THE AUTOMORPHISMS OF PETIT'S ALGEBRAS

C. BROWN AND S. PUMPLÜN

Abstract. Let σ be an automorphism of a field K with fixed field F. We study the automorphisms of nonassociative unital algebras which are canonical generalizations of the associative quotient algebras $K[t;\sigma]/fK[t;\sigma]$ obtained when the twisted polynomial $f \in K[t;\sigma]$ is invariant, and were first defined by Petit.

We compute all their automorphisms if σ commutes with all automorphisms in $\mathrm{Aut}_F(K)$ and $n \geq m-1$, where n is the order of σ and m the degree of f, and obtain partial results for $n < m-1$.

When K/F is a finite Galois field extension, we compute some automorphism groups. We also briefly investigate when two such algebras are isomorphic.

Introduction

Let D be a division algebra, σ an injective endomorphism of D, δ a left σ-derivation and $R = D[t;\sigma,\delta]$ a skew polynomial ring. For an invariant skew polynomial $f \in R$, i.e. when the ideal Rf is a two-sided principal ideal, the quotient algebra R/Rf appears in classical constructions of associative central simple algebras, usually employing an irreducible $f \in R$ to get examples of division algebras, e.g. see [13].

In 1967, Petit [18, 19] introduced a class of unital nonassociative algebras S_f, which canonically generalize the quotient algebras R/Rf obtained when factoring out an invariant $f \in R$ of degree m. The algebra $S_f = D[t;\sigma,\delta]/D[t;\sigma,\delta]f$ is defined on the additive subgroup $\{h \in R \,|\, \deg(h) < m\}$ of R by using right division by f to define the algebra multiplication $g \circ h = gh \,\mathrm{mod}_r f$. The properties of the algebras S_f were studied in detail in [18, 19], and for D a finite base field (hence w.l.o.g. $\delta = 0$) in [16].

Even earlier, the algebra S_f with $f(t) = t^2 - i \in \mathbb{C}[t;^-]$, $^-$ the complex conjugation, appeared in [6] as the first example of a nonassociative division algebra.

Although the algebras themselves have received little attention so far, the right nucleus of S_f (the *eigenspace* of $f \in R$) already appeared implicitly in classical constructions by Amitsur [1, 2, 3], but also in results on computational aspects of operator algebras; they are for instance used in algorithms factoring skew polynomials over $\mathbb{F}_q(t)$ or finite fields, cf. [9, 10, 11, 12].

Moreover, recently space-time block codes, coset codes and wire-tap codes were obtained employing the algebras S_f over number fields, cf. [7, 8, 17, 20, 23, 24, 25], and they also appear useful for linear cyclic codes [21, 22].

1991 *Mathematics Subject Classification.* Primary: 17A35; Secondary: 17A60, 17A36, 16S36.

Key words and phrases. Skew polynomial ring, skew polynomials, Ore polynomials, automorphisms, nonassociative algebras.

If K is a finite field, F the fixed field of σ, K/F a finite Galois field extension and $f \in K[t;\sigma] = K[t;\sigma,0]$ irreducible and invariant, the S_f are *Jha-Johnson semifields* (also called *cyclic semifields*) [16, Theorem 15], and were studied for instance by Wene [31] and more recently by Lavrauw and Sheekey [16]. The main motivation for our paper comes from the question how the automorphism groups of Jha-Johnson semifields look like. The results presented here are applied to some Jha-Johnson semifields in [5].

The structure of the paper is as follows: In Section 1, we introduce the terminology and define the algebras S_f. We limit our observations to the algebras which are not associative. Given a field extension K, $\sigma \in \mathrm{Aut}(K)$ of order n with fixed field F, such that σ commutes with all $\tau \in \mathrm{Aut}_F(K)$, and $f \in K[t;\sigma]$ of degree m not invariant, we compute the automorphisms of S_f in Section 2. We obtain all automorphisms for $n \geq m-1$ and some partial results for $n < m-1$ (Theorems 4 and 5). For $n \geq m-1$, the automorphisms in $\mathrm{Aut}_F(S_f)$ are canonically induced by the F-automorphism G of $R = K[t;\sigma]$ which satisfy $G(f(t)) = af(t)$ for some $a \in K^\times$, and on K restrict to an automorphism that commutes with τ.

The automorphisms groups of S_f where $f(t) = t^m - a \in K[t;\sigma]$, $a \in K \setminus F$, play a special role, as for all nonassociative S_g with $g(t) = t^m - \sum_{i=0}^{m-1} b_i t^i \in K[t;\sigma]$ and $b_0 = a$, $\mathrm{Aut}_F(S_g)$ is a subgroup of $\mathrm{Aut}_F(S_f)$ when $n \geq m-1$.

We then focus on the situation that K/F is a finite Galois field extension such that σ commutes with all $\tau \in \mathrm{Gal}(K/F)$. In many cases, either $\mathrm{Aut}_F(S_f) \cong \mathrm{Gal}(K/F)$ or is trivial (Theorem 11). Necessary conditions for extending Galois automorphisms $\tau \in \mathrm{Gal}(K/F)$ to S_f are studied in Sections 3 and 4. The existence of cyclic subgroups of $\mathrm{Aut}_F(S_f)$ is investigated in Section 5.

For $f(t) = t^m - a \in K[t;\sigma]$ and K/F a cyclic field extension of degree m, the algebra S_f is also called a *nonassociative cyclic algebra* and denoted by $(K/F,\sigma,a)$. These algebras are canonical generalizations of associative cyclic algebras, but also generalizations of the algebras in [2, 13]. The automorphisms of nonassociative cyclic algebras are investigated in Section 6. All the automorphisms of $A = (K/F,\sigma,a)$ extending id_K are inner and form a cyclic subgroup of $\mathrm{Aut}_F(A)$ isomorphic to $\ker(N_{K/F})$. In some cases, this is the whole automorphism group, e.g. if F has no mth root of unity. In these cases, every automorphism of A leaves K fixed and is inner. We explain when the automorphism group of a nonassociative quaternion algebra A (where $m = 2$) contains a dicyclic group and when it contains a subgroup isomorphic to the semidirect product of two cyclic groups.

In Section 7 we briefly investigate isomorphisms between two algebras S_f and S_g.

This work is part of the first author's PhD thesis [4] written under the supervision of the second author. For results on the automorphisms of the more general algebras defined using $f \in D[t;\sigma]$, or a more detailed study and the (less relevant) cases left out in this paper the reader is referred to [4].

1. Preliminaries

1.1. **Nonassociative algebras.** Let F be a field and let A be an F-vector space. A is an *algebra* over F if there exists an F-bilinear map $A \times A \to A$, $(x,y) \mapsto x \cdot y$, denoted simply by juxtaposition xy, the *multiplication* of A. An algebra A is 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 from now on without explicitly saying so.

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* of A is $\mathrm{Nuc}_m(A) = \{x \in A \,|\, [A, x, A] = 0\}$ and the *right nucleus* of A is defined 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 $F1$ and $x(yz) = (xy)z$ whenever one of the elements x, y, z lies in $\mathrm{Nuc}(A)$. The *center* of A is $\mathrm{C}(A) = \{x \in A \,|\, x \in \mathrm{Nuc}(A)$ and $xy = yx$ for all $y \in A\}$.

An F-algebra $A \neq 0$ 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. If A has finite dimension over F, A is a division algebra if and only if A has no zero divisors [27, pp. 15, 16]. An element $0 \neq a \in A$ has a *left inverse* $a_l \in A$, if $R_a(a_l) = a_l a = 1$, and a *right inverse* $a_r \in A$, if $L_a(a_r) = aa_r = 1$.

An automorphism $G \in \mathrm{Aut}_F(A)$ is an *inner automorphism* if there is an element $m \in A$ with left inverse m_l such that $G(x) = (m_l x)m$ for all $x \in A$. Given an inner automorphism $G_m \in \mathrm{Aut}_F(A)$ and some $H \in \mathrm{Aut}_F(A)$, then clearly $H^{-1} \circ G_m \circ H \in \mathrm{Aut}_F(A)$ is an inner automorphism. [30, Lemma 2, Theorem 3, 4] generalize to any nonassociative algebra:

Proposition 1. *Let A be an algebra over F.*
(i) For all invertible $n \in \mathrm{Nuc}(A)$, $G_n(x) = (n^{-1}x)n$ is an inner automorphism of A.
(ii) If G_m is an inner automorphism of A, then so is $G_{nm}(x) = ((m_l n^{-1})x)(nm)$ for all invertible $n \in \mathrm{Nuc}(A)$.
(iii) If G_m is an inner automorphism of A, and $a, b \in \mathrm{Nuc}(A)$ are invertible, then

$$G_{am} = G_{bm} \text{ if and only if } ab^{-1} \in C(A).$$

(iv) For invertible $n, m \in \mathrm{Nuc}(A)$, $G_m = G_n$ if and only if $n^{-1}m \in C(A)$.

The set $\{G_m \,|\, m \in \mathrm{Nuc}(A) \text{ invertible}\}$ is a subgroup of $\mathrm{Aut}_F(A)$. For each invertible $m \in \mathrm{Nuc}(A) \setminus C(A)$, G_m generates a cyclic subgroup which has finite order s if $m^s \in C(A)$, so in particular if m has order s.

Note that if the nucleus is commutative, then for all invertible $n \in \mathrm{Nuc}(A)$, $G_n(x) = (n^{-1}x)n$ is an inner automorphism of A such that $G_n|_{\mathrm{Nuc}(A)} = id_{\mathrm{Nuc}(A)}$.

1.2. **Twisted polynomial rings.** Let K be a field and σ an automorphism of K. The *twisted polynomial ring* $K[t;\sigma]$ is the set of polynomials

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

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

$$ta = \sigma(a)t$$

for all $a \in K$. For $f = a_0 + a_1 t + \cdots + a_n t^n$ with $a_n \neq 0$ define $\deg(f) = n$ and put $\deg(0) = -\infty$. Then $\deg(fg) = \deg(f) + \deg(g)$. 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 $f = gh$.

$R = K[t;\sigma]$ is a left and right principal ideal domain and there is a right division algorithm in R: for all $g, f \in R$, $g \neq 0$, there exist unique $r, q \in R$ with $\deg(r) < \deg(f)$, such that

$$g = qf + r.$$

There is also a left division algorithm in R [13, p. 3 and Prop. 1.1.14]. (Our terminology is the one used by Petit [18] and Lavrauw and Sheekey [16]; it is different from Jacobson's, who calls what we call right a left division algorithm and vice versa.) Define $F = \mathrm{Fix}(\sigma)$.

1.3. **Nonassociative algebras obtained from skew polynomial rings.** Let K be a field, σ an automorphism of K with $F = \mathrm{Fix}(\sigma)$, and $f \in R = K[t;\sigma]$ of degree m. Let $\mathrm{mod}_r f$ denote the remainder of right division by f. Then then additive abelian group

$$R_m = \{g \in K[t;\sigma] \,|\, \deg(g) < m\}$$

together with the multiplication

$$g \circ h = gh \ \mathrm{mod}_r f$$

is a unital nonassociative algebra $S_f = (R_m, \circ)$ over

$$F_0 = \{a \in K \,|\, ah = ha \text{ for all } h \in S_f\}.$$

F_0 is a subfield of K [18, (7)] and it is straightforward to see that $F_0 = F$. The algebra S_f is also denoted by R/Rf [18, 19] if we want to make clear which ring R is involved in the construction. In the following, we call the algebras S_f *Petit algebras* and denote their multiplication simply by juxtaposition.

Using left division by f and the remainder $\mathrm{mod}_l f$ of left division by f instead, we can analogously define the multiplication for another unital nonassociative algebra on R_m over F_0, called ${}_fS$. We will only consider the Petit algebras S_f, since every algebra ${}_fS$ is the opposite algebra of some Petit algebra [18, (1)].

Theorem 2. *(cf.* [18, (2), (5), (9)]*) Let $f(t) \in R = K[t;\sigma]$.*
(i) If S_f is not associative then $\mathrm{Nuc}_l(S_f) = \mathrm{Nuc}_m(S_f) = K$ and

$$\mathrm{Nuc}_r(S_f) = \{g \in R \,|\, fg \in Rf\}.$$

(ii) The powers of t are associative if and only if $t^m t = t t^m$ if and only if $t \in \mathrm{Nuc}_r(S_f)$ if and only if $ft \in Rf$.
(iii) Let $f \in R$ be irreducible and S_f a finite-dimensional F-vector space or free of finite rank as a right $\mathrm{Nuc}_r(S_f)$-module. Then S_f is a division algebra.
Conversely, if S_f is a division algebra then f is irreducible.
(iv) S_f is associative if and only if f is invariant. In that case, S_f is the usual quotient algebra.
(v) Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in R = K[t;\sigma]$. Then f is invariant if and only if $\sigma^m(z)a_i = a_i\sigma^i(z)$ for all $z \in K$, $i \in \{0, \ldots, m-1\}$ and $a_i \in F$ for all $i \in \{0, \ldots, m-1\}$.

Note that the nucleus of any $S_f = K[t;\sigma]/K[t;\sigma]f$, f not invariant, is a subfield of $K = \mathrm{Nuc}_l(S_f)$. If it is larger than F, then $\{G_m \,|\, 0 \neq m \in \mathrm{Nuc}(A)\}$ is a non-trivial subgroup of $\mathrm{Aut}_F(S_f)$ and each inner automorphism G_m in this subgroup extends $id_{\mathrm{Nuc}(A)}$ by Proposition 1.

Proposition 3. *Let $f(t) \in F[t] = F[t;\sigma] \subset K[t;\sigma]$.*
(i) $F[t]/(f(t))$ is a commutative subring of S_f and

$$F[t]/(f(t)) \cong F \oplus Ft \oplus \cdots \oplus Ft^{m-1} \subset \mathrm{Nuc}_r(S_f).$$

In particular, then $ft \in Rf$ which is equivalent to the powers of t being associative, which again is equivalent to $t^m t = t t^m$.
(ii) If $f(t)$ is irreducible in $F[t]$, $F[t]/(f(t))$ is an algebraic subfield of degree m contained in the right nucleus.

Proof. S_f contains the commutative subring $F[t]/(f(t))$. If $f(t)$ is irreducible in $F[t]$, this is an algebraic field extension of F. This subring is isomorphic to the ring consisting of the elements $\sum_{i=0}^{m-1} a_i t^i$ with $a_i \in F$.

Clearly $F \subset \mathrm{Nuc}_r(S_f)$. For all $a, b, c \in K$, $i, j \in \{0, \ldots, m-1\}$ we have

$$[at^i, bt^j, t] = (a\sigma^i(b)t^{i+j})t - (at^i)(bt^{j+1}) = a\sigma^i(b)t^{i+j+1} - a\sigma^i(bc)t^{i+j} = 0.$$

Thus $t \in \mathrm{Nuc}_r(S_f)$ which implies that $F \oplus Ft \oplus \cdots \oplus Ft^{m-1} \subset \mathrm{Nuc}_r(S_f)$, hence the assertion. The rest is obvious. □

We will assume throughout the paper that $\deg(f) = m \geq 2$ (since if f is constant then $S_f \cong K$) and that $\sigma \neq id$. Without loss of generality, we only consider monic polynomials f, since $S_f = S_{af}$ for all non-zero $a \in K$.

2. Automorphisms of S_f

2.1. Let K be a field, σ an automorphism of K of order n (which may be infinite), $F = \mathrm{Fix}(\sigma)$, and

$$f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in K[t;\sigma]$$

a twisted polynomial which is not invariant.

Theorem 4. *Suppose σ commutes with all $\tau \in \mathrm{Aut}_F(K)$. Let $n \geq m-1$. Then H is an automorphism of S_f if and only if $H = H_{\tau,k}$ where*

$$H_{\tau,k}(\sum_{i=0}^{m-1} x_i t^i) = \tau(x_0) + \tau(x_1)kt + \tau(x_2)k\sigma(k)t^2 + \cdots + \tau(x_{m-1})k\sigma(k)\cdots\sigma^{m-2}(k)t^{m-1},$$

where $\tau \in \mathrm{Aut}_F(K)$ and $k \in K^\times$ is such that

$$\tau(a_i) = \Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big) a_i \qquad (1)$$

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

Proof. Let $H : S_f \to S_f$ be an automorphism. Since S_f is not associative, $\mathrm{Nuc}_l(S_f) = K$ by Theorem 2 (i). Since any automorphism preserves the left nucleus, $H(K) = K$ and so $H|_K = \tau$ for some $\tau \in \mathrm{Aut}_F(K)$. Suppose $H(t) = \sum_{i=0}^{m-1} k_i t^i$ for some $k_i \in K$. Then we have

$$H(tz) = H(t)H(z) = (\sum_{i=0}^{m-1} k_i t^i)\tau(z) = \sum_{i=0}^{m-1} k_i \sigma^i(\tau(z))t^i \tag{2}$$

and

$$H(tz) = H(\sigma(z)t) = \sum_{i=0}^{m-1} \tau(\sigma(z))k_i t^i \tag{3}$$

for all $z \in K$. Comparing the coefficients of t^i in (2) and (3) we obtain

$$k_i\sigma^i(\tau(z)) = k_i\tau(\sigma^i(z)) = \tau(\sigma(z))k_i = k_i\tau(\sigma(z)) \tag{4}$$

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

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

for all $i \in \{0, \dots, m-1\}$ and all $z \in K$ since σ and τ commute, i.e.

$$k_i = 0 \text{ or } \sigma^i(z) = \sigma(z) \tag{5}$$

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

σ has order $n \geq m-1$, which means $\sigma^i \neq \sigma$ for all $i \in \{0, \dots, m-1\}$, $i \neq 1$, so (5) implies $k_i = 0$ for all $i \in \{0, \dots, m-1\}$, $i \neq 1$. Therefore $H(t) = kt$ for some $k \in K^\times$. Furthermore, we have

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

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

$$H_{\tau,k}(\sum_{i=0}^{m-1} x_i t^i) = \tau(x_0) + \sum_{i=1}^{m-1} \tau(x_i) \prod_{l=0}^{i-1} \sigma^l(k) t^i, \tag{6}$$

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

$$H(t^m) = H\Big(\sum_{i=0}^{m-1} a_i t^i\Big) = \sum_{i=0}^{m-1} H(a_i)H(t)^i = \tau(a_0) + \sum_{i=1}^{m-1} \tau(a_i)\big(\prod_{l=0}^{i-1} \sigma^l(k)\big)t^i \tag{7}$$

and $H(tt^{m-1}) = H(t)H(t^{m-1}) = H(t)H(t)^{m-1}$, i.e.

$$H(t)^m = H(t)H(t)^{m-1} = k\sigma(k)\cdots\sigma^{m-1}(k)t^m = k\sigma(k)\cdots\sigma^{m-1}(k)\sum_{i=0}^{m-1} a_i t^i. \tag{8}$$

Comparing (7) and (8) gives

$$\tau(a_i) = \Big(\prod_{q=i}^{m-1} \sigma^q(k)\Big)a_i$$

for all $i \in \{0, \dots, m-1\}$. Thus H is as in (6) where $k \in K^\times$ is such that (1) holds for all $i \in \{0, \dots, m-1\}$.

The $H_{\tau,k}$ are indeed automorphisms of S_f: Let G be an automorphism of $R = K[t;\sigma]$. Then for $h(t) = \sum_{i=0}^{r} b_i t^i \in K[t;\sigma]$ we have

$$G(h(t)) = \tau(b_0) + \sum_{i=i}^{m-1} \tau(b_i) \prod_{l=0}^{i-1} \sigma^l(k) t^i$$

for some $\tau \in \mathrm{Aut}(K)$ such that $\sigma \circ \tau = \tau \circ \sigma$ and some $k \in K^\times$ (the proof of [16, Lemma 1] works for any $R = K[t;\sigma]$, or cf. [14, p. 75]). It is straightforward to see that $S_f \cong S_{G(f)}$ (cf. [16, Theorem 7], the proof works for any $R = K[t;\sigma]$). In particular, this means that if $k \in K^\times$ satisfies Equation (1) then

$$G(f(t)) = \big(\prod_{l=0}^{m-1} \sigma^l(k) \big) f(t) = af(t)$$

with $a \in K^\times$ being the product of the $\sigma^l(k)$, and so G induces an isomorphism of S_f with $S_{af} = S_f$, i.e. an automorphism of S_f.

The automorphisms of $\mathrm{Aut}_F(S_f)$ are therefore all canonically induced by the F-automorphism G of $R = K[t;\sigma]$ which satisfy Equation (1). □

The assumption that $n \geq m-1$ is needed in Equation (4) to conclude that $k_i = 0$ for $i = 0, 2, 3, \ldots, m-1$ and so $H(t) = kt$. If $n < m-1$ we still obtain:

Theorem 5. *Suppose σ commutes with all $\tau \in \mathrm{Aut}_F(K)$. Let $n < m-1$.*
(i) For all $k \in K^\times$ satisfying Equation (1) for all $i \in \{0, \ldots, m-1\}$, the maps $H_{\tau,k}$ from Theorem 4 are automorphisms of S_f and form a subgroup of $\mathrm{Aut}_F(S_f)$.
(ii) Let $H \in \mathrm{Aut}_F(S_f)$ and $N = \mathrm{Nuc}_r(S_f)$. Then $H|_K = \tau$ for some $\tau \in \mathrm{Aut}_F(K)$, $H|_N \in \mathrm{Aut}_F(N)$ and $H(t) = g(t)$ with

$$g(t) = k_1 t + k_{1+n} t^{1+n} + k_{1+2n} t^{1+2n} + \ldots + k_{1+sn} t^{1+sn}$$

for some $k_{1+ln} \in K$, $0 \leq l \leq s$. Moreover, $g(t)^i$ is well defined for all $i \leq m-1$, i.e., all powers of $g(t)$ are associative for all $i \leq m-1$, and

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

Thus

$$H\Big(\sum_{i=0}^{m-1} x_i t^i\Big) = \sum_{i=0}^{m-1} \tau(x_i) g(t)^i.$$

Proof. (i) is straightforward, using the relevant parts of the proof of Theorem 4. Note that the inverse of $H_{\tau,k}$ is $H_{\tau^{-1},\tau^{-1}(k^{-1})}$ and

$$H_{\tau,k} \circ H_{\rho,b} = H_{\tau\rho,\tau(b)k}.$$

(ii) Let $H : S_f \to S_f$ be an automorphism. As in Theorem 4, $H|_K = \tau$ for some $\tau \in \mathrm{Aut}_F(K)$, and $H|_N \in \mathrm{Aut}_F(N)$. Suppose $H(t) = \sum_{i=0}^{m-1} k_i t^i$ for some $k_i \in K$. Comparing the coefficients of t in $H(tz) = H(t)H(z) = H(\sigma(z)t)$ we obtain

$$k_i = 0 \text{ or } \sigma^i(z) = \sigma(z) \tag{9}$$

for all $i \in \{0, \dots, m-1\}$ and all $z \in K$. Since σ has order $n < m-1$, (9) here only implies $k_i = 0$ for $i \in \{0, \dots, n\}$, $i \neq 1$. Therefore

$$H(t) = k_1 t + \sum_{i=n+1}^{m-1} k_i t^i$$

for some $k_i \in K$. However, $\sigma^i(z) = \sigma(z)$ for all $z \in K$ if and only if $i = nl + 1$ for some $l \in \mathbb{Z}$ since σ has order n. Therefore (9) implies $k_i = 0$ for every $i \neq 1 + nl$, $l \in \mathbb{N}_0$, $i \in \{0, \dots, m-1\}$. Thus

$$H(t) = k_1 t + k_{1+n} t^{n+1} + \ldots + k_{1+sn} t^{1+sn}$$

for some s, $sn < m-1$. Furthermore,

$$H(t^m) = H(\sum_{i=0}^{m-1} a_i t^i) = \sum_{i=0}^{m-1} \tau(a_i)(k_1 t + k_{1+n} t^{1+n} + \ldots + k_{1+sn} t^{1+sn})^i$$

and

$$H(t^m) = (k_1 t + k_{1+n} t^{1+n} + \ldots + k_{1+sn} t^{1+sn})^m.$$

Similarly,

$$H(t)^i = (k_1 t + k_{1+n} t^{1+n} + \ldots + k_{1+sn} t^{1+sn})^i.$$

Together this implies the assertion. □

Remark 6. Note that for $H_{\tau,k}, H_{\tau',l} \in \mathrm{Aut}_F(S_f)$, $H_{\tau,k} = H_{\tau',l}$ if and only if $\tau = \tau'$ and $l = k$. Thus there is a one-one correspondence between elements in $\mathrm{Aut}_F(S_f)$ and in

$$\{(\tau, k) \,|\, \tau \in \mathrm{Aut}_F(K) \text{ with } \tau \circ \sigma = \sigma \circ \tau, k \in K^\times \text{ with } \tau(a_i) = (\prod_{l=i}^{m-1} \sigma^l(k)) a_i \text{ for all } i\},$$

$$H_{\tau,k} \leftrightarrow (\tau, k).$$

A closer look at the proof of Theorems 4 and 5 reveals that in fact the following holds without requiring σ to commute with all $\tau \in \mathrm{Aut}_F(K)$:

Proposition 7. *(i) For every $k \in K^\times$ satisfying Equation (1) for all $i \in \{0, \dots, m-1\}$ for $\tau = id$, $H_{id,k}$ is an automorphism of S_f and generates a subgroup of $\mathrm{Aut}_F(S_f)$.*
(ii) If any $H \in \mathrm{Aut}_F(S_f)$ restricts to some $\tau \in \mathrm{Aut}_F(K)$ such that $\tau \circ \sigma = \sigma \circ \tau$ then $H = H_{\tau,k}$ with $k \in K^\times$ as in Theorem 4. Moreover,

$$\{H_{\tau,k} \,|\, \tau \in \mathrm{Aut}_F(S_f), \tau \circ \sigma = \sigma \circ \tau, k \in K^\times \text{ with } \tau(a_i) = (\prod_{l=i}^{m-1} \sigma^l(k)) a_i \text{ for all } i \in \{0, \dots, m-1\}\}$$

is a subgroup of $\mathrm{Aut}_F(S_f)$.
(iii) If $m = 2$, $H \in \mathrm{Aut}(S_f)$ if and only if $H = H_{\tau,k}$ with $\tau \circ \sigma = \sigma \circ \tau$ and

$$\tau(a_0) = k\sigma(k) a_0, \quad \tau(a_1) = \sigma(k) a_1.$$

2.2. The automorphisms groups of S_f for $f(t)=t^m-a\in K[t;\sigma]$, $a\in K\setminus F$, are crucial in the understanding of the automorphism groups of all the algebras S_g, as for all nonassociative S_g with $g(t)=t^m-\sum_{i=0}^{m-1}b_it^i\in K[t;\sigma]$ such that $b_0=a$, $\mathrm{Aut}_F(S_g)$ is a subgroup of $\mathrm{Aut}_F(S_f)$:

Theorem 8. *Suppose σ commutes with all $\tau\in\mathrm{Gal}(K/F)$. Let $n\geq m-1$ and $g(t)=t^m-\sum_{i=0}^{m-1}b_it^i\in K[t;\sigma]$ not be invariant.*
(i) If $f(t)=t^m-b_0\in K[t;\sigma]$, $b_0\in K\setminus F$, then

$$\mathrm{Aut}_F(S_g)\subset\mathrm{Aut}_F(S_f)$$

is a subgroup.
(ii) Let $f(t)=t^m-\sum_{i=0}^{m-1}a_it^i\in K[t;\sigma]$ not be invariant and assume $b_i\in\{0,a_i\}$ for all $i\in\{0,\dots,m-1\}$.
Then

$$\mathrm{Aut}_F(S_g)\subset\mathrm{Aut}_F(S_f)$$

is a subgroup.

Proof. (i) Let $H\in\mathrm{Aut}_F(S_g)$. By Theorem 4, H has the form

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

where $\tau\in\mathrm{Aut}_F(K)$ and $k\in K^\times$ satisfy $\tau(b_i)=\Big(\prod_{j=i}^{m-1}\sigma^j(k)\Big)b_i$ for all $i=0,\dots,m-1$. In particular,

$$\tau(b_0)=k\sigma(k)\cdots\sigma^{m-1}(k)b_0$$

and so H is also an automorphism of S_f, again by Theorem 4.
(ii) The proof is analogous to (i). □

Analogously, we still obtain for $n<m-1$ employing Theorem 5:

Theorem 9. *Suppose σ commutes with all $\tau\in\mathrm{Aut}_F(K)$. Let $n<m-1$ and $g(t)=t^m-\sum_{i=0}^{m-1}b_it^i\in K[t;\sigma]$ not be invariant.*
(i) If $f(t)=t^m-b_0\in K[t;\sigma]$, $b_0\in K\setminus F$, then

$$\{H\in\mathrm{Aut}_F(S_g)\,|\,H=H_{\tau,k}\}\text{ is a subgroup of }\{H\in\mathrm{Aut}_F(S_f)\,|\,H=H_{\tau,k}\}.$$

(ii) Let $f(t)=t^m-\sum_{i=0}^{m-1}a_it^i\in K[t;\sigma]$ not be invariant such that $b_i\in\{0,a_i\}$ for all $i\in\{0,\dots,m-1\}$ Then

$$\{H\in\mathrm{Aut}_F(S_g)\,|\,H=H_{\tau,k}\}\text{ is a subgroup of }\{H\in\mathrm{Aut}_F(S_f)\,|\,H=H_{\tau,k}\}.$$

The automorphism groups of S_f with $f(t)=t^m-a\in K[t;\sigma]$ are therefore particularly relevant.

3. Necessary conditions for extending Galois automorphisms to S_f

From now on we restrict ourselves to the situation that $R = K[t;\sigma]$ and $F = \mathrm{Fix}(\sigma)$, where K/F is a finite Galois field extension and σ of order n.

We take a closer look at Equation (1), which gives necessary conditions on how to choose the elements $k \in K^\times$ used to extend $\tau \in \mathrm{Gal}(K/F)$ to $\mathrm{Aut}_F(S_f)$. These become more restrictive for the choice of the elements k, the more coefficients in $f(t)$ are non-zero. Let $N_{K/F} : K \to F$ be the norm of K/F. All monic polynomials f considered in the following are assumed to not be invariant and of degree m.

Proposition 10. *Suppose that σ and τ commute. Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in K[t;\sigma]$ and $k \in K^\times$ such that*

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

for all $i \in \{0,\dots,m-1\}$. Then:
(i) For all $i \in \{0,\dots,m-1\}$ with $a_i \neq 0$, $N_{K/F}(k)$ is an $(m-i)$th root of unity.
In particular, if $a_0 \neq 0$ (e.g., if $f(t)$ is irreducible) then $N_{K/F}(k)$ is an mth root of unity, and if $a_{m-1} \neq 0$ then $N_{K/F}(k) = 1$.
If $a_{m-1} \in \mathrm{Fix}(\tau)^\times$ then $k = 1$.
(ii) If $\tau \neq id$ and there is some i such that a_i is not contained in $\mathrm{Fix}(\tau)$, then $k \neq 1$.
(iii) Suppose that there is some $a_i \neq 0$ and F does not contain any non-trivial $(m-i)$th roots of unity. Then $N_{K/F}(k) = 1$.
(iv) If there is an $i \in \{0,\dots,m-1\}$ such that $a_i \in \mathrm{Fix}(\tau)^\times$, then

$$1 = \prod_{l=i}^{m-1} \sigma^l(k).$$

In particular, if $n = m$, σ generates $\mathrm{Gal}(K/F)$, and $a_0 \in \mathrm{Fix}(\tau)^\times$ then $k \in \ker(N_{K/F})$.
(v) Suppose $\tau = id_K$. Then for all $i \in \{0,\dots,m-1\}$ with $a_i \neq 0$,

$$1 = \prod_{l=i}^{m-1} \sigma^l(k).$$

In particular, if $n = m$, σ generates $\mathrm{Gal}(K/F)$ and $a_0 \neq 0$ then $k \in \ker(N_{K/F})$. In this case, the automorphisms extending id_K are in one-one correspondence with those $k \in \ker(N_{K/F})$ satisfying Equation (1).

Proof. (i) Equation (1) states that $\tau(a_i) = \Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big)a_i$ for all $i \in \{0,\dots,m-1\}$. Thus

$$N_{K/F}(a_i) = \prod_{l=i}^{m-1} N_{K/F}(\sigma^l(k)) N_{K/F}(a_i)$$

(apply $N_{K/F}$ to both sides), and therefore

$$N_{K/F}(a_i) = N_{K/F}(k)^{m-i} N_{K/F}(a_i)$$

for all $i \in \{0,\dots,m-1\}$ is a necessary condition on k. For all $a_i \neq 0$, this yields

$$1 = N_{K/F}(k)^{m-i}$$

therefore $N_{K/F}(k) \in F^\times$ must be an $(m-i)$th root of unity, for all $i \in \{0, \dots, m-1\}$, with $a_i \neq 0$.

Hence if $a_{m-1} \neq 0$ then $\tau(a_{m-1}) = \sigma^{m-1}(k)a_{m-1}$, thus $N_{K/F}(a_{m-1}) = N_{K/F}(k)N_{K/F}(a_{m-1})$, i.e. $N_{K/F}(k) = 1$. If even $a_{m-1} \in \text{Fix}(\tau)^\times$ then $a_{m-1} = \sigma^{m-1}(k)a_{m-1}$ means $\sigma^{m-1}(k) = 1$, i.e. $k = 1$.

(ii) $k = 1$ implies $\tau(a_i) = a_i$, i.e. $a_i \in \text{Fix}(\tau)$ for all $i \in \{0, \dots, m-1\}$.

(iii) By (i), $N_{K/F}(k) \in F^\times$ is an $(m-i)$th root of unity, for all $i \in \{0, \dots, m-1\}$ with $a_i \neq 0$. If F does not contain any non-trivial $(m-i)$th roots of unity, then $N_{K/F}(k) = 1$.

(iv) If there is an $i \in \{0, \dots, m-1\}$ such that $a_i \in \text{Fix}(\tau)^\times$, then (1) becomes $1 = \prod_{l=i}^{m-1} \sigma^l(k)$. In particular, if $a_0 \in \text{Fix}(\tau)^\times$, $m = n$ and σ generates $\text{Gal}(K/F)$, then $N_{K/F}(k) = 1$ is a necessary condition on k.

(v) Here, (1) becomes $1 = \prod_{l=i}^{m-1} \sigma^l(k)$ for all $i \in \{0, \dots, m-1\}$ with $a_i \neq 0$. In particular, if $n = m$, σ generates $\text{Gal}(K/F)$ and $a_0 \neq 0$ (which happens if $f(t)$ is irreducible) then $N_{K/F}(k) = 1$ is a necessary condition on k. □

For instance, Proposition 10 (i) yields that $k = 1$ if $a_{m-1} \in \text{Fix}(\tau)^\times$ and so Theorems 4 and 5 become:

Theorem 11. *Suppose σ commutes with all $\tau \in \text{Gal}(K/F)$ and $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in K[t;\sigma]$ is not invariant with $a_{m-1} \in F^\times$.*

(i) Let $n \geq m-1$. We distinguish two cases: If $a_i \notin \text{Fix}(\tau)$ for all $\tau \neq id$ and all non-zero a_i, $i \neq m-1$, then

$$\text{Aut}_F(S_f) = \{id\}.$$

If $f(t) \in F[t;\sigma]$, any automorphism H of S_f has the form $H_{\tau,1}$ where $\tau \in \text{Gal}(K/F)$, and

$$\text{Aut}_F(S_f) \cong \text{Gal}(K/F).$$

(ii) Let $n < m-1$. If $f(t) \in F[t;\sigma]$ is not invariant, the maps $H_{\tau,1}$ are automorphisms of S_f for all $\tau \in \text{Gal}(K/F)$ and $\text{Gal}(K/F)$ is isomorphic to a subgroup of $\text{Aut}_F(S_f)$.

Proof. (i) H is an automorphism of S_f if and only if H has the form $H_{\tau,k}$, where $\tau \in \text{Gal}(K/F)$ and $k \in K^\times$ is such that

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

for all $i \in \{0, \dots, m-1\}$. Since $a_{m-1} \in F^\times$ we have $a_{m-1} \in \text{Fix}(\tau)^\times$ for all τ which forces $k = 1$ as the only possibility for any $\tau \in \text{Gal}(K/F)$ by Proposition 10 (i). This in turn means that any extension $H_{\tau,k}$ has the form $H_{\tau,1}$. In particular, the existence of an extension $H_{\tau,k}$, $\tau \neq id$, implies $\tau(a_i) = a_i$ for all non-zero a_i, $i \neq m-1$, that is $a_i \in \text{Fix}(\tau)$ for all non-zero a_i.

Thus if $a_i \notin \text{Fix}(\tau)$ for all $\tau \neq id$ and all $i \in \{0, \dots, m-2\}$ then there is no non-trivial τ that extends to an automorphism of S_f and $\text{Aut}_F(S_f) = \{H_{id,1}\} = \{id\}$.

If $f(t) \in F[t;\sigma]$ then $\text{Aut}_F(S_f) = \{H_{\tau,1}\} \cong \text{Gal}(K/F)$.

(ii) follows from (i) and Theorem 9. □

Remark 12. Condition (1) heavily restricts the choice of available k to $k = 1$ in most cases. For instance, suppose we have $n \geq m-1$ and two consecutive non-zero $a_s, a_{s+1} \in \mathrm{Fix}(\tau)$. This implies

$$\prod_{l=s}^{m-1} \sigma^l(k) = 1 = \prod_{l=s+1}^{m-1} \sigma^l(k),$$

thus cancel to get $\sigma^s(k) = 1$, i.e. $k = 1$ for any such τ. This means any $H_{\tau,k}$ will have the form $H_{\tau,1}$, where $\tau \in \mathrm{Gal}(K/F)$ and necessarily, $\tau(a_i) = a_i$ for all non-zero a_i. I.e. $a_i \in \mathrm{Fix}(\tau)$ for all the other non-zero a_i when $\tau \neq id$. Therefore for all non-invariant $f(t) \in K[t;\sigma]$ with two consecutive elements a_s and a_{s+1} in $F^\times$ such that for all other non-zero a_i we have $a_i \notin \mathrm{Fix}(\tau)$ for all $\tau \neq id$,

$$\mathrm{Aut}_F(S_f) = \{id\}.$$

However, if $f(t) \in F[t;\sigma]$ is not invariant and has two consecutive non-zero $a_s, a_{s+1} \in F$, then

$$\mathrm{Aut}_F(S_f) \cong \mathrm{Gal}(K/F).$$

Corollary 13. *Suppose σ commutes with all $\tau \in \mathrm{Gal}(K/F)$. Let $n \geq m-1$ and $f(t) = t^m - a_0 \in K[t;\sigma]$, $a_0 \in K \setminus F$.*
(i) $H \in \mathrm{Aut}_F(S_f)$ if and only if $H = H_{\tau,k}$ where $k \in K^\times$ is such that

$$\tau(a_0) = \Big(\prod_{l=0}^{m-1} \sigma^l(k)\Big) a_0.$$

In particular, here $N_{K/F}(k)$ is an mth root of unity.
(ii) For all $g(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in K[t;\sigma]$ with $a_0 \in K \setminus F$, $\mathrm{Aut}_F(S_g)$ is a subgroup of $\mathrm{Aut}_F(S_f)$.

Proof. (i) follows from Theorem 4 and Proposition 10.
(ii) follows from Theorem 8. □

For $f(t) = t^m - a_0 \in K[t;\sigma]$, $a_0 \in K \setminus F$, the automorphisms $H_{id,k}$ extending id_K thus are in one-one correspondence with those k satisfying

$$\prod_{l=0}^{m-1} \sigma^l(k) = 1$$

(in particular, we have $N_{K/F}(k)^m = 1$). Analogously, we still obtain for $n < m-1$ employing Theorem 5 and Theorem 9:

Corollary 14. *Suppose σ commutes with all $\tau \in \mathrm{Gal}(K/F)$. Let $n < m-1$ and $f(t) = t^m - a_0 \in K[t;\sigma]$, $a_0 \in K \setminus F$.*
(i) For all $k \in K^\times$ with $N_{K/F}(k)$ an mth root of unity and

$$\tau(a_0) = \Big(\prod_{l=0}^{m-1} \sigma^l(k)\Big) a_0,$$

the maps $H_{\tau,k}$ are automorphisms of S_f.
(ii) For all $g(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in K[t;\sigma]$ with $a_0 \in K \setminus F$,

$$\{H \in \mathrm{Aut}_F(S_g) \,|\, H = H_{\tau,k}\} \text{ is a subgroup of } \{H \in \mathrm{Aut}_F(S_f) \,|\, H = H_{\tau,k}\}.$$

For $m = n$ and K/F a cyclic field extension, the algebras considered in Corollary 13 are called *nonassociative cyclic algebras of degree m*, as they can be seen as canonical generalizations of associative cyclic algebras. These algebras are treated in Section 6.

4. Automorphisms extending id_K when K/F is a cyclic field extension

Let

$$f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in K[t;\sigma]$$

not be invariant.

In general, we know that if S_f has nucleus K then every inner automorphism G_c with $c \in K^\times$, extends id_K. Conversely, an extension $H_{id,k}$ of id_K is inner for the right choice of k:

Lemma 15. *Let $k = c^{-1}\sigma(c)$ with $c \in K^\times$, then $H_{id,k} \in \mathrm{Aut}_F(S_f)$ is an inner automorphism.*

Proof. A simple calculation shows that

$$G_c\Big(\sum_{i=0}^{m-1} x_i t^i\Big) = \Big(c^{-1}\sum_{i=0}^{m-1} x_i t^i\Big)c = x_0 + \sum_{i=1}^{m-1} x_i c^{-1}\sigma^i(c) t^i = H_{id,k}\Big(\sum_{i=0}^{m-1} x_i t^i\Big).$$

□

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

$$N_{K/F} : K \to F, \quad N_{K/F}(k) = k\sigma(k)\sigma^2(k)\cdots\sigma^{n-1}(k).$$

By Hilbert's Theorem 90,

$$\ker(N_{K/F}) = \Delta^\sigma(1),$$

where

$$\Delta^\sigma(l) = \{\sigma(c) l c^{-1} \,|\, c \in K^\times\}$$

is the σ-conjugacy class of $l \in K^\times$ [15].

Theorem 16. *(i) Every automorphism $H_{id,k} \in \mathrm{Aut}_F(S_f)$ such that $N_{K/F}(k) = 1$ is an inner automorphism.*
(ii) If

$$n \geq m - 1 \text{ and } a_{m-1} \neq 0$$

or if

$$n = m, \quad a_i = 0 \text{ for all } i \neq 0 \text{ and } a_0 \in K \setminus F$$

these are all the automorphisms extending id_K.

Proof. (i) Suppose there is $H_{id,k} \in \mathrm{Aut}_F(S_f)$ with $N_{K/F}(k) = 1$, then by Hilbert 90, there exists $c \in K^\times$ such that $k = c^{-1}\sigma(c)$. Thus $H_{id,k} = H_{id,c^{-1}\sigma(c)}$ for $c \in K^\times$ and so $G_c = H_{id,k}$ by Lemma 15.
(ii) By Theorem 4 and Proposition 10 (i), these are all the automorphisms extending id_K when $n \geq m-1$ if $a_{m-1} \neq 0$. The remaining assertion is proved analogoulsy. □

5. Cyclic subgroups of $\mathrm{Aut}_F(S_f)$

For any Galois field extension K/F and $\sigma \in \mathrm{Gal}(K/F)$ of order n, we now give some conditions for $\mathrm{Aut}_F(S_f)$ to have cyclic subgroups.

Theorem 17. *Suppose F contains an sth root of unity ω. Suppose that either*

$$f(t) = t^s - a \in K[t;\sigma]$$

where $a \in K \setminus F$, or

$$f(t) = t^{sl} - \sum_{i=0}^{l-1} a_{is} t^{is} \in K[t;\sigma]$$

such that S_f is not associative. Then $\langle H_{id,\omega}\rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(S_f)$ of order at most s and of order s, if ω is a primitive root of unity.

Proof. (i) Let $f(t) = t^s - a$. Then $\omega^j\sigma(\omega^j)\cdots\sigma^{s-1}(\omega^j) = \omega^{js} = 1$ and so $H_{id,\omega^j} \in \mathrm{Aut}_F(S_f)$ for all $0 \leq j \leq s-1$ by Proposition 7.
(ii) Let $f(t) = t^{sl} - \sum_{i=0}^{l-1} a_{is}t^{is}$. Then we have

$$\prod_{q=is}^{ls-1} \sigma^q(\omega^j) = \omega^{j(ls-is)} = 1$$

for all $i = 0, \ldots, l-1$. Hence

$$a_{is} = \Big(\prod_{q=is}^{ls-1} \sigma^q(\omega^j)\Big) a_{is}$$

for all $i = 0, \ldots, l-1$ and so $H_{id,\omega^j} \in \mathrm{Aut}_F(S_f)$ for all $0 \leq j \leq s-1$ by Proposition 7.
In both (i) and (ii), $\langle H_{id,\omega}\rangle$ is a cyclic subgroup of $\mathrm{Aut}(S_f)$ of order less or equal to s, since

$$H_{id,\omega^j} \circ H_{id,\omega^r} = H_{id,\omega^{j+r}}$$

for all $0 \leq j, r \leq sl-1$. □

Lemma 18. *Let F have characteristic not two, m be even and*

$$f(t) = t^m - \sum_{i=0}^{(m-2)/2} a_{2i}t^{2i} \in K[t;\sigma]$$

not invariant. Then $\{H_{id,1}, H_{id,-1}\}$ is a subgroup of S_f of order 2.

Proof. The maps $H_{id,1}$ and $H_{id,-1}$ are automorphisms of S_f by Proposition 7, and $H_{id,-1} \circ H_{id,-1} = H_{id,1}$. □

If $f \in F[t] \subset K[t;\sigma]$, we obtain:

Theorem 19. *Suppose σ commutes with all $\tau \in \mathrm{Gal}(K/F)$, and*

$$f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in F[t;\sigma] \subset K[t;\sigma]$$

is not invariant.
(i) $\langle H_{\sigma,1}\rangle \cong \mathbb{Z}/n\mathbb{Z}$ is a cyclic subgroup of $\mathrm{Aut}_F(S_f)$.
(ii) Suppose $\mathrm{Gal}(K/F) = \langle\sigma\rangle$, $n = m$ is prime, $a_0 \neq 0$ and not all of $a_1, \dots, a_{m-1}$ are zero. Then

$$\mathrm{Aut}_F(S_f) = \langle H_{\sigma,1}\rangle \cong \mathbb{Z}/m\mathbb{Z}.$$

Proof. Let $j \in \{0, \dots, n-1\}$. Since $\tau(a_i) = a_i$ for all i, here Equation (1) becomes

$$a_i = \Big(\prod_{q=i}^{m-1} \sigma^q(k)\Big) a_i \tag{10}$$

for all $i \in \{0, \dots, m-1\}$.
(i) Clearly, (10) is satisfied for $k = 1$ and all $i \in \{0, \dots, m-1\}$, therefore the maps $H_{\tau,1}$ are automorphisms of S_f for all $\tau \in \mathrm{Gal}(K/F)$ by Theorems 4 and 5. We have $H_{\sigma^j,1} \circ H_{\sigma^l,1} = H_{\sigma^{j+l},1}$ and $H_{\sigma^n,1} = H_{id,1}$. Hence $\langle H_{\sigma,1}\rangle = \big\{H_{id,1}, H_{\sigma,1}, \dots, H_{\sigma^{m-1},1}\big\}$ is a cyclic subgroup of order n.
(ii) By Theorem 4, the automorphisms of S_f are exactly the maps $H_{\sigma^j,k}$ where $j \in \{0, \dots, n-1\}$ and $k \in K^\times$ satisfies (10) for all $i \in \{0, \dots, m-1\}$. The maps $H_{\sigma^j,1}$ are therefore automorphisms of S_f for all $j \in \{0, \dots, n-1\}$. We prove that these are the only automorphisms of S_f: $a_0 \neq 0$ and so $N_{K/F}(k) = 1$ by (10). Therefore, by Hilbert 90, there exists $\alpha \in K$ such that $k = \sigma(\alpha)/\alpha$. Let $l \in \{1, \dots, m-1\}$ be such that $a_l \neq 0$. Then by (10),

$$1 = \prod_{q=l}^{m-1} \sigma^q(k) = \prod_{q=l}^{m-1} \sigma^q\big(\frac{\sigma(\alpha)}{\alpha}\big) = \frac{\prod_{q=l+1}^{m} \sigma^q(\alpha)}{\prod_{q=l}^{m-1} \sigma^q(\alpha)} = \frac{\alpha}{\sigma^l(\alpha)}.$$

Thus $\alpha \in \mathrm{Fix}(\sigma^j) = F$ since m is prime. Therefore

$$k = \frac{\sigma(\alpha)}{\alpha} = \frac{\alpha}{\alpha} = 1$$

as required. □

This complements our results from Theorem 11, which in case $\mathrm{Gal}(K/F)$ is cyclic of degree n mean the following:

Corollary 20. *Suppose $\mathrm{Gal}(K/F)$ is cyclic of degree n and $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in F[t;\sigma]$ not invariant with $a_{m-1} \in F^\times$.*
(i) Let $n \geq m-1$ then for all $\tau \in \mathrm{Gal}(K/F)$ the maps $H_{\tau,1}$ are exactly the automorphisms of S_f and

$$\mathrm{Aut}_F(S_f) \cong \mathrm{Gal}(K/F) \cong \mathbb{Z}/n\mathbb{Z}.$$

(ii) Let $n < m-1$ then for all $\tau \in \mathrm{Gal}(K/F)$ the maps $H_{\tau,1}$ are automorphisms of S_f and $\mathrm{Gal}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$ is isomorphic to a subgroup of $\mathrm{Aut}_F(S_f)$.

6. Nonassociative cyclic algebras

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

$$(K/F, \sigma, a) = K[t;\sigma]/K[t;\sigma](t^m - a)$$

is called a *nonassociative cyclic algebra of degree* m over F. It is not associative for all $a \in K \setminus F$ and a cyclic associative central simple algebra over F for $a \in F^\times$. We will only consider the case that $a \in K \setminus F$. If

$$1, a, a^2, \ldots, a^{m-1}$$

are linearly independent over F then $(K/F, \sigma, a)$ is a division algebra (cf. [28], [26] for finite F). In particular, if K/F is of prime degree then $(K/F, \sigma, a)$ is a division algebra for every $a \in K \setminus F$.

Theorem 21. *Let $A = (K/F, \sigma, a)$ be a nonassociative cyclic algebra of degree m.*
(i) All the automorphisms of A which extend id_K are inner automorphisms and of the form $H_{id,l}$ for all $l \in K^\times$ such that $N_{K/F}(l) = 1$.
The subgroup they generate in $\mathrm{Aut}_F(A)$ is isomorphic to $\ker(N_{K/F})$.
(ii) An automorphism $\sigma^j \neq id$ can be extended to $H \in \mathrm{Aut}_F(A)$, if and only if there is some $l \in K$ such that

$$\sigma^j(a) = N_{K/F}(l)a.$$

In that case, $H = H_{\sigma^j,l}$ and if m is prime then $N_{K/F}(l) = \omega$ for an mth root of unity $1 \neq \omega \in F$.
(iii) Let $c \in K \setminus F$ and suppose there exists $r \in \mathbb{N}$ such that $c^r \in F^\times$. Let r be minimal. Then $\langle G_c\rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(S_f)$ of order r.

Proof. Theorem 4, Theorem 16 (ii), and Proposition 10 imply (i) and (ii).
(iii) Let $c \in K \setminus F$. Then G_c is an automorphism, because K is the nucleus of A. Since $G_c \circ G_c = G_{c^2}$, $G_c \circ G_c \circ G_c = G_{c^3}$ and so on, we have $G_{c^r} = id$ if and only if $c^r \in F$. If $r \in \mathbb{N}$ is smallest possible then $\langle G_c\rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(S_f)$ of order r. □

Note that different roots of unity yield different l in Theorem 21 (ii). This yields:

Theorem 22. *Let $A = (K/F, \sigma, a)$ be a nonassociative cyclic algebra of degree m. Suppose F contains a non-trivial mth root of unity ω.*
(i) $\langle H_{id,\omega}\rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(A)$ of order at most m. If ω is a primitive mth root of unity, then $\langle H_{id,\omega}\rangle$ has order m.
(ii) If there is an element $l \in K$, such that $N_{K/F}(l) = \omega$ for ω a primitive mth root of unity and $\sigma(d) = \omega d$, then the subgroup generated by $H_{\sigma,l}$ has order m^2.

Proof. (i) follows from Theorem 17.
(ii) Suppose σ can be extended to an F-automorphism H of A. Then by Theorem 21, there is an element $l \in K$, such that $N_{K/F}(l) = \omega$, $\omega \neq 1$ and $\sigma(d) = \omega d$, and $H = H_{\sigma,l}$. (If $1 = N_{K/F}(l)$, then $\sigma(d) = d$, contradiction.)

The subgroup generated by $H = H_{\sigma,l}$ has order greater than m, since $H_{\sigma,l} \circ \cdots \circ H_{\sigma,l}$ (m-times) becomes $H_{\sigma^m,b} = H_{id,\omega}$ with $\omega = N_{K/F}(l)$. $H_{id,\omega}$ has order m, so the subgroup generated by $H = H_{\sigma,l}$ has order m^2. □

6.2. The case that m is prime. Let us now assume that the cyclic field extension K/F has prime degree $m = \deg(f)$. Suppose that F contains a primitive mth root of unity, where m is prime to the characteristic of F. Then

$$K = F(d)$$

where d is a root of an irreducible polynomial $t^m - c \in F[t]$.

Lemma 23. *(cf. [29, Lemma 6.2.7]) The eigenvalues of $\sigma^j \in \mathrm{Gal}(K/F)$ are precisely the mth roots of unity. Moreover, the only possible eigenvectors are of the form ed^i for some i, $0 \leq i \leq m-1$ and some $e \in F$.*

Let

$$f(t) = t^m - a \in K[t;\sigma], \quad a \notin F.$$

Then we get the following strong restriction for automorphisms of S_f:

Theorem 24. *H is an automorphism of S_f extending $\sigma^j \neq id$ if and only if $H = H_{\sigma^j,k}$ for some $k \in K^\times$, where $N_{K/F}(k)$ is an mth root of unity and $a = ed^s$ for some $e \in F^\times$ and some d^s.*

Proof. H is an automorphism of S_f if and only if $H = H_{\sigma^j,k}$ where $j \in \{0, \dots, m-1\}$ and $k \in K^\times$ is such that

$$\sigma^j(a) = \Big(\prod_{l=0}^{m-1} \sigma^l(k)\Big) a = N_{K/F}(k) a.$$

For all $\sigma^j \neq id$, by Lemma 23 this condition is equivalent to $N_{K/F}(k)$ being an mth root of unity and $a = ed^s$ for some d^s and $e \in F^\times$, for all $k \in K^\times$. □

6.3. For a nonassociative cyclic algebra $A = (K/F, \sigma, a)$ of degree m we can now summarize our previous results:
(i) For each root of unity $\omega \in F$, such that there is $l \in K$ with $N_{K/F}(l) = \omega$ and a $j \in \{1, \dots, m-1\}$ such that $\sigma^j(a) = \omega a$, there is an automorphism $H_{\sigma^j,l}$ extending σ^j.
(ii) Suppose one of the following holds:

- F has no mth root of unity (e.g. $F = \mathbb{Q}$ and m odd).
- m is prime and F contains a primitive mth root of unity, where m is prime to the characteristic of F. Let $K = F(d)$ as in Section 6.2 and $a \neq ed^i$, $e \in F^\times$.

Then every F-automorphism of A leaves K fixed, is inner and

$$\mathrm{Aut}_F(A) \cong \ker(N_{K/F}).$$

Applying Theorem 8, these results now yield the following for more general algebras S_f:

Corollary 25. *Suppose* $\mathrm{Gal}(K/F) = \langle \sigma \rangle$ *is cyclic of degree m and $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in K[t;\sigma]$ is not invariant with $a_0 \in K \setminus F$. Suppose one of the following holds:*

- *F has no mth root of unity.*

- *m is prime and F contains a primitive mth root of unity, where m is prime to the characteristic of F. Let $K = F(d)$ as in Section 6.2 and $a_0 \neq ed^i$, $e \in F^\times$.*

Then every F-automorphism of S_f leaves K fixed, is inner and $\mathrm{Aut}_F(S_f)$ is a subgroup of $\ker(N_{K/F})$, thus cyclic. In particular, if $\ker(N_{K/F})$ has prime order, then either $\mathrm{Aut}_F(S_f)$ is trivial or $\mathrm{Aut}_F(S_f) \cong \ker(N_{K/F})$.

6.4. The automorphism groups of nonassociative quaternion algebras. Recall the *dicyclic group*

$$\mathrm{Dic}_l = \langle x, y \mid y^{2l} = 1,\ x^2 = y^l,\ x^{-1}yx = y^{-1} \rangle \tag{11}$$

of order $4l$. The semidirect product $\mathbb{Z}/s\mathbb{Z} \rtimes_l \mathbb{Z}/n\mathbb{Z}$ between the cyclic groups $\mathbb{Z}/s\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ corresponds to a choice of an integer l such that $l^n \equiv 1 \mod s$. It can be described by the presentation

$$\mathbb{Z}/s\mathbb{Z} \rtimes_l \mathbb{Z}/n\mathbb{Z} = \langle x, y \mid x^s = 1,\ y^n = 1,\ yxy^{-1} = x^l \rangle. \tag{12}$$

We obtain the following result for the automorphism groups of nonassociative quaternion algebras (where $m = 2$):

Theorem 26. *Suppose $K = F(\sqrt{b})$ is a quadratic field extension of F, char$(F) \neq 2$, and consider the nonassociative quaternion algebra $A = (K/F, \sigma, \lambda\sqrt{b})$ for some $\lambda \in F^\times$. Suppose there exists $k \in K^\times$ such that $k\sigma(k) = -1$.*

For every $c \in K \setminus F$ for which there is a positive integer j such that $c^j \in F^\times$, pick the smallest such j.
(i) If j is even then $\mathrm{Aut}_F(S_f)$ contains the dicyclic group of order $2j$.
(ii) If j is odd then $\mathrm{Aut}_F(S_f)$ contains a subgroup isomorphic to the semidirect product

$$\mathbb{Z}/j\mathbb{Z} \rtimes_{j-1} \mathbb{Z}/4\mathbb{Z}.$$

In particular, $\mathrm{Aut}_F(A)$ always contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

Proof. Since $\sigma(\sqrt{b}) = -\sqrt{b}$ and $k\sigma(k) = -1$, $H_{\sigma,k} \in \mathrm{Aut}_F(S_f)$ by Theorem 21. A simple calculation shows that

$$\langle H_{\sigma,k} \rangle = \{H_{\sigma,k}, H_{id,-1}, H_{\sigma,-k}, H_{id,1}\}.$$

$\langle G_c \rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(S_f)$ of order j by Theorem 21 (iii).
(i) Suppose j is even and write $j = 2l$. We prove first that $G_{c^l} = H_{id,-1}$. Write $c^l = \mu_0 + \mu_1\sqrt{b}$ for some $\mu_0, \mu_1 \in F$. Then

$$c^j = c^{2l} = \mu_0^2 + \mu_1^2 b + 2\mu_0\mu_1\sqrt{b} \in F$$

which implies $2\mu_0\mu_1 = 0$. Hence $\mu_0 = 0$ or $\mu_1 = 0$. Since j is minimal, $c^l \notin F$ so $\mu_0 = 0$ and $c^l = \mu_1\sqrt{b}$. We have

$$\begin{aligned} G_{c^l}(x_0 + x_1 t) &= x_0 + x_1(\mu_1\sqrt{b})^{-1}\sigma(\mu_1\sqrt{b})t \\ &= x_0 + x_1\mu_1^{-1}b^{-1}\sqrt{b}(-\mu_1\sqrt{b})t \\ &= x_0 - x_1 t = H_{id,-1}(x_0 + x_1 t) \end{aligned}$$

which implies $G_{c^l} = H_{id,-1}$. Next we prove $(H_{\sigma,k})^{-1}G_cH_{\sigma,k} = G_c^{-1}$. Simple calculations show $(H_{\sigma,k})^{-1} = H_{\sigma,-k}$ and $G_c^{-1} = G_{\sigma(c)}$. We have

$$\begin{aligned} H_{\sigma,-k}\big(G_c\big(H_{\sigma,k}\big(x_0 + x_1 t\big)\big)\big) &= H_{\sigma,-k}\big(G_c\big(\sigma(x_0) + \sigma(x_1)kt\big)\big) \\ &= H_{\sigma,-k}\big(\sigma(x_0) + \sigma(x_1)kc^{-1}\sigma(c)t\big) \\ &= x_0 - x_1\sigma(k)\sigma(c^{-1})ckt \\ &= x_0 + x_1\sigma(c^{-1})ct = G_{\sigma(c)}\big(x_0 + x_1 t\big) \end{aligned}$$

and so $(H_{\sigma,k})^{-1}G_cH_{\sigma,k} = G_c^{-1}$.

Thus $H_{\sigma,k}^2 = H_{id,-1} = G_{c^l} = G_c^l$, $G_c^{2l} = id$ and $(H_{\sigma,k})^{-1}G_cH_{\sigma,k} = G_c^{-1}$. Hence $\langle H_{\sigma,k}, G_c\rangle$ has the presentation (11) as required.

(ii) Suppose j is odd. Then $\langle G_c\rangle$ does not contain $H_{id,-1}$ as $H_{id,-1}$ has order 2 which implies $\langle H_{\sigma,k}\rangle \cap \langle G_c\rangle = \{id\}$. Furthermore $(H_{\sigma,k})^{-1}G_cH_{\sigma,k} = G_c^{-1} = G_c^{j-1} = G_{c^{j-1}}$ can be shown similarly as in (i). Notice

$$(j-1)^4 = j^4 - 4j^3 + 6j^2 - 4j + 1 \equiv 1 \bmod (j).$$

Thus $\mathrm{Aut}_F(S_f)$ contains the subgroup

$$\langle G_c\rangle \rtimes_{j-1} \langle H_{\sigma,k}\rangle \cong \mathbb{Z}/j\mathbb{Z} \rtimes_{j-1} \mathbb{Z}/4\mathbb{Z}$$

as required.

In particular, choose $c = \sqrt{b}$ in (i), so that $j = 2$. This implies $\mathrm{Aut}_F(A)$ contains the dicyclic group of order 4, which is the cyclic group of order 4. □

Example 27. (i) Let $F = \mathbb{Q}(i)$, $K = F(\sqrt{-3})$, $\sigma(\sqrt{-3}) = -\sqrt{-3}$ and $A = (K/F, \sigma, \lambda\sqrt{-3})$ be a nonassociative quaternion algebra with some $\lambda \in F^\times$. Note that for $k = i$ we have $i\sigma(i) = -1$. Let $c = 1 + \sqrt{-3}$. Then

$$c^2 = -2 + 2\sqrt{-3} \text{ and } c^3 = -8$$

which implies $j = 3$ here. Therefore $\mathrm{Aut}_F(S_f)$ contains a subgroup isomorphic to the semidirect product

$$\mathbb{Z}/3\mathbb{Z} \rtimes_2 \mathbb{Z}/4\mathbb{Z}$$

by Theorem 26.

(ii) Let $F = \mathbb{Q}(i)$, $K = F(\sqrt{-1/12})$, $\sigma(\sqrt{-1/12}) = -\sqrt{-1/12}$ and $A = (K/F, \sigma, \lambda\sqrt{-1/12})$ be a nonassociative quaternion algebra for some $\lambda \in F^\times$. Again for $k = i$ we have $i\sigma(i) = -1$. Let $c = 1 + 2\sqrt{-1/12}$. Then

$$c^2 = \frac{2}{3} + \frac{2i}{\sqrt{3}},\ c^3 = \frac{8i}{3\sqrt{3}},\ c^4 = \frac{-8}{9} + \frac{8i}{3\sqrt{3}},\ c^5 = \frac{-16}{9} + \frac{16i}{9\sqrt{3}} \text{ and } c^6 = \frac{-64}{27}.$$

Hence $c, c^2, c^3, c^4, c^5 \in K \setminus F$ and $c^6 \in F$. Therefore $\mathrm{Aut}_F(A)$ contains the dicyclic group of order 12 by Theorem 26.

7. Isomorphisms between S_f and S_g

The proofs of the previous sections can be adapted to check when two Petit algebras are isomorphic and when not. This is not the main focus of this paper so we just point out how some of the results can be transferred.

If K and L are fields, and

$$S_f = K[t;\sigma]/K[t;\sigma]f(t) \cong L[t;\sigma']/L[t;\sigma']g(t) = S_g,$$

then

$$K \cong L, \quad Nuc_r(S_f) \cong Nuc_r(S_g), \quad \deg(f) = \deg(g),$$

and

$$\mathrm{Fix}(\sigma) \cong \mathrm{Fix}(\sigma'),$$

since isomorphic algebras have the same dimensions, and isomorphic nuclei and center.

If G is an automorphism of $R = K[t;\sigma]$ which restricts to an automorphism τ on K which commutes with σ, $f \in R$ is irreducible and $g(t) = G(f(t))$, then G induces an isomorphism $S_f \cong S_{G(g)}$ [16, Theorem 7] (the proof works for any base field).

From now on let F be the fixed field of σ, σ have order n, and

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

be not invariant. Then the following is proved analogously to Theorem 4, Theorem 5 and Proposition 7:

Theorem 28. *Suppose σ commutes with all $\tau \in \mathrm{Aut}_F(K)$ and $n \geq m-1$. Then $S_f \cong S_g$ if and only if there exists $\tau \in \mathrm{Aut}_F(K)$ and $k \in K^\times$ such that*

$$\tau(a_i) = \Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big) b_i \tag{13}$$

for all $i \in \{0, \dots, m-1\}$. Every such τ and k yield a unique isomorphism $G_{\tau,k} : S_f \to S_g$,

$$G_{\tau,k}\Big(\sum_{i=0}^{m-1} x_i t^i\Big) = \tau(x_0) + \sum_{i=1}^{m-1} \tau(x_i) \prod_{l=0}^{i-1} \sigma^l(k) t^i.$$

If $n < m-1$ we still get a partial result:

Theorem 29. *Suppose there exists $\tau \in \mathrm{Aut}_F(K)$ and $k \in K^\times$ such that $\tau \circ \sigma = \sigma \circ \tau$ and*

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

for all $i \in \{0, \dots, m-1\}$, then $S_f \cong S_g$ with an isomorphism given by

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

as in Theorem 28.

Corollary 30. *For every $k \in K^\times$ such that*

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

for all $i \in \{0, \dots, m-1\}$, $G_{id,k} : S_f \to S_g$ is an isomorphism.

As a direct consequence of Theorem 28 we obtain:

Theorem 31. *Suppose σ commutes with all $\tau \in \mathrm{Aut}_F(K)$ and $n \geq m-1$. If $S_f \cong S_g$, then $a_i = 0$ if and only if $b_i = 0$, for all $i \in \{0, \dots, m-1\}$.*

Proof. If $S_f \cong S_g$ then by Theorem 28, there exists $j \in \{0, \dots, n-1\}$ and $k \in K^\times$ such that $\tau(a_i) = \Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big) b_i$ for all $i \in \{0, \dots, m-1\}$. This implies $a_i = 0$ if and only if $b_i = 0$, for all $i \in \{0, \dots, m-1\}$. □

From now on we restrict ourselves to the situation that $R = K[t;\sigma]$ and $F = \mathrm{Fix}(\sigma)$, where K/F is a finite Galois field extension and σ of order n. We take a closer look at the consequences of Equation (13):

Proposition 32. *Let $k \in K^\times$ such that*

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

for all $i \in \{0, \dots, m-1\}$. Then $a_i = 0$ if and only if $b_i = 0$ and:
(i) For all $i \in \{0, \dots, m-1\}$ with $a_i \neq 0$,

$$N_{K/F}(a_i) = N_{K/F}(k)^{m-i} N_{K/F}(b_i).$$

(ii) If there is some $i \in \{0, \dots, m-1\}$ such that $a_i \in \mathrm{Fix}(\tau)^\times$, then

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

In particular, if $a_{m-1} \in F^\times$ and $b_{m-1} \in F^\times$, then $k \in F^\times$ and $a_i = k^{m-i} b_i$ for all $i \in \{0, \dots, m-1\}$.
(iii) If $a_0 \in \mathrm{Fix}(\tau)^\times$, $m = n$ and $\mathrm{Gal}(K/F) = \langle \sigma \rangle$ then

$$a_0 = N_{K/F}(k) b_0.$$

Proof. (i) Equation (13) implies that

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

(apply $N_{K/F}$ to both sides), therefore

$$N_{K/F}(a_i) = N_{K/F}(k)^{m-i} N_{K/F}(b_i)$$

for all $i \in \{0, \dots, m-1\}$ is a necessary condition on k.
(ii) If there is an $i \in \{0, \dots, m-1\}$ such that $a_i \in \mathrm{Fix}(\tau)^\times$, then Equation (13) implies that $a_i = \Big(\prod_{l=i}^{m-1} \sigma^l(k)\Big) b_i$, so that we obtain

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

Alternatively, if $a_{m-1} \in F^\times$ and $b_{m-1} \in F^\times$, then $a_{m-1} = \sigma^{m-1}(k) b_{m-1}$ imply $k \in F^\times$, hence $a_i = k^{m-1-i} b_i$ for all $i \in \{0, \dots, m-1\}$.
(iii) In particular, if $a_0 \in \mathrm{Fix}(\tau)^\times$, $m = n$ and σ generates $\mathrm{Gal}(K/F)$, then $a_0/b_0 = \prod_{l=0}^{m-1} \sigma^l(k) = N_{K/F}(k)$ is a necessary condition on k. □

Corollary 33. *Suppose σ commutes with all $\tau \in \mathrm{Gal}(K/F)$ and $n \geq m-1$. Assume that one of the following holds:*
(i) There exists $i \in \{0, \dots, m-1\}$ such that $b_i \neq 0$ and

$$N_{K/F}(a_i b_i^{-1}) \notin N_{K/F}(K^\times)^{m-i};$$

(ii) $m = n$, $a_0 \in F^\times$ and $b_0 \in K \setminus F$.
Then $S_f \not\cong S_g$.

Corollary 34. *Suppose $\mathrm{Gal}(K/F) = \langle \sigma \rangle$ and $n = m$. Let $f(t) = t^m - a$, $g(t) = t^m - b \in K[t;\sigma]$ where $a, b \in K \setminus F$.*
(i) $S_f \cong S_g$ if and only if there exists $\tau \in \mathrm{Gal}(K/F)$ and $k \in K^\times$ such that

$$\tau(a) = N_{K/F}(k) b.$$

(ii) If

$$\sigma^j(a) \neq N_{K/F}(k) b$$

for all $k \in K^\times$, $j = 0, \dots, m-1$, then $S_f \not\cong S_g$.

These follow from Proposition 32. Note that Corollary 34 canonically generalizes well-known criteria for associative cyclic algebras.

References

[1] A. S. Amitsur, *Differential polynomials and division algebras.* Annals of Mathematics, Vol. 59 (2) (1954) 245-278.

[2] A. S. Amitsur, *Non-commutative cyclic fields.* Duke Math. J. 21 (1954), 87105.

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

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

[5] C. Brown, S. Pumplün, A. Steele, *Automorphisms and isomorphisms of Jha-Johnson semifields obtained from skew polynomial rings.* Preprint, 2016.

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

[7] 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.

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

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

[10] 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.

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

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

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

[14] K. Kishimoto, *On cyclic extensions of simple rings.* J. Fac. Sci. Hokkaido Univ. Ser. I 19 (1966), 74-85.

[15] T. Y. Lam, A. Leroy, *Hilbert 90 theorems over division rings.* Trans. Amer. Math. Soc. 345 (2) (1994), 595-622.

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

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

[18] 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.

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

[20] S. Pumplün, *Quotients of orders in algebras obtained from skew polynomials and possible applications.* Online at arXiv:1609.04201 [math.RA]

[21] S. Pumplün, *Finite nonassociative algebras obtained from skew polynomials and possible applications to* (f, σ, δ)*-codes.* To appear in Advances in Mathematics of Communications. Online at arXiv:1507.01491[cs.IT]

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

[23] 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.

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

[25] 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.

[26] R. Sandler, *Autotopism groups of some finite non-associative algebras.* Amer. J. Math. 84 (1962), 239-264.

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

[28] A. Steele, *Nonassociative cyclic algebras.* Israel Journal of Mathematics 200 (1) (2014), 361-387.

[29] A. Steele, *Some new classes of division algebras and potential applications to space-time block coding.* PhD Thesis, University of Nottingham 2013, online at eprints.nottingham.ac.uk/13934/

[30] G. P. Wene, *Inner automorphisms of semifields.* Note Mat. 29 (2009), suppl. 1, 231-242.

[31] G. P. Wene, *Finite semifields three-dimensional over the left nuclei.* Nonassociative algebra and its applications (Sao Paulo, 1998), Lecture Notes in Pure and Appl. Math., 211, Dekker, New York, 2000, 447-456.

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

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