FINITE NONASSOCIATIVE ALGEBRAS OBTAINED FROM SKEW POLYNOMIALS AND POSSIBLE APPLICATIONS TO (f, σ, δ)-CODES

S. PUMPLÜN

ABSTRACT. Let S be a unital ring, $S[t;\sigma,\delta]$ a skew polynomial ring where σ is an injective endomorphism and δ a left σ-derivation, and suppose $f \in S[t;\sigma,\delta]$ has degree m and an invertible leading coefficient. Using right division by f to define the multiplication, we obtain unital nonassociative algebras S_f on the set of skew polynomials in $S[t;\sigma,\delta]$ of degree less than m. We study the structure of these algebras.

When S is a Galois ring and f base irreducible, these algebras yield families of finite unital nonassociative rings A, whose set of (left or right) zero divisors has the form pA for some prime p.

For reducible f, the S_f can be employed both to design linear (f,σ,δ)-codes over unital rings and to study their behaviour.

INTRODUCTION

Let S be a unital ring. In the present paper we construct a new class of nonassociative unital rings out of subsets of the skew polynomial ring $R = S[t;\sigma,\delta]$ where σ is an injective endomorphism and δ a left σ-derivation. Given a polynomial $f \in R = S[t;\sigma,\delta]$ of degree m, whose leading coefficient is a unit, it is well-known by now (e.g., cf. [31], [26], [13] for commutative S) that it is possible to define a right division by f: for all $g(t) \in R$, there exist uniquely determined $r(t), q(t) \in R$ with $\deg(r) < m$, such that $g(t) = q(t)f(t) + r(t)$. What is much less known is the fact that we can take the additive group $\{g \in R \,|\, \deg(g) < m\}$ of skew polynomials of degree less than m, i.e. the canonical representatives of the remainders in R of right division by f, and define a nonassociative unital ring structure $\circ$ on it via $g \circ h = gh \bmod_r f$. The resulting nonassociative ring S_f, also denoted $S[t;\sigma,\delta]/S[t;\sigma,\delta]f$, is a unital nonassociative algebra over a commutative subring of S. If f is two-sided (also called invariant), i.e. if $S[t;\sigma,\delta]f$ is a two-sided ideal, then $S[t;\sigma,\delta]/S[t;\sigma,\delta]f$ is the well-known associative quotient algebra obtained by factoring out a principal two-sided ideal. This generalizes a construction introduced by Petit for the case when S is a division ring and thus $R = S[t;\sigma,\delta]$ left and right Euclidean [33].

The algebras S_f were previously introduced by Petit, but only for the case that S is a division ring, hence $S[t;\sigma,\delta]$ left and right Euclidean [33]. In that setting, they already appeared in [12], [13], [32], and were used in space-time block coding, cf. [47], [38], [39].

Date: 21.7.2016.

1991 *Mathematics Subject Classification.* Primary: 17A60; Secondary: 94B05.

Key words and phrases. skew polynomial ring, Ore polynomials, nonassociative algebra, commutative finite chain ring, generalized Galois rings, linear codes, (f,σ,δ)-codes, skew-constacyclic codes.

We present two possible applications: We first use our algebras to construct new families of finite nonassociative unital rings, especially generalized nonassociative Galois rings. Generalized nonassociative Galois rings were introduced in [17] and investigated in [18], [19], [20]. They are expected to have wide-ranging applications in coding theory and cryptography [17].

As a second application, we point out the canonical connection between the algebras S_f and cyclic (f,σ,δ)-codes. This connection was first mentioned in [36] for S being a division ring. Well-known results from the literature, e.g. on the pseudo-linear map T_f [11] and on polynomials in Ore extensions from [8] or [28], are rephrased in this setting and put into a nonassociative context.

The paper is organized as follows. We establish our basic terminology in Section 1, define the algebras S_f in Section 2 and investigate their basic structure in Section 3.

The matrix representing left multiplication with t in S_f yields the pseudolinear transformation T_f associated to f defined in [8] which is discussed in Section 4. We generalize [29, Theorem 13 (2), (3), (4)] and show that if S_f has no zero divisors then T_f is irreducible, i.e. $\{0\}$ and S^m are the only T_f-invariant left S-submodules of S^m.

In Section 5, we assume that S is a finite chain ring. If f is base irreducible then S_f is a generalized nonassociative Galois ring. This yields new families of generalized nonassociative Galois rings.

We consider the connection between the algebras S_f and cyclic (f,σ,δ)-codes, in particular skew-constacyclic codes over finite chain rings, in Section 6: We rephrase some results (for instance from [4], [5], [8], [26], [7]), by employing the algebras S_f instead of dealing with cosets in the quotient module $S[t;\sigma,\delta]/S[t;\sigma,\delta]f$. For instance, the matrix generating a cyclic (f,σ,δ)-code $\mathcal{C}\subset S^m$ represents the right multiplication R_g in S_f, calculated with respect to the basis $1,t,\ldots,t^{m-1}$, identifying an element $h=\sum_{i=0}^{m-1}a_it^i$ with the vector $(a_0,\ldots,a_{m-1})$, cf. [8]. This matrix generalizes the circulant matrix from [16] and is a control matrix of $\mathcal{C}$. We also show how to obtain semi-multiplicative maps using their right multiplication. This paper is the starting point for several applications of the algebras S_f to coding theory, e.g. to coset coding, and related areas. Some are briefly explained in Section 7.

1. Preliminaries

1.1. **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 $A\times A\mapsto A$, $(x,y)\mapsto x\cdot y$, 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 $\mathrm{Comm}(A) = \{x \in A \,|\, xy = yx \text{ for all } y \in A\}$ and the *center* of A is $\mathrm{C}(A) = \{x \in A \,|\, x \in \mathrm{Nuc}(A) \text{ and } xy = yx \text{ for all } y \in A\}$ [42].

An algebra $A \neq 0$ over a field F is called a *division algebra* if for any $a \in A$, $a \neq 0$, the left multiplication with a, $L_a(x) = ax$, and the right multiplication with a, $R_a(x) = xa$, 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.

1.2. **Skew polynomial rings.** Let S be a unital associative (not necessarily commutative) 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 $a, b \in S$, implying $\delta(1) = 0$. The *skew polynomial ring* $R = S[t; \sigma, \delta]$ is the set of skew polynomials

$$a_0 + a_1 t + \cdots + a_n t^n$$

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

$$ta = \sigma(a)t + \delta(a) \quad (a \in S).$$

That means,

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

$(a, b \in S)$, 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 $\Delta_{0,0} = id_S$, $\Delta_{1,0} = \delta$, $\Delta_{1,1} = \sigma$ and so $\Delta_{n,j}$ is the sum of all polynomials in σ and δ of degree j in σ and degree $n - j$ in δ ([25, p. 2] or [8, p. 4]). If $\delta = 0$, then $\Delta_{n,j} = \sigma^n$.

$S[t; \sigma] = S[t; \sigma, 0]$ is called a *twisted polynomial ring* and $S[t; \delta] = S[t; id, \delta]$ a *differential polynomial ring*. For $\sigma = id$ and $\delta = 0$, we obtain the usual ring of left polynomials $S[t] = S[t; id, 0]$.

For $f = a_0 + a_1 t + \cdots + a_n t^n$ 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 $\deg(g), \deg(h) < \deg(f)$ such that $f = gh$.

Suppose D is a division ring. Then $R = D[t; \sigma, \delta]$ is a left principal ideal domain (i.e., every left ideal in R is of the form Rf) and there is a right division algorithm in R [25, p. 3]: for all $g, f \in R$, $g \neq 0$, there exist unique $r, q \in R$, and $\deg(r) < \deg(f)$, such that

$$g = qf + r$$

(cf. Jacobson [25] and Petit [33], note that Jacobson calls what we call right a left division algorithm and vice versa.). If σ is a ring automorphism then $R = D[t; \sigma, \delta]$ is a left and right principal ideal domain (a PID) [25, p. 6] and there is also a left division algorithm in R [25, p. 3 and Prop. 1.1.14].

2. Nonassociative rings obtained from skew polynomials rings

From now on, let S be a unital ring and $S[t;\sigma,\delta]$ a skew polynomial ring where σ is injective. $S[t;\sigma,\delta]$ is generally neither a left nor a right Euclidean ring (unless S is a division ring). Nonetheless, we can still perform a left and right division by a polynomial $f \in R = S[t;\sigma,\delta]$, if $f(t) = \sum_{i=0}^{m} d_i t^i$ has an invertible leading coefficient $LC(f) = d_m$ (this was already observed for twisted polynomial rings and special cases of S and assuming $\sigma \in \mathrm{Aut}(S)$ for instance in [31, p. 391], [26, p. 4], [13, 3.1]):

Proposition 1. *Let $f(t) \in R = S[t;\sigma,\delta]$ have degree m and an invertible leading coefficient. (i) 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*

$$g(t) = q(t)f(t) + r(t).$$

(ii) Assume $\sigma \in \mathrm{Aut}(S)$. 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

$$g(t) = f(t)q(t) + r(t).$$

Proof. (i) Let $f(t) = \sum_{i=0}^{m} d_i t^i$ and $g(t) = \sum_{i=0}^{l} s_i t^i$ be two skew polynomials in R of degree m and l. Suppose that $l > m$ and that the leading coefficient $LC(f) = d_m$ of f is invertible. Since $1 = \sigma(d_m d_m^{-1}) = \sigma(d_m)\sigma(d_m^{-1})$, we know that $\sigma(d_m)$ and thus $\sigma^j(d_m)$ is invertible for any integer $j \geq 0$. Now

$$g(t) - s_l\sigma^{l-m}(d_m^{-1})t^{l-m}f(t) = g(t) - s_l\sigma^{l-m}(d_m^{-1})t^{l-m}(d_m t^m + \sum_{i=0}^{m-1} d_i t^i)$$

$$= g(t) - s_l\sigma^{l-m}(d_m^{-1})t^{l-m}d_m t^m - \sum_{i=0}^{m-1} s_l\sigma^{l-m}(d_m^{-1})t^{l-m}d_i t^i$$

$$= g(t) - s_l\sigma^{l-m}(d_m^{-1})(\sum_{j=0}^{l-m} \Delta_{l-m,j}(d_m)t^j)t^m - \sum_{i=0}^{m-1} s_l\sigma^{l-m}(d_m^{-1})(\sum_{j=0}^{l-m} \Delta_{l-m,j}(d_m)t^j)t^i$$

$$= g(t) - s_l\sigma^{l-m}(d_m^{-1})\Delta_{l-m,l-m}(d_m)t^l$$

$$-s_l\sigma^{l-m}(d_m^{-1})\sum_{j=0}^{l-m-1} \Delta_{l-m,j}(d_m)t^{j+m} - \sum_{i=0}^{m-1}\sum_{j=0}^{l-m} s_l\sigma^{l-m}(d_m^{-1})\Delta_{l-m,j}(d_j)t^{i+j}$$

$$= g(t) - s_l t^l$$

$$-s_l\sigma^{l-m}(d_m^{-1})\sum_{j=0}^{l-m-1} \Delta_{l-m,j}(d_m)t^{j+m} - \sum_{i=0}^{m-1}\sum_{j=0}^{l-m} s_l\sigma^{l-m}(d_m^{-1})\Delta_{l-m,j}(d_j)t^{i+j}.$$

Note that we used that $\Delta_{l-m,l-m}(d_m) = \sigma^{l-m}(d_m)$ in the last equation. Therefore the polynomial $g(t) - s_l\sigma^{l-m}(d_m)t^{l-m}f(t)$ has degree $< l$. By iterating this argument, we find $r, q \in R$ with $\deg(r) < \deg(f)$, such that

$$g(t) = q(t)f(t) + r(t).$$

To prove uniqueness of $q(t)$ and the remainder $r(t)$, suppose we have

$$g(t) = q_1(t)f(t) + r_1(t) = q_2(t)f(t) + r_2(t).$$

Then $(q_1(t) - q_2(t))f(t) = r_2(t) - r_1(t)$. If $q_1(t) - q_2(t) \neq 0$ and observing that f has invertible leading coefficient such that $\sigma(d_m)^j$ cannot be a zero divisor for any positive j, we conclude that the degree of the left-hand side of the equation is greater than $\deg(f)$ and the degree of $r_2(t) - r_1(t)$ is less than $\deg(f)$, thus $q_1(t) = q_2(t)$ and $r_1(t) = r_2(t)$.
(ii) The proof is along similar lines as the one of (i), using that the polynomial $g(t) - f(t)\sigma^{-m}(s_l)\sigma^{-m}(d_m^{-1})t^{l-m}$ has degree $< l$ and iterating this argument. The uniqueness of $q(t)$ and the remainder is proved analogously as in (i). □

In the following, we always assume that

$$f(t) \in S[t;\sigma,\delta] \text{ has degree } m > 1 \text{ and an invertible leading coefficient } LC(f).$$

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. Since the remainders are uniquely determined, the skew polynomials of degree less that m canonically represent the elements of the left $S[t;\sigma,\delta]$-module $S[t;\sigma,\delta]/S[t;\sigma,\delta]f$ and when $\sigma \in \mathrm{Aut}(S)$, for the right $S[t;\sigma,\delta]$-module $S[t;\sigma,\delta]/fS[t;\sigma,\delta]$.

Definition 1. Suppose $f(t) = \sum_{i=0}^{m} d_i t^i \in R = S[t;\sigma,\delta]$.
(i) The additive group $\{g \in R \,|\, \deg(g) < m\}$ together with the multiplication

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

defined for all $g, h \in R$ of degree less than m, is a unital nonassociative ring S_f also denoted by R/Rf.
(ii) Suppose $\sigma \in \mathrm{Aut}(S)$. Then the additive group $\{g \in R \,|\, \deg(g) < m\}$ together with the multiplication

$$g \diamond h = gh \bmod_l f$$

defined for all $g, h \in R$ of degree less than m, is a unital nonassociative ring ${}_fS$ also denoted by R/fR.

S_f and ${}_fS$ are unital algebras over $S_0 = \{a \in S \,|\, ah = ha \text{ for all } h \in S_f\}$, which is a commutative subring of S. If S is a division ring, Definition 1 is Petit's algebra construction [33] and S_0 is a subfield of S. In the following, we therefore call the algebras S_f *Petit algebras*.

Remark 2. (i) Let $g, h \in R$ have degrees less than m. If $\deg(gh) < m$ then the multiplication $g \circ h$ in S_f and $g \diamond h$ in ${}_fS$ is the usual multiplication of polynomials in R.
(ii) If Rf is a two-sided ideal in R (i.e. f is *two-sided*, also called *invariant*) then S_f is the associative quotient algebra obtained by factoring out the ideal generated by a two-sided $f \in S[t;\sigma,\delta]$.
(iii) If $f \in S[t;\sigma,\delta]$ is reducible then S_f contains zero divisors: if $f(t) = g(t)h(t)$ then $g(t)$ and $h(t)$ are zero divisors in S_f. The argument leading up to [33, Section 2., (6)] shows that if S is a division ring, then 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_h in S_f is bijective for all $0 \neq h \in S_f$).

However, for general rings S it can happen that S_f has zero divisors, even when f is irreducible.

(iv) 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.

It suffices to consider the algebras S_f, since we have the following canonical anti-automorphism (cf. [33, (1)] when S is a division ring, the proof is analogous):

Proposition 3. *Let $f \in R = S[t;\sigma,\delta]$ have an invertible leading coefficient and let $\sigma \in \mathrm{Aut}(S)$. The canonical anti-automorphism*

$$\psi : S[t;\sigma,\delta] \to S^{op}[t;\sigma^{-1},-\delta\circ\sigma^{-1}],$$

$$\psi(\sum_{k=0}^{n} a_k t^k) = \sum_{k=0}^{n}(\sum_{i=0}^{k} \Delta_{n,i}(a_k))t^k$$

between the skew polynomial rings $S[t;\sigma,\delta]$ and $S^{op}[t;\sigma^{-1},-\delta\circ\sigma^{-1}]$ induces an anti-automorphism between the rings

$$S_f = S[t;\sigma,\delta]/S[t;\sigma,\delta]f$$

and

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

Note that if $\delta = 0$ and $\sigma \in \mathrm{Aut}(S)$, we have

$$\psi(\sum_{k=0}^{n} a_k t^k) = \sum_{k=0}^{n} \sigma^{-k}(a_k)t^k.$$

3. Some structure theory

3.1. In the following, let $f \in R = S[t;\sigma,\delta]$ be monic of degree $m > 1$ and σ injective. When S is a division ring, the structure of S_f is extensively investigated in [33]. For instance, if S is a division ring and the S_0-algebra S_f is finite-dimensional, or free of finite rank as a right module over its right nucleus, then S_f is a division algebra if and only if $f(t)$ is irreducible [33, (9)].

Some of the results in [33] carry over to our more general setting:

Theorem 4. *(i) S_f is a free left S-module of rank m with basis $t^0 = 1, t, \ldots, t^{m-1}$.*
(ii) S_f is associative if and only if f is two-sided.
(iii) If S_f is not associative then

$$S \subset \mathrm{Nuc}_l(S_f),\ S \subset \mathrm{Nuc}_m(S_f)$$

and

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

When S is a division ring, the inclusions become equalities.
(iv) We have $t \in \mathrm{Nuc}_r(S_f)$, if and only if the powers of t are associative, if and only if $t^m t = t t^m$ in S_f.
(v) If S is a division ring and S_f is not associative then

$$C(S_f) = S_0.$$

(vi) Let $f(t) = \sum_{i=0}^{m} d_i t^i \in S[t;\sigma]$ with d_0 invertible. If the endomorphism L_t which is the left multiplication by t as defined in Section 1.1 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.

Proof. (i) is clear.

(ii) If f is two-sided, S_f is clearly associative. Conversely, if S_f is associative then $S_f = \mathrm{Nuc}_r(S_f) = \{g \in R \,|\, \deg(g) < m \text{ and } fg \in Rf\}$. Thus $t \in \mathrm{Nuc}_r(S_f)$ and also $S \subset \mathrm{Nuc}_r(S_f)$. This means $f(t)t \in Rf(t)$ and for all $a \in S$, also $f(t)a = g(t)f(t)$ for a suitable $g(t) \in R$. Comparing degrees (recall we assume f to have an invertible leading coefficient) we see that $g(t) = b \in S$, so we get $f(t)t \in Rf(t)$ and for all $a \in S$, also $f(t)a = bf(t)$ for a suitable $b \in R$. Thus f is invariant, i.e. two-sided.

(iii) The proof of the first two inclusions and that $\{g \in R \,|\, \deg(g) < m \text{ and } fg \in Rf\} \subset \mathrm{Nuc}_r(S_f)$ is similar to [33, (2)] (which proves the result for S being a division ring), as this inclusion does not need S to be a division ring. For instance, for $a \in \mathrm{Nuc}_l(S_f) = \{a \in S_f \,|\, [a,b,c] = 0 \text{ for all } b,c \in S_f\}$ we have $[a,b,c] = 0$ if and only if $pfc = 0$ for some $p \in R$. If a has degree 0 then $p = 0$ as observed in [33, (2)] so $S \subset \mathrm{Nuc}_l(S_f)$. It remains to show that $\mathrm{Nuc}_r(S_f) \subset \{g \in R \,|\, \deg(g) < m \text{ and } fg \in Rf\}$ [10]: Let $b,c,d \in R$ have degree less than m. Write $bc = q_1 f + r_1$, $cd = q_2 f + r_2$ with $q_i, r_i \in R$ uniquely determined of degree smaller than m. A straightforward calculation as in [33, (2)] shows that in S_f we thus have $(bc)d = b(cd)$ if and only if $q_1 fd \bmod_r f = 0$ if and only if $q_1 fd \in Rf$.

Let now $d \in \mathrm{Nuc}_r(S_f)$ and choose $b,c \in R$ with invertible leading coefficient such that $\deg(b)+\deg(c) = m$, so that $\deg(bc) = m$. Write $bc = q_1 f + r_1$. Then $\deg(q_1 f) = \deg(q_1)+m$. But here $bc = q_1 f + r_1$ also means $\deg(q_1) = 0$, so $q_1 \in S$ is non-zero. The leading coefficient of bc is $LC(b)LC(c)$ and the leading coefficient of $q_1 f$ is q_1. Therefore $q_1 = LC(b)\sigma^l(LC(c))$ is invertible in S. Since $d \in \mathrm{Nuc}_r(S_f)$ implies $q_1 fd \in Rf$, this yields $fd \in Rf$.

(iv) If $ft \in Rf$ then $t \in \mathrm{Nuc}_r(S_f)$ by (iii), hence $t, \ldots, t^{m-1} \in \mathrm{Nuc}_r(S_f)$, and so $[t^i, t^j, t^k] = 0$ for all $i,j,k < m$, meaning the powers of t are associative. In particular, this implies $[t, t^{m-1}, t] = 0$, that is $t^m t = t t^m$. A careful analysis of the proof of [33, (5)] shows that the other implications can be proved analogously as in [33, (5)], also when also holds when S is not a division algebra, since we still have that we have $[t^i, t^j, t^k] = 0$ for all $i,j,k < m$ with $i + j < m$ analogously as in [33, 6].

(v) We have $C(S_f) = \mathrm{Comm}(S_f) \cap \mathrm{Nuc}(S_f) = \mathrm{Comm}(S_f) \cap S = S_0$.

(vi) If d_0 is invertible and $\delta = 0$ then L_t surjective implies σ surjective: For $u = \sum_{i=0}^{m-1} u_i t^i \in S_f$, we have (using the multiplication in S_f)

$$L_t(u) = \sum_{i=0}^{m-2} \sigma(u_i) t^{i+1} + \sigma(u_{m-1}) t^m = \sum_{i=0}^{m-2} \sigma(u_i) t^{i+1} + \sigma(u_{m-1}) \sum_{i=0}^{m-1} d_i t^i.$$

Suppose L_t is surjective, then given any $b \in S$, there is $u \in S_f$ such that $L_t(u) = b$. Comparing the constants in this equation, we obtain that for all $b \in S$ there is $u_{m-1} \in S$ such that $\sigma(u_{m-1}) = bd_0$, i.e. for all $c \in S$ there is $u_{m-1} \in S$ such that $\sigma(u_{m-1}) = c$ [10].

The statement that if S is a division ring and f irreducible then L_t is surjective implies σ surjective is [33, Section 2., (6)] and follows as a special case now.

If σ is bijective then L_t is surjective: Let $g = \sum_{i=0}^{m-1} g_i t^i$. Define $u_{m-1} = \sigma^{-1}(g_0 d_0^{-1})$ and $u_{i-1} = \sigma^{-1}(g_i) - u_{m-1}\sigma^{-1}(d_i)$. Then $L_t(u) = g$ [10]. □

Recall that the largest subalgebra of $R = S[t;\sigma,\delta]$ in which Rf is a two-sided ideal is the *idealizer* $I(f) = \{g \in R \,|\, fg \in Rf\}$ of Rf. The *eigenring* of f is then defined as the quotient $E(f) = I(f)/Rf$. The eigenring $E(f) = \{g \in R \,|\, \deg g < m \text{ and } fg \in Rf\}$ equals the right nucleus $\mathrm{Nuc}_r(S_f)$ by Theorem 4 (iii) (or see [33, (2)] if S is a division algebra) which, as the right nucleus, is an associative subalgebra of S_f, cf. Section 1.1. More precisely, the multiplication $\circ$ in S_f makes $\mathrm{Nuc}_r(S_f)$ into an associative algebra which equals the associative quotient ring $E(f)$ equipped with the canonical multiplication induced on it by the multiplication on the ring $I(f) \subset R$. When S is a division ring, non-trivial zero divisors in $E(f) = \mathrm{Nuc}_r(S_f)$ correspond to factors of f:

Proposition 5. *(*[24, Proposition 4]*) Let S be a division ring and $f \in R = S[t;\sigma,\delta]$.*
(i) Let $uv = 0$ for some non-zero $u, v \in E(f)$, then the greatest common right divisor $gcrd(f,u)$ is a non-trivial right factor of f. ($v \in R$ is the greatest common right divisor of f and u, *written $gcrd(f,u) = v$, if there are $s, d \in R$ such that $sf + du = v$.)*
(ii) Let $f \in R$ be bounded *(i.e., there exists $0 \neq f^* \in R$ such that $Rf^* = f^*R$ is the largest two-sided ideal of R contained in Rf) and σ be an automorphism. Then f is irreducible if and only if $E(f) = \mathrm{Nuc}_r(S_f)$ has no non-trivial zero divisors.*

Remark 6. Let S be a division ring.
(i) If f is irreducible then $\mathrm{Nuc}_r(S_f)$ is an associative division algebra [24, p. 17-19].
(ii) Effective algorithms to compute $\mathrm{Nuc}_r(S_f)$ for $f \in \mathbb{F}_q(x)[t;\sigma]$ and $f \in \mathbb{F}_q(x)[t;\delta]$ can be found in [22], for $R = \mathbb{F}_q[t;\sigma]$ in [21], [40]. Proposition 5 is also employed for linear differential operators in [43], to factorize skew polynomials for $S = \mathbb{F}_q$ in [21] and for $S = \mathbb{F}_q(x)$ in [22], [23], [24], without relating it to the algebras S_f however.

Proposition 7. *Let $f \in R = S[t;\sigma,\delta]$.*
(i) Every right divisor g of f of degree $< m$ generates a principal left ideal in S_f.

All non-zero left ideals in S_f which contain a polynomial g of minimal degree with invertible leading coefficient are principal ideal generated by g, and g is a right divisor of f in R.
(ii) Each principal left ideal generated by a right divisor of f is an S-module which is isomorphic to a submodule of S^m.
(iii) If f is irreducible, then S_f has no non-trivial principal left ideals which contain a polynomial of minimal degree with invertible leading coefficient.

The proof is straightforward. If there is no polynomial g of minimal degree with invertible leading coefficient in a non-zero left ideal, then the ideal need not be principal, see [26, Theorem 4.1] for examples.

Theorem 8. *Let $f \in R = S[t;\sigma]$.*
(i) The commuter $\mathrm{Comm}(S_f) = \{g \in S_f \,|\, gh = hg \text{ for all } h \in S_f\}$ *contains the set*

$$\{\sum_{i=0}^{m-1} a_i t^i \,|\, a_i \in \mathrm{Fix}(\sigma) \text{ and } ca_i = a_i\sigma^i(c) \text{ for all } c \in S\}.$$

If t is left-invertible in S_f and S a division ring, the two sets are equal.
(ii) $\mathrm{Fix}(\sigma) \cap C(S) \subset S_0 = \mathrm{Comm}(S_f) \cap S$. *If t is left-invertible and S a division ring, the two sets are equal.*

Proof. (i) and (iii) are straightforward calculations; both generalize [33, (14), (15)].
(ii) follows from (i): $S_0 = \{a \in S \mid ah = ha \text{ for all } h \in S_f\} = \mathrm{Comm}(S_f) \cap S$ and $\mathrm{Fix}(\sigma) \cap C(S) \subset \mathrm{Comm}(S_f) \cap S = S_0$. If t is left-invertible, the two sets are equal. □

Remark 9. For $f(t) = \sum_{i=0}^{m} d_i t^i \in S[t;\sigma]$ monic, t is left-invertible if and only if d_0 is left-invertible. One direction is a simple degree argument (suppose there are $g, h \in S_f$ with $gt = hf+1$, then compare the constant terms of both sides). Conversely, if d_0 is left-invertible then t is left-invertible (say, $h_0 d_0 = 1$, choose $h = -h_0$ and define $g(t) = \sum_{i=0}^{m-1} h d_{i+1} t^i$ to get $gt = hf + 1$). Thus if f is irreducible (hence $d_0 \neq 0$) and S a division ring then t is always left-invertible and $S_0 = \mathrm{Fix}(\sigma) \cap \mathrm{Comm}(S)$.

3.2. When S is an integral domain. In this section, let S be a commutative integral domain with quotient field K, f be monic and σ injective as before. Then σ and δ canonical extend to σ and δ to K via

$$\sigma(\frac{a}{b}) = \frac{\sigma(a)}{\sigma(b)},$$

$$\delta(\frac{a}{b}) = \frac{\delta(a)}{b} - \frac{\sigma(\frac{a}{b})\delta(b)}{b}$$

for all $a, b \in S$, $b \neq 0$.

Proposition 10. *Let S be an integral domain with quotient field K, $f \in S[t;\sigma,\delta]$ and let $S_f = S[t;\sigma,\delta]/S[t;\sigma,\delta]f$.*
(i) $S_f \otimes K \cong K[t;\sigma,\delta]/K[t;\sigma,\delta]f$ again is a Petit algebra.
(ii) If f is irreducible in $K[t;\sigma,\delta]$, then S_f has no zero divisors.

Proof. (i): The isomorphism is clear by [33, 3].
(ii): By (i), we have $S_f \otimes K \cong K[t;\sigma,\delta]/K[t;\sigma,\delta]f$. Since $f(t)$ is irreducible in $K[t;\sigma,\delta]$ and K is field, $K[t;\sigma,\delta]/K[t;\sigma,\delta]f$ is a Petit algebra such that R_h is bijective and L_h is injective, for all $0 \neq h \in S_f$ [33, Section 2., (6)]. This implies that it does not have any zero divisors, and so neither does $S_f = S[t;\sigma,\delta]/S[t;\sigma,\delta]f$. □

Example 11. Nonassociative cyclic division algebras were introduced by Sandler [41] and studied in [44] (to be precise, [44] looks at their opposite algebras). We generalize their definition (see [32] for the associative set-up):

Let S/S_0 be an extension of commutative rings, $\sigma \in \mathrm{Aut}(S)$ and $G = \langle\sigma\rangle$ a finite cyclic group of order m acting on S such that the action is trivial on S_0. For any $c \in S$, the *generalized (associative or nonassociative) cyclic algebra* $A = (S/S_0, \sigma, c)$ is the m-dimensional S-module $A = S \oplus St \oplus St^2 \oplus \cdots \oplus St^{m-1}$ where multiplication is given by the following relations for all $a, b \in S, 0 \leq i, j, < m$, which then are extended linearly to all elements of A:

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

If $\sigma \in \mathrm{Aut}(S)$, then $(S/S_0, \sigma, c) = S_f$ for $f(t) = t^m - c \in S[t;\sigma]$ and $S_0 = \mathrm{Fix}(\sigma)$. If $c \in S \setminus S_0$, the algebra $(S/S_0, \sigma, c)$ has nucleus S and center S_0.

Suppose S_0 and S are integral domains with quotient fields F and K. Canonically extend σ to an automorphism $\sigma : K \to K$, then if m is prime, $(S/S_0, \sigma, c) = S_f$ has no zero divisors for any choice of $c \in S \setminus S_0$ (since then $(K/F, \sigma, c)$ always is a nonassociative cyclic division algebra and contains S_f).

Generalized associative cyclic algebras are used in [13], generalized nonassociative cyclic algebras in [35].

4. Pseudolinear maps

Let σ be injective and $f = \sum_{i=0}^{m} d_i t^i \in S[t;\sigma,\delta]$ be a monic skew polynomial of degree $m > 1$. By Theorem 4, S_f is a free left S-module with S-basis $1, t, \ldots, t^{m-1}$. We identify an element $h \in S_f$, $h(t) = \sum_{i=0}^{m-1} a_i t^i$ with the vector $(a_0, \ldots, a_{m-1}) \in S^m$.

Right multiplication with $0 \neq h \in S_f$ in S_f, $R_h : S_f \longrightarrow S_f, p \mapsto ph$, is an S-module endomorphism [33]. After expressing R_h in matrix form with respect to the S-basis $1, t, \ldots, t^{m-1}$ of S_f, the map

$$\gamma : S_f \to \mathrm{End}_K(S_f), h \mapsto R_h$$

induces an injective S-linear map

$$\gamma : S_f \to \mathrm{Mat}_m(S), h \mapsto R_h \mapsto Y.$$

Left multiplication $L_h : S_f \longrightarrow S_f$, $p \mapsto hp$ is an S_0-module endomorphism. If we consider S_f as a right $\mathrm{Nuc}_r(S_f)$-module then L_h is a $\mathrm{Nuc}_r(S_f)$-module endomorphism.

For a two-sided f, γ is the right regular representation and λ is the left regular representation of the associative algebra S_f.

If S is a commutative ring and $\det(\gamma(h)) = \det Y = 0$, then h is a right zero divisor in S_f. Moreover, S_f is a division algebra if and only if $\gamma(h)$ is an invertible matrix for every nonzero $h \in S_f$.

Remark 12. (i) In [16], where S is a finite field and $f(t) = t^n - a$, $\delta = 0$, $\gamma(h) = Y$ is the *circulant matrix* M_a^θ.
(ii) If S is not commutative, but contains a suitable commutative subring, it is still possible to define a matrix representing left or right multiplication in the S_0-algebra S_f where the entries of the matrix lie in a commutative subring of S which strictly contains S_0 and which displays the same behaviour as above. This is a particularity of Petit's algebras, and not always possible for nonassociative algebras in general. It reflects the fact that the left nucleus of S_f always contains S (and thus is rather 'large') and that also the right nucleus may contain S or subalgebras of S, depending on the f used in the construction.

For instance, this is the case (and was used when designing fast-decodable space-time block codes, e.g. in [38], [39], [37]) when S is a cyclic division algebra $S = (K/F, \rho, c)$ of degree n and $f(t) = t^m - d \in S[t;\sigma]$, with σ suitably chosen. The $m \times m$ matrix $\gamma(h) = Y$ consequently has its entries in $(K/F, \rho, c)$. We can then substitute each entry in the matrix, which has the form $\sigma^i(x)$ for some $x \in (K/F, \rho, c)$, perhaps timed with the scalar d, with an $n \times n$ matrix: take the matrix of the right regular representation of x over K in

$(K/F,\rho,c)$, apply σ^i to each of its entries and using scalar multiplication by d if applicable. We obtain an $mn \times mn$ matrix X with entries in the field K, which still represents right multiplication with an element in S_f, but now written with respect to the canonical K-basis $1,\dots,e,t,\dots,et,\dots,e^{n-1}t^{m-1}$ of S_f, $1,e,\dots,e^{n-1}$ being the canonical basis of $(K/F,\rho,c)$. Again $\det X = 0$ implies that h is a zero divisor in S_f, and were S_f is a division algebra if and only if X is invertible for every non-zero $h \in S_f$. The interested reader is referred to [47], [38], [39], [37] for the details which would be beyond the scope of this paper.

Let

$$C_f = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 1 \\ -d_0 & -d_1 & & \cdots & -d_{m-1} \end{bmatrix}$$

be the *companion matrix* of f. Then

$$T_f : S^m \longrightarrow S^m, \quad T_f(a_1,\dots,a_m) = (\sigma(a_1),\dots,\sigma(a_m))C_f + (\delta(a_1),\dots,\delta(a_m))$$

is a (σ,δ)-pseudolinear transformation on the left S-module S^m, i.e. an additive map such that

$$T_f(ah) = \sigma(a)T_f(h) + \delta(a)$$

for all $a \in S$, $h \in S^m$. T_f is called the *pseudolinear transformation associated to* f [8] and we can translate some results on T_f (e.g., see [28]) to our nonassociative context. For $h = \sum_{i=0}^{n} a_i t^i \in S[t;\sigma,\delta]$ we define

$$h(T_f) = \sum_{i=0}^{n} a_i T_f^i.$$

Theorem 13. *(i) The pseudolinear transformation T_f is the left multiplication $L_t : S_f \longrightarrow S_f, h \mapsto th$ with t in S_f, calculated with respect to the basis $1,t,\dots,t^{m-1}$, identifying an element $h = \sum_{i=0}^{m-1} a_i t^i$ with the vector $(a_0,\dots,a_{m-1})$:*

$$L_t(h) = T_f(h)$$

for all $h \in S_f$.
(ii) We have $L_t^i(h) = L_{t^i}(h)$ for all $h \in S_f$.
(iii) Left multiplication L_h with $h \in S_f$ is given by

$$L_h = h(T_f) = \sum_{i=0}^{n} a_i T_f^i,$$

or equivalently by

$$L_h = h(L_t) = \sum_{i=0}^{n} a_i L_{t^i},$$

when calculated with respect to the basis $1,t,\dots,t^{m-1}$, identifying an element $h = \sum_{i=0}^{n} a_i t^i$ with the vector $(a_1,\dots,a_n)$.
(iv) If S_f has no zero divisors then T_f is irreducible, i.e. $\{0\}$ and S^m are the only T_f-invariant left S-submodules of S^m.

Proof. This is proved for instance in [29, Theorem 13 (2), (3), (4)] for $\delta = 0$, f irreducible and S a finite field. The proofs generalize easily and mostly verbatim to our more general setting. □

From Theorem 4 (vi) together with Theorem 13 (i) we obtain:

Corollary 14. *Let $f(t) = \sum_{i=0}^{m} d_i t^i \in S[t;\sigma]$ with d_0 invertible. If σ is not surjective then the pseudolinear transformation T_f is not surjective. In particular, if S is a division ring, f irreducible and σ is not surjective then T_f is not surjective.*

Moreover, if σ is bijective then T_f is surjective.

Remark 15. (i) From Theorem 13 we obtain [8, Lemma 2], since $pq = 0$ in S_f is equivalent to $L_p(q) = p(T_f) = 0$. Note that

$$T_f^n(ah) = \sum_{i=0}^{n} \Delta_{i,n}(a) T_f^i(h)$$

for all $a \in S$, $h \in S^m$ [8], so L_{t^n} is usually not (σ,δ)-pseudolinear anymore.
(ii) Right multiplication with h in S_f induces the injective S-linear map

$$\gamma : S_f \to \mathrm{Mat}_m(S), \quad h \mapsto R_h \mapsto Y.$$

f is two-sided is equivalent to γ being the right regular representation of S_f. In that case, γ is an injective ring homomorphism. In particular, (1) and (3) in [16, Theorem 6.6] hold in our general setting (i.e., for any choice of f) if and only if S_f is associative: both reflect the fact that then $\gamma : S_f \longrightarrow \mathrm{Mat}_m(S)$ is the right regular representation of S_f.
(iii) Suppose $f = h'g = gh$. Right multiplication in S_f induces the left S-module endomorphisms R_h and R_g. We have $g \in \ker(R_h) = \{u \in R \,|\, \deg(u) < m \text{ and } uh \in Rf\}$ and $h \in \ker(R_g) = \{u \in R \,|\, \deg(u) < m \text{ and } ug \in Rf\}$, cf. [28, Lemma 3] or [16, Theorem 6.6]. If f is two-sided, $\ker(R_g) = S_f h$ and $\ker(R_h) = S_f g$.
(iv) Suppose $f = h'g = gh$. Left multiplication in S_f induces the right S_0-module endomorphisms $L_{h'}$ and L_g. We have $g \in \ker(L_{h'}) = \{u \in R \,|\, \deg(u) < m \text{ and } hu \in Rf\}$ and $h \in \ker(L_g) = \{u \in R \,|\, \deg(u) < m \text{ and } gu \in Rf\}$. If f is two-sided, $\ker(L_{h'}) = gS_f$ and $\ker(L_g) = h'S_f$.

Furthermore, (iii) and (iv) tie in with or generalize (4), (5) in [16, Theorem 6.6].

5. Finite nonassociative rings obtained from skew polynomials over finite chain-rings

5.1. Finite Chain Rings (cf. for instance [31]). When S is a finite ring, S_f is a finite unital nonassociative ring with $|S|^m$ elements and a finite unital nonassociative algebra over the finite subring S_0 of S. E.g., if S is a finite field and f irreducible, then S_f is a finite unital nonassociative division ring, also called a *semifield* [29]. We will look at the special case where S is a finite chain ring. Lately, these rings gained substantial momentum in coding theory, see for instance [3], [4], [7], [11], [14], [15], [27], [30].

A finite unital commutative ring $R \neq \{0\}$ is called a *finite chain ring*, if its ideals are linearly ordered by inclusion.

Every ideal of a finite chain ring is principal and its maximal ideal is unique. In particular, R is a local ring and the residue field $K = R/(\gamma)$, where γ is a generator of its maximal ideal m, is a finite field. The ideals $(\gamma^i) = \gamma^i R$ of R form the proper chain

$$R = (1) \supseteq (\gamma) \supseteq (\gamma^2) \supseteq \cdots \supseteq (\gamma^e) = (0).$$

The integer e is called the *nilpotency index* of R. If K has q elements, then $|R| = q^e$. If $\pi : S \longrightarrow K = R/(\gamma)$, $x \mapsto \overline{x} = x \bmod \gamma$ is the canonical projection, a monic polynomial $f \in R[t]$ is called *base irreducible* if f is irreducible in K.

Let R and S be two finite chain rings such that $R \subset S$ and $1_R = 1_S$ Then S is an extension of R denoted S/R. If m is the maximal ideal of R and M the one of S, then S/R is called *separable* if $mS = M$. The *Galois group of* S/R is the group G of all automorphisms of S which are the identity when restricted to R. A separable extension S/R is called *Galois* if $S^G = \{s \in S \,|\, \tau(s) = s \text{ for all } \tau \in G\} = R$. This is equivalent to $S = R[x]/(f(x))$, where $(f(x))$ is the ideal generated by a monic basic irreducible polynomial $f(x) \in R[x]$ [31, Theorem XIV.8], [48, Section 4]. From now on, a separable extension S/R of finite chain rings is understood to be a separable Galois extension.

The Galois group G of a separable extension S/R is isomorphic to the Galois group of the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, where $\mathbb{F}_{q^n} = S/M$, $\mathbb{F}_q = R/m$. G is cyclic with generator $\sigma(a) = a^q$ for a suitable primitive element $a \in S$, and $\{a, \sigma(a), \ldots, \sigma^{n-1}(a)\}$ is a free R-basis of S. Since S is also an unramified extension of R, $M = Sm = Sp$, and

$$S = (1) \supseteq Sp \supseteq \cdots \supseteq Sp^t = (0).$$

The automorphism groups of S are known [1, 2].

Example 16. (i) The integer residue ring $\mathbb{Z}_{p^e}$ and the ring $\mathbb{F}_{p^n}[u]/(u^e)$ are finite chain rings of characteristic p, the later has nilpotency index e and residue field $\mathbb{F}_{p^n}$.
(ii) A finite unital ring R is called a *Galois ring* if it is commutative, and its zero-divisors $\Delta(R)$ have the form pR for some prime p. $(p) = Rp$ is the unique maximal ideal of R. Given a prime p and positive integers e, n, denote by $G(p^e, n)$ the Galois ring of characteristic p^s and cardinality p^{en} which is unique up to isomorphism. Its residue field (also called *top-factor*) $\overline{G(p^e, n)} = G(p^e, n)/pG(p^e, n)$ is the finite field $\mathbb{F}_{p^n}$.

5.2. Skew-polynomials and Petit's algebras over finite chain rings. Let S be a finite chain ring with residue class field $K = S/(\gamma)$ and $\sigma \in \mathrm{Aut}(S)$, δ a left σ-derivation. Consider the skew polynomial ring $R = S[t; \sigma, \delta]$. Whenever S is a finite chain ring, we suppose $\sigma((\gamma)) = (\gamma)$ and $\delta((\gamma)) \subset (\gamma)$. Then the automorphism σ induces an automorphism

$$\overline{\sigma} : K \to K,\ \overline{\sigma}(\overline{x}) = \overline{\sigma(x)}$$

with $\sigma = \overline{\sigma} \circ \pi$, and analogously δ a left $\overline{\sigma}$-derivation $\overline{\delta} : K \to K$. There is the canonical surjective ring homomorphism

$$^- : S[t; \sigma, \delta] \to K[t; \overline{\sigma}, \overline{\delta}],\ g(t) = \sum_{i=0}^{n} a_i t^i \mapsto \overline{g}(t) = \sum_{i=0}^{n} \overline{a_i} t^i.$$

We call f *base irreducible* if $\overline{f}$ is irreducible in $K[t; \overline{\sigma}, \overline{\delta}]$ and *regular* if $\overline{f} \neq 0$. Obviously, if $\overline{f}$ is irreducible in $K[t; \overline{\sigma}, \overline{\delta}]$ then f is irreducible in $S[t; \sigma, \delta]$. Since $S_f \cong S_{af}$ for all invertible

$a \in S$, without loss of generality we consider only monic f in this section. From now on let $f \in R = S[t;\sigma,\delta]$ be monic of degree $m > 1$.

Lemma 17. *Suppose S is a finite chain ring with cardinality q^e. Then*

$$S_f = S[t;\sigma,\delta]/S[t;\sigma,\delta]f$$

is a nonassociative finite ring with q^{em} elements and $S_{\overline{f}} = K[t;\overline{\sigma},\overline{\delta}]/K[t;\overline{\sigma},\overline{\delta}]\overline{f}$ has q^m elements.

In particular, if $S = G(p^s,n)$ then S_f has p^{snm} elements and $S_{\overline{f}}$ has p^{nm} elements.

Proof. The residue class field K has q elements if $|S| = q^e$. Since S_f is a left S-module with basis t^i, $0 \leq i \leq m-1$, it has q^{em} elements, analogously, $S_{\overline{f}}$ has q^m elements. □

From Remark 6, Proposition 5, [33, (9)] and [33, (7)] we get (as all polynomials in $K = K[t;\overline{\sigma}]$ are bounded for a finite field K, and $K[t;\overline{\sigma},\overline{\delta}] \cong K[t;\sigma']$ for a suitable σ'):

Corollary 18. *Suppose S is a finite chain ring.*
(i) S_f is a unital nonassociative algebra with finitely many elements over the subring $S_0 = \{a \in S \mid ah = ha \text{ for all } h \in S_f\}$ of S.
(ii) $S_{\overline{f}} = K[t;\overline{\sigma},\overline{\delta}]/\overline{f}K[t;\overline{\sigma},\overline{\delta}]$ is a semifield if and only if f is base irreducible, if and only if $\mathrm{Nuc}_r(S_{\overline{f}})$ has no zero divisors.
(iii) If $\delta = 0$ then $\mathrm{Fix}(\sigma) \subset S_0$.

From now on we assume that $\gamma \in \mathrm{Fix}(\sigma) \cap \mathrm{Const}(\delta)$. Then γS_f is a two-sided ideal in S_f.

The canonical surjective ring homomorphism $^- : S[t;\sigma,\delta] \to K[t;\overline{\sigma},\overline{\delta}]$ induces the surjective homomorphism of nonassociative rings

$$\Psi : S_f = S[t;\sigma,\delta]/S[t;\sigma,\delta]f \to K[t;\overline{\sigma},\overline{\delta}]/K[t;\overline{\sigma},\overline{\delta}]\overline{f},$$

$$g(t) \mapsto \overline{g}(t)$$

which has as kernel the two-sided ideal γS_f.

This induces an isomorphism of nonassociative rings:

$$S_f/\gamma S_f \cong K[t;\overline{\sigma},\overline{\delta}]/K[t;\overline{\sigma},\overline{\delta}]\overline{f} = S_{\overline{f}}, \tag{1}$$

$$g(t) + \gamma S_f \mapsto \overline{g}(t).$$

5.3. Generalized Galois rings. A *generalized Galois ring* (GGR) is a finite nonassociative unital ring A such that the set of its (left or right) zero divisors $\Delta(A)$ has the form pA for some prime p. $\Delta(A)$ is a two-sided ideal and the quotient $\overline{A} = A/pA$ is a semifield of characteristic p, called the *top-factor* of A. The characteristic of A is p^s. There is a canonical epimorphism

$$A \longrightarrow \overline{A} = A/pA, \quad a \mapsto \bar{a} = a + pA.$$

A generalized Galois ring A of characteristic p^s is a *lifting* of the semifield $\overline{A}$ *of characteristic* p^s if $\overline{C(A)} = C(A)/pC(A) \cong C(\overline{A})$ (cf. [17]).

A finite unital ring A is a GGR if and only if there is a prime p and a positive integer s such that $\mathrm{char}(A) = p^s$ and $\overline{A} = A/pA$ is a semifield [17, Theorem 1].

Let $S = G(p^e, n)$ be a Galois ring and let $f \in R = S[t; \sigma, \delta]$ be monic of degree $m > 1$ as before.

Let $A = S_f = S[t; \sigma, \delta]/S[t; \sigma, \delta]f$, then by (1) there is the canonical isomorphism

$$A/pA \cong K[t; \overline{\sigma}, \overline{\delta}]/K[t; \overline{\sigma}, \overline{\delta}]\overline{f} = S_{\overline{f}}.$$

Thus all base irreducible such $f \in S[t; \sigma, \delta]$ yield generalized Galois rings S_f:

Theorem 19. *Let S be a Galois ring and let $f(t) \in S[t; \sigma, \delta]$ be base irreducible. Then the finite nonassociative ring*

$$S_f = S[t; \sigma, \delta]/S[t; \sigma, \delta]f$$

is a GGR with p^{enm} elements. If S_f is not associative it is a lifting of its top-factor since $S_0/pS_0 \cong \mathrm{Fix}(\overline{\sigma})$.

Proof. If $\overline{f}$ is irreducible, then $S_{\overline{f}} = K[t; \overline{\sigma}, \overline{\delta}]/K[t; \overline{\sigma}, \overline{\delta}]\overline{f}$ is a semifield. By (1), we have $S_{\overline{f}} \cong A/pA = \overline{A}$, so that $\overline{A}$ is a semifield. Thus S_f is a GGR with p^{enm} elements by Lemma 17 and [17, Theorem 1].

Every left σ-derivation of a finite field is inner, so that there are a suitable y and $\widetilde{f} \in K[y; \overline{\sigma}]$ such that $S_{\overline{f}} \cong K[y; \overline{\sigma}]/K[y; \overline{\sigma}]\widetilde{f}$. The second assertion is now proved using the fact that $S_{\widetilde{f}}$ is a semifield over $\mathrm{Fix}(\overline{\sigma})$ by Theorem 8 (ii) and that $\overline{C(A)} = C(A)/pC(A) \cong C(\overline{A})$. □

Corollary 20. *Let S/S_0 be a Galois extension of Galois rings with Galois group $\mathrm{Gal}(S/S_0) = \langle\sigma\rangle$ of order m and let F denote the residue field of S_0, $char(F) = p$. Choose $f(t) = t^m + ph(t) - d \in R = S[t; \sigma]$ with $d \in S \setminus S_0$ invertible and $h(t) \in S[t; \sigma]$ of degree $< m$.*
(i) If the elements $1, \overline{d}, \ldots, \overline{d}^m$ are linearly independent over F, then S_f is a GGR which is a lifting of its top-factor.
(ii) For every prime m, S_f is a GGR which is a lifting of its top-factor.

Proof. K/F is a Galois extension with Galois group $\mathrm{Gal}(K/F) = \langle\overline{\sigma}\rangle$ of order m. We have $\overline{f}(t) = t^m - \overline{d}$. With the assumptions in (i) resp. (ii), $S_{\overline{f}}$ is a nonassociative cyclic division algebra over F [44] and thus the finite nonassociative ring S_f is a GGR by [17, Theorem 1]. It is straightforward to see that $\mathrm{Fix}(\sigma) = \mathrm{Fix}(\overline{\sigma})$ using isomorphism (1) and that S_f is a lifting of its top-factor by Theorem 4. □

Note that although the top-factor in Corollary 20 is a nonassociative cyclic algebra, it is unlikely that the algebra S_f is isomorphic to a generalized nonassociative cyclic algebra as defined in Example 11 unless $h = 0$.

6. Linear codes

6.1. Cyclic (f, σ, δ)-codes. A *linear code of length m over S* is a submodule of the S-module S^m. From now on, let $f \in S[t; \sigma, \delta]$ be a monic polynomial of degree $m > 1$.

A *cyclic (f, σ, δ)-code* $\mathcal{C} \subset S^m$ is a subset of S^m consisting of the vectors $(a_0, \ldots, a_{m-1})$ obtained from elements $h = \sum_{i=0}^{m-1} a_i t^i$ in a left principal ideal $gS_f = S[t; \sigma, \delta]g/S[t; \sigma, \delta]f$ of S_f, with g a monic right divisor of f.

A code $\mathcal{C}$ over S is called σ-*constacyclic* if $\delta = 0$ and there is a non-zero $d \in S$ such that

$$(a_0, \ldots, a_{m-1}) \in \mathcal{C} \Rightarrow (\sigma(a_{m-1})d, \sigma(a_0), \ldots, \sigma(a_{m-2})) \in \mathcal{C}.$$

If $d = 1$, the code is called σ-*cyclic*.

[8, Theorem 1], the first three equivalences of [8, Theorem 2] and [8, Corollary 1] translate to our set-up as follows (the first equivalences in [8, Theorem 2] are now trivial):

Theorem 21. *Let $g = \sum_{i=0}^{r} g_i t^i$ be a monic polynomial which is a right divisor of f.*
(i) The cyclic (f, σ, δ)-code $\mathcal{C} \subset S^m$ corresponding to the principal ideal gS_f is a free left S-module of dimension $m - \deg g$.
(ii) If $(a_0, \ldots, a_{m-1}) \in \mathcal{C}$ then $L_t(a_0, \ldots, a_{m-1}) \in \mathcal{C}$.
(iii) The matrix generating $\mathcal{C}$ represents the right multiplication R_g with g in S_f, calculated with respect to the basis $1, t, \ldots, t^{m-1}$, identifying elements $h = \sum_{i=0}^{m-1} a_i t^i$ with the vectors $(a_0, \ldots, a_{m-1})$.

Note that (iii) is a straightforward consequence from the fact that the k-th row of the matrix generating $\mathcal{C}$ is given by left multiplication of g with t^k in S_f, i.e. by

$$L_{t^k}(g) = L_t^k(g).$$

In particular, when $\delta = 0$ and $f(t) = t^m - d$, for any $p \in S_f$, the matrix representing right multiplication R_p with respect to the basis $1, t, \ldots, t^{m-1}$ is the circulant matrix defined in [16, Definition 3.1], see also Section 4.

Theorem 22. *Let $g = \sum_{i=0}^{r} g_i t^i$ be a monic polynomial which is a right divisor of f, such that $f = gh = h'g$ for two monic polynomials $h, h' \in S[t; \sigma, \delta]$. Let $\mathcal{C}$ be the cyclic (f, σ, δ)-code corresponding to g and $c = \sum_{i=0}^{m-1} c_i t^i \in S[t; \sigma, \delta]$. Then the following are equivalent:*
(i) $(c_0, \ldots, c_{m-1}) \in \mathcal{C}$.
(ii) $c(t)h(t) = 0$ in S_f.
(iii) $L_c(h) = ch = 0$, resp. $R_h(c) = hc = 0$.

This is already part of [8, Theorem 2] and generalizes [13, Proposition 1]: it shows that sometimes h is a parity check polynomial for $\mathcal{C}$ also when f is not two-sided. Note that when we only have $hg = f$, h monic, and $\mathcal{C}$ is the code generated by g then if $ch = 0$ in S_f, c is a codeword of $\mathcal{C}$.

Corollary 23. *Let $g = \sum_{i=0}^{r} g_i t^i$ be a monic polynomial which is a right divisor of f, such that $f = gh = h'g$ for two monic polynomials $h, h' \in S_f$. Let $\mathcal{C}$ be the cyclic (f, σ, δ)-code corresponding to g. Then the matrix representing right multiplication R_h with h in S_f with respect to the basis $1, t, \ldots, t^{m-1}$ is a control matrix of the cyclic (f, σ, δ)-code corresponding to g.*

Proof. The matrix H with ith row the vector representing

$$L_{t^{i-1}}(h) = t^{i-1}h,$$

$1 \leq i \leq m$, is the matrix representing right multiplication $R_h(p) = ph$ with h in S_f with respect to the basis $1, t, \ldots, t^{m-1}$, since $t^{i-1}h = R_h(t^{i-1})$ is the ith row. □

For a linear code $\mathcal{C}$ of length m we denote by $\mathcal{C}(t)$ the set of skew polynomials $a(t) = \sum_{i=0}^{m-1} a_i t^i \in S_f$ associated to the codewords $(a_0, \ldots, a_n) \in \mathcal{C}$.

As a consequence of Proposition 7 and Theorem 21 we obtain a description of σ-constacyclic codes in terms of left ideals of S_f, generalizing [26, Theorem 2.2]:

Corollary 24. *Let $f = t^m - d \in S[t;\sigma]$, $d \in S$ invertible, and $\mathcal{C}$ a linear code over S of length m.*
(i) Every left ideal of S_f with $f = t^m - d \in S[t;\sigma]$ generated by a monic right divisor g of f in $S[t;\sigma]$ yields a σ-constacyclic code of length m and dimension $m - \deg g$.
(ii) If $\mathcal{C}$ is a σ-constacyclic code then the skew polynomials in the set $\mathcal{C}(t)$ of elements $a(t)$ obtained from $(a_0, \ldots, a_{m-1}) \in \mathcal{C}$ form a left ideal of S_f with $f = t^m - d \in S[t;\sigma]$.

Proof. (i) follows from Theorem 21.
(ii) The argument is analogous to the proof of [6, Theorem 1]. □

For any monic $f \in S[t;\sigma,\delta]$, representing the right multiplication R_g in S_f by the matrix Y calculated with respect to the S-basis $1, t, \ldots, t^{m-1}$ gives the injective S-linear map

$$\gamma : S_f \to \mathrm{Mat}_m(S), \quad h \mapsto R_h \mapsto Y.$$

For algebras S_f which are not associative, this is not a regular representation of the algebra. However, we can prove some weaker results for special choices of f:

Lemma 25. *Suppose that $f(t) = t^m - d_0 \in S[t;\sigma,\delta]$ or $f(t) = t^2 - d_1 t - d_0 \in S[t;\sigma,\delta]$. Then the product of the $m \times m$ matrices representing R_d, $0 \neq d \in S \subset S_f$, and R_g for any $0 \neq g \in S_f$, is the matrix representing R_{dg}, i.e. the matrix representing the right multiplication with dg in S_f.*

The proofs are straightforward but tedious calculations [10]. The case where $f(t) = t^m - d_0 \in S[t;\sigma]$ and S is a cyclic Galois extension of degree m over a field F with σ generating its automorphism group is already treated in [45], its proof holds analogously when S is a commutative ring with an automorphism σ of order m.

When S is a commutative unital ring, we define a map $M : S_f \to S$ by

$$M(h) = \det(\gamma(h))$$

for all $h \in S_f$. Note that this is analogous to the definition of the reduced norm of an associative central simple algebra.

We recall the following: Let A be an algebra over a ring S_0 and D a subalgebra of A, both free of finite rank as S_0-modules. Then a map $M : A \mapsto D$ of degree n is called *left semi-multiplicative* if

$$M(ax) = M(a)M(x) \text{ for all } a \in D, x \in A.$$

Furthermore, a map $M : A \mapsto D$ has *degree* n over S_0 if $M(av) = a^n M(v)$ for all $a \in S_0$, $v \in A$ and if the map $M : A \times \cdots \times A \mapsto D$ defined by

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

$(1 \leq l \leq n)$ is an n-linear map over S_0, i.e., $M : A \times \cdots \times A \mapsto D$ (n-copies) is an S_0-multilinear map where $M(v_1, \ldots, v_n)$ is invariant under all permutations of its variables.

Corollary 26. *Suppose S is a commutative unital ring and both S and the algebra S_f are free of finite rank as S_0-module. For $f(t) = t^m - d_0 \in S[t;\sigma,\delta]$ or $f(t) = t^2 - d_1 t - d_0 \in S[t;\sigma,\delta]$, the map*

$$M : S_f \to S, \quad M(h) = \det(\gamma(h)),$$

is left semi-linear of degree m.

This is a direct consequence of Lemma 25. For properties of left semi-linear maps, especially for those of lower degree, the reader is referred to [45], [46].

Example 27. Let K/F be a cyclic Galois extension of degree m with reduced norm $N_{K/F}$ and reduced trace $T_{K/F}$, $\mathrm{Gal}(K/F) =< \sigma >$ and $f(t) = t^m - d \in K[t;\sigma]$. Then $M : S_f \to S$ is a left semi-multiplicative map of degree m. If $a \in K$ is considered as an element of S_f then $M(a) = N_{K/F}(a)$. In particular, for $m = 3$ and $h = h_0 + h_1 t + h_2 t^2$, we have

$$M(h) = N_{K/F}(h_0) + dN_{K/F}(h_1) + d^2 N_{K/F}(h_2) - dT_{K/F}(h_0 h_1 h_2)$$

[45].

Remark 28. We point out that if $S = (K/F, \varrho, c)$ is a suitable cyclic division algebra with norm $N_{S/F}$, we can describe the right multiplication with h by an $mn \times mn$ matrix $X(h)$ with entries in K as described in Remark 12 (ii), and define a map

$$M : S_f \longrightarrow S, \quad M(h) = \det(R_h) = \det(X(h))$$

which is also left-semilinear for suitable $f(t) = t^m - d$ (cf. [37, Remark 19] where we look at the matrix representing left multiplication instead, since we are dealing with the opposite algebra there). Again the map M can be seen as a generalization of the norm of an associative central simple algebra and

$$M(x) = N_{F/S_0}(N_{S/F}(x))$$

for all $x \in S$ for suitably chosen S_0-algebras S_f, for details see [37].

6.2. Codes over finite chain rings. Let S be a finite chain ring and σ an automorphism of S. The $S[t;\sigma]$-module $S[t;\sigma]/S[t;\sigma]f$ is increasingly favored for linear code constructions over S, with f a monic polynomial of degree m (usually $f(t) = t^m - d$), cf. for instance [4], [7], [26]. For code constructions, we generally look at reducible skew polynomials f.

We take the setup discussed in [4], [7], [26], where the $S[t;\sigma]$-module $S[t;\sigma]/S[t;\sigma]f$ is employed for linear code constructions, and discuss on some examples how the results mentioned previously fit into our view of equipping $S[t;\sigma]/S[t;\sigma]f$ with a nonassociative algebra structure:

- In [26, Theorem 2.2], it is shown that a code of length n is σ-constacyclic if and only if the skew polynomial representation associated to it is a left ideal in S_f, again assuming S_f to be associative, i.e. $f(t) = t^m - d \in S[t;\sigma]$ with $d \in S$ invertible, to be two-sided, and S to be a finite chain ring.

- In [7, Proposition 2.1], it is shown that any right divisor $g(t)$ of $f(t) = t^m - d \in S[t;\sigma]$ generates a principal left ideal in S_f, provided that f is a monic two-sided element and assuming S is a Galois ring. The codewords associated with the elements in the ideal Rg form a code of length m and dimension $m - \deg g$. This also holds in the nonassociative setting, so we can drop the assumption in [7, Proposition 2.1] that f needs to be a monic central element, see Corollary 24.
- In [4, Theorem 2] (or similarly in [26, 3.1]), it is shown that if a skew-linear code $\mathcal{C}$ is associated with a principal left ideal, then $\mathcal{C}$ is an S-free module if and only if g is a right divisor of $f(t) = t^m - 1$, again assuming S to be Galois, and f two-sided. This is generalized in Proposition 7, resp. Corollary 24.
- For $f(t) = t^m - d \in \mathbb{F}_q[t;\sigma]$, the (σ, d)-*circulant matrix* M_d^σ in [16] is the matrix representing R_g in the algebra S_f calculated with respect to the basis $1, t, \ldots, t^{m-1}$. Therefore [16, Theorem 3.6] states that for associative algebras S_f, right multiplication gives the right regular representation of the algebra, so that the product of the matrix representing R_h, and the one representing R_g, for any $0 \neq h \in S_f$, $0 \neq g \in S_f$, is the matrix representing R_{hg} in S_f. The fact that γ is injective and additive is observed in [16, Remark 3.2 (a)].

  Lemma 25 and the fact that γ is S-linear imply [16, Remark 3.2 (b)].

  Moreover, the matrix equation in [16, Theorem 5.6 (1)] can be read as follows: if $t^n - a = hg$ and $c = \gamma(a, g)$, then the matrix representing the right multiplication with the element $g(t) \in R_n$ in the algebra S_f where $f(t) = t^n - a \in \mathbb{F}_q[t;\sigma]$, equals the transpose of the matrix representing the right multiplication with an element $g^\sharp(t) \in S_{f_1}$ where $f_1(t) = t^n - c^{-1} \in \mathbb{F}_q[t;\sigma]$. This suggests an isomorphism between $S_{f_1} = \mathbb{F}_q[t;\sigma]/\mathbb{F}_q[t;\sigma]f_1$ and the opposite algebra of $S_f = \mathbb{F}_q[t;\sigma]/\mathbb{F}_q[t;\sigma]f$.

7. Conclusion and further work

This paper proposes a more general way of looking at cyclic (f, σ, δ)-codes using nonassociative algebras, and unifies different ways of designing cyclic linear (f, σ, δ)-codes in a general, nonassociative theory. Connections between the algebras and some fast-decodable space-time block code designs are pointed out along the way.

It is well known that for any $f \in R = S[t;\sigma,\delta]$, R/Rf is an R-module with the module structure given by the multiplication $g(h + Rf) = gh + Rf = r + Rf$ if r is the reminder of gh after right dividing by f. This is exactly the multiplication which makes the additive group $\{g \in R \,|\, \deg(g) < m\}$ into a nonassociative algebra when f has an invertible leading coefficient. Thus one might argue that the introduction of the nonassociative point of view we suggested here seems to make things only more complicated that actually needed and not necessarily better.

The full benefits of this approach for coding theory might only become visible once more work has been done in this direction. Using the nonassociative Petit algebras S_f over number fields allows us for instance to show how certain cyclic (f, σ, δ)-codes over finite rings canonically induce a $\mathbb{Z}$-lattice in $\mathbb{R}^N$. The observations in [13, Section 5.2, 5.3] hold analogously for our nonassociative algebras and explain the potential of the algebras S_f for

coset coding in space-time block coding, in particular for wiretap coding, cf. [35]. Previous results for lattices obtained from σ-constacyclic codes related to associative cyclic algebras by Ducoat and Oggier [13] are obtained as special cases.

We also canonically obtain coset codes from orders in nonassociative algebras over number fields which are used for fast-decodable space-time block codes [34]. Again, previous results for coset codes related to associative cyclic algebras S_f by Oggier and Sethuraman [32] are obtained as special cases.

References

[1] Y. Alkhamees, *The group of automorphisms of finite chain rings*, Arab Gulf Journal of Scientific Research 8 (1990). 17-28.

[2] Y. Alkhamees, *The determination of the group of automorphisms of a finite chain ring of characteristic p*. The Quarterly Journal of Math. 42 (1991), 387-391.

[3] A. Batoul, K. Guenda, T. A. Gulliver, *On self-dual cyclic codes over finite chain rings*. Des. Codes Cryptogr. 70 (3) (2014), 347-358.

[4] M. Bhaintwal, *Skew quasi-cyclic codes over Galois rings*. Des. Codes Cryptogr. 62 (1) (2012), 85101.

[5] D. Boucher, F. Ulmer, *Linear codes using skew polynomials with automorphisms and derivations*, Des. Codes Cryptogr. 70 (3) (2014), 405-431.

[6] D. Boucher, W. Geiselmann, F. Ulmer, *Skew-cyclic codes*, AAECC 18 (2007), 370-389.

[7] D. Boucher, P. Solè, F. Ulmer, *Skew-constacyclic codes over Galois rings*. Adv. Math. Comm. 2 (3) (2008), 273-292.

[8] M. Boulagouaz, A. Leroy, (σ, δ)*-codes*. Adv. Math. Commun. 7 (4) (2013), 463-474.

[9] P. M. Cohn, "Skew fields". Theory of general division rings. Encyclopedia of Mathematics and its Applications, 57. Cambridge University Press, Cambridge, 1995.

[10] C. Brown, PhD Thesis University of Nottingham, in preparation.

[11] Y. Cao, *On constacyclic codes over finite chain rings.* Finite Fields Appl. 24 (2013), 124-135.

[12] J. Ducoat, F. Oggier, *Lattice encoding of cyclic codes from skew polynomial rings*. Proc. of the 4th International Castle Meeting on Coding Theory and Applications, Palmela, 2014.

[13] J. Ducoat, F. Oggier, *On skew polynomial codes and lattices from quotients of cyclic division algebras.* Adv. Math. Comm. 10 (1) 2016, 79-94.

[14] C. Feng, R. W. Nobrega, F. R. Kschischang, D. Silva, *Communication over finite-chain-ring matrix channels*. IEEE Trans. Inform. Theory 60 (10) (2014), 58995917.

[15] J. Gao, Kong, *Qiong 1-generator quasi-cyclic codes over* $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{s-1}\mathbb{F}_{p^m}$. J. Franklin Inst. 350 (10) (2013), 3260-3276.

[16] N. Fogarty, H. Gluesing-Luerssen, *A Circulant Approach to Skew-Constacyclic Codes.* Finite Fields Appl. 35 (2015), 92114.

[17] S. González, V. T. Markov, C. Martínez, A. A. Nechaev, I. F. Rúa, *Nonassociative Galois rings*. (Russian) Diskret. Mat. 14 (4) (2002), 117-132; translation in Discrete Math. Appl. 12 (6) (2002), 519-606.

[18] S. González, V. T. Markov, C. Martínesz, A. A. Nechaev, I. F. Rúa, *Cyclic generalized Galois rings*. Comm. Algebra 33 (12) (2005), 4467-4478.

[19] S. González, V. T. Markov, C. Martínes, A. A. Nechaev, I. F. Rúa, *On cyclic top-associative generalized Galois rings.* Finite fields and applications, 25-39, Lecture Notes in Comput. Sci. 2948, Springer, Berlin, 2004.

[20] S. González, C. Martínez, I. F. Rúa, V. T. Markov, A. A. Nechaev, *Coordinate sets of generalized Galois rings*. J. Algebra Appl. 3 (1) (2004), 31-48.

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

[22] 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.

[23] 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]

[24] 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.

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

[26] S. Jitman, S. Ling, P. Udomkavanich, *Skew constacyclic codes over finite chain rings*, Adv. Math. Commun. 6 (1) (2012), 39-63.

[27] B. Kong, X. Zheng, H. Ma, *The depth spectrums of constacyclic codes over finite chain rings*. Discrete Math. 338 (2) (2015), 256-261.

[28] A. Leroy, *Noncommutative polynomial maps*. J. Algebra Appl. 11 (4) (2012), 16 pp.

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

[30] X. Liu, H. Liu, *LCD codes over finite chain rings*. Finite Fields Appl. 34 (2015), 1-19.

[31] B. McDonald, "Finite rings with identity". Pure and Applied Mathematics, vol. 28. Marcel Dekker, Inc., New York, 1974.

[32] F. Oggier, B. A. Sethuraman, *Quotients of orders in cyclic algebras and space-time codes*. Adv. Math. Commun. 7 (4) (2013), 441-461.

[33] 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.

[34] S. Pumplün, *Quotients of orders in algebras obtained from skew polynomials and possible applications*. Preprint 2016

[35] S. Pumplün, *How to obtain lattices from (f, σ, δ)-codes via a generalization of Construction A*. Online at arXiv:1607.03787 [cs.IT]

[36] S. Pumplün, *A note on linear codes and nonassociative algebras obtained from skew polynomial rings*. Online at arXiv:1504.00190[cs.IT]

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

[38] S. Pumplün, A. Steele, *The nonassociative algebras used to build fast-decodable space-time block codes*. Advances in Mathematics of Communications 9 (4) 2015, 449-469.

[39] S. Pumplün, A. Steele, *Fast-decodable MIDO codes from nonassociative algebras*. Int. J. of Information and Coding Theory (IJICOT) 3 (1) 2015, 15-38.

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

[41] R. Sandler, *Autotopism groups of some finite non-associative algebras*. American Journal of Mathematics 84 (1962), 239-264.

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

[43] M. F. Singer, *Testing reducibility of linear differential operators: a group-theoretic perspective*. Appl. Algebra Engrg. Comm. Comput. 7 (2) (1996), 77-104.

[44] A. Steele, *Nonassociative cyclic algebras*. Israel J. Math. 200 (1) (2014), 361-387.

[45] A. Steele, *Some new classes of algebras*. PhD Thesis, University of Nottingham 2013. http://eprints.nottingham.ac.uk/13934/1/PhdthesisFinal.pdf

[46] S. Pumplün, A. Steele, *Algebras carrying maps of degree n*. Online at http://homepage.uibk.ac.at/∼c70202/jordan/index.html.

[47] A. Steele, S. Pumplün, F. Oggier, *MIDO space-time codes from associative and non-associative cyclic algebras*. Information Theory Workshop (ITW) 2012 IEEE (2012), 192-196.

[48] E. A. Whelan, *A note on finite local rings*. Rocky Mountain J. Math. 22 (2) (1992), 757-759.

E-mail address: susanne.pumpluen@nottingham.ac.uk

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