Group Theory

Set theory

- Set theory deals with sets

$$S = \{ \text{elements} \}$$

unordered collections of elements with no repetitions.

Set operations:

- **Unions** $S \cup T = \{ x \in S \text{ or } x \in T \}$
- **Intersections** $S \cap T = \{ x \in S \text{ and } x \in T \}$
- **Complements**: $A \subseteq S \to A^c = \{ x \in S, x \notin A \}$

where $A \subseteq S$ means $x \in A \Rightarrow x \in S$

- **Products**

$$S \times T = \{ (x, y) : x \in S, y \in T \}$$

eg: · $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ plane

Functions

$$f : S \longrightarrow T$$

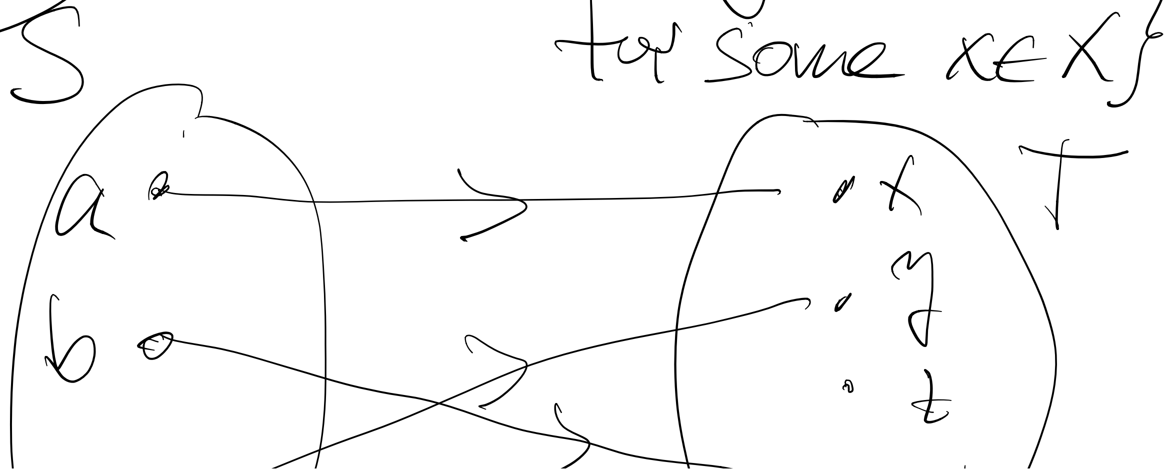
domain Codomain

$$\begin{tikzcd} x \arrow[r, mapsto] \arrow[d, phantom, sloped, "\in"] & f(x) \arrow[d, phantom, sloped, "\in"] \\ S & T \end{tikzcd}$$

image of $f = f(S)$

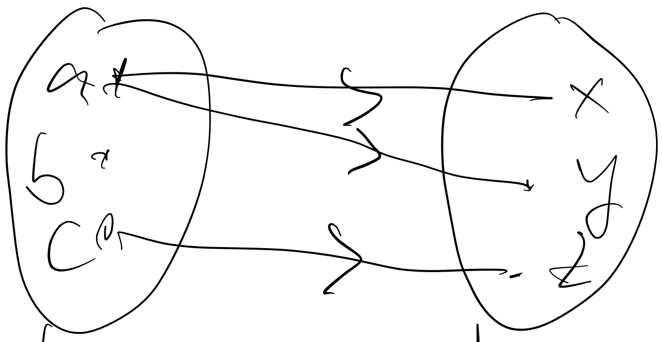
$= \{ y \in T : y = f(x) \text{ for some } x \in X \}$

Ex 1



$f(S) = \{x, y, w\}$

Ex 2

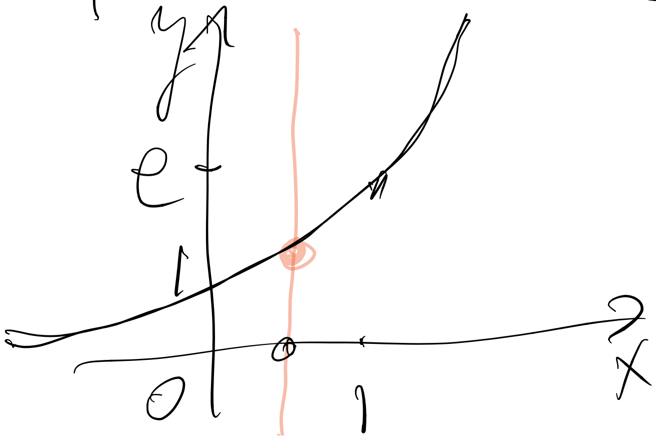


not a function!

$a \rightarrow x$, $a \rightarrow y$ bad!

$b \dashrightarrow ?$ bad!

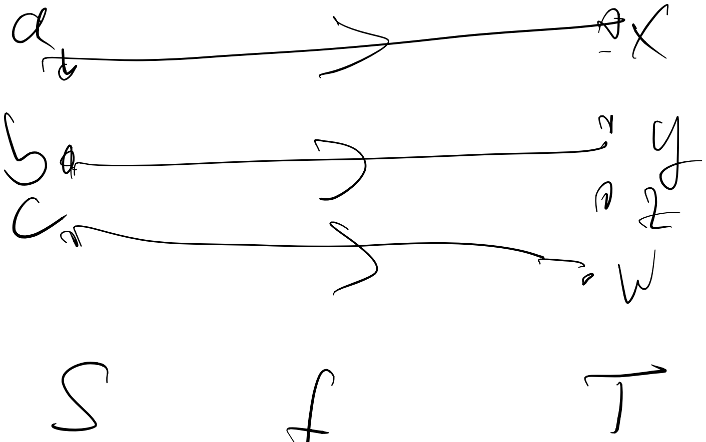
Ex 3 $f: \mathbb{R} \rightarrow \mathbb{R}$ $f(x) = e^x$



Passes vertical line test
– so it is a function.

Properties of functions

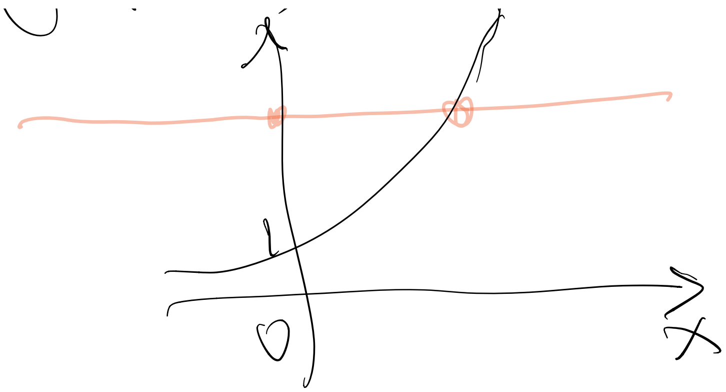
- One-to-one (injective)



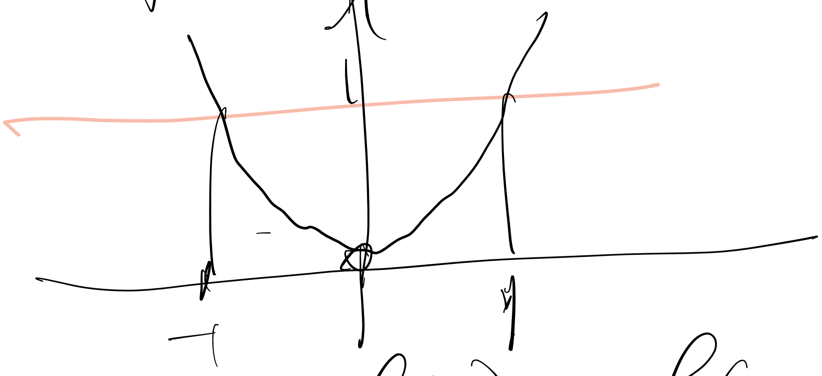
$$\boxed{f(x) = f(y) \Rightarrow x = y}$$

or: $x \neq y \Rightarrow f(x) \neq f(y)$

eg(1) $f(x) = e^x$ is 1-to-1



② $f(x)=x^2$ not 1-to-1



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

- <u>Surjective</u> (or, <u>onto</u>)

$f: S \to T$ is surj.

if $f(S)=T$

i.e. $\forall y \in T$, $\exists x \in S$ st. $f(x)=y$

$f(x) \quad y$

<u>Ex</u> $f(x) = e^x$

$f: \mathbb{R} \longrightarrow \mathbb{R}$ not surj (since $e^x > 0$)

$f: \mathbb{R} \longrightarrow \mathbb{R}_+ = \{y \mid y > 0\}$

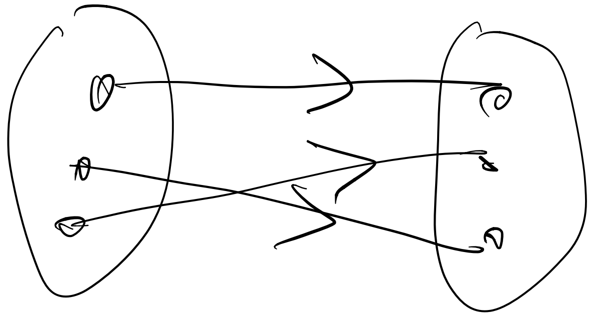
then f surj

f is a <u>bijection</u>

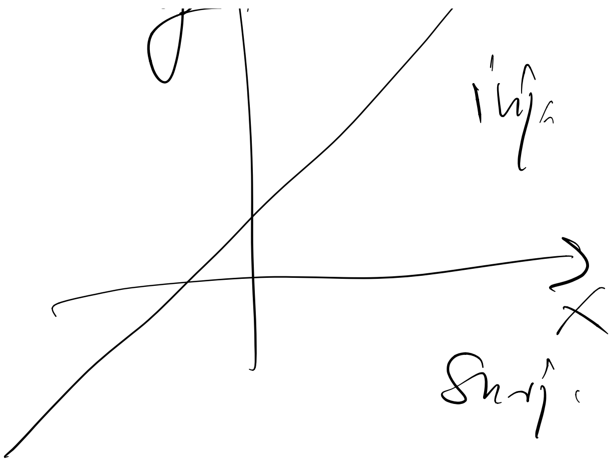
if it is both inj/surj

i.e., both one-to-one and onto

eg:



$f: \mathbb{R}_{u\wedge} \longrightarrow \mathbb{R}, \quad f(x) = 2x+1$



inj: $2x+1 = 2x'+1$

$\Rightarrow x = x'$

$y = 2x+1$

Surj: $\to x = \frac{y-1}{2}$

Composition of functions

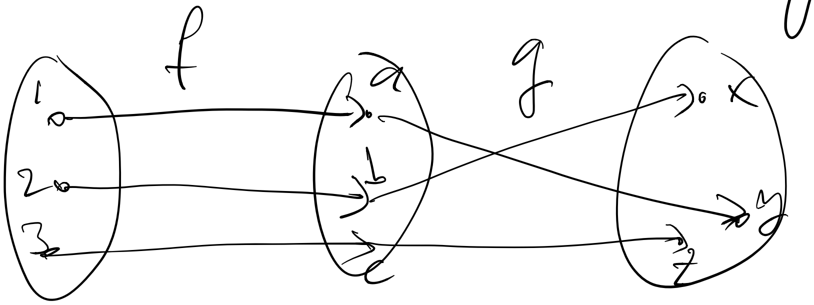
$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d] & B \arrow[r, "g"] & C \\
A \arrow[rr, "g \circ f"] & & C
\end{tikzcd}$$

↑ codomain of f = domain of g

$$\boxed{(g \circ f)(x) = g(f(x))}$$

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, phantom, sloped, "\ni"] & B \arrow[r, "g"] \arrow[d, phantom, sloped, "\ni"] & C \arrow[d, phantom, sloped, "\ni"] \\
x \arrow[r] & f(x) \arrow[r] & g(f(x))
\end{tikzcd}$$

eg: ①



$g \circ f$:
$1 \longrightarrow y$
$2 \longrightarrow x$
$3 \longrightarrow z$

②
$f: \mathbb{R} \to \mathbb{R} \quad f(x) = e^x$
$g: \mathbb{R} \to \mathbb{R} \quad g(x) = 2x+1$
$g \circ f: \mathbb{R} \to \mathbb{R}$

$$(g \circ f)(x) = g(f(x)) = g(e^x) = 2e^x + 1$$

$f \circ g: \mathbb{R} \to \mathbb{R}$

$$(f \circ g)(x) = f(g(x)) = f(2x+1) = e^{2x+1}$$

Inverse functions

If $f: S \to T$

is a bijection, then it has an *inverse* function,

$$g: T \longrightarrow S$$

which satisfies

$$g \circ f = id_T \qquad f \circ g = id_S$$

Here id_S is the *identity function* of S:

$$id_S : S \longrightarrow S$$
$$id_S(x) = x$$

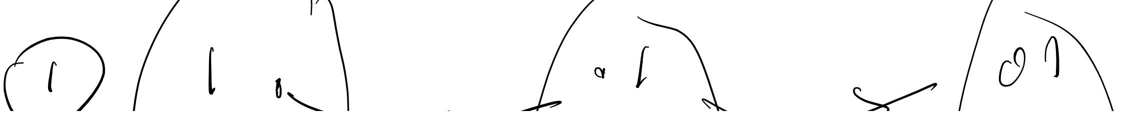
Notation We write $f^{-1} = g$ for this inverse function, which satisfies

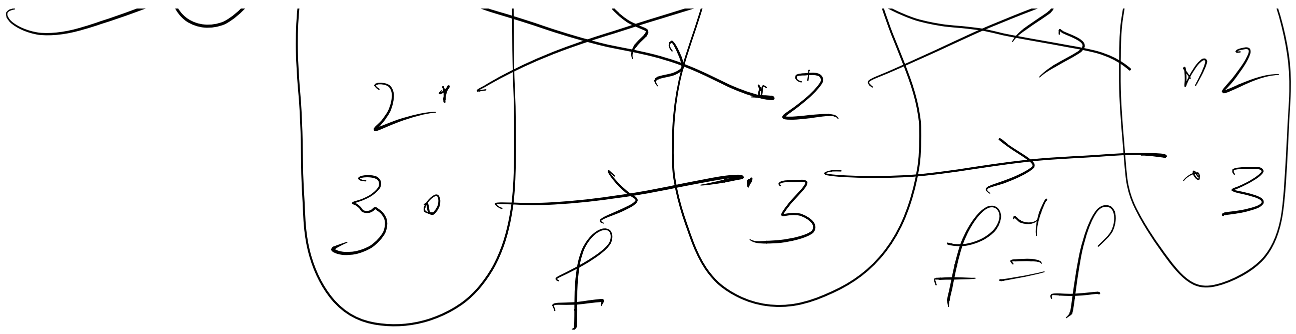
$$y = f(x) \Longleftrightarrow x = f^{-1}(y)$$

also:

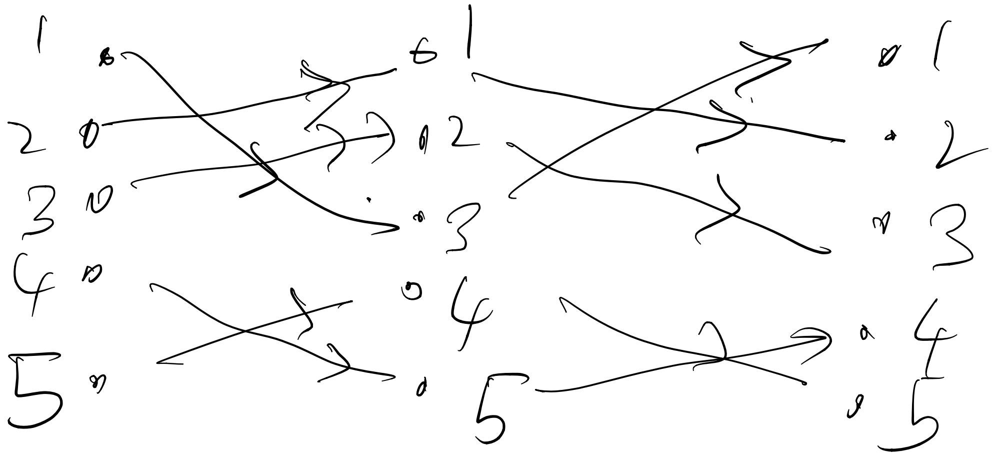
$$f(f^{-1}(y)) = y$$
$$f^{-1}(f(x)) = x$$

Ex ①





①



② $f: \mathbb{R} \to \mathbb{R}_{>0}$ $f(x)=e^x$

$f^{-1}: \mathbb{R}_{>0} \to \mathbb{R}$ $f^{-1}(x)=\ln x$

Permutations

Let S be a set

Define

$$\boxed{\mathrm{Sym}(S)}$$

to be the set of all bijections from S to S (also known as permutations of S)

i.e.

$$\mathrm{Sym}(S) = \{ f : S \to S \mid f \text{ bijection} \}$$

Basic example

$$S = \{1, 2, \dots, n\}$$

$$\mathrm{Sym}(S) := S_n$$

[we will call this the symmetric group on n elements]

II Binary operations

$$*: S \times S \longrightarrow S$$

$$(a,b) \longmapsto a*b$$

is a **binary operation** on the set S

Rem $(S,*)$ is called a **magma**

Examples

(1) $(\mathbb{N}, +)$ ← addition $\mathbb{N} = \{0, 1, 2, \dots\}$

$(\mathbb{N}, \cdot)$ ← multiplication

$(\mathbb{Z}, +)$ $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

$(\mathbb{Z}, \cdot)$ integers

same for $\mathbb{Q}$ rationals

$\mathbb{R}$ reals

$\mathbb{C}$ complex #

(2) $\mathcal{P}(S)$ power set of S

$\{A \subseteq S\}$ all subsets of S

eg: $S = \{0, 1, 2\}$

$\mathcal{P}(S) = \{\emptyset, \{0\}, \{1\}, \{2\},$

$\mathcal{P}(S) = \{\emptyset,$ [illegible]

$\{0,1\}, \{1,2\}, \{0,2\}, \{0,1,4\}\}$

$$\cup : \mathcal{P}(S) \times \mathcal{P}(S) \longrightarrow \mathcal{P}(S)$$

$$(A, B) \longmapsto A \cup B$$

So get $(\mathcal{P}(S), \cup)$

Similarly, $(\mathcal{P}(S), \cap)$

(3) $F = \mathrm{Fun}(S) = \{f : S \to S\}$

$$\circ : F \times F \longrightarrow F$$

$$(f, g) \longmapsto f \circ g$$

induces binary operation on $\mathrm{Sym}(S)$, since

f, g bijections $\Longrightarrow$ $f \circ g$ bijection

in fact

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

exercise!

(4) $M = \mathrm{Mat}_{n \times n}(\mathbb{R})$

$n \times n$ matrices w/entries in $\mathbb{R}$

$$M \times M \xrightarrow{\circ} M$$

$$(A, B) \longmapsto A \cdot B$$

multiplication

(matrix multiplication

eg: $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ $B = \begin{pmatrix} -1 & 1 \\ 2 & 0 \end{pmatrix}$

(n=2)

$$AB = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} -1+4 & -1+0 \\ -3+8 & 3+0 \end{pmatrix} = \begin{pmatrix} 3 & -1 \\ 5 & 3 \end{pmatrix}$$

III Monoids

Def A *monoid* is a set M endowed with a binary operation

$$*: M \times M \longrightarrow M$$

such that:

(1) [Associativity]

$$(a*b)*c = a*(b*c) \quad \forall a,b,c\in M$$

(2) [identity]

$\exists e\in M$ s.t.

$$e*a = a*e = a, \ \forall a\in M$$

Def M is commutative if $a*b = b*a$ $\forall a,b\in M$

Examples

(1) $(\mathbb{Z}, +, e=0)$

- $a+\boxed{0}=a=0+a$
- $(a+b)+c=a+(b+c)$

$(\mathbb{N}, +, e=0)$

$(\mathbb{N}, \cdot, e=1)$

$a\cdot\boxed{1}=a=\boxed{1}\cdot a$

(2) $(\mathcal{P}(S), \cup, e=\emptyset)$

$(A\cup B)\cup C=A\cup(B\cup C)$

$A\cup\boxed{\emptyset}=A=\boxed{\emptyset}\cup A$

$(\mathcal{P}(S), \cap, e=S)$

$$A \cap \boxed{S} = A = \boxed{S} \cap A$$

$$③ \left(\mathrm{Fun}(S), \circ, e = \mathrm{id}_S \right)$$

$$(f \circ g) \circ h = f \circ (g \circ h)$$

<u>exercise</u>!

$$f \circ \underset{\mathrm{id}_S}{\boxed{}} = f = \underset{\mathrm{id}_S}{\boxed{}} \circ f$$

$$\left(\mathrm{Sym}(S), \circ, e = \mathrm{id}_S \right)$$

$$(4) \left(\mathrm{Mat}_{n \times n}(\mathbb{R}), \cdot, e = I_n \right)$$

- $A \cdot (B \cdot C) = (A \cdot B) \cdot C$

<u>exercise</u>!

- $A \cdot \boxed{I_n} A = \boxed{I_n} \cdot A$

(4') $\left(GL_n(\mathbb{R}), \cdot, e=I_n\right)$

$\uparrow$

$n \times n$ invertible matrices

$A \cdot B$ is also invertible

$\uparrow$ $\uparrow$

invertible matrices

in fact

$$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$$

or: · A invertible $\Leftrightarrow \det(A) \neq 0$

· $\det(A \cdot B) = \det A \cdot \det B$

$\therefore$ $\det A \neq 0$, $\det B \neq 0$ $\Rightarrow \det(AB) \neq 0$