QUANTUM FORMALISM

A Brief Introduction to Group Theory

Bambordé Baldé | Co-Founder at Zaiku Group | Twitter: @zaikubalde • **zaikugroup.com** • September 25, 2020

Refined Foundation Module

Rings and Fields 101 #1	Matrix Analysis #1	Quantum Matrix Operators #2
Group Theory 101 #1	Linear Operators #2	Complex Hilbert Spaces #1
Naive Set Theory Overview #1	Complex Vector spaces #1	Matrix Groups: GL(n, C) & U(n) #3

Completed | #n is the number of live lectures

Lecture Agenda Summary

1. Binary Operations on Sets
2. Group Theory Axioms
3. Additive Notation
4. 2x1 Complex Additive Matrix Group
5. 2x2 Complex Matrices
6. General Linear Group of 2x2 Complex Matrices aka GL(2, C)
7. GL(2, C) Left Action
8. GL(2, C) Commutator
9. Study Material Comment

Binary Operations on Sets

Definition (1.0)

Let X be a non-empty set. A binary operation on X is a prescription $*$ that takes two elements ψ_1 and ψ_2 in X to generate a third element $\psi_1 * \psi_2 \in X$.

- A more formal way to define $*$ would be as a map from the Cartesian product of X to itself i.e. $* : X \times X \to X$.

Definition (1.1)

A binary operation $*$ on X is closed if for for all $\psi_1, \psi_2 \in X$, $\psi_1 * \psi_2 \in X$.

- Let $X = \mathbb{N}_0$ and $* = +$ where $+$ is the normal addition in $\mathbb{N}_0$. It's clear that $+$ closed in $\mathbb{N}_0$. Multiplication $\times$ is also closed in $\mathbb{N}_0$.

Group Theory Axioms

Definition (1.2)

A group is a pair $(G, *)$ where G is a non-empty set and $*$ is a closed binary operation on G satisfying the following axioms:

1. There exists an element $e \in G$ such that for all $\psi \in G$, $e * \psi = \psi * e = \psi$ (identity)
2. $\psi_1 * (\psi_2 * \psi_3) = (\psi_1 * \psi_2) * \psi_3$ for all ψ_1, ψ_2, ψ_3 in G (associativity)
3. For all $\psi \in G$ there exists $\tilde{\psi} \in G$ such that $\psi * \tilde{\psi} = e$ (inverse)

Definition (1.3)

A group $(G, *)$ is called commutative (or abelian) group if for all $\psi_1, \psi_2 \in G$, $\psi_1 * \psi_2 = \psi_2 * \psi_1$. Otherwise $(G, *)$ is called noncommutative (or non-abelian) group.

Proposition (1.0)

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

1. There is a unique $e \in G$ such that $e * \psi = \psi * e = \psi \ \forall \psi \in G$
2. The inverse element $\tilde{\psi}$ is unique $\forall \psi \in G$

Proof :

1. Let e and $\tilde{e}$ be both identities in G. By the group axioms, we will have $e * \psi = \psi * e = \psi$ and $\tilde{e} * \psi = \psi * \tilde{e} = \psi \ \forall \psi \in G$. Now since e is an identity, then $e * \tilde{e} = \tilde{e}$. But we also assumed $\tilde{e}$ as identity, hence $e * \tilde{e} = e$ and so $e = e * \tilde{e} = \tilde{e}$.
2. Let $\tilde{\psi}_1$ and $\tilde{\psi}_2$ be two inverses for $\psi \in G$. Then $\psi * \tilde{\psi}_1 = \tilde{\psi}_1 * \psi = e$ and $\psi * \tilde{\psi}_2 = \tilde{\psi}_2 * \psi = e$. But then $\tilde{\psi}_1 = \tilde{\psi}_1 * e = \tilde{\psi}_1 * (\psi * \tilde{\psi}_2) = (\tilde{\psi}_1 * \psi) * \tilde{\psi}_2 = e * \tilde{\psi}_2 = \tilde{\psi}_2$.

Additive Notation

- When dealing with abelian groups, we often replace the abstract binary operation $*$ with $+$ and call $(G, +)$ an additive group.
- When dealing with an additive group $(G, +)$, it is a convention to denote the group identity element 0 instead of e!
- Also, for each $\psi \in G$ we denote it's inverse element $-\psi$ instead of $\tilde{\psi}$.

Hence, we can rewrite the group axioms below using the additive notation convention above i.e. $(G, +)$ is an additive group if:

1. $\psi_1 + \psi_2 = \psi_2 + \psi_1$ for all $\psi_1, \psi_2 \in G$
2. There exists an element $0 \in G$ such that for all $\psi \in G$, $0 + \psi = \psi + 0 = \psi$
3. $\psi_1 + (\psi_2 + \psi_3) = (\psi_1 + \psi_2) + \psi_3$ for all ψ_1, ψ_2, ψ_3 in G
4. For all $\psi \in G$ there exists $-\psi \in G$ such that $\psi + -\psi = 0$

Examples of Additive Groups

- Which of the following pairs form an additive group?
  1. $(\mathbb{N}_0, +)$
  2. $(\mathbb{Z}, +)$
  3. $(\mathbb{R}, +)$
  4. $(\mathbb{C}, +)$

1. $\psi_1 + \psi_2 = \psi_2 + \psi_1$ for all $\psi_1, \psi_2 \in G$
2. There exists an element $0 \in G$ such that for all $\psi \in G$, $0 + \psi = \psi + 0 = \psi$
3. $\psi_1 + (\psi_2 + \psi_3) = (\psi_1 + \psi_2) + \psi_3$ for all ψ_1, ψ_2, ψ_3 in G
4. For all $\psi \in G$ there exists $-\psi \in G$ such that $\psi + -\psi = 0$

- Let $\mathbb{Z}_3 = \{0, 1, 2\}$. Is $(\mathbb{Z}_3, +)$ an additive group?

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

Definition (1.4)

A group G is finite if its underlying set is finite. Likewise G is infinite if its underlying is infinite. The cardinality of $|G|$ is called the order of G.

Definition (1.5)

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

- It's clear that G is a subgroup of itself. The subset with only identity element $\{e\}$ is also a subgroup of G. The two groups are called trivial subgroups.
- We already know that $\mathbb{Z}$ is an additive group. Is the set of even integers $2\mathbb{Z}$ a subgroup of $\mathbb{Z}$?
- We can also naturally define the set $3\mathbb{Z}$ as the set of integers multiples of 3. Is $3\mathbb{Z}$ a subgroup of $\mathbb{Z}$?
- Is every subgroup of $\mathbb{Z}$ of the form $n\mathbb{Z}$ for $n = 0, 1, 2, 3, 4...$?

$2\times$ 1 Complex Additive Matrix Group

Definition (1.6)

We can define the set of all 2×1 matrices with entries in $\mathbb{C}$ as $\mathbb{C}^{2\times 1} = \left\{ \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}$. We'll just write $\mathbb{C}^2$ instead of $\mathbb{C}^{2\times 1}$.

- We can define $+$ in $\mathbb{C}^2$ naturally as follow:
  Let $\psi_1 = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix}$ and $\psi_2 = \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix}$ be any two elements of $\mathbb{C}^2$. We define $\psi_1 + \psi_2 = \begin{pmatrix} \alpha_1 + \alpha_2 \\ \beta_1 + \beta_2 \end{pmatrix}$. We can easily see that $\mathbb{C}^2$ is an additive group right? Where $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ is the zero and for all $\psi = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ its inverse element $-\psi = \begin{pmatrix} -\alpha \\ -\beta \end{pmatrix}$ i.e. $\psi + -\psi = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

Famous Elements of $\mathbb{C}^2$

$$\psi_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \psi_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \psi_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \psi_3 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix}, \psi_4 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix}, \psi_5 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} \end{pmatrix}$$

- We'll now make another convention of using the ψ notation to only denote elements of $\mathbb{C}^2$ or more generally $\mathbb{C}^n$ for some positive $n > 1$.
- We don't have a vector space structure yet in $\mathbb{C}^2$ for us to be able to manipulate its elements the way most of you are used to.
- But can we still do something interesting with $\mathbb{C}^2$ elements using only group theoretic concepts? The answers is yes and we'll use the group theoretic concept of '**left action**'!

2×2 Complex Matrices

Definition (1.7)

We can define the set of all 2×2 matrices with entries in $\mathbb{C}$ as

$$M_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{C} \right\}.$$

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ be two elements of $M_2(\mathbb{C})$. We can define the notion of multiplication $\times$ for A and B as follows:

$$A \times B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} (a \times e) + (b \times g) & (a \times f) + (b \times h) \\ (c \times e) + (d \times g) & (c \times f) + (d \times h) \end{pmatrix}$$

- An alternative notation very often used for the above matrix multiplication is:
  $$AB = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} (ae) + (bg) & (af) + (bh) \\ (ce) + (dg) & (cf) + (dh) \end{pmatrix}$$
- One thing very important to note is that, unlikely ordinary numbers, with matrices in general $A \times B \neq B \times A$! When that happens we say A and B don't commute!

The General Linear Group of 2×2 Matrices

Definition (1.8)

The set $GL(2,\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{C}) \mid ad - bc \neq 0 \right\}$ is a group under the multiplication in $M_2(\mathbb{C})$.

- The identity element of $GL(2,\mathbb{C})$ is $\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ i.e. for any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{C})$ $A\mathbb{I} = \mathbb{I}A = A$.
- For any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{C})$, it's inverse is denoted A^{-1} i.e. $A^{-1} \in GL(2,\mathbb{C})$ such that $AA^{-1} = A^{-1}A = \mathbb{I}$. With a bit of head scratching, we can see that $A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$
- Beware that some authors use the notation $GL_2(\mathbb{C})$ instead of $GL(2,\mathbb{C})$!

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

- The first thing to note is that $GL(2, \mathbb{C})$ is a non abelian group i.e. $AB = BA$ doesn't hold for all $A, B \in GL(2, \mathbb{C})$. For example consider $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Following the multiplication rules, $AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ whereas $BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.
- $GL(2, \mathbb{C})$ contains involutory matrices i.e. $A \in GL(2, \mathbb{C})$ such that $AA = A^2 = \mathbb{I}$ or in other words $A = A^{-1}$! Three of these special matrices that are very important in quantum computing are the X, Y, Z gates:
  $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- More precisely $X, Y, Z \in U(2)$, where $U(2)$ is a subset of $GL(2, \mathbb{C})$ that also forms a group called the unitary group i.e. $U(2)$ is a subgroup of $GL(2, \mathbb{C})$.

$GL(2, \mathbb{C})$ Left Action

Definition (1.9)

Let X be a non-empty set. A left action (or multiplication) of $GL(2, \mathbb{C})$ on X is a prescription $\cdot$ that takes an element $A \in GL(2, \mathbb{C})$ and $\psi \in X$ to produce another element $A \cdot \psi \in X$ such that the following holds:

1. $A \cdot (B \cdot \psi) = (AB) \cdot \psi$ for all $A, B \in GL(2, \mathbb{C})$ and for all $\psi \in X$.
2. $\mathbb{I} \cdot \psi = \psi$ for all $\psi \in X$.

Proposition (1.1)

Let $\psi_1, \psi_2 \in X$ and $A \in GL(2, \mathbb{C})$. Then the following is true:

1. If $A \cdot \psi_1 = \psi_2$ then $\psi_1 = A^{-1} \cdot \psi_2$
2. If $\psi_1 \neq \psi_2$ then $A \cdot \psi_1 \neq A \cdot \psi_2$

Proof : Homework!

$GL(2,\mathbb{C})$ Left Acting on $\mathbb{C}^2$

For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{C})$ and $\psi = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2$, we can define the left action $\cdot$ as follows:

$$A \cdot \psi = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix} \alpha + \begin{pmatrix} b \\ d \end{pmatrix} \beta = \begin{pmatrix} a\alpha \\ c\alpha \end{pmatrix} + \begin{pmatrix} b\beta \\ d\beta \end{pmatrix} = \begin{pmatrix} a\alpha + b\beta \\ c\alpha + d\beta \end{pmatrix}.$$

- As homework, you can verify that the above $\cdot$ multiplication satisfies the axioms for the left action.
- If we consider $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\psi = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Then $X \cdot \psi = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$GL(2,\mathbb{C})$ Left Action Challenge

Calculate the left action between the following elements of $\mathbb{C}^2$ and $GL(2,\mathbb{C})$:

$$\psi_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \psi_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \psi_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \psi_3 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix}, \psi_4 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix},$$

$$\psi_5 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$GL(2,\mathbb{C})$ Group Commutator

Definition (2.0)

Let $A, B \in GL(2,\mathbb{C})$. The commutator between A, B is defined as $[A, B] = A^{-1}B^{-1}AB$.

Proposition (1.2)

Let $[,]$ be the commutator on $GL(2,\mathbb{C})$. Then the following statements are true:

1. For all $A, B \in GL(2,\mathbb{C})$, $[A, B] = \mathbb{I}$ if only if A and B commute i.e. $AB = BA$.
2. $[B, A] = [A, B]^{-1}$ for all $A, B \in GL(2,\mathbb{C})$
3. $[A, BC] = [A, C][A, B][[A, B], C]$ for all $A, B, C \in GL(2,\mathbb{C})$

Proof : Homework!

Extra Commutator Challenge

- Calculate the commmutators between the following elements of $GL(2,\mathbb{C})$:
  $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$
- Apply the result of each commutator calculation to the following elements of $\mathbb{C}^2$: $\psi_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\psi_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $\psi_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$,
  $\psi_3 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix}$, $\psi_4 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix}$, $\psi_5 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} \end{pmatrix}$

Missing Important Concepts

Some important group-theoretic stuff that were deliberately left out but that are important include:

1. Group homomorphisms
2. Symmetry groups
3. Subgroups
4. Cyclic groups
5. Quotient groups
6. Direct Products
7. Direct Sums

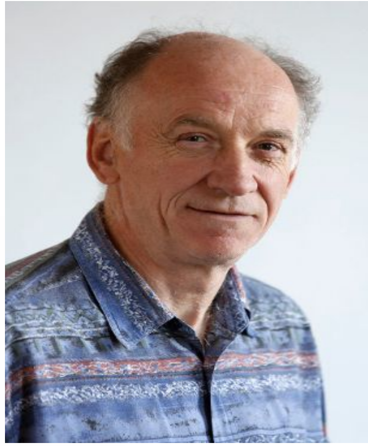
However, we'll have the opportunity to introduce them as we go along at the right time!

F1.3YR1

ABSTRACT ALGEBRA

INTRODUCTION TO GROUP THEORY

LECTURE NOTES AND EXERCISES



Prof. Jim Howie

Where should you focus?

Pages 3 - 25

Extra Bonus

Pages 27 - 44

QF QUANTUM FORMALISM

- **GitHub (Curated study materials):** *github.com/quantumformalism*
- **YouTube:** Search Zaiku Group
- **Twitter:** *@ZaikuGroup*
- ***Slack (coming soon)***