QF Group Theory CC2022
By
Zaiku Group

Lecture 05

Delivered by Bambordé Baldé

Friday, 22/04/2022

quantumformalism.com

Session Agenda

1. Learning Journey Timeline
2. Course Approach Overview
3. Mini Schools Series Idea

Pre-session Comments

+

1. Monoid Inverse Elements
2. The Genesis of Abstract GT
3. Group Structure
4. Group Element Exponentiation

Main Session

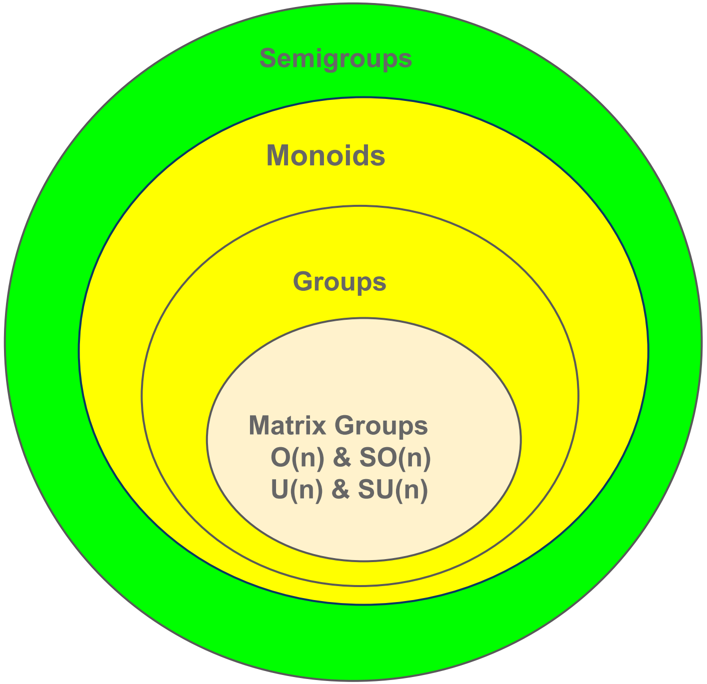
Learning Journey Timeline

Topology & Differential Geometry
9

Group Theory
5/14?

Lie Groups & Rep.
10 - 16?

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

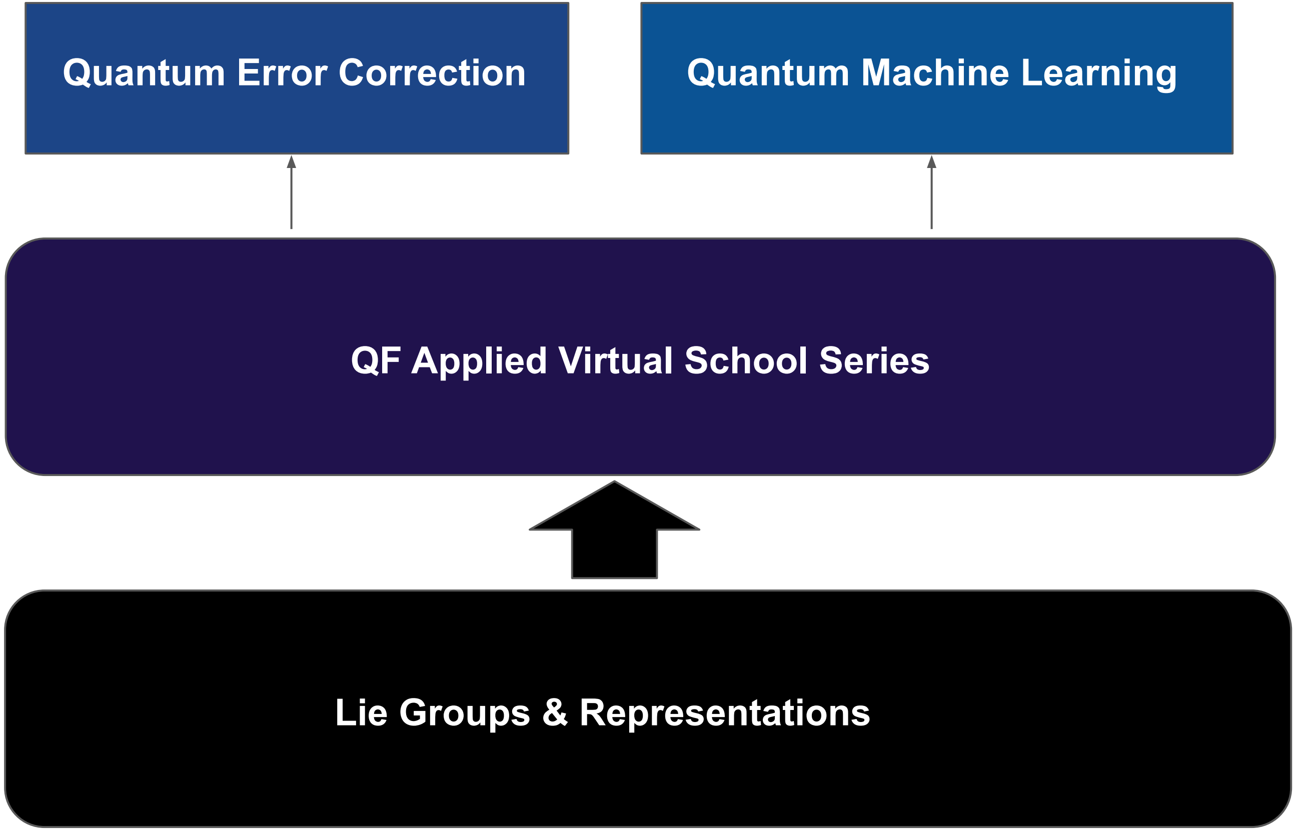


Course Approach Overview

Completed!

We’re here!

Applied QF Initiatives




Join a meetup organized by Washington DC/Warsaw/Toronto Quantum Computing Meetups
Exposing Abstract Mathematical Structures to Aspiring Quantum Pros
May 21, 13:00 - 15:00 EDT
Speaker:
BAMBORDE BALDE
CO-FOUNDER
of Zaiku Group
Moderator:
PAWEŁ GORA
CEO
Quantum AI Foundation
SPONSORS
QUANTUM AI
WARSAW QUANTUM COMPUTING GROUP
ASSOCIATION QUANTUM

Monoid Inverse Elements

Definition 1.0

Let $(M, *, \boldsymbol{e})$ be a monoid and $x \in M$. An element $x^{-1} \in M$ is called:

1. A left inverse of x if $x^{-1} * x = \boldsymbol{e}$.
2. A right inverse if $x * x^{-1} = \boldsymbol{e}$.
3. A two-sided inverse (or group inverse) if $x^{-1} * x = x * x^{-1} = \boldsymbol{e}$.

- Obviously, x^{-1} doesn't necessarily exist for all $x \in M$.

Simple Concrete Examples:

1. Consider the monoid $(\mathbb{R}, \times, 1)$. Then any nonzero element $a \in \mathbb{R}$ has a group inverse $a^{-1} = \frac{1}{a}$ right?
2. Consider now the monoid $(\mathbb{R}, +, 0)$. Then any element $a \in \mathbb{R}$ has a group inverse $a^{-1} = -a$ right?

quantumformalism.com

The Genesis of Group Theory (A)

Fundamental Theorem of Algebra (FTA)

$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0$ with $a_i \in \mathbb{C}$ and $a_n \neq 0$ has at least one root in $\mathbb{C}$.

- Equivalently every polynomial of degree n with real or complex coefficients has exactly n complex roots, counting multiplicity.
- Interestingly, most versions of the FTA proof including the original rely on methods from other branches of mathematics such as Analysis! This led to a healthy debate over the years whether it should be called 'Fundamental Theorem of Algebra'! There are now of course other more algebraic methods that prove FTA, for example Galois theory.
- When we can find the solutions for $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0$ with rational coefficients using only rational numbers and the operations of addition, subtraction, division, multiplication and nth roots, we say that p(x) is solvable by radicals.

The Genesis of Group Theory (B)

- Consider the second degree polynomial $p(x) = a_2x^2 + a_1x + a_0$ with $a_i \in \mathbb{C}$. Then the polynomial equation $p(x) = 0$ can be solved by radicals as we all learned in basic school via the quadratic formula!
- The third degree polynomial equation $p(x) = a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ and the fourth degree polynomial equation $p(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ can also be solved by radicals.

Big Question 1:

Can $p(x) = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ also be solved by radicals? Or even better, can a general polynomial equation $p(x) = a_nx^n + a_{n-}x^{n-1} + \ldots + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ be solved by radicals for any $n \geq 5$?

- Note that the question is whether $p(x) = 0$ can be solved by radicals, not whether $p(x) = 0$ can be solved by other means.

The Genesis of Group Theory (C)

The answer to 'Big Question 1'

The famous Abel–Ruffini theorem (aka Abel's impossibility theorem) shows that not all polynomial of degrees ≥ 5 can be solved by radicals!

- An example of a polynomial equation that cannot be solved by radicals is $x^5 - x - 1 = 0$.
- An example of a polynomial that can be solved by radicals is $x^5 + 15x + 12 = 0$.

Big Question 2

Is there a way to decide whether a polynomial equation $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0$ is solvable by radicals for any $n \geq 5$?

quantumformalism.com

The Genesis of Group Theory (D)

The answer to 'Big Question 2'

Évariste Galois hacked a positive answer in his seminal work that gave birth to a subbranch of abstract algebra now known as 'Galois Theory'!

- In a nutshell, given a polynomial of degree $n \geq 5$, $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$. To find out if the polynomial equation $p(x) = 0$ is solvable by radicals, we do the following:

1. We compute a special group $Gal(p(x))$ for the polynomial aka Galois group of $p(x)$.
2. We check if the Galois group $Gal(p(x))$ is 'solvable' in the group theoretic sense. If $Gal(p(x))$ is solvable then $p(x) = 0$ is solvable by radicals! Otherwise it's not solvable by radicals!

quantumformalism.com

Galois Theory Impact

- Galois theory is nowadays used in many applied topics like Cryptography e.g. Advanced Encryption Standard (AES).
- Sophus Lie took inspiration from Galois Theory and pursued creating a similar theory for differential equations! This led to the creation of what we now know as 'Differential Galois Theory'!
- Differential Galois Theory led to the creation of Lie Groups. In a nutshell, Lie groups are for differential equations what Galois groups are for polynomial equations!

quantumformalism.com

Galois Theory Impact

- Galois theory is nowadays used in many applied topics like Cryptography e.g. Advanced Encryption Standard (AES).
- Sophus Lie took inspiration from Galois Theory and pursued creating a similar theory for differential equations! This led to the creation of what we now know as 'Differential Galois Theory'!
- Differential Galois Theory led to the creation of Lie Groups. In a nutshell, Lie groups are for differential equations what Galois groups are for polynomial equations!

quantumformalism.com

The Group Structure

Definition 1.1

A group is a triple $(G, *, \boldsymbol{e})$ satisfying the following:

1. $(G, *, \boldsymbol{e})$ is a monoid.
2. For every $g \in G$ there exists a group inverse $g^{-1} \in G$ i.e. $g * g^{-1} = g^{-1} * g = \boldsymbol{e}$.

- From now on, we'll just write G to denote an abstract group instead of $(G, *, \boldsymbol{e})$. We'll also abbreviate $g_1 * g_2$ as $g_1 g_2$.
- Given a group G, it's cardinality (number of elements) is called the order of G and it's usually denoted $|G|$.
- When $|G| = p$ for some prime number p, then G is called a $p-$ group.
- A group G is commutative (or abelian) if $g_1 g_2 = g_2 g_1$ for all $g_1, g_2 \in G$. Otherwise, it's called noncommutative (or nonabelian).

quantumformalism.com

Group Examples

Example 1

Let A be a non-empty set and let $G = \{f : A \longrightarrow A \mid f \text{ is a bijection }\}$.
Now suppose that $*$ is the composition $\circ$ of maps in G.

- Is G a group under $\circ$? If yes, is it abelian or non-abelian?

Example 2

Let G be the set $M_n(\mathbb{C})$ of $n \times n$ matrices with complex entries and let the operation $*$ be the ordinary matrix multiplication.

- Is $M_n(\mathbb{C})$ a group under matrix multiplication? Is it abelian or non-abelian? What about under matrix addition?

Example 3

Let G be the set $GL(n, \mathbb{C})$ of invertible $n \times n$ matrices with complex entries and let the operation $*$ be still the ordinary matrix multiplication.

- Is $GL(n, \mathbb{C})$ a group under matrix multiplication?

Group Element Exponentiation

Definition 1.2

Let G be a group and $g \in G$. Then for $k \in \mathbb{Z}$, we define the following:

1. $g^0 = \boldsymbol{e}$.
2. $g^k = gg \dots gg$ for $k > 0$.
3. $g^{-k} = g^{-1}g^{-1} \dots g^{-1}g^{-1}$ for $k < 0$. $k-$ times

- The notion of exponentiation above will lead us to the important notion of a 'cyclic group' that we'll define in the next lecture!
- Cyclic groups are very important in applied topics such as Cryptography e.g. the Diffie-Hellman Key Exchange Protocol.

Challenge 2

Let G be a group and $g \in G$. Then for $k_1, k_2 \in \mathbb{Z}$, prove the following :

1. $g^{k_1}g^{k_2} = g^{k_1+k_2}$ for all $g \in G$.
2. $(g^{k_1})^{k_2} = g^{k_1k_2}$ for all $g \in G$.

quantumformalism.com

QUANTUM FORMALISM

GitHub: github.com/quantumformalism

YouTube: youtube.com/ZaikuGroup

Discord: discord.gg/SPcmcsXMD2

Twitter: twitter.com/ZaikuGroup

LinkedIn: linkedin.com/company/zaikugroup