QF Group Theory CC2022
By
Zaiku Group

Lecture 02

Delivered by Bambordé Baldé

Friday, 11/03/2022

Session Agenda

1. Learning Journey Timeline
2. Course Approach Overview
3. Upcoming Events

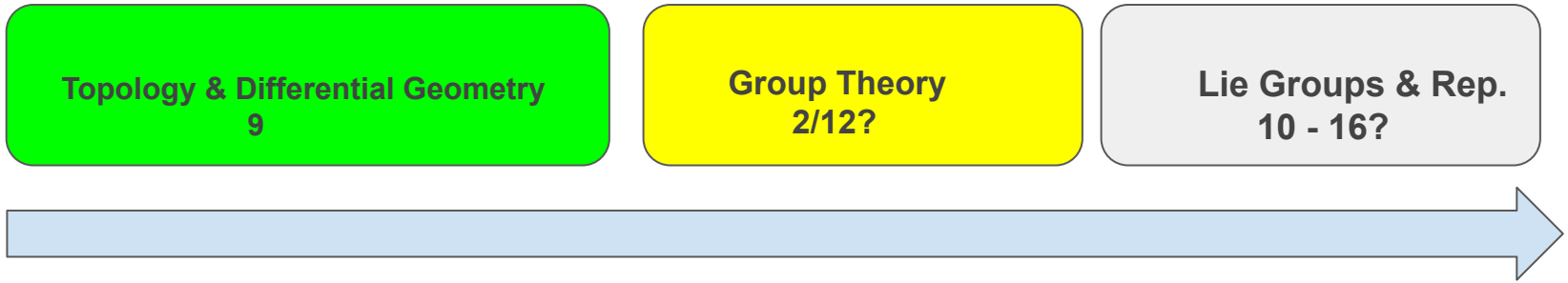
Pre-session Comments

+

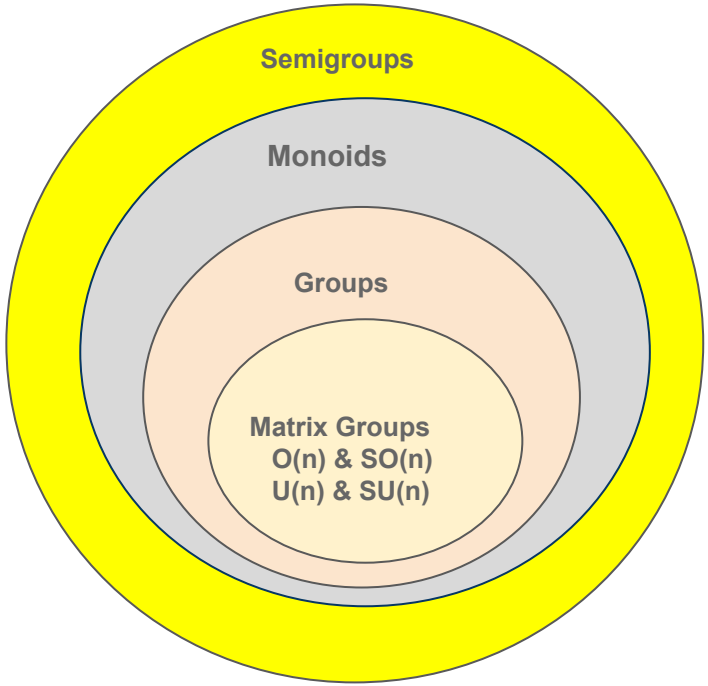
1. Idempotent Elements
2. Idempotent Examples
3. Semigroup Homomorphisms
4. Semigroup Isomorphisms

Main Session

Learning Journey Timeline



Completed | Ongoing | TBC (summer) | n is the number of live lectures |

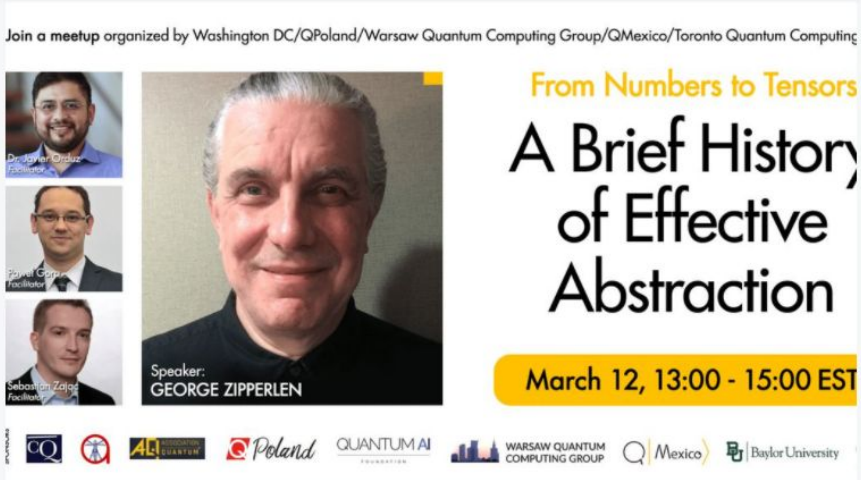


Course Approach Overview

We're here!

Saturday, March 12, 2022

From Numbers to Tensors - A Brief History of Effective Abstraction



Details

Abstract:
We are so used to arithmetic, that it doesn't seem abstract. But there is a long history of extending ordinary whole numbers with fractions, negative numbers, irrational numbers, imaginary numbers... As the number systems flourished, mathematical abstractions like vectors, matrices, sets, groups, and rings grew further away from direct experience. But some of these abstractions became the foundation of Quantum Mechanics.

MAR
23
05:00pm

More than Just a Pretty Space: How Symmetry Hides in Science

By Zaiku Group · Unlisted

16 DAYS 7 HRS 0 MIN 19 SEC

Save my spot!

Your name and email will be shared with the host.

Already joined? **Sign back in**

HOSTED BY

Zaiku Group Follow

Abstract

Group theory (or the study of symmetry) is one of the biggest active research areas of pure mathematics and one of the mainstays of mathematics in general. In this 30 minute presentation, I describe the history of this beautiful area of mathematics and describe key applications to Physics, Virology and Chemistry, with plenty of time for discussion afterwards!

Semigroup definition recap

A semigroup is a pair $(S, *)$ where S is a nonempty set and $*$ is a binary operation on S such that $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$.

- Now that we have the basic algebraic structure of semigroup, our goal is to start exploring:

1. Interesting properties that the algebraic structure give us e.g. identify some interesting behaviours that certain elements have.
2. Explore structure preserving maps between semigroups (homomorphisms).

Semigroup Idempotent Elements

Definition 1.0

Given a semigroup $(S, *)$ and $a \in S$, we define $a^2 = a * a$.

- Can you generalise the above to the power of an arbitrary $n \in \mathbb{N}$?

Definition 1.1

Let $(S, *)$ be a semigroup. An element $a \in S$ is idempotent if $a^2 = a$.

- We denote by $Idem(S)$ the set of all idempotent elements in S i.e $Idem(S) = \{a \in S \mid a^2 = a\}$. Obviously, we may have $Idem(S) = \emptyset$.
- Interestingly, we may also have $Idem(S) = S$ (aka a band).

Homework Challenge 1

Let $(S, *)$ be a semigroup. You're encouraged to try answer the following:

1. Is it true that $Idem(S)$ is a subsemigroup of $(S, *)$?
2. Is it true that if $a \in Idem(S)$ then $a^n = a$ for all $n \in \mathbb{N}$?

Idempotent Elements (Boring Examples)

- Let $(S, *) = (\mathbb{Z}, \times)$ where $\times$ is the ordinary multiplication in $\mathbb{Z}$. Then 1 and 0 are the only idempotent elements i.e. $Idem(\mathbb{Z}) = \{0, 1\}$?
- Now if $(S, *) = (\mathbb{Z}, +)$ where $+$ is the ordinary addition in $\mathbb{Z}$ then $Idem(\mathbb{Z}) = \{0\}$?
- Let now $(S, *) = (\mathbb{R}, \times)$ where $\times$ is the ordinary multiplication in $\mathbb{R}$. Then $Idem(\mathbb{R}) = \{0, 1\}$?
- If $(S, *) = (\mathbb{R}, +)$. Then again $Idem(\mathbb{R}) = \{0\}$?
- Similarly, if now $(S, *) = (\mathbb{C}, \times)$ where $\times$ is the ordinary multiplication in $\mathbb{C}$. Then $Idem(\mathbb{C}) = \{0, 1\}$. Obviously if $(S, *) = (\mathbb{C}, +)$, then $Idem(\mathbb{C}) = \{0\}$.

Question: Are there examples of semigroup structure where $Idem(S)$ is not trivial/boring like the examples above?

Idempotent Elements (Matrix Examples)

- Consider the set $M_2(\mathbb{R})$ of two by two matrices over the reals, then:

1. Trivially, $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ are idempotent in respect to matrix multiplication!
2. Nontrivial examples are $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$.

Side note: The eigenvalues of idempotent matrices are either 0 or 1.

Idempotent Elements (mod 3 Example)

- Consider $\mathbb{Z}_3 = \{0, 1, 2\}$ with the binary operation $+$ defined by the following table:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Clearly $Idem(\mathbb{Z}_3) = \{0\}$ right?

Idempotent Elements (mod 3 Example)

- Consider $\mathbb{Z}_3 = \{0, 1, 2\}$ with the binary operation $\times$ defined by the following table:

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Clearly $Idem(\mathbb{Z}_3) = \{0, 1\}$ right?

Idempotent Elements (mod 4 Example)

- Consider now $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with the binary operation $+$ defined by the following table:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Clearly $Idem(\mathbb{Z}_4) = \{0\}$ right?

Idempotent Elements (mod 4 Example)

- Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with the binary operation $\times$ defined by the following table:

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$Idem(\mathbb{Z}_4) = \{0, 1\}$ right?

- Unfortunately, $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ is boring too because:

$Idem(\mathbb{Z}_5) = \{0\}$ with the respect to $+$ and $Idem(\mathbb{Z}_5) = \{0, 1\}$ with the respect $\times$!

Idempotent Elements (mod 6 Example)

- Consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ in respect to mod 6 multiplication table defined below:

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- Clearly we now have a non-boring example because $Idem(\mathbb{Z}_6) = \{0, 1, 3, 4\}$?!!
- Interestingly, $Idem(\mathbb{Z}_7)$, $Idem(\mathbb{Z}_8)$ and $Idem(\mathbb{Z}_9)$ are also trivial/boring!

Question: What makes mod 6 case above special? Are there other mod n examples for $n > 6$?

Hint: It has to do with prime numbers! Can you guess why prime numbers play a role in this?

Idempotent Elements (mod $n > 6$ Examples)

- For $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ under mod 10 multiplication we have $Idem(\mathbb{Z}_{10}) = \{0, 1, 5, 6\}$?
- For $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ under mod 12 multiplication we have $Idem(\mathbb{Z}_{12}) = \{0, 1, 4, 6, 9\}$?
- For $\mathbb{Z}_{14} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$ under mod 14 multiplication we have $Idem(\mathbb{Z}_{14}) = \{0, 1, 7, 8\}$?
- For $\mathbb{Z}_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$ under mod 15 multiplication we have $Idem(\mathbb{Z}_{15}) = \{0, 1, 6, 10\}$?

Question: What do the above examples and $\mathbb{Z}_6$ have in common regarding prime numbers?

Extra hint: They break an interesting property of prime numbers!!

By the way, $\mathbb{Z}_{18}$, $\mathbb{Z}_{20}$, $\mathbb{Z}_{21}$, $\mathbb{Z}_{22}$, $\mathbb{Z}_{24}$, $\mathbb{Z}_{26}$, and $\mathbb{Z}_{28}$ are also part of the gang!

Semigroup Homomorphisms

Definition 1.2

Let $(S_1, *_1)$ and $(S_2, *_2)$ be semigroups. A map $f : S_1 \longrightarrow S_2$ is a homomorphism if $f(a *_1 b) = f(a) *_2 f(b)$ for all $a, b \in S_1$.

- Let $(S_1, *_1) = (\mathbb{R}, +)$ and $(S_2, *_2) = (\mathbb{R}^+, \times)$. Now consider the map $f : \mathbb{R} \longrightarrow \mathbb{R}^+$ defined as $f(x) = e^x$ for all $x \in \mathbb{R}$. Is this map a homomorphism?

- Let $M_2(\mathbb{R})$ the semigroup of 2 by 2 real matrices under ordinary matrix multiplication.

Recall that given any matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R})$, the determinant $det(A) : M_2(\mathbb{R}) \longrightarrow \mathbb{R}$ is defined as $det(A) = ad - bc$.

Question: Is this a homomorphism to the semigroup $(\mathbb{R}, +)$ or the semigroup $(\mathbb{R}, \times)$?

Side notes:

- Classical Homomorphic Encryption (HE), homomorphism is the underpinning mathematical notion of HE.
- The early HE schemes such as the ones proposed by Rivest and ElGammal were built on groups and so use group homomorphisms.
- Modern Fully Homomorphic Encryption (FHE) schemes are built on rings and fields.
- Can we run quantum computations homomorphically? This question naturally leads to Quantum Homomorphic Encryption (QHF)!

Homework Challenge 2

Let $(S_1, *_1)$ and $(S_2, *_2)$ be semigroups. Now suppose that $f : S_1 \longrightarrow S_2$ is a semigroup homomorphism.

1. Is it true that if $a \in Idem(S_1)$ then $f(a) \in Idem(S_2)$?
2. Is it true that $Im(f) = \{f(a) \mid a \in S_1\}$ is a subsemigroup of $(S_2, *_2)$?

Homework Challenge 3

Let $(S_1, *_1)$, $(S_2, *_2)$ and $(S_3, *_3)$ be semigroups. Now suppose that the maps $f : S_1 \longrightarrow S_2$ and $g : S_2 \longrightarrow S_3$ are homomorphisms.

1. Is the composition map $g \circ f : S_1 \longrightarrow S_3$ a homomorphism?
2. Suppose that f is invertible. Is $f^{-1} : S_2 \longrightarrow S_1$ also a homomorphism?

Homework Challenge 4

Consider the sets $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_6$,$\mathbb{Z}_{10}$, $\mathbb{Z}_{11}$,$\mathbb{Z}_{12}$, $\mathbb{Z}_{14}$ and $\mathbb{Z}_{15}$. Try construct homomorphisms between these sets under both mod n addition and mod n multiplication.

Semigroup Isomomorphisms

Definition 1.3

Let $(S_1, *_1)$ and $(S_2, *_2)$ be semigroups. A homomorphism $f : S_1 \longrightarrow S_2$ is called an isomorphisms if it's bijective.

- We write $S_1 \simeq S_2$ and say the two semigroups are isomomorphic if there exists an isomorphism between the two.
- Isomorphisms are the structure preserving maps of semigroups i.e. two isomorphic semigroups are from an algebraic point of view indistinguishable.

Homework Challenge 5

Let $(S_1, *_1)$, $(S_2, *_2)$ and $(S_3, *_3)$ be semigroups. Now suppose that the maps $f : S_1 \longrightarrow S_2$ and $g : S_2 \longrightarrow S_3$ are isomorphisms.

- Is the composition map $g \circ f : S_1 \longrightarrow S_3$ an isomomorphism i.e. does $S_1 \simeq S_2$ and $S_2 \simeq S_3$ imply $S_1 \simeq S_3$?

QUANTUM FORMALISM

GitHub: github.com/quantumformalism

YouTube: youtube.com/ZaikuGroup

Discord: discord.gg/SPcmcsXMD2

Twitter: twitter.com/ZaikuGroup

LinkedIn: linkedin.com/company/zaikugroup