Rings and Fields (I)

Wednesday, 2 March 2022 15:05

Rings: Algebraic structures w/ both + and $\cdot$ $\mathbb{Z}$

Def: A ring $(\underbrace{R}_{\text{set}}, \underbrace{+, \cdot}_{\text{binary op}}, \underset{R}{0 \in})$

(1) $(R, +, 0)$ is an abelian group

(2) $\cdot$ is associative $a\cdot(b\cdot c) = (a\cdot b)\cdot c$

(3) Distributive law, $\forall a,b,c \in R$

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

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

Examples: (a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

(b) $n\mathbb{Z}$ $nr + ns = n(r+s)$

$(nr)\cdot(ns) = n(nrs)$

(c) $\mathbb{Z}_n$ $n=10$, $3\cdot 7 = 21 = 1 \in \mathbb{Z}_{10}$

Multiplication is well-defined:

$a \cdot b$ $a' = a$ in $\mathbb{Z}_n$

$b' = b$ " "

$a' = a + nx$, $b' = b + ny$

$$a'b' = (a+nx)(b+ny)$$
$$= ab + nxb + any + nxny$$
$$= ab + n(xb + ay + nxy)$$
$$= ab \text{ in } \mathbb{Z}_n$$

(d) $\{ f : \mathbb{R} \to \mathbb{R} \}$ is a ring

$(f+g)(a) = f(a) + g(a) \quad \forall a \in \mathbb{R}$

$(fg)(a) = f(a)g(a)$

Continuous fcns, differentiable fcns.

(e) R ring, $R[x] :=$

$\{ a_0 + a_1 x + \dots + a_d x^d : a_i \in R \}$.

$$(a_0 + \dots + a_d x^d) + (b_0 + \dots + b_d x^d)$$
$$= (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_d + b_d)x^d$$
$$(a_0 + \dots + a_d x^d) \cdot (b_0 + \dots + b_d x^d)$$
$$= a_0 b_0 + (a_1 b_0 + a_0 b_1)x$$
$$+ (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \dots + (a_d b_d) x^{2d}$$

(f) R ring, $M_n(R) := \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} : a_{ij} \in R \right\}$

"Usual $+$ and $\cdot$"

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

Even if R is commutative, $M_n(R)$ might not be commutative

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Prop: (1) $0a = a0 = 0$

(2) $a(-b) = (-a)b = -(ab)$

(3) $(-a)(-b) = ab$

$-x$: inverse w.r.t. $+$, x^{-1}: inverse w.r.t. $\cdot$ (if exists)

Proof: (1) $a0 + a0$

$$= a(0+0)$$

$$= a0 = a0 + 0$$

$$\Rightarrow a0 = 0$$

(2)

$$a(-b) + ab$$

$$= a((-b)+b)$$

$$= a0 \overset{(1)}{=} 0$$

$a(-b) = -(ab)$

(3)

$$(-a)(-b) + (-(ab))$$

$$\overset{(2)}{=} (-a)(-b) + (-a)b$$

$$= (-a)((-b)+b)$$

$$\overset{(1)}{=} (-a)0 = 0$$

$(-a)(-b) = ab$

$\square$

Def: If $\cdot$ is commutative (i.e. $a \cdot b = b \cdot a$), then R is a <u>commutative ring</u>.

A multiplicative identity (if exists) is denoted by 1,
($\text{i.e. } 1a = a1 = a, \ \forall a \in R$)
and is called unity.

A ring that has 1 is a ring with unity.

Example: • $\mathbb{R}[x]$ has the unity 1 $(+0x+0x^2+\ldots)$
• $2\mathbb{Z}$ has no unity.

Prop: The unity is unique (if exists).

Proof: Same as the identity is unique in a group. $\square$

Prop: If $1=0$, then $R=\{0\}$

Proof: $\forall x \in R$, $x = x1 = x0 = 0$ $\square$ (Safe to assume $0 \neq 1$)