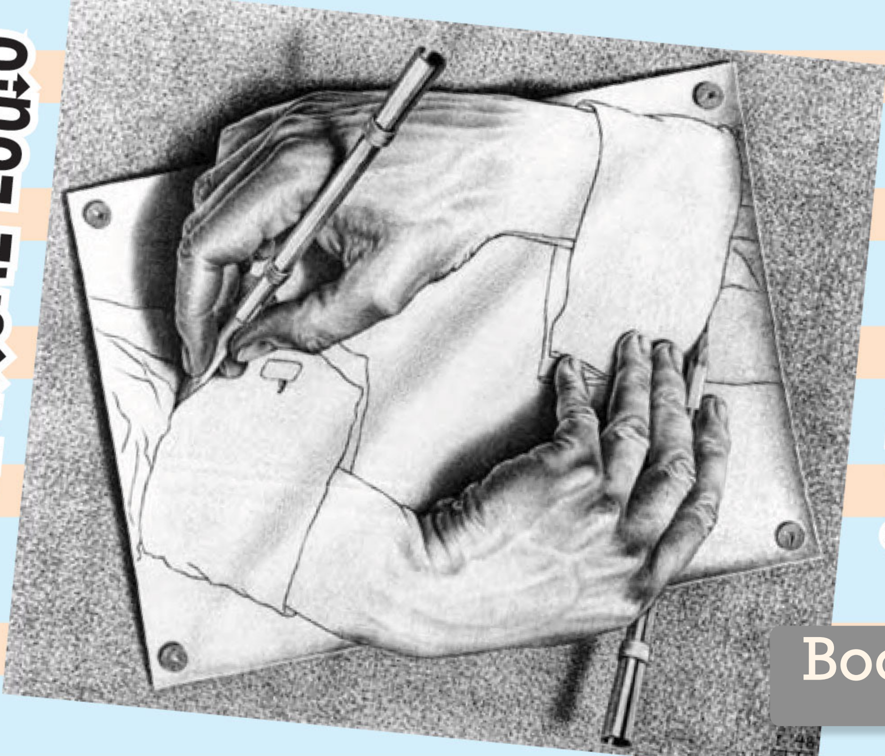
MATHEMATICAL LOGIC & SET THEORY



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.

Ł ł Jerzy Łoś, Robert Vaught (1954)

C-words

Algebra	Topology	Logic
closed	(Cauchy) complete	(model) complete
	continuous	compact
	convergent	categorical
	Connected	
	compact	
	closed	

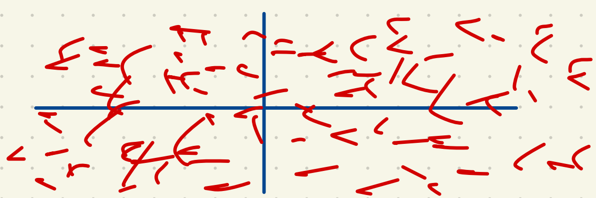
$\aleph_0$

$\aleph_0$

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?

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

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. $t^2 - x \in K[t]$

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

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

$\overline{K}$ 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 $R(a,b)$)

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

$$(\forall a)(\forall b)(\forall c)\big(((a<b) \wedge (b<c)) \to (a<c)\big)$$

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

$\mathbb{R}$ 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?

$$\left.\begin{array}{l}\text{Ordered field axioms}\\ \bullet\ (\forall a)(a\neq 0 \to a^2>0)\\ \bullet\ (\forall a)(a>0 \to (\exists b)(b^2=a))\\ \bullet\ \text{Every polynomial } f(x)\in\mathbb{R}[x] \text{ of odd degree has a root. Eg. for degree 3}\\ \quad (\forall a)(\forall b)(\forall c)(\exists x)(x^3+ax^2+bx+c=0).\end{array}\right]\ \mathrm{RCF}$$

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 $\kappa=\aleph_0$: $\overline{\mathbb{Q}}\cap\mathbb{R}$

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).

$\overline{\mathbb{Q}}$ 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 $f = s_1^2 + \cdots + s_k^2$ 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 $f = s_1^2 + \cdots + s_k^2$ 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

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

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

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

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 $\underbrace{\phi(a) < \phi(b)} \Leftrightarrow a < b$.

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

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

$\Leftrightarrow b - a > 0$

$\Leftrightarrow a < b$.

$\phi(0) = 0$
$\phi(1) = 1$
$\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 1+1 = 2$
$\vdots$
$\phi(n) = n$
$\phi(a) = a$ 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 $f = f(x_1, \dots, x_n) \in \mathbb{R}[x_1, \dots, x_n]$. 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.

$T = \{$ 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 $g \le h$ iff $h-g \in T$.
"$\le$" 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.

$$\tilde{P} + \tilde{P} = \{(a_1 - b_1 f) + (a_2 - b_2 f) = \underbrace{(a_1 + a_2)}_{P} - \underbrace{(b_1 + b_2)}_{P} f : a_i, b_i \in P\} \subseteq \tilde{P}$$

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

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

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

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

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

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