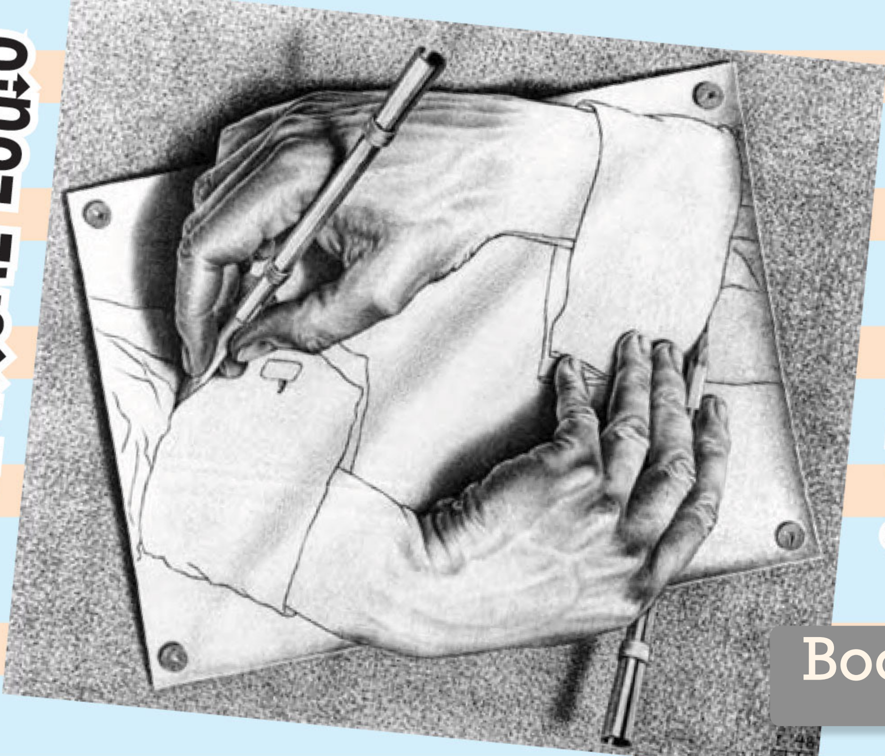
MATHEMATICAL LOGIC & SET THEORY



Book 2

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

Ł ł   Jerzy Łoś, Robert Vaught (1954)

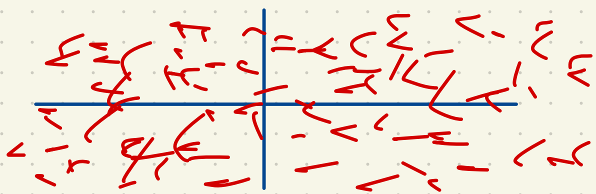
C-words

<u>Algebra</u>	<u>Topology</u>	<u>Logic</u>
closed	(Cauchy) complete	(model) complete
	continuous	compact
	convergent	categorical
	connected	
	compact	
	closed	

$\aleph_0$ No   yes

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_Σ = set of of L-structures satisfying all the sentences in Σ (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. $\{K_\theta : \theta$ 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 $f(x) \longmapsto f(x+a)$

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

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 $\iota(a) = a$.

Axioms for $\mathbb{R}$?

Field axioms
+ Order axioms
 and axioms

Introduce a new binary relation symbol '$<$' ($a<b$ is a shorthand for $R(a,b)$)

$(\forall a)(\forall b)[((a<b) \vee (a=b) \vee (b<a)) \wedge \neg[(a<b) \wedge (b<a)] \wedge \neg[(a<b) \wedge (a=b)] \wedge \neg[(b<a) \wedge (a=b)]]$

$(\forall a)(\forall b)(\forall c)((a<b) \wedge (b<c) \rightarrow (a<c))$

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

$\mathbb{R}$ 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

- $(\forall a)(a \neq 0 \to a^2 > 0)$
- $(\forall a)(a>0 \to (\exists b)(b^2 = a))$
- 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 <u>elementarily equivalent</u> 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 17^{th} 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 that $f = s_1^2 + \dots + s_k^2$ for some rational functions $s_i(x_1, \dots, x_n) \in \mathbb{R}(x_1, \dots, x_n)$? (Pfister: $k \leq 2^n$)

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

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

$s_i(x,y) = a_i + b_ix + c_iy + d_ixy + e_ix^2 + f_iy^2$

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

In $\mathbb{R}$, the positive elements are squares.
(Not true in $\mathbb{Q}$)

Consequence: $|\mathrm{Aut}\,\mathbb{R}| = 1$. If $\phi \in \mathrm{Aut}\,\mathbb{R}$ i.e. $\phi: \mathbb{R} \to \mathbb{R}$ is bijective and $\phi(a+b) = \phi(a) + \phi(b)$, $\phi(ab) = \phi(a)\phi(b)$ 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 $a > 0$.

So $\underset{\sim}{\phi(a) < \phi(b)} \iff a < b$.

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

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

$\iff b - a > 0$

$\iff a < b$.

$\phi(0) = 0$

$\phi(1) = 1$

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

$\vdots$

$\phi(n) = n$

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

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

Compare: $\mathbb{Q}[\sqrt{2}]$ is also an ordered field but it has a nontrivial automorphism $\phi(a+b\sqrt{2}) = a - b\sqrt{2}$ for all $a, b \in \mathbb{Q}$.

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

$$f(x) = \lambda \prod_{i=1}^{m} (x - r_i)^2 \cdot \prod_{j=1}^{n} \left((x - s_i)^2 + t_i^2 \right) \quad \text{where } \lambda \geq 0,\ \lambda = a^2$$

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

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

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

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

$T = \{$ sums of squares of rational functions in $F \}$.

$= \{ s_1^2 + \cdots + s_k^2 : s_i \in F \}$. 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 (total order) iff $T \cup (-T) = F$ and $T \cap (-T) = \{0\}$.

$$-T = \{-g : g \in T\}$$

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 $-1 \notin P$. If $-1 \in P$ 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.

$$\tilde{P} + \tilde{P} = \{(a_1 - b_1 f) + (a_2 - b_2 f) = \underset{\Uparrow \atop \hat{P}}{(a_1 + a_2)} - \underset{\Uparrow \atop P}{(b_1 + b_2)} f : a_i, b_i \in P\} \subseteq \tilde{P}$$

$\tilde{P}\tilde{P}$:
$$(a_1 - b_1 f)(a_2 - b_2 f)$$
$$= \underbrace{(a_1 a_2 + f^2 \cdot b_1 b_2)}_{P} - \underbrace{(a_1 b_2 + a_2 b_1)}_{P} f \in \tilde{P}$$

$\tilde{P} \supset P$ $-f \notin P$
$-f \in \tilde{P}$

By maximality of P, $f \in \tilde{P}$.

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

(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, $\tilde{P} \supseteq P$, $\tilde{P} \supset P$ 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 $g \neq 0$, $g \in P$, $-g \in P$ then

$$-1 = g \cdot (-g) \cdot \left(\frac{1}{g}\right)^2 \in P,$$ contrary to (i).

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

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 $-f \in P$ ie. $f < 0$ 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.

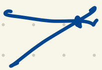
Objects: points and lines

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

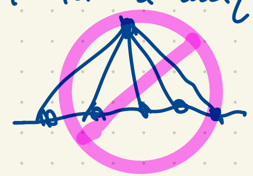
$$(\forall x)(P(x)\leftrightarrow(\neg L(x)))$$
$$(\forall x)(\forall y)(I(x,y)\to(P(x)\leftrightarrow L(y)))$$

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

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

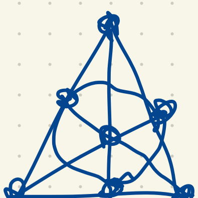
(ii)  Any two distinct lines meet in a unique point.

(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

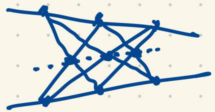


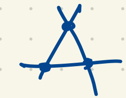
7 points
7 lines
3 points/line
3 lines/point

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).

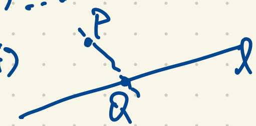
Does there exist an infinite projective plane which is $\aleph_0$-categorical i.e. its theory has a unique countable model?



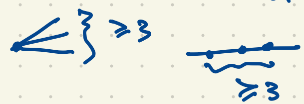


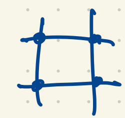
Generalized Quadrangles

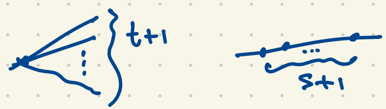
(i) . . . . Any two points are on at most line

(ii) 

If P is not on l then there is a unique Q on l joined to P.

(iii) nondegeneracy. 



In every case 

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

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 $\phi(x_1, \dots, x_k)$, $\phi(s_1, \dots, s_k)$ iff $\phi(t_1, \dots, t_k)$.

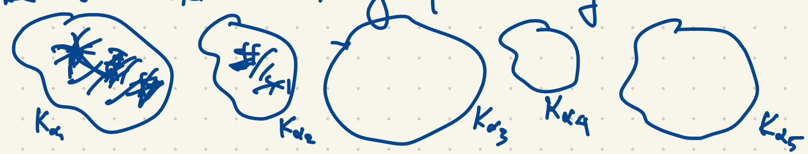
Eg. Let $\mathcal{A}$ be the axioms of field theory, $\mathbb{C} \models \mathcal{A}$. Let S be any algebraically independent subset of $\mathbb{C}$. This means that for all distinct $s_1, \dots, s_k \in S$ and nonzero $f(x_1, \dots, x_k) \in \mathbb{Q}[x_1, \dots, x_k]$ then $f(s_1, \dots, s_k) \neq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

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.

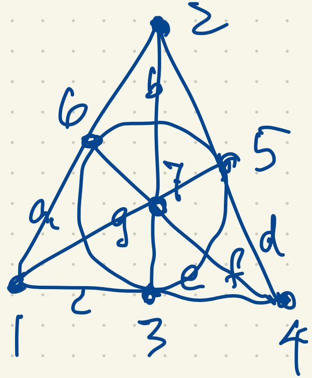
Let $\mathcal{A}$ be the axioms of graph theory. Consider a graph $\Gamma \models \mathcal{A}$ that looks like



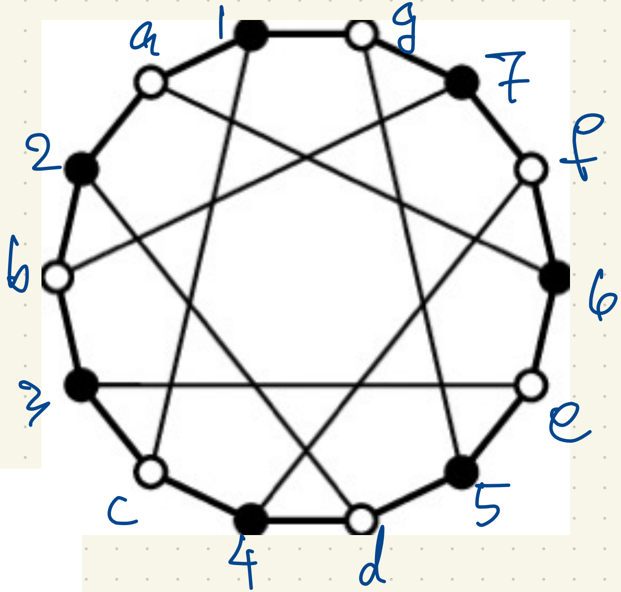
where $\alpha_1, \dots, \alpha_5$ are infinite cardinals.

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

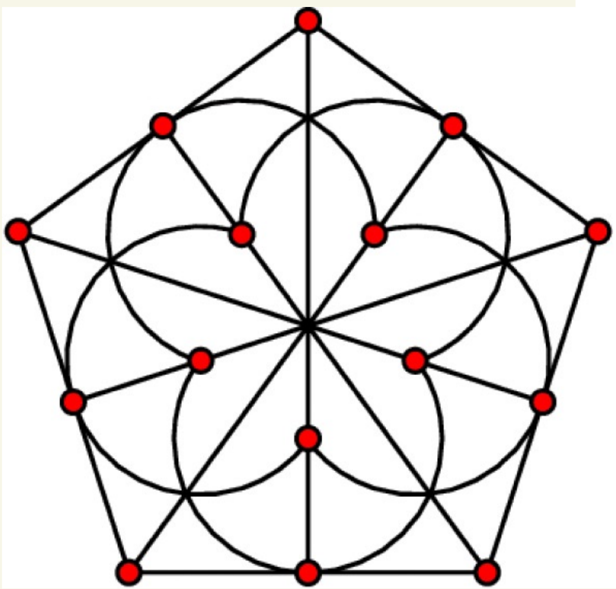
$\{s_1, \dots, s_5\}$ is a set of indiscernibles.



=



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



generalized quadrangle ⟷ bipartite graph of diameter 4 and girth 8.

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

$$M \models \phi(a_1, \cdots, a_k) \Leftrightarrow \phi(b_1, \cdots, b_k).$$

Eg. $\mathcal{L} = (\cdot, +, 0, 1)$ = language of rings with identity:
$\mathcal{A}$ = axioms of field theory
$M = \mathbb{C}$
$S \subset \mathbb{C}$ any algebraically independent set (i.e. for $a_1, \cdots, a_k \in S$ distinct, $f(x_1, \cdots, x_k) \in \mathbb{Q}[x_1, \cdots, x_k]$ nonzero poly., $f(a_1, \cdots, a_k) \neq 0$.)

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 $|S| > 1$. If $s, t \in S$ with $s \neq t$ then (s,t), (t,s) are discernible

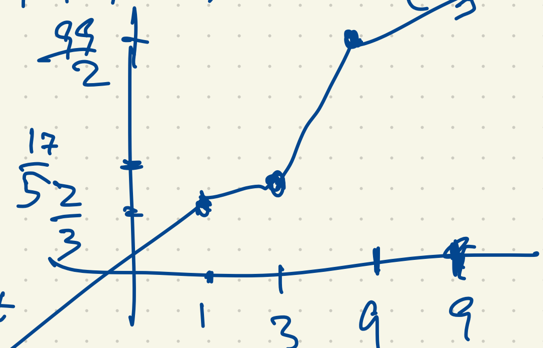
eg. $s < t \rightarrow \neg(t < s)$

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

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

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

$$\{1, 3, 9\} \longrightarrow \left\{ \frac{2}{3}, \frac{17}{5}, \frac{99}{2} \right\}$$



Theorem Let $\mathcal{A}$ be a collection of sentences over a language $\mathcal{L}$. If $\mathcal{A}$ has an infinite model $M \models \mathcal{A}$, then $\mathcal{A}$ 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 $\mathcal{A}$ with sets of order indiscernibles of the desired order type.)

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

$|A| = |B|$ iff there is a bijection $A \longrightarrow B$.

$|A| \le |B|$ iff there is a bijection between A and a subset of B (i.e. an $\overset{1:1 \text{ map}}{\text{injection}}$ $A \to B$)

eg. $\mathbb{N} = \{1, 2, 3, \cdots\}$, $\mathbb{N}_0 = \{0, 1, 2, 3, \cdots\} = \omega$. The map $x \mapsto x$, $\mathbb{N} \to \mathbb{N}_0$ is injective so

$|\mathbb{N}| \le |\mathbb{N}_0|$. But $|\mathbb{N}| = |\mathbb{N}_0|$ since $x \mapsto x-1$ is a bijection $\mathbb{N} \longrightarrow \mathbb{N}_0$.

$|\mathbb{N}| = |\mathbb{N}_0| = |\mathbb{Q}| = |\mathbb{Z}| = |\mathbb{Q}^n| = \aleph_0$ $(n = 1, 2, 3, \dots)$ countably infinite; $|\mathbb{R}| > \aleph_0$. why?

$\mathbb{N} \longrightarrow \mathbb{R}$, $x \mapsto x$ is an injection so $|\mathbb{N}| \le |\mathbb{R}|$. Cantor showed there is no bijection

so $|\mathbb{N}| < |\mathbb{R}|$. More generally, if S is any set then $|S| < |\mathcal{P}(S)|$ where

$\mathcal{P}(S)$ = power set of S = {all subsets of S}.

$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

$$0, 1, 2, 3, \dots, \omega = \omega_0, \omega_1, \omega_2, \omega_3, \omega_4, \dots, \omega_\omega, \omega_{\omega+1}, \dots$$

~~Possible~~ Sizes (cardinalities) of sets: $0, 1, 2, 3, \dots, \aleph_0, \aleph_1, \aleph_2, \aleph_3, \aleph_4, \dots, \aleph_\omega, \aleph_{\omega+1}, \dots$

Since $|\mathbb{R}| > \aleph_0$, we have $|\mathbb{R}| \ge \aleph_1$.

CH (Continuum Hypothesis "Conjecture"): $|\mathbb{R}| = \aleph_1$, i.e. there is no set A with $|\mathbb{N}| < |A| < |\mathbb{R}|$.

$\neg$CH : $|\mathbb{R}| \ge \aleph_2$ i.e. there exists a set B with $|\mathbb{N}| < |B| < |\mathbb{R}|$.

By ZFC, every set S can be well-ordered. There is an order relation "$\trianglelefteq$" on S such that

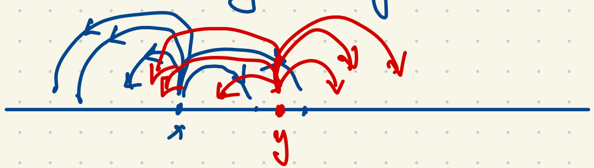
- if $a \trianglelefteq b$ and $b \trianglelefteq c$ then $a \trianglelefteq c$
- if $a \trianglelefteq b$ and $b \trianglelefteq a$ then $a = b$. ($a \trianglelefteq b$ means $\underset{\sim}{a \triangleleft b}$ or $a = b$)
- Every nonempty subset of S has a least element. If $A \subseteq S$, $A \neq \emptyset$ then there exists $a \in A$ with $a \trianglelefteq x$ for all $x \in A$.

($a \triangleleft b$: $a \trianglelefteq b$ but $a \neq b$)

In other words, there is no infinite decreasing sequence $a_1 \triangleright a_2 \triangleright a_3 \triangleright a_4 \triangleright \cdots$ in A.

The Axiom of Symmetry AS: x shoots at positions $A_x \subset \mathbb{R}$, $|A_x| \leq \aleph_0$.

$x \notin A_x$



AS: There exist $x \neq y$ in $\mathbb{R}$ such that $x \notin A_y$, $y \notin A_x$.
(Neither of x, y hits the other.)

AS is very easily believable.

AS is equivalent to $\neg CH$.

Proof of CH implies $\neg$AS: Assuming CH, $|\mathbb{R}| = \aleph_1$ so well-order $(\mathbb{R}, \lhd)$ of type ω_1.

For every $x \in \mathbb{R}$, define $A_x = \{y \in \mathbb{R} : \underbrace{y \lhd x}_{y \in x}\}$. $x \in \mathbb{R}$ says $\underbrace{x \lhd \omega_1}_{x \in \omega_1}$ so x is a countable ordinal.

So $|A_x| \le \aleph_0$.

$$\left.\begin{array}{l} x \in A_y \iff x \lhd y \\ y \in A_x \iff y \lhd x \end{array}\right\}$$ Since $x \neq y$, one of these holds. This contradicts AS.

Proof of $\neg$CH $\to$ AS: Assuming there exists $B \subset \mathbb{R}$ with $\aleph_0 < |B| < |\mathbb{R}|$, say $|B| = \aleph_1$, $|\mathbb{R}| \geq \aleph_2$, and let $x \mapsto A_x$ be any assignment of countable subsets of $\mathbb{R}$ to the real numbers $x \in \mathbb{R}$.

$B_1 = \bigcup_{x \in B} A_x = \{$all points hit from $B\}$. $|B_1| \le \aleph_1$.

$B_2 = \bigcup_{x \in B_1} A_x$ $\quad |B_2| \le \aleph_1$ etc. $B^* = B \cup B_1 \cup B_2 \cup B_3 \cup \cdots$ $\quad |B^*| = \aleph_1$.

Since $|B^*| < |\mathbb{R}|$, we can pick $x \in \mathbb{R}$, $x \notin B^*$. We want to pick $y \in B^*$, $y \notin A_x$. Since $|A_x| = \aleph_0 < |B^*|$, such y exists.

Also $x \notin A_y$ since points $y \in B^*$ can only hit other points in B^*.

Thus AS holds.

Freiling c.1986 introduced AS. But this was actually due to Sierpinski.

$AS = AS_1$

AS_2 says: Given any assignment $\{x,y\} \mapsto A_{x,y} \subseteq \mathbb{R}$ (for $x \neq y$ in $\mathbb{R}$)

$|A_{x,y}| \leq \aleph_0$

there exist three distinct $x, y, z \in \mathbb{R}$ such that none of them are shot by the other two i.e.

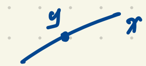
$$x \notin A_{y,z}$$
$$y \notin A_{x,z}$$
$$z \notin A_{x,y} .$$

AS_2 is equivalent to $|\mathbb{R}| \geq \aleph_3$.

AS_3 . - - - .. $|\mathbb{R}| \geq \aleph_4$

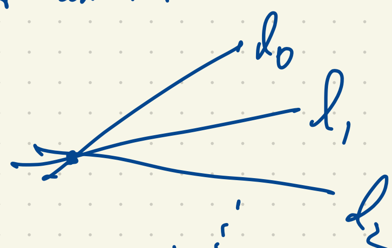
Theorem (Cherlin) Let Q be a generalized quadrangle with k points on every line, $k \in \{3,4,5\}$. Then Q is finite. (Actually known previously for $k = 3,4$.)

Language: $I(x,y)$ binary relation "x is incident with y" i.e. 

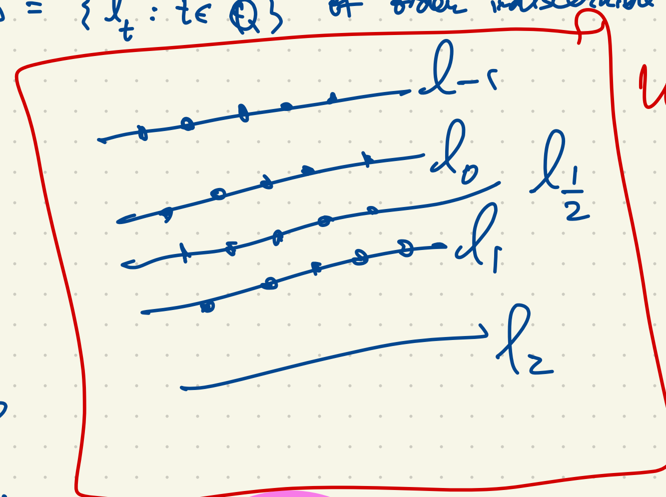
or 

$P(x)$, $L(y)$ unary relations.

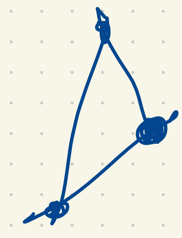
Proof Suppose the theory of GQ's with k points per line has an infinite model. Then it has an infinite model with a set $S = \{\ell_t : t \in \mathbb{Q}\}$ of order indiscernible lines.

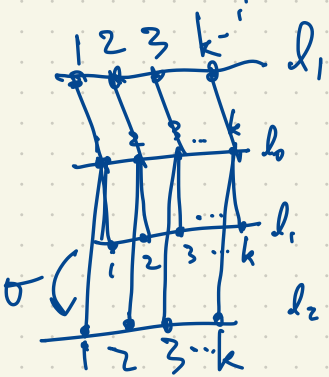


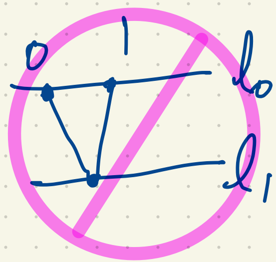
or



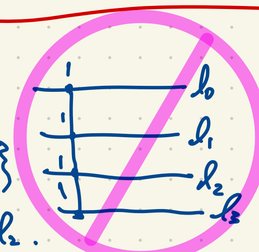
WLOG







There is a permutation $\sigma : \{1,2,\dots,k\} \to \{1,2,\dots,k\}$ such that point i on ℓ_1 is joined to point $\sigma(i)$ on ℓ_2.



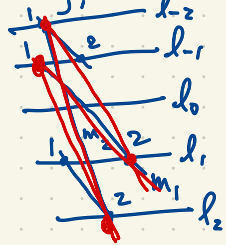
ℓ_0, ℓ_1, ℓ_2 $\quad 0 < 1 < 2$

ℓ_0, ℓ_1, ℓ_3 $\quad 0 < 1 < 3$

(σ is a derangement of $\{1,\dots,k\}$).
σ is fixed-point-free i.e. $\sigma(i) \neq i$.

By order-indiscernibility, whenever $0<s<t$, point i of ℓ_s is joined to point $\sigma(i)$ of ℓ_t.

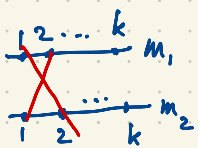
Re-index:



Suppose $\sigma(1)=2$. (WLOG)

For each $t>0$ ($t\in\mathbb{Q}$), let m_t be the line joining point 1 on ℓ_{-t} with point 2 on ℓ_t.

This gives from $\{\ell_t : t\in\mathbb{Q}\}$ a new set of lines $\{m_t : t\in\mathbb{Q},\ t>0\}$. $m_t\cap m_{t'}=\emptyset$ for all $t\neq t'$ and the collation $\{m_t : t\in\mathbb{Q},\ t>0\}$ of lines is again a collection of order indiscernibles.



If we replace the original $\{\ell_t\}_t$ with $\{m_t\}_t$ then the new σ is a derangement satisfying

$\sigma(1)=2$, $\sigma(2)=1$.

If $k=3$ we have a contradiction!

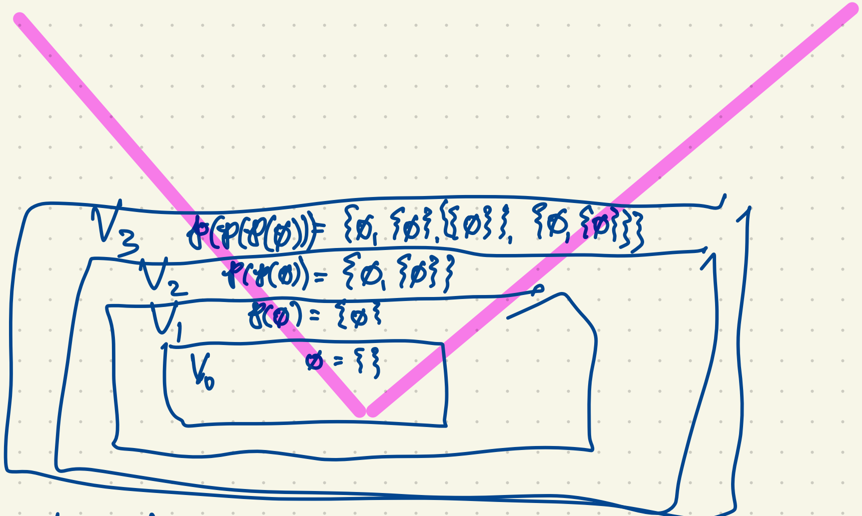
For $k=4,5$ we must work a little harder.

Set Theory ZFC axioms for first order set theory. See Cameron; Borcherds

Richard Borcherds YouTube → Zermelo-Fraenkel ($\approx$ 9 videos)

Avoid Russel's Paradox!

If S has n elements then $\mathcal{P}(S)$ has 2^n elements



The Von Neumann Universe of Sets

Starting with ~~$V_0 = \{\emptyset\}$~~, or $\boxed{V_0 = \emptyset\,??}$

recursively $V_{\alpha+1} = \mathcal{P}(V_\alpha)$

$V_\omega = V_0 \cup V_1 \cup V_2 \cup \cdots$

$V_{\omega+1} = \mathcal{P}(V_\omega)$

$V_{\omega+2} = \mathcal{P}(V_{\omega+1})$

$\vdots$

$V_{\omega\cdot 2} = V_{\omega+\omega} = V_0 \cup V_1 \cup \cdots \cup V_\omega \cup V_{\omega+1} \cup V_{\omega+2} \cup \cdots$

"Keep going"

$V_0, V_1, V_2, \ldots$

$V_a \longmapsto V_{\omega+a}$

Axioms of ZFC : Language '$\in$', '$=$' or just '$\in$' (include '$=$' as a standard symbol in first order logic)

Axiom of Extensionality Two sets are equal iff they have the same elements.

$(\forall x)(\forall y)[\ (\forall z)((z\in x)\leftrightarrow(z\in y)) \ \rightarrow\ (x=y)\ ]$

Axiom of Foundation No set x can satisfy $x\in x$. More generally, there is no infinite descending sequence $x_0 \ni x_1 \ni x_2 \ni x_3 \ni x_4 \ni \cdots$ (*)

Every nonempty set x has an element $y\in x$ which is disjoint from x, i.e. $y\cap x=\emptyset$.

$(\forall x)(\ x\neq\emptyset \rightarrow (\exists y)(y\in x \ \wedge\ y\cap x=\emptyset))$

$(\forall x)(((\exists z)(z\in x)) \rightarrow (\exists y)((y\in x) \wedge \neg(\exists z)(z\in y \wedge z\in x)))$

This is equivalent to (*). If $x_0\ni x_1\ni x_2\ni x_3\ni\cdots$ then $y=\{x_0,x_1,x_2,x_3,\ldots\}$ is a nonempty set but if we take any element of y, it has the form x_n for some n, with $x_{n+1}\in y\cap x_n$.

Conversely if our new axiom fails then $x_0\ni x_1\ni x_2\ni\cdots$

~~$\{x : \phi(x)\}$~~

$B=\{x\in A : \phi(x)\}$

Use Axiom schema of Separation / Selection / Specification : (one axiom for each formula $\phi(x)$)

$(\forall A)(\exists B)(\forall x)((x\in B)\leftrightarrow(x\in A \ \wedge\ \phi(x)))$

$(\forall x \in A)(\phi(x))$ means $(\forall x)((x \in A) \to \phi(x))$

$(\exists x \in A)(\phi(x))$ ... $(\exists x)((x \in A) \wedge \phi(x))$

$(\exists! x \in A)(\phi(x))$. $(\exists x)((x \in A) \wedge \phi(x)) \wedge [(\forall w)((w \in A) \wedge \phi(w)) \to w = x]$

Axioma Schema of Replacement

If you had a function $f: A \to B$ then we want to say the image $C = \{f(a) : a \in A\}$ is a set. Here f can be implicitly defined by a formula $\phi(x,y)$ if for every $x \in A$ there is a unique $y \in B$ satisfying $\phi(x,y)$.

$(\forall A)(\forall B)[(\forall x \in A)(\exists! y \in B)(\phi(x,y)) \to (\exists C)(\forall y)((y \in C \leftrightarrow ((y \in B) \wedge (\exists x \in A)(\phi(x,y)))]$

Axiom of Pairing Justifies $\{x,y\}$.

$(\forall x)(\forall y)(\exists A)((x \in A) \wedge (y \in A))$ Then $\{z \in A : (z = x) \vee (z = y)\} = \{x,y\}$

Note: If $x = y$ this reduces $\{x\}$. (Uses Selection Axiom)

$A \cap B = \{x \in A : x \in B\}$

Axiom of Union Justifies $A \cup B$.

$(\forall A)(\forall B)(\exists S)(\forall x)((x \in S) \leftrightarrow (x \in A \vee x \in B))$.

Axiom of Power Set Given A, we want $B = \mathcal{P}A = \{\text{subsets of } A\}$.

$(\forall A)(\exists B)(\forall y)[(y \subseteq A) \to (y \in B)]$

$(\forall A)(\exists B)(\forall y)[(\forall z)(z \in y \to z \in A) \to (y \in B)]$

Axiom of Infinity

Justifies $\omega = \{0, 1, 2, 3, 4, \dots\}$ where $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, $\dots$

$$(\exists S)\left[(\emptyset \in S) \wedge (\forall x \in S)(x \cup \{x\} \in S)\right]$$

$$(\exists z)\left[(\forall x)(\neg(x \in z)) \wedge (z \in S)\right]$$

Axiom of Choice For any collection C of nonempty sets, there exists a function assigning to each $A \in C$ an element of A.

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \rotatebox{90}{$\in$}$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad f(A)$

A relation between A and B is a subset of $A \times B$; a function $A \to B$ is a relation satisfying $(a, b), (a, b') \in A \times B \to b = b'$.

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

Kuratowski $(a, b) = \{\{a\}, \{a, b\}\}$.

WyoCourses (Math 5590-01) $\to$ Calendar $\to$ April 2023

Calendar Feed link (below)

ZFC Axioms. Models?

How about the entire Von Neumann universe $V = \bigcup_{\alpha} V_\alpha$? No, this is not a set; it is a proper class. What about V_α for some "sufficiently large" ordinal α?

This requires that $|\alpha|$ be inaccessible i.e.

(1) $|\alpha| > |\omega| = \aleph_0$ (α is uncountable)

(2) If $|\lambda| < |\alpha|$ then $2^{|\lambda|} < |\alpha|$

(3) If $\{\lambda_\beta : \beta \in B\}$ is a collection of smaller ordinals $|\lambda_\beta| < |\alpha|$ for all $\beta \in B$, $|B| < |\alpha|$ then $\sup_{\beta \in B} |\lambda_\beta| < |\alpha|$

V_ω satisfies (2), (3) but not (1).

Ordinals: sets which are well-ordered by '$\in$'. They are the canonical examples of well-ordered sets.

$\emptyset = 0$

$\{\emptyset\} = 1 = \{0\}$

$\{\emptyset, \{\emptyset\}\} = 2 = \{0,1\} = 1 \cup \{1\}$

$3 = \{0,1,2\}$ $\quad 0 \in 1 \in 2$

$\vdots$

$\omega = \{0,1,2,3,\cdots\}$

$\omega+1 = \omega \cup \{\omega\}$

$\omega+2 = \omega+1 \cup \{\omega+1\}$

$\alpha+1 = \alpha \cup \{\alpha\}$

$3 = 2 \cup \{2\}$ etc.

Every ordinal is either a successor (eg. $1,2,3,\dots;\ \omega+1$) or a limit ordinal. eg. $0, \omega$

Cardinal numbers are the names for cardinalities of sets.
These may be viewed as a proper subclass of the ordinals:

$$\begin{array}{llllllllllllllllllllll}
\text{Ordinals} & 0, & 1, & 2, & 3, & \cdots, & \omega, & \omega+1, & \cdots, & \omega_1, & \cdots, & \omega_2, & \cdots, & \omega_3, & \cdots & , \omega_\omega \\
 & & & & & & \| & & & \| & & \| & & \| & & \| \\
\text{Cardinals} & 0, & 1, & 2, & 3, & \cdots, & \aleph_0 & & & \aleph_1 & & \aleph_2 & & \aleph_3, & \cdots & \aleph_\omega
\end{array}$$

$$\omega+1 = \{0,1,2,3,\cdots\} \cup \{\omega\}$$

V_{ω_n} satisfies (1), (3) but not (2) $\quad (n = 1,2,3,\cdots)$
V_{ω_ω} satisfies (1), (2) but not (3).

We cannot prove in ZFC that inaccessible cardinals exist (unless ZFC is inconsistent).
Usually one adds an extra assumption ("large cardinal axiom") to justify having an inaccessible cardinal).

Transfinite Induction / Recursion

Given a collection of statements S_α ($\alpha \in A$ where A is well-ordered) we can ask for a proof of all these statements by transfinite induction. To prove S_α for all $\alpha \in A$, it is sufficient to prove the following inductive step:

Whenever S_β holds for all $\beta < \alpha$, S_α also holds.

Why? Assuming the inductive step holds for all $\alpha \in A$, we must show S_α holds for all $\alpha \in A$. This is proved by contradiction. If S_α fails for at least one $\alpha \in A$, then $B = \{\alpha \in A : S_\alpha \text{ fails}\}$ is a nonempty subset of A, so there is a least element $\beta \in B$. Then S_α holds for all $\alpha < \beta$ (by minimality of β) so by the inductive step, S_β holds so $\beta \notin B$. Contradiction.

Eg. It is possible to partition $X = \mathbb{R}^3 - \{0\}$ ($0 \in \mathbb{R}^3$ is a single point) into Euclidean lines. (Clearly $\mathbb{R}^3$ can be partitioned into Euclidean lines. Not so obvious for $X = \mathbb{R}^3 - \{0\}$.) Zorn's lemma doesn't give us such a partition (i.e. a maximal set of mutually disjoint lines in X doesn't necessarily cover X).

$|X| = ?$

$|\mathbb{R}^3| = 2^{\aleph_0} = |\mathbb{R}| = |X|.$

$\Sigma \subset \{\text{lines of } \mathbb{R}^3 \text{ contained in } X\}$

$|\Sigma| = 2^{\aleph_0}$

$\ell \cap m = \emptyset$ whenever $\ell \neq m$ in Σ.