A Very Brief Introduction to Group Theory

$$\phi : G \longrightarrow Sym(X)$$

Quantumformalism.com

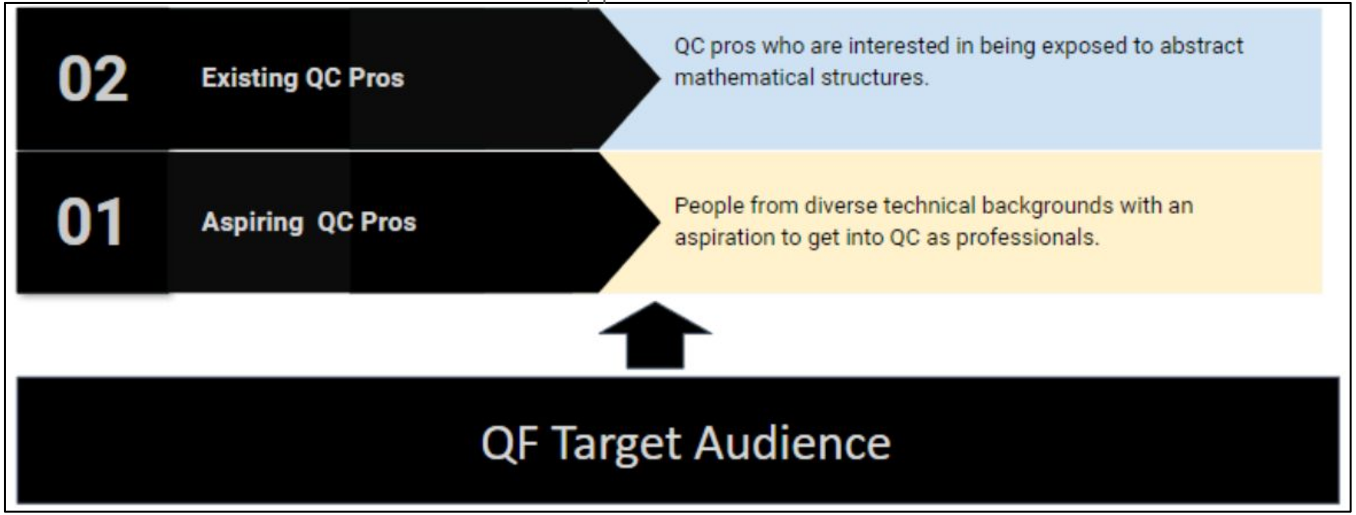
Quantum Computing Hackathon at Zayed University Abu Dhabi

Wednesday, 14/2/2023

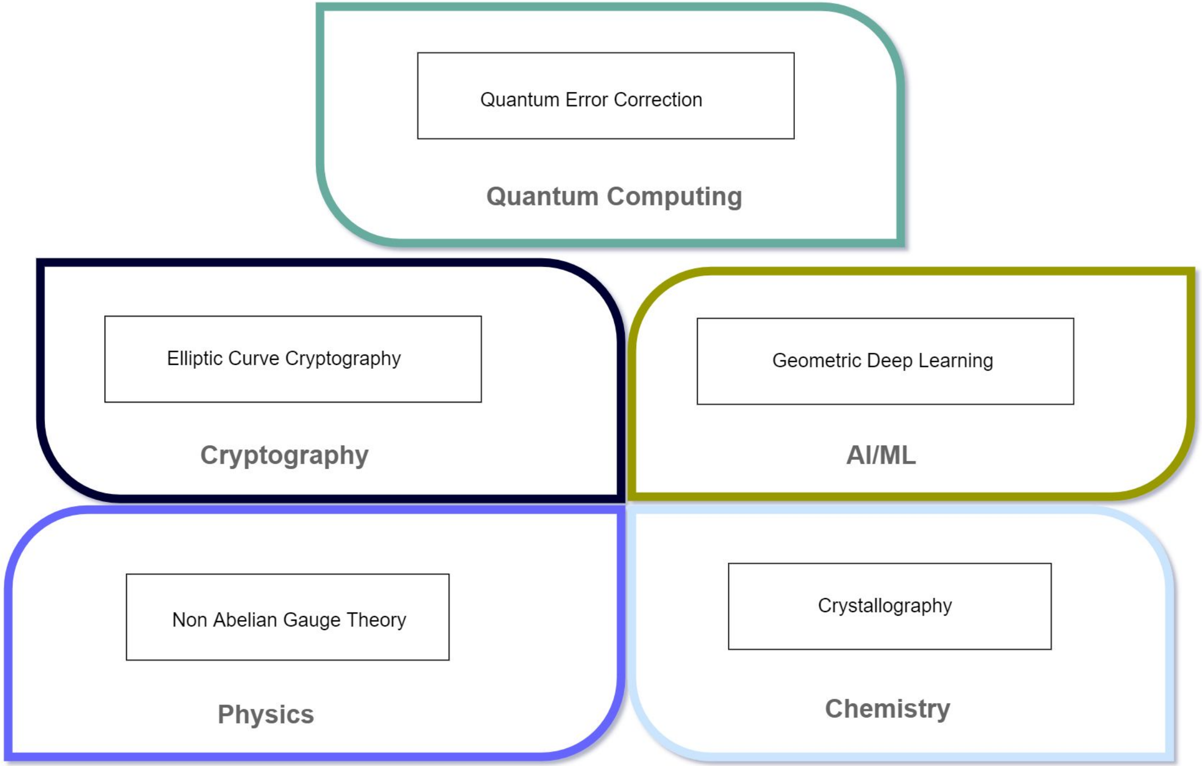
Presenter: Bambordé Baldé

About QF

Quantum Formalism is a free online course series provided by the Zaiku Group, aimed at exposing abstract mathematical topics to a diverse group of STEM professionals looking to break into the nascent quantum computing.



Why should you bother to learn group theory?



Some motivation for learning group theory

Nice to have prerequisite for this talk

- **Basics of Linear Algebra**
  1. Complex vector spaces.
  2. Linear operators between vector spaces.
  3. How to multiply two $n \times n$ complex matrices.
- **Basics of Quantum Computing**
  1. Aware that the n- dimensional complex vector space $\mathbb{C}^n$ is a complex Hilbert space. In particular, for a $k-$ qubit system, we use the Hilbert space $\mathbb{C}^n$ with $n = 2^k$.
     So for example, a single qubit system uses the space $\mathbb{C}^2$ and 2-qubit system uses $\mathbb{C}^{2^2} = \mathbb{C}^4$.
  2. Know the basic quantum gates such as; X, Y, Z and H.

Talk structure

1. The abstract group structure
2. Basic examples
3. Subgroups
4. Homomorphisms & Isomorphisms
5. Complex matrix groups
    - Unitary group
    - Unitary representations
    - Special unitary group

The abstract group structure

Definition 1.0

A group is a pair $(G, *)$ consisting of a nonempty set G and a binary function (operation) $* : G \times G \longrightarrow G$ satisfying the following conditions:

1. $g_1 * g_2 \in G$ for all $g_1, g_2 \in G$ (closure).
2. $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ for all $g_1, g_2, g_3 \in G$ (associativity).
3. There exists an element $e \in G$ such that $e * g = g * e = g$ for all $g \in G$ (identity).
4. For all $g \in G$ there exists a special element $g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$ (inverse).

- Two important consequences of the definition above are:
  1. The identity element e is unique i.e. if e_1 and e_2 are two identities then we must have $e_1 = e_2$.
  2. The inverse g^{-1} of each element g is also unique i.e. if g_1^{-1} and g_2^{-1} are inverses of g, then $g_1^{-1} = g_2^{-1}$.

Simple examples and counterexamples

- Which of the following are groups?
  1. $(\mathbb{N}, +)$ i.e. the set of natural numbers under ordinary addition.
  2. $(\mathbb{Z}, +)$ i.e. the set of integers under ordinary addition.
  3. $(\mathbb{Z}, \times)$ i.e. the set of integers under ordinary multiplication.
  4. $(\mathbb{R}, +)$ i.e. the set of real numbers under ordinary addition.
  5. $(\mathbb{R}, \times)$ i.e. the set of real numbers under ordinary multiplication.
  6. $(\mathbb{C}, +)$ i.e. the set of complex numbers under ordinary addition.
  7. $(\mathbb{C}, \times)$ i.e. the set of complex numbers under ordinary multiplication.
  8. $(\mathbb{C}^*, \times)$ i.e. the set of nonzero complex numbers under ordinary multiplication.
  9. $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ under mod5 addition giving my the following table:

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

quantumformalism.com

Terminology

A group $(G, *)$ is called commutative (or abelian) if $g_1 * g_2 = g_2 * g_1$ for all $g_1, g_2 \in G$. Otherwise, if $g_1 * g_2 \neq g_2 * g_1$ for some $g_1, g_2 \in G$, then $(G, *)$ is called noncommutative (or nonabelian).

- All the previous simple examples are abelian groups.
- In quantum computing, the quantum gates form a nonabelian group!

Notation awareness

Whenever the group operation $*$ on G is understood from the context, then we often just write G and omit writting the pair $(G, *)$.

Subgroups

Definition 1.1

Let $(G, *)$ be a group and $H \subseteq G$. Then we say H is a subgroup of G if $(H, *)$ also forms a group under the group operation $*$.

- By definition, G is a subgroup of itself. The same with the subset $\{e\}$ containing only the group identity element. The two are called 'trivial subgroups'!
- From our previous simple examples, we have the set of the integers $\mathbb{Z}$ is a subgroup of the group of reals $(\mathbb{R}, +)$ under the ordinary addition.

How to identify a subgroup structure?

Given a group $(G, *)$ and $H \subset G$. H is a subgroup of G if and only if the following conditions hold:

1. $h_1 * h_2 \in H$ for all $h_1, h_2 \in H$ i.e. we have closure in H.
2. For each $h \in H$ the group inverse $h^{-1} \in H$ i.e. the group inverse of each element of H also lies in H.

Homomorphisms

Definition 1.2

Let $(G, *)$ and $(G', *')$ be two groups. A map $\phi : G \longrightarrow G'$ is a homomorphism if $\phi(g_1 * g_2) = \phi(g_1) *' \phi(g_2)$ for all $g_1, g_2 \in G$.

- When the map ϕ is bijective (onto and one-to-one), we call it a group isomorphism.
- Two groups $(G, *)$ and $(G', *')$ are isomorphic if there is at an isomomorphism between then, and we write $G \simeq G'$.
- The isomorphism relationship is transitive i.e. $G_1 \simeq G_2$ and $G_2 \simeq G_3$ then $G_1 \simeq G_3$.

Definition 1.3

Let $(G, *)$, $(G', *')$ be two groups and $\phi : G \longrightarrow G'$ a homomorphism. We can define the following two subsets:

1. $Ker(\phi) = \{g \in G \mid \phi(g) = e'\}$ where e' is the identity in G'.
2. $Im(\phi) = \{\phi(g) \mid g \in G\}$.

Observation

It's not hard to prove that $Ker(\phi)$ is a subgroup of G and $Im(\phi)$ is a subgroup of G'. Also, ϕ is an isomorphism iff $Ker(\phi) = \{e\}$.

- A very familiar and famous example of a group homomorphism is when we consider the additive group of the reals $(\mathbb{R}, +)$ and the multiplicative group of the nonzero reals $(\mathbb{R}^*, \times)$. We can take the homomorphism $\phi : \mathbb{R} \longrightarrow \mathbb{R}^*$ to be defined as $\phi(x) = exp(x)$ for all $x \in \mathbb{R}$ where $exp(x)$ is the ordinary exponential function.

quantumformalism.com

Notation awareness

We'll write $M_n(\mathbb{C})$ to denote the set of all $n \times n$ matrices with entries in $\mathbb{C}$.

- Some authors use the notation $\mathbb{C}^{n \times n}$ instead of $M_n(\mathbb{C})$.
- I'll assume everyone knows about the basics of $n \times n$ matrices over the reals $\mathbb{C}$ including; how to compute the transpose, perform addition and multiplication of $n \times n$ matrices.
- When equipped with the ordinary matrix addition or multiplication, which of the following is true?

1. $M_n(\mathbb{C})$ forms an abelian group structure under addition.
2. $M_n(\mathbb{C})$ forms a nonabelian group structure under multiplication.

Important notes: From linear algebra 101 an element $A \in M_n(\mathbb{C})$ induces a linear map $L_A : \mathbb{C}^n \longrightarrow \mathbb{C}^n$, with $\mathbb{C}^n$ equipped with the canonical vector space structure over $\mathbb{C}$. Likewise, any linear map $L : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ induces an element $A_L \in M_n(\mathbb{C})$ i.e. linear operators on $\mathbb{C}^n \equiv n \times n$ matrices over $\mathbb{C}$.

Complex Matrix Groups

Definition 1.4

A subset $G \subset M_n(\mathbb{C})$ is a complex matrix group if it's a group under the ordinary matrix multiplication. This implies the matrices in G must satisfy all the group properties:

1. If $A, B \in G$ then $AB \in G$ i.e. matrix multiplication is a closed binary operation in G.
2. If $A, B, C \in G$ then $A(BC) = (AB)C$ i.e. matrix multiplication is associative in G. This is trivial to show because it is associative in $M_n(\mathbb{C})$!
3. The identity matrix $I_n \in G$.
4. For any $A \in G$ there exists an inverse matrix A^{-1} such that $AA^{-1} = A^{-1}A = I_n$.

Interesting example

The set $G = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1 \right\}$ is a complex matrix group under the ordinary matrix multiplication.

- The group G above is a very special type of group known as $SU(2)$!

Conjugate Transpose

Definition 1.5 (using the physicists notation)

Given $A \in M_n(\mathbb{C})$, we define the conjugate transpose of A as $A^\dagger = (\bar{A})^T$.

- Mathematicians normally use A^* instead of $A^\dagger$!
- For a complex number $\lambda = a + bi \in \mathbb{C}$, we'll write $\bar{\lambda} = a - bi$ to denote its complex conjugate. Be aware, physicists often write λ^*!

Interesting properties of conjugate transpose

Let $A, B \in M_n(\mathbb{C})$ and $\lambda \in \mathbb{C}$. Then the following identities hold:

1. $(A^\dagger)^\dagger = A$.
2. $(\lambda A)^\dagger = \bar{\lambda} A^\dagger$.
3. $(A + B)^\dagger = A^\dagger + B^\dagger$.
4. $(AB)^\dagger = B^\dagger A^\dagger$.
5. $det(A^\dagger) = \overline{det(A)}$.
6. If A is invertible then $A^\dagger$ is also invertible.

The Unitary Group

The unitary group

The set $U(n) = \{A \in M_n(\mathbb{C}) \mid A^\dagger A = AA^\dagger = I_n\}$ is a complex matrix group under the ordinary matrix multiplication.

- The group $U(n)$ is known in the literature as the unitary group.
- The group elements of $U(n)$ are indeed linear isometries in $\mathbb{C}^n$ i.e. they preserve the inner product in $\mathbb{C}^n$ and so the norm.
- $U(n)$ is a very important group with applications in many topics such as theoretical physics and quantum information science.
- $U(1)$ is abelian, but for $n \geq 2$, $U(n)$ is nonabelian of course!
- In quantum computation, the quantum gates for a k-qubit system are elements of the unitary group $U(2^k)$. For example, the gates for a 1-qubit system are elements of $U(2)$. Hence, the basic single qubit quantum gates such as; X, Y, Z and H are elements of $U(2)$!
- You can now see why the group structure of $U(2^k)$ is mathematically behind the reversibility of quantum computation!

Side note: $U(n)$ is compact and connected Lie group with 'real' dimension n^2.

Rotations on the Bloch sphere

We can epresent a single qubit geometrically as a point on the Bloch sphere as $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$. Then the 1-qubit gates can be represented as rotations on the Bloch sphere, which then allows you to do arbitrary rotations by an angle α along the x-axis, y-axis and z-axis as follows:

1. $R_x(\alpha) = e^{-i\frac{\alpha}{2}X}$, where $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.
2. $R_y(\alpha) = e^{-i\frac{\alpha}{2}Y}$, where $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$.
3. $R_z(\alpha) = e^{-i\frac{\alpha}{2}Z}$, where $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

- Each of the rotations above correspond to a 2×2 unitary matrix i.e. to an element of the unitary group $U(2)$.
- We can then view quantum computation as composition of the above rotations on the Bloch sphere!

Unitary representations

Given a group $(G, *)$, a homomorphism $\rho : G \longrightarrow U(n)$ is a called an n-dimensional unitary representation of G.

Examples:

1. Let $G = (\mathbb{R}, +)$ i.e the reals with the group structure under addition. Then we can build a $1-$ dimensional unitary representation of $\mathbb{R}$ by defining $\rho : \mathbb{R} \longrightarrow U(1)$ as $\rho(t) = e^{2\pi i t}$ for all $t \in \mathbb{R}$.
2. Let again $G = (\mathbb{R}, +)$. Then we can build an $n-$ dimensional unitary representation of $\mathbb{R}$ by defining $\rho : \mathbb{R} \longrightarrow U(n)$ as $\rho(t) = e^{-\frac{i}{\hbar}Ht}$ for all $t \in \mathbb{R}$, where H is a Hermitian matrix and $\hbar$ is the Planck's constant.

The Special Unitary Group

The special unitary group

The set $SU(n) = \{A \in U(n) \mid det(A) = 1\}$ is a subgroup of $U(n)$.

- $SU(n)$ is known in the literature as the special unitary group.
- For $n = 2$, we can equivalently obtain $SU(2)$ as follows:
  $SU(2) = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1 \right\}.$

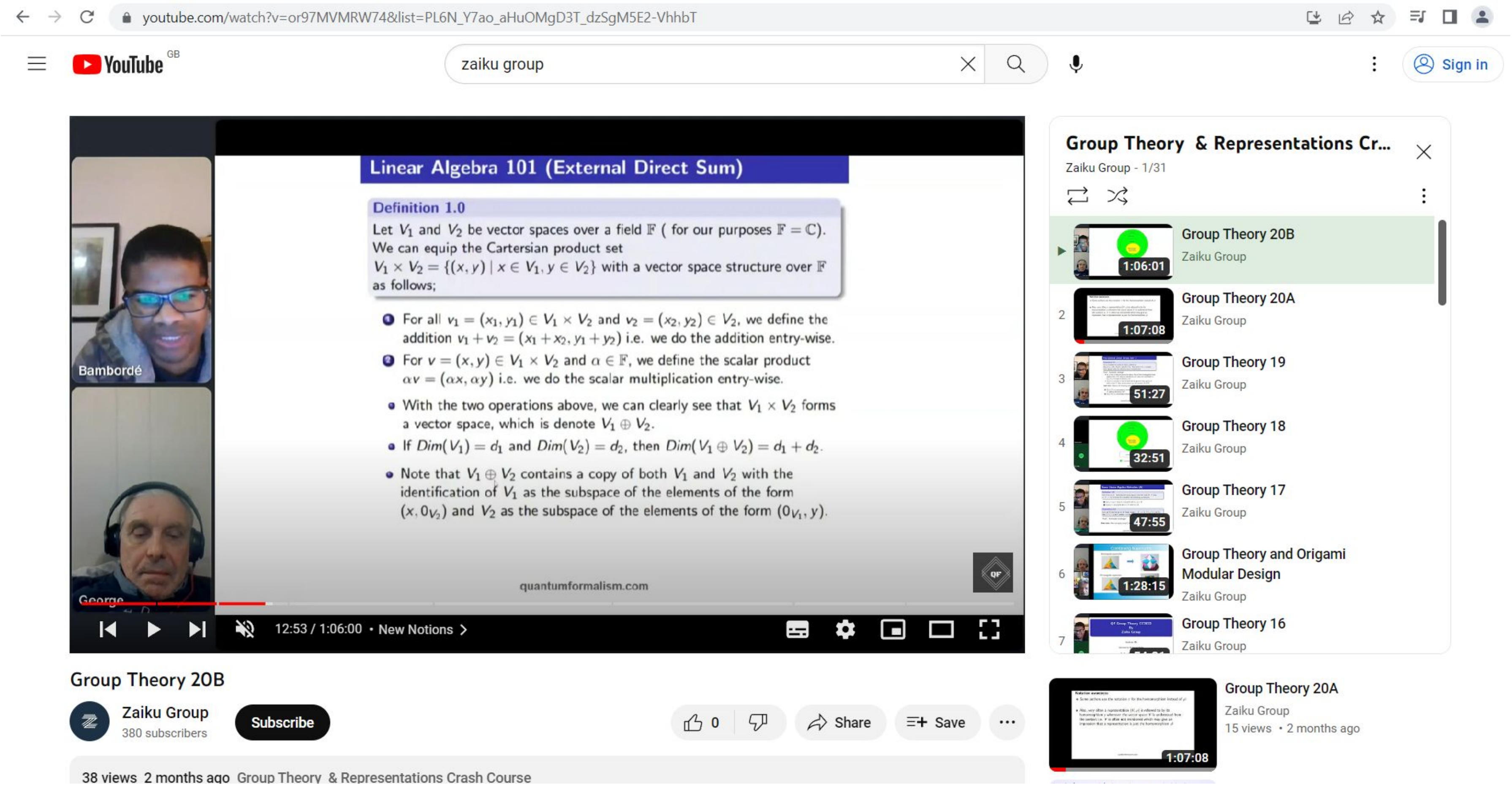
Observation

Let $\mathbb{C}^*$ be the multiplicative group of the nonzero complex numbers. Then the determinant map $det : U(n) \longrightarrow \mathbb{C}^*$ taking $A \in U(n)$ to $det(A) \in \mathbb{C}^*$ is a group homomorphism. Then $Ker(det) = SU(n)$ right?

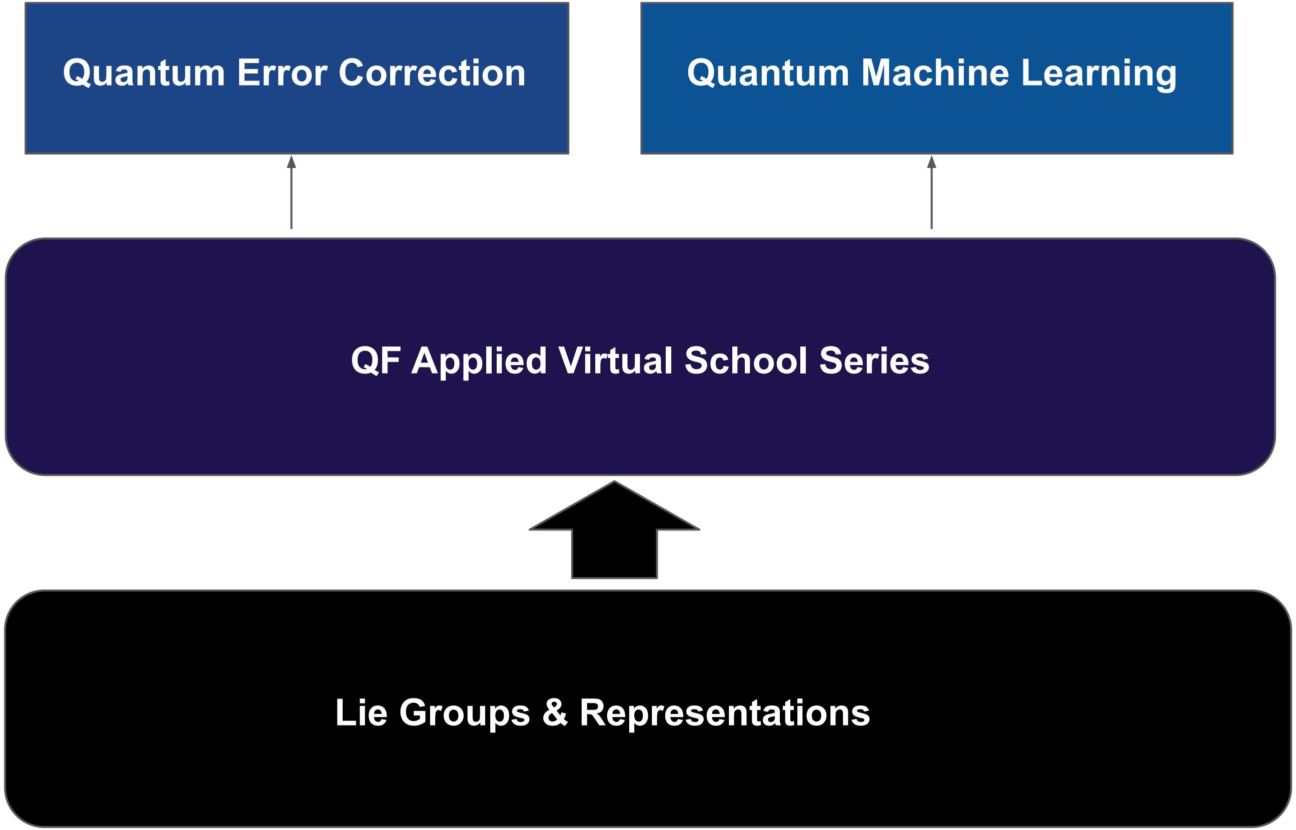
Side notes:

1. $SU(n)$ is compact and connected Lie group with 'real' dimension $n^2 - 1$.
2. The product group $SU(3) \times SU(2) \times U(1)$ is the foundation of the 'Standard Model of Particle Physics'!

Course recommendation



Applied QF Initiatives



QF Open Source Challenge

QUANTUM
FORMALISM

GitHub: github.com/quantumformalism

YouTube: youtube.com/ZaikuGroup

Discord: discord.gg/SPcmcsXMD2

LinkedIn: linkedin.com/company/quantumformalism