# NONASSOCIATIVE CYCLIC EXTENSIONS OF FIELDS AND CENTRAL SIMPLE ALGEBRAS

C. BROWN AND S. PUMPLÜN

ABSTRACT. We define nonassociative cyclic extensions of degree m of both fields and central simple algebras over fields. If a suitable field contains a primitive mth (resp., qth) root of unity, we show that suitable nonassociative generalized cyclic division algebras yield nonassociative cyclic extensions of degree m (resp., qs). Some of Amitsur's classical results on non-commutative associative cyclic extensions of both fields and central simple algebras are obtained as special cases.

### INTRODUCTION

Analogously as both for commutative field extensions [6, 2, 3, 26] and for associative cyclic extensions of fields and central simple algebras [5], nonassocative cyclic extensions of degree m of a field or a central division algebra are investigated separately for prime characteristics and for the case that the characteristic is zero or a prime p with gcd(p,m) = 1. Nonassociative cyclic extensions of degree p in characteristic p were already studied in [18].

Let D be a finite-dimensional central division algebra over a field K. An (associative) central division algebra A over a field F is called a non-commutative cyclic extension of degree m of D over K, if  $\operatorname{Aut}_F(A)$  has a cyclic subgroup of automorphisms of order m which are all extended from  $id_D$ , and if A is a free left D-module of rank m [5]. For instance, if F contains a primitive mth root of unity, then generalized cyclic algebras  $(D, \sigma, a)$  are cyclic extensions of D of degree m [5, Theorem 6]. We recall that a generalized cyclic algebra  $(D,\sigma,a)$  is a quotient algebra  $D[t;\sigma]/(t^m - a)D[t;\sigma]$ , where  $D[t;\sigma]$  is a twisted polynomial ring,  $\sigma \in \operatorname{Aut}(D)$  is an automorphism such that  $\sigma|_K$  has finite order m,  $F_0 = \operatorname{Fix}(\sigma) \cap K$ , and  $f(t) = t^m - a \in D[t;\sigma]$  with  $d \in F_0^{\times}$ . The special case where D = F and  $F_0 = \operatorname{Fix}(\sigma)$  yields the cyclic algebra  $(F/F_0, \sigma, a)$  [12, p. 19].

A finite-dimensional central simple algebra A over F is called a G-crossed product if it contains a maximal field extension K/F which is Galois with Galois group G = Gal(K/F). If G is solvable then A is called a solvable G-crossed product. In [9] we revisited a result by Albert [1] on solvable crossed products and gave a proof for Albert's result using generalized cyclic algebras following Petit's approach [17], proving that a G-crossed product is solvable if and only if it can be constructed as a chain of generalized cyclic algebras. Hence any solvable G-crossed product division algebra is always a generalized cyclic division algebra. In particular, hence if F contains a primitive mth root of unity, solvable crossed product division algebras over F are non-commutative cyclic extensions.

<sup>2010</sup> Mathematics Subject Classification. Primary: 17A35; Secondary: 17A60, 16S36.

Key words and phrases. Skew polynomial, Ore polynomial, cyclic algebra, cyclic extension.

A generalization of associative cyclic extensions of simple rings instead of division rings was considered in [13].

In this paper, we define and investigate nonassociative cyclic extensions of degree m of both fields and central simple algebras employing nonassociative generalized cyclic division algebras: Let A be a unital nonassociative division algebra. Then A is called a *nonassociative* cyclic extension of D of degree m, if A is a free left D-module of rank m and Aut(A) has a cyclic subgroup G of order m, such that for all  $H \in G$ ,  $H|_D = id_D$ .

We show that if F contains a primitive mth root of unity (i.e., F has characteristic 0 or characteristic p with gcd(m,p) = 1), then the nonassociative generalized cyclic division algebras  $(D, \sigma, a) = D[t; \sigma]/(t^m - a)D[t; \sigma]$  with  $a \in D^{\times}$  are nonassociative cyclic extensions of D of degree m. Additionally, the subgroup of order m in  $\operatorname{Aut}_{F_0}(D, \sigma, a)$  that consists of automorphisms extending  $id_D$  contains only inner automorphisms (Corollary 10). We also investigate the structure of the automorphism groups of nonassociative generalized cyclic algebras in general.

Note that nonassociative cyclic division algebras  $(K/F, \sigma, a)$  are a special case of nonassociative generalized cyclic division algebras. If F contains a primitive mth root of unity the nonassociative cyclic division algebras  $(K/F, \sigma, a)$  are nonassociative cyclic extensions of Kof degree m. The subgroup of the automorphisms extending  $id_K$  has order m, is isomorphic to ker $(N_{K/F})$ , and contains only inner automorphisms. If F has no non-trivial mth root of unity and  $a \in K^{\times}$  is not contained in any proper subfield of K, all automorphisms of  $(K/F, \sigma, a)$  are inner and leave  $id_K$  fixed (Theorem 3).

We point out that nonassociative generalized cyclic algebras have been recently successfully used both in constructing space-time block codes and linear codes [19, 20, 21, 22].

The paper is organized as follows: After introducing the basic terminology in Section 1, we define nonassociative cyclic extensions and nonassociative generalized cyclic algebras in Section 2 and investigate nonassociative cyclic extensions of a field. In Section 3 we show when generalized cyclic division algebras  $(D, \sigma, d)$  are nonassociative cyclic extensions of Dof degree m. We briefly look at the question when a nonassociative overring is a nonassociative cyclic extension of a field or a central simple algebra in Section 4.

The results presented in this paper complements the ones for the nonassociative algebras  $(K, \delta, d) = K[t; \delta]/K[t; \delta]f(t)$  for  $f(t) = t^p - t - d \in K[t; \delta]$  constructed using a field K of characteristic p together with some derivation  $\delta$  with minimum polynomial  $g(t) = t^p - t \in F[t]$ ,  $F = \text{Const}(\delta)$ , and of the nonassociative algebras  $(D, \delta, d) = D[t; \delta]/D[t; \delta]f(t)$  for  $f(t) = t^p - t - d \in D[t; \delta]$  constructed using a division algebra D, where the derivation  $\delta$  has minimum polynomial  $g(t) = t^p - t \in F[t]$  and the field F characteristic p. [18].

### 1. Preliminaries

1.1. Nonassociative algebras. Let F be a field and let A be an F-vector space. A is an algebra over F if there exists an F-bilinear map  $A \times A \to A$ ,  $(x, y) \mapsto x \cdot y$ , denoted simply by juxtaposition xy, the multiplication of A. An algebra A is called *unital* if there is an

element in A, denoted by 1, such that 1x = x1 = x for all  $x \in A$ . We will only consider unital algebras 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  $\operatorname{Nuc}_{l}(A) = \{x \in A \mid [x, A, A] = 0\}$ , the middle nucleus of A is  $\operatorname{Nuc}_{m}(A) = \{x \in A \mid [A, x, A] = 0\}$  and the right nucleus of A is  $\operatorname{Nuc}_{r}(A) = \{x \in A \mid [A, A, x] = 0\}$ .  $\operatorname{Nuc}_{l}(A)$ ,  $\operatorname{Nuc}_{m}(A)$ , and  $\operatorname{Nuc}_{r}(A)$  are associative subalgebras of A. Their intersection  $\operatorname{Nuc}(A) = \{x \in A \mid [x, A, A] = [A, x, A] = 0\}$  is the nucleus of A.  $\operatorname{Nuc}(A)$  is an associative subalgebra of A containing F1 and x(yz) = (xy)z whenever one of the elements x, y, z lies in  $\operatorname{Nuc}(A)$ . The center of A is  $\operatorname{C}(A) = \{x \in A \mid x \in \operatorname{Nuc}(A) \text{ and } xy = yx \text{ for all } y \in A\}$ .

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 [24, pp. 15, 16]. An element  $0 \neq a \in A$  has a *left inverse*  $a_l \in A$ , if  $R_a(a_l) = a_l a = 1$ , and a *right inverse*  $a_r \in A$ , if  $L_a(a_r) = aa_r = 1$ . If  $m_r = m_l$  then we denote this element by  $m^{-1}$ .

An automorphism  $G \in \operatorname{Aut}_F(A)$  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 such an automorphism by  $G_m$ . The set of inner automorphisms  $\{G_m \mid m \in \operatorname{Nuc}(A) \text{ invertible}\}$  is a subgroup of  $\operatorname{Aut}_F(A)$ . Note that if the nucleus of A is commutative, then for all  $0 \neq n \in \operatorname{Nuc}(A)$ ,  $G_n(x) = (n^{-1}x)n = n^{-1}xn$  is an inner automorphism of A such that  $G_n|_{\operatorname{Nuc}(A)} = id_{\operatorname{Nuc}(A)}$ .

1.2. Division algebras obtained from twisted polynomial rings. Let D be a unital division ring and  $\sigma$  a ring automorphism of D. The twisted polynomial ring  $D[t;\sigma]$  is the set of polynomials  $a_0 + a_1t + \cdots + a_nt^n$  with  $a_i \in D$ , where addition is defined term-wise and multiplication by  $ta = \sigma(a)t$   $(a \in D)$  [16]. That means,  $at^nbt^m = a\sigma^n(b)t^{n+m}$  and  $t^n a = \sigma^n(a)t^n$  for all  $a, b \in D$  [12, p. 2].  $R = D[t;\sigma]$  is a left principal ideal domain and there is a right division algorithm in R, i.e. for all  $g, f \in R, f \neq 0$ , there exist unique  $r, q \in R$  such that deg $(r) < \deg(f)$  and g = qf + r [12, p. 3]. (Our terminology is the one used by Petit [17] and different from Jacobson's [12], who calls what we call right a left division algorithm and vice versa.)

An element  $f \in R$  is *irreducible* in R if it is no unit and it has no proper factors, i.e there do not exist  $g, h \in R$  such that f = gh [12, p. 11].

Let  $f \in D[t; \sigma]$  be of degree m and let  $\text{mod}_r f$  denote the remainder of right division by f. Then the vector space  $R_m = \{g \in D[t; \sigma] | \deg(g) < m\}$  together with the multiplication

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

becomes a unital nonassociative algebra  $S_f = (R_m, \circ)$  over  $F_0 = \{z \in D \mid zh = hz \text{ for all } h \in S_f\}$  (cf. [17, (7)]), and  $F_0$  is a subfield of D. We also denote this algebra R/Rf.

We note that when  $\deg(g)\deg(h) < m$ , the multiplication of g and h in  $S_f$  is the same as the multiplication of g and h in R [17, (10)].

A twisted polynomial  $f \in R$  is right-invariant if  $fR \subset Rf$ . If f is right invariant then Rf is a two-sided ideal and conversely, every two-sided ideal in R arises this way.

 $S_f$  is associative if and only if f is right-invariant. In that case,  $S_f$  is the usual quotient algebra  $D[t; \delta]/(f)$  [17, (9)].

## 2. Nonassociative generalized cyclic algebras and nonassociative cyclic extensions

In the following, let D be a division algebra which is finite-dimensional over its center F = C(D) and  $\sigma \in Aut(D)$  such that  $\sigma|_F$  has finite order m and fixed field  $F_0 = Fix(\sigma) \cap F$ . Note that  $F/F_0$  is automatically a cyclic Galois field extension of degree m with  $Gal(F/F_0) = \langle \sigma|_F \rangle$ .

2.1. Following Jacobson [12, p. 19], an (associative) generalized cyclic algebra is an associative algebra  $S_f = D[t;\sigma]/D[t;\sigma]f$  constructed using a right-invariant twisted polynomial

$$f(t) = t^m - d \in D[t;\sigma]$$

with  $d \in F_0^{\times}$ . We write  $(D, \sigma, d)$  for this algebra. If D is a central simple algebra over F of degree n, then  $(D, \sigma, d)$  is a central simple algebra over  $F_0$  of degree mn and the centralizer of D in  $(D, \sigma, d)$  is F [12, p. 20]. In particular, if D = F,  $F/F_0$  is a cyclic Galois extension of degree m with Galois group generated by  $\sigma$  and  $f(t) = t^m - d \in F[t; \sigma]$ , we obtain the cyclic algebra  $(F/F_0, \sigma, d)$  of degree m.

This definition generalizes to nonassociative algebras as follows:

**Definition 1.** A nonassociative generalized cyclic algebra of degree mn is an algebra  $S_f = D[t;\sigma]/D[t;\sigma]f$  over  $F_0$  with  $f(t) = t^m - d \in D[t;\sigma], d \in D^{\times}$ . We denote this algebra by  $(D,\sigma,d)$ .

The algebra  $A = (D, \sigma, d), d \in D^{\times}$ , has dimension  $m^2 n^2$  over  $F_0$ . In particular, if D = Fand  $F/F_0$  is a cyclic Galois extension of degree m with Galois group generated by  $\sigma$ , then  $(F/F_0, \sigma, d)$  is a nonassociative cyclic algebra [25]. A is associative if and only if  $d \in F_0$ . If  $(D, \sigma, d)$  is not associative then  $\operatorname{Nuc}_l(A) = \operatorname{Nuc}_m(A) = D$  and  $\operatorname{Nuc}_r(A) = \{g \in S_f \mid fg \in Rf\}$ .

 $(D, \sigma, d)$  is a division algebra over  $F_0$  if and only if  $f(t) = t^m - d \in D[t; \sigma]$  is irreducible [17, (7)]. Moreover, we know that  $f(t) = t^2 - d \in D[t; \sigma]$  is irreducible if and only if  $\sigma(z)z \neq d$ for all  $z \in D$ ,  $f(t) = t^3 - d \in D[t; \sigma]$  is irreducible if and only if  $d \neq \sigma^2(z)\sigma(z)z$  for all  $z \in D$ , and  $f(t) = t^4 - d \in D[t; \sigma]$  is irreducible if and only if

$$\sigma^2(y)\sigma(y)y+\sigma^2(x)y+\sigma^2(y)\sigma(x)\neq 0 \text{ or } \sigma^2(x)x+\sigma^2(y)\sigma(y)x\neq d$$

for all  $x, y \in D$  (cf. [17] or [19], [7, Theorem 3.19], see also [11]). More generally, if  $F_0$  contains a primitive *m*th root of unity and *m* is prime then  $f(t) = t^m - d \in D[t; \sigma]$  is irreducible if and only if  $d \neq \sigma^{m-1}(z) \cdots \sigma(z)z$  for all  $z \in D$  ([7, Theorem 3.11], see also [19, Theorem 6]).

Amitsur's definition [5] of cyclic extensions generalizes to the nonassociative setting as follows:

**Definition 2.** Let  $m \ge 2$ . Let A be a nonassociative division algebra with center  $F_0$  and D an associative division algebra with center F. Then A is a nonassociative cyclic extension of D of degree m, if A is a free left D-module of rank m and Aut(A) has a cyclic subgroup G of order m, such that for all  $H \in G$ ,  $H|_D = id$ .

2.2. Nonassociative cyclic extensions of a field. For a nonassociative cyclic algebra  $(K/F, \sigma, d)$  of degree m, and for all  $k \in K$  such that  $N_{K/F}(k) = 1$ , the map

$$H_{id,k}(\sum_{i=0}^{m-1}a_{i}t^{i}) = a_{0} + \sum_{i=1}^{m-1}a_{i}\big(\prod_{l=0}^{i-1}\sigma^{l}(k)\big)t^{i}$$

is an inner *F*-automorphism of  $(K/F, \sigma, d)$  extending  $id_K$ . The subgroup generated by the automorphisms  $H_{id,k}$  is isomorphic to ker $(N_{K/F})$  [8, Theorem 19].

The maps  $H_{id,k}$  are the only *F*-automorphisms of  $(K/F, \sigma, d)$ , unless for some  $j \in \{1, \ldots, m-1\}$ ,  $\sigma^j$  can be extended to an *F*-automorphism of  $(K/F, \sigma, d)$  as well. More precisely, the automorphism  $\tau = \sigma^j$  with  $j \in \{1, \ldots, m-1\}$  can be extended to an *F*-automorphism *H* of  $(K/F, \sigma, d)$ , if and only if there is an element  $k \in K$  such that

(1) 
$$\sigma^j(d) = N_{K/F}(k)d$$

The extension then has the form  $H = H_{\tau,k}$  with

(2) 
$$H_{\tau,k}(\sum_{i=0}^{m-1} a_i t^i) = \tau(a_0) + \sum_{i=1}^{m-1} \tau(a_i) \Big(\prod_{l=0}^{i-1} \sigma^l(k)\Big) t^i$$

[8, Theorem 4]. We then immediately get the following partial generalization of [5, Theorem 6]:

**Theorem 1.** Suppose F contains a primitive mth root of unity  $\omega$ ,  $A = (K/F, \sigma, d)$  is a nonassociative cyclic division algebra of degree m over F, and  $d \in K \setminus F$ . Then A is a nonassociative cyclic extension of K of degree m. The generating automorphism of the subgroup of  $Aut_F(A)$  of order m is given by  $H_{id,\omega}$ .

*Proof.*  $\langle H_{\mathrm{id},\omega} \rangle$  is a cyclic subgroup of  $\mathrm{Aut}_F(A)$  of order m by [8, Theorem 20]. It consists of automorphisms extending  $id_K$ , therefore A is a nonassociative cyclic extension of K.  $\Box$ 

**Corollary 2.** If m is prime, F contains a primitive mth root of unity and K/F is a cyclic Galois extension of degree m, then K has a nonassociative cyclic extension of degree m.

*Proof.* Let  $d \in K \setminus F$  and suppose  $\operatorname{Gal}(K/F) = \langle \sigma \rangle$ . Then since *m* is prime, the nonassociative cyclic algebra  $A = (K/F, \sigma, d)$  is a division algebra [25, Corollary 4.5]. Thus *A* is a nonassociative cyclic extension of *K* by Theorem 1.

If F has no non-trivial mth root of unity, we obtain:

**Theorem 3.** Suppose F has no non-trivial mth root of unity. Let  $A = (K/F, \sigma, d)$  be a nonassociative cyclic algebra of degree m where  $d \in K^{\times}$  is not contained in any proper subfield of K. Then every F-automorphism of A leaves K fixed and

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

In particular, all automorphisms of A are inner.

*Proof.* Every automorphism of A has the form  $H_{id,k}$ : suppose that there exist  $j \in \{1, \ldots, m-1\}$  and  $k \in K^{\times}$  such that  $H_{\sigma^{j},k} \in \operatorname{Aut}_{F}(A)$ . This implies  $H^{2}_{\sigma^{j},k} = H_{\sigma^{j},k} \circ H_{\sigma^{j},k} \in \operatorname{Aut}_{F}(A)$  and

(3) 
$$H^{2}_{\sigma^{j},k}\left(\sum_{i=0}^{m-1} x_{i}t^{i}\right) = \sigma^{2j}(x_{0}) + \sum_{i=1}^{m-1} \sigma^{2j}(x_{i})\left(\prod_{q=0}^{i-1} \sigma^{j+q}(k)\sigma^{q}(k)\right)t^{i}.$$

Now  $H^2_{\sigma^j,k}$  must have the form  $H_{\sigma^{2j},l}$  for some  $l \in K^{\times}$ , and comparing (2) and (3) yields  $l = k\sigma^j(k)$ . Similarly,  $H^3_{\sigma^j,k} = H_{\sigma^{3j},s} \in \operatorname{Aut}_F(A)$  where  $s = k\sigma^j(k)\sigma^{2j}(k)$ . Continuing in this manner we conclude that the automorphisms  $H_{\sigma^j,k}, H_{\sigma^{2j},l}, H_{\sigma^{3j},s}, \ldots$  all satisfy (1) implying that

(4)  

$$\sigma^{j}(d) = N_{K/F}(k)d,$$

$$\sigma^{2j}(d) = N_{K/F}(k\sigma^{j}(k))d = N_{K/F}(k)^{2}d,$$

$$\vdots \qquad \vdots$$

$$d = \sigma^{nj}(d) = N_{K/F}(k)^{n}d,$$

where  $n = m/\gcd(j, m)$  is the order of  $\sigma^j$ . Note that  $\sigma^{ij}(d) \neq d$  for all  $i \in \{1, \ldots, n-1\}$  since d is not contained in any proper subfield of K. Therefore  $N_{K/F}(k)^n = 1$  and  $N_{K/F}(k)^i \neq 1$  for all  $i \in \{1, \ldots, n-1\}$  by (4), i.e.  $N_{K/F}(k)$  is a primitive *n*th root of unity, thus also an *m*th root of unity, a contradiction. This proves the assertion.  $\Box$ 

Note that if  $d \in K^{\times}$  is not contained in any proper subfield of K then  $1, d, \ldots, d^{m-1}$  are linearly independent over F and thus A is a division algebra [25]. In particular, if m is prime then  $1, d, \ldots, d^{m-1}$  are linearly independent over F. This yields for a field F of arbitrary characteristic:

**Corollary 4.** Suppose that F has no non-trivial mth root of unity. If  $d \in K^{\times}$  is not contained in any proper subfield of K (e.g. if m is prime), and ker $(N_{K/F})$  has a subgroup of order m, then any cyclic algebra  $A = (K/F, \sigma, d)$  is a cyclic extension of K of degree m.

**Example 5.** Let  $K = \mathbb{F}_{q^m}$  be a finite field,  $q = p^r$  for some prime  $p, \sigma$  an automorphism of K of order  $m \ge 2$  and  $F = \operatorname{Fix}(\sigma) = \mathbb{F}_q$ , i.e. K/F is a cyclic Galois extension of degree m with  $\operatorname{Gal}(K/F) = \langle \sigma \rangle$ . Then  $\ker(N_{K/F})$  is a cyclic group of order  $s = (q^m - 1)/(q - 1)$  and any division algebra  $(K/F, \sigma, d)$  has exactly s inner automorphisms, all of them extending  $id_K$ . The subgroup they generate is cyclic and isomorphic to  $\ker(N_{K/F})$  [10]. Hence if m divides s, which is the case if F contains a primitive mth root of unity, then there is a subgroup of automorphisms of order m extending  $id_K$  and hence  $(K/F, \sigma, d)$  is a cyclic extension of K of degree m.

## 3. Nonassociative cyclic extensions of a central simple algebra

3.1. From now until stated otherwise, let  $A = (D, \sigma, d)$  be a nonassociative generalized cyclic algebra of degree mn over  $F_0$ , for some  $d \in D \setminus F_0$ . We first determine the automorphisms of A:

**Theorem 6.** (i) Suppose  $\tau \in \operatorname{Aut}_{F_0}(D)$  commutes with  $\sigma$ . Then  $\tau$  can be extended to an automorphism  $H \in \operatorname{Aut}_{F_0}(A)$ , if and only if there is some  $k \in F^{\times}$  such that  $\tau(d) = N_{F/F_0}(k)d$ . In that case, the extension H of  $\tau$  has the form  $H = H_{\tau,k}$  with

$$H_{\tau,k}(\sum_{i=0}^{m-1} a_i t^i) = \tau(a_0) + \sum_{i=1}^{m-1} \tau(a_i) \Big(\prod_{l=0}^{i-1} \sigma^l(k)\Big) t^i.$$

All maps  $H_{\tau,k}$  where  $\tau \in \operatorname{Aut}_{F_0}(D)$  commutes with  $\sigma$  and where  $k \in F^{\times}$  such that  $\tau(d) = N_{F/F_0}(k)d$  (hence  $N_{F/F_0}(k)^{mn} = 1$ ), are automorphisms of A.

In particular, for  $\tau \neq id$  and  $d \notin \operatorname{Fix}(\tau)$ ,  $N_{F/F_0}(k) \neq 1$ .

(ii)  $id \in \operatorname{Aut}(D)$  can be extended to an automorphism  $H \in \operatorname{Aut}_{F_0}(A)$ , if and only if there is some  $k \in F^{\times}$  such that  $N_{F/F_0}(k) = 1$ . In that case, the extension H of id has the form  $H = H_{id,k}$  with

$$H_{id,k}(\sum_{i=0}^{m-1} a_i t^i) = a_0 + \sum_{i=1}^{m-1} a_i \left(\prod_{l=0}^{i-1} \sigma^l(k)\right) t^i.$$

All  $H_{id,k}$  where  $k \in F^{\times}$  such that  $N_{F/F_0}(k) = 1$  are automorphisms of A.

*Proof.* (i) Let  $H \in \operatorname{Aut}_{F_0}(A)$ , then  $H|_D \in \operatorname{Aut}_{F_0}(D)$ , since H leaves the left nucleus invariant. Thus  $H|_D = \tau$  for some  $\tau \in \operatorname{Aut}_{F_0}(D)$ . Write  $H(t) = \sum_{i=0}^{m-1} k_i t^i$  for some  $k_i \in D$ , then we have

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

and

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

for all  $z \in D$ . Comparing the coefficients of  $t^i$  yields

$$k_i \sigma^i(\tau(z)) = k_i \tau(\sigma^i(z)) = \tau(\sigma(z)) k_i \text{ for all } i = \{0, \dots, m-1\}$$

for all  $z \in D$  since  $\sigma$  and  $\tau$  commute. In particular, we obtain

$$k_i(\tau(\sigma^i(z)) - \tau(\sigma(z))) = 0 \text{ for all } i \in \{0, \dots, m-1\}$$

for all  $z \in F$ , i.e.  $k_i = 0$  or  $\sigma|_F = \sigma^i|_F$  for all  $i \in \{0, \ldots, m-1\}$ . As  $\sigma|_F$  has order m, this means  $k_i = 0$  for all  $1 \neq i \in \{0, \ldots, m-1\}$ . For i = 1, this yields  $k_1\tau(\sigma(z)) = \tau(\sigma(z))k_1$  for all  $z \in D$ , hence  $k_1 \in F$ . This implies H(t) = kt for some  $k \in F^{\times}$ .

Since

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

for all  $i \in \{1, \ldots, m-1\}$  and all  $z \in D$ , H has the form

$$H_{\tau,k}: \sum_{i=0}^{m-1} a_i t^i \mapsto \tau(a_0) + \sum_{i=1}^{m-1} \tau(a_i) \big(\prod_{l=0}^{i-1} \sigma^l(k)\big) t^i,$$

for some  $k \in F^{\times}$ .

Comparing the constant terms in  $H(t)^m = H(t^m) = H(d)$  implies

$$\tau(d) = k\sigma(k) \cdots \sigma^{m-1}(k)d = N_{F/F_0}(k)d$$

Let  $N = N_{F/F_0} \circ N_{D/F}$  be the norm of the  $F_0$ -algebra D. Applying N to both sides of the equation yields  $N(d) = N(k)^m N(d)$ , so that  $N(k)^m = 1$ . Now  $k \in F^{\times}$  and D has degree n, thus

$$N(k) = N_{F/F_0}(N_{D/F}(k)) = N_{F/F_0}(k^n) = N_{F/F_0}(k)^n,$$

and so  $N(k)^m = N_{F/F_0}(k)^{nm} = 1.$ 

Finally, the fact that the maps  $H_{\tau,k}$  are automorphisms when  $\tau$  commutes with  $\sigma$ , and  $\tau(d) = N_{F/F_0}(k)d$ , can be shown similarly to the proof of [8, Theorem 4], see also [7]. (ii) In particular, for  $\tau = id$ , we get from (i) that H has the form

$$H_{id,k} : \sum_{i=0}^{m-1} a_i t^i \mapsto a_0 + \sum_{i=1}^{m-1} a_i \Big(\prod_{l=0}^{i-1} \sigma^l(k)\Big) t^i$$

for some  $k \in F^{\times}$  with  $k\sigma(k) \cdots \sigma^{m-1}(k) = N_{F/F_0}(k) = 1$ .

The above is proved for a more general set-up in the first author's PhD thesis [7]. Note that the automorphisms  $H_{\tau,k}$  are restrictions of automorphisms of the twisted polynomial ring  $D[t;\sigma]$ .

**Corollary 7.** (i) The subgroup of  $F_0$ -automorphisms of A extending  $id_D \in Aut_{F_0}(D)$  is isomorphic to

$$\{k \in F^{\times} \mid k\sigma(k) \cdots \sigma^{m-1}(k) = 1\}.$$

(ii) If  $F_0$  contains a primitive mth root of unity  $\omega$ , then  $\langle H_{id,\omega} \rangle$  is a cyclic subgroup of  $\operatorname{Aut}_{F_0}(A)$  of order m.

3.2. We obtain the following generalization of [5, Theorem 6]:

**Corollary 8.** Suppose  $F_0$  contains a primitive mth root of unity. If  $f(t) = t^m - d \in D[t; \sigma]$  is irreducible, then A is a nonassociative cyclic extension of D of degree m. In particular, if m is prime and

$$d \neq \sigma^{m-1}(z) \cdots \sigma(z) z$$

for all  $z \in D$ , then A is a nonassociative cyclic extension of D of degree m.

*Proof.* If  $F_0$  contains a primitive *m*th root of unity  $\omega$ , then  $\langle H_{id,\omega} \rangle$  is a cyclic subgroup of  $\operatorname{Aut}_{F_0}(A)$  of order *m* by Corollary 7 (ii). If *m* is prime, then  $f(t) = t^m - d \in D[t;\sigma]$  is irreducible if and only if

$$d \neq \sigma^{m-1}(z) \cdots \sigma(z) z$$

for all  $z \in D$ . The rest is trivial.

**Proposition 9.** Every automorphism  $H_{id,k}$  of A is an inner automorphism

$$G_c(\sum_{i=0}^{m-1} a_i t^i) = (c^{-1} \sum_{i=0}^{m-1} a_i t^i)c$$

for some  $c \in F^{\times}$  satisfying  $k = \sigma(c)c^{-1}$ .

Proof. For all  $k \in F$  such that  $N_{F/F_0}(k) = 1$ ,  $H_{id,k}$  is an *F*-automorphism extending  $id_D$ . These are the only  $F_0$ -automorphisms of *A*, unless  $\tau \neq id$  can be also extended. By Hilbert's Satz 90,  $N_{F/F_0}(k) = 1$  if and only if there is  $c \in F^{\times}$  such that  $k = c^{-1}\sigma(c)$  [14]. So there is  $c \in F^{\times}$  such that  $k = c^{-1}\sigma(c)$  and

$$k\sigma(k)\cdots\sigma^{i-1}(k)=c\sigma^{i}(c), \quad i=1,\ldots,m-1$$

yields that  $H_{id,k} = G$  with

$$G(\sum_{i=0}^{m-1} a_i t^i) = a_0 + a_1 c^{-1} \sigma(c) t + \sum_{i=2}^{m-1} a_i c^{-1} \sigma^i(c) t^i,$$

which is an inner automorphism, since  $G = G_c$  with

$$G_c(\sum_{i=0}^{m-1} a_i t^i) = (c^{-1} \sum_{i=0}^{m-1} a_i t^i)c$$

Note that here we use that F = C(D).

**Corollary 10.** If  $F_0$  contains a primitive mth root of unity  $\omega$ , then A is a cyclic extension of D of order m, and all automorphisms extending  $id_D$  are inner.

**Example 11.** Let *F* and *L* be fields and let *K* be a cyclic Galois extension of both *F* and *L* such that [K:F] = n, [K:L] = m,  $Gal(K/F) = \langle \gamma \rangle$  and  $Gal(K/L) = \langle \sigma \rangle$ , and  $\sigma \circ \gamma = \gamma \circ \sigma$ . Define  $F_0 = F \cap L$ .

Let  $D = (K/F, \gamma, c)$  be a cyclic division algebra of degree n with  $c \in F_0$ , i.e.  $D \cong D_0 \otimes_{F_0} K$ for some cyclic algebra  $D_0 = (F/F_0, \gamma, c)$ . Let  $1, e, \ldots, e^{n-1}$  be the canonical basis of D, that is  $e^n = c$ ,  $ex = \gamma(x)e$  for every  $x \in K$ . For  $x = x_0 + x_1e + x_2e^2 + \cdots + x_{n-1}e^{n-1} \in D$ , define an L-linear map  $\sigma \in \operatorname{Aut}_L(D)$  via

$$\sigma(x) = \sigma(x_0) + \sigma(x_1)e + \sigma(x_2)e^2 + \dots + \sigma(x_{n-1})e^{n-1}$$

(note that  $c \in L$  implies  $\sigma(xy) = \sigma(x)\sigma(y)$  for all  $x, y \in D$ ). Then  $\sigma \in \operatorname{Aut}_{F_0}(D)$  has order m. For all  $d \in D^{\times}$ ,

$$D[t;\sigma]/D[t;\sigma](t^m-d) = (D,\sigma,d)$$

is a generalized nonassociative cyclic algebra of degree mn over  $F_0$  (used for instance in [20]).  $(D, \sigma, d)$  is associative if and only if  $d \in F_0$ . In the special case that  $d \in F^{\times}$ ,

$$(D, \sigma, d) = (L/F_0, \gamma, c) \otimes_{F_0} (F/F_0, \sigma, d)$$

is the tensor product of an associative and a nonassociative cyclic algebra.

If  $F_0$  contains a primitive *m*th root of unity and  $d \in D^{\times} \setminus F_0$  is chosen such that  $f(t) = t^m - d \in D[t;\sigma]$  is irreducible, then  $(D,\sigma,d)$  is a cyclic extension of D of order m, and all automorphisms extending  $id_D$  are inner (Corollary 10). Recall that if m is prime then  $f(t) = t^m - d \in D[t;\sigma]$  is irreducible if and only if  $d \neq \sigma^{m-1}(z) \cdots \sigma(z)z$  for all  $z \in D$ .

For m = 2, this algebra is studied in [21], and used in the codes constructed in [15]. For  $d \in F^{\times}$  the algebra is used in [23], see also [20].

3.3. In the following, let D be a division algebra which is finite-dimensional over its center  $F = C(D), \ \sigma \in \operatorname{Aut}(D)$  an automorphism such that  $\sigma|_F$  has finite order q and fixed field  $F_0 = \operatorname{Fix}(\sigma) \cap F$ . If D has degree n then the associative generalized cyclic algebra  $A = (D, \sigma, a)$  has degree qn over  $F_0$ . We choose  $a \in F_0$  such that A is a division algebra.

Now assume  $F_0$  contains a primitive qth root of unity  $\omega$ . Then  $\tau = H_{id_D,\omega} : A \to A$ generates a cyclic subgroup of  $\operatorname{Aut}_{F_0}(A)$  of order q by [5, Theorem 6] which consists of automorphisms which all extend  $id_D$ . We obtain the following generalization of [5, Theorem 7]:

**Theorem 12.** Suppose there exists  $\rho \in Aut(A)$ ,  $b \in A$  and  $1 \neq k \in F_0$  such that

- (1)  $\tau$  commutes with  $\rho$ ,
- (2)  $\tau(b) = k\rho(k)\cdots\rho^{m-1}(k)b$ ,
- (3)  $k^q$  is a primitive mth root of unity,
- (4)  $t^m b \in A[t; \rho]$  is irreducible, and

(5) the algebra  $B = A[t; \rho]/A[t; \rho](t^m - b)$  is either associative, or finite-dimensional over  $F_0 \cap \operatorname{Fix}(\rho)$ , or finite-dimensional over  $\operatorname{Nuc}_r(B)$ .

Then B is a nonassociative cyclic extension of D of degree mq which contains A.

*Proof.* Since B is a free left A-module of rank m and A is a free left D-module of rank q, B is a free left D-module of rank mq. Furthermore, (4) and (5) yield that B is a division algebra by [17, (7)]. Define the map

$$H_{\tau,k}: B \to B, \ \sum_{i=0}^{m-1} x_i t^i \mapsto \tau(x_0) + \sum_{i=1}^{m-1} \tau(x_i) \Big(\prod_{l=0}^{i-1} \rho^l(k)\Big) t^i \qquad (x_i \in A),$$

then (1) and (2) together imply that  $H_{\tau,k}$  is an automorphism of B by [8, Theorem 4].

 $H_{\tau,k}$  has order mq: We have  $\tau(k) = k$  because  $k \in F_0 \subset D$ . Therefore straightforward calculations yield  $H^2_{\tau,k} = H_{\tau,k} \circ H_{\tau,k} = H_{\tau^2,k\tau(k)} = H_{\tau^2,k^2}$ ,  $H^3_{\tau,k} = H_{\tau^3,k^3}$  etc., thus  $H_{\tau,k}$  will have order at least q. After q steps we obtain  $H^q_{\tau,k} = H_{id_A,v}$  with  $v = k^q$  and so  $H_{\tau,k}$  has order mq by (3).

Finally  $H_{\tau,k}|_D = \tau|_D = id_D$ , hence we conclude B is a nonassociative cyclic extension of D of degree mq.

#### 4. When is an ring a nonassociative cyclic extension?

A nonassociative ring  $A \neq 0$  is called a *right division ring*, if for all  $a \in A$ ,  $a \neq 0$ , the right multiplication with a,  $R_a(x) = xa$ , is bijective. If D is a division ring and f is irreducible, then  $S_f = D[t;\sigma]/D[t;\sigma]f$  is a right division algebra and has no zero divisors ([17, (6)] or [11]).

## **Theorem 13.** (cf. [17, (3), (6)])

(i) Let S be a nonassociative ring with multiplication  $\circ$ . Suppose that

(1) S has an associative subring D which is a division algebra and S is a free left D-module of rank m, and there is  $t \in S$  such that  $t^j$ ,  $0 \le i < m$  is a basis of S over D, when defining  $t^{j+1} = t \circ t^j$ ,  $t^0 = 1$ ;

(2) for all  $a \in D$ ,  $a \neq 0$ , there are  $a_1, a_2 \in D$ ,  $a_1 \neq 0$ , such that  $t \circ a = a_1 \circ t + a_2$ ;

(3) for all  $a, b, c \in D$ , i + j < m, k < m, we have  $[a \circ t^i, b \circ t^j, c \circ t^k] = 0$ . Then  $S \cong S_f$  with  $f(t) \in D[t; \sigma, \delta]$  and  $\sigma$ ,  $\delta$  defined via  $t \circ a = \sigma(a) \circ t + \delta(a)$  and where the polynomial  $f(t) = t^m - \sum_{i=0}^{m-1} d_i t^i$  is given by  $t^m = \sum_{i=0}^{m-1} d_i t^i$  with  $t^0 = 1$ ,  $t^{i+1} = t \circ t^i$ ,  $0 \le i < m$ .

(ii) If S is a right division ring in (i) then f is irreducible.

Theorem 13 yields the nonassociative analogues to the existence conditions for associative cyclic extensions in [5, Theorem 6].

**Theorem 14.** (i) Let S be a nonassociative ring with multiplication  $\circ$ , which has a field K as a subring, and is a free left K-vector space of dimension m. Suppose that

(1) there is  $t \in S$  such that  $t^i$ ,  $0 \le i < m$ , is a basis of S over K when defining  $t^0 = 1$ ,  $t^{i+1} = t \circ t^i$ ,  $0 \le i < m$ ;

(2) for all  $a \in K$ ,  $a \neq 0$ , there is  $a' \in K^{\times}$ , such that  $t \circ a = a' \circ t$ ;

(3) for all  $a, b, c \in K$ , i + j < m, k < m, we have  $[a \circ t^i, b \circ t^j, c \circ t^k] = 0$ ;

(4)  $t^m = d$  for some  $d \in K^{\times}$ ;

(5) the map  $\sigma: K \to K$ ,  $\sigma(a) = a'$ , has order m and fixed field  $F = \{a \in K \mid t \circ a = a \circ t\}$ containing a primitive mth root of unity  $\omega$ , and K/F is a finite cyclic Galois extension. Then  $S \cong S_f = (K/F, \sigma, d)$  with  $f(t) = t^m - d \in K[t; \sigma]$ .

(ii) If S is a right division ring in (i) then f is irreducible and  $S \cong (K/F, \sigma, d)$  is a nonassociative cyclic extension of K of degree m.

Proof. (1), (2) and (3) imply that  $S \cong S_f$  with  $f \in K[t; \sigma]$  and  $\sigma$  defined via  $t \circ a = \sigma(a) \circ t$ , i.e.  $\sigma(a) = a'$ , and where the polynomial  $f(t) = t^m - \sum_{i=0}^{m-1} d_i t^i$  is given by  $t^m = \sum_{i=0}^{m-1} d_i t^i$  for some suitably chosen  $d_i$  (cf. [17, (3)]). (4) implies that indeed  $f(t) = t^m - d$ . (5) guarantees that  $(K/F, \sigma, d)$  where F contains a primitive mth root of unity  $\omega$ .

(ii) Here we are in the setup of Theorem 1 which yields the assertion: F contains a primitive mth root of unity  $\omega$ , so  $\langle H_{id,\omega} \rangle$  is a cyclic subgroup of order m of the division algebra  $(K/F, \sigma, d)$ .

For nonassociative cyclic extensions of a central simple algebra D we obtain from Theorem 13:

**Theorem 15.** (i) Let S be a nonassociative ring with multiplication  $\circ$ , which has an associative subring D which is a division algebra and S is a free left D-module of rank m. Suppose that

(1) there is  $t \in S$  such that  $t^i$ ,  $0 \le i < m$ , is a basis of S over D when defining  $t^0 = 1$ ,  $t^{i+1} = t \circ t^i$ ,  $0 \le i < m$ ;

(2) for all  $a \in D$ ,  $a \neq 0$ , there are  $a' \in D$ ,  $a' \neq 0$ , such that  $t \circ a = a' \circ t$ ;

(3) for all  $a, b, c \in D$ , i + j < m, k < m, we have  $[a \circ t^i, b \circ t^j, c \circ t^k] = 0$ ;

$$(4) t^m = d;$$

(5) the map  $\sigma: D \to D$ ,  $\sigma(a) = a'$ , has order m, fixed field  $\{a \in D \mid t \circ a = a \circ t\}$  and D/Fis a central simple algebra, where  $F_0 = F \cap \text{Fix}(\sigma)$  contains a primitive mth root of unity  $\omega$ . Then  $S \cong S_f = (D, \sigma, d)$  with  $f(t) = t^m - d \in D[t; \sigma]$ .

(ii) If S is a right division ring and D a central simple algebra in (i), then f is irreducible and S a nonassociative cyclic extension of D of degree m.

Proof. (1), (2) and (3) imply that  $S \cong S_f$  with  $f \in D[t; \sigma]$  and  $\sigma$  defined via  $t \circ a = \sigma(a) \circ t$ , i.e.  $\sigma(a) = a'$ , and where the polynomial  $f(t) = t^m - \sum_{i=0}^{m-1} d_i t^i$  is given by  $t^m = \sum_{i=0}^{m-1} d_i t^i$  for some suitably chosen  $d_i$  (cf. [17, (3)]). (4) implies  $f(t) = t^m - d$ . (5) guarantees that  $S \cong (D, \sigma, d)$  where F contains a primitive mth root of unity  $\omega$ .

(ii) Here we are in the setup of Theorem 6 which yields the assertion, since F contains a primitive mth root of unity  $\omega$ ,  $\langle H_{id,\omega} \rangle$  is a cyclic subgroup of order m of the division algebra  $(D, \sigma, d)$ .

## References

- [1] A. A. Albert, Structure of algebras. Vol. 24, AMS 1939.
- [2] A. A. Albert, Cyclic fields of degree  $p^n$  over F of characteristic p. Bull. AMS 40 (1934), 625-631.
- [3] A. A. Albert, Modern higher algebra. Chicago 1937, Chapter IX, 192-208.
- [4] A. S. Amitsur, Differential Polynomials and Division Algebras. Annals of Mathematics, Vol. 59 (2) (1954) 245-278.
- [5] A. S. Amitsur, Non-commutative cyclic fields. Duke Math. J. 21 (1954), 87105.
- [6] E. Artin, O. Schreier, Über eine Kennzeichnung der reell algebraischen Körper. Abh. Math. Seminar der Hamburgischen Universitäten, 5 (1927), 225-231.
- [7] C. Brown, Petit's algebras and their automorphisms. PhD Thesis, University of Nottingham, 2018.
- [8] C. Brown, S. Pumplün, The automorphisms of Petit's algebras. Comm. Algebra 46 (2) (2018), 834-849.
- [9] C. Brown, S. Pumplün, Solvable crossed product algebras revisited. Online at arXiv:1702.04605 [math.RA]
- [10] C. Brown, S. Pumplün, A. Steele, Automorphisms and isomorphisms of Jha-Johnson semifields obtained from skew polynomial rings. To appear in Comm. Alg. Online at arXiv:1703.02356 [math.RA]
- [11] C. Brown, S. Pumplün, How a nonassociative algebra reflects the properties of a skew polynomial. Preprint, 2018.
- [12] N. Jacobson, "Finite-dimensional division algebras over fields." Springer Verlag, Berlin-Heidelberg-New York, 1996.
- [13] K. Kishimoto, On cyclic extensions of simple rings. J. Fac. Sci. Hokkaido Univ. Ser. I 19 (1966), 74-85.
- [14] T. Y. Lam, A. Leroy, Hilbert 90 theorems over division rings. Trans. Amer. Math. Soc. 345 (2) (1994), 595-622.
- [15] N. Markin, F. Oggier, Iterated space-time code constructions from cyclic algebras. IEEE Transactions on Information Theory, 59 (9), September 2013.
- [16] O. Ore, Theory of noncommutative polynomials. Annals of Math. 34 (3) (1933), 480-508.
- [17] 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.
- [18] S. Pumplün, Nonassociative differential extensions of characteristic p. Results in Mathematics 72 (1-2) (2017), 245-262, DOI 10.1007/s00025-017-0656-x
- [19] S. Pumplün, Tensor products of nonassociative cyclic algebras. Journal of Algebra 451 (2016), 145-165.
- [20] S. Pumplün, A. Steele, Fast-decodable MIDO codes from nonassociative algebras. Int. J. of Information and Coding Theory (IJICOT) 3 (1) 2015, 15-38.
- [21] S. Pumplün, How to obtain division algebras used for fast decodable space-time block codes. Adv. in Math. Comm. 8 (3) (2014), 323 - 342.
- [22] S. Pumplün, A. Steele, The nonassociative algebras used to build fast-decodable space-time block codes. Adv. Math. Comm. 9 (4) (2015), 449-469.
- [23] K. P. Srinath, B. S. Rajan, Fast-decodable MIDO codes with large coding gain. IEEE Transactions on Information Theory (2) 60 2014, 992-1007.
- [24] R. D. Schafer, "An Introduction to Nonassociative Algebras." Dover Publ., Inc., New York, 1995.
- [25] A. Steele, Nonassociative cyclic algebras. Israel Journal of Mathematics 200 (1) (2014), 361-387.
- [26] E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p<sup>n</sup>. J. Reine Angew. Math. 176 (1936), 126-140.

 ${\it E-mail\ address:\ christian_jb@hotmail.co.uk;\ susanne.pumpluen@nottingham.ac.uk}$ 

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