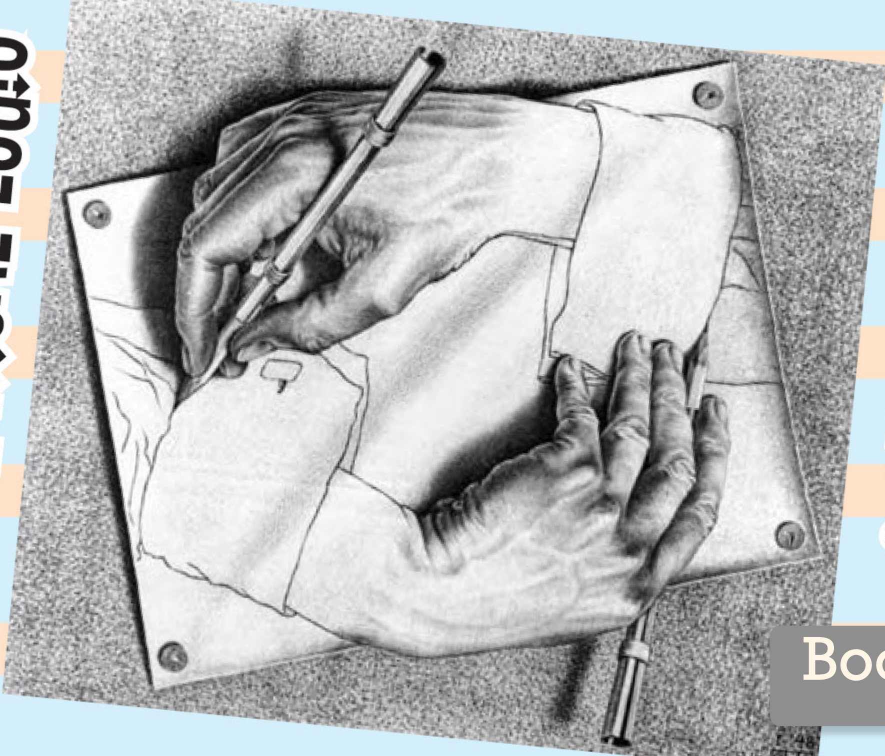
MATHEMATICAL LOGIC & SET THEORY



Book 1

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

An informal proof in group theory

<u>Theorem</u> 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) <u>proof</u>: 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:

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

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

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

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

Start with names for variables $x, y, z, \ldots$ (symbols)

Special symbols for first order logic: $\exists$, $\forall$, parentheses, $\wedge$, $\vee$, $\neg$, $\rightarrow$, …

Symbols for constants: $1, \ldots$

Symbols for functions: $*, \ldots$ $\quad$ $x*y$ 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} = $\{(\forall x)((x*1)= \ \ldots, \ \ldots, \ \ldots\}$ (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 <u>model</u> 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?

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

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

A ~~theorem~~ is a sequence of steps

$\Sigma \vdash \boxed{}$

$\Sigma \vdash \boxed{}$

$\Sigma \vdash \boxed{}$

$\vdots$

$\Sigma \vdash \boxed{}$

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.

This is a formal (symbolic) proof!

An outline of a formal proof:

$\Sigma \vdash$ EXP2 since EXP2 $\in \Sigma$

$\Sigma \vdash$ (EXP2 $\to (\forall a)(a * a = 1)$) (A4) p.86

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

$\vdots$

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

$\vdots$

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

$\vdots$

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

$\vdots$

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

RICHARDS BORCHERDS

JOEL DAVID HAMKINS

$$\text{ORD3}: \underbrace{(\exists x)(\exists y)(\exists z)[(\forall g)((g=x) \vee (g=y) \vee (g=z))}_{\text{"there are at most three elements"}} \wedge \underbrace{(\overset{x \neq y}{\neg(x=y)}) \wedge (\overset{x \neq z}{\neg(x=z)}) \wedge (\overset{y \neq z}{\neg(y=z)})]}_{\text{"there are at least 3 elements"}}$$

ABEL is independent of GROUPS (you cannot either prove or disprove that a general group is abelian). GROUPS $\nvdash$ ABEL and GROUPS $\nvdash \neg$ABEL. This is because $C_3 \models$ GROUPS, $C_3 \models$ ABEL but $S_3 \models$ GROUPS, $S_3 \not\models$ 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, ie. $\Sigma \nvdash (\theta \wedge \neg\theta)$ for some θ.

Equivalently, Σ is consistent iff it has a model.

Eg. ABEL is independent of GROUPS.

ORD3 " — — — — " " ".

GROUPS is consistent.

GROUPS $\cup$ {ORD3} 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 categorial. (There are models, but not a unique model.)

An alternative to INV: $(\forall x)(\exists y)((x*y=1) \wedge (y*x=1))$ 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 $Th(\Sigma) = \{\text{statements provable from } \Sigma\} = \{\text{theorems of } \Sigma\}$.

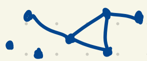
First order theory of graphs has no symbols for constants or functions; there is only one relation symbol $R(\cdot,\cdot)$, for the binary relation of adjacency. We will abbreviate $R(x,y)$ as $x\sim y$.

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

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

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

GRAPHS = {IRREFL, SYM}

 $\models$ GRAPHS  $\not\models$ GRAPHS

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

"there are at least 7 vertices"

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

"There are at most 7 vertices"

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

ORD7: $(\exists x_1)(\exists x_2)\cdots(\exists x_7)\left[((\neg(x_1=x_2))\wedge\cdots\wedge(\neg(x_6=x_7)))\ \wedge\ (\forall y)((y=x_1)\vee(y=x_2)\vee\cdots\vee(y=x_7))\right]$

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

Axioms for infinite graphs:

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

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 17 vertices.

- - - - - - - - - - - - is infinite.

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 at most 2 in first order logic:

$$(\forall x)(\forall y)(\neg(x=y))\to(\underbrace{(x\sim y)}_{\mathrm{dist}(x,y)=1}\vee\underbrace{(\exists z)((x\sim z)\wedge(z\sim y))}_{\mathrm{dist}(x,y)\le 2})$$

Diameter 2:

(diameter at most 2) $\wedge(\exists x)(\exists y)((\neg(x\sim y))\wedge\neg(x=y))$

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): GRAPHS $\cup \{(\forall x)(\forall y)((x=y) \vee (x \sim y))\}$ = COMPL_GRPHS

has models K_0, K_1, K_2, K_3, K_4, ...

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

countably infinite $|\mathbb{R}|$ = continuum

and any two models of the same cardinality are isomorphic.

COMPL_GRPHS $\cup$ {ORD4} has a unique model K_4 =  up to isomorphism.

Th(K_4) = { all statements in graph theory that hold in K_4 }

K_4 (or Th(K_4)) is categorical: K_4 is the unique model (up to isomorphism) of

COMPL_GRPHS $\cup$ {ORD4} or of Th(K_4)

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

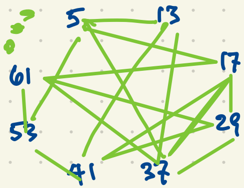
"there are inf. many vertices"

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

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

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).

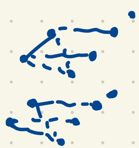


Let's call this graph $R \models \text{GRAPHS} \cup \{\text{INF}\} \cup \{\gamma_{m,n} : m,n \in \mathbb{N}\}$

Quadratic Reciprocity
Dirichlet's Theorem
Chinese Remainder Theorem

$\gamma_{m,n}$: $(\forall x_1)(\forall x_2)\cdots(\forall x_m)(\forall y_1)(\forall y_2)\cdots(\forall y_n)\big((x_i, y_j \text{ distinct}) \to (\exists z)(z \sim x_1 \wedge \cdots \wedge z \sim x_m \wedge z \not\sim y_1 \wedge \cdots \wedge z \not\sim y_n)\big)$

$x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge \cdots \wedge x_1 \neq y_1 \wedge \cdots \wedge y_{n-1} \neq y_n$



$\gamma_{1,0}$, $\gamma_{1,1}$, $\gamma_{0,2}$

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, $R \models \gamma_{m,n}$ for all m,n; even if the coin is biased.

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

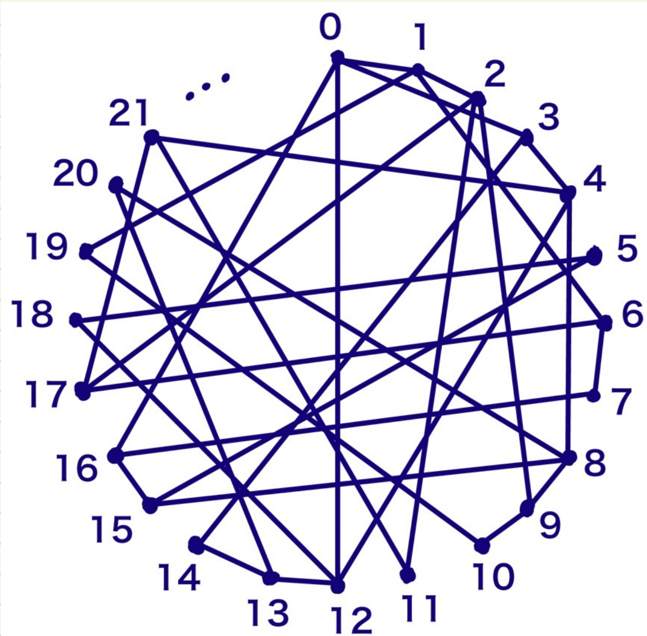
$\text{GRAPHS} \cup \{\text{INF}\} \cup \{\gamma_{m,n} : m,n \in \mathbb{N}\}$ has only one countable model. (up to isomorphism).

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

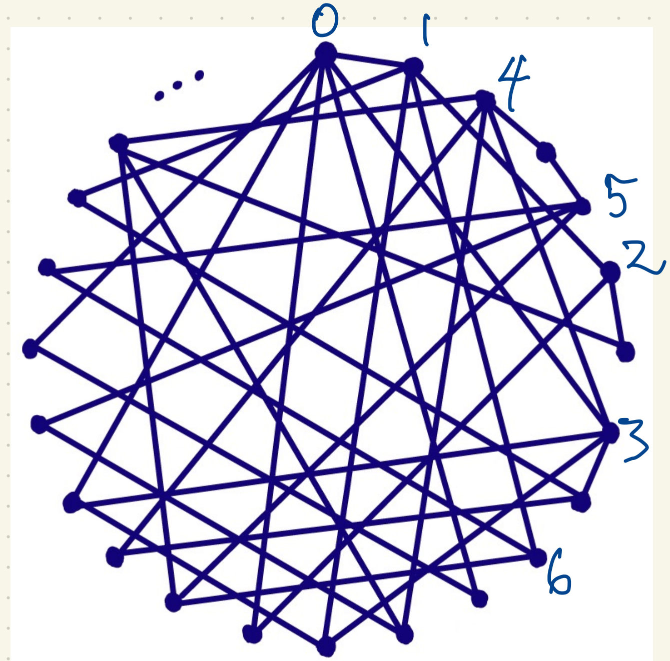
i.e. R is $\aleph_0$-categorical (countably categorical).

RANDOM :=

Proof First try, via greedy construction of a map $\Gamma \to \Gamma'$.
Suppose $\Gamma, \Gamma' \models$ RANDOM and Γ, Γ' have a countably infinite set of vertices.

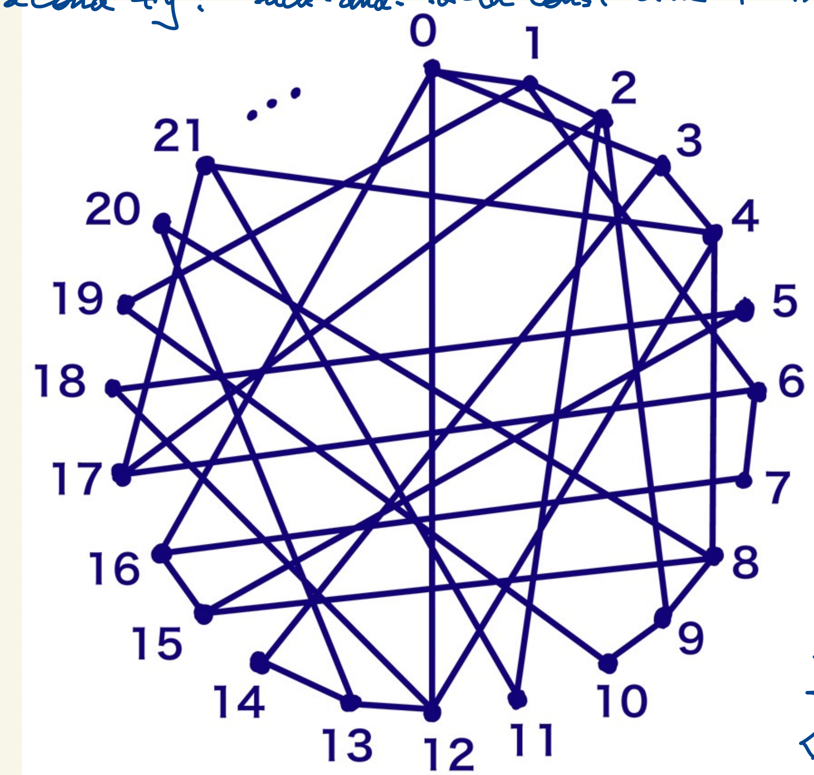


Γ



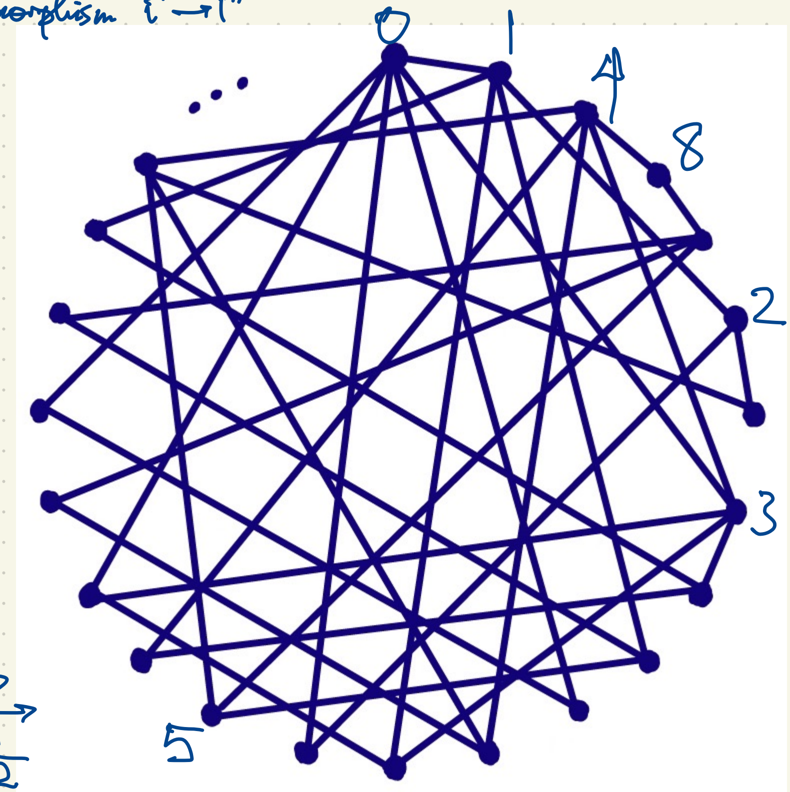
Γ'

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



Γ

$\xrightarrow{0}$
$\xleftarrow{1}$
$\xrightarrow{2}$
$\xleftarrow{4}$
$\xrightarrow{3}$
$\xleftarrow{8}$
$\xrightarrow{5}$

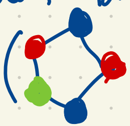


Γ'

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

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

__Theorem__ (Appel-Haken) If Γ is a finite planar graph, then $\chi(\Gamma) \le 4$.

From this result, the generalization to infinite planar graphs holds:
If Γ is any planar graph, then $\chi(\Gamma) \le 4$.

First express the condition $\chi(\Gamma) \le k$ 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 $v_1, v_2, \cdots$, one for each vertex of the graph. Also k many relations $C_1(\cdot), \cdots, C_k(\cdot)$.
Axioms: $(\forall x)\big((C_1(x) \vee C_2(x) \vee \cdots \vee C_k(x)) \wedge \neg((C_1(x) \wedge C_2(x)) \vee (C_1(x) \wedge C_3(x)) \vee \cdots \vee (C_{k-1}(x) \wedge C_k(x))\big)$
For every pair of adjacent vertices $i \sim j$ in Γ, and each l in $\{1, 2, \cdots, k\}$, include an axiom $\neg(C_l(v_i) \wedge C_l(v_j))$.
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 exist iff $\chi(\Gamma) \le k$.

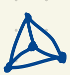
By the compactness theorem, $\Sigma_{\Gamma,k}$ has a model iff every finite subset of $\Sigma_{\Gamma,k}$ has a model i.e. iff every finite subgraph of Γ has chromatic number $\leq k$.

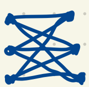
More generally, if Γ is any infinite graph, then $\chi(\Gamma) = k$ iff every finite subgraph $\Gamma_0 \subseteq \Gamma$ has $\chi(\Gamma_0) \leq k$; and $\chi(\Gamma_0) = k$ for some finite $\Gamma_0 \subseteq \Gamma$.

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, and relations C_j. 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:

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

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

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

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

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

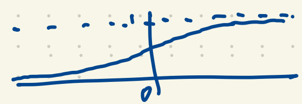
Dense linear order without endpoints:

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":

$(0,1) \subset \mathbb{R}$, with usual '<'
$\mathbb{R}$ with usual '<'.
} isomorphic

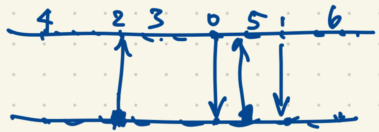
$\mathbb{Q}$ with ordinary '<'

$\mathbb{Q} \cup (0,1)$ with ordinary '<'

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

There are <u>many</u> uncountable models. For every uncountable cardinality κ, there are <u>many</u> models of cardinality κ.

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

Proof  $(\mathbb{Q}, <)$ Back-and-forth.

The theory of dense linear orders without endpoints is $\aleph_0$-categorical (countably categorical, ω-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 κ-categorical for any uncountable cardinality.

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

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: $(\forall v)(\forall w)(v+w = w+v)$

$(\forall u)(\forall v)(\forall w)((u+v)+w = u+(v+w))$

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

Axiom Schema

$(\forall v)(\mu_c(\mu_d(v)) = \mu_{cd}(v))$ (for every $c, d \in F$ we have such an axiom)

$(\forall v)(\mu_c(v) + \mu_d(v) = \mu_{c+d}(v))$

$(\forall v)(\forall w)(\mu_c(v+w) = \mu_c(v) + \mu_c(w))$

$(\forall v)(\mu_1(v) = v)$
$(\forall v)(\mu_0(v) = 0)$

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 κ, there is a unique model of cardinality κ up to isomorphism (the theory of rational vector spaces is uncountably categorical) but not for $\kappa = \aleph_0$: there are infinitely many vector spaces of cardinality $\aleph_0$.

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

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

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

$\mathbb{Q}^\omega$ has basis $\{1, t, t^2, t^3, \ldots\}$
$\quad = \mathbb{Q}[t]$

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: $\mathrm{Aut}\, M$ has only finitely many orbits on k-tuples of "points" (elements of M). Such a group is called <u>oligomorphic</u>. <u>Examples</u>

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

$$1, 2, 4, 11, 34, \ldots$$

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.

Why would we not allow the domain of a model (the underlying set) to be empty?

$\vdash (\forall x)(\phi(x)) \to \phi(a)$

$\vdash \phi(a) \to (\exists x)(\phi(x))$

$\vdash (\forall x)(\phi(x)) \to (\exists x)(\phi(x))$

Clarification: structure vs. model

We start with a language L (symbols for constants, relations, functions).
Any interpretation of the symbols in L on an underlying set (domain) is a structure for L (an L-structure). Given a language L and a set of sentences Σ over L,

a **model** of Σ is an L-structure M satisfying Σ i.e. every sentence $\theta \in \Sigma$ is satisfied by M; we denote $M \models \Sigma$.

How do we understand the statement that if κ is an uncountable cardinal, then a rational vector space of dimension κ is the same thing as a rational vector space of cardinality κ?

$|\mathbb{Q}| = \aleph_0 = |\mathbb{Z}| = |\mathbb{N}|$; $|\mathbb{R}| = 2^{\aleph_0} = |\mathcal{P}(\mathbb{N})|$ ($\mathcal{P}(A)$ = power set of A)

$|\mathbb{Q}^n| = |\mathbb{Q}|$ by induction. If $|A| = \aleph_0$ then $|A \times A| = \aleph_0$

$|\mathbb{Q}^\omega| = \aleph_0$ (union of countably many countable sets is countable).

$$\mathbb{Q}^\omega = \bigcup_{n=1}^{\infty} \mathbb{Q}^n$$

For κ, λ infinite cardinals, $\kappa + \lambda = \kappa\lambda = \max\{\kappa, \lambda\}$

i.e. if A, B are infinite sets then $|A \cup B| = |A \sqcup B| = |A \times B| = \max\{|A|, |B|\}$.

This uses AC (axiom of choice). (And its equivalent to AC.)

If κ is an infinite cardinal and V is a rational vector space, then $\dim V = \kappa \Rightarrow |V| = \kappa$.

Proof Let B be a basis of V. Then $|B| \le |V|$

$$V = \underbrace{\bigcup_{n=1}^{\infty} \underbrace{\bigcup_{v_1,\dots,v_n \in B}}_{} \operatorname{Span}\{v_1,\dots,v_n\}}_{\kappa \cdot \aleph_0 = \kappa}$$

where $|\operatorname{Span}\{v_1,\dots,v_n\}| = |\{a_1v_1 + \cdots + a_nv_n : a_i \in \mathbb{Q}\}| \le \aleph_0$

The number of choices of $(v_1,\dots,v_n) \in B^n$ is $|B^n| = |\underbrace{B \times B \times \cdots \times B}_{n \text{ times}}| = \kappa^n = \kappa$.

$|V| = \aleph_0 \cdot \kappa = \kappa$.

Thus: The theory of rational vector spaces is uncountably categorical but not countably categorical

Fields

Let F be a set containing distinct elements called 0 and 1 (thus $0 \neq 1$). Suppose addition, subtraction, multiplication and division are defined for all elements of F (except division by 0 is not defined). Thus $a+b,\ a-b,\ ab,\ \frac{a}{d} \in F$ whenever $a, b, d \in F$ and $d \neq 0$. Define $-a = 0 - a$.

If the following properties are satisfied by *all* elements $a, b, c, d \in F$ with $d \neq 0$, then F is a field.

$$a+b=b+a \qquad a+(b+c)=(a+b)+c \qquad ab=ba$$
$$a+0=a \qquad a(bc)=(ab)c \qquad 1a=a$$
$$a+(-a)=0 \qquad a(b+c)=ab+ac \qquad \frac{a}{d}d=a$$
$$a+(-b)=a-b$$

A field F has characteristic p if $\underbrace{1+1+1+\cdots+1}_{p} = 0$. (This requires p to be prime) If $1+1+1+1+1+1=0$ then $\underline{(1+1+1)}\,\underline{(1+1)} = 0$. If there is no such p then F has characteristic zero.

If we want to force our field to have characteristic 5, say, add an axiom $1+1+1+1+1=0$.
If we want to work only with characteristic zero fields, then add infinitely many axioms

$$1+1\neq 0$$
$$1+1+1\neq 0$$
$$1+1+1+1\neq 0$$
$$1+1+1+1+1\neq 0$$
etc.

The field of complex numbers is the unique (up to isomorphism) algebraically closed field of characteristic zero having cardinality $2^{\aleph_0}$.

The theory of algebraically closed fields of characteristic zero is uncountably categorical.
(Not countably categorical.)

First order axioms for "algebraically closed":
For each $n\geq 1$ we add an axiom of the form

$$(\forall a_0)(\forall a_1)\cdots(\forall a_{n-1})(\exists z)\left(z^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0=0\right)$$

$$\mathbb{C}\subset\mathbb{C}(x)\subset K=\text{alg. closure of }\mathbb{C}(x)\quad\cong\mathbb{C}$$

$$|\mathrm{Aut}\,\mathbb{C}| = \text{infinite}$$

Given a field F, the <u>algebraic closure</u> of F is the smallest extension field $\overline{F} \supseteq F$ which is algebraically closed, i.e. containing roots of all polynomials in $F[x]$.

eg. $\overline{\mathbb{R}} = \mathbb{C}$, $\overline{\mathbb{C}} = \mathbb{C}$, $\overline{\mathbb{Q}} = \{\text{algebraic numbers}\} \subset \mathbb{C}$ $\quad |\overline{\mathbb{Q}}| = \aleph_0$

$\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$, $|\overline{\mathbb{F}_p}| = \aleph_0$, $\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.

FIELD = { field axioms } (finite set of axioms for all fields)

ALG_CLOS = $\{\alpha_1, \alpha_2, \alpha_3, \dots\}$ $\quad \alpha_n$ is a statement in the language of fields that says every poly. of degree n has a root.

eg. $\alpha_3 : (\forall a)(\forall b)(\forall c)(\exists x)(x^3 + ax^2 + bx + c = 0)$ $\quad$ here x^3 is an abbreviation for $xxx = (xx)x$

ACF = FIELD $\cup$ ALG_CLOS is a set of axioms for algebraically closed fields.

$\mathbb{C} \models$ ACF, $\overline{\mathbb{F}_7} \models$ ACF, $\overline{\mathbb{Q}} \models$ ACF

The statement $1+1+1+1+1+1+1=0$ is true in $\overline{\mathbb{F}_7}$ but not in $\mathbb{C}$ or $\overline{\mathbb{Q}}$.

The theory of algebraically closed fields is not complete ("complete" = "model complete").

$\theta_p : \underbrace{1+1+\cdots+1}_{p} = 0$

$\text{ACF}_p = \text{ACF} \cup \{\theta_p\}$ is a set of axioms for the theory of $\overline{\mathbb{F}_p}$ i.e. $Th(\overline{\mathbb{F}_p}) = \{$ all statements in first-order field theory which hold in $\overline{\mathbb{F}_p}\}$

This theory is complete.

$\text{ACF}_0 = \text{ACF} \cup \{\neg\theta_2, \neg\theta_3, \neg\theta_5, \neg\theta_7, \dots\}$ is a set of axioms for the theory of algebraically closed fields of characteristic zero eg. $\mathbb{C}$, $\overline{\mathbb{Q}}$ so $Th(\mathbb{C}) = Th(\overline{\mathbb{Q}}) = Th(\text{ACF}_0)$ is complete.

For Every statement ξ in the first order theory of fields is either provable or disprovable from ACF_0 i.e. $ACF_0 \vdash \xi$ or $ACF \vdash (\neg \xi)$.

<u>Ax-Grothendiek Theorem</u> Let $f: \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map i.e.

$f(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$ where $f_i(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$.

If f is one-to-one then f is onto.

<u>Proof</u> Take one instance $f(x,y) = (ax^2 + bxy + cy^2 + dx + ey + g,\ hx^2 + jxy + ky^2 + lx + my + n)$ as an example. Consider the statement θ in first-order field theory given by

$$\theta: (\forall a)(\forall b)\cdots(\forall n)\Big[\underbrace{\Big((\forall x_1)(\forall y_1)(\forall x_2)(\forall y_2)\ (f(x_1,y_1) = f(x_2,y_2) \to (x_1 = x_2 \wedge y_1 = y_2))\Big)}_{\text{“}f \text{ is one-to-one”}} \to \underbrace{\Big((\forall x_2)(\forall y_2)(\exists x_1)(\exists y_1)\ (f(x_1,y_1) = (x_2,y_2))\Big)}_{\text{“}f \text{ is onto”}}\Big]$$

We must prove $\mathbb{C} \models \theta$. If not then $\mathbb{C} \models \neg\theta$ and $ACF_0 \vdash (\neg\theta)$. Consider a proof of $\neg\theta$ from ACF_0. Such a proof uses only finitely many of the axioms $\neg\theta_p$. There is some prime p for which $\neg\theta_p$ is not used in the proof of $\neg\theta$. So $\overline{\mathbb{F}_p}$ $(\overline{\mathbb{F}_p} \models \theta_p)$ satisfies $\neg\theta$ $(\overline{\mathbb{F}_p} \models \neg\theta)$. However $\overline{\mathbb{F}_p} \models \theta$. Why? Given $a, b, c, \dots, n \in \overline{\mathbb{F}_p} = \bigcup_{r=1}^{\infty} \mathbb{F}_{p^r}$ so pick r so that $a, b, \dots, n \in \mathbb{F}_{p^r}$. f defines a polynomial map $\mathbb{F}_{p^r} \to \mathbb{F}_{p^r}$ which is one-to-one and therefore onto. Now $\mathbb{F}_{p^n}$ satisfies $\theta \wedge (\neg\theta)$, a contradiction. $\square$

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.

Ł ł   Jerzy Łoś, Robert Vaught (1954)