QF Group Theory CC2022 By Zaiku Group

Lecture 06

Delivered by Bambordé Baldé

Friday, 06/05/2022

Session Agenda

1. Learning Journey Timeline
2. Course Approach Overview

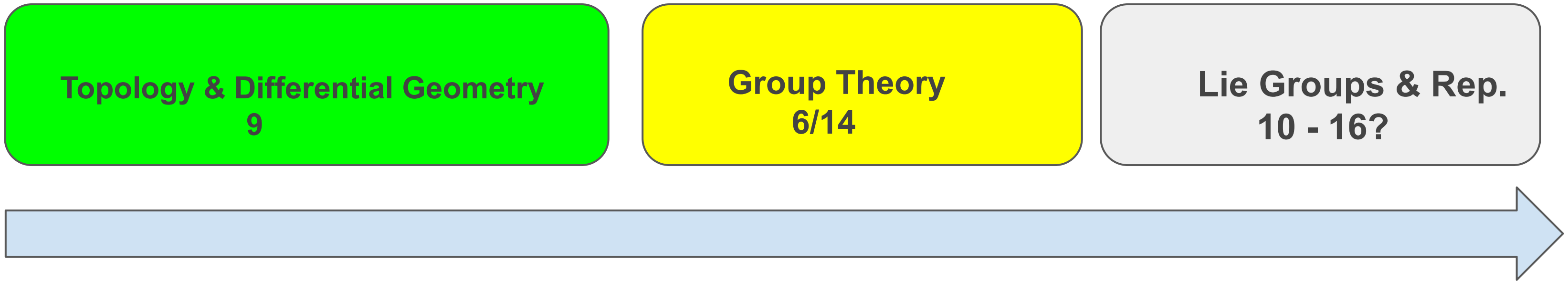
Pre-session Comments

+

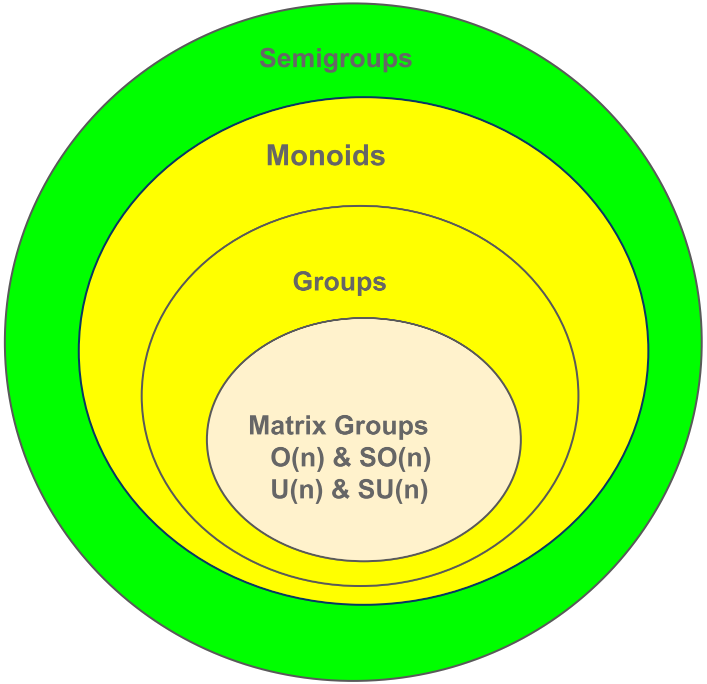
1. Group element exponentiation
2. The order of a group element
3. The subgroup structure
4. The cyclic subgroup structure
5. The cyclic group structure

Main Session

Learning Journey Timeline



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



Course Approach Overview

Completed!

We're here!

quantumformalism.com

Group Exponentiation Recap

Definition 1.0

Let G be a group, $g \in G$ and $k \in \mathbb{Z}$. We can now make the following definitions:

1. For $k = 0$, we define $g^0 = \boldsymbol{e}$.
2. For $k > 0$, we define $g^k = gg \dots gg$
3. For $k < 0$, we define $g^{-k} = (g^{-1})^k = g^{-1}g^{-1} \dots g^{-1}g^{-1}$

Exponentiation Properties

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

Challenge 1

Let G be a group and $g_1, g_2 \in G$. Is it true that if $g_1 g_2 = g_2 g_1$ then $(g_1 g_2)^k = g_1^k g_2^k$ for all $k \in \mathbb{Z}$?

Additive Notation Comment

Convention

Let G be a an additive group such as $(\mathbb{Z}, +)$ with an identity called zero 0. Then for each $g \in G$ and $k \in \mathbb{Z}$, the exponentiation as g^k as defined previously coincides with notion of 'multiple' written kg:

1. For $k = 0$, $g^k = 0$ coincides with $0g = 0$.
2. For $k > 0$, $g^k = g + g + g + \ldots + g + g$ coincides with kg
3. For $k < 0$, we define $g^{-k} = (-g) + (-g) + \ldots (-g)$ which coincides with $k(-g)$.

- Hence, for additive groups like $(\mathbb{Z}, +)$, we'll write kg instead of g^k!

The Order of an Element in a Group

Definition 1.1

Let G be a group and $g \in G$. Then order of g in G is the smallest positive integer $n \in \mathbb{Z}^+$ such that $g^n = \mathbf{e}$. We write $|g| = n$ to denote that n is the order of g.

- If there is no such $n \in \mathbb{Z}^+$, by convention we say g has infinite order and we write $|g| = \infty$.
- The group identity $\boldsymbol{e}$ has order 1 right? Is it the only element of order 1 in G?
- Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with the binary operation $+$ defined by the following table (mod 4 addition):

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

Question: What is the order of the elements 1 i.e. what is the smallest $n \in \mathbb{Z}^+$ such that $n1 = 0$? What about the order of 3?

Challenge 2

Is the order $|g| = n \in \mathbb{Z}^+$ of $g \in G$ unique i.e. if $n_1 = |g|$ and $n_2 = |g|$ then $n_1 = n_2$?

Side note on Idempotent Elements

Recall that in the semigroup section, we defined an element $g \in G$ to be idempotent if $g^2 = g$. Now, taking into the group structure in G, is it true that the only idempotent element in G is the identity $\boldsymbol{e}$?

For the Folks in Quantum Computing

Tricky Challenge 1

Let $G = U(2)$, where $U(2)$ is the unitary group of operators acting on the Hilbert space $\mathbb{C}^2$.

- Now consider the single qubit gates $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ and $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

1. What is the order (as per definition 1.1) of X, Y and Z gates as

elements of the group $U(2)$? What about the Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$?

2. Are all the unitary operators in $U(2)$ of the same order as the gates above? If not, can you find examples of unitary operators in $U(2)$ of the same order as the gates above?

The Subgroup Structure

Definition 1.2

Let G be a group and $H \subseteq G$. H is a subgroup of G if it forms a group structure under the same binary operation as G.

- Indeed, $H \subseteq G$ is a subgroup iff the following hold:

1. $\boldsymbol{e} \in H$.
2. $h_1 h_2 \in H$ for all $h_1, h_2 \in H$.
3. $h^{-1} \in H$ for all $h \in H$.

- Obviously, G and $\{\boldsymbol{e}\}$ are trivially subgroup!
- We'll write $H \leq G$ to denote the fact that H is a subgroup of G. In particular, when H is a proper subset i.e. $H \neq G$, then we write $H < G$.

Challenge 3

Let $H_1 \leq G$ and $H_2 \leq G$.Is it true that $H_1 \cap H_2 \leq G$? Is $H_1 \cup H_2 \leq G$ also necessarily true?

Special Subgroup Structures

Definition 1.3

Let G be group and $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$.

- It's relatively easy to prove that $Z(G) \leq G$! It's also easy to see that $Z(G) = G$ iff G is abelian right?
- In the literature, $Z(G)$ is called the 'centre' of G.

Definition 1.4

Let $H \leq G$ and $C(H) = \{g \in G \mid gh = hg \text{ for all } h \in H\}$.

- $C(H)$ is a subgroup called the 'centraliser' of H in G.

For the Folks in Quantum Computing

Tricky Challenge 2

Let $G = U(2)$, where $U(2)$ is the unitary group of operators acting on the Hilbert space $\mathbb{C}^2$ and let $H = SU(2)$ (the special unitary group) of $U(2)$.

1. Try identify at least 3 concrete elements of the centre $U(2)$ i.e. 3 elements of $Z(U(2))$.
2. Try identify at least 4 concrete elements of the centraliser of $SU(2)$ i.e. 4 elements of $C(SU(2))$.
3. Is any of the single qubit gates X, Y, Z and H in the centre of $U(2)$?
4. Is any of the single qubit gates X, Y, Z and H in the centraliser of $SU(2)$?

The Cyclic Subgroup Structure

Definition 1.5

Let G be a group and for $g \in G$, we define $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$.

- $\langle g \rangle$ is called the 'cyclic subgroup' generated by the element $g \in G$.
- Interestingly, $\langle g \rangle$ is the smallest subgroup of G containing g!
- Also, if $|g| = n$ then $\langle g \rangle = \{\mathbf{e}, g, g^2, \ldots g^{n-1}\}$.

Challenge 4

Is it true that $\langle g \rangle = \langle g^{-1} \rangle$ for all $g \in G$? Is it also true that $\langle g \rangle$ is always abelian regardless whether G is abelian or not?

Simple examples:

- Consider the group structure of the integers $\mathbb{Z}$ under ordinary addition. Then the cyclic subgroup generated by the integer 2 is $\langle 2 \rangle = \{2k \mid k \in \mathbb{Z}\} = 2\mathbb{Z}$.
- Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under mod 4 addition. Then the cyclic subgroup generated by 1 is $\langle 1 \rangle = \{1, 2, 3, 0\}$? What about $\langle 3 \rangle$?

For the Folks in Quantum Computing

Tricky Challenge 3

Let $G = U(2)$, where $U(2)$ is the unitary group of operators acting on the Hilbert space $\mathbb{C}^2$. For each of the single qubit gates X, Y, Z and H, identify the following subgroups:

1. $\langle X \rangle$
2. $\langle Y \rangle$
3. $\langle Z \rangle$
4. $\langle H \rangle$

The Cyclic Group Structure

Definition 1.6

A group G is cyclic if there exists some $g \in G$ such that $G = \langle g \rangle$.

- We say g generates the group G or that g is a generator of G.

Simple concrete examples:

- $G = \mathbb{Z}$ be the additive group of the integers. This is a cyclic a group! Now, which of the following integers is a generator for $\mathbb{Z}$?
  1. 0 i.e. is $\langle 0 \rangle = \mathbb{Z}$?
  2. 1 i.e. is $\langle 1 \rangle = \mathbb{Z}$?
  3. 2 i.e. is $\langle 2 \rangle = \mathbb{Z}$?
  4. -1 i.e. is $\langle -1 \rangle = \mathbb{Z}$?
- Consider $G = 2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ under the addition of integers. This is a cyclic group of course! As we have seen, the integer 2 is its generator i.e. $2\mathbb{Z} = \langle 2 \rangle$.
- Interestingly, $2\mathbb{Z}$ is a subgroup of the cyclic group $\mathbb{Z}$. This motivates the following question: **Is every subgroup of a cyclic group cyclic?**

Challenge 5

Under the normal addition, can any of the following sets be a cyclic group?

1. The set of rationals $\mathbb{Q}$
2. The set of the reals $\mathbb{R}$
3. The set of complex numbers $\mathbb{C}$

QUANTUM FORMALISM

GitHub: github.com/quantumformalism

YouTube: youtube.com/ZaikuGroup

Discord: discord.gg/SPcmcsXMD2

Twitter: twitter.com/ZaikuGroup

LinkedIn: linkedin.com/company/zaikugroup