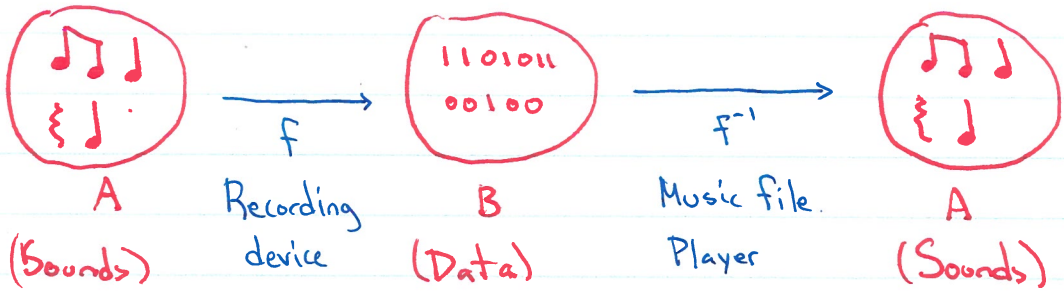
Last time: Suppose that f is a function from a set A to a set B.
We want to create a function which "undoes" f.

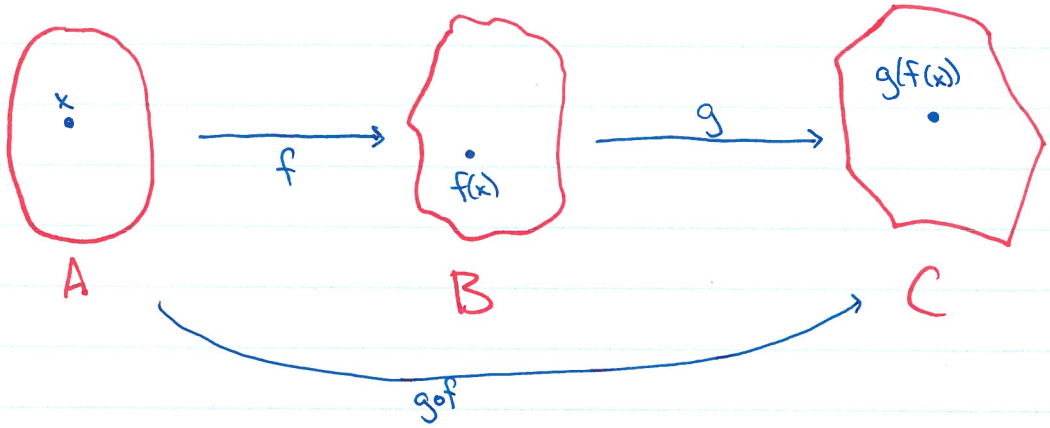
Example: Recording music / sound



We saw last time that this can only be done for certain functions f.
Before we make that precise, let's define...

Composition of functions:

Let A, B, and C be sets. Let $f: A \to B$ and $g: B \to C$ be functions.



The composite, $g \circ f$, is a function from $A \to C$ given by first applying f, then applying g.

Ex: $A = \{\text{Sounds}\}$, $B = \{\text{Data}\}$, f is a recording device.
$B = \{\text{Data}\}$, $C = \{\text{Pictures}\}$, g is image rendering software.
Then $f \circ g$ takes music and converts it into a (possibly meaningless) picture

Notation: The expression "gof" means to do the rightmost function first.

Warning: $g \circ f \neq f \circ g$. In this case $f \circ g$ would not even make sense unless A and C are the same set!

Proposition: In the situation above,

(i) • If f and g are both injective, then $g \circ f$ is injective.

(ii) • If f and g are both surjective, then $g \circ f$ is surjective.

Consequently, if f and g are both bijective, then so is $g \circ f$.

Pf: (i) Suppose that f and g are both injective.

Let $a_1, a_2 \in A$ such that $g(f(a_1)) = g(f(a_2))$. (Notation: $g(f(a)) = (g \circ f)(a)$)

Since g is injective, it follows that $f(a_1) = f(a_2)$

Since f is injective, it follows that $a_1 = a_2$.

Thus, $g(f(a_1)) = g(f(a_2)) \Rightarrow a_1 = a_2$. So the function $g \circ f$ is injective.

(ii) Suppose that f and g are both surjective.

Let $c \in C$. Since g is surjective, there is some $b \in B$, $g(b) = c$.

Since f is surjective, there is some $a \in A$, $f(a) = b$

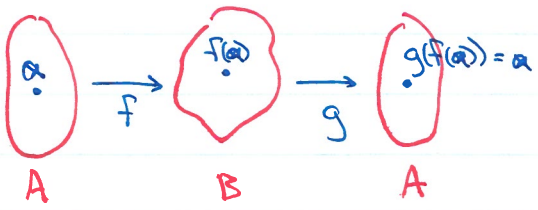
Then $g(f(a)) = g(b) = c$.

We have shown $\forall c \in C, \exists a \in A, g(f(a)) = c$.

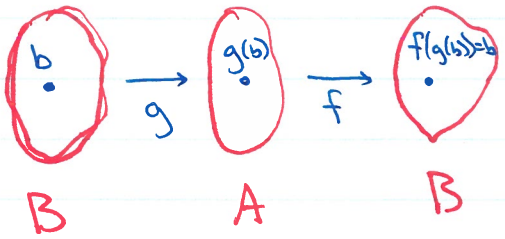
So $g \circ f : A \to C$ is surjective.

Inverse of a function: Let $f: A \to B$ be a function. Suppose that $g: B \to A$ is another function.

Def: We say that g is a "left inverse" to f if $\forall a \in A, (g \circ f)(a) = a$ (Equivalently, if $g \circ f = id_A$, the "identity function from A to A.")



Def: We say that g is a "right inverse" to f if $\forall b \in B, (f \circ g)(b) = b$ (Equivalently, if $f \circ g = id_B$.)

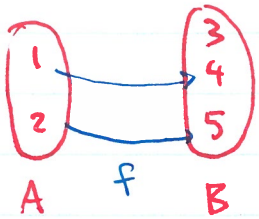


Def: If g is simultaneously a left- and right-inverse of f, then we simply call it the inverse of f.

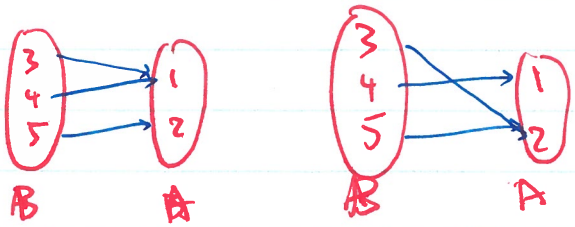
Question: Let $f: A \to B$ be a function. What condition must be true for it to have a left inverse?

A: The preimage of every $b \in B$ has at most one element. I.e., f is injective.

Example:



The function f has two possible left inverses, g_1 and g_2.



Similarly, f has a right inverse $\Leftrightarrow$ f is surjective.
(It could have multiple possible right inverses!)

Prop: f has an inverse $\Leftrightarrow$ f is bijective.
If there is an inverse, then it is unique.

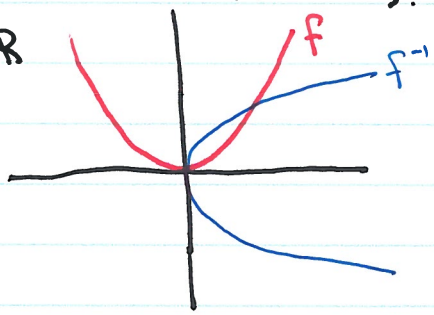
Another perspective: inverse relations.

Def: Let f be a relation from A to B. (ie, f is just a subset of $A \times B$.)

The inverse relation is a relation from B to A and is denoted f^{-1}. It is defined by

$$f^{-1} = \{(b,a) \mid (a,b) \in f\}.$$

Ex: $A = B = \mathbb{R}$



Prop: The relation $f^{-1} \subseteq B \times A$ is a function iff f is bijective.
In this situation, f^{-1} is the inverse function of f,
ie. $f^{-1} \circ f = id_A$ and $f \circ f^{-1} = id_B$.

Exercise: Let $f: A \to B$ and $g: C \to D$ be functions. Let $f \times g: A \times C \to B \times D$.

- Prove that if f and g are both injective, then so is $f \times g$. (Warmup)
- Come up with an example where $f \times g$ is injective, but f is not. (Hint: let one of the sets be $\emptyset$.)

Exercise: Let $f_1: A \to B$, $f_2: A \to B$, $g: B \to C$

- Come up with such a scenario where $f_1 \neq f_2$, but $g \circ f_1 = g \circ f_2$.
- Prove that if g is injective, then $g \circ f_1 = g \circ f_2 \Rightarrow f_1 = f_2$.

Def: Let R be an equivalence relation on A. Then A/R denotes the set of equivalence classes.

Example: $A = \mathbb{Z}$, $R =$ "congruent modulo n". Then $A/R = \{[0], [1], \ldots, [n-1]\}$

Exercise: Let $f: A \to A/R$ be the function $f(a) = [a]$.

- Prove that f is surjective.
- Suppose f is injective. Then what can you conclude about R?

Exercise: For every $n \in \mathbb{N}$, let

$$\mathbb{Z}_n = \text{the set of equivalence classes of } \mathbb{Z} \text{ with respect to "congruent mod } n\text{"}$$
$$= \{[0], [1], \ldots, [n-1]\}$$

Consider the function $f: \mathbb{Z}_5 \to \mathbb{Z}_5$, defined by $f([x]) = [3x]$.

- Check that this is a function.
- Observe that it is bijective
- Show that its inverse is $g: \mathbb{Z}_5 \to \mathbb{Z}_5$, $g([x]) = [2x]$.