Lecture 1

22 January 2024 14:00

Ring Theory

This module focusses on the study of rings: a set with two operations (usually called addition and multiplication) satisfying some axioms.

Examples of rings

- $\mathbb{Z}$: the ring of integers.
- $\mathbb{R}$: the ring of real numbers.
- $M_{n\times n}(\mathbb{R})$: the ring of square matrices with real entries.
- $\mathbb{R}[x]$: the ring of polynomials with real coefficients.
- $\mathbb{Z}/n\mathbb{Z}$: the ring of integers modulo n.

By studying properties of general rings, we'll be understanding all rings at the same time.

Formal definition of rings

An ordered pair (a,b) has a "first element" a and a "second element" b. Two ordered pairs (a,b) and (a',b') are equal if and only if $a=a'$ and $b=b'$. (Ex: $(1,2)\neq(2,1)$).

The Cartesian product of two sets A, B is denoted $A\times B$ and consists of all possible ordered pairs (a,b) with $a\in A$ and $b\in B$.

A binary operation on a set A is a function

$$f: A\times A \longrightarrow A.$$

$$f : A \times A \longrightarrow A.$$

__Examples:__

Addition on the set $\mathbb{Z}$ is a binary operation

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$(a, b) \longmapsto \underset{\text{"}+(a,b)\text{"}}{a+b}$$

Multiplication in $\mathbb{Z}$ is another binary operation.

__Example__

Let's think about binary operations on the set

$A = \{0,1\}$ " $=$ " $\{F,T\}$.

- Addition (modulo 2)
- Xor : "Exclusive or"

$0 \oplus 0 = 0 \quad 0 \oplus 1 = 1$

$1 \oplus 0 = 1 \quad 1 \oplus 1 = 0$

(same binary operation as addition!)

- Or $\vee$
- And $\wedge$

$0 \wedge 0 = 0 \quad 0 \wedge 1 = 0 \quad 1 \wedge 0 = 0 \quad 1 \wedge 1 = 1$

(same as multiplication)

$\vdots$

- Nand

$\vdots$

- "First element": $0 \star 0 = 0 \quad 0 \star 1 = 0 \quad 1 \star 0 = 1 \quad 1 \star 1 = 1$

How many binary operations on $A = \{0,1\}$ are there?

We have to specify for each of the four ordered pairs in $A \times A$ what the result of the binary operation is.

We have 2 choices for each pair, so a total of

$2^4 = 16$ choices.

Rings

Definition: A ring is a set R with two binary operations (usually called "addition" and "multiplication") satisfying the following axioms:

- **Axioms for addition**

(A0) Closure law: If $a, b \in R$ then $a + b \in R$.

(A1) Associative law: For $a, b, c \in R$ we have

$$(a+b)+c = a+(b+c)$$

(A2) Zero law: There exists some element $0 \in R$ such that for any $a \in R$

$$a + 0 = a$$
$$0 + a = a.$$

(A3) Negation law: For any $a \in R$ there exists $b \in R$ such that

$$a + b = 0$$
$$b + a = 0.$$

(A4) Commutative law: For any $a, b \in R$ we have

$$a + b = b + a$$

(in other words, $(R, +)$ is an abelian group).

- **Axioms for multiplication:**

(M0) Closure law: If $a, b \in R$ then $a \cdot b \in R$.

(M1) Associative law: If $a, b, c \in R$ then

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

- Mixed axiom:

(D) Distributive law: For any $a, b, c \in R$

$$a \cdot (b+c) = (a \cdot b) + (a \cdot c)$$

$$(b+c) \cdot a = (b \cdot a) + (c \cdot a).$$

Example: The set of non-negative integers $\mathbb{Z}_{\geq 0} = \{0, 1, 2, \dots\}$ is not a ring as there are no additive negatives (does not satisfy (A3)).

Additional "optional" properties:

- A ring with identity is a ring satisfying

  (M2) Identity law: There exists an element $1 \in R$, $\neq 0$ (different from 0), such that for any $a \in R$

$$a \cdot 1 = a$$

$$1 \cdot a = a$$

- A division ring is a ring satisfying

  (M3) Inverse law: For every non-zero $\forall\, a \in R$, $\neq 0$, there is $b \in R$ such that

$$a \cdot b = 1$$

$$b \cdot a = 1$$

- A commutative ring is a ring satisfying

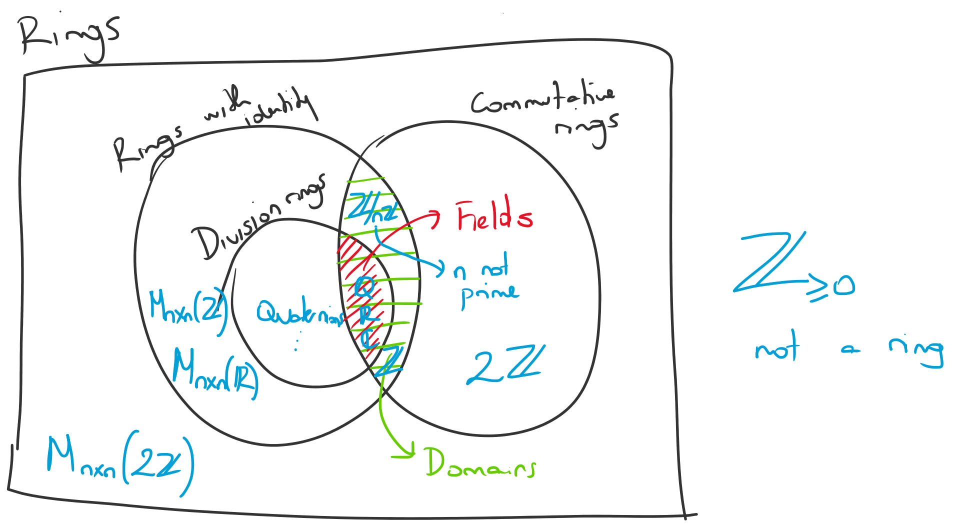
  (M4) Commutative law: For every $a, b \in R$

$$a \cdot b = b \cdot a$$

- A domain is a commutative ring with identity.

- A <u>field</u> is a domain satisfying the inverse law (M3).

Picture



- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields
- $M_{n\times n}(\mathbb{R})$ is a ring with identity, not commutative not a division ring.
- $\mathbb{Z}/n\mathbb{Z}$ is a domain (if n is not prime it is not a division ring)
- $\mathbb{Z}$ is a domain but not a field
- $2\mathbb{Z}$ is a commutative ring without identity
- $M_{n\times n}(2\mathbb{Z})$ is a non-commutative ring without identity
- Quaternions are a division ring (non-commutative).