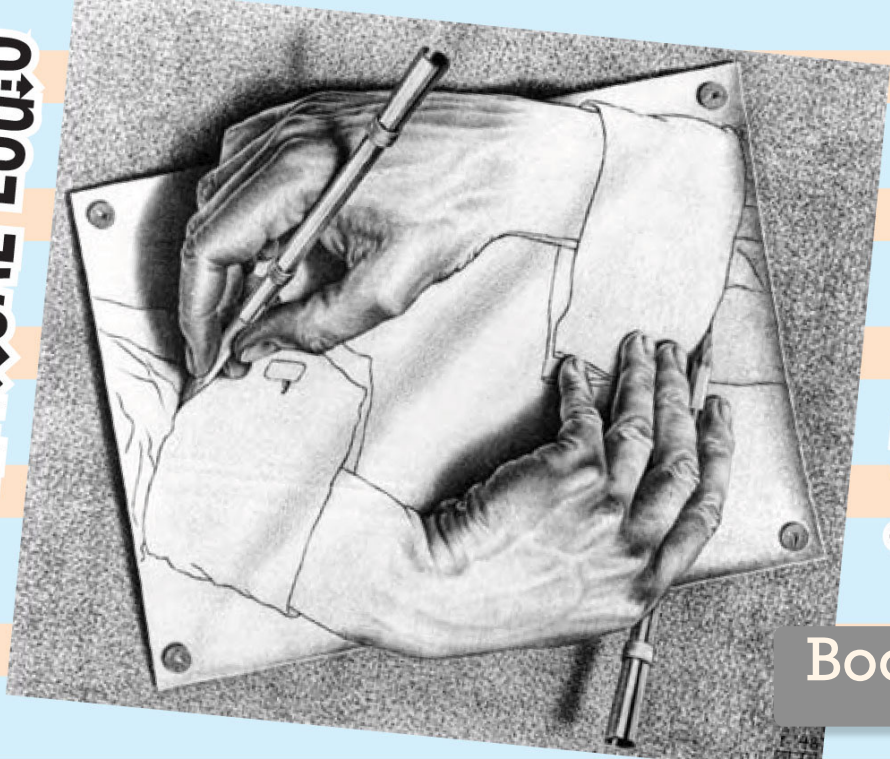


MATHEMATICAL LOGIC

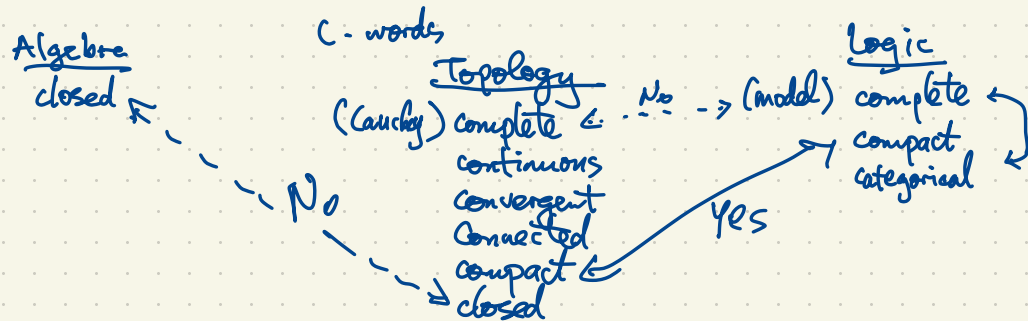


& SET THEORY

Book 2

Łoś-Vaught Test assures us that $Th(ACF_0)$ is complete. This uses: the theory has no finite models; and the theory is 2^{\aleph_0} -categorical.

L Ł Jerzy Łoś, Robert Vaught (1954)



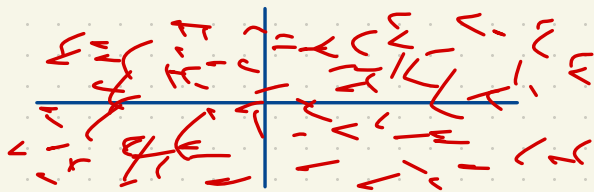
Let L be a language and let X be the collection of all L -structures.

For any set of sentences Σ over L , let $K_\Sigma = \text{set of } L\text{-structures satisfying all the sentences in } \Sigma$ (i.e. the set of models of Σ).

Then X is a top. space with K_Σ as its basic closed set.

This space is (topologically) compact. $\{K_\phi : \phi \text{ sentence over } L\}$ are ^{sub-}basic closed sets.

Eg. $K = \mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ has two field automorphisms, $\iota(a+b\sqrt{2}) = a+b\sqrt{2}$, $\tau(a+b\sqrt{2}) = a-b\sqrt{2}$.



\mathbb{C} has uncountably many automorphisms but only two of them are continuous.
Where do we get this?

$$\mathbb{C} \subset \mathbb{C}[x] \subset \mathbb{C}(x) = K \subset \bar{K}$$

The ^{polynomial} ring $\mathbb{C}[x]$ has automorphisms $f(x) \mapsto f(x+a)$

$$K = \mathbb{C}(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{C}[x] \right\}$$

is a field extension of \mathbb{C} and it's not alg. closed.

$K[t]$ has irreducible polys eg. $t^2 - x \in K[t]$

\bar{K} is an alg. closed field of char. 0, $|\bar{K}| = 2^{\aleph_0} = |\mathbb{C}|$

But there is only one alg. closed field of char. 0 for each uncountable cardinality
(the theory of ACF_0 is uncountably categorical) so $\bar{K} \cong \mathbb{C}$.

\bar{K} has lots of automorphisms i.e. \mathbb{C} has lots of automorphisms.

\mathbb{R} has only one automorphism, the identity $i(a) = a$.

Axioms for \mathbb{R} ?

Field axioms

+ Order axioms
and axioms

Introduce a new binary relation symbol ' $<$ ' ($a < b$ is a shorthand for $R(a, b)$)
 $(\forall a)(\forall b) [(a < b) \vee (a = b) \vee (b < a)] \wedge \neg [(a < b) \wedge (b < a)] \wedge \neg [(a < b) \wedge (a = b)] \wedge \neg [(b < a) \wedge (a = b)]$
 $(\forall a)(\forall b)(\forall c) [(a < b) \wedge (b < c) \rightarrow (a < c)]$

$$(\forall a)(\forall b)(\forall c) ((a < b) \rightarrow [(a+c < b+c) \wedge (c > 0) \rightarrow (ac < bc)])$$

\mathbb{R} is the unique ordered field which is (Cauchy)-complete and having \mathbb{Q} as a dense subfield.

But we cannot state "Cauchy complete" in first order theory of fields.

How much of the theory of \mathbb{R} can be captured in first order logic?

Ordered field axioms

- $(\forall a)(a \neq 0 \rightarrow a^2 > 0)$
- $(\forall a)(a > 0 \rightarrow (\exists b)(b^2 = a))$
- Every polynomial $f(x) \in \mathbb{R}[x]$ of odd degree has a root. Eg. for degree 3
 $(\forall a)(\forall b)(\forall c)(\exists x)(x^3 + ax^2 + bx + c = 0)$

RCF

The first order theory of \mathbb{R} is complete.

However the theory is not κ -categorical for any cardinality κ . (No models for κ finite; more than one for each infinite κ .)

Eg. for $\kappa = \aleph_0$: $\bar{\mathbb{Q}} \cap \mathbb{R}$

For $\kappa = 2^{\aleph_0}$: \mathbb{R} ; hyperreals ${}^*\mathbb{R}$

Any model of RCF is a real closed field.

Every real closed field is elementarily equivalent to \mathbb{R} (i.e. has the same first order theory).

$\bar{\mathbb{Q}}$ and \mathbb{C} are elementarily equivalent.

Emil Artin (1927) proved the Hilbert 17th problem using mathematical logic.

Hilbert's 17th Problem

Let $f(x_1, \dots, x_n) \in \mathbb{R}[x_1, \dots, x_n]$, such that $f \geq 0$ (i.e. $f(x_1, \dots, x_n) \geq 0$ for all $x_1, \dots, x_n \in \mathbb{R}$).
Is it necessary then $f = s_1^2 + \dots + s_k^2$ for some rational functions $s_i(x_1, \dots, x_n) \in \mathbb{R}(x_1, \dots, x_n)$? (Preston: $k \leq 2^n$)

Motzkin's example: $n=2$. $f(x,y) = 1 - 3x^2y^2 + x^2y^4 + x^4y^2 \geq 0$. This is not expressible as a sum of squares of poly's but

$$f(x,y) = \left[\frac{x^2y(x^2+y^2-2)}{x^2+y^2} \right]^2 + \left[\frac{xy^2(x^2+y^2-2)}{x^2+y^2} \right]^2 + \left[\frac{xy(x^2+y^2-2)}{x^2+y^2} \right]^2 + \left[\frac{x^2-y^2}{x^2+y^2} \right]^2.$$

Note: $\frac{1+x^4y^2+x^2y^4}{3} \geq (1 \cdot x^4y^2 \cdot x^2y^4)^{\frac{1}{3}} = x^2y^2$ by the arithmetic-geometric mean inequality

so $f(x,y) \geq 0$ for all x,y .

If $f = s_1^2 + \dots + s_k^2$ for some $s_i(x,y) \in \mathbb{R}[x,y]$ then $\deg s_i \leq 3$, so $s_i(x,y)$ may have terms

$$1, x, y, x^2, xy, y^2, \cancel{x^3}, \cancel{xy^2}, \cancel{xy^2}, \cancel{y^3}$$

$$s_i(x,y) = a_i + b_i x + c_i y + d_i xy + e_i x^2 + f_i y^2$$

$$s_i^2 = \underline{2d_i xy} + \dots$$

In \mathbb{R} , the positive elements are squares.

(Not true in \mathbb{Q})

Consequence: $|\text{Aut } \mathbb{R}| = 1$. If $\phi \in \text{Aut } \mathbb{R}$ i.e. $\phi: \mathbb{R} \rightarrow \mathbb{R}$ is bijective and $\phi(a+b) = \phi(a) + \phi(b)$ for all $a, b \in \mathbb{R}$
then $\phi(a) = a$ for all $a \in \mathbb{R}$. Why? $\phi(a^2) = \phi(a)^2$ so $\phi(a) > 0$ iff $a > 0$. $\phi(ab) = \phi(a)\phi(b)$

So $\phi(a) < \phi(b) \iff a < b.$

$\iff \phi(b) - \phi(a) > 0$

$\iff \phi(b-a) > 0$

$\iff b-a > 0$

$\iff a < b.$

$\phi(0) = 0$

$\phi(1) = 1$

$\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 1+1=2$

\vdots
 $\phi(n) = n$

$\phi(a) = a$ for all $a \in \mathbb{Q}$

$\phi(a) = a$ for all $a \in \mathbb{R}.$

Compare: $\mathbb{D}[\sqrt{-1}]$ is also an ordered field but it has a non-trivial automorphism $\phi(a+b\sqrt{-1}) = a-b\sqrt{-1}$ for all $a, b \in \mathbb{D}.$

Hilbert's 17th problem is true for $n=1$: every $f(x) \in \mathbb{R}[x]$ with $f(x) \geq 0$ for all x satisfies

$f(x) = g(x)^2 + h(x)^2$ for some $g(x), h(x) \in \mathbb{R}[x].$ Why? Factor

$f(x) = \lambda \prod_{i=1}^m (x-r_i)^2 \cdot \prod_{j=1}^n ((x-s_j)^2 + t_j^2)$ where $\lambda \geq 0, \lambda = a^2$

$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$

Proof of Hilbert's 17th Problem (Artin; Serre)

Let $f = f(x_1, \dots, x_n) \in \mathbb{R}[x_1, \dots, x_n].$ Suppose f is not a sum of squares of rational functions; we must show $f(a_1, \dots, a_n) < 0$ for some $a_1, \dots, a_n \in \mathbb{R}.$

$F = \mathbb{R}(x_1, \dots, x_n) =$ field of rational functions in x_1, \dots, x_n with real coefficients.

$T = \{ \text{sums of squares of rational functions in } f \}$

$= \{ s_1^2 + \dots + s_k^2 : s_i \in F \}.$ Note: $T+T \subseteq T, TT \subseteq T, a^2 \in T$ for all $a \in F.$

T defines a preorder on F , namely for $g, h \in F$, we say $g \leq h$ iff $h-g \in T$.
 " \leq " is transitive but it's a partial order in general.

It's an order iff $T \cup (-T) = F$ and $T \cap (-T) = \{0\}$.
 (total order) $-T = \{-g : g \in T\}$

We are assuming $f \notin T$.

Among all preorders containing T but not containing f , choose a maximal preorder P using Zorn's lemma.

Let $\{P_\alpha : \alpha \in A\}$ be a ^{totally ordered} collection of preorders on F with $P_\alpha \supseteq T$, $f \notin P_\alpha$.
 (i.e. for every $\alpha, \beta \in A$, either $P_\alpha \subseteq P_\beta$ or $P_\beta \subseteq P_\alpha$)

($\{P_\alpha\}$ is a chain) Then $P = \bigcup_{\alpha \in A} P_\alpha$ is an upper bound for the chain i.e. $P_\alpha \subseteq P$ for all $\alpha \in A$. Then P is a preorder ($P+P \subseteq P$, $PP \subseteq P$, $a^2 \in P$) and $P \supseteq T$, $f \notin P$.
 By Zorn's lemma there exists a maximal preorder P as above.

(i) Show $-f \notin P$. If $-f \in P$ then $f = \left(\frac{1+f}{2}\right)^2 + (-1)\left(\frac{1-f}{2}\right)^2 \in P$, a contradiction.

(ii) Show $-f \in P$. Suppose $-f \notin P$ and consider $\tilde{P} = P - Pf = \{a-bf : a, b \in P\}$ which is a preorder.
 $\tilde{P} + \tilde{P} = \{(a_1-b_1f) + (a_2-b_2f)\} = \{(a_1+a_2) - (b_1+b_2)f : a_i, b_i \in P\} \subseteq \tilde{P}$

$\tilde{P} \tilde{P}$: $(a_1-b_1f)(a_2-b_2f) = \underbrace{(a_1a_2 + f^2 \cdot b_1b_2)}_P - \underbrace{(a_1b_2 + a_2b_1)}_P f \in \tilde{P}$ $\tilde{P} \supset P$ $-f \notin P$
 $f \in \tilde{P}$

By maximality of P , $-f \in \tilde{P}$.
 $f = a-bf$, some $a, b \in P$. $(1+b)f = a \Rightarrow f = \frac{a}{1+b} = (1+b)a \cdot \frac{1}{(1+b)^2} \in P$

(iii) Given $g \in F$, show $g \in P$ or $-g \in P$.

Assume $g \notin P$; show $-g \in P$. wlog $g \neq 0$.

Consider $\tilde{P} = P + Pg$. As in (ii) \tilde{P} is a preorder, $\tilde{P} \supseteq P$, $\tilde{P} > P$ since $g \notin P$, $g \in \tilde{P}$. By maximality of P , we must have $f \in \tilde{P}$ so $f = a + bg$, some $a, b \in P$.

$$-bg = a - f \Rightarrow -g = \frac{a-f}{b} = b \cdot (a-f) \cdot \left(\frac{1}{b}\right)^2 \in P$$

(iv) $P \cap (-P) = \{0\}$ If $g \neq 0$, $g \in P$, $-g \notin P$ then $-(-g) = g = (-g) \cdot \left(\frac{1}{g}\right)^2 \in P$, contrary to (i).

(F, \leq) is an ordered field where $a \leq b \iff b - a \in P$.

It's an extension of (\mathbb{R}, \leq)

By the Tarski Transfer Principle, if $(x_1, \dots, x_n) \in F^n$ satisfies a statement in first order theory of ordered fields, then there is $(a_1, \dots, a_n) \in \mathbb{R}^n$ realizing this statement.

Here $-f \in P$ i.e. $f < 0$ i.e. $f(x_1, \dots, x_n) < 0$ so $f(a_1, \dots, a_n) < 0$ for some $a_1, \dots, a_n \in \mathbb{R}$.

Indiscernibles ... coming soon


Axioms for projective plane geometry: Here we consider only points, lines and their incidences.

Objects: points and lines

Relations: $\underbrace{P(\cdot) L(\cdot)}_{\text{many relation symbols}}, \underbrace{I(\cdot, \cdot)}_{\text{binary relation symbol}}$

$$(\forall x)(P(x) \leftrightarrow (\exists L(x)))$$

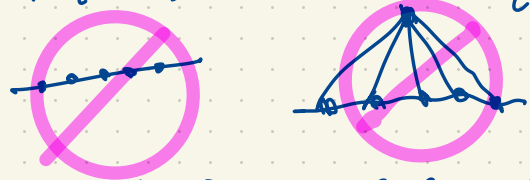
$$(\forall x)(\forall y)(I(x,y) \rightarrow (P(x) \leftrightarrow L(y)))$$

Axioms: (i)  Any two distinct points are on a unique line.

$$(\forall x)(\forall y)(P(x) \wedge P(y) \wedge \neg(x=y) \rightarrow (\exists z)(I(x,z) \wedge I(y,z) \wedge (\forall w)(I(x,w) \wedge I(y,w) \rightarrow (w=z))))$$

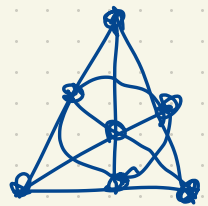
(ii)  Any two distinct lines meet in a unique point.

(iii) nondegeneracy axiom



There exist at least four points with no three of them collinear.

Models? There are some orders (sizes) for which models are unique up to isomorphism



7 points
7 lines
3 points/line
3 lines/point

Finite projective planes:

- $n^2 + n + 1$ points / lines
- $n + 1$ points / line
- $n + 1$ lines / point
- n = order of the plane


Infinite planes:

For every infinite cardinal κ , there are many proj planes of order κ (with cardinality κ).

Does there exist an infinite projective plane which is \aleph_0 -categorical i.e. its theory has a unique countable model?



Generalized Quadrangles

- (i) ... Any two points are on at most one line
- (ii)  IF P is not on l then there is a unique Q on l joined to P .

(iii) nondegeneracy. $\left. \begin{matrix} \leftarrow \\ \leftarrow \\ \leftarrow \end{matrix} \right\} \geq 3$



In every case $\left. \begin{matrix} \leftarrow \\ \leftarrow \\ \leftarrow \end{matrix} \right\} t+1$



Can $s < \infty, t = \infty$?

IF $s = 2$ then $t \leq 4$ (easy).

IF $s = 3$ then $t \leq 9$ (4 pages)

IF $s = 4$ then $t \leq 16$ (Cherlin)

Let A be a set of first order sentences over a language L (i.e. a theory) and let $M \models A$ (a model of A).

A set of indiscernibles $S \subseteq M$ such that for every distinct $s_1, \dots, s_k \in S$ and $t_1, \dots, t_k \in S$ and every propositional function $\phi(x_1, \dots, x_k)$, $\phi(s_1, \dots, s_k) \equiv \phi(t_1, \dots, t_k)$.

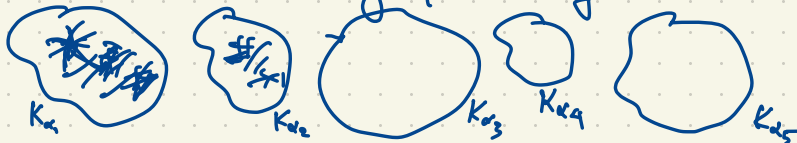
Ex. Let A be the axioms of field theory, $\mathbb{C} \models A$. Let S be ^{any} ^{distinct} algebraically independent subset of \mathbb{C} . This means that for all $s_1, \dots, s_k \in S$ and $f(x_1, \dots, x_k) \in \mathbb{Q}[x_1, \dots, x_k]$ then $f(s_1, \dots, s_k) \neq 0$.

eg. $\{\pi\}$, $\{e\}$. There are alg. ind. subsets of \mathbb{C} of uncountable size!

Is $\{\pi, e\}$ alg. indep.?

Any set $S \subseteq \mathbb{C}$ which is alg. indep. is a set of indiscernibles.

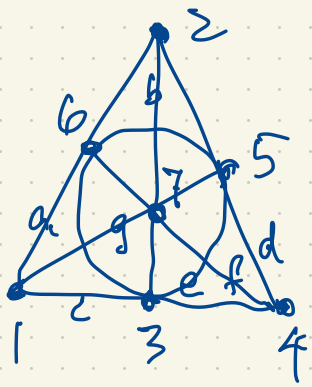
Let A be the axioms of graph theory. Consider a graph $\Gamma \models A$ that looks like



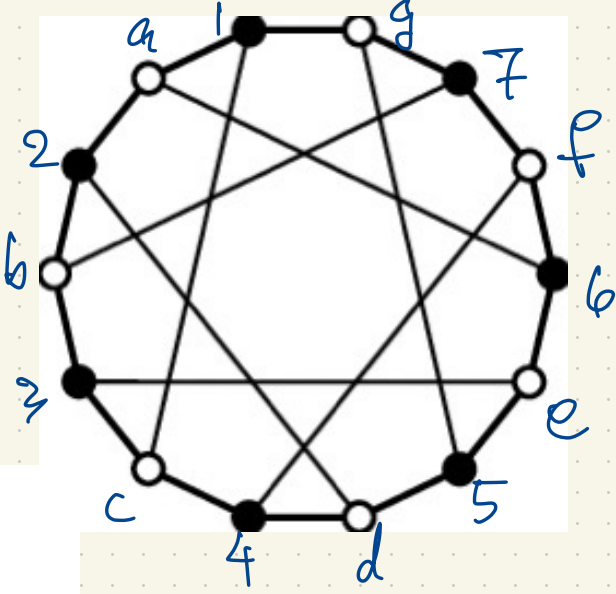
where $\alpha_1, \dots, \alpha_5$ are infinite cardinals

Pick $s_1 \in K_{\alpha_1}, \dots, s_5 \in K_{\alpha_5}$.

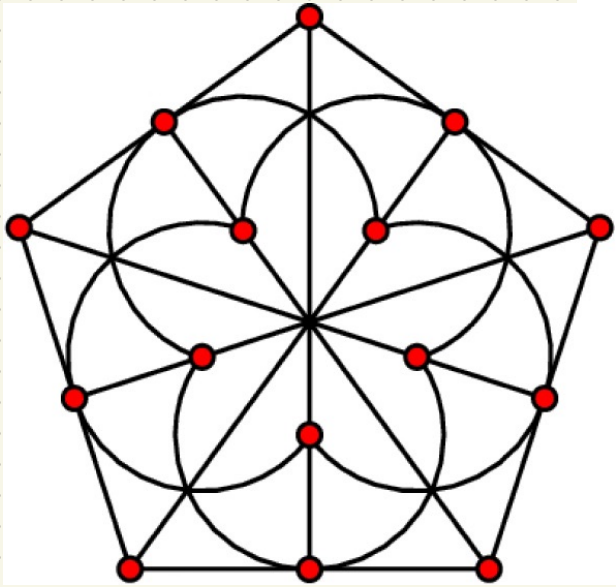
$\{s_1, \dots, s_5\}$ is a set of indiscernibles.



=



Proj. Plane \leftrightarrow
 bipartite graph
 of diameter 3
 and girth 6
 (shortest cycles have
 length 6)



generalized quadrangle \leftrightarrow

bipartite graph
 of diameter 4
 and girth 8.

Let \mathcal{L} be a language and A a set of sentences over \mathcal{L} . Let $M \models A$ be an \mathcal{L} -structure.
 A subset $S \subseteq M$ is a set of indiscernibles if for every $k \geq 1$ and
 $a_1, \dots, a_k \in S$ distinct, also any $\phi(x_1, \dots, x_n)$ formula over \mathcal{L} ,
 $b_1, \dots, b_k \in S$ distinct,
 $M \models \phi(a_1, \dots, a_k) \Leftrightarrow \phi(b_1, \dots, b_k)$.

Eg. $\mathcal{L} = (\cdot, +, 0, 1)$ = language of rings with identity!

A = axioms of field theory

$M = \mathbb{C}$

$S \subseteq \mathbb{C}$ any algebraically independent set (i.e. for $a_1, \dots, a_k \in S$ distinct,

$f(x_1, \dots, x_k) \in \mathbb{Q}[x_1, \dots, x_k]$ nonzero poly., $f(a_1, \dots, a_k) \neq 0$.)

Let $s, t \in S$. Eg. $\phi(x, y) : x^2 + xy + y^2 = 0$.

For all $s, t \in S$ ($s \neq t$), $\phi(s, t)$ is false.

$\psi(x, y) : (\forall u)(\exists v)(ux + vy = 1)$.

$\psi(s, t)$ is true for all $s \neq t$ in S .

Dense Linear Order Without Endpoints

$\mathcal{L} = (<)$, A = axioms of DLO without endpoints, $M = (\mathbb{Q}, <)$ usual ordering on \mathbb{Q} .
 $M \models A$ (the unique countable model up to isomorphism). This structure has no indiscernible
 sets S with $|S| \geq 1$. If $s, t \in S$ with $s \neq t$ then (s, t) , (t, s) are discernible

eg. $s < t \rightarrow \neg(t < s)$

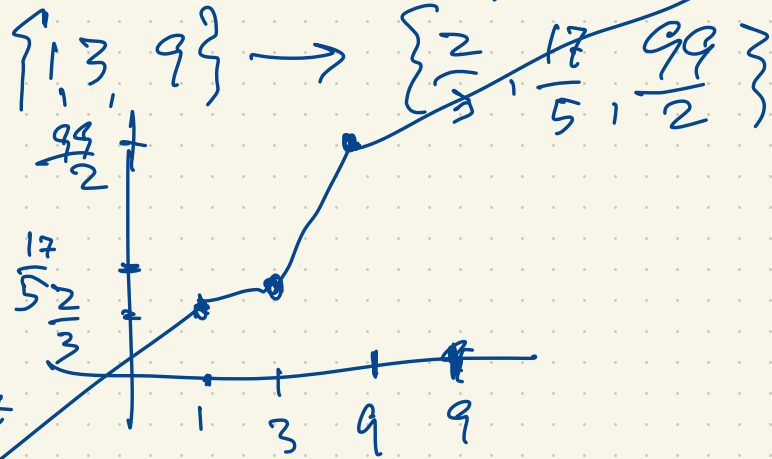
A set of order indiscernibles in M is an ordered set $S = \{s_t : t \in \mathbb{Q}\}$ such that whenever $t_1 < \dots < t_k$ in \mathbb{Q} and $u_1 < \dots < u_k$ in \mathbb{Q} and $\phi(x_1, \dots, x_k)$ is a prop. formula over \mathcal{L} we have

Now $\mathcal{L} = (<)$, $M = (\mathbb{Q}, <)$, $S = \mathbb{Q}$.
 S is a set of order indiscernibles.

$$M \models (\phi(s_{t_1}, \dots, s_{t_k}) \leftrightarrow \phi(s_{u_1}, \dots, s_{u_k})).$$

Theorem Let A be a collection of sentences over a language \mathcal{L} . If A has an infinite model $M \models A$, then A has an infinite model with a set of order indiscernibles $S \subseteq M$, $S = \{s_t : t \in \mathbb{Q}\}$.

(Here we have chosen S having order type $(\mathbb{Q}, <)$ but you can choose any total order you want and get models of A with sets of order indiscernibles of the desired order type.)



Remark: The Upward Löwenheim-Skolem Theorem says: if A has an infinite model M then it also has models of every cardinality $\geq |M|$.