Rings and Fields:

Working with two binary operations $+, \cdot$

Def: A ring R is a set with binary operations $+, \cdot$ where

- $(R,+)$ is an abelian group
- $\cdot$ is associative $(a\cdot b)\cdot c = a\cdot(b\cdot c)$
- left and right distributivity: $a\cdot(b+c) = a\cdot b + a\cdot c$
  $(b+c)\cdot a = b\cdot a + c\cdot a$

We will usually write ab instead of $a\cdot b$

Since R is an abelian group, it has an additive identity 0_R. This is called the zero of R.

David's comment: also have $-r$ for all $r\in R$.

Ex: $\mathbb{Z}$ is a ring w/ usual addition and multiplication

$\mathbb{Z}_n$ is also a ring w/ modular addition and modular multiplication

Ex: $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in \mathbb{Z} \right\}$ $\left(M_2(\mathbb{Z}) \right)$

matrix addition and matrix multiplication

Ex: $R = \{ f(x,y) \mid f(x,y) \text{ polynomial in } x \text{ and } y \}$

w/ usual addition + multiplication

Ex: $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ are all rings too!

Ex: X topological space

$C(X;\mathbb{R}) = \{ f: X\to\mathbb{R} \mid f \text{ continuous} \}$

with operations $(f+g): x \mapsto f(x)+g(x)$ $(fg): x\mapsto f(x)g(x)$

Properties of rings:

- a ring R is **commutative** if $\cdot$ is commutative
- a ring R is a **ring with identity** if it has a multiplicative identity 1_R
- a ring R is a **division ring** or (**skew-field**) if every nonzero $r \in R$ has a multiplicative inverse. NOTE: this only makes sense if R has identity

  $r \cdot r^{-1} = 1_R$
- Super duper special case: a commutative division ring is called a **field**.

Ex: the zero ring $R = \{0\}$ has binary operations $0+0=0$ $\quad 0 \cdot 0 = 0$.

NOTE: $1_R = 0_R = 0$.

As we have defined rings, they might not have multiplicative identities!!

Ex: $R = \{ f : \mathbb{R} \to \mathbb{R} \mid \int |f(x)|^2 \, dx < \infty \}$

Hilbert space!!

If $f, g \in R$ then $fg : x \mapsto f(x)g(x)$ is in R

$f+g : x \mapsto f(x)+g(x)$ is in R.

This is a ring!

There is no identity!! The identity would have to be $f(x) = 1 \;\; \forall x$

but $\int_{-\infty}^{\infty} |1|^2 \, dx = \infty$. so it's not in R.

Ex: $R = \mathbb{Z}_3, +$

Special multiplication: $a \cdot b = 0 \quad \forall a, b \in \mathbb{Z}_3$

associative + distributive

Many authors <u>define</u> rings to have identity by def!

<u>Ex</u>: $\mathbb{Z}$ not a field! 2^{-1} is not an integer

$\mathbb{Q}$ is a field!

$\mathbb{R}$ is a field $\quad \mathbb{C}$ is a field!

$\mathbb{Z}_p$ for prime p is a field

<u>Theorem</u>: $\mathbb{Z}_p$ is a field

<u>Proof</u>: $\mathbb{Z}_p$ is a commutative ring w/ identity so we just need to show that if $a \in \mathbb{Z}_p$ and $a \neq 0$, then a has a multiplicative inverse.

Look at the subgroup $\langle a \rangle \leq \mathbb{Z}_p$

$|\langle a \rangle| \neq 1$ and $|\langle a \rangle| \mid p \Rightarrow |\langle a \rangle| = p$

$\Rightarrow \langle a \rangle = \mathbb{Z}$

$\Rightarrow 1 \in \langle a \rangle$

$\langle a \rangle = \{ ka \mid k \in \mathbb{Z} \}$ so $1 = ka$

Thus $a^{-1} = k$.

$\square$

<u>Ex</u>: $Q = \{ ai + bj + ck + d \mid a, b, c, d \in \mathbb{R} \}$

i, j, k are formal symbols satisfying

$i^2 = -1, \; j^2 = -1, \; k^2 = -1, \; ijk = -1 \quad \star$

This is an example of a noncommutative division ring (skew-field) called the <u>quaternions</u>.

$ijk = -1 \Rightarrow ijk^2 = -k \Rightarrow -ij = -k$

$\Rightarrow ij = k$

$\underline{ij(ij - ji)} = ijij - ijji = ijij - i(-1)i$

$= ijk + i^2 = -1 + -1 = -2$

$\Rightarrow \quad ij - ji \neq 0 \qquad$ so $\quad ij \neq ji$.

<u>Def</u>: A <u>subring</u> S of a ring R is a subset of R which is also a ring under the binary operations $+, \cdot$. If R is a field and S is also a field, we call S a <u>subfield</u>.

Homomorphisms

<u>Def</u>: Let R, S be rings. A <u>ring homomorphism</u> $f: R \to S$ is a function which satisfies

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

Many authors also force R, S to have identities $1_R, 1_S$ and also force $f(1_R) = 1_S$.

<u>Ex</u>: $\quad R = \mathbb{R} \qquad S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \ a, b, c, d \in \mathbb{R} \right\}$

$1_R = 1 \qquad\qquad 1_S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$f: R \to S$$
$$a \longmapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

$$f(a+b) = \begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix}, \qquad f(ab) = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$$

$$\shortparallel \qquad\qquad\qquad\qquad \shortparallel$$

$$f(a) + f(b) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}, \qquad f(a) f(b) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$$

f is a ring homomorphism.

$$f(1_R) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq 1_S$$

For groups or rings or fields:

monomorphism = injective homomorphism

epimorphism = surjective homomorphism

isomorphism = bijective homomorphism

Ex: $f: \mathbb{Z} \to \mathbb{Z}_3$

$k \mapsto k \bmod 3$

ring epimorphism

Ex: $f: \mathbb{R} \to M_2(\mathbb{R})$

$a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ ring monomorphism

Def: The kernel of a ring homomorphism $f: R \to S$ is

$$\ker(f) = \{ r \in R \mid f(r) = 0_S \}$$

NEXT TIME:

Ex: $M_2(\mathbb{R})$ has zero divisors

$A, B \in M_2(\mathbb{R})$ with $A \neq 0$, $B \neq 0$ but $AB = 0$

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$