Let $f : X \to Y$ be a function. Recall the key definitions from last time.

Definition 9.1.
(i) We say f is *injective*, or *an injection*, [or *one-to-one*,] if $\forall a, b \in X, f(a) = f(b) \implies a = b$.
(ii) We say f is *surjective*, or *a surjection*, [or *onto*,] if $f(X) = Y$, or equivalently if $\forall y \in Y, \exists x \in X, f(x) = y$.
(iii) We say f is *bijective*, or *a bijection*, if it is both injective and surjective.

Let's do some warm-up. Let's do an injective function, a surjective function and then a bijective function.

Example. Let S be any set and let T be a subset of S. Let's define a function f from T to S by $f(a) = a$. Is this a function from T to S? Yes it is: if $a \in T$ then $a \in S$ so this is indeed a recipe which takes an element of T and spits out an element of S. Is it an injection? To prove it is, we need to show that if $a, b \in T$ and $f(a) = f(b)$ then $a = b$. But $a = f(a) = f(b) = b$ and we're done.

Definition 9.1.
(ii) We say f is *surjective*, or *a surjection*, [or *onto*,] if $f(X) = Y$, or equivalently if $\forall y \in Y, \exists x \in X, f(x) = y$.

Example. In the last chapter we talked about equivalence relations. So now say S is a set, and $\sim$ is an equivalence relation on S. Remember that if $a \in S$ then there is a *subset* $\mathrm{cl}(a)$ of S defined as $\mathrm{cl}(a) = \{ b \in S \mid a \sim b \}$. Notation: let $S/\sim$ be the set of equivalence classes for this equivalence relation. So if $a \in S$ then $\mathrm{cl}(a) \subseteq S$ but $\mathrm{cl}(a) \in S/\sim$.

Define $f : S \to S/\sim$ by sending $a \in S$ to $\mathrm{cl}(a)$. So f is really the map cl. Claim: f is a surjection. What does this *mean*? It means that if $C \in S/\sim$ then there exists $a \in S$ with $f(a) = C$. But if $C \in S/\sim$ then by definition C is an equivalence class, so by definition $C = \mathrm{cl}(a)$ for some $a \in S$. So $f(a) = C$, and we have proved that f is surjective.
Philosophical remark: this is the “dual” of the previous example.

Definition 9.1.
(i) We say f is *injective*, or *an injection*, [or *one-to-one*,] if $\forall a, b \in X, f(a) = f(b) \implies a = b$.
(ii) We say f is *surjective*, or *a surjection*, [or *onto*,] if $f(X) = Y$, or equivalently if $\forall y \in Y, \exists x \in X, f(x) = y$.
(iii) We say f is *bijective*, or *a bijection*, if it is both injective and surjective.

Now say S is any set and $f : S \to S$ is the identity function. Is f injective? What does this *mean?* We need to prove that if $a, b \in S$ and $f(a) = f(b)$, then $a = b$. Well, f is the identity function! So $a = f(a) = f(b) = b$, and that's what we wanted.

Is the identity function surjective? What does this *mean*? We need to prove $\forall y \in S, \exists x \in S, f(x) = y$. Well, first choose $y \in S$. Now set $x = y$. And then $f(x) = x = y$ so we're done.

Definition 9.1.
(i) We say f is *injective*, or *an injection*, [or *one-to-one*,] if $\forall a, b \in X, f(a) = f(b) \implies a = b$.
(ii) We say f is *surjective*, or *a surjection*, [or *onto*,] if $f(X) = Y$, or equivalently if $\forall y \in Y, \exists x \in X, f(x) = y$.
(iii) We say f is *bijective*, or *a bijection*, if it is both injective and surjective.

We just saw that the identity function from S to S was injective *and* surjective. Hence

Theorem 9.2. The identity function from S to S is bijective.

$\square$

Let's draw pictures of bijective functions.

What about $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f(x) = 3x + 4$? Is it injective? Is it surjective?

Injectivity: what does this *mean*? It means this: say $a, b \in \mathbb{Q}$ with $f(a) = f(b)$. Can we prove that $a = b$? Well, $f(a) = f(b)$ implies $3a + 4 = 3b + 4$, so (subtracting 4) $3a = 3b$, so (dividing by 3) $a = b$. Hence f is injective. During that proof we took a number, subtracted 4, and then divided by 3.

Is f surjective? What does this *mean*? Say $y \in \mathbb{Q}$ is any rational number. Can we find $x \in \mathbb{Q}$ with $f(x) = y$? Define $x = \frac{y-4}{3}$. Then $f(x) = 3x + 4 = (y - 4) + 4 = y$. So f is surjective. During that proof we took a number, subtracted 4, and then divided by 3. What's going on?

We say that a function is *bijective* if it is injective and surjective. Using language you may have heard at school – a function is bijective if it is one-to-one and onto. We just proved that the function f above was bijective. But why did the function $g(y) = \frac{y-4}{3}$ keep showing up?

$f : \mathbb{Q} \to \mathbb{Q}$ defined by $f(x) = 3x + 4$. And $g : \mathbb{Q} \to \mathbb{Q}$ defined by $g(y) = \frac{y-4}{3}$. What is the relationship between these two functions?

If we start with a number x, and then apply the function f, and then apply the function g, what do we get?

f sends x to $3x + 4$. And then g sends $3x + 4$ to $\frac{(3x+4)-4}{3} = \frac{3x}{3} = x$. Doing f then g gets us back to where we started! Using funky composition of functions notation we could write this observation as $g \circ f = id$. What is $f \circ g$ though? Note that usually $f \circ g$ and $g \circ f$ are not the same function.

$(f \circ g)(x) = f(g(x)) = f(\frac{x-4}{3}) = 3\frac{x-4}{3} + 4 = (x - 4) + 4 = x$. So $f \circ g$ is also the identity function!

Here's what's going on.

Definition 9.3. Say $f : X \to Y$ is a function. We say that a function $g : Y \to X$ is a *two-sided inverse* for f if the composite function $g \circ f : X \to X$ is the identity function, and also the composite function $f \circ g : Y \to Y$ is the identity function.

Example. We just saw that if $X = Y = \mathbb{Q}$ and $f(x) = 3x + 4$, then $g(y) = \frac{y-4}{3}$ is a two-sided inverse for f.

Example. if $X = \{1, 2, 3\}$ and $Y = \{A, B, C\}$ and we define $f(1) = C$ and $f(2) = A$ and $f(3) = B$, then a two-sided inverse for f is the function $g : \{A, B, C\} \to \{1, 2, 3\}$ defined by $g(A) = 2$ and $g(B) = 3$ and $g(C) = 1$.

Example. if g is a two-sided inverse for f, then f is a two-sided inverse for g! Because both of these statements are just the assertion that $f \circ g = \mathrm{id}$ and $g \circ f = \mathrm{id}$.

Example. The identity function from X to X has a two-sided inverse – namely the identity function!

Definition 9.3. Say $f : X \to Y$ is a function. We say that a function $g : Y \to X$ is a *two-sided inverse* for f if the composite function $g \circ f : X \to X$ is the identity function, and also the composite function $f \circ g : Y \to Y$ is the identity function.

Theorem 9.4. Say X and Y are sets, and $f : X \to Y$ is a function. Then f is a bijection if and only if f has a two-sided inverse $g : Y \to X$.

Proof. What needs to be done in an "if and only if" proof? We need to prove that if f is a bijection then it has a two-sided inverse. And we also need to prove that if f has a two-sided inverse then f is a bijection.

First, say $f : X \to Y$ has a two-sided inverse $g : Y \to X$, and let's prove that f is a bijection. What does it *mean* to say that f is a bijection? It means that f is both an injection and a surjection.

Let us first prove that f is injective.

[We are proving that if $f : X \to Y$ has a two-sided inverse g then f is injective]. Say $a, b \in X$ and $f(a) = f(b)$. Applying g we deduce that $g(f(a)) = g(f(b))$. In other words, $(g \circ f)(a) = (g \circ f)(b)$. But g is a two-sided inverse for f, and so $g \circ f$ is the identity function! So $(g \circ f)(a) = a$ and $(g \circ f)(b) = b$, so $a = b$.

Now let's prove that if $g : Y \to X$ is a two-sided inverse for $f : X \to Y$ then f is surjective. What do we need to do? We need to prove that for all $y \in Y$ there exists $x \in X$ such that $f(x) = y$. So let's choose $y \in Y$. We are now supposed to come up with an element of X. However are we going to do this? Let's try defining $x := g(y)$. Now can we prove $f(x) = y$? Well, $f(x) = f(g(y)) = (f \circ g)(y) = y$, because $f \circ g$ is the identity function! Hence f is indeed surjective.

Hence if f has a two-sided inverse, it is a bijection.

Now let us prove that if $f : X \to Y$ is a bijection (hence both injective and surjective), then it has a two-sided inverse.

We need to define a function $g : Y \to X$. So let's choose $y \in Y$ and try and figure out how to get some $x \in X$ to send it to.

Well, we know f is a surjection, so this means that there is *at least one* element $x \in X$ such that $f(x) = y$. Let's define $f^{-1}(y)$ to be the *set* of elements in X such that $f(x) = y$. Formally, $f^{-1}(y) := \{ x \in X \mid f(x) = y \}$. Surjectivity of f guarantees that this set is non-empty; in other words, it has *at least one element*.

But how many elements does $f^{-1}(y)$ have? Let's say $a \in f^{-1}(y)$ and $b \in f^{-1}(y)$ are two arbitrary elements of this set. Then by definition $f(a) = y$ and $f(b) = y$. Hence $f(a) = f(b)$. By injectivity of f, we can deduce $a = b$. But a and b were arbitrary elements of $f^{-1}(y)$ and we just proved that they were equal! Hence $f^{-1}(y)$ has *at most one element*.

Hence $f^{-1}(y)$ has *exactly one element*.

We have just shown that if $f : X \to Y$ is a bijection and $y \in Y$ is arbitrary, then the subset $f^{-1}(y)$ of X has *exactly one element*. Let's define $g(y)$ to be that element. Then $g(y) \in f^{-1}(y)$ so by definition of $f^{-1}(y)$ we know that $f(g(y)) = y$. This is true for all $y \in Y$, so we just showed that $(f \circ g)$ is the identity function.

Finally, how about $g(f(x))$ for some arbitrary $x \in X$? Well, if we set $y = f(x)$ then we saw above that $f^{-1}(y)$ had exactly one element. But definitely $x \in f^{-1}(y)$, because $f(x) = y$ by definition of y. Hence $f^{-1}(y) = \{x\}$, and by definition of g we see $g(y) = x$. Hence $g(f(x)) = x$. But x was arbitrary, so $(g \circ f)$ is the identity function.

We just showed that $(f \circ g)$ and $(g \circ f)$ are both identity functions, and hence g is indeed a two-sided inverse for f, assuming f is a bijection.

$\square$

Theorem 9.4. Say X and Y are sets, and $f : X \to Y$ is a function. Then f is a bijection if and only if f has a two-sided inverse $g : Y \to X$.

[we just proved that]

Corollary 9.5 If X and Y are sets and there is a bijection $f : X \to Y$, then there exists a bijection $g : Y \to X$.

Proof.
Say $f : X \to Y$ is a bijection. By 9.4, f has a two-sided inverse g. Then g also has a two-sided inverse, namely f. Hence by 9.4 again, g is a bijection.

□

Now say X and Y and Z are three sets, and $f : X \to Y$ and $g : Y \to Z$ are functions. Recall that in this situation we can define $h := g \circ f$, so $h : X \to Z$.

Theorem 9.6.
(a) If f and g are both injections, then h is an injection.
(b) If f and g are both surjections, then h is a surjection.
(c) If f and g are both bijections, then h is a bijection.

Proof.
(a) What do we have to prove? Say $a, b \in X$ and say $h(a) = h(b)$. We have to prove $a = b$. Well, $h(a) = g(f(a))$ and $h(b) = g(f(b))$. Let's temporarily write $p = f(a)$ and $q = f(b)$, so $p, q \in Y$. Our assumption is then that $g(p) = g(q)$, so by our assumption of injectivity of g we can deduce $p = q$. Hence $f(a) = f(b)$, so by injectivivity of f we can deduce $a = b$. We are done!

(b) The claim is that if $f : X \to Y$ and $g : Y \to Z$ are surjections, then $h := g \circ f$ is too.

What does this *mean*? Go ahead and prove this yourself.

We need to prove $\forall c \in Z, \exists a \in X, h(a) = c$. So let $c \in Z$ be arbitrary and we need to come up with some $a \in X$ (which can depend on c) such that $h(a) = c$. Well, g is surjective by assumption, so we know that there exists $b \in Y$ such that $g(b) = c$. And f is surjective by assumption, so we know that there exists $a \in X$ such that $f(a) = b$. I claim that $h(a) = c$. Indeed

$$\begin{aligned} h(a) &= (g \circ f)(a) \text{ (by definition of } h) \\ &= g(f(a)) \text{ (by definition of } \circ) \\ &= g(b) \text{ (by definition of } a) \\ &= c \text{ (by definition of } b) \end{aligned}$$

$\square$

Theorem 9.6.
(a) If f and g are both injections, then h is an injection.
(b) If f and g are both surjections, then h is a surjection.
(c) If f and g are both bijections, then h is a bijection.

We already proved (a) and (b).

Proof of (c): it follows immediately from (a) and (b) and the definition of a bijection.

$\square$

It turns out that we've been heading towards a main goal in this lecture, which I've been keeping a secret; I think it's one of the coolest results in this course. Here it is.

Let X and Y be sets, and let's define some new notation. Let's define the double-headed arrow $X \leftrightarrow Y$ to mean that there exists a bijection $f : X \to Y$.

Example. $\mathbb{Q} \leftrightarrow \mathbb{Q}$; indeed we have seen several bijections. The identity function works, and we also saw that the function $x \mapsto 3x + 4$ works.

Example. $\{1, 2, 3\} \leftrightarrow \{A, B, C\}$; for example the function mapping 1 to A, 2 to B and 3 to C works.

But here's the best thing of all.

Theorem 9.7. Let $\mathcal{C}$ be a set of sets. Then $\leftrightarrow$ is an equivalence relation on $\mathcal{C}$.

$X \leftrightarrow Y$ means that there exists a bijection $f : X \to Y$.

Theorem 9.7. Let $\mathcal{C}$ be a set of sets. Then $\leftrightarrow$ is an equivalence relation on $\mathcal{C}$.

Proof. We need to prove reflexivity, symmetry and transitivity for $\leftrightarrow$. These immediately follow from

Theorem 9.2. Let S be a set. Then the identity function from S to S is bijective.
Corollary 9.5 If X and Y are sets and there is a bijection $f : X \to Y$, then there exists a bijection $g : Y \to X$.
Theorem 9.6. (c) If $f : X \to Y$ and $g : Y \to Z$ are both bijections, then $g \circ f : X \to Z$ is a bijection.

$\square$

Next time: consider the set $\{ \mathbb{Z}_{\geq 1}, \mathbb{Z}_{\geq 0}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \}$ with this equivalence relation. What are the equivalence classes?