Theorem 134 *For every set* A,

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

PROOF: Define $p : \underline{\mathrm{EqRel}}(A) \longrightarrow \underline{\mathrm{Part}}(A)$

Given $E \in \underline{\mathrm{EqRel}}(A)$, we define $p(E) \in \underline{\mathrm{Part}}(A)$

For $E \subseteq A \times A$ be an equiv. rel; let

$$p(E) = \{ C \subseteq A \mid \exists a \in A.\ C = [a]_E \}$$

{ the equivalence class of a

$$[a]_E = \{ x \in A \mid x \mathrel{E} a \}$$

and show $p(E)$ is a partition.

That is, show

Lemma $[a]_E = [a']_E \Leftrightarrow a E a'$

- $\forall C \in p(E),\ C \neq \emptyset$
- $\forall C, C' \in p(E).\ C \neq C' \Rightarrow C \cap C' = \emptyset$
- $\bigcup p(E) = A$

Let $C \in p(E)$; i.e. $C = [a]_E$ for some $a \in A$.
We argue that $[a]_E \neq \emptyset$, because $a \in [a]_E$ as $a E a$ by reflexivity.

We aim at defining an inverse for p, so define

$$q : \underline{\mathrm{Part}}(A) \longrightarrow \underline{\mathrm{EqRel}}(A)$$

Given $\pi \in \underline{\mathrm{Part}}(A)$, define

$$q(\pi) \subseteq A \times A$$

by stating

$$\forall a, a' \cancel{\in A \times A} . \ (a, a') \in q(\pi) \ \text{iff}_{\text{def}} \ \exists C \in \pi . \ \begin{matrix} a \in C \\ \wedge \\ a' \in C \end{matrix}$$

To show that the above is well defined we need show that $q(\pi)$ is an equiv. relation:

$$\forall a \in A.\ (a,a) \in g(\pi)$$

$$\forall a, a' \in A.\ (a,a') \in g(\pi) \Rightarrow (a',a) \in g(\pi)$$

$$\forall a, a', a'' \in A.\ (a,a') \in g(\pi) \wedge (a',a'') \in g(\pi) \Rightarrow (a,a'') \in g(\pi)$$

exercise.

$$\Longleftrightarrow \forall a \in A.\ \exists c \in \pi.\ a \in c \wedge a \in c$$

$$\Longleftrightarrow \forall a \in A.\ \exists c \in \pi.\ a \in c$$

holds because π is a partition.

Finally, we show

- for all $E \in \underline{\mathrm{EquivRel}}(A)$

$$q(p(E)) = E \ .$$

Exercise

- for all $\pi \in \underline{\mathrm{Part}}(A)$

$$p(q(\pi)) = \pi \ .$$

$\boxtimes$

Calculus of bijections

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

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

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

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

$$c^{a+b} = c^a \cdot c^b$$

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

$$2^a \qquad\qquad c^{a \cdot b} = (c^b)^a$$

Characteristic (or indicator) functions

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

$Rel([n]) \cong (n \times n)$-boolean matrices.

$$\mathcal{P}([n] \times [n]) \cong (([n] \times [n]) \Rightarrow [2])$$

$A = [n] \times [n]$

$[k] = \{0, \ldots, k-1\}$

Finite cardinality

Definition 136 *A set A is said to be* finite *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. $\mathrm{Bij}\big([n], [n]\big) \cong [n!]$

Infinity axiom

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

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. $\big(\forall\, b \in B.\, \exists\, a \in A.\, f(a) = b\big)$ $\wedge$ $\big(\forall\, a_1, a_2 \in A.\, f(a_1) = f(a_2) \implies a_1 = a_2\big)$

existence SURJECTION

uniqueness INJECTION

Surjections

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

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

covers its codomain

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

IDEA

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.*

If

$e : \mathbb{N} \twoheadrightarrow A$

Then $e(0), e(1), e(2), \ldots, e(n), \ldots\ldots$

is the whole of A.

Examples:

$\mathbb{N} \twoheadrightarrow \mathbb{Z}$

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

$\cdots$	-3	-2	-1	0	1	2	3	$\cdots$
$\cdots$	6	4	2	0	1	3	5	$\cdots$

$e(0) = 0$,
$e(1) = 1$,
$e(2) = -1$, ...

$\mathbb{N} \twoheadrightarrow \mathbb{N} \times \mathbb{N}$

$e(0) = (0,0)$

$e(1) = (1,0)$

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

$e(2) = (0,1)$

$e(3) = (0,2)$ ...

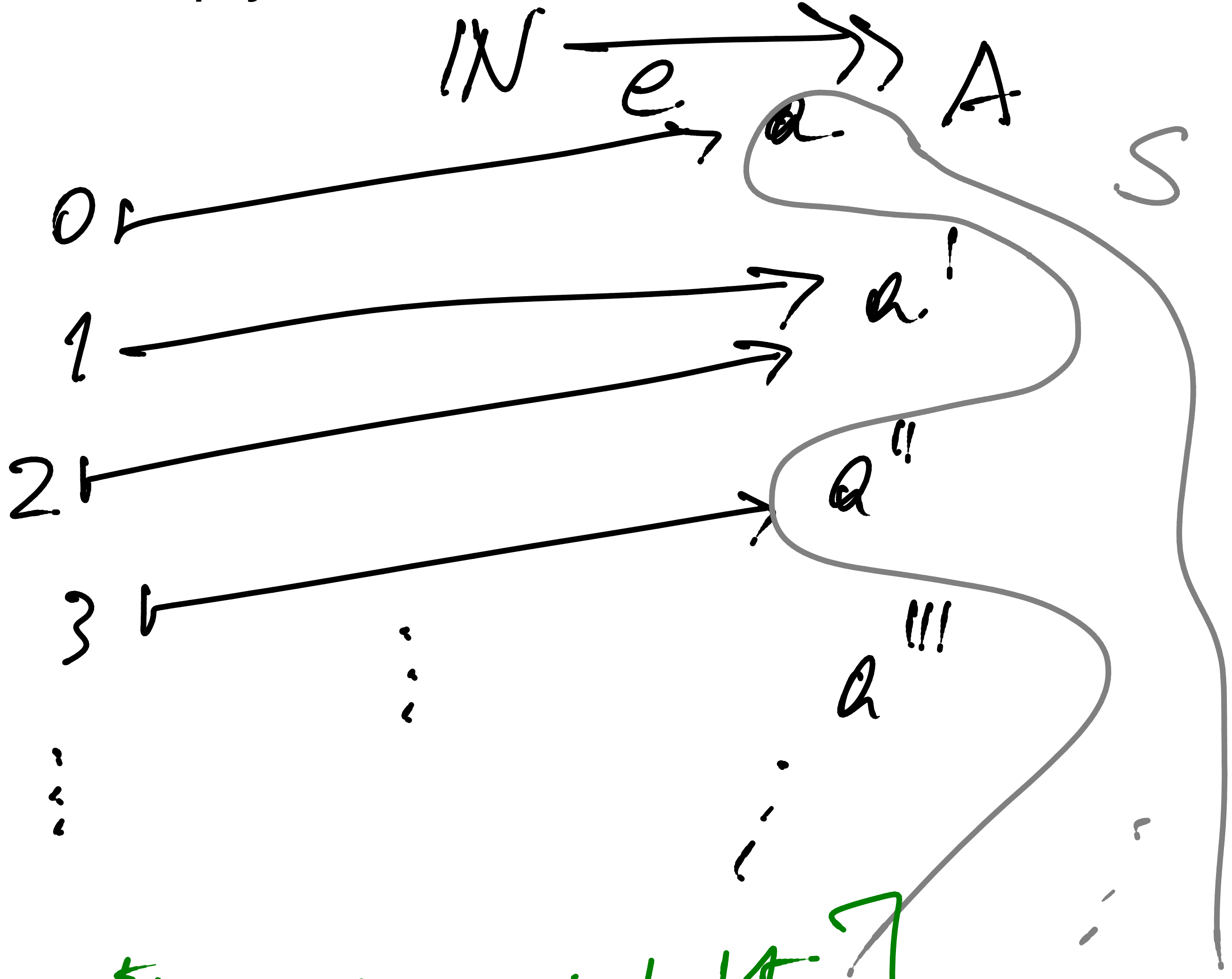
<u>Lemma</u>

If A is enumerable and $\emptyset \neq S \subseteq A$ then S enumerable.

	0	1	2	3	4	5	...
0	0	2	3	9	10		
1	1	4	8	11			
2	5	7	12				
3	6	13					
4	14						
$\vdots$							

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

PROOF:



Define
$e' : \mathbb{N} \twoheadrightarrow S$
a surjection.

$e'(0) = a$
$e'(1) = a''$

[See note on enumerability on web page]

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.*

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

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

with

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

[NOT EXAMINABLE]

Relational images

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

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

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

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.

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:

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

Unbounded cardinality

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

PROOF:

Foundation axiom

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

Thereby, providing a

Principle of $\in$*-Induction* .