number of irreducible factors of h in R, and*

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

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

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

Moreover, s divides $\gcd(m, p^e)$ and $s = p^\epsilon$ for some $\epsilon \in \mathbb{Z}$, with $0 \leq \epsilon \leq e$.

Proof. We refer to the proof of Theorem 40 for

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

since it is identical to the proof in this case, too. We note that h has degree km, and since f is irreducible, $\mathrm{Nuc}_r(S_f)$ is a division algebra. Now R/Rh is a central simple algebra over $E_{\hat{h}}$ and so $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}}$ of dimension s^2. Comparing the dimensions of R/Rh and $M_k(\mathrm{Nuc}_r(S_f))$ over F it follows that $p^e \deg(h) = p^{2e} \deg(\hat{h}) = k^2 s^2 \deg(\hat{h})$, so that we get $p^{2e} = k^2 s^2$, that is $p^e = ks$. In particular, this implies that $\deg(h) = \frac{mp^e}{s}$ and $\deg(\hat{h}) = \frac{m}{s}$. □

Corollary 47. *Let f be irreducible of prime degree m. Then* $\mathrm{Nuc}_r(S_f)$ *a field extension of F of degree m, or $E_{\hat{h}} = F$ and* $\mathrm{Nuc}_r(S_f)$ *is a central division algebra over F of degree p, and* $\deg(\hat{h}) = 1$.

Proof. By Theorem 46, s divides m, and since m is prime we must have $s = 1$ or $s = m$. Suppose first that $s = 1$, then $\mathrm{Nuc}_r(S_f)$ is a central divsion algebra over $E_{\hat{h}}$ of degree 1, i.e. $\mathrm{Nuc}_r(S_f) = E_{\hat{h}}$, a field extension over F of degree $\deg(\hat{h}) = \frac{m}{s} = m$.
Now suppose that $s = m$, then $\deg(\hat{h}) = \frac{m}{s} = 1$ and $E_{\hat{h}} = F$. Hence $\mathrm{Nuc}_r(S_f)$ is a central division algebra over F of degree m. Moreover, $m = s = \frac{p^e}{k}$, so that m divides p^e, and since m is prime $m = p$. □

Corollary 48. *Suppose that δ has minimum polynomial $g(t) = t^p - \gamma t \in F[t]$ (i.e. $e = 1$) If f is irreducible and not right-invariant, then* $\mathrm{Nuc}_r(S_f)$ *is a field extension of F of degree m.*

Proof. Since p is prime and f not right-invariant, by Theorem 46 we are forced to take $s = 1$ and $k = p$. Then $\mathrm{Nuc}_r(S_f) = E_{\hat{h}}$ is a field extension over F of degree $\deg(\hat{h}) = \frac{m}{s} = m$. □

Theorem 49. *Suppose that $\hat{h}(x)$ is irreducible in $F[x]$. Then f is the product of $l \geq 1$ irreducible polynomials in R all of which are mutually similar to each other, and*

$$R/Rh \cong M_k(\mathcal{E}(g))$$

where $g \in R$ is any irreducible divisor of h in R. If $\deg(g) = r \geq 1$, then $m = rl$, $\mathcal{E}(g)$ is a central division algebra over $E_{\hat{h}} = F[x]/(\hat{h}(x))$ of degree $s' = p^e/k$, where k is the number of irreducible factors of h, and

$$\mathrm{Nuc}_r(S_f) \cong M_l(\mathcal{E}(g)).$$

In particular, $\mathrm{Nuc}_r(S_f)$ is a central simple algebra over $E_{\hat{h}}$ of degree $s = ls'$, $\deg(\hat{h}) = \frac{r}{s'} = \frac{m}{s}$, $\deg(h) = \frac{rp^e}{s'} = \frac{mp^e}{s}$, and

$$[\mathrm{Nuc}_r(S_f) : F] = l^2 r s' = ms.$$

In particular s', s, and l divide $\gcd(m, p^e)$.

Proof. This follows immediately from Theorem 40 with $d = 1$. □

Chapter 4

The Eigenring of $f \in R$ with $\hat{h}$ Reducible and Squarefree

Let D be a central division algebra over C of degree d, let σ be an automorphism of D of finite inner order n, with $\sigma^n = \iota_u$, and let $f \in R = D[t;\sigma]$ have degree m. Recall that R has center

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

and that all non-constant polynomials in R are bounded. We let $h(t) = \hat{h}(u^{-1}t^n)$ denote the minimal central left multiple of f for some monic polynomial $\hat{h} \in F[x]$. If $f(t) = t - a$ for some $a \in D^\times$ (i.e. $m = 1$), then $\mathrm{Nuc}_r(S_f) = D$ and $\mathcal{E}(f) = \{b \in D : \sigma(b)a = ab\}$. From now on, we assume that $m > 1$, so that

$$\mathrm{Nuc}_r(S_f) = \mathcal{E}(f) = \mathrm{End}_R(R/Rf).$$

If $(f,t)_r = 1$, then any bound f^* of f has the form $f^* = a\hat{h}(u^{-1}t^n)$ for some $a \in D^\times$ (alternatively, $f^*(t) = ah(t)$).

For the remainder of this chapter we assume that $(f,t)_r = 1$ and that

$\hat{h}$ is a squarefree polynomial in $F[x]$, that is $\hat{h}(x) = \hat{\pi}_1(x)\hat{\pi}_2(x)\cdots\hat{\pi}_z(x)$ for some $z \in \mathbb{N}$ and some monic, irreducible polynomials $\hat{\pi}_z, \hat{\pi}_2, \ldots, \hat{\pi}_z$ in $F[x]$. We also use the notation $\pi_i(t) = \hat{\pi}_i(u^{-1}t^n)$ for $i \in \{1, 2, \ldots, z\}$.

Lemma 50. *If* $\hat{\pi}_i(x) \neq \hat{\pi}_j(x)$ *for* $i, j \in \{1, 2, \ldots, z\}$, *then* $\gcd(\pi_i(t), \pi_j(t)) = 1$.

Proof. Suppose that $\hat{\pi}_i(x) \neq \hat{\pi}_j(x)$ for some $i, j \in \{1, 2, \ldots, z\}$. Since $\hat{\pi}_i, \hat{\pi}_j$ are monic, irreducible polynomials in $F[x]$, $\gcd(\hat{\pi}_i(x), \hat{\pi}_j(x)) = 1$. By Bezout's Lemma, there exist polynomials $\hat{p}, \hat{q} \in F[x]$ such that

$$\hat{p}(x)\hat{\pi}_i(x) + \hat{q}(x)\hat{\pi}_j(x) = 1.$$

Let $p(t) = \hat{p}(u^{-1}t^n)$ and $q(t) = \hat{q}(u^{-1}t^n)$, then

$$p(t)\pi_i(t) + q(t)\pi_j(t) = 1.$$

We conclude that $\gcd(\pi_i(t), \pi_j(t)) = 1$, by Bezout's Lemma. □

Strictly, the proof of Lemma 50 shows that $\operatorname{gcrd}(\pi_i(t), \pi_j(t)) = 1$. However, the polynomials $\pi_i(t)$ and $\pi_j(t)$ lie in $C(R)$, hence they commute with all other polynomials in R, and so there is no distinction between the greatest common right divisor and the greatest common left divisor of $\pi_i(t)$ and $\pi_j(t)$. We call this simply the greatest common divisor. For the rest of the chapter we assume that $\hat{\pi}_i(x) \neq \hat{\pi}_j(x)$ for all $i, j \in \{1, 2, \ldots, z\}$ such that $i \neq j$. In this case $\hat{h}$ is said to be a *squarefree polynomial* in $F[x]$.

Lemma 51. *[Lam06, Chapter 1] Let* S *be a semisimple Artinian ring with direct sum decomposition*

$$S = S_1 \oplus S_2 \oplus \cdots \oplus S_z$$

for S_i a simple Artinian ring $1 \leq i \leq z$, and let M be a left S-module. Then M is a semisimple module over S, and there are exactly z isomorphism classes of simple left S-modules. Moreover, if $\{V_i : i = 1, 2, \ldots, z\}$ is a collection of representatives of the z isomorphism classes of simple left S-modules that occur as submodules of M, then

$$M = \bigoplus_{i=1}^{z} M_i,$$

where M_i denotes the direct sum of all submodules of M that are isomorphic to V_i. That is,

$$M \cong \bigoplus_{i=1}^{z} (V_i)^{\oplus n_i},$$

where n_i is the number of submodules of M that are isomorphic to V_i.

Remark (Submodules of R/Rf)**.** *By [Jac43, pg. 33], any submodule of the left R-module R/Rf has the form Rg/Rf, where $f = pg$ for some $p \in R$. Moreover, there is an R-module isomorphism*

$$Rg/Rf \cong R/Rp.$$

Therefore B is a simple submodule of R/Rf if and only if $B \cong R/Rp$ for some irreducible polynomial $p \in R$ such that $f = pg$ for some $g \in R$

Now, by [GTLN13, Proposition 5.2], there is a "rough decomposition" of f, of the form $f = g_1 g_2 \cdots g_z$ for some $g_i \in R$, such that g_i has minimal central left multiple π_i for each i. We note that, for all i, any two irreducible factors of g_i are also both irreducible factors of π_i, and are therefore similar to each other as polynomials [Jac09, Theorem 1.2.19], as π_i is a two-sided maximal element. Since the irreducible factors $\hat{\pi}_i$ of $\hat{h}$ in $F[x]$ can be permuted in the decomposition of $\hat{h}(x)$ (as $F[x]$ is a commutative ring of polynomials), we infer that the "rough decompo-

sition" of f is not unique, i.e. for any permutation $\beta \in \mathrm{S}_z$, there exist z polynomials $g'_1, g'_2, \ldots, g'_z \in R$, such that $f = g'_1 g'_2 \cdots g'_z$, and g'_i has minimal central left multiple $\pi_{\beta(i)}$.

For $f_i \in R$ any irreducible factor of f with minimal central left multiple $\pi_i(t)$, there exists a "rough decomposition" $f = g'_1 \cdots g'_z$ and a permutation $\beta \in \mathrm{S}_z$, such that f_i is an irreducible factor of g'_1 and that $i = \beta(1)$. Furthermore, since all irreducible factors of g'_1 are mutually similar, there exists some irreducible $f'_i \in R$, and some $g \in R$ such that $f_i \sim f'_i$, and $g'_1 = f'_i g$, i.e. $f = f'_i g g'_2 \cdots g'_z$. This means that R/Rf'_i is a simple submodule of R/Rf, and

$$R/Rf_i \cong R/Rf'_i.$$

From the argument of Remark 4, we immediately obtain the following:

Lemma 52. *If f_i is an irreducible factor of f in R, then the R-module R/Rf_i is isomorphic to a simple submodule of R/Rf.*

Theorem 53. *(i) $A = R/Rh$ is a semisimple Artinian ring which is isomorphic to the direct sum of simple Artinian rings*

$$R/Rh \cong R/R\pi_1 \oplus R/R\pi_2 \oplus \cdots \oplus R/R\pi_z.$$

Moreover, this is an isomorphism of $E_{\hat{h}}$-algebras.

(ii) The center of R/Rh is a direct sum of fields

$$C(R/Rh) = C(R/R\pi_1) \oplus C(R/R\pi_2) \oplus \cdots \oplus C(R/R\pi_z).$$

That is,

$$E_{\hat{h}} \cong E_{\hat{\pi}_1} \oplus E_{\hat{\pi}_2} \oplus \cdots \oplus E_{\hat{\pi}_z},$$

where $E_{\hat{\pi}_i} := F[x]/\langle \hat{\pi}_i(x) \rangle$ *is a field extension of* F *of degree equal to the degree of* $\hat{\pi}_i$ *in* $F[x]$ *for each* i*.*

(iii) Let $f_1, f_2, \ldots, f_z \in R$ *be irreducible polynomials of degrees* $m_1, m_2, \ldots, m_z$ *respectively, such that* $f_i(t)$ *is an irreducible factor of* $\pi_i(t)$*, and let* k_i *be the number of irreducible factors in any factorisation of* π_i *into irreducibles in* R*, for each* i*. Then* $\mathcal{E}(f_i)$ *is a central division algebra over* $E_{\hat{\pi}_i}$ *of degree* $s_i = dn/k_i$*, and*

$$R/R\pi_i \cong M_{k_i}(\mathcal{E}(f_i))$$

is a central simple algebra over $E_{\hat{\pi}_i}$ *of degree* $k_i s_i$*. In particular,* $\deg(\hat{\pi}_i) = \frac{m_i d}{s_i}$, $\deg(\pi_i) = \frac{m_i dn}{s_i}$*, and the following is an isomorphism of rings and of* $E_{\hat{h}}$*-algebras*

$$R/Rh \cong M_{k_1}(\mathcal{E}(f_1)) \oplus M_{k_2}(\mathcal{E}(f_2)) \oplus \cdots \oplus M_{k_z}(\mathcal{E}(f_z)).$$

(iv) There is a factorisation $f(t) = g_1(t)g_2(t)\cdots g_z(t)$ *for* $g_1, g_2, \ldots, g_z \in R$ *such that, for each* i*,* g_i *has minimal central left multiple* π_i*, and all irreducible factors of* g_i *are mutually similar to each other.*

(v) The following is an isomorphism of left A*-modules,*

$$R/Rf \cong (R/Rf_1)^{\oplus r_1} \oplus (R/Rf_2)^{\oplus r_2} \oplus \cdots \oplus (R/Rf_z)^{\oplus r_z},$$

where r_i *denotes the number of irreducible factors of* g_i *for each* i*.*

(vi) The following is an isomorphism of rings, and of $E_{\hat{h}}$*-algebras:*

$$\mathrm{Nuc}_r(S_f) \cong M_{r_1}(\mathcal{E}(f_1)) \oplus M_{r_2}(\mathcal{E}(f_2)) \oplus \cdots \oplus M_{r_z}(\mathcal{E}(f_z)).$$

In particular, $\mathrm{Nuc}_r(S_f)$ *is both a semisimple Artinian ring and a*

semisimple $E_{\hat{h}}$-algebra.

Proof. (i) By assumption, the polynomial $\hat{h}$ admits a factorisation into distinct monic, irreducible polynomials in $F[x]$, i.e. $\hat{h}(x) = \hat{\pi}_1(x)\hat{\pi}_2(x)\cdots\hat{\pi}_z(x)$ where $\hat{\pi}_i(x) \neq \hat{\pi}_j(x)$ for $i \neq j$. A decomposition of $\hat{h}$ into irreducible polynomials in $F[x]$ always exists, and is unique, since $F[x]$ is a unique factorisation domain (e.g. see [AW12, pg. 92-95]). Now, since $\hat{\pi}_i(x) \neq \hat{\pi}_j(x)$ for $i \neq j$, we have that $(\pi_i(t), \pi_j(t)) = 1$ for each distinct pair i, j, by Lemma 50. Also, by [GTLN13, pg. 3], we have that $R\pi_i + R\pi_j = R(\pi_i, \pi_j)_r = R$, since $\gcd(\pi_i(t), \pi_j(t)) = (\pi_i, \pi_j)_r = 1$ for any $i \neq j$. Hence the Chinese Remainder Theorem for non-commutative rings (e.g. [Ore52]) yields

$$\frac{R}{Rh} = \frac{R}{R\pi_1 \cap R\pi_2 \cap \cdots \cap R\pi_z} \cong \frac{R}{R\pi_1} \oplus \frac{R}{R\pi_2} \oplus \cdots \oplus \frac{R}{R\pi_z}$$

with the first equality due to the fact that

$$R\pi_1 \cap R\pi_2 \cap \cdots \cap R\pi_z = R\,\mathrm{lcm}(\pi_1, \pi_2, \ldots, \pi_z) = Rh$$

(e.g. [GT12, pg. 14]).

(ii) Since R/Rh is a semisimple Artinian ring isomorphic to the direct sum of the simple Artinian rings $R/R\pi_i$ for $i = 1, 2, \ldots, z$, we have that

$$C(R/Rh) \cong C(R/R\pi_1) \oplus C(R/R\pi_2) \oplus \cdots \oplus C(R/R\pi_z),$$

and $C(R/R\pi_i)$ is a field for each i, by [Jac43, Theorems 23-24]. Now, since $C(R/R\pi_i) \cong F[x]/\langle\hat{\pi}_i(x)\rangle =: E_{\hat{\pi}_i}$ for all i and $C(R/Rh) \cong$

$E_{\hat{h}}$ by Lemma 14,

$$E_{\hat{h}} \cong E_{\hat{\pi}_1} \oplus E_{\hat{\pi}_2} \oplus \cdots \oplus E_{\hat{\pi}_z}.$$

(iii) By Theorem 19, the eigenring $\mathcal{E}(f_i)$ is a central division algebra over $E_{\hat{\pi}_i}$ of degree $s_i = dn/k_i$ for all i. Moreover,

$$R/R\pi_i \cong M_{k_i}(\mathcal{E}(f_i)),$$

is a central simple algebra of degree $k_i s_i = dn$ over $E_{\hat{\pi}_i}$, $\deg(\hat{\pi}_i) = m_i d/s_i$, and $\deg(h) = m_i dn/s_i$, for all i. The stated isomorphism follows immediately from (i) and (ii).

(iv) The existence of the factorisation $f(t) = g_1(t) \cdots g_z(t)$ with each g_i having minimal central left multiple π_i, is essentially [GTLN13, Proposition 5.2]. We point out that for each i, any irreducible divisor of g_i is also an irreducible divisor of π_i, by definition of the minimal central left multiple of g_i. In the language of [Jac09], π_i is a two-sided maximal element of R, and by [Jac09, Theorem 1.2.19], any two irreducible divisors of π_i in R are similar polynomials. In particular, any two irreducible divisors of g_i are similar, for each i.

(v) By (i), $A = R/Rh$ is a semisimple Artinian ring, with z summands in any direct sum decomposition into simple Artinian rings. Then any left A-module is isomorphic to a direct sum of simple left A-modules, and there are precisely z isomorphism classes of simple left A-modules, by Lemma 51.

Consider the left A-module R/Rf. By [GTLN13, pg. 1], the lattice of submodules of R/Rf as a left A-module is identical to its lattice of submodules as a left R-module. By Lemma 52, we have that any

irreducible factor p of f in R, yields a simple left R-module R/Rp that is isomorphic to a simple R-submodule of R/Rf, and hence is isomorphic to a simple left A-submodule of R/Rf also. Now, every simple left A-module which occurs as a submodule of R/Rf appears as a direct summand in such a decomposition (up to isomorphism), by Lemma 51. Therefore, since there are r_i irreducible polynomials similar to f_i in any factorisation of f into irreducibles in R for each i, we have that the isomorphism class of R/Rf_i has size r_i for all i. Hence,

$$R/Rf \cong (R/Rf_1)^{\oplus r_1} \oplus (R/Rf_2)^{\oplus r_2} \oplus \cdots \oplus (R/Rf_z)^{\oplus r_z},$$

as left A-modules.

(vi) By (iii) and Lemma 1,

$$\mathrm{End}_A(R/Rf) \cong \mathrm{End}_A((R/Rf_1)^{\oplus r_1} \oplus (R/Rf_2)^{\oplus r_2} \oplus \cdots \oplus (R/Rf_z)^{\oplus r_z})$$

as rings. By Lemmas 2 and 3,

$$\mathrm{End}_A(R/Rf) \cong \bigoplus_{i=1}^{z} \mathrm{End}_A((R/Rf_i)^{\oplus r_i}) \cong \bigoplus_{i=1}^{z} M_{r_i}(\mathrm{End}_A(R/Rf_i)).$$

Also, since Rh is a two-sided ideal of R contained in $\mathrm{Ann}_R(R/Rf_i)$ and $Rh = \mathrm{Ann}_R(R/Rf)$, we have

$$\mathrm{End}_R(R/Rf) \cong \bigoplus_{i=1}^{z} M_{r_i}(\mathrm{End}_R(R/Rf_i)),$$

by Lemma 4. Therefore, since $\mathrm{End}_R(R/Rp) = \mathcal{E}(p)$ for any $p \in R$, and since $\mathcal{E}(p) = \mathrm{Nuc}_r(S_p)$ for any $p \in R$ of degree at least 2, we

have

$$\mathrm{Nuc}_r(S_f) \cong \bigoplus_{i=1}^{z} M_{r_i}(\mathcal{E}(f_i)).$$

□

Chapter 5

Subalgebras of the Right Nucleus

Throughout this chapter, unless stated otherwise, let D be an associative division algebra over its center C, let σ be an endomorphism of D, and let δ be a left σ-derivation of D. Let $F = C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$. The results of this chapter in the special case that $\delta = 0$ and D is a cyclic field extension of F appear in [OP19].

5.1 The General Case $R = D[t; \sigma, \delta]$

In this section we take yet another approach to investigate the Petit algebras associated with the polynomials in the ring $R = D[t; \sigma, \delta]$, and their nuclei. Throughout this chapter we let $f \in R$ be monic polynomial of degree $m > 1$.

In order to better understand the right nucleus of $S_f = D[t; \sigma, \delta]/D[t; \sigma, \delta]f$, we investigate firstly which elements of the coefficient ring D lie in $\mathrm{Nuc}_r(S_f)$, and secondly which powers of t lie in $\mathrm{Nuc}_r(S_f)$, before con-

structing a particular vector subspace of $\mathrm{Nuc}_r(S_f)$. To this end, we define

$$L^{(\sigma,\delta,f)} = \mathrm{Nuc}_r(S_f) \cap D$$

which is equal to the set

$$\{c \in D : [a, b, c] = 0 \text{ for all } a, b \in S_f\}.$$

For $\sigma = \mathrm{id}$, we use the notation $L^{(\mathrm{id},\delta,f)} = L^{(\delta,f)}$, and for $\delta = 0$ we use the notation $L^{(\sigma,0,f)} = L^{(\sigma,f)}$. From the definition of $L^{(\sigma,\delta,f)}$ we immediately have:

Lemma 54. *If f is not right-invariant, then*

$$L^{(\sigma,\delta,f)} = \mathrm{Nuc}(S_f) = D \cap \mathrm{Nuc}_r(S_f).$$

Proof. Since f is not right-invariant $\mathrm{Nuc}_l(S_f) = \mathrm{Nuc}_m(S_f) = D$, by Theorem 10. Hence

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

and the result follows. □

From now on, we write $L = L^{(\sigma,\delta,f)}$ when it is clear from the context which skew polynomial ring $D[t; \sigma, \delta]$ and which skew polynomial f is used.

In the following proposition we show that $\mathrm{Nuc}(S_f)$ is a division subring of D containing the field F, if f is not right-invariant:

Proposition 55. *(i) If f is right-invariant then $L = D$.*

(ii) If f is not right-invariant then L is a division subring of D con-

taining F.

Proof. (i) If f is right-invariant, then S_f is associative, i.e. $[a, b, c] = 0$ for all $a, b, c \in S_f$. In particular, $[a, b, c] = 0$ for all $a, b \in S_f$ and all $c \in D$, hence $L = D$.

(ii) Suppose that f is not right-invariant. Then $L = \mathrm{Nuc}(S_f) = \mathrm{Nuc}_r(S_f) \cap D$ is a subring of D. Moreover, it is well known that $\mathrm{Nuc}(S_f)$ is an associative subalgebra of S_f over F, hence it contains F as a subfield. It remains to show that every nonzero element of L has a multiplicative inverse, i.e. L is division. Let $c \in L$ be nonzero. Then c has a unique multiplicative inverse $c^{-1} \neq 0$ in D since $L \subseteq D$. Then we have

$$[a, b, c^{-1}]c = (a(bc^{-1}) - (ab)c^{-1})c = ab - ab,$$

as $c \in L \subseteq \mathrm{Nuc}_r(S_f)$. Hence $[a, b, c^{-1}]c = 0$ for any $a, b \in S_f$, which yields

$$([a, b, c^{-1}]c)c^{-1} = [a, b, c^{-1}](cc^{-1}) = [a, b, c^{-1}] = 0$$

because $c \in D = \mathrm{Nuc}_m(S_f)$. Therefore $c^{-1} \in \mathrm{Nuc}_r(S_f) \cap D = L$, and so $L = \mathrm{Nuc}(S_f)$ is a division ring.

□

Corollary 56. *If D is a field and f not right-invariant, then $L = \mathrm{Nuc}(S_f)$ is an intermediate field of D/F.*

We call $a \in D$ a *(right) semi-invariant element* with respect to f (or f-semi-invariant) if $fa \in Df$. Let M be a division subring of D. We say that f is *M-weak semi-invariant* if $fM \subset Df$. If f is D-weak semi-invariant, it is called *(right) semi-invariant*. It is clear that $fb \in Df$

for any $b \in L$. Hence any polynomial $f \in R$ is L-weak semi-invariant. A polynomial $f \in R$ is right-invariant if and only if it is (right) semi-invariant, and $ft \in Rf$ (e.g. [LLLM89]). We can now restate this criteria in terms of f-semi-invariant elements, and L.

Proposition 57. *f is right-invariant if and only if $L = D$ and $t \in \mathrm{Nuc}_r(S_f)$.*

Proof. We recall that f is right-invariant if and only if S_f is associative. Suppose that f is right-invariant. Then $L = D$ by Proposition 55. As previously stated, if f is right-invariant then S_f is associative, which in turn implies that S_f is equal to its right nucleus. Hence $t \in S_f$ yields $t \in \mathrm{Nuc}_r(S_f)$. Conversely, suppose that $L = D$ and $t \in \mathrm{Nuc}_r(S_f)$. Since L is contained in the right nucleus, and the right nucleus is closed under addition and multiplication the direct sum

$$D \oplus Dt \oplus Dt^2 \oplus \cdots \oplus Dt^{m-1}$$

is an F-subspace of $\mathrm{Nuc}_r(S_f)$. But $D \oplus Dt \oplus Dt^2 \oplus \cdots \oplus Dt^{m-1}$ is equal to S_f as vector spaces, hence $S_f \subseteq \mathrm{Nuc}_r(S_f)$. Since $\mathrm{Nuc}_r(S_f)$ is a subalgebra of S_f, $S_f = \mathrm{Nuc}_r(S_f)$, i.e. S_f is associative. The result follows immediately. □

The following theorem describes equivalent conditions for an element $c \in D$ to be semi-invariant with respect to f, and further we show that L is precisely the subset of D consisting of the semi-invariant elements with respect to f.

Theorem 58. *Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ and $c \in D$. Then the following are equivalent:*

(1) c is a semi-invariant element with respect to f,

(2) $c \in L^{(\sigma,\delta,f)}$,

(3) $\sigma^m(c)a_k = \sum_{j=k}^{m-1} a_j \Delta_{j,k}(c) - \Delta_{m,k}(c)$ *for all* $k \in \{0, 1, \ldots, m-1\}$.

Proof. To prove this we show first that (1) is true if and only if (2) is true, then we show that (1) is true if and only if (3) holds.

Suppose that c is semi-invariant with respect to f. Then $fc \in Df \subset Rf$ by definition, i.e. $c \in \mathrm{Nuc}_r(S_f)$. Hence $c \in \mathrm{Nuc}_r(S_f) \cap D = L$. Conversely, let $c \in L$. Then, in particular, $c \in \mathrm{Nuc}_r(S_f)$, and so $fc \in Rf$. This means that there exists $c' \in R$ such that $fc = c'f$. Comparing the degree of fc and $c'f$ it follows that $c' \in D$, hence c is a semi-invariant element with respect to f. Therefore the statements (1) and (2) are equivalent.

Now suppose that c is semi-invariant with respect to f. By definition, $fc \in Df$, that is $fc = c'f$ for some $c' \in D$. Computing each side gives

$$fc = (t^m - \sum_{i=0}^{m-1} a_i t^i)c = \sum_{j=0}^{m} \Delta_{m,j}(c)t^j - \sum_{i=0}^{m-1}\sum_{j=0}^{i} a_i \Delta_{i,j}(c)t^j = c't^m - \sum_{i=0} c'a_i t^i. \tag{5.1}$$

If we compare the coefficients of t^m we get:

$$c' = \Delta_{m,m}(c) = \sigma^m(c). \tag{5.2}$$

Now, comparing the coefficients of t^k for $k \in \{0, 1, ..., m-1\}$ gives

$$a_k \Delta_{k,k}(c) + a_{k+1}\Delta_{k+1,k}(c) + \cdots + a_{m-1}\Delta_{m-1,k}(c) - \Delta_{m,k}(c) = c'a_k. \tag{5.3}$$

Combining Equations 5.2 and 5.3 yields

$$\sigma^m(c)a_k = \sum_{i=k}^{m-1} a_i \Delta_{i,k}(c) - \Delta_{m,k}(c) \tag{5.4}$$

for all $k \in \{0, 1, \ldots, m-1\}$. Conversely, suppose that

$$\sigma^m(c)a_k = \sum_{i=k}^{m-1} a_i \Delta_{i,k}(c) - \Delta_{m,k}(c)$$

for all $k \in \{0, 1, \ldots, m-1\}$. Then

$$fc = \sum_{j=0}^{m} \Delta_{m,j}(c)t^j - \sum_{i=0}^{m-1} \sum_{j=0}^{i} \Delta_{i,j}(c)t^j = \sigma^m(c)f$$

by Equation 5.1. Hence (1) is equivalent to (3). □

Due to Theorem 58, we sometimes refer to L as the subring of semi-invariant elements in D with respect to the skew polynomial f. This means that if f is not right-invariant, then the set of semi-invariant elements in D with respect to f is the nucleus of S_f. Petit provides the following result in [Pet66]:

Theorem 59. *[Pet66, (5)] Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R = D[t; \sigma, \delta]$. Then the following are equivalent:*

(1) $t \in \mathrm{Nuc}_r(S_f)$,

(2) $t^m \circ_f t = t \circ_f t^m$,

(3) $ft \in Rf$,

(4) all powers of t are associative in S_f.

We obtain the following additional criterium for t to be contained in the right nucleus:

Theorem 60. *Let* $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$. *If* $a_i \in \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$ *for all* $i \in \{0, 1, ..., m-1\}$, *then* $t \in \mathrm{Nuc}_r(S_f)$.

Proof. Suppose that $a_i \in \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$. Then

$$ft = (t^m - \sum_{i=0}^{m-1} a_i t^i)t = t^{m+1} - \sum_{i=0}^{m-1} a_i t^{i+1} = t^{m+1} - \sum_{i=0}^{m-1} (t\sigma^{-1}(a_i) - \delta(\sigma^{-1}(a_i)))t^i,$$

but $a_i \in \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$ for all $i \in \{0, 1, \ldots, m-1\}$, which gives $\sigma^{-1}(a_i) = a_i$ and $\delta(\sigma^{-1}(a_i)) = \delta(a_i) = 0$ for all i. So

$$ft = t^{m+1} - \sum_{i=0}^{m-1} (t\sigma^{-1}(a_i) - \delta(\sigma^{-1}(a_i)))t^i = t(t^m - \sum_{i=0}^{m-1} a_i t^i) = tf \in Rf.$$

Hence $t \in \mathrm{Nuc}_r(S_f)$ by Theorem 59. □

From now on, we denote by F_k the set $\mathrm{Fix}(\sigma^k) \cap \mathrm{Const}(\delta)$ for any $k \in \mathbb{Z}$. We obtain the following generalization of Theorem 60:

Theorem 61. *Let* $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ *and let* $k \in \{1, 2, \ldots, m-1\}$. *If* $a_i \in F_k$ *for all* $i \in \{0, 1, \ldots, m-1\}$, *then* $t^k \in \mathrm{Nuc}_r(S_f)$. *In particular, then*

$$t^m \circ_f t^k = t^k \circ_f t^m.$$

Proof. Suppose that $a_i \in F_k$ for all i. Then in R, we have

$$\begin{aligned} t^k f &= t^k(t^m - \sum_{i=0}^{m-1} a_i t^i) \\ &= t^{m+k} - t^k \sum_{i=0}^{m-1} a_i t^i \\ &= t^{m+k} - \sum_{i=0}^{m-1} \sum_{j=0}^{k} \Delta_{k,j}(a_i) t^{i+j} \\ &= t^{m+k} - \sum_{i=0}^{m-1} \sigma^k(a_i) t^{i+k} \text{ (as } a_i \in \text{Const}(\delta)\ \forall i) \\ &= t^{m+k} - \sum_{i=0}^{m-1} a_i t^{i+k} \text{ (as } a_i \in \text{Fix}(\sigma^k)\ \forall i) \\ &= f t^k \in Rf, \end{aligned}$$

i.e. $ft^k = t^k f \in Rf$, and so $t^k \in \text{Nuc}_r(S_f)$ as claimed.

Since $t^k \in \text{Nuc}_r(S_f)$, we have in particular that $[t^k, t^{m-k}, t^k] = 0$ in S_f, that is $t^k \circ_f (t^{m-k} \circ_f t^k) = (t^k \circ_f t^{m-k}) \circ_f t^k$. Therefore $t^k \circ_f t^m = t^m \circ_f t^k$. □

Proposition 62. *Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$. Suppose that there exist $k \in \{1, 2, \ldots, k-1\}$ such that $a_i \in F_k$ for all i and that there is no $j \in \{1, 2, \ldots, k-1\}$ such that $a_i \in F_j$ for all i.*

(i) If $m = qk$ for some positive integer q, then

$$L \oplus Lt^k \oplus Lt^{2k} \oplus \cdots \oplus Lt^{(q-1)k} \oplus L(\sum_{i=0}^{m-1} a_i t^i)$$

is an F-sub vector space of $\text{Nuc}_r(S_f)$.

(ii) If $m = qk + r$ for some positive integers q, r with $0 < r < k$, then

$$L \oplus Lt^k \oplus Lt^{2k} \oplus \cdots \oplus Lt^{qk}$$

is an F-sub vector space of $\text{Nuc}_r(S_f)$.

Proof. (i) Since $a_i \in F_k$, we have that $t^k \in \mathrm{Nuc}_r(S_f)$ by Theorem 61. The right nucleus is a subalgebra of S_f, which implies that $t^{2k}, \ldots, t^{(q-1)k}, (t^k)^q = t^m = \sum_{i=0}^{m-1} a_i t^i \in \mathrm{Nuc}_r(S_f)$. Furthermore, we know that $L \subset \mathrm{Nuc}_r(S_f)$, and so $Lt^{jk} \subset \mathrm{Nuc}_r(S_f)$ for any $j \in \{0, 1, \ldots, q\}$. Therefore

$$L \oplus Lt^k \oplus \cdots \oplus Lt^{(q-1)k} \oplus L(\sum_{i=0}^{m-1} a_i t^i) \subset \mathrm{Nuc}_r(S_f)$$

as claimed.

(ii) We have $t^k \in \mathrm{Nuc}_r(S_f)$. Again since $\mathrm{Nuc}_r(S_f)$ is a subalgebra of S_f, this implies that $t^{2k}, \ldots t^{qk}, t^{(q+1)k}, \cdots \in \mathrm{Nuc}_r(S_f)$, hence the assertion follows by a similar argument to the proof of (i). □

Note that the powers $t^{qk}, t^{(q+1)k}, t^{(q+2)k}, \ldots$ of t^k in Proposition 62 (ii) lie in $\mathrm{Nuc}_r(S_f)$, but they need not be equal to polynomials in t^k, since $qk, (q+1)k, (q+2)k, \ldots \geq m$.

Lemma 63. *Suppose that* $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ *with* $a_i \in F_1$ *for all* $i \in \{0, 1, \ldots, m-1\}$. *If* $\sigma|_L$ *and* $\delta|_L$ *commute (i.e.* $\sigma(\delta(c)) = \delta(\sigma(c))$ *for all* $c \in L$*), then* $\sigma|_L$ *is an injective ring endomorphism of* L *and* $\delta|_L$ *is a left* $\sigma|_L$*-derivation of* L.

Proof. Let $c \in L$. Clearly, if $c = 0$, then $\sigma(c), \delta(c) \in L$, so we assume that $c \neq 0$. By Theorem 58

$$\sigma^m(c)a_k = \sum_{j=k}^{m-1} a_j \Delta_{j,k}(c) - \Delta_{m,k}(c) \tag{5.5}$$

for all $k \in \{0, 1, \ldots, m-1\}$. Applying σ to both sides of 5.5 yields

$$\sigma^{m+1}(c)a_k = \sum_{j=k}^{m-1} a_j \sigma(\Delta_{j,k}(c)) - \sigma(\Delta_{m,k}(c)) \tag{5.6}$$

as $a_i \in \mathrm{Fix}(\sigma)$ for all i. Now, since $\sigma(\delta(c)) = \delta(\sigma(c))$ we have

$$\sigma^m(\sigma(c))a_k = \sum_{j=k}^{m-1} a_j \Delta_{j,k}(\sigma(c)) - \Delta_{m,k}(\sigma(c)), \tag{5.7}$$

i.e. $\sigma(c) \in L$. Therefore $\sigma|_L$ is a ring endomorphism of L, which is necessarily injective since L is a division ring.

Now we apply δ to both sides of Equation 5.5, which yields

$$\begin{aligned}
&\delta(\sigma^m(c)a_k) = \delta(\sum_{j=k}^{m-1} a_j \Delta_{j,k}(c) - \Delta_{m,k}(c)) \\
\Rightarrow\ &\delta(\sigma^m(c))a_k = \sum_{j=k}^{m-1} a_j \delta(\Delta_{j,k}(c)) - \delta(\Delta_{m,k}(c)),\ \text{(since } \delta(a_k) = 0 \text{ for all } k) \\
\Rightarrow\ &\sigma^m(\delta(c))a_k = \sum_{j=k}^{m-1} a_j \Delta_{j,k}(\delta(c)) - \Delta_{m,k}(\delta(c)),
\end{aligned}$$

for all $k \in \{0, 1, \ldots, m-1\}$, that is $\delta(c) \in L$.

Finally, for any $a, b \in L$

$$\delta|_L(ab) = \sigma|_L(a)\delta|_L(b) + \delta|_L(a)b \in L.$$

Hence $\delta|_L$ is a left $\sigma|_L$-derivation of L. □

Theorem 64. *Suppose that $\sigma|_L$ and $\delta|_L$ commute, and let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in F[t] \subset R$. Write $\sigma = \sigma|_L$, and $\delta = \delta|_L$. Then*

$$L_f := L[t; \sigma, \delta]/L[t; \sigma, \delta]f(t)$$

is a subalgebra of $\mathrm{Nuc}_r(S_f)$.

Proof. Since σ is an injective endomorphism of L, and δ is a left σ-derivation of L, the skew polynomial ring $L[t; \sigma, \delta]$ is well-defined, $f(t) \in$

$F[t] \subset L[t;\sigma,\delta]$, and hence $L_f = L[t;\sigma,\delta]/L[t;\sigma,\delta]f(t)$ is a subalgebra of S_f.

On the other hand, L is contained in the right nucleus by definition, and since $a_i \in F$ for all i, we have that t lies in the right nucleus by Theorem 61. Thus $L \oplus Lt \oplus \cdots \oplus Lt^{m-1}$ is a subspace of the right nucleus, as $\mathrm{Nuc}_r(S_f)$ is an algebra, i.e. it is closed under addition and multiplication. Moreover the elements of $L \oplus Lt \oplus \cdots \oplus Lt^{m-1}$ are precisely the elements of L_f, that is $L_f \subseteq \mathrm{Nuc}_r(S_f)$. Therefore L_f is a subalgebra of $\mathrm{Nuc}_r(S_f)$. □

5.2 The Special Case $R = D[t;\sigma]$

Throughout this section we consider the Petit algebras associated with the polynomial ring $R = D[t;\sigma]$, and their nuclei. As a Corollary to Theorem 58, we obtain:

Theorem 65. *Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ and $c \in D$. Then $c \in L$ if and only if $\sigma^m(c)a_k = a_k\sigma^k(c)$ for all $k \in \{0,1,\ldots,m-1\}$.*

Proof. For $\delta = 0$, $\Delta_{j,i} = 0$ for all non-negative integers i, j with $i \neq j$, and $\Delta_{j,j} = \sigma^j$. We apply this to Theorem 58. □

From now on we denote the indices of the nonzero coefficients a_i in $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in D[t;\sigma]$ by $\lambda_1,\ldots,\lambda_r$, $1 \leq r \leq m$. We denote the set of these indices by

$$\Lambda_f = \{\lambda_1, \lambda_2, \ldots, \lambda_r\} \subset \{0,1,\ldots,m-1\}.$$

If it is clear from the context which f is used, we simply write Λ.

Corollary 66. *Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ and assume that $a_i \in C$ for*

all $i \in \{0, 1, \ldots, m-1\}$. *Then*

$$L = \bigcap_{\lambda_j \in \Lambda} \mathrm{Fix}(\sigma^{m-\lambda_j}).$$

In the case that D is commutative (i.e. D is a field and $D = C$) Petit states that t lies in the right nucleus if and only if the coefficients of f are all fixed by σ [Pet66, (16)]. We extend this result to the case that D is a (noncommutative) unital division ring:

Theorem 67. *[Pet66, (16) for D commutative] Let* $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$. *Then* $a_i \in \mathrm{Fix}(\sigma)$ *for all* $i \in \{0, 1, \ldots, m-1\}$ *if and only if* $t \in \mathrm{Nuc}_r(S_f)$.

Proof. If $a_i \in \mathrm{Fix}(\sigma)$ for all i, then $t \in \mathrm{Nuc}_r(S_f)$ by Theorem 60 with $\delta = 0$. Conversely, suppose that $t \in \mathrm{Nuc}_r(S_f)$, then $[t, t^{m-1}, t] = 0$ which implies that

$$(\sum_{i=0}^{m-1} a_i t^i)t = t(\sum_{i=0}^{m-1} a_i t^i),$$

i.e.,

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

This yields

$$a_{m-1}t^m + \sum_{i=0}^{m-2} a_i t^{i+1} = \sigma(a_{m-1})t^m + \sum_{i=0}^{m-2} \sigma(a_i)t^{i+1}.$$

We note that

$$t^m = (\sum_{i=0}^{m-1} a_i t^i) \bmod_r f.$$

Suppose that k is the smallest element of $\{0, 1, \ldots, m-1\}$ such that $a_k \neq 0$, i.e. $a_i = 0$ for all $i < k$. Then

$$\sum_{i=k}^{m-1} a_{m-1}a_i t^i + \sum_{i=k}^{m-2} a_i t^{i+1} = \sum_{i=k}^{m-1} \sigma(a_{m-1})a_i t^i + \sum_{i=k}^{m-2} \sigma(a_i)t^{i+1}.$$

Equating the t^k terms gives $a_{m-1}a_k = \sigma(a_{m-1})a_k \Rightarrow a_{m-1} \in \mathrm{Fix}(\sigma)$. Therefore

$$a_{m-1}\sum_{i=k}^{m-1} a_i t^i + \sum_{i=k}^{m-2} a_i t^{i+1} = a_{m-1}\sum_{i=k}^{m-1} a_i t^i + \sum_{i=k}^{m-2} \sigma(a_i) t^{i+1}$$
$$\Rightarrow \sum_{i=k}^{m-2} a_i t^{i+1} = \sum_{i=k}^{m-2} \sigma(a_i) t^{i+1}$$

and we have $a_i \in \mathrm{Fix}(\sigma)$ for all $i \in \{k, k+1, \ldots, m-2\}$. Since $a_i = 0$ for $i < k$, and $a_{m-1} \in \mathrm{Fix}(\sigma)$, we have $a_i \in \mathrm{Fix}(\sigma)$ for all $i \in \{0, 1, \ldots, m-1\}$. □

The following result of Brown and Pumplün [BP18, Proposition 2] is an immediate Corollary to Theorem 67:

Corollary 68. *[BP18, Proposition 2] Let $f(t) \in F[t] \subset R$. Then $F[t]/(f(t))$ is a commutative subring of $\mathrm{Nuc}_r(S_f)$, and a subfield of degree m if f is irreducible in $F[t]$.*

Proof. S_f contains the commutative subring $F[t]/(f)$ which is isomorphic to the ring consisting of the elements $\sum_{i=0}^{m-1} a_i t^i$ with $a_i \in F$. In particular, the powers of t are associative. This implies that $t \in \mathrm{Nuc}_r(S_f)$ [Pet66, (5)]. Clearly $F \subset \mathrm{Nuc}_r(S_f)$, so $F \oplus Ft \oplus \cdots \oplus Ft^{m-1} \subset \mathrm{Nuc}_r(S_f)$, hence we obtain the assertion. □

Corollary 69. *Suppose that $f(t) \in F[t] \subset R$ is not right-invariant such that $f(t) \neq t$, and let $h = \hat{h}(t^n)$ be its minimal central left multiple. If f is irreducible and $[L : F] = n/k$, where k is the number of irreducible factors of the minimal central left multiple h of f, then $\mathrm{Nuc}_r(S_f) = L_f$. In particular, then f is irreducible in $K[t;\sigma]$ if and only if f is irreducible in $L[t;\sigma]$.*

Proof. We know that $L_f = L[t;\sigma]/L[t;\sigma]f(t)$ is a subalgebra of $\mathrm{Nuc}_r(S_f)$ (Theorem 64). If f is irreducible then $\mathrm{Nuc}_r(S_f)$ has degree ms over F

by Theorem 19, therefore comparing the degrees of the field extensions we obtain the assertion. □

Below are two examples showing how we may compute the right nucleus of S_f using the preceding theory as well as the Wedderburn theory of Chapter 2.

Example 1 Let $D = (-1,-1)_{\mathbb{Q}}$, $\sigma : D \longrightarrow D$, $\sigma(d) = udu^{-1}$ with $u = i+1$ and $R = D[t;\sigma]$. Thus σ has inner order one, $\mathrm{Fix}(\sigma) = \mathbb{Q}(i)$, and $C(R) = \mathbb{Q}[x]$ with $x = u^{-1}t$. Also since $\sigma^4 = id$ and $\mathrm{Fix}(\sigma^2) = \mathrm{Fix}(\sigma^3) = \mathrm{Fix}(\sigma) = \mathbb{Q}(i)$, every $f \in R$ is bounded. Let $f \in R$ be monic and irreducible of degree $m > 1$ such that $(f,t)_r = 1$. Let $h(t) = \hat{h}(u^{-1}t)$ be its minimal central left multiple, such that $\hat{h}(x) \neq x$. Then one of the following holds:

- $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ is a field extension of degree $2m$, $k = 2$, and $\deg(h) = 2m$, or
- $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}}$ of degree 2, h is irreducible in R, $\deg(h) = m = \deg(\hat{h})$ and $[\mathrm{Nuc}_r(S_f) : F] = 4m$ (Corollary 22), in which case f must be right-invariant checking the dimensions.

So assume that f is not right-invariant, monic and irreducible, such that $(f,t)_r = 1$. Then $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ is a field extension of $\mathbb{Q}$ of degree $2m$. In particular, let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in \mathbb{Q}(i)[t] \subset D[t;\sigma]$ then $\mathbb{Q}(i) \subset L^{(\sigma,f)}$ (Proposition 55) and $t, t^2, \ldots, t^{m-1} \in \mathrm{Nuc}_r(S_f)$. Thus we obtain that

$$\mathbb{Q}(i)[t]/\mathbb{Q}(i)[t]f(t) \subset \mathrm{Nuc}_r(S_f)$$

and that

$$\mathrm{Nuc}_r(S_f) = \mathbb{Q}(i)[t]/\mathbb{Q}(i)[t]f(t)$$

for irreducible $f \in \mathbb{Q}(i)[t]$, by comparing dimensions of the vector spaces. Let $f(t) = it^2 + (k+1)t + j + k$, then

$$f^*(t) = -4t^4 + (4+4i)t^3 - 8it^2 + (8-8i)t + 8$$

[GTLN13, Example 2.13]. This means that

$$\hat{h}(x) = 16x^4 - 16x^3 + 16x^2 + 16x + 8 \in \mathbb{Q}[x]$$

and

$$h(t) = t^4 - (1+i)t^3 + 2it^2 - (2-2i)t - 2.$$

Scaling f to make it monic does not change its minimal central left multiple, so w.l.o.g. assume $f(t) = t^2 + i(k+1)t + k + ik$. If f is irreducible then the above result tells us that

$$\mathrm{Nuc}_r(S_f) \cong \mathbb{Q}[x]/(x^4 - x^3 + x^2 + x + 1/2).$$

Example 2 Let D be a quaternion algebra over a field F of characteristic not 2 and $\sigma \in \mathrm{Aut}_F(D)$ of order two. Then $K = \mathrm{Fix}(\sigma)$ is a quadratic field extension in D. We know that $\sigma(d) = udu^{-1}$ and $u^2 \in F$. W.l.o.g. choose $u \in K^\times$. Then $C(R) = F[x]$ with $x = u^{-1}t$. Let $f \in R$ be monic and irreducible of degree $m > 1$, such that $(f,t)_r = 1$. Let $h(t) = \hat{h}(u^{-1}t)$ be its minimal central left multiple. Then either

- $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ is a field extension of degree $2m$, $k = 2$, and $\deg(h) = 2m$, or
- $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}}$ of degree 2, h is irreducible in R, $\deg(h) = m = \deg(\hat{h})$ and $[\mathrm{Nuc}_r(S_f) : F] = 4m$ (Corollary 22), in which case f must be invariant checking the

dimensions.

So assume that f is not right-invariant, monic and irreducible. Then $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ is a field extension of degree $2m$. In particular, let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in \mathrm{Fix}(\sigma)[t] \subset D[t;\sigma]$ then $\mathrm{Fix}(\sigma) \subset L^{(\sigma,f)}$ (Proposition 55) and $t, t^2, \ldots, t^{m-1} \in \mathrm{Nuc}_r(S_f)$. Thus we obtain that

$$\mathrm{Fix}(\sigma)[t]/(f(t)) \subset \mathrm{Nuc}_r(S_f),$$

with equality if f is irreducible and not right-invariant.

5.2.1 The Right Nucleus of $t^m - a \in D[t;\sigma]$

In the particular case $f(t) = t^m - a \in R = D[t;\sigma]$ we obtain stronger results on the right nucleus than in the general case for any $f \in R$. Later we will see how this can be used to obtain irreducibility criteria for the polynomials of the form $t^m - a$ where $a \in F^\times$ where F denotes the field $C \cap \mathrm{Fix}(\sigma)$.

For $f(t) = t^m - a \in F[t] \subset D[t;\sigma]$ we get the reverse inclusion of Theorem 64, i.e. we can show that the right nucleus of S_f is equal to the subalgebra

$$L_f = L[t;\sigma]/L[t;\sigma]f(t) :$$

Theorem 70. *Let $f(t) = t^m - a \in F[t] \subset R$. Then*

$$\mathrm{Nuc}_r(S_f) = L[t;\sigma]/L[t;\sigma]f(t).$$

Proof. If $f(t) \in F[t] \subset D[t;\sigma]$, then

$$L[t;\sigma]/L[t;\sigma]f(t)$$

is a subalgebra of $\mathrm{Nuc}_r(S_f)$, by Theorem 64 with $\delta = 0$.
Now, we suppose that $g(t) = \sum_{i=0}^{m-1} g_i t^i \in \mathrm{Nuc}_r(S_f)$. Then $fg \in Rf$, i.e. there exists a polynomial $g' \in D[t;\sigma]$ such that $fg = g'f$. It is easy to see that $\deg(g) = \deg(g')$, so we let $g'(t) = \sum_{j=0}^{m-1} g'_j t^j$ for some $g'_j \in D$. Then we have

$$(t^m - a)\sum_{i=0}^{m-1} g_i t^i = (\sum_{j=0}^{m-1} g'_j t^j)(t^m - a)$$
$$\Rightarrow \sum_{i=0}^{m-1} \sigma^m(g_i)t^{m+i} - \sum_{i=0}^{m-1} a g_i t^i = \sum_{j=0}^{m-1} g'_j t^{m+j} - \sum_{j=0}^{m-1} g'_j a t^j.$$

Comparing coefficients of t^{m+j} for $j \in \{0, 1, ..., m-1\}$ yields $g'_j = \sigma^m(g_j)$, and comparing coefficients of t^j for $j \in \{0, 1, \ldots, m-1\}$ yields $g'_j a = a g_j$. Combining these gives

$$\sigma^m(g_j)a = a g_j$$

for all $j \in \{0, 1, \ldots, m-1\}$, that is $g_j \in L$ for all j. Hence $g(t) \in L[t;\sigma]/L[t;\sigma]f(t)$. The result follows immediately. □

5.2.2 $L^{(\sigma,f)}$ for $f \in K[t;\sigma]$ with K a Cyclic Field Extension of F

For the remainder of the section (Section 5.2) suppose that K/F is a Galois extension of F of degree n with cyclic Galois group $\mathrm{Gal}(K/F) = \langle\sigma\rangle$, let $R = K[t;\sigma]$ and let

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

Proposition 71.

$$L = \{u \in K : u \in \mathrm{Fix}(\sigma^{m-\lambda_j}) \text{ for all } \lambda_j \in \Lambda\} = \bigcap_{\lambda_j \in \Lambda} \mathrm{Fix}(\sigma^{m-\lambda_j}).$$

Proof. Let

$$u \in L = \{u \in K : \sigma^m(u)a_i = a_i\sigma^i(u) \text{ for all } i \in \{0, 1, \ldots, m-1\}\}.$$

Then

$$\begin{aligned} &\sigma^m(u)a_i = a_i\sigma^i(u) \text{ for each } i \\ \Leftrightarrow\, &\sigma^m(u)a_i = \sigma^i(u)a_i \text{ for each } i \\ \Leftrightarrow\, &\sigma^{m-i}(u) = u \text{ for each } i \text{ such that } a_i \neq 0 \\ \Leftrightarrow\, &\sigma^{m-\lambda_j}(u) = u \text{ for each } \lambda_j \in \Lambda. \end{aligned}$$

This yields the assertion. □

Corollary 72. *If $a_{m-1} \neq 0$, then $L = F$.*

Proof. Let $u \in L$, then $\sigma^m(u)a_{m-1} = a_{m-1}\sigma^i(u)$ yields $\sigma(u) = u$, hence $u \in F$. This implies immediately that $L = F$. □

Lemma 73. *(i) Let $E = \mathrm{Fix}(\sigma^{u_1}) \cap \mathrm{Fix}(\sigma^{u_2})$ for some $u_1, u_2 \in \mathbb{Z}$ such that $1 \leq u_1, u_2 < n$. If $\alpha = \gcd(u_1, u_2, n)$, then $\mathrm{Gal}(K/E) = \langle\sigma^\alpha\rangle$ and $E = \mathrm{Fix}(\sigma^\alpha)$.*
(ii) Let $E' = \mathrm{Fix}(\sigma^{u_1}) \cap \mathrm{Fix}(\sigma^{u_2}) \cap \cdots \cap \mathrm{Fix}(\sigma^{u_k})$ for some $u_1, u_2, \ldots, u_k \in \mathbb{Z}$ such that $1 \leq u_1, u_2, \ldots, u_k < n$. If $\alpha = \gcd(u_1, u_2, \ldots, u_k, n)$, then $\mathrm{Gal}(K/E') = \langle\sigma^\alpha\rangle$, and $E' = \mathrm{Fix}(\sigma^\alpha)$.

Proof. (i) Let $v_1 = \gcd(u_1, n)$ and $v_2 = \gcd(u_2, n)$. Now

$$\mathrm{ord}(\sigma^{u_1}) = \frac{n}{\gcd(u_1, n)} = \frac{n}{v_1}$$

and

$$\mathrm{ord}(\sigma^{v_1}) = \frac{n}{\gcd(v_1, n)} = \frac{n}{v_1}.$$

Therefore $\langle\sigma^{u_1}\rangle = \langle\sigma^{v_1}\rangle$, and similarly $\langle\sigma^{u_2}\rangle = \langle\sigma^{v_2}\rangle$ (note that also

$E = \mathrm{Fix}(\sigma^{v_1}) \cap \mathrm{Fix}(\sigma^{v_2})$). We have that $\mathrm{Gal}(K/E)$ is a cyclic subgroup of $\langle\sigma\rangle$. Thus there exists a smallest integer β, $1 \leq \beta < n$, such that $\mathrm{Gal}(K/E) = \langle\sigma^{\beta}\rangle$.

E is a subfield of $\mathrm{Fix}(\sigma^{v_1})$, which means that $\langle\sigma^{v_1}\rangle$ is a subgroup of $\langle\sigma^{\beta}\rangle$, and β divides v_1. Similarly, we get that β also divides v_2. Therefore β is a common divisor of v_1 and v_2. By [Lan04, Chapter VI, Section 1, Corollary 1.4] we know that $\mathrm{Gal}(K/E) = \langle\sigma^{v_1}, \sigma^{v_2}\rangle$, i.e. if $\tau \in \mathrm{Gal}(K/E)$, then

$$\tau = \sigma^{\tau_1 v_1}\sigma^{\tau_2 v_2} = \sigma^{\tau_1 v_1 + \tau_2 v_2},$$

for some $\tau_1, \tau_2 \in \mathbb{Z}$.

Now $\langle\sigma^{\beta}\rangle = \mathrm{Gal}(K/E) = \langle\sigma^{v_1}, \sigma^{v_2}\rangle$, and so $\sigma^{\beta} \in \langle\sigma^{v_1}, \sigma^{v_2}\rangle$. Hence $\sigma^{\beta} = \sigma^{xv_1+yv_2}$ for some $x, y \in \mathbb{Z}$, and so we take $\beta = xv_1 + yv_2 + zn$ for some $z \in \mathbb{Z}$. Let $\alpha = \gcd(v_1, v_2, n)$. Then α divides v_1, v_2 and n, by definition. Therefore α divides $x_0v_1 + y_0v_2 + z_0n$ for any $x_0, y_0, z_0 \in \mathbb{Z}$; in particular α divides $xv_1 + yv_2 + zn = \beta$. In summary, we have shown that β is a common divisor of v_1, v_2, and n, and $\alpha = \gcd(v_1, v_2, n)$ divides β; so we must have that $\alpha = \beta$. Moreover,

$$\alpha = \gcd(v_1, v_2, n) = \gcd(\gcd(u_1, n), \gcd(u_2, n), n) = \gcd(u_1, u_2, n).$$

Hence we obtain that $\mathrm{Gal}(K/E) = \langle\sigma^{\alpha}\rangle$, and $E = \mathrm{Fix}(\sigma^{\alpha})$ with $\alpha = \gcd(u_1, u_2, n)$ as claimed.

(ii) This follows by induction from (i). □

Theorem 74. *If $\alpha = \gcd(m - \lambda_1, m - \lambda_2, \ldots, m - \lambda_r, n)$, then*

$$L = \mathrm{Fix}(\sigma^{\alpha})$$

and $[L : F] = \alpha$. In particular, $L = F$ if and only if $\alpha = 1$.

Proof. By Proposition 71, we have

$$L = \bigcap_{\lambda_j \in \Lambda} \mathrm{Fix}(\sigma^{m-\lambda_j}) = \mathrm{Fix}(\sigma^{m-\lambda_1}) \cap \mathrm{Fix}(\sigma^{m-\lambda_2}) \cap \cdots \cap \mathrm{Fix}(\sigma^{m-\lambda_r}).$$

Therefore it follows that $L = \mathrm{Fix}(\sigma^\alpha)$ where $\alpha = \gcd(m-\lambda_1, m-\lambda_2, \ldots, m-\lambda_r, n)$ by Lemma 73. Obviously $L = F$ if and only if $\mathrm{Fix}(\sigma^\alpha) = F$, if and only if $\langle\sigma^\alpha\rangle = \langle\sigma\rangle$, which is true if and only if σ^α has order n. Now $\mathrm{ord}(\sigma^\alpha) = \frac{n}{\gcd(n,\alpha)} = n$ if and only if $\gcd(n,\alpha) = 1$. That is, $L = F$ if and only if $\gcd(n,\alpha) = 1$, if and only if $\alpha = 1$. □

Theorem 75. *(i) $L = K$ if and only if $m - \lambda_j$ is a multiple of n for all $\lambda_j \in \Lambda$.*
(ii) Suppose that n is prime. Then $L = F$ if and only if there exists $\lambda_j \in \Lambda$ such that $m - \lambda_j$ is not divisible by n.

Proof. We have $L = \mathrm{Fix}(\sigma^\alpha)$ where $\alpha = \gcd(m-\lambda_1, m-\lambda_2, \ldots, m-\lambda_r, n)$ (Lemma 73).
(i) $\alpha = \gcd(m-\lambda_1, m-\lambda_2, \ldots, m-\lambda_r, n) = n$ if and only if $m - \lambda_j$ is a multiple of n for all $\lambda_j \in \Lambda$. That is $L = \mathrm{Fix}(\sigma^n) = K$ if and only if $m - \lambda_j$ is a multiple of n for all $\lambda_j \in \Lambda$.
(ii) If n is prime, then $\alpha | n \Rightarrow \alpha \in \{1, n\}$. The result now follows immediately from (i). □

Recall that $C(R) = F[x]$ with the identification $x = t^n$. We obtain the following well-known result (cf. [Jac09]) rewritten in terms of the Petit algebra S_f:

Corollary 76. *Suppose that f has the form $f(t) = ag(t^n)t^l$ for some scalar $a \in K$, some polynomial $g(t) = \hat{g}(t^n)$ such that $\hat{g} \in F[x]$ and some integer $l \geq 0$. Then S_f is associative and hence f is right-invariant.*

Proof. By Theorem 64, we know that $L[t;\sigma]/L[t;\sigma]f(t)$ is a subalgebra of the right nucleus. Since $m - \lambda_j$ is a multiple of n for all $\lambda_j \in \Lambda$, it

follows that $L = K$ by Theorem 75 (i). Thus $K[t;\sigma]/K[t;\sigma]f(t)$ is a subalgebra of $\mathrm{Nuc}_r(S_f)$, which implies that $S_f = \mathrm{Nuc}_r(S_f)$. Hence S_f is an associative algebra which is true if and only if f in right-invariant in R. □

5.2.3 The Case $n < m$.

Let K/F be a cyclic Galois extension of degree n with Galois group $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ and

$$\mathrm{ord}(\sigma) = n < m = \deg(f).$$

Then there exist integers q, r such that $q \neq 0$, and $m = qn + r$ where $0 \leq r < n$. Moreover, $K = \mathrm{Fix}(\sigma^n)$ hence the coefficients of $f \in R$ always lie in $\mathrm{Fix}(\sigma^n)$. Applying this to Theorem 61 yields the following:

(i) If $m = qn$, then

$$L \oplus Lt^n \oplus Lt^{2n} \oplus \cdots \oplus Lt^{(q-1)n}$$

is an F-sub vector space of $\mathrm{Nuc}_r(S_f)$ of dimension $q[L : F]$ and

$$t^{qn} = t^m = \sum_{i=0}^{m-1} a_i t^i \in \mathrm{Nuc}_r(S_f).$$

(ii) If $m = qn + r$ for some positive integers q, r with $0 < r < n$, then

$$L \oplus Lt^n \oplus Lt^{2n} \oplus \cdots \oplus Lt^{qn}$$

is an F-sub vector space of $\mathrm{Nuc}_r(S_f)$ of dimension $(q + 1)[L : F]$. If we assume that n is either prime or $\gcd(m, n) = 1$, f is not right-invariant and $(f, t)_r = 1$, as well as $[L : F] = n$, then f is reducible.

Theorem 77. *Suppose that $[L : F] = \rho$ where $n = b\rho$ for some $b \in \mathbb{N}$. Then $m = q\rho + r$ for some integers q, r with $0 \leq r < \rho$, and $f(t) = g(t^\rho)t^r$, where g is a polynomial of degree q in $K[t^\rho; \sigma^\rho]$.*

Proof. By Theorem 74, we have that $L = \mathrm{Fix}(\sigma^\alpha)$, where $\alpha = \gcd(m - \lambda_1, m - \lambda_2, \ldots, m - \lambda_r, n)$. Now $\alpha = \rho$ if and only if $m - \lambda_j$ is a multiple of ρ for all $\lambda_j \in \Lambda$. But $m - \lambda_j$ is equal to a multiple of ρ if and only if $\lambda_j = r + \rho l$ for some integer l such that $0 \leq l < q$ (since $m = q\rho + r$). Therefore we obtain $\Lambda \subset \{r, r + \rho, r + 2\rho, \ldots, r + (q-1)\rho\}$. Thus

$$\begin{aligned} f(t) &= t^{q\rho+r} - a_{(q-1)\rho+r}t^{(q-1)\rho+r} - \cdots - a_{r+\rho}t^{r+\rho} - a_r t^r \\ &= [(t^\rho)^q - a_{(q-1)\rho+r}(t^\rho)^{(q-1)} - \cdots - a_{r+\rho}t^\rho - a_r]t^r \\ &= g(t^\rho)t^r \end{aligned}$$

where g has degree q in $K[t^\rho; \sigma^\rho]$. □

5.3 The Special Case $R = D[t;\delta]$

Throughout this section we consider the Petit algebras associated with the polynomial ring $R = D[t;\delta]$, and their nuclei. As a Corollary to Theorem 58 we obtain:

Theorem 78. *Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ and $c \in D$. Then $c \in L$ if and only if*

$$ca_k = \sum_{i=k}^{m-1} a_i \binom{i}{k} \delta^{i-k}(c) - \binom{m}{k}\delta^{m-k}(c)$$

for all $k \in \{0, 1, \ldots, m-1\}$.

Proof. Since here $\sigma = \mathrm{id}$, the map $\Delta_{j,i}$ is equal to $\binom{j}{i}\delta^{j-i}$ for any $i, j \in \mathbb{Z}$ such that $0 \leq i \leq j$. The result follows immediately by Theorem 58. □

Corollary 79. *Suppose that D has prime characteristic p. Let $f(t) = t^p - \sum_{i=0}^{p-1} a_i t^i \in R$, and let $c \in D$. Then $c \in L$ if and only if*

$$ca_k = \sum_{i=k}^{p-1} a_i \binom{i}{k} \delta^{i-k}(c)$$

for all $k \in \{1, 2 \ldots, m-1\}$, and

$$ca_0 = \sum_{i=0}^{p} a_i \delta^i(c)$$

where $a_p = -1$.

Proof. We note that $\binom{p}{k}$ is divisible by p for all $k \in \{1, 2, \ldots, p-1\}$, and $\binom{p}{0} = 1$. The result follows immediately. □

We can also prove the converse to Theorem 60, for the special case $\sigma = \mathrm{id}$:

Theorem 80. *Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R = D[t;\delta]$. Then $a_i \in \mathrm{Const}(\delta)$ for all $i \in \{0, 1, \ldots, m-1\}$ if and only if $t \in \mathrm{Nuc}_r(S_f)$.*

Proof. By Theorem 60 with $\sigma = \mathrm{id}$, if $a_i \in \mathrm{Const}(\delta)$ for all $i \in \{0, 1, \ldots, m-1\}$, then $t \in \mathrm{Nuc}_r(S_f)$. On the other hand, if $t \in \mathrm{Nuc}_r(S_f)$, then $[t, t^{m-1}, t] = 0$ which gives

$$(\sum_{i=0}^{m-1} a_i t^i)t = t(\sum_{i=0}^{m-1} a_i t^i),$$

that is

$$a_{m-1}t^m + \sum_{i=0}^{m-2} a_i t^{i+1} = a_{m-1}t^m + \sum_{i=0}^{m-2} a_i t^i + \sum_{i=0}^{m-1} \delta(a_i) t^i. \tag{5.8}$$

We note that $t^m = (\sum_{i=0}^{m-1} a_i t^i) \bmod_r f$, however, we need not explicitly substitute this into Equation 5.8, since only $a_{m-1}t^m$ appears on each side

of 5.8, hence all terms in t^m sum to 0. We are left with

$$\sum_{i=0}^{m-1} \delta(a_i)t^i = 0. \tag{5.9}$$

Since Equation 5.9 is an equality in S_f, we have that $\delta(f(t)) := \sum_{i=0}^{m-1} \delta(a_i)t^i \in Rf$, i.e that $\delta(f) = gf$ for some $g(t) \in R$. Then

$$\deg(gf) = \deg(g) + \deg(f) = \deg(g) + m = \deg(\delta(f)) \leq m - 1,$$

which forces $g = 0$, and $\delta(f) = gf = 0$. Therefore Equation 5.9 is also true in R, and so $\delta(a_i) = 0$ for each $i \in \{0, 1, \ldots, m-1\}$. The result follows immediately. □

5.3.1 The Right Nucleus of $t^p - a \in D[t;\delta]$ when $\mathrm{Char}(D) = p > 0$

For the remainder of the chapter we suppose that D has prime characteristic p, and we consider the polynomial $f(t) = t^p - a \in D[t;\delta]$.

In a similar fashion to the results of Section 5.2.1, we obtain stronger results on the right nucleus of S_f for the particular polynomial $f(t) = t^p - a$ under certain conditions on the constant coefficient $a \in D^\times$. In particular Theorem 82 is analogous to Theorem 70. Again we will make use of the following results in the coming chapters to determine irreducibility criteria for the polynomial $f = t^p - a \in D[t;\delta]$. Recall that the bracket defined by $[b, c] = bc - cb$ for $b, c \in D$ is the commutator on D.

Lemma 81.

$$L = \{c \in D : [a, c] = \delta^p(c)\}.$$

In particular, if $a \in C$, then

$$L = \{c \in D : \delta^p(c) = 0\} = \mathrm{Const}(\delta^p).$$

Proof. Let $c \in L$. By definition, this is true if and only if $fc = c'f$ for some $c' \in D$, i.e. $(t^p - a)c = c'(t^p - a)$. Computing both sides gives

$$\sum_{i=0}^{p} \binom{p}{i} \delta^{p-i}(c)t^i - ac = c't^p - c'a.$$

Now, since $\binom{p}{i}$ is divisible by p for all $i \neq 0, p$, this simplifies to

$$ct^p + \delta^p(c) - ac = c't^p - c'a.$$

This yields $c = c'$ and $\delta^p(c) - ac = -ca$, i.e. $\delta^p(c) = [a, c]$. Therefore $L \subset \{c \in D : [a, c] = \delta^p(c)\}$. Conversely, let $c \in \{c \in D : [a, c] = \delta^p(c)\}$. Then

$$fc = \sum_{i=0}^{p} \binom{p}{i} \delta^{p-i}(c)t^i - ac = ct^p + \delta^p(c) - ac = ct^p - ca = cf.$$

Therefore $c \in L$, and $\{c \in D : [a, c] = \delta^p(c)\} \subset L$. The second part follows easily, since $[a, c] = 0$ for all $c \in D$ when a is in the center C of D. □

Theorem 82. *If $a \in \mathrm{Const}(\delta)$, then*

$$\mathrm{Nuc}_r(S_f) = L[t; \delta|_L]/L[t; \delta|_L]f(t).$$

Proof. First we note that $a \in L$, since $[a, a] = \delta^p(a) = 0$ (Lemma 73), i.e. $f(t) \in L[t; \delta|_L]$. Then

$$L_f = L[t; \delta|_L]/L[t; \delta|_L]f(t)$$

is a well-defined Petit algebra. Now since $a \in \mathrm{Const}(\delta)$, the algebra L_f is an associative subalgebra of $\mathrm{Nuc}_r(S_f)$. To complete the proof we show that the right nucleus $\mathrm{Nuc}_r(S_f)$ is contained in the set

$$L \oplus Lt \oplus \cdots \oplus Lt^{p-1}.$$

Let $g(t) = \sum_{i=0}^{p-1} g_i t^i \in \mathrm{Nuc}_r(S_f)$. Then $fg = g'f$ for some $g' \in D[t;\delta]$. Assume w.l.o.g. that $g'(t) = \sum_{i=0}^{p-1} g'_i t^i$, then we have

$$\begin{aligned}
&(t^p - a)\sum_{i=0}^{p-1} g_i t^i = \sum_{i=0}^{p-1} g'_i t^i (t^p - a) \\
\Rightarrow &\sum_{i=0}^{p-1}\sum_{j=0}^{p} \binom{p}{j} \delta^{p-j}(g_i) t^{i+j} - \sum_{i=0}^{p-1} a g_i t^i = \sum_{i=0}^{p-1} g'_i t^{p+i} - \sum_{i=0}^{p-1} g'_i \sum_{j=0}^{i} \binom{i}{j} \delta^{i-j}(a) t^j
\end{aligned}$$

Since $\binom{p}{j}$ is divisible by p for all $j \neq 0, p$, and D has characteristic p, and $\delta(a) = 0$ we reduce to the following:

$$\sum_{i=0}^{p-1} g_i t^{p+i} + \sum_{i=0}^{p-1} \delta^p(g_i) t^i - \sum_{i=0}^{p-1} a g_i t^i = \sum_{i=0}^{p-1} g'_i t^{p+i} - \sum_{i=0}^{p-1} g'_i a t^i.$$

This yields $g_i = g'_i$ and $[a, g_i] = \delta^p(g_i)$ for all $i = 0, 1, \ldots, p-1$, that is $g_i \in L$ for each $i = 0, 1, \ldots, p-1$. Hence $g(t) \in L \oplus Lt \oplus \cdots \oplus Lt^{p-1}$, and the result follows. □

Chapter 6

The Right Nucleus of S_f for Low Degree Polynomials in $K[t;\sigma]$

In this chapter we assume that K is a cyclic Galois field extension of finite degree n over F with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. We repeatedly use that $[\mathrm{Fix}(\sigma^\rho) : F] = \gcd(n, \rho)$. We now use the previous results to explore the structure of $\mathrm{Nuc}_r(S_f)$ for some polynomials of low degree in $K[t;\sigma]$. The same arguments then apply for those of higher degree as well but of course quickly become tedious. The results of this chapter also appear in [OP19].

6.1.1 $\deg(f) = 2$

Let $f(t) = t^2 - a_1 t - a_0 \in K[t;\sigma]$. Then $L^{(\sigma,f)} = \bigcap_{\lambda_j \in \Lambda} \mathrm{Fix}(\sigma^{2-\lambda_j})$ by Proposition 71.

(1) If $f(t) = t^2 - a_0$ with $a_0 \in K^\times$, then $L^{(\sigma,f)} = \mathrm{Fix}(\sigma^2)$.

(2) If $f(t) = t^2 - a_1 t - a_0$ with $a_1 \in K^\times$, then $L^{(\sigma,f)} = F$.

Note that if $n = [K : F]$ is even, then σ^2 has order $\frac{n}{2}$ in $\mathrm{Gal}(K/F)$, which means that $F \neq \mathrm{Fix}(\sigma^2)$. If n is odd, then $\gcd(n, 2) = 1$, therefore $\mathrm{Fix}(\sigma^2) = F$.

If we additionally assume that $f(t) \in F[t]$, then we obtain:

Proposition 83. *Let $f(t) = t^2 - a_0 \in F[t] \subset K[t;\sigma]$, $a_0 \neq 0$ then*

$$\mathrm{Fix}(\sigma^2)[t;\sigma]/\mathrm{Fix}(\sigma^2)[t;\sigma]f(t)$$

is a subalgebra of $\mathrm{Nuc}_r(S_f)$ of dimension $2[\mathrm{Fix}(\sigma^2) : F]$ over F. In particular, if n is odd, f not right-invariant such that $(f,t)_r = 1$, and $\hat{h}(x) \neq x$, then f is reducible.

Proof. By Theorem 64, $L^{(\sigma,f)}[t;\sigma]/L^{(\sigma,f)}[t;\sigma]f(t)$ is a subalgebra of $\mathrm{Nuc}_r(S_f)$ and $L^{(\sigma,f)} = \mathrm{Fix}(\sigma^2)$ by (1), which yields the first assertion. The second assertion follows from the fact that the right nucleus has dimension 2 over F for irreducible right-invariant f under our assumptions. □

6.1.2 $\deg(f) = 3$

Let $f(t) \in K[t;\sigma]$ be monic of degree 3. Then $L^{(\sigma,f)} = \bigcap_{\lambda_j \in \Lambda} \mathrm{Fix}(\sigma^{3-\lambda_j})$ by Proposition 71.

(1) If $f(t) = t^3 - a_0 \in K[t;\sigma]$, where $a_0 \in K^\times$, then $L^{(\sigma,f)} = \mathrm{Fix}(\sigma^3)$.

(2) If $f(t) = t^3 - a_1 t \in K[t;\sigma]$, where $a_1 \in K^\times$, then $L^{(\sigma,f)} = \mathrm{Fix}(\sigma^2)$.

(3) In all other cases, we obtain $L^{(\sigma,f)} = F$.

Proposition 84. *(i) If $f(t) = t^3 - a_0$ with $0 \neq a_0 \in F$, then*

$$\mathrm{Fix}(\sigma^3)[t;\sigma]/\mathrm{Fix}(\sigma^3)[t;\sigma]f(t)$$

is a subalgebra of $\mathrm{Nuc}_r(S_f)$ *of dimension* $3[\mathrm{Fix}(\sigma^3) : F]$ *over* F. *In particular, if* f *is not right-invariant,* n *is prime or not divisible by 3, such that* $(f,t)_r = 1$, *and* $\hat{h}(x) \neq x$ *then* f *is reducible.*
(ii) If $f(t) = t^3 - a_1 t$ *with* $0 \neq a_1 \in F$, *then*

$$\mathrm{Fix}(\sigma^2)[t;\sigma]/\mathrm{Fix}(\sigma^2)[t;\sigma]f(t)$$

is a subalgebra of $\mathrm{Nuc}_r(S_f)$ *of dimension* $3[\mathrm{Fix}(\sigma^2) : F]$ *over* F.

Proof. By Theorem 64, $L^{(\sigma,f)}[t;\sigma]/L^{(\sigma,f)}[t;\sigma]f(t) \subset \mathrm{Nuc}_r(S_f)$.
(i) If $f(t) = t^3 - a_0 \in F[t]$ with $a_0 \neq 0$, then $L^{(\sigma,f)} = \mathrm{Fix}(\sigma^3)$ which proves the assertion looking at the dimensions.
(ii) If $f(t) = t^3 - a_1 t \in F[t]$ with $a_1 \neq 0$, then $L^{(\sigma,f)} = \mathrm{Fix}(\sigma^2)$. □

6.1.3 $\deg(f) = 4$

Let $f(t) \in K[t;\sigma]$ be monic of degree $m = 4$. Then $L^{(\sigma,f)} = \bigcap_{\lambda_j \in \Lambda} \mathrm{Fix}(\sigma^{4-\lambda_j})$ by Proposition 71.

(1) If $f(t) = t^4 - a_0$ with $a_0 \in K^\times$ then $L^{(\sigma,f)} = \mathrm{Fix}(\sigma^4)$.

(2) If $f(t) = t^4 - a_1 t$ with $a_1 \in K^\times$ then $L^{(\sigma,f)} = \mathrm{Fix}(\sigma^3)$.

(3) If $f(t) = t^4 - a_2 t^2$ with $a_2 \in K^\times$ then $L^{(\sigma,f)} = \mathrm{Fix}(\sigma^2)$.

(4) If $f(t) = t^4 - a_2 t^2 - a_0$ with $a_0, a_2 \in K^\times$, then $L^{(\sigma,f)} = \mathrm{Fix}(\sigma^4) \cap \mathrm{Fix}(\sigma^2) = \mathrm{Fix}(\sigma^2)$.

(5) In all other cases, $L^{(\sigma,f)} = \mathrm{Fix}(\sigma) = F$.

Observe that:

- If n is odd then $\mathrm{Fix}(\sigma^4) = \mathrm{Fix}(\sigma^2) = F$.
- If $n \equiv 0 (mod\ 4)$, then $[\mathrm{Fix}(\sigma^4) : F] = 4$.

- If $n \equiv 2(mod\ 4)$, then $[\mathrm{Fix}(\sigma^4) : F] = 2$.
- If $n \equiv 0(mod\ 3)$, then $[\mathrm{Fix}(\sigma^3) : F] = 3$.
- If $n \equiv 1$ or $2(mod\ 3)$, then $\mathrm{Fix}(\sigma^3) = F$.
- If $n \equiv 0(mod\ 2)$ then $[\mathrm{Fix}(\sigma^2) : F] = 2$.

The above cases for n are not mutually exclusive.

Proposition 85. *(i) If $f(t) = t^4 - a_0 \in F[t]$ with $0 \neq a_0$, then the subalgebra*

$$\mathrm{Fix}(\sigma^4)[t;\sigma]/\mathrm{Fix}(\sigma^4)[t;\sigma]f(t)$$

of the right nucleus of S_f has dimension $4[\mathrm{Fix}(\sigma^4) : F] = 4\gcd(n,4)$ over F. In particular:
(a) If f is irreducible, not right-invariant and either $n \neq 2$ is prime or $\gcd(n,4) = 1$, and $f(t) \neq t$, then

$$\mathrm{Nuc}_r(S_f) \cong \mathrm{Fix}(\sigma^4)[t;\sigma]/\mathrm{Fix}(\sigma^4)[t;\sigma]f(t).$$

(b) If f is not right-invariant and $n = 2$, then f is reducible.
(ii) If $f(t) = t^4 - a_1 t \in F[t;\sigma]$ with $0 \neq a_1$, then the subalgebra

$$\mathrm{Fix}(\sigma^3)[t;\sigma]/\mathrm{Fix}(\sigma^3)[t;\sigma]f(t)$$

of the right nucleus of S_f has dimension $4[\mathrm{Fix}(\sigma^3) : F] = 4\gcd(n,3)$ over F.
(iii) If $f(t) = t^4 - a_2 t - a_0 \in F[t;\sigma]$ with $0 \neq a_2$, then the subalgebra

$$\mathrm{Fix}(\sigma^2)[t;\sigma]/\mathrm{Fix}(\sigma^2)[t;\sigma]f(t)$$

of the right nucleus of S_f has dimension $4[\mathrm{Fix}(\sigma^2) : F] = 4\gcd(n,2)$ over

F. In particular:

(a) If f is irreducible, not right-invariant and either $n \neq 2$ is prime or $\gcd(n,4) = 1$, *and $f(t) \neq t$, then*

$$\mathrm{Nuc}_r(S_f) \cong \mathrm{Fix}(\sigma^2)[t;\sigma]/\mathrm{Fix}(\sigma^2)[t;\sigma]f(t).$$

(b) If f is not right-invariant and $n = 2$, $f(t) \neq t$, then f is reducible.

Proof. $L^{(\sigma,f)}[t;\sigma]/L^{(\sigma,f)}[t;\sigma]f(t) \subset \mathrm{Nuc}_r(S_f)$ by Theorem 64.
(i) Here $L^{(\sigma,f)} = \mathrm{Fix}(\sigma^4)$ by (1), and thus

$$\mathrm{Fix}(\sigma^4)[t;\sigma]/\mathrm{Fix}(\sigma^4)[t;\sigma]f(t) \subset \mathrm{Nuc}_r(S_f).$$

(ii) We know $L^{(\sigma,f)} = \mathrm{Fix}(\sigma^3)$ by (2), and hence

$$\mathrm{Fix}(\sigma^3)[t;\sigma]/\mathrm{Fix}(\sigma^3)[t;\sigma]f(t) \subset \mathrm{Nuc}_r(S_f).$$

(iii) We have $L^{(\sigma,f)} = \mathrm{Fix}(\sigma^2)$ by (3), and so

$$\mathrm{Fix}(\sigma^2)[t;\sigma]/\mathrm{Fix}(\sigma^2)[t;\sigma]f(t) \subset \mathrm{Nuc}_r(S_f).$$

□

6.2 Conclusion

Let K/F be a cyclic Galois extension of degree n with Galois group $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. We assume that n is either prime or that $\gcd(m,n) = 1$ for m the degree of the polynomial f we look at. For certain types of skew polynomials $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in K[t;\sigma]$ such that $\hat{h}(x) \neq x$ and $(f,t)_r = 1$ which are not right-invariant, we can decide if they are

reducible based on the following "algorithm" with output $\boxed{\text{TRUE}}$ if f is reducible and $\boxed{\text{STOP}}$ if we cannot decide:

(1) If $f \in F[t]$ then: if f is not right-invariant and f is reducible in $F[t]$, then f is reducible in $K[t;\sigma]$ $\boxed{\text{TRUE}}$, else $\boxed{\text{STOP}}$. If $f \notin F[t]$ then go to (2).

(2) Compute $L = L^{(\sigma,f)} = \text{Fix}(\sigma^d)$, where $d = \gcd(m - \lambda_1, m - \lambda_2, \ldots, m - \lambda_r, n)$.
If $[L : F] > m$, then f is reducible $\boxed{\text{TRUE}}$.
If $[L : F] \leq m$ then go to (3).

(3) Find the smallest integer ρ, such that $a_i \in \text{Fix}(\sigma^\rho)$ for all i, and such that $\text{Fix}(\sigma^\rho)$ is a proper subfield of K.
If $\text{Fix}(\sigma^\rho) = L$ then f is reducible $\boxed{\text{TRUE}}$.
If $m = q\rho$ and $[L : F] > \rho$, then f is reducible $\boxed{\text{TRUE}}$.
If $m = q\rho + r$ with $0 < r < \rho$, and $[L : F] \geq \rho$ then f is reducible $\boxed{\text{TRUE}}$.
In all other cases, go to (4).

(4) If all a_i are not contained in a proper subfield of K, then we *cannot decide* if f is reducible $\boxed{\text{STOP}}$.

Furthermore, if $f(t) \in F[t]$ then we can use the fact that

$$L^{(\sigma,f)}[t;\sigma]/L^{(\sigma,f)}[t;\sigma]f(t)$$

is a subalgebra of $\text{Nuc}_r(S_f)$ to look for zero divisors in $\text{Nuc}_r(S_f)$ in order to factor f.

Chapter 7

When is the Eigenring of f a Central Simple Algebra over F?

Let K be a field of characteristic 0 and $R = K[t;\delta]$ be the ring a differential polynomials with coefficients in K. In order to derive results on the structure of the left R-modules R/Rf, Amitsur studied spaces of linear differential operators via differential transformations [Ami53, Ami54, Ami55]. He observed that every central simple algebra B over a field F of characteristic 0 that is split by an algebraically closed field extension K of F, is isomorphic to the eigenring [1] of some polynomial $f \in K[t;\delta]$, for a suitable derivation δ of K. This identification of a central simple algebra B with a suitable differential polynomial $f \in K[t;\delta]$ he called A-polynomial also holds when K has prime characteristic p [Ami53, Section 10], [Pum18]. Let D be a central division algebra of degree d over its center C, σ an endomorphism of D and δ a left σ-derivation of D. Our aim is to provide a partial answer to the following generalisation of Amitsur's investigation:

[1] Amitsur refers to the eigenring of f as the invariant ring of f in [Ami54]

"For which polynomials f in a skew polynomial ring $D[t;\sigma,\delta]$ is the eigenring $\mathcal{E}(f)$ a central simple algebra over its subfield $F = C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$?"

After a brief review of the Amitsur's theory in Section 7.1, we investigate three different setups, always assuming that f has degree $m \geq 1$ and that the minimal central left multiple of f is square-free. We look at generalised A-polynomials in $D[t;\sigma]$ in Section 7.2, where σ is an automorphism of D of finite inner order n with $\sigma^n = \iota_u$ for some $u \in D^\times$. In Section 7.3, we study generalised A-polynomials in $D[t;\delta]$ where C has characteristic 0 and δ is the inner derivation δ_c in D for some $c \in D$. Finally, in Section 7.4, we investigate A-polynomials in $D[t;\delta]$ where C has prime characteristic p and δ is an algebraic derivation of D with minimum polynomial $g \in F[t]$ of degree p^e such that $g(\delta) = \delta_c$ for some $c \in D$. The contents of this chapter will also appear in [OP21].

7.1 Differential Transformations and Amitsur's A-polynomials

All of the definitions and results in this section can be found in [Ami54] unless stated otherwise, although some are attributed to Jacobson, and have appeared earlier in [Jac37].

Let K be a field of any characteristic, σ be an automorphism of K, δ be a left σ-derivation of K, and let $F = \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$. Let V be a vector space over K of dimension m. A *pseudo-linear transformation* (p.l.t.) of V is an additive map $T : V \longrightarrow V$ such that

$$T(av) = \sigma(a)T(v) + \delta(a)v.$$

The ring of transformations in V generated by T and the elements of K is equal to the polynomial ring $K[T]$. For the rest of this section we focus only on the case $\sigma = \mathrm{id}_K$, in which case (K, δ) is a differential field, and we call the p.l.t. T a *differential transformation* (d.t.). The ring $K[T]$ of polynomials in T is then a ring of left differential operators on V, and we write $V = (V, T)$ to make clear this association.

Given a basis $(b_1, \ldots, b_m)$ of V we can represent the d.t. T by a matrix $B(T) = (a_{ij}) \in M_m(K)$, where the entries a_{ij} are determined by the images of the basis vectors b_i under T, i.e.

$$T(b_i) = \sum_{j=0}^{m} a_{ij} b_j.$$

If we write $B = B(T)$, then

$$(V, T) \cong \frac{K[t;\delta]}{K[t;\delta]g_1(t)} \times \frac{K[t;\delta]}{K[t;\delta]g_2(t)} \times \cdots \times \frac{K[t;\delta]}{K[t;\delta]g_m(t)},$$

where $g_1, \ldots, g_m \in K[t;\delta]$ are the invariant factors of the matrix $B - tI_m$.

Additionally, we assume from now on that K has characteristic zero for the remainder of the section. In this case the matrix $(B - tI_m)$ has only one proper invariant factor [Jac37, p. 499] and

$$(V, T) \cong \frac{K[t;\delta]}{K[t;\delta]g(t)}$$

for some $g \in K[t;\delta]$ of degree m. We call the polynomial $g(t)$ the *characteristic polynomial* of both the matrix A and the differential transformation T, and we note that the characteristic polynomial of any differential transformation is unique up to similarity. On the other hand, for any differential polynomial $f \in R$ of degree m, write $V_f = K[t;\delta]/K[t;\delta]f(t)$.

Then V_f is a K-vector space of dimension m, and $f(t)$ is the characteristic polynomial of the differential transformation T on V_f defined by $p(t) \mapsto tp(t)$. Now let V' be a vector space over K of dimension m' equipped with a differential transformation T'. We define a differential transformation $T \times T'$ on the tensor product space $V \otimes_K V'$ by

$$(T \times T')(u) = (T \times T')(\sum_i v_i \otimes v_i') = \sum_i T(v_i) \otimes v_i' + \sum_j v_j \otimes T'(v_j'),$$

for all $u = \sum_i v_i \otimes v_i' \in V \otimes_K V'$. Related to this 'product' differential transformation, Amitsur also introduced the related notion for characteristic polynomials. The so-called resultant is defined in the following way:

Definition 86. *Let $f, g \in K[t;\delta]$ be the characteristic polynomials of the differential transformations T and T' respectively. Then the resultant of f and g, denoted by $f \times g$, is defined as the characteristic polynomial of the differential transformation $T \times T'$ over $V \otimes_K V'$.*

Remark. *In the notation of Definition 86, with $\deg(f) = m$ and $\deg(g) = m'$, the resultant $f \times g$ is a differential polynomial of degree mm' uniquely determined up to similarity.*

For $r \in \mathbb{N}$, we denote by $e_r(t)$ a fixed characteristic polynomial of the $r \times r$ zero matrix.

Definition 87. *Let $f \in R$ have degree m. Then f is called an A-polynomial if there exists some polynomial $g \in R$, such that $f \times g \sim e_{mn}(t)$, where $n = \deg(g)$.*

Theorem 88. *(1) If $f \in K[t;\delta]$ is an A-polynomial, and $f \sim g$, then g is also an A-polynomial.*

(2) If $f, g \in K[t;\delta]$ are A-polynomials, then the resultant $f \times g$ is an A-polynomial.

(3) *If $f, g \in K[t;\delta]$ are A-polynomials such that $f \sim g$, and $f \times p \sim g \times q$ for some $p, q \in K[t;\delta]$, then $p \sim q$.*

(4) *If $f \in K[t;\delta]$ is an A-polynomial, then $f \sim g \times e_r(t)$ for some $r \in \mathbb{N}$ and some irreducible A-polynomial $g \in R$ uniquely determined up to similarity.*

(5) *If $f \in K[t;\delta]$ is an A-polynomial and $f \sim g \times h$ or $f = gh$ for some $g, h \in K[t;\delta]$, then g and h are also A-polynomials.*

In fact, the set of all A-polynomials in $K[t;\delta]$, denoted by $\mathcal{A}(K,\delta)$, forms a semigroup under the product $\times$ (i.e. if $f, g \in \mathcal{A}(K,\delta)$, we take $f \times g$ to be their product in $\mathcal{A}(K,\delta)$) and the relation $\sim$ (similarity of polynomials in $K[t;\delta]$), with the polynomial t acting as the identity in $\mathcal{A}(K,\delta)$. In [Ami53] it is shown that the A-polynomials are precisely the polynomials in $K[t;\delta]$ such that $\mathcal{E}(f)$ is a central simple algebra over F of degree $m = \deg(f)$, which is split by K. Below are the main results relating such A-polynomials to central simple algebras:

Theorem 89. *(1) If $f, g \in K[t;\delta]$ are A-polynomials, then $h = f \times g$ is an A-polynomial, and*

$$\mathcal{E}(h) \cong \mathcal{E}(f) \otimes_F \mathcal{E}(g).$$

(2) *If $f \in K[t;\delta]$ is an A-polynomial of degree m, then $\mathcal{E}(f)$ is a central simple algebra over F of degree m, which is split by K.*

(3) *Every central simple algebra over F of degree m which is split by K, is isomorphic to $\mathcal{E}(f)$ for some A-polynomial $f \in K[t;\delta]$ of degree m.*

Suppose instead that we take F to be a field of characteristic $p \neq 0$, with K a finite purely inseparable field extension of exponent 1, i.e.

$K^p \subseteq F \subset K$. Then the theory of differential transformations also holds in the setting. The related theory of A-polynomials and central simple algebras holds when the A-polynomial $f \in K[t;\delta]$ involved has degree $m < [K : F] = p^e$ for some $e \in \mathbb{N} \cup \{\infty\}$ (with slight abuse of notation writing $e = \infty$ for $[K : F] = \infty$). In particular, we note that the results of Theorem 89 hold in this setting, for A-polynomials f of degree $m < [K : F]$, and for central simple algebras over F of degree m which are split by K, satisfying $m < [K : F]$ [Ami54, Section 10]. This is the most important case that we can say more on.

7.2 Generalised A-polynomials

For $f \in D[t;\sigma,\delta]$ we are interested in answering the question:

"When is $\mathcal{E}(f)$ a central simple algebra over the field
$F = C \cap \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$?"

To this end we define a generalised A-polynomial as follows:

Definition 90. *Let $f \in D[t;\sigma,\delta]$. We call f a generalised A-polynomial if $\mathcal{E}(f)$ is a central simple algebra over F.*

If D is commutative (i.e. a field), then $d = 1$ and without loss of generality we can take $\sigma = \mathrm{id}_D$ or $\delta = 0$. Then a polynomial f in $D[t;\sigma]$ (resp. $D[t;\delta]$) is a generalised A-polynomial if $\mathcal{E}(f)$ is a central simple algebra over $F = \mathrm{Fix}(\sigma)$ (resp. $F = \mathrm{Const}(\delta)$).

For each $v \in D^\times$, we define a map $\Omega_v : D \longrightarrow D$ by

$$\Omega_v(\alpha) = \sigma(v)\alpha v^{-1} + \delta(v)v^{-1}.$$

If D is commutative, we note that $\delta = 0$ yields $\Omega_v(\alpha) = \sigma(v)\alpha v^{-1}$ and $\sigma = \mathrm{id}$ yields $\Omega_v(\alpha) = \alpha + \delta(v)v^{-1}$ for all $v \in D^\times$.

The following is an easy consequence of the definition of similarity of skew polynomials in R, and will prove to be very useful:

Lemma 91. *[Ami54, Lemma 2 for $\sigma = \mathrm{id}$] Let $\alpha, \beta \in D$. Then $(t-\alpha) \sim (t-\beta)$ in $D[t;\sigma,\delta]$ if and only if $\Omega_v(\alpha) = \beta$ for some $v \in D^\times$.*

Proof. $(t-\alpha) \sim (t-\beta)$ is equivalent to the existence of $v, w \in D^\times$ such that $w(t-\alpha) = (t-\beta)v$ [Jac43, pg. 33], i.e. there exists $v, w \in D^\times$ such that

$$w(t-\alpha) = \sigma(v)t + \delta(v) - \beta v.$$

This is the case if and only if $w = \sigma(v)$ and $w\alpha = \sigma(v)\alpha = \beta v - \delta(v)$. The result follows immediately. □

7.3 Generalised A-polynomials in $D[t;\sigma]$

Let R denote the twisted polynomial ring $D[t;\sigma]$ with D a central division algebra over C of degree d and σ an automorphism of D. We assume that σ has finite inner order n, with $\sigma^n = \iota_u$ for some $u \in D^\times$.

Recall that R has center $F[u^{-1}t^n] \cong F[x]$. For the remainder of this section we suppose that $f \in R$ is a monic polynomial of degree $m \geq 1$ such that $(f,t)_r = 1$. Then f has a unique minimal central left multiple $h(t) = \hat{h}(u^{-1}t^n)$ for some $\hat{h} \in F[x]$ of degree at most dm. Since $(f,t)_r = 1$, the polynomial $h(t)$ is a bound of f.

We aim to provide some necessary, and some sufficient conditions for $f \in R$ to be a generalised A-polynomial.

First suppose that

$$\hat{h}(x) = \hat{\pi}_1(x)^{e_1}\hat{\pi}_2(x)^{e_2}\cdots\hat{\pi}_z(x)^{e_z}$$

for some irreducible polynomials $\hat{\pi}_1, \hat{\pi}_2, \ldots \hat{\pi}_z \in F[x]$ such that $\hat{\pi}_i \neq \hat{\pi}_j$ for $i \neq j$, and some exponents $e_1, e_2, \ldots, e_z \geq 1$, and let $\pi_i(t) = \hat{\pi}_i(u^{-1}t^n)$ for each $i = 1, 2, \ldots, z$.

We assume that the decomposition of $\hat{h}$ is square-free, i.e. that $e_1 = e_2 = \cdots = e_z = 1$ and

$$\hat{h}(x) = \hat{\pi}_1(x)\hat{\pi}_2(x)\cdots\hat{\pi}_z(x).$$

By Theorem 53, $\mathcal{E}(f)$ has center $E_{\hat{h}} = F[x]/(\hat{h}(x))$, and by the Chinese Remainder Theorem for commutative rings (see for example [Coh63, §5])

$$E_{\hat{h}} \cong E_{\hat{\pi}_1} \oplus E_{\hat{\pi}_2} \oplus \cdots \oplus E_{\hat{\pi}_z},$$

where $E_{\hat{\pi}_i} = F[x]/(\hat{\pi}_i(x))$ for each i. Hence $\mathcal{E}(f)$ has center F if and only if $E_{\hat{\pi}_1} \oplus E_{\hat{\pi}_2} \oplus \cdots \oplus E_{\hat{\pi}_z} = F$, which is true if and only if $z = 1$ and $E_{\hat{\pi}_1} = F$. Therefore we can assume $\hat{h}$ is irreducible in $F[x]$ without loss of generality, and apply the results of Chapter 2.

In particular by Theorem 20, for $f \in R$ with $\hat{h} \in F[x]$ irreducible, we have that $f = f_1 f_2 \cdots f_l$ for $f_1, f_2, \ldots, f_l \in R$ irreducible polynomials, which are all similar to each other (i.e. $f_i \sim f_j$ for all i, j). Moreover

$$\mathcal{E}(f) \cong M_l(\mathcal{E}(f_i)),$$

and $\mathcal{E}(f_i)$ is a central division algebra over $E_{\hat{h}}$ of degree $s' = \frac{dn}{k}$, $\deg(\hat{h}) =$

$\frac{dm}{ls'}$, and $[\mathcal{E}(f_i) : F] = \frac{dms'}{l}$ where k is the number of irreducible factors of h in any complete factorisation in R. Hence, $\mathcal{E}(f)$ is a central simple algebra over $E_{\hat{h}}$ of degree $s = ls'$ and $[\mathcal{E}(f) : F] = dms$.

After considering the above we are left almost immediately with the following result:

Theorem 92. *Suppose that $\hat{h}(x)$ is irreducible in $F[x]$. Then f is a generalised A-polynomial in R if and only if $\hat{h}(x) = x - a$ for some $a \in F$ if and only if f right divides $u^{-1}t^n - a$ for some $a \in F$. In particular, if f is a generalised A-polynomial, then $m \leq n$.*

Proof. Suppose that f is a generalised A-polynomial in R. By the discussion preceding this result, for f to be a generalised A-polynomial it is necessary that $\hat{h}(x) = x - a$ for some $a \in F$. Conversely if $\hat{h}(x) = x - a \in F[x]$, then $E_{\hat{h}} = F[x]/(x - a) = F$. Hence $\mathcal{E}(f)$ is a central simple algebra over F by Theorem 20, i.e. f is a generalised A-polynomial. It is easy to see that $\hat{h}(x) = x - a$ is equivalent to f being a right divisor of $u^{-1}t^n - a$ by definition of the minimal central left multiple. Moreover, if f right divides $u^{-1}t^n - a$, then $\deg(f) \leq n$. □

For n prime we are able to provide a more concrete description of f:

Theorem 93. *Suppose that $\hat{h}$ is irreducible in $F[x]$. Suppose that n is prime and not equal to d. Then f is a generalised A-polynomial in R if and only if one of the following holds:*

(1) There exists some $a \in F^\times$ such that $ua \neq \prod_{j=1}^{n} \sigma^{n-j}(b)$ for every $b \in D$, and

$$f(t) = t^n - ua.$$

In this case f is an irreducible polynomial in R.

(2) $m \leq n$ *and there exist some constants* $c_1, c_2, \ldots, c_{m-1}, c_m, b \in D^\times$, *with* $c_m = 1$, *such that the product* $u^{-1}\prod_{j=0}^{n-1}\sigma^{n-j}(b)$ *lies in* $F^\times$, *and*

$$f(t) = \prod_{i=1}^{m}(t - \Omega_{c_i}(b)).$$

In this case f *is a reducible polynomial unless* $m = 1$.

Proof. By Theorem 92 f is a generalised A-polynomial in R if and only if f right divides $u^{-1}t^n - a$ for some $a \in F^\times$. So suppose that f is a generalised A-polynomial in R, then there exists some $a \in F^\times$ and some nonzero $g \in R$ such that

$$u^{-1}t^n - a = gf \tag{7.1}$$

In the notation of Theorem 20, $ldn = ks$ and since f is a generalised A-polynomial $\deg(\hat{h}) = \frac{dm}{s} = 1$, i.e. $dm = s$. Combining these yields $\frac{n}{k} = \frac{m}{l} \in \mathbb{N}$. That is k must divide n, and so we must have that $k = 1$ or $k = n$ as n is prime. We analyse the cases $k = 1$ and $k = n$ separately.

First suppose that $k = 1$, then $h(t)$ is irreducible. Therefore Equation (7.1) becomes

$$u^{-1}t^n - a = gf(t) \tag{7.2}$$

for some $a \in F^\times$ and some $g \in D^\times$. This yields $g = u^{-1}$ and $f(t) = t^n - ua$ for some $a \in F^\times$. Suppose that f were reducible, then f would be the product of n linear factors as n is prime, hence f is irreducible if and only if $ua \neq \prod_{j=1}^{n}\sigma^{n-j}(b)$ for any $b \in D$, by [Bro18, Corollary 3.4].

On the other hand, if $k = n$, then $h(t)$ is equal to a product of n linear factors in R, all of which are mutually similar to one another. Also, since

$\frac{n}{k} = \frac{m}{l}$ and $n = k$, we have $m = l \leq n$. Hence f is the product of $m \leq n$ linear factors in R, all of which are similar.

So there exist constants $b_1, b_2, \ldots, b_m \in D^\times$ such that $(t - b_i) \sim (t - b_j)$ for all $i, j \in \{1, 2, \ldots, m\}$, and

$$f(t) = \prod_{i=1}^{m} (t - b_i).$$

In particular $(t - b_i) \sim (t - b_m)$ for all $i \neq m$, which is true if and only if there exist constants $c_1, c_2, \ldots, c_{m-1}, c_m \in D^\times$ such that $b_i = \Omega_{c_i}(b_m)$ for all i by Lemma 91. Hence setting $b = b_m$ and $c_m = 1$ yields

$$f(t) = \prod_{i=1}^{m} (t - \Omega_{c_i}(b)).$$

Finally, we note that $(t - b)|_r(t^n - ua)$ for some $a \in F^\times$ if and only if $u^{-1} \prod_{j=0}^{n-1} \sigma^{n-j}(b) = a \in F^\times$, by [Bro18, Corollary 3.4]. □

So there are no generalised A-polynomials in R of degree greater than n under the assumption that $\hat{h}$ is irreducible in $F[x]$.
If $e_i > 1$ for at least one i, then it is not clear to the author when $\mathcal{E}(f)$ is a central simple algebra over the field F.

7.3.1 Generalised A-polynomials in $K[t;\sigma]$ and $\mathbb{F}_{q^n}[t;\sigma]$

Throughout this section we suppose that $R = K[t;\sigma]$ with K a field, and that σ an automorphism of K of finite order n with fixed field F. Now the center of R is $F[t^n] \cong F[x]$. Let $f \in R$ be of degree $m \geq 1$ and satisfy $(f, t)_r = 1$, and suppose that f has minimal central left multiple $h(t) = \hat{h}(t^n)$ for some irreducible polynomial $\hat{h} \in F[x]$.

Theorem 94. *f is a generalised A-polynomial in R if and only if $\hat{h}(x) = x - a$ for some $a \in F[x]$ if and only if f right divides $t^n - a$ in R. In*

particular, if f is a generalised A-polynomial in R, then $m \leq n$.

This follows from Theorem 93. In the case that n is prime, we obtain the following as an immediate corollary to both Theorem 93 and Theorem 94:

Theorem 95. *Let n be prime. Then f is a generalised A-polynomial in R if and only if one of the following holds:*

(1) There exists some $a \in F^\times$ such that $a \neq N_{K/F}(b)$ for any $b \in K$, and

$$f(t) = t^n - a.$$

In this case f is an irreducible polynomial in R.

(2) $m \leq n$ and there exist some constants $c_1, c_2, \ldots, c_{m-1}, c_m, b \in K^\times$ with $c_m = 1$, such that

$$f(t) = \prod_{i=1}^{m} (t - \Omega_{c_i}(b)).$$

Proof. The proof is identical to the proof of Theorem 93 with $d = u = 1$. We also dropped the condition that $\prod_{j=0}^{n-1} \sigma^j(b)$ lie in $F^\times$ since this product is equal to the field norm $N_{K/F}(b)$ which is always in $F^\times$ for $b \in K^\times$. □

In particular, let $K = \mathbb{F}_{q^n}$, where $q = p^e$ for some prime p and exponent $e \geq 1$, and where $\sigma : K \longrightarrow K$, $a \mapsto a^q$, is the Frobenius automorphism of order n, with fixed field $F = \mathbb{F}_q$. In this case the only central division algebra over the field $\mathbb{F}_q$ is $\mathbb{F}_q$ itself. The following result is therefore an easy consequence of Theorem 94:

Theorem 96. *Suppose that $f \in \mathbb{F}_{q^n}[t;\sigma]$ satisfies $(f,t)_r = 1$, and has minimal central left multiple $h(t) = \hat{h}(t^n)$ for some irreducible polynomial $\hat{h} \in \mathbb{F}_q[x]$. Then f is an A-polynomial if and only if $m \leq n$ and there*

exist some constants $c_1, c_2, \ldots, c_{m-1}, c_m, b \in K^\times$ *with* $c_m = 1$*, such that*

$$f(t) = \prod_{i=1}^{m}(t - \Omega_{c_i}(b)).$$

In particular, f *is a reducible polynomial in* $\mathbb{F}_{q^n}[t;\sigma]$ *unless* $m = 1$*.*

Proof. First we note that $E_{\hat{h}} = \frac{\mathbb{F}_q[x]}{(\hat{h}(x))}$ is a field extension of $\mathbb{F}_q$ of finite degree, hence it is also a finite field. In the notation of Theorem 32, $\mathcal{E}(f) \cong M_l(E_{\hat{h}})$ since the only central division algebra over the finite field $E_{\hat{h}}$ is $E_{\hat{h}}$ itself. Hence $\mathcal{E}(f)$ is a central simple algebra over $E_{\hat{h}}$ of degree $s = l$. By Theorem 32, $\deg(h) = \frac{mn}{s} = \frac{mn}{l}$. On the other hand, we know that $\deg(h) = k\deg(f_i)$ where f_i is any irreducible divisor of f in R, and $\deg(f_i) = \frac{m}{l}$. Combining the expressions for $\deg(h)$ yields $n = k$.

The rest of the proof can be taken verbatim to be the proof of Theorem 93 from the point that we examine the $n = k$ case. We note that the part of the proof of Theorem 93 that we invoke here does not rely on n being a prime. □

7.4 Generalised A-polynomials in $D[t;\delta]$

This section is dedicated to finding necessary and sufficient conditions for certain polynomials $f \in D[t;\delta]$. To do this, we focus on the cases $\mathrm{Char}(D) = 0$ and $\mathrm{Char}(D) = p \neq 0$, separately. Again, it can be seen that all of the results in this section follow from a similar argument to those use throughout the previous sections of this chapter.

7.4.1 $\mathrm{Char}(D) = 0$

In this section we impose that D has characteristic 0, and that δ is the inner derivation defined by some element $c \in D^\times$, that is $\delta(a) = [c, a] =$

$ca - ac$ for all $a \in D$.

Recall that R has center $F[t-c] \cong F[x]$ where $F = C \cap \text{Const}(\delta)$, and that all polynomials $f \in R = D[t;\delta]$ have a unique minimal central left multiple $h(t) = \hat{h}(t-c)$ for some $\hat{h} \in F[x]$, which is equal to a bound of f.

Remark. *As in the search for generalised A-polynomials in a twisted polynomial ring $D[t;\sigma]$, we restrict ourselves to the case $\hat{h}$ is square-free in $F[x]$, otherwise the author was unable to determine when the eigenring of $f \in R$ is indeed a central simple algebra over F. Then by a similar argument to Section 3 (pg. 74), we lose no generality in the search for A-polynomials in R, if we take $\hat{h}$ to be an irreducible polynomial in $F[x]$.*

By Theorem 38, for any $f \in R$ of degree $m \geq 1$ with $\hat{h} \in F[x]$ irreducible, we have that $f = f_1 f_2 \cdots f_l$ for $f_1, \ldots, f_l$ irreducible polynomials in R, which are all mutually similar to each other,

$$\mathcal{E}(f) \cong M_l(\mathcal{E}(f_i)),$$

and $\mathcal{E}(f_i)$ is a central division algebra over $E_{\hat{h}}$ of degree $s' = \frac{d}{k}$, where k is the number of irreducible factors of h in R. Moreover, $\deg(\hat{h}) = \frac{dm}{ls'}$, and $[\mathcal{E}(f_i) : F] = \frac{dms'}{l}$. Hence, $\mathcal{E}(f)$ is a central simple algebra over $E_{\hat{h}}$ of degree $s = ls'$ and $[\mathcal{E}(f) : F] = dms$.

This yields the following result almost immediately:

Theorem 97. *Suppose that $f \in R$ has degree m, and that f has minimal central left multiple $h(t) = \hat{h}(t-c)$ for some irreducible polynomial $\hat{h} \in F[x]$. Then f is a generalised A-polynomial in R if and only if $f(t) = t - (c+a)$ for some $a \in F$.*

Proof. Suppose that f is a generalised A-polynomial in R, that is $\mathcal{E}(f)$ is a central simple algebra over F of degree dm. This is true if and only if $E_{\hat{h}} = F$, i.e. if and only if $\deg(\hat{h}) = \frac{md}{s} = 1$. Having $\hat{h}$ of degree one is equivalent to having $h(t) = t - (c + a)$ for some $a \in F$, and by definition $h(t) = g(t)f(t)$ for some $g \in R$. □

Remark. *The above result shows that there are in fact no generalised A-polynomials in R with a square-free minimal central left multiple, other than the central element $t - c$ up to a possible shift by some element of F and a possible scalar multiplication by some element of $D^{\times}$.*

7.4.2 $\mathrm{Char}(D) = p > 0$

From now on let $R = D[t;\delta]$ where D is a central division algebra of degree d over C. Assume that C has prime characteristic p, and that δ is an algebraic derivation of D with minimum polynomial $g(t) = t^{p^e} + \gamma_1 t^{p^{e-1}} + \cdots + \gamma_e t \in F[t]$, such that $g(\delta)(a) = [c, a] = ca - ac$ for some nonzero $c \in D$ and for all $a \in D$. Here, $F = C \cap \mathrm{Const}(\delta)$ ($D = K$ is a field is included here as special case). Then R has center $F[g(t) - c] \cong F[x]$. For every $f \in R$, the minimal central left multiple of f in R is the unique polynomial of minimal degree $h \in C(R) = F[x]$ such that $h = gf$ for some $g \in R$, and such that $h(t) = \hat{h}(g(t) - c)$ for some monic $\hat{h} \in F[x]$. All $f \in R = D[t;\delta]$ have a unique minimal central left multiple, which is a bound of f. Again we can restrict our investigation to the case $\hat{h}$ is square-free in $F[x]$, and note that it is necessary that $\hat{h}$ be irreducible in $F[x]$ for f to be a generalised A-polynomial in R.

By Theorem 43, for any $f \in R$ of degree $m \geq 1$ with $\hat{h} \in F[x]$ irreducible, we have that $f = f_1 f_2 \cdots f_l$ for $f_1, \ldots, f_l$ irreducible polynomials in R,

which are all mutually similar to each other,

$$\mathcal{E}(f) \cong M_l(\mathcal{E}(f_i)),$$

and $\mathcal{E}(f_i)$ is a central division algebra over $E_{\hat{h}}$ of degree $s' = \frac{dp^e}{k}$, where k is the number of irreducible factors of h in R. Moreover, $\deg(\hat{h}) = \frac{dm}{ls'}$, and $[\mathcal{E}(f_i) : F] = \frac{dms'}{l}$. Hence, $\mathcal{E}(f)$ is a central simple algebra over $E_{\hat{h}}$ of degree $s = ls'$ and $[\mathcal{E}(f) : F] = dms$. We obtain the following:

Theorem 98. *f is a generalised A-polynomial in R if and only if f right divides $g(t) - (b + c)$ for some $b \in F$. In particular,* $\deg(f) \leq p^e$.

Proof. Suppose that f is a generalised A-polynomial in R, that is $\mathcal{E}(f)$ is a central simple algebra over F of degree dm. This is true if and only if $E_{\hat{h}} = F$, i.e. if and only if $\deg(\hat{h}) = \frac{md}{s} = 1$. Having $\hat{h}$ of degree one is equivalent to having $h(t) = g(t) - (b + c)$ for some $b \in F$, and by definition $h(t) = r(t)f(t)$ for some $r \in R$. □

In $D[t;\delta]$

$$(t - \alpha)^p = t^p - V_p(\alpha),\ V_p(\alpha) = \alpha^p + \delta^{p-1}(\alpha) + \nabla_\alpha \tag{7.3}$$

for all $\alpha \in D$, where ∇_α is a sum of commutators of $\alpha, \delta(\alpha), \delta^2(\alpha), \ldots, \delta^{p-2}(\alpha)$ [Jac09, pg. 17-18]. In particular, if D is commutative, then $\nabla_\alpha = 0$ and

$$V_p(\alpha) = \alpha^p + \delta^{p-1}(\alpha) \tag{7.4}$$

for all $\alpha \in D$. Using the identities $t^p = (t-\alpha)^p + V_p(\alpha)$ and $t = (t-\alpha) + \alpha$ for all $\alpha \in D$, we arrive at:

Lemma 99. *[Jac09, Proposition 1.3.25 ($e = 1$)] Let $f(t) = t^p - \gamma_1 t - \gamma \in D[t;\delta]$ and $\alpha \in D$. Then $(t-\alpha)|_r f(t)$ if and only if $V_p(\alpha) - \gamma_1\alpha - \gamma = 0$.*

The identity (7.3) can be iterated to obtain

$$(t-\alpha)^{p^i} = t^{p^i} - V_{p^i}(\alpha) \tag{7.5}$$

for all $\alpha \in D$ and all integer exponents $i \geq 1$, where

$$V_{p^i}(\alpha) = V_p^i(\alpha) = \underbrace{(V_p \circ V_p \circ \cdots \circ V_p)}_{\text{i terms}}(\alpha).$$

In a similar fashion to Lemma 99 the identities $t^{p^i} = (t-\alpha)^{p^i} + V_{p^i}(\alpha)$ and $t = (t-\alpha) + \alpha$ may be used to obtain:

Lemma 100. *[Jac09, Proposition 1.3.25] Let $f(t) = t^{p^e} + \gamma_1 t^{p^{e-1}} + \cdots + \gamma_e t - \gamma \in D[t;\delta]$ and $\alpha \in D$. Then $(t-\alpha)|_r f(t)$ if and only if*

$$V_{p^e}(\alpha) + \gamma_1 V_{p^{e-1}} + \cdots + \gamma_e \alpha - \gamma = 0.$$

If $e = 1$ (i.e. δ is an algebraic derivation of D of degree p), we can determine necessary and sufficient conditions for f to be an A-polynomial in R:

Theorem 101. *Suppose that δ has minimum polynomial $g(t) = t^p - \gamma_1 t$ and that $\hat{h}$ is irreducible in $F[x]$. Then f is a generalised A-polynomial in R if and only if one of the following holds:*

(1) $f(t) = h(t) = t^p - \gamma_1 t - (\gamma + c)$ for some $\gamma \in F$, and

$$V_p(\alpha) - \gamma_1 \alpha - (\gamma + c) \neq 0$$

for all $\alpha \in D$. In this case f is irreducible in R.

(2) $h(t) = t^p - \gamma_1 t - (\gamma + c)$ for some $\gamma \in F$, $m \leq p$ and

$$f(t) = \prod_{i=1}^{m} (t - \Omega_{c_i}(\alpha))$$

for some $c_1, c_2, \ldots, c_m, \alpha \in D^\times$ *with* $c_m = 1$ *(w.l.o.g.) such that*

$$V_p(\alpha) - \gamma_1\alpha - (\gamma + c) = 0.$$

In particular, f *is a reducible polynomial in* R *unless* $m = 1$.

Proof. By Theorem 98, f is a generalised A-polynomial in R if and only if f right divides $t^p - \gamma_1 t - (\gamma + c)$ for some $\gamma \in F$. So suppose that f is a generalised A-polynomial in R, then there exists some $\gamma \in F$ and some nonzero $f' \in R$ such that $t^p - \gamma_1 t - (\gamma + c) = f'f$. In the notation of Theorem 43, $ldp = ks$ and since f is a generalised A-polynomial, $\deg(\hat{h}) = \frac{dm}{s} = 1$, i.e. $dm = s$. Combining these yields $\frac{p}{k} = \frac{m}{l} \in \mathbb{N}$. That is k must divide p, and so we must have that $k = 1$ or $k = p$ as p is prime.

First suppose that $k = 1$, then $h(t)$ is irreducible in R and $t^p - \gamma_1 t - (\gamma + c) = f'f$ yields $f' = 1$, i.e. $f(t) = t^p - \gamma_1 t - (\gamma + c)$. Suppose that f were reducible, then f would be the product of p linear factors as p is prime, hence f is irreducible if and only if $V_p(\alpha) - \gamma_1\alpha - (\gamma + c) \neq 0$ for any $\alpha \in D$, by Lemma 99.

On the other hand, if $k = p$, then $h(t)$ is equal to a product of p linear factors in R, all of which are similar to one another. Also, since $\frac{p}{k} = \frac{m}{l}$ and $p = k$, we have $m = l \leq p$. Hence f is the product of $m \leq p$ linear factors in R, all of which are mutually similar to each other. So there exist constants $\alpha_1, \alpha_2, \ldots, \alpha_m \in D^\times$ such that $f(t) = \prod_{i=1}^{m}(t - \alpha_i)$, and $(t - \alpha_i) \sim (t - \alpha_j)$ for all $i, j \in \{1, 2, \ldots, m\}$. In particular $(t - \alpha_i) \sim (t\alpha_m)$ for all $i \neq m$, which is true if and only if there exist constants $c_1, c_2, \ldots, c_{m-1}, c_m \in D^\times$ such that $\alpha_i = \Omega_{c_i}(\alpha_m)$ for all i by Lemma 91. Hence setting $\alpha = \alpha_m$ and $c_m = 1$ yields $f(t) = \prod_{i=1}^{m}(t - \Omega_{c_i}(\alpha))$. Finally, we note that $(t - \alpha)$ right divides $t^p - \gamma_1 t - (\gamma + c)$ if and only if $V_p(\alpha) - \gamma_1\alpha - (\gamma + c) = 0$ by Lemma 99. □

In the following, $\mathbb{K}$ denotes a finite field of characteristic p and δ is an algebraic derivation of $\mathbb{K}$ with fixed field $\mathbb{F}$ and minimum polynomial $g(t) = t^{p^e} + \gamma_1 t^{p^{e-1}} + \cdots + \gamma_e t \in \mathbb{F}[t]$ such that $g(\delta) = 0$. Then $\mathbb{K}[t;\delta]$ has centre $\mathbb{F}[g(t)] \cong \mathbb{F}[x]$. In this particular case we obtain a more detailed description on the generalised A-polynomials in $\mathbb{K}[t;\delta]$.

Theorem 102. *Suppose that $f \in \mathbb{K}[t;\delta]$ has degree $m \geq 1$ and minimal central left multiple $h(t) = \hat{h}(g(t))$ for some irreducible polynomial $\hat{h} \in \mathbb{F}[x]$. Then f is a generalised A-polynomial if and only if $h(t) = g(t) - \gamma$ for some $\gamma \in \mathbb{F}$, $m \leq p^e$, and*

$$f(t) = \prod_{i=1}^{m} (t - \Omega_{c_i}(\alpha)),$$

for some $c_1, c_2, \ldots, c_{m-1}, c_m, \alpha \in \mathbb{K}^\times$ with $c_m = 1$ (w.l.o.g.), such that

$$V_{p^e}(\alpha) + \gamma_1 V_{p^{e-1}}(\alpha) + \cdots + \gamma_e \alpha - \gamma = 0.$$

In particular, f is a reducible polynomial in $\mathbb{K}[t;\delta]$ unless $m = 1$.

Proof. First we note that $E_{\hat{h}} = \frac{\mathbb{F}[x]}{(\hat{h}(x))}$ is a field extension of $\mathbb{F}$ of finite degree, hence it is also a finite field. In the notation of Theorem 43, $\mathcal{E}(f) \cong M_l(E_{\hat{h}})$ since the only central division algebra over the finite field $E_{\hat{h}}$ is $E_{\hat{h}}$ itself. Hence $\mathcal{E}(f)$ is a central simple algebra over $E_{\hat{h}}$ of degree $s = l$. By Theorem 43, $\deg(h) = \frac{mp^e}{s} = \frac{mp^e}{l}$. On the other hand, we know that $\deg(h) = k\deg(f_i)$ where f_i is any irreducible divisor of f in R, and $\deg(f_i) = \frac{m}{l}$. Combining the expressions for $\deg(h)$ yields $p^e = k$.

Now by Theorem 98, f is a generalised A-polynomial in R if and only if $f|_r(g(t) - \gamma)$ for some $\gamma \in \mathbb{F}$ which is true if and only if $h(t) = g(t) - \gamma$ for some $\gamma \in \mathbb{F}$, i.e. $\deg(\hat{h}) = 1$. Since $\deg(\hat{h}) = \frac{m}{s} = \frac{m}{l}$ we have that $m = l$, that is f is the product of m irreducible polynomials in R that are

all similar to each other. Hence there exist elements $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{K}$ such that

$$f(t) = \prod_{i=1}^{m}(t - \alpha_i)$$

and elements $c_1, c_2, \ldots, c_m \in \mathbb{K}^\times$ such that $\Omega_{c_i}(\alpha_m) = \alpha_i$ for each i by Lemma 91. We use the notation $\alpha = \alpha_m$ and without loss of generality we may take $c_m = 1$. Finally we note that $(t-\alpha)$ right divides $h(t) = g(t)-\gamma$ if and only if $V_{p^e}(\alpha) + \gamma_1 V_{p^{e-1}}(\alpha) + \cdots + \gamma_e\alpha - \gamma = 0$ by Lemma 100. $\square$

.

Bibliography

[Alb52] A. A. Albert. On nonassociative division algebras. *Transactions of the American Mathematical Society*, 72(2):296–309, 1952.

[Ami53] S. A. Amitsur. Noncommutative cyclic fields. In *Bulletin of the American Matematical Society*, volume 59, pages 522–522. American Mathematical Society 201 Charles St, Providence, RI 02940-2213, 1953.

[Ami54] S. A. Amitsur. Differential polynomials and division algebras. *Annals of mathematics*, pages 245–278, 1954.

[Ami55] S. A. Amitsur. Generic splitting fields of central simple algebras. *Annals of mathematics*, pages 8–43, 1955.

[AW12] William A. Adkins and Steven H. Weintraub. *Algebra: an approach via module theory*, volume 136. Springer Science & Business Media, 2012.

[BO13] Grégory Berhuy and Frédérique Oggier. *An introduction to central simple algebras and their applications to wireless communication*, volume 191. American Mathematical Soc., 2013.

[Bou03] Nicolas Bourbaki. *Elements of mathematics: Algebra*. Springer, 2003.

[BP18] Christian Brown and Susanne Pumplün. How a nonassociative algebra reflects the properties of a skew polynomial. *arXiv preprint arXiv:1806.04537*, 2018.

[Bro18] Christian Brown. Petit algebras and their automorphisms, 2018.

[Car69] Jean Carcanague. Quelques résultats sur les anneaux de ore. *CR Acad. Sci. Paris Sr. AB*, 269:A749–A752, 1969.

[Coh63] Paul M. Cohn. Noncommutative unique factorization domains. *Transactions of the American Mathematical Society*, 109(2):313–331, 1963.

[Dic06] Leonard Eugene Dickson. Linear algebras in which division is always uniquely possible. *Transactions of the American Mathematical Society*, 7(3):370–390, 1906.

[DO15a] Jérôme Ducoat and Frédérique Oggier. Lattice encoding of cyclic codes from skew-polynomial rings. In *Coding Theory and Applications*, pages 161–167. Springer, 2015.

[DO15b] Jérôme Ducoat and Frédérique Oggier. On skew polynomial codes and lattices from quotients of cyclic division algebras. *arXiv preprint arXiv:1506.06079*, 2015.

[Gie98] Mark Giesbrecht. Factoring in skew-polynomial rings over finite fields. *Journal of Symbolic Computation*, 26(4):463–486, 1998.

[GT12] José Gómez-Torrecillas. Basic module theory over noncommutative rings with computational aspects of operator algebras. In *International Meeting on Algebraic and Algo-*

rithmic Aspects of Differential and Integral Operators, pages 23–82. Springer, 2012.

[GTLN13] José Gómez-Torrecillas, F. J. Lobillo, and Gabriel Navarro. Computing the bound of an ore polynomial. applications to factorization. *arXiv preprint arXiv:1307.5529*, 2013.

[GWJ04] Kenneth R. Goodearl and Robert Breckenridge Warfield Jr. *An introduction to noncommutative Noetherian rings*, volume 61. Cambridge university press, 2004.

[Jac37] Nathan Jacobson. Pseudo-linear transformations. *Annals of Mathematics*, pages 484–507, 1937.

[Jac43] Nathan Jacobson. *The theory of rings*. Number 2. American Mathematical Soc., 1943.

[Jac09] Nathan Jacobson. *Finite-dimensional division algebras over fields*. Springer Science & Business Media, 2009.

[Lam06] T. Y. Lam. *Exercises in classical ring theory*. Springer Science & Business Media, 2006.

[Lan04] Serge Lang. Algebra, volume 211 of. *Graduate Texts in Mathematics*, pages 29–30, 2004.

[LLLM89] T. Y. Lam, A. Leroy, K. H. Leung, and J. Matczuk. Invariant and semi-invariant polynomials in skew polynomial rings, israel mathematics conference proceedings, 1 (1989), 247-261. *MR1029317 (90k: 16004)*, 1989.

[LS13] Michel Lavrauw and John Sheekey. Semifields from skew polynomial rings. *Advances in Geometry*, 13(4):583–604, 2013.

[MRS01] John C. McConnell, James Christopher Robson, and Lance W. Small. *Noncommutative noetherian rings*, volume 30. American Mathematical Soc., 2001.

[OP19] Adam Owen and Susanne Pumplün. The eigenspaces of twisted polynomials over cyclic field extensions. *arXiv preprint arXiv:1909.07728*, 2019.

[OP21] Adam Owen and Susanne Pumplün. A generalisation of amitsur's a-polynomials. *Communications in Mathematics*, volume 29:pages 281–289, 2021.

[Ore33] Oystein Ore. Theory of non-commutative polynomials. *Annals of mathematics*, pages 480–508, 1933.

[Ore52] Oystein Ore. The general chinese remainder theorem. *The American Mathematical Monthly*, 59(6):365–370, 1952.

[OS12] Frédérique Oggier and B. A. Sethuraman. Quotients of orders in cyclic algebras and space-time codes. *arXiv preprint arXiv:1210.7044*, 2012.

[Pet66] Jean-Claude Petit. Sur certains quasi-corps généralisant un type d'anneau-quotient. *Séminaire Dubreil. Algèbre et théorie des nombres*, 20(2):1–18, 1966.

[PS15a] Susanne Pumplün and Andrew Steele. Fast–decodable mido codes from non–associative algebras. *International Journal of Information and Coding Theory*, 3(1):15–38, 2015.

[PS15b] Susanne Pumplün and Andrew Steele. The nonassociative algebras used to build fast-decodable space-time block codes. *arXiv preprint arXiv:1504.00182*, 2015.

[Pum15a] Susanne Pumplün. Finite nonassociative algebras obtained from skew polynomials and possible applications to (f, σ, δ)-codes. *arXiv preprint arXiv:1507.01491*, 2015.

[Pum15b] Susanne Pumplün. A note on linear codes and nonassociative algebras obtained from skew-polynomial rings. *arXiv preprint arXiv:1504.00190*, 2015.

[Pum18] Susanne Pumplün. Algebras whose right nucleus is a central simple algebra. *Journal of Pure and Applied Algebra*, 222(9):2773–2783, 2018.

[SH04] Tim J. Sullivan and Charudatta Hajarnavis. Rings and modules, 2004.

[She18] John Sheekey. New semifields and new mrd codes from skew polynomial rings. *arXiv preprint arXiv:1806.00251*, 2018.

[SPO12] Andrew Steele, Susanne Pumplün, and Frédérique Oggier. Mido space-time codes from associative and nonassociative cyclic algebras. In *2012 IEEE Information Theory Workshop*, pages 192–196. IEEE, 2012.