Rings.

<u>Defn:</u> A <u>ring</u> R is a set with two binary operations $+, \cdot$ (addition and multiplication)

$$\begin{pmatrix} + : R \times R \longrightarrow R \\ \cdot : R \times R \longrightarrow R \end{pmatrix}$$

s.t.

① $(R, +)$ is an <u>abelian group</u>

i.e. • $\exists!\ 0 \in R$ s.t. (Additive Identity)

$\forall a \in R \quad a + 0 = 0 + a = a$

• $\forall a \in R,\ \exists!\ (-a) \in R$ s.t. (Additive Inverses)

$$a + (-a) = (-a) + a = 0$$

• $\forall a, b, c \in R \quad (a+b) + c = a + (b+c)$ (Associativity)

• $\forall a, b \in R \quad a + b = b + a.$ (Commutative)

② $\cdot$ is <u>associative</u>, i.e.

$\forall a, b, c \in R$

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

(3) $\cdot$ distributes over $+$, i.e.

$$\forall a,b,c \in R$$
$$a\cdot(b+c) = a\cdot b + a\cdot c$$

we say R has an identity element, 1_R

if (4) $\exists\ 1_R \in R$ s.t.

$$\forall a \in R, \quad a\cdot 1_R = 1_R \cdot a = a$$

we say R is commutative if

(5) $\forall a,b \in R \quad a\cdot b = b\cdot a$

If R is a comm. ring w/ $1 \neq 0$

then we say R is a field if

(6) $\forall a \neq 0 \in R,\ \exists\ a^{-1} \in R$ s.t.

$$a\cdot(a^{-1}) = (a^{-1})a = 1$$

Examples:

(0) $(\mathbb{Z}, +, \cdot)$ is a ring

(1) $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$, $(\mathbb{Q},+,\cdot)$ are fields.

② "Non-example" $(\mathbb{N}, +, \cdot)$ is not a ring

(not even a group b/c there are no additive inverses)

③ "Non-example" $\mathbb{R}^3$ is not a ring

$\mathbb{R}^3$ has addition (if $\vec{v}, \vec{w} \in \mathbb{R}^3$, $\vec{v}+\vec{w} \in \mathbb{R}^3$)

BUT no multiplication.

((Exercise: Cross-product does not work!))

<u>Defn</u>: We say $a \in R$ is a <u>unit</u> if

$$\exists\, b \in R \text{ s.t. } a \cdot b = b \cdot a = 1.$$

<u>Example</u>: In $\mathbb{R}$, every element except 0 is a unit.

In $\mathbb{Z}$, $\{1, -1\}$ are the units

<u>Example 4</u>: $\mathbb{Z}/n\mathbb{Z}$

$$n\mathbb{Z} := \{ n \cdot a \mid a \in \mathbb{Z} \}$$

$$\mathbb{Z}/n\mathbb{Z} := \mathbb{Z}/\sim \qquad x, y \in \mathbb{Z},\ x \sim y \text{ iff } x - y \in n\mathbb{Z}$$

$$= \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \ldots, \overline{n-1} \}$$

If $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ say $a \in \bar{a}$, $b \in \bar{b}$

then we define

$$\bar{a} + \bar{b} = \overline{a+b}, \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

Exercise: This is well-defined.

Example 5 Rings of functions

Let R be a ring, X a set

Define $\mathcal{F} := \{ f : X \to R \}$

$$(f+g) : X \to R, \quad x \mapsto f(x) + g(x) \qquad , \; (f \cdot g) : X \to R, \quad x \mapsto f(x) \cdot g(x)$$

Example 6:

$$C[0,1] := \{ f : [0,1] \to \mathbb{R} \mid f \text{ continuous} \}$$

Fact from calculus: $f+g$, $f \cdot g$ are continuous

$\Longrightarrow$ $C[0,1]$ is a ring.

Example: Matrix rings.

$M_n(\mathbb{R}) := \{n \times n \text{ matrices w/ real coefficients}\}$

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ \vdots & & & & \vdots \\ a_{n1} & \cdots & & & a_{nn} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} & b_{13} & \cdots & b_{1n} \\ \vdots & & & & \vdots \\ b_{n1} & \cdots & & & b_{nn} \end{pmatrix}$$

$$A + B := \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{11} \\ \vdots & & & \vdots \\ a_{n1}+b_{n1} & \cdots & & a_{nn}+b_{nn} \end{pmatrix}$$

$$A \cdot B = (a_{ik} \cdot b_{kj})$$

$0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ is additive identity

$1 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ is multiplicative identity.