Journal of Algebra 451 (2016) 145–165

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Tensor products of nonassociative cyclic algebras

S. Pumplün

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

ARTICLE INFO

Article history:
Received 23 February 2015
Available online 22 December 2015
Communicated by Alberto Elduque

MSC:
primary 17A35
secondary 16S36, 94B05

Keywords:
Cyclic algebra
Nonassociative cyclic algebra
Nonassociative quaternion algebra
Tensor product
Division algebra

ABSTRACT

We study the tensor product of an associative and a nonassociative cyclic algebra. The condition for the tensor product to be a division algebra equals the classical one for the tensor product of 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. Applications to space–time block coding are discussed.

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 [17]. Nonassociative quaternion algebras (the case $n = 2$) constituted the first known examples of a nonassociative division algebra (Dickson [5]). Nonassociative cyclic algebras were investigated over arbitrary fields by Steele [19,20], see also [14].

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

http://dx.doi.org/10.1016/j.jalgebra.2015.12.007

In the following we study the tensor product $A = D_0 \otimes_{F_0} D_1$ of an associative and a nonassociative cyclic algebra over a field F_0 and give conditions for A to be a division algebra. We discover that these tensor product algebras are used in space–time block coding [11–13], and employed to construct some of the iterated codes by Markin and Oggier [9].

After recalling results needed in the paper in Section 1, results by Petit [10] are used to show that the iterated algebras $\mathrm{It}_R^m(D, \tau, d)$ introduced in [11–13] can be defined using polynomials in skew-polynomial rings over D when D is a cyclic division algebra (Theorem 7) in Section 2. In Section 3 we show that for an associative division algebra $D = (L/F_0, \sigma, c) \otimes_{F_0} F$, L and F linearly disjoint over F_0,

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

where the twisted polynomial $f(t) = t^m - d \in D[t; \widetilde{\tau}^{-1}]$, $\widetilde{\tau}$ an automorphism of D canonically extending τ, is used to construct the algebra S_f (Theorem 11). Section 3 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, L and F linearly disjoint over F_0, 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 16).

Assume further that m is prime and if $m \neq 2, 3$, that F_0 contains a primitive mth root of unity. Then $(L/F_0, \sigma, c) \otimes_{F_0} (F/F_0, \tau, d)$ is a division algebra if and only if

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

for all $z \in D$. This generalizes the classical condition for the tensor product of two associative cyclic algebras [6, Theorem 1.9.8] (see also Theorem 13), to the nonassociative setting. Some more detailed conditions are obtained for special cases. For instance, if $\mathrm{char}\, F_0 \neq 2$, D_0 is an associative quaternion algebra over F_0 which remains a division algebra over F, and D_1 a nonassociative quaternion algebra, such that D_0 and D_1 do not share a common subfield, then $D_0 \otimes_{F_0} D_1$ is always a division algebra over F_0 (Theorem 17). In Section 4, we discuss how our results can be applied to systematically construct fully diverse fast-decodable space–time block codes for nm transmit and m receive antennas. We thus generalize the set-up discussed in [9, Section V.A] which is limited to tensor products of a cyclic algebra of degree three and a nonassociative quaternion algebra, i.e. to $n = 3$, $m = 2$, and see that Theorems 16, 17 and 18 provide conditions for an iterated code consisting of larger matrices (where $m > 2$) to be fully diverse. We then design a new family of fast-decodable fully diverse 4×2-codes with non-vanishing determinant starting with the Silver code, which have decoding complexity $O(M^{4.5})$, i.e. the same decoding complexity as all state-of the art fast-decodable fully diverse 4×2 codes. Thus our construction allows us to systematically design codes whose decoding complexity is competitive with the ones designed 'ad hoc' like the SR-code [16, IV.B] or the code in [8] and which also have non-vanishing determinant.