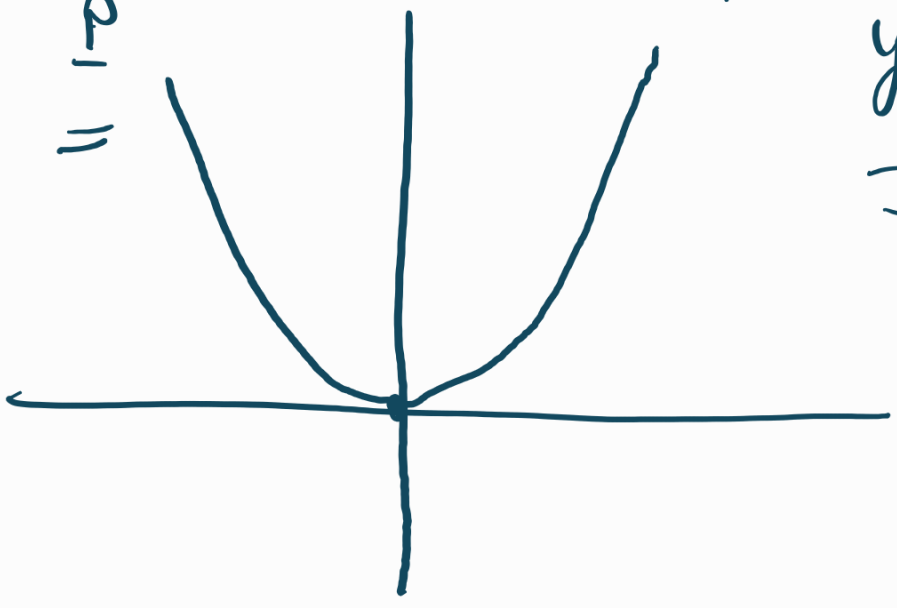
Overview / motivation

Parabola in plane $\mathbb{R}^2$

P = 

$y = x^2$

$$f(x,y) := y - x^2$$

$$P = Sol(f(x,y))$$

$$= \{(x,y) \mid f(x,y) = 0\}$$

This makes sense over

$\mathbb{F}_p = \{0, \dots, p-1\}$ p prime.

$+ \pmod p$

$\cdot \pmod p$

$$\mathrm{Sol}_{\mathbb{F}_p}\left(f(x,y)\right)$$

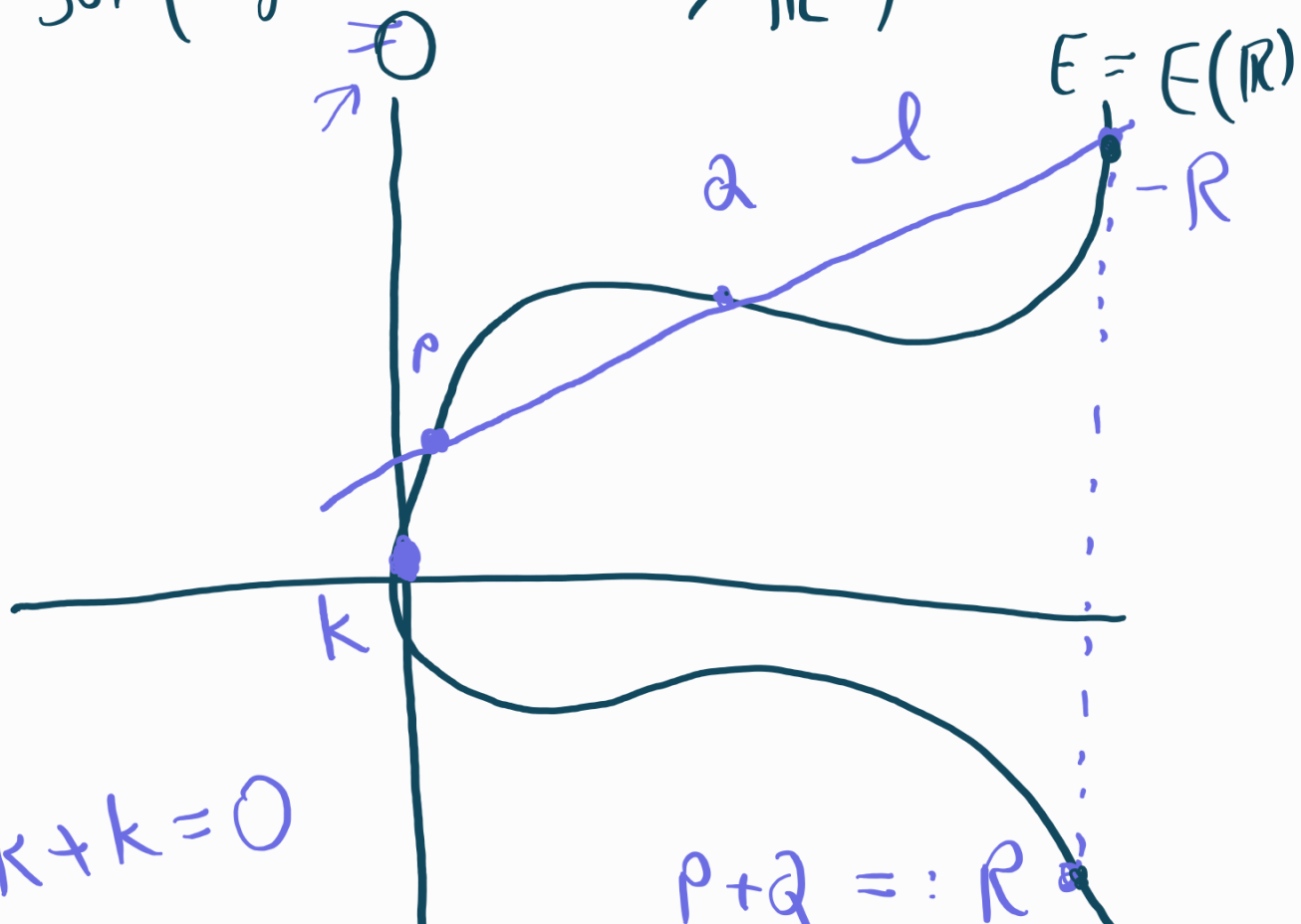
"Algebraic geometry"

Elliptic curve (over $\mathbb{R}$)

is an equation

$$E: y^2 = x^3 + ax + b \quad a, b \in \mathbb{R}$$

$$E(\mathbb{R}) = \mathrm{Sol}\left(y^2 - x^3 - ax - b \,/_{\mathbb{R}}\right)$$



$$+ : E(\mathbb{R}) \times E(\mathbb{R}) \to E(\mathbb{R})$$

This associative

$$(P+Q)+K = P+(Q+K)$$

$\rightsquigarrow$ $E(\mathbb{R})$ is an abelian gp.

If $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$

$$y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)$$

This makes sense over any field eg $\mathbb{F}_p$.

$\rightsquigarrow E(\mathbb{F}_p)$

admits

$$+ : E(\mathbb{F}_p) \times E(\mathbb{F}_p) \to E(\mathbb{F}_p)$$

that is an abelian gp.

Elliptic curves admits special maps $\rightsquigarrow$

$$e : E(\mathbb{F}_p) \times E(\mathbb{F}_p) \to \mathbb{F}_p$$

$\cup$ $\cup$

$$e : G_1 \times G_1 \to G_T$$

$$e(g^a, g^b) = e(g, g)^{ab}$$

BLS signature

Sets

A set S is a collection of elements such that for every object x (in a universe) x belongs to S ($x \in S$) or x does not belong to S ($x \notin S$).

e.g. (1) $S = \{1, 2, 3\}$

$= \{1, 1, 2, 3\}$.

(2) $S = \{x \mid^{x \text{ is an int}}_{x \geq 1}\}$

(3) $S = \{1, 2, 3, \ldots\}$

Famous sets

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

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

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; \begin{array}{c} a, b \in \mathbb{Z} \\ b \neq 0 \end{array} \right\}$$

$\mathbb{R}$ ———————

$$\mathbb{C} = \{ a + bi \mid a, b \in \mathbb{R} \}$$

$$i^2 = -1.$$

———————

empty set

for sets $\emptyset = \{ x \mid x \neq x \}$

$A \subseteq B$ if $\forall a \in A$

$a \in B$.

eg. $A = \{\emptyset\}$

Natural number as sets

$0 := \emptyset$ $\quad \emptyset \neq \{\emptyset\}$

$1 := \{\emptyset\}$

$2 := \{\emptyset, \{\emptyset\}\} = 0 \cup 1$

$3 := 0 \cup 1 \cup 2$

$= \emptyset \cup \{\emptyset\} \cup \{\emptyset, \{\emptyset\}\}$

$= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

Op'n on sets

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}.$$

if I a set of "indices" and $\forall i \in I$ A_i is a set.

$$\bigcup_{i \in I} A_i = \{ x \mid \exists i : x \in A_i \}$$

$$\bigcap_{i \in I} A_i = \{ x \mid \forall i \; x \in A_i \}.$$

Given objects a, b the ordered pair $O_{ab} := \{\{a\}, \{a,b\}\}$

$\forall a, b, a', b'$

Obs: $O_{ab} = O_{a'b'}$

$\iff a = a' \wedge b = b'$

Sketch: if $O_{ab} = O_{a'b'}$

then $\{\{a\}, \{a,b\}\}$

$$= \{\{a'\}, \{a', b'\}\}$$

So $\{a'\} \in \partial_{ab}$

$\Rightarrow \{a\} = \{a'\}$

$\Rightarrow a = a'$

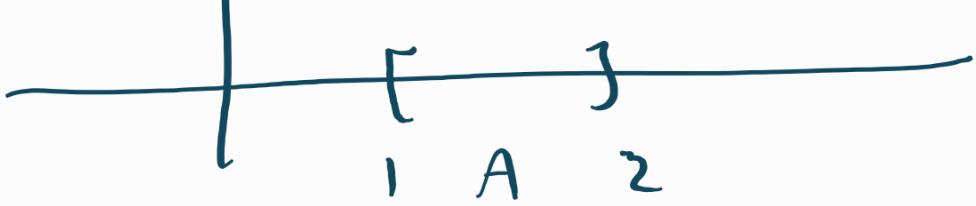
... $b = b'$.

Notation: $\partial_{ab} =: (a, b)$

Def: The cartesian product of set A, B is

$$A \times B := \{ (a,b) \mid \begin{array}{l} a \in A \wedge \\ b \in B \end{array} \}$$

e.g. $A = [1, 2]$ $B = [2, 3]$



$A = \{1, 2\}$ $B = \{3, 4\}$

$A \times B = \{(1,3), (1,4), (2,3), (2,4)\}$

- if A & B are finite

$$\# A \times B = \# A \cdot \# B.$$

"Def": Let A, B be sets.

a function f from A to B is a rule that assigns $\forall a \in A$ a unique element $f(a) \in B$.

Notation $f: A \to B$

$a \longmapsto f(a)$

A = "input set"

B = "output set"

f is machine

Def: A function f from A to B is a subset

"$Gr(f)$" $\subseteq A \times B$ s.th

" $\{(a, f(a)) \mid a \in A\}$ " $\{(a,b) \mid a \in A, b \in B\}$

(1) $\forall a \in A \; \exists b \in B$ s.th

$(a,b) \in f$

(2) if $\exists a \in A$, $b, b' \in B$

s.th $(a,b) \in f$

and $(a,b') \in f$

then $b = b'$

if $(a,b) \in f$ we denote

$$b =: f(a)$$

- If $A \neq \emptyset$ and $\#B \geq 2$ then $A \times B$ is never a function.

$b \neq b' \in B$

$(a,b) \in A \times B$

$(a,b') \in A \times B$

so (2) is not satisfied.

e.g: (1) $f : \mathbb{R} \longrightarrow \mathbb{R}$

$x \longmapsto x^2$

$f(x) = x^2$.

(2) $f : \mathbb{R} \longrightarrow \mathbb{R}_{\geq 0}$

$x \longmapsto x^2$

domain

$f \neq f'$

Note: two functions $f : A \to B$ and $g : C \to D$ are equal if range

$A = C \wedge B = D$

and $\forall a \in A \quad f(a) = g(a)$.

alt $f = g \subseteq A \times B$.

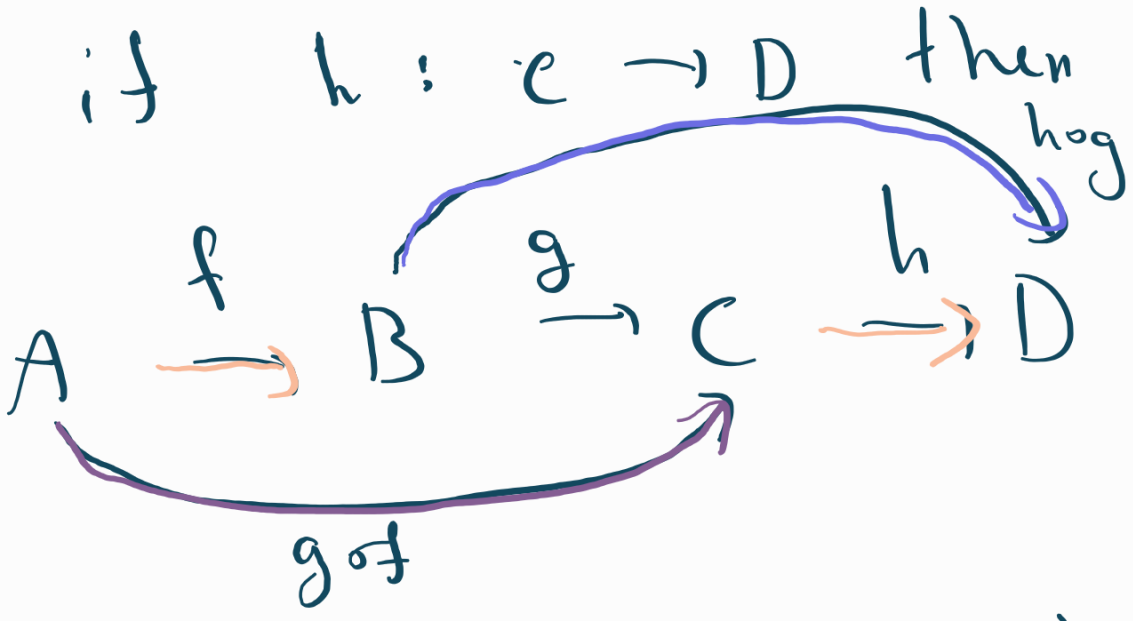
as sets.

- If $f : A \to B$ and $g : B \to C$ then we set composition.

$g \circ f : A \to C$

as $(g \circ f)(a) := g(f(a))$

obs: if $h : C \to D$ then



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

(associativity)

$$x \longmapsto y^3$$

e.g. $f : \mathbb{R} \to \mathbb{R} \xrightarrow{g} \mathbb{R}$

$$x \longmapsto x^2$$

$$g(f(x)) = (x^2)^3 = x^6.$$

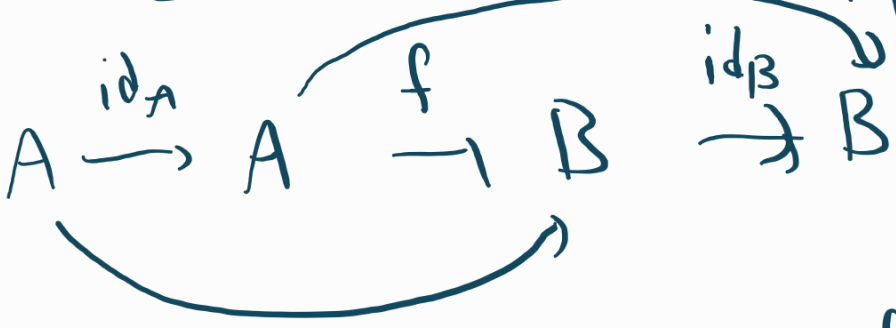
- $\forall$ set A, the identity

$$id_A : A \to A$$

$$a \longmapsto a.$$

exercise: $\forall f : A \to B$

id ∘ f = f ∘ id = f



$f \circ id_A$ $\qquad$ $id_B \circ f = f = f \circ id_A$.

Def: A function $f: A \to B$ is

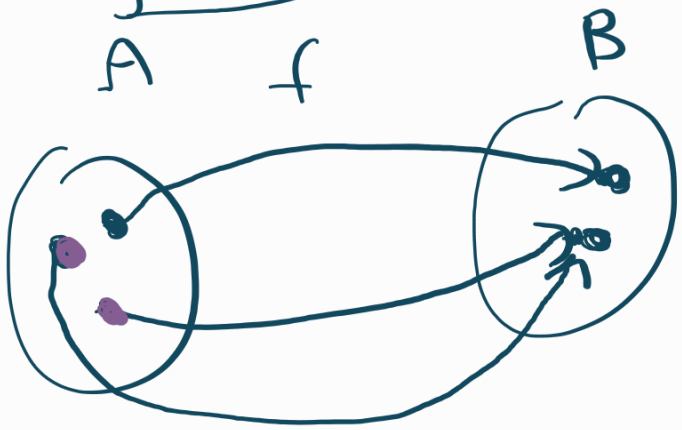
(1) injective if $\forall\, a \neq a' \in A$

$f(a) \neq f(a')$.

(2) surjective if $\forall\, b \in B$

$\exists\, a \in A$ s.th $f(a) = b$.

(3) bijective if inj + surj.



f is surj and not inj.

Proposition: for finite sets

A, B , Cantor diagonal argument

(1) $\#A \leq \#B$ iff $\#\mathbb{N} < \#\mathbb{R}$

$\exists$ inj $f: A \to B$.

(2) $\#A \geq \#B$ iff

$\exists$ surj $f: A \to B$

(3) $\#A = \#B$ iff

$\exists$ bijective $f: A \to B$.

Sketch: (1) if $\#A \leq \#B$,

enumerate A, B as

$A = \{a_1, \cdots, a_n\}$ $B = \{b_1, \cdots, b_k\}$

$n \leq k$. Define

$f: A \to B$

as $f(a_i) = b_i$

$\forall\ 1 \le i \le n$.

if $a_i \neq a_j$ then

clearly $f(a_i) = f(a_j)$

so f is injective

conversly, if $\exists$ inj

$f : A \to B$,

we enumerate A

$A = \{a_1, \dots, a_n\}$

$\Rightarrow B \supseteq \{f(a_1), \dots, f(a_n)\}$

↗

of size n

bcs f is inj

$\Rightarrow \quad \#B \geq n = \#A$ //

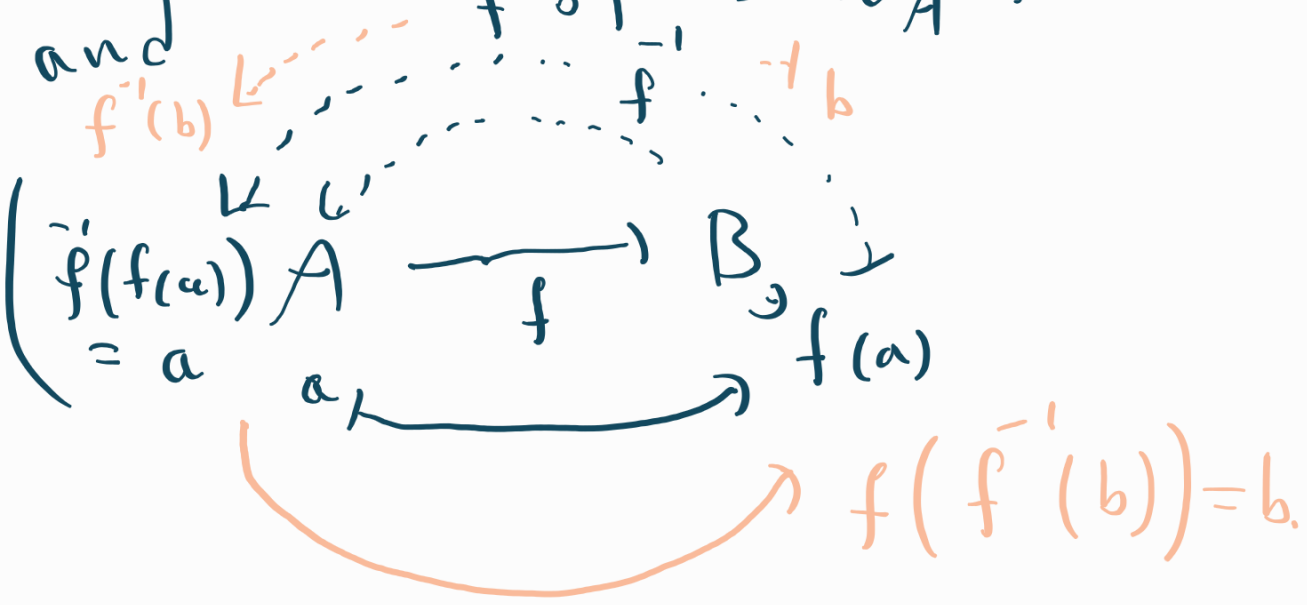
Prop: Let A, B be sets.

Then if $f: A \to B$

is bijective then $\exists\, f^{-1}: B \to A$

s.th $f \circ f^{-1} = id_B$

and $f^{-1} \circ f = id_A$.



Proof: $\forall\, b \in B$. Since f

is surj, $\exists$ $\$$ $a \in A$ s.th

$f(a) = b$. Since f is inj,

this a is unique.

So define $f^{-1}(b) = a$.

(this defines a function.)

(1) $f^{-1} \circ f = id_A$:

Let $a \in A$. Then $f^{-1}(f(a)) = a$.

(2) exercise. //

ZFC