Medial and Isospectral Algebras

Vladimir G. Tkachev

Linköping University

(joint work with Yakov Krasnov, Bar Ilan University)

Find the differences!

Friday 25 September

09:30 - 10:00	Dr. Jouko Mickelsson Or: How I Learned To Stop Worrying And Love The Gerbe (Stefan Wagner)
10:10 - 10:40	Hom-algebra structures (Sergei Silvestrov)
10:40 - 11:00	**Coffee break**
11:00 - 11:30	On solvability and nilpotency of n-Hom-Lie algebras (Abdennour Kitouni)
11:40 - 12:10	When is a group ring a Köthe ring? (Johan Öinert)
12:10 - 13:30	**Lunch**
13:30 - 14:00	Medial and Isospectral Algebras (Vladimir G. Takchev)
14:10 - 14:40	The hom-associative Weyl algebras in prime characteristic (Per Bäck)

Participants

Joakim Arnlind (Linköping University)
Masood Aryapoor (Mälardalen University)
Per Bäck (Mälardalen University)
Magnus Goffeng (Lund University/LTH)
Kwalombota Ilwale (Linköping University)
Abdennour Kitouni (Mälardalen University)
Lars Hellström (Mälardalen University)
Daniel Lännström (Blekinge Institute of Technology)
Melanija Mitrovic (University of Nis)
Patrik Nystedt (University West)
Johan Richter (Blekinge Institute of Technology)
Sergei Silvestrov (Mälardalen University)
Axel Tiger Norkvist (Linköping University)
Vladimir G. Tkachev (Linköping University)
Stefan Wagner (Blekinge Institute of Technology)
Chia Zargeh (University of Sao Paolo)
Johan Öinert (Blekinge Institute of Technology)

. . . Now, more seriously

In a commutative algebra, the **spectrum** of an idempotent is the multiset of eigenvalues of the (left/right) multiplication operator by the idempotent.

The **algebra spectrum** is the union of all idempotent spectra.

Proposition

Idempotents and their spectra play a prominent role in (non)associative algebra.

Some natural questions:

1. How much an algebra is determined by its spectrum?
2. Characterize **isospectral** algebras, i.e. those where all idempotents share the same spectrum.

The main result

Let $z^n - 1$ be solvable over a field $\mathbb{K}$ and let $\mathscr{C}_n(z, \circ)$ denote the quotient algebra

$$\mathscr{C}_n = \mathbb{K}[z]/(z^n - 1)$$

with a new **non-associative commutative** multiplication on $\mathscr{C}_n$ defined by

$$p(z) \circ q(z) = p(\epsilon_n z) q(\epsilon_n z) \mod (z^n - 1),$$

where ϵ_n is a primitive root of unity of order n. In other words, $\mathscr{C}_n$ is a **strong isotopy** of the associative commutative algebra $\mathbb{K}[z]/(z^n - 1)$ by a *cyclic linear substitution*.

Theorem 1

A commutative algebra is a generic medial isospectral algebra, i.e.

$$(xy)(zw) = (xz)(yw),$$

if and only if it is isomorphic to some $\mathscr{C}_n$.

Basic notation and terminology

By an **algebra** $\mathbf{A}$ we shall always mean

- a *commutative*, maybe *nonassociative*
- finite dimensional algebra over a field $\mathbb{K}$ of $\mathrm{char}(\mathbb{K}) \neq 2, 3$.

The (left) multiplication operator $L_x : y \to xy$. It completely determines the algebra structure. For example, a *commutative* algebra is associative if and only if

$$(xy)z = x(yz) \quad \Leftrightarrow \quad L_{xy} = L_x L_y.$$

The **spectrum** of $x \in \mathbf{A}$ is the multiset of eigenvalues of L_x. The characteristic polynomial

$$\mathrm{Char}_x(t) := \det(L_x - tI)$$

The set of nonzero idempotents (i.e. $c^2 = c$) of $\mathbf{A}$ is denoted by $\mathrm{Idm}(\mathbf{A})$.

Basic notation and terminology

The **Peirce spectrum of an algebra $\mathbf{A}$** is the union of all possible distinct eigenvalues of L_c, $c \in \mathrm{Idm}(\mathbf{A})$.

An idempotent c is **semisimple** if $\mathbf{A}$ decomposes into a direct sum of eigenspaces of L_c (Peirce subspaces):

$$\mathbf{A} = \bigoplus_{\lambda \in \sigma(\mathbf{A})} \mathbf{A}_c(\lambda)$$

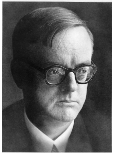
Benjamin Peirce (1809-1880)

EXAMPLE 1. The Peirce spectrum of an associative algebra is $\{0, 1\}$, an idempotent is a projector and the multiplicity of 1 is the dimension of the projection target space.

EXAMPLE 2. A commutative algebra is **Jordan** if

$$[L_{x^2}, L_x] = 0.$$

The Peirce spectrum of a Jordan algebra is $0, \frac{1}{2}, 1$



Pascal Jordan (1902-1980)

Isotopism

The isotopism of algebras is an important concept of nonassociative algebra introduced by A. Albert in 1942 (motivated by N. Steenrod work on homotopy groups in topology).

Two algebras $\mathbf{A}$ and $\mathfrak{B}$ over a field $\mathbb{K}$ are **isotopic** if there exist non-singular linear transformations f, g, $h : \mathbf{A} \to \mathfrak{B}$ such that

$$f(x)g(y) = h(xy).$$

Adrian Albert (1905-1972)

If $f = g$, $\mathbf{A}$ and $\mathfrak{B}$ are called **strongly isotopic**.

If $f = g = h$, the algebras $\mathbf{A}$ and $\mathfrak{B}$ are called **isomorphic**.

Some starting points and motivations

How to recover an algebra structure?

Some starting points and motivations

- Typically one works with the structure constants

$$e_i e_j = \sum_{k=1}^{n} \theta_{ijk} e_k, \qquad \{e_i\} \text{ is a basis of } \mathbf{A}$$

- Alternatively, one may decompose an algebra into bigger 'blocks' $\mathbf{A} = \bigoplus_{\alpha \in I} \mathbf{A}_\alpha$ and prescribe (recover) the multiplication (**fusion**) rules between the blocks

$$\mathbf{A}_\alpha \mathbf{A}_\beta \subset \bigoplus_{\gamma \in \theta(\alpha,\beta)} \mathbf{A}_\gamma, \qquad \theta(\alpha, \beta) \subset I \text{ is a fusion rule}$$

- In particular, the Peirce decomposition is a perfect tool for an 'algebra analysis'. For example, any Jordan algebra satisfies

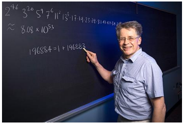
$\star$	1	0	$\frac{1}{2}$
1	1	$\emptyset$	$\frac{1}{2}$
0	$\emptyset$	0	$\frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$1, 0$

The Griess-Conway-Norton algebra

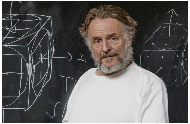
Another example, the 196884-dimensional Griess-Conway-Norton algebra (its automorphism group is the Monster sporadic simple group) **unital commutative nonassociative metrized algebra** with fusion rules:

$\star$	1	0	$\frac{1}{4}$	$\frac{1}{32}$
1	1	$\emptyset$	$\frac{1}{4}$	$\frac{1}{32}$
0	$\emptyset$	0	$\frac{1}{4}$	$\frac{1}{32}$
$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$1, 0$	$\frac{1}{32}$
$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{32}$	$1, 0, \frac{1}{4}$

Only a part of idempotents ('**axes**') share the spectrum and fusion rules. To identify the Monster group some further axioms are needed (Majorana algebras, axel algebras, code algebras).



Robert Griess, born 1945



John Conway, born 1937

Simon P. Norton (1952-2019)

Algebras of cubic minimal cones

A completely different context coming from **PDEs and Calculus of Variations**: classification of commutative nonassociative algebras of minimal cones (*soap films given by zero level sets of a cubic polynomial*) gives rise to a class of commutative nonassociative metrized algebras with the Peirce spectrum $1, -1, -\frac{1}{2}, \frac{1}{2}$ and

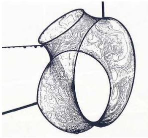
$\star$	1	-1	$-\frac{1}{2}$	$\frac{1}{2}$
1	1	-1	$-\frac{1}{2}$	$\frac{1}{2}$
-1	-1	1	$\frac{1}{2}$	$-\frac{1}{2}, \frac{1}{2}$
$-\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	$1, -\frac{1}{2}$	$-1, \frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}, \frac{1}{2}$	$-1, \frac{1}{2}$	$1, -1, -\frac{1}{2}$

In this case **all** (actually infinitely many) **idempotents share the same spectrum and satisfy the same fusion law**.

♡ A recent book *Nonlinear Elliptic Equations and Nonassociative Algebras* Vol.200, Math. Surveys and Monographs, AMS, 2015 by N. Nadirashvili, V.T., S. Vlăduţ

Algebras of cubic minimal cones

A **minimal surface** is a critical point of the area functional. Geometrically, this means that the **mean curvature vanishes**. A **minimal cone** is a typical singularity of a minimal surface.



A homogeneous **cubic** polynomial $u \in \mathbb{R}[x_1, \ldots, x_n]$ defines a minimal cone $u(x) = 0$ iff it satisfies the Hsiang equation

$$|\nabla u|^2 \Delta u - \tfrac{1}{2}\langle \nabla u; \nabla |\nabla u|^2 \rangle = C\, u(x)\, \|x\|^2$$

The corresponding *commutative metrized* algebra satisfies the algebra identity:

$$4z^4 + z^2 z^2 - 3b(z,z)z^2 - 2b(z,z^2)z = 0.$$

Wu-yi Hsiang (born 1937)

where $b(x, y)$ is the standard scalar product in $\mathbb{R}^n$. Any such an algebra is **isospectral** with the Peirce decomposition

$$\mathbf{A} = \mathbb{R}c \oplus \mathbf{A}_c(-1) \oplus \mathbf{A}_c(-\tfrac{1}{2}) \oplus \mathbf{A}_c(\tfrac{1}{2})$$

but with infinitely many idempotents.

Remarkably (a nontrivial result), $\mathbb{R}c \oplus \mathbf{A}_c(-\frac{1}{2})$ is an isotope of a certain Jordan algebra structure which completely determines the ambient algebra structure.

So, how much the algebra structure is determined by its Peirce spectrum?

Generic algebras

Following to B. Segre (1938), one can interpret idempotents in commutative algebras over $\mathbb{C}$ as solutions of a quadratic system

$$\sum_{i,j=1}^{n} \theta_{ijk} x_i x_j = x_k, \qquad 1 \le k \le n.$$

where $x = \sum_i x_i e_i$ is a basis decomposition.

Beniamino Segre (1903-1977)

Since a generic (in the Zariski sense) polynomial system has always *Bézout's number* of solutions, a *generic* algebra must have exactly $2^{\dim A}$ **distinct** idempotents (including 0). The genericity here should be understood in the sense that the subset of nonassociative algebra structures on a vector space V is an open Zariski subset in $V^* \otimes V^* \otimes V$.

Definition

An algebra over $\mathbb{C}$ is called a *generic* if it contains exactly $2^{\dim \mathbf{A}}$ distinct idempotents.

Syzygies in generic algebras

The statement below provides us with a **global** information about $\mathrm{Idm}(\mathbf{A})$.

Theorem 2 (Krasnov Y., V.T., 2018)

A commutative nonassociative algebra $\mathbf{A}$ *over* $\mathbb{C}$ *is generic iff* $\frac{1}{2} \notin \sigma(\mathbf{A})$ *and* $\mathbf{A}$ *does not contain* 2*-nilpotents. In that case*

$$\sum_{c \in \mathrm{Idm}(\mathbf{A})} \frac{\mathrm{Char}_c(t)}{\mathrm{Char}_c(\frac{1}{2})} = 2^n(1-t^n), \quad \forall t \in \mathbb{C}, \tag{1}$$

where $\mathrm{Char}_c(t) = \det(L_c - \mathbf{1}t)$ *is the characteristic polynomial of* L_c*. Furthermore, if* $H(x) : \mathbb{K}^n \to \mathbb{K}^s$ *is a vector-valued polynomial map such that* $\deg H_i \le n-1$ *then*

$$\sum_{c \in \mathrm{Idm}_0(\mathbf{A})} \frac{H(c)}{\mathrm{Char}_c(\frac{1}{2})} = 0$$

$$\sum_{c \in \mathrm{Idm}(\mathbf{A})} \frac{c}{\mathrm{Char}_c(\frac{1}{2})} = 0$$

In this talk I will discuss what happens if *all idempotents share the same spectrum*?

One has two different principal cases: non-generic and generic algebras.

In this talk I will discuss what happens if *all idempotents share the same spectrum*?

One has two different principal cases: non-generic and generic algebras.

The **non-generic** case is the most difficult. So far, the only known example is the algebras of *cubic minimal cones*.

In this talk I will discuss what happens if *all idempotents share the same spectrum*?

One has two different principal cases: non-generic and generic algebras.

The **non-generic** case is the most difficult. So far, the only known example is the algebras of *cubic minimal cones*.

In the **generic** case, $\mathrm{Char}_c(t)$ does not depend on a choice of c, hence the syzygy relation implies

$$\sum_{c\in \mathrm{Idm}(\mathbf{A})} \frac{\mathrm{Char}_c(t)}{\mathrm{Char}_c(\frac{1}{2})} = (2^n-1)\frac{\mathrm{Char}_c(t)}{\mathrm{Char}_c(\frac{1}{2})} = 2^n(1-t^n)$$

therefore

$$\mathrm{Char}_c(t) = t^n - 1,$$

i.e. the characteristic polynomial of each idempotent must be **cyclotomic**.

An example: the 2D Harada algebra

Let $\mathbf{A}_2(\mathbb{K})$ be the commutative algebra generated by idemotents c_1 and c_2 with

$$c_1 c_2 = -c_1 - c_2.$$

This immediately implies for $c_3 = -c_1 - c_2$ that

$$c_3^2 = c_1^2 + 2c_1c_2 + c_2^2 = c_1 + 2(-c_1 - c_2) + c_2 = c_3.$$

One can show that c_1, c_2, c_3 are the only nonzero idempotents in $\mathbf{A}_2(\mathbb{K})$ and

$$c_i c_j = c_k, \quad \text{where } \{i, j, k\} = \{1, 2, 3\}.$$

Thus the spectrum of each c_i is $\{1, -1\}$, i.e. $\mathbf{A}_2(\mathbb{K})$ is an **isospectral algebra**.

A family algebras including $\mathbf{A}_2(\mathbb{K})$ has been defined and studied by Koichiro Harada in 1981 and

$$\mathrm{Aut}(\mathbf{A}_2(\mathbb{K})) = \mathrm{Perm}(\mathrm{Idm}(\mathbf{A}_2)) \cong S_3,$$

Remark. The general Harada algebras in dimensions $n \geq 3$ are **not** isospectral.

On a Commutative Non-Associative Algebra Associated with a Doubly Transitive Group

KOICHIRO HARADA

Department of Mathematics, Ohio State University, Columbus, Ohio 43210

Communicated by Walter Feit

Received July 6, 1983

1. PERMUTATION GROUPS AND COMMUTATIVE ALGEBRAS

In [2], the author constructed a commutative (nonassociative) algebra A defined as follows[1]:

(1) A is a vector space over a field K with basis $\{x_1, x_2, \ldots, x_n\}$; and
(2) A possesses a commutative algebra structure satisfying

$$x_i x_i = (n-1) x_i \quad \text{for} \quad 1 \leqslant i \leqslant n,$$

and

$$x_i x_j = x_j x_i = -x_i - x_j \quad \text{for} \quad 1 \leqslant i < j \leqslant n.$$

Put $x_0 = -x_1 - x_2 - \cdots - x_n$. As shown in Lemma 1 of [2], we have

$$x_0 x_0 = (n-1) x_0,$$

An example: the 2D Harada algebra

One can prove that $\mathbf{A}_2$ satisfies the identity

$$x^3 = \beta_2(x)x, \qquad \forall x \in \mathbf{A}_2,$$

where the positive definite quadratic form

$$\beta_2(x) = x_1^2 - x_1x_2 + x_2^2, \quad \text{where } x = x_1c_1 + x_2c_2.$$

is a *multiplicative* homomorphism:

$$\beta_2(xy) = \beta_2(x)\beta_2(y).$$

Hence $\mathbf{A}_2$ is a commutative **composition nonunital** algebra.

The corresponding bilinear form

$$b(x, y) = \beta_2(x + y) - \beta_2(x) - \beta_2(y)$$

is *invariant*, therefore $\mathbf{A}_2$ metrized.

Furthermore, one can show that $\mathbf{A}_2$ is a Hsiang algebra (the algebra of the union of two perpendicular lines in $\mathbb{R}^2$).

An isospectral algebra in 3D

One can appropriately generalized the above in dimension $n = 3$: the corresponding isospectral algebra $\mathbf{A}_3(\mathbb{C})$ over the field of complex numbers $\mathbb{C}$ has been announced in (Krasnov, V.T., *Trends in Math.*, 2019). More precisely, let us consider the free commutative algebra over $\mathbb{C}$ spanned by three **idempotents** c_1, c_2, c_3 subject to

$$
\begin{aligned}
c_1c_2 &= (\gamma-1)c_1 - \gamma c_2 + \gamma c_3 &&=: c_5,\\
c_2c_3 &= \gamma c_1 + (\gamma-1)c_2 - \gamma c_3 &&=: c_6,\\
c_3c_1 &= -\gamma c_1 + \gamma c_2 + (\gamma-1)c_3 &&=: c_7,
\end{aligned}
$$

where γ is the *Kleinian integer unit*, i.e. a root of $2\gamma^2 - \gamma + 1 = 0$. Then one can show that $\{0, c_1, c_2, \ldots, c_7\}$ with

$$c_4 = -\gamma(c_1 + c_2 + c_3).$$

are the only idempotents of $\mathbf{A}_3$ with the same (cyclotomic) spectrum: for any $1 \leq i \leq 7$

$$\sigma(c_i) = \{1, \epsilon, \epsilon^2\}, \qquad \epsilon = \tfrac{-1-\sqrt{-3}}{2}, \quad \epsilon^3 = 1.$$

In particular, the algebra $\mathbf{A}_3$ is **generic and isospectral**.

An isospectral algebra in 3D

As in 2D, all nonzero idempotents in $\mathbf{A}_3(\mathbb{C})$ are closed under the algebra multiplication, i.e. form a **quasigroup**:

$$c_i c_j \in \mathrm{Idm}(\mathbf{A}_3(\mathbb{C})).$$

The multiplication rules between c_i follow the pattern in the **left** table below:

	1	2	3	4	5	6	7
1	**1**	3	2	5	4	7	6
2	3	**2**	1	6	7	4	5
3	2	1	**3**	7	6	5	4
4	5	6	7	**4**	1	2	3
5	4	7	6	1	**5**	3	2
6	7	4	5	2	3	**6**	1
7	6	5	4	3	2	1	**7**

$\Rightarrow$ an isotopy $\Rightarrow$

	1	2	3	4	5	6	7
1	1	5	2	6	3	7	4
2	5	2	6	3	7	4	1
3	2	6	3	7	4	1	5
4	6	3	7	4	1	5	2
5	3	7	4	1	5	2	6
6	7	4	1	5	2	6	3
7	4	1	5	2	6	3	7

The multiplication table is a *Latin square*, i.e. each index occurs precisely one time in each column and row. Remarkably, it also satisfies the **medial magma identity**

$$(xy)(zw) = (xz)(yw), \qquad \forall x, y, z, w \in \mathrm{Idm}(\mathbf{A}_3). \tag{MMI}$$

An isospectral algebra in 3D

Let us consider the permutation of c_i given accordingly to

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 2 & 3 & 6 & 4 & 7 \end{pmatrix}$$

The resulting multiplication (a *isotopy* of the Latin squares) gives the right table above which is more illuminating and informative. In particular, one has a nice pattern:

$$i \circledast j = \frac{1}{2}(i+j) \mod 7.$$

The latter multiplication $\circledast$ is commutative but nonassociative. But, since

$$(i \circledast j) \circledast (k \circledast l) \equiv \frac{1}{4}(i+j+k+l) \mod 7,$$

the new multiplication $\circledast$ **immediately** satisfies (MMI).

Finally, any element of $\mathbf{A}_3(\mathbb{C})$ satisfies a similar principal power identity

$$x^4 = \beta_3(x)x, \qquad \forall x \in \mathbf{A}_3(\mathbb{C}),$$

where $\beta_3(x) : \mathbf{A}_3(\mathbb{C}) \to \mathbb{C}$ is a certain **multiplicative homomorphism**.

Some further natural questions

- In which math contexts isospectral algebras could be relevant?
- Given $n \geq 2$, do there exist isospectral algebras in dimension n? How many?
- Describe generic isospectral algebras.
- What is about nongeneric isospectral algebras? (for example, Hsiang algebras)

Medial algebras

We have seen that some generic medial algebras satisfy the **medial magma identity**.

Definition

A commutative algebra $\mathbf{A}$ satisfying

$$(xy)(zw) = (xz)(yw)$$

is said to be *medial*.

If the characteristic of the field not 2 or 3 then the definition is equivalent to

$$x^2y^2 = (xy)(xy).$$

An important immediate corollary of the definitions:

Proposition 1

The product of two idempotents in a medial algebra is again an idempotent.

Medial algebras and associative algebras

Proposition 2

Any associative commutative algebra is medial. Any **unital** *medial algebra is associative.*

Proof. Indeed, if e is the algebra unit then

$$x(yz) = (ex)(yz) = (ez)(xy) = z(xy) = (xy)z.$$

□

Conversely, a medial algebra having an idempotent with nondegenerate multiplication is *a (strong) isotope of a commutative associative unital algebra*.

Proposition 3

Let $\mathbf{A}$ *be a medial algebra,* $c \in \mathrm{Idm}(A)$ *and suppose that* L_c *is invertible (i.e.* $0 \notin \sigma(c)$*). Define the strong isotopy* $(\mathbf{A}, \circ)$ *with the new multiplication*

$$x \circ y = L_c^{-1}(xy). \tag{2}$$

Then $(\mathbf{A}, \circ)$ *is a unital commutative associative algebra.*

Existence: The cyclotomic polynomial model

Let $z^n - 1$ be solvable over $\mathbb{K}$ and let $\mathscr{C}_n(z, \circ)$ denote the quotient algebra

$$\mathscr{C}_n = \mathbb{K}[z]/(z^n - 1)$$

with a new non-associative multiplication on $\mathscr{C}_n$ defined by

$$p(z) \circ q(z) = p(\epsilon_n z) q(\epsilon_n z) \mod (z^n - 1),$$

where ϵ_n is a primitive root of unity of order n. In other words, $\mathscr{C}_n$ is a **strong isotopy** of the associative commutative algebra $\mathbb{K}[z]/(z^n - 1)$ by a *cyclic linear substitution*.

Proposition 4

$\mathscr{C}_n$ is a medial (nonassociative) algebra.

Proof. Since

$$(p(z) \circ q(z)) \circ (r(z) \circ s(z)) = p(\epsilon_n^2 z) q(\epsilon_n^2 z) r(\epsilon_n^2 z) s(\epsilon_n^2 z) \mod (z^n - 1),$$

the **algebra $\mathscr{C}_n$ is medial**. We have $p(z) \circ q(z) = q(z) \circ p(z)$, but $\circ$ is **not** associative.

The cyclotomic polynomial model: an example

If $n = 2$ then $\epsilon_2 = -1$, hence

	1	z
1	1	$-z$
z	$-z$	1

In particular, $c_1 = 1$ is an idempotent and z is its eigenvector with eigenvalue -1. Also

$$(a + bz)^2 = (a^2 + b^2) \cdot 1 - 2ab \cdot z$$

implies that $c_{2,3} := -\frac{1}{2} \pm \frac{b}{2} z$ are the only idempotents $\neq c_1$ where $b^2 = -3$ in $\mathbb{K}$.

The algebra $\mathscr{C}_n(z)$ is generic and one can prove that *it is isomorphic to the 2D Harada algebra*. Indeed, the multiplication by c_1 interchange c_2 and c_3, while

$$c_2 c_3 = \frac{1}{4} + \frac{3}{4} z^2 \equiv 1 = c_1.$$

Isospectral medial generic algebras

Theorem 3 (Existence)

The $\mathscr{C}_n$ is an isospectral medial generic algebra. Furthermore,

$$L_{p(z)}^{\circ n} = \Delta(p)\mathbf{1}, \tag{3}$$

where

$$\Delta(p) := p(1)p(\epsilon_n)p(\epsilon_n^2)\cdots p(\epsilon_n^{n-1}) : \mathscr{C}_n \to \mathbb{K}$$

is a multiplicative homomorphism. In particular,

$$x^{\circ(n+1)} = \Delta(x)x$$

Theorem 4 (Uniqueness)

If two generic medial isospectral algebras over an algebraically closed field $\mathbb{K}$ have the same dimension they are isomorphic.

Remarks

While the algebra structure on $\mathscr{C}_n$ is given very explicitly, the structure of idempotents of $\mathscr{C}_n$ is more sophisticated.

In order to understand the relations between idempotents in a satisfactory way, one need to look at $\mathrm{Idm}(\mathbf{A})$ as a **quasigroup**.

A *quasigroup* is a set Q with a binary operation $\circ$ in which the equations $a \circ x = b$ and $y \circ a = b$ have unique solutions x and y for any given a and b from Q.

A quasigroup $(Q, \circ)$ is called *commutative* (resp. *idempotent*) if $x \circ y = y \circ x$ (resp. the identity $x \circ x = x$ holds for any $x \in Q$). Similarly, Q and it is called *medial* if the identity $(x \circ y) \circ (z \circ w) = (x \circ z) \circ (y \circ w)$ holds.

Theorem (The Bruck-Murdoch-Toyoda)

For any medial quasigroup $(Q, \circ)$, there exists an abelian group $(G, +)$, a fixed element $g \in G$, and commuting automorphisms $\phi, \psi : G \to G$ such that $x \circ y = g + \phi(x) + \psi(y)$.

Hence, *any medial quasigroup is an isotope of a certain abelian group G.*

Question. How to characterize the underlying abelian group G in a medial algebra?

Theorem 5

Let $\mathbf{A}$ *be a medial isospectral algebra of dimension* n*. Then* G *is* **cyclic***. Moreover, the there exists a bijection* $\phi : \mathrm{Idm}(\mathbf{A}) \to \mathbb{Z}_{2^n-1}$ *such that*

$$\phi(xy) \equiv \frac{1}{2}(\phi(x) + \phi(y)) \mod 2^n - 1.$$

Key ideas of the proof

The first part of the proof, the existence of a 'hidden' **abelian** group structure, repeats the argument due to A. Leibak and P. Puusemp (2014). One can prove that there exists an abelian group $(Q, \oplus)$, $Q = \mathrm{Idm}(\mathbf{A})$, with a neutral element $\nu \in Q$ such that

$$xy = T^{-1}(x) \oplus T^{-1}(y) = T^{-1}(x \oplus y),$$

where $T(x) = x \oplus x : Q \to Q$ is the doubling map. The most nontrivial part is the proof of the **cyclicity** of $(Q, \oplus)$, i.e. $Q \cong \mathbb{Z}_{2^n-1}$.

Let us consider $(Q, \oplus)$ as a module over $\mathbb{Z}$ in the canonical way. We have

$$2^s \otimes x = (2^{s-1} \otimes x) \oplus (2^{s-1} \otimes x) = T(2^{s-1} \otimes x) = \ldots = T^s(x). \tag{4}$$

Let $x \in Q$. Since $\mathrm{order}(Q, \oplus) = 2^n - 1$ we have $T^n(x) = 2^n \otimes x = x$. Therefore

$$T^{n-1}(x) \oplus \ldots \oplus T^1(x) \oplus x = (2^n - 1) \otimes x = \nu, \qquad \forall x \in Q. \tag{5}$$

The obtained identity holds for any $x \in Q$ and contains exactly n distinct summands $T^k(x)$.

Key ideas of the proof

We claim that there is no identity of the kind

$$T^{m_k}(x) \oplus \ldots \oplus T^{m_1}(x) = \nu, \qquad n > m_k > \ldots > m_1 \geq 0 \tag{6}$$

holding true for all $x \in Q$ and containing less than n summands. Indeed, suppose (6) holds. We have

$$u \oplus v = T(uv),$$

therefore, one combines successively the terms into a nonassociative product

$$\begin{aligned} T^{m_2}(x) \oplus T^{m_1}(x) &= T(T^{m_2}(x)T^{m_1}(x)) \\ T^{m_3}(x) \oplus T^{m_2}(x) \oplus T^{m_1}(x) &= T(T^{m_3}(x)T(T^{m_2}(x)T^{m_1}(x))) \\ \ldots &= \ldots \\ T^{m_k}(x) \oplus \ldots \oplus T^{m_1}(x) &= H(x), \end{aligned}$$

where by the linearity of T, the function H is a **homogeneous degree k polynomial** in $x \in \mathbf{A}$ and by the assumption

$$H(x) = \nu \qquad \text{for all } x \in Q.$$

By the syzygy relation

$$(2^n - 1)\nu = \sum_{x \in Q} H(x) = 0,$$

a contradiction follows.

Key ideas of the proof

Now we are ready to finish the proof. Suppose that $(Q, \oplus)$ is **not** cyclic. Then the lcm of the orders of all elements of $(Q, \oplus)$ is $m < 2^n - 1$. Then $m \otimes x = \nu$ for all $x \in Q$. Note that m divides $2^n - 1$, thus odd.

Let $m = 2^{s_1} + \ldots + 2^{s_{k-1}} + 1$ be the binary decomposition of m. Then using (4)

$$\begin{aligned} \nu &= m \otimes x \\ &= (2^{s_1} + \ldots + 2^{s_{k-1}} + 1) \otimes x \\ &= T^{s_1}(x) \oplus \ldots \oplus T^{s_{k-1}}(x) \oplus x, \end{aligned}$$

where the above sum contains less than n summands, that contradicts to the above claim. This proves that $(Q, \oplus)$ is cyclic, and thus isomorphic to $\mathbb{Z}_{2^n-1}$. In the latter case, the doubling operator is the usual multiplication by 2:

$$T(x) = 2x : \mathbb{Z}_{2^n-1} \to \mathbb{Z}_{2^n-1},$$

which yields the theorem.

THANK YOU FOR YOUR ATTENTION!