AUTOMORPHISMS AND ISOMORPHISMS OF JHA-JOHNSON SEMIFIELDS OBTAINED FROM SKEW POLYNOMIAL RINGS

C. BROWN, S. PUMPLÜN, AND A. STEELE

Abstract. We study the automorphisms of Jha-Johnson semifields obtained from a right invariant irreducible twisted polynomial $f \in K[t;\sigma]$, where $K = \mathbb{F}_{q^n}$ is a finite field and σ an automorphism of K of order n, with a particular emphasis on inner automorphisms and the automorphisms of Sandler and Hughes-Kleinfeld semifields. We include the automorphisms of some Knuth semifields (which do not arise from skew polynomial rings).

Isomorphism between Jha-Johnson semifields are considered as well.

Introduction

Semifields are finite unital nonassociative division algebras. Since two semifields coordinatize the same non-Desarguesian projective plane if and only if they are isotopic, semifields are usually classified up to isotopy rather than up to isomorphism and consequently, usually only their autotopism group is computed.

Among the semifields with known automorphism groups are the three-dimensional semifields over a field of characteristic not 2 (Dickson [13] and Menichetti [24, 25]), and the semifields with 16 elements (Kleinfeld [19] and Knuth [21]). Burmester [10] investigated the automorphisms of Dickson commutative semifields of order $p^{2n}, p \neq 2$, and Zemmer [37] proved the existence of commutative semifields with a cyclic automorphism group of order $2n$. More recent results can be found for instance in [1, 2, 3, 4, 5, 6, 8, 9].

Jha-Johnson semifields (also called *cyclic semifields* in [14]) were introduced in [18] and are generalizations of both Sandler and Hugh-Kleinfeld semifields. With the exception of one subcase, the autotopism groups of all Jha-Johnson semifields were computed by Dempwolff using representation theory [14]. One of our motivations for computing the automorphism groups of a certain family of Jha-Johnson semifields is a question by C. H. Hering [16]: Given a finite group G, does there exist a semifield such that G is a subgroup of its automorphism group? Another incentive arose from the search for classes of finite loops with non-trivial automorphism groups. Examples can be now obtained as the multiplicative loops of Jha-Johnson semifields [29].

We will compute the automorphism groups using noncommutative polynomials: Let K be a field, σ an automorphism of K with fixed field F, $R = K[t;\sigma]$ a twisted polynomial ring and $f \in R$. In 1967, Petit [27, 28] studied a class of unital nonassociative algebras S_f obtained by employing a right invariant irreducible $f \in R = K[t;\sigma]$.

1991 *Mathematics Subject Classification.* Primary: 12K10; Secondary: 17A35, 17A60, 16S36, 17A36.

Key words and phrases. Skew polynomials, automorphisms, automorphism group, Jha-Johnson semifields, cyclic semifields.

Every finite nonassociative Petit algebra is a *Jha-Johnson semifield*. These algebras were studied by Wene [36] and more recently, Lavrauw and Sheekey [23].

While each Jha-Johnson semifield is isotopic to some such algebra S_f it is not necessarily itself isomorphic to an algebra S_f. We will focus on those Jha-Johnson semifields which are, and apply the results from [12] to investigate their automorphisms.

The structure of the paper is as follows: In Section 1, we introduce the basic terminology and define the algebras S_f. Given a finite field $K = \mathbb{F}_{q^n}$, an automorphism σ of K of order n with $F = \mathrm{Fix}(\sigma) = \mathbb{F}_q$ and an irreducible polynomial $f \in K[t;\sigma]$ of degree m that is not right invariant (i.e., where $K[t;\sigma]f$ is not a two-sided ideal), we know the automorphisms of the Jha-Johnson semifields S_f if $n \geq m-1$ and a subgroup of them if $n < m-1$ [12, Theorems 4, 5]. The automorphism groups of *Sandler semifields* [30] (obtained by choosing $n \geq m$ and $f(t) = t^m - a \in K[t;\sigma]$, $a \in K \setminus F$) are particularly relevant: for all Jha-Johnson semifields 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 $\mathrm{Aut}_F(S_f)$ (Theorem 2). We summarize results on the automorphism groups, and give examples when it is trivial and when $\mathrm{Aut}_F(S_f) \cong \mathbb{Z}/n\mathbb{Z}$ (Theorem 4). Inner automorphisms of Jha-Johnson semifields are considered in Section 2. In Section 3 we consider the special case that $n = m$ and $f(t) = t^m - a$. In this case, the algebras S_f are Sandler semifields and also called *nonassociative cyclic algebras* $(K/F, \sigma, a)$. The automorphisms of $A = (K/F, \sigma, a)$ extending id are inner and form a cyclic group isomorphic to $\ker(N_{K/F})$. We show when $\mathrm{Aut}_F(A) \cong \ker(N_{K/F})$ and hence consists only of inner automorphisms, when $\mathrm{Aut}_F(A)$ contains or equals the dicyclic group Dic_r of order $4r = 2q+2$, or when $\mathrm{Aut}_F(A) \cong \mathbb{Z}/(s/m)\mathbb{Z} \rtimes_q \mathbb{Z}/(m^2)\mathbb{Z}$ contains or equals a semidirect product, where $s = (q^m-1)/(q-1)$, $m > 2$ (Theorems 19 and 20). We compute the automorphisms for the Hughes-Kleinfeld and most of the Knuth semifields in Section 4. Not all Knuth semifields are algebras S_f, however, the automorphisms behave similarly in all but one case. We compute the automorphism groups in some examples, improving results obtained by Wene [35]. In Section 5 we briefly investigate the isomorphisms between two semifields S_f and S_g. In particular, we classify nonassociative cyclic algebras of prime degree up to isomorphism.

Sections of this work are part of the first and last author's PhD theses [11, 33] written under the supervision of the second author.

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 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 without saying so explicitly.

The *associator* of A is given by $[x,y,z] = (xy)z - x(yz)$. The *left nucleus* of A is defined as $\mathbb{N}_l(A) = \{x \in A \mid [x,A,A] = 0\}$, the *middle nucleus* of A is $\mathbb{N}_m(A) = \{x \in A \mid [A,x,A] = 0\}$ and the *right nucleus* of A is $\mathbb{N}_r(A) = \{x \in A \mid [A,A,x] = 0\}$. $\mathbb{N}_l(A)$, $\mathbb{N}_m(A)$, and $\mathbb{N}_r(A)$ are associative subalgebras of A. Their intersection $\mathbb{N}(A) = \{x \in A \mid [x,A,A] = [A,x,A] = [A,A,x] = 0\}$ is the *nucleus* of A. $\mathbb{N}(A)$ is an associative subalgebra of A containing $F1$

and $x(yz) = (xy)z$ whenever one of the elements x, y, z lies in $\mathbb{N}(A)$. The *center* of A is $\mathrm{C}(A) = \{x \in A \mid x \in \mathrm{Nuc}(A) \text{ and } xy = yx \text{ for all } y \in A\}$.

An 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 [31, pp. 15, 16]. A *semifield* is a finite-dimensional unital division algebra over a finite field. A semifield is called *proper* if it is not associative. 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 $L_a(a_r) = aa_r = 1$. If $m_r = m_l$ then we denote this element by m^{-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 $G(x) = G_m(x) = (m_l x)m$ for all $x \in A$. The set of inner automorphisms $\{G_m \mid m \in \mathbb{N}(A) \text{ invertible}\}$ is a subgroup of $\mathrm{Aut}_F(A)$. Note that if the nucleus of A is central, then for all $0 \neq n \in \mathbb{N}(A)$, $G_n(x) = (n^{-1}x)n = n^{-1}xn$ is an inner automorphism of A such that $G_n|_{\mathbb{N}(A)} = id_{\mathbb{N}(A)}$.

1.2. **Semifields obtained from skew polynomial rings.** Let K be a field and σ an automorphism of K. The *twisted polynomial ring* $R = K[t;\sigma]$ 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 $a \in K$ [26]. For $f = a_0 + a_1 t + \cdots + a_m t^m$ with $a_m \neq 0$ define $\deg(f) = m$ 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 $g = qf + r$ [15]. From now on, we assume that

$$K = \mathbb{F}_{q^n}$$

is a finite field, $q = p^r$ for some prime p, σ an automorphism of K of order $n > 1$ and

$$F = \mathrm{Fix}(\sigma) = \mathbb{F}_q,$$

i.e. K/F is a cyclic Galois extension of degree n with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. The norm $N_{K/F} : K^\times \to F^\times$ is surjective, and $\ker(N_{K/F})$ is a cyclic group of order $s = (q^n - 1)/(q - 1)$.

Let $f \in R = K[t;\sigma]$ have degree m. Let $\mathrm{mod}_r f$ denote the remainder of right division by f. Then the additive abelian group $R_m = \{g \in K[t;\sigma] \mid \deg(g) < m\}$ together with the multiplication $g \circ h = gh \bmod_r f$ is a unital nonassociative algebra $S_f = (R_m, \circ)$ over F [27, (7)]. S_f is also denoted by R/Rf if we want to make clear which ring R is involved in the construction.

Note that 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 ${}_fS$. Every algebra ${}_fS$ is the opposite algebra of some Petit algebra [27, (1)].

In the following, we call the algebras S_f *Petit algebras* and denote their multiplication by juxtaposition. Without loss of generality, we will only consider monic $f(t)$, since $S_f = S_{af}$

for all $a \in K^\times$. Let

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

S_f is a semifield if and only if f is irreducible, and a proper semifield if and only if f is not right invariant (i.e., the left ideal Rf generated by f is not two-sided), cf. [27, (2), p. 13-03, (5), (9)], or [23]. If S_f is a proper semifield then $\mathbb{N}_l(S_f) = \mathbb{N}_m(S_f) = K \cdot 1 = \mathbb{F}_{q^n} \cdot 1$ and

$$\mathbb{N}_r(S_f) = \{g \in R \,|\, fg \in Rf\} \cong \mathbb{F}_{q^m}$$

[23]. S_f has order q^{mn}. The powers of t are associative if and only if $t^m t = t t^m$ if and only if $t \in \mathbb{N}_r(S_f)$ if and only if $ft \in Rf$.

In particular, let $f(t) \in F[t] = F[t;\sigma] \subset K[t;\sigma]$ be monic, irreducible and not right invariant. Then

$$F[t]/(f(t)) \cong F \oplus Ft \oplus \cdots \oplus Ft^{m-1} \cong \mathbb{N}_r(S_f)$$

and thus $\mathbb{N}(S_f) = F \cdot 1$. Moreover, we have $ft \in Rf$ [12, Proposition 3].

Remark 1. Note that $f(t) \in K[t;\sigma] \setminus F[t;\sigma]$ is never right invariant and that if $f(t) \in F[t] \subset K[t;\sigma]$ has degree $m < n$, then $f(t)$ is never right invariant, either. For $n = m$ the only rght invariant $f(t) \in F[t]$ are of the form $f(t) = t^m - a$, and these polynomials are not irreducible. So for $n = m$, all irreducible polynomials in $F[t]$ are not right invariant.

If the semifield $A = K[t;\sigma]/K[t;\sigma]f$ has a nucleus which is larger than its center, then the inner automorphisms $\{G_c \,|\, 0 \neq c \in \mathbb{N}(A)\}$ form a non-trivial subgroup of $\mathrm{Aut}_F(S_f)$ [35, Lemma 2, Theorem 3] and each such inner automorphism G_c extends $id_{\mathbb{N}(A)}$.

We will assume throughout the paper that $f \in K[t;\sigma]$ is irreducible of degree $m \geq 2$, since if f has degree 1 then $S_f \cong K$, and that $\sigma \neq id$.

We will always choose irreducible polynomials $f \in K[t;\sigma]$ which are not right invariant, which is equivalent to S_f being a proper semifield. Each Jha-Johnson semifield is isotopic to some Petit algebra S_f [23, Theorem 16] but not necessarily a Petit algebra itself. We will focus on those Jha-Johnson semifields which are Petit algebras S_f, and apply the results from [12].

1.3. **Automorphisms of Jha-Johnson semifields S_f.** Assume that

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

has degree m, is monic, irreducible and not right invariant. Then S_f is a Jha-Johnson semifield over $F = \mathbb{F}_q$ [23]. We recall some results from [12] for the convenience of the reader: Let $\tau = \sigma^j \in \mathrm{Gal}(K/F)$ for some j, $0 \leq j \leq n-1$ 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 $i \in \{0, \ldots, m-1\}$. Then the map $H : S_f \longrightarrow S_f$,

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

is an automorphism of S_f. These $H_{\tau,k}$ form a subgroup of $\mathrm{Aut}_F(S_f)$. In particular, if $n \geq m-1$ then

$$\mathrm{Aut}_F(S_f) = \{H_{\tau,k} \mid \text{ with } \tau = \sigma^j, 0 \leq j \leq n-1 \text{ and } k \in K^\times \text{ satisfying Equation (1)}\}$$

[12, Theorems 4, 5].

An algebra S_f with $f(t) = t^m - a \in K[t;\sigma]$, $a \in K \setminus F$ and $n \geq m$ is called a *Sandler semifield* [30]. For $m = n$, these algebras are also called *nonassociative cyclic (division) algebras of degree* m, as they can be seen as canonical generalizations of associative cyclic algebras (since for $a \in F^\times$, S_f with $f(t) = t^m - a \in K[t;\sigma]$ is a classical cyclic algebra of degree m as defined in [20, p. 414]). These algebras are treated in Section 3.

The automorphism groups of Sandler semifields are particularly relevant:

Theorem 2. [12, Theorem 8] *Let $n \geq m-1$ and $g(t) = t^m - \sum_{i=0}^{m-1} b_i t^i \in K[t;\sigma]$ be irreducible and not right invariant. Assume one of the following:*
(i) $b_0 \in K \setminus F$ and $f(t) = t^m - b_0 \in K[t;\sigma]$.
(ii) $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in K[t;\sigma]$ be such that $b_i \in \{0, a_i\}$ for all $i \in \{0, \ldots, m-1\}$.
Then $\mathrm{Aut}_F(S_g) \subset \mathrm{Aut}_F(S_f)$ is a subgroup.

Theorem 3. [12, Theorem 9] *Let $n < m-1$ and $g(t) = t^m - \sum_{i=0}^{m-1} b_i t^i \in K[t;\sigma]$ be irreducible and not be right invariant. Assume one of the following:*
(i) $f(t) = t^m - b_0 \in K[t;\sigma]$ with $b_0 \in K \setminus F$.
(ii) $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in K[t;\sigma]$ be such that $b_i \in \{0, a_i\}$ for all $i \in \{0, \ldots, m-1\}$.
Then

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

Theorem 4. *(* [12, Theorem 5, Remark 12, Theorem 11]*) Suppose $a_{m-1} \in F^\times$, or that two consecutive coefficients a_s and a_{s+1} lie in $F^\times$.*
(i) For $n \geq m-1$ we distinguish two cases:
If $a_i \notin \mathrm{Fix}(\tau)$ for all $\tau \neq id$ and all non-zero a_i, $i \neq m-1$, then $\mathrm{Aut}_F(S_f) = \{id\}$.
If $f(t) \in F[t] \subset K[t;\sigma]$ then any automorphism H of S_f has the form $H_{\tau,1}$ where $\tau \in \mathrm{Gal}(K/F)$, and

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

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

Theorem 5. *(*[12, Theorem 19]*) Let $f(t) \in F[t] \subset K[t;\sigma]$.*
(i) $\langle H_{\sigma,1} \rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(S_f)$ of order n.
(ii) Suppose one of the following holds:
(a) $n \geq m-1$ and $a_{m-1} \in F^\times$.
(b) $n = m$ is prime, $a_0 \neq 0$ and at least one of $a_1, \ldots, a_{m-1}$ is non-zero.
Then $\mathrm{Aut}_F(S_f) = \langle H_{\sigma,1} \rangle \cong \mathbb{Z}/n\mathbb{Z}$ and any automorphism extends exactly one $\tau \in \mathrm{Gal}(K/F)$.

Proposition 6. [12, Corollaries 13, 14] *Let $f(t) = t^m - a \in K[t;\sigma]$, $a \in K \setminus F$ and $\tau \in \mathrm{Gal}(K/F)$.*

(i) For all $k \in K^\times$ with

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

the maps $H_{\tau,k}$ are automorphisms of S_f. In particular, $N_{K/F}(k)$ is an mth root of unity. If $n \geq m-1$ these are all 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 $a_0 = a$,

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

If $n \geq m-1$ then these groups are the automorphism groups of S_g and S_f, hence in that case $\mathrm{Aut}_F(S_g)$ is a subgroup of $\mathrm{Aut}_F(S_f)$.

Corollary 7. *Let $n \geq m-1$ and $f(t) = t^m - a \in K[t;\sigma]$ with $a \in K \setminus F$. Let m and $(q-1)$ be coprime.*
(i) There are at most $s = (q^n-1)/(q-1)$ automorphisms extending each $\tau = \sigma^j$.
(ii) For all irreducible $g(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in K[t;\sigma]$ with $a_0 = a$, $\mathrm{Aut}_F(S_g)$ is a subgroup of $\mathrm{Aut}_F(S_f)$.

Proof. (i) We know that $H \in \mathrm{Aut}_F(S_f)$ if and only if $H = H_{\sigma^j,k}$ where $j \in \{0,\ldots,n-1\}$ and $k \in K^\times$ is such that

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

by Proposition 6. In particular, $N_{K/F}(k) = 1$. So there are at most $s = (q^n-1)/(q-1)$ automorphisms extending each σ^j.
(ii) is obvious. □

2. Inner automorphisms

Let $f \in K[t;\sigma]$ have degree m, and be monic, irreducible and not right invariant. [35, Corollary 5] yields immediately:

Proposition 8. *Suppose $N = \mathbb{N}(S_f) = \mathbb{F}_{q^l} \cdot 1$ for some integer $1 < l \leq n$. Then S_f has at least*

$$(q^l - 1)/(q-1)$$

inner automorphisms, determined by those q^l elements in its nucleus that do not lie in F. They all are extensions of id_N.
In particular, if S_f has nucleus $K \cdot 1$ then there are $s = (q^n-1)/(q-1)$ inner automorphisms of S_f and all extend id_K; thus all have the form $H_{id,k}$ for a suitable $k \in K^\times$.

Every automorphism $H_{id,k} \in \mathrm{Aut}_F(S_f)$ such that $N_{K/F}(k) = 1$ is an inner automorphism. 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 [12, Theorem 16].

Let $\Delta^\sigma(l) = \{\sigma(c)lc^{-1} \mid c \in K^\times\}$ denote the σ-conjugacy class of l [22]. By Hilbert's Theorem 90, $\ker(N_{K/F}) = \Delta^\sigma(1)$. In particular, for every $a \in F^\times$ there exist exactly $s = (q^n-1)/(q-1)$ elements $u \in K$ with $N_{K/F}(u) = a$.

Proposition 9. *Let $n \geq m-1$. Then there exist at most*

$$|\ker(N_{K/F})| = (q^n-1)/(q-1)$$

distinct automorphisms of S_f of the form $H_{id,k}$ such that $N_{K/F}(k) = 1$. These are inner.

Proof. Every automorphism $H_{id,k} \in \mathrm{Aut}_F(S_f)$ extending id_K such that $N_{K/F}(k) = 1$ is an inner automorphism by [12, Theorem 16]. More precisely, for any $k, l \in K^\times$ with $N_{K/F}(k) = 1 = N_{K/F}(l)$ there are $c, d \in K^\times$ such that $k = c^{-1}\sigma(c)$, $l = d^{-1}\sigma(d)$, and $H_{id,k} = G_c$, $H_{id,l} = G_d$ (cf. the proof of [12, Theorem 16]). We have

$$H_{id,k} = H_{id,l} \text{ if and only if } c^{-1}\sigma(c) = d^{-1}\sigma(d).$$

Therefore there exist at most $|\ker(N_{K/F})| = |\Delta^\sigma(1)|$ distinct automorphisms of S_f of the form $H_{id,k}$. □

Proposition 9 and Proposition 8 imply the following estimates for the number of inner automorphisms of S_f:

Theorem 10. *Let $n \geq m-1$. If S_f has nucleus $K \cdot 1$ then it has $s = (q^n-1)/(q-1)$ inner automorphisms extending id_K. These form a cyclic subgroup of $\mathrm{Aut}_F(S_f)$ isomorphic to $\ker(N_{K/F})$.*

Proof. By Proposition 9, there are at most $|\ker(N_{K/F})| = (q^n-1)/(q-1)$ distinct automorphisms $H_{id,k}$ of S_f and all of these are inner and extend id_K. By Proposition 8, if S_f has nucleus $K \cdot 1 = \mathbb{F}_{q^n} \cdot 1$ then there exist at least $s = (q^n-1)/(q-1)$ inner automorphisms, all extending id_K, those determined by the elements in its nucleus which do not lie in F. Then there are exactly s inner automorphisms. □

Thus if $N = \mathbb{N}(S_f) = \mathbb{F}_{q^l} \cdot 1$, $l > 1$, is strictly contained in $K \cdot 1$, then S_f has t inner automorphisms extending id_N, with

$$\frac{q^l-1}{q-1} \leq t \leq \frac{q^n-1}{q-1}.$$

3. Nonassociative cyclic algebras

In this section unless specifically noted otherwise, let

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

be irreducible (which is always the case if a belongs to no proper subfield of K/F), σ have order $n = m$ and let

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

Then A is an example of a Sandler semifield [30]. A is also called a *nonassociative cyclic (division) algebra of degree m*, because its construction (hence its multiplication) is similar to the one of an associative cyclic algebra which is defined by $K[t;\sigma]/K[t;\sigma](t^m - a)$ but

choosing $a \in F^\times$. For $m = n = 2$, A is also called a *nonassociative quaternion algebra* and was first described by Dickson [13]. We know that $\mathbb{N}_l(A) = \mathbb{N}_m(A) = \mathbb{N}_r(A) = K \cdot 1$. Moreover,

$$(K/F, \sigma, a) \cong (K/F, \sigma, b)$$

if and only if

$$\sigma^i(a) = kb \text{ for some } 0 \leq i \leq m-1 \text{ and some } k \in F^\times$$

[12, Corollary 34].

By Theorem 10, A has exactly $s = (q^m - 1)/(q - 1)$ inner automorphisms, all of them extending id_K. These are given by the F-automorphisms $H_{id,l}$ for all $l \in K$ such that $N_{K/F}(l) = 1$. The subgroup they generate is cyclic and isomorphic to $\ker(N_{K/F})$.

3.1.

Theorem 11. *(*[12, Theorem 22]*) Suppose m divides $(q-1)$ and let ω denote a non-trivial mth root of unity in F.*
(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) Suppose $N_{K/F}(l) = \omega$ is a primitive mth root of unity and $\sigma(a) = \omega a$. Then the subgroup generated by $H = H_{\sigma,l}$ has order m^2.
(iii) For each mth root of unity $\omega \in F$, $l \in K$ with $N_{K/F}(l) = \omega$ and a $j \in \{1, \ldots, m-1\}$ such that $\sigma^j(a) = \omega a$, there is an automorphism $H_{\sigma^j,l}$ extending σ^j.

Proposition 12. *(*[12, Theorem 21]*) A Galois automorphism $\sigma^j \neq id$ can be extended to an automorphism $H \in \mathrm{Aut}_F(A)$ 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 $N_{K/F}(l) = \omega$ is a primitive mth root of unity and there exist $s = (q^m - 1)/(q - 1)$ such extensions.

Theorem 13. [12, Theorem 24] *Let K/F have prime degree m. Suppose that F contains a primitive mth root of unity, where m is coprime to the characteristic of F and so $K = F(d)$ where d is a root of an irreducible polynomial $t^m - c \in F[t]$. Then H is an automorphism of A 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 a primitive mth root of unity and $a = cd^l$ for some $c \in F^\times$ and some power d^l.*

For more general polynomials this yields:

Corollary 14. *Suppose that F contains a primitive mth root of unity, where m is coprime to the characteristic of F and so $K = F(d)$ where d is a root of some $t^m - c \in F[t]$. Let*

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

and $a_0 \in K \setminus F$, such that $a_0 \neq cd^i$ for any $0 \leq i \leq m-1$, $c \in F^\times$. Then every F-automorphism of S_g leaves K fixed, is inner and $\mathrm{Aut}_F(S_g) \subset \ker(N_{K/F})$ is a subgroup, thus cyclic with at most $s = (q^m - 1)/(q - 1)$ elements.

This follows from [12, Corollary 25].

Corollary 15. *Suppose that F does not contain an mth root of unity (i.e., m and $(q-1)$ are coprime). Let*

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

and $a_0 \in K \setminus F$. Then every F-automorphism of S_g leaves K fixed, is inner and $\mathrm{Aut}_F(S_g)$ is isomorphic to a subgroup of $\ker(N_{K/F})$, thus cyclic with at most $s = (q^m-1)/(q-1)$ elements. In particular, if $\ker(N_{K/F})$ has prime order, then either $\mathrm{Aut}_F(S_g)$ is trivial or $\mathrm{Aut}_F(S_g) \cong \ker(N_{K/F})$.

We can also rephrase our results as follows:

Proposition 16. *Let α be a primitive element of K, i.e. $K^\times = \langle\alpha\rangle$.*
(i) $\langle G_\alpha\rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(A)$ of order $s = (q^m-1)/(q-1)$, containing inner automorphisms.
(ii) Suppose one of the following holds:
(a) m and $(q-1)$ are coprime.
(b) m is prime and F a field where m is coprime to the characteristic of F, containing a primitive mth root of unity. Let $K = F(d)$ be a cyclic field extension of F of degree m. Let $a \in K \setminus F$ and $a \neq \lambda d^i$ for every $i \in \{0,\dots,m-1\}$, $\lambda \in F^\times$.
Then $\mathrm{Aut}_F(A) = \langle G_\alpha\rangle$.

Proof. If $K^\times = \langle\alpha\rangle$ then $F^\times = \langle\alpha^s\rangle$ for $s = (q^m-1)/(q-1)$. In particular $\alpha^s \in F^\times$ but $\alpha^j \notin F$ for all smaller j. The result now follows from [12, Theorem 21(iii)] □

For more general choices of twisted polynomials this means:

Theorem 17. *With the assumptions of Proposition 16 (ii) on K/F and a, for each irreducible*

$$g(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \text{ with } a_0 = a \in K \setminus F,$$

$\mathrm{Aut}_F(S_g)$ is a subgroup of $\ker(N_{K/F})$ and therefore cyclic of order at most $s = (q^m-1)/(q-1)$.

This is a consequence of Theorem 2.

3.2. The automorphism groups of some nonassociative cyclic algebras. In this subsection, we assume that F is a field where m is coprime to the characteristic of F, and that F contains a primitive mth root of unity ω, so that $K = F(d)$. Let $s = (q^m-1)/(q-1)$.

Lemma 18. *Suppose $m|(q-1)$ then:*
(i) $m|s$.
(ii) If m is odd then $m^2 \nmid (ls)$ for all $l \in \{1,\dots,m-1\}$.
(iii) If $(q-1)/m$ is even then $m^2 \nmid (ls)$ for all $l \in \{1,\dots,m-1\}$.

Proof. (i) We prove first that

$$(q-1)\Big|\Big((\sum_{i=0}^{m-1} q^i) - m\Big) \tag{2}$$

for all $m \geq 2$ by induction:

Clearly (2) holds for $m = 2$. Suppose (2) holds for some $m \geq 2$, then

$$(\sum_{i=0}^{m} q^i) - (m+1) = (\sum_{i=0}^{m-1} q^i) - m + q^m - 1 = (\sum_{i=0}^{m-1} q^i) - m + (\sum_{i=0}^{m-1} q^i)(q-1). \tag{3}$$

Now, $(q-1)\Big|\Big((\sum_{i=0}^{m-1} q^i) - m\Big)$ and so (2) holds by induction. In particular

$$m\Big|\Big((\sum_{i=0}^{m-1} q^i) - m\Big),$$

therefore m divides $\big(\sum_{i=0}^{m-1} q^i\big) - m + m = s$ as required.
(ii) and (iii): Write $q = 1 + rm$ for some $r \in \mathbb{N}$, then

$$\begin{aligned} q^j = (1+rm)^j &= \sum_{i=0}^{j} \binom{j}{i} (rm)^i \equiv \sum_{i=0}^{1} \binom{j}{i} (rm)^i \bmod (m^2) \\ &\equiv (1 + jrm) \bmod (m^2) \end{aligned}$$

for all $j \geq 1$. Therefore

$$\begin{aligned} ls = l\sum_{j=0}^{m-1} q^j &\equiv l\big(1 + \sum_{j=1}^{m-1} (1+jrm)\big) \bmod (m^2) \\ &\equiv \Big(lm + lrm\frac{(m-1)m}{2}\Big) \bmod (m^2), \end{aligned}$$

for all $l \in \{1, \ldots, m-1\}$. If m is odd or $r = (q-1)/m$ is even then

$$\frac{lr(m-1)}{2} \in \mathbb{Z}$$

which means

$$ls \equiv lm \bmod (m^2) \not\equiv 0 \bmod (m^2),$$

that is, $m^2 \nmid (ls)$ for all $l \in \{1, \ldots, m-1\}$. □

Recall that the semidirect product

$$\mathbb{Z}/m\mathbb{Z} \rtimes_l \mathbb{Z}/n\mathbb{Z} = \langle x, y \,|\, x^m = 1, y^n = 1, yxy^{-1} = x^l \rangle$$

of $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ corresponds to the choice of an integer l with $l^n \equiv 1 \bmod m$. Let $A = (K/F, \sigma, a)$ where $a = \lambda d^i$ for some $i \in \{1, \ldots, m-1\}$, $\lambda \in F^\times$.

Theorem 19. *Suppose m is odd or $r = (q-1)/m$ is even. Then $\mathrm{Aut}_F(A)$ is a group of order ms and contains a subgroup isomorphic to the semidirect product*

$$\mathbb{Z}/\Big(\frac{s}{m}\Big)\mathbb{Z} \rtimes_q \mathbb{Z}/(m\mu)\mathbb{Z}, \tag{4}$$

where $\mu = m/\gcd(i, m)$. Moreover, if i and m are coprime, then

$$\mathrm{Aut}_F(A) \cong \mathbb{Z}/\Big(\frac{s}{m}\Big)\mathbb{Z} \rtimes_q \mathbb{Z}/(m^2)\mathbb{Z}. \tag{5}$$

Proof. Let $\tau : K \to K,\ k \mapsto k^q$, then

$$\tau^j(a) = \omega^{ij}a,$$

for all $j \in \{0, \ldots, m-1\}$ where $\omega \in F^\times$ is a primitive m^{th} root of unity by [12, Lemma 23]. As τ generates $\mathrm{Gal}(K/F)$, the automorphisms of A are precisely the maps $H_{\tau^j,k}$, where $j \in \{0, \ldots, m-1\}$ and $k \in K^\times$ are such that $\tau^j(a) = N_{K/F}(k)a$ by Proposition 12. Moreover there are exactly s elements $k \in K^\times$ with $N_{K/F}(k) = \omega^{ij}$ by Proposition 12, and each of these elements corresponds to a unique automorphism of A. Therefore $\mathrm{Aut}_F(A)$ is a group of order ms.

Choose $k \in K^\times$ such that $N_{K/F}(k) = \omega^i$ so that $H_{\tau,k} \in \mathrm{Aut}_F(S_f)$. As τ has order m, $H_{\tau,k} \circ \ldots \circ H_{\tau,k}$ (m-times) becomes $H_{id,b}$ where $b = \omega^i = N_{K/F}(k)$. Notice ω^i is a primitive μ^{th} root of unity where $\mu = m/\gcd(i,m)$, then $H_{id,b}$ has order μ and so the subgroup of $\mathrm{Aut}_F(S_f)$ generated by $H_{\tau,k}$ has order $m\mu$.

$\langle G_\alpha \rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(S_f)$ of order s by Proposition 16 where α is a primitive element of K. Furthermore, $m|s$ by Lemma 18 and so $\langle G_{\alpha^m} \rangle$ is a cyclic subgroup of $\mathrm{Aut}_F(A)$ of order s/m. We will prove $\mathrm{Aut}_F(A)$ contains the semidirect product

$$\langle G_{\alpha^m} \rangle \rtimes_q \langle H_{\tau,k} \rangle : \tag{6}$$

The inverse of $H_{\tau,k}$ in $\mathrm{Aut}_F(A)$ is $H_{\tau^{-1},\tau^{-1}(k^{-1})}$ and a tedious calculation shows that

$$H_{\tau,k} \circ G_{\alpha^m} \circ H_{\tau,k}^{-1} = G_{\alpha^{mq}} = (G_{\alpha^m})^q.$$

Notice $q^m = qs - s + 1$, i.e. $q^m \equiv 1 \bmod s$, and so $q^{m\mu} \equiv 1 \bmod s$. Then $m|s$ by Lemma 18, hence $q^{m\mu} \equiv 1 \bmod (s/m)$. In order to prove (6), we are left to show that $\langle H_{\tau,k} \rangle \cap \langle G_{\alpha^m} \rangle = \{\mathrm{id}\}$.

Suppose for contradiction $\langle H_{\tau,k} \rangle \cap \langle G_{\alpha^m} \rangle \neq \{\mathrm{id}\}$, then $H_{id,\omega^l} \in \langle G_{\alpha^m} \rangle$ for some $l \in \{1, \ldots, m-1\}$. Therefore $\langle G_{\alpha^m} \rangle$ contains a subgroup of order $m/\gcd(l,m)$ generated by H_{id,ω^l} and so $(m/\gcd(l,m))|(s/m)$. This means $m^2|(s\gcd(l,m))$, a contradiction by Lemma 18.

Therefore $\mathrm{Aut}_F(A)$ contains the subgroup

$$\langle G_{\alpha^m} \rangle \rtimes_q \langle H_{\tau,k} \rangle \cong \mathbb{Z}/\Big(\frac{s}{m}\Big)\mathbb{Z} \rtimes_q \mathbb{Z}/(m\mu)\mathbb{Z}.$$

If $\gcd(i,m) = 1$ this subgroup has order ms and since $|\mathrm{Aut}_F(A)| = ms$, this is all of $\mathrm{Aut}_F(A)$. □

Theorem 20. *Suppose m is prime and $m|(q-1)$.*

(i) *If $m = 2$ then $\mathrm{Aut}_F(A)$ is the dicyclic group Dic_r of order $4r = 2q + 2$.*
(ii) *If $m > 2$ then*

$$\mathrm{Aut}_F(A) \cong \mathbb{Z}/\Big(\frac{s}{m}\Big)\mathbb{Z} \rtimes_q \mathbb{Z}/(m^2)\mathbb{Z}. \tag{7}$$

Proof. (i) We already know that $\mathrm{Aut}_F(A)$ has order $2(q+1)$. Let $\alpha \in K$ be a primitive element. Then $\langle G_\alpha \rangle$ is a subgroup of $\mathrm{Aut}_F(A)$ of order s by Proposition 16. Furthermore, since $\sigma(a) = -a$, there are precisely $s = q+1$ automorphisms $H_{\sigma,k}$ where $k \in K$ is such that

$N_{K/F}(k) = -1$. Pick any such $k \in K$. Then an easy calculation shows that $\mathrm{Aut}_F(A) \cong Dic_r$, i.e. that

$$\mathrm{Aut}_F(A) = \langle H_{\sigma,k}, G_\alpha \mid G_\alpha^{2r} = 1,\ H_{\sigma,k}^2 = G_\alpha^r,\ H_{\sigma,k}^{-1} G_\alpha H_{\sigma,k} = G_\alpha^{-1} \rangle.$$

(ii) follows immediately from Theorem 19. □

Recall that the smallest dicyclic group Dic_2 of order $4r = 8$ (this only occurs if $q = 3$) is isomorphic to the quaternion group. More generally, when r is a power of 2, the dicyclic group Dic_r of order $4r = 2q + 2$ is isomorphic to the generalized quaternion group.

Note that if $m = 2$ and 4 divides $s = q + 1$ then $\mathrm{Aut}_F(A)$ is not a semidirect product, since in this case $\langle H_{\sigma,k} \rangle \cap \langle G_{\alpha^2} \rangle \neq \{id\}$.

Remark 21. Let F have characteristic not 2 and $K = F(d)$ be a quadratic field extension of F, then $A = (K/F, \sigma, a)$ is a *nonassociative quaternion algebra*. Nonassociative quaternion algebras are up to isomorphism the only proper semifields of order q^4 with center $F1$ and nucleus containing $K \cdot 1$ [34, Theorem 1]. Although being not associative, they are closely related to associatve quaternion algebras, as their multiplication can be seen as a canonical generalization of the classical Cayley-Dickson doubling process used to construct quaternion algebras out of a separable quadratic field extension [7]. If $a \neq \lambda d$ for any $\lambda \in F^\times$, then $\mathrm{Aut}_F(A) \cong \mathbb{Z}/(q+1)\mathbb{Z}$ and all automorphisms are inner (as it is the case for classical quaternion algebras). If $a = \lambda d$ for some $\lambda \in F^\times$, then $\mathrm{Aut}_F(A)$ is the dicyclic group of order $2q + 2$ (Theorem 20).

4. The automorphisms of Hughes-Kleinfeld and Knuth semifields

Let K/F be a Galois field extension of degree n. Choose $\eta, \mu \in K$ and a nontrivial automorphism $\sigma \in \mathrm{Aut}_F(K)$. For $x, y, u, v \in K$ the following four multiplications make the F-vector space $K \oplus K$ into an algebra over F:

$$\begin{aligned}
Kn_1 &: (x,y) \circ (u,v) = (xu + \eta\sigma(v)\sigma^{-2}(y), vx + y\sigma(u) + \mu\sigma(v)\sigma^{-1}(y)),\\
Kn_2 &: (x,y) \circ (u,v) = (xu + \eta\sigma^{-1}(v)\sigma^{-2}(y), vx + y\sigma(u) + \mu v\sigma^{-1}(y)),\\
Kn_3 &: (x,y) \circ (u,v) = (xu + \eta\sigma^{-1}(v)y, vx + y\sigma(u) + \mu vy),\\
HK &: (x,y) \circ (u,v) = (xu + \eta y\sigma(v), xv + y\sigma(u) + \mu y\sigma(v)).
\end{aligned}$$

The unital algebras given by each of the above multiplications are denoted $Kn_1(K, \sigma, \eta, \mu)$, $Kn_2(K, \sigma, \eta, \mu)$, $Kn_3(K, \sigma, \eta, \mu)$ and $HK(K, \sigma, \eta, \mu)$, respectively. The first three algebras were defined by Knuth and the last one by Hughes and Kleinfeld [17], [21]. If $\sigma^2 = id$ and $\mu = 0$, they are the same algebra with multiplication $(x,y) \circ (u,v) = (xu + \eta y\sigma(v), xv + y\sigma(u))$. Each of the algebras is a division algebra if and only if

$$f(t) = t^2 - \mu t - \eta \in K[t; \sigma]$$

is irreducible [17], [21]. For $F = \mathbb{F}_q$, $K = \mathbb{F}_{q^n}$ and irreducible $f(t)$ (i.e. $\eta \neq 0$), we thus obtain semifields. Identifying (u, v) with $u + tv$, we see that the Hugh-Kleinfeld algebra

$$HK(K, \tau, \eta, \mu) = S_f \text{ with } f(t) = t^2 - \mu t - \eta \in K[t; \tau]$$

is a Petit algebra and that

$$Kn_2(K,\sigma,\eta,\mu) =_f S \text{ with } f(t) = t^2 - \mu t - \eta \in K[t;\sigma],$$

hence is the opposite algebra of a suitable Petit algebra. Thus $Kn_2(K,\sigma,\eta,\mu) = S_g$ for $g(t) = t^2 - \mu' t - \eta' \in K[t;\sigma^{-1}]$ for some suitable $\mu', \eta' \in K$ by [23, Corollary 4]. Thus the automorphisms for any $Kn_2(K,\sigma,\eta,\mu)$ will be the same as for a Petit algebra $HK(K,\sigma^{-1},\eta',\mu')$.

Suppose that either $\sigma^2 \neq id$ or that $\mu \neq 0$. Then the following is well-known (cf. [17], [21]):

- $K \cdot 1$ is not contained in the left, right or middle nucleus of $Kn_1(L,\sigma,\eta,\mu)$.
- $\mathbb{N}_m(A) = \mathbb{N}_r(A) = K \cdot 1$ and $\mathbb{N}_l(A) \cong \mathbb{F}_{q^2}$ for $A = Kn_2(K,\sigma,\eta,\mu)$
- $\mathbb{N}_l(A) = \mathbb{N}_r(A) = K \cdot 1$ for $A = Kn_3(K,\sigma,\eta,\mu)$ but $K \cdot 1$ is not contained in the middle nucleus.

Hence $Kn_1(K,\sigma,\eta,\mu)$, $Kn_2(K,\sigma,\eta,\mu)$, $Kn_3(K,\sigma,\eta,\mu)$ and $HK(K,\sigma,\eta,\mu)$ are mutually non-isomorphic algebras.

We now describe all automorphisms for the algebras $HK(K,\sigma,\eta,\mu)$ (hence also for $Kn_2(K,\sigma,\eta,\mu)$) and $Kn_3(K,\sigma,\eta,\mu)$. We also exhibit some automorphisms for the algebra $Kn_1(K,\sigma,\eta,\mu)$. This complements and improves the results in [35].

Theorem 22. *(i) All automorphisms of the Petit algebra $A = HK(K,\sigma,\eta,\mu)$ are of the form*

$$H_{\tau,k}(x_0 + x_1 t) = \tau(x_0) + k\tau(x_1)t$$

where $\tau \in \mathrm{Aut}_F(K)$ and $k \in K^\times$ such that $\eta k\sigma(k) = \tau(\eta)$ and $\mu\sigma(k) = \tau(\mu)$.
(ii) All automorphisms of $Kn_3(K,\sigma,\eta,\mu)$ are of the form

$$H_{\tau,k}(x_0 + x_1 t) = \tau(x_0) + k\tau(x_1)t,$$

where $\tau \in \mathrm{Aut}_F(K)$ and $k \in K^\times$ such that $\eta\sigma^{-1}(k)\sigma^{-2}(k) = \tau(\eta)$ and $\mu\sigma^{-1}(k) = \tau(\mu)$.
In both (i) and (ii), $N_{K/F}(k) = \pm 1$ and if $\mu \neq 0$, even $N_{K/F}(k) = 1$.

Proof. (i) This follows from the results mentioned in Subsection 1.3, i.e. Theorem [12, Theorem 4]. Furthermore, $\eta k\sigma(k) = \tau(\eta)$ implies $N_{K/F}(\eta k^2) = N_{K/F}(\eta)$, i.e $N_{K/F}(k^2) = N_{K/F}(k)^2 = 1$ since $\eta \neq 0$, thus $N_{K/F}(k) = \pm 1$. If $\eta \in F^\times$ then $\eta k\sigma(k) = \tau(\eta)$ yields $\eta k\sigma(k) = \eta$, hence $k\sigma(k) = 1$. The equation $\mu\sigma(k) = \tau(\mu)$ implies $N_{K/F}(\mu k) = N_{K/F}(\mu)$, i.e $N_{K/F}(k) = 1$ for $\mu \neq 0$.
(ii) Since any automorphism preserves the left nucleus $K \cdot 1$, it follows that $H|_K = \tau$ for some $\tau \in \mathrm{Aut}_F(K)$. Although here we are not dealing with a Petit algebra, (ii) is now proved analogous to (i) with the same arguments as used in the proof of [12, Theorem 4], since comparing coefficients also yields $H(t) = kt$ for some $k \in K^\times$. □

Corollary 23. *Let $\mu \in F^\times$ and A be either $HK(K,\sigma,\eta,\mu)$, $Kn_2(K,\sigma,\eta,\mu)$ or $Kn_3(K,\sigma,\eta,\mu)$.*
(i) If $\eta \in K \setminus F$ then $\mathrm{Aut}_F(A) = \{id\}$.
(ii) If $\eta \in F$ and $f(t) = t^2 - \mu t - \eta$ is not right invariant then

$$\mathrm{Aut}_F(A) \cong \mathbb{Z}/n\mathbb{Z}.$$

Proof. Theorem 4 for S_f implies the statement for the first two types. The argument for the third type is analogous: if $\mu \in F^\times$ then $k = 1$, thus $\eta = \tau(\eta)$ forces $\tau = id$ or $\eta \in F^\times$. If $\eta \in K \setminus F$ thus $\tau = id$ and $\mathrm{Aut}_F(A) = \{id\}$. If $\eta \in F$ and $f(t)$ is not right invariant then $\mathrm{Aut}_F(A) \cong \mathrm{Gal}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$. □

Proposition 24. *Let A be one of the algebras $HK(K,\sigma,\eta,\mu), Kn_2(K,\sigma,\eta,\mu)$ or $Kn_3(K,\sigma,\eta,\mu)$ where $\mu \neq 0$. Then*

$$\mathrm{Aut}_F(A) \cong \{\tau \in \mathrm{Gal}(K/F) \mid \tau\left(\frac{\mu\sigma(\mu)}{\sigma(\eta)}\right) = \frac{\mu\sigma(\mu)}{\sigma(\eta)}\} \text{ via } H_{\tau,k} \mapsto \tau.$$

Proof. Suppose for instance $A = HK(K,\sigma,\eta,\mu)$. Take the automorphism $H_{\tau,k}$. By Proposition 22, $\mu\sigma(k) = \tau(\mu)$ and $\eta b\sigma(k) = \tau(\eta)$. (Note that since $\mu \neq 0$, the element $k \in K$ is determined completely by the action of τ on μ.) Substituting in $k = \sigma^{-1}(\tau(\mu))\sigma^{-1}(\mu)^{-1}$ and rearranging gives $\sigma(\eta)\tau(\mu)\sigma(\tau(\mu)) = \sigma(\tau(\eta))\mu\sigma(\mu)$. This implies

$$\tau\left(\frac{\mu\sigma(\mu)}{\sigma(\eta)}\right) = \frac{\mu\sigma(\mu)}{\sigma(\eta)}.$$

□

For $Kn_1(K,\sigma,\eta,\mu)$, $K \cdot 1$ is not contained in any of the nuclei. However, if we assume that an automorphism of $Kn_1(K,\sigma,\eta,\mu)$ restricts to an automorphism of K, then it must be of a similar form to the above automorphisms:

Proposition 25. *Suppose H is an automorphism of $A = Kn_1(L,\sigma,\eta,\mu)$ which restricts to an automorphism $\tau \in \mathrm{Aut}_F(K)$. Then*

$$H(x_0 + x_1 t) = \tau(x_0) + k\tau(x_1)t$$

for some $k \in K^\times$, such that $\eta\sigma^{-1}(k)\sigma^{-2}(k) = \tau(\eta)$ and $\mu\sigma(b)\sigma^{-1}(k) = \tau(\mu)k$. In particular, $N_{K/F}(k) = \pm 1$ and if $\mu \neq 0$, $N_{K/F}(k) = 1$. If $\eta \in F^\times$ then $\sigma^{-1}(k)\sigma^{-2}(k) = 1$.

The proof is similar to that of Proposition 22.

5. Isomorphisms between semifields

5.1. If K and L are finite fields and

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

two isomorphic Jha-Johnson semifields with $f \in K[t;\sigma]$ and $g \in L[t;\sigma']$ both monic, irreducible and not right invariant, then

$$K \cong L, \quad \deg(f) = \deg(g) \text{ and } \mathrm{Fix}(\sigma) \cong \mathrm{Fix}(\sigma'),$$

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

Moreover, if G is an automorphism of $R = K[t;\sigma]$, $f(t) \in R$ is irreducible and $g(t) = G(f(t))$, then G induces an isomorphism $S_f \cong S_g$ [23, Theorem 7]. In the following we focus on the situation that $F = \mathbb{F}_q$, $K = \mathbb{F}_{q^n}$, $\mathrm{Gal}(K/F) = \langle\sigma\rangle$, and use

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

[12, Theorems 28 and 29] yield in this setting a generalization of [36, Theorem 4.2 and 5.4] which proved this statement only for $m = 2, 3$.:

Theorem 26. *(i) Suppose $n \geq m-1$. Then $S_f \cong S_g$ if and only if there exists $\tau \in \mathrm{Gal}(K/F)$ and $k \in K^\times$ such that*

$$\tau(a_i) = \Big(\prod_{l=i}^{m-1} \sigma^l(k) \Big) b_i \tag{8}$$

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

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

(ii) Suppose $n < m-1$. If there exists $\tau \in \mathrm{Gal}(K/F)$ and $k \in K^\times$ such that Equation (8) holds for all $i \in \{0, \ldots, m-1\}$ then $S_f \cong S_g$ with an isomorphism $G_{\tau,k} : S_f \to S_g$ as in (i).

As a direct consequence of Theorem 26 we obtain:

Corollary 27. *Let $n \geq m-1$.*
(i) If $S_f \cong S_g$ then $a_i = 0$ if and only if $b_i = 0$, for all $i \in \{0, \ldots, m-1\}$.
(ii) If there exists an $i \in \{0, \ldots, m-1\}$ such that $a_i = 0$ but $b_i \neq 0$ or vice versa, then $S_f \ncong S_g$.

[12, Corollaries 33, 34] yield for instance:

Corollary 28. *Suppose $n \geq m-1$ and that one of the following holds:*
(i) There exists $i \in \{0, \ldots, m-1\}$ such that $b_i \neq 0$ and

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

(ii) $N_{K/F}(a_0) \neq N_{K/F}(b_0)$ in $F^\times / F^{\times m}$;
(iii) $b_{m-1} \neq 0$ and $N_{K/F}(a_{m-1} b_{m-1}^{-1}) \notin F^\times$;
(iv) $m = n$, $a_0 \in F^\times$ and $b_0 \in K \setminus F$.
Then $S_f \ncong S_g$.

Corollary 29. *Let $n = m$, $f(t) = t^m - a$, $g(t) = t^m - b \in K[t; \sigma]$ 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 $a \neq \alpha b$ for all $\alpha \in F^\times$ or if $N_{K/F}(a/b) \notin F^{\times m}$ then $S_f \ncong S_g$.

5.2. The isomorphism classes of nonassociative cyclic algebras of prime degree. As an example, we count how many nonisomorphic semifields $(K/F, \sigma, a)$ there are for a given field extension K/F.

Example 30. Let $F = \mathbb{F}_2$ and let $K = \mathbb{F}_4$, then we can write $K = \{0, 1, x, 1+x\}$ where $x^2 + x + 1 = 0$. Thus for $(K/F, \sigma, a)$ we can either choose $a = x$ or $a = 1 + x$. Both choices will give a division algebra. We also know that $(K/F, \sigma, a) \cong (K/F, \sigma, b)$ if and only if $\sigma(a) = N_{K/F}(l) b$ or $a = N_{K/F}(l) b$. $N_{K/F} : L^\times \to F^\times$ is surjective, so $N_{K/F}(l) = 1$ for all

$l \in K^\times$. The statement then reduces to $(K/F, \sigma, a) \cong (K/F, \sigma, b)$ if and only if $\sigma(a) = b$ or $a = b$. Now

$$\sigma(x) = x^2 = 1 + x.$$

Therefore $(K/F, \sigma, x) \cong (K/F, \sigma, 1 + x)$, so there is only one nonassociative (quaternion) algebra up to isomorphism which can be constructed using K/F. Its automorphism group consists of inner automorphisms and is isomorphic to $\langle G_x \rangle \cong \mathbb{Z}/3\mathbb{Z}$.

More generally we obtain:

Theorem 31. *(i) If m does not divide $q - 1$ then there are exactly*

$$\frac{q^m - q}{m(q-1)}$$

non-isomorphic semifields $(K/F, \sigma, a)$ of degree m.
(ii) If m divides $q - 1$ and is prime then there are exactly

$$m - 1 + \frac{q^m - q - (q-1)(m-1)}{m(q-1)}$$

non-isomorphic semifields $(K/F, \sigma, a)$ of degree m.

Proof. Define an equivalence relation on the set $K \setminus F$ by

$$a \sim b \text{ if and only if } (K/F, \sigma, a) \cong (K/F, \sigma, b).$$

For each $a \in K \setminus F$ we have

$$(K/F, \sigma, a) \cong (K/F, \sigma, \sigma^i(a))$$

for $0 \leq i \leq m - 1$ and

$$(K/F, \sigma, a) \cong (K/F, \sigma, ka)$$

for $k \in F^\times$. If the elements $k\sigma^i(a)$ for $0 \leq i \leq m - 1$ and $k \in F^\times$ are all distinct, then the equivalence class of a has $m(q-1)$ elements. If they are not all distinct then $\sigma^i(a) = ka$ for some i, $i \neq 0$, and some $k \in F^\times$ ([12, Lemma 23]). If $\sigma^i(a) = ka$ $(i \neq 0)$ then k is an mth root of unity, $k \neq 1$. This happens if and only if m divides $q - 1$.
(i) If m does not divide $q-1$ then from $q^m - q$ elements in $K \setminus F$ we get $(q^m - q)/(m(q-1))$ equivalence classes.
(ii) If m divides $q - 1$ then F contains all primitive mth roots of unity and so $K = F(d)$ where d is a root of an irreducible polynomial $t^m - c \in F[t]$. By [12, Lemma 23], the only elements $a \in K \setminus F$ with $\sigma^i(a) = ka$ are the elements d^j, $1 \leq j \leq m - 1$, and their F-scalar multiples. Moreover, for each d^j, $\sigma^i(d^j) = \zeta^{ij} d^j$ and $\zeta^{ij} \in F$, so there are only $q - 1$ distinct elements in the equivalence class of each d^j. Hence the $(q-1)(m-1)$ elements kd^j $(k \in F^\times$ and $j \in \{1, \ldots, m-1\})$ form exactly $m - 1$ equivalence classes. Since these are all the elements in $K \setminus F$ which are eigenvectors for the automorphisms σ^i, the remaining $q^m - q - (q-1)(m-1)$ elements will form

$$\frac{q^m - q - (q-1)(m-1)}{m(q-1)}$$

equivalence classes. In total, we obtain

$$m-1+\frac{q^m-q-(q-1)(m-1)}{m(q-1)}$$

equivalence classes. □

Example 32. Let $F=\mathbb{F}_3$ and $K=\mathbb{F}_9$, i.e.

$$K=F[x]/(x^2-2)=\{0,1,2,x,2x,x+1,x+2,2x+1,2x+2\}.$$

There are two non-isomorphic semifields which are nonassociative quaternion algebras with nucleus $K\cdot 1$, given by $A_1=(K/F,\sigma,x)$ and $A_2=(K/F,\sigma,x+1)$. Now $\mathrm{Aut}_F(A_1)\cong\mathbb{Z}/4\mathbb{Z}$ whereas $\mathrm{Aut}_F(A_2)$ has order 8 and is isomorphic to the group of quaternion units, the smallest dicyclic group Dic_2, by Theorem 20.

By Corollary 31, these are the only non-isomorphic semifields of order 81 of the type $(K/F,\sigma,a)$.

References

[1] M. I. Al-Ali, *On existence of semifields with free automorphism groups*. J. Geom. 92 (1-2) (2009), 17-22.

[2] M. I. Al-Ali, *The automorphism group of a semifield of order q^4*. Comm. Algebra 36 (9) (2008), 3347-3352.

[3] M. I. Al-Ali, *Semifields with free automorphism groups*. Forum Math. 20 (1) (2008), 181-186.

[4] M. I. Al-Ali, Hering, C.; Neumann, A.; Rawashdeh, A. *A semifield of order 5^4 admitting a free 4-group of automorphisms*. Comm. Algebra 35 (6) (2007), 1808-1813.

[5] M. I. Al-Ali, *On the automorphism group of a semifield of order 5^4*. Comm. Algebra 35 (1) (2007), 71-75.

[6] M. I. Al-Ali, C. Hering, A. Neumann, A. Rawashdeh, *On the existence of semifields of prime power order admitting free automorphism groups*. J. Geom. 86 (1-2)(2006/7), 1-5.

[7] V. Astier, S. Pumplün, *Nonassociative quaternion algebras over rings*. Israel J. Math. 155 (2006), 125-147.

[8] M. I. Bani-Ata, S. Aldhafeeri, F. Belgacem, M. Laila, *On four-dimensional unital division algebras over finite fields*. Algebr. Represent. Theory 18 (1) (2015), 215-220.

[9] M. I. Bani-Ata, E. Al-Shemas, *On the existence of semifields of order q^8 admitting elementary abelian groups of order 8*. Forum Math. 26 (2) (2014), 637-644.

[10] M. V. D. Burmester, *On the commutative non-associative division algebras of even order of LE Dickson*. Rend. Mat. Appl 21 (1962), 143-166.

[11] C. Brown, *Petit's algebras and their automorphisms*. PhD Thesis, University of Nottingham, 2018.

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

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

[14] U. Dempwolff, *Autotopism groups of cyclic semifield planes*. J. Algebraic Combin. 34 (4) (2011), 641-669.

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

[16] C. Hering, Christoph, *Fibrations in free modules*. IX Latin American School of Mathematics: Algebra (Spanish) (Santiago de Chile, 1988). Notas Soc. Mat. Chile 10 (1) (1991), 151-163.

[17] D. R. Hughes, E. Kleinfeld, *Seminuclear extensions of Galois fields*. Amer. J. Math. 82 (1960) 389-392.

[18] V. Jha, N. L. Johnson, *An analog of the Albert-Knuth theorem on the orders of finite semifields, and a complete solution to Cofman's subplane problem.* Algebras Groups Geom. 6 (1) (1989), 1-35.

[19] E. Kleinfeld, *Techniques for enumerating Veblen-Wedderburn systems*. Journal of the ACM (JACM) 7(4) (1960), 330-337.

[20] M. A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, "The Book of Involutions", AMS Coll. Publications, Vol.44 (1998).

[21] D. E. Knuth, *Finite semifields and projective planes.* J. Algebra 2 (1965) 182-217.

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

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

[24] G. Menichetti, *Algebre tridimensionali su un campo di Galois.* Ann. Mat. Pura Appl. (4) 97 (1973), 283-301.

[25] G. Menichetti, *On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field.* J. Algebra 47 (2) (1977), 400-410.

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

[27] 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.

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

[29] S. Pumplün, *The multiplicative loops of Jha-Johnson semifields.* To appear in the Conference Proceedings of the Fourth Mile High Conference on Nonassociative Mathematics, Contemporary Mathematics (CONM), AMS. Online at arXiv:1707.03790 [math.GR]

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

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

[32] D. Simon, *Solving norm equations in relative number fields using S-units.* Mathematics of computation 71(239) (2002), 1287-1305.

[33] 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/

[34] W. C. Waterhouse, *Nonassociative quaternion algebras.* Algebras, Groups and Geometries 4 (1987), 365-378.

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

[36] 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.

[37] J.L. Zemmer, *On the subalgebras of finite division algebras.* Canadian J. Math. 4 (1952), 391-503.

E-mail address: Christian.Brown@nottingham.ac.uk; susanne.pumpluen@nottingham.ac.uk; andrew.steele@aquaq.co.uk

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