Jan20

Sunday, January 16, 2022 3:27 PM

More Set Theory: Functions

Defn

map

Let S, T be sets. A function from S to T is a rule assigning to each element of S, one of T.

Notation

$$\begin{aligned} f : S &\longrightarrow T \\ x &\longmapsto f(x) \end{aligned}$$

or

$$S \xrightarrow{f} T$$

Ex

* $S = T = \mathbb{N} = \{1, 2, 3, 4, \ldots\}$

$$\begin{aligned} f : \mathbb{N} &\longrightarrow \mathbb{N} \\ x &\longmapsto x^2 \end{aligned}$$

* Binary operations are functions!

$$S = \mathbb{Z} \times \mathbb{Z} = \{(a, b) \mid a, b \in \mathbb{Z}\}$$

$T = \mathbb{Z}$

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(a, b) \longmapsto a + b$$

Rmk

Math is often the study of certain function on certain sets.

- Calculus: differentiable function from $\mathbb{R}$ to $\mathbb{R}$.
- Topology: continuous functions.
- Algebra: homomorphisms...

Def^n S, T sets. $f : S \longrightarrow T$ a function

1) S is called the domain (source)
   T is called the codomain (target)

2) If $S = T$ & $f(x) = x$ $\forall x \in S$.
   Then f is called the identity map. on S.

$f = id_S = id$

3) If for all $x, y \in S$ we have

$$(*) \quad \left(f(x) = f(y) \implies x = y. \right)$$

contrapositive

Then f is injective.

[notice $(*)$ is equivalent

$$x \neq y \implies f(x) \neq f(y)$$]

Slogan "different things must to different things"

Ex $f : \mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto x^2$ not injective bc

$$f(1) = 1 = f(-1)$$

but $1 \neq -1$.

Also called one-to-one.

4) If given any $y \in T$, there exists some $x \in S$ s.t. $f(x) = y$, then f is surjective. (also called onto)

Slogan: f hits the entire target.

Example $f : \mathbb{R} \longrightarrow \mathbb{R}$

$$x \longmapsto x^2$$

not surjective b/c -1 isn't f of anything.

5) If f is injective and surjective we call it bijective.

Def^n (composing functions).

Let S, T, R be sets. $f: S \longrightarrow T$ & $g: T \longrightarrow R$ are two functions. We can define a new function: g composed with f

$$g \circ f : S \longrightarrow R$$
$$x \longmapsto g(f(x))$$

Diagram:

$$\begin{tikzcd}
S \arrow[r, "f"] \arrow[rr, bend left, "g \circ f"] & T \arrow[r, "g"] & R \\
x \arrow[r, mapsto] & f(x) \arrow[r, mapsto] & g(f(x)).
\end{tikzcd}$$

Def^n Let $f: S \longrightarrow T$.

A function $g: T \to S$ is....

1) A left inverse if

$$\begin{tikzcd} S \arrow[r, "f"] \arrow[rr, bend right, "\mathrm{id}_S"'] & T \arrow[r, "g"] & S \end{tikzcd}$$

with $g \circ f$: as above.

i.e. $g(f(x)) = x \quad \forall \; x \in S$

"for all"

2) A right inverse if

$f \circ g$:

$$\begin{tikzcd} T \arrow[r, "g"] \arrow[rr, bend right, "\mathrm{id}_T"'] & S \arrow[r, "f"] & T \end{tikzcd}$$

i.e. $\forall \; y \in T, \quad f(g(y)) = y$

3) An inverse to f if it is both a left & right inverse.

Theorem (HW) S, T nonempty sets.

1) f is injective $\iff$ it has a left inverse.

2) f is surjective $\Longleftrightarrow$ it has a right inverse.

→ 3) f is bijective $\Longleftrightarrow$ it has an inverse.

4) If f has an inverse, that inverse is unique.

Consequence

If f is injective & surjective, I know it has an inverse.

Proof ①

($\Longleftarrow$) Assume f has a left inverse, say g. Show f is injective.

Assume have $x, y \in S$ &

$f(x) = f(y)$. ← elements of T

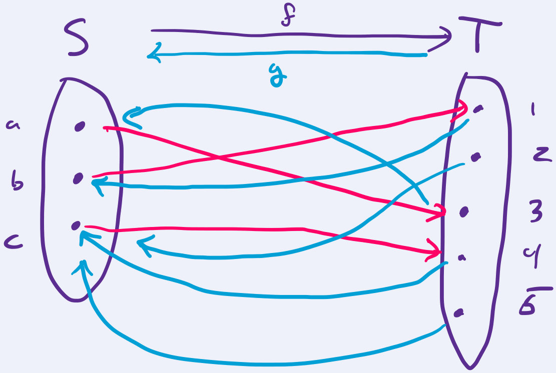
Apply g to both sides!

$$x = g(f(x)) = g(f(y)) = y$$

So we win!!

($\Longrightarrow$)

Let's give an example of an injection



Build a left inverse, g.

$g(1) = b \qquad g(3) = a \qquad g(4) = c$

What about $g(2)$ & $g(5)$?

Can be anything.

g is a left inverse!

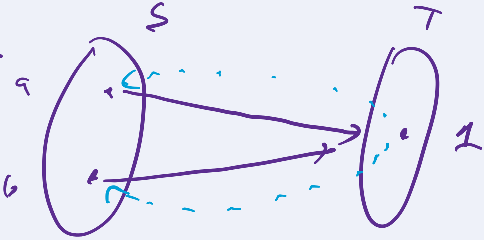
$$g(f(a)) = g(3) = a$$
$$g(f(b)) = g(1) = b$$
$$g(f(c)) = g(4) = c$$

✓

Saw

for this particular f which is injective, there is a left inverse.

Example



Wait! $g(1)$ can't be both...

Remarks:

- Make clear the relationship between injectivity & $\exists$ of left inverse.
- Argument for general case will be very similar.
- Philosophy: when working on a proof work out a simple example first, you will often observe the main idea of the proof.

Important Stucture: Equivalence Relations

Example:

$x \sim y$

→ Say two numbers $x, y \in \mathbb{Z}$ are related if they parity (i.e. both even or both odd)

i.e., if $x-y$ is even.

→ Behaves a lot like $=$ in the following way:

- $x \sim y \implies y \sim x$
- $x \sim x$
- $x \sim y$ & $y \sim z$ $\implies x \sim z$

This defines a subset $U \subseteq \mathbb{Z} \times \mathbb{Z}$.

$$U = \{(x,y) \mid x \sim y\}.$$

Defn

A equivalence relation on a set S is a subset $U \subseteq S \times S$ satisfying.

(Symmetric) 1) $(x,y) \in U \iff (y,x) \in U$

$$x \sim y \iff y \sim x$$

(reflexive) 2) $(x,x) \in U$. $x \sim x$

(transitive) 3) $(x,y) \in U$ & $(y,z) \in U \implies (x,z) \in U$

$$x \sim y \text{ \& } y \sim z \implies x \sim z$$

Related Notion: Partitions.

Let S be a set. A collection $\{X_i\}$ of subsets of S is called a partition of S if:

i) $X_i \neq \emptyset$ (nonempty)

ii) $\bigcup_i X_i = S$ (cover S)

iii) $i \neq j$ $X_i \cap X_j = \emptyset$ (pairwise disjoints).

Example $S = \mathbb{Z}$.

$\longrightarrow X_0 =$ even numbers
$\longrightarrow X_1 =$ odd numbers.
$\}$ are a partition!!

i) Nonempty. ✓

ii) $X_0 \cup X_1 = \mathbb{Z}$. (every number is either even or odd).

iii) $X_0 \cap X_1 = \emptyset$ (no numbers are both even & odd).

Notice

Evenness & oddness also appeared in our equivalence relation!!

No coincidence.

Proposition Let S be a nonempty set. There is a bijection

$$\left\{\begin{matrix}\text{Equivalence}\\ \text{relations}\\ \text{on } S\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{Partitions}\\ \text{of}\\ S\end{matrix}\right\}$$

Proof: Homework.

Describe $\longrightarrow$

Def$^{\underline{n}}$

Let $\sim$ be an equivalence relation on S.

Let $a \in S$. The equivalence class of a is

$$[a] = \overline{a} := \{ b \in S \mid a \sim b \}$$

$$[a] \subseteq S$$

Example $S = \mathbb{Z}$.

$x \sim y$ if they have same parity.

$$\left.\begin{aligned} [0] &= \text{Even numbers.} = X_0 \\ [15] &= \text{Odd numbers} = X_1 \end{aligned}\right\}$$

Partition of $\mathbb{Z}$.

Prop: S a set.

1) If $\sim$ is an equivalence relation of S, the equivalence classes of $\sim$ form a partition of S.
2) Let $\{X_i\}$ be a partion of S. The X_i are equivalence classes of a unique equivalence relation of S.

Pf/ HW.

1). Have an equivalene relation.
Equivalee classes are a partition
- i) Nonempty ✓
- ii) Cover S
- iii) Pairwise disjoint

} for you

Take $[a]$ an equivalence class. Show it's not empty.

Well $a \sim a$ by reflexive.

So $\underset{\substack{\rotatebox{90}{$\in$} \\ a}}{[a]} = \{ b \in S \mid \underline{b \sim a} \}$

Algebraic Properties of $\mathbb{Z}$

The integers form a prototypical example of a ring (2 binary operations)

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$\times : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}.$$

Satisfying: $\forall\ a, b, c \in \mathbb{Z}$

abelian group

group

① $a + (b + c) = (a + b) + c$ (assoc)

② $a + 0 = 0 + a = a$ (identity)

③ $a + (-a) = (-a) + a = 0$ (inverse)

④ $a + b = b + a$ (commutativity).

Ring

⑤ $a \times (b \times c) = (a \times b) \times c$ (assoc).

⑥ $a \times 1 = 1 \times a = a$ (identity)

comm ring

⑦ $a\times(b+c) = a\times b + a\times c$ (distributes)

$(a+b)\times c = a\times c + b\times c$

⑧ $a\times b = b\times a$ (commutes).

---

§ Divisibility

Defⁿ Let $a,b\in\mathbb{Z}$. We say a divides b if $\exists\ k\in\mathbb{Z}$ w/ $ak=b$.

(write $a|b$ if a divides b.
else $a\nmid b$)

Examples $3|21$ bc $3\cdot \underset{\uparrow k}{7} = 21$

$3\nmid 22$.

Fact: $a|b$ & $a|c \implies a|b+c$

pf/ $a|b \Rightarrow b=ka$ $\quad k,l\in\mathbb{Z}$

$a|c \Rightarrow c=la$

So $b+c = ka+la = (k+l)a$ ⊘

Defⁿ (Greatest Common Divisors).

$a, b \in \mathbb{Z}$. The greatest common divisor of a & b is

$$\gcd(a,b) = g \in \mathbb{Z} \quad \text{s.t.}$$

1) $g \mid a$ & $g \mid b$ $\leftarrow$ common div.

2) If $d \mid a$ & $d \mid b \Rightarrow d \leq g$.

$\uparrow$ greatest

Ex

$\gcd(12, 15) = 3$

Def^n (Long Division) (division w/ remainder)

$a, b \in \mathbb{Z} \setminus \{0\}$. There exist unique $q, r \in \mathbb{Z}$ w/ $0 \leq r < |b|$ s.t.

$$a = bq + r.$$

Example $a = 23$ $b = 7$

$$\begin{array}{r|l} & \overset{q}{\boxed{0\;3}} \quad R = 2 \\ 7 & 23. \\ & -21 \\ \hline & 2 \end{array}$$

$0 \leq r = 2 < |7|$

$$23 = 7 \cdot 3 + 2.$$

Proof: Exercise.

Theorem (Euclidean algorithms)

Let $a, b \in \mathbb{Z} \setminus \{0\}$. Iterate the following algorithm

$$\underline{\underline{a}} = q_0 \underline{b} + \boxed{r_0} \qquad 0 \lneq r_0 < |b|$$

$$\underline{\underline{b}} = q_1 r_0 + r_1 \qquad 0 \lneq r_1 < |r_0|$$

$$r_0 = q_2 r_1 + r_2 \qquad 0 \lneq r_2 < |r_1|$$

$$\rightarrow \; r_1 = q_3 r_2 + r_3 \qquad 0 \lneq r_3 < |r_2|$$

$$\vdots$$

$$\rightarrow \; r_{n-2} = \underline{\underline{q_n r_{n-1}}} + \boxed{r_n} \qquad 0 \lneq r_n < |r_{n-1}|$$

$$r_{n-1} = q_{n+1} r_n + 0$$

Stop.

Then $\gcd(a,b) = r_n$.

Proof (Exercise).

$a = bq + r$

Hint

1) $\gcd(a,b) = \gcd(b,r)$.

2) $\gcd(a,0) = ??$

Corollary (Extended Euclidean Algorithm).

$a, b \in \mathbb{Z}$. Then

$\gcd(a,b) = au + bv$ some $u, v \in \mathbb{Z}$.

Pf/ $\gcd = r_n = r_{n-2} - q_n r_{n-1}$

solve r_{n-1} in terms of r_{n-2} & r_{n-3}

r_{n-2} in terms of r_{n-3} & r_{n-4}

$\vdots$

in terms of a & b.

Example: $\gcd(20, 35). = \underline{\underline{5}}$

$$\left.\begin{aligned} &(b)\; 35 = 20 \cdot 1 + 15 \\ &(a)\; 20 = 15 \cdot 1 + \underline{5} \\ & 15 = 5 \cdot 3 + 0 \end{aligned}\right\}$$

$(*)\; 5 = 20 - 15 \cdot 1$

$(**)\; 15 = 35 - 20 \cdot 1$

$$\begin{aligned} \boxed{5} &= 20 - (35 - 20 \cdot 1) \\ &= 20 - 35 + 20 \\ &= 2 \cdot \underline{\underline{20}} + (-1) \cdot \underline{\underline{35}} \end{aligned}$$