QF Group Theory CC2022
By
Zaiku Group

Lecture 10

Delivered by Bambordé Baldé

Friday, 08/7/2022

Session Agenda

1. Learning Journey Timeline
2. Course Approach Overview
3. NIST PQC Comment

Pre-session Comments

+

1. Symmetric Groups over Sets
2. Concrete Examples & Challenges

Main Session

Learning Journey Timeline

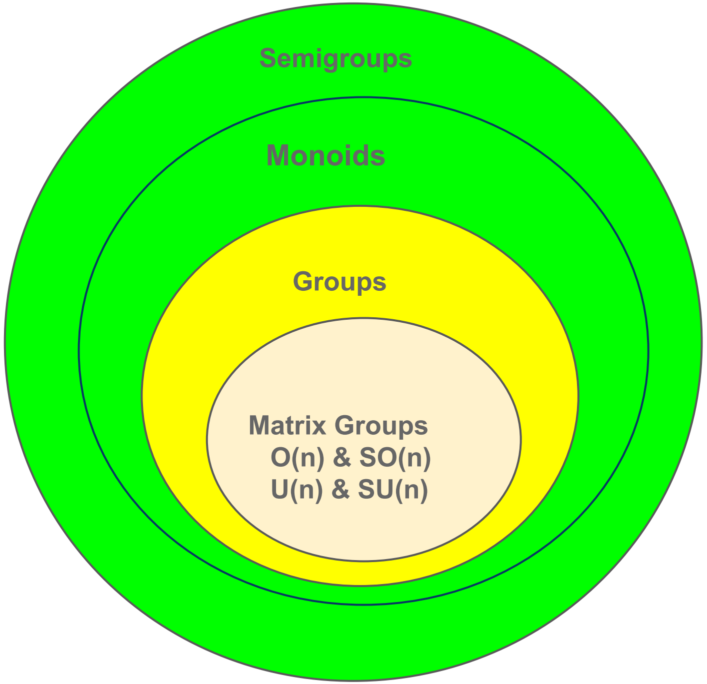
Topology & Differential Geometry
9

Group Theory
10/20?

Lie Groups & Rep.
10 - 16?

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

quantumformalism.com



Course Approach Overview

Completed!

We’re here!

Cryptosystem	RSA	Diffie-Hellman KE (DHKE)	Elliptic Curve Cryptography (ECC)
Underlying Mathematical Hardness Problem	Prime Factorization	Discrete Logarithm Problem	Elliptic Curve Discrete Logarithm Problem
Can it be solved by a quantum algorithm?	Yes	Yes	Yes

Current Public Key Cryptography

NIST IR 8413 Third Round Status Report

Table 4. Algorithms to be Standardized

Public-Key Encryption/KEMs	Digital Signatures
CRYSTALS–KYBER	CRYSTALS–Dilithium
	FALCON
	SPHINCS$^+$

Table 5. Candidates advancing to the Fourth Round

Public-Key Encryption/KEMs	Digital Signatures
BIKE	
Classic McEliece	
HQC	
SIKE	

NIST's PQC Standards Proposal

Symmetric Groups over Sets

Definition 1.0

Let X be a nonempty set. The set of all bijective maps on X is denoted $Sym(X)$ i.e. $Sym(X) = \{f : X \longrightarrow X \mid f \text{ is a bijection}\}$.

- Some authors use the notation Sym_X instead of $Sym(X)$.
- When X is finite with cardinality n then the notation S_n is used!
- It's easy to show that the composition of maps $\circ$ is a binary operation in $Sym(X)$ i.e. $f_2 \circ f_1 \in Sym(X)$ for all $f_1, f_2 \in Sym(X)$.

Proposition 1.0

$Sym(X)$ forms a group under the composition $\circ$ with the identity map $id_X : X \longrightarrow X$ as the group identity.

Proof : Homework challenge!

- In general, is $Sym(X)$ an abelian or nonabelian group?

Concrete Example (S_3)

Let $X = \{1, 2, 3\}$. Then $Sym(X) = S_3$ has $3! = 6$ elements including:

1. $id_X : X \longrightarrow X$ defined as $id_X(1) = 1$, $id_X(2) = 2$ and $id_X(3) = 3$. id_X can be represented using the 'two-line notation'

$$id_X = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix}$$

2. $\sigma_1 : X \longrightarrow X$ defined as $\sigma_1(1) = 2$, $\sigma_1(2) = 1$ and $\sigma_1(3) = 3$. In two-line notation σ_1 becomes represented as

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{pmatrix}$$

3. $\sigma_2 : X \longrightarrow X$ defined as $\sigma_2(1) = 1$, $\sigma_2(2) = 3$ and $\sigma_2(3) = 2$. In two-line notation σ_2 becomes represented as

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix}$$

S_3 Challenges

Challenge 1

Identify the remaining elements of S_3 using the two-line notation without using arrows. Also, complete the following challenges:

1. Compute $\sigma_2 \circ \sigma_1$.
2. Compute σ_1^2, σ_1^3, σ_2^2 and σ_2^3.
3. Find σ_1^{-1} and σ_2^{-1}.
4. Find at least a nontrivial subgroup of S_3. Even better, can you identify all the nontrivial subgroups of S_3?
5. Is any of the identified nontrivial subgroups of S_3 cyclic?

Challenge 2

Let $H_3 = \{\sigma \in S_3 \mid \sigma(3) = 3\} \subset S_3$. Is H_3 a subgroup of S_3?

- If H_3 is a subgroup, is it cyclic?

Concrete Example (S_4)

Let $X = \{1, 2, 3, 4\}$. Then $Sym(X) = S_4$ has $4! = 24$ elements including:

1. $id_X : X \longrightarrow X$ defined as $id_X(1) = 1$, $id_X(2) = 2$ $id_X(3) = 3$ and $id_X(4) = 4$. id_X can be represented using the 'two-line notation'

$$id_X = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

2. $\sigma_1 : X \longrightarrow X$ defined as $\sigma_1(1) = 3$, $\sigma_1(2) = 2$, $\sigma_1(3) = 1$ and $\sigma_1(4) = 4$. In two-line notation σ_1 becomes represented as

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

3. $\sigma_2 : X \longrightarrow X$ defined as $\sigma_2(1) = 4$, $\sigma_2(2) = 3$, $\sigma_2(3) = 2$ and $\sigma_2(4) = 1$. In two-line notation σ_2 becomes represented as

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

S_4 Challenges

Challenge 1

Identify the remaining elements of S_4 using the two-line notation. Also, complete the following challenges:

1. Compute $\sigma_2 \circ \sigma_1$.
2. Compute σ_1^2, σ_1^3, σ_2^2 and σ_2^3.
3. Find σ_1^{-1} and σ_2^{-1}.
4. Find at least two nontrivial subgroups of S_4. Even better, can you identify all the nontrivial subgroups of S_4?
5. Is any of the identified nontrivial subgroups of S_4 cyclic?

Challenge 2

Let $H_4 = \{\sigma \in S_4 \mid \sigma(4) = 4\} \subset S_4$. Is H_4 a subgroup of S_4?

- If H_4 is a subgroup, is it cyclic?

Food for thought

- In practice, we are more interested in studying $Sym(X)$ when X has an additional structure rather than just being a plain set! This motivates the following natural questions:

1. Let X be a group. What interesting subgroup of $Sym(X)$ that would be interesting to study?
2. Let X be a topological space. What interesting subgroup of $Sym(X)$ that would be interesting to study?
3. Let X be an $n-$ dimensional smooth manifold. What interesting subgroup of $Sym(X)$ that would be interesting to study?
4. What if X is a complex Hilbert space? What interesting subgroup of $Sym(X)$ that would be interesting to study?

QF QUANTUM FORMALISM

GitHub: github.com/quantumformalism

YouTube: youtube.com/ZaikuGroup

Discord: discord.gg/SPcmcsXMD2

Twitter: twitter.com/ZaikuGroup

LinkedIn: linkedin.com/company/zaikugroup