- so $\exists$ wins
- Thus $\exists$ wins no matter what
  i.e. has a winning strat
- By thm $\mathcal{M} \models A$ ✓

First-order theories

- we can think of sets of sentences S as axioms for the models $\mathcal{M}$ of S

Def'n Sps S is a set of sentences (in a fixed language L). The set of logical consequences of S is:

$$Con(S) := \{A : A \text{ is a sentence in } L \text{ and } S \models A\}$$

- observe: for an L-structure $\mathcal{M}$:
  $\mathcal{M} \models S$ iff $\mathcal{M} \models Con(S)$
- it follows: $Con(Con(S)) = Con(S)$
  i.e. $Con(S)$ is closed under logical consequence

Def'n A set of sentences T is a theory if $T = Con(T)$

- theories are "large and complicated"

- e.g. *any* theory T has to contain lots of "junk truths" like the tautology $\forall x\,((x = x \vee x \neq x) \wedge (x = x))$

- often interested in axiomatizing a given theory by a *simple* collection of sentences

<u>Def'n</u> if $Con(S) = T$, we say S is a <u>set of axioms</u> for T.

- if T is a theory then T is always a set of axioms for T
- but usually we want *simple* axioms for T

<u>Ex's</u> (i) Sps $L = \{<\}$ binary rel'n symbol

- let PO denote the sentences
  ① $\forall x \forall y\,(x < y \Rightarrow (y \not< x))$ (anti symmetry)
  ② $\forall x, y, z\,(x < y \wedge y < z \Rightarrow x < z)$ (transitivity)

$\forall x \forall y \forall z$

- if $\mathcal{M} = \langle M, < \rangle$ is an L-structure and $\mathcal{M} \models PO$, $\mathcal{M}$ is called a (strict) <u>partial order</u>
  - $Con(PO)$ is the <u>theory of partial orders</u>

(ii) Let LO denote PO + following axiom:
(3) $\forall x,y\ (x<y \vee y<x \vee x=y)$ (totality)

- LO are the axioms for linear orders
- a model $M \models LO$ is a linear order

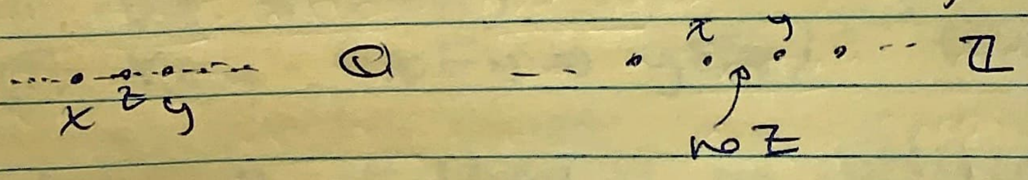
(iii) Let DLO denote LO plus:
(5) $\exists x, \exists y\ (x \neq y)$
(6) $\forall x,y\ (x<y \Rightarrow \exists z\ (x<z \wedge z<y))$

- DLO are the axioms for dense linear orders

(iv) Consider also
(7) $\forall x \exists y\ (x<y)$ (no right endpoint)
(8) $\forall x \exists y\ (y<x)$ (no left endpoint)

- DLO + (7), (8) are axioms for dense linear orders w/o endpoints

E.g.'s - $\langle \mathbb{N},<\rangle$, $\langle \mathbb{Z},<\rangle$, $\langle \mathbb{Q},<\rangle$, $\langle \mathbb{R},<\rangle$ and $\langle [0,1],<\rangle$ all models of LO
- $\langle \mathbb{Q},<\rangle$, $\langle \mathbb{R},<\rangle$, $\langle [0,1],<\rangle$ are dense linear orders, but $\langle \mathbb{N},<\rangle$, $\langle \mathbb{Z},<\rangle$ are not



- $\langle \mathbb{Q}, < \rangle$ and $\langle \mathbb{R}, < \rangle$ are d.l.o.'s w/o endpoints but $\langle [0,1], < \rangle$ is not.

<u>Def'n</u> a <u>well-order</u> is a linear order $\langle X, < \rangle$ s.t. every nonempty subset $Y \subseteq X$ has a least element.

- e.g. $\langle \mathbb{N}, < \rangle$ is a well-order but $\langle \mathbb{Z}, < \rangle$ is not

$$\underbrace{\cdots \odot \cdot \odot \cdot \odot \cdot \odot}_{\text{subset w/ no least el't}} \cdots \quad \mathbb{Z}$$

- <u>notice</u>: the defining property of well-orders is a <u>second order</u> property (refers to <u>subsets</u> of X instead of <u>elements</u> of X)
- and in fact can show: there is no collection of sentences WO in first-order logic s.t.
  $\mathcal{M} \models WO$ iff $\mathcal{M}$ is a well-order.

<u>Ex</u> Consider $L = \{E\}$ binary rel'n symb.
- theory of <u>undirected graphs</u> has the axioms:
  1. $\forall x \; \neg(xEx)$ (no loops)
  2. $\forall x, y \; (xEy \Rightarrow yEx)$ (undirected)
- a model $\mathcal{M}$ of these is an <u>undirected graph</u>

Fact: there are no first-order axioms CG whose models are precisely the connected graphs
(... connectedness is a second order property!)

Ex Consider $L = \{e, \cdot\}$ const symb, binary funct. symb
- theory of groups has the axioms:
  ① $\forall x,y,z\ ((x\cdot(y\cdot z)) = ((x\cdot y)\cdot z))$
  ② $\forall x\ (x\cdot e = e\cdot x = x)$ ← really a conjunction
  ③ $\forall x\, \exists y\ (x\cdot y = e \wedge y\cdot x = e)$
- model of these is called a group
- e.g. $\langle \mathbb{Z}, 0, +\rangle$ and $\langle S_6, 1, \cdot\rangle$ are groups

- theory of abelian groups has additional axiom
  ④ $\forall x,y\ (x\cdot y = y\cdot x)$
- e.g. $\langle \mathbb{Z}, 0, +\rangle$ is abelian but $\langle S_6, 1, \cdot\rangle$ is not

Ex Now sps $L = \{0, 1, +, \cdot\}$ constants, binary functs
- theory of commutative rings w/ identity has axioms:
  ①–④ above (replacing e w/ 0 and $\cdot$ w/ +)

  ⑤ $\forall x,y,z\ (x\cdot(y\cdot z) = (x\cdot y)\cdot z)$
  ⑥ $\forall x,y\ (x\cdot y = y\cdot x)$

7. $\forall x\,(x\cdot 1 = x)$
8. $\forall x,y,z\,(x\cdot(y+z) = x\cdot y + x\cdot z)$

- e.g. $\langle \mathbb{Z}, 0, 1, +, \cdot \rangle$, $\langle \mathbb{Q}, 0, 1, +, \cdot \rangle$ and $\langle \mathbb{Z}_m, 0, 1, +, \cdot \rangle$ model these axioms.

  $\mathbb{Z}/m\mathbb{Z}$ modulo m

- theory of integral domains has additional axiom:
  9. $\forall x,y\,(x\cdot y = 0 \Rightarrow x = 0 \vee y = 0)$
- e.g. $\langle \mathbb{Z}, 0, 1, +, \cdot \rangle$ $\langle \mathbb{Q}, 0, 1, +, \cdot \rangle$ $\langle \mathbb{Z}_p, 0, 1, +, \cdot \rangle$ (p prime) are integral domains but $\langle \mathbb{Z}_m, 0, 1, +, \cdot \rangle$ not for m composite (can multiply to 0 in $\mathbb{Z}/m\mathbb{Z}$)

- theory of fields has add'l axioms:
  10. $0 \neq 1$
  11. $\forall x\,(x \neq 0 \Rightarrow \exists y\,(x\cdot y = 1))$

- e.g. $\langle \mathbb{Q}, 0, 1, +, \cdot \rangle$ $\langle \mathbb{R}, 0, 1, +, \cdot \rangle$ and $\langle \mathbb{Z}_p, 0, 1, +, \cdot \rangle$ (p prime) are fields
  $\langle \mathbb{Z}, 0, 1, +, \cdot \rangle$ is not.

- theory of fields of characteristic 0 has add'l axioms:

(12.2) $1+1 \neq 0$

(12.3) $1+1+1 \neq 0$

(12.4) $1+1+1+1 \neq 0$

$\vdots$

- e.g. $\langle \mathbb{Q}, 0, 1, +, \cdot \rangle$ $\langle \mathbb{R}, 0, 1, +, \cdot \rangle$ have char. 0 but $\langle \mathbb{Z}_p, 0, 1, +, \cdot \rangle$ does not $(\underbrace{1+1+\cdots+1}_{p \text{ times}} = 0)$

- one way to generate a theory is as above:
  ↳ start w/ some axioms S (e.g. $S = LO$ or S = axioms for fields) and consider $T = Con(S)$

- another way is: start w/ a structure $\mathcal{M}$ (in a language L) and let T = theory of $\mathcal{M}$, where:

<u>Def'n</u> The <u>theory of $\mathcal{M}$</u> is
$Th(\mathcal{M}) := \{A : A$ is a sentence and $\mathcal{M} \models A\}$

<u>Prop'n</u> $Th(\mathcal{M})$ is indeed a theory, i.e. $Con(Th(\mathcal{M})) = Th(\mathcal{M})$

<u>Pf</u>: exercise.

- often interested in finding axioms S for $Th(\mathcal{M})$ (i.e. S s.t. $Con(S) = Th(\mathcal{M})$)
- can think of such S as "essential properties" of the structure $\mathcal{M}$ from which all other properties follow.
- can always take $S = Th(\mathcal{M})$, but this isn't interesting
  - ↳ want S to be simple.
  - (usually this means "computable" ... or maybe even "finite")

<u>Ex</u> Consider $L = \{0, 1, +, \cdot\}$ and $\mathcal{M} = \langle \mathbb{R}, 0, 1, +, \cdot \rangle$

- it can be shown: following are a set of axioms for $Th(\mathcal{M})$

1 - 11 above (i.e. axioms for fields of char. 0)

12 $\forall x \exists y (x = y^2 \vee x + y^2 = 0)$

("x is positive or non-positive")

13 $\forall x, y \exists z (x^2 + y^2 = z^2)$

(completeness)

14 $\forall x \; (x^2 \neq -1)$

(no imaginaries)

and, for every <u>odd</u> n, the axiom

15.n $\forall x_0, x_1, \ldots, x_n (x_n \neq 0 \Rightarrow$

$\exists y (x_n \cdot y^n + x_{n-1} \cdot y^{n-1} + \cdots + x_0 =$

("polynomials of odd degree have a real root")

<u>Ex</u> Similarly can axiomatize $Th(\langle \mathbb{C}, 0, 1, +, \cdot \rangle)$ by removing (14) and adding (15.n) axioms for even n's as well.

<u>Ex</u> Now consider $L_{ar} = \{0, S, +, \cdot, <\}$ and the standard structure of arithmetic $\mathcal{N} = \langle \mathbb{N}, 0, S, +, \cdot, < \rangle$

- the <u>Peano axioms</u> (PA) are the following:

(1) $\forall x\, (S(x) \neq 0)$

(2) $\forall x, y\, (x \neq y \Rightarrow S(x) \neq S(y))$

(3) $\forall x\, (x + 0 = x)$

(4) $\forall x, y\, (x + S(y) = S(x + y))$

(5) $\forall x\, (x \cdot 0 = 0)$

(6) $\forall x, y\, (x \cdot S(y) = x \cdot y + x)$

and, for every fmla $A(x, y_1, \ldots, y_n)$ in L_{ar}, an <u>induction axiom</u>

(7.A) $\forall y_1, \ldots, y_n \big[A(0, y_1, \ldots, y_n) \wedge \forall x (A(x, y_1, \ldots, y_n) \Rightarrow A(S(x), y_1, \ldots, y_n))$
$$\Rightarrow$$
$$\forall x\, A(x, y_1, \ldots, y_n) \big]$$

- in practice, every number theoretic fact of interest can be proved from PA

- however: PA is not a set of axioms for $Th(\mathcal{N})$
- in fact, by Gödel's incompleteness theorem there is no computable collection of axioms for $Th(\mathcal{N})$
- "computable" is a very generous notion of "nice" – just means we can recognize if a given axiom is in S or not
  - ↳ so: in a very strong sense, we can't write down a nice set of axioms S from which all arithmetic truths can be derived!

Proof system for FOL

- we introduce a Hilbert style proof system for FOL
- Goal is: prove Gödel's completeness theorem for FOL:

$$S \models A \quad \text{iff} \quad S \vdash A$$

  - ↳ first order analogue of completeness theorem for PL.

- just as w/ PL formal proofs, will be useful to restrict our language and view all formulas