Math 318
Lecture 1
September 2 2020

Naive Set Theory
What is a set? Intuitively, a set x is a collection of objects which are called elements of x

E.g.
- set of integers
- the set of all students in this lecture
- the set containing the symbols a, b, c
  We denote this set by $\{a, b, c\} \to$ (a bag containing a, b, c).

Note: $\{a, b, c\} = \{a, a, b, b, b, c\}$ We attempt to "define" a set by defining the membership relation.
Write $x \in y$, read "x belongs in y", "x is an element of y".

What set is $\{\}$? It's the emptyset. We denote this by $\emptyset$.

$$\emptyset \coloneqq \{\}$$

Question:
- $\emptyset \neq \{\emptyset\}$
- $x \notin \emptyset$
- $\emptyset \notin \emptyset$
- $\emptyset \in \{\emptyset\}$
- $\emptyset \notin \{\{\emptyset\}\}$
- $\emptyset \in \{\emptyset, \{\emptyset\}\}$
- $\{\emptyset\} \in \{\{\emptyset\}\}$

Subset: Fo set x, y, we say that x is a subset of y if all elements of x are elements of y. Symbolically,

$$\underset{\text{for all}}{\forall} z, \quad z \in x \underset{\text{implies}}{\Rightarrow} z \in y$$

We denote this by $x \subseteq y$ (some write $\subset$)

E.g.
- $\{a, b\} \subseteq \{a, b, c, d\}$
- $\{2, 7\} \subseteq \mathbb{Z} \coloneqq$ the set of integers
- $\emptyset \subseteq \emptyset$, in fact $\emptyset \subseteq X$ for any set X
- In particular, $\emptyset \subseteq \{\emptyset\}$ but also $\emptyset \in \{\emptyset\}$.
- $\{\emptyset\} \not\subseteq \emptyset$
- $\{\emptyset\} \subseteq \{\emptyset, \{\emptyset\}\}$, also $\{\emptyset\} \in \{\emptyset, \{\emptyset\}\}$
- $\{\{\emptyset\}\} \subseteq \{\emptyset, \{\emptyset\}\}$, however $\{\{\emptyset\}\} \notin \{\emptyset, \{\emptyset\}\}$

Math 318
Lecture 2
September 4 2020

Leftover from Lecture 1
"Definition" of a set(Extensionality Axiom).
A set is determined by its elements, i.e. if A and B have the same elements, then $A = B$. In other words, $A = B \underbrace{\text{ if and only if }}_{\Leftrightarrow} A \subseteq B$ and $B \subseteq A$.

We use this to prove that $A = B$.

Note: In particular, it doesn't matter which order and how many times we write the elements:

$$\{a, a, b, c, c, c\} = \{a, b, c\} = \{b, a, c\}.$$

Lecture 2
Powerset The powerset of a set X is the set of all subsets of X, denoted by $\mathcal{P}(X)$.

E.g
- $X \coloneqq \{a, b\}$ then $\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, X\}$
- $X \coloneqq \{a, b, c\}$ then $\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, X\}$

Union: For sets A, B, the union $A \cup B$ is the set of all elements of A & B

- $A \cup B = \{x \underbrace{:}_{\text{s.t.}} x \in A \underbrace{\vee}_{\text{or}} x \in B\}$
- E.g. $A = \{1, 2, 3, \}, B = \{2, 4, 5\}, A \cup B = \{1, 2, 3, 4, 5\}$

Intersection: For sets A, B, the intersection $A \cap B$ is the set of all elements that are both in A and B.

- $A \cap B = \{x : x \in A \underbrace{\wedge}_{\text{and}} x \in B\}$

Exercise: For finite sets A, B, $\underbrace{|}_{\sqcup} \underbrace{A \cup B}_{-\text{size}-} \underbrace{|}_{\sqcup} = |A| + |B| - |A \cap B|$

"no you can't use venn diagrams for proofs"

Subtraction For sets A, B, the difference $A \setminus B$ is the set of all elements in A that are not in B.

- $A \setminus B \coloneqq \{x : x \in A \text{ and } x \notin B\}$

Complements. Let U be a set (think of this as an ambient set) and $A \subseteq U$.

- E.g. $U \coloneqq \mathbb{Z}$, $A \coloneqq$ all even numbers.
- The complement A^c of A (within U) is just the set $U \setminus A$.
- In the example above: A^c is the set of all odd numbers.

(a) $A \cap B = (A^c \cup B^c)^c$

(b) $A \cup B = (A^c \cap B^c)^c$

Proof of (a) $A \cap B \subseteq (A^c \cup B^c)^c$.
Fix an arbitrary $x \in A \cap B$.
$x \in A \underbrace{\Rightarrow}_{\text{implies}} x \notin A^c$ and
$x \in B \Rightarrow x \notin B^c$.
Hence $x \notin A^c \cup B^c$.
Thus $x \in (A^c \cup B^c)^c$.

$A \cap B \supseteq (A^c \cup B^c)^c$
Fix an arbitrary $x \in (A^c \cup B^c)^c$.
Hence $x \notin A^c \cup B^c$.
Hence $x \notin A^c$ and $x \notin B^c$.
Thus $x \in A$ and $x \in B$
Therefore $x \in A \cap B$.

Proof of (b) #1. Use (a).

$$A \cup B = (A^c \cap B^c)^c$$
$$\Rightarrow (A \cup B)^c = A^c \cap B^c$$
$$\text{By part (a), } A^c \cap B^c = ((A^c)^c \cup (B^c)^c)^c = (A \cup B)^c$$

Proof of (b) #2. Fix an arbitrary element x in an ambient set U (i.e. any $U \supseteq A, B$)

$$\begin{aligned} x \in A \cup B &\Leftrightarrow x \in A \text{ or } x \in B \\ &\Leftrightarrow x \notin A^c \text{ or } x \notin B^c \\ &\Leftrightarrow \text{ not true that } (x \in A^c \text{ and } x \in B^c) \\ &\Leftrightarrow \text{ not true that } x \in A^c \cap B^c \\ &\Leftrightarrow x \in (A^c \cap B^c)^c \end{aligned}$$

Cartesian Product. For sets A, B, we define their Cartesian product $A \times B$ by

$$A \times B \coloneqq \{(a, b) : a \in A, b \in B\}$$

E.g.
- $A \coloneqq \{1, 2\}$, $B \coloneqq \{a, b, c\}$, $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$
- $\emptyset \times A = \emptyset$

In general, for finite sets A, B, $\quad |A \times B| = |A| \cdot |B|$

Here, (a, b) is the ordered pair, which is "defined" by the property that:

$$(a, b) = (c, d) \Leftrightarrow a = c \text{ and } b = d.$$

In particular, $(a, b) \neq (b, a)$ unless $a = b$.

How would we encode (a, b) as a set?

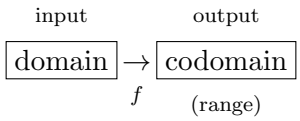
Attempts: (1) $(a, b) \coloneqq \{a, b\}$? No because $\{a, b\} = \{b, a\}$

(2) $(a, b) \coloneqq \{a, \{b\}\}$?
No because if $a = \{c\}$ then $(a, b) = \{\{c\}, \{b\}\} = \{\{b\}, \{c\}\} = (\{b\}, c)$

(3) $(a, b) \coloneqq \{\{a\}, \{a, b\}\}$ This works! Homework!

Math 318
Lecture 3
September 9 2020

Functions: Intuitively, a function is:



Each input has a unique output (although different inputs may have the same output.

E.g
- $f : \mathbb{Z} \to \mathbb{Z}$
- $x \mapsto x^2$

In general, a function f from a set X to a set Y, denoted $f : X \mapsto Y$, is a set of arrows from X to Y with a special property.

Formally, what is an arrow going from a point $x \in X$ to a point $y \in Y$?
We model this by the ordered pair (x, y).
The set of all arrows (= ordered pairs) is precisely the Cartesian product $X \times Y$.
Hence each function f is a subset of $X \times Y$ with a special property.

Definition: A function $f : X \mapsto Y$ from a set X to a set Y is a subset of $X \times Y$.
i.e. $f \subseteq X \times Y$ such that for each $x \in X$, there is a unique $y \in Y$ with $(x, y) \in f$

Notation: Instead of writing $(x, y) \in f$, we write $f(x) = y$.

Definition: A function $f : X \mapsto Y$ is called

- injective (or one-to-one) if whenever $x_1 \neq x_2$, we have $f(x_1) \neq f(x_2)$ for all $x_1, x_2 \in X$. Equivalently, for all $x_1, x_2 \in X$, $\quad f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
- surjective (or onto) if for each $y \in Y$, there is $x \in X$ with $f(x) = y$
- bijective if it's both injective and surjective.

Examples

Examples
- $f : \mathbb{Z} \to \mathbb{Z}$ $x \mapsto x^2$
  - not injective: $f(-n) = f(n)$
  - not surjective: for example 2 doesn't have an arrow coming to it.

set of all natural numbers, including 0
- $f : \overbrace{\mathbb{N}} \to \mathbb{Z}$ $x \mapsto x^2$
  - injective: if $\underbrace{f(x)}_{=x^2} = \underbrace{f(y)}_{=y^2}$, since $x, y \geq 0$ it must be that $x = y$
  - still not surjective
- $f : \mathbb{N} \to \{y \in \mathbb{Z} : \exists\ x \in \mathbb{N} \text{ s.t. } x^2 = y\}$.
  - This is bijective

Definition: For $f : X \mapsto Y$ & sets $A \subseteq X$, $B \subseteq Y$

- the f-image of A is the set

$$f(A) \coloneqq \{f(x) : x \in A\} = \{y : \exists\, x \in A \text{ s.t. } f(x) = y)\}$$

- the f-preimage of B is the set

$$f^{-1}(B) \coloneqq \{x \in X \text{ s.t. } f(x) \in B\}.$$

  Note: For $x \in X$, $f(\{x\})$ is not the same as $f(x)$:

  - for $f(x) = x^2$, $f(2) = 4$, but $f(\{2\}) = \{4\}$

  Similarly, for $y \in Y$, $f^{-1}(\{y\})$ is not the same as $f^{-1}(y)$ $---$ the latter is typically not even defined.
  For example, $f : \mathbb{N} \to \mathbb{N}$, $x \mapsto 1 + x$,

  - $f^{-1}(\{0\}) = \emptyset$
  - $f^{-1}(\{1\}) = \{0\}$ and not 0

Note: $F(A) \subseteq Y$, $f^{-1}(f(A)) = A$? No in general. Only if injective.
Let $f(a) = c$ and $f(b) = c$

- $f(A) = \{f(a)\} = \{c\}$
- $f^{-1}(\{c\}) = \{a, b\} \not\supseteq f(A)$

In general, $f^{-1}(f(A)) \supseteq A$

Is $f(f^{-1}(B))$? No, unless f is surjective. (more precisely, $\forall b \in B$, $\exists\, x \in X$ s.t. $f(x) = b$.)
Let $f(a) = b_1$ and simply b_2

- $f^{-1}(B) = \{a\}$
- $f(\{a\}) = \{b_1\} \neq B$

In general, $f(f^{-1}(B)) \supseteq B$

Note: f is injective $\Leftrightarrow \forall y \in Y$, $f^{-1}(\{y\})$ has at most one element
f is surjective $\Leftrightarrow f(X) = Y \Leftrightarrow \forall y \in Y$, $f^{-1}(\{y\}) \neq \emptyset$.

Definition: For functions $f : X \mapsto Y$, $g : Y \mapsto Z$, the composition $g \circ f : X \mapsto Z$ as the function $g \circ f(x) = g(f(x))$.

$f : \mathbb{Z} \mapsto \mathbb{N}$, $x \mapsto x^2$ and $g : \mathbb{N} \to \mathbb{N}^+ \coloneqq \{1, 2, 3, \ldots\}$ and $y \mapsto 1 + y$

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

Definition: For a set X, the identity on X is the function $\mathrm{id}_X : X \to X$, $x \mapsto x$

DefinitionFor $f : X \to Y$, a function $g : Y \to X$ is called

- a left-inverse of f if $g \circ f = \mathrm{id}_x$
- a right-inverse of f if $f \circ g = \mathrm{id}_y$
- a (two-sided) inverse of f if $f \circ g = \mathrm{id}_y$ & $g \circ f = \mathrm{id}_x$
  (if this exists, it's unique, so we'd say "the inverse".)

Math 318
Lecture 4
September 11 2020

Note: Left and right inverses may not be unique, but since the two-sided inverse is unique, we may denote it by f^{-1}.

Proposition: let $f : X \to Y$

(a) f has a left-inverse $\Leftrightarrow$ f is injective

(b) f has a right-inverse $\Leftrightarrow$ f is surjective

(c) f has a (two-sided) inverse $\Leftrightarrow$ f is bijective

Proof (a)
($\Rightarrow$) Suppose f has a left-inverse $g : Y \to X$
Fix arbitrary $x_1, x_2 \in X$
Suppose $f(x_1) = f(x_2)$. Want: $x_1 = x_2$.
Apply g to $f(x_1) = f(x_2)$ and get $x_1 = g \circ f(x_1) = g \circ f(x_2) = x_2$

($\Leftarrow$:) Suppose f is injective. This means that for every $y \in f(x)$, $f^{-1}(\{y\})$ has exactly one element.
Suppose $X \neq \emptyset$ since otherwise, $f = \emptyset$ and $g \coloneqq \emptyset$ is a left-inverse.
Fix $x_0 \in X$.
Now define $g : Y \to X$ by $y \mapsto \begin{cases} \text{the unique } x \in f^{-1}(\{y\}) & \text{if } y \in f(x) \\ x_0 & \text{otherwise} \end{cases}$ Immediate the check that for each $x \in X$, $g \circ f(x) = x$.

Proof of (b)
($\Rightarrow$): Suppose f has a right-inverse $g : Y \to X$.
Fix an arbitrary $y \in Y$. Need to find an $x \in X$ with $f(x) = y$.
$X \coloneqq g(y)$ then $f(x) = f(g(y)) = f \circ g(y) = y$.
$\Leftarrow$: Suppose f is surjective. For each $y \in Y$, any right-inverse has to take y to one of the points in $f^{-1}(\{y\})$.
Note surjectivity is the same as $f^{-1}(\{y\}) \neq \emptyset$ for all $y \in Y$.
Because of this, by Axiom Choice, there is a function $g : Y \to X$ s.t. $\forall y \in Y$, $g(y) \in f^{-1}(\{y\})$.
It's immediate that $\forall y \in Y$, $f \circ g(y) = f(g(y)) = y$.

Proof of (c)
($\Rightarrow$): Follows from ($\Rightarrow$) of parts (a) and (b).
$\Leftarrow$: Suppose f is bijective. Then $\forall y \in Y$, $f^{-1}(\{y\})$ is a singleton.
Let g: $Y \to X$ be defined by $y \mapsto$ the unique $x \in f^{-1}(\{y\})$.
Easy to check that

- $forallx \in X$, $g \circ f(x) = x$
- $forally \in Y$, $g \circ f(y) = y$

Relations: For any set A, denote by $A^2 \coloneqq A \times A$.

define
- $A^n \coloneqq A^{n-1} \times A$ for all $n \geq 1$.
- $A^0 \coloneqq \emptyset$.

Technically, an element of A^3 looks like this $((a_1, a_2), a_3)$, and that of A^4 $\ldots$ $(((a_1, a_2), a_3), a_4)$, but we will just write (a_1, a_2, a_3, a_4).

Definition: For $n \geq 0$, any subset $R \subseteq A^n$ is called an n-arg relation on A.
In particular, a binary relation on A is just a subset of A^2.

Notation: Instead of writing $(a_1, a_2) \in R$, we write $a_1 \ R \ a_2$.

Partial orders. A binary relation R on a set X is called an equivalence relation if

i R is reflexive: $\forall x \in X, \quad x \ R \ x$

ii R is symmetric: $\forall x, y \in X, \quad x \ R \ y \to y \ R \ x$

iii R is transitive: $\forall x, y, z \in X, \quad x \ R \ y$ and $y \ R \ z \to x \ R \ z$

Examples

- let $X \coloneqq$ all people, and R be the relation of having the same number of hair.
- let $X \coloneqq \mathbb{Z}$ and define the binary relation $\equiv_7$ on $\mathbb{Z}$ as follows:

$$\text{for } x, y \in \mathbb{Z}, x \equiv_7 y \Leftrightarrow \underbrace{x - y \text{ is divisible by } 7}_{7|x-y}$$

I claim this is an equivalence relation on $\mathbb{Z}$

Indeed:

- Reflexivity: For any $x \in \mathbb{Z}$, $x - x = 0$ so divisible by $7 \Rightarrow x \equiv_7 x$.
- Symmetricity: For any $x, y \in \mathbb{Z}$, if $x \equiv_7 y$, then $7|x - y$ so $7|y - x$ hence $y \equiv_7 x$.
- Transitivity: For any $x, y, z \in \mathbb{Z}$, suppose $x \equiv_7 y$ and $y \equiv_7 z$.
  We have $7|x - y$ and $7|y - z$.
  Want $7|x - z$.
  $x - z = x - y + y - z = (x - y) + (y - z)$ and since $7|x - y$ and $7|y - z$, it must divide $x - z$.

Definition: For an equivalence relation R on a set X, for any $x \in X$, define the R-clan of x by

$$[x]_R \coloneqq \{y \in X : x \ R \ y\}.$$

Claim: For all $x, y \in X$, $x \ R \ y \Leftrightarrow [x]_R = [y]_R$
Proof of claim
($\Rightarrow$) $x \ R \ y$ then $y \in [x]_R$.
Enough to show $[y]_R \subseteq [x]_R$ hence $x \ R \ y \Rightarrow y \ R \ x$ which will give $[x]_R \subseteq [y]_R$.
Fix $z \in [y]_R$. Hence $y \ R \ z$. But $x \ R \ y$, so by transitivity, $x \ R \ z \Rightarrow z \in [x]_R$.
Thus $[y]_R \subseteq [x]_R$.
($\Leftarrow$) $y \in [y]_R$ by reflexivity, so $y \in [x]_R \Rightarrow x \ R \ y$.

Math 318
Lecture 5
September 14 2020

Corollary
For an equivalence relation R, distinct classes are disjoint.

Proof. Let $\{x\}_R$ and $\{y\}_R$ be R-classes.
Suppose $\{x\}_R \cap \{y\}_R \neq \emptyset$. Hence $\exists z \in \{x\}_R \cap \{y\}_R$.
This means $x \; R \; z$ and $y \; R \; z$.
By previous proposition, $[x]_R = [z]_R = [y]_R$ □

Definition A partition P of a set X is a subset of $\underbrace{\mathcal{P}}_{\text{the powerset}}(X)$ s.t.

1. distinct elements of P are disjoint
2. $\forall x \in X \; \exists$ (necessarily unique) $C \in P$ s.t. $x \in C$.

What we showed is that for an equivalence relation R, the set

$$\{[x]_R : x \in X\}$$

of R-classes is a partition of X.

Example For $\equiv_7$ on $\mathbb{Z}$, what are the $\equiv_7$-classes?

$$\begin{aligned}
[0]_{\equiv_7} &= \{n \in \mathbb{Z} : 7|n\} = \{7n : n \in \mathbb{Z}\} = [7]_{\equiv_7} \\
[1]_{\equiv_7} &= \{n \in \mathbb{Z} : 7|n-1\} = \{n \in \mathbb{Z} : \text{ n has remainder 1 when divided by 7}\} = [8]_{\equiv_7} \\
&= \{7n+1 : n \in \mathbb{Z}\} \\
&\vdots \\
[6]_{\equiv_7} &= \{7n+6 : n \in \mathbb{Z}\} = [13]_{\equiv_7}
\end{aligned}$$

Remark Equivalence relations define a partition. But conversely every partition defines an equivalence relation (shown in HW 2).

Definition For an equivalence relation R on a set X, the quotient of X by R is the set $X/R \coloneqq \{[x]_R : x \in X\}$.

In the example of $\equiv_7$, $\mathbb{Z}/\equiv_7$ has 7 elements.
In other words, $\mathbb{Z}/\equiv_7$ can be "canonically identified" with $\{0, 1, \ldots, 6\}$

In fact, what are rational numbers? What is the set $\mathbb{Q}$ of rational numbers?
You can say that $\frac{3}{4}$ is a rational number and somehow $\frac{3}{4} = \frac{9}{12} = \frac{6}{8}$.

Rational numbers are equivalence classes for a particular equivalence relation R on $\mathbb{Z} \times \mathbb{Z}^+$, where $\mathbb{Z}^+ \coloneqq \{n : n > 0\}$.
This R defined by $(x_0, y_0) \; R \; (x_1, y_1) \coloneqq x_0 y_1 = y_0 x_1$.

Denote $\underbrace{\frac{x}{y}}_{\text{a rational number}} \coloneqq [(x, y)]_R$, so now $\frac{3}{4} = [(3, 4)]_R = [(9, 12)]_R = \frac{9}{12}$.
Denote $\mathbb{Q} \coloneqq \mathbb{Z} \times \mathbb{Z}^+ / R$ — the set of rationals.
$\mathbb{Z}$ is identified as $\left\{\frac{n}{1} : n \in \mathbb{Z}\right\}$, so $\mathbb{Z} \subseteq \mathbb{Q}$

ZFC $\coloneqq$ Zermelo-Fraenkel Set Theory with Choice

Language: The alphabet of set theory consists of the following symbols:

$$= \; \wedge \; \vee \; \underbrace{\neg}_{\text{negation}} \; \forall \; \exists \; \Rightarrow \; (\;) \; , \; \in$$

and symbols for variables: $x_0\ x_1\ x_2\ x_3\ \ldots$

A math statement or formula is a sequence of symbols from the alphabet defined as follows:

1. $x_i = x_j$ is a formula, for all i, j (atomic formula)
2. $x_i \in x_j$ is a formula, for all i, j (atomic formula)
3. If φ and ψ are formulas, then so are the following
   $(\varphi) \vee (\psi)$, $(\varphi) \wedge (\psi)$, $\neg(\varphi)$, $(\varphi) \Rightarrow (\psi)$
4. If φ is a formula, then for all x:
   $\forall x_i(\varphi)$ and $\exists x_i(\varphi)$
   are formulas

Math 318
Lecture 6
September 16 2020

Examples
- $\forall x_0(x_0 = x_0)$ is a formula, but $\forall x_0 x_0 = x_0$ isn't
- $\exists x_0(x_0 = x_0) \vee x_1 \in x_1$ isn't a formula, but $(\exists x_0(x_0 = x_0)) \vee (x_1 \in x_1)$ is.

We will abuse the definition of fomula & use other letters for variables, like $x, y, z, A, B, C, \alpha, \beta, \gamma$, ??, ... & we will also not strictly follow the parentheses rules.
We will also use abbreviations

- $x \neq x$ stands for $\neg(x = x)$
- $x \notin x$ stands for $\neg(x \in x)$
- $\forall x \in A(\varphi)$ stands for $\forall x(x \in A \Rightarrow \varphi)$
- $\exists x \in A(\varphi)$ stands for $\exists x(x \in A \wedge \varphi)$

Sometimes, we would like to emphasize certain variables when writing a formula.
For example in a formula $\varphi := x \notin X$, we may want to emphasize x, so we write $\varphi(x)$ & we read this as "φ of x holds" or "x satisfies φ.

Similarly, we may write more than one variable: $\varphi(x, y)$. And these variables don't have to show up in φ: e.g., $\varphi := x = x$, but we may write $\varphi(y, z)$

Russell's Paradox: In math, we often define a set using a property, i.e. a formula φ. For example, we may write

- $\{x : x = x\}$
- $\{x : x \notin x\}$
- $\{x : x \neq x\} = \emptyset$

Are these valid definitions of sets? We interpret $\{x : x \notin x\}$ as "the set of all sets x such that $x \notin x$".
More generally, $\{x : \varphi(x)\}$ is interpreted as "the set of all sets x for which φ holds".

Claim: $\{x : x \notin x\}$ is not a valid definition of a set.

Proof. Say it is, let's denote this set by $y \coloneqq \{x : x \notin x\}$.
For a set x, x would be in y, $\Leftrightarrow x \notin x$. Take $x \coloneqq y$.
Then $y \in y \Leftrightarrow y \notin y$. This is a contradiction. □

The axioms of ZFC

0. **Set existence**: This axiom says that there exists a set (we have to start with something). Formally,
$$\exists x(x = x)$$

1. **Pairing**: This says that for any set x, y there is a set z that contains both x, y, i.e.
$$\forall x \forall y \exists z(x \in z \wedge y \in z)$$
   - **Note**: This axiom doesn't say that $z = \{x, y\}$. Rather, it says that $z \supseteq \{x, y\}$.

   This axiom doesn't guarantee the existence of the set $\{x, y\}$

2. **Union**: This says given a set ζ, there is a set z that contains as members all elements of sets $x \in \zeta$. In other words, z contains the the union of all sets in ζ
$$\forall \zeta \exists z \forall x \in \zeta(x \subseteq z)$$
   where $a \subseteq b$ abbreviates $\forall c \in a(c \in b)$.
   - **Note**: This axiom doesn't give us exactly the union of all sets $x \in \zeta$, but rather, a superset of it.
   - **Intuition**: Think of ζ as a collection of sets like
$$\zeta \coloneqq \{\{a, b\}, \{b, c, d\}, \{a\}\}$$
     The union of all sets in ζ, denoted by $\cup\zeta$, is
$$\cup\zeta = \{a, b\} \cup \{b, c, d\} \cup \{a\} = \{a, b, c, d\}$$

3. **Powerset**: This says that for any set x there is a set that contains as member every subset of x.
$$\forall x \exists z \forall y(y \subseteq x \Rightarrow y \in z).$$
   - **Note**: This doesn't say that $\mathcal{P}(x)$ exists, but rather it gives us a superset of $\mathcal{P}(x)$.

4. **Subset** (aka Comprehension) axiom schema (infinitely-many axioms)
   This bunch of axioms is one axiom for every formula φ.
   For a given formula φ, the φ-subset axiom says that for every set x there is z whose members are exactly those elements y of x for which the formula φ holds.
$$\forall x \exists z \forall y(y \in z \Leftrightarrow (\varphi(y) \wedge y \in X))$$

4. **Continuation of** Subset (aka Comprehension) axiom schema (infinitely-many axioms) In other words, this says that for any given set x, the following is a set

$$\{y \in x : \varphi(y)\}$$

Remark: Russell's paradox used the "definition" $\{y_{\underset{\in X \text{ is missing}}{\sqcup}} : \varphi(y)\}$ without an apriori ambient set x to which all of these y-s belong.

Examples of use

- **Emptyset**. Let x be a set given by the Existence axiom. By the subset axiom,

$$\emptyset = \{y \in x : y \neq y\}$$

is a set.
But $\forall y(y = y)$ so this set doesn't have any elements.
Denote this setby $\emptyset$.

- **Pair**. Fix any sets x, y. By the pairing axiom, there is a set z s.t. $x \in z$ and $y \in z$. Then by the subset axiom, this is a set: $\{t \in z : t = x \vee t = y\}$.
We denote this set by $\{x, y\}$
- Same for the Union
- Same for the Powerset.

5. Replacement (axiom schema) For a set X, we say that the formula $\varphi(x, y)$ defines a function X if $\forall x \in X$, $\exists$ a unique set y s.t. $\varphi(x, y)$ holds.
Formally, this is written $\forall x \in X \exists y(\varphi(x, y) \wedge \underbrace{(\forall y'(\varphi(x, y') \Rightarrow y' = y))}_{\Leftrightarrow \text{ such a } y \text{ is unique}})$

Formally, this is written $\forall x \in X \exists! y(\varphi(x, y))$.

For the future, we would write $\exists! y(\psi(y))$ to mean that there exists a unique y such that $\varphi(y)$ holds, i.e.

$$\underset{\text{unique}}{\exists \underset{\sqcup}{!} y}(\psi(y)) :- \underbrace{\exists y(\psi(y))}_{\text{existence}} \wedge \underbrace{\forall y \forall y'(\psi(y) \wedge \psi(y') \Rightarrow y = y')}_{\text{uniqueness}}$$

The φ-Replacement axiom says that for every set X, if φ defines a function on X, then there is a set Y that is a codomain for this function, i.e.

$$\forall X \underbrace{(\forall x \in X \ \exists! y \ \varphi(x, y))}_{\varphi \text{ defines a function on } X} \Rightarrow \exists Y \forall x \in X \ \exists y \in Y \ \varphi(x, y))$$

6. **Infinity** ...

7. **Foundation axiom** ...

8. **Axiom of Choice** ...

9. **Extensionality** Sets are determined by what elements they contain, i.e.

$$\forall x \forall y(\forall z(z \in x \Leftrightarrow z \in y) \Leftrightarrow X = Y).$$

Partial orders
Definition A partial order (or just order) on a set X is a binary relation $\leq$ satisfying the following:

1. Reflexivity: $\forall x \in X \; x \leq x$
2. Anti-symmetry: $\forall x \in X \; \forall y \in X \; (x \leq y \wedge y \leq x \Rightarrow x = y)$.
3. Transitivity: $\forall x, y, z \in X \; x \leq y \wedge y \leq z \Rightarrow x \leq z$.

Examples
- The usual $\leq$ on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. This is a total order.
- The relation $\subseteq$ on $P(X)$ for any set X.
  This is easy to check to be a partial order, but here there are incomparable elements, for example, if $X \coloneqq \{0, 1, 2\}$ then the subsets $Y \coloneqq \{0, 1\}$ and $Z \coloneqq \{0, 2\}$ are incomparable.
- Divisibility on $\mathbb{Z}^+$.
  - If $x|y$ and $y|z$ then $x|z$, so it's transitive.
  - If $x|y$ and $y|x$ then $x = y$, so it's anti-symmetric.
  - $x|x$ so it's reflexive.

  However, there are incomparable elements: 14 and 9.

An order $(X, <)$ is called total (or linear) if any two elements of X are $\leq$-comparable, i.e. $\forall x, y \in X \; x \leq y$ or $y \leq x$.

An order $(X, \leq)$ is called a well-order if every *subset* $Y \subseteq X$ admits a least element.
An element $y_0 \in Y$ is called the least-element of Y if $\forall y \in Y (y_0 \leq y)$.

Proposition Any well-order $(X, \leq)$ is total.

Proof. Fix any $x, y \in X$. Let $Y \coloneqq \{x, y\}$. Then well-orderness for Y implies that Y has a least element $z \in Y$. Then $z \leq x$ and $z \leq y$ (and $z = x$ or $z = y$). Thus, $x \leq y$ or $y \leq x$ □

Math 318
Lecture 8
September 21 2020

The word minimum element means the same as least.

Definition Let $(x, \leq)$ be a partial order and $Y \leq X$. Call $y_0 \in Y$ a minimal of Y (with respect to $\leq$) if $\nexists y \in Y \setminus \{y_0\}$ s.t. $y \leq y_0$.
In other words, $\forall y \in Y$, if $y \leq y_0$, then $y = y_0$

Observation A least element is also minimal, however, the converse isn't true.

Example Take $(\mathbb{Z}^+, 1)$, i.e. positive integers with | being divisibility.
Let $Y \coloneqq \{3, 27, 10\}$.
3 and 10 are minimal elements, but there is no least element.
However, $Y \coloneqq \{2, 12, 100\}$, then 2 is the least element of Y.

Observation The least element of a set is unique (follows from anti-symmetry).

Definition: A strict partial order $<$ on a set X is a binary relation on X satisfying:

1. Anti-reflexivity $x \not< x$ for all $x \in X$
2. Asymmetric if $x < y$, then $y \not< x$ for all $x, y \in X$

3. Transitivity: if $x < y$ and $y < z$ then $x < z$, for all $x, y, z \in X$.

Note (i) follows from (ii) by taking $y \coloneqq x$

We can define a strict order from a non-strict order, and vice versa as follows:

- $<\rightsquigarrow\leq$. Define $x \leq y :\Leftrightarrow x = y$ or $x < y$
- $\leq\rightsquigarrow<$. Define $x < y :\Leftrightarrow x \leq y$ and $x \neq y$.

Definition Let $(X, <_X)$, $(Y, <_Y)$ be strict partial orders.
A function $f : X \to Y$ is called order-preserving if $\forall x_0, x_1 \in X$

$$x_0 <_X x_1 \Rightarrow f(x_0) <_Y f(x_1).$$

f is called an order-isomorphism if it's a bijection and both f and f^{-1} are order-preserving. In other words, f is a bijection and

$$x_0 < x_1 \Leftrightarrow f(x_0) < f(x_1)$$

for all $x_0, x_1 \in X$.
$(X, <_X)$ and $(Y, <_X)$ are called isomorphic if there is an isomorphism between them.

Example: Let $X \coloneqq \{0, 1\}$ with $0 <_X 1$.
Let $Y \coloneqq \{0, 1\}$ with $<_Y \coloneqq \emptyset$.
f is a bijection, f^{-1} is order preserving, but f isn't order preserving.

Observation. If both $(X, <_X)$ and $(Y, <_Y)$ are both total, then any bijective order-preserving function $f : X \to Y$ is an order-isomorphism.

Proof. If $f(x_0) < f(x_1)$ then x_0 must be $< x_1$, because otherwise, $x_1 = xx_0$ or $x < x_0$ so we would have $f(x_1) = f(x_0)$ or $f(x_1) < f(x_0)$, contradiction $f(x_0) < f(x_1)$ □

Definition: Let $(X, <)$ be a well-order. A set $Y \subseteq X$ is said to be an **initial segment** if it is closed downward, i.e. $\forall x \in X$ if $x \in Y$ then all elements $< x$ are also in Y. Symbolically:

$$\forall x \in Y \forall y \in X (y < x \Rightarrow y \in Y).$$

Example: Let $X \coloneqq \mathbb{N}$ and $<$ the usual order.
Then $\{0, 1, 2, \ldots, n\}$ is an initial segment.
Also $\mathbb{N}$ itself is an initial segment.

This cannot happen in total orders

Math 318
Lecture 9
September 23 2020

Note that for an order $(X, <)$ X itself is an initial segment. So for an initial segment $I \subseteq X$, we call I proper if $I \neq X$

Observation If $(X, <)$ is a well-order, then every proper initial argument is of the form $X_{<_a} \coloneqq \{b \in X : b < a\}$ for some $a \in X$.

Proof. Let I be a proper initial segment. In particular $X \setminus I \neq \emptyset$, this has a least element $a \in X \setminus I$.
Therefore, $X_{<_a} \subseteq I$.
But I is an initial segment, so $a \notin I \Rightarrow \forall b \geq a, b \notin I$.
Hence, $I \subseteq X_{<_a}$ □

Uniqueness Lemma Let $(A, <_A)$ and $(B, <_B)$ be well orders.
For any initial segment $A' \subseteq A$ of $(A, <_A)$ there is at most one order-isomorphism from A' to an initial segment of $(B, <_B)$.

Proof. Let $f : A' \to B'$ and $g : A' \to B''$ be order-isomorphisms from A' to initial segments $B', B'' \subseteq B$ of $(B, <_B)$, where B', B'' are distinct or the same.
Suppose towards a contradiction that $f \neq g$.
Hence $\{a \in A' : f(a) \neq g(a)\} \neq \emptyset$, so it has a least element a_0.
WLOG, suppose $F(a_0) <_B g(a_0)$. In particular, $f(a_0) \in B''$ because B'' is an initial segment and $g(a_0) \in B''$.
Hence we can apply g^{-1} to both sides of $f(a_0) <_B g(a_0)$ and get $g^{-1}(f(a_0)) <_A a_0$.
But $a_1 < a_0$ so $f(a_1) = g(a_1)$ because a_0 was the least at which f and g differ.
$g(a_1) = g(g^{-1}(f(a_0))) = f(a_0)$, thus $f(a_0) = f(a_1)$, contradicting f being order-preserving (also injective). □

Notation For well-orders $(A, <_A)$ and $(B, <_B)$, we write

- $(A, <_A) \preceq (B, <_B)$ if $(A, <_B)$ is order-isomorphic to an initial segment of $(B, <_B)$.
- $(A, <_A) \prec (B, <_B)$ if $(A, <_B)$ if $(A, <_A)$ is order-isomorphic to a proper initial segment of $(B, <_B)$.

Corollary For a well-order $(A, <_A), (A, <_A) \not\prec (A, <_A)$.

Proof. We already have that the identity map $A \to A$, $a \mapsto a$ is an order-isomorphism from A to A itself so if $(A, <_A) \prec (A, <_A)$ was true, we'd have another order-isomorphism from A to a proper initial segment of $(A, <_A)$, contradicting the uniqueness lemma. □

Observation. For well-orders $(A, <_A), (B, <_B), (C, <_C)$,

1. $(A, <_A) \prec (B, <_B) \preceq (C, <_C) \Rightarrow (A, <_A) \prec (C, <_C)$
2. $(A, <_A) \preceq (B, <_B) \prec (C, <_C) \Rightarrow (A, <_A) \prec (C, <_C)$

Theorem (Fundamental theorem about well-orders). For well-orders $(A, <_A), (B, <_B)$, exactly one of the following holds:

1. $(A, <_A) \prec (B, <_B)$
2. $(A, <_A) \cong (B, <_B)$, i.e. they are order-isomorphic,
3. $(A, <_A) \succ (B, <_B)$

Proof. These are mutually exclusive by the Corollary and the Observation above,: for example, if (i) and (ii) holds, then $(A, \leq_A) \prec (B, \leq_B) \cong (A, \leq_A) \Rightarrow (A, \leq_A) \prec (A, <_A)$ contradicting the Corollary.
Now we prove that at least one of them holds. □

We suppose that (ii) and (iii) fail, i.e. $(A, <_A) \not\preceq (B, <_B)$ and show (i)
i.e. $(A, <_A) \prec (B, <_B)$
This can technically be done by transfinite induction
Even if $A \neq \emptyset$, there exists isomorphisms between some initial segments of A and initial segments of B.
Intuitively: By the uniqueness lemma, any two such isomorphisms have to agree on the common A part of their domains.
Let $F \coloneqq \{f \in B^A : f \text{ is an order-isomorphism from an initial segment of } A \text{ to that of } B\}$.
By the uniqueness lemma, $\forall f, g \in F$, either $f \subseteq g$ or $g \subseteq f \ldots$

Math 318
Lecture 10
September 25 2020

Claim 1 $\forall f, g \in F$, $\text{dom}(f) \subseteq \text{dom}(g)$ or $\text{dom}(g) \subseteq \text{dom}(f)$.

Proof. If $\text{dom}(f)$ or $\text{dom}(g)$ is equal to the whole A, we're done. So suppose both are proper initial segments of $(A, \leq_A)$, hence $\exists a_0, a_1 \in A$ s.t. $\text{dom}(f) = A_{<a_0}$ and $\text{dom}(g) = A_{<a_1}$ (proved earlier). But $a_0 \leq a_1$, or $a_1 \leq a_0$, so $\text{dom}(f) \subseteq \text{dom}(g)$ or $\text{dom}(g) \leq \text{dom}(f)$. □

Claim 2 $\forall f, g \in F$ s.t. $\text{dom}(f) \subseteq \text{dom}(g)$, $\forall a \in \text{dom}(f)$, $f(a) = g(a)$.
In other words, $g|_{\text{dom}(f)} = f$.

Proof. By the uniqueness lemma, because $g|_{\text{dom}(f)}$ is also an order-isomorphism from $\text{dom}(f)$ to an initial segment of $(B, <_B)$. □

These two claims imply that $\forall f, g \in F$, $f \subseteq g$ or $g \subseteq f$. (*)

Now let $h \coloneqq \cup F$. By (*), h is a function and by Claim 1, $\text{dom}(h)$ is an initial segment of A.
Moreover, f is an order-isomorphism from $\text{dom}(h)$ to an initial segment of B.
We claim that $\text{dom}(h) = A$.
Suppose not, then $\text{dom}(h) = A_{<_a}$ for some $a \in A$.
But $\text{im}(h) \coloneqq h(A_{<_a})$ is an initial segment of $(B, <_B)$ because h is an order-isomorphism from an initial segment of A.
If $\text{im}(h) = B$, then h^{-1} is an order-isomorphism from B with an initial segment of A, i.e., $(B, <_B) \preceq (A, <_A)$, but we'll assume this isn't the case.
Thus $\text{im}(h)$ is a proper initial segment of B, hence is of the form $B_{<_b}$ for some $b \in B$. Let $\overline{h} \coloneqq h \cup \{(a, b)\}$. But now $\overline{h}$ is an order isomorphism from an initial segment of A to that of B, thus $\overline{h} \in F$, hence $\overline{h} \subseteq \cup F = h$, contradicting that $a \notin \text{dom}(h)$.

Ordinals

Definition: A set x is called transitive (not to be confused with transitive relation) if $\forall y, z$, if $z \in y$ and $y \in x$ then $z \in x$

Example
- $x \coloneqq \emptyset$ is a transitive set.
- $x \coloneqq \{\emptyset\}$ is a transitive set: $y \coloneqq \emptyset$, so $y \in \{\emptyset\}$ but there is not $z \in y$.
- $x \coloneqq \{\emptyset, \{\emptyset\}\}$ is transitive: $y \coloneqq \{\emptyset\}$ and $z \in y$, then $z \in x$
- $x \coloneqq \{\{\emptyset\}\}$ isn't transitive: $y \coloneqq \{\emptyset\}$ then $z \coloneqq \emptyset \in y$ but $z \notin x$.

Definition A set α is called an ordinal if it is transitive and the relation $\in$ on α is a strict well-order.

Example
- $\emptyset$ is an ordinal.
- $\{\emptyset\}$ is an ordinal.
- $\{\emptyset\{\emptyset\}\}$ is an ordinal.
- $\alpha \coloneqq \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$ isn't an ordinal.
  α is a transitive set:
  - $y \coloneqq \{\emptyset\}$ and $z \coloneqq \emptyset$, then $z \in \alpha$
  - $y \coloneqq \{\{\emptyset\}\}$ and $z \coloneqq \{\emptyset\}$, then $z \in \alpha$

  But $\in$ is not a transitive relation on α,
  Indeed: $\emptyset \in \{\emptyset\} \in \{\{\emptyset\}\}$ but $\emptyset \notin \{\{\emptyset\}\}$.

Lemma: Let α be an ordinal.

(a) $\alpha \notin \alpha$

(b) For any $y \in \alpha$, $y = \alpha_{\in y} \coloneqq \{z \in \alpha : z \in y\}$

(c) The $\in$-least element of α (if $\alpha \neq \emptyset$), is $O \coloneqq \emptyset$.

(d) Every $\beta \in \alpha$ is itself an ordinal

Proof (a) Suppose α is an element of α.
But $\in$ is an antireflective binary relation on α (because it is a strict partial order), thus $\forall z \in \alpha$, $z \notin z$.
In particular, for $z \coloneqq \alpha$ this is true as well, i.e. $\alpha \notin \alpha$ which contrdicts the assumption that $\alpha \in \alpha$.

(b) The set $\alpha_{\in y} \coloneqq \{z \in \alpha : z \in y\} \subseteq y$ (by definition)
For the converse, fix $z \in y$, hoping to show that $z \in \alpha_{\in y}$.
By transitivity of α, $z \in \alpha$, so $z \in \alpha_{\in y}$ by definition.
Thus, by Extensionality, $y = \alpha_{\in y}$.

(c) If α is nonempty, then being well-ordered by $\in$, $\exists$ an $\in$-least element $\beta \in \alpha$.
If $\beta \neq \emptyset$, then $\exists \alpha \in \beta$ and by transitivity of α, $\gamma \in \alpha$, contradicting β being $\in$-least in α.

(d) left as homework

Math 318
Lecture 11
September 28 2020

Lemma: Let α, β be ordinals.

(a) If $(\alpha, \in) \cong (\beta, \in)$, i.e. they are order-isomorphic, then $\alpha = \beta$.

(b) $\alpha \in \beta$ or $\alpha = \beta$ or $\beta \in \alpha$, i.e. $\in$ is a total order on all ordinals.

(c) If $\alpha \subsetneq \beta$ then $\alpha \in \beta$

Proof (a) Fix an isomorphism $f : \alpha \to \beta$. Suppose towards a contradiction that $\exists \gamma \in \alpha$ s.t. $\delta \coloneqq f(\gamma) \neq \gamma$.
Let γ be the least such ??.
By the previous lemma, $\gamma = \alpha_{\in \gamma}$ and $\delta = \beta_{\in \delta}$.
But f is an order-isomorphism, $f(\alpha_{\in \gamma} = \beta_{\in \delta}$ but $f(\alpha_{\in \gamma}) = \alpha_{\in \gamma}$ because γ was the least s.t. $f(\gamma) \neq \gamma$. Hence $\gamma = f(\alpha_{\in \gamma}) = B_{\in \gamma} = \alpha_{\in \gamma} = \delta$, so $\delta = \gamma$.

(b) This, by the comparison theorem for well-orders. We have that

$$(\alpha, \in) \prec (\beta, \in) \text{ or } (\alpha, \in) \qquad \cong (\beta, \in) \text{ or } (\beta, \in) \prec (\alpha, \in)$$
$$\Updownarrow$$
$$(\alpha, \in) \cong (\beta', \in) \text{ where } \beta' \text{ is a proper initial segmentof } \beta$$

Hence $\beta' = \beta_{\in\gamma}$. But the previous lemma, $\beta_{\in\gamma} = \gamma$, so $(\alpha, \in) \cong (\gamma, \in)$, thus, by (a), $\alpha = \gamma \in \beta$, so $\alpha \in \beta$

(c) Suppose $\alpha \subsetneq \beta$, in particular, $\alpha \neq \beta$. By part (b), we just need to exclude $\beta \in \alpha$. So suppose towards a contradiction that $\beta \in \alpha$.
Then by transitivity, $\beta \subseteq \alpha \subsetneq \beta$, a contradiction.

In light of this lemma, for ordinals α, β, we write $\alpha < \beta$ and α instead of $\alpha \in \beta$ and $(\alpha, \in)$.

Lemma.

(a) Every nonempty set C of ordinals has an $\in$-least element.
I.e. $\exists \alpha \in C$ s.t. for any other $\alpha' \in C$, $\alpha \in \alpha'$.

(b) More generally, for any formula $\varphi(x)$, if there is an ordinal α s.t. $\varphi(\alpha)$ holds, then there is an $\in$-last ordinal α for which $\varphi(\alpha)$ holds.

(c) Any transitive set of ordinals is an ordinal itself.

Proof (a) If we knew that $C \subseteq \gamma$ for some ordinal γ, then because
gamma is well-ordered by $\in$, we'd know that C has an $\in$-least-element.
But we don't know know this.
Take $\gamma \in C$, so γ is an ordinal.
If γ is $\in$-least in C, we are done.
Suppose it isn't true, i.e. $\exists \delta \overset{<}{\in} \gamma$ and $\delta \in C$. In other words, $\gamma \cap C \neq \emptyset$. But now $\gamma \cap C \subseteq \gamma$, so it has an $\in$-least element $\gamma' \in \gamma \cap C$. Then it's easy to verify (at home) that γ' is also the $\in$-least element of C.

(b) We can't just apply part (a) because $\{x : \varphi(x)\}$ may not be a set.
We know that for some ordinal α, $\varphi(\alpha)$ holds.
If α is the least such ordinal then we're done.
Otherwise the set $\{\gamma \in \alpha : \varphi(\alpha)\}$ is nonempty, hence has an $\in$-least element γ'.
This γ' will be the $\in$-least ordinal satisfying $\varphi(x)$. Finish the details at home.

(c) Let D be a transitive set of ordinals.
By the previous lemma, $\in$ is a total order on D and by part (c) of the current lemma applied to each nonempty subset $C \subseteq D$, $\in$ is a well-order on D.
Hence D is an ordinal.

Definition For any set x, define $S(x) \coloneqq \{x\} \cup x$, the successor of x.
We call an ordinal α a limit ordinal if $\alpha \neq \emptyset$ and α isn't a successor (or some other ordinal) i.e. $\nexists$ an ordinal β s.t. $\alpha = S(\beta)$

Thus, there are three kinds of ordinals: $O \coloneqq \emptyset$, successor, and limit.

Lemma For any ordinal α, $S(\alpha)$ is the least ordinal bigger than α, i.e. $S(\alpha)$ is an ordinal, $\alpha < S(\alpha)$, and $S(\alpha)$ is the least such ordinal.

Proof. Recall that $S(\alpha) \coloneqq \alpha \cup \{\alpha\}$, so is particular $\alpha \subseteq S(\alpha)$ and $\alpha \in S(\alpha)$.
Thus, the fact that α is a transitive set implies that $S(\alpha$ too is a transitive set (fill in the details as to why).
Hence $S(\alpha)$ is a transitive set of ordinals, so it itself is an ordinal.
Nw we let β be an ordinal s.t. $\alpha \overset{\in}{<} \beta$ and show that $S(\alpha \leq \beta$, i.e. either $S(\alpha) = \beta$ or $S(\alpha) \in \beta$.
Because β is transitive and $\alpha \in \beta$, we have $\alpha \subseteq \beta$, so $S(\alpha) \subseteq \beta$.
If $S(\alpha) = \beta$, we are done.
Otherwise, $S(\alpha) \subsetneq B$ so by a previous lemma, $S(\alpha) \overset{\in}{<} \beta$. □

Math 318
Lecture 12
September 30 2020

Lemma: For a set C of ordinals, the least ordinal α s.t.$\alpha \geq \beta \forall \beta \in C$, is denoted by $\sup(C)$ (supremum) and is equal to $\cup C$
Proof. Homework.

Natural numbers and beyond
Recall we defined $0 \coloneqq \emptyset$. We can define $1 \coloneqq S(0) = \{0\}$, $2 \coloneqq S(1) = \{0, 1\}$, $3 \coloneqq S(2) = \{0, 1, 2\}$, ... This gives a definition for each "natural number" separately. But which ordinals should be called natural numbers?

Definition An ordinal α is called a natural number if $\forall \beta \leq \alpha$ (i.e. $\beta = \alpha$ or $\beta \in \alpha$) β is 0 or a successor ordinal.

Observation: If n is a natural number, then $\forall m \overset{\in}{<} n$, m is also a natural number.

To get the set of all natural numbers, we need an ambient set that contains all natural numbers, so we can use the Subset axiom.
We can't take the "set" of all ordinals because this is *not* a set.

Proposition. There is no set that contains all ordinals.

Proof. Suppose there is a set that contains all ordinals, hence by the Subset axiom there is a set O that contains exactly all ordinals and nothing else.
But then O is transitive because if $\alpha \in O$, then all elements of α are also ordinals, so $\alpha \subseteq O$.
Thus, O is transitive set of ordinals, so by an earlier lemma, O is itself an ordinal.
In particular $O \in O$ which contradicts an earlier lemma. □

We need an axiom to give us an "inifinite set".

Definition Call a set I inductive if $\emptyset \in I$ and $\forall x \in I$, $S(x) \in I$

Infinity Axiom. There is an inductive set:

$$\exists x(\emptyset \in x \text{ and } y \in xS(y) \in x)$$

Proposition Every inductive set I contains all natural numbers.

Proof. Suppose this isn't true, then $\exists$ a least natural number n that is not in I. Hence all ordinals $m < n$ mustbe in I.
Note that $n \neq \emptyset$. Thus n is a successor: $\exists m$ s.t. $n = S(m)$. Then $m \in I$, so $S(m) \in I$, but $S(m) = n$, a contradiction. □

The set of natural numbers: Take an inductive set I, and define the set $\mathbb{N} \coloneqq \{n \in I : n \text{ is a natural number } \}$ which exists by the subset axiom.
Another notation for $\mathbb{N}$ is ω, which is used when thinking of $\mathbb{N}$ as an ordinal.
Lemma

(a) ω is an ordinal

(b) ω is an inductive set.

(c) ω is the $\subseteq$-least inductive set.

(d) ω is a limit ordinal and a least such.

Proof (a) ω is a transitive set of ordinals because every natural number contains only natural numbers.
Thus, ω is a transitive set of ordinals, so it is itself an ordinal.

(b) This is because a successor of a natural is a natural number.

(c) This is what the previous proposition says.

(d) Clearly, $\omega \ni \emptyset$, so $\omega \neq \emptyset$.
If ω was a successor, i.e. $\omega = S(\alpha)$, then $\alpha \in \omega$, so α is a natural number, hence $\omega = S(\alpha)$ is also a natural number, so $\omega \in \omega$, a contradiction.
Hence, ω is a limit ordinal.
Also, any limit ordinal α is an inductive (check this!), hence $\omega \subseteq \alpha$ by (c).

$$\underbrace{0, 1, 2, \ldots, \omega}_{S(\omega)}, S(\omega) = \omega \cup \{\omega\}$$

Let's denote, for an ordinal α, $\alpha + 1 \coloneqq S(\alpha)$.

Now we can define more ordinals: $\omega + 4 \coloneqq (((\omega + 1) + 1) + 1) + 1$, which is $0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \omega + 3, \omega + 4$.
In particular, $\omega + 4 > \omega$.

$$\omega + \omega \coloneqq \underbrace{0, 1, 2, \ldots,}_{\omega} \underbrace{\omega, \omega + 1, \omega + 2, \ldots}_{\text{a copy of } \omega}$$

Transfinite induction/recursion. Given an ordinal α, we would like to prove a statement $\varphi(\beta)$ for all $\beta \in \alpha$.
When $\alpha = \omega$, this can be done by ordinary induction. However, if $\alpha > \omega$, we need the following:

Transfinite induction theorem. For any ordinal α and any formula $\varphi(x)$,
if $\forall \beta \in \alpha$, ($\forall \varphi < \beta$, $\varphi(\gamma)$ holds) $\Rightarrow$ $\varphi(\beta)$ holds,
then $\forall \beta \in \alpha$, $\varphi(\beta)$ holds.

Math 318
Lecture 13
October 2 2020

Detour
Theorem (the fundamental theorem of ordinals)
Every well-order is isomorphic to a unique ordinal.

Proof. Let $(A, <_A)$ be a well-order. The uniqueness is because of the statement that if two ordinals are isomorphic (as orders with respect to $\in$), then they are equal.
For existence, consider the set

$$A' \coloneqq \{a \in A : (A_{<_a}, <_A) \text{ is isomorphic to an ordinal}\}.$$

Note that A' is an initial segment of A because if $A_{<_a}$ is isomorphic to an ordinal α and $b < a$ then $A_{<_b}$ is isomorphic to an initial segment of α by the restriction of the isomorphism from $A_{<_a}$ to $A_{<_b}$.
We want to consider

$$B' \coloneqq \{\alpha : \alpha \text{ an ordinal isomorphic to } A_{<_a} \text{ for some } a \in A\}.$$

Why is this a set? What axiom implies that this is a set?
The axiom schema of Replacement (in tandem with the subset axiom) applied to A' with the function formula $a \mapsto$ the unique ordinal α s.t. $A_{<_a}, <_A) \cong (\alpha, \in)$ gives that B' is a set and
$\uparrow_{A'}$
it is immediate to check that $f : A' \to B'$ given by $a \mapsto$ the unique α with $(A_{<_a}, <_A) \cong (\alpha, \in)$ where the order on B' is $\in$.
Moreover, B' is a transitive set of ordinals, so it's itself an ordinal.
It remains to check that $A' = A$.
Suppose not, and let $a \in A$ be the $<_A$-least s.t. $a \notin A'$.
But then taking $\overline{f} \coloneqq f \cup \{(a, B')\}$ is an order isomorphism between $A' \cup \{a\}$ and $S(B')$, so $a \in A'$, a contradiction. □

In light of this, for every well-order $(A, <)$, we define its order type, denoted by $\mathrm{tp}(A, <)$, as the unique ordinal α isomorphic to $(A, <)$.

Examples • Take $A \coloneqq \mathbb{N} \cup \{\infty\}$ where we define $<$ on $\mathbb{N}$ as usual and declare $\infty > n \ \forall n \in \mathbb{N}$.
$(\mathbb{N}, <) = (\omega, \in)$, so $(A, <) \cong \omega + 1$.
$\underbrace{012\ldots\infty}_{A} \cong \omega + 1$. $\mathrm{tp}(A, <) = \omega + 1$

- Def $<_{\underbrace{\mathrm{lex}}_{\text{lexicographical}}}$ on $\mathbb{N} \times \mathbb{N}$ by $(n_0, m_0) <_{\mathrm{lex}} (n_1, m_1)$ if either $n_0 < n_1$ or $n_0 = n_1$ and $m_0 < m_1$.
One can show that $\mathrm{tp}(\mathbb{N} \times \mathbb{N}, <_{\mathrm{lex}}) = \omega^2$, where $\omega^2 \coloneqq \omega \cdot \omega$ and we will define ordinal multiplication below.

Back to transfinite induction/recursion

Transfinite induction theorem. For any ordinal α and any formula $\varphi(x)$,
if $\forall \beta \in \alpha$, $(\forall \varphi < \beta$, $\varphi(\gamma)$ holds) $\Rightarrow \varphi(\beta)$ holds,
then $\forall \beta \in \alpha$, $\varphi(\beta)$ holds.

Proof. Suppose $\exists \beta \in \alpha$ s.t. $\varphi(\beta)$ doesn't hold.
Take the least such β, so $\forall \gamma < \beta$, $\varphi(\gamma)$ holds.
By our hypothesis, $\varphi(\beta)$ must hold as well, a contradiction. □

What is a recursive definition of a function f on an ordinal α?
How do we call a function f defined on $\mathbb{N}$? Sequences! We have recursive definitions of sequence, for example, the Fibonacci sequence:

$$\begin{cases} & f(0) \coloneqq 1 \\ & f(1) \coloneqq 1 \\ n \geq 2, & f(n) \coloneqq f(n-2) + f(n-1). \end{cases}$$

It's intuitively clear that this defines a unique function $f : \mathbb{N} \to \mathbb{N}$. But technically we need to prove this, especially if $\mathbb{N}$ is replaced by an arbitrary ordinal. And that's what the following theorem does.

Definition For sets A, B, a partial function $f : A \to B$ is just a function $f : A' \to B$ where $A' \subseteq A$.

Note that every $f : A \to B$ is a subset $f \subseteq A \times B$, so $f \in \mathcal{P}(A \times B)$, hence the subset axiom gives that there is a set of all partial functions from A to B, which we denote by $\text{Partial}(A, B)$.

Transfinite recursion theorem. For every ordinal κ, for every set A, and function ("the rule of the recursion") $F : \text{Partial}(\kappa, A) \times \kappa \to A$, there is a unique function $f : \kappa \to A$ s.t. $\forall \alpha \in \kappa$, $f(\alpha) = F(f|_\alpha, \alpha)$.

Example For the Fibonacci sequence $\kappa \coloneqq \mathbb{N}(= \omega)$, $A \coloneqq \mathbb{N}$ and $F : \text{Partial}(\mathbb{N}, \mathbb{N}) \times \mathbb{N} \to \mathbb{N}$ is defined as follows:

$$\begin{cases} 1 & \text{if } n = 0 \text{ or } n = 1 \\ p(n-1) + p(n-2) & \text{if } \text{dom}(p) = n \ (= \{0, 1, \ldots, n-1\}) \\ 0 & \text{otherwise} \end{cases}$$

Proof-sketch. Same technique as before: put together all functions defined on the initial segments of κ and satisfy the definition.
The uniqueness gives that these functions cohere, so we can take their union and this would be the desired function f defined on all of κ.

Math 318
Lecture 14
October 5 2020

Definition For ordinals α, β, we define $\alpha + \beta$ and $\alpha \cdot \beta$ by transfinite recursion as follows:

$$\alpha + \beta \coloneqq \begin{cases} \alpha & \text{if } \beta \coloneqq 0 \\ (\alpha + \beta') + 1 & \text{if } \beta \coloneqq \beta' + 1 \\ \sup\limits_{\gamma < \beta} \ \alpha + \gamma & \text{if } \beta \text{ is a limit ordinal} \end{cases}$$

Recall: for a set C of ordinals, sub$C$ is the least ordinal $\supseteq$ every ordinal in C.

$$\alpha \cdot \beta \coloneqq \begin{cases} 0 & \text{if } \beta \coloneqq 0 \\ \alpha \cdot \beta' + \alpha & \text{if } \beta \coloneqq \beta' + 1 \\ \sup\limits_{\gamma < \beta} \ \alpha \cdot \gamma & \text{if } \beta \text{ is a limit} \end{cases}$$

Proposition The ordinal addition and multiplication are associative: $\forall \alpha, \beta, \gamma$ ordinals,

(a) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$

(b) $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$

Proof. (a) We prove by transfinite induction on γ.
Suppose $\forall \gamma' < \gamma$, we know that $\alpha + (\beta + \gamma') = \alpha + (\beta + \gamma')$.

By definition, $(\alpha+\beta)+\gamma = ((\alpha+\beta)+\gamma')+1$, if $\gamma = \gamma'+1$.
Then

$$\begin{aligned}(\alpha+\beta)+\gamma &= ((\alpha+\beta)+\gamma')+1 \\ &= (\alpha+(\beta+\gamma'))+1 && \text{induction hypothesis} \\ &= \alpha+((\beta+\gamma')+1) && \text{definition} \\ &= \alpha+(\beta+\gamma) && \text{definition}\end{aligned}$$

Now suppose γ is a limit.

$$\begin{aligned}(\alpha+\beta)+\gamma &= \sup_{\gamma'<\gamma} (\alpha+\beta)+\gamma' && \text{By definition} \\ &= \sup_{\gamma'<\gamma} \ \gamma+(\beta+\gamma') && \text{induction} \\ &= \alpha+\sup_{\gamma'<\gamma} \ \beta+\gamma' && \text{easy to show} \\ &= \alpha+(\beta+\gamma) && \text{definition}\end{aligned}$$

□

Proof. (b) Similar argument □

Examples
- $1+7=8$
- $1+\omega=\omega$ $\qquad 1+\omega := \sup_{n<\omega} 1+n = \sup_{n<\omega} n = \omega$
- $29+\omega=\omega$
- $\underbrace{\omega+1}_{:=\omega\cup\{\omega\}} \neq \omega$ (why? ω is a limit ordinal and $\omega+1$ is a successor).
- $\omega\cdot 2 \neq \omega$ (because it contains a limit ordinal, namely ω) (I.e. $\omega \in \omega\cdot 2$)
- $2\cdot\omega := \sup_{n<\omega} 2\cdot n = \omega$.

Warning As the examples above show, ordinal $+$ and $\cdot$ are *not* commutative.

$$\omega+1 > 1+\omega \text{ and } \omega\cdot 2 > 2\cdot\omega.$$

Equinumerosity

Definition Sets A and B are said to be equinnumerous if there is a bijection between them.
(i.e. if and only if)

We denote this by $A \cong B$.

Examples
- $\underbrace{\mathbb{N}}_{:=\{0,1,2,\ldots\}} \cong \underbrace{\mathbb{N}^+}_{:=\{1,2,3,\ldots\}}$ even though $\mathbb{N}^+ \subsetneq \mathbb{N}$ $\qquad$ A bijection is $n \mapsto n+1$.
- $\mathbb{Z} \cong \mathbb{N}$
- $\mathbb{N}^2 \cong \mathbb{N}$
  HW: find an explicit definition for this bijection $(n,m) \mapsto k$, find what k is.

Math 318
Lecture 15
October 7 2020

- $\mathbb{N}^2 \cong \mathbb{N}$
  How many elements are on the n^{th} diagonal? $n+1$.
  - 0: $(0,0)$
  - 1: $(0,1)$, $(1,0)$
  - 2: $(0,2)$, $(1,1)$, $(2,0)$
  - 3: ...

  (n,m) sits on the diagonal $n+m$.
  There are $n+m$ diagonals before it containing in total $1+2+3+\ldots+(n+m-1+1) = \sum_{i=1}^{n+m} i = \frac{(n+m)(n+m+1)}{2}$

  We need to add the elements on the diagonal $n+m$ that come before (n,m): there are $m-1$ many.
  Thus the $\#(n,m) = \frac{(n+m)(n+m+1)}{2} + m$

  Thus $f : \mathbb{N}^2 \to \mathbb{N}$, $(n,m) \mapsto \frac{(n+m)(n+m+1)}{2} + m$ is a bijection.
- $(0,1) \cong (-2,3)$
  Linear mapping $0 \mapsto -2 \quad 1 \mapsto 3$
- $(0,1) \cong \mathbb{R}$
  Can be done using arctan, or $\frac{1}{1+e^x}$, ?? or some rational function (google it)
- $(0,1) \cong (0,1]$
  find a Hilbert hotel in $(0,1]$ and use it to accommodate 1.

Recall
Lemma If $f : A \to B$ is injective, then it has a left-inverse $g : B \to A$ which is necessarily surjective.

Proof. Fix $a_0 \in A$ and define $g : B \to A$ by

$$g(b) \coloneqq \begin{cases} \text{the unique } a \text{ s.t. } f(a) = b & \text{if } b \in f(A) \\ a_0 & \text{otherwise} \end{cases}$$

□

Notation For sets A, B, we write

- $A \hookrightarrow B$ if $\exists$ an injection $f : A \to B$
- $A \twoheadrightarrow B$ if $\exists$ a surjection $f : A \to B$

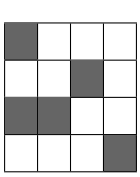
The following is what started set theory:

Theorem (Cantor) let A be a set.

1. $A \not\twoheadrightarrow \mathcal{P}(A)$.
2. $\mathcal{P}(A) \not\hookrightarrow A$.

Proof. (b) Follows from (a) by the previous lemma. □

Proof. (a) This Cantor's famous diagonalization (or rather, antidiagonalization) argument. First intuition. If I gave you a table and asked you to produce a column that doesn't appear as a column in the table.



diagonal

antidiagonal

Actual Proof Suppose there is a surjection $f : A \to \mathcal{P}(A)$.
$A_f \coloneqq \{a \in A : a \notin f(a)\}$
Picture it as a table: we shade an entry (a, b) if $b \in f(a) \subseteq A$. $f(a_3) = \{a_1, a_4, a_5\}$.
Claim: $A_f \notin f(A)$.
Proof: Otherwise $\exists a \in A$, $f(a) = A_f$.
$a \in A_f \underset{\text{def of } A_f}{\Leftrightarrow} a \notin f(a) = A_f$. a contradiction □

Theorem (Cantor - Schröder - Bernstein)
For sets A, B, if $A \hookrightarrow B$ and $B \hookrightarrow A$, then $A \cong B$.

Before proving this in general, let's consider an example

$$f : \mathbb{N}_0 \to \mathbb{N}_1, \quad n \mapsto (n+1)'$$

$$g : \mathbb{N}_1 \to \mathbb{N}_0, \quad n' \mapsto n+1$$

We look at pairs: missing diagram. Do the same for other pairs.

Math 318
Lecture 16
October 9 2020

Theorem (Cantor - Schröder - Bernstein)
For sets A, B, if $A \hookrightarrow B$ and $B \hookrightarrow A$, then $A \cong B$.

Before proving this in general, let's consider an example

- $A \coloneqq \omega + 1 = \mathbb{N} \cup \{\omega\}$
- $B \coloneqq (\omega + 1)' \coloneqq \{0', 1', 2', \ldots\} \cup \{\omega'\}$.
- $f : A \to B, \quad \omega \mapsto \omega', \quad n \mapsto (n+1)'$
- $g : B \to A, \quad \omega' \mapsto \omega, \quad n' \mapsto n+1$

Using f and g, we obtain a bijection $h : A \to B$ by taking

$$\alpha \begin{cases} f(\alpha) = g^{-1}(\alpha) & \text{if } \alpha = \omega \\ f(\alpha) & \text{if } \alpha \in \mathbb{N} \text{ is even} \\ g^{-1}(\alpha) & \text{if } \alpha \in \mathbb{N} \text{ is odd} \end{cases}$$

Proof. Proof of general case. Let $f : A \hookrightarrow B$ and $g : B \hookrightarrow A$ be injections. We will obtain partitions $A = \bigcup_{n\in\aleph} A_n \cup A_\infty$ and $B = \bigcup_{n\in\aleph} B_n \cup B_\infty$ such that

- $f(A_\infty = B_\infty$ and $g(B_\infty = A_\infty$.
- $f(A_n) = B_{n+1}$ and $g(B_n) = A_{n+1}$. $\quad n \in \mathbb{N}$

We then will define $h : A \to B$ as before:

$$\alpha \begin{cases} f(\alpha) = g^{-1}(\alpha) & \text{if } a \in A_\infty \\ f(\alpha) & \text{if } a \in A_{2k} \text{ for some } k \in \mathbb{N} \\ g^{-1}(\alpha) & \text{if } a \in A_{2k+1} \text{ for some } k \in \mathbb{N} \end{cases}$$

It's immediate to check that this is a bijection.
It remains to obtain these partitions and we do so by obtaining nested sets:

- $A \coloneqq \overline{A_0} \supseteq \overline{A_1} \supseteq \overline{A_2} \ldots$
- $B \coloneqq \overline{B_0} \supseteq \overline{B_1} \supseteq \overline{B_2} \ldots$

then

- $A_n \coloneqq \overline{A_n} \setminus \overline{A_{n+1}}$
- $B_n \coloneqq \overline{B_n} \setminus \overline{B_{n+1}}$
- $A_\infty \coloneqq \bigcap_{n\in\mathbb{N}} \overline{A_n}$
- $B_\infty \coloneqq \bigcap_{n\in\mathbb{N}} \overline{B_n}$

We need these $\overline{A_n}$ and $\overline{B_n}$ to satisfy the following:

$$(*) \quad \begin{matrix} f(\overline{A_n}) = \overline{B_{n+1}} \\ g(\overline{B_n}) = \overline{A_{n+1}} \end{matrix} \ \forall n \in \mathbb{N} \text{ If we find such nested sets, we're done}$$

We define these sets by recursion on $n \in \mathbb{N}$

$$\begin{cases} \overline{A_0} \coloneqq A & \overline{A_{n+1}} \coloneqq g(\overline{B_n}) \\ \overline{B_0} \coloneqq B & \overline{B_{n+1}} \coloneqq f(\overline{A_n}) \end{cases} \text{ After this, we obtain the partitions}$$

$A = \bigcup_{n\in\mathbb{N}} A_n \cup A_\infty$ and $B = \bigcup_{n\in\mathbb{N}} B_n \cup B_\infty$ as above and we check that these are as desired,
i.e. $f(A_n) = B_{n+1}, \quad f(A_\infty) = B_\infty, \quad g(B_\infty) = A_\infty$.

Recall/learn that if a function $j : X \to Y$ is injective and $X_0, X_1 \subseteq X_j$, then $j(X_1 \setminus X_0) = j(X_1) \setminus j(X_0)$, which happens only due to injectivity.
So we check

$$f(A_n) \underset{\text{def}}{=} f(\overline{A_n} \setminus \overline{A_{n+1}}) \underset{\text{injectivity}}{=} f(\overline{A_n}) \setminus f(\overline{A_{n+1}}) \underset{\text{by (*)}}{=} \overline{B_{n+1}} \setminus \overline{B_{n+2}} \underset{\text{def}}{=} B_{n+1}$$

$$g(B_n) = \ldots \text{ similar } \ldots = A_{n+1}$$

$$
\begin{aligned}
f(A_\infty) &= f\left(\bigcap_{n\in\mathbb{N}} \overline{A_n}\right) && \text{definition}\\
&= \bigcap_{n\in\mathbb{N}} f(\overline{A_n}) && \text{injectivity}\\
&= \bigcap_{n\in\mathbb{N}} \overline{B_{n+1}} && \text{by (*)}\\
&= \bigcap_{n\in\mathbb{N}} \overline{B_n} && \text{because } \overline{B_0} \supseteq \overline{B_n}\ \forall n \in \mathbb{N}\\
&= B_\infty && \text{def}
\end{aligned}
$$

$$g(B_\infty) = \ldots = A_\infty$$

□

Proposition $\mathbb{Q} \cong \mathbb{N}$.

Proof. Recall $\mathbb{Q} \coloneqq {}^{\mathbb{Z}\times\mathbb{N}^+}/_{\equiv}$ by some equivalence relation $\equiv$ on $\mathbb{Z} \times \mathbb{N}^+$.
$\mathbb{Q} \hookrightarrow \mathbb{Z} \times \mathbb{N}^+$
$q \mapsto (n, m)$, where $\frac{n}{m}$ is reduced form of q.
$g : \mathbb{Z} \times \mathbb{N}^+ \hookrightarrow \mathbb{N} \times \mathbb{N}^+$, $(z, n) \mapsto (j(z), n)$ where $j : \mathbb{Z} \overset{\text{bij}}{\to} \mathbb{N}$
$h : \mathbb{N} \times \mathbb{N}^+ \hookrightarrow \mathbb{N}$ defined last time.
Then $h \circ g \circ f : \mathbb{Q} \hookrightarrow \mathbb{N}$ and obviously identity : $\mathbb{N} \hookrightarrow \mathbb{Q}$,
so by Cantor - Schröder - Bernstein, $\mathbb{Q} \cong \mathbb{N}$. □

Definition A set A is said to be countable if A is equinumerous with an ordinal $\alpha \leq \omega$ (so either a natural number or ω).

Math 318
Lecture 17
October 14 2020

Definition A set is equinumerous with a natural number.
Otherwise, the set is called infinite.

Definition A set A is Dedekind infinite if it is equinumerous with a proper subset of itself, i.e. $\exists A' \subsetneq A$ s.t. $A \cong A'$.
Otherwise, is Dedekind finite.

Proposition (The Pigeonhole Principle) Finite sets are Dedekind finite.

Proof. Let A be finite, i.e. $A \cong n$ for some $n \in \mathbb{N}$.
Without loss of generality, it is enough to prove the statement for n instead of A.
We do by induction on n.
Base $n = 0$. Vacuously true since $\emptyset$ doesn't have proper subsets.
Step $n \Rightarrow n + 1$. Suppose n is Dedekind finite. To show that $n + 1$ is Dedekind finite, suppose that $f : n + 1 \hookrightarrow n + 1$ is an injection and show that it is also a surjection.

Unambiguous new notatio for f-image: For a function $f : X \to Y$ and $A \subseteq X$, we used to denote by $f(A)$ the set $\{f(a) : a \in A\}$,
But when A is also an element of X, i,e, $A \in X$, this is ambiguous, so for the image set, we'll write $f''(A) \coloneqq \{f(a) : a \in A\}$.

Case 1: $f''(n) \subseteq n$. Then applying induction to $f|_n$, hence $f|_n : n \to n$ is injective, we get that $f|_n$ is also surjective, i.e. $f''(n) = n$.
Then $f(n) \notin n$ because f is injective, hence $f(n)$ must be n. Thus, f is also surjective.

Case 2: $f''(n) \not\subseteq n$. Thus $n \in f''(n)$, i.e. $\exists k \in n$ s.t. $f(k) = n$.
Here, $f(n) \in n$, put $m \coloneqq f(n)$.
Let g be the same as f but $g(n) \coloneqq n$ and $g(k) \coloneqq m$.

$$n \mapsto n \quad k \mapsto m$$

Then $g : n+1 \to n+1$ is an injection and it satisfies Case 1, so it is surjective.
But $f''(n+1) = g''(n+1) = n+1$, so f too is surjective. □

Another notion for a set A to be infinite is $\omega \hookrightarrow A$.

Proposition A set A is Dedekind infinite $\Leftrightarrow \omega \hookrightarrow A$.

Proof. $\Leftarrow$ Suppose $h : \omega \hookrightarrow A$ is an injection.
Then using the h-image of ω as a Hilbert hotel, define $f : A \to A$ by

$$f(a) \coloneqq \begin{cases} h(n+1) & \text{if } a = h(n) \text{ for some } n \in \mathbb{N} \\ a & \text{otherwise} \end{cases}$$

It's clear that f is injective and $f''(A) = A \setminus \{h(0)\}$.
Thus, f witnesses that A is Dedekind infinite.

$\Rightarrow$ Suppose A is Dedekind infinite, so $\exists\ f : A \hookrightarrow A$ s.t. $f''(A) \subsetneq A$.
Let $a \in A \setminus f''(A)$.
Define $h : \omega \to A$ by $n \mapsto f^n(a)$ where

$$f^0(a) \coloneqq a \quad f^{n+1}(a) \coloneqq f(f^n(a)).$$

It's easy to check that h is an injection.

□

Yet another notion of infinite for a set A is $A \underbrace{\twoheadrightarrow}_{\exists \text{ surjection}} \omega$

Theorem The following are equivalent for a set A:

1. A is infinite, i.e. $\nexists n \in \mathbb{N}$ s.t. $A \cong n$.
2. A is Dedekind infinite.
3. $\omega \hookrightarrow A$.
4. $A \twoheadrightarrow \omega$.

What we have shown already: (2) $\Rightarrow$ (1), (2) $\Leftrightarrow$ (3), (3) $\Rightarrow$ (4) (which is true for any sets)..

Math 318
Lecture 18
October 16 2020

Theorem The following are equivalent for a set A:

1. A is infinite, i.e. $\nexists n \in \mathbb{N}$ s.t. $A \cong n$.

2. A is Dedekind infinite.

3. $\omega \hookrightarrow A$.

4. $A \twoheadrightarrow \omega$.

What we have shown already: (2) $\Rightarrow$ (1), (2) $\Leftrightarrow$ (3), (3) $\Rightarrow$ (4) (which is true for any sets). We still need to show (1) $\Rightarrow$ (3) and (4) $\rightarrow$ (3).

(4) $\Rightarrow$ (3): More generally, if $f : X \twoheadrightarrow Y$, then it has a right-inverse $g : Y \to X$ (which is necessarily injective), so $X \twoheadrightarrow Y \Rightarrow Y \hookrightarrow X$.

Proof.

$$f : X \twoheadrightarrow Y \qquad g : Y \hookrightarrow X$$

$g : Y \to X$ is a right-inverse $\Leftrightarrow \forall y \in Y$, $g(y) \in f^{-1}(\{y\})$.
Well why not define $g : Y \to X$ by $y \mapsto$ some point in $f^{-1}(\{y\})$
To make this definition rigorous, we need a function that would make all choices (for all $y \in Y$) at once.
This function is given by the Axiom of Choice...
Applying the Axiom of Choice to the set $C \coloneqq \{f^{-1}(\{y\}) : y \in Y\}$ (why is this a set?) we get a choice function $h : C \to X$, i.e. $\forall P \in C$, $h(P) \in P$.
Then define $g : Y \to X$ by $g(y) \coloneqq h(f^{-1}(\{y\})) \in f^{-1}(\{y\})$, so g is a right-inverse of f. □

Axiomn of Choice Given a set C of nonempty sets, $\exists$ a function $f : C \to \cup C$ such that $\forall b \in C$, $f(b) \in b$.

Remark If C is finite, the conclusion is true without this axiom (just write a formula that makes the choices), but when C is infinite, the conclusion doesn't follow from ZF.

(1) $\Rightarrow$ (3):

Proof. Let A be infinite, i.e. $A \ncong n$ $\forall n \in \mathbb{N}$.
Want: $\omega \hookrightarrow A$.
Let's attempt to do this intuitively.

0. $A \neq \emptyset$ because then $A \cong 0$. Hence $\exists a_0 \in A$

1. $A \setminus \{a_0\} \neq \emptyset$ because then $A \cong 1$. Hence $\exists a_1 \in A \setminus \{a_0\}$

2. $A \setminus \{a_0, a_1\} \neq \emptyset$ because then $A \cong 2$. Hence $\exists a_0 \in A \setminus \{a_0, a_1\}$

$\vdots$

get a function $f : \omega \hookrightarrow A$, $n \mapsto a_n$.

Using the Axiom of Choice, get a choice function $h : \mathcal{P}(A) \setminus \{\emptyset\} \to A$,
i.e. $\forall A' \in \mathcal{P}(A) \setminus \{\emptyset\}$, $h(A') \in A'$. Fix $a \in A$.

Formally, we define $f : \omega \to A$ by recursion

$$f(n) \coloneqq \begin{cases} h(A \setminus f''(n)) & \text{if } A \setminus f''(n)) \neq \emptyset \\ a & \text{otherwise} \end{cases}$$

where we recall that $f''(n) \coloneqq \{f(i) : i \in n\} = \{f(0), f(1), \ldots, f(n-1)\}$.
Using that A isn't finite, easy induction on n shows that $\forall n \in \omega$, $A \setminus f''(n) \neq \emptyset$. Hence f is an injection. □

Cardinals and cardinality. Cardinals are ordinals that we use to "measure" the size of a set.

Definition: A cardinal κ is an ordinal s.t. $\kappa \ncong \alpha \ \forall \alpha < \kappa$.

Examples
- Each $n \in \omega$ is a cardinal.
  Proof. By the Pigeonhole Principle.
- ω is a cardinal.
  Proof. If $f : \omega \to n$ is a bijection where $n \in \omega$,
  then $f|_{n+1} : n+1 \hookrightarrow n$, contradiction the PHP.
- $\omega + 1$ isn't a cardinal, in fact, $\omega + 1 \cong \omega$.
  Proof. $\omega + 1 : 0\searrow\ 1\searrow\ 2\searrow\ \dots\ {}_{0}\swarrow\omega$ $\quad f(n) \coloneqq n+1 \forall n \in \omega$
  $\omega : 0 \quad 1 \quad 2 \quad \dots$ $\quad f(\omega) \coloneqq 0$

Definition: For a cardinal κ and a set A, we say that A has cardinality κ if $A \cong \kappa$.
We denote this by $|A| = \kappa$.

Question: Does every set have a cardinality?

Math 318
Lecture 19
October 19 2020

Definition: For a cardinal κ and a set A, we say that A has cardinality κ if $A \cong \kappa$.
We denote this by $|A| = \kappa$.

Question: Does every set have a cardinality?

Answer Yes if we assume the Axiom of Choice. In fact, it's equivalent to AC.

Proposition A set A has cardinality if and only if it can be well-ordered.
i.e. $\exists$ a well-ordering $-$ on A.

Proof. $\Rightarrow$. Suppose $f : A \to \kappa$ is a bijection, where κ is some cardinal.
Then we can copy the well-order of κ onto A via f,
i.e. define $<$ on A by: $a < b :\Leftrightarrow f(a) \in f(b) \ \forall a, b \in A$.
$<$ on A is a well-ordering because f is order-preserving by definition.
$\Leftarrow$. Let $<$ be a well-order on A, then $(A, <)$ is order-isomorphic to an ordinal $(\alpha, \in)$.
Let κ be the least ordinal equinumerous with α (in particular $\kappa \leq \alpha$).
Then κ is a cardinal, by definition, and $A \cong \alpha \ cong\kappa$. □

Now the question above translates to whether every set can be well-ordered.
Think about $\mathbb{R}$. The standard order on $\mathbb{R}$ is not a well-order, e.g. $\{\frac{1}{n} : n \in \mathbb{N}\}$ doesn't have a least element, is there a well-order of $\mathbb{R}$?

Zermelo's theorem (depends on AC). Every set can be well-ordered.

Definition. For a partial order $(A, \leq)$, we call a subset $C \subseteq A$ a chain if $\leq|_C$ is total,
(restriction)
i.e. any two elements of C are $\leq$-comparable.
For a set $B \subseteq A$, an element $a \in A$ is called an upper bound of B if $\forall b \in B$, $b \leq a$.

We say that $(A, \leq)$ has the chain property if every chain in A has an upper bound. note $\emptyset$ has the chain property)
Note. If an upper bound a of B is itself $\in B$, then a is a maximum element of B.

Zorn's lemma (depends on AC). Every partial order with the chain property has a maximal element.

Caution. Maximal means there is nothing above it, not that it is above everyone.

We will sketch that AC and the last two statements are equivalent.
But first, let's discuss a technique of showing that something is "too big" to be a set.
Recall that there is no set of all ordinals.
We expressed this by saying that all ordinals form a proper class.

Proposition For any set A, there is no formula $\varphi(x, y)$ s.t. for each ordinal α, there is a unique element $a \in A$ s.t. $\varphi(\alpha, a)$ holds and this correspondence $\alpha \mapsto a$ is one-to-one.

Proof. Otherwise, by Subset Axiom, $A' \coloneqq \{a \in A : \exists \text{ an ordinal } \alpha \text{ with } \varphi(\alpha, a)\}$ is a set.
We apply Replacement to $\varphi'(x, y) \coloneqq \varphi(y, x)$ and A', to get that there is a set of all ordinals, which is a contradiction. □

Theorem (in ZF) The following are equivalent.

1. Axiom of Choice
2. Zorn's lemma
3. Zermelo's theorem.

Proof. Proof sketch. (3) $\Rightarrow$ (1). Assume that every set admits a well-ordering.
Let C be a set of nonempty set and need to prove it admits a choice function, i.e. $\exists f : C \to \cup C$ s.t. $\forall A \in C$, $f(A) \in A$.

Caution. It may be tempting to say let's well-ordr each $A \in C$ and then take the least element in A with respect to that well-ordering. But this itself uses AC because for each A we would be *choosing* a well-ordering.

Instead, we let $<$ be a well-ordering of $\cup C$ and define $f : C \to \cup C$ by $A \mapsto$ the $<$-least element of A. □

Math 318
Lecture 20
October 21 2020

Theorem (in ZF) The following are equivalent.

1. Axiom of Choice
2. Zorn's lemma
3. Zermelo's theorem.

Proof. (3) $\Rightarrow$ (1). Done last time □

Proof. (1) $\Rightarrow$ (2). Recall Zorn's lemma: Every nonempty partial order with hthe chain property has a maximal element.
Fix such a partial order $(A, \leq)$.
Intuition: Take any $a_0 \in A$. If a_0 is maximal, we're done.
If not, then $\exists a_1 \in A$ s.t. $a_1 > a_0$.
Is a_1 maximal? If yes, we're done. If not $\exists a_2 > a_1 \ldots \exists A_\omega > a_n \ \forall n \in \mathbb{N}$ by the chain condition.
If a_w is maximal, we're done. If not $\exists a_{\omega+1} > a_\omega$.
The Axiom of Choice is used to make the choices of a_α at once.
Rigourously, assuming towards a contradiction that there is no maximal element, we build an injection of Ordinals into A by transfinite recursion (as in the intuitive argument), which contradicts A being a set (see Q9 of Basic Set Theory notes). $\square$

Proof. (2) $\Rightarrow$ (3). We fix a set X and need to show that it admits a well-ordering.
The idea is to consider the $\subseteq$-maximal subset $X' \subseteq X$ that admits a well-ordering.
Then, X' must be equal to X since otherwise we'd take any $x \in X \setminus X'$, declare it $>$ than every element of X', so $X' \cup \{x\}$ would still be a well-ordering, contradicting the $\subseteq$-maximality of X'.
But how do we obtain such a maximal X'? To apply Zorn's lemma, we would need the chain to hold for the partial order $\subseteq$ on the set A of all subsets of X that admit a well-ordering.
But unfortunately this partial order $(A, \subseteq)$ doesn't satisfy the chain property : $\exists X_0 \subseteq X_1 \subseteq X_2 \subseteq \ldots \subseteq X$ each admitting its own well-ordering $<_{X_i}$. There is no guarantee that $\bigcup_{i \in \kappa} X_i$ will admit a well-ordering because these $<_{X_i}$ may not cohere.
Instead of A, we will consider the set A' of all well-orders $(Y, <_Y)$ where $Y \subseteq X$ and we will equip A' with the order α (being an initial segment).
Then it is not hard to check that (A', α) satisfies the chain condition.
So Zorn's applies and yields a α-maximal $(X', <)$, and by the argument above, $X' = X$. $\square$

Uncountable sets and the Continuum Hypothesis.
Cantor's theorem gives that $\mathcal{P}(\mathbb{N})$ is uncountable.
In particular, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ and $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$ and in fact $\mathcal{P}^\alpha(\mathbb{N})$ are bigger and bigger sets.
What other down-to-earth sets are uncountable?
In the midterm practice, we saw that $\mathbb{P}(\mathbb{N}) \cong 2^{\mathbb{N}}$, $A \mapsto \mathbb{1}_A$ indicator function.
We've also seen that $\mathbb{R} \cong (0, 1)$.

Proposition $\mathbb{R} \cong (0, 1) \cong [0, 1] \cong 2^{\mathbb{N}} \cong \mathcal{P}(\mathbb{N})$.

Proof. It remains to show $[0, 1] \cong 2^{\mathbb{N}}$, and one way to do this is by CSB:
For $[0, 1] \hookrightarrow 2^{\mathbb{N}}$, it is enough to show that $2^{\mathbb{N}} \twoheadrightarrow [0, 1]$ and we define this map by treating a binary sequence $x \in 2^{\mathbb{N}}$ as a binary representation of a real.
This map is not quite injective because

$$\text{same real } \begin{cases} a_0 a_1 a_2 \ldots \underbrace{a_n}_{\neq 0} 0000 \ldots \\ a_0 a_1 a_2 \ldots a_{n-1}(a_n - 1)1111 \ldots \end{cases}$$

for $2^{\mathbb{N}} \hookrightarrow [0, 1]$, we map every $\underbrace{x}_{=(x_n)} \in 2^{\mathbb{N}} \mapsto \underbrace{0.x'_0 x'_1 x'_2 \ldots}_{\substack{\text{treating as base-3} \\ \text{rep. of a real.}}}$, where

$$x'_n := \begin{cases} 0 & \text{if } x_n = 0 \\ 2 & \text{if } x_n = 1. \end{cases}$$

This is injective and the image of this map is called a Cantor set.
This shows that $\mathbb{R}$ has the same cardinality c of $\mathcal{P}(\mathbb{N}$, which is called continuum. $\square$

Proof. **Direct proof that $\mathbb{R}$ is uncountable**. It's enough to show that no function $\mathbb{N} \to (0,1)$ is surjective.
To this end, let $f : \mathbb{N} \to (0,1)$, i.e. f is a sequence of reals.
Consider the decimal representation of these reals:

$$f(0) : 0.\boxed{a_0^0}a_1^0a_2^0\dots$$
$$f(1) : 0.a_0^1\boxed{a_1^1}a_2^1\dots$$
$$f(0) : 0.a_0^2a_1^2\boxed{a_2^2}\dots$$

By diagonalization, we obtain a new real $b \coloneqq 0.b_0b_1b_2\dots$, where each $b_n \coloneqq \begin{cases} 2 & \text{if } a_n^n \neq 2 \\ 3 & \text{if } a_n^n = 2 \end{cases}$, so $b_n \neq a_n^n \forall n \in \mathbb{N}$
As before, it's clear that $b \neq f(n) \forall n \in \mathbb{N}$, a contradiction. □

Math 318
Lecture 21
October 23 2020

Question Is there a set $A \subseteq \mathbb{R}$ s.t. $|\mathbb{N}| < |A| < |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$?

Answer. The anser is independent from ZFC, i.e. from just the axioms of ZFC, we cannot prove the positive answer, neither can we prove the negative answer.

Continuum Hypothesis. There is no set $A \subseteq \mathbb{R}$ s.t. $|\mathbb{N}| < |A| < |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$.

- Gödel 1940. The Continuum Hypothesis (CH) is consistent with ZFC, i.e. if ZFC is consistent ($\Leftrightarrow$ has a model), then so is ZFC+CH ($\Leftrightarrow$ has a model).
- Cohen 1963. The $\neg$CH is consistent with ZFC, i.e. if ZFC is consistent, then so is ZFC + $\neg$CH ($\Leftrightarrow$ has a model).
  To do this, Cohen invented a method of adding "imaginary" sets to a given model of ZFC, called forcing (because we "force" a new element into our model).

Foundation Axiom. The $\ni$ relation on all sets is well-founded, i.e.

$$\forall C \exists x (x \text{ is } \ni\text{-minimal in } C)$$
$$\Leftrightarrow \forall C \exists x (\nexists y \in C \quad y \in x)$$
$$\Leftrightarrow \forall C \exists x (x \cap C = \emptyset)$$

Remark. This x doesn't have to be unique
Proposition (AC) Foundation Axiom $\Leftrightarrow$ there is no $\ni$-decreasing sequence (x_n) of sets, i.e. $\nexists$ sequence (x_n) with $x_n \ni x_{n+1}$ $\forall n \in \mathbb{N}$.

Proof. ($\Rightarrow$) We prove the contrapositive: Let (x_n) be an $\ni$-decreasing sequence if $\exists f : \mathbb{N} \to Y$ s.t. $f(n) =: x_n$.
Let $X \coloneqq f[\mathbb{N}]$, i.e. $X = \{x_n : n \in \mathbb{N}\}$. Then X doesn't have an $\in$-minimal element, indeed, for any $x \in X$, $x = x_n$ for some $n \in \mathbb{N}$, so $x_{n+1} \in x_n$, hence x_n isn't $\in$-minimal

($\Leftarrow$) (AC). We prove the contrapositive: suppose Foundation fails, i.e. $\exists C$ s.t. $\forall x \in C$ $\exists y \in C$ s.t. $y \in x$.

Intuitively, $C \neq \emptyset$, so $\exists x_0 \in C$
Then $\exists x_1 \in C$ and $x_1 \in x_0$.
Then $\exists x_2 \in C$ and $x_2 \in x_1$, ...
The choices of x_n all at once are made by the Axiom of Choice and the construction of (x_n) has to be done by recursion:
Fix a choice function $c : \mathcal{P}(C) \setminus \{\emptyset\} \to C$ s.t. $\forall A \subseteq C$, $c(A) \in A$.
Define $f : \mathbb{N} \to C$ by recursion:

$$\underbrace{f(n)}_{=x_n} \coloneqq \begin{cases} c(\underbrace{f(n-1)}_{=x_{n-1}} \cap C & \text{if } f(n-1) \cap C \neq \emptyset \\ c(C) & \text{otherwise} \end{cases}$$

This gives a sequence $f(n)\, \inf(n-1) \forall n \in \mathbb{N}$. □

Corollary. Foundation $\Rightarrow \forall x (x \notin x)$.

Proof. Otherwise, if $\exists x$ s.t. $x \in x$, then $C \coloneqq \{x\}$ has no $\in$-minimal element. □

We define a hierarchy of sets by transfinite recursion as follows:
For every ordinal α, we define

$$V_\alpha \coloneqq \begin{cases} \emptyset & \text{if} \alpha = \emptyset \\ \mathcal{P}(V_\beta) & \text{if } \alpha = \beta + 1 \\ \bigcup\limits_{\beta < \alpha} V_\beta & \text{if } \alpha \text{ is a limit} \end{cases}$$

If we take $\bigcup\limits_{\beta \text{ ord.}} V_\alpha$, is this all of the sets, i.e. is it true that $\forall x\ \exists \alpha\ (x \in V_\alpha)$?

Proposition Foundation $\Leftrightarrow \forall x\ \exists \alpha\ (x \in V_\alpha$, i.e. $\bigcup\limits_{\alpha \text{ ord}} = \{x : x = x\}$.

Proof. Not hard, left for homework. □

So, with Foundation, the universe of sets looks like (missing diagram).
This is why the universe of sets is often denoted by V.

Classes. Given a formula $\varphi(x)$, we think of $\{x : \varphi(x)\}$, intuitively, the class of all sets satisfying φ. We say that $\{x : \varphi(x)\}$ is a set if $\exists$ a set Y s.t. $Y = \{x : \varphi(x)\}$, i.e.

$$\forall x (\varphi(x) \Leftrightarrow x \in Y)$$

Otherwise, we say that $\{x : \varphi(x)\}$ is a proper class.

Note. Every set Y is itself a class by taking $\varphi(x) \coloneqq x \in Y$

Examples of proper classes.

- Russell's class $\{x : x \notin x\}$
- Class of all sets $\{x : x = x\}$
- Class of all ordinals $\{\alpha : \alpha \text{ is an ordinal}\}$.

Math 318
Lecture 22
October 26 2020

Corollary. There exists uncountable cardinals.

Proof. (AC). By AC, $|\mathcal{P}(\mathbb{N})|$ exists and is uncountable by Cantor's theorem. □

Proof. (without AC). This is called Hartog's theorem, proven in the notes. □

Notation for cardinals. When we would like to emphasize the order structure of $\mathbb{N}$, we write ω.
We also write ω_0 — the first infinite ordinal.
We denote by ω_1 the first uncountable ordinal (which is hence a cardinal), i.e. ω_1 is te least cardinal bigger than ω_0
$\ldots, \omega_2, \omega_3, \ldots$
When we only care about the "size" of a cardinal, and not necessarily the order, we write

- $\aleph_0 \coloneqq \omega_0 \coloneqq \omega \coloneqq \mathbb{N}$
- $\aleph_1 \coloneqq \omega_1$
- $\aleph_0 \coloneqq$ next cardinal after $\aleph_1$

  $\vdots$
- $\aleph_\omega \coloneqq \bigcup_{n<\omega} \aleph_n$

For a cardinal κ, let κ^+ denote the next cardinal, i.e. the least cardinal $> \kappa$

$$\aleph_\alpha \coloneqq \begin{cases} \omega & \alpha = 0 \\ \aleph_\beta^+ & \alpha = \beta + 1 \\ \bigcup_{\beta<\alpha} \aleph_\beta & \alpha \text{ is a limit} \end{cases}$$

Continuum hypothesis rephrased (AC). $\underbrace{|2^{\mathbb{N}}|}_{\substack{=|\mathbb{R}| \\ =|\mathcal{P}(\mathbb{N})|}} = \aleph_1$.

Basic model theory (Predicate logic)

Mathematical structures. What is a mathematical structure? We know it when we see it.

Examples
- A graph is a pair $\mathbf{G} \coloneqq (V, E)$, where V is a set (of vertices) and $E \subseteq V^2$ called the set of edges.
  Recall: E is just a binary relation on V.
  An undirected graph is one where E is
  - antireflexive
  - symmetric
- A partial order is a pair $A \coloneqq (A, \leq)$, where
  - A is a set (which we refer to as the underlying set of the structure A)

- $\leq$ is a binary relation on A that's
  - reflexive
  - antisymmetric
  - transitive

- A group is a pair $\Gamma := (\Gamma, \mathbf{1}, \bullet, (\ )^{-1})$, where
  - Γ is the underlying set,
  - $\mathbf{1}$ is just an element of γ,
  - $\bullet$ is a binary operation on Γ, i.e. $\bullet\colon \Gamma \underset{\text{binary}}{\sqcup} \Gamma \to \Gamma$
  - $(\ )^{-1}$ is a unary operation on Γ, i.e. $(\ )^{-1} : \Gamma \underset{\text{unary}}{\sqcup} 1 \to \Gamma$

  Satisfy the following properties (called group axioms):

  (i) $\bullet$ is associative: $\forall x, y, z \in \Gamma$, $(x \bullet y) \bullet z = x \bullet (y \bullet z)$.

  (ii) $\mathbf{1}$ is the identity: $\forall x \in \Gamma$, $x \bullet 1 = x = 1 \cdot x$

  (iii) $(\ )^{-1}$ is the inverse: $x \bullet x^{-1} = 1 = x^{-1} \bullet x$

Examples of groups

- $(\mathbb{Z}, \underset{:=0}{\mathbf{1}}, \underset{:=+}{\bullet}, \underbrace{(\ )^{-1}}_{:=-(\ )})$
- $(\mathbb{R}^+, \underset{:=1}{\mathbf{1}}, \underset{:=\cdot}{\bullet}, \underbrace{(\ )^{-1}}_{:=(\ )^{-1}})$
- $\mathbf{G}L_n(\mathbb{R}) :=$ the set of invertible matrices ($\Leftrightarrow$ matrices with nonzero determinant)
  $\mathbf{G}L_n(\mathbb{R}) := (\mathbf{G}L_n(\mathbb{R}), \underset{:=I_n:=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ & & \ddots & \\ 0 & 0 & 0 & 1 \end{pmatrix}}{\mathbf{1}}, \underset{:=\text{matrix multiplication}}{\bullet}, \underbrace{(\ )^{-1}}_{:=\text{matrix inverse}})$
- Let $X := (X, \leq)$ be a partial order.
  Let $\mathrm{Aut}(\underline{X})$ be the set of all order-automorphisms of $\underline{X}$, i.e. order-isomorphism from $\underline{X}$ to $\underline{X}$
  $\mathrm{Aut}(X) := (\mathrm{Aut}(\underline{X}), \underset{\mathrm{id}_x \ 0}{\mathbf{1}}, \underset{\text{composition}}{\bullet}, \underbrace{(\ )^{-1}}_{:=\text{two-sided inverse}})$

Math 318
Lecture 23
October 28 2020

Examples of structures (continued)

- $(\mathbb{N}, 0, S, +, \bullet)$, where 0 is just 0.
  S is the successor function $n \mapsto n + 1$.
  $+$ and $\bullet$ are as usual.
  This is called the standard structure of natural numbers.
- $(\mathbb{Q}, 0, 1, +, \bullet, <)$, where all symbols are as usual.
  This structure is called the ordered field of rationals.

Attempt at defining a structure A structure is a set equipped with constant elements, operations and relations.

But we need a system of referring to these constant elements, operations and relation for all structures of the same "nature" without the information as to how these are defined in concretes structures.

Definition A signature is a tuple $(\mathcal{C}, \mathcal{F}, \mathcal{R}, a)$, where $\mathcal{C}, \mathcal{F}, \mathcal{R}$ are

- $\mathcal{C}$ – the set of constant symbols
- $\mathcal{F}$ – the set of function symbols
- $\mathcal{R}$ – the set of relation symbols

and $a : \mathcal{F} \cup \mathcal{R} \to \mathbb{N}^+$ is a function called the arity function that tells us what is the arity of the function and relation symbols in their interpretation in concrete structures.

Examples of signatures

- Signatre for graphs $\sigma_{\text{gr}} \coloneqq (\underbrace{\emptyset}_{\mathcal{C}}, \underbrace{\emptyset}_{\mathcal{F}}, \underbrace{\{E\}}_{\mathcal{R}}, \underbrace{E \mapsto 2}_{a})$ (the braces over $\{E\}$ and $E \mapsto 2$ read "means E is a symbol for a binary relation")
  This is too tedious to write every time and hard to read, so we usually just write "$\sigma_{\text{gr}} \coloneqq (E)$, where E is a binary relation symbol"
- Signature for groups: $\sigma_{\text{groups}} \coloneqq (\{1\}, \{\bullet, (\ )^{-1}\}, \emptyset, \{\bullet \mapsto 2, (\ )^{-1} \mapsto 1\})$
  As a more human friendly way, we would write $\sigma_{\text{groups}} \coloneqq (1, \bullet, (\ )^{-1})$, where 1 is a constant symbol, $\bullet$ is a binary function symbol, $(\ )^{-1}$ is a unary function symbol.
- Signature for arithmetic: $\sigma_{\text{arithm}} \coloneqq (0, S, +, \cdot)$, where
  - 0 is a constant symbol,
  - S is a unary function symbol,
  - $+$ and $\bullet$ are binary function symbols.

Definition. A structure $\mathcal{A}$ in a signature $\sigma \coloneqq (\mathcal{C}, \mathcal{F}, \mathcal{R}, a)$ is (technically) a pair (A, i), where

- $\mathcal{A}$ is a set called the underlying set (aka universe) of the structure $\mathcal{A}$
- i is the interpretation of σ in $\mathcal{A}$, i.e.
  - for $c \in \mathcal{C}$, $i(c) \in A$
  - for $f \in \mathcal{F}$, $i(f) : A^{a(f)} \to A$ A to the power arity of f
  - for $r \in \mathcal{R}$, $i(r)$ is an a(r)-ary relation on A, i.e. $i(r) \subseteq A^{a(r)}$. a binary relation is just a subset of A^2

Examples of structure in various signatures

- An example of a graph $G \coloneqq (\{0, 1, 2\}, i)$ in $\sigma_{\text{gr}} \coloneqq (E)$, where $i(E) \coloneqq \{(0, 1), (1, 0), (1, 1), (0, 2), (1, 2)\}$. Missing Diagram
- The group GL_n is a structure in the signature of $\sigma_{\text{gr}} \coloneqq (1, \bullet, (\ )^{-1})$, i.e. $GL_n(\mathbb{R}) \coloneqq (GL_n(\mathbb{R}), i)$ where

- $GL_n(\mathbb{R}) :=$ the set of all $n \times n$ invertible matrices
- $i(1) := I_n$
- $i(\bullet) :=$ matrix multiplication
- $i((\ )^{-1}) :=$ matrix inversion.

In a more human way, we would write
$GL_n(\mathbb{R}) := (GL_n(\mathbb{R}), 1^{GL_n(\mathbb{R})}, \bullet^{GL_n(\mathbb{R})}, ((\ )^{-1})^{GL_n(\mathbb{R})})$, where

- $1^{GL_n(\mathbb{R})} := I_n$
- $\bullet^{GL_n(\mathbb{R})} :=$ matrix multiplication
- $((\ )^{-1})^{GL_n(\mathbb{R})} :=$ matrix inversion.

Math 318
Lecture 24
October 30 2020

Examples of structure in various signatures (continued)

- $\mathcal{N} := (\mathbb{N}, 0^{\mathcal{N}}, S^{\mathcal{N}}, +^{\mathcal{N}}, \bullet^{\mathcal{N}})$, where $0^{\mathcal{N}}, S^{\mathcal{N}}, +^{\mathcal{N}}, \bullet^{\mathcal{N}}$ are defined as usual (= standard interpretations).
  In these cases when the interpretations are the standard ones, we write $(\mathbb{N}, 0, S, +, \bullet)$ instead, omitting the superscripts.
- $\mathcal{R}_< := (\mathbb{R}, 0, 1, +, \bullet, <)$ with the standard interpretations.
- $\mathcal{R}_{\text{crazy}} := (\mathbb{R}, 0^{\mathcal{R}_{\text{crazy}}}, 1^{\mathcal{R}_{\text{crazy}}}, +^{\mathcal{R}_{\text{crazy}}}, \bullet^{\mathcal{R}_{\text{crazy}}}, <^{\mathcal{R}_{\text{crazy}}})$ where
  - $0^{\mathcal{R}_{\text{crazy}}} := \pi$,
  - $1^{\mathcal{R}_{\text{crazy}}} := -7.2$,
  - $+^{\mathcal{R}_{\text{crazy}}} : \mathbb{R}^2 \to \mathbb{R}$, $(x, y) \mapsto \sin(x \cdot y)$
  - $\bullet^{\mathcal{R}_{\text{crazy}}} : \mathbb{R}^2 \to \mathbb{R}$, $(x, y) \mapsto 3$
  - $<^{\mathcal{R}_{\text{crazy}}} := \{(x, y) : x^2 = y - 1\}$.

Notation For a set A, we denote by $\vec{a}$ an element from A^n, for any $n \in \mathbb{N}$, and write $|\vec{a}| := n$. We write a_i for the i^{th} element of $\vec{a}$, so $\vec{a} = (a_0, a_1, \ldots, a_{n-1})$.
If h is a function defined on A, then we write $h(\vec{a})$ to mean the tuple $(h(a_0), h(a_1), \ldots, h(a_{n-1}))$.

Definition A substructure $\mathcal{B}$ of a structure $\mathcal{A} := (A, \sigma^{\mathcal{A}})$ in a given signature σ is a structure in the signature σ, $\mathcal{B} := (B, \sigma^{\mathcal{B}})$, where

- $\mathcal{B} \subseteq \mathcal{A}$
- $\forall c \in \mathcal{C}(\sigma)$, $c^{\mathcal{B}} = c^{\mathcal{A}}$
- $\forall f \in \mathcal{F}(\sigma)$, $f^{\mathcal{B}} = f^{\mathcal{A}}\big|_{\mathcal{B}^{a(f)}} \Leftrightarrow f^{\mathcal{B}} \subseteq f^{\mathcal{A}}$
- $\forall \mathcal{R} \in \mathscr{R}(\sigma)$, $\mathcal{R}^{\mathcal{B}} = \mathcal{R}^{\mathcal{A}}\big|_{\mathcal{B}} := \underbrace{\mathcal{R}^{\mathcal{A}}}_{\subseteq \mathcal{A}^{a(\mathcal{R})}} \cap \mathcal{B}^{a(\mathcal{R})} \underbrace{\Rightarrow}_{\not\Leftarrow} \mathcal{R}^{\mathcal{B}} \subseteq \mathcal{R}^{\mathcal{A}}$ Not every subgraph is a substructure precisely because it's $\Rightarrow$ only

We write $\underline{\mathcal{B} \subseteq \mathcal{A}}$ to mean that $\mathcal{B}$ is a substructure of $\mathcal{A}$.

Examples of substructures.

- Let $\mathcal{G} \coloneqq (V, E^{\mathcal{G}})$ be a graph and let $U \subseteq V$.
  $H \coloneqq (u, E^{\mathcal{H}})$ is a substructure of $\mathcal{G}$ i.f.f. $E^{\mathcal{H}} = E^{\mathcal{G}}\big|_u$.
  $\mathcal{H}$ is not considered a substructure because the edges $(0,2)$ and $(2,0)$ are missing. Yet $\mathcal{H}$ is a subgraph.
  Missing Diagram
  $\mathcal{H}$ is a substructure of $\mathcal{G}$.
  Missing Diagram
  It is called the induced subgraph of $\mathcal{G}$ on u.
  Thus: a subgraph of a graph is a substructure if and only if it is an induced subgraph.

- $\mathcal{N} \coloneqq (\mathbb{N}, 0, S, +, \cdot)$ has no proper substructure because any substructure has to contain 0 and be closed under the successor S.

- $\mathcal{Z} \coloneqq (\mathbb{Z}, 0, 1, +, \cdot)$, what are the substructures of this?
  Any $\mathcal{A} \subseteq \mathcal{Z}$, $A \ni 0, 1$ and be closed under $+$ and $\cdot$.

For example • $\mathcal{A} \coloneqq (\mathbb{N}, 0, 1, +, \cdot) \subseteq \mathcal{Z}$.

  – $\mathcal{B} \coloneqq (\mathbb{N} \cup \{-1\}, 0, 1, +, \cdot)$ isn't defined because $\cdot$ isn't defined on $\mathbb{N} \cup \{-1\}$: $-1 \cdot 7 = -7 \notin \mathbb{N} \cup \{-1\}$.
    Also $+$ isn't defined because $(-1) + (-1) = -2 \notin \mathbb{N} \cup \{-1\}$.

  – $\mathcal{C} \coloneqq (\{0,1\}, 0, 1, +, \cdot)$ isn't defined because $1 + 1 = 2 \notin \{0, 1\}$

- $\mathcal{D} \coloneqq (\{0,1\}, 0^{\mathcal{D}}, 1^{\mathcal{D}}, +^{\mathcal{D}}, \cdot^{\mathcal{D}})$ where $0^{\mathcal{D}} \coloneqq 0$, $1^{\mathcal{D}} \coloneqq 1$

  – $+^{\mathcal{D}}$: $\{0,1\}^2 \to \{0,1\}$
    $(x, y) \mapsto x + y \bmod 2 \coloneqq$ the remainder of $x + y$ when divided by 2

  – $\cdot^{\mathcal{D}}$ $\{0,1\}^2 \to \{0,1\}$
    $(x, y) \mapsto x \cdot y \bmod 2 \coloneqq$ the remainder of $x \cdot y$ when divided by 2

  $\mathcal{D}$ is well-defined, but $\mathcal{D} \not\subseteq \mathcal{Z}$ because $(1+1)^{\mathcal{Z}} = 2$ whereas $(1+1)^{\mathcal{D}} = 1$ and $1 \neq 2$.

Math 318
Lecture 25
November 2 2020

Definition. For a σ-structure $\mathcal{A} \coloneqq (A, \sigma^{\mathcal{A}})$, $B \subseteq A$ is called the underlying set of a substructure or we say that B forms a substructure if there is a substructure $\mathcal{B} \subseteq \mathcal{A}$ whose underlying set is B

Proposition. For a σ-structure $\mathcal{A}$, a set $B \subseteq A$ forms a substructure i.f.f.

(i) B contains all the constants of $\mathcal{A}$, i.e. for each constant symbol c in σ, $C^{\mathcal{A}} \in B$.

(ii) B is closed under all functions of $\mathcal{A}$, i.e. for each function symbol f in σ, B is closed under $f^{\mathcal{A}}$, which means $\forall \vec{b} \in B^{a(f)}$, $f^{\mathcal{A}}(\vec{b}) \in B$.

Proof. ($\Rightarrow$): By definition of a substructure $\mathcal{B} = (B, \sigma^{\mathcal{B}})$.
($\Leftarrow$): Define $\mathcal{B} \coloneqq (B, \sigma^{\mathcal{B}})$ where $\sigma^{\mathcal{B}}$ is defined as follows:

- for each constant symbol c in σ, $c^{\mathcal{B}} = c^{\mathcal{A}}$.
- for each function symbol f in σ, define $f^{\mathcal{B}} \coloneqq f^{\mathcal{A}}\big|_{B^{a(f)}}$.
- for each relation symbol $\mathcal{R}$ in σ, define $\mathcal{R}^{\mathcal{B}} \coloneqq \mathcal{R}^{\mathcal{A}}\big|_B \coloneqq \mathcal{R} \cap \mathcal{B}^{a(\mathcal{R})}$.

□

Proposition. Intersection (finite or infinite) of substructures (more precisely, the underlying sets of substructures) is again a substructure (more precisely, the underlying set of a substructure).

Proof. Immediate from the previous proposition: if $\{B_i\}_{i\in I}$ is a collection of underlying sets of substructures, then $\bigcap_{i\in I} B_i$ satisfies (i) and (ii) of the proposition above. □

Definition In the light of the last proposition, we define, for a subset $S \subseteq A$ of a σ-structure $\mathcal{A} \coloneqq (A, \sigma^{\mathcal{A}})$, the substructure generated by S as the $\subseteq$-smallest substructure that contains S, namely, the intersection of all substructures that contain S. We denote this structure by $\langle S\rangle_{\mathcal{A}}$.

This is a nonconstructive (top-to-bottom) definition, but the following gives how to construct $\langle S\rangle_{\mathcal{A}}$ (bottom-up).

Proposition. For a σ-structure $\mathcal{A}$ and $S \subseteq A$,

(a) The underlying set of $\langle S\rangle_{\mathcal{A}}$ is $S_\infty \coloneqq \bigcup_{n\in\mathbb{N}} S_n$, where

- $S_0 \coloneqq S \cup \{c^{\mathcal{A}} : c \text{ is a constant symbol in } \sigma\}$
- $S_{n+1} \coloneqq S_n \cup \{f^{\mathcal{A}}(\vec{b}) : f \text{ is a function symbol in } \sigma \text{ and } \vec{b} \in {S_n}^{a(f)}\}$

(b) $|S_\infty| \leq \max\{|S|, |\sigma|, \aleph_0\}$

Proof. Proof of (a). $S_\infty \supseteq$ all constants of $\mathcal{A}$, by definition, it remains to show that it's closed under all functions of $\mathcal{A}$.
Fix a function symbol f in σ and let $\vec{b} \in S_\infty^{a(f)}$.
We want to show that $f^{\mathcal{A}}(\vec{b}) \in S_\infty$.
Because the S_n are increasing, i.e. $S_n \subseteq S_{n+1}$, and $\vec{b} = (b_0, b_1, \ldots, b_x)$ is finite, $\exists n \in \mathbb{N}$ s.t. $b_0, b_1, \ldots, b_k \in S_n$.
The least cardinal that is higher than the number of elements in each tuple
Then, by definition, $S_{n+1} \ni f^{\mathcal{A}}(\vec{b})$. □

Example. What is the substructure of $\mathcal{R} = (\mathbb{R}, 0, 1, +, \cdot)$ generated by $\emptyset$?
$\langle\emptyset\rangle_{\mathcal{R}} = (\mathbb{N}, 0, 1, +, \cdot)$.

Definition Let $\mathcal{A} \coloneqq (A\sigma^{\mathcal{A}})$ and $\mathcal{B} \coloneqq (B\sigma^{\mathcal{B}})$ be σ-structures.
A σ-homomorphism from $\mathcal{A}$ to $\mathcal{B}$, denoted by $h : \mathcal{A} \to \mathcal{B}$, is just a function $h : A \to B$ that preserves theσ-structure, i.e.

(i) $h(c^{\mathcal{A}}) = c^{\mathcal{B}}$ for each constant symbol c in σ,

(ii) $h(f^{\mathcal{A}}(\vec{a})) = f^{\mathcal{B}}(\underbrace{h(\vec{a})}_{\coloneqq(h(a_0), h(a_1), \ldots, h(a_{n-1}))})$ for each function symbol f in σ, $\forall \vec{a} \in A^{a(f)}$

(iii) $\mathcal{R}^{\mathcal{A}}(\vec{a})$ holds $\Rightarrow \mathcal{R}^{\mathcal{B}}(h(\vec{a}))$ for each relation symbol $\mathcal{R}$ in σ and $\forall \vec{a} \in A^{a(\mathcal{R})}$.

Remark. We don't require $\Leftarrow$ in (iii) because it would be too restrictive.
For example, if $\mathcal{R}^{\mathcal{A}}$ and $\mathcal{R}^{\mathcal{B}}$ are binary relations of equality, the requiring $\Leftarrow$ would force every σ-homomorphism to be injective.

Observation. For σ-structures $\mathcal{A}$ and $\mathcal{B}$, and a σ-homomorphism $h : \mathcal{A} \to \mathcal{B}$, the image $h[A]$ forms a substructure of $\mathcal{B}$.

Proof. We just need to check that $h[A]$ contains all the constants of $\mathcal{B}$ and is closed under all functions of $\mathcal{B}$, but this is immediate from parts (i) and (ii) of the definition of σ-homomorphism. □

Definition For σ-structures $\mathcal{A}$, $\mathcal{B}$, a σ-isomorphism if h has a two sided inverse h^{-1}, which is also a σ-homomorphism.

Warning A bijective σ-homomorphism may not be an isomorphism if σ contains relation symbols because the $\Rightarrow$ is only one way in (iii) of the definition of σ-homomorphism.
missing diagram
$h : n \mapsto n'$ is a bijective homomorphism, but is not an isomorphism.

Observation A *sigma*-homomorphism $h : \mathcal{A} \to \mathcal{B}$ is an isomorphism i.f.f. h is bijective and for relations, the implication is both ways: $\forall$ relation symbols $\mathcal{R}$ n σ,

$$\mathcal{R}^{\mathcal{A}}(\vec{a}) \Leftrightarrow \mathcal{R}^{\mathcal{B}}(h(\vec{b}))$$

Definition A σ-homomorphism $h : \mathcal{A} \to \mathcal{B}$ is called a σ-embedding if, recalling that the image $h[A]$ forms a substructure $\mathcal{B}' \subseteq \mathcal{B}$, h is a σ-isomorphism from $\mathcal{A}$ to $\mathcal{B}'$.
Again, this is equivalent to h being injective and the implication for relations going both ways.

Example. For any $\mathcal{A} \subseteq \mathcal{B}$, the identity map id: $A \to B$ is an embedding.

Definition Let $\sigma \subseteq \sigma'$ be two signatures (e.g. $\sigma := (0, +)$ and $\sigma' := (0, 1, +, \cdot)$).
A σ-structure $\mathcal{A}$ is called a reduct of a σ'-structure $\mathcal{B}$ (also, $\mathcal{B}$ is called an expansion of $\mathcal{A}$) if

(i) $A = B$

(ii) every symbol of σ is interpreted exactly the same way in $\mathcal{A}$ and $\mathcal{B}$

Examples
- $(\mathbb{R}, 0, +)$ is a reduct of $(\mathbb{R}, 0, 1, +, -, \cdot)$ which, in turn, is a reduct of $(\mathbb{R}, 0, 1, +, -, \cdot, <)$.
- But $(\mathbb{N}, 0, +)$ is not a reduct of $(\mathbb{Z}, 0, +, \cdot)$
- Also $(\mathbb{N}, 01, , +)$ is not a reduct of $(\mathbb{N}, 0, S, +)$.

Language and interpretation
We now define the language of First Order Logic that we will use to write statements about structures (like axioms and theorems).

Definition. For a signature σ, the alphabet of the first order language of σ, denoted by $\mathbb{FOL}(\sigma)$ is the following collection of symbols:

- all symbols of σ
- $\doteq$
- Boolean connective symbols $\neg \vee \wedge \Rightarrow \Leftarrow, \Leftrightarrow$
- quantifier symbols $\forall \exists$
- punctuation symbols ( ) ,

- variable symbols $v_0\ v_1\ v_2\ v_3\ \ldots$

We call a finitie sequence of symbols in $\mathbb{FOL}$ σ-words.

We now define the words that are to be interpreted as functions.
For example, in $(\mathbb{N}, 0, 1, +, \cdot)$, $(v_0 + v_1) \cdot v_3 + 1$.

Definition A σ-term is a σ-word defined recursively as follows:

(i) c is a σ-term for each constant symbol c in σ.

(ii) v_i is a σ-term for each variable symbol v_i (in $\mathbb{FOL}$).

(iii) $f(t_0, t_1, \ldots, t_{n-1})$ is a σ-term for each function symbol f in σ with $a(f) = n$ and $t_0, t_1, \ldots, t_{n-1}$ σ-term.

Math 318
Lecture 27
November 6 2020

Definition σ-terms are σ-words defined recursively as follows:

(i) c is a σ-term for each constant symbol c in σ.

(ii) v_i is a σ-term for each variable symbol v_i (in $\mathbb{FOL}(\sigma)$).

(iii) $f(t_0, t_1, \ldots, t_{n-1})$ is σ-term for each function symbol f in σ with $a(f) = n$ and $t_0, t_1, \ldots, t_{n-1}$ σ-term.

We denote by Terms(σ) the set of σ-terms.

Examples
- In $\sigma \coloneqq (0, 1, +, \cdot)$, $t \coloneqq (1 + 1) \cdot 0 + v_0 \cdot v_1$ is a σ-term.
  Actually, it's technically not because the function symbols $+$ and $\cdot$ must be written $+(1, 1)$ and $\cdot((1 + 1), 0)$ and $\cdot(v_0, v_1)$, so officially, the term would be $+(\cdot(+(1, 1), 0), \cdot(v_0, v_1))$.
  But since this is unreadable, we will write it more casually as above.
  Same for $(\ )^{-1}(x)$, we instead write x^{-1}.
- In $\sigma_{\text{artim.}} \coloneqq (0, S, +, \cdot)$, $S(S(S(0))) + S(0) \cdot v_0$ is a term.
  We abbreviate $\underbrace{S(S(\ldots(S(0)))}_{n \text{ times}}$ by $S^n(0)$ or simply $\dot{n}$
- In $\sigma_{\text{graph}} \coloneqq (E)$, the only terms are v_i, for $i \in \mathbb{N}$.
  More casually, we will use other letters for variables like x, y, z, if there is no confusion.

$$\sigma\text{-terms } = \sigma\text{-names for functions}$$

σ-terms are interpreted as functions in σ-structures, just like polynomials, e.g. $2v_1 + v_0$, are interpreted as functions on a given "ring", say $\mathbb{R}$.
One way to interpret $2v_1 + v_0$ is as a function $\mathbb{R}^2 \to \mathbb{R}$ given by $(v_0, v_1) \mapsto 2v_1 + v_0$.
But what if we actually had $2v_1 + v_0 + 0 \cdot v_2$ in mind?
Then it should be interpreted as $\mathbb{R}^3 \to \mathbb{R}$ by $(v_0, v_1, v_2) \mapsto 2v_1 + v_0$.
The upshot is that from just the term $2v_1 + v_0$ we can't determine what other variable should be taken as input, we only know that the output depends on v_0, v_1, so at least v_0, v_1 have to be taken into the input.

Definition. For a signature σ, an extender σ-term is a σ-term t together with a vector $\vec{v}$ of variables, $\vec{c} = (v_{i_0}, v_{i_1}, \ldots, v_{i_{n-1}})$, that includes all the variables that occur in t. We denote this

by $t[\vec{v}]$.

Definition. Let $t[\vec{v}]$ be an extended σ-term. We define its interpretation in a σ-structure $\mathcal{A}$ as a function $t^{\mathcal{A}}[\vec{v}] : A^{|\vec{v}|} \to A$ defined by recursion on the structure of t as follows:

(i) if $t = c$ for some constant symbol c in σ, then $\forall \vec{a} \in A^{|\vec{v}|}$,

$$t^{\mathcal{A}}[\vec{v}](\vec{a}) \coloneqq c^{\mathcal{A}}$$

(ii) if $t = v_j$ for some $j \in \mathbb{N}$, then $\forall \underset{=(a_0,a_1,\ldots,a_{|\vec{v}|-1})}{\vec{a}} \in A^{|\vec{v}|}$, recall that v_j occurs in $\vec{v}$, say $v_j = v_{i_k}$, then

$$t^{\mathcal{A}}[\vec{v}](\vec{a}) \coloneqq a_k$$

(iii) if $t = f(t_0, t_1, \ldots t_{n-1})$ for some n-ary function symbol f in σ, then $\forall \vec{a} \in A^{|\vec{v}|}$,

$$t^{\mathcal{A}}[\vec{v}](\vec{a}) \coloneqq f^{\mathcal{A}}(t_0^{\mathcal{A}}[\vec{v}](\vec{a}), t_1^{\mathcal{A}}[\vec{v}](\vec{a}), \ldots, t_{n-1}^{\mathcal{A}}[\vec{v}](\vec{a}))$$

Examples
- $\mathcal{A} \coloneqq (\mathbb{Z}, \mathbf{1}, \cdot)$ and $\mathcal{B} \coloneqq (\mathbb{Z}, \mathbf{1}^{\mathcal{B}}, \cdot^{\mathcal{B}})$ where $\mathbf{1}^{\mathcal{B}} \coloneqq 0$, $\cdot^{\mathcal{B}} \coloneqq +$.
  Let $t \coloneqq (v_0 \cdot 1) \cdot v_3$.
  $t^{\mathcal{A}}[v_0, v_1, v_3] : \mathbb{Z}^3 \to \mathbb{Z}$, $(x, y, z) \mapsto (x \cdot 1) \cdot y = xy$, whereas
  $t^{\mathcal{B}}[v_0, v_1, v_3] : \mathbb{Z}^3 \to \mathbb{Z}$, $(x, y, z) \mapsto (x + 0) + y = x + y$.
- But if we just took $t[v_0, v_1]$, with the same t as in the previous example, then the functions $t^{\mathcal{A}}[v_0, v_1]$ and $t^{\mathcal{B}}[v_0, v_1]$ would be $\mathbb{Z}^2 \to \mathbb{Z}$.

So one more time, σ-terms are names of functions in σ-structures and their interpretations are functions in σ-structures.
Similarly, we want to have names for relations in σ-structures, in particular, we want to be able to write true/false statements.

Definition. A σ-formula is a σ-word formed by the following recursive rules:

(i) $t \doteq t'$ is a σ-formula, for any σ-terms t and t'.

(ii) $\mathcal{R}(t_0, \ldots, t_{n-1})$ is a σ-formula, for any n-ary relation symbol $\mathcal{R}$ in σ and any σ-terms $t_0, t_1, \ldots, t_{n-1}$.

(iii) $\neg(\varphi), (\varphi) \wedge (\psi), (\varphi) \vee (\psi), (\varphi) \Rightarrow (\psi), (\varphi) \Leftarrow (\psi), (\varphi) \Leftrightarrow (\psi)$ are σ-formulas for any σ-formulas φ, ψ.

(iv) $\forall v_i(\varphi)$ and $\exists v_i(\varphi)$ are σ-formulas for any variable v_i and any σ-formula φ.

$$\sigma\text{-formulas } = \sigma\text{-names for relations}$$

Math 318
Lecture 28
November 9 2020

Definition. A σ-formula is a σ-word formed by the following recursive rules:

(i) $t \doteq t'$ is a σ-formula, for any σ-terms t and t'.

(ii) $\mathcal{R}(t_0, \ldots, t_{n-1})$ is a σ-formula, for any n-ary relation symbol $\mathcal{R}$ in σ and any σ-terms $t_0, t_1, \ldots, t_{n-1}$.

(iii) $\neg(\varphi), (\varphi) \wedge (\psi), (\varphi) \vee (\psi), (\varphi) \Rightarrow (\psi), (\varphi) \Leftarrow (\psi), (\varphi) \Leftrightarrow (\psi)$ are σ-formulas for any σ-formulas φ, ψ.

(iv) $\forall v_i(\varphi)$ and $\exists v_i(\varphi)$ are σ-formulas for any variable v_i and any σ-formula φ.

$$\sigma\text{-formulas } = \sigma\text{-names for relations}$$

The formulas in (i) and (ii) are called atomic. The formulas that are formed only using (i), (ii), and (iii) are called quantifier free.

Consider the formula $(\forall x(x \doteq y)) \wedge (x = z)$. Here the first two occurrences of the variable x have nothing to do with the third occurrence.

This is like $\underbrace{\int_0^x x^2 dx}_{=\frac{1}{3}} + x + z = g(x,z) = \frac{1}{3} + x + z$.

Although there is no ambiguity, this is confusing notation, so:

Convention. Say that a variable v is quantified in a σ-formula φ if it occurs after a quantifier $\forall v$ or $\exists v$.
We will restrict ourselves to formulas that if a variable is quantified, i.e. occurs in a subformula $Qv\psi$ where $Q \coloneqq \forall, \exists$, then it can only occur in ψ, but nowhere else in φ.
We call such formulas legal.
E.g. $(\forall x(\underbrace{x \doteq y}_{\psi})) \wedge (x \doteq z)$ is illegal because x is quantified, occurring in $\forall x(x \doteq y)$ but ψ it also occurs in $x \doteq z$.

Definition. We call a variable v free in a formula φ if it occurs in φ but isn't quantified.
A formula with no free variables is called a sentence.

Just like with terms, we define an extended σ-formula $\varphi[\vec{v}]$ to be a σ-formula φ with $\vec{v} \coloneqq (v_{i_0}, v_{i_1}, \ldots, v_{i_k})$ that includes all free variables of φ and does not include any quantified variable in φ.
E.g. $\varphi \coloneqq \forall x(x \doteq y) \wedge (y \neq z)$ then $\varphi[y,z,v]$ is an extended formula, so is $\varphi[y,z]$, but not $\varphi[y,z,x]$ and not $\varphi[y]$.

Definition. We define interpretation for an extended σ-formula $\varphi[\vec{v}]$, $\vec{v} = (v_{i_0}, \ldots, v_{i_{k-1}})$ in a σ-structure $\mathcal{A} \coloneqq (A, \sigma^{\mathcal{A}})$ by recursion on the structure of φ as follows: $\varphi^{\mathcal{A}}[\vec{v}]$ is a $|\vec{v}|$-ary relation on A defined in each case as follows:
So again, because we define formulas by induction, anything else we define for them has to be a recursive definition and anything we prove about them has to be an inductive proof

(i) $\varphi \coloneqq t_1 \doteq t_2$, then $\forall \vec{a} \in A^{|\vec{v}|}$, $\varphi^{\mathcal{A}}[\vec{v}](\vec{a})$ holds $:\Leftrightarrow t_1^{\mathcal{A}}[\vec{v}](\vec{a}) = t_2^{\mathcal{A}}[\vec{v}](\vec{a})$.

(ii) $\varphi \coloneqq \mathcal{R}(t_1, t_2, \ldots, t_n)$, then $\forall \vec{a} \in A^{|\vec{v}|}$, $\varphi^{\mathcal{A}}[\vec{v}](\vec{a})$ holds $:\Leftrightarrow \mathcal{R}^{\mathcal{A}}(t_1^{\mathcal{A}}[\vec{v}](\vec{a}), \ldots, t_n^{\mathcal{A}}[\vec{v}](\vec{a}))$

(iii) a. $\varphi \coloneqq \neg\psi$, then $\varphi^{\mathcal{A}}[\vec{v}](\vec{a})$ holds $:\Leftrightarrow \psi^{\mathcal{A}}[\vec{v}](\vec{a})$ doesn't hold

(iii) b. $\varphi \coloneqq \psi_1 \cap \psi_2$, then $\varphi_1^{\mathcal{A}}[\vec{v}](\vec{a})$ and $\varphi_2^{\mathcal{A}}[\vec{v}](\vec{a})$.

(iii) c. same for $\vee$, $\Rightarrow$, $\Leftarrow$, $\Leftrightarrow$. Recall $P \vee Q \Leftrightarrow \neg P \wedge \neg Q$. $P \Rightarrow Q \Leftrightarrow \neg P \vee Q$.

(iv) a. $\varphi \coloneqq \forall v_{i_k}\psi$. Then since φ is legal, v_{i_k} shouldn't be quantified in ψ.
Therefore, $\vec{w} \coloneqq (v_{i_0}, \ldots, v_{i_{k-1}})$ is such that $\psi[\vec{w}]$ is an extended formula.
So $\forall \vec{a} \in A^{|\vec{v}|}$, $\varphi^{\mathcal{A}}[\vec{v}](\vec{a})$ holds $:\Leftrightarrow \forall b \in A\ \psi^{\mathcal{A}}[\vec{w}](\vec{a}, b)$ holds.

(iv) b. $\varphi \coloneqq \exists v_{i_k} \psi$.
Define this similarly, with $\forall$ replaced by $\exists$.

An alternative way to write that $\varphi^{\mathcal{A}}[\vec{v}](\vec{a})$ holds is $\mathcal{A} \models \varphi[\vec{v}](\vec{a})$, and we read this as $\underline{\mathcal{A} \text{ models}}$ (or satisfies)$\varphi[\vec{v}](\vec{a})$.
For a sentence φ if we take the empty vector $\vec{v} = \emptyset$, then $\varphi^{\mathcal{A}}$ either holds or not and we say that φ is true/false in $\mathcal{A}$.

Convention Instead of writing $t[\vec{v}](\vec{a})$ and $\varphi[\vec{v}](\vec{a})$, we write $t(\vec{a})$ and $\varphi(\vec{a})$ if there is no ambiguity.

Math 318
Lecture 29
November 11 2020

Convention. Note that we can express the Boolean connectives in terms of $\neg$ and $\vee$ as follows:

- $P \wedge Q \Leftrightarrow \neg(\neg P \vee \neg Q)$.
- $P \Rightarrow Q \Leftrightarrow \neg P \vee Q$

We will often just write $\varphi(\vec{a})$ instead of $\varphi[\vec{v}](\vec{a})$ if there is no confusion. Similarly, $t(\vec{a}$ instead of $t[\vec{v}](\vec{a})$.

Examples
- Let $\sigma \coloneqq \sigma_{\text{arithm}} = (0, S, +, \cdot)$. $\varphi \coloneqq S(S(0)) \doteq v_0$.
  Then both $\varphi[v_0]$ and $\varphi[v_0, v_1]$ are extended formulas and letting $\mathcal{N} \coloneqq (\mathbb{N}, 0, S, +, \cdot)$, $\mathcal{N} \models \varphi[v_0](2)$ and $\mathcal{N} \models \varphi[v_0, v_1](2, 7)$.
  But $\mathcal{N} \not\models \varphi[v_0](0)$.

- Again in σ_{arithm}, let:
  - $x \leq y \coloneqq (x = y)$ or $\exists v_0 \in \mathbb{N} S^{v_0}(x) = y$. this isn't defined. $S^3(x)$ is defined: $S(S(S(0)))$.
  - $x \leq y \coloneqq \exists z(x + z \doteq y)$
  - $x|y \coloneqq \exists z(x \cdot z \doteq y)$
  - $\text{Even}[x] \coloneqq \dot{2}|x$, where $\dot{2} \coloneqq S(S(0))$.
  - $\text{Prime}[x] \coloneqq \forall y(y|x \Rightarrow (y \doteq 1 \vee y \doteq x))$.

Goldbach conjecture $\coloneqq \forall x \exists y \exists z(\text{Prime}[y]) \wedge \text{Prime}[z] \wedge (x \doteq y + z))$.
We still don't know (major open question) whether $\mathcal{N} \models$ Goldback conjecture.
$\mathcal{R} \coloneqq (\mathbb{R}, 0, 1, +, -, \cdot)$, $\varphi \coloneqq \exists y(y \cdot y \doteq x)$, $\mathcal{R} \models \varphi(a) \Leftrightarrow a \geq 0$.

Proposition. For σ-structures $\mathcal{A}$ and $\mathcal{B}$, and extended σ-term $t[\vec{v}]$, and a σ-homomorphism $h : \mathcal{A} \to \mathcal{B}$, $\forall \vec{a} \in A^{|\vec{v}|}$,

$$h(t^{\mathcal{A}}(\vec{a})) = t^{\mathcal{B}}(h(\vec{a})).$$

Proof. By induction on the structure of t.

- If $t \coloneqq c$ for some constant symbol in φ, then $t^{\mathcal{A}}(\vec{a}) = c^{\mathcal{A}}$ and

$$h(t^{\mathcal{A}}(\vec{a})) = h(c^{\mathcal{A}}) \underbrace{=}_{h \text{ is a homomorphism}} c^{\mathcal{B}} = t^{\mathcal{B}}(h(\vec{a})).$$

- If $t \coloneqq v$ then v is some v_{i_j} in $\vec{v} = (v_{i_1}, \ldots, v_{i_n})$ and

$$h(t^{\mathcal{A}}(\vec{a})) = h(a_j) = t^{\mathcal{B}}(h(\vec{a})) = t^{\mathcal{B}}(h(a_1), h(a_2), \ldots, h(a_n)).$$

- If $t \coloneqq f(t_1, \dots t_k)$ for some function symbol in σ of arity k.

$$\begin{aligned} h(t^{\mathcal{A}}(\vec{a})) &= h(f^{\mathcal{A}}(t_1^{\mathcal{A}}(\vec{a}), \dots, t_k^{\mathcal{A}}(\vec{a})) \\ [h \text{ is a homomorphism}] \quad &= f^{\mathcal{B}}(h(t_1^{\mathcal{A}}(\vec{a}), \dots, t_k^{\mathcal{A}}(\vec{a})) \\ &= f^{\mathcal{B}}(h(t_1^{\mathcal{A}}(\vec{a}), \dots, t_k^{\mathcal{A}}(\vec{a})) \\ [\text{by induction}] \quad &= f^{\mathcal{B}}(t_1^{\mathcal{B}}(h(\vec{a})), \dots, t_k^{\mathcal{B}}(h(\vec{a}))). \end{aligned}$$

□

Proposition. Let $\mathcal{A}, \mathcal{B}$, be σ-structure and $h : \mathcal{A} \to \mathcal{B}$ a σ-isomorphism. Let $\varphi[\vec{v}]$ be an extended σ-formula.

For every $\vec{a} \in A^{|\vec{v}|}$, $\mathcal{A} \models \varphi(\vec{a}) \Leftrightarrow \mathcal{B} \models \varphi(h(\vec{a}))$.

Proof. By induction on the construction of φ.

- $\varphi \coloneqq \mathcal{R}(t_1, \dots, t_k)$. Then, by the definition of isomorphism,

$$\mathcal{R}^{\mathcal{A}}(t_1^{\mathcal{A}}(\vec{a}), \dots, t_k^{\mathcal{A}}(\vec{a})) \Leftrightarrow \mathcal{R}^{\mathcal{B}}(\underbrace{h(t_1^{\mathcal{A}}(\vec{a}))}_{\substack{=t_1^{\mathcal{B}}(h(\vec{a})) \\ \text{by the previous} \\ \text{proposition}}} , \dots, \underbrace{h(t_k^{\mathcal{A}}(\vec{a}))}_{=t_k^{\mathcal{R}}(h(\vec{a}))}$$

- $\varphi \coloneqq \neg\psi$.

$$\begin{aligned} \text{Then } \mathcal{A} \models \varphi(\vec{a}) &:\Leftrightarrow \mathcal{A} \not\models \psi(\vec{a}) \\ [\text{by induction}] \quad &\Leftrightarrow \mathcal{B} \not\models \psi(h(\vec{a})) \\ &\Leftrightarrow: \mathcal{B} \models \varphi(h(\vec{a})). \end{aligned}$$

□

Math 318
Lecture 30
November 13 2020

- $\varphi \coloneqq t_1 \doteq t_2$. By a previous proposition, $h(t_i^{\mathcal{A}}(\vec{a})) = t_i^{\mathcal{B}}(h(\vec{a}))$, $i = 1, 2$.
So $t_1^{\mathcal{A}}(\vec{a}) = t_2^{\mathcal{A}}(\vec{a}) \Rightarrow t_1^{\mathcal{B}}(h(\vec{a})) = t_2^{\mathcal{B}}(h(\vec{a}))$ by the definition of a function and $\Leftarrow$ also holds because h is injective.

- $\varphi \coloneqq \psi_1 \vee \psi_2$. Similar to $\neg\psi$.

- $\varphi \coloneqq \exists u\psi$.

$$\begin{aligned} \text{Then } \mathcal{A} \models \varphi(\vec{a}) &\overset{\text{definition}}{\Leftrightarrow} \exists \text{ an element } a' \in A \text{ s.t. } \mathcal{A} \models \psi[\vec{v}, u](\vec{a}, a') \\ (\text{by induction}) \quad &\Leftrightarrow \exists \text{ an element } a' \in A \text{ s.t. } \mathcal{B} \models \psi[\vec{v}, u](h(\vec{a}), h(a')) \\ (\Rightarrow b' \coloneqq h(a'), \underbrace{\Leftarrow}_{\text{surjectivity}} a' \coloneqq h^{-1}(b')) &\Leftrightarrow \exists \text{ an element } b' \in B \text{ s.t. } \mathcal{B} \models \psi[\vec{v}, u](h(\vec{a}), b). \\ &\overset{\text{definition}}{\Leftrightarrow} \mathcal{B} \models \varphi[\vec{v}](h(\vec{a})). \end{aligned}$$

- $\varphi \coloneqq \forall u\psi \Leftrightarrow \neg\exists u\neg\psi$.

In particular, isomorphic structures satisfies the same sentences.

Proposition. Let $\mathcal{A} \coloneqq (A, \sigma)$ be a reduct of $\mathcal{A}' \coloneqq (A, \sigma')$, i.e. $\sigma \subseteq sigma'$.
Then for any extended σ-term $t(\vec{v})$ and any extended σ-formula $\varphi(\vec{v})$, $\forall \vec{a} \in A^{|\vec{v}|}$,

$$t^{\mathcal{A}}(\vec{a}) = t^{\mathcal{A}'}(\vec{a}) \text{ and } \mathcal{A} \models \varphi(\vec{a}) \Leftrightarrow \mathcal{A}' \models \varphi(\vec{a}).$$

Proof. A very straightforward induction on terms and on formulas. □

Definability.
Definition. For σ-structure $\mathcal{A} \coloneqq (A, \sigma^{\mathcal{A}})$, $P \subseteq A$, and $n \in \mathbb{N}$, a set $S \subseteq A^n$ is said to be P-definable in $\mathcal{A}$ if there is an extended formula $\varphi[\vec{u}, \vec{v}]$ with $|\vec{v}| = n$ and $\vec{p} \in P^{|\vec{u}|}$ s.t.

$$S = \{\vec{a} \in A^n : \mathcal{A} \models \varphi(\vec{p}, \vec{a})\}.$$

In other words, the set S is exactly the set carved out by some formula with parameters.
We say that $\vec{a} \in A^n$ is P-definable if the set $\{\vec{a}\}$ is P-definable.
We say that a function $g : A^n \to A$ is P-definable if its graph

$$\text{graph}(g) \coloneqq \{(\vec{a}, b) \in A^{n+1} : f(\vec{a}) = b\} \subseteq A^{n+1}$$

is P-definable.
We say definable if it is A-definable.
We say 0-definable if it is $\emptyset$-definable.

Examples • $\mathcal{R} \coloneqq (\mathbb{R}, 0, 1, +, \cdot)$

- Is $-(\ ) : \mathbb{R} \to \mathbb{R}$ a definable function?
  Yes, in fact, it is 0-definable.
  $\varphi(x, y) \coloneqq x + y \doteq 0$.
- Is $\mathbb{R}^+ \coloneqq (0, \infty)$ definable?
  Yes, it's 0-definable.
  $\varphi_{\geq 0}(x) \coloneqq \exists y(y^2 \doteq x)$, where y^2 stands for $y \cdot y$.
  $\varphi_{>0}(x) \coloneqq \varphi_{\geq}(x) \wedge (x \neq 0)$.
- Is $\leq$ definable?
  Yes, 0-definable by $x \leq y \coloneqq \exists z(\varphi_{=}(x, y) \wedge \varphi_{\geq} \underbrace{y + z}_{=y-x})$.

• $\mathcal{Z} \coloneqq (\mathbb{Z}, 0, 1, +, \cdot)$

- Is $\mathbb{N}$ definable?
  Yes, it's 0-definable.
  By Lagrange's Four Square theorem, every natural number is a sum of four squares of natural numbers.
  For example, $6 = 2^2 + 1^2 + 1^2 + 0^2$.
  $\varphi_{\mathbb{N}}(x) \coloneqq \exists y \exists z \exists u \exists v(x \doteq y^2 + z^2 + u^2 + v^2)$, where $y^2 \coloneqq y \cdot y$.

• $\mathcal{Q} \coloneqq (\mathbb{Q}, <)$.

- Is $\mathcal{Q}^+$ definable? No.

For any σ-structure $\mathcal{A}$, every automorphism of $\mathcal{A}$ fixes setwise every 0-definable set.
In fact, every automorphism $h : \mathcal{A} \to \mathcal{A}$ that fixes a subset $P \subseteq A$ pointwise, ie. $h\big|_P = \text{id}_P$, also fixes every P-definable set $S \subseteq A^n$ setwise, i.e. $h(S) = S$.

Math 318
Lecture 31
November 16 2020

Corollary. For any σ structure $\mathcal{A}$, every automorphism of $\mathcal{A}$ fixes setwise every 0-definable set.
In fact, every automorphism $h : \mathcal{A} \to \mathcal{A}$ that fixes a subset $P \subseteq A$ pointwise, i.e. $h\big|_P = \mathrm{id}_P$, also fixes every P-definable set $S \subseteq A^n$ setwise, i.e. $h(S) = S$.

Proof. Let $\varphi(\vec{x}, \vec{y})$ be a formula that defines S in $\mathcal{A}$ with a vector $\vec{p} \in P^{|\vec{x}|}$, i.e.

$$S = \{\vec{a} \in A^{|\vec{y}|} : \mathcal{A} \models \varphi(\vec{p}, \vec{a})\}$$

By an earlier proposition about isomorphisms respecting fortmulas, $\forall \vec{a} \in A^{|\vec{y}|}$,

$$\begin{aligned} \vec{a} \in S \Leftrightarrow \mathcal{A} \models \varphi(\vec{p}, \vec{a}) &\Leftrightarrow \mathcal{A} \models \varphi(h(\vec{p}), h(\vec{a})) \\ &\Leftrightarrow \mathcal{A} \models \varphi(\vec{p}, h(\vec{a})) \\ &\Leftrightarrow h(\vec{a}) \in S \end{aligned}$$

Thus, indeed, $h(S) = S$. □

Going back to examples of definable sets:

- $\mathcal{Q} \coloneqq (\mathbb{Q}, <)$. Is the set $\mathbb{Q}^+$ of positive rationals $\emptyset$-definable? No.

  Proof. Take $h : \mathbb{Q} \to \mathbb{Q}$ by $q \to q + 1$.
  This is a bijection and preserves $<^{\mathcal{Q}}$ both ways, so it's an automorphism.
  Yet, $h(\mathbb{Q}^+) = \{q \in \mathbb{Q} : q > 1\} \neq \mathbb{Q}^+$. □

  Proposition $\mathbb{Q}^+$ is definable in $\mathcal{Q}$, in fact, it is $\{0\}$-definable.

  Proof. Indeed, $\varphi(x, y) \coloneqq x < y$ and $0 \in \mathbb{Q}$, then $\mathcal{Q}^+ = \{q \in \mathbb{Q} : \mathcal{Q} \models \varphi(0, q)\}$. □

- $\mathcal{R} \coloneqq (\mathbb{R}, 0, 1, +, \cdot)$. Is the set $\{\sqrt{2}, -\sqrt{2}\}$ 0-definable? Yes.

  Proof. $\varphi(x) \coloneqq x^2 \doteq 2$, where $x^2 = x \cdot x$. □

  Is $\sqrt{2}$ 0-definable? (I.e., is $\{\sqrt{2}\}$ 0-definable?) No but the technique of showing this, called quantifier elimination, is beyond this course

- $\mathcal{G} \coloneqq (V, E)$, where $V \coloneqq \mathbb{Z} \times \{0, 1\}$ and $(x, i)E(y, j) :\Leftrightarrow i = j$ and $|x - y| = 1$
  missing diagram
  Proposition. The relation of being of graph-distance 2 is 0-definable.
  Proof $\varphi(y_0, y_1) \coloneqq \exists z(y_0 \; E \; z \wedge z \; E \; y_1)$.
  Similarly, for each $n \in \mathbb{N}$, the relation $d_n(u, v) \subseteq V^2$ of being of graph-distance u is 0-definable:

  $$d_n(y_0, y_1) \coloneqq \exists z_1 \exists z_2 \ldots \exists z_{n-1}((y_0 \; E \; z_1) \wedge (z_1 \; E \; z_2) \wedge \ldots \wedge (z_{n-2} \; E \; z_{n-1}) \wedge (z_{n-1} \; E \; y_1))$$

  Note. We write one formula for each u (without any "…").
  Question. Is the relation $C(u, v) \subseteq V^2$ of being in the same connected component 0-definable?
  I.e. $\forall u, v \in V$, $C(u, v) :\Leftrightarrow \exists n \in \mathbb{N} \; d_n(u, v)$.

If you write $\exists n$, it's going to range over the set V, even though you purposefully gave it the name n.

Answer. No, in fact, this isn't definable. One uses the Compactness (or Completeness) theorem to show this.

The issue is that $\exists n \in \mathbb{N}\ d_n(u,v)$ isn't a formula.

Also we couldn't use the automorphism technique because any automorphism $h : \mathbb{G} \to \mathbb{G}$ will map the connected components to connected components.

For example, $h((x,i)) \coloneqq (x, 1-i)$ switches the components, but $h(C) = C$ because $\forall n, v \in V$.

$$C(u,v) \Leftrightarrow C(h(u), h(v))$$

Theories, models, and axiomatization

Definition. A σ-theory is just a (possibly empty) set of σ-sentences.
A σ-structure $\mathcal{M}$ is called a model of a σ-theory T if $\mathcal{M} \models \varphi$ for each $\varphi \in T$.
We write this as $\mathcal{M} \models T$, and read "$\mathcal{M}$ satisfies/models T".

Notation. For a σ-structure $\mathcal{M}$, let

$$\mathrm{Th}(\mathcal{M}) \coloneqq \{\varphi \in \text{ sentences}(\sigma) : \mathcal{M} \models \varphi\}.$$

For a σ-theory T, let $\mu_\sigma(T)$ denote the class (necessarily a proper class) of all models of T.

Math 318
Lecture 32
November 18 2020

Notation. For a σ-structure $\mathcal{M}$, let

$$\mathrm{Th}(\mathcal{M}) \coloneqq \{\varphi \in \text{ sentences}(\sigma) : \mathcal{M} \models \varphi\}.$$

For a σ-theory T, let $\mu_\sigma(T)$ denote the class (necessarily a proper class) of all models of T, i.e. all σ-structures $\mathcal{M}$ with $\mathcal{M} \models T$.

Definition. Let $\mathcal{C}$ be a class of σ-structures.
We say that a σ-theory T axiomatizes or is an axiomatization of $\mathcal{C}$ if $\mathcal{M}_\sigma(T) = \mathcal{C}$.
Also, given a σ-theory T, a σ-theory S is called an axiomatization of T if $\mathcal{M}_\sigma(S) = \mathcal{M}_\sigma(T)$, i.e. for each σ-structure $\mathcal{M}$, $\mathcal{M} \models S \Leftrightarrow \mathcal{M} \models T$.

Examples
- Let σ be a signature. then the class of all σ-structures with at most 798 elements is axiomatizable.
  In fact, it is axiomatizable with one sentence:

  $$\varphi_{\leq 798} \coloneqq \forall x_1\, \forall x_2 \ldots \forall x_{799} \bigvee_{1 \leq i < j \leq 799} x_i \doteq x_j.$$

  For any $n \in \mathbb{N}$, we can do this with the sentence φ
- The class of σ-structures with at least 798 elements is axiomatizable by the following sentence:

  $$\varphi_{\geq 798} \coloneqq \exists x_1\, \exists x_2 \ldots \exists x_{798} \bigwedge_{1 \leq i < j \leq 798} x_i \neq x_j.$$

  Similarly, we can do this for any $n \in \mathbb{N}$ by the sentence $\varphi_{\geq n}$.

- The class of σ-structures that have exactly 798 elements is axiomatized by the sentence $\varphi_{=798} \coloneqq \varphi_{\leq 798} \bigwedge \varphi_{\geq 798}$.
  Similarly, for each $n \in \mathbb{N}$, we have $\varphi_{=n}$

- The class of all infinite σ-structures is axiomatized by the theory

$$T_\infty \coloneqq \{\varphi_{\geq n} : n \in \mathbb{N}\}.$$

  By the Compactness theorem, this class isn't finitely axiomatizable.

- Is the class of finite σ-structures axiomatizable? The answer is no. The issue is that the naive attempt

$$\varphi_{\leq 1} \vee \varphi_{\leq 2} \vee \varphi_{\leq 3} \vee \varphi_{\leq 4} \dots$$

  isn't a finite word, in particular, isn't a formula.
  Another naive attempt is to write

$$\exists v \varphi_{\leq v}$$

  We have defined $\varphi_{\leq \text{a concrete number}}$ and for different numbers n and m, $\varphi_{\leq n}$ and $\varphi_{\leq m}$ are different sentences.
  Again, the "no" answer follows from the Compactness theorem.

- The class of undirected graphs without loops is axiomatized by

  (i) undirected: $\forall x \forall y \ (x \ E \ y \Rightarrow y \ E \ x)$.

  (ii) no loops: $\forall x \ \neg(x \ E \ x)$

- The class of partial orders, in the signature $\sigma_\leq \coloneqq (\leq)$, where $\leq$ is a binary relation symbol, is axiomatized by

  (i) reflexive: $\forall x (x \subseteq x)$

  (ii) antisymmetrix: $\forall x \forall y ((x \subseteq y \wedge y \subseteq x) \Rightarrow x \doteq y)$.

  (iii) transitive: $\forall x \forall y \forall z ((x \subseteq y \wedge y \subseteq z) \Rightarrow x \subseteq z)$.

- The class of all groups in the signature $\sigma_{\text{gp}} \coloneqq (1, \bullet, (\ )^{-1})$, where 1 is a constant symbol, $\bullet$ is a binary function symbol, and $(\ )^{-1}$ is a unary function symbol, is axiomatized by:

  (i) associativity of $\bullet$: $\forall x \forall y \forall z (x \bullet (y \bullet z) \doteq (x \bullet y) \bullet z)$.

  (ii) 1 is the identity: $\forall x (1 \bullet x = x \wedge x \bullet 1 = x)$.

  (iii) $(\ )^{-1}$ is the $\bullet$-inverse: $\forall x (x \bullet x^{-1} = 1 \wedge x^{-1} \bullet x = 1)$.

- An (undirected) graph $G \coloneqq (V, E^{\mathcal{G}})$ is called bipartite if $\exists$ a partition $V = V_1 \cup V_2$, with $V_1 \cap V_2 = \emptyset$, s.t. $V_1 \times V_1 \cap E^{\mathcal{G}} = \emptyset$ and$V_2 \times V_2 \cap E^{\mathcal{G}} = \emptyset$.
  missing diagram
  Is the class of bipartite graphs axiomatizable? Yes.
  The definition itself is not expressible by a formula, the naive attempt is $\exists v_1 \exists v_2 \ \forall x \in v_1 \forall y \in v_1 \ (x \not{E} y)$

  – $\exists v_1 \exists v_2$ range over vertices and not sets of vertices

  – $\forall x \in v_1 \forall y \in v_1$ isn't in signature

  We cannot quantify over all subsets of V, i.e. write $\forall V_1 \subset V \dots$
  However, it's an easy theorem in graph theory that a graph is bipartite $\Leftrightarrow$ it has no odd

cycles.
And the latter statement can be axiomatized as follows: for each $n \in \mathbb{N}$

$$\varphi_n \coloneqq \exists x_1 \exists x_2 \ldots \exists x_n ((x_1 \; E \; x_2) \wedge (x_2 \; E \; x_3) \wedge \ldots \wedge (x_{n-1} \; E \; x_n) \wedge (x_n \; E \; x_1)$$

The theory $T_{\text{bip}} \coloneqq \{\neg\varphi_{2k+1} : k \in \mathbb{N}\} \cup \underbrace{\text{Graphs}}_{\substack{\text{the two axioms for} \\ \text{undirected graphs}}}$
Then $\forall \mathcal{G} \coloneqq (V, E^{\mathcal{G}})$, $\mathcal{G} \models T_{\text{bip}} \Leftrightarrow \mathcal{G}$ has no odd cycle.
Thus, T_{bip} axiomatizes the class of bipartite graphs.

- The class of connected graphs isn't axiomatizable and the tool to show this is the Compactness theorem.
  Same for disconnected graphs. Try attempting to axiomatize to appreciate the difficulty.

The compactness theorem is a way to show that a class is not axiomatizable. You can also sometimes use Gödel's Completeness Theorem

Math 318
Lecture 33
November 20 2020

Important examples of theories.

- ZFC is an infinite theory in the signature $\sigma_{\text{set}} \coloneqq (\ni)$, where $\ni$ is a binary relation symbol. All the axioms of ZFC are σ_{set}-sentences.
- PA - Peano Arithmetic is a theory in the signature $\sigma_{\text{arithm}} \coloneqq (0, S, +, \cdot)$, where 0 is a constant symbol, S is a unary function symbol, and $+$, $\cdot$ are binary function symbols. This theory has infinitely-many axioms:

(PA1) $\forall x[\neg S(x) \doteq 0]$ - 0 is not a successor
(PA2) $\forall x \forall y[S(x) \doteq S(y) \to x \doteq y]$ - successor is an injective function
(PA3) $\forall x[x + 0 \doteq x]$ - 0 is the $+$ − identity (because it follows from other axioms that $+$ is commutative)
(PA4) $\forall x \forall y[S(x + y) \doteq x + S(y)]$ - the successor and $+$ interact in the standart way.
(PA5) $\forall x[x \cdot 0 \doteq 0]$ - multiplication by 0
(PA6) $\forall x \forall y[x \cdot S(y) \doteq x \cdot y + x]$ - the successor, $+$, and $\cdot$ interact in the standard way
(PA7) (Axiom schema of induction) For each σ_{arithm}-formula $\varphi(x, \vec{y})$, where x is a variable and $\vec{y}$ is a vector of variables, the following is an axiom:

$$\forall \vec{y} \Big[\big(\varphi(0, \vec{y}) \wedge \forall x \big[\varphi(x, \vec{y}) \to \varphi(S(x), \vec{y})\big]\big) \to \forall x \varphi(x, \vec{y}) \Big]$$

Clearly, $\mathcal{N} \coloneqq (\mathbb{N}, 0, S, +, \cdot) \models \text{PA}$. But $\text{Th}(\mathcal{N})$ (complete) is much larger than PA (not complete).

Semantic implication (satisfiability), consistency, and completeness.

In general, syntax refers to symbolic notation, for instance, writing the symbol v to denote a variable writing "Anush".
Semantics, on the other hand, refers to content, for example, the value of the variable v, which may be, say, a matrix of numbers, and the person, whose name is "Anush".
Semantic aspect of logic is model theory, while syntactic aspect is proof theory.

Definition. We say that a σ-theory T satisfies (or semantically implies) a σ-sentence φ if $\forall$ models $\mathcal{M}$ of T, $\mathcal{M} \models \varphi$. We denote this by $T \models \varphi$.

To show $T \models \varphi$, we need to fix an arbitrary model $\mathcal{M}$ of T and show that φ holds in $\mathcal{M}$.

Example. Denoting by GROUPS the theory of groups (the mentioned axioms) in the signature $\sigma_{\text{gp}} := (1, \cdot, (\,)^{-1})$, we see that

$$\text{GROUPS} \models \forall x \forall y \forall y' \big[(y \cdot x \doteq 1 \wedge x \cdot y' \doteq 1) \to y \doteq y' \big]$$

Proof. Fix an arbitrary group $\mathcal{G} := (G, 1^{\mathcal{G}}, \cdot^{\mathcal{G}}, (\,)^{-1^{\mathcal{G}}})$.
To verify the sentence, fix arbitrary $g, h, h' \in G$ and suppose that $h \cdot^{\mathcal{G}} g = 1^{\mathcal{G}}$ and $g \cdot^{\mathcal{G}} h' = 1^{\mathcal{G}}$.
We multiply $h \cdot g = 1^{\mathcal{G}}$ by h' on the right:

$$\begin{aligned}
(h \cdot^{\mathcal{G}} g) \cdot^{\mathcal{G}} h' &= 1^{\mathcal{G}} \cdot^{\mathcal{G}} h' \\
h \cdot^{\mathcal{G}} (g \cdot^{\mathcal{G}} h') &= 1^{\mathcal{G}} \cdot^{\mathcal{G}} h' && \text{[by associativity axiom]} \\
h \cdot^{\mathcal{G}} 1^{\mathcal{G}} &= 1^{\mathcal{G}} \cdot^{\mathcal{G}} h' && \text{[by the other equality]} \\
h &= h' && \text{[by the identity axiom]}
\end{aligned}$$

Thus, the sentence is indeed true in $\mathcal{G}$ □

Definition. A σ-theory T is said to be satisfiable if it has a model.
We say that T is finitely satisfiable if every finite $T' \subseteq T$ is satisfiable.

Observation. For a σ-theory T, these are equivalent:

(1) T is satisfiable.

(2) $T \not\models \bot$, where $\top := \forall x (x \doteq x)$ and $\bot := \neg \top$

(3) $T \not\models \varphi$, for some σ-sentence φ.

Compactness Theorem (Gödel 1929, also independently, Maltsev)
If a σ-theory T is finitely satisfiable, then it is satisfiable.

Math 318
Lecture 34
November 23 2020

Compactness Theorem (Gödel 1929, also independently, Maltsev)
If a σ-theory T is finitely satisfiable, then it is satisfiable.

This theorem is the bread-and-butter of model theory, and has many applications in other areas of math, especially in combinatorics, algebra, and algebraic geometry.

Corollary. If a σ-theory T has arbitrarily large finite models, then it has an infinite model.

Proof. Let $\overline{\sigma} := \sigma \cup \{c_n : n \in \mathbb{N}\}$, where the c_n are "fresh" constant symbols, i.e. symbols that don't appear in σ.
For each $n \geq 2$, let

$$\varphi_n := \bigwedge_{0 \leq i < j < n} (c_i \neq c_j)$$

let $\overline{T} := T \cup \{\varphi_n : n \geq 2\}$.

Claim. $\overline{T}$ is finitely satisfiable.
Proof of claim. Let $T' \subseteq \overline{T}$ be finite.
Let $n :=$ max s.t. $\varphi_n \in T'$.
Let $\mathcal{M} \models T$ with $|\mathcal{M}| \geq n$.
Note: $\mathcal{M}$ is a σ-structure.
We let $\overline{\mathcal{M}}$ be the expansion of $\mathcal{M}$ to a $\overline{\sigma}$-structure by interpreting the constant symbols $c_0, c_1, \ldots, c_{n-1}$ as pairwise distinct elements of $\mathcal{M}$, and the rest of $c_n, c_{n+1}, c_{n+2}, \ldots$ interpreted in some way (doesn't matter how).
By definition, $\overline{\mathcal{M}} \models T'$, so T' is satisfiable. ($\square$ claim)

By the Compactness theorem, $\overline{T}$ has a model, $\mathcal{A} \models \overline{T}$.
For any $i < j$, $c_i^{\mathcal{A}} \neq c_j^{\mathcal{A}}$, hence A is infinite.
The reduct of $\mathcal{A}$ to σ is a model of T.

$\square$

This corollary is equivalent to:

Corollary. If C is a class of σ-structures that contains only finite structures but of arbitrarily large size, then C is not axiomatizable.

In particular, the class of all finite groups (graphs, fields, partial orders, etc.) is not axiomatizable.

Another application. The class $\mathcal{C}$ of all connected graphs is not axiomatizable.

Proof. Let $\sigma_{\text{gr}} := (E)$. Let $\sigma := (E, a, b)$, where a and b are constant symbols.
Suppose towards a contradiction that $\mathcal{C}$ is axiomatized by a σ_{gr}-theory T, i.e. for any graph $\mathcal{G}$, $\mathcal{G}$ is connected $\Leftrightarrow \mathcal{G} \models T$.
For each $n \geq 2$, define the σ-sentence $\varphi_n := d_{\geq n}(a, b)$
Recall that $d_{\geq n}(x, y)$ is a formula that says that the graph-distance between x and y is at least n.)
Let $T' := T \cup \{\varphi_n : n \geq 2\}$.
It is easy to see that T' is finitely satisfiable, for instance, by graphs of the form missing diagram.
Hence, by the Compactness theorem, T' has a model $\mathcal{G}$ with vertices $a^{\mathcal{G}}$ and $b^{\mathcal{G}}$ whose graph-distance is not finite, in other words, there is not path between $a^{\mathcal{G}}$ and $b^{\mathcal{G}}$ in $\mathcal{G}$.
Thus $\mathcal{G}$ is disconnected, contradicting that $\mathcal{G} \models T$. $\square$

Corollary If a σ-theory T is finitely axiomatizable (i.e. there is a finite σ-theory S s.t. $\forall\sigma$-structure $\mathcal{M}$, $\mathcal{M} \models T \Leftrightarrow \mathcal{M} \models S$), then $\exists$ a finite axiomatization $T' \subseteq T$.

Proof. We will use the following equivalent form of the Compactness theorem (from HW8).

$$\text{If } T \models \varphi \text{ then } \exists \text{ finite } T' \subseteq T, T' \models \varphi.$$

Suppose T has a finite axiomatisation S. Let

$$\varphi := \bigwedge_{\psi \in S} \psi,$$

which is indeed a sentence because S is finite.
Then $T \models \varphi$ because every model of T satisfies S.
Then $\exists T' \subseteq T$ finite with $T' \models \varphi$.
This T' is an axiomatization of T.
Indeed, for any σ-structure $\mathcal{M}$, if $\mathcal{M} \models T$ then trivially $\mathcal{M} \models T'$.
Conversely, if $\mathcal{M} \models T'$, then $\mathcal{M} \models \varphi$, hence $\mathcal{M} \models S$ so $\mathcal{M} \models T$. $\square$

An application. Let $T_\infty \coloneqq \{\varphi_n : n \geq 1\}$, where $\varphi_n \coloneqq \exists x_1, \ldots, \exists x_n \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j$.

This axiomatized the class of infinite σ-structures for any fixed σ.
T_∞ is not finitely axiomatizable.

Proof. If it were, there would be $T' \subseteq T_\infty$ finite that axiomatizes it.
But then, letting $u \coloneqq \max \varphi_n \in T'$, we take a σ-structure that has exactly $n+2$ elements and see that it satisfies T', while being finite, a contradiction. □

Math 318
Lecture 35
November 25 2020

Recall that we are defining a semantic version of implication, consistency, and completeness.
We've already defined semantic implication $T \models \varphi$.
We've also defined semantic consistency as satisfiability of T, i.e. saying "T is satisfiable" is the same as saying "T is semantically consistent".

Definition. Call a σ-theory T semantically complete if for each σ-sentence φ, $T \models \varphi$ or $T \models \neg\varphi$.
Call T maximally complete if for each σ-sentence φ, $\varphi \in T$ or $\neg\varphi \in T$. Finally, call a σ-theory $\overline{T} \supseteq T$ a semantic completion of T if it is satisfiable and semantically complete.

Examples
- For any σ-structure $\mathcal{A}$, $\mathrm{Th}(\mathcal{A}) \coloneqq \{\varphi \in \text{ Sentences}(\sigma) : \mathcal{A} \models \varphi\}$ is maximally complete satisfiable σ-theory ($\mathcal{A}$ is a model of $\mathrm{Th}(\mathcal{A})$).
  In particular, for $\mathcal{N} \coloneqq (0, S, +, \cdot)$, $\mathrm{Th}(\mathcal{N})$ is maximally complete and satisfiable.
- GROUPS is not semantically complete because, for example, for the sentence $\varphi \coloneqq \exists x(x \neq 1 \wedge x \cdot x \cdot x \doteq 1)$, there are groups that satisfy it (e.g. $\mathbb{Z}/_{3\mathbb{Z}} \coloneqq \{0, 1, 2\}$ with addition mod 3) and there are groups that don't (e.g. $\mathbb{Z}$).

Gödel's Incompleteness Theorem. Peano Arithmetic PA is not semantically complete, i.e. $\exists$ $\sigma_{\text{arithm.}}$-sentence γ s.t. $PA \not\models \gamma$ and PA $\not\models \neg\gamma$.
(We may assume WLOG, $\mathcal{N} \models \gamma$.)
Moreover, there is no computer-recognizable $\sigma_{\text{arithm.}}$-theory T s.t. $\mathcal{N} \models T$ is semantically complete.
By computer recognizable we mean that there is a program that given a sentence φ, answers Yes if $\varphi \in T$, and No, otherwise.

Observation. Any satisfiable σ-theory T has a satisfiable maximal completion $\overline{T}$, namely, take any model $\mathcal{M} \models T$, and let $\overline{T} \coloneqq \mathrm{Th}(\mathcal{M})$.

Definition. Call σ-structures $\mathcal{A}, \mathcal{B}$ elementarily equivalent (I'd personally call it first-order equivalent), denoted by $\mathcal{A} \equiv \mathcal{B}$, if $\mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$, i.e. for each σ-sentence φ,

$$\mathcal{A} \models \varphi \Leftrightarrow \mathcal{B} \models \varphi.$$

We already know that $\mathcal{A} \cong \mathcal{B} \Rightarrow \mathcal{A} \equiv \mathcal{B}$.
But the converse is very much not true.
For example, it can be proven that $\mathcal{R} \coloneqq (\mathbb{R}, <)$ and $\mathcal{Q} \coloneqq (\mathbb{Q}, <)$ are elementarily equivalent, yet they cannot be isomorphic because $\mathcal{Q}$ is countable, while $\mathcal{R}$ isn't.

Proposition. A σ-theory T is semantically complete if and only if any models $A, B \models T$ are elementarily equivalent.

Proof.
- ($\Rightarrow$): Suppose T is semantically complete, fix $\mathcal{A}, \mathcal{B} \models T$ and a σ-sentence φ.
  We want to show that $\mathcal{A} \models \varphi \Leftrightarrow \mathcal{B} \models \varphi$.
  But we know that $T \models \varphi$ or $T \models \neg\varphi$, so because $\mathcal{A}, \mathcal{B} \models T$, either, $\mathcal{A}, \mathcal{B} \models \varphi$ or $\mathcal{A}, \mathcal{B} \models \neg\varphi$
- ($\Leftarrow$): Suppose for any $\mathcal{A}, \mathcal{B} \models T$, $\mathrm{Th}(A) = \mathrm{Th}(B)$.
  Fix a σ-sentence φ.
  We show that if $T \not\models \varphi$, then $T \models \neg\varphi$.
  Suppose $T \not\models \varphi$.
  Then there is a model $\mathcal{A} \models \neg\varphi$.
  But then all models of T must satisfy $\neg\varphi$, so $T \models \neg\varphi$.

□

Syntactic aspect: syntactic versions of implication, consistency, and completeness
We would like to define what it means to "prove" a σ-sentence φ from a σ-theory T.
This will be denoted $T \vdash \varphi$.
Intuitively, a proof is a sequence of σ-formulas s.t. each formula in this sequence is an "axiom" or can be "deduced" previous formulas in the sequence.

Math 318
Lecture 36
November 27 2020

Syntactic aspect: syntactic versions of implication, consistency, and completeness
We would like to define what it means to "prove" a σ-sentence φ from a σ-theory T.
This will be denoted $T \vdash \varphi$.
Intuitively, a proof is a sequence of σ-formulas s.t. each formula in this sequence is an "axiom" or can be "deduced" previous formulas in the sequence.
We begin with deifning the (infinitely-many) axioms of first-order logic.

Axioms of First-order Logic.

Definition. Let φ be a σ-formula and t be a σ-term.
We say that t is free for variable v in φ (also, we say that t is ok to be plugged-in for v) if v and any other variable in t are not quantified in φ.
In this case, we denote by $\varphi(t \underset{\text{replaces}}{\sqcup} v)$ the formula obtained from φ by replacing all the occurrences of v with t.

Examples
- $\sigma \coloneqq \sigma_{\text{arithm}} \coloneqq (0, S, +, \cdot)$, $t \coloneqq S(0) + u$, $\varphi \coloneqq \forall x(x + v \doteq v)$.
  Then t is free for v in φ, but t is not free for x in φ, and $\varphi(t/v) \coloneqq \forall x(x + (S(0) + u) \doteq (S(0) + u))$

Conventions. Whenever we write $\varphi(t/v)$ it is assumed that t is free for v in φ. Also, we will take $\varphi \wedge \psi$, $\varphi \vee \psi$, $\exists x\varphi$ as abbreviations for $\neg(\varphi \Rightarrow \neg\psi)$, $(\neg\varphi) \Rightarrow \psi$, $\neg\forall x\neg\varphi$.

For each fixed signature σ, we have its own set of first-order axioms, which we denote by $\mathrm{Axioms}(\sigma)$. Here they are:

Propositional / Boolean Axioms. The following are axioms for each σ-formula φ, ψ, χ

1. If-true-then-implied: $\varphi \Rightarrow (\psi \Rightarrow \varphi)$
2. Implication-is-transitive $(\varphi \Rightarrow \psi) \Rightarrow \big(((\varphi \Rightarrow (\psi \Rightarrow \chi)) \Rightarrow (\varphi \Rightarrow \chi)\big)$.
   Equivalently $((\varphi \Rightarrow \psi) \wedge ((\varphi \wedge \psi) \Rightarrow \chi)) \Rightarrow (\varphi \Rightarrow \chi)$

3. Proof-by-contradiction: $(\neg\varphi \Rightarrow \psi) \Rightarrow ((\neg\varphi \Rightarrow \neg\psi) \Rightarrow \varphi)$
   Equivalently $((\neg\varphi \Rightarrow \psi) \wedge (\neg\varphi \Rightarrow \neg\psi)) \Rightarrow \varphi$

Annoying remark. Some of these formulas technically may not be legal even if φ, ψ, χ are. For example, $\varphi := \forall x(x \doteq x)$, then $\varphi \Rightarrow (\psi \Rightarrow \varphi)$ is $(\forall x(x \doteq x)) \Rightarrow \big(\psi \Rightarrow (\forall x(x \doteq x))\big)$, so x is quantified twice.
We make a convention to use legal versions of these axioms by changing the quantified variables when needed.
For example: $(\forall x(x \doteq x)) \Rightarrow \big(\psi \Rightarrow (\forall y(y \doteq y))\big)$.

Quantifier Axioms. The following are axioms for each σ-formula φ, σ-term t that is free for v in φ

4. Instantiation: $(\forall v\varphi) \Rightarrow \varphi(t/v)$
5. Generalization: $\varphi \Rightarrow (\forall v\varphi)$

The annoying remark also holds here.

Equality Axiom.

6. Equality-is-equivalence-relation:
   (i) Reflexivity: $u \doteq u$, for any variable u
   (ii) Symmetry: $(u \doteq v) \Rightarrow (v \doteq u)$
   (iii) Transitivity: $(u \doteq v) \Rightarrow ((v \doteq w) \Rightarrow (u \doteq w))$
   Equivalently, $((u \doteq v) \wedge (v \doteq w)) \Rightarrow (u \doteq w)$
7. Functions-respect-equality: For every n-ary function symbol f and vectors of variables $\vec{x}, \vec{y}$ of length n,
$$\underbrace{(\vec{x} \doteq \vec{y})}_{x_0 \doteq y_0 \wedge x_1 \doteq y_1 \wedge \ldots \wedge x_{n-1} \doteq y_{n-1}} \Rightarrow (f(\vec{x}) \doteq f(\vec{y}))$$
8. Relations-respect-equality: For every n-ary relation symbol $\mathcal{R}$ in σ and vectors of variables $\vec{x}, \vec{y}$ of length n,
$$(\vec{x} \doteq \vec{y}) \Rightarrow (\mathcal{R}(\vec{x}) \Rightarrow \mathcal{R}(\vec{y}))$$

Math 318
Lecture 37
November 30 2020

Rule of inference of the first-order logic
Modus Ponens: for all σ-formulas φ, ψ,

$$\varphi, \varphi \Rightarrow \psi \overset{MP}{\rightsquigarrow} \psi$$

Definition. Let T be a set of σ-formulas.
We say that T proves a σ-formula φ, and we denote this by $T \vdash \varphi$, if there is a finite sequence $\varphi_0\ \varphi_1\ \varphi_2\ \ldots\ \varphi_n$ of σ-formulas with $\varphi_n = \varphi$ and for each φ_k, $k \leq n$,

- either $\varphi_k \in \text{Axiom}(\varphi)$
- or $\varphi_k \in T$

- or φ_k follows from the previous φ_i by Modus Ponens (MP),
  i.e. $\exists i, j < k$ s.t. $\varphi_j = (\varphi_i \Rightarrow \varphi_k)$.
  In this case we say that φ_k is obtained from i, j by MP.

We call any such sequence $\varphi_0\ \varphi_1\ \ldots\ \varphi_n$ a proof from T.
If $T = \emptyset$, we just write $\vdash \varphi$ instead of $\emptyset \vdash \varphi$.

Definition. We say that a σ-structure $\mathcal{A}$ satisfies a σ-formula if $\mathcal{A} \models \forall \vec{x} \varphi$, where $\vec{x}$ is a vector of variables so that $\varphi[\vec{x}]$ is an extended formula.

Proposition (Soundness). For any set T of σ-formulas and a σ-formula φ, if $T \vdash \varphi$ then $T \models \varphi$, i.e. $\mathcal{A} \models \varphi$ for every σ-structure $\mathcal{A} \models T$.

Proof. Each $\varphi \in \text{Axiom}(\sigma)$ and each $\varphi \in T$ satisfies this and MP preserves satisfiability, i.e. if $\mathcal{A} \models \varphi$ and $\mathcal{A} \models (\varphi \Rightarrow \psi)$ then $\mathcal{A} \models \psi$. □

Proposition. Let θ, χ be σ-formulas.

(a) Self-implication $\vdash \theta \Rightarrow \theta$

(b) Everything-implies-an-axiom: $\chi \vdash \theta \Rightarrow \chi$.

Proof. (a)

(0) Axiom 2 for $\varphi \coloneqq \chi \coloneqq \theta$, $\psi \coloneqq (\theta \Rightarrow \theta)$

$$(\theta \Rightarrow (\theta \Rightarrow \theta)) \Rightarrow \big[[\theta \Rightarrow ((\theta \Rightarrow \theta) \Rightarrow \theta)] \Rightarrow (\theta \Rightarrow \theta)\big]$$

(1) Axiom 1 for $\varphi \coloneqq \psi \coloneqq \theta$

$$\theta \Rightarrow (\theta \Rightarrow \theta)$$

(2) MP applied to (1), (0)

$$\big[\theta \Rightarrow ((\theta \Rightarrow \theta) \Rightarrow \theta)\big] \Rightarrow (\theta \Rightarrow \theta)$$

(3) Axiom 1 for $\varphi \coloneqq \theta$, $\psi \coloneqq (\theta \Rightarrow \theta)$

$$\vdash \theta \Rightarrow ((\theta \Rightarrow \theta) \Rightarrow \theta)$$

(4) MP applied to (3), (2)

$$\vdash \theta \Rightarrow \theta$$

□

Proof. (b)

(0) Axiom 1 for $\varphi \coloneqq \chi$ and $\psi \coloneqq \theta$

$$\vdash \chi \Rightarrow (\theta \Rightarrow \chi)$$

(1) $\chi \in \{\chi\}$ so

$$\{\chi\} \vdash \chi$$

(2) MP applied to (0), (1)

$$\{\chi\} \vdash \theta \Rightarrow \chi$$

□

Deduction theorem. For any set T of σ-formulas, for any σ-formulas χ, φ,

$$T, \chi \vdash \varphi \Leftrightarrow T \vdash (\chi \Rightarrow \varphi).$$

Proof. ($\Leftarrow$) Suppose $T \vdash (\chi \Rightarrow \varphi)$. We also have $T, \chi \vdash \chi$.
By MP, we get $T, \chi \vdash \varphi$.
($\Rightarrow$) Suppose that $T, \chi \vdash \varphi$ and let $\varphi_0\ \varphi_1\ \ldots\ \varphi_n = \varphi$ be a proof.
We prove that $T \vdash (\chi \Rightarrow \varphi_n)$ by induction on n.

- Case 1. $\varphi_n \in T \cup \text{Axiom}(\sigma)$.
  Then by (ii) of the previous proposition, we have that $T \vdash (\chi \Rightarrow \varphi_n)$.
- Case 2. φ_n is obtained from φ_i, φ_j by MP.
  So $\varphi_j \coloneqq (\varphi_i \Rightarrow \varphi_n)$.
  By induction, $T \vdash (\chi \Rightarrow \varphi_i)$ and $T \vdash (\chi \Rightarrow \varphi_j)$, i.e. $T \vdash (\chi \Rightarrow (\varphi_i \Rightarrow \varphi_n))$.
  Axiom 2 for $\varphi \coloneqq \chi$, $\psi \coloneqq \varphi_i$, $\chi \coloneqq \varphi_n$ is $\vdash (\chi \Rightarrow \varphi_i) \Rightarrow \big[(\chi \Rightarrow (\varphi_i \Rightarrow \varphi_n) \Rightarrow (\chi \Rightarrow \varphi_n)\big]$.
  Two applications of MP yields $T \vdash (\chi \Rightarrow \varphi_n)$.

□

Proposition. Let φ, ψ be σ-formulas, v be a variable, and t a σ-term that is free (i.e. OK to be plugged in) for v in φ.
The following formulas are provable from the empty theory.

(a) Double-negation-elimination: $\neg\neg\varphi \Rightarrow \varphi$

(b) Double-negation-introduction: $\varphi \Rightarrow \neg\neg\varphi$

(c) If-false-then-implies: $\neg\varphi \Rightarrow (\varphi \Rightarrow \psi)$

(d) Forward-contrapositive: $(\varphi \Rightarrow \psi) \to (\neg\psi \Rightarrow \neg\varphi)$

(e) Truth $\top \coloneqq \forall v(v \doteq v)$

(f) Contradiction-implies-everything: $(\neg\varphi \wedge \varphi) \Rightarrow \psi$

(g) Falsity-implies-everything: $\bot \Rightarrow \psi$, where $\bot \coloneqq \neg\top$

(h) Witness-implies-existence: $\varphi(t/v) \Rightarrow \exists v\varphi$

Proof. (i) By Deduction Theorem, it is enough to show $\neg\neg\varphi \vdash \varphi$
Axiom 3 for $\varphi \coloneqq \varphi$, $\psi \coloneqq \neg\varphi$ is $(\neg\varphi \Rightarrow \neg\varphi) \Rightarrow \big[(\neg\varphi \Rightarrow \neg\neg\varphi) \Rightarrow \varphi\big]$.
By the previous proposition, we have $\vdash (\neg\varphi \Rightarrow \neg\varphi)$ and $\neg\neg\varphi \vdash (\neg\varphi \Rightarrow \neg\neg\varphi)$, so two applications of MP yield $\neg\neg\varphi \vdash \varphi$.
⋮
The remaining parts are also not hard and are left as an exercise (you can read the proofs in my logic lecture notes). □

Math 318
Lecture 38
December 2 2020

Recall that semantic consistence for a theory T is defined to be satisfiability, and semantic completeness is this: for each sentence φ, $T \models \varphi$ or $T \models \neg\varphi$

Definition T is said to be (syntactically) <u>consistent</u> if $T \nvdash (\varphi \wedge \neg\varphi)$ for some σ-sentence φ.
T is called <u>syntactically complete</u> if for each σ-sentence φ, $T \vdash \varphi$ or $T \vdash \neg\varphi$.

Proposition. For each σ-theory T, the following are equivalent

(i) T is syntactically consistent.

(ii) $T \nvdash \bot$

(iii) $T \nvdash \varphi$, for some σ-sentence φ.

Proof.

- $\neg(ii) \Rightarrow \neg(i)$. $T \vdash \bot$, then by (g) of the previous proposition and MP, $T \vdash (\varphi \wedge \neg\varphi)$ for any σ-sentence φ.
- $\neg(iii) \Rightarrow \neg(ii)$. Trivial
- $\neg(i) \Rightarrow \neg(iii)$. $T \vdash (\varphi \wedge \neg\varphi)$ for some sentence φ. Then for any σ-sentence ψ, we have by (f) of previous proposition that $\vdash ((\varphi \wedge \neg\varphi) \Rightarrow \psi)$, hence MP yields $T \vdash \psi$, so $\neg(iii)$.

□

Lemma (about consistent theories). Let T be a σ theory and let φ be a σ-sentence.

(a) $T \cup \{\varphi\}$ is syntactically inconsistent $\Leftrightarrow T \vdash \neg\varphi$.

(b) If T is syntactically consistent then at least one of $T \cup \{\varphi\}$ and $T \cup \{\neg\varphi\}$ is syntactically consistent.

Proof.

- Proof (a)
  - ($\Rightarrow$). Suppose $T \cup \{\varphi\}$ is syntactically inconsistent, equivalently $T \cup \{\varphi\} \vdash \bot$.
    By the Deduction Theorem, $T \vdash (\varphi \Rightarrow \bot)$.
    By (d) of the previous proposition, $T \vdash (\neg\bot) \Rightarrow \neg\varphi$.
    But $\neg\bot = \neg\neg\top$ by definition, so using (a) of the previous proposition and MP, we get $T \vdash (\top \implies \neg\varphi)$.
    But by (e) of the previous proposition, $T \vdash \top$, hence by MP, $T \vdash \neg\varphi$.
  - ($\Leftarrow$) Suppose $T \vdash \neg\varphi$.
    Then $T \cup \{\varphi\} \vdash \neg\varphi$ and $T \cup \{\varphi\} \vdash \varphi$, so $T \vdash \varphi \wedge \neg\varphi$.
    The last fact uses: $T \vdash \psi_1$ and $T \vdash \psi_2$ then $T \vdash (\psi_1 \wedge \psi_2)$, which is left as an exercise.
- Suppose both $T \cup \{\varphi\}$ and $T \cup \{\neg\varphi\}$ are syntactically inconsistent.
  Then by (a) of this lemma, $T \vdash \neg\varphi$ and $T \vdash \neg\neg\varphi$.
  By (a) of the previous proposition, $\vdash (\neg\neg\varphi \Rightarrow \varphi)$, so MP yields, $T \vdash \varphi$.
  Hence, $T \vdash (\varphi \wedge \neg\varphi)$, i.e., T is syntactically inconsistent.

□

Proposition. Any syntactically consistent σ-theory T admits a (typically non-unique) syntactically consistent maximal σ-theory $\overline{T} \supseteq T$, i.e. for any σ-sentence φ, either $\varphi \in \overline{T}$ or $\neg\varphi \in \overline{T}$ and $\overline{T}$ is syntactically consistent.

Proof.

- Proof 1. By Zermelo's theorem, well-order the set of all σ-sentences, in fact, get a bijection from some ordinal λ to it, i.e. an ennumeration $(\varphi_\alpha)_{\alpha<\lambda}$. Recursively define $(T_\alpha)_{\alpha\leq\lambda}$ as follows:

$$T_\alpha \coloneqq \begin{cases} T \cup \bigcup_{\beta<\alpha} T_\beta \cup \{\varphi_\alpha\} & \text{if this is consistent} \\ T \cup \bigcup_{\beta<\alpha} T_\beta \cup \{\neg\varphi_\alpha\} & \text{otherwise} \end{cases}$$

Note that syntactic compactness theorem implies that an increasing union of consistent theories is consistent.
Using this and part (b) of the consistency lemma, we show by transfinity induction that T_α is consistent for each $\alpha < \lambda$.
Thus $\overline{T} \coloneqq \bigcup_{\alpha<\lambda} T_\alpha$ is also consistent as it's an increasing union of consistent theories.
Moreover, $\overline{T}$ is maximal: for any σ-sentence φ, $\exists \alpha < \lambda$ with $\varphi_\alpha = \varphi$ and $\overline{T} \supseteq T_\alpha$ contains either φ_α or $\neg\varphi_\alpha$, by definition.

- Proof 2. Apply Zorn's lemma to $\mathcal{T} \coloneqq \{T' \supset T : T' \text{ is a syntactically consistent } \sigma\text{-theory }\}$ with respect to $\subseteq$ as the partial order, after verifying the chain condition.
Let $\overline{T} \in \mathcal{T}$ be a $\subseteq$-maximal element given by Zorn's lemma.
Then $\overline{T}$ is consistent and also a maximal σ-theory: for each σ-sentence φ, at least on of $\overline{T} \cup \{\varphi\}$ and $\overline{T} \cup \{\neg\varphi\}$ is consistent, so the $\subseteq$-maximality implies that $\varphi \in \overline{T}$ or $(\neg\varphi) \in T$.

□

Math 318
Lecture 39
December 3 2020

Semantic-Syntactic Duality: The Completeness of First-order Logic

Notions	**Syntactic** (Proof-theoretic)	**Semantic** (Model-theoretic)
Consistency	$T \nvdash \bot :\Leftrightarrow \nexists$ a proof	$T \not\models \bot$, i.e. T is satisfiable $:\Leftrightarrow \exists$ model
Implication	$T \vdash \varphi :\Leftrightarrow \exists$ a proof	$T \models \varphi :\Leftrightarrow \forall$ models ...
Completeness	$\forall \varphi$, $T \vdash \varphi$ or $T \vdash \neg\varphi$	$\forall \varphi, T \models \varphi$ or $T \models \neg\varphi$
Compactness	$T \vdash \varphi \Longrightarrow \exists$ finite $T_0 \subseteq T, T_0 \vdash \varphi$	$T \models \varphi \Longrightarrow \exists$ finite $T_0 \subseteq T, T_0 \models \varphi$

Recall that if T is satisfiable, then it is syntactically consistent.
This is a triviality, but the converse is a deep theorem:

Theorem (the Completeness of FOL, Gödel 1929). If a σ-theory T is syntactically consistent, then T is satisfiable.
In fact, there is a model $\mathcal{M} \models T$ of cardinality $\leq \max\{\aleph_0, |\sigma|\}$, i.e. $|\mathcal{M}| \leq \max\{\aleph_0, |\sigma|\}$.
⇕
Theorem (Syntactic-Semantic Duality). For any σ-theory T and a σ-sentence φ,

$$T \vdash \varphi \text{ if and only if } T \models \varphi.$$

In particular, the two columns in the above table are the same.

Proof. ($\Rightarrow$). By the soundness theorem.
($\Leftarrow$). We prove the contrapositive: Suppose $T \nvdash \varphi$.
Then T is consistent and by the consistency lemma, $T \cup \{\neg\varphi\}$ is consistent.
But the Completeness theorem, $T \cup \{\neg\varphi\}$ has a model $\mathcal{M}$.
But then $\mathcal{M} \models T$ and $\mathcal{M} \models \neg\varphi \Rightarrow T \not\models \varphi$. □

(Semantic) Compactness Theorem. If a σ-theory T is finitely satisfiable, then it is satisfiable.
In fact, it has a model of cardinality $\leq \max\{\aleph_0, |\sigma|\}$.

Proof. If T is finitely satisfiable, then by the soundness theorem, every finite $T_0 \subseteq T$ is syntactically consistent.
But then T is consistent by the syntactic compactness theorem, so by the Completeness theorem, T has a model of cardinality $\leq \max\{\aleph_0, |\sigma|\}$ □

Corollary. Suppose a σ-theory T has arbitrarily large finite models or an infinite model. Then T has a model of any cardinality $\alpha \geq \max\{\aleph_0, |\sigma|\}$.

Proof. Let $\{c_\alpha : \alpha \leq \kappa\}$ be a set of new constant symbols and let

$$\sigma' \coloneqq \sigma \cup \{c_\alpha : \alpha < \kappa\}.$$

Let $T' \coloneqq T \cup \{c_\alpha \neq c_\beta : \forall \alpha < \beta < \kappa\}$.
T' is finitely satisfiable: indeed, let $T_0 \subseteq T'$ be finite.
Then T_0 only demands that finitely-many of the C_α-s are distinct, so we can take a model $\mathcal{M} \models T$ of cardinality bigger than $|T_0|$ and expand it to a σ'-structure by interpreting these constants that appear in T_0 by distinct elements of $\mathcal{M}$, hence obtaining a model of T_0.
By the compactness theorem, there is a model $\mathcal{A} \models T'$ of cardinality $\leq \max\{\aleph_0, |\sigma|\} = \kappa$, i.e. $|\mathcal{A}| \leq \kappa$.
But because ${c_\alpha}^{\mathcal{A}} \neq {c_\beta}^{\mathcal{A}}$ $\forall \alpha < \beta < \kappa$, $|\mathcal{A}| \geq \kappa$, so $|\mathcal{A}| = \kappa$ □

Corollary. There is an uncountable model $\mathcal{M}$ of $\mathrm{Th}(\mathbb{N}, 0, S, +, \cdot) \supset$ PA.

Corollary (Skolem's paradox). If ZFC is consistent, then it has a countable model.

Proof. The signature σ is just $(\in)$, so $\max\{\aleph_0, |\sigma|\} = \aleph_0$, so the Completeness theorem gives a countable model. □

Definition A model of PA (or of $\mathrm{Th}(\mathbb{N}, 0, S, +, \cdot)$) is said to be nonstandard if it's not isomorphic to $(\mathbb{N}, 0, S, +, \cdot)$.

We just saw that there is an uncountable nonstandard model.

Proposition. There is a countable nonstandard model of $T \coloneqq \mathrm{Th}(\mathbb{N}, 0, S, +, \cdot)$.

Proof. Let $\sigma \coloneqq \sigma_{\text{arithm.}} \cup \{w\}$, where w is a new constant symbol.
$T' \coloneqq T \cup \{w \neq 0, w \neq \dot{1}, w \neq \dot{2}, \ldots\}$, where $\dot{n} \coloneqq \underbrace{S(S \ldots S}_{n}(0)\ldots)$.
T' is finitely-satisfiable, so by the Compactness theorem, T' is satisfiable, in fact has a countable model $\mathcal{M}$. The reduct of $\mathcal{M}$ to a $\sigma_{\text{arithm.}}$-structure is not isomorphic to $(\mathbb{N}, 0, S, +, \cdot)$ because it has an element $w^{\mathcal{M}} \neq \dot{n}^{\mathcal{M}}$ for any $n \in \mathbb{N}$. □

Idea of Proof of Completeness theorem (Henkin).

Proof. Let $\kappa \coloneqq \max\{\aleph_0, |\sigma|\}$. Suppose T is consistent.
The aim is to build a model of T with the underlying set being κ "or so".

Definition. A σ-theory S is called Henkin-complete if it is consistent maximally complete and whenever a sentence of the form $\exists v \varphi \in S$, there is a constant symbol c in σ s.t. $\varphi(c/_v) \in S$.
We call c a Henkin witness.
For a theory T, call a theory $\overline{T}$ a Henkin completion of T if $\overline{T} \supseteq T$ is Henkin-complete.

We let $\sigma' \coloneqq \sigma \cup \{c_\alpha : \alpha < \kappa\}$, and we build (by recursion) a σ'-Henkin completion $\overline{T}$ of T.
Then $A \coloneqq \kappa$ and interpret ${c_\alpha}^{\mathcal{A}} \coloneqq \alpha$ and the rest according to $\overline{T}$, then $\mathcal{A} \coloneqq (A, \sigma^{\mathcal{A}})$ is almost

a model $\overline{T}$, but not quite: maybe $\overline{T}$ contains sentences of the form $c_\alpha \doteq c_\beta$ for $\alpha \neq \beta$.
To fix this, we take a quotient of A by the equivalence relation

$$\alpha \equiv \beta :\Leftrightarrow c_\alpha \doteq c_\beta \in \overline{T}.$$

$B \coloneqq A/_\equiv$ and this gives a model $\mathcal{B} \coloneqq (B, \sigma^{\mathcal{B}})$ of $\overline{T}$, whose reduction to a σ-structure is a model of T. □