Sets

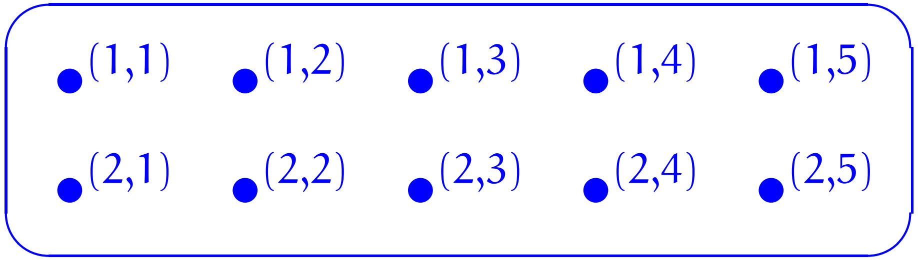
Lecturer: Dr Thomas Sauerwald (substituting Prof Glynn Winskel)

Objectives

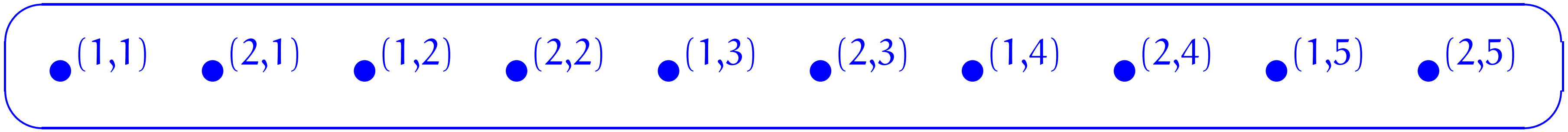
To introduce the basics of the theory of sets and some of its uses.

Abstract sets

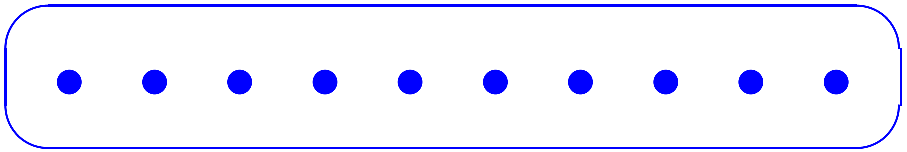
It has been said that a set is like a mental "bag of dots", except of course that the bag has no shape; thus,



may be a convenient way of picturing a certain set for some considerations, but what is apparently the same set may be pictured as



or even simply as



for other considerations.

Naive Set Theory

We are not going to be formally studying Set Theory here; rather, we will be *naively* looking at ubiquitous structures that are available within it.

Extensionality axiom

$\boxed{\text{Two sets are equal if they have the same elements.}}$

Thus,

$$\forall \text{ sets } A, B.\ A = B \iff (\forall x. x \in A \iff x \in B) \quad .$$

Example:

$$\{0\} \neq \{0, 1\} = \{1, 0\} \neq \{2\} = \{2, 2\}$$

Subsets and supersets

We say that A is a subset of B, denoted $A \subseteq B$, whenever

$$\forall x. x \in A \implies x \in B$$

Also B is a superset of A, denoted $B \supseteq A$.

Lemma 83

1. *Reflexivity.*

   For all sets A, $A \subseteq A$.

2. *Transitivity.*

   For all sets A, B, C, $(A \subseteq B \ \wedge \ B \subseteq C) \implies A \subseteq C$.

3. *Antisymmetry.*

   For all sets A, B, $(A \subseteq B \ \wedge \ B \subseteq A) \implies A = B$.

Separation principle

For any set A and any definable property P, there is a set containing precisely those elements of A for which the property P holds.

$$\{\, x \in A \mid P(x) \,\}$$

Note:

$$a \in \{x \in A \mid P(x)\} \Leftrightarrow (a \in A \wedge P(a))$$

Russell's paradox

Informal Statement:

> The barber is the "one who shaves all those, and those only, who do not shave themselves." The question is, does the barber shave himself?

Empty set

$$\emptyset \quad \text{or} \quad \{\,\}$$

defined by

$$\forall x.\, x \notin \emptyset$$

or, equivalently, by

$$\neg(\exists x.\, x \in \emptyset)$$

Using the Separation principle, we could also write

$$\{x \in A \mid x \neq x\}$$

Cardinality

The *cardinality* of a set specifies its size. If this is a natural number, then the set is said to be *finite*.

Typical notations for the cardinality of a set S are $\#S$ or $|S|$.

Example:

$$\#\emptyset = 0$$

Powerset axiom

For any set, there is a set consisting of all its subsets.

$$\mathcal{P}(U)$$

$$\forall X.\ X \in \mathcal{P}(U) \iff X \subseteq U \quad .$$

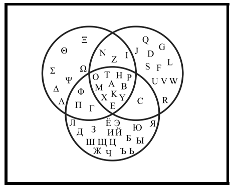
Hasse diagrams

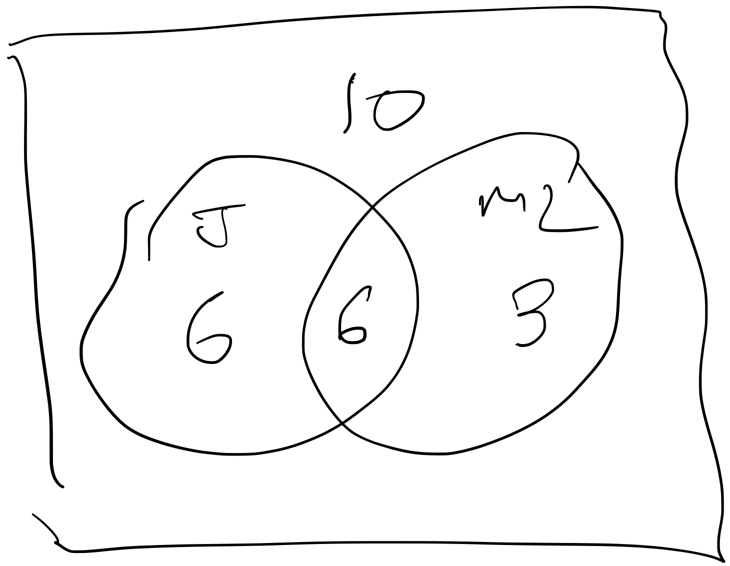
Proposition 84 *For all finite sets* U*,*

$$\#\,\mathcal{P}(\mathsf{U}) = 2^{\#\mathsf{U}} \quad .$$

PROOF IDEA:

Venn diagrams[a]





Quiz. In a class there are:

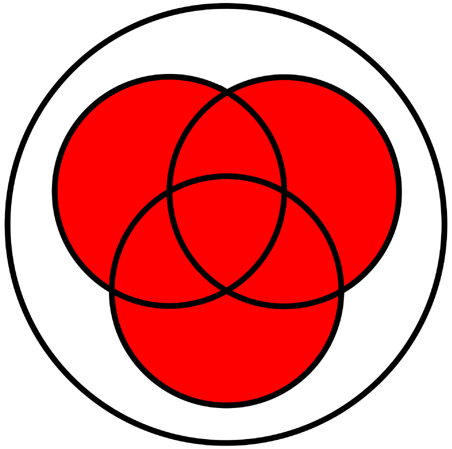
- 6 students who program in JAVA and ML
- 10 students who do not program anything
- 12 students who program in JAVA
- 9 students who program in ML

How many students are in the class?

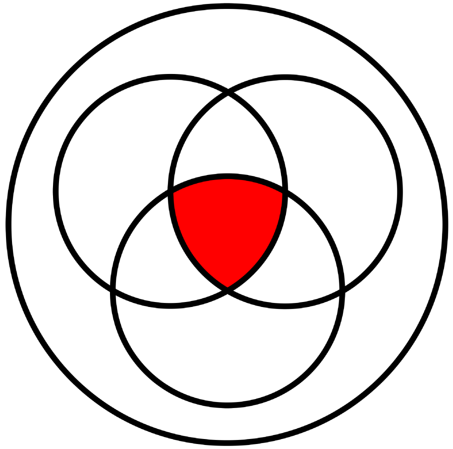
---

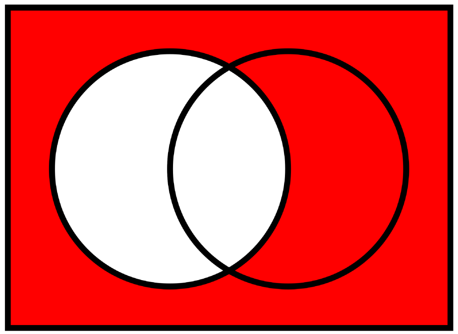
[a] From http://en.wikipedia.org/wiki/Intersection_(set_theory) .

Union



Intersection





Complement

The powerset Boolean algebra

$$(\quad \mathcal{P}(U) \;,\quad \emptyset \;,\quad U \;,\quad \cup \;,\quad \cap \;,\quad (\cdot)^c \quad)$$

For all $A, B \in \mathcal{P}(U)$,

$$\begin{aligned}
A \cup B &= \{\, x \in U \mid x \in A \ \vee\ x \in B \,\} &&\in \mathcal{P}(U) \\
A \cap B &= \{\, x \in U \mid x \in A \ \wedge\ x \in B \,\} &&\in \mathcal{P}(U) \\
A^c &= \{\, x \in U \mid \neg(x \in A) \,\} &&\in \mathcal{P}(U)
\end{aligned}$$

- The union operation $\cup$ and the intersection operation $\cap$ are associative, commutative, and idempotent.

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

$$(A \cap B) \cap C = A \cap (B \cap C) \quad , \quad A \cap B = B \cap A \quad , \quad A \cap A = A$$

- The *empty set* $\emptyset$ is a neutral element for $\cup$ and the *universal set* $\mathcal{U}$ is a neutral element for $\cap$.

$$\emptyset \cup A \;=\; A \;=\; \mathcal{U} \cap A$$

- The union operation $\cup$ and the intersection operation $\cap$ are associative, commutative, and idempotent.

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

$$(A \cap B) \cap C = A \cap (B \cap C) \ , \quad A \cap B = B \cap A \ , \quad A \cap A = A$$

- The *empty set* $\emptyset$ is a neutral element for $\cup$ and the *universal set* $\mathcal{U}$ is a neutral element for $\cap$.

$$\emptyset \cup A \ = \ A \ = \ \mathcal{U} \cap A$$

- The empty set $\emptyset$ is an annihilator for $\cap$ and the universal set $\mathcal{U}$ is an annihilator for $\cup$.

$$\emptyset \cap A = \emptyset$$

$$\mathcal{U} \cup A = \mathcal{U}$$

- With respect to each other, the union operation $\cup$ and the intersection operation $\cap$ are distributive and absorptive.

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \ , \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

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

- The empty set $\emptyset$ is an annihilator for $\cap$ and the universal set $\mathcal{U}$ is an annihilator for $\cup$.

$$\emptyset \cap A = \emptyset$$

$$\mathcal{U} \cup A = \mathcal{U}$$

- With respect to each other, the union operation $\cup$ and the intersection operation $\cap$ are distributive and absorptive.

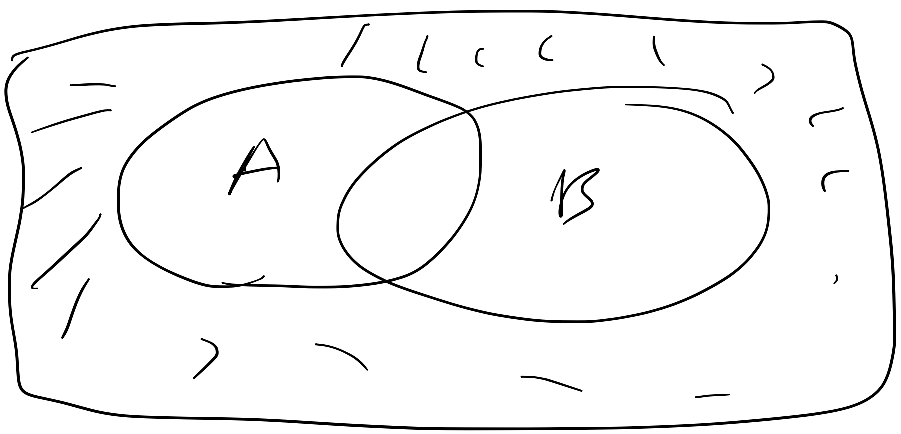
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad , \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cup (A \cap B) \; = \; A \; = \; A \cap (A \cup B)$$

- The complement operation $(\cdot)^c$ satisfies complementation laws.

$$A \cup A^c = \mathcal{U} \ , \quad A \cap A^c = \emptyset$$

- De Morgan's Law: $(A \cup B)^c = ??$ $\quad A^c \cap B^c$



Proposition 85 *Let* U *be a set and let* $A, B \in \mathcal{P}(U)$.

1. $\forall X \in \mathcal{P}(U).\ A \cup B \subseteq X \iff (A \subseteq X \wedge B \subseteq X)$.
2. $\forall X \in \mathcal{P}(U).\ X \subseteq A \cap B \iff (X \subseteq A \wedge X \subseteq B)$.

PROOF: (1) Let $X \subseteq U$.

($\Rightarrow$) Assume $A \cup B \subseteq X$. $A \subseteq A \cup B \subseteq X$

$\therefore A \subseteq X$.

($\Leftarrow$) $A \subseteq X \wedge B \subseteq X$

Let $u \in A \cup B$. Case $u \in A$ $\therefore u \in X$

Case $u \in B$. $\therefore u \in X$.

Corollary 86 *Let* U *be a set and let* $A, B, C \in \mathcal{P}(U)$.

1. $$C \underset{\subseteq}{\overset{\supseteq}{=}} A \cup B$$

$\Uparrow$ $\Downarrow$ *iff*

$$\big[A \subseteq C \wedge B \subseteq C\big]$$

$$\wedge$$

$$\big[\forall X \in \mathcal{P}(U).\ (A \subseteq X \ \wedge\ B \subseteq X) \implies C \subseteq X\big]$$

2. $$C = A \cap B$$

iff

$$\big[C \subseteq A \wedge C \subseteq B\big]$$

$$\wedge$$

$$\big[\forall X \in \mathcal{P}(U).\ (X \subseteq A \ \wedge\ X \subseteq B) \implies X \subseteq C\big]$$

Sets and logic

$\{x \in U \mid P(x)\}$ $\qquad$ $P(x)$

$\mathcal{P}(\mathbb{U})$	$\{$ **false**, **true** $\}$
$\emptyset$	**false**
$\mathbb{U}$	**true**
$\cup$	$\vee$
$\cap$	$\wedge$
$(\cdot)^{c}$	$\neg(\cdot)$

$\{x \in U \mid \text{false}\}$

$\{x \in U \mid \text{true}\}$

$\{x \in U \mid P(x)\} \cup \{x \in U \mid Q(x)\}$

$\cap$

$\{x \in U \mid \neg P(x)\}$

$= \{x \in U \mid P(x)\}^{c}$

fa

$P(x) \vee Q(x)$

$\wedge$

$\neg P(x)$

Pairing axiom

For every a and b, there is a set with a and b as its only elements.

$$\{a, b\}$$

defined by

$$\forall x.\, x \in \{a, b\} \iff (x = a \lor x = b)$$

NB The set $\{a, a\}$ is abbreviated as $\{a\}$, and referred to as a *singleton*.

Examples:

- $\#\{\emptyset\} = 1$
- $\#\{\{\emptyset\}\} = 1$
- $\#\{\emptyset, \{\emptyset\}\} = 2$

Ordered pairing

For every pair a and b, the set

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

is abbreviated as

$$\langle a, b\rangle$$

and referred to as an *ordered pair*.

$\{a, \emptyset\} \neq \{a\}$ if $a \neq \emptyset$.

Proposition 87 (Fundamental property of ordered pairing)

For all a, b, x, y,

$$\langle a, b\rangle = \langle x, y\rangle \iff (a = x \wedge b = y) \quad .$$

PROOF: $(\Rightarrow)$ Ass. $\{\{a\}, \{a, b\}\} = \{\{x\}, \{x, y\}\}$.

Case $a = b$. lhs $= \{\{a\}\}$. $\therefore \{x\} = \{a\}$ $\therefore x = a$.

Also $\{x, y\} = \{a\}$ $y = a$.

Case $a \neq b$.

. . . .

Products

The *product* $A \times B$ of two sets A and B is the set

$$A \times B = \{\, x \mid \exists\, a \in A, b \in B.\, x = (a, b)\,\}$$

$$= \{\ (a,b) \mid a \in A \wedge b \in B \}$$

where

$$\forall a_1, a_2 \in A, b_1, b_2 \in B.$$
$$(a_1, b_1) = (a_2, b_2) \iff (a_1 = a_2 \wedge b_1 = b_2) \quad .$$

Thus,

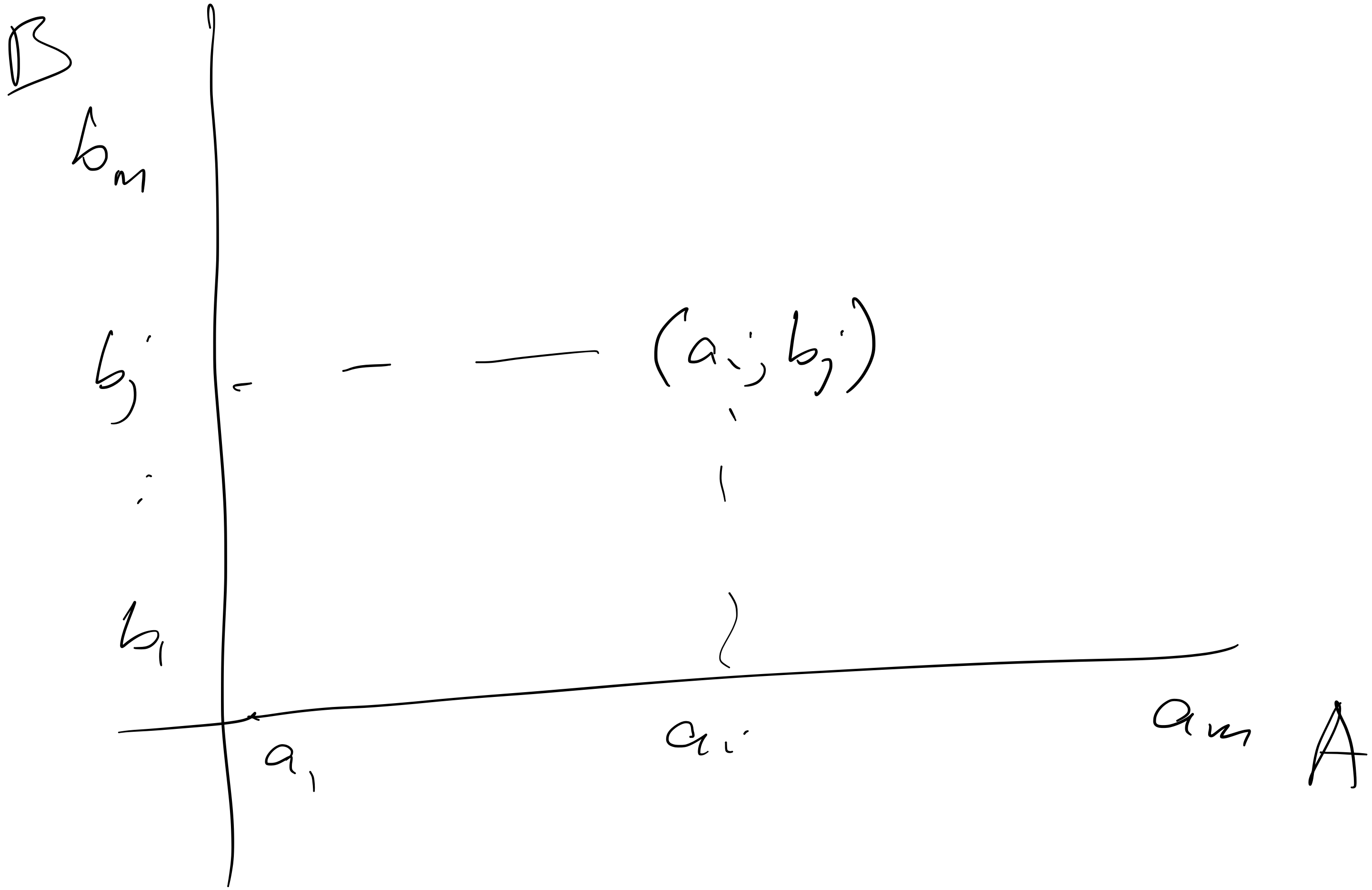
$$\forall\, x \in A \times B.\, \exists!\, a \in A.\, \exists!\, b \in B.\, x = (a, b) \quad .$$

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

Proposition 89 *For all finite sets* A *and* B, $= \{b_1, \dots, b_m\}$

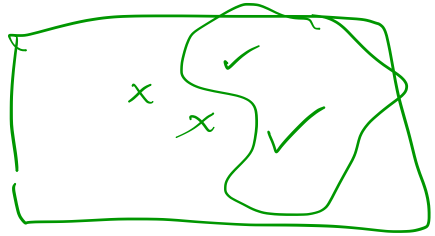
$$\#(A \times B) = \#A \cdot \#B \quad .$$

PROOF IDEA:



Set Comprehension/Separation: Given a set $\mathcal{U}$ and a property $Q(x)$, $x \in \mathcal{U}$, can form set

$$\{x \in \mathcal{U} \mid Q(x)\}.$$



Powerset axiom: Given a set $\mathcal{U}$ can form

$$P(\mathcal{U}) = \{X \mid X \subseteq \mathcal{U}\}.$$

$$X \in P(\mathcal{U}) \iff X \subseteq \mathcal{U}.$$

$\mathcal{F} = \emptyset$

$\bigcup \mathcal{F} = \emptyset$

Big unions

$\mathcal{F} \subseteq \mathcal{P}(U)$

Definition 90 *Let* $\mathcal{U}$ *be a set. For a collection of sets* $\mathcal{F} \in \mathcal{P}(\mathcal{P}(\mathcal{U}))$*, we let the* big union *(relative to* $\mathcal{U}$*) be defined as*

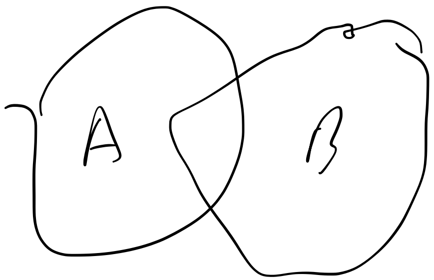
$$\bigcup \mathcal{F} = \{\, x \in \mathcal{U} \mid \exists A \in \mathcal{F}.\, x \in A \,\} \in \mathcal{P}(\mathcal{U}) \quad .$$

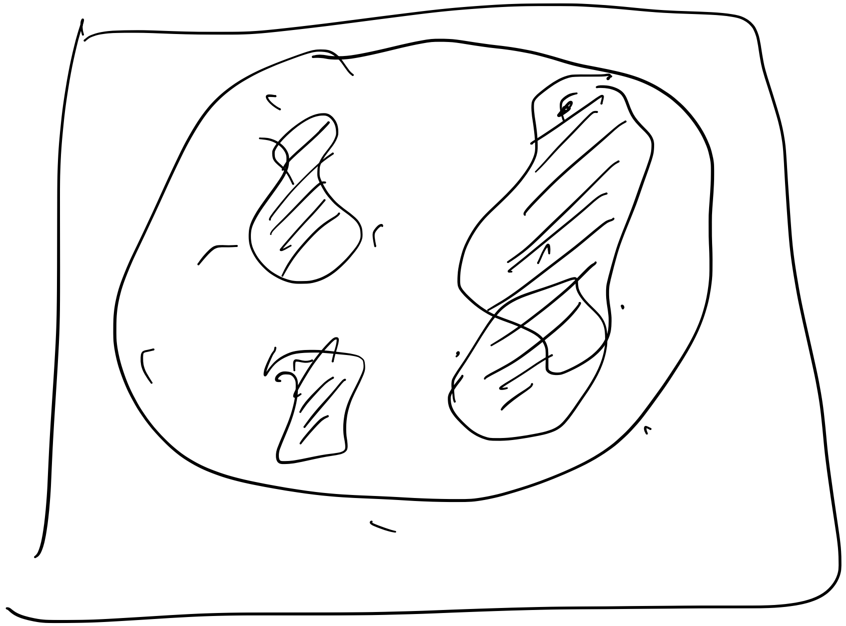
$x \in \bigcup \mathcal{F} \iff \exists A \in \mathcal{F}.\, x \in A$

$A, B \subseteq U$

$\mathcal{F} = \{A, B\}$

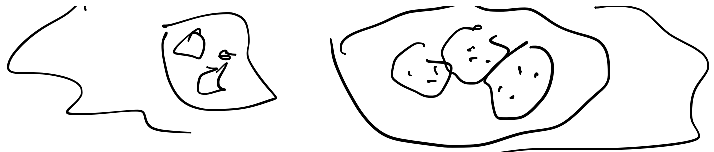
$\bigcup \mathcal{F} = A \cup B$





$\mathcal{F} = \{A, B, C\}$

$\bigcup \mathcal{F} = (A \cup B) \cup C = A \cup (B \cup C)$



Proposition 91 *For all* $\mathcal{F} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(U)))$, $\qquad \mathcal{Y} \subseteq \mathcal{P}(\mathcal{P}(U))$

$$\bigcup\big(\bigcup \mathcal{F}\big) = \bigcup\Big\{ \bigcup \mathcal{A} \in \mathcal{P}(U) \;\Big|\; \mathcal{A} \in \mathcal{F} \Big\} \in \mathcal{P}(U) .$$

PROOF: $\quad u \in \bigcup(\bigcup \mathcal{Y}) \iff u \in X \wedge X \in \bigcup \mathcal{Y}$ for some X.

$\iff u \in X \wedge X \in \mathcal{A} \wedge \mathcal{A} \in \mathcal{Y}$ for some X, $\mathcal{A}$.

$\iff u \in \bigcup \mathcal{A} \wedge \mathcal{A} \in \mathcal{Y}$ for some $\mathcal{A}$.

$\iff u \in \bigcup\{\bigcup \mathcal{A} \mid \mathcal{A} \in \mathcal{Y}\}$

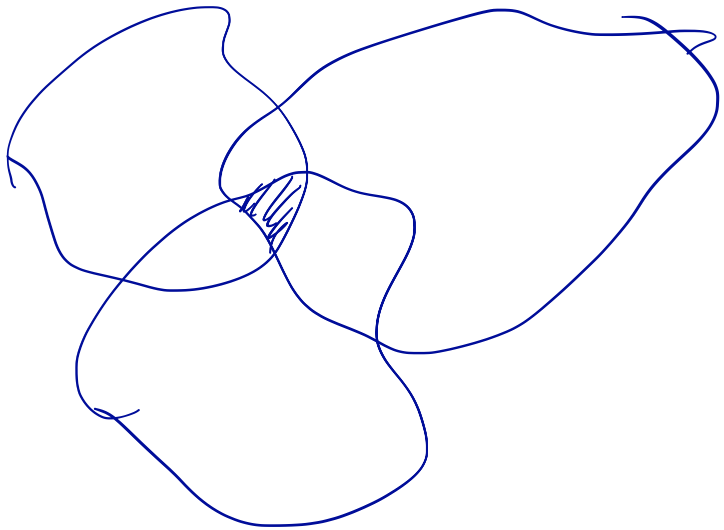
Big intersections

Definition 92 *Let U be a set. For a collection of sets $\mathcal{F} \subseteq \mathcal{P}(U)$, we let the* big intersection *(relative to U) be defined as*

$\forall A. (A \in \mathcal{Y} \Rightarrow x \in A)$

$$\bigcap \mathcal{F} = \{ x \in U \mid \forall A \in \mathcal{F}. x \in A \} .$$

$x \in \bigcap \mathcal{Y} \iff \forall A \in \mathcal{Y}. x \in A$



$\mathcal{Y} = \emptyset$

$\bigcap \mathcal{Y} = U$

$\mathcal{Y} = \{A, B\}$

$\bigcap \mathcal{Y} = A \cap B$

Theorem 93 *Let*

$$\mathcal{F} = \left\{ S \subseteq \mathbb{R} \;\middle|\; (0 \in S) \wedge (\forall x \in \mathbb{R}.\, x \in S \implies (x+1) \in S) \right\} .$$

Then, (i) $\mathbb{N} \in \mathcal{F}$ *and* (ii) $\mathbb{N} \subseteq \bigcap \mathcal{F}$. *Hence,* $\bigcap \mathcal{F} = \mathbb{N}$.

$\bigcap \mathcal{F} \subseteq \mathbb{N}$

PROOF:

(ii) RTP $\mathbb{N} \subseteq S$ for all $S \in \mathcal{F}$.

By M.I.,

Base: $0 \in S$

Step: $n \in \mathbb{N}$ $n \in S \implies (n+1) \in S$

$$\frac{b_1 : Bexp \quad b_2 : Bexp}{b_1 \wedge b_2 : Bexp} \qquad \overline{0} \qquad \frac{x : \mathbb{N}}{x+1 : \mathbb{N}}$$

$$\frac{\langle c, \sigma \rangle \longrightarrow \sigma' \quad \langle d, \sigma' \rangle \longrightarrow \sigma''}{\langle c; d; \sigma \rangle \longrightarrow \sigma''}$$

Union axiom

set

Every collection of sets has a union.

$$\bigcup \mathcal{F}$$

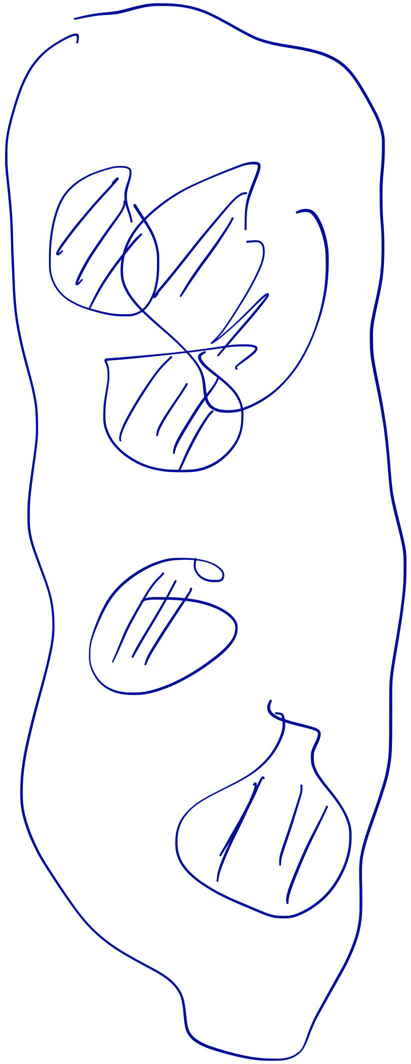
$$x \in \bigcup \mathcal{F} \iff \exists X \in \mathcal{F}. x \in X$$

$$\bigcup \mathcal{Y} =_{def} \{x \mid \exists X \in \mathcal{Y}. x \in X\}$$

$$\bigcup \emptyset = \emptyset$$

$$x \in \bigcup \emptyset \iff \exists X \in \emptyset. x \in X \iff \exists X. X \in \emptyset \wedge x \in X$$

$$\iff \text{false}$$



For *non-empty* $\mathcal{F}$ we also have

$$\bigcap \mathcal{F}$$

$\forall X .\ x \notin X \Rightarrow X \notin \emptyset .$

defined by

$$\forall x.\ x \in \bigcap \mathcal{F} \iff (\forall X \in \mathcal{F} . x \in X) \quad .$$

$\bigcap \mathcal{Y} = \{ x \mid \forall X \in \mathcal{Y}, x \in X \}$

$x \in \bigcap \emptyset \iff \forall X \in \emptyset .\ x \in X .$

$\iff \forall X .\ X \in \emptyset \Rightarrow x \in X \iff$ true

$\bigcap \emptyset = \{ x \mid \text{any old } x \}$ Russell!

Disjoint unions

Definition 94 *The* disjoint union $A \uplus B$ *of two sets* A *and* B *is the set*

$$A \uplus B \;=\; \big(\{1\} \times A\big) \cup \big(\{2\} \times B\big) \quad .$$

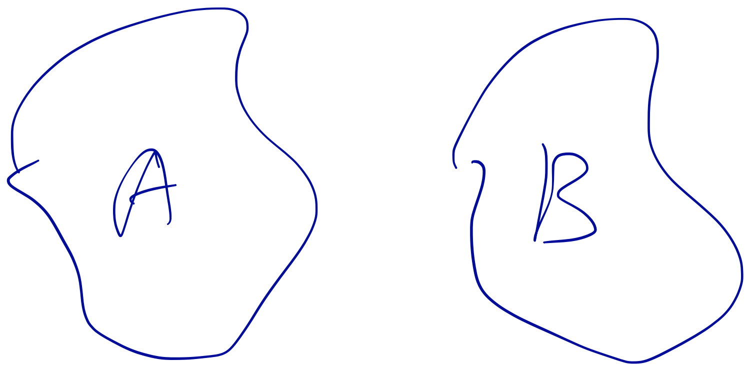
Thus,

$$\forall\, x.\, x \in (A \uplus B) \iff \big(\exists a \in A.\, x = (1, a)\big) \,\vee\, \big(\exists b \in B.\, x = (2, b)\big) \,.$$

Proposition 96 *For all finite sets* A *and* B,

$$\mathrm{A} \cap \mathrm{B} = \emptyset \implies \#(\mathrm{A} \cup \mathrm{B}) = \#\mathrm{A} + \#\mathrm{B} \quad .$$

PROOF IDEA:



Corollary 97 *For all finite sets* A *and* B,

$$\#(\mathrm{A} \uplus \mathrm{B}) = \#\mathrm{A} + \#\mathrm{B} \quad .$$

A, B not nec. disjoint

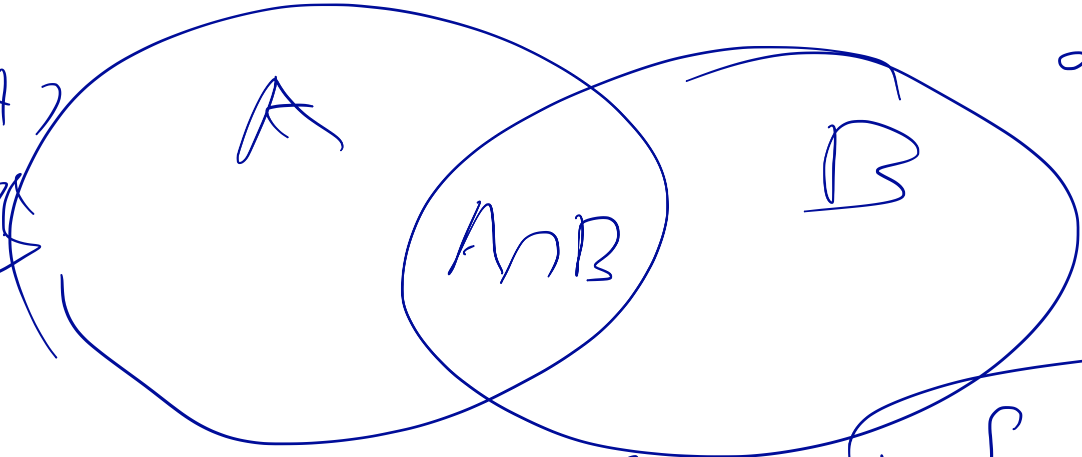
$$\#(A \cup B)$$

$$= \#(A) + \#(B) - \#(A \cap B)$$

$$\{x \in U \mid P(x)\} \in \mathcal{P}(U)$$

$$\{\textstyle\bigcup A \mid A \in \mathcal{Y}\}$$

$$\{y \mid \exists x.\ y = x+1 \wedge x \in \mathbb{N}\}$$



$$= \{x+1 \mid x \in \mathbb{N}\}$$

$$\boxed{\{e(x) \mid P(x)\}}$$

Relations

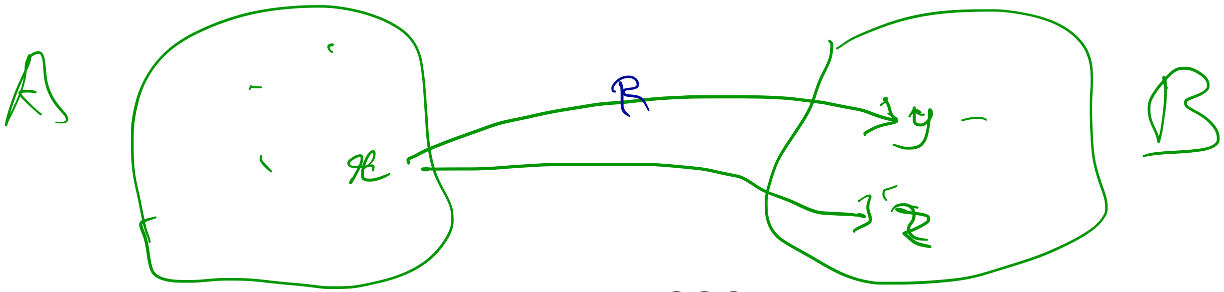
Definition 99 *A* <u>(binary) relation</u> R *from a set* A *to a set* B

$$\mathrm{R} : \mathrm{A} \longrightarrow\!\!\!\!\!\!+\;\; \mathrm{B} \quad \textit{or} \quad \mathrm{R} \in \mathrm{Rel}(\mathrm{A}, \mathrm{B}) \quad ,$$

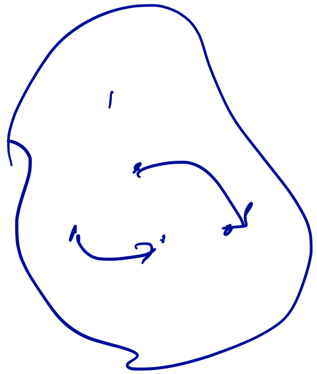
is

$$\mathrm{R} \subseteq \mathrm{A} \times \mathrm{B} \quad \textit{or} \quad \mathrm{R} \in \mathcal{P}(\mathrm{A} \times \mathrm{B}) \quad .$$

Notation 100 *One typically writes* $\mathrm{a}\,\mathrm{R}\,\mathrm{b}$ *for* $(\mathrm{a}, \mathrm{b}) \in \mathrm{R}$*.*



Informal examples: states



- Computation.

  $t : \mathrm{Bool}$

- Typing.

  $t \sim s$

- Program equivalence.

- Networks.
- Databases.

Examples:

- Empty relation.

  $\emptyset : A \leftrightarrow B$ $\qquad$ $(a\ \emptyset\ b \iff \mathbf{false})$

- Full relation.

  $(A \times B) : A \leftrightarrow B$ $\qquad$ $(a\ (A \times B)\ b \iff \mathbf{true})$

- Identity (or equality) relation.

  $\mathrm{id}_A = \{\ (a, a) \mid a \in A\ \} : A \leftrightarrow A$ $\qquad$ $(a\ \mathrm{id}_A\ a' \iff a = a')$

- Integer square root.

  $R_2 = \{\ (m, n) \mid m = n^2\ \} : \mathbb{N} \leftrightarrow \mathbb{Z}$ $\qquad$ $(m\ R_2\ n \iff m = n^2)$

Internal diagrams

$S \circ R : A \nrightarrow C$ $\quad R : A \nrightarrow B$

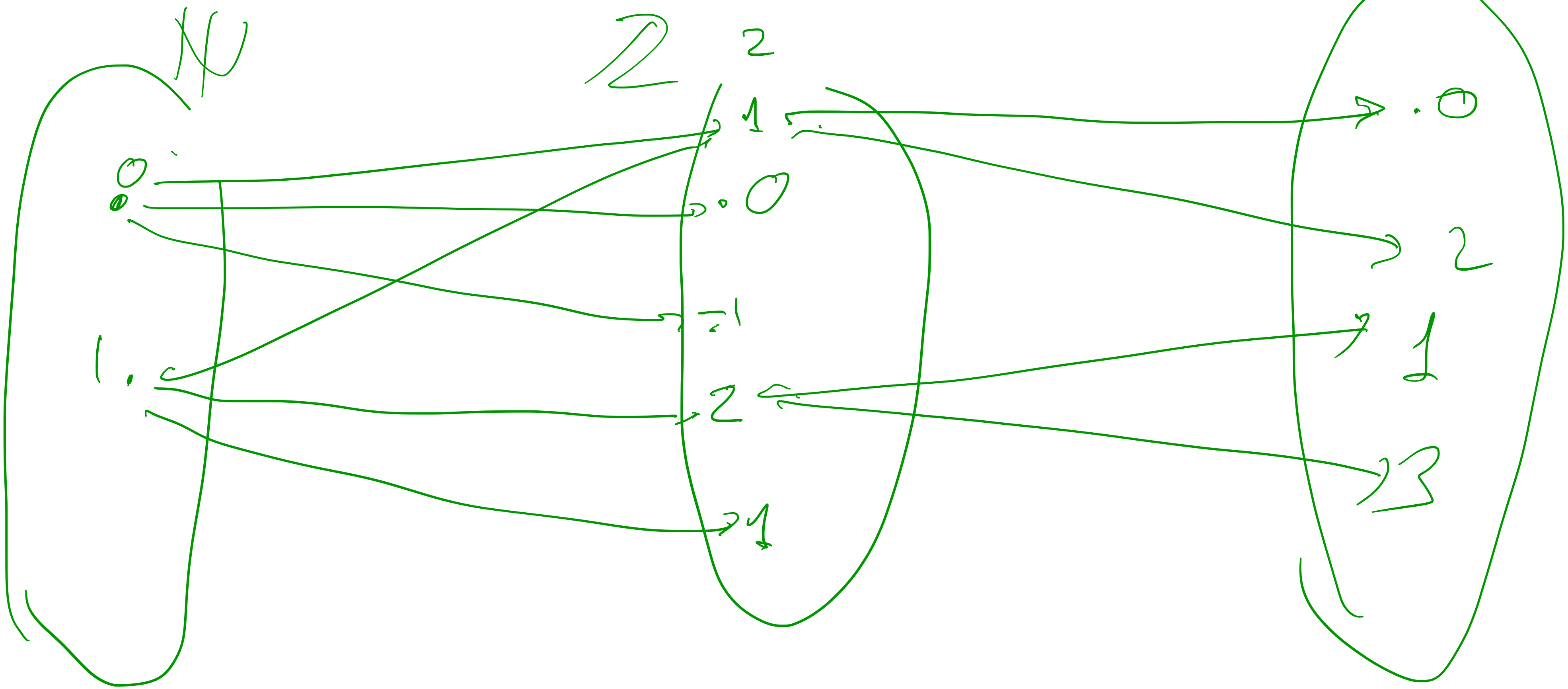
$S : B \nrightarrow C$

Example:

$$R = \{\, (0,0), (0,-1), (0,1), (1,2), (1,1), (2,1) \,\} : \mathbb{N} \nrightarrow \mathbb{Z}$$

$\mathbb{Z}$

$$S = \{\, (1,0), (1,2), (2,1), (2,3) \,\} : \mathbb{Z} \nrightarrow \mathbb{Z}$$



Relational extensionality

$$R = S : A \nrightarrow B$$

iff

$$\forall a \in A.\, \forall b \in B.\; a\, R\, b \iff a\, S\, b$$

$$\{(a,b) \mid a R b\} = \{(a,b) \mid a S b\}$$

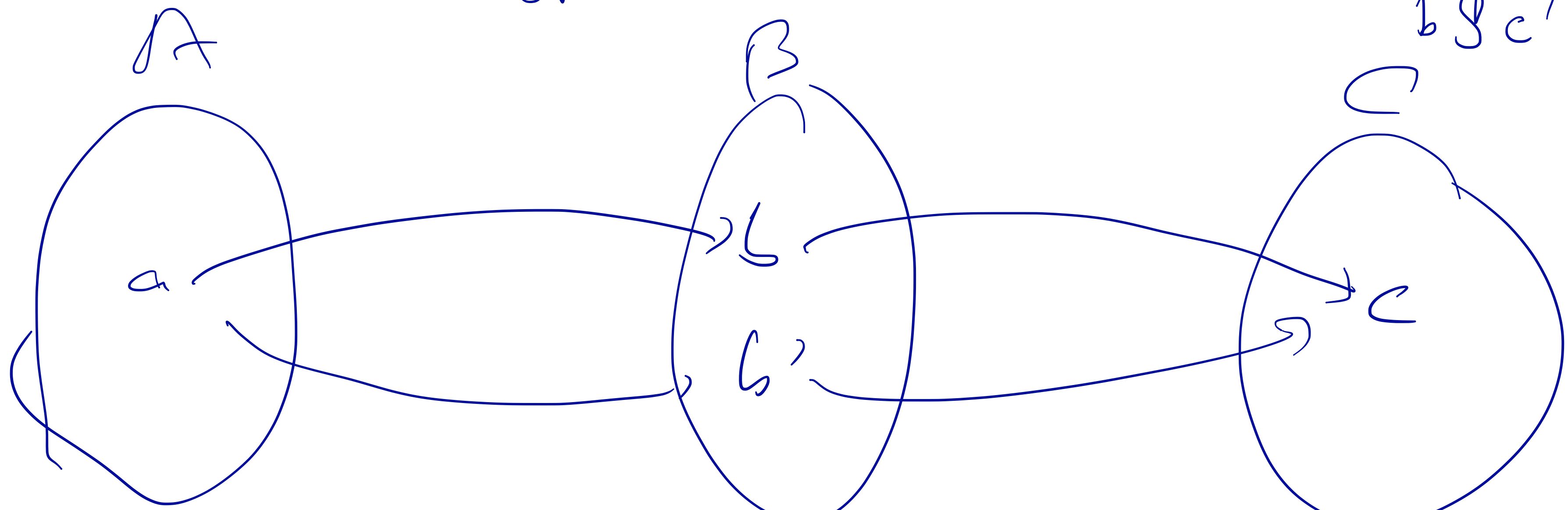
Relational composition

$$R : A \relbar\!\!\!+\!\!\!\rightarrow B \qquad S : B \relbar\!\!\!+\!\!\!\rightarrow C \implies S \circ R : A \relbar\!\!\!+\!\!\!\rightarrow C$$

$$a \; S \circ R \; c \quad \text{iff}$$

$$\exists b \in B.\; a \, R \, b \;\wedge\; b \, S \, c$$

$$(a, c) \in S \circ R \quad \text{iff} \quad (a, c) \in \{ (a', c') \mid \exists b.\; a' R b \wedge b S c' \}$$



Theorem 102 *Relational composition is associative and has the identity relation as neutral element.*

- *Associativity.*

  For all $R : A \nrightarrow B$, $S : B \nrightarrow C$, *and* $T : C \nrightarrow D$,

  $$(T \circ S) \circ R = T \circ (S \circ R)$$

  Can write $T \circ S \circ R$

- *Neutral element.*

  $id_A : A \nrightarrow A$

  For all $R : A \nrightarrow B$,

  $$R \circ id_A = R = id_B \circ R \quad .$$

$$(T \circ S) \circ R \overset{?}{=} T \circ (S \circ R)$$

$$(a,d) \in {}^{D}(T \circ {}^{C}S) \circ {}^{B}R^{A} \iff \exists b \in B.\ (a,b) \in R \land (b,d) \in T \circ S$$

$$\iff \exists b \in B.\ (a,b) \in R \land \exists c \in C.\ (b,c) \in S \land (c,d) \in T$$

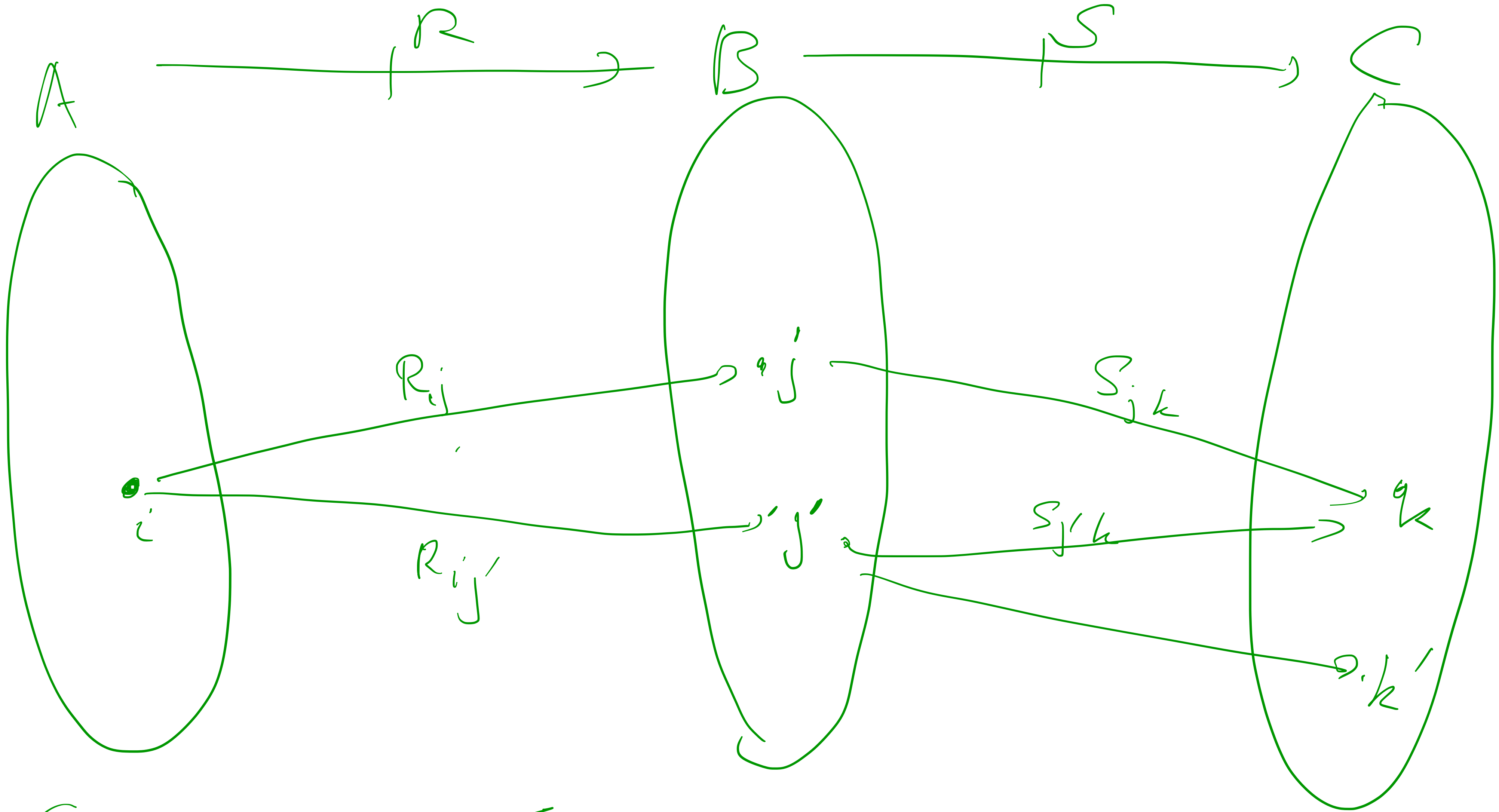
$$\iff \exists b \in B.\ \exists c \in C.\ (a,b) \in R \land (b,c) \in S \land (c,d) \in T$$

$$\vdots$$

$$\iff (a,d) \in T \circ (S \circ R)$$

Provided x not in φ

$$\exists x.\ \varphi \land \psi \iff \varphi \land \exists x\, \psi$$



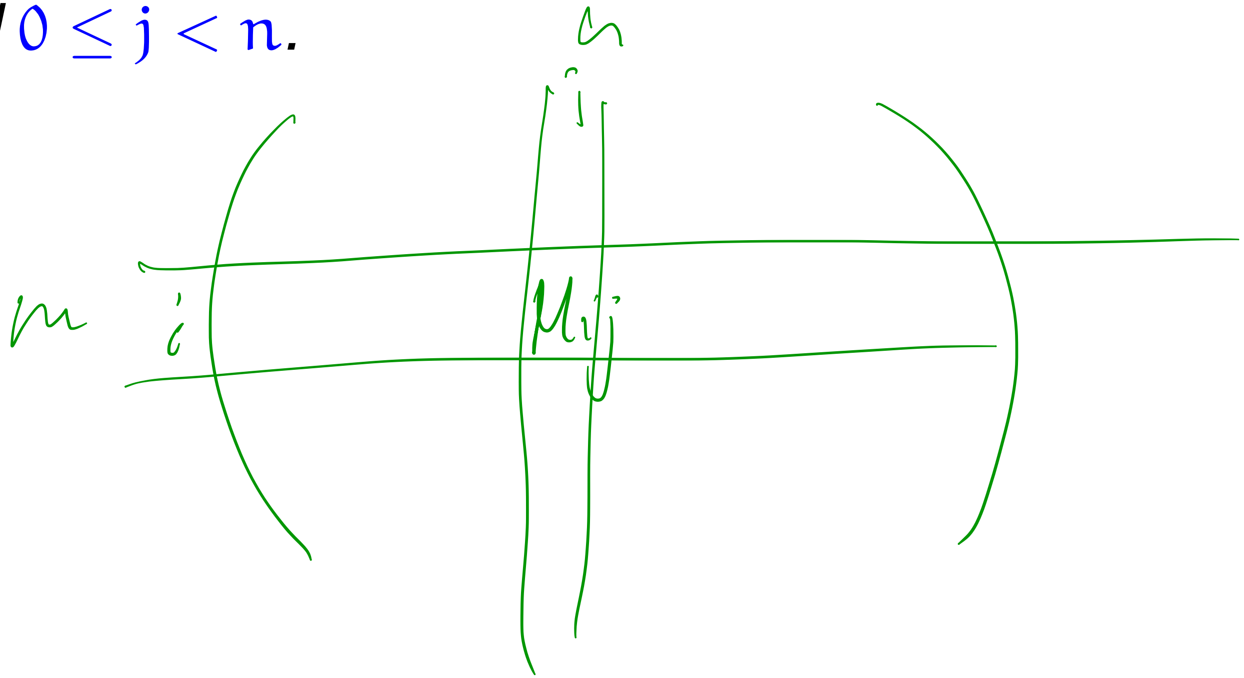
$$(S \circ R)_{ki} = \sum_j S_{jk} \cdot R_{ij}$$

need semiring.

Relations and matrices

Definition 103

1. *For positive integers* m *and* n*, an* $(m \times n)$*-*[*matrix*]() M *over a semiring* $(S, 0, \oplus, 1, \odot)$ *is given by entries* $M_{i,j} \in S$ *for all* $0 \leq i < m$ *and* $0 \leq j < n$*.*



Theorem 104 *Matrix multiplication is associative and has the identity matrix as neutral element.*

Relations from $[m]$ to $[n]$ and $(m \times n)$-matrices over Booleans provide two alternative views of the same structure.

This carries over to identities and to composition/multiplication .

$mat(R)$ $rel(M)$

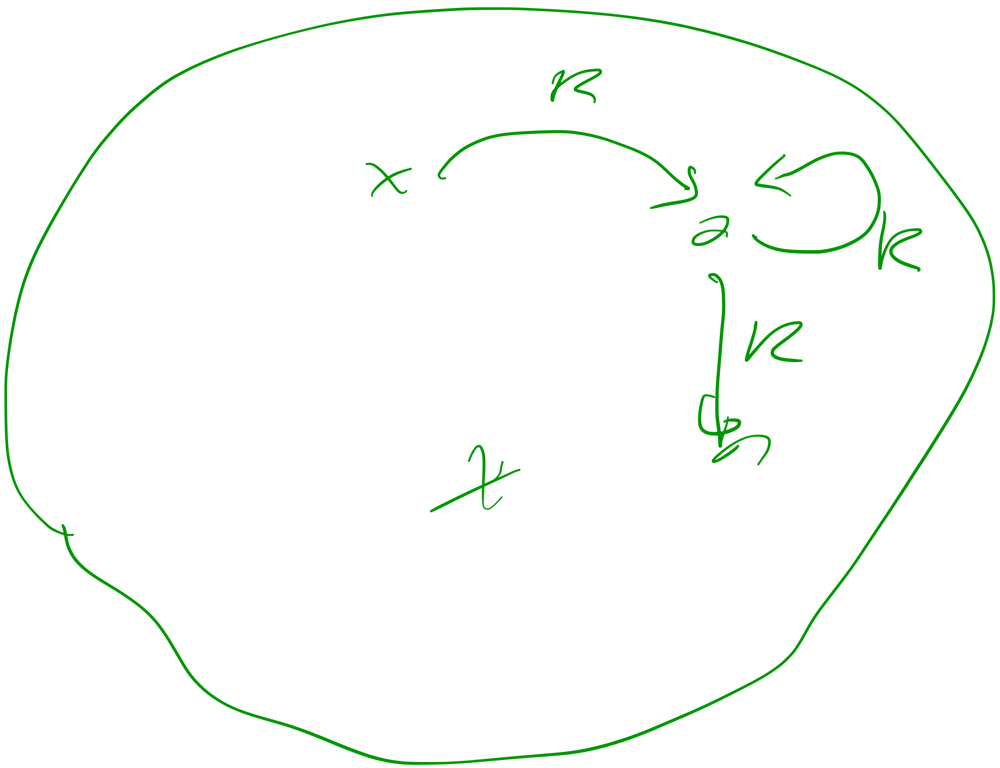
$rel(mat(R)) = R$

$mat(rel(M)) = M$

$mat(S \circ R) = mat(S) \circ mat(R)$

Directed graphs

Definition 108 *A* directed graph (A, R) *consists of a set* A *and a relation* R *on* A *(i.e. a relation from* A *to* A*).*



Corollary 110 *For every set A, the structure*

$$(\,\mathrm{Rel}(A)\,,\ \mathrm{id}_A\,,\circ\,)$$

is a monoid.

Definition 111 *For $R \in \mathrm{Rel}(A)$ and $n \in \mathbb{N}$, we let*

Often R^n

$$R^{\circ n} = \underbrace{R \circ \cdots \circ R}_{n \text{ times}} \in \mathrm{Rel}(A)$$

be defined as id_A for $n = 0$, and as $R \circ R^{\circ m}$ for $n = m + 1$.

$R^{\circ(n+1)} = R \circ R^{\circ n}$

i.e. $(a_0, \cdots, a_n) \in A^{n+1} \wedge a_0 = s \wedge a_n = t \wedge \forall i. (0 \leq i < n). a_i R a_{i+1}$

Paths

$s \curvearrowright \cdot \curvearrowright \cdot \curvearrowright \cdot \curvearrowright t$

Proposition 113 *Let* (A, R) *be a directed graph. For all* $n \in \mathbb{N}$ *and* $s, t \in A$, $s \, R^{\circ n} \, t$ *iff there exists a path of length* n *in* R *with source* s *and target* t.

PROOF: Basis $n = 0$. $s R^{\circ 0} t \iff s = t$.

0-path (s) from s to t.

Step $s R^{\circ(n+1)} t \iff \exists a \in A. \; s R a \wedge a R^{\circ n} t$

$\iff \exists a \in A. \; s R a \wedge$ there is an n-path from a to t.

Note: $s R a \wedge n$-path $(a_0, \cdots, a_n)$ from a to t

$\iff n{+}1$-path $(s, a_0, \cdots, a_n)$ from s to t.

$\iff \exists \; n{+}1$-path from s to t. $\boxtimes$

Definition 114 *For* $R \in \mathrm{Rel}(A)$, *let*

$$R^{\circ *} = \bigcup \left\{ R^{\circ n} \in \mathrm{Rel}(A) \mid n \in \mathbb{N} \right\} = \bigcup_{n \in \mathbb{N}} R^{\circ n} \quad .$$

Corollary 115 *Let* (A, R) *be a directed graph. For all* $s, t \in A$, $s\ R^{\circ *}\ t$ *iff there exists a path with source* s *and target* t *in* R.

The $(n \times n)$-matrix $M = \mathrm{mat}(R)$ of a finite directed graph $\big([n], R\big)$ for n a positive integer is called its *adjacency matrix*.

The adjacency matrix $M^* = \mathrm{mat}(R^{\circ *})$ can be computed by matrix multiplication and addition as M_n where

$$\begin{cases} M_0 &= I_n \\ M_{k+1} &= I_n + \big(M \cdot M_k\big) \end{cases}$$

This gives an algorithm for establishing or refuting the existence of paths in finite directed graphs.

Preorders

Definition 116 *A* preorder $(P, \sqsubseteq)$ *consists of a set* P *and a relation* $\sqsubseteq$ *on* P *(i.e.* $\sqsubseteq \in \mathcal{P}(P \times P)$*) satisfying the following two axioms.*

- *Reflexivity.*

$$\forall x \in P.\ x \sqsubseteq x$$

- *Transitivity.*

$$\forall x, y, z \in P.\ (x \sqsubseteq y \land y \sqsubseteq z) \implies x \sqsubseteq z$$

$$x_0 \sqsubseteq x_1 \sqsubseteq x_2 \sqsubseteq \cdots \sqsubseteq x_4$$

$$x_0 \sqsubseteq x_1 \quad \wedge \quad x_1 \sqsubseteq x_2 \quad - \quad - \quad -$$

$$x_0 \sqsubseteq x_2$$

$$x_0 \sqsubseteq x_3$$

$$\vdots$$

$$x_0 \sqsubseteq x_4$$

Partial orders

anti-symmetry.

$x \sqsubseteq y \wedge y \sqsubseteq x$

$\Rightarrow x = y$.

Examples:

- $(\mathbb{R}, \leq)$ and $(\mathbb{R}, \geq)$.
- $(\mathcal{P}(A), \subseteq)$ and $(\mathcal{P}(A), \supseteq)$.
- $(\mathbb{Z}, \mid)$.

not partial order

$-n \mid n$

$n \mid -n$

Theorem 118 *For* $R \subseteq A \times A$, *let*

$$\mathcal{F}_R = \{ Q \subseteq A \times A \mid R \subseteq Q \wedge Q \textit{ is a preorder} \} \quad .$$

Then, (i) $R^{\circ *} \in \mathcal{F}_R$ ✓ *and* (ii) $R^{\circ *} \subseteq \bigcap \mathcal{F}_R$. *Hence,* $R^{\circ *} = \bigcap \mathcal{F}_R$.

$\therefore R^{\circ *} \supseteq \bigcap \mathcal{F}_R$

PROOF:

(i) refl. $x \, R^{\circ *} x$ as $R^{\circ *} \supseteq R^{\circ 0} = Id_A$

trans $x \, R^{\circ *} y \wedge y \, R^{\circ *} z \overset{?}{\Longrightarrow} x \, R^{\circ *} z$

$(a_0, \ldots a_n)$ $(b_0, \ldots b_m)$

$(a_0 \ldots a_n, b_0 \ldots b_m)$

(ii) RTP $R^{\circ *} \subseteq \bigcap \mathcal{Y}_R$

S.T.P. $R^{\circ *} \subseteq Q$ for all $Q \in \mathcal{Y}_R$.

"$\bigcup \{R^{\circ n} \mid n \in \mathbb{N}\}$"

S.T.P. $R^{\circ n} \subseteq Q$ for all n.

By M I.

Basis $n=0$: $x R^{\circ 0} y \therefore x = y \therefore x Q y$ as Q preorder.

Step. $x R^{\circ(n+1)} y \iff x R a \wedge a R^{\circ n} y$ for some a.

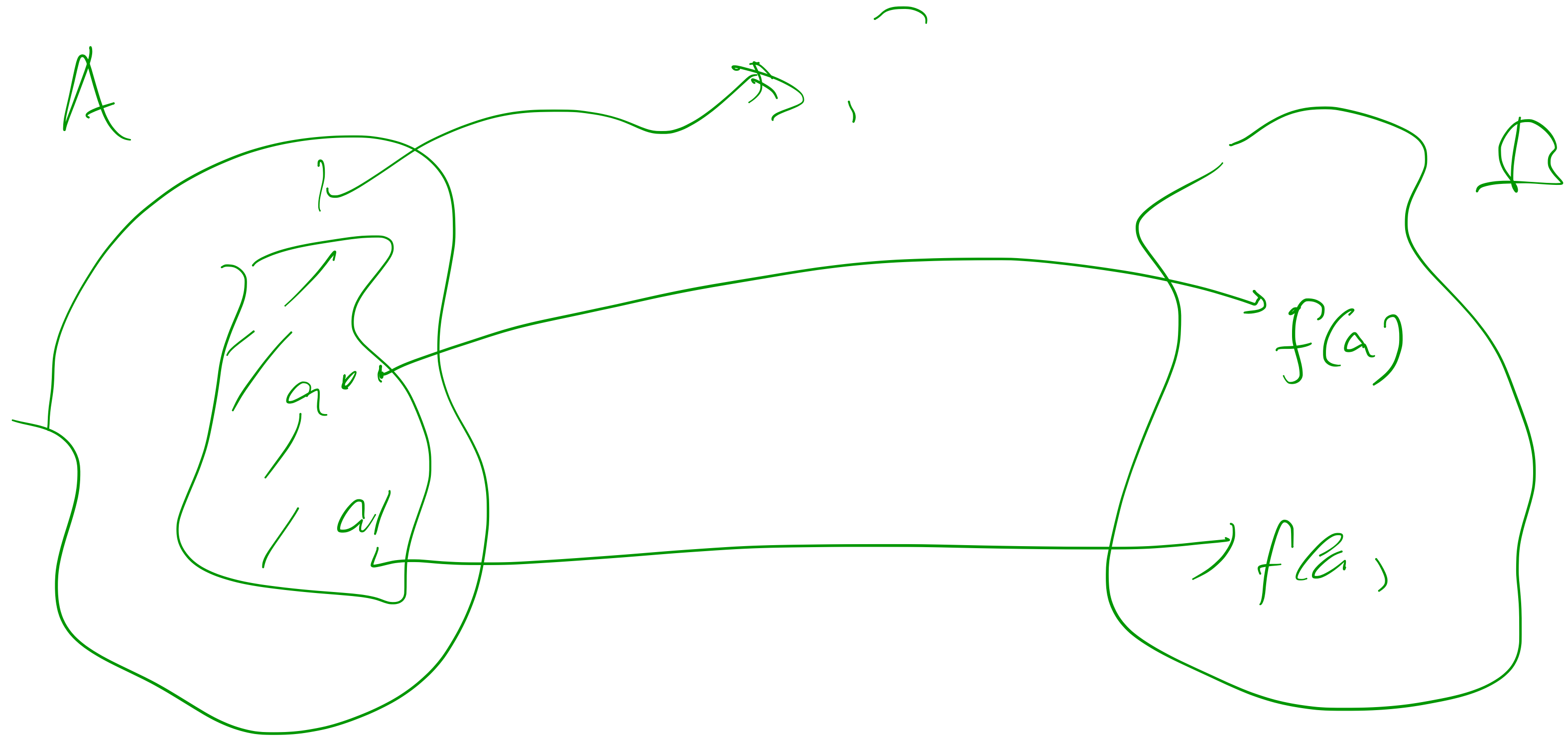
$\implies x Q a \wedge a Q y$

$\implies x Q y$ $\boxtimes$

Partial functions

Definition 119 *A relation* $R : A \mathrel{-\!\!\!+\!\!\!\rightarrow} B$ *is said to be* functional, *and called a* partial function, *whenever it is such that*

$$\forall a \in A. \forall b_1, b_2 \in B. \ a \, R \, b_1 \wedge a \, R \, b_2 \implies b_1 = b_2 \quad .$$



Theorem 121 *The identity relation is a partial function, and the composition of partial functions yields a partial function.*

NB

$$f = g : A \rightharpoonup B$$

iff

$$\forall a \in A.\, \big(f(a)\!\downarrow \iff g(a)\!\downarrow \big) \,\wedge\, f(a) = g(a)$$

Example: The following defines a partial function $\mathbb{Z} \times \mathbb{Z} \rightharpoonup \mathbb{Z} \times \mathbb{N}$:

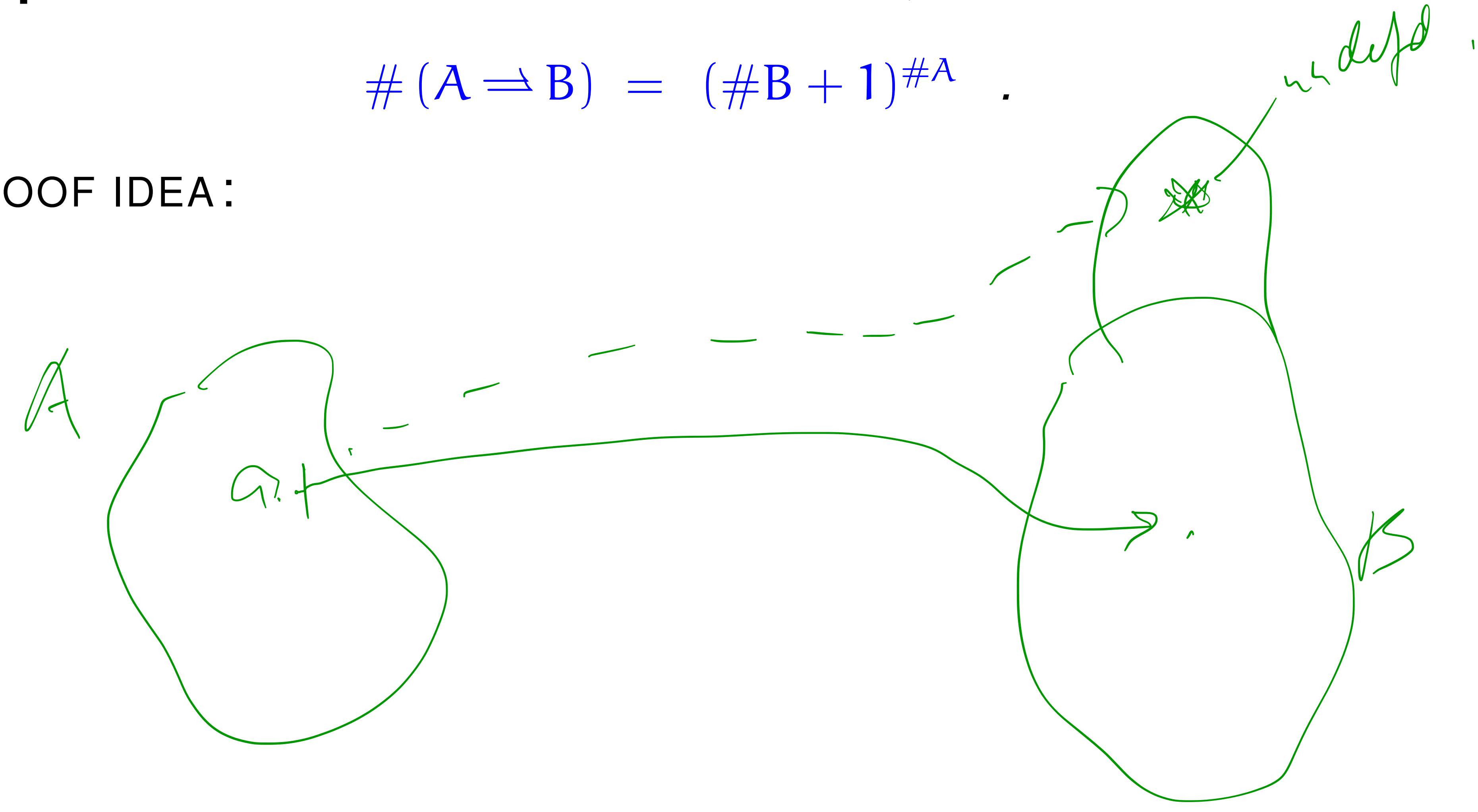
- for $n \geq 0$ and $m > 0$,
  $$(n, m) \mapsto \big(\,\mathrm{quo}(n, m)\,,\ \mathrm{rem}(n, m)\,\big)$$
- for $n \geq 0$ and $m < 0$,
  $$(n, m) \mapsto \big(\,-\mathrm{quo}(n, -m)\,,\ \mathrm{rem}(n, -m)\,\big)$$
- for $n < 0$ and $m > 0$,
  $$(n, m) \mapsto \big(\,-\mathrm{quo}(-n, m) - 1\,,\ \mathrm{rem}(m - \mathrm{rem}(-n, m), m)\,\big)$$
- for $n < 0$ and $m < 0$,
  $$(n, m) \mapsto \big(\,\mathrm{quo}(-n, -m) + 1\,,\ \mathrm{rem}(-m - \mathrm{rem}(-n, -m), -m)\,\big)$$

Its domain of definition is $\{\,(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid m \neq 0\,\}$.

Proposition 122 *For all finite sets* A *and* B*,*

$$\#(A \rightharpoonup B) \;=\; (\#B+1)^{\#A} \quad .$$

PROOF IDEA:



Functions (or maps)

Definition 123 *A partial function is said to be* total, *and referred to as a* (total) function *or* map, *whenever its domain of definition coincides with its source.*

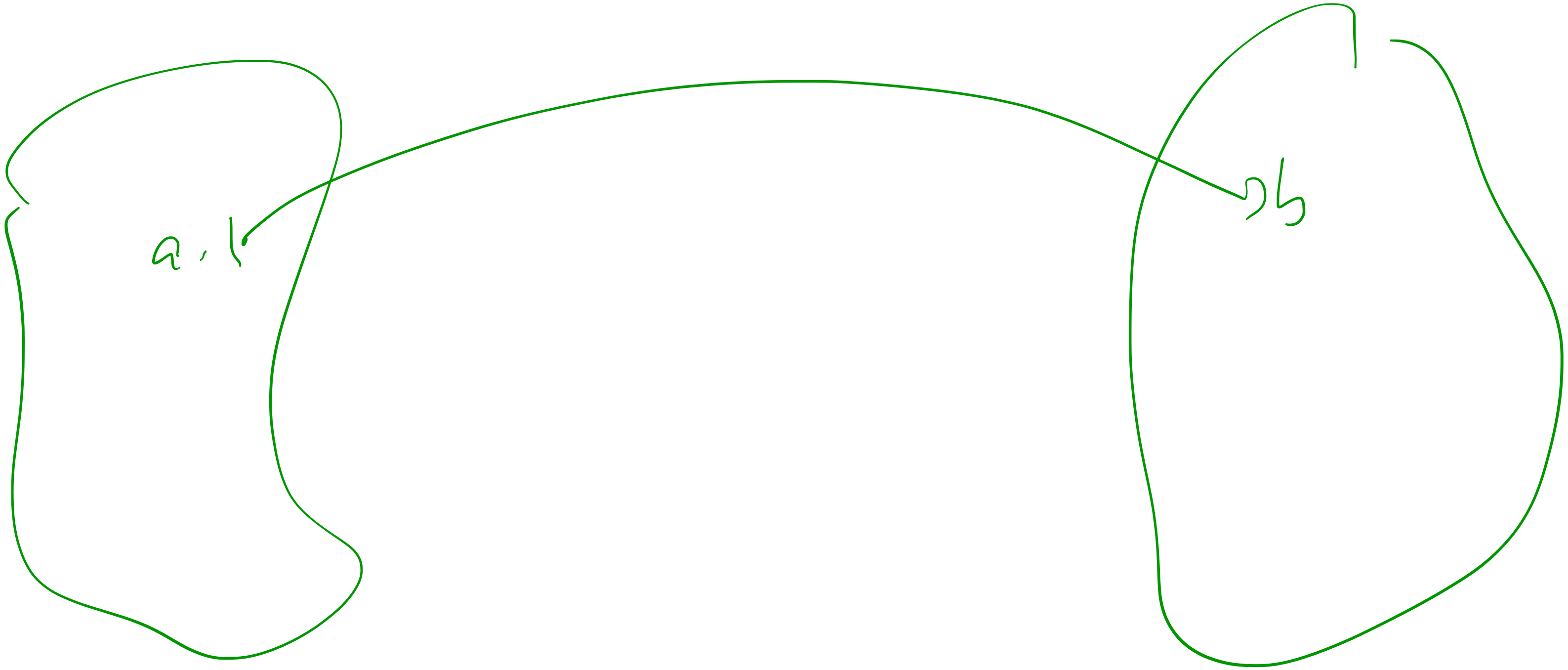
Theorem 124 *For all* $f \in \mathrm{Rel}(A, B)$,

$$f \in (A \Rightarrow B) \iff \forall\, a \in A.\, \exists!\, b \in B.\ a\, f\, b \quad .$$

Proposition 125 *For all finite sets* A *and* B,

$$\#(A \Rightarrow B) = \#B^{\#A} \quad .$$

PROOF IDEA:



Theorem 126 *The identity partial function is a function, and the composition of functions yields a function.*

NB

1. $f = g : A \to B$ iff $\forall\, a \in A.\, f(a) = g(a)$.

2. For all sets A, the identity function $\mathrm{id}_A : A \to A$ is given by the rule

   $$\mathrm{id}_A(a) = a$$

   and, for all functions $f : A \to B$ and $g : B \to C$, the composition function $g \circ f : A \to C$ is given by the rule

   $$\big(g \circ f\big)(a) = g\big(f(a)\big) \quad .$$

Bijections

Definition 127 *A function* $f : A \to B$ *is said to be* bijective*, or a* bijection*, whenever there exists a (necessarily unique) function* $g : B \to A$ *(referred to as the* inverse *of* f*) such that*

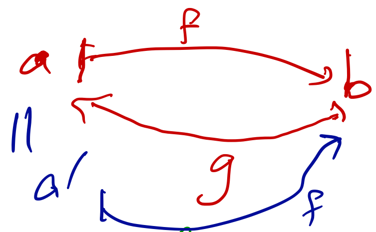
1. g *is a* retraction *(or* left inverse*) for* f*:*

   $$g \circ f = \mathrm{id}_A \quad ,$$

2. g *is a* section *(or* right inverse*) for* f*:*

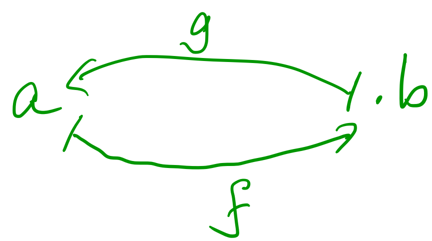
   $$f \circ g = \mathrm{id}_B \quad .$$

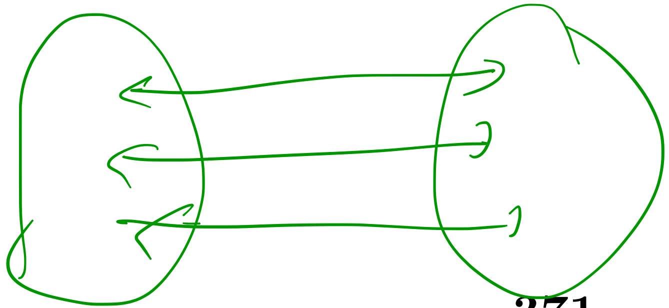
ensures f is injective.



ensures f is surjective.

$g(b) = a$





Proposition 129 *For all finite sets* A *and* B,

$$\# \mathrm{Bij}(A, B) = \begin{cases} 0 & , \textit{if } \#A \neq \#B \\ n! & , \textit{if } \#A = \#B = n \end{cases}$$

PROOF IDEA:

Theorem 130 *The identity function is a bijection, and the composition of bijections yields a bijection.*

Definition 131 *Two sets* A *and* B *are said to be* isomorphic *(and to have the* same cardinatity*) whenever there is a bijection between them; in which case we write*

$$A \cong B \quad \textit{or} \quad \#A = \#B \quad .$$

Examples:

1. $\{0, 1\} \cong \{\mathbf{false}, \mathbf{true}\}$.
2. $\mathbb{N} \cong \mathbb{N}^{+}$, $\mathbb{N} \cong \mathbb{Z}$, $\mathbb{N} \cong \mathbb{N} \times \mathbb{N}$, $\mathbb{N} \cong \mathbb{Q}$. $\mathbb{N} \not\cong \mathbb{R}$

Equivalence relations and set partitions

- Equivalence relations. $E \subseteq A \times A$, a binary relation s.t.

Reflexive: $a E a$ for all $a \in A$

Symmetric: $a E b \Rightarrow b E a$ for all $a, b \in A$

Transitive: $a E b$ & $b E c \Rightarrow a E c$
for all $a, b, c \in A$.

Equivalence classes: $\{a\}_E =_{def} \{ b \in A \mid b E a \}$

Example $\equiv \pmod{n}$

► **Set partitions.** From an equivalence relation $E \subseteq A \times A$

Each $\{a\}_E$ is non-empty, for $a \in A$

$$A = \bigcup \{ \{a\}_E \mid a \in A \}$$

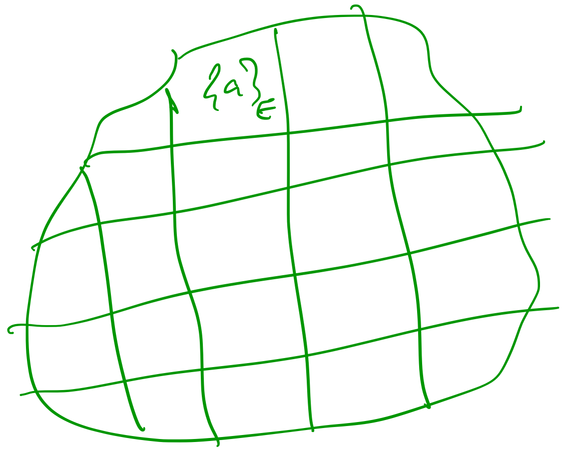
$$\underbrace{\{a\}_E \cap \{b\}_E \neq \emptyset}_{\Downarrow} \implies \{a\}_E = \{b\}_E \quad \checkmark$$

for all $a, b \in A$.

$$c\,E\,a \;\wedge\; c\,E\,b$$

$$\therefore a\,E\,c \;\wedge\; c\,E\,b$$

$$\therefore a\,E\,b$$



$$x \in \{a\}_E \implies x\,E\,a \implies x\,E\,b \implies x \in \{b\}_E$$

Theorem 134 *For every set A,*

$$\mathrm{EqRel}(A) \cong \mathrm{Part}(A) \quad .$$

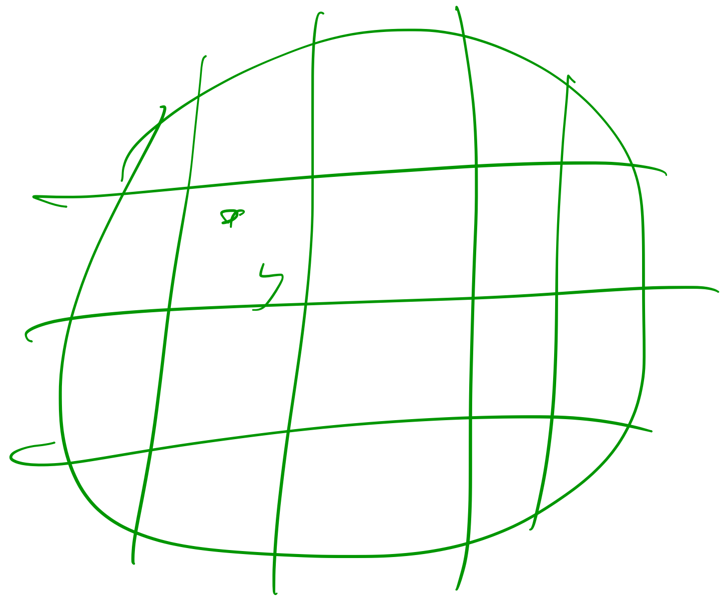
PROOF:

$$E \longmapsto \{ [a]_E \mid a \in A \}$$

$x \mathrel{E} y$

same block

$E \longleftarrow\!\shortmid$



Calculus of bijections

- $A \cong A$, $A \cong B \implies B \cong A$, $(A \cong B \wedge B \cong C) \implies A \cong C$
- If $A \cong X$ and $B \cong Y$ then

$$\mathcal{P}(A) \cong \mathcal{P}(X) \quad , \quad A \times B \cong X \times Y \quad , \quad A \uplus B \cong X \uplus Y \quad ,$$

$$\mathrm{Rel}(A, B) \cong \mathrm{Rel}(X, Y) \quad , \quad (A \rightharpoonup B) \cong (X \rightharpoonup Y) \quad ,$$

$$(A \Rightarrow B) \cong (X \Rightarrow Y) \quad , \quad \mathrm{Bij}(A, B) \cong \mathrm{Bij}(X, Y)$$

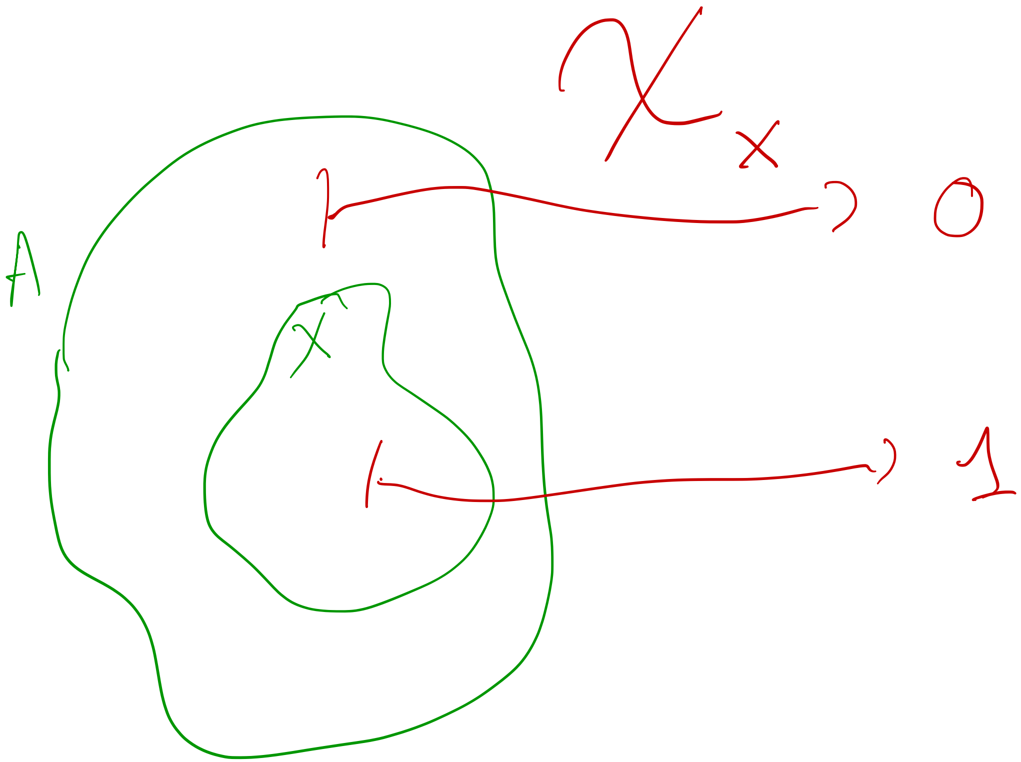
- $A \cong [1] \times A$, $(A \times B) \times C \cong A \times (B \times C)$, $A \times B \cong B \times A$
- $[0] \uplus A \cong A$, $(A \uplus B) \uplus C \cong A \uplus (B \uplus C)$, $A \uplus B \cong B \uplus A$
- $[0] \times A \cong [0]$, $(A \uplus B) \times C \cong (A \times C) \uplus (B \times C)$
- $(A \Rightarrow [1]) \cong [1]$, $(A \Rightarrow (B \times C)) \cong (A \Rightarrow B) \times (A \Rightarrow C)$
- $([0] \Rightarrow A) \cong [1]$, $((A \uplus B) \Rightarrow C) \cong (A \Rightarrow C) \times (B \Rightarrow C)$
- $([1] \Rightarrow A) \cong A$, $((A \times B) \Rightarrow C) \cong (A \Rightarrow (B \Rightarrow C))$
- $(A \rightharpoonup B) \cong (A \Rightarrow (B \uplus [1]))$
- $\mathcal{P}(A) \cong (A \Rightarrow [2])$

$[2] = \{0, 1\}$

Characteristic (or indicator) functions

$$\mathcal{P}(\mathbf{A}) \cong (\mathbf{A} \Rightarrow [\mathbf{2}])$$

$\cong \{0, 1\}$



Finite cardinality

$\{0, 1, \ldots, n-1\}$

Definition 136 *A set* A *is said to be* <u>finite</u> *whenever* $A \cong [n]$ *for some* $n \in \mathbb{N}$*, in which case we write* $\#A = n$.

Theorem 137 *For all* $m, n \in \mathbb{N}$,

1. $\mathcal{P}\big([n]\big) \cong [2^n]$
2. $[m] \times [n] \cong [m \cdot n]$
3. $[m] \uplus [n] \cong [m + n]$
4. $\big([m] \rightharpoonup [n]\big) \cong \big[(n+1)^m\big]$
5. $\big([m] \Rightarrow [n]\big) \cong [n^m]$
6. $\mathrm{Bij}\big([n], [n]\big) \cong [n!]$

$0 \qquad 1 \qquad 2 \qquad\qquad\qquad n$

$\emptyset \qquad \{\emptyset\} \qquad \{\underset{0}{\emptyset}, \underset{1}{\{\emptyset\}}\} \qquad\qquad \{0, \ldots, n-1\}$

$Succ(\{\emptyset\}) = \{\emptyset\} \cup \{\{\emptyset\}\}$

Infinity axiom

$\boxed{\text{There is an infinite set, containing } \emptyset \text{ and closed under successor.}}$

$Succ(x) =_{def} x \cup \{x\}.$

Bijections

Proposition 138 *For a function* $f : A \to B$*, the following are equivalent.*

1. f *is bijective.*
2. $\forall\, b \in B.\, \exists!\, a \in A.\, f(a) = b$.
3. $$\big(\forall\, b \in B.\, \exists\, a \in A.\, f(a) = b\big)$$ f is surjective
$$\wedge$$
$$\big(\forall\, a_1, a_2 \in A.\, f(a_1) = f(a_2) \implies a_1 = a_2\big)$$ f is injective

Surjections

Definition 139 *A function* $f : A \to B$ *is said to be* surjective*, or a* surjection*, and indicated* $f : A \twoheadrightarrow B$ *whenever*

$$\forall\, b \in B.\, \exists\, a \in A.\, f(a) = b \quad .$$

Theorem 140 *The identity function is a surjection, and the composition of surjections yields a surjection.*

The set of surjections from A to B is denoted

$$\mathrm{Sur}(A, B)$$

and we thus have

$$\mathrm{Bij}(A, B) \subseteq \mathrm{Sur}(A, B) \subseteq \mathrm{Fun}(A, B) \subseteq \mathrm{PFun}(A, B) \subseteq \mathrm{Rel}(A, B) \ .$$

Enumerability

Definition 142

1. *A set* A *is said to be* enumerable *whenever there exists a surjection* $\mathbb{N} \twoheadrightarrow A$*, referred to as an* enumeration*.*

2. *A* countable *set is one that is either empty or enumerable.*

Theorem. A set A is countable iff its elements can be arranged in a finite or infinite sequence

$$a_0, a_1, a_2, \cdots, a_n, \cdots$$

i.e. so $A = \{a_0, a_1, \cdots, a_n, \cdots\}$.

Proof. If $A = \emptyset$ then A can be arranged as the empty sequence. Otherwise there is

$$f : \mathbb{N} \twoheadrightarrow A.$$

Idea: Each $a \in A$ is associated with a least "index" k s.t. $f(k) = a$. Use indices to order A in a sequence.

Define $a_0, a_1, \ldots, a_n, \ldots$ by induction:

$a_0 = f(0)$;

$a_{n+1} = f(k)$ where k is the least $k \in \mathbb{N}$ for which $f(k) \notin \{a_0, \ldots, a_n\}$ if such exists; otherwise the sequence stops.

Exercise. Show $A = \{a_0, \ldots, a_n, \ldots\}$.

$\boxtimes$

Examples:

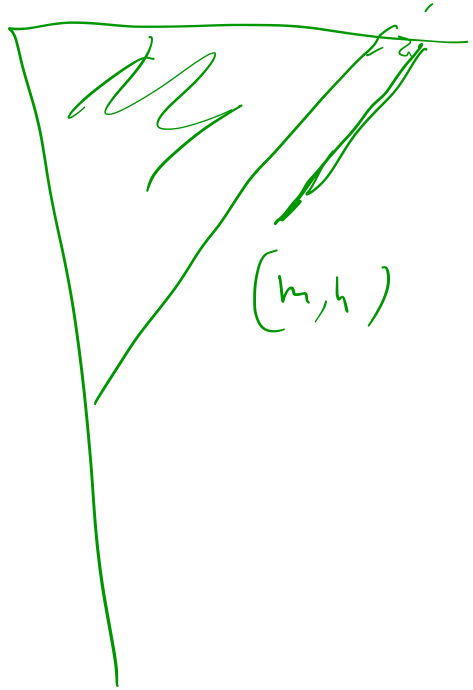
$\mathbb{N} \cong \mathbb{Z}$

1. A bijective enumeration of $\mathbb{Z}$.

$$\begin{pmatrix} -n \\ 2n-1 \end{pmatrix} \quad \begin{array}{c|c|c|c|c|c|c|c|c} \cdots & -3 & -2 & -1 & 0 & 1 & 2 & 3 & \cdots \\ \hline\hline & 5 & 3 & 1 & 0 & 2 & 4 & 6 & - \end{array} \quad - \begin{pmatrix} n \\ 2n \end{pmatrix}$$

Same idea shows $\mathbb{N} \uplus \mathbb{N}$ enumerable.

2. A bijective enumeration of $\mathbb{N} \times \mathbb{N}$.

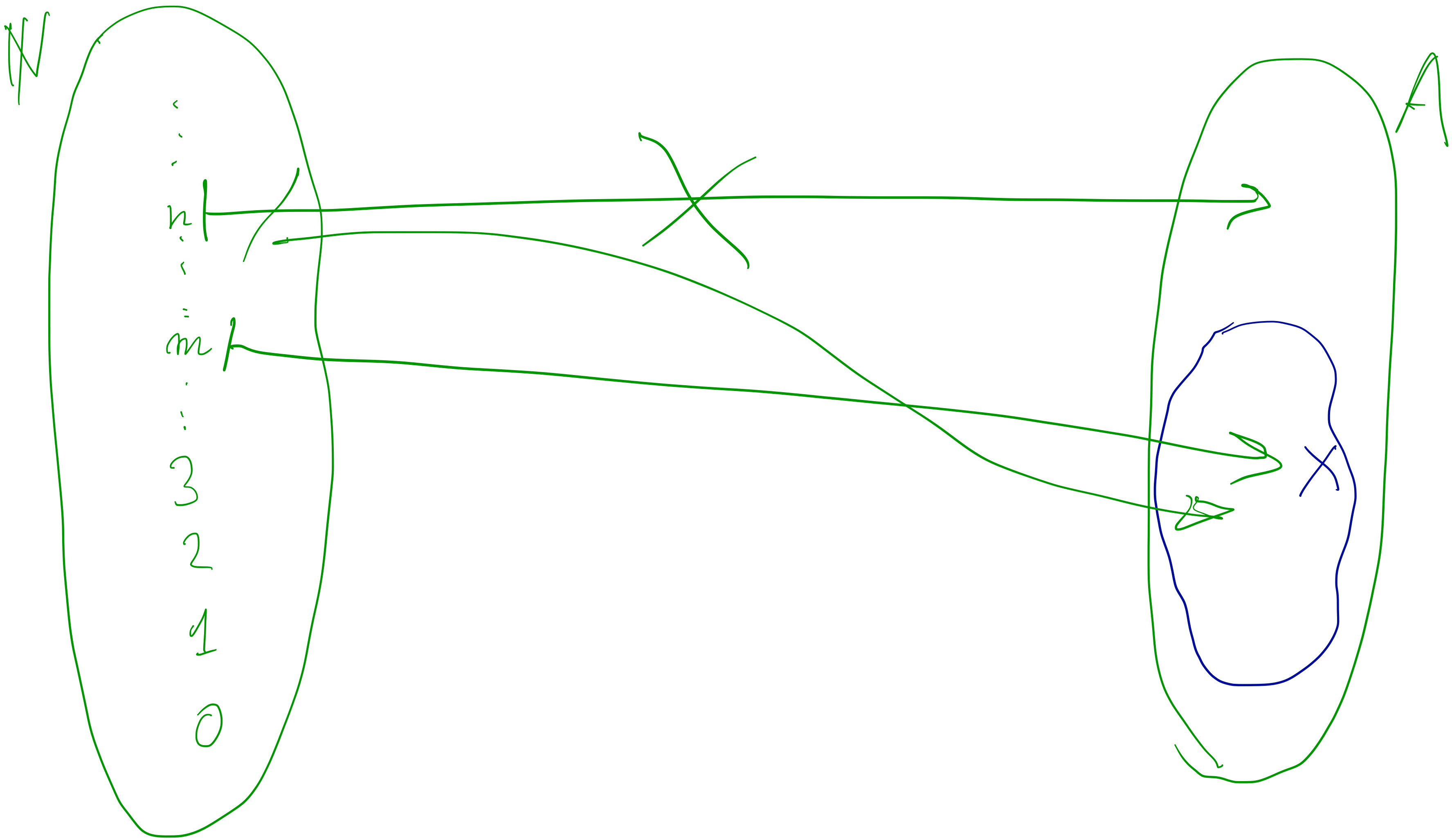


	0	1	2	3	4	5	$\cdots$
0	0	1	3	6			
1	2	4	7				
2	5	8					
3	9						
4							
$\vdots$							

$$(m,n) \longmapsto \frac{(m+n)(m+n+1)}{2} + n$$

Proposition 143 *Every non-empty subset of an enumerable set is enumerable.*

PROOF: Have a surjection $f : \mathbb{N} \twoheadrightarrow A$.



A proof technique:

To show a set B is enumerable it suffices to exhibit a surjection

$$f : A \twoheadrightarrow B$$

from an enumerable set A.

[The composition with the enumeration of A

$$\mathbb{N} \twoheadrightarrow A \twoheadrightarrow B$$

gives an enumeration of B.]

$$(\mathbb{N} \cong)\ \mathbb{N}\times\mathbb{N} \xrightarrow{f\times g} A \times B$$

$$(m, n) \longmapsto (f(m), g(n))$$

Countability

Proposition 144

1. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ *are countable sets.*
2. *The product and disjoint union of countable sets is countable.*
3. *Every finite set is countable.*
4. *Every subset of a countable set is countable.*

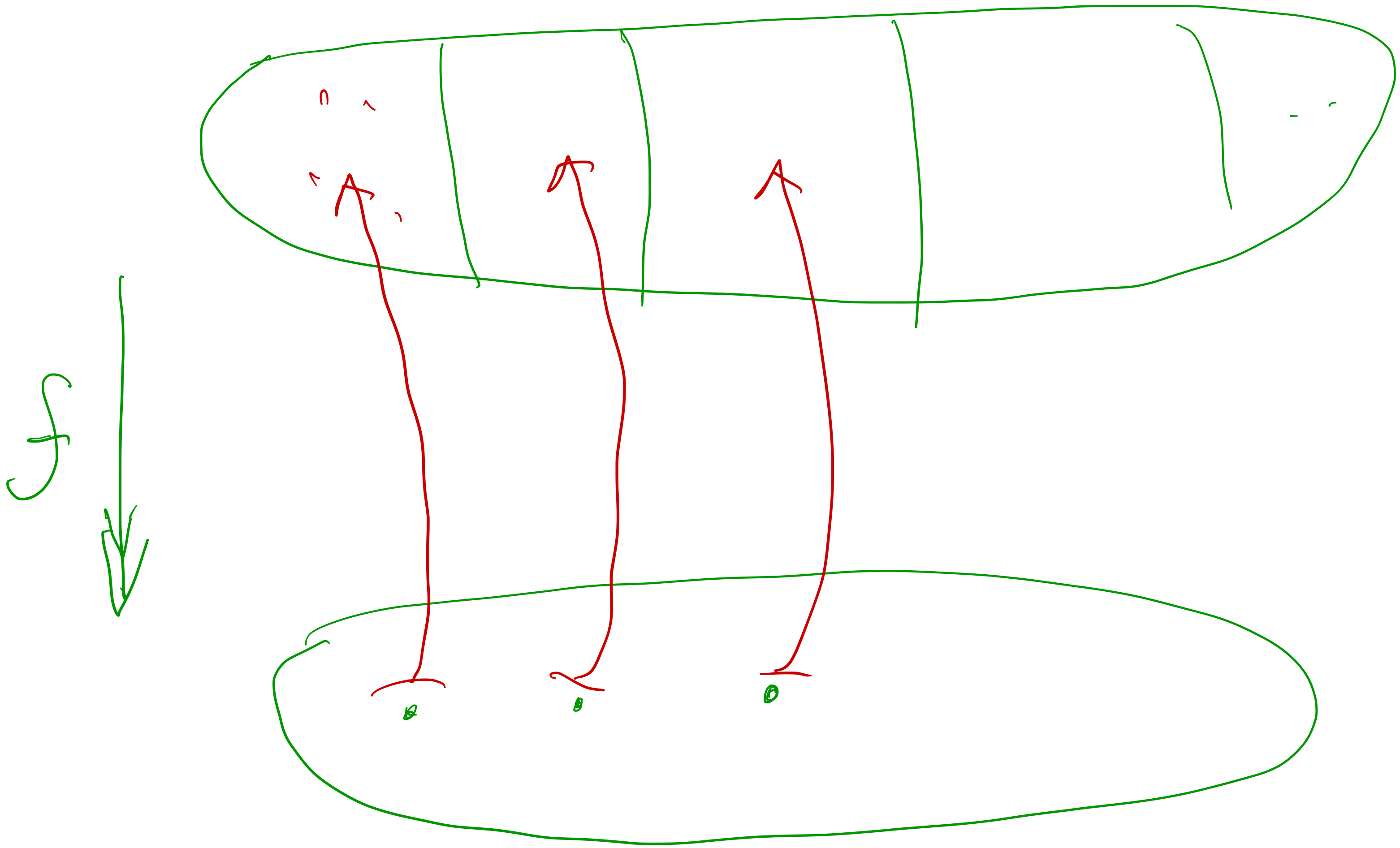
A, B

$\mathbb{N} \xrightarrow{f} A$

$\mathbb{N} \xrightarrow{g} B$

Axiom of choice

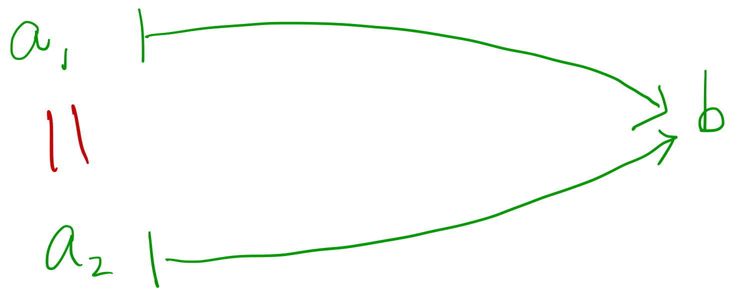
$\boxed{\text{Every surjection has a section.}}$



Injections

Definition 145 *A function* $f : A \to B$ *is said to be* injective*, or an* injection*, and indicated* $f : A \rightarrowtail B$ *whenever*

$$\forall a_1, a_2 \in A.\, \big(f(a_1) = f(a_2)\big) \implies a_1 = a_2 \quad .$$



Theorem 146 *The identity function is an injection, and the composition of injections yields an injection.*

The set of injections from A to B is denoted

$$\mathrm{Inj}(A, B)$$

and we thus have

$$\begin{tikzcd}[column sep=small]
 & \mathrm{Sur}(A, B) \arrow[dr, phantom, sloped, "\subseteq"] & \\
\mathrm{Bij}(A, B) \arrow[ur, phantom, sloped, "\subseteq"] \arrow[dr, phantom, sloped, "\subseteq"] & & \mathrm{Fun}(A, B) \subseteq \mathrm{PFun}(A, B) \subseteq \mathrm{Rel}(A, B) \\
 & \mathrm{Inj}(A, B) \arrow[ur, phantom, sloped, "\subseteq"] &
\end{tikzcd}$$

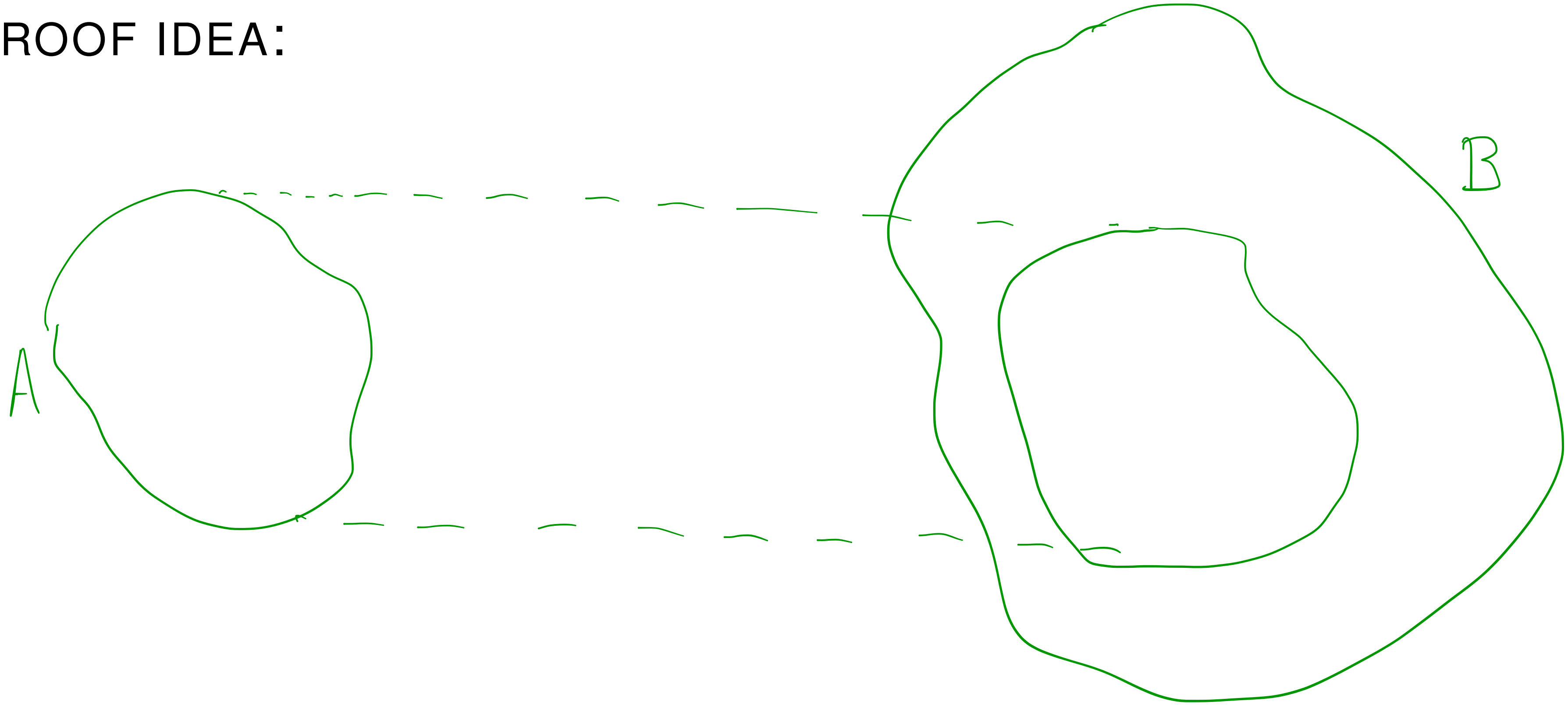
with

$$\mathrm{Bij}(A, B) = \mathrm{Sur}(A, B) \cap \mathrm{Inj}(A, B) \quad .$$

Proposition 147 *For all finite sets* A *and* B,

$$\#\mathrm{Inj}(A,B) = \begin{cases} \binom{\#B}{\#A} \cdot (\#A)! & \text{, if } \#A \leq \#B \\ 0 & \text{, otherwise} \end{cases}$$

PROOF IDEA:

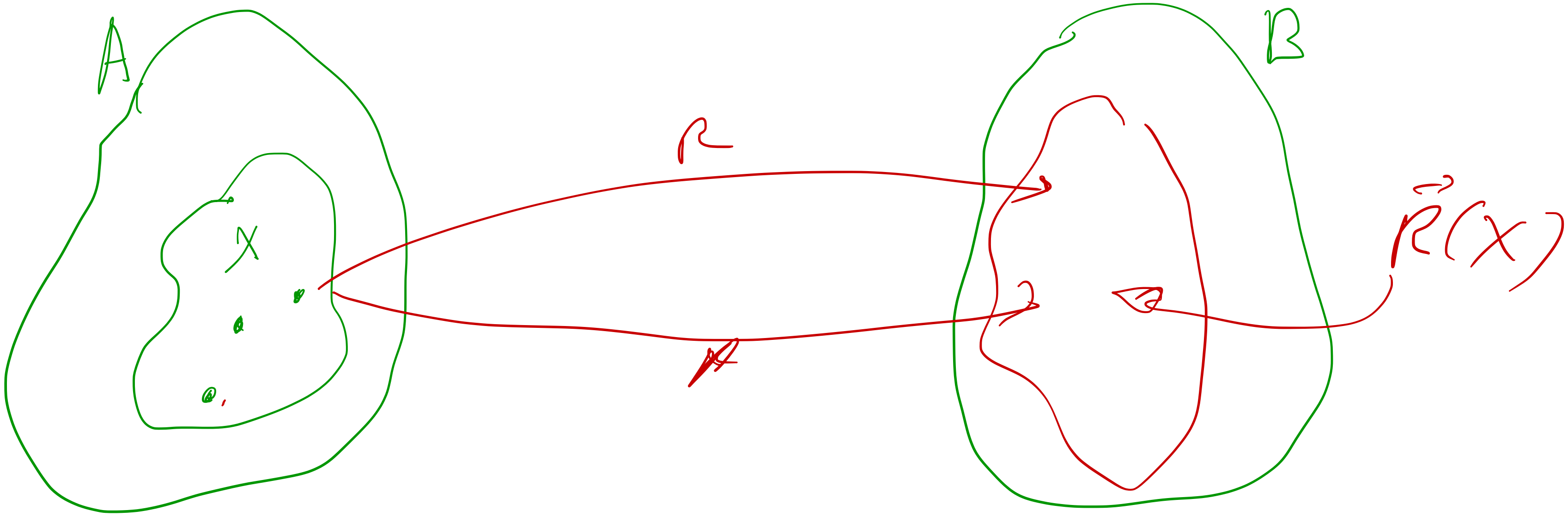


Relational images

Definition 150 *Let* $R : A \rightarrow\!\!\!\!\!+\;\; B$ *be a relation.*

- *The* direct image *of* $X \subseteq A$ *under* R *is the set* $\overrightarrow{R}(X) \subseteq B$, *defined as*

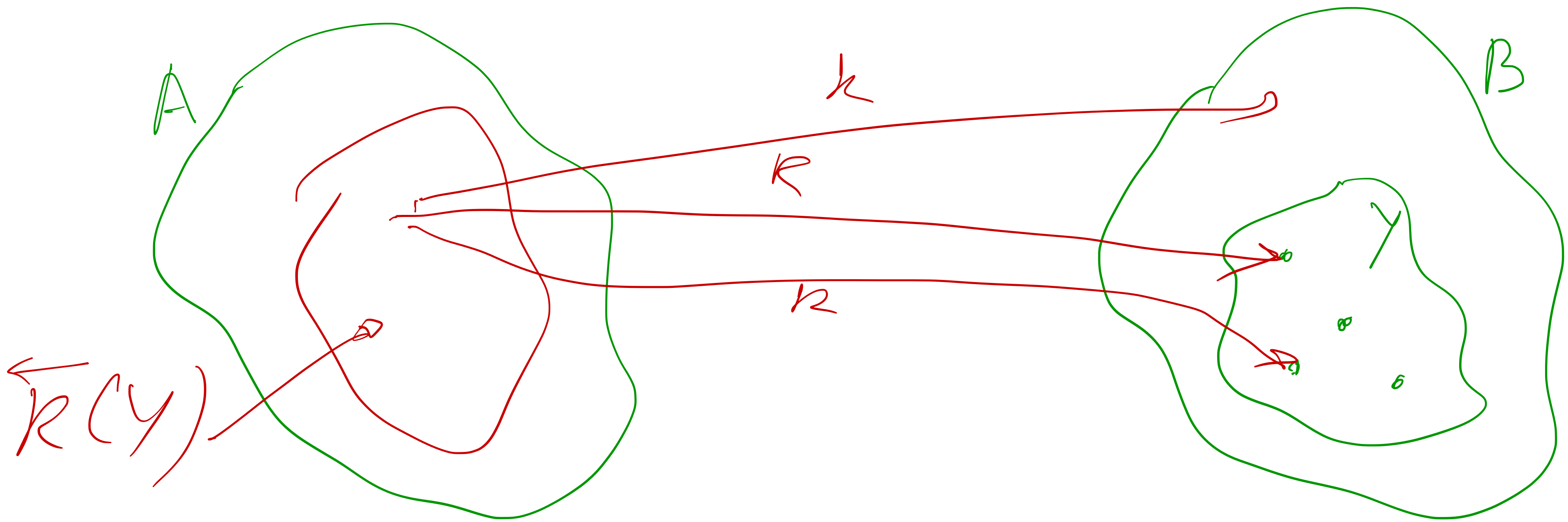
$$\overrightarrow{R}(X) \;=\; \{\, b \in B \mid \exists x \in X.\, x \mathrel{R} b \,\} \;.$$



NB *This construction yields a function* $\overrightarrow{R} : \mathcal{P}(A) \to \mathcal{P}(B)$.

- *The* inverse image *of* $Y \subseteq B$ *under* R *is the set* $\overleftarrow{R}(Y) \subseteq A$*, defined as*

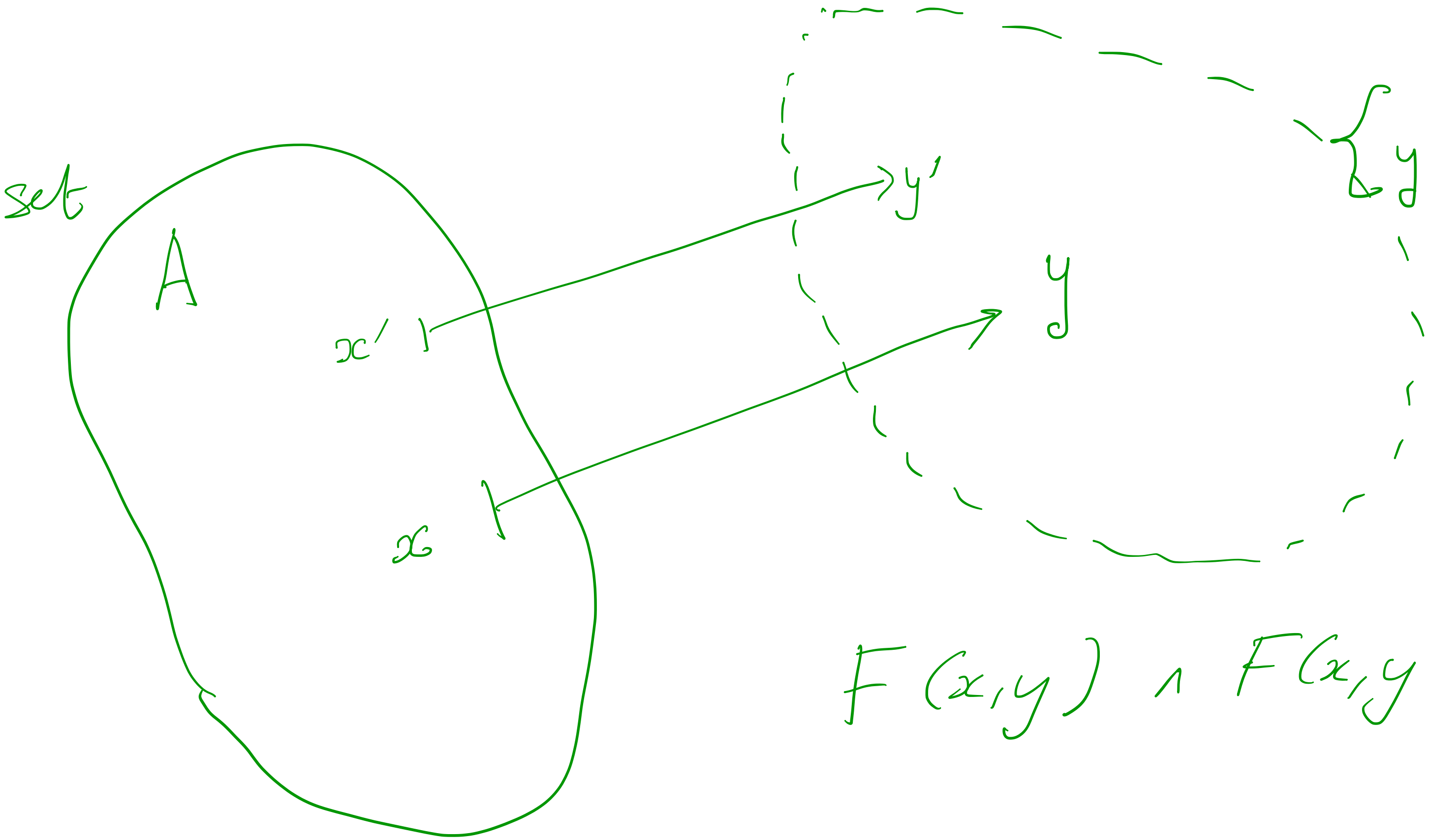
$$\overleftarrow{R}(Y) \;=\; \{ a \in A \mid \forall b \in B.\, a \, R \, b \implies b \in Y \}$$



NB *This construction yields a function* $\overleftarrow{R} : \mathcal{P}(B) \to \mathcal{P}(A)$.

Replacement axiom

The direct image of every definable functional property on a set is a set.



$\{ y \mid \exists x.\ F(x,y) \}$

a set!

$F(x,y) \wedge F(x,y') \Rightarrow y = y'$

Set-indexed constructions

For every mapping associating a set A_i to each element of a set I, we have the set

$$\bigcup_{i \in I} A_i = \bigcup \{A_i \mid i \in I\} = \{a \mid \exists i \in I.\, a \in A_i\} \quad .$$

Examples:

1. Indexed disjoint unions:

$$\biguplus_{i \in I} A_i = \bigcup_{i \in I} \{i\} \times A_i$$

2. Finite sequences on a set A:

$$A^* = \biguplus_{n \in \mathbb{N}} A^n$$

3. Finite partial functions from a set A to a set B:

$$(A \rightharpoonup_{\mathrm{fin}} B) \;=\; \biguplus_{S \in \mathcal{P}_{\mathrm{fin}}(A)} (S \Rightarrow B)$$

where

$$\mathcal{P}_{\mathrm{fin}}(A) = \{\, S \subseteq A \mid S \text{ is finite} \,\}$$

4. Non-empty indexed intersections: for $I \neq \emptyset$,

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

5. Indexed products:

$$\prod_{i \in I} A_i \;=\; \left\{\, \alpha \in (I \Rightarrow \bigcup_{i \in I} A_i) \;\middle|\; \forall i \in I .\, \alpha(i) \in A_i \,\right\}$$

cf. dependent types

Proposition 153 *An enumerable indexed disjoint union of* $\biguplus_{i \in I} A_i$
enumerable sets is enumerable.

PROOF: Have $g : \mathbb{N} \twoheadrightarrow I$, $f_i : \mathbb{N} \twoheadrightarrow A_i$ all $i \in I$.

Define $h : \mathbb{N} \times \mathbb{N} \twoheadrightarrow \bigcup_{i \in I} \{i\} \times A_i$

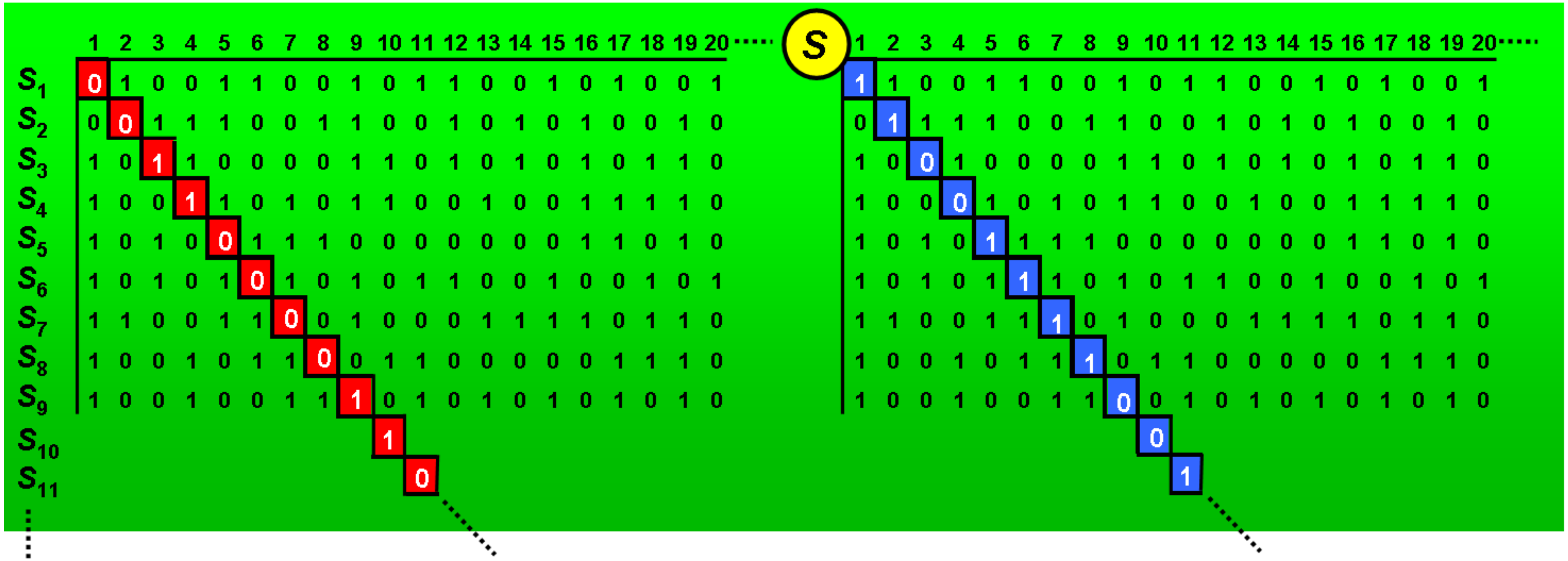
$$(m, n) \longmapsto (g(m), f_{g(m)}(n)).$$

$\boxtimes$

Corollary 155 *If* X *and* A *are countable sets then so are* A^**,* $\mathcal{P}_{\mathrm{fin}}(\mathrm{A})$*, and* $(\mathrm{X} \rightrightarrows_{\mathrm{fin}} \mathrm{A})$*.*

THEOREM OF THE DAY

Cantor's Uncountability Theorem *There are uncountably many infinite 0-1 sequences.*



Proof: Suppose you *could* count the sequences. Label them in order: $S_1, S_2, S_3, \ldots$, and denote by $S_i(j)$ the j-th entry of sequence S_i. Now define a new sequence, S, whose i-th entry is $S_i(i)+1 \pmod 2$. So S is $S_1(1)+1, S_2(2)+1, S_3(3)+1, S_4(4)+1, \ldots$, with all entries remaindered modulo 2. S is certainly an infinite sequence of 0s and 1s. So it must appear in our list: it is, say, S_k, so its k-th entry is $S_k(k)$. But this is, by definition, $S_k(k) + 1 \pmod 2 \neq S_k(k)$. So we have contradicted the possibility of forming our enumeration. QED.

The theorem establishes that the real numbers are *uncountable* — that is, they cannot be enumerated in a list indexed by the positive integers $(1, 2, 3, \ldots)$. To see this informally, consider the infinite sequences of 0s and 1s to be the binary expansions of fractions (e.g. $0.010011\ldots = 0/2 + 1/4 + 0/8 + 0/16 + 1/32 + 1/64 + \ldots$). More generally, it says that the set of subsets of a countably infinite set is uncountable, and to see *that*, imagine every 0-1 sequence being a different recipe for building a subset: the i-th entry tells you whether to include the i-th element (1) or exclude it (0).

Georg Cantor (1845–1918) discovered this theorem in 1874 but it apparently took another twenty years of thought about what were then new and controversial concepts: 'sets', 'cardinalities', 'orders of infinity', to invent the important proof given here, using the so-called *diagonalisation method*.

Web link: www.math.hawaii.edu/~dale/godel/godel.html. There is an interesting discussion on mathoverflow.net about the history of diagonalisation: type 'earliest diagonal' into their search box.

Further reading: *Mathematics: the Loss of Certainty* by Morris Kline, Oxford University Press, New York, 1980.

Unbounded cardinality

Theorem 156 (Cantor's diagonalisation argument) *For every set A, no surjection from A to $\mathcal{P}(A)$ exists.*

PROOF: By contradiction. Suppose there were

$$f : A \twoheadrightarrow \mathcal{P}(A)$$

Define

$$X = \{ a \in A \mid a \notin f(a) \}.$$

As f is surjective, there is $b \in A$ s.t. $f(b) = X$.

Either $b \in X$ or $b \notin X$. But ...

$$\left.\begin{array}{l} b \in X = f(b) \quad \therefore \quad b \notin X \\ b \notin X = f(b) \quad \therefore \quad b \in X \end{array}\right\}$$

$\boxtimes$

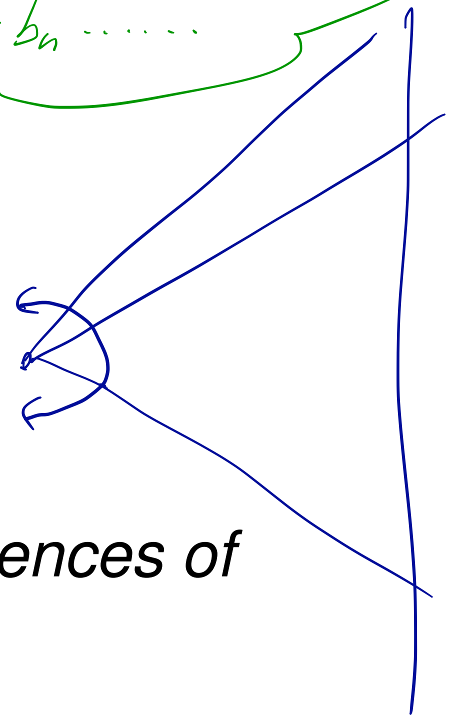
of Theorem 156

Corollary 159 *The sets*

correspond to infinite binary expansions $0 . b_0 b_1 b_2 b_3 \cdots b_n \cdots\cdots$

$$\mathcal{P}(\mathbb{N}) \;\cong\; \big(\mathbb{N} \Rightarrow [2]\big) \;\cong\; [0,1] \;\cong\; \mathbb{R}$$

are not enumerable.



Corollary 160 *There are* non-computable *infinite sequences of bits.*

For the sake of completeness – the last axiom of Set Theory:

Foundation axiom

$\boxed{\text{The membership relation is well-founded.}}$

infinite chain $\ldots \in x_n \in \cdots \in x_2 \in x_1 \in x_0$ not possible.

Thereby, providing a

Principle of $\in$*-Induction* .

Special case of well-founded induction.