# TENSOR PRODUCTS OF NONASSOCIATIVE CYCLIC ALGEBRAS

S. PUMPLÜN

Abstract. We study the tensor product of two not necessarily associative cyclic algebras. The condition for the tensor product of an associative cyclic algebra and a nonassociative cyclic algebra to be division generalizes the classical one for two associative cyclic algebras by Albert or Jacobson, if the base field contains a suitable root of unity. Stronger conditions are obtained in special cases.

## Introduction

Nonassociative cyclic algebras of degree $n$ are canonical generalizations of associative cyclic algebras of degree $n$ and were first introduced over finite fields by Sandler [14]. Nonassociative quaternion algebras (the case $n = 2$) constituted the first known examples of a nonassociative division algebra (Dickson [3]). Properties of nonassociative cyclic algebras were investigated over arbitrary fields by Steele [16], [17], see also [12].

In the following we study the tensor product $A = D_0 \otimes_{F_0} D_1$ of two (not necessarily associative) cyclic algebras $D_0$ and $D_1$ over a field $F_0$ and give conditions for $A$ to be a division algebra. These algebras are used for space-time block coding [9], [10], [11], and are behind the iterated codes by Markin and Oggier [7].

After recalling some results needed in the paper in Section 1, we generalize the definition of iterated algebras $\mathrm{It}_R^m(D,\tau,d)$ from [9], [11] to allow nonassociative cyclic algebras $D = (K/F,\sigma,c)$ in their construction in Section 2.

In Section 3, results by Petit [8] are used to show that iterated algebras $\mathrm{It}_R^m(D,\tau,d)$ can be defined using polynomials in skew-polynomial rings over $D$ when $D$ is associative (Theorem 8).

The main result is established in Section 4: if $D = (L/F_0,\sigma,c)\otimes_{F_0} F$ is an associative division algebra then

$$(L/F_0,\sigma,c)\otimes_{F_0}(F/F_0,\tau,d)\cong S_f\cong \mathrm{It}_R^m(D,\tau,d),$$

where the twisted polynomial $f(t) = t^m - d \in D[t;\widetilde{\tau}^{-1}]$, $\widetilde{\tau}$ an automorphism of $D$ canonically extending $\tau$, is used to construct the algebra $S_f$ (Theorem 13).

Section 5 contains the main results: if $D_0$ is an associative cyclic algebra over $F_0$ such that $D = D_0 \otimes_{F_0} F$ is a division algebra, and $D_1 = (F/F_0,\tau,d)$ a nonassociative cyclic algebra of degree $m$, then $D_0 \otimes_{F_0} D_1$ is a division algebra if and only if $f(t) = t^m - d$ is irreducible in $D[t;\widetilde{\tau}^{-1}]$ (Theorem 17).

*Date*: 14.1.2015.

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

*Key words and phrases.* cyclic algebra, nonassociative cyclic algebra, nonassociative quaternion algebra, tensor product, division algebra.

This generalizes the classical condition for the tensor product of two associative cyclic algebras [4, Theorem 1.9.8], see Theorem 15. Some more detailed conditions are obtained for special cases. Section 6 concludes with some remarks on the tensor product of two nonassociative cyclic algebras.

## 1. Preliminaries

1.1. **Nonassociative algebras.** Let $F$ be a field and let $A$ be a finite-dimensional $F$-vector space. We call $A$ 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.

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. $A$ is a division algebra if and only if $A$ has no zero divisors [15, pp. 15, 16].

For an $F$-algebra $A$, associativity in $A$ is measured by the *associator* $[x,y,z]=(xy)z-x(yz)$. The *middle nucleus* of $A$ is defined as $\mathrm{Nuc}_m(A)=\{x\in A\,|\,[A,x,A]=0\}$ and the *nucleus* of $A$ is defined as $\mathrm{Nuc}(A)=\{x\in A\,|\,[x,A,A]=[A,x,A]=[A,A,x]=0\}$. It 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 *commuter* of $A$ is defined as $\mathrm{Comm}(A)=\{x\in A\,|\,xy=yx \text{ for all } y\in A\}$ and the *center* of $A$ is $\mathrm{C}(A)=\{x\in A\,|\,x\in\mathrm{Nuc}(A) \text{ and } xy=yx \text{ for all } y\in A\}$.

For two nonassociative algebras $C$ and $D$ over $F$,

$$\mathrm{Nuc}(C)\otimes_F\mathrm{Nuc}(D)\subset\mathrm{Nuc}(C\otimes_F D).$$

Thus we can consider the tensor product $A=C\otimes_F D$ as a right $R$-module over any ring $R\subset\mathrm{Nuc}(C)\otimes_F\mathrm{Nuc}(D)$.

1.2. **Associative and nonassociative cyclic algebras.** Let $K/F$ be a cyclic Galois extension of degree $n$ with Galois group $\mathrm{Gal}(K/F)=\langle\sigma\rangle$.

An associative cyclic algebra $(K/F,\sigma,c)$ of degree $n$ over $F$, $c\in F^\times$, is an $n$-dimensional $K$-vector space

$$(K/F,\sigma,c)=K\oplus eK\oplus e^2K\oplus\cdots\oplus e^{n-1}K,$$

with multiplication given by the relations

$$e^n=c,\ le=e\sigma(l),$$

for all $l\in K$. $(K/F,\sigma,c)$ is division for all $c\in F^\times$, such that $c^s\not\in N_{K/F}(K^\times)$ for all $s$ which are prime divisors of $n$, $1\leq s\leq n-1$.

For $c\in K\setminus F$, we define a unital nonassociative algebra $(K/F,\sigma,c)$ (Sandler [14]) as the $n$-dimensional $K$-vector space

$$(K/F,\sigma,c)=K\oplus eK\oplus e^2K\oplus\cdots\oplus e^{n-1}K,$$

where multiplication is given by the following rules for all $a, b \in K, 0 \leq i, j, < n$, which then are extended linearly to all elements of $A$:

$$(e^i a)(e^j b) = \begin{cases} e^{i+j}\sigma^j(a)b & \text{if } i+j < n, \\ e^{(i+j)-n}d\sigma^j(a)b & \text{if } i+j \geq n. \end{cases}$$

We call $D = (K/F, \sigma, c)$ with $c \in K \setminus F$ a *nonassociative cyclic algebra of degree $n$*. $D$ has nucleus $K$ and center $F$. $D$ is not $(n+1)$th power associative since $(e^{n-1}e)e = e\sigma(a)$ and $e(e^{n-1}e) = ea$. The map $M_D : D \longrightarrow K$, $M_D(x) = \det(L_x)$, is a polynomial map in $c$ of degree $n-1$ with coefficients in $F$ which is *semi-multiplicative*, i.e.

$$M_D(ax) = N_{K/F}(a)M_D(x) = M_D(xa)$$

for all $a \in K$, $x \in D$. If $D$ is a division algebra then $M_D(x) \neq 0$ for all $x \in D^\times$, cf. [17, Section 4.2] or [12].

If $[K : F]$ is prime, $D$ always is a division algebra. If $[K : F]$ is not prime, $D$ is a division algebra for any choice of $c$ such that $1, c, \dots, c^{n-1}$ are linearly independent over $F$ [17].

For $n = 2$, $(K/F, \sigma, c) = \mathrm{Cay}(K, c)$ is an associative (if $c \in F$) or nonassociative (if $c \in K \setminus F$) quaternion algebra over $F$, cf. [2], [13] or [18].

From now on, when we say $D = (K/F, \sigma, c)$ is a cyclic algebra, we mean an associative or nonassociative cyclic algebra over $F$ without always explicitly stating that we also allow $c \in K^\times$. We call $\{1, e, e^2, \dots, e^{n-1}\}$ the *standard basis* of $(K/F, \sigma, c)$.

$D = (K/F, \sigma, c)$ is a $K$-vector space of dimension $n$ (since $K = \mathrm{Nuc}(D)$ if the algebra is nonassociative) and, after a choice of a $K$-basis, we can embed the $K$-vector space $\mathrm{End}_K(D)$ into $\mathrm{Mat}_n(K)$. The left multiplication of elements of $D$ with $y = y_0 + ey_1 + \cdots + e^{n-1}y_{n-1} \in D$ ($y_i \in K$) induces the $K$-linear embedding $\lambda : D \to \mathrm{Mat}_n(K)$.

## 2. Iterated algebras

Let $D = (K/F, \sigma, c)$ be a cyclic algebra of degree $n$ over $F$. If $D$ is associative, let $N_{D/F}$ denote the reduced norm of $D$. If $D$ is nonassociative, we consider the semi-multiplicative polynomial map $M_D$ instead. For $x = x_0 + ex_1 + e^2x_2 + \cdots + e^{n-1}x_{n-1} \in D$ ($x_i \in K$, $1 \leq i \leq n$), and any $\tau \in \mathrm{Aut}(K)$, $L = \mathrm{Fix}(\tau)$, define the $L$-linear map $\widetilde{\tau} : D \to D$ via

$$\widetilde{\tau}(x) = \tau(x_0) + e\tau(x_1) + e^2\tau(x_2) + \cdots + e^{n-1}\tau(x_{n-1}).$$

If $c \in L$ then

$$\widetilde{\tau}(xy) = \widetilde{\tau}(x)\widetilde{\tau}(y) \text{ and } \lambda(\widetilde{\tau}(x)) = \tau(\lambda(x))$$

for all $x, y \in D$, where for any matrix $X = \lambda(x)$ representing left multiplication with $x$, $\tau(X)$ means applying $\tau$ to each entry of the matrix.

$D' = (K/F, \sigma, \tau(c))$ is a cyclic algebra, call its standard basis $1, e', \dots, e'^{n-1}$. For $y = y_0 + ey_1 + \cdots + e^{n-1}y_{n-1} \in D$ define $y_{D'} = y_0 + e'y_1 + \cdots + e'^{n-1}y_{n-1} \in D'$. By [9, Proposition 1], if both $D$ and $D'$ are associative, we know that $N_{D/F}(\widetilde{\tau}(y)) = \tau(N_{D'/F}(y_{D'}))$. The proof of this result carries over verbatim to nonassociative $D$ and $D'$:

**Proposition 1.** *Suppose $\tau$ commutes with $\sigma$ and that $D$ is nonassociative. Let $D' = (K/F, \sigma, \tau(c))$ be a nonassociative cyclic algebra with standard basis $\{1, e', \dots, e'^{n-1}\}$. For $y = y_0 + ey_1 + \cdots + e^{n-1}y_{n-1} \in D$ define $y_{D'} = y_0 + e'y_1 + \cdots + e'^{n-1}y_{n-1} \in D'$. Then*

$$M_D(\widetilde{\tau}(y)) = \tau(M_{D'/F}(y_{D'})).$$

*If $c \in L$, then*

$$M_D(\widetilde{\tau}(y)) = \tau(M_D(y)).$$

We will use the following notation from now on: Let $F$ and $L$ be fields and let $K$ be a cyclic field extension of both $F$ and $L$ such that

(1) $Gal(K/F) = \langle\sigma\rangle$ and $[K : F] = n$,
(2) $Gal(K/L) = \langle\tau\rangle$ and $[K : L] = m$,
(3) $\sigma$ and $\tau$ commute: $\sigma\tau = \tau\sigma$.

Define $F_0 = F \cap L$. Let $D = (K/F, \sigma, c)$ be a nonassociative cyclic algebra over $F$.

For associative $D$, $\mathrm{It}_R^m(D, \tau, d)$ was defined in [10]. We generalize the definition in [9], [10], [11] to be able to include nonassociative cyclic algebras $D$:

**Definition 1.** Pick $d \in F^\times$, $c \in F_0$. For $x = (x_0, x_1, \dots, x_{m-1})$, $y = (y_0, y_1, \dots, y_{m-1})$, with $x_i, y_i \in D$, define a product on the $F$-vector space

$$\mathrm{It}_R^m(D, \tau, d) = D \oplus D \oplus D \oplus \cdots \oplus D \text{ ($m$-copies)}$$

as the matrix multiplication

$$xy = (M(x)y^T)^T,$$

where

$$M(x) = \begin{bmatrix} x_0 & d\widetilde{\tau}(x_{m-1}) & d\widetilde{\tau}^2(x_{m-2}) & \cdots & d\widetilde{\tau}^{m-1}(x_1) \\ x_1 & \widetilde{\tau}(x_0) & d\widetilde{\tau}^2(x_{m-1}) & \cdots & d\widetilde{\tau}^{m-1}(x_2) \\ x_2 & \widetilde{\tau}(x_1) & \widetilde{\tau}^2(x_0) & \cdots & d\widetilde{\tau}^{m-1}(x_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{m-1} & \widetilde{\tau}(x_{m-2}) & \widetilde{\tau}^2(x_{m-3}) & \cdots & \widetilde{\tau}^{m-1}(x_0) \end{bmatrix}.$$

The algebra $\mathrm{It}_R^m(D, \tau, d)$ is called an *iterated algebra*.

$\mathrm{It}_R^m(D, \tau, d)$ is a nonassociative algebra over $F_0$ of dimension $m^2n^2$ with unit element $(1, 0, \dots, 0)$ and contains $D$ as a subalgebra. The multiplication is well-defined as $d \in \mathrm{Nuc}(D) = K$. Put $f = (0, 1_D, 0 \dots, 0)$. Then $f^i$ is well-defined for $1 \leq i \leq m$ and $f^2 = (0, 0, 1_D, 0 \dots, 0), \dots, f^{m-1} = (0, \dots, 0, 1_D)$ and $f^{m-1}f = (d, 0, \dots, 0) = ff^{m-1}$. We call

$$\{1, e, e^2, \dots, e^{n-1}, f, fe, fe^2, \dots, f^{m-1}e^{n-1}\}$$

the *standard basis* of the $K$-vector space $\mathrm{It}_R^m(D, \tau, d)$.

**Example 2.** (i) The multiplication in $\mathrm{It}_R^2(D, \tau, d) = D \oplus D$ is given by

$$(u, v) \cdot (u', v') = (\begin{bmatrix} u & d\widetilde{\tau}(v) \\ v & \widetilde{\tau}(u) \end{bmatrix} \begin{bmatrix} u' \\ v' \end{bmatrix})^T = (uu' + d\widetilde{\tau}(v)v', vu' + \widetilde{\tau}(u)v').$$

for $u, u', v, v' \in D$.
(ii) Let $A = \mathrm{It}_R^3(D, \tau, d)$ and $f = (0, 1, 0)$. Here, $f^2 = (0, 0, 1)$ and $f^2 f = (d, 0, 0) = ff^2$. The multiplication in $A$ is given by

$$(u, v, w)(u', v', w') = (\begin{bmatrix} u & d\widetilde{\tau}(w) & d\widetilde{\tau}^2(v) \\ v & \widetilde{\tau}(u) & d\widetilde{\tau}^2(w) \\ w & \widetilde{\tau}(v) & \widetilde{\tau}^2(u) \end{bmatrix} \begin{bmatrix} u' \\ v' \\ w' \end{bmatrix})^T$$

$$= (uu' + d\widetilde{\tau}(w)v' + d\widetilde{\tau}^2(v)w', vu' + \widetilde{\tau}(u)v' + d\widetilde{\tau}^2(w)w', wu' + \widetilde{\tau}(v)v' + \widetilde{\tau}^2(u)w')$$

for $u, v, w, u', v', w' \in D$.

From now on, let

$$A = \mathrm{It}_R^m(D, \tau, d).$$

**Lemma 3.** *(i) The cyclic algebra $(K/L, \tau, d)$ over $L$, viewed as an algebra over $F_0$, is a subalgebra of $A$, and is nonassociative if $d \in F \setminus F_0$.*
*(ii) Let $m$ be even. Then $It_R^2(D, \tau, d)$ is isomorphic to a subalgebra of $A$.*

*Proof.* (i) This is easy to see by restricting the multiplication of $A$ to $K \oplus \cdots \oplus K$.
(ii) Suppose that $m = 2s$ for some integer $s$. Then $\mathrm{It}_R^2(D, \tau, d)$ is isomorphic to $D \oplus f^s D$, which is a subalgebra of $A$ under the multiplication inherited from $A$. □

In particular, the quaternion algebra $(K/L, \tau, d) = \mathrm{Cay}(K, d)$ over $L$, viewed as algebra over $F_0$, is a subalgebra of $\mathrm{It}_R^2(D, \tau, d)$, which is nonassociative and division if $d \in F \setminus F_0$.

We can embed $\mathrm{End}_K(A)$ into the module $\mathrm{Mat}_{nm}(K)$. Left multiplication $L_x$ with $x \in A$ is a right $K$-endomorphism, so that we obtain a well-defined additive map

$$L : A \to \mathrm{End}_K(A) \hookrightarrow \mathrm{Mat}_{nm}(K), \quad x \mapsto L_x \mapsto L(x) = X$$

which is injective if $A$ is division.

Take the standard basis $\{1, e, \dots, e^{n-1}, f, fe, \dots, f^{m-1}e^{n-1}\}$ of the $K$-vector space $A$. Then

$$xy = (\lambda(M(x))y^T)^T,$$

where

$$\lambda(M(x)) = \begin{bmatrix} \lambda(x_0) & d\tau(\lambda(x_{m-1})) & \cdots & d\tau^{m-1}(\lambda(x_1)) \\ \lambda(x_1) & \tau(\lambda(x_0)) & \cdots & d\tau^{m-1}(\lambda(x_2)) \\ \vdots & \vdots & \ddots & \vdots \\ \lambda(x_{m-1}) & \tau(\lambda(x_{m-2})) & \cdots & \tau^{m-1}(\lambda(x_0)) \end{bmatrix} \tag{1}$$

is obtained by taking the matrix $\lambda(x_i)$, $x_i \in D$, representing left multiplication in $D$ of each entry in the matrix $M(x)$.

$\lambda(M(x))$ represents the left multiplication by the element $x$ in $A$. Define

$$M_A : A \to K, \quad M_A(x) = \det(\lambda(M(x))).$$

**Theorem 4.** *(i) Let $x \in A$ be nonzero. If $x$ is not a left zero divisor in $A$, then $M_A(x) \neq 0$.*
*(ii) $A$ is a division algebra if and only if $M_A(x) \neq 0$ for all $x \neq 0$.*

*Proof.* (i) The proof is obvious and analogous to the one of [11, Theorem 9].
(ii) If $A$ is a division algebra then $L_x$ is bijective for all $x \neq 0$ and thus $\lambda(M(x))$ invertible, i.e. $M_A(x) \neq 0$. Conversely, if $M_A(x) \neq 0$ for all $x \neq 0$ then for all $x, y \in A$, $x \neq 0$, $y \neq 0$, also $xy = (\lambda(M(x))y^T)^T \neq 0$. □

## 3. Division algebras obtained from skew-polynomial rings

In the following, we use results from [4] and [8]. Let $D$ be a unital division ring and $\sigma$ a ring isomorphism of $D$. The *twisted polynomial ring* $D[t;\sigma]$ is the set of polynomials

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

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

$$ta = \sigma(a)t \quad (a \in D).$$

That means,

$$at^n bt^m = \sum_{j=0}^{n} a\sigma^j(b)t^{m+j} \text{ and } t^n a = \sigma^n(a)t^n$$

for all $a, b \in D$ [4, p. 2]. $R = D[t;\sigma]$ is a left principal ideal domain and there is a right division algorithm in $R$ [4, p. 3], i.e. for all $g, f \in R$, $g \neq 0$, there exist unique $r, q \in R$ such that $\deg(r) < \deg(f)$ and

$$g = qf + r.$$

$R = D[t;\sigma]$ is also a right principal ideal domain [4, p. 6] with a left division algorithm in $R$ [4, p. 3 and Prop. 1.1.14]. (We point out that our terminology is the one used by Petit [8] and Lavrauw and Sheekey [6]; it is different from Jacobson's [4], who calls what we call right a left division algorithm and vice versa.)

Thus $R = D[t;\sigma]$ is a (left and right) principal ideal domain (PID).

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 $g, h \in R$ with $\deg(g), \deg(h) < \deg(f)$ such that $f = gh$ [4, p. 11].

**Definition 2.** (cf. [8, (7)]) Let $f \in D[t;\sigma]$ be of degree $m$ and let $\mathrm{mod}_r f$ 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

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

becomes a unital nonassociative algebra $S_f = (R_m, \circ)$ over $F_0 = \{z \in D \,|\, zh = hz \text{ for all } h \in S_f\}$.

The multiplication is well-defined because of the right division algorithm and $F_0$ is a subfield of $D$ [8, (7)].

Since $\sigma$ is a ring isomorphism, we also have a left division algorithm and can use it to define a second algebra construction (cf. [8]): Let $f \in D[t;\sigma]$ be of degree $m$ and let $\mathrm{mod}_l f$ denote the remainder of left division by $f$. Then $R_m$ together with the multiplication

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

becomes a nonassociative algebra ${}_fS = (R_m, \circ)$, which, however, turns out to be anti-isomorphic to a suitable algebra $S_g$ for some $g \in R'$ and some twisted polynomial ring $R'$.

**Remark 5.** (i) 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 $R$ [8, (10)]. For $f(t) = t^m - d_0 \in R$, multiplication in $S_f$ is defined via

$$(at^i)(bt^j) = \begin{cases} a\sigma^i(b)t^{i+j} & \text{if } i+j < m, \\ a\sigma^i(b)t^{(i+j)-m}d_0 & \text{if } i+j \geq m, \end{cases}$$

and multiplication in ${}_fS$ is defined via

$$(at^i)(bt^j) = \begin{cases} a\sigma^i(b)t^{i+j} & \text{if } i+j < m, \\ a\sigma^i(b)d_0t^{(i+j)-m} & \text{if } i+j \geq m, \end{cases}$$

for all $a, b \in D$ and then linearly extended. The algebra ${}_fS$ with $f(t) = t^m - d_0 \in R$ and $[K : F] = m$ is treated in [17]. If $D = K$ is a cyclic Galois field extension of $F$ of degree $m$ with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$, this is the opposite algebra of the cyclic algebra $(K/F, \sigma, d)$, cf. [17, 3.2.14].
(ii) Given a cyclic Galois field extension $K/F$ of degree $m$ with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$, the cyclic algebra $(K/F, \sigma, d)$ is the algebra $S_f$ with $f(t) = t^m - d \in R = K[t; \sigma^{-1}]$ [8, p. 13-13].
(iii) Let $D$ be a finite-dimensional central division algebra over $F$ and $\sigma$ an automorphism of $D$ of order $m$. In [4], the associative algebras

$$E(f) = \{g \in D[t;\sigma] \,|\, \deg(g) < m,\ f \text{ right divides } fg\}$$

for $f = t^m - d \in D[t; \sigma]$, were investigated. $E(f)$ is division iff $f$ is irreducible.

**Theorem 6.** *(cf.* [8, (2), p. 13-03, (9), (15),(17), (18), (19)]*) Let* $f = t^m - \sum_{i=0}^{m-1} d_i t^i \in R = D[t; \sigma]$.
*(i) If* $S_f$ *is not associative then*

$$\mathrm{Nuc}_l(S_f) = \mathrm{Nuc}_m(S_f) = D$$

*and*

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

*(ii) If* $f$ *is irreducible then* $\mathrm{Nuc}_r(S_f)$ *is an associative division algebra.*
*(iv) Let* $f \in R$ *be irreducible and* $S_f$ *a finite-dimensional* $F_0$*-vector space or a finite-dimensional right* $\mathrm{Nuc}_r(S_f)$*-module. Then* $S_f$ *is a division algebra.*
*(v)* $f(t) = t^2 - d_1t - d_0$ *is irreducible in* $D[t; \sigma]$ *if and only if* $\sigma(z)z - d_1z - d_0 \neq 0$ *for all* $z \in D$.
*(vi)* $f(t) = t^3 - d_2t^2 - d_1t - d_0$ *is irreducible in* $D[t; \sigma]$ *if and only if*

$$\sigma(z)^2\sigma(z)z - \sigma^2(z)\sigma(z)d_2 - \sigma(z)^2\sigma(d_1) - \sigma^2(d_0) \neq 0$$

*and*

$$\sigma(z)^2\sigma(z)z - d_2\sigma(z)z - d_1z - d_0 \neq 0$$

*for all $z \in D$.*
*(vii) Suppose $m$ is prime and $\mathrm{C}(D)\cap \mathrm{Fix}(\sigma)$ contains a primitive $m$th root of unity. Then $f(t)=t^m-d$ is irreducible in $D[t;\sigma]$ if and only if*

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

*for all $z\in D$.*

**Theorem 7.** *(i) $D[t;\sigma]$ is anti-isomorphic to $D^{op}[t;\sigma^{-1}]$, i.e. there is a linear isomorphism $H : D[t;\sigma] \to D^{op}[t;\sigma^{-1}]$, $H(\sum a_it^i) = \sum\sigma^{-i}(a_i)t^i$ such that $H(fg) = H(g)H(f)$. In particular,*

$$(D[t;\sigma])^{op} \cong D^{op}[t;\sigma^{-1}].$$

*(ii) If $f \in D[t;\sigma]$ is irreducible then so is $H(f)\in D^{op}[t;\sigma^{-1}]$.*
*(iii) Let ${S'}_g$ denote the algebra given by some $g\in R' = D^{op}[t;\sigma^{-1}]$ and $f \in R$. Then ${}_fS$ and ${S'}_{H(f)}$ are anti-isomorphic algebras, so $({}_fS)^{op}\cong S'_{H(f)}$.*

*Proof.* (i) Denote by $\circ$ the multiplication in the opposite algebra $D^{op}$. We have

$$\begin{aligned} H(a)H(b) &= H((\sum_i a_it^i)(\sum_j b_it^i)) = H(\sum_{i,j} a_i\sigma^i(b_j)t^{i+j}) \\ &= \sum_{i,j}\sigma^{-i-j}(a_i)\circ\sigma^{-i-j}(\sigma^i(b_j))t^{i+j} = \sum_{i,j}\sigma^{-i-j}(\sigma^i(b_j))\sigma^{-i-j}(a_i)t^{i+j} \\ &= \sum_{i,j}\sigma^{-j}(b_j)\sigma^{-j}(\sigma^{-i}(a_i))t^{i+j} = \sum_{i,j} H(b)_j\,\sigma^{-j}(H(a)_i)t^{i+j} = H(b)\circ H(a). \end{aligned}$$

(ii) is obvious.
(iii) is [8, (1)], see also [6, Cor. 4] if $D$ is a field. □

The iterated algebras $\mathrm{It}^m_R(D,\tau,d)$ with $D$ an associative cyclic algebra, originally introduced for space-time coding, can be obtained from skew-polynomial rings:

**Theorem 8.** *Let $F$ and $L$ be fields, $F_0 = F\cap L$, and let $K$ be a cyclic field extension of both $F$ and $L$ such that*

1. *$Gal(K/F)=\langle\sigma\rangle$ and $[K:F]=n$,*
2. *$Gal(K/L)=\langle\tau\rangle$ and $[K:L]=m$,*
3. *$\sigma$ and $\tau$ commute: $\sigma\tau=\tau\sigma$.*

*Let $D=(K/F,\sigma,c)$ be an associative cyclic division algebra over $F$ of degree $n$, $c\in F_0$ and $d\in D^\times$. Then*

$$\mathrm{It}^m_R(D,\tau,d) = S_f$$

*where $R = D[t;\widetilde{\tau}^{-1}]$ and $f(t)=t^m-d$.*

*Proof.* Let $f=(0,1_D,0,\dots,0)\in A=\mathrm{It}^m_R(D,\tau,d)$. The multiplication on

$$A = D\oplus fD\oplus f^2D\oplus\cdots\oplus f^{m-1}D$$

is given by

$$(f^ix)(f^jy) = \begin{cases} f^{i+j}\widetilde{\tau}^j(x)y & \text{if } i+j<m \\ f^{(i+j)-m}\widetilde{\tau}^j(x)yd & \text{if } i+j\geq m\end{cases}$$

for all $x,y\in D$ [11] which corresponds to the multiplication of the algebra $S_f$. □

Theorems 6, 7 (iii) and 8 imply:

**Corollary 9.** *Assume the setup of Theorem 8.*
*(i) If $d \notin F_0$ then*

$$\mathrm{Nuc}_l(\mathrm{It}_R^m(D,\tau,d)) = \mathrm{Nuc}_m(\mathrm{It}_R^m(D,\tau,d)) = D$$

*and*

$$\mathrm{Nuc}_r(\mathrm{It}_R^m(D,\tau,d)) = \{g \in R \,|\, fg \in Rf\}.$$

*(ii) $\mathrm{It}_R^m(D,\tau,d)$ is a division algebra if and only if $f(t)$ is irreducible in $D[t;\widetilde{\tau}^{-1}]$.*
*(iii) Suppose that $m$ is prime and in case $m \neq 3$, additionally that $F_0$ contains a primitive $m$th root of unity. Then $\mathrm{It}_R^m(D,\tau,d)$ is a division algebra if and only if*

$$d \neq z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{m-1}(z) \text{ and } \widetilde{\tau}^{m-1}(d) \neq z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{m-1}(z)$$

*for all $z \in D$.*

**Lemma 10.** *Assume the setup of Theorem 8 and $d \in F$.*
*(i) If $\tau(d^n) \neq d^n$ for all $z \in D$, then $d \neq z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{m-1}(z)$ for all $z \in D$.*
*(ii) If $\tau^{m-1}(d^n) \neq d^n$ for all $z \in D$, then $\tau^{m-1}(d) \neq z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{m-1}(z)$ for all $z \in D$.*

The proof generalizes the idea of the proof of [7, Proposition 13]:

*Proof.* (i) If $d = z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{m-1}(z)$ for some $z \in D$, then for $Z = \lambda(z)$ this means

$$Z\tau(Z)\cdots\tau^{m-1}(Z) = dI_n$$

and therefore $\det(Z)\det(\tau(Z))\cdots\det(\tau^{m-1}(Z)) = d^n$. Since the left-hand-side is fixed by $\tau^i$, this implies that $\tau^i(d^n) = d^n$ for $1 \leq i < m$, in particular, $\tau(d^n) = d^n$.
(ii) If $\tau^{m-1}(d) = z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{m-1}(z)$ for some $z \in D$ then analogously,

$$Z\tau(Z)\cdots\tau^{m-1}(Z) = \tau^{m-1}(d)I_n$$

and therefore $\det(Z)\det(\tau(Z))\cdots\det(\tau^{m-1}(Z)) = \tau^{m-1}(d)^n = \tau^{m-1}(d^n)$. Since the left-hand-side is fixed by $\tau$, this implies that $\tau^{m-1}(d^n) = d^n$. □

**Corollary 11.** *Assume the setup of Theorem 8 and $d \in F^\times$.*
*(i) Suppose that $m$ is prime and $F_0$ contains a primitive $m$th root of unity. If $\tau(d^n) \neq d^n$ and $\tau^{m-1}(d^n) \neq d^n$ for all $z \in D$, then $\mathrm{It}_R^m(D,\tau,d)$ is a division algebra.*
*(ii) Suppose $m = 3$. If $\tau(d^n) \neq d^n$ and $\tau^2(d^n) \neq d^n$ for all $z \in D$, then $\mathrm{It}_R^3(D,\tau,d)$ is a division algebra.*

## 4. The tensor product of two not necessarily associative cyclic algebras

Let $L/F_0$ be a cyclic Galois field extension of degree $n$ with $\mathrm{Gal}(L/F_0) = \langle\sigma\rangle$, and $F/F_0$ be a cyclic Galois field extension of degree $m$ with $\mathrm{Gal}(F/F_0) = \langle\tau\rangle$. Let $L$ and $F$ be linearly disjoint over $F_0$ and let $K = L \otimes_{F_0} F = L \cdot F$ be the composite of $L$ and $F$ over $F_0$, with Galois group $\mathrm{Gal}(K/F_0) = \langle\sigma\rangle \times \langle\tau\rangle$, where $\sigma$ and $\tau$ are canonically extended to $K$.

In the following, let $D_0 = (L/F_0, \sigma, c)$ and $D_1 = (F/F_0, \tau, d)$ be two cyclic algebras over $F_0$, i.e. $c \in L^\times$ and $d \in F^\times$. Let

$$A = (L/F_0, \sigma, c) \otimes_{F_0} (F/F_0, \tau, d).$$

Then $K$ is a subfield of $A$ of degree $mn$ over $F_0$ and $K = L \otimes_{F_0} F \subset \mathrm{Nuc}(A)$.

**Remark 12.** (i) Assume w.l.o.g. that $D_0$ is associative and $D_1$ is nonassociative. Then $D_0 \otimes_{F_0} F = \mathrm{Nuc}(D_0) \otimes_{F_0} \mathrm{Nuc}(D_1) \subset \mathrm{Nuc}(A)$ implies that the tensor product $A$ cannot be a nonassociative cyclic algebra.
(ii) $\mathrm{Gal}(K/F_0)$ is a cyclic group if and only if $m$ and $n$ are coprime. For two linearly disjoint cyclic fields $F$ and $L$ whose degrees over $F_0$ are not coprime and nonassociative cyclic algebras $(L/F_0, \sigma, c)$ and $(F/F_0, \tau, d)$, thus their tensor product $A = (L/F_0, \sigma, c) \otimes_{F_0} (F/F_0, \tau, d)$ has $K \subset \mathrm{Nuc}(A)$, which is not a cyclic field, and hence $A$ is not a nonassociative cyclic algebra. If $m$ and $n$ are coprime, $K$ is a cyclic field extension of degree $mn$ contained in $\mathrm{Nuc}(A)$. It is not clear if in that case $A$ could be isomorphic to a nonassociative cyclic algebra itself.

Let $\{1, e, e^2, \dots, e^{n-1}\}$ be the standard basis of the $L$-vector space $D_0$ and $\{1, f, f^2, \dots, f^{m-1}\}$ be the standard basis of the $F$-vector space $D_1$. $A$ is a $K$-vector space with basis

$$\{1 \otimes 1, e \otimes 1, \dots, e^{n-1} \otimes 1, 1 \otimes f, e \otimes f, \dots, e^{n-1} \otimes f^{m-1}\}.$$

Identify

$$A = K \oplus eK \oplus \dots \oplus e^{n-1}K \oplus fK \oplus efK \oplus \dots \oplus e^{n-1}f^{m-1}K.$$

Note that $D_0 \otimes_{F_0} F = (K/F, \sigma, c)$. An element in $\lambda(A)$ has the form

$$\begin{bmatrix} Y_0 & d\tau(Y_{n-1}) & d\tau^2(Y_{n-2}) & \dots & d\tau^{m-1}(Y_1) \\ Y_1 & \tau(Y_0) & d\tau^2(Y_{n-1}) & \dots & d\tau^{m-1}(Y_2) \\ \vdots & & \vdots & & \vdots \\ Y_{n-2} & \tau(Y_{n-3}) & \tau^2(Y_{n-4}) & \dots & d\tau^{m-1}(Y_{n-1}) \\ Y_{n-1} & \tau(Y_{n-2}) & \tau^2(Y_{n-3}) & \dots & \tau^{m-1}(Y_0) \end{bmatrix} \tag{2}$$

with $\lambda(d) \in \lambda(D_0 \otimes_{F_0} F)$, $Y_i \in \lambda(D_0 \otimes_{F_0} F)$. That means, $Y_i \in \mathrm{Mat}_n(K)$, and when the entries in $Y_i$ are restricted to elements in $L$, $Y_i \in \lambda(D_0)$ (multiplication with $d$ in the upper right triangle of the matrix means simply scalar multiplication with $d$).

**Theorem 13.** *(i) For $c \in L^\times$ and $d \in F^\times$, $(L/F_0, \sigma, c) \otimes_{F_0} (F/F_0, \tau, d) \cong \mathrm{It}_R^m(D_0 \otimes_{F_0} F, \tau, d)$.*
*(ii) Suppose that $D = (L/F_0, \sigma, c) \otimes_{F_0} F$ is an associative cyclic division algebra. Then*

$$S_f \cong (L/F_0, \sigma, c) \otimes_{F_0} (F/F_0, \tau, d)$$

*where $R = D[t; \widetilde{\tau}^{-1}]$ and $f(t) = t^m - d$.*

*Proof.* (i) The matrices in (2) also represent left multiplication with an element in the algebra $\mathrm{It}_R^m((K/F, \sigma, c), \tau, d)$, see (1). Thus the multiplications of both algebras are the same.
(ii) If $D_0 \otimes_{F_0} F$ is an associative division algebra then $S_f \cong \mathrm{It}_R^m((K/F, \sigma, c), \tau, d)$ with $R = (D_0 \otimes_{F_0} F)[t; \widetilde{\tau}^{-1}]$ and $f(t) = t^m - d$ by Theorem 8. $\square$

**Corollary 14.** *(i)* $\mathrm{It}_R^m(D_0 \otimes_{F_0} F, \tau, d) \cong \mathrm{It}_R^n(D_1 \otimes_{F_0} L, \sigma, c)$.
*(ii) The cyclic algebras*

$$(K/L, \tau, d) \text{ and } (K/F, \sigma, c)$$

*viewed as algebras over* $F_0$*, are subalgebras of*

$$(L/F_0, \sigma, c) \otimes_{F_0} (F/F_0, \tau, d)$$

*of dimension* $m^2 n$*, resp.* $n^2 m$*.*
*(iii) If* $(F/F_0, \tau, d)$ *is nonassociative then the subalgebra* $(K/L, \tau, d)$ *is nonassociative and thus division if* $m$ *is prime or, if* $m$ *is not prime, if* $1, d, \ldots, d^{m-1}$ *are linearly independent over* $L$*.*
*If* $(L/F_0, \sigma, c)$ *is nonassociative then the subalgebra* $(K/F, \sigma, c)$ *is nonassociative and thus division if* $n$ *is prime or, if* $n$ *is not prime, if* $1, c, \ldots, c^{n-1}$ *are linearly independent over* $F$*.*
*(iv) If* $m = st$ *and* $F_s = \mathrm{Fix}(\tau^s)$ *then*

$$(L/F_0, \sigma, c) \otimes_{F_0} (F/F_s, \tau^s, d)$$

*is isomorphic to a subalgebra of*

$$(L/F_0, \sigma, c) \otimes_{F_0} (F/F_0, \tau, d) = \mathrm{It}_R^m(D_0 \otimes_{F_0} F, \tau, d).$$

*Proof.* (i) This follows directly from Theorem 13 and the fact that

$$(L/F_0, \sigma, c) \otimes_{F_0} (F/F_0, \tau, d) \cong (F/F_0, \tau, d) \otimes_{F_0} (L/F_0, \sigma, c).$$

(ii) This is Lemma 3 and [11], Lemma 5 (which also holds if $D_0 \otimes_{F_0} F$ is not division), together with (i).
(iii) This follows from (ii), since $(F/F_0, \tau, d)$ is nonassociative if and only if $d \in F \setminus F_0$. This means $d \in K \setminus L$. The same argument holds for nonassociative $(L/F_0, \sigma, c)$.
(iv) This follows from [17], Theorem 3.3.2, see also [16]. □

## 5. Conditions on the tensor product to be a division algebra

**5.1.** To see when the tensor product of two associative algebras is a division algebra we have the classical result by Jacobson [4, Theorem 1.9.8], see also Albert [1, Theorem 12, Ch. XI]:

**Theorem 15.** *Let* $(F/F_0, \tau, d)$ *be a cyclic associative division algebra of prime degree* $p$*. Suppose that* $D_0$ *is a central associative algebra over* $F_0$ *such that* $D = D_0 \otimes_{F_0} F$ *is a division algebra. Then* $D_0 \otimes_{F_0} (F/F_0, \tau, d)$ *is a division algebra if and only if*

$$d \neq \widetilde{\tau}^p(z) \cdots \widetilde{\tau}(z) z$$

*for all* $z \in D$*.*

Note that here

$$d \neq \widetilde{\tau}^p(z) \cdots \widetilde{\tau}(z) z \text{ is equivalent to } d \neq z \widetilde{\tau}(z) \cdots \widetilde{\tau}^{m-1}(z)$$

since $d \in F_0$. This classical result has the following generalizations in the nonassociative setting:

**Theorem 16.** *Let* $(F/F_0,\tau,d)=\mathrm{Cay}(F,d)$ *be a nonassociative quaternion algebra. Let* $D_0=(L/F_0,\sigma,c)$ *be an associative cyclic algebra over* $F_0$ *of degree* $n$*, such that* $D=D_0\otimes_{F_0}F=(K/F,\sigma,c)$ *is a cyclic division algebra. Then*

$$(L/F_0,\sigma,c)\otimes_{F_0}(F/F_0,\tau,d)$$

*is a division algebra if and only if*

$$d\neq z\widetilde{\tau}(z)$$

*for all* $z\in D$.

*Proof.* This is Theorem 13 together with [9], Theorem 3.2 or alternatively, together with Theorem 6 (i). □

In the following, we use that $t^m-d\in D[t;\widetilde{\tau}^{-1}]$ is irreducible if and only if $t^m-d\in D^{op}[t;\widetilde{\tau}]$ is irreducible. Theorem 13 together with Theorem 6 and Lemma 10 yields a generalization of [4, Theorem 1.9.8]:

**Theorem 17.** *Let* $(F/F_0,\tau,d)$ *be an associative or nonassociative cyclic algebra of degree* $m$*. Let* $D_0=(L/F_0,\sigma,c)$ *be an associative cyclic algebra over* $F_0$ *of degree* $n$*, such that* $D=D_0\otimes_{F_0}F=(K/F,\sigma,c)$ *is a division algebra.*
*(a)* $(L/F_0,\sigma,c)\otimes_{F_0}(F/F_0,\tau,d)$ *is a division algebra if and only if one of the following holds:*
*(i)* $f(t)=t^m-d\in D[t;\widetilde{\tau}^{-1}]$ *is irreducible.*
*(ii)* $m$ *is prime,* $F_0$ *contains a primitive* $m$*th root of unity,*

$$d\neq z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{m-1}(z) \text{ and } \widetilde{\tau}^{m-1}(d)\neq z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{m-1}(z)$$

*for all* $z\in D$.
*(iii)* $m=3$ *and*

$$d\neq z\widetilde{\tau}(z)\widetilde{\tau}(z)^2 \text{ and } \widetilde{\tau}^2(d)\neq z\widetilde{\tau}(z)\widetilde{\tau}(z)^2$$

*for all* $z\in D$.
*(b) Suppose one of the following holds:*
*(i)* $m$ *is prime,* $F_0$ *contains a primitive* $m$*th root of unity,* $\tau(d^n)\neq d^n$ *and* $\tau^{m-1}(d^n)\neq d^n$ *for all* $z\in D$.
*(ii)* $m=3$, $\tau(d^n)\neq d^n$ *and* $\tau^2(d^n)\neq d^n$ *for all* $z\in D$.
*(iii)* $m=2$ *and* $\tau(d^n)\neq d^n$ *for all* $z\in D$.
*Then*

$$(L/F_0,\sigma,c)\otimes_{F_0}(F/F_0,\tau,d)$$

*is a division algebra.*

We also obtain the following condition using that $\mathrm{It}_R^m(D_0\otimes_{F_0}F,\tau,d)\cong(L/F_0,\sigma,c)\otimes_{F_0}(F/F_0,\tau,d)$ by Theorem 13:

**Corollary 18.** *Let* $A=(L/F_0,\sigma,c)\otimes_{F_0}(F/F_0,\tau,d)$ *where* $D_0=(L/F_0,\sigma,c)$ *is associative,* $D=D_0\otimes_{F_0}F$*. Suppose that* $m$ *is prime,* $m\neq 3$ *and* $F_0$ *contains a primitive* $m$*th root of unity, or that* $m=3$*. If* $d^n\neq a\tau(a)\cdots\tau^{m-1}(a)$ *and* $\tau^{m-1}(d^n)\neq a\tau(a)\cdots\tau^{m-1}(a)$ *for all* $a\in F^\times$*, then* $A$ *is a division algebra.*

*Proof.* Since $c \in F_0$ we have $N_{D/F}(\widetilde{\tau}(x)) = \tau(N_{D/F}(x))$ for all $x \in D$. Assume $d = z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{m-1}(z)$ and $\tau^{m-1}(d) = z\widetilde{\tau}(z)\cdots\widetilde{\tau}^{m-1}(z)$, then

$$N_{D/F}(d) = N_{D/F}(z)N_{D/F}(\widetilde{\tau}(z))\cdots N_{D/F}(\widetilde{\tau}^{n-1}(z)) = N_{D/F}(z)\tau(N_{D/F}(z))\cdots\tau^{m-1}(N_{D/F}(z))$$

and, analogously,

$$N_{D/F}(\tau^{m-1}(d)) = N_{D/F}(z)\tau(N_{D/F}(z))\cdots\tau^{m-1}(N_{D/F}(z)).$$

Put $a = N_{D/F}(z)$ to obtain the assertion from Theorem 17. □

In special cases, Theorem 16 yields straightforward conditions for the tensor product to be a division algebra, e.g. for the tensor product of two quaternion algebras (one of them associative and one not):

**Theorem 19.** *Let $F_0$ be of characteristic not 2. Let $(a, c)_{F_0}$ be a quaternion algebra over $F_0$ which is a division algebra over $F = F_0(\sqrt{b})$, and $(F_0(\sqrt{b})/F_0, \tau, d)$ a nonassociative quaternion algebra. Then the tensor product*

$$(a, c)_{F_0} \otimes_{F_0} (F_0(\sqrt{b})/F_0, \tau, d)$$

*is a division algebra over $F_0$.*

*Proof.* Here, $K = F_0(\sqrt{a}, \sqrt{b})$ with Galois group $G = \mathrm{Gal}(K/F_0) = \{id, \sigma, \tau, \sigma\tau\}$, where

$$\sigma(\sqrt{a}) = -\sqrt{a}, \quad \sigma(\sqrt{b}) = \sigma(\sqrt{b}),$$

$$\tau(\sqrt{a}) = \sqrt{a}, \quad \tau(\sqrt{b}) = -\sqrt{b},$$

$L = F_0(\sqrt{a})$ and $D = (a, c)_{F_0} \otimes F$. For $z = z_0 + iz_1 + jz_2 + kz_3 \in D$, $z_i \in F_0(\sqrt{b})$, $i^2 = a$, $j^2 = c$, we get

$$z\widetilde{\tau}(z) = (z_0\tau(z_0) + az_1\tau(z_1) + cz_2\tau(z_2) - acz_3\tau(z_3))$$

$$+i(z_0\tau(z_1) + z_1\tau(z_0) - cz_2\tau(z_3) + cz_3\tau(z_2))$$

$$+j(z_0\tau(z_2) + z_2\tau(z_3) + az_1\tau(z_3) - az_3\tau(z_1))$$

$$+k(z_0\tau(z_3) + z_3\tau(z_2) + z_1\tau(z_2) - z_2\tau(z_1)).$$

Since $(F_0(\sqrt{b})/F_0, \tau, d)$ is nonassociative, $d \in F_0(\sqrt{b})\setminus F_0$. Hence if we assume that $d = z\widetilde{\tau}(z)$ for some $z \in D$ then

$$d = z_0\tau(z_0) + a\sigma(z_1)\tau(z_1) + c\sigma(z_2)\tau(z_2) - ac\sigma(z_3)\tau(z_3)$$

$$= N_{F/F_0}(z_0) + aN_{F/F_0}(z_1) + cN_{F/F_0}(z_2) - acN_{F/F_0}(z_3) \in F_0,$$

a contradiction. Thus, by Theorem 16, the tensor product

$$(a, c)_{F_0} \otimes_{F_0} (F_0(\sqrt{b})/F_0, \tau, d)$$

is a division algebra. □

**Theorem 20.** *Let $F_0$ be of characteristic not 2, $F = F_0(\sqrt{b})$. Let $D_0 = (L/F_0, \sigma, c)$ be a cyclic algebra over $F_0$ of degree 3 such that $D = D_0 \otimes_{F_0} F$ is a division algebra over $F$, and $(F_0(\sqrt{b})/F_0, \tau, d)$ a nonassociative quaternion algebra. Let $d = d_0 + \sqrt{b}d_1 \in F \setminus F_0$ with $d_0, d_1 \in F_0$.*
*(i) If $3d_0^2 + bd_1^2 \neq 0$, then*

$$D_0 \otimes_{F_0} (F_0(\sqrt{b})/F_0, \tau, d)$$

*is a division algebra over $F_0$.*
*(ii) Let $F_0 = \mathbb{Q}$. If $b > 0$, or if $b < 0$ and $-\frac{b}{3} \notin \mathbb{Q}^{\times 2}$ then*

$$D_0 \otimes_{F_0} (F_0(\sqrt{b})/F_0, \tau, d)$$

*is a division algebra over $F_0$.*

*Proof.* $F = F_0(\sqrt{b})$ and $K = F_0(\sqrt{b})$.
(i) Here, $d^3 = d_0^3 + 3bd_0d_1^2 + \sqrt{b}d_1(3d_0^2 + bd_1^2)$, so if we want that $d^3 \neq \widetilde{\tau}(d^3)$, this is equivalent to $3d_0^2 + bd_1^2 \neq 0$. The assertion follows from Theorem 17 (b).
(ii) is a direct consequence from (i): for $F_0 = \mathbb{Q}$, $3d_0^2 + bd_1^2 > 0$ for all $b > 0$. For $b < 0$, the assertion is true since $3d_0^2 + bd_1^2 = 0$ if and only if $\frac{d_0}{d_1}^2 = -\frac{b}{3}$. □

We conclude with a necessary condition for $d$ in the general case:

**Proposition 21.** *Let $D_0 = (L/F_0, \sigma, c)$ be a an associative cyclic algebra of degree $n$ over $F_0$, such that $D = D_0 \otimes_{F_0} F$ is a division algebra. If $D_0 \otimes_{F_0} (F/F_0, \tau, d)$ is a division algebra then*

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

*for all $z \in D$.*

*Proof.* Again use that $t^m - d \in D[t; \widetilde{\tau}^{-1}]$ is irreducible if and only if $t^m - d \in D^{op}[t; \widetilde{\tau}]$ is irreducible. Let $\circ$ denote multiplication in $D^{op}$. By [4, p. 15, (1.3.8)], for $b \in D$, if $d = \widetilde{\tau}^{m-1}(z) \circ \cdots \circ \widetilde{\tau}(z) \circ z = z\widetilde{\tau}(z) \cdots \widetilde{\tau}^{m-1}(z)$ for some $z \in D^{op}$ then $f(t) = g(t)(t - b)$. Thus if $f(t) = t^m - d$ is irreducible then $d \neq z\widetilde{\tau}(z) \cdots \widetilde{\tau}^{m-1}(z)$ for all $z \in D$. □

## 6. Tensoring two nonassociative algebras

For the sake of completeness, we finish by studying the tensor product of two nonassociative cyclic algebras.

Let us consider the case that $K/L$ is a Galois field extension of degree 2. Imitating the proof of [9, Theorem 3.2] we obtain:

**Theorem 22.** *Let $D = (K/F, \sigma, c)$ be a nonassociative cyclic division algebra and $A = \mathrm{It}_R(D, \tau, d)$.*
*(i) If $A$ is a division algebra then $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.*
*(ii) If*

$$d \neq (\ u\,(v^{-1}(\,\widetilde{\tau}(u)w)\,)\,)(\,w^{-1}\widetilde{\tau}(v)^{-1}\,)$$

*for all $u, v, w \in D$, then $A$ is a division algebra.*
*(iii) If*

$$N_{K/F}(d) \neq M_D(\widetilde{\tau}(v)w)^{-1} M_D(\widetilde{\tau}((vu)w^{-1})u),$$

*for all $u, v, w \in D$, then $A$ is a division algebra.*

It is not clear if the criteria (ii) or (iii) can be satisfied.

*Proof.* (i) If there is $z \in D$ such that $d = z\widetilde{\tau}(z)$, then

$$(z,1)(-\widetilde{\tau}(z),1) = (-z\widetilde{\tau}(z)+d, -\widetilde{\tau}(z)+\widetilde{\tau}(z)) = (0,0),$$

so $A$ contains zero divisors. We conclude that if $A$ is division then $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.
(ii) Suppose

$$(0,0) = (u,v)\cdot(u',v') = (uu' + d\widetilde{\tau}(v)v', vu' + \widetilde{\tau}(u)v')$$

for some $u, v, u', v' \in D$. This is equivalent to

$$uu' + d\widetilde{\tau}(v)v' = 0 \text{ and } vu' + \widetilde{\tau}(u)v' = 0. \tag{3}$$

Assume $v' = 0$, then $uu' = 0$ and $vu' = 0$. Hence either $u' = 0$ and so $(u', v') = 0$ or $u' \neq 0$ and $u = v = 0$. Also, if $v = 0$ then $uu' = 0$ and $\widetilde{\tau}(u)v' = (0,0)$, thus $u = 0$ and $(u,v) = (0,0)$, or $(u',v') = (0,0)$ and we are done.

So let $v' \neq 0$ and $v \neq 0$. Then $u' = -v^{-1}(\widetilde{\tau}(u)v')$, hence $u(v^{-1}(\widetilde{\tau}(u)v')) = d\widetilde{\tau}(v)v'$. Rearranging gives

$$d = (\ u\,(v^{-1}(\,\widetilde{\tau}(u)v')\,)\ )(\,\widetilde{\tau}(v)v'\,)^{-1} =$$
$$(\ u\,(v^{-1}(\,\widetilde{\tau}(u)v')\,)\ )(\,v'^{-1}\widetilde{\tau}(v)^{-1}\,),$$

so if

$$d \neq (\ u\,(v^{-1}(\,\widetilde{\tau}(u)w)\,)\ )(\,w^{-1}\widetilde{\tau}(v)^{-1}\,)$$

for all $u, v, w \in D$ then $A$ is a division algebra.
(iii) From (3) we obtain for $v \neq 0$, $v' \neq 0$ that $vu' = -\widetilde{\tau}(u)v'$ yields $\widetilde{\tau}(u) = -(vu')v'^{-1}$, i.e. $u = -\widetilde{\tau}((vu')v'^{-1})$. Substituted into the first equation this gives

$$\widetilde{\tau}((vu')v'^{-1})u' = d\widetilde{\tau}(v)v'.$$

Applying $M_D$ to both sides of this equation we get

$$M_D(\widetilde{\tau}((vu')v'^{-1})u') = M_D(d\widetilde{\tau}(v)v'),$$

i.e.

$$M_D(\widetilde{\tau}((vu')v'^{-1})u') = N_{K/F}(d)M_D(\widetilde{\tau}(v)v'),$$

implying

$$N_{K/F}(d) = M_D(\widetilde{\tau}(v)v')^{-1}M_D(\widetilde{\tau}((vu')v'^{-1})u').$$

□

For the tensor product of a nonassociative cyclic algebra and a nonassociative quaternion algebra, we get from Theorem 22 (i):

**Corollary 23.** *Let $(F/F_0, \tau, d) = \mathrm{Cay}(F, d)$ be a nonassociative quaternion algebra. Let $D_0 = (L/F_0, \sigma, c)$ be a nonassociative cyclic algebra of degree $n$ over $F_0$, such that $D = D_0 \otimes_{F_0} F$ is a division algebra. If $(L/F_0, \sigma, c) \otimes_{F_0} (F/F_0, \tau, d)$ is a division algebra then $d \neq z\widetilde{\tau}(z)$ for all $z \in D$.*

It is not clear whether this is an 'if and only if' condition, since by Theorem 22 (ii), (iii) we can only say that in the set-up of Corollary 23, $A$ is a division algebra, if

$$d \neq (\ u\,(v^{-1}(\,\widetilde{\tau}(u)w)\,)\ )(\,w^{-1}\widetilde{\tau}(v)^{-1}\,)$$

for all $u, v, w \in D$ or, alternatively, if

$$N_{K/F}(d) \neq M_D(\widetilde{\tau}(v)w)^{-1}M_D(\widetilde{\tau}((vu)w^{-1})u),$$

for all $u, v, w \in D$.

The situation seems to get even more complicated for $m > 2$ where we have some partial results:

**Proposition 24.** *Let $A = (L/F_0, \sigma, c) \otimes_{F_0} (F/F_0, \tau, d)$ with $(F/F_0, \tau, d)$ of degree 3 and $(K/F, \sigma, c)$ a division algebra (with both algebras not assumed to be associative). If $A$ is a division algebra then $d \neq z(\widetilde{\tau}(z)\widetilde{\tau}^2(z))$ for all $z \in D$.*

*Proof.* Write $A = \mathrm{It}_R^3((L/F_0, \sigma, c) \otimes_{F_0} F, \tau, d)$. Suppose $d = z(\widetilde{\tau}(z)\widetilde{\tau}^2(z))$ for some $z \in D$. Then $(-z, 1, 0)(\widetilde{\tau}(z)\widetilde{\tau}^2(z), \widetilde{\tau}^2(z), 1) = (0, 0, 0)$ and $A$ has zero divisors. □

**Remark 25.** For $A = (L/F_0, \sigma, c) \otimes_{F_0} (F/F_0, \tau, d)$, the map $M_A(x) = \det(L_x) = \det(\lambda(M(x)))$ can be seen as a generalization of the norm of an associative central simple algebra, since $M_A = N_{A/F}$ if both cyclic algebras in the tensor product $A$ are associative.

For all $X = \lambda(M(x)) = \lambda(x) \in \lambda(A) \subset \mathrm{Mat}_{nm}(K)$, and $D_0 = (L/F_0, \sigma, c)$ associative, $D = D_0 \otimes_{F_0} F$, we have $\det X \in F$ (cf. [10], [9, Corollary 2] for $m = 2$). Thus if $D_0$ is associative, $M_A : A \to F$. In that case, we also have

$$M_A(x) = N_{D/F}(x)\tau(N_{D/F}(x)) \cdots \tau(N_{D/F}(x)) = N_{F/F_0}(N_{D/F}(x))$$

for all $x \in (K/F, \sigma, c)$ (which is easy to see from applying the determinant to the matrix of $L_x$ in Equation (4) for some $x \in D$).

## References


[1] A. A. Albert, "Structure of algebras", in American Mathematical Society Colloquium Publications, Provdence, RI, USA AMS 24, 1961.

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

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

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

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

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

[7] N. Markin, F. Oggier, *Iterated Space-Time Code Constructions from Cyclic Algebras*, IEEE Trans. Inform. Theory (9) 59, September 2013, 5966-5979.

[8] 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.

[9] S. Pumplün, *How to obtain algebras used for fast-decodable space-time block codes*, Adv. Math. Comm. 8 (3) (2014), 323-342.

[10] S. Pumplün, A. Steele, *Fast-decodable MIDO codes from nonassociative algebras*, to appear in Int. J. of Information and Coding Theory (IJICOT), available at `http://molle.fernuni-hagen.de/~loos/jordan/index.html`

[11] S. Pumplün, A. Steele, *The nonassociative algebras used to build fast-decodable space-time block codes*, preprint 2014, available at `http://molle.fernuni-hagen.de/~loos/jordan/index.html`

[12] S. Pumplün, A. Steele, *Algebras with semi-multiplicative maps*, preprint 2013, available at `http://molle.fernuni-hagen.de/~loos/jordan/index.html`

[13] S. Pumplün, T. Unger, *Space-time block codes from nonassociative division algebras*, Adv. Math. Comm. 5 (3) (2011), 609-629.

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

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

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

[17] A. Steele, *Some new classes of algebras*, PhD Thesis, Nottingham, 2013.

[18] W.C. Waterhouse, *Nonassociative quaternion algebras*, Algebras Groups Geom. 4 (3) (1987), 365–378.

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

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