DOI: 10.2478/auom-2023-0012
An. Şt. Univ. Ovidius Constanţa **Vol. 31(1),2023, 221–240**

The eigenspaces of twisted polynomials over cyclic field extensions

Adam Owen and Susanne Pumplün

Abstract

Let K be a field and σ an automorphism of K of order n. Employing a nonassociative algebra, we study the eigenspace of a bounded skew polynomial $f \in K[t;\sigma]$. We mainly treat the case that K/F is a cyclic field extension of degree n with Galois group generated by σ. We obtain lower bounds on the dimension of the eigenspace, and compute it in special cases as a quotient algebra. Conditions under which a monic polynomial $f \in F[t] \subset K[t;\sigma]$ is reducible are obtained in special cases.

Introduction

Let D be a unital associative division ring and $R = D[t;\sigma,\delta]$ be a skew polynomial ring, where σ is an automorphism of D and δ a left σ-derivation. Let $f \in R$ be a skew polynomial of degree $m > 1$. The associative algebra $E(f) = \{g \in R \,|\, \deg(g) < m \text{ and } fg \in Rf\}$ is the *eigenspace* of f. If f is a bounded polynomial, then the nontrivial zero divisors in the eigenspace are in one-to-one correspondence with the irreducible factors of f in $D[t;\sigma,\delta]$, cf. for instance [10]. Therefore eigenspaces of skew polynomials regularly appear whenever skew polynomials are factorized, e.g. in results on computational aspects of operator algebras, or in algorithms factoring skew polynomials over $\mathbb{F}_q(t)$ or over $\mathbb{F}_q$, cf. [7, 8, 11, 12]. For skew polynomial rings over local fields of

Key Words: Skew polynomial ring, reducible skew polynomials, eigenspace, nonassociative algebra.
2010 Mathematics Subject Classification: Primary: 17A35; Secondary: 17A60, 17A36, 16S36
Received: 17.06.2022
Accepted: 20.09.2022

positive characteristic, where the Brauer group is non-trivial, the irreducibility of a skew polynomial is equivalent to understanding a ring isomorphism to a full matrix ring over a field extension of the local field. This problem is not completely solved in the non-split case. Partial results have been obtained e.g. in [9].

The eigenspace of f also appears implicitly in classical constructions by Amitsur [1, 2, 3], but was never recognized as the right nucleus of some nonassociative algebra.

In this paper, we investigate eigenspaces using a class of unital nonassociative algebras S_f defined by Petit [17, 18], which canonically generalize the quotient algebras R/Rf obtained when factoring out a right invariant $f \in R$. The algebra $S_f = D[t;\sigma,\delta]/D[t;\sigma,\delta]f$ is defined on the additive subgroup $\{h \in R \,|\, \deg(h) < m\}$ of R by using right division by f to define the algebra multiplication via $g \circ h = gh \bmod_r f$. Petit's algebras were studied in detail in [17, 18], and for K a finite field (hence w.l.o.g. $\delta = 0$) in [15]. Indeed, the algebra S_f with $f(t) = t^2 - i \in \mathbb{C}[t;^-]$, $^-$ the complex conjugation, already appeared in [6] as the first example of a nonassociative division algebra. The right nucleus of S_f is the eigenspace of f, if f is not linear. Thus the eigenspace of f is an associative subalgebra of S_f.

We concentrate on the case that $R = K[t;\sigma]$, where K/F is a cyclic Galois extension of degree n with Galois group generated by σ, and find conditions under which a monic polynomial $f \in R$ is reducible.

In Section 1, we introduce our terminology and some results we need later. In Section 2 we determine when a power of t lies in the right nucleus. This yields some lower bounds on the dimension of the right nucleus as an F-vector space. These bounds can then later be used to decide if certain polynomials f of degree m which are not right invariant are reducible. Let $f \in R$ be a bounded monic polynomial that is not right invariant with $\mathrm{gcrd}(f,t) = 1$, and minimal central left multiple $h(t) = \hat{h}(t^n)$, $\hat{h}(x) \in F[x]$ monic. We show that for $f \in F[t] \subset K[t;\sigma]$, the quotient algebra $\mathrm{Nuc}(S_f)[t;\sigma]/\mathrm{Nuc}(S_f)[t;\sigma]f$ is a subalgebra of $\mathrm{Nuc}_r(S_f)$ (Theorem 10). In particular if $f \in F[t] \subset K[t;\sigma]$ is bounded and we have $\mathrm{Nuc}_r(S_f) = \mathrm{Nuc}(S_f)[t;\sigma]/\mathrm{Nuc}(S_f)[t;\sigma]f$, then f is irreducible in R, if and only if f is irreducible in $\mathrm{Nuc}(S_f)[t;\sigma]$. In Section 3 we look at the nucleus of S_f for $f \in R$. Since $\mathrm{Nuc}(S_f) = \mathrm{Nuc}_r(S_f) \cap K$, this helps us to understand which elements of K lie in $\mathrm{Nuc}_r(S_f)$. In Section 4 we assume only that $\hat{h}$ is irreducible in $F[x]$ and obtain some partial results for this case as well. In Section 5, we look at the right nucleus of S_f for low degree polynomials in $F[t] \subset K[t;\sigma]$, and in Section 6, we summarize for which types of skew polynomials which are not right invariant we can decide if they are reducible using our methods.

Note that cyclotomic extensions where $F = \mathbb{Q}$ and $K = \mathbb{Q}(\eta)$, with η a primitive p^nth root of unity and p prime, which have Galois group $\mathbb{Z}/p^n\mathbb{Z}$, and Kummer extensions $K = F(\sqrt[r]{a})$ of F, where F contains a primitive rth root of unity μ and $\sigma(\sqrt[r]{a}) = \mu\sqrt[r]{a}$, are examples of skew polynomial rings that are employed in coding theory (e.g. in space-time block coding or for certain linear codes), where both reducible and irreducible f are needed.

This work is part of the first author's PhD thesis [16] written under the supervision of the second author. For more general results on eigenspaces of skew polynomials $f \in D[t; \sigma, \delta]$ the reader is referred to [16].

1 Preliminaries

1.1 Nonassociative algebras

Let F be a field and let A be an F-vector space. A is an *algebra* over F if there exists an F-bilinear map $A \times A \to A$, $(x, y) \mapsto x \cdot y$, denoted simply by juxtaposition xy, the *multiplication* of A. An algebra A is *unital* if there is an element in A, denoted by 1, such that $1x = x1 = x$ for all $x \in A$. We will only consider unital algebras.

Associativity in A is measured by the *associator* $[x, y, z] = (xy)z - x(yz)$. The *left nucleus* of A is defined as $\text{Nuc}_l(A) = \{x \in A \mid [x, A, A] = 0\}$, the *middle nucleus* of A is $\text{Nuc}_m(A) = \{x \in A \mid [A, x, A] = 0\}$ and the *right nucleus* of A is defined as $\text{Nuc}_r(A) = \{x \in A \mid [A, A, x] = 0\}$. $\text{Nuc}_l(A)$, $\text{Nuc}_m(A)$, and $\text{Nuc}_r(A)$ are associative subalgebras of A. Their intersection $\text{Nuc}(A) = \{x \in A \mid [x, A, A] = [A, x, A] = [A, A, x] = 0\}$ is the *nucleus* of A. $\text{Nuc}(A)$ is an associative subalgebra of A containing F and $x(yz) = (xy)z$ whenever one of the elements x, y, z lies in $\text{Nuc}(A)$. Commutativity in A is measured by the *commutator* $[x, y] = xy - yx$. The subspace of A defined by $\text{Comm}(A) = \{x \in A : [x, y] = 0 \text{ for all } y \in A\}$ is called the *commutator* of A. The *center* of A is $C(A) = \text{Nuc}(A) \cap \text{Comm}(A)$.

An F-algebra $A \neq 0$ is called a *division algebra* if for any $a \in A$, $a \neq 0$, both the left multiplication with a, $L_a(x) = ax$, and the right multiplication with a, $R_a(x) = xa$, are bijective. If A has finite dimension over F, A is a division algebra if and only if A has no zero divisors [19, pp. 15, 16].

1.2 Twisted polynomial rings $K[t; \sigma]$

Let K be a field and σ an automorphism of K with fixed field $F = \text{Fix}(\sigma) = \{a \in K : \sigma(a) = a\}$. The *twisted polynomial ring* $R = K[t; \sigma]$ is the set of polynomials $a_0 + a_1t + \cdots + a_nt^n$ with $a_i \in K$, where addition is defined term-wise and multiplication by $ta = \sigma(a)t$ for all $a \in K$. For $f = a_0 + a_1t + \cdots + a_nt^n$ with $a_n \neq 0$ define the *degree* of f to be $\deg(f) = n$, by convention $\deg(0) = -\infty$. Then $\deg(fg) = \deg(f) + \deg(g)$. An element $f \in R$ of degree m is *irreducible* in R if it is not a unit and it has no proper factors, i.e if there do not exist $g, h \in R$ such that $\deg(g), \deg(h) < \deg(f)$ and $f = gh$.

R is a left and right principal ideal domain and there is a right division algorithm in R: for all $g, f \in R$, $g \neq 0$, there exist unique $q, r \in R$ with $\deg(r) < \deg(f)$, such that $g = qf + r$ [13, p. 3 and Proposition 1.1.14].

A twisted polynomial $f \in R$ is *bounded* if there exists a nonzero polynomial $f^* \in R$, such that Rf^* is the largest two-sided ideal of R contained in Rf^*. The polynomial f^* is uniquely determined by f up to scalar multiplication by elements in $K^\times$. f^* is called the *bound* of f. The *left idealiser* of $f \in R$ is the set $I(f) = \{g \in R \,|\, fg \in Rf\}$, which is the largest subring of R within which Rf is a two-sided ideal. The *eigenspace* of f is the quotient ring $E(f) = I(f)/Rf = \{g \in R \,|\, \deg(g) < m \text{ and } fg \in Rf\}$.

1.3 Nonassociative algebras obtained from twisted polynomial rings

From now on, let $f \in R$ have positive degree m, and for $g \in R$ let $g \,\mathrm{mod}_r f$ denote the remainder of g upon right division by f. The set $\{g \in R \,|\, \deg(g) < m\}$ endowed with the usual term-wise addition of polynomials and the multiplication $g \circ h = gh \,\mathrm{mod}_r f$ is a unital nonassociative ring S_f. We usually will simply use juxtaposition for the multiplication in S_f. S_f is a unital nonassociative algebra over $F_0 = \{a \in K \,|\, ag = ga \text{ for all } g \in S_f\} = \mathrm{Comm}(S_f) \cap K$. F_0 is a subfield of K [17]. S_f is called a *Petit algebra*. It can be easily seen that $F_0 = \mathrm{Fix}(\sigma)$, see [5, pg. 6]. For all $a \in K^\times$ we have $S_f = S_{af}$, and if $f \in R$ has degree 1 then $S_f \cong K$. In the following, we thus assume that f is monic and that it has degree $m \geq 2$, unless specifically mentioned otherwise. S_f is associative if and only if f is *right invariant*, i.e. Rf a two-sided ideal in R. In that case, S_f is equal to the classical associative quotient algebra $R/(f)$. Note that $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ is right invariant if and only if $a_i \in F$ and $\sigma^m(d)a_i = a_i\sigma^i(d)$ for all $i \in \{0, 1, \dots, m-1\}$ and for all $d \in K$ [17, (15)]. In other words, f is right invariant in R if and only if $f(t) = g(t)t^n$ for some $g \in C(R)$ and some integer $n \geq 0$ [13, Theorem 1.1.22].
If S_f is not associative then $\mathrm{Nuc}_l(S_f) = \mathrm{Nuc}_m(S_f) = K$ and $C(S_f) = F$. Moreover,

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

is the eigenspace of $f \in R$ [17].

S_f is a division algebra, if and only if f is irreducible, if and only if $\mathrm{Nuc}_r(S_f)$ is a division algebra. It is well known that each nontrivial zero divisor q of f in $\mathrm{Nuc}_r(S_f)$ gives a proper factor $\mathrm{gcrd}(q, f)$ of f, e.g. see [10], where $\mathrm{gcrd}(q, f)$ denotes the greatest common right divisor of q and f in R.
If $f(t) \in F[t] \subset R$, then $F[t]/(f)$ is a commutative subring of $\mathrm{Nuc}_r(S_f)$, and

a field extension of F of degree m if f is irreducible as a polynomial in $F[t]$ [4, Proposition 2].

1.4 The right nucleus of S_f for irreducible f

Throughout this section we assume that σ has finite order $n > 1$. Then R has center $C(R) = F[t^n] \cong F[x]$, where $x = t^n$ [13, Theorem 1.1.22].
For any bounded $f \in R$ we define the *minimal central left multiple of f in R* as the unique polynomial of minimal degree $h \in F[t^n]$ such that $h = gf$ for some $g \in R$, and such that $h(t) = \hat{h}(t^n)$ for some monic $\hat{h} \in F[x]$. If the greatest common right divisor $\mathrm{gcrd}(f, t)$ of f and t is one, then $f^* \in C(R)$ [10, Lemma 2.11]), and the minimal central left multiple of f equals f^* up to a scalar multiple from $K^\times$. From now on we therefore assume that f is bounded with

$$\mathrm{gcrd}(f, t) = 1$$

and denote the minimal central left multiple of f by $h(t) = \hat{h}(t^n)$ with $\hat{h}(x) \in F[x]$ monic.

If f is irreducible in R, then $\hat{h}(x)$ is irreducible in $F[x]$. If $\hat{h}$ is irreducible in $F[x]$, then h generates a maximal two-sided ideal Rh in R [13, p. 16] and $f = f_1 \cdots f_r$ for irreducible $f_i \in R$ such that $f_i \sim f_j$ for all i, j (for a proof see [22] or [16]).

The quotient algebra R/Rh has the commutative F-algebra $C(R/Rh) \cong F[x]/(\hat{h}(x))$ of dimension $deg(\hat{h})$ over F as its center, cf. [10, Lemma 4.2]. Define $E_{\hat{h}} = F[x]/(\hat{h}(x))$. If $\hat{h}$ is irreducible in $F[x]$, then $E_{\hat{h}}$ is a field extension of F of degree $\deg(\hat{h})$.

In [15], Lavrauw and Sheekey determine the size of the right nucleus of S_f for irreducible $f \in \mathbb{F}_{q^n}[t;\sigma]$, where $F = \mathbb{F}_q$ with $q = p^e$ for some prime p and integer e. In this setting, S_f is a semifield of order q^{mn} whenever f is irreducible and not right invariant, and $|\mathrm{Nuc}_r(S_f)| = q^m$ [15, Lemma 4]. This result generalizes as follows:

Theorem 1. *(for the proof, cf. [16] or [22]) Suppose that f is irreducible. Let k be the number of irreducible factors of h in R.*
(i) $\mathrm{Nuc}_r(S_f)$ is a central division algebra over $E_{\hat{h}}$ of degree $s = n/k$, 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.
(ii) If 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 $\deg(h) = mn$.

Comparing vector space dimensions we obtain that $[S_f : \mathrm{Nuc}_r(S_f)] = k$. Moreover, if $\deg(h) = mn$ and $\hat{h}$ is irreducible in $F[x]$, then f is irreducible and $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$ [10, Proposition 4.1].

Corollary 2. *Suppose that f is irreducible and 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.* $h(t) = t^n + a$.

Proof. Since s divides m by Theorem 1, $s = 1$ which implies (i), or $s = m$. If $s = m$ then $\hat{h}$ has degree one and so $F = E_{\hat{h}}$. Furthermore, then $\mathrm{Nuc}_r(S_f)$ is a central simple algebra over F degree m. Thus f is not right invariant in both cases. Since here we have $\deg(h) = km = n$, m also must divide n in this case. □

Corollary 3. *Suppose that f is irreducible and not right invariant. Let $n = pq$ for p and q prime.*
(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.*

Proof. (i) Since f is not right invariant, we note that $k > 1$. If $n = pq$ then the equation $n = ks$ forces either that $s = 1$ and $k = n$, hence that $\mathrm{Nuc}_r(S_f) \cong E_{\hat{h}}$, or that $s \neq 1$ and then w.o.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, $\deg(h) = pm$, $\deg(\hat{h}) = pm/pq = m/q$, and $[\mathrm{Nuc}_r(S_f) : F] = q^2 \frac{m}{q} = qm$. In particular, q divides m.
(ii) If m is not divisible by p and q, then $s = 1$ by the proof of (i), or else we obtain a contradiction. □

This observation generalizes as follows by induction:

Corollary 4. *Suppose that f is irreducible and not right invariant. Let $n = p_1 \cdots p_l$ be the prime decomposition of n.*
(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 5. *Let $f \in F[t] \subset R$. Suppose that f is irreducible in R and not right invariant. Let n either be prime or* $\gcd(m,n) = 1$. *Then* $\mathrm{Nuc}_r(S_f) \cong F[t]/(f)$.

Proof. If f is irreducible in R, then $F[t]/(f)$ is a subfield of the right nucleus of degree m, hence must be all of the right nucleus, since that has dimension m due to our assumptions (Theorem 1 (ii), Corollary 4 (ii)). □

2 Powers of t that lie in the right nucleus of S_f

Throughout this section, let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R = K[t;\sigma]$ be not right invariant. Initially, we do not assume anything on the ring R.

Theorem 6. *[17] The following are equivalent:*
(i) $a_i \in \mathrm{Fix}(\sigma)$ *for all* $i \in \{0, 1, \dots, m-1\}$,
(ii) $t \in \mathrm{Nuc}_r(S_f)$,
(iii) $t^m t = t t^m$,
(iv) $ft \in Rf$.
(v) all powers of t *are associative in* S_f.

Proof. (i) and (ii) are equivalent by [17, (16)] and (ii), (iii), (iv) and (v) are equivalent by [17, (5)]. □

We obtain the following weak generalization of Theorem 6:

Theorem 7. *Let* $k \in \{1, 2, \dots, m-1\}$. *If* $a_i \in \mathrm{Fix}(\sigma^k)$ *for all* $i \in \{0, 1, \dots, m-1\}$, *then* $t^k \in \mathrm{Nuc}_r(S_f)$. *In particular, then* $t^m t^k = t^k t^m$ *in* S_f.

Proof. Suppose that $a_i \in \mathrm{Fix}(\sigma^k)$ for all i. Then

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

i.e. $ft^k \in Rf$, and so $t^k \in \mathrm{Nuc}_r(S_f)$ as claimed. Since $t^k \in \mathrm{Nuc}_r(S_f)$, we have in particular that $[t^k, t^{m-k}, t^k] = 0$ in S_f, that is $t^k(t^{m-k}t^k) = (t^k t^{m-k})t^k$. Therefore $t^k t^m = t^m t^k$ in S_f. □

From now on we often write $N = \mathrm{Nuc}(S_f)$ for ease of notation.

Proposition 8. *Suppose that there exists* $s \in \{1, 2, \dots, m-1\}$ *such that* $f \in \mathrm{Fix}(\sigma^s)[t;\sigma]$.
(i) If $m = qs$ *for some positive integer* q*, then*

$$N \oplus Nt^s \oplus Nt^{2s} \oplus \cdots \oplus Nt^{(q-1)s} \oplus N(\sum_{i=0}^{m-1} a_i t^i)$$

is an F*-sub vector space of* $\mathrm{Nuc}_r(S_f)$.
(ii) If $m = qs + r$ *for some positive integers* q, r *with* $0 < r < s$*, then*

$$N \oplus Nt^s \oplus Nt^{2s} \oplus \cdots \oplus Nt^{qs}$$

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

Proof. (i) Since $a_i \in \mathrm{Fix}(\sigma^s)$, we have that $t^s \in \mathrm{Nuc}_r(S_f)$ by Theorem 7. Since the right nucleus is a subalgebra of S_f, this implies that $t^{2s}, \dots, t^{(q-1)s}, (t^s)^q = t^m = \sum_{i=0}^{m-1} a_i t^i \in \mathrm{Nuc}_r(S_f)$. Furthermore, we know that $N \subset \mathrm{Nuc}_r(S_f)$, and so $Nt^{js} \subset \mathrm{Nuc}_r(S_f)$ for any $j \in \{0, 1, \dots, q\}$. Therefore $N \oplus Nt^s \oplus \cdots \oplus Nt^{(q-1)s} \oplus N(\sum_{i=0}^{m-1} a_i t^i) \subset \mathrm{Nuc}_r(S_f)$ as claimed.
(ii) We have $t^s \in \mathrm{Nuc}_r(S_f)$. Again since $\mathrm{Nuc}_r(S_f)$ is a subalgebra of S_f, this implies that $t^{2s}, \dots t^{qs}, t^{(q+1)s}, \dots \in \mathrm{Nuc}_r(S_f)$, hence the assertion as in (i). □

Note that the powers $t^{qs}, t^{(q+1)s}, t^{(q+2)s}, \dots$ of t^s in Proposition 8 (ii) lie in $\mathrm{Nuc}_r(S_f)$, but they need not be equal to polynomials in t^s, since $qs, (q+1)s, (q+2)s, \dots \geq m$.

Corollary 9. *Let* K/F *be a cyclic Galois extension of degree* $n < m$ *with Galois group* $\mathrm{Gal}(K/F) = \langle \sigma \rangle$.
(i) If $m = qn$*, then*

$$N \oplus Nt^n \oplus Nt^{2n} \oplus \cdots \oplus Nt^{(q-1)n}$$

is an F*-sub vector space of* $\mathrm{Nuc}_r(S_f)$ *of dimension* $q[N : F]$ *and* $t^m = \sum_{i=0}^{m-1} a_i t^i \in \mathrm{Nuc}_r(S_f)$.
(ii) If $m = qn + r$ *for some positive integers* q, r *with* $0 < r < n$*, then*

$$N \oplus Nt^n \oplus Nt^{2n} \oplus \cdots \oplus Nt^{qn}$$

is an F*-sub vector space of* $\mathrm{Nuc}_r(S_f)$ *of dimension* $(q+1)[N : F]$*. In particular, if* n *is either prime or* $\gcd(m, n) = 1$*,* $\mathrm{gcrd}(f, t) = 1$*, as well as* $[N : F] = n$*, then* f *is reducible.*

Proof. There exist integers q, r such that $q \neq 0$, and $m = qn + r$ where $0 \leq r < n$. Moreover, we have $a_i \in \mathrm{Fix}(\sigma^n) = K$ for all $i \in \{0, 1, \dots, m-1\}$ for every $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$. By Theorem 7 this yields the assertions. □

We write $\sigma = \sigma|_{\mathrm{Fix}(\sigma^c)}$, for ease of notation, then:

Theorem 10. *Suppose that $f(t) \in F[t] \subset R$. Then $N[t;\sigma]/N[t;\sigma]f$ is a Petit algebra and an associative subalgebra of* $\mathrm{Nuc}_r(S_f)$*.*

Proof. Clearly $N[t;\sigma|_N]$ is well-defined, $f(t) \in F[t] \subset N[t;\sigma]$, and so $N[t;\sigma]/N[t;\sigma]f$ is a subalgebra of S_f.

Now $N \subset \mathrm{Nuc}_r(S_f)$, and since $a_i \in F$ for all i, we have that $t^j \in \mathrm{Nuc}_r(S_f)$ for all j by Theorem 7. Thus $N \oplus Nt \oplus \cdots \oplus Nt^{m-1} \subset \mathrm{Nuc}_r(S_f)$ is contained in the right nucleus. We have proved the assertion. □

Corollary 11. *Suppose that $f(t) \in F[t] \subset R$ is bounded and that*

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

Then f is irreducible in R, if and only if f is irreducible in $N[t;\sigma]$.

Proof. Let f be irreducible in $N[t;\sigma]$, then $N[t;\sigma]/N[t;\sigma]f = \mathrm{Nuc}_r(S_f)$ is a division algebra and therefore f is irreducible in R. □

3 The nucleus of S_f

In this section we again assume that f is not right invariant. Then the elements of K which lie in $\mathrm{Nuc}_r(S_f)$ are exactly the elements in the nucleus of S_f:

Lemma 12. *$K \cap \mathrm{Nuc}_r(S_f) = \mathrm{Nuc}(S_f)$.*

Proof. Since f is not right invariant, S_f is not associative and thus $\mathrm{Nuc}_l(S_f) = \mathrm{Nuc}_m(S_f) = K$. Therefore $\mathrm{Nuc}(S_f) = \mathrm{Nuc}_l(S_f) \cap \mathrm{Nuc}_m(S_f) \cap \mathrm{Nuc}_r(S_f) = K \cap \mathrm{Nuc}_r(S_f)$. □

Clearly $F \subset \mathrm{Nuc}(S_f)$. Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$.

Theorem 13. $\mathrm{Nuc}(S_f) = \{b \in K \mid \sigma^m(b) a_i = a_i \sigma^i(b)$ *for all* $i = 0, 1, 2, \dots, m-1\}$.

Proof. Let $c \in \{b \in K \mid \sigma^m(b) a_i = a_i \sigma^i(b)$ for all $i = 0, 1, 2, \dots, m-1\}$. Then an easy calculation shows that $f(t)c \in Rf$, hence that $c \in \mathrm{Nuc}_r(S_f) = \{g \in R \mid \deg(g) < m$ and $fg \in Rf\}$.

Conversely, let $c \in \mathrm{Nuc}(S_f) = \mathrm{Nuc}_r(S_f) \cap K$. Then $[a(t), b(t), c] = 0$ for all $a(t), b(t) \in S_f$, in particular, $[t^k, t^{m-k}, c] = 0$ for all $k \in \{1, 2, \dots, m-1\}$. This implies $(t^k t^{m-k})c = t^k(t^{m-k}c)$, hence

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

and thus $a_i\sigma^i(c) = \sigma^m(c)a_i$ for each $i = 0, 1, \dots, m-1$. Therefore $c \in \{b \in K : \sigma^m(b)a_i = a_i\sigma^i(b)$ for all $i = 0, 1, 2, \dots, m-1\}$ as required. □

We denote the indices of the nonzero coefficients a_i of $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ by $\lambda_1, \dots, \lambda_r$, $1 \leq r \leq m$. The set of these indices we call $\Lambda_f = \{\lambda_1, \lambda_2, \dots, \lambda_r\} \subset \{0, 1, \dots, m\}$, and write $\Lambda = \Lambda_f$ when it is clear from context which f is being used.

Proposition 14. *(i)* $\mathrm{Nuc}(S_f) = \bigcap_{j=1}^{r} \mathrm{Fix}(\sigma^{m-\lambda_j})$. *In particular,* $\mathrm{Nuc}(S_f)$ *is a subfield of* K.
(ii) If $a_{m-1} \neq 0$, *then* $\mathrm{Nuc}(S_f) = F$.

Proof. (i) Let $u \in \mathrm{Nuc}(S_f) = \{u \in K \,|\, \sigma^m(u)a_i = a_i\sigma^i(u)$ for all $i \in \{0, 1, \dots, m-1\}\}$. Then $\sigma^m(u)a_i = a_i\sigma^i(u)$ for each i if and only if $\sigma^{m-i}(u) = u$ for each i such that $a_i \neq 0$, which is equivalent to $\sigma^{m-\lambda_j}(u) = u$ for each $\lambda_j \in \Lambda_f$. This yields the assertion.
(ii) Let $u \in \mathrm{Nuc}(S_f)$, then $\sigma^m(u)a_{m-1} = a_{m-1}\sigma^{m-1}(u)$ yields $\sigma(u) = u$, hence $u \in F$. This implies the assertion. □

Example 15. Let $\mathbb{F}_{16} = \mathbb{F}(a)$ with $a^4 = a + 1$ and $K = \mathbb{F}_{16}(z)$ be the rational function field over $\mathbb{F}_{16}$. Define $\sigma : K \longrightarrow K$, $\sigma(t) = a^5 t$, then σ has order 3 and $F = \mathrm{Fix}(\sigma) = \mathbb{F}_{16}(z^3) = \mathrm{Fix}(\sigma^2)$. Let $R = K[t; \sigma]$, then $C(R) = F[t^3]$ [10, Example 2.16]. Note that not every f is bounded in this setup.

Let $f \in R$ be monic of degree m, then $\mathrm{Nuc}(S_f) = \bigcap_{j=1}^{r} \mathrm{Fix}(\sigma^{m-\lambda_j})$ (Proposition 14). If we have $m - i = 3l$ for all $a_i \neq 0$ then $N = K$, else $\mathrm{Nuc}(S_f) = F$.
(i) Suppose that f has degree $m = 3q \geq 4$, then $\mathrm{Nuc}_r(S_f)$ contains an F-vector space of dimension $q[N : F]$. If $f = g(t^3)$ for some $g \in K[x]$ then $\mathrm{Nuc}(S_f) = K$ and $K[x]/(g(x)) = K \oplus Kt^3 \oplus Kt^6 \oplus \dots \oplus Kt^{3(q-1)}$ is a sub vector space of $\mathrm{Nuc}_r(S_f)$.
(ii) Let $f(t) = t^2 + \frac{1}{t+a}t + az^2 + 1$, then $f^*(t) = t^6 + \frac{(a^3+a)z^3+a^2+a+1}{a^2t^3+a^2+a}t^3 + a^3z^6 + 1$ [10, Example 2.16], so f is bounded and $f^* \in C(R)$. Here

$$\hat{h}(x) = x^2 + \frac{(a^3+a)z^3 + a^2 + a + 1}{a^2t^3 + a^2 + a}x + a^3z^6 + 1 \in F[x]$$

has degree 2, and h has degree $6 = mn$. Therefore f is irreducible and

$$\mathrm{Nuc}_r(S_f) \cong F[x]/(x^2 + \frac{(a^3+a)z^3 + a^2 + a + 1}{a^2t^3 + a^2 + a}x + a^3z^6 + 1)$$

by Theorem 1.

From now on unless specified otherwise let K/F be a cyclic Galois extension of degree $n > 1$ with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Then R has center $C(R) = F[t^n] \cong F[x]$, where $x = t^n$ [13, Theorem 1.1.22] and every $f \in R$ is bounded.

Theorem 16. *If* $d = \gcd(m - \lambda_1, m - \lambda_2, \dots, m - \lambda_r, n)$*, then*

$$\mathrm{Nuc}(S_f) = \mathrm{Fix}(\sigma^d),$$

that is $[\mathrm{Nuc}(S_f) : F] = d$*. In particular,* $\mathrm{Nuc}(S_f) = F$ *if and only if* $d = 1$.

Proof. By Proposition 14, we have

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

It follows immediately that $\mathrm{Nuc}(S_f) = \mathrm{Fix}(\sigma^d)$. Clearly $\mathrm{Nuc}(S_f) = F$ if and only if $\mathrm{Fix}(\sigma^d) = F$ if and only if $\langle\sigma^d\rangle = \langle\sigma\rangle$, which is true if and only if σ^d has order n. Now $ord(\sigma^d) = \frac{n}{\gcd(n,d)} = \frac{n}{d} = n$ if and only if $d = 1$. □

Corollary 17. *Let* K/F *have prime degree* p*. Then* $\mathrm{Nuc}(S_f) = K$ *if and only if* $m - \lambda_j$ *is a multiple of* p *for all* $\lambda_j \in \Lambda$*. In other words,* $\mathrm{Nuc}(S_f) = F$ *if and only if there exists* $\lambda_j \in \Lambda$ *such that* $m - \lambda_j$ *is not divisible by* p*.*

Proof. We have $\mathrm{Nuc}(S_f) = K$ if and only if $[\mathrm{Nuc}(S_f) : F] = p$, i.e. if and only if $d = p$. Now $d = \gcd(m-\lambda_1, m-\lambda_2, \dots, m-\lambda_r, p) = p$ if and only if $m - \lambda_j$ is a multiple of p for all $\lambda_j \in \Lambda$. Since second assertion is equivalent to the first the result follows immediately. □

Theorem 18. *Let* K/F *be of degree* $n = bc < m$ *for some* $b \in \mathbb{N}$*. If* $[\mathrm{Nuc}(S_f) : F] = c$ *then* $m = qc + r$ *for some integers* q, r *with* $0 \le r < c$*, and* $f(t) = g(t^c)t^r$*, where* g *is a polynomial of degree* q *in* $K[t^c; \sigma^c]$*.*

Proof. By Theorem 16, we have that $\mathrm{Nuc}(S_f) = \mathrm{Fix}(\sigma^d)$, where $d = \gcd(m - \lambda_1, m - \lambda_2, \dots, m - \lambda_r, n)$. Now $d = c$ if and only if $m - \lambda_j$ is a multiple of c for all $\lambda_j \in \Lambda$. But $m - \lambda_j$ is equal to a multiple of c if and only if $\lambda_j = r + cl$ for some integer l such that $0 \le l < q$ (since $m = qc + r$). Therefore we obtain $\Lambda \subset \{r, r+c, r+2c, \dots, r+(q-1)c\}$. Thus

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

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

Example 19. Let $K = \mathbb{Q}(\zeta)$, $\sigma : K \longrightarrow K$, $\sigma(\zeta) = \zeta^2$, and R. Then σ has order three, $F = \text{Fix}(\sigma) = \mathbb{Q}(\zeta^4 + \zeta^2 + \zeta)$, and $C(R) = \text{Fix}(\sigma)[x]$ with $x = t^3$. Every $f \in R$ is bounded. Moreover, $[K : F] = 3$ and $[\mathbb{Q}(\zeta^4 + \zeta^2 + \zeta) : \mathbb{Q}] = 2$. Let $f \in \mathbb{Q}(\zeta)[t, \sigma]$ be monic of degree m, then $\text{Nuc}(S_f) = \bigcap_{j=1}^{r} \text{Fix}(\sigma^{m-\lambda_j}) \in \{K, F\}$ (Proposition 14). If we have $m - i = 3l$ for all $a_i \neq 0$ then $\text{Nuc}(S_f) = K$, else $\text{Nuc}(S_f) = F$.
(i) Suppose that f has degree $m = 3q \geq 4$, then $\text{Nuc}_r(S_f)$ contains a F-sub vector space of dimension $q[\text{Nuc}(S_f) : F]$. If $f(t) = g(t^3)$ for some $g \in K[x]$, then $\text{Nuc}(S_f) = K$ and $K[x]/(g(x)) \cong K \oplus Kt^3 \oplus Kt^6 \oplus \cdots \oplus Kt^{3(q-1)}$ is an F-sub vector space of $\text{Nuc}_r(S_f)$. If this f is also irreducible and not right invariant, then $a_0 \neq 0$, and $[\text{Nuc}_r(S_f) : F] = m$. Thus in this case

$$\text{Nuc}_r(S_f) \cong K[x]/(g(x)).$$

(ii) Suppose that $f \in \mathbb{Q}(\zeta^4 + \zeta^2 + \zeta)[t]$ is not right invariant and we have $m - i \neq 3l$ for some $a_i \neq 0$. Then

$$\text{Nuc}(S_f)/\text{Nuc}(S_f)f = \mathbb{Q}(\zeta^4 + \zeta^2 + \zeta)[t]/(f(t)) \subset \text{Nuc}_r(S_f).$$

In particular, if f is irreducible in R then

$$\text{Nuc}_r(S_f) = \mathbb{Q}(\zeta^4 + \zeta^2 + \zeta)[t]/(f(t)).$$

4 The case that only $\hat{h}(x)$ is irreducible in $F[x]$

In this section we assume that σ has finite order $n > 1$, f is bounded and that $\hat{h}$ is irreducible in $F[x]$. Then $f = f_1 \cdots f_l$ for irreducible $f_i \in R$ such that $f_i \sim f_j$ for all i, j ([16], cf. [22]). Let $\deg(f_i) = r$, then $m = rl$, and let k be the number of irreducible factors of h in R (then $l \leq k$).

Theorem 20. *For every i, $1 \leq i \leq l$, $E(f_i)$ is a central division algebra over $E_{\hat{h}}$ of degree $s' = n/k$ and*

$$R/Rh \cong M_k(E(f_i)), \quad \text{Nuc}_r(S_f) \cong M_l(E(f_i)).$$

In particular, $\text{Nuc}_r(S_f)$ *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*

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

Moreover, s' divides $\gcd(r, n)$*, and s and l divide* $\gcd(m, n)$*.*

Proof. Since h is a two-sided maximal element in R, the irreducible factors h_i of any factorization $h = h_1 \cdots h_k$ of h in R are all similar. Now $h(t) = p(t)f(t)$ for some $p(t) \in R$ and so comparing the irreducible factors of f and h and employing [13, Theorem 1.2.9], we see that $f = f_1 \cdots f_l$ for irreducible $f_i \in R$ such that $f_i \sim f_j$ for all i, j (and also $f_i \sim h_j$ for all i, j), with $l \leq k$. In particular, $R/Rf_i \cong R/Rf_j$ for all i, j. Moreover, $R/Rh \cong M_k(E(f_i))$ is a simple Artinian ring [13, Theorem 1.2.19]. Each of the polynomials h_i, resp., f_i, has minimal central left multiple h [10, Proposition 5.2]. Let $A = R/Rh$. We obtain

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

as a direct sum of simple left A-modules (e.g. see [10, Corollary 4.7]). Let g be an irreducible factor of h in R. Since $R/Rf_i \cong R/Rg$, we get $R/Rf \cong (R/Rg)^{\oplus l}$ as left A-modules. By [21, Exercise 6.7.2, Lemma 6.7.5] we have

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

as rings.

Since h is the minimal central left multiple of f and of g, $Rh = \mathrm{Ann}_R(R/Rf) = \mathrm{Ann}_R(R/Rg)$ [14, pg. 38], hence $\mathrm{End}_R(R/Rf) = \mathrm{End}_A(R/Rf)$, $\mathrm{End}_R(R/Rg) = \mathrm{End}_A(R/Rg)$, and

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

Finally, $E(g) \cong \mathrm{End}_R(R/Rg)$, therefore

$$E(f) \cong M_l(E(g)).$$

Since g is irreducible of degree r with minimal central left multiple $h(t) = \hat{h}(t^n)$, $E(g)$ is a central division algebra over $E_{\hat{h}}$ of degree $s' = n/k$, where k is the number of irreducible divisors of h in R, $\deg(\hat{h}) = \frac{r}{s'} = \frac{m}{s}$ and $\deg(h) = \frac{rn}{s'} = \frac{mn}{s}$ by Theorem 1. Finally, since $E(f) \cong M_l(E(g))$, $E(f)$ is a central simple algebra over $E_{\hat{h}}$ of degree $s = ls'$, and $[E(f) : F] = s^2 \deg(\hat{h}) = ms$. The assertion follows since $E(f_i) = E(g)$.

Now $s' = n/k$, and $\deg(\hat{h}) = r/s'$, i.e. s' divides both n and r, hence s' divides $\gcd(n, r)$. Next, s divides $\gcd(m, n)$: $\deg(\hat{h}) = m/s$ means s divides m. Also $[S_f : F] = b[\mathrm{Nuc}_r(S_f) : F]$ for some positive integer b. We know that $[S_f : F] = mn$ and that $[\mathrm{Nuc}_r(S_f) : F] = ms$, hence $mn = bms$. Cancelling m yields $n = bs$, i.e. s divides n. The result follows immediately. Finally, l divides $\gcd(m, n)$: Since $s = ls'$, l divides s. Hence l divides $\gcd(m, n)$ by the above. □

Comparing F-vector space dimensions, we obtain that $[S_f : \mathrm{Nuc}_r(S_f)] = k/l$.

Corollary 21. *Suppose that $\hat{h}(x)$ is irreducible in $F[x]$.*
(i) 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 degree m,
(b) $\mathrm{Nuc}_r(S_f)$ is a central division algebra over F of degree m,
(c) $\mathrm{Nuc}_r(S_f) \cong M_m(F)$.
(ii) 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 $m = \deg(\hat{h})$, and $\deg(h) = mn$.

Corollary 22. *Suppose that $f \in F[t] \subset R$ is not right invariant, and that $\hat{h}(x)$ is irreducible in $F[x]$.*
(i) If $\hat{h}(x)$ is irreducible and $[N : F] = ln/k$, then $\mathrm{Nuc}_r(S_f) = N[t;\sigma]/N[t;\sigma]f$.
(ii) If $[N : F] > \frac{nl}{k}$, then $\hat{h}(x)$ is reducible, and therefore f as well.

Proof. (i) We know that $N[t;\sigma]/N[t;\sigma]f(t)$ is a subalgebra of $\mathrm{Nuc}_r(S_f)$ of dimension $\frac{lnm}{k}$ over F (Theorem 10). If $\hat{h}(x)$ is irreducible then $\mathrm{Nuc}_r(S_f)$ has degree $ms = mln/k$ over F by Theorem 20, therefore comparing the dimensions of the vector spaces we obtain the assertion.
(ii) If $f(t) \in F[t] \subset R$ then $N[t;\sigma]/N[t;\sigma]f$ has dimension $m[N : F]$ over F and is a subalgebra of $\mathrm{Nuc}_r(S_f)$ by Theorem 10. Suppose that $\hat{h}$ is irreducible, then $\mathrm{Nuc}_r(S_f)$ has dimension $\frac{mnl}{k}$ as an F-vector space (Theorem 20). In particular, this implies $\frac{mnl}{k} = [\mathrm{Nuc}_r(S_f) : F] \geq m[N : F]$, a contradiction if $[N : F] > \frac{nl}{k}$. □

As a direct consequence of Proposition 8, we obtain:

Theorem 23. *Suppose that $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in \mathrm{Fix}(\sigma^c)[t;\sigma]$ for some minimal $c \in \{1, 2, \dots, m-1\}$. Suppose that f is not right invariant and that $\hat{h}(x)$ is irreducible in $F[x]$.*
(i) If $m = qc$ for some positive integer q and $[N : F] > \frac{cnl}{k}$, then f is reducible.
(ii) If $m = qc + r$ for some positive integers q, r with $0 < r < c$, and $[N : F] \geq \frac{cnl}{k}$ then f is reducible.

Proof. Since $\hat{h}$ is irreducible in $F[x]$, then the right nucleus has dimension $\frac{mnl}{k}$ as an F-vector space.
(i) If $m = qc$ for some positive integer q, then

$$N \oplus Nt^c \oplus Nt^{2c} \oplus \cdots \oplus Nt^{(q-1)c}$$

is an F-sub vector space of $\mathrm{Nuc}_r(S_f)$ of dimension $q[N : F]$.
(ii) If $m = qc + r$ for some positive integers q, r with $0 < r < c$, then

$$N \oplus Nt^c \oplus Nt^{2c} \oplus \cdots \oplus Nt^{qc}$$

is an F-sub vector space of $\mathrm{Nuc}_r(S_f)$ of dimension $(q+1)[N:F]$.
If $[N:F] > \frac{cnl}{k}$ in (i), then $q[N:F] > \frac{mnl}{k}$, a contradiction. If $[N:F] \geq \frac{cnl}{k}$ in (ii), then $(q+1)[N:F] \geq q\frac{cnl}{k} + \frac{cnl}{k} > \frac{mnl}{k}$, a contradiction. Thus $\hat{h}$ must be reducible, and therefore f, too. □

5 The right nucleus of S_f for low degree polynomials in $F[t] \subset K[t;\sigma]$

We assume that K/F is a cyclic Galois field extension of degree n with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. We now explore the structure of $\mathrm{Nuc}_r(S_f)$ for $f \in F[t] \subset R$ of low degree (the same arguments apply for higher degrees). We repeatedly use that $[\mathrm{Fix}(\sigma^s):F] = \gcd(n,s)$, $N = \bigcap_{\lambda_j \in \Lambda} \mathrm{Fix}(\sigma^{m-\lambda_j})$ by Theorem 13 and Corollary 14. We also use that if $f \in F[t] \subset R$ then $N[t;\sigma]/N[t;\sigma]f$ is a subalgebra of $\mathrm{Nuc}_r(S_f)$ (Theorem 10).

5.1 $m = 2$

Let $f(t) = t^2 - a_1 t - a_0 \in R$, then $N = \bigcap_{\lambda_j \in \Lambda} \mathrm{Fix}(\sigma^{2-\lambda_j})$.

1. If $f(t) = t^2 - a_0$ with $a_0 \in K^\times$, then $N = \mathrm{Fix}(\sigma^2)$.
2. If $f(t) = t^2 - a_1 t - a_0$ with $a_1 \in K^\times$, then $N = F$.

Note that if n 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 $\mathrm{Fix}(\sigma^2) = F$.

Proposition 24. *Let $f(t) = t^2 - a_0 \in F[t] \subset R$, $a_0 \neq 0$ then $\mathrm{Fix}(\sigma^2)[t;\sigma]/\mathrm{Fix}(\sigma^2)[t;\sigma]f$ is a subalgebra of $\mathrm{Nuc}_r(S_f)$ of dimension $2[\mathrm{Fix}(\sigma^2):F]$ over F. In particular, if n is prime or odd, then f is reducible.*

Proof. $N[t;\sigma]/N[t;\sigma]f$ is a subalgebra of $\mathrm{Nuc}_r(S_f)$ and $N = \mathrm{Fix}(\sigma^2)$ 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. □

5.2 $m = 3$

Let $f(t) \in R$ be of degree 3, then $N = \bigcap_{\lambda_j \in \Lambda} \mathrm{Fix}(\sigma^{3-\lambda_j})$.

1. If $f(t) = t^3 - a_0 \in R$, where $a_0 \in K^\times$, then $N = \mathrm{Fix}(\sigma^3)$.

2. If $f(t) = t^3 - a_1 t \in R$, where $a_1 \in K^\times$, then $N = \mathrm{Fix}(\sigma^2)$.
3. In all other cases, $N = F$.

Proposition 25. *(i) If $f(t) = t^3 - a_0$ with $0 \neq a_0 \in F$, then*

$$\mathrm{Fix}(\sigma^3)[t;\sigma]/\mathrm{Fix}(\sigma^3)[t;\sigma]f$$

is a subalgebra of $\mathrm{Nuc}_r(S_f)$ of dimension $3[\mathrm{Fix}(\sigma^3) : F]$ over F. In particular, if n is prime or not divisible by 3, then f is reducible.
(ii) If $f(t) = t^3 - a_1 t$ with $0 \neq a_1 \in F$, then

$$\mathrm{Fix}(\sigma^2)[t;\sigma]/\mathrm{Fix}(\sigma^2)[t;\sigma]f$$

is a subalgebra of $\mathrm{Nuc}_r(S_f)$ of dimension $3[\mathrm{Fix}(\sigma^2) : F]$ over F.

Proof. By Proposition 10, $N[t;\sigma]/N[t;\sigma]f(t) \subset \mathrm{Nuc}_r(S_f)$.
(i) If $f(t) = t^3 - a_0 \in F[t]$ with $a_0 \neq 0$, then $N = \mathrm{Fix}(\sigma^3)$ 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 $N = \mathrm{Fix}(\sigma^2)$. □

5.3 $m = 4$

Let $f(t) \in R$ be of degree 4, then $N = \bigcap_{\lambda_j \in \Lambda} \mathrm{Fix}(\sigma^{4-\lambda_j})$.

1. If $f(t) = t^4 - a_0$ with $a_0 \in K^\times$ then $N = \mathrm{Fix}(\sigma^4)$.
2. If $f(t) = t^4 - a_1 t$ with $a_1 \in K^\times$ then $N = \mathrm{Fix}(\sigma^3)$.
3. If $f(t) = t^4 - a_2 t^2$ with $a_2 \in K^\times$ then $N = \mathrm{Fix}(\sigma^2)$.
4. If $f(t) = t^4 - a_2 t^2 - a_0$ with $a_0, a_2 \in K^\times$, then $N = \mathrm{Fix}(\sigma^4) \cap \mathrm{Fix}(\sigma^2) = \mathrm{Fix}(\sigma^2)$.
5. In all other cases, $N = \mathrm{Fix}(\sigma) = F$.

Observe that:

- If $n \equiv 0 (mod\ 4)$, then $[\mathrm{Fix}(\sigma^4) : F] = 4$.
- If $n \equiv 1$ or $3 (mod\ 4)$, then $\mathrm{Fix}(\sigma^4) = F$.
- 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 $[\mathrm{Fix}(\sigma^2) : F] = 2$.
- If $n \equiv 1(mod\ 2)$ then $\mathrm{Fix}(\sigma^2) = F$.

Proposition 26. *(i) If $f(t) = t^4 - a_0 \in F[t]$ with $0 \neq a_0$, then*

$$\mathrm{Fix}(\sigma^4)[t;\sigma]/\mathrm{Fix}(\sigma^4)[t;\sigma]f$$

is a subalgebra of $\mathrm{Nuc}_r(S_f)$ *of dimension* $\mathrm{gcd}(n,4)$ *over F. In particular:*
(a) If f is irreducible and either $n \neq 2$ is prime or $gcd(n,4) = 1$, then

$$\mathrm{Nuc}_r(S_f) \cong \mathrm{Fix}(\sigma^4)[t;\sigma]/\mathrm{Fix}(\sigma^4)[t;\sigma]f.$$

(b) If $n = 2$, then f is reducible.
(ii) If $f(t) = t^4 - a_1 t \in F[t;\sigma]$ with $0 \neq a_1$, then

$$\mathrm{Fix}(\sigma^3)[t;\sigma]/\mathrm{Fix}(\sigma^3)[t;\sigma]f$$

is a subalgebra of $\mathrm{Nuc}_r(S_f)$ *of dimension* $4\mathrm{gcd}(n,3)$ *over F.*
(iii) If $f(t) = t^4 - a_2 t - a_0 \in F[t;\sigma]$ with $0 \neq a_2$, then

$$\mathrm{Fix}(\sigma^2)[t;\sigma]/\mathrm{Fix}(\sigma^2)[t;\sigma]f$$

is a subalgebra of $\mathrm{Nuc}_r(S_f)$ *of dimension* $4\mathrm{gcd}(n,2)$ *over F. In particular:*
(a) If f is irreducible, and either $n \neq 2$ is prime or $\mathrm{gcd}(n,4) = 1$*, then*

$$\mathrm{Nuc}_r(S_f) \cong \mathrm{Fix}(\sigma^2)[t;\sigma]/\mathrm{Fix}(\sigma^2)[t;\sigma]f.$$

(b) If $n = 2$, then f is reducible.

Proof. $N[t;\sigma]/N[t;\sigma]f(t) \subset \mathrm{Nuc}_r(S_f)$ by Theorem 10.
(i) Here $N = \mathrm{Fix}(\sigma^4)$ by (1), and thus

$$\mathrm{Fix}(\sigma^4)[t;\sigma]/\mathrm{Fix}(\sigma^4)[t;\sigma]f \subset \mathrm{Nuc}_r(S_f).$$

(ii) We know $N = \mathrm{Fix}(\sigma^3)$ by (2), and hence

$$\mathrm{Fix}(\sigma^3)[t;\sigma]/\mathrm{Fix}(\sigma^3)[t;\sigma]f \subset \mathrm{Nuc}_r(S_f).$$

(iii) We have $N = \mathrm{Fix}(\sigma^2)$ by (3), and so

$$\mathrm{Fix}(\sigma^2)[t;\sigma]/\mathrm{Fix}(\sigma^2)[t;\sigma]f \subset \mathrm{Nuc}_r(S_f).$$

□

6 A small algorithm to check if f is reducible

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 $\gcd(m, n) = 1$ to simplify the process. For some skew polynomials $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ 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. Check if $f \in F[t]$. If f is reducible in $F[t]$, then f is reducible in R $\boxed{\text{TRUE}}$. If $f \notin F[t]$ then go to (2).
2. Compute $N = \mathrm{Fix}(\sigma^d)$, where $d = \gcd(m - \lambda_1, m - \lambda_2, \dots, m - \lambda_r, n)$ as per Theorem 16.
   If $[N : F] > m$, then f is reducible $\boxed{\text{TRUE}}$.
   If $[N : F] \leq m$ then go to (3).
3. Find the smallest integer c, such that $a_i \in \mathrm{Fix}(\sigma^c)$ for all i, and where $\mathrm{Fix}(\sigma^c)$ is a proper subfield of K.
   If $\mathrm{Fix}(\sigma^c) = N$ then f is reducible $\boxed{\text{TRUE}}$.
   If $m = qc$ and $[N : F] > c$, then f is reducible $\boxed{\text{TRUE}}$.
   If $m = qc + r$ with $0 < r < c$, and $[N : F] \geq c$ 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 $N[t;\sigma]/N[t;\sigma]f$ is a subalgebra of $\mathrm{Nuc}_r(S_f)$ to look for zero divisors in $\mathrm{Nuc}_r(S_f)$ in order to factor f.

References

[1] A. S. Amitsur, *Non-commutative cyclic fields.* Duke Math. J. 21 (1954), 87-105.

[2] A. S. Amitsur, *Differential Polynomials and Division Algebras.* Annals of Mathematics, Vol. 59 (2) (1954) 245-278.

[3] A. S. Amitsur, *Generic splitting fields of central simple algebras.* Ann. of Math. 62 (2) (1955), 8-43.

[4] C. Brown, S. Pumplün, *How a nonassociative algebra reflects the properties of a skew polynomial.* Glasgow Math. J. 63 (2021) (1), 6-26. https://doi.org/10.1017/S0017089519000478

[5] C. Brown *Petit algebras and their automorphisms*, PhD Thesis, University of Nottingham, 2018. Online at arXiv:1806.00822 [math.RA]

[6] L. E. Dickson, *Linear algebras in which division is always uniquely possible.* Trans. Amer. Math. Soc. 7 (3) (1906), 370-390.

[7] M. Giesbrecht, *Factoring in skew-polynomial rings over finite fields.* J. Symbolic Comput. 26 (4) (1998), 463-486.

[8] M. Giesbrecht, Y. Zhang, *Factoring and decomposing Ore polynomials over* $\mathbb{F}_q(t)$. Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, 127-134, ACM, New York, 2003.

[9] J. Gòmez-Torrecillas, P. Kutas, F. J. Lobillo, G. Navarro, *Primitive idempotents in central simple algebras over* $\mathbb{F}_q(t)$ *with an application to coding theory.* Online at arXiv:2006.12116 [math.RA]

[10] J. Gòmez-Torrecillas, F. J. Lobillo,; G. Navarro, *Computing the bound of an Ore polynomial. Applications to factorization.* J. Symbolic Comput. 92 (2019), 269-297.

[11] J. Gòmez-Torrecillas, F. J. Lobillo, G. Navarro, *Factoring Ore polynomials over* $\mathbb{F}_q(t)$ *is difficult.* Online at arXiv:1505.07252[math.RA]

[12] J. Gòmez-Torrecillas, *Basic module theory over non-commutative rings with computational aspects of operator algebras. With an appendix by V. Levandovskyy.* Lecture Notes in Comput. Sci. 8372, Algebraic and algorithmic aspects of differential and integral operators, Springer, Heidelberg (2014) 23-82.

[13] N. Jacobson, "Finite-dimensional division algebras over fields." Springer Verlag, Berlin-Heidelberg-New York, 1996.

[14] N. Jacobson, "The theory of rings." American Mathematical Soc., 1943

[15] M. Lavrauw, J. Sheekey, *Semifields from skew-polynomial rings.* Adv. Geom. 13 (4) (2013), 583-604.

[16] A. Owen, *On the eigenspaces of certain classes of skew polynomials.* PhD Thesis, University of Nottingham, 2022.

[17] J.-C. Petit, *Sur certains quasi-corps généralisant un type d'anneau-quotient.* Séminaire Dubriel. Algèbre et théorie des nombres 20 (1966-67), 1-18.

[18] J.-C. Petit, *Sur les quasi-corps distributifes à base momogène.* C. R. Acad. Sc. Paris 266 (1968), Série A, 402-404.

[19] R. D. Schafer, "An Introduction to Nonassociative Algebras." Dover Publ., Inc., New York, 1995.

[20] J. Sheekey *New semifields and new MRD codes from skew polynomial rings*, September 2019 Journal of the LMS, DOI: 10.1112/jlms.12281

[21] T. J. Sullivan, C. Hajarnavis, *Rings and Modules*, Lecture Notes 2004, online at http://www.tjsullivan.org.uk/pdf/MA377_Rings_and_Modules.pdf

[22] D. Thompson, S. Pumplün, *The norm of a skew polynomial*, J. Algebra and Representation Theory, https://doi.org/10.1007/s10468-021-10051-z

Adam OWEN,
Department of Mathematical Sciences,
University of Nottingham,
University Park, Nottingham, NG72RD, UK.
Email: owena004@gmail.com

Susanne PUMPLÜN,
Department of Mathematical Sciences,
University of Nottingham,
University Park, Nottingham, NG72RD, UK.
Email: susanne.pumpluen@nottingham.ac.uk