Communications in Mathematics **32** (2024), no. 2, 153–184
DOI: https://doi.org/10.46298/cm.12223

Inner isotopes associated with automorphisms of commutative associative algebras

Vladimir Tkachev

Abstract. The principal observation of the present paper is that an inner isotopy (i.e. a principal isotopy defined by an algebra endomorphism) is a very helpful instrument in constructing and studying interesting classes of nonassociative algebras. By using methods developed in the paper, we define a new class of commutative nonassociative algebras obtained by inner isotopy from commutative associative polynomial algebras. There is a natural bijection between isomorphism classes of our algebras and integer partitions of the algebra dimensions. Among the interesting features of the nonassociative algebras constructed are that these algebras are generic, some of examples are axial and metrized algebras. We completely describe both the set of algebra idempotents and their spectra.

Contents

MSC 2020: 12E05 (primary), 17A01 (secondary)
Keywords: Polynomial rings, Nonassocative algebras, Medial algebras, Idempotents, Integer Partitions.
Contact information:
Vladimir Tkachev:
Affiliation: Linköping University, Sweden.
Email: vladimir.tkatjev@liu.se

To the memory of Yakov Krasnov (1956-2023)
my friend and colleague.

1 Introduction

By an algebra $(\mathbb{A}, *)$ we understand a nonassociative algebra over a field $\mathbf{K}$ of $\mathrm{char}(\mathbf{K}) \neq 2, 3$ with multiplication $*$. An element $c \in \mathbb{A}$ is called an idempotent if $c * c = c$. The set of nonzero idempotents of $(\mathbb{A}, \cdot)$ is denoted by $\mathrm{Idm}(\mathbb{A}, *)$. Given an element $a \in (\mathbb{A}, *)$, we denote by $L_*(a)x \to a * x$ the left multiplication operator by a and $\mathbb{A}_\lambda(a)$ the kernel of $(\lambda \mathbb{1}_{\mathbb{A}} - L_*(a))$, where $\mathbb{1}_{\mathbb{A}}$ is the identity operator.

A commutative algebra $(\mathbb{A}, *)$ is called *isospectral* if the spectrum of $L_*(c)$ is the same for any nonzero idempotent c. By using the syzygy method, it was established in [16] that if an isospectral algebra $(\mathbb{A}, *)$ is generic (see Definition 1.1 below) then the common spectrum of the algebra idempotents consists of simple eigenvalues satisfying $\lambda^{\dim \mathbb{A}} = 1$. A further analysis given in [17] reveals that under some mild conditions, an isospectral generic algebra must be *medial*, i.e. the algebra multiplication associates on pairs:

$$(x * y) * (z * t) = (x * z) * (y * t),$$

and, moreover, such an algebra is an inner isotopy of a certain commutative associative algebra. Recall that given an algebra $(\mathbb{A}, *)$, its *inner isotope* $(\mathbb{A}, *_h)$ is the vector space $\mathbb{A}$ with the new multiplication

$$x *_h y = h(x * y) = h(x) * h(y),$$

where $h \in \mathrm{Aut}(\mathbb{A}, *)$ is an automorphism of $(\mathbb{A}, *)$. More precisely, the medial isospectral generic algebras discussed in [17] are exactly the inner isotopes of the quotient polynomial algebra $\mathbf{K}[z]/(z^n - 1)$ under the automorphism $\tau \in \mathrm{Aut}(\mathbf{K}^n, \bullet)$ acting by substitution $[p(z)] \to [p(\epsilon_n z)]$, where ϵ_n is a primitive root of unity of order n. The corresponding inner isotope algebra $(\mathbf{K}[z]/(z^n - 1), \bullet_\tau)$ has many distinguished properties (see Section 10.2 below for $n = 3$ and Section 7 for the general case).

In this regard, it is natural to find the full automorphism group $\mathrm{Aut}(\mathbf{K}^n, \bullet)$ and characterize the corresponding (isomorphy classes of) inner isotopes of $(\mathbf{K}^n, \bullet)$. A similar approach is also relevant for an arbitrary algebra $(\mathbb{A}, *)$ and its inner isotopes $(\mathbb{A}, *_h)$.

These questions were an original motivation for the present paper. As we shall see, an inner isotopy is a very helpful instrument for constructing of interesting classes of nonassociative algebras. In particular, this approach is already fruitful for the simplest possible case when the initial algebra is commutative and associative. In that case, any nontrivial inner isotopy destroys the associativity but not so much: any inner isotope of a (commutative) associative algebra is always a medial algebra, see Corollary 5.2.

A relevant in the present context is the mentioned above concept of *generic* nonassociative algebras [16]. The definition comes back to Segre's observation [24] that idempotents in an n-dimensional commutative algebra $(\mathbf{K}^n, *)$ over an algebraically closed field $\mathbf{K}$ with a basis $\{e_i\}_{1\le i\le n}$ can be interpreted as the set of common zeros of n quadratic polynomials

$$\Phi_k(x) := (x * x - x)_k = \sum_{1\le i,j\le n} a_{ijk} x_i x_j - x_k = 0, \qquad 1 \le k \le n,$$

in $\mathbf{K}^n$, where $x = \sum_{1\le i\le n} x_i e_i$ and a_{ijk} are the structural constant of $*$ in the basis $\{e_i\}$. By the Bézout theorem the number of intersection points (i.e. the algebra idempotents) properly counted in the projective space $\mathbf{K}\mathbb{P}^n$ is either 2^n or infinite. An intersection point c is simple if the quadrics are in relative general position at c. On the algebra level, the latter is equivalent to that the idempotent c is *regular* [32], i.e. the Jacobian of the quadratic endomorphism $\Phi(x) : \mathbf{K}^n \to \mathbf{K}^n$ is nonzero: $\det(D\Phi(x)) = \det(L_*(c) - \frac{1}{2}\mathbb{1}_{\mathbb{A}}) \neq 0$. Then the Bézout estimate holds:

$$\text{the number of } \textit{regular} \text{ idempotents of } \mathbb{A} \ \le 2^{\dim \mathbb{A}}. \tag{1}$$

In general, if the ground field $\mathbf{K}$ is not algebraically closed then the algebra $(\mathbb{A}, *, \mathbf{K}')$ over an algebraic extension $\mathbf{K}'$ of $\mathbf{K}$ has the same dimension, and any idempotent regular in $(\mathbb{A}, *, \mathbf{K})$ is a regular idempotent in $(\mathbb{A}, *, \mathbf{K}')$. Applying (1) to $(\mathbb{A}, *, \mathbf{K}')$, this implies that (1) also holds in $(\mathbb{A}, *, \mathbf{K})$. This motivates the following definition.

Definition 1.1. A commutative nonassociative algebra $\mathbb{A}$ over an arbitrary field $\mathbf{K}$ is called **generic** if it has exactly $2^{\dim \mathbb{A}}$ distinct regular idempotents.

Remark 1.2. An algebra on a vector space V is uniquely identified with a point of the set of all bilinear multiplication $V^* \otimes V^* \otimes V$ on V. In this sense, the subset of generic algebras is a Zariski open subset of $V^* \otimes V^* \otimes V$. The above definition has appeared in [16], [15] and it should not be confused with some similar analogues, for example in [27], [28].

In this paper, we show that under some natural assumptions any inner isotope of a commutative associative algebra is generic and, moreover, we explicitly characterize the set of idempotents and their spectral properties.

Another relevant concept here is the so-called axial algebras, i.e. the algebras generated by a finite subset of idempotents which satisfy a common fusion law. More precisely, a **fusion law** is a set $\mathcal{F} \subset \mathbf{K}$ together with a symmetric binary map $\theta : \mathcal{F} \times \mathcal{F} \to 2^{\mathcal{F}}$.

Definition 1.3 ([14]). Given a fusion law $\mathcal{F}$, a commutative algebra $(\mathbb{A}, *)$ over $\mathbf{K}$ together with a distinguished subset of elements X (the called *axes*) is an $\mathcal{F}$-axial algebra if $(\mathbb{A}, *)$ is generated by X, for each $c \in X$, c is a semisimple idempotent, namely $\mathbb{A} = \oplus_{\lambda\in\mathcal{F}}\mathbb{A}_\lambda(c)$ and for $\lambda, \mu \in \mathcal{F}$:

$$\mathbb{A}_\lambda(c) * \mathbb{A}_\mu(c) \subset \mathbb{A}_{\theta(\lambda,\mu)}(c).$$

An axial algebra is called *primitive* if each idempotent in X is primitive, i.e. $\dim \mathbb{A}_1(a) = 1$ for any $a \in X$.

The isospectral generic algebras considered in [16] and [17] are *axial* algebras. The axial algebra concept is an important tool in understanding of finite groups: it appears that many interesting groups (for example, 3-transposition groups including certain simple sporadic groups, in particular, the monster group) arise as automorphism groups of cubic forms on suitable modules [25], [19], [26], [22], [8] by virtue of a correspondence between certain involutions generating a group and a distinguished family of idempotents in an appropriate (non)associative commutative algebra. Such a correspondence normally is very individual and drastically depends on a source group/algebra, as well as its combinatorial or geometrical realizations [3], [6]. Some recent developments in the axial algebra project can be found [21], [9], [4], [7], [14], [10], [2] and the references therein.

The algebras discussed in the present paper fit perfectly this context and provide us with new examples of axial algebras with known automorphism groups. We only outline some partial results in this direction (see especially the explicit examples in Section 10), while the general discussion will be addressed elsewhere in the second part of this paper.

Remark 1.4. We are very grateful to the referees for pointing us out the existence of the isomorphism (17). In the original version of our paper [31], we used a different exposition based on the polynomial model $\mathbf{K}[z]/P$. The isomorphism (17) simplifies several proofs below and the structure of the idempotent set becomes more transparent when written in this form. Still, we believe that the polynomial model $\mathbf{K}[z]/P$ is also of interest, especially for some particular choices of the polynomial P; see fore example, the criterion given in Proposition 9.9 below. We refer an interested reader to [31] for the original presentation and more details concerning the polynomial model.

The paper is **organized** as follows. In Section 2, we recall some general concepts and facts used in the paper. In section 3, we outline the general properties of inner isotopes of an arbitrary algebra and in section 4 we specify these results for commutative associative algebras. In particular, we show that an inner isotope of a commutative associative algebra must be medial. In section 5, we develop an appropriate category-theoretical context for our considerations. The main result of this section states that the categories of calibrated special commutative medial algebras is isomorphic to the category of calibrated commutative associative algebras. In section 6 we discuss the properties of idempotents in an arbitrary medial algebra. In section 7 we study the automorphism group of a quotient polynomial algebra and determine its inner isotopes. We characterize the set of idempotents and theirs spectra in Section 8. The automorphism groups of the obtained algebras

are studied in Section 9. Finally, in section 10 we illustrate our results in the case $n = 3$.

2 Preliminaries

By $\bar{n}$ we denote the set of indices $\{1, 2, \dots, n\}$. We recall some standard definitions following [23], see also [1, p.149]. $(\mathbb{A}, \bullet)$ denotes an algebra with a multiplication $\bullet$ on a vector space $\mathbb{A}$. All algebras below are assumed to be commutative but maybe nonassociative.

If $(\mathbb{B}, \bullet)$ and $(\mathbb{C}, \bullet)$ are ideals of an algebra $(\mathbb{A}, \bullet)$ such that $\mathbb{A}$ as a vector space is the direct sum of $\mathbb{B}$ and $\mathbb{C}$ then $(\mathbb{A}, \bullet)$ is called the *direct sum*:

$$(\mathbb{A}, \bullet) = (\mathbb{B}, \bullet) \oplus (\mathbb{C}, \bullet).$$

Note that in this case $\mathbb{B} \bullet \mathbb{C} = 0$, so that $(\mathbb{B}, \bullet)$ and $(\mathbb{C}, \bullet)$ are *orthogonal*.

Given any two arbitrary algebras $(\mathbb{B}, \star)$ and $(\mathbb{C}, *)$ over a field $\mathbf{K}$, one can construct an algebra $(\mathbb{A}, \bullet)$ over $\mathbf{K}$ such that $(\mathbb{A}, \bullet)$ is the direct sum $(\mathbb{A}, \bullet) = (\mathbb{B}', \bullet) \oplus (\mathbb{C}', \bullet)$ of ideals $(\mathbb{B}', \bullet)$ and $(\mathbb{C}', \bullet)$ which are isomorphic respectively to $(\mathbb{B}, \star)$ and $(\mathbb{C}, *)$: $\mathbb{A}$ as a vector space is the Cartesian product of $\mathbb{B}$ and $\mathbb{C}$ with the multiplicative structure $\bullet$ defined by the coordinate-wise multiplication $(b_1, c_1) \bullet (b_2, c_2) = (b_1 \star b_2, c_1 * c_2)$ for elements $(b_1, c_1), (b_2, c_2) \in \mathbb{B} \times \mathbb{C}$. Then, for example, $(\mathbb{B}, \star)$ is isomorphic to the ideal $(\mathbb{B}', \bullet) = ((\mathbb{B}, 0), \bullet)$ of $(\mathbb{A}, \bullet)$. The resulting algebra is called the direct product of algebras $(\mathbb{B}, \star)$ and $(\mathbb{C}, *)$. In the above notation,

$$(\mathbb{B}, \star) \times (\mathbb{C}, *) \cong (\mathbb{B} \times \mathbb{C}, \bullet) \cong (\mathbb{B}', \bullet) \oplus (\mathbb{C}', \bullet)$$

As in the case of vector spaces, the notion of direct sum extends to an arbitrary set of summands. We shall have occasion to use only finite direct sums.

In particular, rhe field $\mathbf{K}$ is a commutative associative algebra over itself, denoted by $(\mathbf{K}, \cdot)$. The direct summa of $n \geq 1$ copies of $\mathbf{K}$ with the coordinate-wise multiplication is denoted by $(\mathbf{K}^n, \bullet)$. The $\bullet$-idempotents

$$e_i = (0, \dots, 1, \dots, 0), \qquad 1 \leq i \leq n \tag{2}$$

form the standard basis of $\mathbf{K}^n$. Let x_i denote the corresponding coordinate of $x \in \mathbf{K}^n$. Given any index $j \in \{1, 2, \dots, n\}$, the subspaces

$$\langle e_i \rangle := \{x \in \mathbf{K}^n : \, x_i = 0 \ \text{ for all } i \neq j\} \tag{3}$$

are (pairwise orthogonal) ideals of $(\mathbf{K}^n, \bullet)$ and

$$(\mathbf{K}^n, \bullet) = \bigoplus_{j=1}^{n} \langle e_j \rangle.$$

Below we shall need the following observation.

Proposition 2.1. *Let* $(\mathbb{A},\bullet)=\bigoplus_{j=1}^r(\mathbb{B}_j,\bullet)$*, where* $(\mathbb{B}_j,\bullet)$ *are ideals. Then* c *is an idempotent in* $(\mathbb{A},\bullet)$ *if and only if there are (uniquely determined) pairwise orthogonal idempotents* $c_j\in(\mathbb{B}_j,\bullet)$ *such that* $c=\sum_{j=1}^r c_j$*. Moreover, in this case*

$$\det(\lambda\mathbb{1}_{\mathbb{A}})-L_\bullet(c))=\prod_{j=1}^r\det(\lambda\mathbb{1}_{\mathbb{B}_j}-L_\bullet(c_j)) \tag{4}$$

The algebra $(\mathbb{A},\bullet)$ *is generic if and only each ideal* $(\mathbb{B}_j,\bullet)$ *is so.*

Proof. It follows for the assumptions that $\mathbb{B}_i\bullet\mathbb{B}_j=0$ for $i\neq j$. Let $x\in\mathbb{A}$ and let $x=\sum_{j=1}^r x_j$ be the corresponding orthogonal decomposition, $x_j\in\mathbb{B}_j$. Then $x\bullet x=\sum_{j=1}^r x_j\bullet x_j$, where $x_j\bullet x_j\in\mathbb{B}_j$ and $x_i\bullet x_j=0$ whenever $i\neq j$. It follows that x is an idempotent on $(\mathbb{A},\bullet)$ if and only if x_j is an idempotent in $(\mathbb{B}_j,\bullet)$ for all $1\leq j\leq r$, thus implying the first part of the proposition.

Next, let $(\mathbb{A},\bullet)$ be generic. Then $(\mathbb{A},\bullet)$ contains exactly 2^n distinct regular idempotents, where $n=\dim\mathbb{A}$. It follows from (4) that all idempotents in each ideal $\mathbb{B}_j$ are regular. If $\dim\mathbb{B}_j=n_j$ then $n=n_1+\ldots+n_r$. It follows from the above idempotent decomposition that $m_1\cdot\ldots\cdot m_r=2^n$, where m_j is the cardinality of the set of idempotents in $\mathbb{B}_j$, hence $m_j=2^{k_j}$ for some nonnegative integer k_j. On the other hand by the Bezout inequality (1) we have $m_j=2^{k_j}\leq 2^{n_j}$, hence $2^n=m_1\cdot\ldots\cdot m_r\leq 2^{n_1+\ldots+n_r}=2^n$ which implies that in fact $m_j=2^{k_j}=2^{n_j}$, i.e. each $\mathbb{B}_j$ is generic. In the converse direction, if each ideal $\mathbb{B}_j$ is generic then $(\mathbb{A},\bullet)=\bigoplus_{j=1}^r(\mathbb{B}_j,\bullet)$ has by Proposition 2.1 at least $2^{n_1}\cdot\ldots 2^{n_r}=2^n$ distinct regular idempotents, hence it is generic. □

We also fix some standard terminology and facts from permutation theory. Any permutation $\sigma\in S_n$ can be written in *cyclic form* (or a disjoint cycle decomposition)

$$\sigma=\sigma_1\ldots\sigma_r\in S_n. \tag{5}$$

For any $1\leq i,j\leq r$, the *cycles* σ_i and σ_j commute, therefore the order in (5) in inessential. Then cycles σ_j can be naturally thought of as orbits of a faithful action of the cyclic group $\langle\sigma\rangle$ generated by σ on the et of indices $\bar{n}:=\{1,\ldots,n\}$. To differ a cycle σ_j as a group element and as an orbit, we denote the latter by $[\sigma_j]\subset\bar{n}$. By $|\sigma_i|$ we denote the *length* of the cycle σ_i, i.e. the cardinality of the orbit $[\sigma_i]$. The *type of a permutation* is the integer partition of n,

$$|\sigma_1|+\ldots+|\sigma_r|=n, \tag{6}$$

formed from the cycle; we write it by $\mathrm{type}(\sigma)=(|\sigma_1|,\ldots,|\sigma_r|)$.

Definition 2.2. Given $\sigma\in S_n$ let $\sigma=\sigma_1\ldots\sigma_r$ be its disjoint cycle decomposition and $s_i=|\sigma_i|$. A field $\mathbf{K}$ will be said σ-**admissible**, if it is a splitting field for all polynomials z^t-1, where $t\in S:=\{s_1,\ldots,s_r,2^{s_1}-1,\ldots,2^{s_r}-1\}$. If $\mathbf{K}$ has a finite characteristic, to avoid complications, we additionally assume that the characteristic is co-prime with all numbers in S,

3 Inner isotopes

Two algebras $(\mathbb{A}, \diamond)$ and $(\mathbb{B}, \cdot)$ are called **isotopic**, if there is an *isotopism* (α, β, γ), i.e. a triple of nondegenerate linear maps $\mathbb{A} \to \mathbb{B}$ such that $\alpha(x) \cdot \beta(y) = \gamma(x \diamond y)$ holds for any $x, y \in \mathbb{A}$. If $\alpha = \beta$ the isotopy is called *strong*. If $\mathbb{A} = \mathbb{B}$ and $\gamma = \mathbb{1}_{\mathbb{A}}$ in the identity map, then an isotopy is called a **principal autotopy**.

Definition 3.1. Given an algebra $(\mathbb{A}, \bullet)$ and an algebra endomorphism $h \in \mathrm{End}(\mathbb{A}, \bullet)$, we define a new algebra $(\mathbb{A}, \bullet_h)$ on the vector space $\mathbb{A}$ by

$$x \bullet_h y = h(x) \bullet h(y) = h(x \bullet y). \tag{7}$$

The new algebra $(\mathbb{A}, \bullet_h)$ is called a **weak inner isotope** of $(\mathbb{A}, \bullet)$. If $h \in \mathrm{Aut}(\mathbb{A}, \bullet)$, $(\mathbb{A}, \bullet_h)$ is called an **inner isotope**.

The above definition is a particular case of a **strong principal autotopy**; more precisely, the algebra $(\mathbb{A}, \bullet_h)$ is an principal isotopic of $(\mathbb{A}, \bullet)$ with $(h, h, \mathbb{1}_{\mathbb{A}})$ where the map h is an $\bullet$-*algebra homomorphism*.

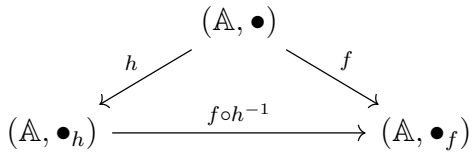
Remark 3.2. In the converse direction, if an endomorphism h is invertible then $(\mathbb{A}, \bullet)$ is an inner isotope of $(\mathbb{A}, \bullet_h)$. Indeed, by virtue of (7), $x \bullet y = h^{-1}(x \bullet_h y)$, therefore the linear endomorphism h^{-1} is also an $\bullet_h$-algebra endomorphism.

We distinguish the case when h is an bijective, i.e. h is an automorphism of $(\mathbb{A}, \bullet)$ and $(\mathbb{A}, \bullet_h)$ is an inner isotopy. In this case, if $h, f \in \mathrm{Aut}(\mathbb{A}, \bullet)$ then $(\mathbb{1}_{\mathbb{A}}, \mathbb{1}_{\mathbb{A}}, f \circ h^{-1})$ is an isotopy between the corresponding inner isotopes:

$$x \bullet_f y = f(x \bullet y) = f \circ h^{-1}(x \bullet_h y), \tag{8}$$

where $\circ$ here and in what follows denote the composition of two maps.

Comparing (8) with (7) a natural question arises: when the algebra $(\mathbb{A}, \bullet_f)$ is an *inner* isotope of $(\mathbb{A}, \bullet_h)$? Note that $f \circ h^{-1} \in \mathrm{Aut}(\mathbb{A}, \bullet)$, but it is not clear whether $f \circ h^{-1} \in \mathrm{Aut}(\mathbb{A}, \bullet_h)$, see the diagram below



The next proposition reveals that this is true for commuting automorphisms only.

Proposition 3.3. *Let* $(\mathbb{A}, \bullet)$ *satisfy*

$$\mathbb{A}^{\bullet 2} := \mathbb{A} \bullet \mathbb{A} = \mathbb{A} \tag{9}$$

and let $h, f \in \mathrm{Aut}(\mathbb{A}, \bullet)$. *Then* $(\mathbb{A}, \bullet_f)$ *is an inner isotope of* $(\mathbb{A}, \bullet_h)$ *if and only if* f *and* h *commute.*

Proof. First suppose that $(\mathbb{A}, \bullet_f)$ is an inner isotope of $(\mathbb{A}, \bullet_h)$, i.e.

$$x \bullet_f y = g(x \bullet_h y) = g(x) \bullet_h g(y), \qquad \forall x, y \in \mathbb{A}, \tag{10}$$

holds for some $\bullet_h$-algebra endomorphism g. Comparing this with (8), we obtain

$$f(x \bullet y) = f \circ h^{-1}(x \bullet_h y) = g(x \bullet_h y) = (g \circ h)(x \bullet y).$$

Since the latter holds for any $x, y \in \mathbb{A}$ we conclude that $f = g \circ h$ on $\mathbb{A}^{\bullet 2}$, and thus by (9) on $\mathbb{A}$. Therefore $g = f \circ h^{-1}$. In particular, g is an $\bullet$-automorphism too. Therefore, using the second identity in (10) we get

$$\begin{aligned} f(x \bullet y) &= g(x) \bullet_h g(y) = h(g(x) \bullet g(y)) \\ &= (h \circ g(x)) \bullet (h \circ g(y)) \\ &= (h \circ g)(x \bullet y) \qquad \forall x, y \in \mathbb{A}, \end{aligned}$$

implying that $f = h \circ g = h \circ f \circ h^{-1}$ on $\mathbb{A}^{\bullet 2} = \mathbb{A}$, hence $f \circ h = h \circ f$ as desired.

Conversely, if $f \circ h = h \circ f$ then using (8)

$$x \bullet_f y = g(x \bullet_h y), \tag{11}$$

where $g = f \circ h^{-1} = h^{-1} \circ f \in \mathrm{Aut}(\mathbb{A}, \bullet)$. We have

$$g(x \bullet_h y) = g \circ h(x \bullet y) = f \circ h^{-1} \circ h(x \bullet y) = f(x \bullet y),$$

and on the other hand,

$$g(x) \bullet_h g(y) = h \circ (g(x) \bullet g(y)) = (h \circ g)(x \bullet y) = f(x \bullet y),$$

implying $g(x \bullet_h y) = g(x) \bullet_h g(y)$, hence $g \in \mathrm{Aut}(\mathbb{A}, \bullet_h)$, i.e. it follows from (11) that $(\mathbb{A}, \bullet_f)$ is an inner isotope of $(\mathbb{A}, \bullet_h)$. □

The next two propositions explain when two inner isotopes are isomorphic.

Proposition 3.4. *Let $f : (\mathbb{A}, \bullet) \to (\mathbb{A}', \bullet')$ be an algebra isomorphism and let $h \in \mathrm{Aut}(\mathbb{A}, \bullet)$. Then $h' := f \circ h \circ f^{-1} \in \mathrm{Aut}(\mathbb{A}', \bullet')$ and $f : (\mathbb{A}, \bullet_h) \to (\mathbb{A}', \bullet'_{h'})$ is an algebra isomorphism.*

Proof. We have $f(x \bullet y) = f(x) \bullet' f(y)$ and $h(x) \bullet h(y) = h(x \bullet y)$ for any $x, y \in \mathbb{A}$, therefore

$$\begin{aligned} f \circ h \circ f^{-1}(x' \bullet' y') &= f \circ h(f^{-1}(x') \bullet f^{-1}(y')) \\ &= f(h(f^{-1}(x')) \bullet h(f^{-1}(y'))) \\ &= f(h(f^{-1}(x')) \bullet' f(h(f^{-1}(y')), \end{aligned}$$

readily implying that $h' := f \circ h \circ f^{-1} \in \mathrm{Aut}(\mathbb{A}', \bullet')$. Furthermore,

$$f(x \bullet_h y) = f \circ h(x \bullet y) = f \circ h \circ f^{-1}(f(x) \bullet' f(y)) = f(x) \bullet'_{h'} f(y)$$

implying that $f : (\mathbb{A}, \bullet_h) \to (\mathbb{A}', \bullet'_{h'})$ is an algebra isomorphism.

□

Proposition 3.5. *Let $h, f \in \mathrm{Aut}(\mathbb{A}, \bullet)$. If h and f conjugate in $\mathrm{Aut}(\mathbb{A}, \bullet)$ then $(\mathbb{A}, \bullet_h)$ is isomorphic to $(\mathbb{A}, \bullet_f)$. In the converse direction, if $g : (\mathbb{A}, \bullet_h) \to (\mathbb{A}, \bullet_f)$ is an isomorphism and $g \in \mathrm{Aut}(\mathbb{A}, \bullet)$ then h and f conjugate in $\mathrm{Aut}(\mathbb{A}^{\bullet 2}, \bullet)$.*

Proof. If f and h conjugate in $\mathrm{Aut}(\mathbb{A}, \bullet)$ then $f = g \circ h \circ g^{-1}$ for some $g \in \mathrm{Aut}(\mathbb{A}, \bullet)$, hence

$$g(x \bullet_h y) = g \circ h(x \bullet y) = f \circ g(x \bullet y) = f(g(x) \bullet g(y)) = g(x) \bullet_f g(y),$$

hence $g : (\mathbb{A}, \bullet_h) \to (\mathbb{A}, \bullet_f)$ is an algebra isomorphism. Conversely, by our assumptions we have

$$g \circ h(x \bullet y) = g(x \bullet_h y) = g(x) \bullet_f g(y) = f(g(x) \bullet g(y)) = f \circ g(x \bullet y),$$

hence $g \circ h = f \circ g$ on $\mathbb{A}^{\bullet 2}$. □

Corollary 3.6. *Let $(\mathbb{A}, \bullet)$ satisfy (9) and $h, f \in \mathrm{Aut}(\mathbb{A}, \bullet)$. Then $(\mathbb{A}, \bullet_h)$ is isomorphic to $(\mathbb{A}, \bullet_f)$ if and only if h and f conjugate in $\mathrm{Aut}(\mathbb{A}, \bullet)$.*

4 Inner isotopes of commutative associative algebras

So far, we have not specified any additional algebraic structure on $(\mathbb{A}, \bullet)$. Below we shall focus on the simplest case when the original algebra $(\mathbb{A}, \bullet)$ is commutative and associative. Sometimes we shall also require that the algebra $(\mathbb{A}, \bullet)$ is unital. Note that any unital algebra satisfies automatically (9).

If $(\mathbb{A}, \bullet)$ is a commutative associative algebra then any inner isotope $(\mathbb{A}, \bullet_h)$ is obviously commutative but it maybe non-associative, because

$$x \bullet_h (y \bullet_h z) = h(x \bullet h(y \bullet z)) = h(x) \bullet h^2(y) \bullet h^2(z)$$

and

$$(x \bullet_h y) \bullet_h z = h^2(x) \bullet h^2(y) \bullet h(z)$$

are not equal in general. On the other hand, such an inner isotope is nearly associative, namely, it is medial. We recall the definition.

Definition 4.1. An algebra $(\mathbb{A}, \bullet)$ is called *medial* if

$$(x \bullet y) \bullet (z \bullet w) = (x \bullet z) \bullet (y \bullet w), \qquad \forall x, y, z, w \in \mathbb{A}. \tag{12}$$

An important corollary of the definition is

$$(x \bullet y) \bullet (x \bullet y) = (x \bullet x) \bullet (y \bullet y).$$

which immediately implies

Proposition 4.2. *Product of two idempotents in a medial algebra is an idempotent again.*

Proof. If $c_i \bullet c_i = c_i$, $i = 1, 2$ then

$$(c_1 \bullet c_2) \bullet (c_1 \bullet c_2) = (c_1 \bullet c_1) \bullet (c_2 \bullet c_2) = c_1 \bullet c_2.$$

□

Proposition 4.3. *If an algebra $(\mathbb{A}, \bullet)$ is commutative and associative, $h \in \mathrm{End}(\mathbb{A}, \bullet)$, then the inner isotope $(\mathbb{A}, \bullet_h)$ is a commutative medial algebra. Furthermore, if $h \in \mathrm{Aut}(\mathbb{A}, \bullet)$ and $(\mathbb{A}, \bullet)$ is additionally a unital algebra with unity e then e is an idempotent in $(\mathbb{A}, \bullet_h)$ and $L_{\bullet_h}(e)$ is an invertible operator.*

Proof. We have

$$\begin{aligned}(x \bullet_h y) \bullet_h (z \bullet_h w) &= h((x \bullet_h y) \bullet_h (z \bullet_h w)) \\ &= h(h(x \bullet y) \bullet h(z \bullet w)) \\ &= h^2(x \bullet y \bullet z \bullet w),\end{aligned}$$

where the right hand side is symmetric under any permutation of factors, implying (12).

Next, assume that $(\mathbb{A}, \bullet)$ is additionally a unital algebra with unity e. Since an automorphism stabilizes the unity element, we have

$$e \bullet_h e = h(e \bullet e) = h(e) = e$$

therefore e becomes an idempotent in $(\mathbb{A}, \bullet_h)$. Furthermore, $e \bullet_h x = h(e \bullet x) = h(x) = 0$ if and only if $x = 0$, thus $L_{\bullet_h}(e)$ is an invertible operator.

□

Proposition 4.4. *Any associative commutative algebra is medial. A unital commutative medial algebra is associative.*

Proof. Indeed, if $(\mathbb{A}, \bullet)$ is an associative commutative algebra then it is medial:

$$(x \bullet y) \bullet (z \bullet w) = x \bullet y \bullet z \bullet w = x \bullet z \bullet y \bullet w = (x \bullet z) \bullet (y \bullet w).$$

On the other hand, if $(\mathbb{A}, \bullet)$ is a unital commutative medial algebra and e is the algebra unity then

$$x \bullet (y \bullet z) = (e \bullet x) \bullet (y \bullet z) = (e \bullet z) \bullet (x \bullet y) = z \bullet (x \bullet y) = (x \bullet y) \bullet z,$$

hence $(\mathbb{A}, \bullet)$ is associative. □

We refer to [17] for general medial algebras and their spectral theory.

5 Categories of calibrated medial algebras

We denote by $\mathrm{Idm}^{\times}(\mathbb{A},*)$ the subset of nonzero idempotents in an algebra $(\mathbb{A},*)$ such that the left multiplication operator $L_*(c)$ is invertible.

Definition 5.1. A medial algebra $(\mathbb{A},*)$ is called **special** if the set $\mathrm{Idm}^{\times}(\mathbb{A},*)$ is non-empty.

The terminology 'special' here correspond exactly to what is called 'medial class (iii) algebras' in [17].

It follows from Proposition 4.3 above that if $(\mathbb{A},\bullet)$ unital commutative associative algebra then its unity element e of becomes an idempotent in the inner isotope $(\mathbb{A},\bullet_h)$, $h\in\mathrm{Aut}(\mathbb{A},\bullet)$ and furthermore $e\in\mathrm{Idm}^{\times}(\mathbb{A},\bullet_h)$. This proves

Corollary 5.2. *Any inner isotope $(\mathbb{A},\bullet_h)$ of a unital commutative associative algebra $(\mathbb{A},\bullet)$ is a special medial algebra.*

Idempotents in $\mathrm{Idm}^{\times}(\mathbb{A},*)$ are distinguished in many aspects and a particular choice of such an idempotent can be thought of as a *calibration* or *pointing* of an algebra. To put this observation into an appropriate context, we define a concept of calibrations for special medial algebras and unital commutative associative algebras. An important ingredient in our constructions is Kaplansky's trick [13], [20].

Definition 5.3. A special (commutative) medial algebra $(\mathbb{A},*)$ with a distinguished idempotent $c\in\mathrm{Idm}^{\times}(\mathbb{A},*)$ is called *calibrated* and denoted by $(\mathbb{A},*,c)$. An algebra homomorphism between two special medial algebras $f:(\mathbb{A},*,a)\to(\mathbb{B},\circledast,b)$ is called a *calibrated* if $f(a)=b$.

Definition 5.4. A unital commutative associative algebra $(\mathbb{A},\diamond,e)$ with algebra unity e and a distinguished automorphism $h\in\mathrm{Aut}(\mathbb{A},\diamond,e)$ is called *calibrated* and denoted by $(\mathbb{A},\diamond,e,h)$. An algebra homomorphism between two calibrated commutative associative algebras $f:(\mathbb{A},\diamond,e,h)\to(\mathbb{A}',\diamondsuit,e',h')$ is called a *calibrated homomorphism* if $h'\circ f=f\circ h$ (note that $f(e)=e'$).

We denote two calibrated isomorphic algebras by $\mathbb{A}\,\dot{\cong}\,\mathbb{A}'$. Of course, $\mathbb{A}\,\dot{\cong}\,\mathbb{A}'$ implies that $\mathbb{A}\cong\mathbb{A}'$.

Denote by $\mathfrak{M}$ (respectively by $\mathfrak{A}$) the class of calibrated special commutative medial algebras (respectively calibrated commutative associative unital algebras). These classes are categories in an obvious way, where the corresponding morphisms are calibrated homomorphisms.

Theorem 5.5. *The functor $\Phi:\mathfrak{A}\to\mathfrak{M}$ given by $\Phi(\mathbb{A},\diamond,e,h)=(\mathbb{A},*,e)$, where $x*y=h(x\diamond y)$ and $e\in\mathrm{Idm}^{\times}(\mathbb{A},*,e)$, is a category isomorphism. The inverse functor $\Psi=\Phi^{-1}$ is given by $\Psi(\mathbb{A},*,c)=(\mathbb{A},\diamond,c,h)$, where $x\diamond y=L_*^{-1}(x*y)$, c is a unity in $(\mathbb{A},\diamond)$ and $h=L_*(c)\in\mathrm{Aut}(\mathbb{A},\diamond)$.*

Proof. The proof is divided into three steps.

Step 1. The map Φ is a functor $\mathfrak{A} \to \mathfrak{M}$.

Our first claim is that given $(\mathbb{A}, \diamond, e, h) \in \mathfrak{A}$, a new multiplication on $\mathbb{A}$ by

$$x * y = h(x \diamond y) = h(x) \diamond h(y) \tag{13}$$

defines a calibrated medial algebra $\mathbb{A}, *, e) \in \mathfrak{M}$ of class (iii) with an idempotent $e \in \mathrm{Idm}^{\times}(\mathbb{A}, *)$. Indeed, since $h \in \mathrm{Aut}(\mathbb{A}, \diamond)$ we have

$$(x * y) * (z * w) = h((x * y) \diamond (z * w)) = h(h(x \diamond y) \diamond h(z \diamond w)) = (h \circ h)(x \diamond y \diamond z \diamond w)$$

where the right hand side is obviously symmetric for any permutation of factors. Since e is the unitity element and h is an algebra automorphism in $(\mathbb{A}, \diamond)$ then $h(e) = e$, hence $e * e = h(e \diamond e) = e$, i.e. e is an idempotent in $(\mathbb{A}, *)$. Also, $e * x = h(e \diamond x) = h(x)$, hence $L_*(e) = h$ is a bijection, i.e. $e \in \mathrm{Idm}^{\times}(\mathbb{A}, h, *)$.

Next, we prove that Φ acts correspondingly on morphisms. To this end consider a calibrated $\mathfrak{A}$-algebra homomorphism $f : (\mathbb{A}, \diamond, e, h) \to (\mathbb{A}', \diamondsuit, e', h')$. Then f is an algebra homomorphism and $h' \circ f = f \circ h$. Let $\Phi(\mathbb{A}, \diamond, e, h) = (\mathbb{A}, *, e)$ and $\Phi(\mathbb{A}', \diamondsuit, e', h') = (\mathbb{A}', \circledast, e')$. We consider $\Phi(f) = f$. Then $f(e) = e'$ and

$$f(x * y) = (f \circ h)(x \diamond y) = (h' \circ f)(x \diamond y) = h'(f(x) \diamondsuit f(y)) = f(x) \circledast f(y),$$

hence $f : (\mathbb{A}, *, e) \to (\mathbb{A}', \circledast, e')$ is a calibrated $\mathfrak{M}$-algebra homomorphism. The fact that Φ preserves identity morphisms and composition of morphisms trivially follows by its definition.

Step 2. The map Ψ is a functor $\mathfrak{M} \to \mathfrak{A}$.

Let $(\mathbb{A}, *, c) \in \mathfrak{M}$. Define a new multiplication on $\mathbb{A}$ by

$$x \diamond y = L_*(c)^{-1}(x * y). \tag{14}$$

The algebra $(\mathbb{A}, \diamond)$ is commutative and $c \diamond x = L_*(c)^{-1}(c * x) = L_*(c)^{-1} L_*(c) x = x$, hence c is a unit in $(\mathbb{A}, \diamond)$. By 1 in Proposition 6.1, $L_*(c)^{-1}$ is an algebra isomorphism of $(\mathbb{A}, *, c)$ hence

$$(x \diamond y) \diamond (z \diamond w) = L_*(c)^{-1}\big(L_*(c)^{-1}(x * y) * L_*(c)^{-1}(z * w)\big) = L_*(c)^{-2}((x * y) * (z * w))$$

which implies that $(\mathbb{A}, \diamond)$ is medial. By Proposition 4.4, $(\mathbb{A}, \diamond)$ is associative. Since $L_*(c)$ is an algebra isomorphism of $(\mathbb{A}, *, c)$, it is a bijection. Furthermore,

$$\begin{aligned} L_*(c)(x \diamond y) &= L_*(c) L_*(c)^{-1}(x * y) = x * y \\ L_*(c)(x) \diamond L_*(c)(y) &= L_*(c)^{-1}\big(L_*(c)(x) * L_*(c)(y)\big) = x * y, \end{aligned}$$

hence $L_*(c)(x \diamond y) = L_*(c)(x) \diamond L_*(c)(y)$, i.e. $L_*(c) \in \mathrm{Aut}(\mathbb{A}, \diamond, c)$. Then $\Psi(\mathbb{A}, *, c) = (\mathbb{A}, \diamond, c, L_*(c)) \in \mathfrak{A}$.

Next, we prove that Φ acts correspondingly on morphisms. Let $f : (\mathbb{A}, *, c) \to (\mathbb{A}', \circledast, c')$ be a calibrated $\mathfrak{M}$-algebra homomorphism, i.e. $f(c) = c'$. Let $\Psi(\mathbb{A}, *, c) = (\mathbb{A}, \diamond, c, L_*(c))$

and $\Psi((\mathbb{A}', \circledast, c') = (\mathbb{A}', \diamondsuit, c', L_{\circledast}(c'))$. Then $f : (\mathbb{A}, \diamond) \to (\mathbb{A}', \diamondsuit)$ is vector space homomorphism and

$$(L_{\circledast}(c') \circ f)(x) = c' \circledast f(x) = f(c) \circledast f(x) = f(c * x) = (f \circ L_*(c))(x),$$

hence $L_{\circledast}(c') \circ f = f \circ L_*(c)$ and therefore $f \circ L_*(c)^{-1} = L_{\circledast}(c')^{-1} \circ f$, and it follows that

$$\begin{aligned} f(x \diamond y) &= \big(f \circ L_*(c)^{-1}\big)(x * y) = \big(L_{\circledast}(c')^{-1} \circ f\big)(x * y) \\ &= L_{\circledast}(c')^{-1}(f(x) \circledast f(y)) = f(x) \diamondsuit f(y) \end{aligned}$$

i.e. f is a calibrated $\mathfrak{A}$-algebra homomorphism. The fact that Ψ preserves identity morphisms and composition of morphisms readily follows by its definition.

Step 3. $\Psi \circ \Phi = \mathrm{id}_{\mathfrak{A}}$.

We have $\Phi(\mathbb{A}, \diamond, e, h) = (\mathbb{A}, *, e)$ and $\Psi(\mathbb{A}, *, e) = (\mathbb{A}, \diamondsuit, e, L_*(e))$, where

$$\begin{aligned} x * y &= h(x \diamond y), \\ x \diamondsuit y &= L_*(e)^{-1}(x * y). \end{aligned}$$

We have $e * z = h(e \diamond y) = h(e) \diamond h(z) = h(z)$, i.e. $L_*(e) = h$, therefore $x \diamondsuit y = L_*(e)^{-1}(x * y) = h^{-1}(x * y) = x \diamond y$. This implies that $\Psi(\mathbb{A}, *, e) = (\mathbb{A}, \diamond, e, h)$, hence $\Psi \circ \Phi = \mathrm{id}_{\mathfrak{A}}$. The theorem follows. □

We have several important corollaries of the above result.

Corollary 5.6. *$\Psi(\mathbb{A}) \dot{\cong} \Psi(\mathbb{A}')$ if and only if $\mathbb{A} \dot{\cong} \mathbb{A}'$ for $\mathbb{A}, \mathbb{A}' \in \mathfrak{M}$ and $\Phi(\mathbb{A}) \dot{\cong} \Phi(\mathbb{A}')$ if and only if $\mathbb{A} \dot{\cong} \mathbb{A}'$ for $\mathbb{A}, \mathbb{A}' \in \mathfrak{A}$.*

The following propositions describe how the functors $\Phi : \mathfrak{A} \to \mathfrak{M}$ and $\Psi : \mathfrak{M} \to \mathfrak{A}$ depend on a particular choice of calibrating.

Proposition 5.7. *If $(\mathbb{A}, *)$ is a special commutative medial algebra and $c_1, c_2 \in \mathrm{Idm}^{\times}(\mathbb{A}, *)$ then $(\mathbb{A}, *, c_1) \dot{\cong} (\mathbb{A}, *, c_2)$. In particular, given a special commutative medial algebra, there exists a unique calibrated isomorphy class of $\mathbb{A}$.*

Proof. By 1 in Proposition 6.1, $f = L_*(c_1)^{-1}L_*(c_2)$ is a $*$-algebra automorphism of $(\mathbb{A}, *)$. Furthermore, $f(c_1) = L_*(c_1)^{-1}L_*(c_2)(c_1) = L_*(c_1)^{-1}(c_1 * c_2) = c_2$, hence f a calibrated isomorphism of $f : (\mathbb{A}, *, c_1) \to (\mathbb{A}, *, c_2)$. □

Proposition 5.8. *Let $(\mathbb{A}, \diamond)$ be a unital commutative associative algebra, $h_1, h_2 \in \mathrm{Aut}(\mathbb{A}, \diamond)$. Then $(\mathbb{A}, \diamond, e, h_1) \dot{\cong} (\mathbb{A}, \diamond, e, h_2)$ if and only if h_1 and h_2 are conjugate in $\mathrm{Aut}(\mathbb{A}, \diamond)$.*

Proof. By the definition, $(\mathbb{A}, \diamond, e, h_1) \dot{\cong} (\mathbb{A}, \diamond, e, h_2)$ if and only if there exists an isomorphism $f : (\mathbb{A}, \diamond) \to (\mathbb{A}, \diamond)$ such that $h_2 \circ f = f \circ h_1$, i.e. $f \in \mathrm{Aut}(\mathbb{A}, \diamond)$ and $h_2 = f \circ h_1 \circ f^{-1}$, which is equivalent to that h_1 and h_2 are conjugate in $\mathrm{Aut}(\mathbb{A}, \diamond)$. □

Corollary 5.9. *Given a unital commutative associative algebra $(\mathbb{A}, \diamond)$, there is a natural bijection between its calibrated isomorphy classes and the conjugacy classes of its automorphism group:*

$$\mathbb{A}/_{\underset{\cong}{\cdot}} = \mathrm{Aut}(\mathbb{A})/_{\mathrm{conj}}$$

6 Idempotents in inner isotopes

We start with a general result which holds for any commutative medial algebra.

Proposition 6.1 ([17]). *Let $(\mathbb{A}, *)$ be commutative medial algebra. If $c_1, c_2 \in \mathrm{Idm}(\mathbb{A}, *)$ then so is $c_1 * c_2$. In other words, the set of all idempotents $\mathrm{Idm}(\mathbb{A}, *) \cup \{0\}$ is a multiplicative magma. Furthermore, for any idempotent $c \in \mathrm{Idm}(\mathbb{A}, *)$:*

1. *$L_*(c)$ is a $(\mathbb{A}, *)$-algebra endomorphism;*
2. *The 0-Peirce subspace $\ker L_*(c)$ is an ideal of $(\mathbb{A}, *)$ and the image $L_*(c)(\mathbb{A})$ is a subalgebra of $\mathbb{A}$;*
3. *The 1-Peirce subspace $\{x \in \mathbb{A} : L_*(c)x = x\}$ is a subalgebra of the image $L_*(c)(\mathbb{A})$ and $\dim \mathbb{A}_c(1) \geq 1$;*
4. *For any idempotents $c_1, c_2 \in \mathrm{Idm}(\mathbb{A})$ the following composition rule holds:*

$$L_*(c_2)L_*(c_1) = L_*(c_1 * c_2)L_*(c_2) \tag{15}$$

Proof. The first claim is an immediate corollary of the medial magma identity (12). Furthermore, the multiplication operator $L_*(c) : \mathbb{A} \to \mathbb{A}$ is linear and it follows from (12) that for any idempotent $c \in \mathrm{Idm}(\mathbb{A}, *)$

$$\begin{aligned} L_*(c)(x * y) &= c * (x * y) = (c * c) * (x * y) = (c * x) * (c * y) \\ &= L_*(c)x * L_*(c)y, \end{aligned}$$

hence $L_*(c)$ is an algebra endomorphism. As the kernel of a homomorphism, $\mathbb{A}_c(0) = \ker L_*(c)$ is an ideal and as the image of a homomorphism, $L_*(c)(\mathbb{A})$ is a subalgebra. Further, $\mathbb{A}_c(1) = \{x : L_*(c)x = x\}$ is the set of fixed points of the algebra homomorphism $L_*(c)$, thus it is a subalgebra of $\mathbb{A}$. Since $L_*(c)$ stabilizes $\mathbb{A}_c(1)$, the latter is also a subalgebra of $L_*(c)(\mathbb{A})$. Also, the one-dimensional subspace $\mathrm{span}(c) \subset L_*(c)(\mathbb{A})$, hence $\dim \mathbb{A}_c(1) \geq 1$. Finally, (15) follows from

$$\begin{aligned} L_*(c_2)L_*(c_1)x &= c_2 * (c_1 * x) = (c_2 * c_2)(c_1 * x) = (c_2 * c_1)(c_2 * x) \\ &= L_*(c_1 * c_2)L_*(c_2)x. \end{aligned}$$

□

Now let $(\mathbb{A}, \bullet)$ be a commutative algebra and $(\mathbb{A}, \bullet_h)$ its inner isotope, $h \in \mathrm{Aut}(\mathbb{A}, \bullet)$. Then c is an idempotent in $(\mathbb{A}, \bullet_h)$ if $c = c \bullet_h c$, which implies

$$\mathrm{Idm}(\mathbb{A}, \bullet_h) \cup \{0\} = \{c \in \mathbb{A} : h(c \bullet c) = c\}. \tag{16}$$

Combining Proposition 4.3 and Proposition 6.1 we obtain

Corollary 6.2. *Let $(\mathbb{A}, \bullet)$ be commutative associative algebra. The set of all idempotents $\mathrm{Idm}(\mathbb{A}, \bullet_h) \cup \{0\}$ is a multiplicative magma.*

The latter makes it natural to ask when the set of all *nonzero* idempotents $\mathrm{Idm}(\mathbb{A}, \bullet_h)$ is a quasigroup. Note that this property does not hold in general because the product of two idempotents may be zero. But, under some natural assumptions, one has the desired property.

Corollary 6.3. *If $(\mathbb{A}, \bullet)$ is a commutative associative division algebra and $h \in \mathrm{Aut}(\mathbb{A}, \bullet)$ then $(\mathbb{A}, \bullet_h)$ is also a division algebra and the set of nonzero idempotents $\mathrm{Idm}(\mathbb{A}, \bullet_h)$ is a commutative idempotent medial quasigroup.*

Proof. Indeed, given $x, y \in (\mathbb{A}, \bullet_h)$, $x \bullet_h y = 0$ if and only if $h(x \bullet y) = 0$, where the latter by the bijectivity of h is equivalent to $x \bullet y = 0$, therefore $(\mathbb{A}, \bullet_h)$ is also a division algebra. This implies by Proposition 6.1 that for any $c_1, c_2 \in \mathrm{Idm}(\mathbb{A}, \bullet_h)$ in fact $c_1 \bullet_h c_2 \in \mathrm{Idm}(\mathbb{A}, \bullet_h)$. Suppose that $c_1 \bullet_h c_2 = c_1 \bullet_h c_3$ for some $c_1, c_2, c_3 \in \mathrm{Idm}(\mathbb{A}, \bullet_h)$. Then $c_1 \bullet_h (c_2 - c_3) = 0$, therefore $c_2 - c_3 = 0$, hence $\mathrm{Idm}(\mathbb{A}, \bullet_h)$ is in fact a quasigroup, which is obviously commutative idempotent and medial, the proposition follows. □

Proposition 6.4. *Let $(\mathbb{A}, \bullet)$ be a commutative associative division algebra and $h \in \mathrm{Aut}(\mathbb{A}, \bullet)$. Then all idempotents $c \in \mathrm{Idm}(\mathbb{A}, \bullet_h)$ have the same characteristic polynomial.*

Proof. By Corollary 6.3, if $c_1, c_2 \in \mathrm{Idm}(\mathbb{A}, \bullet_h)$ then $c_1 \bullet_h c_2 \in \mathrm{Idm}(\mathbb{A}, \bullet_h)$ and $L_{\bullet_h}(c_1)$ is invertible, hence by Proposition 6.1 we obtain

$$L_{\bullet_h}(c_1 \bullet_h c_2) = L_{\bullet_h}(c_1) L_{\bullet_h}(c_2) L_{\bullet_h}(c_1)^{-1}.$$

and similarly

$$L_{\bullet_h}(c_2 \bullet_h c_1) = L_{\bullet_h}(c_2) L_{\bullet_h}(c_1) L_{\bullet_h}(c_2)^{-1}.$$

Since $c_1 \bullet_h c_2 = c_2 \bullet_h c_1$ we obtain from the last two relations that the characteristic polynomials of $L_{\bullet_h}(c_2)$ and $L_{\bullet_h}(c_1)$ are equal. The proposition follows. □

Proposition 6.5. *Let $(\mathbb{A}, \bullet)$ be a unital commutative associative division algebra with unity e and let $h \in \mathrm{Aut}(\mathbb{A}, \bullet)$ be an automorphism of finite order d. Then $c^{\bullet(2^d-1)} = e$ for any $c \in \mathrm{Idm}(\mathbb{A}, \bullet_h)$.*

Proof. By (16) $c = c \bullet_h c = h(c \bullet c) = h(c^{\bullet 2})$, therefore for all $k = 1, 2, \ldots$

$$c = h(c) \bullet h(c) = h(h(c^{\bullet 2})) \bullet h(h(c^{\bullet 2})) = h^2(c^{\bullet 2^2}) = \ldots = h^k(c^{\bullet 2^k}).$$

Since $h^d = \mathrm{id}$, we obtain $c = h^d(c^{\bullet 2^d}) = c^{\bullet 2^d}$, i.e. $c \bullet (c^{\bullet(2^d-1)} - e) = 0$, hence by the assumptions $(\mathbb{A}, \bullet)$ does not contain divisors of zero, we conclude that $c^{\bullet(2^d-1)} = e$. □

7 Inner isotopes of a quotient polynomial algebra

It worthy to point out that although the algebras $\mathbf{K}[z]/P$ considered in the introduction originate from polynomials, their multiplicative structure does not depend on a particular choice of a polynomial or set of its roots, but only on the dimension n (i.e. the number of *distinct* roots) and the choice of a conjugacy class of permutation $\sigma \in S_n$. Furthermore, under the splitting condition, the algebra $\mathbf{K}[z]/P$ turns out isomorphic the direct product algebra of $n = \deg P$ copies of the ground field $\mathbf{K}$, the theorem below claims.

Theorem 7.1. *Let a polynomial $P \in \mathbf{K}[z]$ split over $\mathbf{K}$ and have $n = \deg P$ distinct roots. Then*

$$\mathbf{K}[z]/P \cong (\mathbf{K}^n, \bullet). \tag{17}$$

The automorphism group

$$\mathrm{Aut}(\mathbf{K}[z]/P) \cong \mathrm{Aut}(\mathbf{K}^n, \bullet) \cong S_n$$

is isomorphic to the symmetric group S_n. Furthermore, two inner isotopes of $(\mathbf{K}^n, \bullet_\sigma)$ and $(\mathbf{K}^n, \bullet_\tau)$, $\sigma, \tau \in S_n$ are isomorphic if and only if σ and τ conjugate in S_n.

Proof of Theorem 7.1. Under our assumptions, $P = (z-a_1)\dots(z-a_n)$, where $\{a_1, \dots, a_n\}$ are the distinct roots of P. Then the Chinese Remainder Theorem [5, Propoisition 15] gives an explicit isomorphism

$$\begin{aligned}
\mathbf{K}[z]/P &\cong \mathbf{K}[z]/(z-a_1)\cdot\ldots\cdot(z-a_n) \\
&\cong (\mathbf{K}[z]/(z-a_1)) \times \ldots \times (\mathbf{K}[z]/(z-a_n)) \\
&\cong \underbrace{(\mathbf{K},\cdot) \times \ldots \times (\mathbf{K},\cdot)}_{n \text{ times}} \\
&\cong (\mathbf{K}^n, \bullet).
\end{aligned}$$

implying (17), where $\bullet$ is the standard coordinate-wise multiplication on $\mathbf{K}^n$. Let $e_i = (0, \dots, 1, \dots, 0)$, $1 \le i \le n$ be the standard basis of $\mathbf{K}^n$ (see section 2). Then it follows that $e_i \bullet e_i = e_i$, hence e_i are idempotents of $(\mathbf{K}^n, \bullet)$, and, moreover, the partial sums

$$e_I := \sum_{i \in I} e_i, \qquad I \in 2^{\{1,2,\dots,n\}} \tag{18}$$

are the only nonzero idempotents in $\mathrm{Idm}(\mathbf{K}^n, \bullet)$. Furthermore, since $e_i \bullet e_j = 0$ for any $1 \le i < j \le n$, $\{e_i\}_{1 \le i \le n}$ are the only primitive (i.e. indecomposable) idempotents in $\mathrm{Idm}(\mathbf{K}^n, \bullet)$. If $\phi \in \mathrm{Aut}(\mathbf{K}^n, \bullet)$ is an algebra automorphism then $\phi(x \bullet x) = \phi(x) \bullet \phi(x)$, hence ϕ is a permutation of the set of nonzero idempotents $\mathrm{Idm}(\mathbf{K}^n, \bullet)$. Since $\phi(x + y) = \phi(x) + \phi(y)$, ϕ preserve primitive idempotents, thus ϕ is a permutation of the set $\{e_i\}_{1 \le i \le n} \subset \mathrm{Idm}(\mathbf{K}^n, \bullet)$. This implies that $\mathrm{Aut}(\mathbf{K}^n, \bullet)$ is a subgroup of S_n. On the other hand, if $\sigma \in S_n$ is an arbitrary permutation, then the linear map

$$\psi_\sigma : (x_1, \dots, x_n) \to (x_{\sigma(1)}, \dots, x_{\sigma(n)}) \tag{19}$$

is an isomorphism of $(\mathbf{K}^n, \bullet)$ implying that in fact $\mathrm{Aut}(\mathbf{K}^n, \bullet) \cong S_n$. Finally, since $(\mathbf{K}^n, \bullet)$ trivially satisfies (9), we conclude by Corollary 3.6 that two inner isotopes of $(\mathbf{K}^n, \bullet_\sigma)$ and $(\mathbf{K}^n, \bullet_\tau)$, $\sigma, \tau \in S_n$ are isomorphic if and only if σ and τ conjugate in S_n. □

Remark 7.2. It follows from Theorem 7.1 that it suffices to consider some specific polynomial $P(z)$ in each degree n. The circular polynomials $P(z) = z^n - 1$ are distinguished in many respects. The corresponding polynomial quotient algebra $(\mathbf{K}^n, \bullet) := (\mathbf{K}[z]/(z^n - 1), \bullet)$ and its inner isotopes $(\mathbf{K}^n, \bullet_\sigma)$ have originally been introduced and studied in [17] in the particular case when $\sigma = (2\,3\,\ldots\,n\,1)$ (in cycle notation). The corresponding algebra is isospectral and as a corollary of the syzygy relation [16], the spectrum of each idempotent is the set of roots of $z^n - 1$.

Below we consider the general case of a permutation σ with several cycles. It turns out that the resulting algebra decomposes as a direct sum of the ideals corresponding to the decomposition of σ into disjoint permutations. By abuse of notation, we shall write

$$\langle \sigma_j \rangle = \mathrm{span}(\{e_i : i \in [\sigma_j]\}) = \bigoplus_{i \in [\sigma_j]} \langle e_i \rangle, \tag{20}$$

where $[\sigma_j] \subset \bar{n} = \{1, 2, \ldots, n\}$ is the orbit of the cycle σ_j. Each cycle σ_j acts as a cyclic permutation of order $|\sigma_j|$ on the orbit $[\sigma_j]$ such that the set of indices $\bar{n}$ is a disjoint union of the orbits $[\sigma_j]$, $1 \le j \le r$.

Proposition 7.3. *Let a permutation $\sigma \in S_n$ have a disjoint cycle decomposition $\sigma = \sigma_1 \ldots \sigma_r$. Then*

$$(\mathbf{K}^n, \bullet_\sigma) \cong \bigoplus_{j=1}^{r} (\langle \sigma_j \rangle, \bullet_\sigma), \qquad (\langle \sigma_j \rangle, \bullet_\sigma) \cong (\mathbf{K}^{|\sigma_j|}, \bullet_{\sigma_j}). \tag{21}$$

Proof. In the above notation, we have

$$(\langle \sigma_j \rangle, \bullet) \cong (\mathbf{K}^{|\sigma_j|}, \bullet). \tag{22}$$

The corresponding isomorphism ψ_σ of $(\mathbf{K}^n, \bullet)$ in (19) decomposes in the direct sum $\psi_\sigma = \bigoplus_{1 \le j \le r} \psi_{\sigma_j}$, where each $\psi_{\sigma_j} \in \mathrm{End}(\langle \sigma_j \rangle)$ is determined as the restriction of ψ_σ to $\langle \sigma_j \rangle$ and moreover

$$(\mathbf{K}^n, \bullet) = \bigoplus_{j=1}^{r} (\langle \sigma_j \rangle, \bullet). \tag{23}$$

It follows from the definitions that $\langle \sigma_i \rangle \bullet \mathbb{A} \subset \langle \sigma_i \rangle$ and $\langle \sigma_i \rangle \bullet \langle \sigma_j \rangle = 0$ for $i \ne j$, therefore (23) is a decomposition into the direct sum of *ideals*. Let $\pi_j : \mathbf{K}^n \to \langle \sigma_j \rangle$ denote the canonical projection (a linear homomorphism). Then $\pi_j : (\mathbf{K}^n, \bullet) \to (\langle \sigma_j \rangle, \bullet)$ is also an algebra homomorphism and the following commutative diagram holds:

$$\begin{array}{ccc} (\mathbf{K}^n, \bullet) & \xrightarrow{\pi_j} & (\langle \sigma_j \rangle, \bullet) \\ \downarrow{\scriptstyle \psi_\sigma} & & \downarrow{\scriptstyle \psi_{\sigma_j}} \\ (\mathbf{K}^n, \bullet) & \xrightarrow{\pi_j} & (\langle \sigma_j \rangle, \bullet) \end{array} \tag{24}$$

where the vertical arrows are algebra isomorphisms. Since $\psi_{\sigma_j} \in \mathrm{Aut}(\langle\sigma_j\rangle, \bullet)$, arguing as above we conclude that

$$(\mathbf{K}^n, \bullet_\sigma) = \bigoplus_{j=1}^{r} (\langle\sigma_j\rangle, \bullet_\sigma), \tag{25}$$

where $(\langle\sigma_j\rangle, \bullet_\sigma) \cong (\mathbf{K}^{|\sigma_j|}, \bullet_{\sigma_j})$ are pairwise orthogonal ideals in $(\mathbf{K}^n, \bullet_\sigma)$, implying (21). □

By virtue of Proposition 7.3 and Proposition 2.1, it suffices to study inner isotopes $(\mathbf{K}^n, \bullet_\tau)$ for the case of a single cycle τ, we will consider this in the next section.

8 The structure of idempotents

First we consider the case $(\mathbf{K}^n, \bullet_\tau)$ (which is equivalent to the construction mentioned in Remark 7.2) in more detail, i.e. we assume that τ contains a single cycle. More precisely, let $n \geq 2$ be an integer and $\tau = (2\,3\,\ldots\,n\,1) \in S_n$ be the right cyclic shift (in cycle notation). We shall suppose that a field $\mathbf{K}$ is τ-admissible (see Definition 2.2 above), i.e. there are primitive roots of unity of orders n and $2^n - 1$ in $\mathbf{K}$; denote them by ϵ and ζ, respectively.

Proposition 8.1. *The set of nonzero idempotents of* $(\mathbf{K}^n, \bullet_\tau)$ *can be parameterized by*

$$\{c_k = (\zeta^{2^{n-1}k}, \zeta^{2^{n-2}k}, \ldots, \zeta^{2k}, \zeta^k) : \quad k \in \mathbb{Z}/(2^n - 1)\mathbb{Z}\}, \tag{26}$$

where all c_k *are pairwise distinct. The idempotents satisfy*

$$c_i \bullet_\tau c_j = c_{i \circledast j}, \tag{27}$$

where the binary operation $\circledast$ *on* $\mathbb{Z}/(2^n - 1)\mathbb{Z}$ *is defined by*

$$i \circledast j \equiv \frac{1}{2}(i + j) \equiv 2^{n-1}(i + j) \mod (2^n - 1). \tag{28}$$

Proof. The multiplication of $c = (x_1, \ldots, x_n)$ in $(\mathbf{K}^n, \bullet_\tau)$ is given by

$$c \bullet_\tau c = (x^2_{\tau(1)}, \ldots, x^2_{\tau(n)}) = (x_2^2, x_3^2, \ldots, x_n^2, x_1^2),$$

thus c is an idempotent if and only if

$$x^2_{i+1} = x_i \quad \text{for each } i \in \mathbb{Z}/n\mathbb{Z}. \tag{29}$$

Iterating the latter relations n times yields $x_i^{2^n} = x_i$ for any i. Together with (29) this implies that *either all of* x_i *are zero (and in that case* $c = 0$*), or all* x_i *are nonzero, and in the latter case they satisfy*

$$x_i^{2^n - 1} - 1 = 0, \qquad \forall i \in \mathbb{Z}/n\mathbb{Z}. \tag{30}$$

It follows from (29) that any nonzero idempotent x can be written as

$$x = (t^{2^{n-1}}, t^{2^{n-2}}, \dots, t^{2^1}, t), \tag{31}$$

where t is a primitive root of unity of order $2^n - 1$, hence (31) readily implies (26). Finally, we have

$$c_i \bullet_\tau c_j = (\zeta^{2^{n-2}(i+j)}, \zeta^{2^{n-3}(i+j)}, \dots, \zeta^{(i+j)}, \zeta^{2^{n-1}(i+j)})$$

implying (27).

□

Identity (27) expresses the fact that the product of any two nonzero idempotents in $\mathrm{Idm}(\mathbf{K}^n, \bullet_\tau)$ is a nonzero idempotent again, in other words, the set $\mathrm{Idm}(\mathbf{K}^n, \bullet_\tau)$ is a multiplicative magma. Furthermore, (27) implies a magma isomorphism

$$\mathrm{Idm}(\mathbf{K}^n, \bullet_\tau) \cong (\mathbb{Z}/(2^n - 1)\mathbb{Z}, \circledast)$$

Moreover, we have

Proposition 8.2. *The multiplicative magma $(\mathbb{Z}/(2^n-1)\mathbb{Z}, \circledast)$ is a commutative idempotent medial quasigroup.*

Proof. The quasigroup property can be seen as follows: if $s, t, r \in (\mathbb{Z}/(2^n - 1)\mathbb{Z}, \circledast)$ are such that $s \circledast r = s \circledast t$ then $(t - r)/2 \equiv 0 \mod (2^n - 1)$, hence $t = r$ in $(\mathbb{Z}/(2^n - 1)\mathbb{Z}, \circledast)$. Also, given arbitrary $s, t \in (\mathbb{Z}/(2^n - 1)\mathbb{Z}, \circledast)$, there exists precisely one solution $r := 2t - s$ to the following equation:

$$s \circledast r = r \circledast s = \frac{1}{2}(s + 2t - s) = t.$$

Next, $s \circledast s = s$ for all $s \in (\mathbb{Z}/(2^n - 1)\mathbb{Z}, \circledast)$, thus the quasigroup is idempotent. Finally, since

$$(i \circledast j) \circledast (k \circledast l) \equiv \frac{1}{2}(i + j + k + l) \mod (2^n - 1)$$

is totally symmetric in all variables, $(\mathbb{Z}/(2^n - 1)\mathbb{Z}, \circledast)$ is a medial quasigroup. □

Proposition 8.3. *The algebra $(\mathbf{K}^n, \bullet_\tau)$ has exactly $2^n - 1$ distinct regular idempotents c_k, i.e. it is generic. Each idempotent $c_k \in \mathrm{Idm}(\mathbf{K}^n, \bullet_\tau)$ has the spectrum $\epsilon, \epsilon^2, \dots, \epsilon^n$, each eigenvalue has multiplicity one. In other words, the characteristic polynomial of $L_{\bullet_\tau}(c_k)$ is given by*

$$\det(\lambda \mathbb{1} - L_{\bullet_\tau}(c_k)) = \lambda^n - 1. \tag{32}$$

In particular,

$$(L_{\bullet_\tau}(c_k))^n = \mathbb{1}. \tag{33}$$

Proof. Given $p \in \mathbb{Z}/n\mathbb{Z}$ and $k \in \mathbb{Z}/(2^n-1)\mathbb{Z}$, we define

$$\eta_{k,p} := (z_1, \epsilon^p z_2, \epsilon^{2p} z_3, \dots, \epsilon^{(n-1)p} z_n), \tag{34}$$

where z_i will be specified later. By (26) to $c_k = (\zeta^{2^{n-1}k}, \zeta^{2^{n-2}k}, \dots, \zeta^{2^1 k}, \zeta^k)$, hence

$$\begin{aligned} c_k \bullet_\tau \eta_{k,p} &= (\epsilon^p \zeta^{2^{n-2}k} z_2,\ \epsilon^{2p} \zeta^{2^{n-3}k} z_3,\ \dots\ \epsilon^{(n-1)p} \zeta^{2^0 k} z_n,\ \epsilon^{np} \zeta^{2^{n-1}k} z_1) \\ &= \epsilon^p \cdot (\zeta^{2^{n-2}k} z_2,\ \zeta^{2^{n-3}k} \epsilon^p z_3,\ \dots\ \zeta^{2^0 k} \epsilon^{(n-2)p} z_n,\ \zeta^{2^{n-1}k} \epsilon^{(n-1)p} z_1), \end{aligned}$$

therefore, setting

$$z_i := \zeta^{-(2^{n-2}+\dots+2^{n-i})k} z_1 \quad \text{for } i = 2, 3, \dots, n$$

we see that

$$\zeta^{2^{n-i}k} z_i = \zeta^{2^{n-i}k} \cdot \zeta^{-(2^{n-2}+\dots+2^{n-i})k} z_1 = z_{i-1}, \quad 2 \le i \le n.$$

Since $2^{n-2} + \dots + 2^1 + 2^0 = 2^{n-1} - 1 \equiv -2^{n-1} \mod (2^n - 1)$, we get

$$z_n = \zeta^{-(2^{n-2}+\dots+2^1+2^0)k} z_1 = \zeta^{2^{n-1}k} z_1$$

implying together with the above that

$$c_k \bullet_\tau \eta_{k,p} = \epsilon^p \cdot (z_1, \epsilon^p z_2, \epsilon^{2p} z_3, \dots, \epsilon^{(n-1)p} z_n) = \epsilon^p \eta_{k,p}. \tag{35}$$

In other words,

$$\eta_{k,p} = (1, \epsilon^p \zeta^{-2^{n-2}k},\ \epsilon^{2p} \zeta^{-(2^{n-2}+2^{n-2})k}, \dots, \epsilon^{(n-1)p} \zeta^{-(2^{n-2}+\dots+2^1+2^0)k}) \tag{36}$$

is an eigenvector of $L_{\bullet_\tau}(c_k)$ with eigenvalue ϵ^p, for any $p \in \mathbb{Z}/n\mathbb{Z}$. Since all $\epsilon, \epsilon^2, \dots, \epsilon^n$ are pairwise distinct, for the dimension reasons this implies that each eigenvalue ϵ^p is simple, and moreover the eigen-decomposition of $L_{\bullet_\tau}(c_k)$ holds:

$$(\mathbf{K}^n, \bullet_\tau) = \bigoplus_{p=1}^{n} \operatorname{span}(\eta_{k,p}). \tag{37}$$

This also implies the explicit form of the characteristic polynomial of $L_{\bullet_\tau}(c_k)$ is given by (32). This implies that $\det(\frac{1}{2}\mathbb{1} - L_{\bullet_\tau}(c_k)) \neq 0$, therefore $(\mathbf{K}^n, \bullet_\tau)$ is a generic algebra. □

Remark 8.4. It follows from (32) that the generic algebra $(\mathbf{K}^n, \bullet_\tau)$ is *isospectral*. On the other hand, there are nongeneric commutative isospectral algebras containing *infinitely* many idempotents. Then their Peirce spectrum (i.e. the total set of eigenvalues of all idempotents) can have a completely different structure. This holds for the Hsiang algebras that appear in the context of cubic minimal cones; we refer an interested reader to [18], [30], [29] for more details.

We need the following auxiliary property

Lemma 8.5. $\sum_{k=1}^{2^n-1} (L_{\bullet_\tau}(c_k))^s = 0$ *for any* $s \in \{1, 2, \dots, n-1\}$.

Proof. Note that by the definition of isotopy, $x \bullet_\tau y = \tau(x \bullet y)$, where $\tau(x_1, \dots, x_{n-1}, x_n) = (x_2, \dots, x_n, x_1)$ and $\bullet$ is the (commutative associative) coordinate-wise multiplication on $\mathbf{K}^n$. Write (26) as $c_k = (a_1^k, \dots, a_n^k)$, where $a_i = \zeta^{2^{n-i}}$ do not depend on k. Then iterating the definition of $\bullet_\tau$ we obtain

$$\begin{aligned}(L_{\bullet_\tau}(c_k))^s x &= \tau^s(c_k) \bullet \tau^{s-1}(c_k) \bullet \ldots \bullet \tau(c_k) \bullet \tau^s(x) \\ &= \omega_k \bullet \tau^s(x),\end{aligned}$$

where $\omega_k = \tau^s(c_k) \bullet \tau^{s-1}(c_k) \bullet \ldots \bullet \tau(c_k)$. Since $\tau, \ldots, \tau^s$ are cyclic coordinate shifts $\omega_k = (\zeta^{km_1}, \zeta^{km_2}, \dots, \zeta^{km_n})$, where $m_i \in \mathbb{Z}_{2^n-1}$ do not depend on k, more precisely

$$m_j = 2^{n-j-1} + \ldots + 2^{n-j-s} = 2^{n-j-s} \cdot (2^s - 1) \neq 0 \quad \text{in } \mathbb{Z}_{2^n-1}$$

Therefore $\zeta^{km_j} \neq 1$ and we have

$$\begin{aligned}\sum_{k=1}^{2^n-1} (L_{\bullet_\tau}(c_k))^s x &= \sum_{k=1}^{2^n-1} \omega_k \bullet \tau^s(x) \\ &= \left(\sum_{k=1}^{2^n-1} (\zeta^{km_1}, \zeta^{km_2}, \dots, \zeta^{km_n}) \right) \bullet \tau^s(x) = 0\end{aligned}$$

because $\sum_{k=1}^{2^n-1} \zeta^{km_j} = \zeta^{m_j}(\zeta^{m_j(2^n-1)} - 1)(\zeta^{m_j} - 1)^{-1} = 0$ for any m_j, the claim follows. □

Corollary 8.6. $\operatorname{span}(\operatorname{Idm}(\mathbf{K}^n, \bullet_\tau)) = \mathbf{K}^n$.

Proof. Let $x \in \mathbf{K}^n$ and $z := \sum_{s=0}^{n-1} (L_{\bullet_\tau}(c_k))^s x$. Then using (33) we find

$$L_{\bullet_\tau} z = \sum_{s=1}^{n} (L_{\bullet_\tau}(c_k))^s x = \sum_{s=0}^{n-1} (L_{\bullet_\tau}(c_k))^s x = z,$$

therefore z is an eigenvector of $L_{\bullet_\tau}(c_k)$ with eigenvalue 1, therefore by Proposition 8.3, $z \in \operatorname{span}(c_k)$. This yields $\sum_{s=0}^{n-1} (L_{\bullet_\tau}(c_k))^s x = \mu_k c_k$ for some $\mu_k \in \mathbf{K}$. Summing up the obtained identities and applying Lemma 8.5, we get

$$\begin{aligned}\sum_{k=1}^{2^n-1} \mu_k c_k &= \sum_{k=1}^{2^n-1} \sum_{s=0}^{n-1} (L_{\bullet_\tau}(c_k))^s x \\ &= \sum_{s=0}^{n-1} \sum_{k=1}^{2^n-1} (L_{\bullet_\tau}(c_k))^s x \\ &= \sum_{k=1}^{2^n-1} x + \sum_{s=1}^{n-1} \sum_{k=1}^{2^n-1} (L_{\bullet_\tau}(c_k))^s x \\ &= (2^n - 1)x,\end{aligned}$$

and since $2^n - 1 \neq 0$ in $\mathbf{K}$, we arrive at the desired conclusion. □

Theorem 8.7. $\mathbb{A} := (\mathbf{K}^n, \bullet_\tau)$ *is an axial algebra with the cyclic fusion law*

$$\mathbb{A}_{\epsilon^p}(c_k) * \mathbb{A}_{\epsilon^q}(c_k) = \mathbb{A}_{\epsilon^{p+q}}(c_k), \quad \forall p, q \in \mathbb{Z}_n. \tag{38}$$

Proof. By Corollary 8.6, $\mathbb{A}$ is spanned by the set of nonzero idempotents $\mathrm{Idm}(\mathbb{A})$ and by Proposition 8.3 all nonzero idempotents in $(\mathbf{K}^n, \bullet_\tau)$ have the same spectrum $\epsilon, \epsilon^2, \dots, \epsilon^n$, each eigenvalue ϵ^p is simple, and the eigen-decomposition (37) holds. Moreover, applying (36) we obtain for the corresponding eigenvectors

$$\eta_{k,p} \bullet_\tau \eta_{k,q} = (\epsilon^{p+q}\zeta^{-2^{m-1}k}, \epsilon^{2(p+q)}\zeta^{-(2^{m-1}+2^{m-2})k}, \dots) = \epsilon^{p+q}\zeta^{-2^{m-1}k}\eta_{k,p+q},$$

which gives $\mathrm{span}(\eta_{k,p}) \bullet_\tau \mathrm{span}(\eta_{k,q}) = \mathrm{span}(\eta_{k,p+q})$ and thereby implies the fusion law (38). □

Now we are ready to formulate our main result for the case of an arbitrary $\sigma \in S_n$. Combining the above results with Proposition 7.3 and Proposition 2.1 we arrive at the following general conclusion:

Theorem 8.8. *Let a permutation $\sigma \in S_n$ have the disjoint cycle decomposition $\sigma = \sigma_1 \dots \sigma_r$ and a field $\mathbf{K}$ be σ-admissible. Then the following properties hold:*

(a) There are exactly 2^n distinct regular idempotents in $(\mathbf{K}^n, \bullet_\sigma)$ naturally stratified in 2^r classes I_α, enumerated by binary codes $\alpha \in \mathbb{F}_2^r$.

(b) For each $\alpha \in \mathbb{F}_2^r$, all idempotents in I_α have the same spectrum. More precisely,

$$\det(\lambda \mathbb{1} - L_{\bullet_\tau}(c)) = \prod_{i=1}^{r} (\lambda^{|\sigma_i|} - \alpha(i)), \qquad \forall c \in I_\alpha. \tag{39}$$

(c) The algebra $(\mathbf{K}^n, \bullet_\sigma)$ is generic.

9 Automorphisms

In order to describe the automorphism group for $(\mathbf{K}^n, \bullet_\sigma)$, we recall some definitions. For two groups G, H, and an action $f : H \to \mathrm{Aut}(G)$, the corresponding *semidirect product* $G \rtimes_f H$ is defined by the group multiplication on $G \times H$ given by $(g_1, h_1)(g_2, h_2) = (g_1 f_{h_1}(g_2), h_1 h_2)$. In particular, if $H = \mathrm{Aut}(G)$ with $f = \mathrm{id}$ then one obtains the classical notion of the *holomorph* of a group G is the semi-direct product $G \rtimes_{\mathrm{id}} \mathrm{Aut}(G)$ with the multiplication given by

$$(g_1, \alpha_1) \cdot (g_2, \alpha_2) = (g_1 \alpha_1(g_2),\ \alpha_1 \alpha_2) \tag{40}$$

The automorphism group of the additive cyclic group $\mathbb{Z}_N := (\mathbb{Z}_N, +)$ is isomorphic to the multiplicative group $(\mathbb{Z}_N)^\times = (\mathbb{Z}_N^\times, \cdot)$ of integers modulo N (the group of multiplicative units):

$$\mathrm{Aut}(\mathbb{Z}_N) \cong (\mathbb{Z}_N)^\times,$$

where we write for short

$$\mathbb{Z}_k := (\mathbb{Z}/k\mathbb{Z}, +), \qquad (\mathbb{Z}_N)^\times = (\mathbb{Z}_N^\times, \cdot).$$

The group $(\mathbb{Z}_N)^\times$ is not cyclic in general, but by the fundamental theorem of finite abelian groups, it is isomorphic to a direct product of cyclic groups of prime power orders. For our analysis the relevant case is when $N = 2^n - 1$, $n \in \mathbb{Z}^+$. Then $(\mathbb{Z}_N)^\times$ is the direct product of the groups corresponding to each of the (odd) prime power factors $N = p_1^{k_1} \dots p_s^{k_s}$:

$$(\mathbb{Z}_N)^\times = (\mathbb{Z}_{p_1^{k_1}})^\times \times \dots \times (\mathbb{Z}_{p_s^{k_s}})^\times \cong C_{p_1^{k_1} - p_1^{k_1 - 1}} \times \dots C_{p_s^{k_s} - p_s^{k_s - 1}},$$

where C_m denote a cyclic group of order m. For example, for $n = 6$, $B = 2^6 - 1 = 63 = 3^2 \cdot 7$, hence

$$(\mathbb{Z}_{63})^\times = C_6 \times C_6.$$

A relevant in the present context is the general affine group of $\mathbb{Z}_N$ which is isomorphic to the holomorph of $\mathbb{Z}_N$:

$$\begin{aligned} \mathrm{Aff}(\mathbb{Z}_N) &\cong \mathbb{Z}_N \rtimes_{\mathrm{id}} (\mathbb{Z}_N)^\times \\ &\cong \{ \begin{pmatrix} m & k \\ 0 & 1 \end{pmatrix} : \ m \in \mathbb{Z}_N^\times, \ k \in \mathbb{Z}_N \} \\ &\cong \{ \psi_{m,k}(i) = mi + k : \ m \in \mathbb{Z}_N^\times, \ k \in \mathbb{Z}_N \}, \end{aligned} \tag{41}$$

where the last line is the group of compositions of affine functions $\psi_{m,k} : \mathbb{Z}_N \to \mathbb{Z}_N$,

$$\psi_{m,k} \circ \psi_{m',k'} = \psi_{mm', mk'+k}. \tag{42}$$

The exponential map

$$\delta(i) := 2^i, \quad \delta : (\mathbb{Z}_n, +) \to (\mathbb{Z}_{2^n-1}^\times, \cdot) \cong \mathrm{Aut}((\mathbb{Z}_{2^n-1}, +)), \tag{43}$$

is a well-defined injective group homomorphism, hence there holds the following exact sequence of abelian groups:

$$0 \longmapsto (\mathbb{Z}_n, +) \overset{\delta}{\longmapsto} (\mathbb{Z}_{2^n-1}^\times, \cdot) \overset{\mu}{\longmapsto} (\mathbb{Z}_{2^n-1}^\times, \cdot)/(\mathbb{Z}_n, +) \longmapsto 0. \tag{44}$$

Denote

$$\Delta_n = \mathrm{im}\, \delta = \{1, 2, \dots, 2^{n-1}\} \subset \mathbb{Z}_{2^n-1}.$$

Note that $\Delta_n \cong (\mathbb{Z}_n, +) \cong C_n$ is a multiplicative subgroup of $(\mathbb{Z}_{2^n-1})^\times$. We shall also need the semi-direct product

$$(\mathbb{Z}_{2^n-1}, +) \rtimes_\delta (\mathbb{Z}_n, +) \cong \{ \psi_{2^q,k}(i) : \ q, k \in \mathbb{Z}_n \} \tag{45}$$

Remark 9.1. Notice that any algebra automorphism stabilizes the algebra idempotents. Therefore the automorphism group of an algebra $\mathbb{A}$ is a subgroup of the group of symmetries of nonzero idempotents of $\mathbb{A}$. As above, it suffices to consider the case when $\sigma = \tau \in S_n$ is a single cycle element(the right shift permutation). In this case, Proposition 8.2 yields that the set of nonzero idempotents is a multiplicative quasigroup. Below we completely characterize its automorphism group.

Theorem 9.2. *Let $\tau = (2\,3\,\dots\,n\,1) \in S_m$ be the right cyclic shift. Then the idempotent quasigroup is*

$$\mathrm{Aut}(\mathrm{Idm}(\mathbf{K}^n, \bullet_\tau)) \cong \mathbb{Z}_{2^n-1} \rtimes_{\mathrm{id}} \mathbb{Z}_{2^n-1}^\times \cong \mathrm{Aff}(\mathbb{Z}_{2^n-1}). \tag{46}$$

Proof. Given a pair $m \in \mathbb{Z}_{2^n-1}^\times$ and $k \in \mathbb{Z}_{2^n-1}$, we define a map $\psi_{m,k}(c_i) := c_{mi+k}$, $i \in \mathbb{Z}_{2^n-1}$, of $\mathrm{Idm}(\mathbf{K}^n, \bullet_\tau))$ to itself. Then for any pair $i, j \in \mathbb{Z}_{2^n-1}$ we obtain using (27)–(28)

$$\begin{aligned}\psi_{m,k}(c_i \bullet_\tau c_j) &= \psi_{m,k}(c_{2^{n-1}(i+j)}) = c_{2^{n-1}m(i+j)+k} = c_{2^{n-1}m(i+j)+2^n k}\\ &= c_{2^{n-1}(mi+k+mj+k)} = c_{mi+k} \bullet_\tau c_{mj+k}\\ &= \psi_{m,k}(c_i) \bullet_\tau \psi_{m,k}(c_j)\end{aligned}$$

i.e. $\psi_{m,k} \in \mathrm{Aut}(\mathrm{Idm}(\mathbf{K}^n, \bullet_\tau))$.

In the converse direction, if $g \in \mathrm{Aut}(\mathrm{Idm}(\mathbf{K}^n, \bullet_\tau))$ then $g(c_i) = c_{h(i)}$ for some bijection $h : \mathbb{Z}_{2^n-1} \to \mathbb{Z}_{2^n-1}$, hence for any pair $i, j \in \mathbb{Z}_{2^n-1}$

$$c_{h(2^{n-1}(i+j))} = g(c_{2^{n-1}(i+j)}) = g(c_i \bullet_\tau c_j) = g(c_i) \bullet_\tau g(c_j) = c_{2^{n-1}(h(i)+h(j))},$$

implying $h(2^{n-1}(i+j)) = 2^{n-1}h(i) + 2^{n-1}h(j)$. Multiplying this by 2 and setting $i = j+2$ yields in view of $2^n = 1$ in $\mathbb{Z}_{2^n-1}$ that

$$2h(2^n j + 2^n) = 2h(j+1) = h(j+2) + h(j),$$

hence

$$h(j+2) - h(j+1) = h(j+1) - h(j) = \dots = h(2) - h(1) =: m. \tag{47}$$

Since h is an injection, $m \neq 0$ in $\mathbb{Z}_{2^n-1}$, thus $m \in \mathbb{Z}_{2^n-1}^\times$. Therefore (47) implies $h(j) = m \cdot (j-1) + h(1) = mj + k$, where $k := h(1) - m \in \mathbb{Z}_{2^n-1}$. This yields $g = \psi_{m,k}$ and (41) establishes the desired isomorphisms in (46).

□

Now we consider the automorphism group of the ambient algebra $(\mathbf{K}^n, \bullet_\tau)$. Recall that by Remark 9.1, $\mathrm{Aut}(\mathbf{K}^n, \bullet_\tau)$ is a subgroup of $\mathrm{Aut}(\mathrm{Idm}(\mathbf{K}^n, \bullet_\tau))$. A part of $\mathrm{Aut}(\mathbf{K}^n, \bullet_\tau)$ can be identified by the definitions. More precisely, let $k, q \in \mathbb{Z}_n$ and consider the maps given by

$$\begin{aligned}\alpha_q(x_1, x_2, \dots, x_n) &= (x_{1-q}, x_{2-q}, \dots, x_{n-q})\\ \beta_k(x_1, x_2, \dots, x_n) &= (\zeta^{2^{n-1}k} x_1, \zeta^{2^{n-2}k} x_2, \dots, \zeta^k x_n)\end{aligned}$$

where α_q is the right cyclic shift of the coordinates (understood as elements of $\mathbb{Z}/n\mathbb{Z}$), for example, $\alpha_1(x) = (x_n, x_1, x_2, \dots, x_{n-1})$ etc.

Lemma 9.3. *In the notation of (41),*

$$\alpha_q = \psi_{2^q,0} \in \mathrm{Aut}(\mathbf{K}^n, \bullet_\tau) \tag{48}$$

$$\beta_k = \psi_{1,k} \in \mathrm{Aut}(\mathbf{K}^n, \bullet_\tau) \tag{49}$$

Furthermore, $\langle \alpha_1, \beta_1 \rangle \cong \mathbb{Z}_{2^n-1} \rtimes_\delta \mathbb{Z}_n$, where δ is defined in (43).

Proof. By their definitions, both α_q and β_k are linear isomorphisms of $\mathbf{K}^n$. An easy verification implies the relation $\alpha_q(x \bullet_\tau y) = \alpha_q(x) \bullet_\tau \alpha(y)$. Furthermore,

$$\begin{aligned}\beta_k(x \bullet_\tau y) &= \beta((x_2y_2, \dots, x_ny_n, x_1y_1)) \\ &= (\zeta^{2^{n-1}k}x_2y_2, \dots, \zeta^{2^1k}x_ny_n,\ \zeta^{2^0k}x_1y_1),\end{aligned}$$

and on the other hand,

$$\beta_k(x) \bullet_\tau \beta_k(y) = (\zeta^{2^{n-2}k}x_2 \cdot \zeta^{2^{n-2}k}y_2, \dots,\ \zeta^{2^{n-1}m}x_1 \cdot \zeta^{2^{n-1}m}y_1).$$

Comparing the obtained expressions yields $\beta_k(x \bullet_\tau y) = \beta_k(x) \bullet_\tau \beta_k(y)$, hence both α_q and β_k are automorphisms of $(\mathbf{K}^n, \bullet_\tau)$. Applying the definitions to (26) implies (48) and (49). Furthermore, elements α_1, β_1 generate a subgroup in $\mathrm{Aff}(\mathbb{Z}_{2^n-1})$ consisting of all elements of the kind $\psi_{2^q,k}$, $q, k \in \mathbb{Z}_n$, which by virtue of (45) implies the last claim of the lemma. □

Recall that the cyclotomic polynomial $\Phi_N(z)$ is the unique irreducible polynomial with integer coefficients that is a divisor of $z^N - 1$ and is not a divisor of $z^k - 1$ for any $k < N$. Its roots are all Nth primitive roots of unity. It is well known that

$$\prod_{d|N} \Phi_d(z) = z^N - 1. \tag{50}$$

Definition 9.4. Let $n \geq 2$ be an integer and

$$\Lambda_n(z) := z + z^2 + z^4 + \ldots + z^{2^{n-1}}.$$

The number n is said to be *regular* if the cyclotomic polynomial $\Phi_{2^n-1}(z)$ does *not* divide $\Lambda_n(z^m) - \Lambda_n(z)$ for all $m \in \mathbb{Z}^\times_{2^n-1} \setminus \Delta_n$.

Theorem 9.5. *If $n \geq 2$ is a regular integer then* $\mathrm{Aut}(\mathbf{K}^n, \bullet_\tau) \cong \mathbb{Z}_{2^n-1} \rtimes_\delta \mathbb{Z}_n$.

Proof. An algebra automorphism stabilizes the set of nonzero idempotents, inducing an automorphism on the idempotent quasigroup. By Corollary 8.6, $\mathrm{span}(\mathrm{Idm}(\mathbf{K}^n, \bullet_\tau)) = \mathbf{K}^n$, hence if some $f \in \mathrm{Aut}(\mathbf{K}^n, \bullet_\tau)$ stabilize each nonzero idempotent in $\mathrm{Idm}(\mathbf{K}^n, \bullet_\tau)$ then $f = \mathbb{1}$. This implies that $\mathrm{Aut}(\mathbf{K}^n, \bullet_\tau)$ is a subgroup of $\mathrm{Aut}(\mathrm{Idm}(\mathbf{K}^n, \bullet_\tau))$, in particular, any algebra automorphism has the form $\psi_{m,k}$, where $m \in \mathbb{Z}^\times_{2^n-1}$, $k \in \mathbb{Z}_{2^n-1}$.

Therefore we need to identify only those $\psi_{k,m} \in \mathrm{Aff}(\mathbb{Z}_{2^n-1})$ which can be extended to a linear isomorphism of $\mathbf{K}^n$. To this end, we note that since $m \in \mathbb{Z}^\times_{2^n-1}$, then $s := m^{-1}k$ is well-defined and by Lemma 9.3 $\psi_{1,s} \in \mathrm{Aut}(\mathbf{K}^n)$, therefore using (42) we conclude that $\psi_{m,k} \circ \psi_{1,s} = \psi_{m,0} \in \mathrm{Aut}(\mathbf{K}^n, \bullet_\tau)$. In other words, we can assume without loss of generality that $k = 0$.

So let us assume that $\psi_{m,0} \in \mathrm{Aut}(\mathbf{K}^n, \bullet_\tau)$. By Lemma 9.3, it suffices to show that $m \in \Delta_n = \{1, 2, \dots, 2^{n-1}\}$. We argue by contradiction and assume that $m \in \mathbb{Z}^\times_{2^n-1} \setminus \Delta_n$. Then by virtue of (26) we find $c_{2^n-1} = (1, 1, \dots, 1)$ and also

$$H_l := c_l + c_{2l} + c_{4l} + \ldots + c_{2^{n-1}l} = \Lambda_n(\zeta^l)c_{2^n-1}, \qquad \forall l \in \mathbb{Z}_{2^n-1}. \tag{51}$$

Since $\psi_{m,0}(c_i) = c_{mi}$ for any $i \in \mathbb{Z}_{2^n-1}$ (in particular, $\psi_{m,0}(c_{2^n-1}) = c_{2^n-1}$) we have $\psi_{m,0}(H_l) = H_{ml}$, implying by virtue of (51) that

$$\Lambda_n(\zeta^l) = \Lambda_n(\zeta^{lm}), \quad \forall l \in \mathbb{Z}_{2^n-1}.$$

Since the latter holds for any primitive root ζ of unity of order $2^n - 1$, we conclude that by the definition, the cyclotomic polynomial $\Phi_{2^n-1}(z)$ divides $\Lambda_n(z^{lm}) - \Lambda_n(z^l)$ for any $l \in \mathbb{Z}_{2^n-1}$, in particular, for $l = 1$, which implies that n is not a regular integer, a contradiction. □

Remark 9.6. Conjecturally, all positive integer numbers are regular, an application of Galois theory of cyclotomic polynomials would be helpful to establish this conjecture, but we now are not able to prove this conjecture in the full generality. There are however several particular cases when the verification can be easily done, for example, for any Mersenne prime $2^n - 1$, n is a regular number. In practice, a verification of that a given n is regular can be done using the resultant, as it shown in the example below.

Example 9.7. Let $n = 2$, then $\mathbb{Z}_3^\times \setminus \Delta_2 = \emptyset$, hence $n = 2$ is a regular integer, implying that

$$\mathrm{Aut}(\mathbf{K}^2, \bullet_\tau) \cong \mathbb{Z}_3 \rtimes_\delta \mathbb{Z}_2 \cong S_3.$$

The latter is the well-known fact that S_3 is an internal semi-direct product of the subgroups $\mathbb{Z}_3$ and $\mathbb{Z}_2$, where $\mathbb{Z}_3$ is the subgroup generated by one of the two 3-cycles and $\mathbb{Z}_2 \cong C_2$ is the subgroup generated by any transposition.

Example 9.8. Let $n = 3$, then $\Lambda_3(z) = z + z^2 + z^4$ and $\mathbb{Z}_7^\times \setminus \Delta_3 = \{3, 5, 6\}$. An easy verification shows that the resultant

$$R(\frac{\Lambda_3(z^q) - \Lambda_3(z)}{z(z-1)}, \Phi_7(z)) = 7^2 \neq 0, \qquad \forall q \in \{3, 5, 6\},$$

hence $\Lambda_3(z^q) - \Lambda_3(z)$ does not have common divisors with $\Phi_7(z)$ (note that $z = 0, 1$ cannot be common zeros). Therefore $n = 3$ is a regular integer. Similarly, for $\Lambda_4(z) = z + z^2 + z^4 + z^8$, $\mathbb{Z}_{15}^\times \setminus \Delta_3 = \{7, 11, 13, 14\}$ and

$$R(\frac{\Lambda_4(z^q) - \Lambda_4(z)}{z(z-1)}, \Phi_{15}(z)) = 3^4 \cdot 5^4 \neq 0, \qquad \forall q \in \Delta_3,$$

Finally, we point out the following useful observation. Let $n \geq 2$ be an integer, and $\Phi_n(z)$ be the cyclotomic polynomial of degree n. Consider the quotient polynomial algebra

$$\mathbb{T}_n := (\mathbf{K}[z]/\Phi_{2^n-1}(z), \bullet) \cong (\mathbf{K}^{\phi(2^n-1)}, \bullet)$$

where ϕ is Euler's totient function. Then $\mathrm{Aut}(\mathbb{T}_n) \cong S_{\phi(2^n-1)}$, where any automorphism is a substitution $P(z) \to P(t_\alpha(z))$, with $\alpha \in S_n$ and $t_\alpha(z)$ is the Lagrange polynomial of degree $\leq \phi(2^n - 1)$ uniquely determined the relations $t_\alpha(\zeta^k) = \zeta^{\alpha(k)}$ for any $k \in \mathbb{Z}_{2^n-1}^\times$, where ζ is

a fixed primitive root of unity of degree 2^n-1. Note that $h_m(z) := z^m \in \mathrm{Aut}(\mathbb{T}_n)$, where $m \in \mathbb{Z}^\times_{2^n-1}$ ($\mathbb{Z}^\times_{2^n-1}$ is an abelian subgroup of $S_{\phi(2^n-1)}$).

Now, let us consider $\Lambda_n(z)$ as an element in $\mathbb{T}_n$. By (50), $\Phi_{2^n-1}(z)|(z^{2^n-1}-1)$, hence

$$\Lambda_n(z^2) - \Lambda_n(z) = z^{2^n} - z \equiv 0 \mod \Phi_{2^n-1}(z),$$

therefore $\Lambda_n(z^2) = \Lambda_n(z)$, in other words we conclude that

Proposition 9.9. *Λ_n is a fixed point of the natural action of Δ_n by substitutions. Moreover, the integer n is regular if and only if the stabilizer subgroup of Λ_n in $\mathbb{Z}^\times_{2^n-1}$ is exactly Δ_n.*

10 Three examples for $n = 3$

The main goal of this section is to illustrate our results for $(\mathbf{K}^n, \bullet_\sigma)$ in the particular case $n = 3$. We shall assume that $\mathbf{K}$ is splitting field of polynomial $P(z) = z^3 - 1$ and ϵ will denote a primitive root of unity of degree 3 (in section 10.2 we additionally assume that also a primitive root of unity of degree 7 exists). By Theorem 7.1, there are exactly three distinct (isomorphy classes of) inner isotopes coded by the conjugacy classes of S_3, which are in a one-to-one correspondence with integer partitions of 3, i.e.

$$\begin{aligned} 3 &= 1+1+1 \\ &= 2+1 \\ &= 3. \end{aligned} \tag{52}$$

Each of the three-dimensional isotope algebras will be considered below.

10.1 The case "1 + 1 + 1": a unital commutative associative algebra

In this case we have the trivial three cycle partition $1+1+1$ which uniquely determines the unity in S_3: $e = (1)(2)(3)$ (in the cyclic notation), thus

$$(\mathbf{K}^3, \bullet_e) \cong (\mathbf{K}^3, \bullet)$$

i.e. the corresponding inner isotope is the associative (direct product) algebra $(\mathbf{K}^3, \bullet)$ itself. The multiplication structure is a uniquely determined by the multiplication table in the standard basis $\{e_1, e_2, e_3\}$ (2):

$$e_i \bullet e_j = e_{i+j(\mathrm{mod}\,3)}.$$

The automorphism group is given by Theorem 7.1

$$\mathrm{Aut}(\mathbf{K}^3, \bullet_e) \cong S_3.$$

The algebra $(\mathbf{K}^3, \bullet_e)$ is generic and any algebra idempotent can be written as $c_k = (\alpha_1, \alpha_2, \alpha_3)$, where $(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{F}_2^3$ is the binary decomposition of k, $0 \le k \le 7$. For

example, the binary codes $1 = 001_2$, $2 = 010_2$ and $4 = 100_2$ correspond to the three standard basis idempotents e_3, e_2, e_1. The idempotent $c_7 = e_1 + e_2 + e_3$ is the algebra unity. This yields the multiplication table (Table 1 below) and the characteristic polynomials χ_i of $L_{\bullet_e}(c_i)$ are given by (cf. with (32))

$$\begin{aligned} \chi_0 = \lambda^3, \qquad \chi_1 = \chi_2 = \chi_4 = (\lambda-1)\lambda^2, \\ \chi_3 = \chi_4 = \chi_6 = (\lambda-1)^2\lambda, \qquad \chi_7 = (\lambda-1)^3. \end{aligned} \tag{53}$$

$\bullet_\tau$	1	2	3	4	5	6	7
1	1	0	1	0	1	0	1
2	0	2	2	0	0	2	2
3	1	2	3	0	1	2	3
4	0	0	0	4	4	4	4
5	1	0	1	4	5	4	5
6	0	2	2	4	4	6	6
7	1	2	3	4	5	6	7

Table 1: The multiplication table of idempotents $i \sim c_i$ in $(\mathbf{K}^3, \bullet_e)$ with $e = (1)(2)(3) \in S_3$

Note that $(\mathbf{K}^3, \bullet_e)$, as an associative algebra is axial in the sense of Definition 1.3 above, it follows from the classical results due to Benjamin Peirce. Indeed, $(\mathbf{K}^3, \bullet_e) = \mathrm{span}(\{e_1, e_2, e_4\})$, these idempotents are primitive and satisfye the same fusion law:

$\bullet_e$	$\mathbb{A}_1$	$\mathbb{A}_0$
$\mathbb{A}_1$	$\mathbb{A}_1$	$\mathbb{A}_0$
$\mathbb{A}_0$	0	$\mathbb{A}_0$

(54)

However, in contrast to the single cycle case (see section 10.2 below), the set of nonzero idempotents is *not* a multiplicative magma, see table 1.

10.2 The single cycle case "3": a commutative isospectral medial algebra

The one-cycle partition corresponds to the conjugacy class of $\tau = (2\,3\,1) \in S_3$, i.e. shifts. Such algebras have been introduced and studied first for $n = 3$ in [16] in the context of isospectral algebras and later for any $n \geq 2$ in [17] in the polynomial setting. It is natural to assume that the ground field $\mathbf{K}$ additionally contains a primitive root of unity of order $7 = 2^3 - 1$, denote it by ζ.

The standard basis elements are no longer idempotents, for example $e_1 \bullet_\tau e_1 = e_2$. By Proposition 8.1, the algebra $(\mathbf{K}^3, \bullet_\tau)$ is generic and contains 7 distinct nonzero idempotents, which can be explicitly written by

$$\mathrm{Idm}(\mathbf{K}^3, \bullet_\tau) = \{c_k = (\zeta^{4k}, \zeta^{2k}, \zeta^k) : \quad k \in \mathbb{Z}/7\mathbb{Z}\}. \tag{55}$$

The multiplication rule (27) between idempotents takes the form

$$c_i \bullet_\tau c_j = c_{4(i+j)} = c_{i \circledast j}, \tag{56}$$

where $\circledast$ on $\mathbb{Z}/7\mathbb{Z}$ is defined by

$$i \circledast j \equiv 4(i+j) \mod 7. \tag{57}$$

The characteristic polynomials are given by

$$\det(\lambda \mathbb{1} - L_{\bullet_\tau}(c_k)) = \lambda^3 - 1. \tag{58}$$

Therefore $(\mathbf{K}^3, \bullet_\tau)$ is **isospectral** and furthermore it is an **axial** algebra with the following fusion law:

$\bullet_\omega$	$\mathbb{A}_1$	$\mathbb{A}_\epsilon$	$\mathbb{A}_{\epsilon^2}$
$\mathbb{A}_1$	$\mathbb{A}_1$	$\mathbb{A}_\epsilon$	$\mathbb{A}_{\epsilon^2}$
$\mathbb{A}_\epsilon$	$\mathbb{A}_\epsilon$	$\mathbb{A}_{\epsilon^2}$	$\mathbb{A}_1$
$\mathbb{A}_{\epsilon^2}$	$\mathbb{A}_{\epsilon^2}$	$\mathbb{A}_1$	$\mathbb{A}_\epsilon$

(59)

Combining Theorem 9.2 and Theorem 9.5 with Example 9.8, we obtain

Theorem 10.1. *The idempotent quasigroup and the algebra automorphism groups are respectively:*

$$\mathrm{Aut}(\mathrm{Idm}(\mathbf{K}^3, \bullet_\tau)) \cong \mathbb{Z}_7 \rtimes_{\mathrm{id}} \mathbb{Z}_7^\times \tag{60}$$

$$\mathrm{Aut}(\mathbf{K}^3, \bullet_\tau) \cong \mathbb{Z}_7 \rtimes_\delta \mathbb{Z}_3, \tag{61}$$

where $\mathbb{Z}_7 \rtimes_\delta \mathbb{Z}_3$ is the smallest non-abelian group of odd order.

Furthermore, $(\mathbf{K}^3, \bullet_\tau)$ has many other remarkable properties (see [17] for a more detailed discussion), for example it satisfies the algebra identity

$$(x \bullet_\tau (x \bullet_\tau (x \bullet_\tau y))) = \Delta(x) y, \qquad \forall x, y \in (\mathbf{K}^3, \bullet_\tau),$$

where Δ is a multiplicative homomorphism of degree 3 given explicitly by a circulant:

$$\Delta(a_0 e_0 + a_1 e_1 + a_2 e_2) = \begin{vmatrix} a_0 & a_2 & a_1 \\ a_1 & a_0 & a_2 \\ a_2 & a_1 & a_0 \end{vmatrix} : (\mathbf{K}^3, \bullet_\tau) \to (\mathbf{K}, \bullet).$$

10.3 The case $[2+1]$

Finally, we consider the two-cycle partition $[2+1]$ corresponding to the conjugacy class of transpositions. Without loss of generality we can assume that $\omega = (2\,1)(3) \in S_3$. As in section 10.1, the algebra $(\mathbf{K}^3, \bullet_\omega)$ is decomposable, more precisely:

$$(\mathbf{K}^3, \bullet_\omega) \cong (\mathbf{K}^2, \bullet_\tau) \times (\mathbf{K}, \bullet_e). \tag{62}$$

The second factor is trivial and the first factor is the two-dimensional *Harada algebra* [11], i.e. a uniquely determined up to isomorphism two-dimensional commutative algebra generated by two distinct idempotents c_1 and c_2 subject to the condition $c_1 \bullet c_2 = -c_1 - c_2$ (we don't need this characterization later and leave the details to an interested reader).

Combining (62) with Example 9.7, we get

Proposition 10.2. *There holds* $\mathrm{Aut}(\mathbf{K}^3, \bullet_\omega) \cong S_3$.

11 Final remarks and questions

There are at least two natural questions that remained unanswered in this article: 1) Determine the automorphism group of the obtained inner isotopes of commutative associative algebras $(\mathbf{K}^n, \bullet)$ for the general dimensions, and 2) Which of the constructed above inner isotopes are axial algebras. Note that in Section 10 we completely discussed these two questions in the case $n = 3$ (the case $n = 2$ is trivial). A further analysis reveals that by the same methods are applicable to $n = 4$; also some partial results were mentioned in [17].

Another interesting natural question is how to apply the present methods to general *nonassociative* commutative algebras or at least to inner isotopes of the 2nd order:

$$(\mathbb{A}, \star) \rightsquigarrow (\mathbb{A}, \star_h) \rightsquigarrow (\mathbb{A}, \star_{hg}) \rightsquigarrow \dots$$

where $h \in \mathrm{Aut}(\mathbb{A}, \star)$, $g \in \mathrm{Aut}(\mathbb{A}, \star_h)$ etc?

Finally, we mention that some methods and ideas of the present paper (inner isotopies) can be useful in the case $\mathbf{K} = \mathbb{C}$ in the study, for example, of algebras of holomorphic functions in the unit disk like Bergman and Bloch spaces of holomorphic functions defined on the open unit disc in the complex plane [12].

References

[1] *Studies in modern algebra*, volume Vol. 2 of *Studies in Mathematics*. Mathematical Association of America, distributed by Prentice-Hall, Inc., Englewood Cliffs, NJ, 1963. edited by A. Albert.

[2] A. Castillo-Ramirez and J. McInroy. Miyamoto groups of code algebras. *J. Pure Appl. Algebra*, 225(6):106619, 2021.

[3] T. De Medts, S. F. Peacock, S. Shpectorov, and M. Van Couwenberghe. Decomposition algebras and axial algebras. *J. Algebra*, 556:287–314, 2020.

[4] T. De Medts and M. Van Couwenberghe. Modules over axial algebras. *Algebr. Represent. Theory*, 23:209–227, 2020.

[5] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[6] D. J. F. Fox. Killing metrized commutative nonassociative algebras associated with Steiner triple systems. *J. Algebra*, 608:186–213, 2022.

[7] C. Franchi, M. Mainardis, and S. Shpectorov. An infinite-dimensional 2-generated primitive axial algebra of Monster type. *Ann. Mat. Pura Appl. (4)*, 201(3):1279–1293, 2022.

[8] R. L. Griess, Jr. The Monster and its nonassociative algebra. In *Finite groups—coming of age (Montreal, Que., 1982)*, volume 45 of *Contemp. Math.*, pages 121–157. Amer. Math. Soc., Providence, RI, 1985.

[9] J. Hall, F. Rehren, and S. Shpectorov. Universal axial algebras and a theorem of Sakuma. *J. Algebra*, 421:394–424, 2015.

[10] J. I. Hall and S. Shpectorov. The spectra of finite 3-transposition groups. *Arab. J. Math. (Springer)*, 10(3):611–638, 2021.

[11] K. Harada. On a commutative nonassociative algebra associated with a doubly transitive group. *J. Algebra*, 91(1):192–206, 1984.

[12] H. Hedenmalm, B. Korenblum, and K. Zhu. *Theory of Bergman spaces*, volume 199 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[13] I. Kaplansky. Infinite-dimensional quadratic forms admitting composition. *Proc. Amer. Math. Soc.*, 4:956–960, 1953.

[14] S. M. S. Khasraw, J. McInroy, and S. Shpectorov. On the structure of axial algebras. *Trans. Amer. Math. Soc.*, 373(3):2135–2156, 2020.

[15] Y. Krasnov and V. G. Tkachev. Idempotent geometry in generic algebras. *Adv. Appl. Clifford Algebr.*, 28:84, 2018.

[16] Y. Krasnov and V. G. Tkachev. Variety of idempotents in nonassociative algebras. In *Topics in Clifford Analysis. A Special Volume in Honor of Wolfgang Sprössig*, Trends Math. Birkhäuser/Springer, 2019.

[17] Y. Krasnov and V. G. Tkachev. Medial and isospectral algebras. 2022. arXiv:2210.08245.

[18] N. Nadirashvili, V. G. Tkachev, and S. Vlăduţ. *Nonlinear elliptic equations and nonassociative algebras*, volume 200 of *Math. Surveys and Monographs*. AMS, Providence, RI, 2014.

[19] S. Norton. The Monster algebra: some new formulae. In *Moonshine, the Monster, and related topics (South Hadley, MA, 1994)*, volume 193 of *Contemp. Math.*, pages 297–306. Amer. Math. Soc., Providence, RI, 1996.

[20] H. P. Petersson. The classification of two-dimensional nonassociative algebras. *Results Math.*, 37(1-2):120–154, 2000.

[21] F. Rehren. Generalised dihedral subalgebras from the Monster. *Trans. Amer.Math.Soc.*, 369(10):6953–6986, 2017.

[22] A. J. E. Ryba. A natural invariant algebra for the Harada-Norton group. *Math. Proc. Cambridge Philos. Soc.*, 119(4):597–614, 1996.

[23] R. Schafer. *An introduction to nonassociative algebras*. Pure and Applied Mathematics, Vol. 22. Academic Press, New York, 1966.

[24] B. Segre. Famiglie di ipersuperficie isoparametrische negli spazi euclidei ad un qualunque numero di demesioni. *Atti. Accad. naz Lincie Rend. Cl. Sci. Fis. Mat. Natur.*, 21:203–207, 1938.

[25] S. D. Smith. Nonassociative commutative algebras for triple covers of 3-transposition groups. *Michigan Math. J.*, 24(3):273–287, 1977.

[26] H. Suzuki. Commutative algebras associated with a doubly transitive group. *Osaka J. Math.*, 23(3):541–561, 1986.

[27] E. A. Tevelev. Generic algebras. *Transform. Groups*, 1(1-2):127–151, 1996.

[28] E. A. Tevelev. *Projective duality and homogeneous spaces*, volume 133 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2005. Invariant Theory and Algebraic Transformation Groups, IV.

[29] V. G. Tkachev. Spectral properties of nonassociative algebras and breaking regularity for nonlinear elliptic type PDEs. *Algebra i Analiz*, 31(2):51–74, 2019.

[30] V. G. Tkachev. The universality of one half in commutative nonassociative algebras with identities. *J. Algebra*, 569:466–510, 2021.

[31] V. G. Tkachev. Inner isotopes associated with automorphisms of commutative associative algebras (the polynomial setup). 2023. arXiv:2308.16284v1.

[32] S. Walcher. On algebras of rank three. *Comm. Algebra*, 27(7):3401–3438, 1999.

Received: September 1, 2023
Accepted for publication: July 26, 2024
Communicated by: Adam Chapman, Mohamed Elhamdadi and Ivan Kaygorodov