Lecture 1: Rings

29 August 2020
16:45

Def^n: A ring $(R, +, \cdot)$: R set
$+, \cdot : R \times R \longrightarrow R$ binary operators

satisfying the following axioms

1) $(R, +)$ is a commutative group (with 0_R the additive identity)
2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in R$
3) (i) $a \cdot (b + c) = a \cdot b + a \cdot c$ "
   (ii) $(b + c) \cdot a = b \cdot a + c \cdot a$ "

* R is said to be a ring with identity/unity if $\exists 1_R \in R$ s.t. $a \cdot 1_R = 1_R \cdot a = a \quad \forall a \in R$.

* R is said to be commutative if $\forall a, b \in R$
  $a \cdot b = b \cdot a$.

Examples: 1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $M_{n \times n}(\mathbb{R})$ (Math)

Fields

* A comm ring R is said to be a field if $(R \setminus \{0_R\}, \cdot)$ is a group.

2) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a ring.

3) $R = \{0\}$, the zero ring.

⊛ Ring homomorphism :

A function/map $\varphi : R_1 \to R_2$ is said to be a ring homorphism if φ behaves well with respect to the two binary operators.

i.e. $$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$
$$\forall\, a, b \in R_1 .$$

Example: 1) $\varphi : \mathbb{Z} \to \mathbb{Q}$, $n \mapsto n$ is a ring homo.

$w : \mathbb{Z} \to \mathbb{Q}$, $n \mapsto -n$ Is this a ring homo? No!

$w_1 : \mathbb{Z} \to \mathbb{Q}$, $n \mapsto 2n$ Is this a ring homo?

$\varphi(nm) = 2nm \neq \varphi(n)\varphi(m)$

⊛ Let R_1, R_2 be two rings with unity.
Then a ring homo. $\varphi : R_1 \to R_2$ is additionally required to send 1_{R_1} to 1_{R_2}
i.e. $\varphi(1_{R_1}) = 1_{R_2}$

$n \mapsto (n,0)$

$\mathbb{Z} \to \mathbb{Z}^2 := \{(a,b) \mid a,b \in \mathbb{Z}\}$

$+, \cdot$ $(a_1,b_1)\cdot(a_2,b_2) = (a_1b_1, a_2b_2)$

⊛ Note that $\varphi(0_{R_1}) = 0_{R_2}$ ($\because \varphi$ is a group homo $(R_1,+) \to (R_2,+)$)

⊛ R is a ring with unity$^{(1)}$ then
$-a = -1 \cdot a \quad \forall a \in R$.

Pf: $$\left.\begin{aligned}(a + -1\cdot a) &= (1\cdot a + -1\cdot a) \\ &= (1 + -1)\cdot a \\ &= 0\cdot a = 0\end{aligned}\right\} \Rightarrow -a = -1\cdot a$$

⊛ $M_{n\times n}(\mathbb{R}) \xrightarrow{\det} \mathbb{R}$; Is this a ring homomorphism?

In general $\det(A+B) \neq \det(A) + \det(B)$

Def^n: Let R be a ring with unity. An element $u \in R$ is said to be a unit if $\exists\, u' \in R$ s.t. $u\cdot u' = u'\cdot u = 1_R$.

Ex: 1) Units in $\mathbb{Z}$? $1, -1$. 2) $(\mathbb{Z}/n\mathbb{Z})^\times := \{[a] \mid (a,n) = 1\}$

Euler no $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$

Example : The set of all continuous function from $[0,1] \longrightarrow \mathbb{R}$. $\mathcal{C}[0,1]$ is a ring : $(f+g)(x) = f(x)+g(x)$, /// by multiplication

$$\varphi_{1/5} : \mathcal{C}[0,1] \longrightarrow \mathbb{R}$$ is
$$f \longmapsto f(1/5)$$

ring homo.

$\mathcal{C}[0,1]$ is a ring with unity.

$\mathbb{1}(x) = 1 \quad \forall x \in [0,1]$

$(f \cdot \mathbb{1})(x) = f(x) \cdot 1 = f(x)$

Defⁿ: A ring homo $\varphi: R_1 \to R_2$ is said to be an injective ring homo / a monomorphism if φ is injective.

IIIˡʸ φ is an epimorphism if φ is surjective and φ is an isomorphism if φ is bijective.

* φ is an isomorphism $\Rightarrow$ $\psi := \varphi^{-1}: R_2 \to R_1$ is a homomorphism. And in this scenario R_1 is said to be isomorphic to R_2.

Exercise

* Let $\varphi: R_1 \to R_2$ be a ring homomorphism. Then $\operatorname{Im}(\varphi)$ is a subring of R_2 and $\ker(\varphi)$ is an ideal of R_1. $\operatorname{Im}(\varphi) = \{\varphi(x) \mid x \in R_1\}$ $\ker(\varphi) = \{x \in R_1 \mid \varphi(x) = 0\}$

Defⁿ: Let $(R, +, \cdot)$ be a ring and $R_1 \subseteq R$. We say R_1 is a subring of R if $(R_1, +, \cdot)$ is ring.
i.e. $\forall a, b \in R_1$, $a+b \in R_1$, $a \cdot b \in R_1$ and $-a \in R_1$.

Ex: $\mathbb{Z}$ is a subring of $\mathbb{Q}$. $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

$2\mathbb{Z} \subseteq \mathbb{Z}$ is subring
is not a ring with unity

* In $\mathbb{Z}^2$, the set $\underbrace{\{(n,0) \mid n \in \mathbb{Z}\}}_{= R_1}$ is a subring
$1_{R_1} \neq (1,1) = 1_{\mathbb{Z}^2}$

* $1_R \in R_1 \Rightarrow 1_{R_1} = 1_R$

with unity

(commutative)

Def^n: Let R be a ring. A subset $I \subseteq R$ is said to be an <u>ideal</u> of R if

(1) $\forall a, b \in I$, $a+b \in I$

(2) $\forall a \in I$ & $\forall r \in R$, $ra \in I$ ← left ideal

(2') $\forall a \in I$ & $\forall r \in R$, $ar \in I$ ← right ideal

Prop: Kernel of a ring homo. is an ideal.

Pf: $\varphi : R_1 \to R_2$ be a ring homo.

$a, b \in \ker(\varphi)$ then $\varphi(a+b) = \varphi(a) + \varphi(b) = 0$

$r \in R_1$ & $a \in \ker\varphi \Rightarrow \varphi(ra) = \varphi(r)\varphi(a) = 0$ ∎

Example: Ideals of $\mathbb{Q}$ 1) $\{0\} \subseteq \mathbb{Q}$ is an ideal

zero ideal $\longrightarrow \{0\}$ is always an ideal in any ring

2) $\mathbb{Q}$ is an ideal of $\mathbb{Q}$

R is always an ideal of any ring R.

⊛ These are all the ideals of $\mathbb{Q}$.

Pf: $I \subseteq \mathbb{Q}$ be a nonzero ideal. $\Rightarrow \exists\, a \neq 0$ s.t. $a \in I$, $a \in \mathbb{Q}$

Let $b \in \mathbb{Q}$ then $\frac{b}{a} \in \mathbb{Q}$ & $\frac{b}{a} \cdot a = b \in I \Rightarrow I = \mathbb{Q}$.

⊛ Let $(F, +, \cdot)$ be a field then the only ideals of F are (0) & F.

Pf: I nonzero ideal F, let $\underset{\neq 0}{a} \in I$ then $a^{-1} \in F$. Let $b \in F$ then $ba^{-1} \in F \Rightarrow \underbrace{ba^{-1} \cdot a}_{b} \in I$ ∎

Ex: In $\mathbb{Z}$, what are the ideals?

(0), $\mathbb{Z}$, $n\mathbb{Z}$

Text books: 1) Dummit & Foote

2) M. Artin

3) S. Lang