

Model theory studies the map

$$M \longmapsto \text{Th}(M),$$

assigning to a *structure*, M , its complete first-order *theory*, $\text{Th}(M)$.

Example. 0. ACF is the theory of algebraically closed fields, axiomatized by

$$\{\text{field-axioms}\} \cup \{\sigma_n : n > 0\},$$

where σ_n is the sentence

$$\forall \mathbf{x} \exists y y^n + x_{n-1}y^{n-1} + \dots + x_0 = 0.$$

The theory ACF_0 is ACF with additional axioms

$$\{n \cdot 1 \neq 0 : n > 0\}.$$

Then $\text{Th}(\mathbb{C}) = ACF_0$.

1. Also $\text{Th}(\mathbb{R}) = RCF$, axiomatized by

$$\{\text{ordered-field axioms}\} \cup \{\sigma_n : n \text{ odd}\}.$$

2. **Gödel's Incompleteness Theorem:**

$\text{Th}(\mathbb{N})$ has no recursive axiomatization.

A **structure** is a set equipped with functions, relations and constants; its **language** is the set of symbols for the functions, relations and constants.

Example. 0. \mathbf{R} and \mathbf{Z} are structures in the language

$$\{+, -, \cdot, 0, 1, \leq\}$$

of ordered rings.

1. The language $\{\cdot, {}^{-1}, 1\}$ of groups can be augmented with a symbol for the commutator, but *not* for the map $S \mapsto \langle S \rangle$.

Let \mathcal{L} be a language. The **formulas** of \mathcal{L} are built up by formal rules from the symbols of \mathcal{L} , a symbol ($=$) for equality, variables *for individuals*, connectives ($\wedge, \vee, \neg, \rightarrow$), brackets and quantifiers (\forall, \exists).

A **sentence** is a formula with no *free variables*.

Let $\text{Sn}_{\mathcal{L}}$ be $\{\text{sentences of } \mathcal{L}\}$, and let:
 σ range over $\text{Sn}_{\mathcal{L}}$;
 Σ range over subsets of $\text{Sn}_{\mathcal{L}}$;
 M and N be structures of $\text{Sn}_{\mathcal{L}}$.

The following are equivalent by definition:

- σ is true in M .
- M is a model of σ .
- $M \models \sigma$.

$M \models \Sigma$ means $M \models \sigma$ for all σ in Σ .

$\Sigma \models \sigma$ means $M \models \sigma$ whenever $M \models \Sigma$.

$\Sigma \vdash \sigma$ means σ is *provable* from Σ .

Theorem (Gödel's Completeness).

$\Sigma \vdash \sigma$ if and only if $\Sigma \models \sigma$.

Σ is **consistent** if $\Sigma \not\vdash \exists x x \neq x$; so, Σ has a model if it is consistent, by Completeness.

Theorem (Compactness). Σ has a model if every finite subset does.

Σ is a **theory** if $\Sigma = \{\sigma : \Sigma \vdash \sigma\}$.

$\text{Th}(M) = \{\sigma : M \models \sigma\}$.

We say M and N are **elementarily equivalent**, and write $M \equiv N$, if $\text{Th}(M) = \text{Th}(N)$. Isomorphism implies elementary equivalence.

Let T be a consistent theory of \mathcal{L} .

Σ **axiomatizes** T if $T = \{\sigma : \Sigma \vdash \sigma\}$.

T is **complete** if $\sigma \in T$ or $\neg\sigma \in T$ for each σ .

Let T be a complete theory of \mathcal{L} , and let κ be an infinite cardinal. We define

$$I(T, \kappa)$$

to be the number of non-isomorphic models of T of size κ . Then $I(T, \kappa) \leq 2^\kappa$ when $|T| \leq \kappa$.

Theorem (Löwenheim–Skolem).

If $I(T, \kappa) \geq 1$ for some κ with $\kappa \geq |T|$, then for every.

Theorem (Morley–Shelah).

If $I(T, \kappa) = 1$ for some κ with $\kappa > |T|$, then for every.

Hart and Laskowski describe the possible maps $\kappa \mapsto I(T, \kappa)$ for *countable* theories T .

Example. 0. $I(\text{ACF}_0, \kappa) = 1$ when κ is uncountable.

1. $I(\text{RCF}, \kappa) = 2^\kappa$ for all κ .

Henceforth k is an algebraically closed field.

Let FF^m be the class of function-fields in m variables over k .

Let FF be $\bigcup_{n \in \omega} FF^m$; are its elements uniquely determined by their theories?

Say $K \in FF^m$. Then $K = k(a_0, \dots, a_{n-1})$, where the n -tuple (a_0, \dots, a_{n-1}) or \mathbf{a} is a *generic point* of a *variety* $V(\mathbf{a}/k)$, which is the zero-set of the polynomials f over k that are zero at \mathbf{a} .

Conversely, K is the field $k(V(\mathbf{a}/k))$ of rational functions on $V(\mathbf{a}/k)$.

A k -embedding

$$f^* : k(\mathbf{a}) \longrightarrow k(\mathbf{b})$$

with $f^*(a_i) = f_i(\mathbf{b})$ corresponds to the dominant rational map

$$f : V(\mathbf{b}/k) \longrightarrow V(\mathbf{a}/k)$$

with $f(\mathbf{y}) = (f_0(\mathbf{y}), \dots, f_{n-1}(\mathbf{y}))$.

Proposition. *Fields from different classes FF^m have different theories.*

Proof. For K in FF^m , by the Tsen–Lang Theorem,

$$K \models \forall \mathbf{x} \exists \mathbf{y} \left(\sum_{i < n} x_i y_i^2 = 0 \wedge \bigvee_{i < n} y_i \neq 0 \right)$$

just in case $n > 2^m$. □

FF^1 is the class of function fields of *curves* over k . A curve C has a genus $g(C)$ in ω .

Say C_0 and C_1 are curves over k , and there is a k -embedding of $k(C_0) \rightarrow k(C_1)$. By the Hurwitz Theorem, one of the following holds:

$$g(C_0) < g(C_1);$$

$$g(C_0) = g(C_1) > 1, \text{ and } k(C_0) \cong k(C_1);$$

$$g(C_0) = g(C_1) = 0, \text{ so } k(C_0) \cong k(C_1);$$

$$g(C_0) = g(C_1) = 1.$$

Theorem (Duret). *If $k(C_0) \equiv k(C_1)$, then $k(C_0) \cong k(C_1)$, unless $g(C_0) = g(C_1) = 1$.*

Proof. First, k is definable in $k(C_i)$:

Take a curve D with $g(D) > g(C_i)$; say D is given by $X^d + Y^d = 1$ with $(d-1)(d-2) > 2g(C_i)$.

If $a, b \in k(C_i)$ and $(a, b) \in D$, then $a, b \in k$, since otherwise (a, b) would be a generic point of D and we would have a k -embedding

$$k(D) \cong k(a, b) \longrightarrow k(C_i).$$

Hence the formula ' $\exists y x^d + y^d = 1$ ' defines k in $k(C_i)$.

Similarly, and hence, agreement of the theories yields k -embeddings $k(C_i) \rightarrow k(C_{1-i})$.
Now use Hurwitz. □

A curve of genus 1 is an **elliptic curve**, one of the *abelian varieties*. Over \mathbf{C} , it is a torus \mathbf{C}/Λ .

Let E_0 and E_1 be elliptic curves. A rational map $E_0 \rightarrow E_1$ taking identity to identity is an **isogeny** and is a group-homomorphism.

$\text{Hom}(E_0, E_1) = \{\text{isogenies } E_0 \rightarrow E_1\}$ and $\text{End}(E_i) = \text{Hom}(E_i, E_i)$.

There is an embedding

$$n \mapsto [n] : \mathbf{Z} \rightarrow \text{End}(E_i)$$

where $[n]$ is multiplication by n . The degree-map

$$f \mapsto \deg f : \text{Hom}(E_0, E_1) \rightarrow \{1, 2, \dots\} \cup \{\infty\}$$

has $\deg f = [k(E_0) : f^*k(E_1)]$, and we have also

$$f \mapsto \hat{f} : \text{Hom}(E_0, E_1) \rightarrow \text{Hom}(E_1, E_0),$$

where $\hat{f} \circ f = [\deg f]$.

Theorem (P.). *The following are equivalent:*

- *For every integer m there is f in $\text{Hom}(E_0, E_1)$ such that $\gcd(m, \deg f) = 1$.*
- *$k(E_0)$ and $k(E_1)$ agree on all sentences*

$$\forall x_0, \dots, x_{n-1} \exists y \phi(\mathbf{x}, y),$$

where ϕ is quantifier-free.

Proof. (\Rightarrow) There is m (depending on ϕ) such that, if $k \subseteq K$ and

$$K \models \phi(\mathbf{a}, b)$$

for some \mathbf{a} and b from K , then

$$[k(\mathbf{a}, b) : k(\mathbf{a})] \mid m \text{ or } k(\mathbf{a}) \models \exists y \phi(\mathbf{a}, y).$$

(\Leftarrow) If $f \in \text{Hom}(E_0, E_1)$ and the prime p divides $\deg f$, then there are isogenies

$$E_0 \xrightarrow{\ell} E_2 \xrightarrow{h} E_1$$

with $h \circ \ell = f$ and $\deg h = p$; moreover, there are only finitely many possibilities for E_2 (independently of f). □

The elliptic curve E_i has **complex multiplication** if $\text{End}(E_i)$ properly includes the image of \mathbf{Z} .

If E_0 has no complex multiplication, then the conditions of the last theorem obtain only if $E_0 \cong E_1$ (Duret).

Over \mathbf{C} , an isogeny $E_0 \rightarrow E_1$ corresponds to

$$z \mapsto \alpha z : \mathbf{C}/\Lambda_0 \rightarrow \mathbf{C}/\Lambda_1,$$

so $\text{Hom}(E_0, E_1) \cong \{\alpha \in \mathbf{C} : \alpha\Lambda_0 \subseteq \Lambda_1\}$.

Theorem (P.). *If $\text{char } k = 0$ and E_i have complex multiplication, then the following are equivalent:*

- *There are f_i in $\text{Hom}(E_0, E_1)$ with $\text{gcd}(\deg f_0, \deg f_1) = 1$.*
- $\text{End}(E_0) \cong \text{End}(E_1)$.

Proof. (\Rightarrow) There are a_i in \mathbf{Z} with $a_0 \deg f_0 + a_1 \deg f_1 = 1$. The isomorphism $\text{End}(E_1) \rightarrow \text{End}(E_0)$ is

$$\alpha \mapsto \sum_{i < 2} a_i \hat{f}_i \circ \alpha \circ f_i.$$

(\Leftarrow) Over \mathbf{C} , we may assume $E_0 = \mathbf{C}/\langle 1, \tau \rangle$ and $E_1 = \mathbf{C}/\langle 1, n\tau \rangle$, where

$$A\tau^2 + B\tau + C = 0$$

for some integers A, B and C with no common divisor, and $n|A$, so that

$$\text{Hom}(E_0, E_1) = \langle n, A\bar{\tau} \rangle.$$

If $\alpha = nx + Ay\bar{\tau}$, then

$$\deg \alpha = \frac{1}{n} |\alpha|^2 = nx^2 - Bxy + \frac{AC}{n}y^2;$$

the coefficients of the quadratic form have no common factor. \square