Rings & Fields 101

Bambordé Baldé | Co-Founder at Zaiku Group | Twitter: @zaikubalde • **zaikugroup.com** • October 2, 2020

Community Acknowledgement

Big thanks to Amir Ebrahimi for lecture 01 errata!

Community Chat Moderators

{Rolf Lobo, Soham Pal, Harshit Garg, Barry Burd}

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 #2
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. Additive Groups Axioms (Recap)
2. Ring Axioms
3. Ring Examples
4. Integral Domains
5. 2x2 Complex Matrix Ring
6. Matrix Ring Commutators
7. Definition of Field
8. Study Material Comment

Additive Groups Recap

Definition

Recall that an additive group is an abelian group $(G, +)$ i.e. a group satisfying the following conditions:

1. $g_1 + g_2 = g_2 + g_1$ for all $g_1, g_2 \in G$
2. There exists an element $0 \in G$ such that for all $g \in G$, $0 + g = g + 0 = g$ (identity or zero element)
3. $g_1 + (g_2 + g_3) = (g_1 + g_2) + g_3$ for all g_1, g_2, g_3 in G (associative)
4. For all $g \in G$ there exists $-g \in G$ such that $g + -g = 0$ (inverse)

- Examples of additive groups:
  1. $(\mathbb{Z}, +)$
  2. $(\mathbb{R}, +)$
  3. $(\mathbb{C}, +)$
  4. $(\mathbb{C}^2, +)$

Definition (1.0)

A ring is a triple $(R, +, \times)$ where R is a non-empty set and $+$ and $\times$ are closed binary operations on R satisfying the following axioms:

1. $(R, +)$ is an additive group
2. $A \times (B \times C) = (A \times B) \times C$ for all $A, B, C \in R$ (associative)
3. $A \times (B + C) = (A \times B) + (A \times C)$ for all $A, B, C \in R$ (distributive)

- Sometimes mathematicians drop the associativity condition. In that case the ring is called a non-associative ring if associativity doesn't hold!
- From now on, whenever convenient we'll just write AB instead of $A \times B$ to denote the product of two ring elements $A, B \in R$.

Definition (1.1)

A ring $(R, +, \times)$ is called commutative (or abelian) if $AB = BA$ for all $A, B \in R$. Else R is called noncommutative (or non abelian).

Examples of Rings

Which of the following triples are ring?

1. $(\mathbb{Z}, +, \times)$
2. $(2\mathbb{Z}, +, \times)$
3. $(\mathbb{Q}, +, \times)$
4. $(\mathbb{R}, +, \times)$
5. $(\mathbb{C}, +, \times)$

- Which of the examples above are abelian? Are they all abelian rings?

Definition (1.2)

$(R, +, \times)$ is called a ring with multiplicative identity (or just identity) if there exists an element $1 \in R$ such that $1A = A1 = A \ \forall A \in R$.

- Which of the rings above has an identity?

Proposition (1.0)

Let $(R, +, \times)$ be a ring. Then the following identities hold:

1. $A \times 0 = 0$ for all $A \in R$
2. $A \times -B = -A \times B$ for all $A, B \in R$
3. $-A \times -B = A \times B$ for all $A, B \in R$

Proof :

1. Lets first observe that $A \times 0 = A \times (0 + 0) = A \times 0 + A \times 0$. Now because R is a group under $+$ then $A \times 0 = 0$ because 0 is the only element in $(R, +)$ that can satisfy $A \times 0 = A \times 0 + A \times 0$ i.e. 0 is the only element in $(R, +)$ that when added to itself the result remains itself.
   Will leave the remaining proof parts for you as homework challenge!

Definition (1.3)

A ring $(R, +, \times)$ is finite if its underlying set is finite, otherwise it's infinite.

- The rings $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are obviously infinite.
- The set $\mathbb{F}_2 = \{0, 1\}$ with the $+$ and $\times$ tables defined below does form a finite ring. Is it a ring with identity? Also, is it abelian?

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Convention: Sometimes I may just write R instead of $(R, +, \times)$.

Definition (1.4)

Let R be a ring with a multiplicative identity 1. The characteristics of R is defined as $\text{Char}(R) = n$ where n is the smallest positive integer such that $n \times 1 = 0$ where $n \times 1 = 1 + 1 + 1 \ldots + 1$ (sum n times). If no such n exists we say $\text{Char}(R) = 0$

Try figure out what the following characteristics are:

1. $\text{Char}(\mathbb{Z})$
2. $\text{Char}(\mathbb{Q})$
3. $\text{Char}(\mathbb{R})$
4. $\text{Char}(\mathbb{C})$
5. $\text{Char}(\mathbb{F}_2)$

Definition (1.5)

Let R be a ring and let $S \subseteq R$. We say S is a subring of R if S is also a ring under the same binary operations as R.

Integral Domains

Definition (1.6)

Let R be an abelian ring with a multiplicative identity 1. R is an integral domain if $ab = 0$ if only if $a = 0$ or $b = 0$.

Which of the following rings are integral domains?

- $\mathbb{Z}$
- $\mathbb{Q}$
- $\mathbb{R}$
- $\mathbb{C}$
- $\mathbb{F}_2$
- $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ where $+$ and $\times$ are mod4 operations.

2 x 2 Complex Matrix Ring

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

- With the above rules, we can prove that $M_2(\mathbb{C})$ is a ring with identity $1 = \mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Is it an integral domain?

Properties of $M_2(\mathbb{C})$

- $M_2(\mathbb{C})$ is of course a non abelian ring i.e. $AB = BA$ doesn't hold for all $A, B \in M_2(\mathbb{C})$. 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 $BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.
- Three special elements of $M_2(\mathbb{C})$ that are very important in quantum mechanics are the Pauli matrices: $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
- $M_2(\mathbb{C})$ is an example of what we call $\mathbb{C}^*$ - algebra! In quantum mechanics, the set of all bounded operators on a Hilbert space forms a special type of $\mathbb{C}^*$ - algebra called von Neumann algebra.

$M_2(\mathbb{C})$ Commutator

Definition (1.8)

Let $A, B \in M_2(\mathbb{C})$. The commutator of A and B is defined as $[A, B] = AB + (-BA)$ or in a less abstract algebra fashion $[A, B] = AB - BA$.

As a homework challenge, verify if the following identities hold:

1. For all $A, B \in M_2(\mathbb{C})$, $[A, B] = 0$ iff A and B commute.
2. $[A, B] = -[B, A]$ for all $A, B \in M_2(\mathbb{C})$.
3. $[A, B + C] = [A, B] + [A, C]$ for all $A, B, C \in M_2(\mathbb{C})$.
4. $[AB, C] = A[B, C] + [A, C]B$ for all $A, B, C \in M_2(\mathbb{C})$.
5. $[A, BC] = B[A, C] + [A, B]C$ for all $A, B, C \in M_2(\mathbb{C})$.
6. $[\alpha A, B] = [A, \alpha B] = \alpha[A, B]$ for all $A, B, C \in M_2(\mathbb{C})$ and $\forall \alpha \in \mathbb{C}$.

- In the advanced module of the course we'll also deal with anti-commutators defined as $\{A, B\} = AB + BA$!

Pauli Matrices Commutator Challenge

Let $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ be the Pauli matrices. Calculate the following commutators:

1. $[\sigma_x, \sigma_y]$
2. $[\sigma_y, \sigma_x]$
3. $[\sigma_x, \sigma_z]$
4. $[\sigma_z, \sigma_x]$
5. $[\sigma_y, \sigma_z]$
6. $[\sigma_z, \sigma_y]$

What Is a Field?

Definition (1.9)

A field is a triple $(F, +, \times)$ satisfying the following axioms:

1. $(F, +, \times)$ is an integral domain
2. Every non-zero element $a \in F$ has a multiplicative inverse a^{-1} i.e. $aa^{-1} = a^{-1}a = 1$

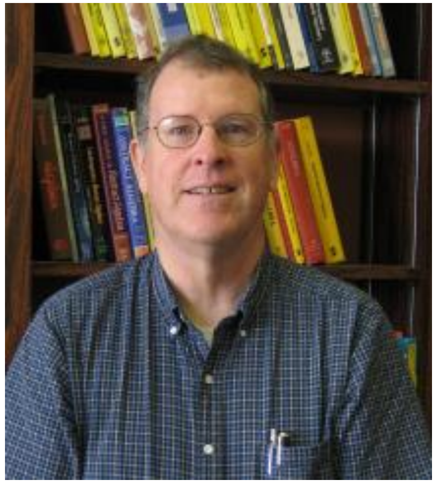
Which of the following integral domains are fields?

1. $\mathbb{Z}$
2. $\mathbb{Q}$
3. $\mathbb{R}$
4. $\mathbb{C}$
5. $\mathbb{F}_2$

- Let p be a prime number and let $\mathbb{F}_p = \{0, ...p - 1\}$. Can $\mathbb{F}_p$ be made into a field? If yes, what is the $\mathrm{Char}(\mathbb{F}_p)$?

Abstract Algebra

Theory and Applications



Prof. Thomas W. Judson

Where should you focus?

Section 16 Rings (*Pages 192 - 208)*

QF

QUANTUM
FORMALISM

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