The University of
Nottingham

UNITED KINGDOM · CHINA · MALAYSIA

Pumpluen, Susanne (2018) The multiplicative loops of Jha-Johnson semifields. Contemporary Mathematics . ISSN 0271-4132 (In Press)

Access from the University of Nottingham repository:
http://eprints.nottingham.ac.uk/49292/8/Loops.pdf

THE MULTIPLICATIVE LOOPS OF JHA-JOHNSON SEMIFIELDS

S. PUMPLÜN

ABSTRACT. The multiplicative loops of Jha-Johnson semifields are non-automorphic finite loops whose left and right nuclei are the multiplicative groups of a field extension of their centers. They yield examples of finite loops with non-trivial automorphism group and non-trivial inner mappings. Upper bounds are given for the number of non-isotopic multiplicative loops of order $q^{nm} - 1$ that are defined using the twisted polynomial ring $K[t; \sigma]$ and a twisted irreducible polynomial of degree m, when the automorphism σ has order n.

INTRODUCTION

For loops the role of automorphisms is not the same as for groups, as inner mappings need not be automorphisms, and almost all finite loops have a trivial automorphism group [14]. One systematic way to find finite loops with a non-trivial automorphism group is to find semifields (i.e., finite unital nonassociative division algebras) with a non-trivial automorphism group, as their multiplicative loops clearly will also have non-trivial automorphisms. The automorphism groups of semifields, however, have not been studied in great detail so far, mostly because it is usually important to understand semifields only up to isotopy. The multiplicative loops and multiplication groups of semifields were considered for instance in [4, 15, 16].

We look at the multiplicative loops of a family of Jha-Johnson semifields, which include Sandler and Hughes-Kleinfeld semifields as special cases. These multiplicative loops yield examples of finite loops with both non-trivial automorphism groups and non-trivial inner automorphisms, which form non-trivial subgroups of their inner mapping groups.

For their definition, let $K = \mathbb{F}_{q^n}$ be a finite field, σ an automorphism of K of order n with fixed field $F = \mathbb{F}_q$, and $R = K[t; \sigma]$ a twisted polynomial ring. Given an irreducible monic twisted polynomial $f \in R = K[t; \sigma]$ of degree $m \geq 2$ that is not right-invariant (i.e., Rf is not a two-sided ideal), the set of all twisted polynomials in R of degree less than m, together with the usual addition of polynomials, can be equipped with a nonassociative ring structure using right division by f to define the multiplication as $g \circ h = gh \mod_r f$, employing the remainder of dividing by f on the right. The resulting nonassociative unital ring S_f, also denoted by $K[t; \sigma]/K[t; \sigma]f$,

---

is a proper semifield over its center F of order q^{mn} and is an example of a *Jha-Johnson semifield*. Its left and middle nucleus is $K = \mathbb{F}_{q^n}$ and its right nucleus is isomorphic to $\mathbb{F}_{q^m}$. In particular, *Sandler semifields* [19] are obtained by choosing $n \geq m$ and $f(t) = t^m - a \in K[t; \sigma]$ with $a \in K \setminus F$, and *Hughes-Kleinfeld semifields* by choosing $f(t) = t^2 - a_1 t - a_0$ [7], [12].

This nonassociative algebra construction was initially introduced in a more general setup by Petit [18]. It was used for the first time for semifields by Wene [22] and then more recently by Lavrauw and Sheekey [13].

The structure of the paper is as follows: in Section 1, we introduce the basic terminology and the algebras S_f. We then determine some subgroups of automorphism groups of the multiplicative loops $L_f = S_f \setminus \{0\}$ of semifields S_f in Section 2 by restricting the automorphisms of S_f to L_f. We give examples of loops of order $q^{mn} - 1$ with multiplicative subgroups of order m. The inner automorphisms of the loops L_f are treated in Section 3 and certain types of Sandler semifields (also called *nonassociative cyclic algebras* due to the similarity in their construction and behaviour to associative cyclic algebras) are studied in Section 4: their loops have nontrivial automorphism groups containing a cyclic subgroup of order $s = (q^m - 1)/(q - 1)$ of inner automorphisms, i.e. middle inner mappings. Upper bounds for the number of isotopic loops obtained as multiplicative loops of Jha-Johnson semifields are briefly considered in Section 5.

Since the multiplication tables of finite loops yield regular Latin squares, all results can be carried over to regular Latin squares if desired.

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. We will only consider unital algebras which have a unit element denoted by 1, such that $1x = x1 = x$ for all $x \in A$.

The *associator* of A is given by $[x, y, z] = (xy)z - x(yz)$. The *left nucleus* of A is defined as $\mathrm{Nuc}_l(A) = \{x \in A \,|\, [x, A, A] = 0\}$, the *middle nucleus* of A as $\mathrm{Nuc}_m(A) = \{x \in A \,|\, [A, x, A] = 0\}$ and the *right nucleus* of A 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 is in $\mathrm{Nuc}(A)$. The *center* of A is $\mathrm{C}(A) = \{x \in A \,|\, x \in \mathrm{Nuc}(A) \text{ and } xy = yx \text{ for all } y \in A\}$.

An algebra A 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, then A is a division algebra if and only if A has no zero divisors [20, 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 $L_a(a_r) = a a_r = 1$.

A *semifield* is a finite-dimensional unital division algebra over a finite field. It is called *proper* if it is not associative.

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 $x \in A$. We denote this automorphism by G_m. The set of inner automorphisms $\{G_m \,|\, m \in \mathrm{Nuc}(A) \text{ invertible}\}$ is a subgroup of $\mathrm{Aut}_F(A)$ [23, Lemma 2, Theorem 3].

1.2. **Loops.** A *loop* L is a quasigroup with a unit element, i.e. a set L together with a multiplicative structure $\cdot : L \times L \longrightarrow L$ such that two of the elements $x, y, z \in L$ in $x \cdot y = z$ uniquely determine the third one. The left and right multiplication maps are the bijections $L_a : x \mapsto ax$, $R_a : x \mapsto xa$ on L. The *multiplication group* $\mathrm{Mlt}(L)$ is the permutation group generated by the left and right multiplication maps of L.

We define the middle, left and right inner mappings on L as $T_x = L_x^{-1} R_x$, $L_{x,y} = L_{yx}^{-1} L_y L_x$ and $R_{x,y} = R_{xy}^{-1} R_y R_x$. The inner mapping T_x plays the role of conjugation and measures how commutative the loop is, and the mappings $L_{x,y}$ and $R_{x,y}$ measure deviations from associativity. The *inner mapping group* is defined as $\mathrm{Inn}(L) = \{f \in \mathrm{Mlt}(L) \,|\, f(1) = 1\}$ and it is well-known that $\mathrm{Inn}(L) = \langle L_{x,y}, R_{x,y}, T_x \,|\, x, y \in L \rangle$.

The set $A^\times$ of non-zero elements of any division algebra A is a multiplicative loop. Thus examples of finite loops canonically appear as the multiplicative loops of semifields. The center, left, right and middle nucleus of the multiplicative loop of a semifield (defined analogously as for an algebra) are cyclic groups. If A is a semifield with center $F \cdot 1 = \mathbb{F}_q \cdot 1$ and q^r elements, then its multiplicative loop has $q^r - 1$ elements and for $r \geq 3$, the multiplication group $\mathrm{Mlt}(A^\times)$ is a transitive subgroup of $\mathrm{GL}(r, q)$ [16, Proposition 5.1]. Furthermore,

$$\mathrm{SL}(r, q) \leq \mathrm{Mlt}(A^\times) \leq \mathrm{GL}(r, q)$$

([16, Proposition 5.2] or [16, Proposition 2.2]), so that

$$q^{r(r-1)/2}(q^r - 1)(q^{r-1} - 1) \cdots (q^2 - 1) \leq |\mathrm{Mlt}(A^\times)| \leq q^{r(r-1)/2}(q^r - 1)(q^{r-1} - 1) \cdots (q - 1).$$

In particular, for $q = 2$, we get $|\mathrm{Mlt}(A^\times)| = 2^{r(r-1)/2}(2^r - 1)(2^{r-1} - 1) \cdots (2^2 - 1)$.

For a semifield A, $A^\times$ is *left cyclic* (or *left primitive*) if $A^\times = \{a, a^{(2}, a^{(3}, \ldots, a^{(s-1)}\}$ where the left principal powers $a^{(n}$ of a are defined as $a^{(1} = a$, $a^{(n} = a^{(n-1}a$, and *right cyclic* (or *right primitive*) if $A^\times = \{a, a^{2)}, a^{3)}, \ldots, a^{s-1)}\}$ where the the right principal powers $a^{n)}$ of a are defined as $a^{1)} = a$, $a^{n)} = a a^{n-1)}$. For instance, the multiplicative loops of semifields of order 16, 27, 32, 125 and 343 are all right cyclic. Semifields of order 81 are left and right cyclic [6].

A loop L has the *weak Lagrange property* if for each subloop M of L, $|M|$ divides $|L|$, and the *strong Lagrange property* if every subloop M of L has the weak Lagrange property. (A loop may have the weak Lagrange property but not the strong one.)

In general, the structure of the multiplicative loop of a semifield is not known.

1.3. 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 $a \in K$ [17]. 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 $g, f \in R$, $f \neq 0$, there exist unique $r, q \in R$ with $\deg(r) < \deg(f)$, such that $g = qf + r$ [8].

Let $f \in R = K[t; \sigma]$ have degree $m \geq 1$. 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 $g \circ h = gh \, \mathrm{mod}_r f$ is a unital nonassociative algebra $S_f = (R_m, \circ)$ over $F = \{a \in K \mid ah = ha \text{ for all } h \in S_f\}$, which is a subfield of K [18, (7)]. S_f is also denoted by R/Rf if we want to make clear which ring R is involved in the construction. In the following, we denote the multiplication by juxtaposition. Note that when $\deg(g)\deg(h) < m$, the multiplication of g and h in S_f and hence in L_f is the same as the multiplication of g and h in R [18, (10)].

We assume throughout the paper that

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

has degree $m \geq 2$, since if f has degree 1 then $S_f \cong K$. We also assume that $\sigma \neq id$. W.l.o.g. we may consider only monic $f(t)$, since $S_f = S_{af}$ for all $a \in K^\times$.

From now on,

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

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

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

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 $s = (q^n - 1)/(q - 1)$. Then 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. [18, (2), p. 13-03, (5), (9)], or [13]. We will hence assume from now on that f is not right-invariant and irreducible. Then S_f is a *Jha-Johnson semifield*. Moreover, each Jha-Johnson semifield is isotopic to some such algebra S_f [13, Theorem 16], so in particular, each multiplicative loop of a Jha-Johnson semifield is isotopic to the multiplicative loop of some algebra S_f.

Let $L_f = S_f \setminus \{0\}$ denote the multiplicative loop of the proper semifield S_f. Then

$$|L_f| = q^{mn} - 1, \quad \mathrm{Nuc}_l(L_f) = \mathrm{Nuc}_m(L_f) = K^\times = \mathbb{F}_{q^n}^\times$$

and $\mathrm{Nuc}_r(S_f) = \{g \in R_m \mid fg \in Rf\} \cong \mathbb{F}_{q^m}$ implies $\mathrm{Nuc}_r(L_f) \cong \mathbb{F}_{q^m}^\times$.

Proposition 1. *([2, Proposition 3]) Let $f(t) \in F[t] = F[t; \sigma] \subset K[t; \sigma]$ be monic, irreducible and not right-invariant. Then $\mathrm{Nuc}_r(L_f) \cong F[t]/(f(t))^\times$. In particular, $\mathrm{Nuc}(L_f) = F^\times \cdot 1$ and $ft \in Rf$.*

Remark 2. (i) The powers of t are associative if and only if $t^m t = t t^m$ in S_f if and only if $t \in \mathrm{Nuc}_r(S_f)$ if and only if $ft \in Rf$ [18, (5)]. Note that the associativity of the powers of t does not imply that S_f is a field.
(ii) The powers of t form a multiplicative group in S_f if and only if $f(t) \in F[t]$ [18, (16) or (20)].
(iii) Note that $f(t) \in K[t; \sigma] \setminus F[t; \sigma]$ is never right-invariant and that if $f(t) \in F[t]$ has degree $m < n$, then $f(t) \in K[t; \sigma]$ is also never right-invariant in $K[t; \sigma]$. For $n = m$ the only right-invariant $f(t) \in F[t]$ are of the form $f(t) = t^m - a$, and these polynomials are reducible. Hence all irreducible polynomials in $F[t]$ of degree n are not right-invariant in $K[t; \sigma]$.

By [10, Lemma 10], we have

$$|\mathrm{Mlt}(L_f)| = |L_f||\mathrm{Inn}(L_f)| = (q^{mn} - 1)|\mathrm{Inn}(L_f)|.$$

We will focus on those Jha-Johnson semifields which are algebras S_f, and apply the results from [2]. We concentrate on the case that $n \geq m - 1$. For $n < m - 1$ similar but weaker results can be obtained.

2. The automorphisms of the multiplicative loops of S_f

Let $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in K[t; \sigma]$ be irreducible and not right-invariant. Let L_f be the multiplicative loop of S_f. We obtain the following necessary conditions for a loop automorphism of L_f:

Proposition 3. *Let $H \in \mathrm{Aut}(L_f)$ be a loop automorphism.*
(i) $H|_{K^\times} = \tau$ for some $\tau \in Aut(K^\times)$.
(ii) If σ has order $n \geq m - 1$ then $H(t) = kt$ for some $k \in K^\times$.

(iii) If σ has order $n \geq m-1$ then for all $i \in \{1, \ldots, m-1\}$ and $z \in K^\times$,

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

(iv) If σ has order $n \geq m-1$ then

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

for all $i \in \{1, \ldots, m\}$. In particular, $H\Big(\sum_{i=0}^{m-1} a_i t^i\Big) = k\sigma(k)\cdots\sigma^{m-1}(k)\sum_{i=0}^{m-1} a_i t^i$.

Proof. (i) Since L_f is not associative, $\mathrm{Nuc}_l(L) = K^\times$. Since any automorphism preserves the left nucleus, $H(K^\times) = K^\times$ and so $H|_{K^\times} = \tau$ for some $\tau \in \mathrm{Aut}(K^\times)$.
(ii) Suppose $H(t) = \sum_{i=0}^{m-1} k_i t^i$ for some $k_i \in K$. Then we have

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

and

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

for all $z \in K^\times$. Comparing the coefficients of t^i in (1) and (2) we obtain

$$(3) \qquad k_i\sigma^i(\tau(z)) = k_i\tau(\sigma^i(z)) = \tau(\sigma(z))k_i = k_i\tau(\sigma(z))$$

for all $i \in \{0, \ldots, m-1\}$ and all $z \in K^\times$. This implies $k_i(\tau(\sigma^i(z)) - \tau(\sigma(z))) = 0$ for all $i \in \{0, \ldots, m-1\}$ and all $z \in K$ since σ and τ commute, i.e. $k_i = 0$ or $\tau(\sigma^i(z)) = \tau(\sigma(z))$, that means (since τ is bijective)

$$(4) \qquad\qquad k_i = 0 \text{ or } \sigma^i(z) = \sigma(z)$$

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

Since σ has order $n \geq m-1$, $\sigma^i \neq \sigma$ for all $i \in \{0, \ldots, m-1\}$, $i \neq 1$, so (4) implies $k_i = 0$ for all $i \in \{0, \ldots, m-1\}$, $i \neq 1$. Therefore $H(t) = kt$ for some $k \in K^\times$.
(iii) For all $i \in \{1, \ldots, m-1\}$ and $z \in K$,

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

(iv) By (iii) we have $H(t^i) = H(t)^i = (kt)^i = \Big(\prod_{l=0}^{i-1} \sigma^l(k)\Big)t^i$ for all $i \in \{1, \ldots, m-1\}$. Moreover, we know that $t^m = tt^{m-1}$ and $H(tt^{m-1}) = H(t)H(t^{m-1}) = H(t)H(t)^{m-1}$, i.e.

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

This gives $H(t)^m = H(t^m) = H\left(\sum_{i=0}^{m-1} a_i t^i\right) = k\sigma(k)\cdots\sigma^{m-1}(k)\sum_{i=0}^{m-1} a_i t^i$. We obtain

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

or in other words, $H(t^m) = k\sigma(k)\cdots\sigma^{m-1}(k)t^m$. □

A closer look at the proofs of [2, Theorem 4, 5] shows that these can be generalized to obtain the following statement:

Theorem 4. *(i) Let $n \geq m - 1$. Then a map $H : S_f \longrightarrow S_f$ is an automorphism of the ring S_f if and only if $H = H_{\tau,k}$ where $\tau \in \mathrm{Aut}(K)$ and*

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

with $k \in K^\times$ such that

$$(5) \qquad \tau(a_i) = \left(\prod_{l=i}^{m-1} \sigma^l(k)\right)a_i$$

for all $i \in \{0, \ldots, m-1\}$.
(ii) Let $n < m - 1$. For all $k \in K^\times$ satisfying Equation (5) the maps $H_{\tau,k}$ from (i) are automorphisms of the ring S_f and form a subgroup of $\mathrm{Aut}(S_f)$.

Corollary 5. *Let $\tau \in \mathrm{Aut}(K)$ and $k \in K^\times$ satisfy (5) for all $i \in \{0, \ldots, m-1\}$. Then*

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

is an automorphism of the multiplicative loop L_f which extends to an automorphism of the ring S_f. For all $k \in K^\times$ satisfying (5) and $\tau \in \mathrm{Aut}(K)$, the automorphisms $H_{\tau,k}$ form a subgroup of $\mathrm{Aut}(L_f)$.

Remark 6. (i) Let $n \geq m - 1$. For all $\tau \in \mathrm{Aut}_F(K^\times)$ and $k \in K^\times$ such that $\tau(a_i) = \left(\prod_{l=i}^{m-1} \sigma^l(k)\right)a_i$ for all $i \in \{0, \ldots, m-1\}$, a tedious calculation shows that

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

is only an automorphism of L_f, if τ is additive. So if there are automorphisms of L_f not induced by automorphisms of S_f, they will not have the form $H_{\tau,k}$.
(ii) Let G be a ring automorphism of $R = K[t; \sigma]$. Then for $h(t) = \sum_{i=0}^r b_i t^i \in R$ 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 $\tau \in \mathrm{Aut}(K)$ and some $k \in K^{\times}$ ([13, Lemma 1], or cf. [11, p. 75]). The automorphisms $H_{\tau,k}$ of $\mathrm{Aut}(L_f)$ with $\tau \in \mathrm{Aut}(K)$ a field automorphism are canonically induced by the automorphisms G of R which satisfy (5): It is straightforward to see that $S_f \cong S_{G(f)}$ [13, Theorem 7] and consequently, $L_f \cong L_{G(f)}$. In particular, if $k \in K^{\times}$ satisfies Equation (5) then

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

thus G induces an automorphism of L_f.

From [2, Theorem 4] we obtain analogously as in the proofs for [2, Theorems 7, 8] that the subgroups of $\mathrm{Aut}(L_f)$ that are induced by automorphisms of S_f restricted to L_f, all are subgroups induced by the automorphisms of Sandler semifields for certain f:

Proposition 7. *Let $g(t) = t^m - \sum_{i=0}^{m-1} b_i t^i \in K[t; \sigma]$ be irreducible and not right-invariant. Let*

$$f(t) = t^m - b_0 \in K[t; \sigma] \ \text{such that } b_0 \in K \setminus F$$

or more generally,

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

where $a_i \in \{0, b_i\}$ for all $i \in \{0, \dots, m-1\}$, be irreducible and not right-invariant. Then

$$\{H \in \mathrm{Aut}(L_g) \,|\, H \ \text{extends to some } H_{\tau,k} \in \mathrm{Aut}(S_g)\}$$

is a subgroup of

$$\{H \in \mathrm{Aut}(L_f) \,|\, H \ \text{extends to some } H_{\tau,k} \in \mathrm{Aut}(S_f)\}.$$

Proposition 8. *Suppose $f(t) = t^m - \sum_{i=0}^{m-1} a_i t^i \in F[t] \subset K[t; \sigma]$ is irreducible and not right-invariant.*
(i) ([2, Theorem 11]) $\langle H_{\sigma,1} \rangle \cong \mathbb{Z}/n\mathbb{Z}$ is a cyclic subgroup of $\mathrm{Aut}(L_f)$.
(ii) ([2, Corollary 20]) Suppose $a_{m-1} \in F^{\times}$. Then for all $\tau \in \mathrm{Aut}(K)$, the maps $H_{\tau,1}$ are ring automorphisms of S_f, and thus $\mathrm{Aut}(K)$ is isomorphic to a subgroup of $\mathrm{Aut}(L_f)$.
(iii) (Remark 2) The powers of t form a multiplicative group of order m in the loop L_f which has order $q^{mn} - 1$.

Example 9. Write $K = \mathbb{F}_{p^l}$, so that with $K = \mathbb{F}_{q^n}$, $q = p^r$ we have $l = nr$. For $r \neq 0$ choose

$$\sigma(x) = x^{p^r},$$

i.e. $\text{Fix}(\sigma) = \mathbb{F}_{p^r} = F$ and σ has order n. Let $K^\times = \langle \alpha \rangle$ and m be a prime divisor of $p^{\gcd(r,l)} - 1 = p^r - 1$. Then there is some $a \in K^\times$ such that $K[t;\sigma]/K[t;\sigma](t^m - a)$ is a proper semifield if and only if

$$\gcd\big((p^l - 1)(p^r - 1), (p^{mr} - 1)\big) > p^r - 1.$$

These $a \in K^\times$ are given by $a = \alpha^u$ for any $u \notin \mathbb{Z}(p^{mr} - 1)(p^r - 1)^{-1}$.

For $m = 2, 3$, the assumption that m divides $p^r - 1$ is not needed. Note that for

$$(p, m) \in \{(11, 5), (29, 7), (67, 11), \dots \}$$

where $p = 1 \mod m$ and where $l = nr$ is a multiple of m, sufficient conditions are easier to find ([18, (22)]). This way we obtain loops of order $|K|^m - 1 = p^{mnr} - 1$ with left and middle nucleus $\mathbb{F}_{p^l} \cdot 1$ and center $\mathbb{F}_{p^r} \cdot 1$. For $n \geq m$ these are the multiplicative loops of Sandler semifields. Using the results on the automorphisms of S_f for $f(t) = t^m - a$ in [2] (cf. also [1, Corollary 5.32]) or simply a straightforward calculation, we can conclude the following: Let $s = (p^{rm} - 1)/(p^r - 1)$. If ω is an sth root of unity in K, then $H_{id,\omega} \in \text{Aut}(S_f)$ and the subgroup of automorphisms $\langle H_{id,\omega} \rangle$ is isomorphic to the cyclic subgroup in $K^\times$ of all the sth roots of unity in K, which has

$$S(r, m, l) = \gcd\Big(\frac{p^{rm} - 1}{p^r - 1}, p^l - 1\Big)$$

elements. Therefore there are at least $S(r, m, l)$ distinct automorphisms of L_f of the form $H_{id,k}$ with k an sth root of unity, which form a subgroup of $\text{Aut}(L_f)$. In particular we have:

(i) If $p \equiv 1 \mod m$ then $S(r, m, l) \geq m$ and so there are at least m automorphisms of L_f of the form $H_{id,k}$, which form a subgroup of $\text{Aut}(L_f)$.

(ii) Suppose l is even and at least one of r, m is also even. Then if $p \equiv -1 \mod m$, there are at least m automorphisms of L_f of the form $H_{id,k}$, which form a subgroup of $\text{Aut}(L_f)$.

(iii) Suppose p is odd and $m = 2$. Then $\text{Aut}(L_f)$ is not trivial by (i).

Example 10. Suppose $K = \mathbb{F}_{11^2}$ and $\sigma(x) = x^{11}$. Then σ has order $n = 2$. Write $K^\times = \langle \alpha \rangle$ and choose $a = \alpha^{12}$, then for $f(t) = t^5 - a$,

$$S_f = K[t;\sigma]/K[t;\sigma](t^5 - a)$$

is a proper semifield over $F = \mathbb{F}_{11}$, where the powers of t form a multiplicative group [18, (22)]. Its multiplicative loop has order $11^{10} - 1$, left and middle nucleus $(\mathbb{F}_{11^2})^\times \cdot 1$ and right nucleus isomorphic to $\big(\mathbb{F}_{11}[t]/(t^5 - a)\big)^\times \cong (\mathbb{F}_{11^5})^\times$. Thus its nucleus is $(\mathbb{F}_{11})^\times \cdot 1$ and equals its center. It has a subgroup of order 5 generated by t and is clearly not weak Lagrangian. Its automorphism group contains $\langle H_{\sigma,1} \rangle \cong \mathbb{Z}/2\mathbb{Z}$ as a subgroup (Proposition 8). It also contains at least 5 automorphisms of the form

$H_{id,k}$ by Example 9 (iii). Since the nucleus of L_f equals its center, there are no non-trivial inner mappings of L_f induced by inner automorphisms of S_f and

$$11^{45}(11^9 - 1) \cdots (11^2 - 1) \le |\mathrm{Inn}(L_f)| \le 11^{45}(11^9 - 1) \cdots (11^2 - 1)10;$$

see the next Section.

Example 11. Let $f(t) = t^2 - a_1 t - a_0 \in K[t; \sigma]$ be irreducible and not right-invariant. Then S_f is a *Hughes-Kleinfeld semifield*. L_f is a loop of order $q^{2n} - 1$ with left and middle nucleus $K^\times \cdot 1 = \mathbb{F}_{q^n}^\times \cdot 1$ and right nucleus $\mathbb{F}_{q^2}^\times \cdot 1$. For $a_0, a_1 \in F^\times$, $\mathrm{Aut}(S_f) \cong \mathbb{Z}/n\mathbb{Z}$, so $\mathrm{Aut}(L_f)$ contains a cyclic subgroup of order n. (If $a_0 \in K \setminus F$ and $a_1 \in F^\times$ then $\mathrm{Aut}(S_f)$ is trivial.) We know that $f(t) = t^2 - a_1 t - a_0 \in K[t; \sigma]$ is irreducible if and only if $z\sigma(z) + a_1 z - a_0 = 0$ has no solutions in K (e.g. see [18, (17)]). If σ has order 2 and $a_1 \ne 2$, then $f(t) = t^2 - a_1 t - a_0 \in F[t]$ is irreducible in $K[t; \sigma]$ if and only if it is irreducible in $F[t]$ [18, (23)].

Example 12. Let $F = \mathbb{F}_5$ and $K = \mathbb{F}_{5^3}$, with σ generating the Galois group of K/F. Let $f(t) = t^2 - 2 \in K[t; \sigma]$. The multiplicative loop L_f of the Hughes-Kleinfeld semifield S_f has order $5^6 - 1 = 15\,624$ with left and middle nucleus $\mathbb{F}_{5^3}^\times \cdot 1$ and right nucleus $\mathbb{F}_{25}^\times \cdot 1$. By [23, Example 16], $\mathrm{Aut}(L_f)$ contains a cyclic subgroup of order 6.

3. Inner automorphisms

Let $f \in K[t; \sigma]$ have degree m, and be monic, irreducible and not right-invariant.

Because of $|\mathrm{Inn}(L_f)| = |\mathrm{Mlt}(L_f)|/(q^{mn} - 1)$, the size of the inner mapping group is bounded by

$$q^{mn(mn-1)/2}(q^{mn-1} - 1) \cdots (q^2 - 1) \le |\mathrm{Inn}(L_f)| \le q^{mn(r-1)/2}(q^{mn-1} - 1) \cdots (q - 1);$$

cf. Section 1.3. In particular, for $q = 2$, we get $|\mathrm{Inn}(L_f)| = 2^{mn(mn-1)/2}(2^{mn-1} - 1) \cdots (2^2 - 1)$. If the semifield $A = K[t; \sigma]/K[t; \sigma]f$ has a nucleus which is larger than its center $F \cdot 1$, then the inner automorphisms $\{G_c \,|\, 0 \ne c \in \mathrm{Nuc}(A)\}$ with $G_c(x) = cxc^{-1}$ form a non-trivial subgroup of $\mathrm{Aut}_F(A)$ [23, Lemma 2, Theorem 3] and each such inner automorphism G_c extends $id_{\mathrm{Nuc}(A)}$. In particular, the elements in $\{G_c \,|\, 0 \ne c \in \mathrm{Nuc}(A)\}$ are middle inner mappings T_c and $\{G_c \,|\, 0 \ne c \in \mathrm{Nuc}(A)\}$ is a non-trivial subgroup of loop isomorphisms in $\mathrm{Inn}(L_f)$.

[3, Proposition 8] yields immediately:

Proposition 13. *Suppose* $N = \mathrm{Nuc}(L_f) \cong \mathbb{F}_{q^l}^\times$ *for some integer* $1 < l \le n$. *Then* L_f *has*

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

inner automorphisms which extend to an inner automorphism of S_f *and thus all are middle inner mappings. They are determined by the* q^l *elements in its nucleus that*

do not lie in F and are all extensions of id_N.

In particular, if L_f has nucleus $K^\times \cdot 1$ then there are exactly

$$s = (q^n - 1)/(q - 1)$$

inner automorphisms of L_f which extend to an inner automorphism of S_f and thus are middle inner mappings. All extend $id_{K^\times}$ and have the form $H_{id,k}$ for a suitable $k \in K^\times$.

[3, Proposition 9] yields:

Proposition 14. *Let $n \geq m - 1$. Then there exist at most*

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

distinct inner automorphisms of L_f that extend to $H_{id,k}$ such that $N_{K/F}(k) = 1$. These are middle inner mappings on L_f.

Proposition 14 and Proposition 13 imply the following estimates for the number of middle inner mappings T_c that are inner automorphisms of L_f:

Theorem 15. *Let $n \geq m - 1$. If L_f has nucleus $K^\times \cdot 1$ then it has at least $s = (q^n - 1)/(q - 1)$ inner automorphisms extending $id_{K^\times}$. These form a cyclic subgroup of $\mathrm{Aut}(L_f)$ isomorphic to $\ker(N_{K/F})$, and a cyclic subgroup of middle inner mappings in $\mathrm{Inn}(L_f)$ isomorphic to $\ker(N_{K/F})$.*

Hence if $N = \mathrm{Nuc}(L_f) = \mathbb{F}_{q^l}^\times \cdot 1$, is strictly contained in $K^\times$, $l > 1$, then L_f has at least t inner automorphisms extending id_N, with

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

These are middle inner mappings on L_f.

Corollary 16. *Let $n \geq m - 1$ and assume that L_f has nucleus $K^\times \cdot 1$. Then*

$$|\{T_c \in \mathrm{Inn}(L_f) \,|\, T_c \text{ automorphism}\}| \geq \frac{q^n - 1}{q - 1}.$$

Example 17. As in Example 9, write $K = \mathbb{F}_{p^l}$, so that $q = p^r$ with $l = nr$, and for $r \neq 0$ choose $\sigma(x) = x^{p^r}$, i.e. $\mathrm{Fix}(\sigma) = \mathbb{F}_{p^r} = F$ and σ has order n. Let $f(t) = t^m - a$. By a straightforward calculation (cf. also [1, Section 5]) we obtain immediately:

(i) If $c \in K^\times$ is a primitive $(p^{rm} - 1)$th root of unity, then G_c is an inner automorphism of L_f.

(ii) If $p^{\gcd(rm,l)} > p^{\gcd(r,l)}$, then there exists a non-trivial inner automorphism G_c in L_f for some $(p^{rm} - 1)$th root of unity $c \in K^\times$, which is not a $(p^r - 1)$th root of unity.

(iii) Suppose $rm \,|\, l$. Then K contains a primitive $(p^{rm} - 1)$th root of unity c and $\mathrm{Aut}(L_f)$ has a cyclic subgroup $\langle G_c \rangle$ of inner automorphisms of order $s = (p^{rm} - 1)/(p^r - 1)$.

4. NONASSOCIATIVE CYCLIC ALGEBRAS

4.1. An algebra S_f with $f(t) = t^m - a \in K[t; \sigma]$ irreducible, $a \in K \setminus F$ and $n \geq m$ is called a *Sandler semifield* [19]. Since $(t^{m-1}t)t = at$ and $t(t^{m-1}t) = ta = \sigma(a)t$, a Sandler semifield is not $(m+1)$th power-associative. For $m = n$, these algebras are also called *nonassociative cyclic (division) algebras of degree m* and denoted by $(K/F, \sigma, a)$, as they can be seen as canonical generalizations of associative cyclic algebras. We have

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

if and only if $\sigma^i(a) = kb$ for some $0 \leq i \leq m - 1$ and some $k \in F^\times$ [2, Corollary 34]. If the elements $1, a, a^2, \ldots, a^{m-1}$ are linearly independent over F then $(K/F, \sigma, a)$ is a semifield. In particular, if m is prime then every $a \in K \setminus F$ yields a semifield $(K/F, \sigma, a)$.

In this section let $a \in K \setminus F$ and $f(t) = t^m - a \in K[t; \sigma]$ be irreducible (i.e. a does not lie in any proper subfield of K/F), σ have order m and

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

Then $\mathrm{Nuc}_l(A^\times) = \mathrm{Nuc}_m(A^\times) = \mathrm{Nuc}_r(A^\times) = K^\times \cdot 1$. $A^\times$ 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 $\ker(N_{K/F})$. Moreover, $\mathrm{SL}(m^2, q) \leq \mathrm{Mlt}(A^\times) \leq \mathrm{GL}(m^2, q)$ implies

$$q^{m^2(m^2-1)/2}(q^{m^2} - 1)(q^{m^2-1} - 1) \cdots (q^2 - 1)$$

$$\leq |\mathrm{Mlt}(A^\times)| \leq (q^{m^2} - 1)q^{m^2(m^2-1)/2}(q^{m^2-1} - 1) \cdots (q - 1),$$

and

$$q^{m^2(m^2-1)/2}(q^{m^2-1} - 1) \cdots (q^2 - 1) \leq |\mathrm{Inn}(A^\times)| \leq q^{m^2(m^2-1)/2}(q^{m^2-1} - 1) \cdots (q - 1).$$

In particular, for $q = 2$,

$$\mathrm{Mlt}(A^\times) = 2^{m^2(m^2-1)/2}(2^{m^2} - 1)(2^{m^2-1} - 1) \cdots (2^2 - 1),$$

$$\mathrm{Inn}(A^\times) = 2^{m^2(m^2-1)/2}(2^{m^2-1} - 1) \cdots (2^2 - 1).$$

By Corollary 16 we know that $|\{T_c \in \mathrm{Inn}(A^\times) \,|\, T_c \text{ automorphism}\}| \geq s$. In other words:

Proposition 18. [3, Proposition 16] *Let α be a primitive element of K, i.e. $K^\times = \langle \alpha \rangle$. Then $\langle G_\alpha \rangle \subset \mathrm{Aut}(A^\times)$ is a cyclic subgroup of inner automorphisms of order $s = (q^m - 1)/(q - 1)$.*

Corollary 19. *For every prime number m there is a loop L of order $q^{m^2} - 1$ with center $\mathbb{F}_q^\times \cdot 1$, left, middle and right nucleus $\mathbb{F}_{q^m}^\times \cdot 1$ and a non-trivial automorphism group with a cyclic subgroup of inner automorphisms of order s.*

Proof. L is the multiplicative loop of a nonassociative cyclic division algebras of degree m over $\mathbb{F}_q$. $\qquad\square$

Example 20. There can be non-isomorphic Jha-Johnson semifields S_f of a given order q^{m^2} with different nuclei. For example consider $q = 2$ and $n = m = 4$. Then for any a not contained in any proper subfield of $\mathbb{F}_{2^4}/\mathbb{F}_2$, we have the nonassociative cyclic algebra $A = (\mathbb{F}_{2^4}/\mathbb{F}_2, \sigma, a)$ of degree 4. $A^\times$ has $2^{16} - 1$ elements, left, right and middle nucleus $\mathbb{F}_{2^4}^\times \cdot 1$ and center $\mathbb{F}_2^\times \cdot 1$,

$$|\mathrm{Mlt}(A^\times)| = 2^{16(16-1)/2}(2^{16} - 1)(2^{15} - 1) \cdots (2^2 - 1),$$

$$|\mathrm{Inn}(A^\times)| = 2^{16(16-1)/2}(2^{15} - 1) \cdots (2^2 - 1),$$

and $|\{T_c \in \mathrm{Inn}(L_f) \,|\, T_c \text{ automorphism}\}| \geq 15$. Alternatively, we can construct the multiplicative loop of a semifield with $2^{16} - 1$ elements choosing $q = 16$ and $n = m = 2$ (i.e., of a nonassociative quaternion algebra $A = (\mathbb{F}_{2^8}/\mathbb{F}_{16}, \sigma, a)$). In this case the left, middle and right nucleus is $\mathbb{F}_{2^8}^\times \cdot 1$ and the center $\mathbb{F}_{16}^\times \cdot 1$. Then we get

$$16^6(16^4 - 1)(16^3 - 1) \cdots (16^2 - 1) \leq |\mathrm{Mlt}(A^\times)| \leq 16^6(16^4 - 1)(16^3 - 1) \cdots (16^2 - 1)15,$$

$$16^6(16^3 - 1) \cdots (16^2 - 1) \leq |\mathrm{Inn}(A^\times)| \leq 16^6(16^3 - 1) \cdots (16^2 - 1)15,$$

and $|\{T_c \in \mathrm{Inn}(L_f) \,|\, T_c \text{ automorphism}\}| \geq 17$.

We obtain an upper bound on the number of non-isomorphic loops arising from the nonassociative cyclic algebras of a fixed degree m from [3, Theorem 31]:

Theorem 21. *Let $[K : F] = m$.*
(i) If m does not divide $q - 1$ then there are at most

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

non-isomorphic multiplicative loops of order $q^{m^2} - 1$ arising from nonassociative cyclic algebras $(K/F, \sigma, a)$ of degree m.
(ii) If m divides $q - 1$ and is prime then there are at most

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

non-isomorphic multiplicative loops of order $q^{m^2} - 1$ arising from nonassociative cyclic algebras $(K/F, \sigma, a)$ of degree m.

4.2. The automorphism groups. 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 $K = F(d)$ where d is a root of some $t^m - c \in F[t]$. Let $s = (q^m - 1)/(q - 1)$. The following results are implied by the theorems on the automorphism groups for the related algebras S_f [3, Theorems 19, 20]:

Theorem 22. *Let $S_f = (K/F, \sigma, a)$ where $a = \lambda d^i$ for some $i \in \{1, \ldots, m - 1\}$, $\lambda \in F^\times$.*
(a) Suppose m is odd or $(q - 1)/m$ is even. Then $\mathrm{Aut}(L_f)$ contains a subgroup isomorphic to the semidirect product

$$(7) \qquad \mathbb{Z}/\left(\frac{s}{m}\right)\mathbb{Z} \rtimes_q \mathbb{Z}/(m\mu)\mathbb{Z},$$

where $\mu = m/\gcd(i, m)$. Its automorphisms extend to automorphisms of S_f.
(b) Suppose m is prime and divides $q - 1$.

   (i) *If $m = 2$ then $\mathrm{Aut}(L_f)$ contains a subgroup isomorphic to the dicyclic group Dic_l of order $4l = 2q + 2$.*
   (ii) *If $m > 2$ then $\mathrm{Aut}(L_f)$ contains a subgroup isomorphic to the semidirect product*

$$(8) \qquad \mathbb{Z}/\left(\frac{s}{m}\right)\mathbb{Z} \rtimes_q \mathbb{Z}/(m^2)\mathbb{Z}.$$

The automorphisms in these subgroups extend to automorphisms of S_f.

Corollary 23. *Let F have characteristic not 2, K/F be a quadratic field extension and $S_f = (K/F, \sigma, a)$ a nonassociative quaternion algebra.*
(i) If $a \neq \lambda d$ for any $\lambda \in F^\times$, then $\mathrm{Aut}(L_f)$ contains a subgroup isomorphic to the cyclic group $\mathbb{Z}/(q + 1)\mathbb{Z}$. All the automorphisms in this subgroup are inner and extend to automorphisms of S_f.
(ii) If $a = \lambda d$ for some $\lambda \in F^\times$, then $\mathrm{Aut}(L_f)$ contains a subgroup isomorphic to the dicyclic group of order $2q + 2$ and all its elements extend to automorphisms of S_f.

Note that nonassociative quaternion algebras (where $m = 2$ in Theorem 22) are up to isomorphism the only proper semifields of order q^4 with center $F \cdot 1$ and nucleus containing the quadratic field extension K of F (embedded into the algebra as $K \cdot 1$ as usual) [21, Theorem 1]. For the loop L_f of a nonassociative quaternion algebra, moreover

$$q^6(q^4 - 1)(q^3 - 1)(q^2 - 1) \leq |\mathrm{Mlt}(L_f)| \leq q^6(q^4 - 1)(q^3 - 1)(q^2 - 1)(q - 1).$$

Example 24. Let $F = \mathbb{F}_2$ and let $K = \mathbb{F}_4$, then $K = \{0, 1, x, 1+x\}$ where $x^2 + x + 1 = 0$. There is up to isomorphism only one nonassociative quaternion algebra which can be constructed using K/F given by $(K/F, \sigma, x)$ [3, Example 30]. This is up

to isomorphism the only proper semifield of order 16 with center $F \cdot 1$ and nucleus containing $K \cdot 1$.

Its F-automorphism group consists of inner automorphisms and is isomorphic to $\langle G_x \rangle \cong \mathbb{Z}/3\mathbb{Z}$. Its multiplicative loop L thus has 15 elements, left, right and middle nucleus $\mathbb{F}_4^\times \cdot 1$, center $\mathbb{F}_2^\times \cdot 1$ and non-trivial automorphism group containing $\langle G_x \rangle$. L is right cyclic. The inner mapping group of L contains a cyclic subgroup of inner automorphisms isomorphic to $\mathbb{Z}/3\mathbb{Z}$ induced by the inner automophisms of the algebra. We know $|\text{Inn}(L)| = 1\,344$ and $|\text{Mlt}(L)| = 20\,160$.

Example 25. 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 exactly two non-isomorphic semifields which are nonassociative quaternion algebras with nucleus $K \cdot 1$, given by $A_1 = (K/F, \sigma, x)$ with $\text{Aut}_F(A_1) \cong \mathbb{Z}/4\mathbb{Z}$ and by $A_2 = (K/F, \sigma, x + 1)$ with $\text{Aut}_F(A_2)$ isomorphic to the group of quaternion units, the smallest dicyclic group Dic_2 (of order 8) [3, Example 32]. These are up to isomorphism the only two proper semifields of order 81 with center $F \cdot 1$ and nucleus containing $K \cdot 1$ [21, Theorem 1]. They are listed as cases (X) and (XI) in [5].

Their multiplicative loops L_1 and L_2 both have order 80, left, middle and right nucleus $\mathbb{F}_9^\times \cdot 1$ and center $\mathbb{F}_3^\times \cdot 1$. Both are left and right cyclic. Their multiplicative mapping group has $12\,130\,560$ elements and their inner mapping group has $151\,632$ elements. The automorphism group of L_1 and the inner mapping group of L_1 contain a subgroup of inner automorphisms which is isomorphic to $\mathbb{Z}/4\mathbb{Z}$, while the automorphism group of L_2 contains a subgroup of order 8 isomorphic to the group of quaternion units Dic_2, all of whose elements can be extended to automorphisms of S_f.

Example 26. Let $F = \mathbb{F}_5$ and $K = \mathbb{F}_{25} \cong \mathbb{F}_5(\sqrt{2})$. Then

$$(\mathbb{F}_5(\sqrt{2})/\mathbb{F}_5, \sigma, \sqrt{2})$$

is a nonassociative quaternion division algebra with $|\text{Aut}(L_f)| \geq 12$ and

$$(\mathbb{F}_5(\sqrt{2})/\mathbb{F}_5, \sigma, 1 + 2\sqrt{2})$$

is a nonassociative quaternion division algebra with $|\text{Aut}(L_f)| \geq 6$. The algebras are non-isomorphic [23, Example 13]. Their multiplicative loops have order $5^4 - 1 = 624$, left, middle and right nucleus $\mathbb{F}_{25}^\times \cdot 1$ and center $\mathbb{F}_5^\times \cdot 1$. Their multiplicative mapping group has $29\,016\,000\,000$ elements and their inner mapping group $46\,500\,000$ elements.

5. ISOTOPIES

Two semifields A and A' are *isotopic* if there are linear bijective maps $F, G, H : A \longrightarrow A'$ such that for all $x, y \in A$, we have $F(x)G(y) = H(xy)$. The triple (F, G, H)

is called an *isotopism*. Any isotopy of semifields canonically induces an isotopy of the multiplicative loops L and L' of A and A'.

Note that if f and g are *similar* irreducible monic polynomials of degree m, i.e. $gu \equiv 0 \bmod f$ for some $0 \neq u \in R_m$, then L_f and L_g are isotopic loops by [13, Theorem 7].

Indeed, Kantor showed that there are less than $r\sqrt{log_2(r)}$ non-isotopic semifields of order r that can be obtained through our construction [9], so that there are less than $r\sqrt{log_2(r)}$ non-isotopic loops of order $r-1$ obtained as their multiplicative loops. By [13, Section 8], we have some more upper bounds on the number of isotopic loops which can be obtained as multiplicative loops of Jha-Johnson semifields:

Let $N(q,m) = |I(q,m)|$ where

$$|I(q,m)| = \frac{1}{m}\sum_{l/m}\mu(l)q^{m/l} = \frac{q^m - \theta}{m}$$

is the number of monic irreducible polynomials of degree m in the center of R which is $\mathbb{F}_q[y] \cong \mathbb{F}_q[t^n; \sigma]$. Here, μ is the Moebius function, and θ the number of elements of $\mathbb{F}_{q^m}$ contained in a proper subfield $\mathbb{F}_{q^e}$ of $\mathbb{F}_{q^m}$. Let $A(q,n,m)$ denote the number of isotopy classes of semifields $A = K[t;\sigma]/K[t;\sigma]f(t)$ of order q^{nm} defined using $f(t) \in K[t;\sigma]$ as in the previous sections, with

$$(|C(A)|, |\mathrm{Nuc}_l(A)|, |\mathrm{Nuc}_m(A)|, |\mathrm{Nuc}_r(A)|) = (q, q^n, q^n, q^m).$$

Then

$$A(q,n,m) \leq N(q,m) = \frac{q^m - \theta}{m}$$

and, even stronger,

$$A(q,n,m) \leq M(q,m)$$

with $M(q,d)$ being the number of orbits in $I(q,m)$ under the action of the group

$$G = \Gamma L(1,q) = \{(\lambda,\rho) \mid \lambda \in \mathbb{F}_q^\times, \rho \in \mathrm{Aut}(\mathbb{F}_q)\}$$

on $I(q,m)$ defined via

$$f^{(\lambda,\rho)}(y) = \lambda^{-m}f^\rho(\lambda y).$$

For $q = p^r$ we have

$$\frac{q^m - \theta}{mr(q-1)} \leq M(q,m) \leq \frac{q^m - \theta}{m}$$

[13]. These are also upper bounds for the number of non-isotopic multiplicative loops $A^\times$ of order $q^{nm} - 1$ defined using A.

Example 27. (i) For $q = 2,3,4,5$ and $n = m = 2$ we have the tight bound $M(q,m) = 1,2,1,3$ [13] and so there is up to isotopy exactly one loop L with

$$(|C(L)|, |\mathrm{Nuc}_l(L)|, |\mathrm{Nuc}_m(L)|, |\mathrm{Nuc}_r(L)|) = (q-1, q^2-1, q^2-1, q^2-1)$$

that is the multiplicative loop of a Jha-Johnson semifield when $q = 2, 4$, and at most 2 (respectively 3) loops, when $q = 3$ (respectively 5).

When $q = 2$ this loop is given by the invertible elements in the nonassociative quaternion algebra in Example 24. When $q = 3$ (respectively, 5) there are the two non-isomorphic, and hence necessarily also non-isotopic, nonassociative quaternion algebras in Examples 25 and 26. It is not clear if the corresponding two multiplicative loops are isotopic or not.

(ii) If $q = p$ and $gcd(p - 1, m) = 1$ then

$$M(p, m) = \frac{N(p, m)}{(p - 1)} = \frac{q^m - \theta}{m(p - 1)}$$

and so there are at most $(q^m - \theta)(m(p - 1))$ non-isotopic loops L of order $p^{mn} - 1$ with

$$(|C(L)|, |\mathrm{Nuc}_l(L)|, |\mathrm{Nuc}_m(L)|, |\mathrm{Nuc}_r(L)|) = (p - 1, p^n - 1, p^n - 1, p^m - 1)$$

which arise as the multiplicative loop of a Jha-Johnson semifield.

We conclude by noting that it would be interesting to also obtain lower bounds for the number of isotopy classes of loops arising from this construction.

REFERENCES

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

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

[3] C. Brown, S. Pumplün, A. Steele, *Automorphisms and isomorphisms of Jha-Johnson semifields obtained from skew polynomial rings.* To appear in Comm. Algebra. Online at arXiv:1703.02356v2 [math.RA]

[4] M. Cordero, V. Jha, *On the multiplicative structure of quasifields and semifields: cyclic and acyclic loops.* Note Mat. 29 (1) (2009), 45-58.

[5] U. Dempwolff, *Semifield planes of order 81.* J. Geom. 89 (2008), 1-2, 1-16.

[6] I. R. Hentzel, I. F. Rúa, *Primitivity of finite semifields with 64 and 81 elements.* Internat. J. Algebra Comput. 17 (7) (2007), 1411-1429.

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

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

[9] W. M. Kantor, R. A. Liebler, *Semifields arising from irreducible semilinear transformations.* J. Aust. Math. Soc. 85 (3) (2008), 333-339.

[10] J. Kirshtein, *Multiplication groups and inner mapping groups of Cayley-Dickson loops.* J. Algebra Appl. 13 (1) (2014), 26 pages.

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

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

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

[14] B. D. McKay, I. M. Wanless, *On the number of Latin squares.* Ann. Comb. 9 (3) (2005), 335-344.

[15] G. P. Nagy, *Semifields in loop theory and in finite geometry.* Quasigroups Related Systems 19 (1) (2011), 109-122.

[16] G. P. Nagy, *On the multiplication groups of semifields.* European J. Combin. 31 (1) (2010), 18-24. 12K10 (20N05)

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

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

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

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

[22] 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.

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

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

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