HOW A NONASSOCIATIVE ALGEBRA REFLECTS THE PROPERTIES OF A SKEW POLYNOMIAL

C. BROWN AND S. PUMPLÜN

ABSTRACT. Let D be a unital associative division ring and $D[t; \sigma, \delta]$ be a skew polynomial ring, where σ is an endomorphism of D and δ a left σ-derivation. For each $f \in D[t; \sigma, \delta]$ of degree $m > 1$ with a unit as leading coefficient, there exists a unital nonassociative algebra whose behaviour reflects the properties of f. These algebras yield canonical examples of right division algebras when f is irreducible. The structure of their right nucleus depends on the choice of f. In the classical literature, this nucleus appears as the eigenspace of f, and is used to investigate the irreducible factors of f. We give necessary and sufficient criteria for skew polynomials of low degree to be irreducible. These yield examples of new division algebras S_f.

INTRODUCTION

The investigation of skew polynomials is an active area in algebra which has applications to coding theory, to solving differential and difference equations, and in engineering, to name just a few. For instance, linear differential operators (where $\sigma = id$) and linear difference operators (where $\delta = 0$) are special cases of skew polynomials.

Let D be a unital associative division ring and $R = D[t; \sigma, \delta]$ a skew polynomial ring, where σ is an endomorphism of D and δ a left σ-derivation. Suppose $f \in D[t; \sigma, \delta]$ has degree m. Using right division by f to define a multiplication on the set of skew polynomials of degree less than m, this set becomes a unital nonassociative algebra we denote by S_f. The algebra S_f generalizes the classical quotient algebra construction when factoring out a two-sided ideal generated by a right invariant skew polynomial f. When choosing f and R in the right way, it can be also seen as a generalization of certain crossed product algebras and some Azumaya algebra constructions. First results on the structure of the algebras S_f which initially were defined by Petit in [30] have appeared in [30, 31, 5, 6, 35, 36, 34]. First applications to coding theory have appeared for instance in [37, 38, 39].

Recently, a computational criterion for deciding whether a bounded skew polynomial is irreducible was developed in [17]. The method heavily relies on being able to find the zero divisors in the right nucleus of S_f (although the simple algebra employed there, called the eigenspace of f, is not recognized as the right nucleus of S_f in that paper). The method is only applicable for certain set-ups when the input data S, σ and δ are effective and computable, but it demonstrates the importance of developing a better understanding of the algebras S_f and their algebraic structure. Independently, effective algorithms to compute

---

the eigenspace (and thus the right nucleus of S_f, again not recognized as such) for the special case that $R = \mathbb{F}_q(x)[t; \sigma, \delta]$ can be found in [14], and for $R = \mathbb{F}_q[t; \sigma]$ in [13], [40]. In all cases the eigenspace is a crucial tool to understand the decomposability of the skew polynomial f.

This paper consists of two parts. The first one considers the structure of the right nucleus of the algebras S_f, establishing how it reflects the type of the skew polynomial f it is defined with, but also the important role irreducible polynomials play in the construction of classes of nonassociative unital (right) division algebras.

The second part looks at skew polynomials of low degree as well as the polynomial $f(t) = t^m - a$, and when these polynomials are irreducible in $D[t; \sigma, \delta]$, in order to obtain examples for the construction of (right) division algebras.

After establishing the basic terminology in Section 1, we define Petit algebras in Section 2 and collect some results on their right nuclei in Section 3. We investigate when the algebras S_f are right (and not left) division algebras in Section 4. A necessary condition for S_f being a right division algebra is that the polynomial f is irreducible. We then collect some irreducibility criteria for polynomials of low degree and the polynomial $f(t) = t^m - a$ in both $R = D[t; \sigma]$ and $R = D[t; \sigma, \delta]$ in Sections 5 and 6, including the special case where D is a finite field.

We point out that there exists some kind of Eisenstein valuation criteria to test a skew polynomial over a division ring for reducibility, using some (noncommutative) valuation theory for skew polynomial rings [11, 18]. We believe our criteria are more tractable for the types of skew polynomials we consider. Moreover, some results on twisted polynomials over algebraically and real closed fields have been obtained in [2] and [32, 33].

Most of this work is part of the first author's PhD thesis [4] written under the supervision of the second author.

1. PRELIMINARIES

1.1. **Skew polynomial rings.** Let S be a unital associative ring, σ a ring endomorphism of S and $\delta : S \to S$ a *left σ-derivation*, i.e. an additive map such that $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ for all $a, b \in S$. Then the *skew polynomial ring* $R = S[t; \sigma, \delta]$ is the set of skew polynomials $g(t) = a_0 + a_1 t + \cdots + a_n t^n$ with $a_i \in S$, with term-wise addition and where the multiplication is defined via $ta = \sigma(a)t + \delta(a)$ for all $a \in S$ [29]. That means,

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

for all $a, b \in S$, where the map $\Delta_{n,j}$ is defined recursively via

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

with $\Delta_{0,0} = id_S$, $\Delta_{1,0} = \delta$, $\Delta_{1,1} = \sigma$. Therefore $\Delta_{n,j}$ is the sum of all monomials in σ and δ of degree j in σ and degree $n - j$ in δ [20, p. 2]. If $\delta = 0$, then $\Delta_{n,n} = \sigma^n$.

For $\sigma = id$ and $\delta = 0$, we obtain the usual ring of left polynomials $S[t] = S[t; id, 0]$. Define $\mathrm{Fix}(\sigma) = \{a \in S \,|\, \sigma(a) = a\}$ and $\mathrm{Const}(\delta) = \{a \in S \,|\, \delta(a) = 0\}$.

For $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in R$ with $a_n \neq 0$ define $\deg(f) = n$ and $\deg(0) = -\infty$. Then $\deg(gh) \leq \deg(g) + \deg(h)$ (with equality if h has an invertible leading coefficient, or g has an invertible leading coefficient and σ is injective, or if S is a division ring). An element $f \in R$ is *irreducible* in R if it is not a unit and it has no proper factors, i.e if there do not exist $g, h \in R$ with $1 \leq \deg(g), \deg(h) < \deg(f)$ such that $f = gh$.

1.2. **Nonassociative algebras.** Let R be a unital commutative ring and let A be an R-module. We call A an *algebra* over R if there exists an R-bilinear map $A \times A \mapsto A$, $(x, y) \mapsto x \cdot y$, usually denoted simply by juxtaposition xy, the *multiplication* of A. An algebra A is called *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.

For an R-algebra A, associativity in A is measured by the *associator* $[x, y, z] = (xy)z - x(yz)$. The *left nucleus* of A is defined as $\mathrm{Nuc}_l(A) = \{x \in A \,|\, [x, A, A] = 0\}$, the *middle nucleus* as $\mathrm{Nuc}_m(A) = \{x \in A \,|\, [A, x, A] = 0\}$ and the *right nucleus* as $\mathrm{Nuc}_r(A) = \{x \in A \,|\, [A, A, x] = 0\}$. $\mathrm{Nuc}_l(A)$, $\mathrm{Nuc}_m(A)$ and $\mathrm{Nuc}_r(A)$ are associative subalgebras of A. Their intersection $\mathrm{Nuc}(A) = \{x \in A \,|\, [x, A, A] = [A, x, A] = [A, A, x] = 0\}$ is the *nucleus* of A. $\mathrm{Nuc}(A)$ is an associative subalgebra of A containing $R1$ and $x(yz) = (xy)z$ whenever one of the elements x, y, z is in $\mathrm{Nuc}(A)$. The *commuter* of A is defined as $\mathrm{Comm}(A) = \{x \in A \,|\, xy = yx$ for all $y \in A\}$ and the *center* of A is $\mathrm{C}(A) = \mathrm{Nuc}(A) \cap \mathrm{Comm}(A)$ [41].

A nonassociative ring $A \neq 0$ (resp., an algebra $A \neq 0$ over a field F) is called a *left division ring (resp., algebra)*, if for all $a \in A$, $a \neq 0$, the left multiplication with a, $L_a(x) = ax$, is a bijective map, and a *right division ring (resp., algebra)*, if for all $a \in A$, $a \neq 0$, the right multiplication with a, $R_a(x) = xa$, is a bijective map. An algebra $A \neq 0$ over a field F is called a *division algebra* if for all $a \in A$, $a \neq 0$, both the left and right multiplication with a are bijective. A division algebra A does not have zero divisors. If A is a finite-dimensional algebra over F, then A is a division algebra over F if and only if A has no zero divisors [41]. A nonassociative ring $A \neq 0$ has no zero divisors if and only if R_a and L_a are injective for all $0 \neq a \in A$.

Note that every algebra A is a right $\mathrm{Nuc}_r(A)$-module and the left multiplication L_a is $\mathrm{Nuc}_r(A)$-linear for all $0 \neq a \in A$.

2. Nonassociative algebras obtained from skew polynomials

Let S be a unital associative ring and $S[t; \sigma, \delta]$ a skew polynomial ring where σ is injective.

2.1. Assume $f(t) = \sum_{i=0}^{m} a_i t^i \in R = S[t; \sigma, \delta]$ has an invertible leading coefficient $a_m \in S^\times$. Then for all $g(t) \in R$ of degree $l \geq m$, there exist uniquely determined $r(t), q(t) \in R$ with $\deg(r) < \deg(f)$, such that $g(t) = q(t)f(t) + r(t)$, and if $\sigma \in \mathrm{Aut}(D)$, also uniquely determined $r(t), q(t) \in R$ with $\deg(r) < \deg(f)$, such that $g(t) = f(t)q(t) + r(t)$ ([4],[35, Proposition 1]).

Let $\mathrm{mod}_r f$ denote the remainder of right division by f and $\mathrm{mod}_l f$ the remainder of left division by f. The skew polynomials of degree less that m canonically represent the elements of the (left resp. right) $S[t; \sigma, \delta]$-modules $S[t; \sigma, \delta]/S[t; \sigma, \delta]f$ and $S[t; \sigma, \delta]/fS[t; \sigma, \delta]$.

Moreover,
$$R_m = \{g \in S[t; \sigma, \delta] \,|\, \deg(g) < m\}$$
together with the multiplication
$$g \circ h = \begin{cases} gh \text{ if } \deg(g) + \deg(h) < m, \\ gh \bmod_r f \text{ if } \deg(g) + \deg(h) \geq m, \end{cases}$$
is a unital nonassociative ring $S_f = (R_m, \circ)$ also denoted by R/Rf.
If $\sigma \in \text{Aut}(S)$, then R_m together with
$$g \circ h = \begin{cases} gh \text{ if } \deg(g) + \deg(h) < m, \\ gh \bmod_l f \text{ if } \deg(g) + \deg(h) \geq m, \end{cases}$$
is a unital nonassociative ring $_f S = (R_m, \circ)$ also denoted by R/fR. When the context is clear, we will drop the $\circ$ notation and simply use juxtaposition for multiplication in S_f.

S_f and $_f S$ are unital nonassociative algebras over the commutative subring
$$S_0 = \{a \in S \,|\, ah = ha \text{ for all } h \in S_f\} = \text{Comm}(S_f) \cap S$$
of S, and
$$C(S) \cap \text{Fix}(\sigma) \cap \text{Const}(\delta) \subset S_0.$$
For all invertible $a \in S$ we have $S_f = S_{af}$, so that without loss of generality it suffices to only consider monic polynomials in the construction. If f has degree 1 then $S_f \cong S$. If f is reducible then S_f contains zero divisors.

In the following, we assume $m \geq 2$ and call the algebras S_f *Petit algebras* as the construction goes back to Petit [30, 31] (who only considered division rings S). We will focus on the algebras S_f, since the algebras $_f S$ are anti-isomorphic to Petit algebras [35, Proposition 3].

For $0 \neq a \in S_f$, left multiplication L_a is an S_0-module endomorphism. Moreover, R_a is a left S-module homomorphism for $0 \neq a \in S_f$.

Let $f \in S[t; \sigma, \delta]$ have degree $m \geq 2$ and an invertible leading coefficient. Then S_f is a free left S-module of rank m with basis $t^0 = 1, t, \ldots, t^{m-1}$. S_f is associative if and only if Rf is a two-sided ideal in R. If S_f is not associative then $S \subset \text{Nuc}_l(S_f)$, $S \subset \text{Nuc}_m(S_f)$ and
$$\{g \in R \,|\, \deg(g) < m \text{ and } fg \in Rf\} = \text{Nuc}_r(S_f).$$
When S is a division ring, these inclusions become equalities. We have $t \in \text{Nuc}_r(S_f)$, if and only if the powers of t are associative, if and only if $t^m t = t t^m$ in S_f. If S is a division ring and S_f is not associative then $C(S_f) = S_0$. Let $f(t) = \sum_{i=0}^m a_i t^i \in S[t; \sigma]$ with a_0 invertible. If the endomorphism L_t (i.e. left multiplication by t) is surjective then σ is surjective. In particular, if S is a division ring and f irreducible, then L_t surjective implies σ surjective. Moreover, if σ is bijective then L_t is surjective [35, Theorem 4].

Since $C(S_f) = \text{Comm}(S_f) \cap \text{Nuc}_l(S_f) \cap \text{Nuc}_m(S_f) \cap \text{Nuc}_r(S_f)$, we have
$$S_0 = \{a \in S \,|\, ah = ha \text{ for all } h \in S_f\} = \text{Comm}(S_f) \cap S \subset C(S_f)$$
when S_f is not associative. If $\text{Nuc}_l(S_f) = \text{Nuc}_m(S_f) = S$ this yields that the center $C(S_f) = \text{Comm}(S_f) \cap S \cap \text{Nuc}_r(S_f) = \text{Comm}(S_f) \cap S$ of S_f is identical to the ring S_0.

3. The right nucleus of S_f

In this Section, let D be a division algebra with center F, $R = D[t; \sigma, \delta]$ with σ any endomorphism of D and δ any left σ-derivation. Let $f \in R = D[t; \sigma, \delta]$ be monic of degree $m \geq 2$ and $D_0 = \{a \in D \mid ah = ha \text{ for all } h \in S_f\}$.

The largest subalgebra of $R = D[t; \sigma, \delta]$ in which Rf is a two-sided ideal is the *idealizer* $I(f) = \{g \in R \mid fg \in Rf\}$ of Rf. The *eigenring* of f is then defined as the quotient $E(f) = I(f)/Rf = \{g \in R \mid \deg(g) < m \text{ and } fg \in Rf\}$. This is also the right nucleus of the algebra S_f [35, Theorem 4].

3.1. Some general observations. The right nucleus is important when finding right factors of f; if $\operatorname{Nuc}_r(S_f)$ contains zero divisors then f is reducible [30]. If $u, v \in \operatorname{Nuc}_r(S_f)$ are non-zero such that $uv = 0$, then the greatest common right divisor $gcrd(f, u)$ is a non-trivial right factor of f, see e.g. [35]. This was employed for instance in [17].

Moreover, if $ft \in Rf$ then $t \in \operatorname{Nuc}_r(S_f)$, hence the powers of t are associative in S_f. This in turn implies $t^m t = t t^m$ [35, Theorem 5]. Moreover, $ft \in Rf$ if and only if $t \in \operatorname{Nuc}_r(S_f)$, if and only if the powers of t are associative, if and only if $t^m t = t t^m$ [30]. This yields:

Lemma 1. *Let $f \in D[t; \sigma, \delta]$. If $t \notin \operatorname{Nuc}_r(S_f)$ or $f \in Rt$ then S_f does not have any associative subalgebra that contains all powers of t.*

In particular, if f is irreducible and $t \notin \operatorname{Nuc}_r(S_f)$, then S_f does not have any associative subalgebra that contains all powers of t (and then f cannot lie in $D_0[t]$).

Proof. There exists a subset X of S_f which is a multiplicative group and contains all powers of t, if and only if $ft \in Rf$ and $f \notin Rt$ [30, (8)], i.e. if and only if $t \in \operatorname{Nuc}_r(S_f)$ and $f \notin Rt$. Now suppose A is an associative subalgebra of S_f that contains all powers of t, choose $X = A$ and obtain that $t \in \operatorname{Nuc}_r(S_f)$ and $f \notin Rt$.

If f is irreducible, we know that $f \notin Rt$. If, additionally, $f \in D_0[t]$ then $D_0[t]/(f)$ is a subalgebra of S_f that contains all powers of t, a contradiction. $\square$

Proposition 2. *For all $f \in D_0[t]$, $D_0[t]/(f)$ is a commutative subring of S_f and*

$$D_0[t]/(f) = D_0 \oplus S_0 t \oplus \cdots \oplus S_0 t^{m-1} \subset \operatorname{Nuc}_r(S_f).$$

If $\operatorname{Nuc}_r(S_f)$ is larger than $D_0[t]/(f)$, then $\operatorname{Nuc}_r(S_f)$ is not commutative.

Proof. S_f contains the commutative subring $D_0[t]/(f)$, where $D_0 = \operatorname{Const}(\delta) \cap C(D) \cap \operatorname{Fix}(\sigma)$. This subring is isomorphic to the ring consisting of the elements $\sum_{i=0}^{m-1} a_i t^i$ with $a_i \in D_0$. In particular, we know that the powers of t are associative. By Theorem [35, Theorem 4], this implies that $t \in \operatorname{Nuc}_r(S_f)$. Clearly $D_0 \subset \operatorname{Nuc}_r(S_f)$, so if $t \in \operatorname{Nuc}_r(S_f)$ then $D_0 \oplus D_0 t \oplus \cdots \oplus D_0 t^{m-1} \subset \operatorname{Nuc}_r(S_f)$, hence we obtain the assertion. The last part is trivial then. $\square$

If $f \in D_0[t]$ is irreducible in $D_0[t]$, then $D_0[t]/(f)$ is an algebraic field extension of D_0 of degree m contained in $\operatorname{Nuc}_r(S_f)$. Thus if K is a finite field, $\delta = 0$ and f irreducible, then $\operatorname{Nuc}_r(S_f) = F \oplus Ft \oplus \cdots \oplus Ft^{m-1} = F[t]/(f)$, employing the fact that in this case we know that the right nucleus has exactly $|F[t]/(f)|$ elements [24].

3.2. Right semi-invariant polynomials. We first investigate for which f the algebra D is contained in the right nucleus of S_f. By [35, Theorem 4], this implies that either S_f is associative or $\mathrm{Nuc}(S_f) = D$.

Recall that $f \in R = D[t; \sigma, \delta]$ is called *right semi-invariant* if for every $a \in D$ there is $b \in D$ such that $f(t)a = bf(t)$ which is equivalent to $fD \subseteq Df$. Similarly, f is *left semi-invariant* if $Df \subseteq fD$ [26, 27]. Moreover, f is right semi-invariant if and only if df is right semi-invariant for all $d \in D^\times$ [26, p. 8]. Hence we only need to consider monic f. Furthermore, if σ is an automorphism, then f is right semi-invariant if and only if it is left semi-invariant if and only if $fD = Df$ [26, Proposition 2.7]. Right semi-invariant polynomials canonically arise in the theory of semi-linear transformations [21]. For a thorough background on right semi-invariant polynomials see [26, 27].

If f is semi-invariant and also satisfies $f(t)t = (bt + a)f(t)$ for some $a, b \in D$ then f is called *right invariant* which is equivalent to $fR \subset Rf$. If f is right invariant then Rf is a two-sided ideal in R and conversely, every two-sided ideal in R is generated by a right-invariant polynomial. That means R is not simple if and only if there is a non-constant right-invariant $f \in R$. Moreover, assuming σ is an automorphism, R is not simple if and only if there is a non-constant monic semi-invariant $f \in R$ if and only if δ is a quasi-algebraic derivation [27] (this last observation actually holds for any simple ring D).

Theorem 3. $f \in R$ *is right semi-invariant if and only if* $D \subseteq \mathrm{Nuc}_r(S_f)$. *In particular, if f is right semi-invariant, then either* $\mathrm{Nuc}(S_f) = D$ *or S_f is associative.*

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

The second assertion follows by [35, Theorem 4].   □

Proposition 4. *([28, (9.21)])*. *Suppose σ is an automorphism of D, then the following are equivalent:*
(i) There exists a non-constant right semi-invariant polynomial in R.
(ii) R is not simple.
(iii) There exist $b_0, \ldots, b_n \in D$ with $b_n \neq 0$ such that $b_0\delta_{c,\theta} + \sum_{i=1}^{n} b_i\delta^i = 0$, where θ is an endomorphism of D and $\delta_{c,\theta}$ denotes the θ-derivation of D sending $x \in D$ to $cx - \theta(x)c$.

Corollary 5. *Suppose σ is an automorphism of D and R is simple. Then there are no nonassociative algebras S_f with $D \subseteq \mathrm{Nuc}_r(S_f)$. In particular, there are no nonassociative algebras S_f with $D \subseteq \mathrm{Nuc}(S_f)$.*

Proof. R is not simple if and only if there exists a non-constant right semi-invariant polynomial in R by Proposition 4, and hence the assertion follows by Theorem 3.   □

Corollary 5 actually also holds when $f \in S[t; \sigma, \delta]$, where S is only a simple ring and σ an automorphism of S [27, Theorem 5.2].

Recall that if S is a division ring, or if S is a simple ring and $\sigma \in \mathrm{Aut}(S)$, then $R = S[t; \sigma, \delta]$ is not simple if and only if δ is quasi-algebraic [27]. Recall also that σ is an automorphism of D of *finite inner order* k if $\sigma^k = I_u$ for some $u \in D^\times$. Using Theorem 3 we can rephrase

the results [26, Lemma 2.2, Corollary 2.12, Propositions 2.3 and 2.4], [27, Corollary 2.6] on right semi-invariant polynomials in terms of the right nucleus of the nonassociative algebra S_f:

Theorem 6. *Let $f(t) = \sum_{i=0}^{m} a_i t^i \in R$ be monic of degree m.*
(i) $D \subseteq \operatorname{Nuc}_r(S_f)$ if and only if $f(t)c = \sigma^m(c)f(t)$ for all $c \in D$, if and only if

$$\sigma^m(c)a_j = \sum_{i=j}^{m} a_i \Delta_{i,j}(c) \tag{1}$$

for all $c \in D$ and $j \in \{0, \ldots, m-1\}$.
(ii) Suppose σ is an automorphism of D of infinite inner order. Then $D \subseteq \operatorname{Nuc}_r(S_f)$ implies S_f is associative.
(iii) Suppose $\delta = 0$. Then $D \subseteq \operatorname{Nuc}_r(S_f)$ if and only if

$$\sigma^m(c) = a_j \sigma^j(c) a_j^{-1} \tag{2}$$

for all $c \in D$ and all $j \in \{0, \ldots, m-1\}$ with $a_j \neq 0$. Furthermore, S_f is associative if and only if $f(t)$ satisfies (2) and $f(t) \in \operatorname{Fix}(\sigma)[t] \subset \operatorname{Fix}(\sigma)[t; \sigma]$.
(iv) Suppose $\sigma = id$. Then $D \subseteq \operatorname{Nuc}_r(S_f)$ is equivalent to

$$ca_j = \sum_{i=j}^{m} \binom{i}{j} a_i \delta^{i-j}(c), \tag{3}$$

for all $c \in D$, $j \in \{0, \ldots, m-1\}$. Furthermore, S_f is associative if and only if $f(t)$ satisfies (3) and $f(t) \in \operatorname{Const}(\delta)[t] \subset \operatorname{Const}(\delta)[t; \delta]$.
(v) Suppose $\delta = 0$ and σ is an automorphism of D of finite inner order k, i.e. $\sigma^k = I_u$ for some $u \in D^{\times}$. Then the polynomials $g \in D[t; \sigma]$ such that $D \subseteq \operatorname{Nuc}_r(S_g)$ are precisely those of the form

$$g(t) = b \sum_{j=0}^{n} c_j u^{n-j} t^{jk}, \tag{4}$$

where $n \in \mathbb{N}$, $c_n = 1$, $c_j \in F$ and $b \in D^{\times}$. Furthermore, S_g is associative if and only if $g(t)$ has the form (4) and $g(t) \in \operatorname{Fix}(\sigma)[t] \subset \operatorname{Fix}(\sigma)[t; \sigma]$.

3.3. Right B-weak semi-invariant polynomials. Let now B be a subring of D. We can find conditions on f such that B is contained in $\operatorname{Nuc}_r(S_f)$ by generalizing the definition of right semi-invariant polynomials as follows: we say $f \in D[t; \sigma, \delta]$ is *(right) B-weak semi-invariant* if $fB \subseteq Df$. Clearly any right semi-invariant polynomial is also B-weak semi-invariant for every subring B of D. We call $f \in R$ a *(right) B-weak invariant* polynomial if f is right B-weak semi-invariant and $f(t)t = (bt + a)f(t)$ for some $a, b \in B$.

Note that when we have an extension of rings $B \subset D$, which induces an extension of skew-polynomial rings $B[t, \sigma, \delta] \subset D[t, \sigma, \delta]$ (i.e., $\sigma|_B = \sigma$, $\delta|_B = \delta$), every right semi-invariant $f \in B[t, \sigma, \delta]$ is right B-weak semi-invariant in $D[t, \sigma, \delta]$, and every invariant $f \in B[t, \sigma, \delta]$ is right B-weak invariant in $D[t, \sigma, \delta]$.

Example 7. Let K be a field, σ be a non-trivial automorphism of K, $L = \text{Fix}(\sigma^j)$ be the fixed field of σ^j for some $j > 1$ and $f(t) = \sum_{i=0}^{n} a_i t^{ij} \in K[t; \sigma]$. Then

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

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

Proposition 8. Let B be a subring of D.
(i) f is B-weak semi-invariant if and only if $B \subseteq \text{Nuc}_r(S_f)$.
(ii) If f is B-weak semi-invariant but not right invariant, then $B \subseteq \text{Nuc}(S_f) \subseteq D$.

Proof. (i) If $f \in R$ is B-weak semi-invariant, $fB \subseteq Df \subseteq Rf$ and hence $B \subseteq \text{Nuc}_r(S_f)$. Conversely, if $B \subseteq \text{Nuc}_r(S_f)$ then for all $b \in B$, there exists $q(t) \in R$ such that $f(t)b = q(t)f(t)$. Comparing degrees, we see $q(t) \in D$ and thus $fB \subseteq Df$.
(ii) If f is B-weak semi-invariant but not right invariant, the assertion follows from (i) and [35, Theorem 4]. $\qquad\square$

Proposition 9. Let B be a subring of D and $f \in R$ be a right B-weak invariant polynomial. Then

$$B \oplus Bt \oplus \cdots \oplus Bt^{m-1} \subset \text{Nuc}_r(S_f).$$

Proof. (i) If $f \in R$ is a right B-weak invariant polynomial then $B \subset \text{Nuc}_r(S_f)$ by Proposition 8. Since $f(t)t = (bt + a)f(t)$ for some $a, b \in B$, we have $ft \in Rf$ which implies $t \in \text{Nuc}_r(S_f)$, hence the powers of t are associative. This in turn implies $t^m t = tt^m$ ([35, Theorem 5] and [30]). Now $\text{Nuc}_r(S_f)$ is an associative subalgebra of S_f, thus $B \oplus Bt \oplus \cdots \oplus Bt^{m-1} \subset \text{Nuc}_r(S_f)$. $\qquad\square$

We then obtain results similar to Theorem 6 (i), (iii) and (v) for B-weak semi-invariant polynomials:

Proposition 10. Let $f(t) = \sum_{i=0}^{m} a_i t^i \in D[t; \sigma, \delta]$ be monic of degree m and B a subring of D.
(i) f is B-weak semi-invariant if and only if $f(t)c = \sigma^m(c)f(t)$ for all $c \in B$, if and only if

$$\sigma^m(c)a_j = \sum_{i=j}^{m} a_i \Delta_{i,j}(c) \tag{5}$$

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

$$ca_j = \sum_{i=j}^{m} \binom{i}{j} a_i \delta^{i-j}(c) \tag{6}$$

for all $c \in B$, $j \in \{0, \ldots, m-1\}$.

Proof. (i) We have

$$(7) \qquad f(t)c = \sum_{i=0}^{m} a_i t^i c = \sum_{i=0}^{m} a_i \sum_{j=0}^{i} \Delta_{i,j}(c) t^j = \sum_{j=0}^{m} \sum_{i=j}^{m} a_i \Delta_{i,j}(c) t^j$$

for all $c \in B$, hence the t^m coefficient of $f(t)c$ is $\Delta_{m,m}(c) = \sigma^m(c)$, and so f is B-weak semi-invariant if and only if $f(t)c = \sigma^m(c) f(t)$ for all $c \in B$. Comparing the t^j coefficient of (7) and $\sigma^m(c) f(t)$ for all $j \in \{0, \ldots, m-1\}$ yields (5).

(ii) When $\delta = 0$, $\Delta_{i,j} = 0$ unless $i = j$ in which case $\Delta_{j,j} = \sigma^j$. Therefore (5) simplifies to $\sigma^m(c) a_j = a_j \sigma^j(c)$ for all $c \in B$, $j \in \{0, \ldots, m-1\}$.

(iii) When $\sigma = id$ we have

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

for all $c \in D$ by [20, (1.1.26)] and thus

$$(8) \qquad f(t)c = \sum_{i=0}^{m} a_i t^i c = \sum_{i=0}^{m} a_i \sum_{j=0}^{i} \binom{i}{j} \delta^{i-j}(c) t^j = \sum_{j=0}^{m} \sum_{i=j}^{m} \binom{i}{j} a_i \delta^{i-j}(c) t^j$$

for all $c \in B$. Furthermore f is B-weak semi-invariant is equivalent to $f(t)c = cf(t)$ for all $c \in B$ by (i). Comparing the t^j coefficient of (8) and $cf(t) = \sum_{i=0}^{m} ca_i t^i$ for all $c \in B$, $j \in \{0, \ldots, m-1\}$ yields (6). $\square$

4. (RIGHT) DIVISION ALGEBRAS OBTAINED FROM PETIT ALGEBRAS

Petit algebras can be used to find classes of algebras that are right but not left division algebras.

Let D be a division algebra with center F and $R = D[t; \sigma, \delta]$. We say $f \in R$ is *bounded* if there exists $0 \neq f^* \in R$ such that $Rf^* = f^*R$ is the largest two-sided ideal of R contained in Rf. The element f^* is determined by f up to multiplication on the left by elements of $D^\times$. If $f \in R$ is irreducible then $E(f)$ is a division ring [30, p. 13-07].

Remark 11. If σ is an automorphism and f is bounded, then f is irreducible if and only if $E(f) = \mathrm{Nuc}_r(S_f)$ is an associative division algebra [15, Proposition 4] which sums up classical results from [22]. The condition that f is bounded is necessary here, as is shown in [15, Example 3] where $f \in \mathbb{Q}(x)[t; d/dt]$ is reducible in the differential operator ring $\mathbb{Q}(x)[t; d/dt]$, but $\mathrm{Nuc}_r(S_f)$ is a division algebra. For instance, if D is a finite field and $\delta = 0$, all polynomials are bounded and hence f is irreducible if and only if $E(f)$ is a finite field [13, Theorem 3.3].

The argument leading up to [30, Section 2., (6)] implies that S_f has no zero divisors if and only if f is irreducible, which is in turn equivalent to S_f being a right division ring (i.e., right multiplication R_a in S_f is bijective for all $0 \neq a \in S_f$):

Theorem 12. *([30, (6)], but without a full proof). Let $f \in R$ have degree m and $0 \neq a \in S_f$.*
(i) R_a is bijective is equivalent to 1 being a greatest common right divisor of f and a (i.e., $Da(t) + Df(t) = D$).
(ii) S_f is a right division algebra if and only if f is irreducible, if and only if S_f has no zero

divisors.

(iii) If f is irreducible then L_a is injective for all $0 \neq a \in S_f$.

Proof. (i) Let $0 \neq a \in S_f$. Since S_f is a free left D-module of finite rank m and R_a is left D-linear, R_a is bijective if and only if it is injective [19, Chapter IV, Corollary 2.14], which is equivalent to $\ker(R_a) = \{0\}$. Now $R_a(z) = za = 0$ is equivalent to $za \in Rf$, which means we can write

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

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

Let $b \in R$ be a right greatest common divisor of a and f. Then $\deg(f) + \deg(a) = \deg(g) + \deg(b) = \deg(ha) + \deg(b)$ by [20, Proposition 1.3.1], and so $\deg(b) = \deg(f) - \deg(h)$. Thus $\deg(h) \leq m - 1$ if and only if $\deg(b) \geq 1$. We conclude $\ker(R_a) = \{0\}$ if and only if $\deg(b) = 0$, if and only if 1 is a right greatest common divisor of $f(t)$ and a. In particular, S_f is a right division algebra if and only if R_a is bijective for all $0 \neq a \in S_f$, if and only if 1 is a right greatest common divisor of $f(t)$ and a for all $0 \neq a \in S_f$, if and only if $f(t)$ is irreducible.

(ii) If f is irreducible then L_a and R_a are injective for all $0 \neq a \in S_f$ (i), therefore S_f has no zero divisors. The converse of the last equivalence statement is trivial.

(iii) If R_h is bijective this automatically implies that L_h is injective, for all $0 \neq h \in S_f$. □

Lemma 13. *If $f \in R$ is right invariant, then S_f is associative and a division algebra if and only if f is irreducible.*

Proof. Suppose f is right invariant. Then S_f is associative by [35, Theorem 4]. If f is reducible then S_f is trivially not a division algebra. Conversely, if f is irreducible the maps R_b are bijective for all $0 \neq b \in S_f$ by Theorem 12. This implies the maps L_b are also bijective for all $0 \neq b \in S_f$ by [7, Lemma 1B], and so S_f is a division algebra. □

This implies a generalization of Theorem [35, Theorem 4]:

Theorem 14. *Let $f(t) = \sum_{i=0}^{m} a_i t^i \in D[t; \sigma]$ be monic and $a_0 \neq 0$. Then for every $j \in \{1, \ldots, m-1\}$, L_{t^j} is surjective if and only if σ is surjective. In particular, if σ is not surjective then S_f is not a left division algebra.*

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

$$L_t(z) = t \circ z = \sum_{i=0}^{m-2} \sigma(z_i) t^{i+1} + \sigma(z_{m-1}) t \circ t^{m-1}$$

(9)

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

$\Rightarrow$: Suppose L_t is surjective, then given any $b \in D$ there exists $z \in S_f$ such that $t \circ z = b$. The t^0-coefficient of $L_t(z)$ is $\sigma(z_{m-1})a_0$ by (9), and thus for all $b \in D$ there exists $z_{m-1} \in D$

such that $\sigma(z_{m-1})a_0 = b$. Therefore σ is surjective.

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

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

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

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

by (9), which implies L_t is surjective.

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

(10) $$L_{t^j} = L_t^j,$$

for all $j \in \{1, \ldots, m-1\}$, then it follows σ is surjective if and only if L_t is surjective if and only if $L_t^j = L_{t^j}$ is surjective. In the special case when $D = \mathbb{F}_q$ is a finite field, σ is an automorphism and f is monic and irreducible, the equality (10) is proven in [24, p. 12]. A similar proof also works in our context: suppose inductively that $L_{t^j} = L_t^j$ for some $j \in \{1, \ldots, m-2\}$. Then $L_t^j(b) = t^j b \bmod_r f$ for all $b \in R_m$. Let $L_t^j(b) = b'$ so that $t^j b = qf + b'$ for some $q \in R$. We have

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

hence (10) follows by induction. $\square$

Recall that for $\delta = 0$, L_t is a *pseudo-linear transformation*, i.e. $L_t(ah(t)) = \sigma(a)L_t(h(t))$ for all $a \in S$, $h(t) \in S_f$, and that $L_h = h(t)(L_t) = \sum_{i=0}^{m-1} a_i L_t^i$ for $h(t) = \sum_{i=0}^{m-1} a_i t^i$. If f is irreducible, then L_t is irreducible, that means the only L_t-invariant subspaces of the left D-module D^m are $\{0\}$ and D^m, as pointed out in [24].

Corollary 15. *Suppose σ is not surjective and $f \in D[t; \sigma]$ is irreducible. Then S_f has no zero divisors and is a right division algebra but not a left division algebra. In particular, S_f is an infinite-dimensional D_0-algebra.*

The following result was stated but not proved by Petit [30, (7)]:

Theorem 16. *Let $f \in D[t; \sigma, \delta]$ be such that S_f is either a finite-dimensional D_0-vector space or a right $\mathrm{Nuc}_r(S_f)$-module which is free of finite rank. Then S_f is a division algebra if and only if f is irreducible.*

Proof. When S_f is associative the assertion follows by Lemma 13 so suppose S_f is not associative. If f is reducible, S_f is not a division algebra. Conversely, suppose f is irreducible, so that S_f is a right division algebra by Theorem 12. Let $0 \neq a \in S_f$ be arbitrary, then L_a is injective for all $0 \neq a \in S_f$ by Lemma 12. We prove L_a is surjective, hence that S_f is also a left division algebra:

(i) If S_f is a finite-dimensional D_0-vector space then L_a is clearly surjective by [19, Chapter IV, Corollary 2.14], since L_a is F-linear.

(ii) Suppose S_f is a free right $\mathrm{Nuc}_r(S_f)$-module of finite rank, then $E(f)$ is a division ring. Furthermore, L_a is right $\mathrm{Nuc}_r(S_f)$-linear. Therefore L_a is again surjective by [19, Chapter IV, Corollary 2.14]. $\qquad\square$

Theorem 17. *Let σ be an automorphism of D, B be a subring of D such that D is a free right B-module of finite rank, and $f \in D[t; \sigma, \delta]$ be B-weak semi-invariant. Then S_f is a division algebra if and only if f is irreducible. In particular, if σ is an automorphism of D and f is right semi-invariant then S_f is a division algebra if and only if f is irreducible.*

Proof. If f is reducible then S_f is not a division algebra. Conversely, suppose f is irreducible. Then S_f is a right division algebra by Theorem 12 so we are left to show S_f is also a left division algebra. Let $0 \neq a \in S_f$ be arbitrary and recall L_a is injective by Lemma 12. Since f is B-weak semi-invariant, $B \subseteq \mathrm{Nuc}_r(S_f)$ which implies that L_a is right B-linear. S_f is a free right D-module of rank $m = \deg(f)$ because σ is an automorphism. Since D is a free right B-module of finite rank then also S_f is a free right B-module of finite rank. Thus [19, Chapter IV, Corollary 2.14] implies L_a is bijective as required. $\qquad\square$

Theorem 18. *Let $f \in R = D[t; \sigma, \delta]$ be irreducible. Then f is bounded if and only if S_f is free of finite rank as a $\mathrm{Nuc}_r(S_f)$-module. In this case, S_f is a division algebra.*

Proof. The first part of the statement is [8, Theorem 4]. Since f irreducible, S_f is a right division algebra and L_a is injective for all $0 \neq a \in S_f$ as observed in [30, Section 2., (7)]. The second part then follows from the fact that S_f is free of finite rank as a $\mathrm{Nuc}_r(S_f)$-module, which means the injective $\mathrm{Nuc}_r(S_f)$-linear map L_a is also surjective. $\qquad\square$

For $\sigma = 0$ this is [37, Theorem 2].

Corollary 19. *Let $f \in R = D[t; \sigma, \delta]$ be irreducible.*
(i) Let σ be surjective and $D = \mathrm{Nuc}_r(S_f)$. Then f is bounded and S_f is a division algebra.
(ii) Let f be bounded, then S_f is a division algebra.

Proof. (i) If σ is surjective then S_f is a right D-module, free of rank m. Since $D = \mathrm{Nuc}_r(S_f)$, Theorem 18 yields the assertion.
(ii) is trivial. $\qquad\square$

If σ is an automorphism, $R = D[t; \sigma, \delta]$ has finite rank over its center if and only if D is of finite rank over $C_t = \{a \in F \mid at = ta\}$ if and only if all polynomials of R are bounded and if for all f of degree non-zero, $\deg(f^*)/\deg(f)$ is bounded in $\mathbb{Q}$ (f^* being the bound of f) [9, Theorem IV]. Since $C_t = \mathrm{Const}(\delta) \cap \mathrm{Fix}(\sigma) = D_0 \subset F$ we conclude:

Proposition 20. *Assume $R = D[t; \sigma, \delta]$, σ is an automorphism, and one of the two following equivalent conditions hold:*
(i) $R = D[t; \sigma, \delta]$ has finite rank over its center;
(ii) D has finite rank over D_0.
Then every $f \in R$ is bounded. In particular, if f is irreducible then S_f is a division algebra.

For $\sigma = 0$, this is [37, Proposition 3].

Suppose now that σ is an automorphism. Then S_f is a free right D-module of rank m and since L_a is $\mathrm{Nuc}_r(S_f)$-linear for any non-zero $a \in S_f$, in this case S_f is a division algebra for an irreducible f if $D \subset \mathrm{Nuc}_r(S_f)$ or if there is a subalgebra $B \subset D$ such that $B \subset \mathrm{Nuc}_r(S_f)$ and D has finite rank as a right B-module (these conditions were not stated in [30, p. 13-14] but seem necessary). We obtain:

Proposition 21. *Suppose that σ is an automorphism and f is irreducible.*
(i) If $D \subset \mathrm{Nuc}_r(S_f)$ then S_f is a division algebra.
(ii) If there is a subalgebra $B \subset D$ such that $B \subset \mathrm{Nuc}_r(S_f)$ and D is free of finite rank as a right B-module then S_f is a division algebra.

Proof. S_f is a right D-module and left multiplication L_a is $\mathrm{Nuc}_r(S_f)$-linear, so in particular D-linear. Since f is irreducible, L_a is injective for all nonzero $a \in S_f$. If $D \subset \mathrm{Nuc}_r(S_f)$ then S_f is a free right D-module of rank m, and if there is a subalgebra $B \subset D$ such that $B \subset \mathrm{Nuc}_r(S_f)$ and S is free of finite rank as a right B-module, then S_f is a free right B-module of finite rank. Thus L_a is bijective for all nonzero $a \in S_f$. $\qquad\square$

5. Irreducibility criteria for some polynomials in $R = D[t; \sigma]$

Let D be a division algebra over F and $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R = D[t; \sigma]$.

5.1. There are already several irreducibility criteria for f available in the literature. We start by collecting some that are useful for constructing (right) division algebras S_f for the convenience of the reader.

We first determine the remainder after dividing $f(t)$ on the right by $t - b$ where $b \in D$. By [20, p. 15ff] we have $(t - b)|_r f(t)$ is equivalent to

$$(11) \qquad a_m N_m(b) - \sum_{i=0}^{m-1} a_i N_i(b) = 0$$

where $N_i(b) = \sigma^{i-1}(b) \cdots \sigma(b) b$ for $i > 0$ and $N_0(b) = 1$, i.e. to this remainder being zero.

When σ is an automorphism of D, we can also determine the remainder after dividing $f(t)$ on the left by $(t - b)$, $b \in D$: Similarly to [20, p. 15ff] we have

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

for all $i \in \mathbb{N}$. Multiplying (12) on the right by $\sigma^{-i}(a_i)$, and using $a_i t^i = t^i \sigma^{-i}(a_i)$ gives

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

Summing over i, we obtain

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

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

Proposition 22. *Suppose σ is an automorphism. Then $(t-b)|_l f(t)$ if and only if $M_m(b) - \sum_{i=0}^{m-1} M_i(b)\sigma^{-i}(a_i) = 0$.*

Corollary 23. *Suppose σ is an automorphism and $f(t) = t^m - a \in D[t;\sigma]$. Then $f(t)$ has a left linear divisor if and only if it has a right linear divisor.*

Proof. Let $b \in D$, then $(t-b)|_r f(t)$ is equivalent to $\sigma^{m-1}(b)\cdots\sigma(b)b = a$ by (11), if and only if $c\sigma^{-1}(c)\cdots\sigma^{1-m}(c) = a$ where $c = \sigma^{m-1}(b)$, if and only if $(t-c)|_l f(t)$ by Proposition 22. □

Theorem 24. *[30, (17), (18)] (i) $f(t) = t^2 - a_1 t - a_0 \in D[t;\sigma]$ is irreducible if and only if*

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

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

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

and

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

for all $b \in D$.

Corollary 25. *Suppose σ is an automorphism, then $f(t) = t^3 - a \in D[t;\sigma]$ is irreducible if and only if $\sigma^2(b)\sigma(b)b \neq a$ for all $b \in D$.*

Proof. By Corollary 23, $f(t)$ has a right linear divisor if and only if it has a left linear divisor. Therefore $f(t)$ is irreducible if and only if $(t-b) \nmid_r f(t)$ for all $b \in D$, if and only if $\sigma^2(b)\sigma(b)b \neq a$ for all $b \in D$ by (11). □

Lemma 26. *Let $f(t) \in R = D[t;\sigma]$ and suppose $f(t) = q(t)g(t)$ for some $q(t), g(t) \in R$. Then $f(bt) = q(bt)g(bt)$ for all $b \in D_0 = F \cap \mathrm{Fix}(\sigma)$.*

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

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

and so we obtain for all $b \in D_0$:

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

$$= \sum_{i=0}^l \sum_{j=0}^n q_i \sigma^i(g_j)(bt)^{i+j} = f(bt).$$

□

Theorem 27. *[3, p. 344] Let σ be an endomorphism of D, $f(t) = t^m - a \in R = D[t;\sigma]$ and suppose $D_0 = F \cap \mathrm{Fix}(\sigma)$ contains a primitive mth root of unity ω. If $g(t) \in R$ is a monic irreducible polynomial dividing $f(t)$ on the right, then the degree d of $g(t)$ divides m and $f(t)$ is the product of m/d polynomials of degree d.*

For a proof of Theorem 27 see [4]; the special case where σ is an automorphism of order m is shown in [12, Proposition 3.7.5].

Theorem 27 implies [1, Lemma 10], cf. also [36, Theorem 6 (iii)], which improves [30, (19)]:

Theorem 28. *Suppose m is prime, σ is an endomorphism of D and $D_0 = F \cap \mathrm{Fix}(\sigma)$ contains a primitive mth root of unity. Then $f(t) = t^m - a \in D[t; \sigma]$ is irreducible if and only if it has no right linear divisors, if and only if*

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

for all $b \in D$.

Proof. Let $g(t) \in D[t; \sigma]$ be an irreducible polynomial of degree d dividing $f(t)$ on the right. Without loss of generality $g(t)$ is monic, otherwise if $g(t)$ has leading coefficient $c \in D^\times$, then $c^{-1}g(t)$ is monic and also right divides $f(t)$. Thus d divides m by Theorem 27 and since m is prime, either $d = m$, in which case $g(t) = f(t)$, or $d = 1$, which means $f(t)$ can be written as a product of m linear factors. Therefore $f(t)$ is irreducible if and only if $(t - b) \nmid_r f(t)$ for all $b \in D$, if and only if $a \neq \sigma^{m-1}(b) \cdots \sigma(b)b$, for all $b \in D$ by (11). $\qquad\square$

5.2. Skew polynomials of degree four. Suppose σ is an automorphism of D and $f(t) = t^4 - a_3 t^3 - a_2 t^2 - a_1 t - a_0 \in R = D[t; \sigma]$. Then either $f(t)$ is irreducible, $f(t)$ is divisible by a linear factor from the right, from the left, or $f(t) = g(t)h(t)$ for some $g(t), h(t) \in R$ of degree 2. In (11) and Proposition 22 we computed the remainders after dividing $f(t)$ by a linear polynomial on the right and the left. We now compute the remainder after dividing $f(t)$ by $t^2 - ct - d$ on the right, with $c, d \in D$. To do this we use the identities

$$(13) \qquad t^2 = (t^2 - ct - d) + (ct + d),$$

$$(14) \qquad t^3 = (t + \sigma(c))(t^2 - ct - d) + (\sigma(d) + \sigma(c)c)t + \sigma(c)d,$$

and

$$(15) \qquad \begin{aligned} t^4 &= (t^2 + \sigma^2(c)t + \sigma^2(d) + \sigma^2(c)\sigma(c))(t^2 - ct - d) \\ &\quad + (\sigma^2(c)\sigma(c)c + \sigma^2(d)c + \sigma^2(c)\sigma(d))t + \sigma^2(d)d + \sigma^2(c)\sigma(c)d. \end{aligned}$$

If we define

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

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

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

then multiplying (13), (14) and (15) on the left by a_i and summing over i yields

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

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

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

which evidently implies:

Proposition 29. $f(t) = t^4 - a_3t^3 - a_2t^2 - a_1t - a_0 \in R = D[t;\sigma]$. $(t^2 - ct - d)|_r f(t)$ is equivalent to

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

and

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

Propositions 22 and 29 together with (11) yield:

Theorem 30. $f(t) = t^4 - a_3t^3 - a_2t^2 - a_1t - a_0 \in R = D[t;\sigma]$ is irreducible if and only if

(16) $$\sigma^3(b)\sigma^2(b)\sigma(b)b + a_3\sigma^2(b)\sigma(b)b + a_2\sigma(b)b + a_1b + a_0 \neq 0,$$

and

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

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

(18) $$\sigma^2(c)\sigma(c)c + \sigma^2(d)c + \sigma^2(c)\sigma(d) + a_3(\sigma(d) + \sigma(c)c) + a_2c + a_1 \neq 0,$$

or

(19) $$\sigma^2(d)d + \sigma^2(c)\sigma(c)d + a_3\sigma(c)d + a_2d + a_0 \neq 0.$$

I.e., $f(t)$ is irreducible if and only if (16) and (17) and ((18) or (19)) hold.

Proof. $f(t)$ is irreducible if and only if $(t-b) \nmid_r f(t)$ for all $b \in D$, $(t-b) \nmid_l f(t)$ for all $b \in D$ and $(t^2 - ct - d) \nmid_r f(t)$ for all $c, d \in D$. Therefore the result follows from (11), Propositions 22 and 29. $\square$

Lemma 31. Let $f(t) = t^4 - a \in R$. Suppose $(t - b)|_r f(t)$, then $f(t) = (t + \sigma^3(b))(t^2 + \sigma^2(b)\sigma(b))(t - b)$ and $f(t) = (t^2 + \sigma^3(b)\sigma^2(b))(t + \sigma(b))(t - b)$ are factorisations of $f(t)$. In particular, $(t + \sigma(b))(t - b) = t^2 - \sigma(b)b$ also right divides $f(t)$.

Proof. Multiplying out these factorisations gives $t^4 - \sigma^3(b)\sigma^2(b)\sigma(b)b$ which is equal to $f(t)$ by (11). $\square$

Hence if $f(t) = t^4 - a$ has a right linear divisor then it also has a right quadratic divisor and Theorem 30 simplifies to:

Corollary 32. $f(t) = t^4 - a \in R$ is reducible if and only if

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

for some $c, d \in D$.

Proof. By Corollary 23, $f(t)$ has a right linear divisor if and only if it has a left linear divisor. Moreover if $f(t)$ has a right linear divisor then it also has a quadratic right divisor by Lemma 31, therefore $f(t)$ is reducible if and only if $(t^2 - ct - d)|_r f(t)$ for some $c, d \in D$. The result now follows from Proposition 29. $\square$

5.3. Examples in $\mathbb{F}_{p^h}[t;\sigma]$. Let $K = \mathbb{F}_{p^h}$ be a finite field of order p^h for some prime p and σ be a non-trivial $\mathbb{F}_p$-automorphism of K. This means $\sigma : K \to K$, $k \mapsto k^{p^r}$, for some $r \in \{1,\ldots,h-1\}$. Here σ has order $n = h/\gcd(r,h)$ and $\mathrm{Gal}(K/\mathrm{Fix}(\sigma)) = \langle \sigma \rangle$. Algorithms for efficiently factorising polynomials in $\mathbb{F}_{p^h}[t;\sigma]$ exist, see [13] or more recently [10].

Lemma 33. $\gcd(p^h - 1, p^r - 1) = p^{\gcd(h,r)} - 1$.

Proof. Let $d = \gcd(r,h)$ so that $h = dn$. We have
$$p^h - 1 = (p^d - 1)(p^{d(n-1)} + \ldots + p^d + 1),$$
therefore $p^h - 1$ is divisible by $p^d - 1$. A similar argument shows $(p^d - 1)|(p^r - 1)$. Suppose that c is a common divisor of $p^h - 1$ and $p^r - 1$, this means $p^h \equiv p^r \equiv 1 \bmod (c)$. Write $d = hx + ry$ for some integers x, y, then we have
$$p^d = p^{hx+ry} = (p^h)^x (p^r)^y \equiv 1 \bmod (c)$$
which implies $c|(p^d - 1)$ and hence $p^d - 1 = \gcd(p^h - 1, p^r - 1)$. $\qquad\square$

Given $k \in K^\times$, we have $k \in \mathrm{Fix}(\sigma)$ if and only if $k^{p^r-1} = 1$, if and only if k is a $(p^r - 1)^{\mathrm{th}}$ root of unity. There are $\gcd(p^r - 1, p^h - 1)$ such roots of unity in K, thus
$$|\mathrm{Fix}(\sigma)| = \gcd(p^r - 1, p^h - 1) + 1 = p^{\gcd(r,h)}$$
by Lemma 33 and so $\mathrm{Fix}(\sigma) \cong \mathbb{F}_q$ where $q = p^{\gcd(r,h)}$.

Proposition 34. *(i) Suppose $n \in \{2,3\}$, then $f(t) = t^n - a \in K[t;\sigma]$ is irreducible if and only if $a \in K \setminus \mathrm{Fix}(\sigma)$.*
(ii) Suppose n is a prime and $n|(q - 1)$. Then $f(t) = t^n - a \in K[t;\sigma]$ is irreducible if and only if $a \in K \setminus \mathrm{Fix}(\sigma)$.
In particular, in both (i) and (ii), there are precisely $p^h - q$ irreducible polynomials in $K[t;\sigma]$ of the form $t^n - a$ for some $a \in K$.

Proof. (i) $f(t)$ is irreducible if and only if $\prod_{l=0}^{n-1} \sigma^l(b) = N_{K/\mathrm{Fix}(\sigma)}(b) \neq a$ for all $b \in K$ by Theorem 24 or Corollary 25, where $N_{K/\mathrm{Fix}(\sigma)}$ is the field norm. It is well-known that as K is a finite field, $N_{K/\mathrm{Fix}(\sigma)} : K^\times \to \mathrm{Fix}(\sigma)^\times$ is surjective and so $f(t)$ is irreducible if and only if $a \notin \mathrm{Fix}(\sigma)$. There are $p^h - q$ elements in $K \setminus \mathrm{Fix}(\sigma)$, hence there are precisely $p^h - q$ irreducible polynomials of the form $t^n - a$ for some $a \in K$.
(ii) $\mathrm{Fix}(\sigma) \cong \mathbb{F}_q$ contains a primitive n^{th} root of unity because $n|(q - 1)$ [23, Proposition II.2.1]. The rest of the proof is similar to (i) but uses Theorem 28. $\qquad\square$

Let $a, b \in K$ and recall $(t - b)|_r(t^m - a)$ is equivalent to $a = \sigma^{m-1}(b) \cdots \sigma(b)b = b^s$ by (11) where $s = \sum_{j=0}^{m-1} p^{rj} = (p^{mr} - 1)/(p^r - 1)$. Suppose z generates the multiplicative group $K^\times$. Writing $b = z^l$ for some $l \in \mathbb{Z}$ yields $(t - b)|_r(t^m - a)$ if and only if $a = z^{ls}$. This implies the following:

Proposition 35. *Let $f(t) = t^m - a \in K[t;\sigma]$ and write $a \in K$ as $a = z^u$ for some $u \in \{0,\ldots,p^h - 2\}$.*
(i) $(t - b) \nmid_r f(t)$ for all $b \in K$ if and only if $u \notin \mathbb{Z}s \bmod (p^h - 1)$.
(ii) If $m \in \{2,3\}$ then $f(t)$ is irreducible if and only if $u \notin \mathbb{Z}s \bmod (p^h - 1)$.

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

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

(ii) $f(t)$ has a left linear divisor if and only if it has a right linear divisor by Corollary 23. Therefore if $m \in \{2, 3\}$ then $f(t)$ is irreducible if and only if $(t-b) \nmid_r f(t)$ for all $b \in K$ and so the assertion follows by (i).

(iii) If m is a prime divisor of $(q-1)$ then $\mathrm{Fix}(\sigma) \cong \mathbb{F}_q$ contains a primitive m^{th} root of unity. Therefore the result follows by (i) and Theorem 28.   □

Corollary 36. *(i) There exists $a \in K$ such that $(t-b) \nmid_r (t^m - a)$ for all $b \in K$ if and only if $\gcd(s, p^h - 1) > 1$.*
(ii) [30, (22)] Suppose $m \in \{2, 3\}$ or m is a prime divisor of $(q-1)$. Then there exists $a \in K^{\times}$ such that $t^m - a \in K[t; \sigma]$ is irreducible if and only if $\gcd(s, p^h - 1) > 1$.

Proof. There exists $u \in \{0, \ldots, p^h - 2\}$ such that $u \notin \mathbb{Z}s \mod (p^h - 1)$, if and only if s does not generate $\mathbb{Z}_{p^h - 1}$, if and only if $\gcd(s, p^h - 1) > 1$. Hence the result follows by Proposition 35.   □

Corollary 37. *Suppose $p \equiv 1 \mod m$.*
(i) There exists $a \in K$ such that $(t-b) \nmid_r (t^m - a)$ for all $b \in K$.
(ii) If p is an odd prime, then there exists $a \in K^{\times}$ such that $t^2 - a \in K[t; \sigma]$ is irreducible.
(iii) If $m = 3$, then there exists $a \in K^{\times}$ such that $t^3 - a \in K[t; \sigma]$ is irreducible.
(iv) Suppose m is a prime divisor of $(q-1)$, then there exists $a \in K^{\times}$ such that $t^m - a \in K[t; \sigma]$ is irreducible.

Proof. We have

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

and $p^h \equiv 1 \mod m$. This means $m | s$ and $m | (p^h - 1)$, therefore $\gcd(s, p^h - 1) \geq m$ and so the assertion follows by Corollary 36.   □

6. IRREDUCIBILITY CRITERIA FOR POLYNOMIALS OF DEGREE TWO AND THREE AND FOR
$t^m - a$ IN $D[t; \sigma, \delta]$

In this Section we generalize some results from Section 5 to polynomials in $R = D[t; \sigma, \delta]$, where D is a division ring with center F and σ an endomorphism of D. We recursively define a sequence of maps $N_i : D \to D$, $i \geq 0$, by

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

i.e., $N_1(b) = b$, $N_2(b) = \sigma(b)b + \delta(b), \ldots$

Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$. Then $(t-b)|_r f(t)$ is equivalent to

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

[25, Lemma 2.4].

If σ is an automorphism of D, we can also view $R = D[t; \sigma, \delta]$ as a right polynomial ring. In particular, this means we can write $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R$ in the form $f(t) = t^m - \sum_{i=0}^{m-1} t^i a_i'$ for some uniquely determined $a_i' \in D$. To find the remainder after left division of $f(t)$ by $(t - b)$, we recursively define a sequence of maps $M_i : D \to D$, $i \geq 0$, by

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

that is $M_0(b) = 1, \ M_1(b) = b, \ M_2(b) = b\sigma^{-1}(b) - \delta(\sigma^{-1}(b)), \dots$

Proposition 38. *Suppose σ is an automorphism of D. Then $(t - b)|_l f(t)$ is equivalent to $M_m(b) - \sum_{i=0}^{m-1} M_i(b)a_i' = 0$. In particular, $(t - b)|_l (t^m - a)$ if and only if $M_m(b) \neq a$.*

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

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

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

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

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

for some $q(t) \in R$. $\qquad\square$

Theorem 39. *(i) $f(t) = t^2 - a_1 t - a_0 \in D[t; \sigma, \delta]$ is irreducible if and only if $\sigma(b)b + \delta(b) - a_1 b - a_0 \neq 0$ for all $b \in D$.*
(ii) Suppose σ is an automorphism of D and $f(t) = t^3 - a_2 t^2 - a_1 t - a_0 \in D[t; \sigma, \delta]$. Write $f(t) = t^3 - t^2 a_2' - t a_1' - a_0'$ for some unique $a_0', a_1', a_2' \in D$. Then $f(t)$ is irreducible if and only if

$$(21) \qquad N_3(b) - \sum_{i=0}^{2} a_i N_i(b) \neq 0 \ and \ M_3(b) - \sum_{i=0}^{2} M_i(b)a_i' \neq 0,$$

for all $b \in D$.

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

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

for all $b \in D$ by (20).
(ii) $f(t)$ is irreducible if and only if it has no left or right linear factors, if and only if (21) holds for all $b \in D$ by (20) and Proposition 38.

$\qquad\square$

We can thus generalize Theorem 28:

Theorem 40. *Suppose m is prime,* $\operatorname{char}(D) \neq m$ *and* $F \cap \operatorname{Fix}(\sigma)$ *contains a primitive mth root of unity ω. Then $f(t) = t^m - a \in D[t; \sigma, \delta]$ is irreducible if and only if $N_m(b) \neq a$ for all $b \in D$.*

Proof. Recall that $\delta(b^n) = \sum_{i=0}^{n-1} \sigma(b)^i \delta(b) b^{n-1-i}$ for all $b \in D$, $n \geq 1$ by [16, Lemma 1.1] and so

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

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

where we have used $\omega \in F \cap \operatorname{Fix}(\sigma)$. Therefore $\omega \in \operatorname{Const}(\delta)$ because $\operatorname{char}(D) \neq m$, hence also $\omega^i \in \operatorname{Const}(\delta)$ and so $(\omega t)^i = \omega^i t^i$ for all $i \in \{1, \ldots, m\}$. Furthermore if $b \in D$, then $(t - b) \nmid_r f(t)$ is equivalent to $N_m(b) \neq a$ by (20). The proof now follows exactly as in Theorem 24. $\qquad\square$

Corollary 41. *Suppose* $\operatorname{char}(D) \neq 3$, $\sigma = \operatorname{id}$ *and* $F \cap \operatorname{Fix}(\sigma)$ *contains a primitive third root of unity. Then $f(t) = t^3 - a \in D[t; \delta]$ is irreducible if and only if*

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

for all $b \in D$.

References

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

[2] J. Bergen, M. Giesbrecht, P. N. Shivakumar, Y. Zhang, *Factorizations for difference operators.* Advances in Difference Equations 57 (2015), DOI 10.1186/s13662-015-0402-1 (Springer)

[3] N. Boubaki, "Éléments de mathématique. Fasc. XXIII. Algèbre; Chapitre 8, modules e anneaux semi-simples." Hermann, 1973.

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

[5] C. Brown, S. Pumplün, *The automorphisms of Petit's algebras.* Comm. Algebra 46 (2) (2018), 834-849.

[6] C. Brown, S. Pumplün, *Nonassociative cyclic extensions of fields and central simple algebras.* J. Pure Applied Algebra 223 (6) 2019, 2401-2412.

[7] R. H. Bruck, *Contributions to the theory of loops.* Trans. AMS 60 (2) (1946), 245-345.

[8] J. Carcanague, *Ideaux bilaterales d'un anneau de polynomes non commutatifs sur un corps.* J. Algebra (18) 1971, 1-18.

[9] J. Carcanague, *Quelques resultats sur les anneaux de Ore.* C. R. Acad. Sci. Paris Sr. A-B 269 (1969), A749-A752.

[10] X. Caruso, J. Le Borgne, *A new faster algorithm for factoring skew polynomials over finite fields.* J. Symb. Comp. 79 (2017), 411-443.

[11] R. C. Churchill, Y. Zhang, *Irreducibility criteria for skew polynomials.* J. Algebra 322 (2009), 3797-3822.

[12] P. M. Cohn, "Skew fields. Theory of general division rings." Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1995.

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

[14] 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, 127134, ACM, New York, 2003.

[15] 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.

[16] K. Goodearl, *Prime ideals in skew polynomial rings and quantized Weyl algebras.* J. Algebra 150 (2) (1992), 324-377.

[17] J. Gòmez-Torrecillas, F. J. Lobillo, G. Navarro, *Computing the bound of an Ore polynomial. Applications to factorization.* J. Symbolic Comp. 2018, online at https://doi.org/10.1016/j.jsc.2018.04.018

[18] A. Granja, C. Martinez, C. Rodriguez, *Real Valuations on Skew Polynomial Rings.* Algebras and Representation Theory 17 (5) (2014), 1413-1436.

[19] Hungerford, "Algebra." Vol. 73 of Graduate Texts in Mathematics. Springer Verlag, New York, 1980.

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

[21] N. Jacobson, *Pseudo-linear transformations.* Ann. of Math. (2) 38 (1937), no. 2, 484-507.

[22] N. Jacobson, "The Theory of Rings", AMS, Providence, RI, 1943

[23] N. Koblitz, "A course in number theory and cryptography." Vol. 114, Springer Science and Business Media, 1994.

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

[25] T. Y. Lam, A. Leroy, *Vandermonde and Wroskian matrices over division rings.* J. Alg. 19(2)(1988), 308-336.

[26] T. Y. Lam, A. Leroy, *Algebraic conjugacy classes and skew-polynomial rings.* In Perspectives in Ring Theory, 153-203, Springer, 1988.

[27] T. Y. Lam, K. H. Leung, A. Leroy, J. Matczuk, *Invariant and semi-invariant polynomials in skew polynomial rings.* Ring theory 1989 (Ramat Gan and Jerusalem, 1988/1989), 247-261, Israel Math. Conf. Proc., 1, Weizmann, Jerusalem, 1989.

[28] B. Lemonnier, *Dimension de Krull et codeviations, quelques applications en theorie des modules.* PhD Thesis, Poitiers, 1984.

[29] O. Ore, *Theory of noncommutative polynomials.* Annals of Math. 34 (3) (1933), 480-508.

[30] 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.

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

[32] S. Pumplün, *Factoring skew polynomials over Hamilton's quaternion algebra and the complex numbers.* J. Algebra 427 (2015), 20-29.

[33] S. Pumplün, *Corrigendum to: "Factoring skew polynomials over Hamilton's quaternion algebra and the complex numbers" [J. Algebra 427 (2015), 20-29].* Online at http://agt2.cie.uma.es/ loos/jordan/

[34] S. Pumplün, *Nonassociative differential extensions of characteristic p.* Results in Mathematics 72 (1-2) (2017), 245-262.

[35] S. Pumplün, *Finite nonassociative algebras obtained from skew polynomials and possible applications to (f, σ, δ)-codes.* Adv. Math. Comm. 11 (3) (2017), 615-634. doi:10.3934/amc.2017046

[36] S. Pumplün, *Tensor products of nonassociative cyclic algebras.* Journal of Algebra 451 (2016), 145-165.

[37] S. Pumplün, *Algebras whose right nucleus is a central simple algebra.* J. Pure and Applied Algebra 222 (9) (2018), 2773-2783. https://doi.org/10.1016/j.jpaa.2017.10.019

[38] S. Pumplün, *How to obtain lattices from (f, σ, δ)-codes via a generalization of Construction A.* Appl. Algebra Engrg. Comm. Comput. 29 (4) (2018), 313-333.

[39] S. Pumplün, *Quotients of orders in algebras obtained from skew polynomials with applications to coding theory.* Comm. Algebra 46 (11) (2018), 5053-5072.

[40] L. Rónyai, *Factoring polynomials over finite fields.* J. Algorithms 9 (3) (1988), 391-400.

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

Email address: christian_jb@hotmail.co.uk; susanne.pumpluen@nottingham.ac.uk

School of Mathematical Sciences, University of Nottingham, University Park, Nottingham NG7 2RD, United Kingdom