Model-theory of elliptic curves

David Pierce

preliminary version: 2005.04.28

These notes are intended for a talk to be given at Bilgi University, Istanbul, April 29, 2005.

Contents

0 Introduction

Model-theory: mathematics done 'self-consciously'—with an eye on language and interconnections.

General question: When are two *structures* mathematically the same (that is, *isomorphic*)?

Necessary model-theoretic condition: when they are *elementarily equivalent*.

When is this condition sufficient?

Is it sufficient when the structures are function-fields of curves over an algebraically closed field?

—Yes, unless the curves are elliptic curves with complex multiplication.

1 Powers of sets

$$\begin{aligned}\omega &= \{0, 1, 2, \dots\} \\ &= \text{closure of } \{\varnothing\} \text{ under } A \mapsto A \cup \{A\} \\ &= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \dots\}.\end{aligned}$$

Then $0 = \varnothing$ and $1 = \{0\} = \{\varnothing\}$.

$n \in \omega$ means $n = \{0, 1, 2, \dots, n-1\}$, so $n \subset_{\mathrm{f}} \omega$.

Let $I \subset_{\mathrm{f}} \omega$, let $M \neq \varnothing$, and define

$$M^I = \{\text{functions from } I \text{ to } M\}.$$

Typical element: $(a_i : i \in I)$ or $i \mapsto a_i$ or $\vec{a}$.

Special case: Elements of M^n are also $(a_0, a_1, \dots, a_{n-1})$, and M^n itself is

$$\underbrace{M \times \cdots \times M}_{n}.$$

$M^0 = \{0\} = 1$.

$M^1 = M$.

Each $\mathcal{P}(M^I)$ is a Boolean algebra, equipped with:

(0) the operations $\cap$, $\cup$ and ${}^{\mathrm{c}}$;

(1) the distinguished elements $\varnothing$ and M^I; and

(2) the relation $\subseteq$.

Special case:

$$\mathcal{P}(M^0) = \mathcal{P}(\{0\}) = \{0, \{0\}\} = \{0, 1\} = 2.$$

One can think of 2 as $\{\mathsf{F}, \mathsf{T}\}$ and identify the study of $\mathcal{P}(M^0)$ with **propositional logic**.

$\mathcal{P}(M^2)$ contains $\{(a, a) : a \in M\}$, the **diagonal** Δ_M.

Let also $J \subset_{\mathrm{f}} \omega$, and let $\alpha : I \to J$. This induces

$$\begin{aligned} M^J &\xrightarrow{\alpha^*} M^I \\ (b_j : j \in J) &\longmapsto (b_{\alpha(i)} : i \in I) \end{aligned}$$

and hence

$$\begin{aligned} \mathcal{P}(M^J) &\xrightarrow{\alpha^* \text{ or } (\alpha^*)''} \mathcal{P}(M^I) \\ B &\longmapsto \{\alpha^*(\vec{b}\,) : \vec{b}\, \in B\} \end{aligned}$$

as well as

$$\begin{aligned} \mathcal{P}(M^I) &\xrightarrow{\alpha_* \text{ or } (\alpha^*)^{-1}} \mathcal{P}(M^J) \\ A &\longmapsto \{\vec{b}\, : \alpha^*(\vec{b}\,) \in A\}. \end{aligned}$$

For example, $\Delta_M = \alpha^* M$ when $\alpha : 2 \to 1$.

Also, let ι be the inclusion of n in $n + 1$. Then

$$\iota^*(b_0, \dots, b_{n-1}, b_n) = (b_0, \dots, b_{n-1}).$$

If $B \subseteq M^{n+1}$, then $\iota^* B = \{\vec{a}\, \in M^n : (\vec{a}\,, b) \in B$ for some b in $M\}$.

If $A \subseteq M^n$, then $\iota_* A = A \times M$.

2 Structures

M becomes a **structure** $\mathfrak{M}$ when equipped with some (or no):

(0) maps $f^{\mathfrak{M}}$ from $M^{n(f)}$ to M for some $n(f)$ in $\omega \smallsetminus \{0\}$; then $f^{\mathfrak{M}}$ is an $n(f)$**-ary operation on** M;

(1) distinguished elements $c^{\mathfrak{M}}$ of M;

(2) subsets $R^{\mathfrak{M}}$ of $M^{n(R)}$ for some $n(R)$ in $\omega \smallsetminus \{0\}$; then $R^{\mathfrak{M}}$ is an $n(R)$**-ary relation on** M.

Then the **signature** $\mathcal{L}$ of $\mathfrak{M}$ consists of the various symbols f, c and R,—**names** for the corresponding operations, elements and relations.

M is the **universe** of $\mathfrak{M}$, and $\mathfrak{M}$ is an **$\mathcal{L}$-structure**.

For example, $\mathbb{R}$ is a structure with signature $\{+, -, \cdot, 0, 1, \leqslant\}$.

Structures with more than one universe are possible, *e.g.* vector-spaces.

Different structures can have the same signature. Any ordered field is a structure with the same signature as $\mathbb{R}$.

Since $M = M^1$ and $1 = M^0$, elements of M are 0-ary operations on M.

Any n-ary operation f on M is identified with the $(n+1)$-ary relation

$$\{(\vec{a}\,, f(\vec{a}\,)) : \vec{a}\, \in M^n\}.$$

Hence the operations, distinguished elements and relations of $\mathfrak{M}$ correspond to certain elements of various $\mathcal{P}(M^n)$: the **primitive relations** of $\mathfrak{M}$.

Suppose $D_I^{\mathfrak{M}} \subseteq \mathcal{P}(M^I)$ and $\coprod_I D_I^{\mathfrak{M}}$ is the smallest subset X of $\coprod_{I \subset_{\mathrm{f}} \omega} \mathcal{P}(M^I)$ such that:

(0) X contains Δ_M and each primitive relation of $\mathfrak{M}$;

(1) $X \cap \mathcal{P}(M^I)$ is a sub-algebra of $\mathcal{P}(M^I)$;

(2) if $\alpha : I \to J$, then $\alpha_*(X \cap \mathcal{P}(M^I)), \alpha^*(X \cap \mathcal{P}(M^J)) \subseteq X$.

The elements of $\coprod_I D_I^{\mathfrak{M}}$ are the **definable relations** of $\mathfrak{M}$.

$\mathcal{L}$-structures $\mathfrak{M}$ and $\mathfrak{N}$ are **isomorphic**,

$$\mathfrak{M} \cong \mathfrak{N},$$

if there is a bijection from M to N taking each primitive relation of $\mathfrak{M}$ to the corresponding relation of $\mathfrak{N}$.

$\mathfrak{M}$ and $\mathfrak{N}$ are **elementarily equivalent**,

$$\mathfrak{M} \equiv \mathfrak{N},$$

if there is an isomorphism from $\coprod_I D_I^{\mathfrak{M}}$ to $\coprod_I D_I^{\mathfrak{N}}$ taking each primitive relation of $\mathfrak{M}$ to the corresponding relation of $\mathfrak{N}$. Then

$$\mathfrak{M} \cong \mathfrak{N} \implies \mathfrak{M} \equiv \mathfrak{N}.$$

Example. All algebraically closed fields of the same characteristic are elementarily equivalent. Their definable sets are the constructible sets over the prime field.

3 Formulas

Every definable relation X of the $\mathcal{L}$-structure $\mathfrak{M}$ has a non-unique name ϕ: a string of symbols from

$$\mathcal{L} \cup \{x_n : n \in \omega\} \cup \{=, \wedge, \neg, \exists\}.$$

Also symbols from $\{\vee, \to, \leftrightarrow, \forall\}$ can be used. Then ϕ is a **formula** (of first-order logic), and X is the **interpretation**

$$\phi^{\mathfrak{M}}$$

of ϕ in $\mathfrak{M}$.

Dictionary: (Here, $n = n(f) = n(R)$, and $\alpha : n \to I$.)

s	$s^{\mathfrak{M}}$
x_k	$\vec{a} \mapsto a_k = \iota^*(\vec{a})$, where $\iota : \{k\} \subseteq I$
$fx_{\alpha(0)} \cdots x_{\alpha(n-1)}$	$\vec{a} \mapsto f^{\mathfrak{M}}(\alpha^*(\vec{a}))$
$Rx_{\alpha(0)} \cdots x_{\alpha(n-1)}$	$\alpha_*(R^{\mathfrak{M}})$
$=$	Δ_M
$\wedge$	$\cap$
$\neg$	${}^{\mathrm{c}}$
$\exists x_k\ \phi$	$\iota^*(\phi^{\mathfrak{M}})$, where $\iota : I \smallsetminus \{k\} \subseteq I$

If $\phi^{\mathfrak{M}} \subseteq M^0$, then ϕ is a **sentence** σ.

If $\sigma^{\mathfrak{M}} = 1$, then σ is **true in** $\mathfrak{M}$:

$$\mathfrak{M} \models \sigma.$$

So truth is a *relation* between sentences and structures.

Let $\mathrm{Th}(\mathfrak{M}) = \{\sigma : \mathfrak{M} \models \sigma\}$, the **theory of** $\mathfrak{M}$; then

$$\mathfrak{M} \equiv \mathfrak{N} \iff \mathrm{Th}(\mathfrak{M}) = \mathrm{Th}(\mathfrak{N}).$$

4 Curves

Let $K = K^{\mathrm{alg}}$. (Perhaps $K = \mathbb{C}$.) If $K \subseteq L$, let

$$\mathbb{A}^n(L) = L^n.$$

Any irreducible p in $K[X, Y]$ determines a **curve** C over K:

$$C(L) = \{(x, y) \in \mathbb{A}^2(L) : p(x, y) = 0\}.$$

Let $(\alpha, \beta) \in C$ and $\{\alpha, \beta\} \nsubseteq K$; then (α, β) is a **generic point of** C **over** K.
The **field of rational functions on** C **over** K, denoted

$$K(C),$$

is generated by

$$\left.\begin{array}{l}(x, y) \longmapsto x \\ (x, y) \longmapsto y\end{array}\right\} : C \longrightarrow \mathbb{A}.$$

these are coordinates of a generic point of C; hence

$$K(C) \cong K(\alpha, \beta).$$

Say also D is a curve over K, with generic point (γ, δ), and

$$h : K(\gamma, \delta) \longrightarrow K(\alpha, \beta)$$

over K. Let $h(\gamma) = f(\alpha, \beta)$ and $h(\delta) = g(\alpha, \beta)$. Then

$$(x, y) \longmapsto (f(x, y), g(x, y)) : C \dashrightarrow D,$$

a **dominant** rational map (its image contains a generic point).
Any such map ϕ induces the K-embedding ϕ^* of $K(D)$ in $K(C)$ given by

$$\phi^*(f) = f \circ \phi.$$

Then

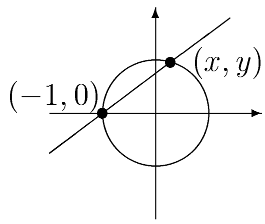
$$\deg \phi = [K(C) : \phi^* K(D)].$$

Example. $K(\mathbb{A}^1) \cong K(X)$. Then

$$\deg(x \mapsto x^n : \mathbb{A}^1 \to \mathbb{A}^1) = [K(X) : K(X^n)] = n.$$

Example. Let C be given by $x^2 + y^2 = 1$, and let

$$\phi : (x,y) \longmapsto \frac{y}{1+x} : C \longrightarrow \mathbb{A}.$$



Let (α, β) be a generic point of C; then

$$\phi^* : f(X) \longmapsto f\left(\frac{\beta}{1+\alpha}\right) : K(X) \longrightarrow K(\alpha,\beta);$$
$$\deg \phi = \left[K(\alpha,\beta) : K\left(\frac{\beta}{1+\alpha}\right)\right] = 1$$

since ϕ^* is invertible: If $t = \beta/(1+\alpha)$, then

$$t^2 = \frac{\beta^2}{(1+\alpha)^2} = \frac{1-\alpha^2}{(1+\alpha)^2} = \frac{1-\alpha}{1+\alpha}; \qquad \alpha = \frac{1-t^2}{1+t^2}; \qquad \beta = \frac{2t}{1+t^2}.$$

Each curve C has a **genus** $\mathrm{g}(C)$ in ω. (A curve over $\mathbb{C}$ is a Riemann surface, hence an orientable surface over $\mathbb{R}$; its genus is the number of holes.)

If $\phi : C \dashrightarrow D$, dominant, then (by the Hurwitz formula)

(0) $\mathrm{g}(C) > \mathrm{g}(D)$, or

(1) $\mathrm{g}(C) = \mathrm{g}(D) \in \{0, 1\}$, or

(2) h is an isomorphism.

If $\mathrm{g}(C) < \mathrm{g}(D)$, then every point of $D(K(\alpha,\beta))$ has coordinates in K.

Theorem.

- *K is a definable subset of $K(C)$.*
- *If $\mathrm{g}(C) \neq 1$ or $\mathrm{g}(D) \neq 1$, then*

$$K(C) \equiv K(D) \iff K(C) \cong K(D).$$

(Jean-Louis Duret proved this in case $\operatorname{char} K = 0$.)

5 Function-fields (optional)

A **function-field** over K is $K(\alpha_0, \dots, \alpha_n)$ (finitely generated). If L_i are such, then

$$L_0 \equiv L_1 \implies \text{tr. deg}(L_0/K) = \text{tr. deg}(L_1/K)$$

by the Tsen–Lang Theorem:

A **quadratic form** over K is a polynomial

$$\vec{x} \ \cdot A \cdot \vec{x}^{\ \mathrm{t}}$$

where $A^{\mathrm{t}} = A$ with entries from K. Then A is diagonalizable, so by change of variables, the form becomes

$$\sum_{i<n} a_i x_i^2.$$

By Tsen and Lang, this form has a non-trivial zero from a function-field L over K if and only if

$$n > 2^{\text{tr. deg}(L/K)}.$$

Every form $ax^2 + by^2 + cz^2$ has a non-trivial zero if and only if every non-trivial equation $ax^2 + by^2 = 1$ has a solution. So a function-field L over K is the function-field of a curve if and only if

$$L \models \forall z \ \forall w \ \exists x \ \exists y \ (zw = 0 \lor zx^2 + wy^2 = 1).$$

Hence in particular

$$K(X) \not\equiv K(X, Y).$$

6 Elliptic curves

A curve of genus 1 is an **elliptic curve**.

A **lattice** is a subgroup $\langle\omega_0, \omega_1\rangle$ of $\mathbb{C}$, where $\omega_0\omega_1 \neq 0$ and $\omega_0/\omega_1 \notin \mathbb{R}$.

Over $\mathbb{C}$, an elliptic curve is a torus

$$\mathbb{C}/\Lambda,$$

Λ a lattice. Then we may assume $\Lambda = \langle 1, \tau\rangle$ for some τ in $\mathfrak{H}$.

How is $\mathbb{C}/\Lambda$ a curve? The **Weierstraß $\wp$-function for** Λ is given by

$$\wp(z) = \wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \smallsetminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

$\wp$ is doubly periodic:

$$\wp(z + \omega) = \wp(z)$$

if $\omega \in \Lambda$. So $\wp$ is well-defined on $\mathbb{C}/\Lambda$. Now let

$$G_k = G_k(\Lambda) = \sum_{\omega \in \Lambda \smallsetminus \{0\}} \frac{1}{\omega^{2k}},$$

and let E be the curve given by

$$y^2 = 4x^3 - 60G_2 x - 140G_3.$$

Then $(\wp, \wp') \in E$, so $\mathbb{C}(E) = \mathbb{C}(\wp, \wp')$, and there is an isomorphism

$$z \longmapsto (\wp(z), \wp'(z)) : \mathbb{C}/\Lambda \dashrightarrow E.$$

The induced group-structure of E is given by polynomials:

$$4(\wp(a) + \wp(b) + \wp(a+b)) = \lambda^2,$$

where

$$\lambda = \begin{cases} \dfrac{\wp'(b) - \wp'(a)}{\wp(b) - \wp(a)}, & \text{if } a \neq b; \\ \wp''(a), & \text{if } a = b. \end{cases}$$

Let E_i be $\mathbb{C}/\Lambda_i$. A non-zero homomorphism from E_0 to E_1 is an **isogeny** and corresponds to α in $\mathbb{C}^\times$ such that

$$\alpha\Lambda_0 \subseteq \Lambda_1;$$

the degree of the isogeny is $|\Lambda_1/\alpha\Lambda_0|$.

Any integer induces an endomorphism of $\mathbb{C}/\Lambda$; if any other complex numbers do, then $\mathbb{C}/\Lambda$ has **complex multiplication**.

Theorem. *Let E_i be elliptic curves over K algebraically closed. The following are equivalent:*

(0) *There are two isogenies from E_0 to E_1 of relatively prime degrees.*

(1) *$K(E_0)$ and $K(E_1)$ agree on all sentences*

$$\forall x_0 \, \forall x_1 \cdots \forall x_{n-1} \, \exists x_n \, \phi(\vec{x}\,),$$

where ϕ is quantifier-free.

(2) *$K(E_0)$ and $K(E_1)$ agree on all $\forall\exists$ sentences.*

If one of the E_i has no complex multiplication, then the following is equivalent to the foregoing:

(3) $K(E_0) \cong K(E_1)$.

If one of the E_i does have complex multiplication, and $\operatorname{char} K = 0$*, then the following is equivalent to* (0) et al.*:*

(4) $\operatorname{End}(E_0) \cong \operatorname{End}(E_1)$.

(Duret proved (1) $\iff$ (3) when $\operatorname{char} K = 0$.)

Relevant facts:

- There are just 13 elliptic curves over $\mathbb{C}$ that are determined by their endomorphism-rings.
- Say $E = \mathbb{C}/\langle 1, \tau \rangle$. Then

  $$\operatorname{End}(E) \cong \{\alpha \in \mathbb{C} : \alpha \langle 1, \tau \rangle \subseteq \langle 1, \tau \rangle\} \leqslant \langle 1, \tau \rangle .$$

  If E has complex multiplication, then τ is quadratic (and conversely), since then

  $$(x + A\tau)\tau \in \langle 1, \tau \rangle$$

  for some non-zero A. If $|A|$ is minimal, then

  $$\operatorname{End}(E) \cong \langle 1, A\bar{\tau} \rangle .$$

  Example. $\operatorname{End}(\mathbb{C}/\langle 1, \tau \rangle) \cong \langle 1, \tau \rangle$ when τ is i or $(1 + i\sqrt{3})/2$.
- Every isogeny $\alpha : E_0 \to E_1$ has a **dual**

  $$\widehat{\alpha} : E_1 \to E_0$$

  of the same degree d; then $\widehat{\alpha} \circ \alpha = [d]$ (multiplication by d).

Ideas of proof:

(1) $\Longrightarrow$ (0). If p always divides $[K(E_0) : \phi^* K(E_1)]$, then for some E_2,

$$\begin{gathered}\phi^* K(E_1) \subseteq \phi^* K(E_2) \subseteq K(E_0);\\ [K(E_0) : K(E_2)] = p.\end{gathered}$$

Then $K(E_0)$ says—but $K(E_1)$ does not—that every point of E_1 is the image of a point of some E_2 under a map of degree p.

(0) $\Longrightarrow$ (2). By (0), when $n > 1$, some isogeny has degree prime to n. Say $K(E_0) \vDash \forall \vec{x} \ \exists \vec{y} \ \phi(\vec{x}, \vec{y})$, where ϕ is quantifier-free. Let n be the factorial of the degrees of the polynomials in ϕ, and say

$$\gcd(n, [K(E_0) : K(E_1)]) = 1.$$

If $\vec{a}$ is from $K(E_1)$, then $\phi(\vec{a}, \vec{y})$ must have a solution from $K(E_1)$.

(0) $\Longrightarrow$ (4). If $\alpha_i : E_0 \to E_1$ and $\deg \alpha_i = d_i$ and $\sum a_i d_i = 1$, then

$$\begin{aligned}\operatorname{End}(E_1) &\xrightarrow{\cong} \operatorname{End}(E_0)\\ \beta &\longmapsto \sum a_i \widehat{\alpha}_i \circ \beta \circ \alpha_i.\end{aligned}$$

(4) $\Longrightarrow$ (0). Say $\operatorname{End}(E_0) \cong \operatorname{End}(E_1)$. Then we may assume

$$\begin{gathered}E_0 = \mathbb{C}/\langle 1, \tau\rangle, \quad E_1 = \mathbb{C}/\langle 1, n\tau\rangle,\\ A\tau^2 + B\tau + C = 0, \quad \gcd(A, B, C) = 0, \quad n \mid A.\end{gathered}$$

Hence

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

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

$$\begin{gathered}\deg(z \mapsto \alpha z) = \frac{1}{n}|\alpha| = nx^2 - Bxy + \frac{AC}{n}y^2,\\ \gcd\left(n, B, \frac{AC}{n}\right) = 1,\end{gathered}$$

so the degree takes two relatively prime values.