Math 220 Fall 2021, Lecture 25: Cardinalities

1. Relations and functions

1.1. Jecitivities (injectivity, surjectivity and bijectivity)

Definition 1.1.1. Let $f : X \to Y$ be a function. Then:

(a) We say that f is **injective** (aka **one-to-one**) if for each $y \in Y$, there exists **at most one** $x \in X$ such that $f(x) = y$. In other words: We say that f is **injective** if there are no two distinct elements $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$.

(b) We say that f is **surjective** (aka **onto**) if for each $y \in Y$, there exists **at least one** $x \in X$ such that $f(x) = y$.

(c) We say that f is **bijective** (aka a **one-to-one correspondence**) if for each $y \in Y$, there exists **exactly one** $x \in X$ such that $f(x) = y$. Thus, f is bijective if and only if f is both injective and surjective.

Here are some examples:

- The function

$$f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0},$$
$$x \mapsto x^2$$

is injective (because no two distinct numbers $x_1, x_2 \in \mathbb{R}_{\geq 0}$ have the same square) and surjective (since each number $y \in \mathbb{R}_{\geq 0}$ is the square of some number $x \in \mathbb{R}_{\geq 0}$). Thus, it is bijective.

- However, the function

$$\widehat{f} : \mathbb{R} \to \mathbb{R}_{\geq 0},$$
$$x \mapsto x^2$$

(which differs from f only in that it has been extended to the whole $\mathbb{R}$ as opposed to $\mathbb{R}_{\geq 0}$ only) is not injective (since different real numbers can have the same square: e.g., we have $5^2 = (-5)^2$), and thus not bijective either. It is still surjective, though.

- The function

$$\widetilde{f} : \mathbb{R} \to \mathbb{R},$$
$$x \mapsto x^2$$

(which does the same as $\widehat{f}$, but is a function to $\mathbb{R}$ rather than a function to $\mathbb{R}_{\geq 0}$) is not surjective (since there are real numbers that are not squares of any real number: for example, -1 is not a square of a real number). Nor is it injective or bijective.

1.2. Inverses

Bijective maps have a special role to play. Namely, they can be **inverted**:

> **Definition 1.2.1.** Let $f : X \to Y$ be a function. An **inverse** of f means a map $g : Y \to X$ such that
>
> $$f \circ g = \mathrm{id}_Y \qquad \text{and} \qquad g \circ f = \mathrm{id}_X .$$
>
> (Recall that id_P means the identity map on a set P – that is, the map from P to P that sends each element to itself.)
>
> In other words, an **inverse** of f means a map $g : Y \to X$ such that
>
> $$f(g(y)) = y \qquad \text{for each } y \in Y, \qquad \text{and}$$
> $$g(f(x)) = x \qquad \text{for each } x \in X.$$

Roughly speaking, an inverse of f is therefore a map that both undoes f and is undone by f.

Not every function has an inverse:

- Let $f : \{1, 2, 3\} \to \{7, 8, 9\}$ be the "add 6" function (i.e., the function that sends each x to $6 + x$). Then, f has an inverse: the "subtract 6" function (i.e., the function that sends each y to $y - 6$).

- Let $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ be the function that sends $1, 2, 3, 4, 5$ to $2, 4, 5, 1, 3$, respectively. Then, f has an inverse: namely, the function g that sends $1, 2, 3, 4, 5$ to $4, 1, 5, 2, 3$, respectively. We can check that $f(g(y)) = y$ for each $y \in \{1, 2, 3, 4, 5\}$: For example, for $y = 3$, this is because $f(g(3)) = f(5) = 3$. Similarly we can check that $g(f(x)) = x$ for each $x \in \{1, 2, 3, 4, 5\}$.

- Let $f : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ be the function that sends $1, 2, 3, 4$ to $1, 2, 2, 3$, respectively. Then, f has no inverse. Indeed, if g was an inverse of f, then $f(2) = 2$ would entail $g(2) = 2$, whereas $f(3) = 2$ would entail $g(2) = 3$; but this would mean that $g(2)$ has two different values 2 and 3 at the same time.

  More generally, if $f : X \to Y$ is to have an inverse, then f should be injective, because if for an element $y \in Y$ we have two different elements x_1 and x_2 satisfying $f(x_1) = y$ and $f(x_2) = y$, then $g(y)$ must be both x_1 and x_2 at the same time.

- Let $f : \{1, 2, 3\} \to \{1, 2, 3, 4\}$ be the function that sends $1, 2, 3$ to $1, 2, 3$, respectively. Then, f has no inverse. Indeed, if g was an inverse of f, then we would have $f(g(4)) = 4$, which is impossible no matter what $g(4)$ is (because f sends nothing to 4).

  More generally, if $f : X \to Y$ is to have an inverse, then f should be surjective, because each $y \in Y$ will satisfy $y = f(g(y))$ and thus be a value of f.

We have learned from these examples that only bijective maps have a chance at having inverses. This is actually sufficient as well: If a map is bijective, it has an inverse. Let us summarize this as a theorem:

Theorem 1.2.2. Let $f : X \to Y$ be a map between two sets X and Y. Then, f has an inverse if and only if f is bijective.

Proof. We must prove the equivalence

$$(f \text{ has an inverse}) \iff (f \text{ is bijective}).$$

Let us prove the $\Longrightarrow$ and $\Longleftarrow$ directions separately:

$\Longrightarrow$: Assume that f has an inverse. We must show that f is bijective.

We assumed that f has an inverse. Let g be this inverse.

Let us show that f is injective. Let $x_1, x_2 \in X$ satisfy $f(x_1) = f(x_2)$. We must prove that $x_1 = x_2$. Set $y = f(x_1)$; then, $y = f(x_2)$ as well (since $f(x_1) = f(x_2)$). Since g is an inverse of f, we have $x_1 = g(f(x_1)) = g(y)$ (since $f(x_1) = y$) and $x_2 = g(f(x_2)) = g(y)$ (since $f(x_2) = y$). Thus, $x_1 = g(y) = x_2$. This completes our proof that f is injective.

Let us show that f is surjective. Let $y \in Y$. Then, $y = f(g(y))$ (since g is an inverse of f). Therefore, there exists an $x \in X$ such that $y = f(x)$ (namely, $x = g(y)$). So we have proved for each $y \in Y$ that there exists an $x \in X$ such that $y = f(x)$. In other words, f is surjective.

So f is both injective and surjective, thus bijective. This proves the "$\Longrightarrow$" direction of our equivalence.

$\Longleftarrow$: Assume that f is bijective. We must show that f has an inverse.

Since f is bijective, for each $y \in Y$, there exists a **unique** $x \in X$ such that $f(x) = y$. Thus, we can define a map

$$g : Y \to X$$

which sends each $y \in Y$ to this unique x. It is easy to see that g is an inverse of f. Thus, f has an inverse. This proves the "$\Longleftarrow$" direction of our equivalence. □

So bijective maps are the same as invertible maps (i.e., maps that have an inverse).

Here are some more properties of inverses:

Theorem 1.2.3. Let $f : X \to Y$ be a map. Then, f has at most one inverse.

Proof. Let g_1 and g_2 be two inverses of f. We must show that $g_1 = g_2$.

Since g_1 is an inverse of f, we have $g_1 \circ f = \mathrm{id}_X$ and $f \circ g_1 = \mathrm{id}_Y$.

Since g_2 is an inverse of f, we have $g_2 \circ f = \mathrm{id}_X$ and $f \circ g_2 = \mathrm{id}_Y$.

Now, associativity of composition shows that $(g_1 \circ f) \circ g_2$ and $g_1 \circ (f \circ g_2)$ are the same map. Hence, we can simply drop the parentheses and write $g_1 \circ f \circ g_2$. We have

$$g_1 \circ \underbrace{f \circ g_2}_{=\mathrm{id}_Y} = g_1 \circ \mathrm{id}_Y = g_1,$$

but also

$$\underbrace{g_1 \circ f}_{=\mathrm{id}_X} \circ g_2 = \mathrm{id}_X \circ g_2 = g_2.$$

Comparing these two equalities, we obtain $g_1 = g_2$, qed. □

Definition 1.2.4. Let $f : X \to Y$ be a map that has an inverse. Then, its inverse (which, as we just showed, is unique) will be called f^{-1}.

Example 1.2.5. Let $\mathbb{R}_{\geq 0}$ be the set of all nonnegative real numbers. Then:

(a) The function

$$f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0},$$
$$x \mapsto x^2$$

has an inverse. This inverse f^{-1} is the function

$$f^{-1} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0},$$
$$x \mapsto \sqrt{x}.$$

(b) However, the function

$$\widetilde{f} : \mathbb{R} \to \mathbb{R},$$
$$x \mapsto x^2$$

has no inverse (since it is neither injective nor surjective).

(c) But the function

$$g : \mathbb{R} \to \mathbb{R},$$
$$x \mapsto x^3$$

has an inverse.

Example 1.2.6. Let X be any set. The identity map $\mathrm{id}_X : X \to X$ is bijective. It is its own inverse.

Theorem 1.2.7. Let $f : X \to Y$ be a map that has an inverse $g : Y \to X$. Then, g has an inverse, which is f.

Proof. Since g is an inverse of f, we have $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$. However, the same two equalities can be read as saying that f is an inverse of g. □

Theorem 1.2.8 (socks-and-shoes formula)**.** Let $g : X \to Y$ and $f : Y \to Z$ be two bijective functions. Then, the composition $f \circ g : X \to Z$ is bijective as well, and its inverse is

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}.$$

Proof. For any $x \in X$, we have

$$\left(g^{-1} \circ f^{-1}\right)((f \circ g)(x)) = g^{-1}\left(\underbrace{f^{-1}(f(g(x)))}_{=g(x)}\right) = g^{-1}(g(x)) = x.$$

For any $z \in Z$, we have

$$(f \circ g)\left(\left(g^{-1} \circ f^{-1}\right)(z)\right) = f\left(\underbrace{g\left(g^{-1}\left(f^{-1}(z)\right)\right)}_{=f^{-1}(z)}\right) = f\left(f^{-1}(z)\right) = z.$$

Thus, $g^{-1} \circ f^{-1}$ is an inverse of $f \circ g$. Hence, $f \circ g$ has an inverse, thus is bijective. □

Remark 1.2.9. Note that $g^{-1} \circ f^{-1}$ is not the same as $f^{-1} \circ g^{-1}$. Indeed, $f^{-1} \circ g^{-1}$ might not even exist.

A surprising feature of the socks-and-shoes formula $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ is that the order in which the inverses f^{-1} and g^{-1} appear on the right hand side is different from the order in which f and g appear on the left hand side. However, this is completely natural: If you want to undo two things you have done in some order, then you should undo them in the opposite order! For example, if you have put on your socks and then your shoes in the morning, then you need to first take off the shoes and then the socks when you go to bed. This is what the name "socks-and-shoes formula" refers to.

Remark 1.2.10. The converse of the socks-and-shoes formula is not true: A composition $f \circ g$ can be bijective even if neither f nor g is bijective.

Definition 1.2.11. Let X and Y be two sets. We say that these two sets X and Y are **isomorphic as sets** (or, short, **isomorphic**) if there exists a bijective map from X to Y.

What sets are isomorphic?

Example 1.2.12. The sets $\{1,2\}$ and $\{1,2,3\}$ are not isomorphic. In fact, there is no surjective map $f : \{1,2\} \to \{1,2,3\}$ (since a map from $\{1,2\}$ to $\{1,2,3\}$ would not have "enough arrows" to hit all three elements of $\{1,2,3\}$), and therefore no bijective map $f : \{1,2\} \to \{1,2,3\}$ either.

Example 1.2.13. The sets $\{1,2,3\}$ and $\{7,8,9\}$ are isomorphic, because we saw above that there is a bijective map from $\{1,2,3\}$ to $\{7,8,9\}$ (namely, "add 6").

Example 1.2.14. The sets $\{1,2,3\}$ and $\{1,3,5\}$ are isomorphic.

Example 1.2.15. The sets $\mathbb{N}$ and $E := \{\text{all even nonnegative integers}\}$ are isomorphic, since the map

$$\mathbb{N} \to E,$$
$$n \mapsto 2n$$

is bijective.

Example 1.2.16. The sets $\mathbb{N}$ and $O := \{\text{all odd nonnegative integers}\}$ are isomorphic, since the map

$$\mathbb{N} \to O,$$
$$n \mapsto 2n+1$$

is bijective.

Example 1.2.17. Are the sets $\mathbb{N}$ and $\mathbb{Z}$ isomorphic? Yes, since there is a bijective map $f : \mathbb{N} \to \mathbb{Z}$ that sends

$$\begin{aligned} &0,1,2,3,4,5,6,\ldots && \text{to} \\ &0,1,-1,2,-2,3,-3,4,-4,\ldots, && \text{respectively.} \end{aligned}$$

Explicitly, this map f can be defined as follows:

$$f(2n) = -n \qquad \text{and} \qquad f(2n+1) = n+1 \qquad \text{for each } n \in \mathbb{N}.$$

In other words,

$$f(n) = \begin{cases} -n/2, & \text{if } n \text{ is even;} \\ (n+1)/2, & \text{if } n \text{ is odd.} \end{cases}$$

It is not hard to see that this map f is indeed bijective. So $\mathbb{N}$ and $\mathbb{Z}$ are isomorphic.

Example 1.2.18. Are the sets $\mathbb{N}$ and $\mathbb{Q}$ isomorphic? Yes! But this is trickier to prove.