FUNCTIONS

DEF Given two sets A, B, a **function** f from A to B is a subset of

$$A \times B := \{(a,b) : a \in A,\ b \in B\}$$

satisfying: for all $a \in A$, there is a unique element of $f \subseteq A \times B$ whose first coordinate is a.

MORE TYPICAL: A function $f: A \to B$ is a rule that assigns to each element $a \in A$ a unique el't $f(a) \in B$.

$f(x)$: **image** of x under f

$f^{-1}(b) := \{a \in A : f(a) = b\}$: **preimage** of b (under f)

↑ f^{-1} is not always a function!

$f: A \to B$

A: **domain** $\qquad$ B: **codomain**

$f(A) := \{b \in B : f(a) = b$ for some $a \in A\}$:

image (of A) or **range**

If $f: A \to B$ and $g: A \to B$, then

$f = g$ means $f(a) = g(a)$ for all $a \in A$.

If $S \subseteq A$, then $f_S: S \to B$ is the restriction of f to S, where

$f_S(x) = f(x)$ for all $x \in S$.

If $g: A \to B$ and $f: B \to C$, then

$f \circ g(x) := f(g(x))$ composition

PROP (Function composition is associative)

Given $f: A \to B$, $g: B \to C$, $h: C \to D$,

then $h \circ (g \circ f) = (h \circ g) \circ f$

Pf: HW

DEF A "function" is well-defined if it actually satisfies the definition of being a function: each element of the domain

is assigned to exactly one element of the codomain.

NOTE This is really important when the "elements" of the domain are sets and exactly where the "element" is sent depends on a (noncanonical) choice of representative.

EX Let $\mathcal{E}$ be the set of all even integers, $\mathcal{O}$ the set of odd integers.

$\{\mathcal{E}, \mathcal{O}\}$ is a partition of $\mathbb{Z}$

Given $x \in \mathbb{Z}$, $[x]$ denotes the equivalence class $(\mathcal{E}$ or $\mathcal{O})$ containing x.

Define two "rules":

$f: \{\mathcal{E}, \mathcal{O}\} \longrightarrow \mathbb{Z}$ by $f([x]) = x^2$

$g: \{\mathcal{E}, \mathcal{O}\} \longrightarrow \mathbb{Z}$ by $g([x]) = (-1)^x$

Are these well-defined?

f is not well-defined.

For instance, since $\mathcal{E} = [0] = [2] = \dots$,

$$f(\mathcal{E}) = f([0]) = 0^2 = 0$$

but $$f(\mathcal{E}) = f([2]) = 2^2 = 4$$

Is $g : \{\mathcal{E}, \mathcal{O}\} \to \mathbb{Z}$ by $g([x]) = (-1)^x$ well-defined? YES.

Regardless of choice of representative,

$$g(\mathcal{E}) = g([2j]) = (-1)^{2j} = 1 \qquad j \in \mathbb{Z}$$

$$g(\mathcal{O}) = g([2k+1]) = (-1)^{2k+1} = -1 \qquad k \in \mathbb{Z}$$

DEF A function $f : A \to B$ is injective (or one-to-one) if, for all $x, y \in A$,

$$f(x) = f(y) \Rightarrow x = y$$

(equivalently: $x \neq y \Rightarrow f(x) \neq f(y)$, so different elements of A are assigned to different elements of B)

DEF A function $f : A \to B$ is <u>surjective</u> (or <u>onto</u>) if, for all $b \in B$, there exists $a \in A$ such that $f(a) = b$.

(for every $b \in B$, something in A is assigned to b; $f(A) = B$, range = codomain)

DEF A function $f : A \to B$ is <u>bijective</u> if it is both injective and surjective.

(intuition: the elements of A are "matched" w/ elements of B; these sets have the "same size")

FIELDS

DEF A <u>binary operation</u> on a set S is a function from $S \times S$ to S.

EX $+$, $\cdot$ in $\mathbb{R}$

$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ where, for example, $+ : (3, 4.27) \mapsto 7.27$

$3 + 4.27 = 7.27$

$\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ where, for example,

$\cdot : (3, 4.27) \longmapsto 12.81$

$3 \cdot 4.27 = 12.81$

DEF A <u>field</u> is a set $\mathbb{F}$ equipped with two binary operations, $+$ and $\cdot$, satisfying, for all $a, b, c \in \mathbb{F}$:

(F1) (COMMUTATIVITY OF ADDITION AND MULTIPLICATION)

$a + b = b + a$ and $ab = ba$

(we'll often denote $a \cdot b$ by ab)

(F2) (ASSOCIATIVITY OF ADDITION AND MULTIPLICATION)

$a + (b + c) = (a + b) + c$ and $a(bc) = (ab)c$

(F3) (IDENTITY ELEMENTS)

There exist elements $0, 1 \in \mathbb{F}$ such that, for all $a \in \mathbb{F}$, $a + 0 = a$ and $a \cdot 1 = a$

(0: additive identity; 1: multiplicative identity)

(F4) (INVERSE ELEMENTS) For every $a \in F$ and each nonzero $b \in F$, there exist elements $c, d \in F$ such that

$$a + c = 0 \quad \text{and} \quad b \cdot d = 1$$

(c: additive inverse of a; d: multiplicative inverse of b)

(F5) (DISTRIBUTIVE LAW)

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

EX $\mathbb{R}$, set of real numbers. Field?

Comm.? YES. $a+b = b+a$, $ab = ba$

Assoc.? YES. $a+(b+c) = (a+b)+c$,

$a(bc) = (ab)c$

Identities? YES. $0, 1$

Inverses? YES. If $x \in \mathbb{R}$, $-x$ is its additive inverse:

$$x + (-x) = 0$$

If $y \in \mathbb{R}$, $y \neq 0$, then

$y^{-1} = \frac{1}{y}$ is its mult. inverse:

$$y \cdot \frac{1}{y} = 1$$

Dist.? YES. $a(b+c) = ab+ac$.

So $\mathbb{R}$ is a field (w/ ops $+, \cdot$)

EX $\mathbb{Z}$, the integers, w/ operations $+, \cdot$

Field?

NO. We don't have multiplicative inverses!

No $x \in \mathbb{Z}$ such that $2x = 1$

FIX: $\mathbb{Q}$, rational numbers

$$\mathbb{Q} := \left\{ \frac{m}{n} : m, n \in \mathbb{Z},\ n \neq 0 \right\}$$

is a field.