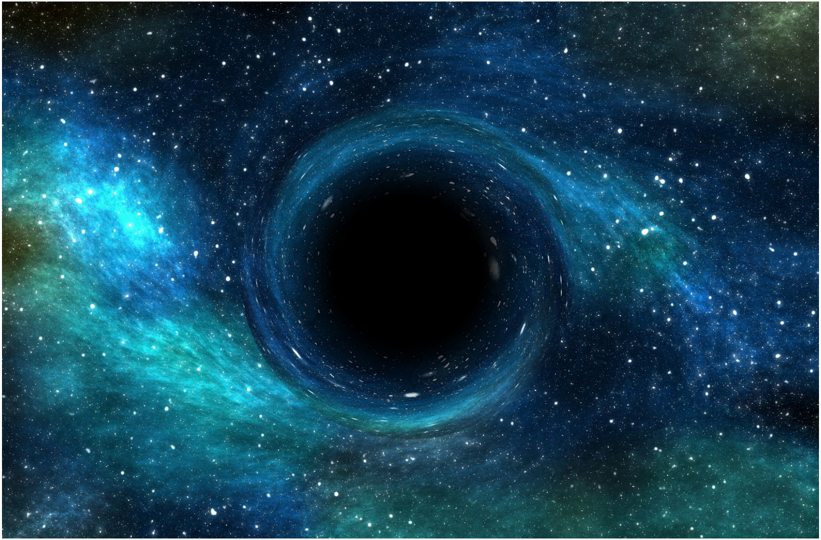
Mathieu-Zhao spaces of finite rings

Jan Schoone

Radboud University

30 August, 2018



Content

Questions?

If any questions arise, please feel free to ask them during the presentation.

Mathieu-Zhao spaces

Recap on ideals

In this talk all rings are considered to be commutative and have an identity, unless specified otherwise. All algebras are associative and contain 1.

Let R be a ring and A an R-algebra. An ideal I of A is an additive subspace of A such that for all $a, b \in A$ we have

$$a \in I \implies ba \in I.$$

Hence in particular, for all $a, b \in A$, if for all $m \geq 1$ we have $a^m \in I$, then for all $m \geq 1$ we have $ba^m \in I$.

Generalising

So for ideals:

for all $a, b \in A$, if for all $m \geq 1$ we have $a^m \in I$, then for all $m \geq 1$ we have $ba^m \in I$.

We can relax this a bit:

for all $a, b \in A$, if for all $m \geq 1$ we have $a^m \in I$, then for all $m \gg 0$ we have $ba^m \in I$.

(Here for all $m \gg 0$ we have $ba^m \in I$ means there exists some $N > 0$ such that for all $m \geq N$ we have $ba^m \in I$.)

Definition

We now define a *Mathieu-Zhao space* of A as an R-linear subspace M of A for which the following property holds:

If $a^m \in M$ for all $m \geq 1$, then for any $b \in A$ we have $ba^m \in M$ for all $m \gg 0$.

Example 1 (Ideals)

Ideals of algebras.

Not every Mathieu-Zhao space is an ideal!

Definition

We now define a *Mathieu-Zhao space* of A as an R-linear subspace M of A for which the following property holds:

If $a^m \in M$ for all $m \geq 1$, then for any $b \in A$ we have $ba^m \in M$ for all $m \gg 0$.

Not every Mathieu-Zhao space is an ideal!

Example 2

Consider $\mathbb{F}_4$ as a $\mathbf{Z}$-algebra. We know that $\mathbb{F}_4$ only has two ideals: 0 and 1. But the set $M := \{0, x\}$ is a Mathieu-Zhao space.

We have $x^2 = x + 1$. Since $x + 1$ is not an element of $\{0, x\}$, we find that this set indeed satisfies the conditions for a Mathieu-Zhao space.

Non-example

Let R be any ring, and A an R-algebra. Then $\Delta_A \subset A \times A$ is an R-linear space, but not a Mathieu-Zhao space:

We have:

$$\forall a \in A \; \forall n \geq 1 : (a,a)^n = (a^n, a^n) \in \Delta_A.$$

Hence, if Δ_A were a Mathieu-Zhao space, then we should have

$$\forall (b,c) \in A \times A \; \exists N \geq 0 \; \forall m \geq N : (b,c)(a,a)^m \in \Delta_A.$$

Let a be any non-nilpotent element and $(b,c) = (1,0)$ we have $(1,0)(a,a)^m = (a^m, 0) \notin \Delta_A$ for all $a \neq 0$.

So Δ_A is not a Mathieu-Zhao space.

Background and improvement

Mathieu Conjecture

Mathieu Conjecture (1995) Let G be a compact connected real Lie group with Haar measure σ. Let f be a complex-valued G-finite function on G such that $\int_G f^m d\sigma = 0$ for all $m \geq 1$. Then for every G-finite function g on G, also $\int_G g f^m d\sigma = 0$ for all large m.

The similarities to Mathieu-Zhao spaces is clear, and we can write (MC) in terms of Mathieu-Zhao spaces:

Mathieu Conjecture Let G be a compact connected real Lie group with Haar measure σ and let A be the algebra of complex-valued G-finite functions on G. Then

$$\left\{ f \in A \mid \int_G f d\sigma = 0 \right\}$$

is a Mathieu-Zhao space of A.

Duistermaat and Van der Kallen's theorem

Theorem 3 (Duistermaat-Van der Kallen (1998))

Let $X_1, \ldots, X_n$ be n commutative variables and let M be the subspace of the Laurent polynomial algebra $\mathbf{C}[X_1, \ldots, X_n, X_1^{-1}, \ldots, X_n^{-1}]$ consisting of those Laurent polynomials with no constant term. Then M is a Mathieu-Zhao space of $\mathbf{C}[X_1, \ldots, X_n, X_1^{-1}, \ldots, X_n^{-1}]$.

1-dimensional case:

Theorem 4 (DvdK 1-dimensional)

Let $\mathbf{C}[X, X^{-1}]$ be the Laurent polynomial algebra in one variable. Then

$$\{f \in \mathbf{C}[X, X^{-1}] \mid f_0 = 0\}$$

is a Mathieu-Zhao space of $\mathbf{C}[X, X^{-1}]$.

Duistermaat and Van der Kallen's theorem

The set $\{f \in \mathbf{C}[X, X^{-1}] \mid f_0 = 0\}$ is of course the kernel of the linear map $L\colon \mathbf{C}[X, X^{-1}] \to \mathbf{C}$ defined by $L(f) = f_0$.

Properties:

- $L(1) \neq 0$;
- $L(X^n) = 0$ for all $n \geq 1$ and all $n \leq -1$.

Generalization

Theorem 5 (DvdK1 - generalization)

Let $L\colon \mathbf{C}[X, X^{-1}] \to \mathbf{C}$ be a non-zero $\mathbf{C}$-linear map for which there exists an $N \geq 1$ such that $L(X^n) = 0$ for all $n \in \mathbf{Z}_{\geq N}$ and all $n \in \mathbf{Z}_{\leq -N}$. Then $\operatorname{Ker} L$ is a Mathieu-Zhao space of $\mathbf{C}[X, X^{-1}]$ if and only if $L(1) \neq 0$.

General Results

MZ-spaces containing 1

From now on we shall say "MZ-space" instead of Mathieu-Zhao space.

Lemma 6

Let R be a ring and A an R-algebra. Let M be an MZ-space of A such that $1 \in M$. Then $M = A$.

Proof.

Since $1^m = 1$ for all $m \geq 1$, we find that for all $b \in A$ we have $b1^m \in M$ for all $m \gg 0$ since M is an MZ-space. Hence $b \in M$, and $M = A$. $\square$

A closer look

We take a closer look at the argument given just now. What is the special property of 1 that we use here?

Since $1^m = 1$ for all $m \geq 1$, we find that for all $b \in A$ we have $b1^m \in M$ for all $m \gg 0$ since M is an MZ-space. Hence $b \in M$, and $M = A$.

That $1^2 = 1$ is that special property! Let $e \in A$ be an element that satisfies $e^2 = e$. We call such an element an *idempotent*.

A closer look

We take a closer look at the argument given just now. What is the special property of 1 that we use here?

Since $e^m = e$ for all $m \geq 1$, we find that for all $b \in A$ we have $be^m \in M$ for all $m \gg 0$ since M is an MZ-space. Hence $be \in M$, and $M = A$.

That $1^2 = 1$ is that special property! Let $e \in A$ be an element that satisfies $e^2 = e$. We call such an element an *idempotent*.

A closer look

We take a closer look at the argument given just now. What is the special property of 1 that we use here?

Since $e^m = e$ for all $m \geq 1$, we find that for all $b \in A$ we have $be^m \in M$ for all $m \gg 0$ since M is an MZ-space. Hence $be \in M$, and $M \supset Ae$.

That $1^2 = 1$ is that special property! Let $e \in A$ be an element that satisfies $e^2 = e$. We call such an element an *idempotent*.

MZ-spaces containing an idempotent e

Now we have:

Lemma 7

Let R be a ring and A an R-algebra. Let M be an MZ-space of A such that $e \in M$, where e is an idempotent. Then $Ae \subset M$.

Proof.

Since $e^m = e$ for all $m \geq 1$, we find that for all $b \in A$ we have $be^m \in M$ for all $m \gg 0$ since M is an MZ-space. Hence $be \in M$, and $Ae \subset M$. △

Operations on MZ-spaces

The intersection of two MZ-spaces is again an MZ-space:

Lemma 8 (Intersection)

Let M_1, M_2 be MZ-spaces of an R-algebra A. Then $M_1 \cap M_2$ is an MZ-space of A.

Products of MZ-spaces are MZ-spaces:

Lemma 9 (Product)

Let A and B be R-algebras and $M \subset A$ and $N \subset B$ be MZ-spaces of A, B respectively. Then $M \times N$ is an MZ-spaces of $A \times B$.

MZ-space of $A \times B$ that is not of the form $M \times N$

It is not true that all MZ-spaces of $A \times B$ are of the form $M \times N$:

Example 10

Consider the ring $R := \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. Then $M := \{(0,0),(1,2)\}$ is a $\mathbf{Z}$-linear subspace and an MZ-space of R. Clearly, it is not of the described form.

Since $2(1,2) = (0,0)$, we find that M is a $\mathbf{Z}$-linear subspace and since $(1,2)^2 = (1,0) \notin M$, we find that M satisfies the conditions for being an MZ-space.

There exists a partial converse to the product lemma for finite rings, which we will discuss later.

Finite rings

Finite rings are Artin rings

An *Artin ring* is a ring R such that every descending chain of ideals becomes stationary, i.e., if

$$I_1 \supset I_2 \supset \ldots$$

then there exists some $n \in \mathbf{N}$ such that $I_n = I_{n+1} = \ldots$

In particular, since a finite ring has only finitely many ideals, it is clear that finite rings are Artin rings.

Structure Theorem for Artin rings

Theorem 11 (Structure Theorem for Artin rings)

Let A be an Artin ring with maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. Then for some $k \in \mathbf{N}$ we have $A \cong \prod_{n=1}^{n} A/\mathfrak{m}_i^k$.

This is now also a structure theorem for finite rings. So every finite ring can be seen as a product of finitely many local rings.

$\mathbf{Z}/100\mathbf{Z}$

Lemma 12 ($\mathbf{Z}/n\mathbf{Z}$)

Let n be a positive integer and let R be the ring $\mathbf{Z}/n\mathbf{Z}$. Then all $\mathbf{Z}$-linear subspaces of $\mathbf{Z}/n\mathbf{Z}$ are actually ideals. Since ideals are MZ-spaces, we have now classified all the MZ-spaces of $\mathbf{Z}/n\mathbf{Z}$.

So the MZ-spaces of $\mathbf{Z}/100\mathbf{Z}$ are:

$$0, 50\mathbf{Z}/100\mathbf{Z}, 25\mathbf{Z}/100\mathbf{Z}, 20\mathbf{Z}/100\mathbf{Z}, 10\mathbf{Z}/100\mathbf{Z},$$

$$5\mathbf{Z}/100\mathbf{Z}, 4\mathbf{Z}/100\mathbf{Z}, 2\mathbf{Z}/100\mathbf{Z}, \mathbf{Z}/100\mathbf{Z}.$$

Finite Fields

Lemma 13 (Finite Fields)

Let p be a prime, $n \geq 1$ an integer and $q = p^n$. Then all $\mathbf{Z}$-linear subspaces of $\mathbb{F}_q$ that do not contain 1 are MZ-spaces of $\mathbb{F}_q$, and of course $\mathbb{F}_q$ itself is also an MZ-space.

Proof.

Let M be a $\mathbf{Z}$-linear subspace of $\mathbb{F}_q$ that does not contain 1. Let $x \in M$ be such that $x^n \in M$ for all $n \geq 1$. If $x \neq 0$, then this implies $1 \in M$, a contradiction. So only $x = 0$ satisfies the hypothesis $x^n \in M$ and clearly for all $y \in \mathbb{F}_q$ we then have $y \cdot 0^m = 0 \in M$ for all $m \gg 0$. △

The finite field $\mathbb{F}_4$ has MZ-spaces $0, \{0, x\}, \{0, x+1\}, \mathbb{F}_4$.

Main theorems of classification

Classification Theorem #1.

We introduce here the definition
$r(M) = \{a \in A \mid a^n \in M \ \forall n \geq 1\}$. (*We call this the radical of* M)

Lemma 14 (Radical of nilpotents)

Let R *be a ring and* M *a* $\mathbf{Z}$*-linear subspace of* R *with* $r(M) \subset \mathfrak{n}(R)$*, where* $\mathfrak{n}(R)$ *is the set of nilpotent elements of* R*, then* M *is an MZ-space of* R*.*

Theorem 15 (First Classification Theorem)

Let R *be a finite ring. Let* M *be a* $\mathbf{Z}$*-linear subspace of* R*. Write* $E(R)$ *for the set of idempotents of* R*. If* $M \cap E(R) = 0$*, then* $r(M) = \mathfrak{n}(R)$ *and* M *is an MZ-space.*

Partial converse to the product lemma, or: Classification Theorem #2

Theorem 16 (Second Classification Theorem')

Let R be a finite ring of the form $R \cong R_1/\mathfrak{m}_1^{k_1} \times R_2/\mathfrak{m}_2^{k_2}$. Then every MZ-space that is not of the form $r(M) \subset \mathfrak{n}(R)$ is of the form $M_1 \times M_2$ where each $M_i \subset R_i/\mathfrak{m}_i^{k_i}$ is an MZ-space of $R_i/\mathfrak{m}_i^{k_i}$.

Example 17

Let $R := \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. The product MZ-spaces are:

$$0 = 0 \times 0, 0 \times 2\mathbf{Z}/4\mathbf{Z}, 0 \times \mathbf{Z}/4\mathbf{Z},$$

$$\mathbf{Z}/2\mathbf{Z} \times 0, \mathbf{Z}/2\mathbf{Z} \times 2\mathbf{Z}/4\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} = R.$$

By the above theorem, the remaining subspaces have the property that $r(M) \subset \mathfrak{n}(R)$.

Example, continued

Example 17

Still, let $R := \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. We have previously met the MZ-space $\{(0,0),(1,2)\}$. How do we proceed to find other MZ-spaces M with $r(M) \subset \mathfrak{n}(R)$?

If $M \cap E(R) \neq 0$, then we can determine a non-zero idempotent $e \in M$. Hence $e^n = e \in M$ for all $n \in \mathbf{N}$, and $e \in r(M)$. This contradicts $r(M) \subset \mathfrak{n}(R)$. Thus we must have $M \cap E(R) = 0$.

Furthermore, if there exists some $x \in M$ such that $nx = e$ for some $n \in \mathbf{N}$ and non-zero $e \in E(R)$, then since M is $\mathbf{Z}$-linear we have $e \in M$. This contradicts $M \cap E(R) = 0$.

Example, continued

Example 17

The elements of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ that are not idempotent or nilpotent are:

$$(0,3), (1,2), (1,3).$$

Note that $3 \cdot (0,3) = (0,1)$ and $3 \cdot (1,3) = (1,1)$.
So we have elements $(0,0), (0,2)$ and $(1,2)$ that may be elements of the remaining M. If $(0,2)$ and $(1,2)$ are both elements of M, then their sum, $(1,0)$ is also an element of M. But this was ruled out before. Hence we have the following possibilities:

$$\{(0,0)\}$$

$$\{(0,0),(0,2)\}$$

$$\{(0,0),(1,2)\}$$

Example of product of three rings

Example 18

Let $R := \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. Then the $\mathbf{Z}$-linear subspace M defined by

$$M := \{(0,0),(1,2)\} \times \mathbf{Z}/4\mathbf{Z}$$

is an MZ-space of R that is both:

- not of the form $r(M) \subset \mathfrak{n}(R)$. For we have $(0,0,1) \in M$.
- not of the form $M_1 \times M_2 \times M_3$.

So for products of three rings (and hence arbitrary $n > 2$) there is still some more work. This is done in my thesis.

Questions

Thank you all for your attention, and if there are any lingering questions, please do not hesitate to ask them.