QF QUANTUM FORMALISM

Matrix Groups - Part 1

Bambordé Baldé | Co-Founder at Zaiku Group | Twitter: @zaikubalde • **zaikugroup.com** • November 27, 2020

Lecture Agenda Summary

1. Pre-Lecture Comments
2. Abstract Multiplicative Groups
3. Subgroups
4. Group Centres
5. Group Homomorphisms

Part A

1. Determinant (focus on 2 x 2 matrices)
2. Determinant & Invertibility
3. The General Linear Group
4. Special Linear Group
5. Study Materials Comments

Part B

Foundation Module Review

Rings and Fields 101 #1	Matrix Algebra #2	Quantum Operators + Composite Systems #3
Group Theory 101 #1	Linear Operators 101 #2	Finite dim. Hilbert Spaces #2
Naive Set Theory Overview #1	Complex Vector spaces 101 #2	Mat. Groups: GL(2, C) & U(2) + SU(2) #2

Completed | Ongoing | #n is the number of live lectures

YouTube Policy Implications

42,823 views | Nov 18, 2020, 11:15pm EST

YouTube Will Now Show Ads On All Videos Even If Creators Don't Want Them

John Koetsier Senior Contributor

Consumer Tech

John Koetsier is a journalist, analyst, author, and speaker.

PART A: GROUP THEORY REFRESH

Abstract Multiplicative Group

Definition (1.0)

A multiplicative group is $(G, \times)$ where G is a non-empty set and $\times$ is a closed binary operation on G called multiplication satisfying the following axioms:

1. There exists an element $e \in G$ such that for all $A \in G$, $e \times A = A \times e = A$ (identity).
2. $A \times (B \times C) = (A \times B) \times C$ for all $A, B, C \in G$ (associativity).
3. For all $A \in G$ there exists $A^{-1} \in G$ such that $A \times A^{-1} = A^{-1} \times A = e$ (inverse)

Definition (1.1)

A group $(G, \times)$ is said to be commutative (or abelian) if for all $A, B \in G$, $A \times B = B \times A$. Otherwise $(G, \times)$ is called noncommutative (or non-abelian) group.

Proposition (1.0)

If $(G, \times)$ is a group, then the following statements are true:

1. There is a unique $e \in G$ such that $A \times e = A \times e = A \; \forall A \in G$.
2. The inverse element A^{-1} is unique $\forall A \in G$.

Proof : Homework challenge!

Convention: From now on, we'll just write AB to denote the multiplication instead of $A \times B$. We'll also just write G instead of $(G, \times)$.

Definition (1.2)

$\mathbb{C}^* = \left\{ z \in \mathbb{C} \mid z \neq 0 \right\}$ i.e. the set of all non-zero complex numbers.

- Is $\mathbb{C}^*$ a group under the multiplication in $\mathbb{C}$? If yes, is it abelian or non-abelian?

Subgroups

Definition (1.3)

Let G be a group and let $H \subseteq G$. We say H is a subgroup of G if H is also a group under the same multiplication.

- It's clear that G is a subgroup of itself. The subset with only identity element $\{e\}$ is also a subgroup of G.
- Can you find any non-trivial subgroup of $\mathbb{C}^*$?

Proposition (1.1)

A subset $H \subseteq G$ is a subgroup of G iff the following conditions hold:

1. $e \in H$ where e is the identity in G.
2. $AB \in H$ for all $A, B \in H$.
3. If $A \in H$ then $A^{-1} \in H$.

Proof : Homework challenge?

Group Homomorphisms

Definition (1.4)

Let G_1 and G_2 be groups. A map $f : G_1 \to G_2$ is called homomorphism if $f(AB) = f(A)f(B)$ for all $A, B \in G_1$.

- Let e_1 and e_2 be the respective identity elements of the two groups. Is it true that $f(e_1) = e_2$?
- If f is a bijection then we call f a group isomorphism and write $G_1 \simeq G_2$.

Definition (1.5)

The image of a homomorphism f is defined as $Im_f = \{f(A) \mid A \in G_1\}$.

- Is Im_f a subgroup of G_2? If yes, can you say whether it is abelian or non-abelian?

Definition (1.6)

The kernel of a homomorphism $f : G_1 \longrightarrow G_2$ is defined as $Ker_f = \{A \in G_1 \mid f(A) = e_2\}$ where e_2 is the identity in G_2.

- Is Ker_f a subgroup of G_1? If yes, can you say whether it's abelian or non-abelian?

Group Commutators

Definition (1.7)

Let G be a group. The commutator between any two elements A, B is defined as $[A, B] = A^{-1}B^{-1}AB$.

Proposition (1.2)

Let $[,]$ be the commutator on G. Then the following are true:

1. G is abelian iff $[A, B] = e$ for all $A, B \in G$.
2. $[B, A] = [A, B]^{-1}$ for all $A, B \in G$
3. $[A, BC] = [A, C][A, B][[A, B], C]$ for all $A, B, C \in G$.

Proof : Homework!

- Hence, the commutator is a measures on how abelian a group is!
- For most practical and interesting applications of group theory, the less abelian the better!

Group Centre

Definition (1.8)

Let G be a group. The centre of G is defined as
$Z(G) = \{A \in G \mid [A, B] = e \text{ for all } B \in G\}$.

- In most textbooks the centre is equivalently defined as $Z(G) = \{A \in G \mid AB = BA \text{ for all } B \in G\}$.
- The reason for using the commutator in the definition above is to force you to get familiar with commutators before Lie Groups Lie Algebras section!

Proposition (1.3)

The centre $Z(G)$ is a subgroup of G.

Proof : Homework challenge?

- In a nutshell, the smaller the centre, the less abelian a group is!

PART B: MATRIX GROUPS

Matrix Determinant

Definition (1.0)

For $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(\mathbb{C})$, we define $\det(A) = a_{11}a_{22} - a_{12}a_{21}$.

- Be aware that some authors use the notation $|A|$ instead of $det(A)$.
- Let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then we have: $\det(X) = \det(Z) = -1$ and $\det(\mathbb{I}) = 1$.
- What about the determinant matrices such as Y and H?
- The concept of determinant can indeed be defined for any $n \geq 1$. In this course section we'll focus in the $n = 2$ case for simplicity.
- Interestingly, for diagonal matrices $D = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix} \in M_n(\mathbb{C})$, we have

$$\det(D) = a_{11} \times a_{22} \times \ldots \times a_{nn}.$$

Determinant Properties

Proposition (1.0)

Let $A, B \in M_2(\mathbb{C})$ and $\lambda \in \mathbb{C}$. Then the following properties hold:

1. $\det\left(A^T\right) = \det(A)$
2. $\det(\lambda A) = \lambda^2 det(A)$.
3. $\det(AB) = det(A)det(B)$.

Proof : Homework challenge?

- Just as curiosity, for $A \in M_n(\mathbb{C})$ we have that $det(\lambda A) = \lambda^n det(A)$.

Proposition (1.1)

If $A \in M_2(\mathbb{C})$ is invertible then $\det\left(A^{-1}\right) = \frac{1}{\det(A)}$.

Proof : Homework challenge? Recall that $A \in M_2(\mathbb{C})$ is invertible if there exists $A^{-1} \in M_2(\mathbb{C})$ such that $AA^{-1} = A^{-1}A = \mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Determinants and Invertibility

Theorem (1.0)

Let $A \in M_2(\mathbb{C})$. Then the following statements are equivalent:

1. $\det(A) \neq 0$.
2. A is invertible.
3. $\text{Rank}(A) = 2$ i.e. $\dim Ran(A) = 2$.
4. The rows of A are linearly independent.

Proof : Check the study materials or homework challenge?

- Hence, $A \in M_2(\mathbb{C})$ is invertible iff $\det(A) \neq 0$ and conversely if A is invertible then $\det(A) \neq 0$.
- If A is invertible, how do we compute its inverse? Can the determinant help us?

Computing Matrix Inverse

Proposition (1.2)

If $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(\mathbb{C})$ is invertible i.e. $\det(A) \neq 0$ then its inverse is given by $A^{-1} = \frac{1}{det(A)} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$.

Proof : Homework challenge?

- In general, if $A \in M_n(\mathbb{C})$ is invertible then $A^{-1} = \frac{1}{det(A)} Adj(A)$ where $Adj(A)$ is the so-called adjoint (classical) matrix of A.
- A bit trivial, but try apply the inverse formula to:
$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$.

The General Linear Group

Definition (1.2)

Let us define the set $GL(2,\mathbb{C}) = \left\{ A \in M_2(\mathbb{C}) \mid \det(A) \neq 0 \right\}$.

- We can generalise the definition above to any $n > 1$ i.e.

  $GL(n,\mathbb{C}) = \left\{ A \in M_n(\mathbb{C}) \mid \det(A) \neq 0 \right\}$.

Proposition (1.3)

$GL(2,\mathbb{C})$ is a group under matrix multiplication in $M_2(\mathbb{C})$.

Proof : Homework challenge?

- On a side note, $GL(n,\mathbb{C})$ is an example of a Lie group i.e. a group that comes with a topological manifold structure!

Some Comments

- Recall that $GL(2,\mathbb{C})$ being group implies the following:
  1. $AB \in GL(2,\mathbb{C})$ for all $A, B \in GL(2,\mathbb{C})$ i.e if $det(A)$ and $det(B)$ are non-zero then $det(AB)$ is non-zero.
  2. The matrix identity $\mathbb{I} \in GL(2,\mathbb{C})$ is the group identity element i.e. $A\mathbb{I} = \mathbb{I}A = A$ for all $A \in GL(2,\mathbb{C})$.
  3. $A(BC) = (AB)C$ for all $A, B, C \in GL(2,\mathbb{C})$.
  4. For all $A \in GL(2,\mathbb{C})$ there exists $A^{-1} \in GL(2,\mathbb{C})$ such that $AA^{-1} = A^{-1}A = \mathbb{I}$.
- Proposition 1.3 is generally true for any $GL(n,\mathbb{C})$. But for QC purposes, you'll probably want $n = 2^k$ where k is the number of qubits under consideration so that $GL(n,\mathbb{C})$ matrices can act as operators on $\mathbb{C}^{2^k}$.
- Indeed most interesting constructions we make for $GL(2,\mathbb{C})$ will also be valid $GL(n,\mathbb{C})$. But be careful, there are some stuff that dependent on whether n is even or odd natural number!

The Center of $GL(2, \mathbb{C})$

Proposition (1.4)

$$Z(GL(2,\mathbb{C})) = \left\{ \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \mid \lambda \in \mathbb{C}^* \right\}.$$

Proof : Homework challenge?

- As you can see the centre of $GL(2, \mathbb{C})$ is very small and so it's a very non-abelian group!
- The same applies to $GL(n, \mathbb{C})$ since its centre is also of the form:

$$Z(GL(n,\mathbb{C})) = \left\{ \lambda \mathbb{I}_n \mid \lambda \in \mathbb{C}^* \right\} \text{ where } \mathbb{I}_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \text{ is the identity matrix.}$$

Special Linear Group

Definition (1.3)

We can define the set $SL(2, \mathbb{C}) = \left\{ A \in GL(2, \mathbb{C}) \mid \det(A) = 1 \right\}.$

- We can also generalise the definition above to any $n > 1$ i.e.
  $SL(n, \mathbb{C}) = \left\{ A \in GL(n, \mathbb{C}) \mid \det(A) = 1 \right\}.$

Proposition (1.5)

$SL(2, \mathbb{C})$ is a subgroup of $GL(2, \mathbb{C})$.

Proof : Homework challenge?

- The above proposition can of course be generalised to $SL(n, \mathbb{C})$.
- What could be Z(SL(2, C)) or more generally Z(SL(n, C))?

- As home challenge, try identity as many single qubit gates as possible that are elements of $SL(2, \mathbb{C})$. Then apply these to the qubits on the block sphere and see what happens!

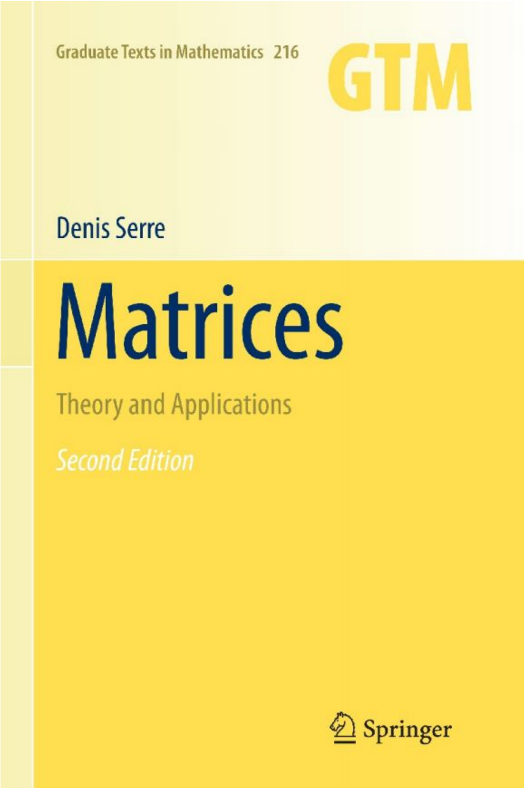
The Determinant as Homomorphism

Proposition (1.6)

The map $\det : GL(2, \mathbb{C}) \longrightarrow \mathbb{C}^*$ is a group homomorphism i.e. $\det(AB) = \det(A)det(B)$ for all $A, B \in G$.

Proof : You've already proved it!

- Of course, the above proposition is true for any $\det : GL(n, \mathbb{C}) \longrightarrow \mathbb{C}^*$.
- Since $\det : GL(2, \mathbb{C}) \longrightarrow \mathbb{C}^*$ is a group homomorphism, a natural question to ask is what is $Ker(\det)$? We know from Part A that $Ker(\det)$ is indeed a subgroup of $GL(2, \mathbb{C})$.
- The observation above also applies to $\det : GL(n, \mathbb{C}) \longrightarrow \mathbb{C}^*$.



Denis Serre

Where should you focus?

Chapter 2: What Are Matrices | **Chapter 3:** Square Matrices

--------(*Pages 15 - 38)*----------

QUANTUM FORMALISM

- **GitHub (Curated study materials):** *github.com/quantumformalism*
- **YouTube:** youtube.com/zaikugroup
- **Twitter:** *@ZaikuGroup*
- ***Gitter:*** *gitter.im/quantumformalism/community*