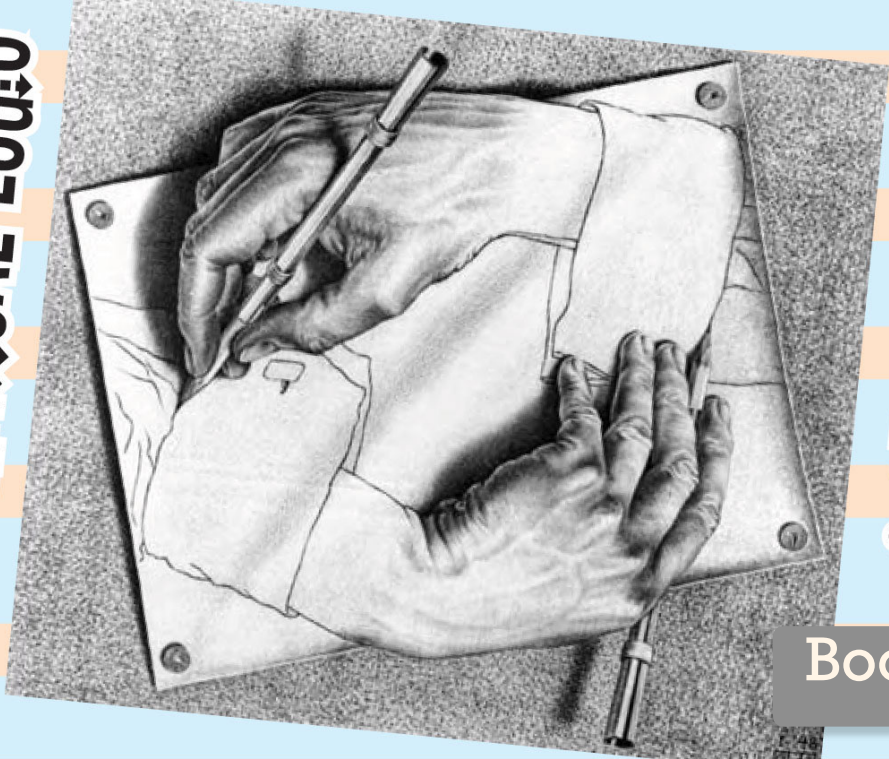


MATHEMATICAL LOGIC



& SET THEORY

Book 1

Group Theory: an example of a first-order axiomatic system

An informal proof in group theory

Theorem If G is a (multiplicative) group of exponent 2, then G is abelian.

(G has exponent n if $g^n = 1$ for all $g \in G$.)

(Informal) proof: Let $a, b \in G$. Since $abab = (ab)^2 = 1$, multiplying on the left by "a" and on the right by "b" gives $aababb = a1b$, i.e. $ba = ab$. \square

Axioms of Group Theory:

ID: $(\forall x) ((x * 1 = x) \wedge (1 * x = x))$

ASSOC: $(\forall x)(\forall y)(\forall z) ((x * y) * z = x * (y * z))$

INV: $(\forall x) (\exists y) ((x * y = 1) \wedge (y * x = 1))$

i.e. $\mu(\mu(x,y),z) = \mu(x,\mu(y,z))$

Start with names for variables x, y, z, \dots (symbols)
Special symbols for first order logic: \exists, \forall , parentheses, \neg, \rightarrow, \dots

Symbols for constants: $1, \dots$

Symbols for functions: $*$, ... $x * y$ means $\mu(x, y)$

Symbols for relations: $=$

We happen to know some groups including C_n (cyclic group of order n), S_n (symmetric group of degree n), ...

GROUPS = $\{ID, ASSOC, INV\} = \{(\forall x)((x * 1) = \dots, \dots, \dots)\}$ (the set consisting of our three axioms of group theory)

S_5 is a group, i.e. $S_5 \models$ GROUPS (S_5 is a model of GROUPS)

ABEL: $(\forall x)(\forall y) (x * y = y * x)$

ABEL-GPS = GROUPS \cup {ABEL}. S_5 is a non-abelian group; $S_5 \not\models$ ABEL; $S_5 \not\models$ ABEL-GPS.

A structure has an underlying set of elements, together with an interpretation of all the symbols for constants, functions, and relations.

How do we rewrite our informal proof (above) as a formal proof in first order logic?

$\Sigma = \text{GROUPS} \cup \{\text{EXP2}\}$ where $\text{EXP2}: (\forall x)(x*x=1)$

ABEL is a theorem in the theory of groups of exponent 2, i.e. $\Sigma \vdash \text{ABEL}$.

A theorem is a sequence of steps $\Sigma \vdash \square$ in which every step follows from previous steps by a statement in Σ , or an axiom of first order logic, or a rule of inference.

$\Sigma \vdash \square$
 $\Sigma \vdash \square$
 $\Sigma \vdash \square$
 \vdots
 $\Sigma \vdash \square$

This is a formal (symbolic) proof!

An outline of a formal proof: $\Sigma \vdash \text{EXP2}$ since $\text{EXP2} \in \Sigma$

$\Sigma \vdash (\text{EXP2} \rightarrow (\forall a)(a*a=1))$ (A4) p.86

$\Sigma \vdash (\forall a)(a*a=1)$ Modus Ponens (R1) p.86

$\Sigma \vdash (\forall b)(b*b=1)$

$\Sigma \vdash (\forall a)(\forall b)((a*b)*(a*b)=1)$

$\Sigma \vdash (\forall a)(\forall b)((a*(a*b))*(a*b)=a*1)$

$\Sigma \vdash (\forall a)(\forall b)(a*b=b*a)$

RICHARDS BORCHERDS
 JOEL DAVID HAMKINS

$\text{ORD3}: (\exists x)(\exists y)(\exists z)[(\forall q)((q=x) \vee (q=y) \vee (q=z)) \wedge (\overset{x \neq y}{\neg(x=y)}) \wedge (\overset{x \neq z}{\neg(x=z)}) \wedge (\overset{y \neq z}{\neg(y=z)})]$

"there are at most three elements"

"there are at least 3 elements"

ABEL is independent of GROUPS (you cannot either prove or disprove that a general group is abelian). GROUPS $\not\vdash$ ABEL and GROUPS $\not\vdash \neg$ ABEL. This is because $C_3 \models \text{GROUPS}$ but $C_3 \not\models \text{ABEL}$ and $S_3 \models \text{GROUPS}$ but $S_3 \not\models \text{ABEL}$.

In an arbitrary first-order theory, with axioms Σ , a statement θ is independent of Σ if

$\Sigma \nvdash \theta$ and $\Sigma \nvdash \neg\theta$:

Soundness Theorem: If $\Sigma \vdash \theta$ then θ holds in every model of Σ i.e. $M \models \theta$ whenever $M \models \Sigma$.

Completeness Theorem: Converse holds: If θ holds in every model of Σ , then it is provable from Σ i.e. if $M \models \theta$ whenever $M \models \Sigma$, then $\Sigma \vdash \theta$.

Assume Σ is consistent

So: θ is independent of Σ iff there are models of Σ in which θ holds, and models of θ in which θ fails.

Σ is consistent if we cannot prove a contradiction from Σ , i.e. $\Sigma \nvdash (\theta \wedge \neg\theta)$ for some θ .

Equivalently, Σ is consistent iff it has a model.

Eq. ABEL is independent of GROUPS.

ORDS

GROUPS is consistent.

GROUPS \cup {ORDS} is consistent since it has a model. In fact it has a unique model up to isomorphism: the cyclic group C_3 of order 3. The group C_3 (or its theory) is categorical.
GROUPS is not categorical. (There are models, but not a unique model.)

An alternative to MV: $(\forall x)(\exists y)((x*y=1) \wedge (y*x=1))$ is to add a function symbol $\iota(\cdot)$ to the language
namely $(\forall x)((x*\iota(x)=1) \wedge (\iota(x)*x=1))$
We already have a binary function symbol $\mu(\cdot, \cdot)$, $\mu(x,y) = x*y$

A theorem of Σ is a statement that can be proved from Σ . A proof is a sequence of statements such....
The theory of Σ is $Th(\Sigma) = \{ \text{statements provable from } \Sigma \} = \{ \text{theorems of } \Sigma \}$.

First order theory of graphs has no symbols for constants or functions; there is only one relation symbol $R(\cdot, \cdot)$, for the binary relation of adjacency. We will abbreviate $R(x, y)$ as $x \sim y$.

Axioms of graph theory: two axioms to indicate that our relation is symmetric and reflexive.

IRREFL: $(\forall x) (\neg(x \sim x))$

SYM: $(\forall x)(\forall y) ((x \sim y) \rightarrow (y \sim x))$

GRAPHS = $\{IRREFL, SYM\}$



\models GRAPHS



$\not\models$ GRAPHS

MIN7: $(\exists x_1)(\exists x_2) \dots (\exists x_7) ((x_1 = x_2) \wedge \dots \wedge (x_6 = x_7))$

"there are at least 7 vertices"

MAX7: $(\exists x_1)(\exists x_2) \dots (\exists x_7) (\forall y) ((y = x_1) \vee \dots \vee (y = x_7))$

"There are at most 7 vertices"

To say that Γ has exactly 7 vertices, we could write

ORD7: $(\exists x_1)(\exists x_2) \dots (\exists x_7) [((x_1 = x_2) \wedge \dots \wedge (x_6 = x_7)) \wedge (\forall y) ((y = x_1) \vee (y = x_2) \vee \dots \vee (y = x_7))]$

GRAPHS \cup $\{ORD7\}$: axioms for graphs with exactly 7 vertices

Axioms for infinite graphs:

GRAPHS \cup $\{MIN1, MIN2, MIN3, MIN4, \dots\}$

In first order graph theory, we cannot express the condition that a graph is finite. We can express the condition that a graph has at most n vertices.

We cannot express the condition that a graph is countably infinite.

The diameter of a graph is the max. distance between two vertices.

The distance between two vertices is the length of the shortest path between them.

eg. To say that a graph has diameter ≥ 2 in first order logic:

$(\forall x)(\forall y) ((x = y) \rightarrow \underbrace{(x \sim y)}_{\text{dist}(x,y)=1}) \vee \underbrace{(\exists z) ((x \sim z) \wedge (z \sim y))}_{\text{dist}(x,y) \leq 2}$

Diameter ≤ 2 :

$(\text{diameter at most } 2) \wedge (\exists x)(\exists y) (\neg(x \sim y) \wedge \neg(x \sim z))$

In first order theory, we can express the condition that a graph has diameter 7 or diameter at most 7 but we cannot express the notion that a graph is connected.

Graphs of diameter ≤ 1 (i.e. cliques): $\text{GRAPHS} \cup \{(\forall x)(\forall y)(x=y) \vee (x \sim y)\} = \text{COMPL_GRPHS}$

has models $K_0, K_1, K_2, K_3, K_4, \dots$

For each cardinality κ (eg. $\kappa = 0, 5, \aleph_0, 2^{\aleph_0}, \dots$) there is a model $K_\kappa \models \text{COMPL_GRPHS}$

and any two models of the countably infinite same cardinality are isomorphic. $|\mathbb{R}| = \text{continuum}$

$\text{COMPL_GRPHS} \cup \{\text{ORD4}\}$ has a unique model $K_\aleph = \square$ up to isomorphism.

$\text{Th}(K_\aleph) = \{ \text{all statements in graph theory that hold in } K_\aleph \}$

K_\aleph (or $\text{Th}(K_\aleph)$) is categorical: K_\aleph is the unique model (up to isomorphism) of

$\text{COMPL_GRPHS} \cup \{\text{ORD4}\}$ or of $\text{Th}(K_\aleph)$

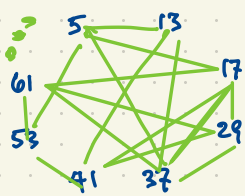
$\text{COMPL_GRPHS} \cup \{\text{MIN1, MIN2, ...}\}$ has infinitely many models. But for each cardinality κ , there is only one model (up to isomorphism) of cardinality κ .

"there are inf. many vertices"

This theory is not categorical but it is κ -categorical.

Consider the graph with countably infinite vertex set $\{5, 13, 17, 29, 37, 41, 53, 61, \dots\}$ (all primes $\equiv 1 \pmod{4}$).

We say $p \sim q$ if p is a nonsquare mod q (iff q is a nonsquare mod p , by Quadratic Reciprocity).
 eg. $5 \sim 13$ ($0, 1, 4$ are squares mod 5 but $2, 3$ are nonsquares mod 5).



Let's call this graph $R \equiv \text{GRAPHS} \cup \{\text{INF}\} \cup \{\mathcal{T}_{m,n} : m, n \in \mathbb{N}\}$

Quadratic Reciprocity
 Dirichlet's Theorem
 Chinese Remainder Theorem

$$\mathcal{T}_{m,n} : (\forall x_i)(\forall x_j) \cdot (\forall y_i)(\forall y_j) \dots (\forall y_n) ((x_i, y_j \text{ distinct}) \rightarrow (\exists z) (z \sim x_1 \wedge \dots \wedge z \sim x_m \wedge z \not\sim y_1 \wedge \dots \wedge z \not\sim y_n))$$

$$x_i \neq x_j \wedge x_i \neq y_1 \wedge \dots \wedge x_i \neq y_n \wedge y_1 \neq y_n$$

$\mathcal{T}_{2,0}, \mathcal{T}_{1,1}, \mathcal{T}_{0,2}$



$R =$ Random graph = Erdős-Rényi graph = Rado graph = Universal Graph

Take any countably infinite set V as vertices.

For all $x \neq y$ in V , flip a coin. Heads? join $x \sim y$. Tails? $x \not\sim y$ (unjoined).
 With probability $1/2$, $R \equiv \mathcal{T}_{m,n}$ for all m, n ; even if the coin is biased.

Theorem Every countably infinite graph satisfying $\mathcal{T}_{m,n}$ for all m, n is isomorphic to R .

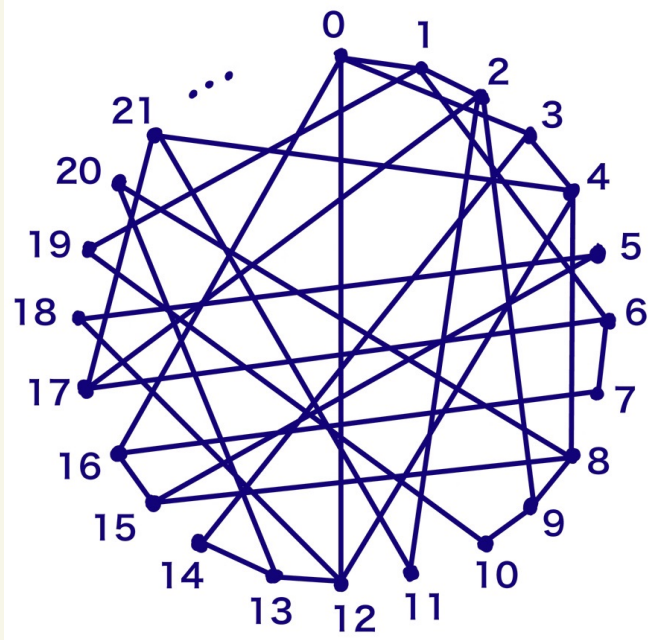
$\text{GRAPHS} \cup \{\text{INF}\} \cup \{\mathcal{T}_{m,n} : m, n \in \mathbb{N}\}$ has only one countable model. (up to isomorphism).

↑ don't need this axiom; it follows from $\{\mathcal{T}_{m,n} : m, n \in \mathbb{N}\}$

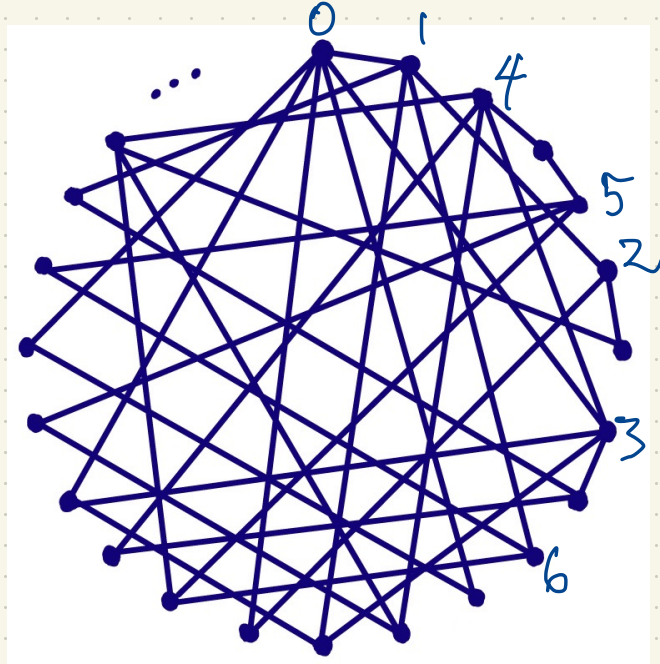
ie. R is \aleph_0 -categorical (countably categorical).

RANDOM :=

Proof First try, via greedy construction of a map $\Gamma \rightarrow \Gamma'$.
Suppose $\Gamma, \Gamma' \in \text{RANDOM}$ and Γ, Γ' have a countably infinite set of vertices.

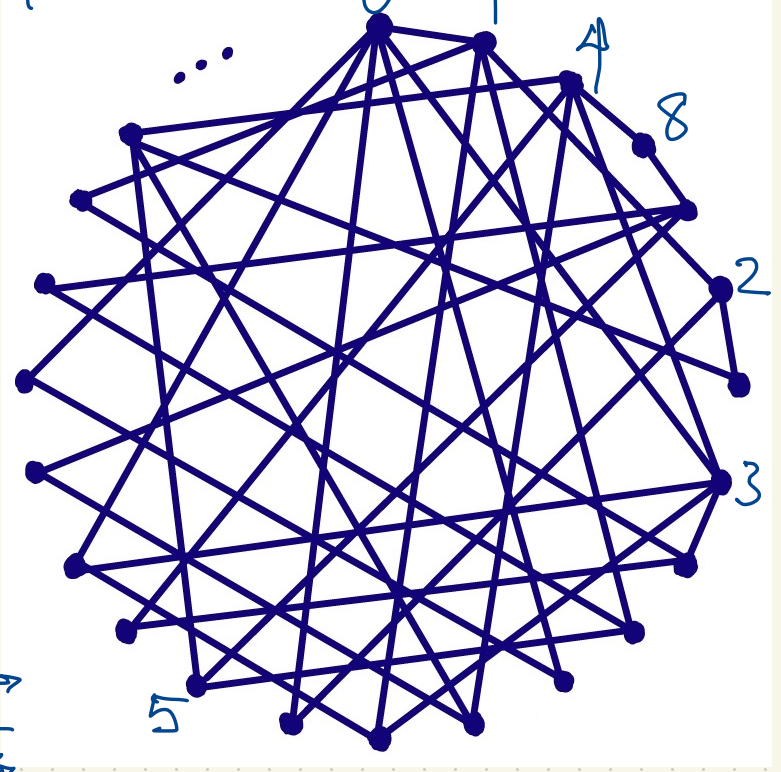
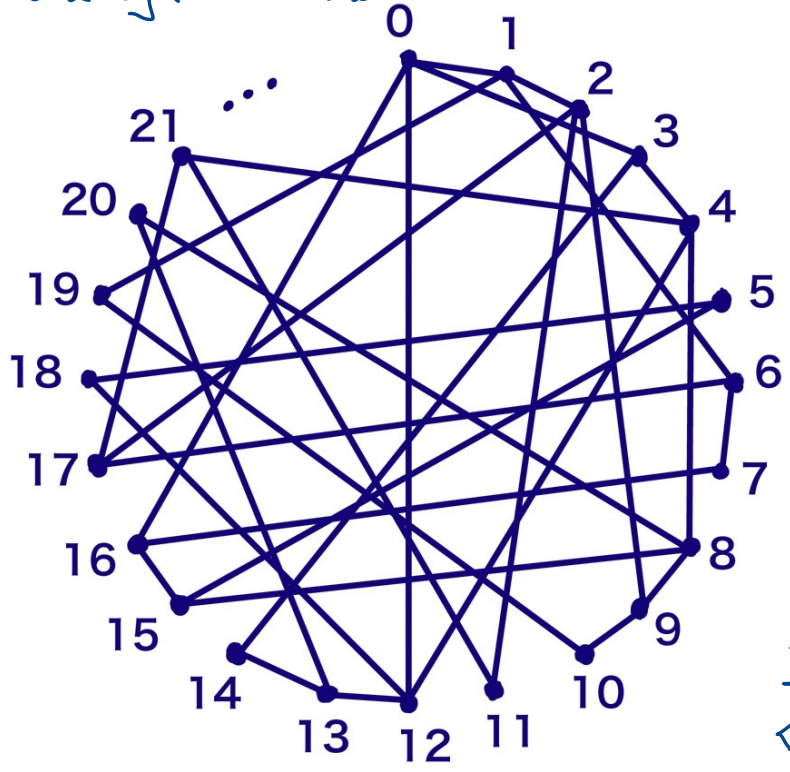


Γ



Γ'

Second try: Back-and-forth construction of isomorphism $\Gamma \rightarrow \Gamma'$



\downarrow
 \uparrow
 \downarrow
 \uparrow
 \downarrow
 \uparrow
 \downarrow
 \uparrow
 \downarrow
 \uparrow
 \downarrow
 \uparrow
 \downarrow

↙

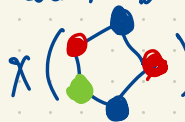
↙

Question: Is there a universal random graph on $|R| = 2^{\aleph_0}$ vertices?

Status of this problem is not fully known, but independent of ZFC, depends on CH; (Shelah)

Chromatic numbers of graphs:

Given a graph Γ , a proper (vertex) coloring of Γ is a coloring of the vertices so that no two vertices of the same color are joined. The chromatic number of Γ , $\chi(\Gamma)$, is the smallest number of colors for which Γ has a proper coloring. Eg.


$$\chi(\Gamma) = 3.$$

Theorem (Appel-Haken) If Γ is a ^{finite} planar graph, then $\chi(\Gamma) \leq 4$.

From this result, the generalization to infinite planar graphs holds:

If Γ is any planar graph, then $\chi(\Gamma) \leq 4$.

First express the condition $\chi(\Gamma) \leq k$ in first order logic:

Language in any first-order system has symbols for constants, r -ary functions, r -ary relations.

We are given a graph Γ and a positive integer k .

Introduce constants v_1, v_2, \dots , one for each vertex of the graph. Also k many relations $C_1(\cdot), \dots, C_k(\cdot)$.

Axioms: $(\forall x)((C_1(x) \vee C_2(x) \vee \dots \vee C_k(x)) \wedge \neg((C_1(x) \wedge C_2(x)) \vee (C_1(x) \wedge C_3(x)) \vee \dots \vee (C_{k-1}(x) \wedge C_k(x))))$

For every pair of adjacent vertices i, j in Γ , include an axiom $\neg(C_l(v_i) \wedge C_l(v_j))$ and each l in $\{1, 2, \dots, k\}$.

Let $\Sigma_{\Gamma, k}$ be the set of axioms listed here. A model of $\Sigma_{\Gamma, k}$, i.e. $M \models \Sigma_{\Gamma, k}$, is a proper k -coloring of Γ . Such a model exists $\iff \chi(\Gamma) \leq k$.

By the compactness theorem, $\Sigma_{\Gamma, k}$ has a model iff every finite subset of $\Sigma_{\Gamma, k}$ has a model i.e. iff every finite subgraph of Γ has chromatic number $\leq k$.

More generally, if Γ is any infinite graph, then $\chi(\Gamma) = k$ iff every finite subgraph $\Gamma_0 \subseteq \Gamma$ has $\chi(\Gamma_0) \leq k$; and $\chi(\Gamma_0) = k$ for some finite $\Gamma_0 \subseteq \Gamma$.

By the way, the compactness theorem follows easily from the completeness theorem. We won't prove the completeness theorem. Here's the argument in the case of graph coloring:

If $\Sigma_{\Gamma, k}$ has a model $M \models \Sigma_{\Gamma, k}$, then every finite subset $\Sigma_0 \subseteq \Sigma_{\Gamma, k}$ has a model $M \models \Sigma_0$.

Conversely, suppose every finite subset $\Sigma_0 \subseteq \Sigma_{\Gamma, k}$ has a model ("every finite subgraph $\Gamma_0 \subseteq \Gamma$ is properly k -colorable"). Suppose $\Sigma_{\Gamma, k}$ does not have a model (Γ is not properly k -colorable). This says $\Sigma_{\Gamma, k}$ is inconsistent and we can derive a contradiction from $\Sigma_{\Gamma, k}$ by the completeness theorem i.e.

$\Sigma_{\Gamma, k} \vdash (\theta \wedge \neg\theta)$ for some θ . A proof of $\theta \wedge \neg\theta$ from $\Sigma_{\Gamma, k}$ only uses finitely many of our constants v_i , C_j and relations. These v_i 's lie in a finite subgraph $\Gamma_0 \subseteq \Gamma$. This is a contradiction.



K_5



K_4



$K_{3,3}$



is not planar: it has K_5 as a minor.

Axioms for linear (total) order:

Language: single binary relation symbol $R(\cdot, \cdot)$. We denote $R(x, y)$ by $x < y$.

Axioms for linear order: $(\forall x)(\forall y) ((x=y) \vee (x < y) \vee (y < x))$

Nonempty axiom: $(\exists x)(x=x)$

$$(\forall x)(\forall y) (\neg(x=y) \leftrightarrow ((x < y) \vee (y < x)))$$

$$(\forall x)(\forall y) (\neg((x < y) \wedge (y < x)))$$

$$(\forall x)(\forall y)(\forall z) (((x < y) \wedge (y < z)) \rightarrow (x < z))$$

Dense linear order without endpoints:

axioms for linear order

$$(\forall x)(\forall y) ((x < y) \rightarrow (\exists z) ((x < z) \wedge (z < y)))$$

$$(\forall x)(\exists y) (x < y)$$

$$(\forall x)(\exists y) (y < x)$$



Models of "dense linear order without endpoints":

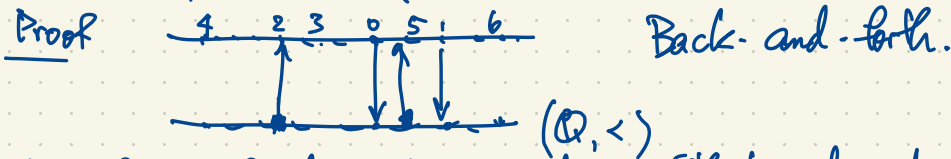
Here are three models, no two of which are isomorphic.

$\left. \begin{array}{l} (0, 1) \subset \mathbb{R}, \text{ with usual } '<' \\ \mathbb{R} \text{ with usual } '<' \\ \mathbb{Q} \text{ with ordinary } '<' \end{array} \right\} \text{ isomorphic}$

There are many uncountable models. For every uncountable cardinality κ , there are many models of cardinality κ .

$\left[\begin{array}{l} \mathbb{Q} \text{ with ordinary } '<' \\ \mathbb{Q} \cup (0, 1) \text{ with ordinary } '<' \end{array} \right]$

Theorem ^(Cantor) $(\mathbb{Q}, <)$ is "dense linear order without endpoints" \models the unique countable model up to isomorphism.



The theory of dense linear orders without endpoints is \aleph_0 -categorical (countably categorical).

Other \aleph_0 -categorical theories: the theory of the complete graph; the theory of the random graph.

"Dense linear order without endpoints" is not \aleph_1 -categorical for any uncountable cardinality.

Theorem (Morley) If a theory is \aleph_1 -categorical for some uncountable cardinality \aleph_1 , then it is \aleph_1 -categorical for all uncountable \aleph_1 (hence "uncountably categorical").

Linear Algebra: what are suitable axioms for vector spaces? Fix a field F and write down axioms for vector spaces over F . One way: All elements of the domain (underlying set of the model) are vectors. Implement scalar multiplication using unary functions $\mu_c(\cdot)$ $c \in F$ in addition to binary function "+" for adding vectors. We'll also use a constant symbol '0'.

Axioms:

$$\begin{aligned} & (\forall v)(\forall w)(v+w = w+v) \\ & (\forall u)(\forall v)(\forall w)((u+v)+w = u+(v+w)) \\ & (\forall v)(0+v = v) \end{aligned}$$

Axiom Schema

$$\begin{aligned} & (\forall v)(\mu_c(\mu_d(v)) = \mu_{cd}(v)) \quad (\text{for every } c, d \in F \text{ we have such an axiom}) \\ & (\forall v)(\mu_c(v) + \mu_d(v) = \mu_{cd}(v)) \\ & (\forall v)(\forall w)(\mu_c(v+w) = \mu_c(v) + \mu_c(w)) \end{aligned}$$

$$(\forall v)(\mu_1(v) = v)$$

$$(\forall v)(\mu_0(v) = 0)$$

Models of this theory are vector spaces over F .

There can be nonisomorphic models of the same cardinality.

Suppose $F = \mathbb{Q}$. For every uncountable K , there is a unique model of cardinality K up to isomorphism (the theory of rational vector spaces is uncountably categorical) but not for $K = \aleph_0$: there are infinitely many vector spaces of cardinality \aleph_0 .

$$\mathbb{Q}, \mathbb{Q}^2, \mathbb{Q}^3, \mathbb{Q}^4, \dots, \mathbb{Q}^\omega = \bigcup_{n=1}^{\infty} \mathbb{Q}^n$$

Think of $\mathbb{Q}^\omega = \mathbb{Q}[t]$ as the vector space of all polynomials in t with rational coefficients;

$$\mathbb{Q}^n = \{ f(t) \in \mathbb{Q}[t] : \deg f(t) < n \} \quad \text{has basis } \{1, t, t^2, t^3, \dots, t^{n-1}\}$$

$$\mathbb{Q}^\omega \text{ has basis } \{1, t, t^2, t^3, \dots\}$$

$$\mathbb{Q}[t]$$

Don't confuse with $\mathbb{Q}[[t]]$ = all power series in t with rational coefficients which has uncountable dimension.

Theorem of Engeler, Ryll-Nardzewski, Svenonius: \aleph_0 -categoricity of M is equivalent to a "large" group of automorphisms of M : $\text{Aut } M$ has only finitely many orbits on k -tuples of "points" (elements of M). Such a group is called oligomorphic. Examples

Any two k -sets of distinct rationals are in the same orbit of $\text{Aut}(\mathbb{Q}, <)$.
For the countable random graph R , the number of orbits on k -sets of distinct vertices
for $k=1, 2, 3, 4, \dots$ gives a sequence

1, 2, 4, 11, 34, ...

Nothing is better than a meal in a four-star restaurant.

A plain cafeteria meal is better than nothing.

Therefore a plain cafeteria meal is better than a meal in a four-star restaurant.