3/15

Basic Mathematical Structures: Functions §3.1

Having concluded our study of proofs (Chapter 2) we are starting a new chapter, Chapter 3, which discusses basic mathematical structures. The most basic mathematical structures are sets, which we have already discussed in Chapter 1. The next most basic structures in math are functions, which are procedures for going from one set to another.

There are many ways to think about functions. One is that a function f from a set X to a set Y is a machine or a rule that takes something in X and spits out something in Y:

$$x \in X \Rightarrow \underbrace{\boxed{\quad f \quad}}_{\text{machine}} \Longrightarrow y = f(x) \in Y$$

For example, consider the following procedure:

- given a 10-digit number x like
  $$x = 1\,0\,4\,3\,2\,1\,3\,5\,9\,8$$
  we sum together the digits:
  $$1+0+4+3+2+1+3+5+9+8 = 3\underline{6}$$
  and then "spit out" the ones digit of the resulting sum as our $y = f(x)$:
  $$y = f(x) = 6 \text{ in the example.}$$

This describes a function f whose domain X is the set of 10-digit numbers and codomain Y is the set of one digit numbers.

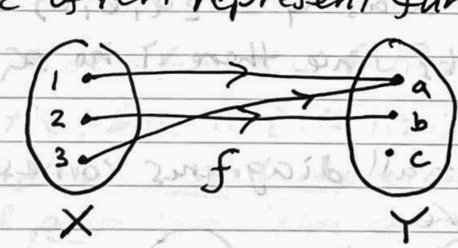
(It is a simplified version of the "check sum" procedure for credit card numbers...)

Notice that the domain of a function f is the name we give to the input set X and codomain is the name we give to the output set Y.

That was an intuitive definition of function as machine. The formal definition of function uses ordered pairs:

Def'n A function from set X (called the domain) to set Y (called the codomain) is a subset of $X \times Y$ (set of ordered pairs (x,y) w/ $x \in X$, $y \in Y$), such that: for every $x \in X$, there is a unique $y \in Y$ with (x,y) in our subset.

E.g. We often represent functions by arrow diagrams:



This corresponds to the subset $\{(1,a), (2,b), (3,c)\}$ of $X \times Y$ where $X = \{1,2,3\}$ and $Y = \{a,b,c\}$. For each arrow $x \to y$ we include the pair (x,y) in our subset.

Notice now for every $x \in X$ there is a unique $y \in Y$ with (x,y) in our subset: we write $f(x) = y$, where "f" is the name of our function.

In this example: $f(1) = a$
$f(2) = b$
$f(3) = a$

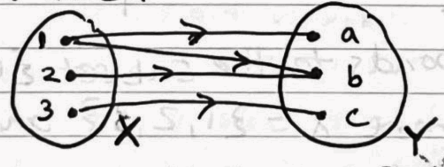
$\Leftarrow$ can also think of a function as a "chart" like this.

We also write $f: X \to Y$ to mean f is a function from X to Y. The arrow helps you remember what f does: it takes something in X to something in Y.

Since the set of ordered pairs will always be $\boxed{\{(x, f(x))\}}$ the "rule" description of a function also defines the pairs: e.g., in the credit card check sum example we had $f(1043598) = 6$, but writing all pairs would <u>take</u> a <u>while</u>!

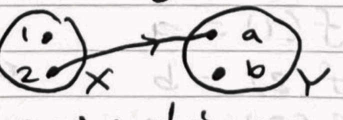
The set $\{f(x) : x \in X\}$ of <u>values</u> our function f actually takes <u>on</u> is called the <u>range</u> of f, and it is a <u>subset</u> of the codomain: <u>e.g.</u> in arrow diagram example f above the <u>codomain</u> was $Y = \{a, b, c\}$ but the <u>range</u> is $\{a, b\}$ since there is no $x \in X$ w/ $f(x) = c$.

<u>WARNING</u>: Not all diagrams correspond to functions. A diagram like:



is not the arrow diagram of a function because the key property of a function f is that for every $x \in X$ there is a <u>unique</u> $f(x) = y$ it is "sent to" and here $1 \in X$ is "sent" to both a and b!

Similarly, a diagram like:



is not the arrow diagram of a function: can you see <u>why</u>?

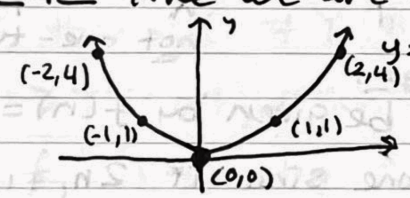
From calculus you are probably used to functions like

$$f(x) = x^2$$

whose domain and codomain are the real numbers $\mathbb{R}$.
Notice how "$f(x) = x^2$" is the "rule/machine" description of the function - it tells us for a given input x how to produce the output $f(x)$:

$$\text{e.g., } f(3) = 3^2 = 3 \times 3 = 9$$

But we can also represent a function $f: \mathbb{R} \to \mathbb{R}$ by its graph like we are used to doing:

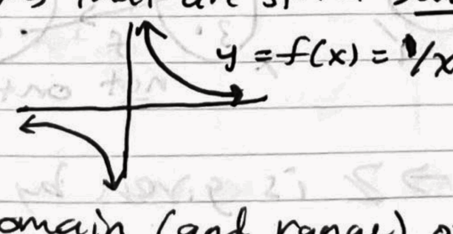


The graph of a function $f: \mathbb{R} \to \mathbb{R}$ is just a drawing of all the points in $\{(x, f(x)) : x \in \mathbb{R}\}$, i.e., it is another visual representation of the ordered pair definition of function.
(Recall: "vertical line test" for graph of a function.)

Some functions defined algebraically like

$$f(x) = 1/x$$

have domains that are strict subsets of $\mathbb{R}$:



Here the domain (and range) of $f(x) = 1/x$ is $\{x \in \mathbb{R} : x \neq 0\}$ since we are not allowed to divide by zero...

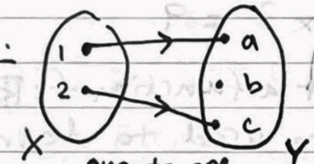
3/17

<u>More about functions</u> (§3.1): Let $f: X \to Y$ be a function.

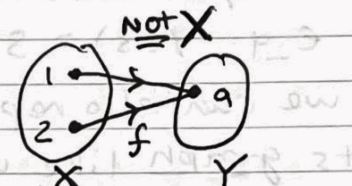
<u>Def'n</u> The function f is called <u>one-to-one</u> (or <u>injective</u>) if there are <u>not</u> two different $x_1, x_2 \in X$ with $f(x_1) = f(x_2)$.

"Everything in X is sent to a different thing in Y."

<u>E.g.</u>



<u>one-to-one</u>



<u>not</u> one-to-one

<u>E.g.</u> Let $f: \mathbb{Z} \to \mathbb{Z}$ (← integers) be given by $f(n) = 2n+1$. (so... $f(0) = 1$, $f(1) = 3$, $f(-1) = -1, \ldots$)

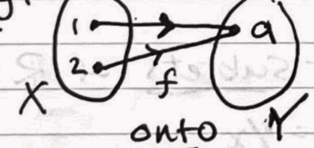
This f <u>is</u> one-to-one since if $2n_1 + 1 = 2n_2 + 1$ then $n_1 = n_2$. ✓

<u>Def'n</u> The function f is called <u>onto</u> (or <u>surjective</u>) if for every $y \in Y$, there is some $x \in X$ with $f(x) = y$.

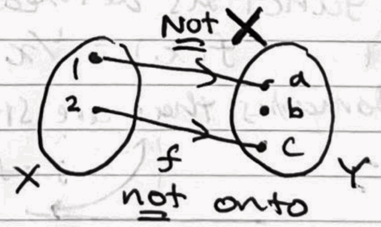
"Everything in Y is mapped to by something in X."

<u>Note</u>: Onto same as "range of f = codomain of f".

<u>E.g.</u>



<u>onto</u>

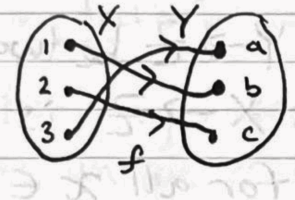


<u>not</u> onto

<u>E.g.</u> If $f: \mathbb{Z} \to \mathbb{Z}$ is given by $f(n) = 2n+1$ then f is <u>not</u> onto since there is <u>no</u> integer $n \in \mathbb{Z}$ with $2n+1 = 0$ (or any even integer)

Def'n The function f is called <u>bijective</u> (or a <u>bijection</u>) if it is <u>both</u> one-to-one and onto.

<u>E.g.</u>



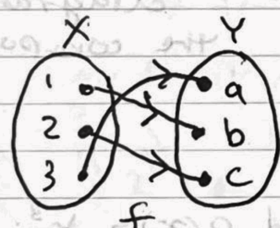
is <u>bijective</u>.

<u>E.g.</u> $f(n) = n+1 : \mathbb{Z} \to \mathbb{Z}$ is a bijection. (<u>Why</u>?)

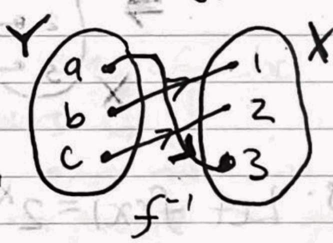
<u>Exercise</u>: If $f: X \to Y$ is a bijection between <u>finite</u> sets X and Y, then $\#X = \#Y$ (the sets have the same # of elements).

<u>Def'n</u> If $f: X \to Y$ is a bijection, then we define its <u>inverse</u> <u>function</u> $f^{-1}: Y \to X$ by $f^{-1}(y) = x$ if and only if $f(x) = y$, for all $y \in Y$.

<u>E.g.</u>

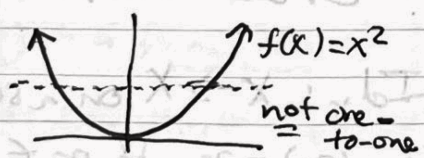


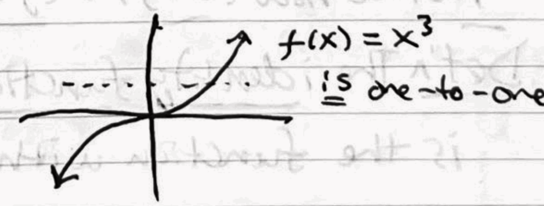
has inverse



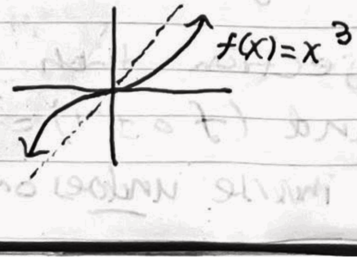
"flip arrows"

<u>E.g.</u> To check whether a function $f: \mathbb{R} \to \mathbb{R}$ is one-to-one we have the "<u>horizontal line test</u>":

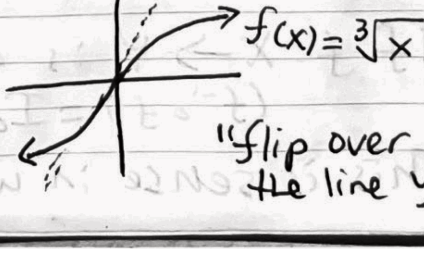




The inverse of $f(x) = x^3$ is $f^{-1}(x) = \sqrt[3]{x}$:



$\Rightarrow$



"flip over the line $y = x$" //

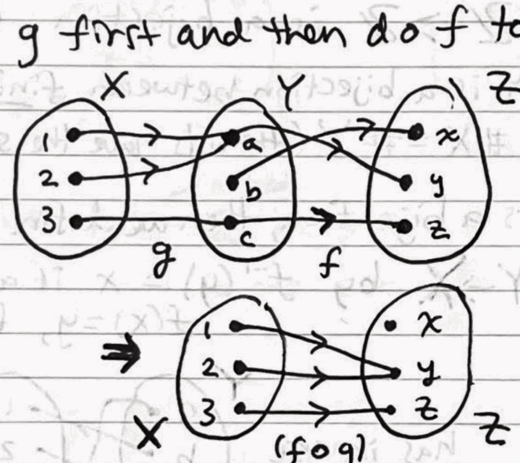
3/20

The inverse function f^{-1} "undoes" whatever f does.
Let's make this precise by talking about compositions.

Def'n Let $g: X \to Y$ and $f: Y \to Z$ be two functions. Their composition $(f \circ g): X \to Z$ is defined by $(f \circ g)(x) = f(g(x))$ for all $x \in X$.

"Do g first and then do f to what you get."

E.g.



"Combine arrow diagrams" to form the arrow diagram of the composition

Eg. Let $f(x) = 2^x : \mathbb{R} \to \mathbb{R}$ and $g(x) = x^3 : \mathbb{R} \to \mathbb{R}$.
Then $(f \circ g)(x) = 2^{x^3}$ and $(g \circ f)(x) = (2^x)^3 = 2^{3x}$.
Notice how $(f \circ g) \neq (g \circ f)$! Order matters!

Def'n The identity function $Id_X : X \to X$ on a set X is the function with $Id_X(x) = x \;\; \forall x \in X$.

"The identity function 'does nothing': gives the input as output."

If $f: X \to Y$ is a bijection then
$$(f^{-1} \circ f) = Id_X \text{ and } (f \circ f^{-1}) = Id_Y.$$
This is sense in which inverse undoes original function.

Modular arithmetic functions §3.1

Let $n \in \mathbb{Z}$ be a positive integer $n \geq 1$.

The "modulo n" function is an important function in discrete math:

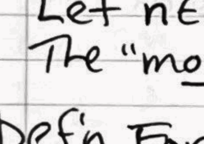
Def'n For any integer $m \in \mathbb{Z}$, m mod n (or "m modulo n") is the unique $r \in \{0,1,2,\ldots,n-1\}$ such that r is the remainder when dividing m by n, i.e. $\exists k \in \mathbb{Z}$ such that $m = k \cdot n + r$.

E.g. 3 mod 5 = 3 and 8 mod 5 = 3 too since $8 = 5+3$.

1247 mod 10 = 7 since we just look at ones place.

E.g. For any n, n mod $n = 0$ and -1 mod $n = n-1$.

E.g. Can think of m mod n in terms of "clock arithmetic":



Put the numbers $0, 1, \ldots, n-1$ on a circle, and move m steps to compute m mod n.
(If m is negative, step backwards).

In this way, for every positive integer n we get a function $f: \mathbb{Z} \to \mathbb{Z}$ given by $f(m) = m$ mod n.

Notice that the range of f is $\{0, 1, \ldots, n-1\}$.

The mod n functions can be useful for problems dealing with clocks or calendars, e.g.:

Exercise If the first day of the year is a Tuesday, what day of the week is the 100^{th} day of the year?

3/22 Sequences § 3.2

A <u>sequence</u> is a <u>list</u> of things, such as:

1, 2, 3, 4, 5, ...
2, 4, 8, 16, 32, ...
1, 2, 3
b, a, n, a, n, a ; <u>etc.</u>

It can be <u>finitely</u> long, or <u>infinitely</u> long.
It can have <u>repetitions</u> (like in the letters of "banana")
The important thing is that the <u>order</u> of the sequence <u>matters</u>, so that $1, 2, 3 \neq 3, 1, 2$.

Formally, we represent a sequence by a <u>function</u> s whose domain is a subset of the <u>positive integers</u>
(we denote the positive integers by $\mathbb{Z}_{>0}$)

<u>E.g.</u> $s: \mathbb{Z}_{>0} \to \mathbb{Z}$ with $s(n) = n$
gives the sequence $1, 2, 3, 4, \ldots$

<u>E.g.</u> $s: \mathbb{Z}_{>0} \to \mathbb{Z}$ with $s(n) = 2^n$
gives the sequence $2, 4, 8, 16, \ldots$

<u>E.g.</u> $s: \{1, 2, 3, 4, 5, 6\} \to \{a, b, n\}$
with $s(1) = b$, $s(2) = a$, $s(3) = n$, $s(4) = a$, $s(5) = n$, $s(6) = a$
gives the sequence b, a, n, a, n, a.

Usually, domain is either <u>all</u> of $\mathbb{Z}_{>0}$ (for <u>infinite</u> sequence)
or $\{1, 2, \ldots, n\}$ (for <u>finite</u> sequence).
We write the sequence as $s_1, s_2, s_3, \ldots$
where $s_i = s(i)$ is "sequence notation".
We also sometimes write it as $\{s_n\}_{n=1}^{\infty}$.

If the codomain of the sequence is a set of numbers, we say s is <u>increasing</u> if $s_i < s_j$ when $i < j$ and say s is <u>decreasing</u> if $s_i > s_j$ when $i < j$.

E.g. $2, 4, 8, 16, 32, \dots$ is increasing and $1/2, 1/4, 1/8, 1/16, \dots$ is decreasing.

<u>Nonincreasing</u> ($s_i \geq s_j$) and <u>nondecreasing</u> ($s_i \leq s_j$) defined similarly.

For a finite sequence $\{s_n\}_{n=1}^{k}$ of numbers, we define its <u>sum</u> $\sum_{n=1}^{k} s_n = s_1 + s_2 + \dots + s_k$.

E.g. We already saw (using induction) that

$$\sum_{n=1}^{k+1} 2^{n-1} = 2^0 + 2^1 + 2^2 + \dots + 2^k = 2^{k+1} - 1.$$

Can define <u>product</u> $\prod_{n=1}^{k} s_n = s_1 \times s_2 \times \dots \times s_k$ as well...

A <u>subsequence</u> of a sequence s is a sequence we get by selecting some of the items of list s, not necessarily consecutive, but <u>in the same order</u>!

E.g. subsequences of (b, a, n, a, n, a) include (b, a) & (b, n) & (a, a, a), but <u>not</u> (a, b) (don't have an "a" before a "b")

If the sequence is $\{s_n\}$ then the subsequence will be $s_{n_1}, s_{n_2}, s_{n_3}, \dots$ where $\{n_1 < n_2 < \dots\}$ is a subset of the domain of s.

E.g. (2, 4, 6, 8, ...) is a subsequence of (1, 2, 3, 4, ...) as is (2, 3, 4, 5, ...), as is (1, 2, 3) (finite sequence), but... (2, 1, 3, 4) is <u>not</u> a subsequence.

Strings §3.2

If X is a finite set, then a string over X is any finite sequence of elements from X.
We use X^* to denote the set of all strings over X.

E.g. If $X = \{a, b\}$ then some elements of X^* are
$a, b, aa, ab, bba, baba$

We call X the alphabet and its elements letters.
The length of a string is its length as a sequence.
There is a special string that's always in X^* called the null string, denoted λ, which has length zero.
In other words, λ has no letters in it!

If $\alpha, \beta \in X^*$ are two strings, their concatenation $\alpha\beta$ is what we get by putting α right before β.

E.g. $\alpha = aba$, $\beta = bba$, then $\alpha\beta = ababba$.

Notice length of $\alpha\beta$ = length of α + length of β.

Question: What is $\alpha\lambda$ (alpha concatenated w/ null string)?

A substring of a string $\alpha \in X^*$ is any string of consecutive letters from α. (Different from subsequence!)

E.g. For $\alpha = aba$, ab & ba are substrings, but aa is not a substring.

Exercise: Show β is a substring of α if and only if $\alpha = \delta\beta\gamma$ for some strings δ and γ.