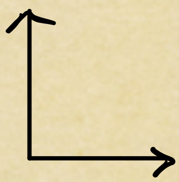
Day 19 July 1, 2024

Idea: Rings are "coefficient systems"

e.g., what arrows can we build from



? The answer depends on the coefficient system.

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}^2, \mathbb{Z}_3, \ldots$

<u>Def</u>. A **ring** is a triple $(R, +, \cdot)$, where $R \neq \emptyset$ is a set and $+, \cdot : R \times R \to R$ are binary operations s.t.

1. $(R, +)$ is an abelian group;
2. $\cdot$ is associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $\forall\, a, b, c \in R$;
3. $\cdot$ distributes over $+$:
$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$\text{\& } (a + b) \cdot c = a \cdot c + b \cdot c,$$
$\forall\, a, b, c \in R$.

Call the add. ident. 0

- We call R a **ring with unity** if $\exists\, 1 \neq 0 \in R$ s.t. $1a = a = a1$, $\forall\, a \in R$.
- We call R a **commutative ring** if $\cdot$ is commutative.
- If $a, b \in R$ are nonzero elements s.t. $ab = 0$, then each of a, b is a **zero divisor**.

- An integral domain is a commutative ring with unity which contains no zero divisors.
- A unit of a ring with unity is a nonzero elt. $a \in R$ s.t. $\exists!\ a^{-1} \in R$ s.t. $aa^{-1} = a^{-1}a = 1$.
- A division ring is a ring with unity where every nonzero elt. is a unit.
- A field is a commutative division ring.

$$\begin{tikzcd}
 & \text{ring} \quad 2\mathbb{Z} & \\
\mathbb{Z}_6 \quad \text{commutative ring} \arrow[ur] & & \text{ring with unity} \quad \mathbb{Z}_6, M_{n\times n}(\mathbb{R}) \arrow[ul] \\
\mathbb{Z} \quad \text{integral domain} \arrow[u] \arrow[urr] & & \text{division ring} \quad \mathbb{H} = \mathbb{R}\langle 1, i, j, k \rangle \arrow[u] \\
 & \text{field} \quad \mathbb{Q}, \mathbb{R}, \mathbb{C} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

NTS: fields don't have zero divisors

$ij = k = -ji$

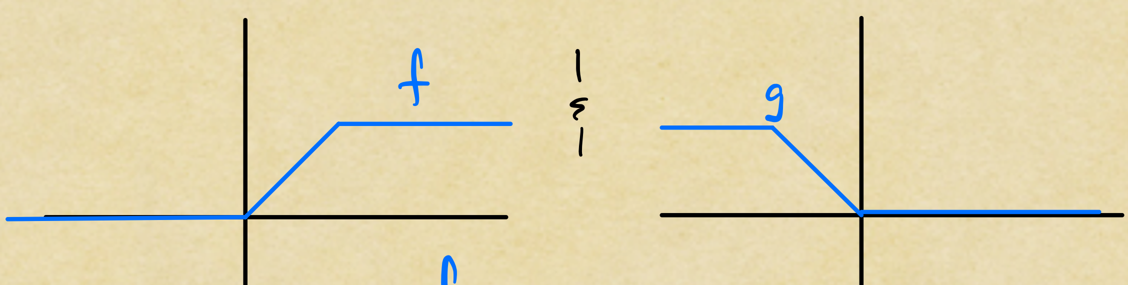
$jk = i = -kj$

$ki = j = -ki$

$i^2 = j^2 = k^2 = -1$

Ex ① $C^0(\mathbb{R}) = \{\text{cts functions } \mathbb{R} \to \mathbb{R}\}$ is a ring under pointwise addition & multiplication.

Not an ID:



$fg = 0$

② We'll denote by $\mathbb{Z}[x]$ the collection of polynomials in x with integer coefficients. (Usual operations on polynomials.)

Claim: This is an I.D. So is $\mathbb{R}[x]$.

R an I.D.

$\Updownarrow$

$R[x]$ an I.D.

$\frac{1}{x} \notin \mathbb{R}[x]$

So not a field.

③ $M_{n \times n}(\mathbb{R})$ is a non-comm. ring with unity which is not a division ring

④ The set

$$\mathbb{Z}[i] := \{m + ni \mid m, n \in \mathbb{Z}\},$$

with operations as in $\mathbb{C}$, forms a ring known as the Gaussian integers.

Check: I.D., but not a field.

Properties & subrings

Prop. Let R be a ring and pick $a, b \in R$. Then

① $a0 = 0a = 0$;

② $a(-b) = (-a)b = -ab$;

③ $(-a)(-b) = ab$.

(Proof.) Exercise. ∎

Def. A subring of $(R, +_R, \cdot_R)$ is a ring $(S, +_S, \cdot_S)$ s.t. S is a subset of R and the operations $+_S$ & $\cdot_S$ are restrictions of $+_R$ & $\cdot_R$.

Prop. Let R be a ring, S a subset of R. Then S is a subring of R iff:

1. $S \neq \emptyset$;
2. $rs \in S$, $\forall r, s \in S$;
3. $r - s \in S$, $\forall r, s \in S$.

(Proof.) Exercise. ∎

Ex. Let $R = M_{2\times 2}(\mathbb{R})$ and let

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \, a, b, c \in \mathbb{R} \right\} \subseteq R.$$

Then T is a subring.

Integral domains

Prop. Let D be a commutative ring with unity. Then D is an integral domain iff $ab = ac$ implies $b = c$, whenever $a \neq 0$, $\forall a, b, c \in D$.

(Proof.) Exercise. ∎

Thm [Wedderburn's Theorem] Every finite integral domain is a field.

Ex. $\mathbb{Z}_p$ is an I.D. $\Rightarrow$ in fact, a field

(Proof.) Let D be a finite I.D. and let

$D^\times := D - \{0\}$.

For each $a \in D^\times$, we have $\lambda_a : D^\times \longrightarrow D^\times$.

$$d \longmapsto ad$$

B/c D is an I.D., $ad \neq 0$, so $ad \in D^\times$.

Note that λ_a is injective: prev. prop.

$$\lambda_a(d_1) = \lambda_a(d_2) \Rightarrow ad_1 = ad_2 \Rightarrow d_1 = d_2.$$

B/c $D^\times$ is finite, λ_a injective $\Rightarrow$ λ_a surjective.

In particular, $\exists\, d \in D^\times$ s.t. $\lambda_a(d) = 1$.

i.e., $ad = 1$, so d is a multiplicative inverse for a.

This works for every $a \in D^\times$, so D is a commutative division ring. $\blacksquare$