MODEL THEORY AND LINEAR ALGEBRA

DAVID PIERCE

These are notes were written originally in preparation for a talk to be given on Friday, March 26, 2010, in the Department of Mathematics and Computer Science at Çankaya University, Ankara. The talk itself is just a selection. What is said here about vector spaces is based mainly on [10].

Contents

1. History of algebra

¶ **1.** In the *Elements* [4] of Euclid (fl. 300 b.c.e.), Proposition II.5 is,

> If a straight line be cut into equal and unequal segments, the rectangle contained by the unequal segments of the whole together with the square on the straight line between the points of section is equal to the square on the half.

In other words, if a straight line be divided unequally, the rectangle bounded by the unequal pieces falls short of the square on the half by the square on the segment between the midpoint and the point of unequal section. See Figure 1, where

$$\text{rect.}\,AD, DB = \text{sq.}\,AC - \text{sq.}\,DC.$$

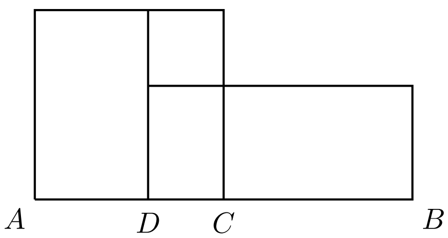

Figure 1

Date: March 26, 2010.

¶ **2.** Consequently, Muhammad ibn Mūsā al-Khwārizmī (*c.* 780–850) [7, pp. 525, 544] asks,

> what must be the amount of a square, which, when twenty-one dirhams are added to it, becomes equal to the equivalent of ten roots of that square? Solution: …nine. Or…forty-nine.

See Figure 2. In our terms, if

$$x^2 + 21 = 10x,$$

then

$$x = \frac{10}{2} \pm \sqrt{\left(\frac{10}{2}\right)^2 - 21} = 5 \pm \sqrt{4} = 5 \pm 2 = 3 \text{ or } 7,$$

so $x^2 = 9$ or 49.

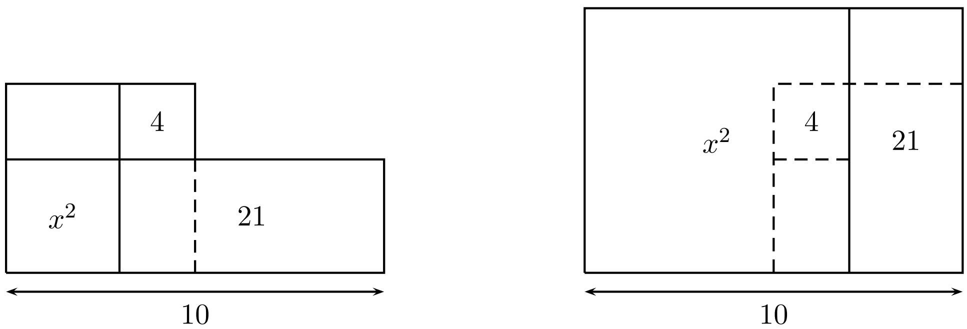

FIGURE 2

¶ **3.** Descartes observes in the *Geometry* (1637) [2, pp. 4, 5]: lines can be multiplied to make *lines,* not rectangles. So, in Figure 3, if

$$AB = 1, \qquad BD = a, \qquad BC = b,$$

then

$$BE = ab.$$

Descartes's purpose is apparently to use geometry as a model for field theory.

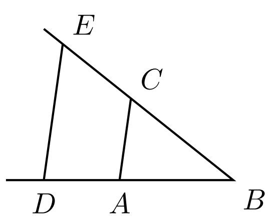

FIGURE 3

He implicitly shows that the *scalar field* of a *vector space* (of dimension 2 or more) can be found in the space.

2. Vector spaces

¶ 4. A **vector space** is a triple $(\mathfrak{V}, \mathfrak{K}, *)$, where

(1) $\mathfrak{V}$ is an abelian group of **vectors,**
$$(V, \mathbf{0}, -, +);$$
(2) $\mathfrak{K}$ is a field of **scalars,**
$$(K, 0, 1, -, +, \cdot\,);$$
(3) $*$ is an **action** of $\mathfrak{K}$ on $\mathfrak{V}$, that is, a function from $K \times V$ to V such that
  (a) each operation
$$\boldsymbol{v} \mapsto x * \boldsymbol{v}$$
  on V is an endomorphism of $\mathfrak{V}$, and
  (b) the function
$$x \mapsto (\boldsymbol{v} \mapsto x * \boldsymbol{v})$$
  is a ring-homorphism from $\mathfrak{K}$ to $(\mathrm{End}(\mathfrak{V}), \circ)$.

So a vector space is a kind of **2-sorted structure,** with the **signature**
$$\{\mathbf{0}, -, +; 0, 1, -, +, \cdot; *\}.$$

¶ 5. Descartes's example suggests how, given a vector space $(\mathfrak{V}, \mathfrak{K}, *)$, where
$$\dim_{\mathfrak{K}}(\mathfrak{V}) \geqslant 2,$$
we can **interpret** $\mathfrak{K}$ and its action on $\mathfrak{V}$ *in* $\mathfrak{V}$. To do this, we introduce a new symbol $\parallel$ for the binary relation of **parallelism** on V; this relation is *defined* by
$$\boldsymbol{u} \parallel \boldsymbol{v} \Leftrightarrow \exists x\ \exists y\ (x * \boldsymbol{u} + y * \boldsymbol{v} = \mathbf{0}\ \&\ (x \neq 0 \vee y \neq 0)).$$
Now let
$$M = \{(\boldsymbol{u}, \boldsymbol{v}) \in V \times V \colon \boldsymbol{u} \neq 0\ \&\ \boldsymbol{u} \parallel \boldsymbol{v}\}.$$
If $(\boldsymbol{u}, \boldsymbol{v}) \in M$, then we can define the element $[\boldsymbol{u} : \boldsymbol{v}]$ of K by the rule
$$\boldsymbol{v} = [\boldsymbol{u} : \boldsymbol{v}] * \boldsymbol{u}.$$
So we have a surjection $(\boldsymbol{u}, \boldsymbol{v}) \mapsto [\boldsymbol{u} : \boldsymbol{v}]$ from M onto K. This induces an equivalence-relation $\sim$ on M:
$$(\boldsymbol{u}_0, \boldsymbol{u}_1) \sim (\boldsymbol{v}_0, \boldsymbol{v}_1) \iff [\boldsymbol{u}_0, \boldsymbol{u}_1] = [\boldsymbol{v}_0, \boldsymbol{v}_1].$$
We now give $M/{\sim}$ the structure of $\mathfrak{K}$. We shall use the formula
$$\boldsymbol{s} \nparallel \boldsymbol{u}\ \&\ \boldsymbol{s} \parallel \boldsymbol{t}\ \&\ \boldsymbol{u} \parallel \boldsymbol{v}\ \&\ \boldsymbol{s} - \boldsymbol{u} \parallel \boldsymbol{t} - \boldsymbol{v},$$
which we denote by
$$\Delta(\boldsymbol{s}, \boldsymbol{t}, \boldsymbol{u}, \boldsymbol{v}).$$
See Figure 4. To interpret the field $\mathfrak{K}$ in $\mathfrak{V}$, we have to express the formulas
$$x = y, \qquad x + y = z, \qquad x \cdot y = z, \qquad x * \boldsymbol{u} = \boldsymbol{v}$$
wholly in terms of vectors. We do this as follows:

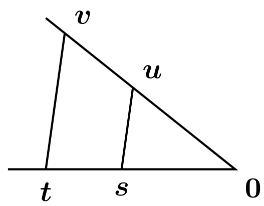

FIGURE 4. $\Delta(\boldsymbol{s},\boldsymbol{t},\boldsymbol{u},\boldsymbol{v})$

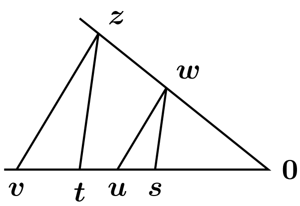

FIGURE 5. $[\boldsymbol{s}:\boldsymbol{t}]=[\boldsymbol{u}:\boldsymbol{v}]$ (one case)

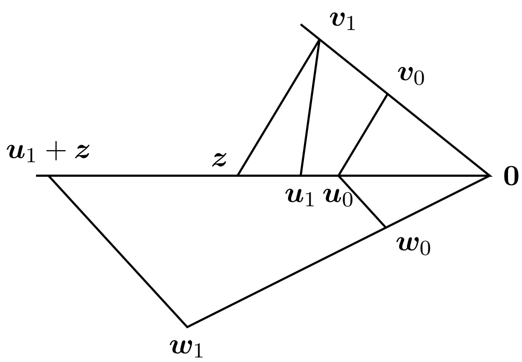

FIGURE 6. $[\boldsymbol{u}_0:\boldsymbol{u}_1]+[\boldsymbol{v}_0:\boldsymbol{v}_1]=[\boldsymbol{w}_0:\boldsymbol{w}_1]$

(1) Equality in K, or
$$[\boldsymbol{s}:\boldsymbol{t}]=[\boldsymbol{u}:\boldsymbol{v}], \tag{$*$}$$
is expressed in $\mathfrak{V}$ by
$$\Delta(\boldsymbol{s},\boldsymbol{t},\boldsymbol{u},\boldsymbol{v})\vee\exists\boldsymbol{w}\ \exists\boldsymbol{z}\ (\Delta(\boldsymbol{s},\boldsymbol{t},\boldsymbol{w},\boldsymbol{z})\ \&\ \Delta(\boldsymbol{w},\boldsymbol{z},\boldsymbol{u},\boldsymbol{v})), \tag{$\dagger$}$$
where the latter condition is shown in Figure 5; now we can use $(*)$ to stand for $(\dagger)$.

(2) Addition in $\mathfrak{K}$, or
$$[\boldsymbol{u}_0:\boldsymbol{u}_1]+[\boldsymbol{v}_0:\boldsymbol{v}_1]=[\boldsymbol{w}_0:\boldsymbol{w}_1],$$
is expressed in $\mathfrak{V}$, as in Figure 6, by
$$\exists\boldsymbol{z}\ ([\boldsymbol{u}_0:\boldsymbol{z}]=[\boldsymbol{v}_0:\boldsymbol{v}_1]\ \&\ [\boldsymbol{u}_0:\boldsymbol{u}_1+\boldsymbol{z}]=[\boldsymbol{w}_0:\boldsymbol{w}_1].$$

(3) Multiplication in $\mathfrak{K}$, or
$$[\boldsymbol{u}_0:\boldsymbol{u}_1]\cdot[\boldsymbol{v}_0:\boldsymbol{v}_1]=[\boldsymbol{w}_0:\boldsymbol{w}_1],$$

is expressed in $\mathfrak{V}$, as in Figure 7, by

$$\exists \boldsymbol{z}\ ([\boldsymbol{u}_1 : \boldsymbol{z}] = [\boldsymbol{v}_0 : \boldsymbol{v}_1] \ \&\ [\boldsymbol{u}_0 : \boldsymbol{z}] = [\boldsymbol{w}_0 : \boldsymbol{w}_1].$$

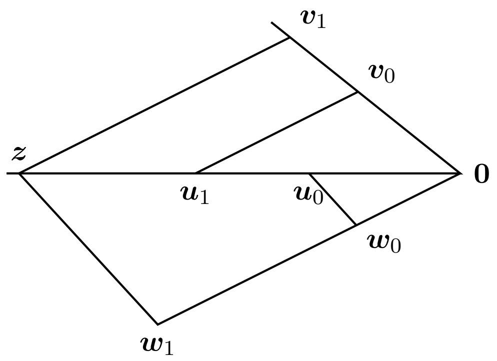

FIGURE 7. $[\boldsymbol{u}_0 : \boldsymbol{u}_1] \cdot [\boldsymbol{v}_0 : \boldsymbol{v}_1] = [\boldsymbol{w}_0 : \boldsymbol{w}_1]$

(4) Finally, scalar multiplication, or

$$[\boldsymbol{u}_0 : \boldsymbol{u}_1] * \boldsymbol{v}_0 = \boldsymbol{v}_1,$$

is expressed in $\mathfrak{V}$ by

$$[\boldsymbol{u}_0 : \boldsymbol{u}_1] = [\boldsymbol{v}_0 : \boldsymbol{v}_1] \vee (\boldsymbol{v}_0 = \mathbf{0} \ \&\ \boldsymbol{v}_1 = \mathbf{0}).$$

¶ **6.** So one can define a vector space as a pair $(\mathfrak{V}, \|_{\mathfrak{K}})$, where

(1) $\mathfrak{V}$ is an abelian group $(V, \mathbf{0}, -, +)$, and
(2) the binary relation $\|$ respects axioms ensuring that $\mathfrak{V}$ is acted on by a field, $\mathfrak{K}$.

In this sense, a vector space is a 1-sorted structure in the signature

$$\{\mathbf{0}, -, +, \|\}.$$

However, the two notions of a vector space are not entirely equivalent, and not just because spaces in the latter sense are at least 2-dimensional. The **substructure** relation differs also. For example, we have

$$(\mathbb{H}, \mathbb{R}, *) \subseteq (\mathbb{H}, \mathbb{C}, *),$$

but

$$(\mathbb{H}, \|_{\mathbb{R}}) \nsubseteq (\mathbb{H}, \|_{\mathbb{C}}),$$

since the relations $\|_{\mathbb{R}}$ and $\|_{\mathbb{C}}$ do not agree, even on $\mathbb{C}$ (much less on $\mathbb{H}$):

$$1 \nparallel_{\mathbb{R}} \mathbf{i}, \qquad\qquad 1 \|_{\mathbb{C}} \mathbf{i}.$$

(However, $(\mathbb{C}, \|_{\mathbb{R}}) \subseteq (\mathbb{H}, \|_{\mathbb{C}})$.)

¶ **7.** Let VS be the **theory** of vector spaces in the original sense, in the signature

$$\{\mathbf{0}, -, +; 0, 1, -, +\cdot; *\}.$$

That is, VS is the set of **sentences** of **first-order logic** in the given signature that are true in all vector spaces. (A logic is first order when all variables stand for individuals, not sets as such.) Every **model** $(\mathfrak{V}, \mathfrak{K}, *)$ of VS embeds in a 1-dimensional model

$$(\mathfrak{L}, \mathfrak{L}, *);$$

just let $\mathfrak{L}$ be a field-extension of $\mathfrak{K}$ such that

$$[\mathfrak{L} : \mathfrak{K}] \geqslant \dim_{\mathfrak{K}} \mathfrak{V},$$

and embed a basis of $(\mathfrak{V}, \mathfrak{K}, *)$ in a basis of $(\mathfrak{L}, \mathfrak{K}, *)$.

¶ **8.** Let VS_2 be the **theory** of vector spaces of dimension at least 2 in the signature

$$\{\mathbf{0}, -, +, \|\}.$$

Every model embeds in a 2-dimensional model. Indeed, suppose L/K is a field-extension, and $a, b \in L$, and $(a, b, 1)$ is linearly independent over K. Then $(K^3, \|_K)$ embeds in $(L^2, \|_L)$ under

$$(x, y, z) \mapsto (x - az, y - bz),$$

that is,

$$\begin{pmatrix} x & y & z \end{pmatrix} \mapsto \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ -a & -b \end{pmatrix}.$$

For, the following are equivalent:

$$\begin{aligned} &(x, y, z) \|_K (u, v, w), \\ 0 &= \det \begin{pmatrix} x & y & z \\ u & v & w \\ a & b & 1 \end{pmatrix} \\ &= \det \left(\begin{pmatrix} x & y \\ u & v \end{pmatrix} - \begin{pmatrix} z \\ w \end{pmatrix} \begin{pmatrix} a & b \end{pmatrix} \right) \\ &= \det \left(\begin{pmatrix} x & y & z \\ u & v & w \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ -a & -b \end{pmatrix} \right), \\ &(x - az, y - zb) \|_L (u - aw, v - bw). \end{aligned}$$

We used here the identity

$$\det \left(\begin{array}{c|c} U & \boldsymbol{v}^{\mathrm{t}} \\ \hline \boldsymbol{a} & 1 \end{array} \right) = \det(U - \boldsymbol{v}^{\mathrm{t}} \cdot \boldsymbol{a}),$$

which follows from

$$\left(\begin{array}{c|c} U & \boldsymbol{v}^{\mathrm{t}} \\ \hline \boldsymbol{a} & 1 \end{array} \right) \cdot \left(\begin{array}{c|c} I & \mathbf{0}^{\mathrm{t}} \\ \hline -\boldsymbol{a} & 1 \end{array} \right) = \left(\begin{array}{c|c} U - \boldsymbol{v}^{\mathrm{t}} \cdot \boldsymbol{a} & \boldsymbol{v}^{\mathrm{t}} \\ \hline \mathbf{0} & 1 \end{array} \right).$$

3. Model theory (outline)

¶ **9.** We have entered **model theory,** which I define as

the study of **structures** *quâ* **models** of **theories.**

Examples of structures include

$$(\mathfrak{V}, \mathfrak{K}, *), \quad (\mathfrak{V}, \|_{\mathfrak{K}}), \quad (\mathbb{Q}, <), \quad (\mathbb{Q}, +, \cdot), \quad (\mathbb{R}, +, \cdot, <), \quad (\mathbb{C}, +, \cdot).$$

Model theory has also been called

the geography of **tame** mathematics.

Tameness has no one definition. However, one measure of tameness is the **effective axiomatizability** of the (first-order) theory,

$$\mathrm{Th}(\mathfrak{A}),$$

of a structure $\mathfrak{A}$.

¶ 10. In the following,

$$\mathbb{N} = \{1, 2, 3, \dots\},$$

and S stands for $x \mapsto x + 1$. Outer universal quantifiers of sentences are suppressed. The structure $(\mathbb{N}, 1, S, +)$ is "tame", because of:

Theorem (Presburger, 1929)**.** $\mathrm{Th}(\mathbb{N}, 1, S, +)$ *is axiomatized by:*

(1) $1 \neq Sx$*;*
(2) $Sx = Sy \Rightarrow x = y$*;*
(3) $x + 1 = Sx$*;*
(4) $x + (y + 1) = (x + y) + 1$*;*
(5) *the* ***first-order induction axioms:*** *for each formula* $\varphi(x)$*,*

$$\varphi(1) \mathbin{\&} \forall x\, (\varphi(x) \Rightarrow \varphi(Sx)) \Rightarrow \forall \varphi\, (x).$$

¶ 11. An arbitrary theory T is **complete** if

$$T \vdash \sigma \text{ or } T \vdash \neg\sigma$$

for all sentences σ of the signature of T. The theory *of* a structure is automatically complete. Then Presburger's theorem is that a particular theory given by axioms is complete.

¶ 12. By contrast, $(\mathbb{N}, 1, S, +, \cdot)$ is "wild", by **Gödel's Incompleteness Theorem:**

Theorem (Gödel, 1931 [5])**.** $\mathrm{Th}(\mathbb{N}, 1, S, +, \cdot)$ *cannot be effectively axiomatized.*

¶ 13. Even though $\mathrm{Th}(\mathbb{N}, 1, S, +)$ can be (effectively) completely axiomatized in first-order logic, the axioms do not determine $(\mathbb{N}, 1, S, +)$ (up to isomorphism), as we shall see. However, $(\mathbb{N}, 1, S)$ is characterized (up to isomorphism) by its satisfaction of the axioms identified by Dedekind (1888) [1] and Peano (1889) [9], namely Presburger's (1) and (2)—

$$1 \neq Sx, \qquad\qquad Sx = Sy \Rightarrow x = y,$$

—along with the **second-order induction axiom:** the sentence

$$1 \in X \mathbin{\&} \forall t\, (t \in X \Rightarrow St \in X) \Rightarrow \forall t\; t \in X.$$

¶ 14. That $(\mathbb{N}, 1, S)$ satisfies (second-order) induction means $\mathbb{N}$ is the *smallest* set that contains 1 and is closed under S. Another way to say this is that $\mathbb{N}$ has a **recursive definition:**

(1) $1 \in \mathbb{N}$,
(2) if $x \in \mathbb{N}$, then $Sx \in \mathbb{N}$.

This, *together with* the other two axioms (1) and (2), is logically equivalent to the validity of recursive definitions of operations on $\mathbb{N}$: operations such as addition, given by Presburger's (3) and (4)—

$$x + 1 = Sx, \qquad x + (y + 1) = (x + y) + 1$$

—, or multiplication, given by

$$x \cdot 1 = x, \qquad x \cdot (y + 1) = x \cdot y + x,$$

or exponentiation, given by

$$x^1 = x, \qquad x^{y+1} = x^y \cdot x. \tag{‡}$$

In particular, despite Gödel's Incompleteness Theorem, $(\mathbb{N}, 1, S, +, \cdot)$ *can* be completely characterized, in a sense, in second-order logic.

¶ 15. From Peano on, some people have not recognized that the possibility of defining a set recursively does not, by itself, allow functions *on* the set to be defined recursively. Addition and multiplication *are* justified by induction alone, as is shown implicitly in Landau's *Foundations of Analysis* (1929) [8]; but exponentiation is not:

Theorem (Dyer-Bennet, 1940 [3]; P., 2009)**.** *If* $n \in \mathbb{N}$*, then* $(\mathbb{Z}/(n), 1, S)$ *satisfies (second-order) induction; but it admits exponentiation defined as in* (‡) *if and only if* $n \in \{1, 2, 6, 42, 1806\}$.

4. Model theory (detail)

¶ 16. That induction does not always imply recursion can be seen in the development of logic itself. I now review this development in detail. To be precise then, a **structure** is one or more disjoint sets called **sorts,** together with some (or no) distinguished

(1) **operations:** functions from finite products of sorts to one sort;
(2) **constants:** operations taking no arguments;
(3) **relations:** subsets of finite products of the sorts.

If G is a group, and f is the function $X \mapsto \langle X \rangle$ that converts a subset of G into the subgroup that it generates, then the pair

$$(G, f)$$

is *not* a structure, although the quadruple

$$(G, \mathscr{P}(G), \in, f)$$

is a (two-sorted) structure.

¶ 17. A structure has a **signature,** namely a set of **symbols** for the distinguished operations (including constants) and relations. So the signature of $(\mathfrak{V}, \mathfrak{K}, *)$ is

$$\{\mathbf{0}, \boldsymbol{-}, \boldsymbol{+}, 0, 1, -, +, \cdot, *\}.$$

The symbols 'know' which sorts their arguments are from. The symbols are called **non-logical,** to distinguish them from **logical symbols,** namely,

(1) **Boolean connectives:** $\neg$, &, $\vee$, $\Rightarrow$, $\Leftrightarrow$, ...;
(2) **quantifiers:** $\exists$ and $\forall$;
(3) **punctuation:** (and);
(4) the sign of **equality,** $=$;

(5) **variables.**

In **first-order logic,** each variable is required to range only over the elements of a particular sort, and not (for example) over the *subsets* of a sort. In talking about $(\mathfrak{V}, \mathfrak{K}, *)$, we let boldface variables like $\boldsymbol{u}$ range over V; and plainface variables like x, over K.

¶ **18.** From logical and non-logical symbols, one builds up **formulas** that refer to structures of a particular signature. The construction will be discussed later. *All formulas here will be first-order, unless otherwise specified.* A formula may have **free variables;** if it does not, then the formula is a **sentence.** A sentence is either **true** or **false** in a structure (with a suitable signature); if the sentence σ is true in the structure $\mathfrak{A}$, we write

$$\mathfrak{A} \vDash \sigma;$$

we may say also that $\mathfrak{A}$ **satisfies** σ. For example,

$$\mathbb{Q} \vDash \forall x \; \exists y \; (x = 0 \lor x \cdot y = 1),$$
$$\mathbb{Z} \nvDash \forall x \; \exists y \; (x = 0 \lor x \cdot y = 1).$$

A set of sentences of some signature is a **theory.** If T is a theory, and all of its elements are true in $\mathfrak{A}$, then $\mathfrak{A}$ is a **model** of T. If σ is a sentence that is true in every model of T, then σ is a **logical consequence** of T, and we may write

$$T \vDash \sigma.$$

¶ **19.** A (first-order) theory T is **complete** if, for every sentence σ of its signature, either $T \vDash \sigma$ or $T \vDash \neg\sigma$. The set of sentences that are true in $\mathfrak{A}$ is the **theory of** $\mathfrak{A}$, denoted by

$$\mathrm{Th}(\mathfrak{A});$$

it is automatically complete. If $\Sigma \subseteq T$, and every sentence of T is a logical consequence of Σ, then Σ is a set of **axioms** for T.

¶ **20.** Given a signature $\mathscr{L}$ and a set C of **parameters,** we recursively define the set

$$\mathrm{Fm}_{\mathscr{L}}(C)$$

of first-order **formulas** of $\mathscr{L}$ in C. For each formula, there is a finite **tree,** as in Figure 8, **proving** that the formula is a formula. Moreover, such trees are *unique;* so we can also recursively define functions on $\mathrm{Fm}_{\mathscr{L}}(C)$. For example, given an $\mathscr{L}$-structure $\mathfrak{A}$ that includes C, and given a function v that assigns values from $\mathfrak{A}$ to the variables used in formulas, we can determine recursively whether

$$\mathfrak{A} \vDash \varphi[v],$$

that is, whether φ **true** in $\mathfrak{A}$ under v.

¶ **21.** We distinguish some sentences as **logical axioms.** Then the set of **theorems** is the closure of the set of axioms under **detachment** (or ***modus ponens***,

$$(\sigma, (\sigma \Rightarrow \tau)) \mapsto \tau.$$

Again, for each theorem, there is a finite tree, as in Figure 9, proving that the theorem is a theorem. But now the tree is not unique; so we cannot define

$$\begin{tikzcd}[column sep=small]
& \exists x\ \exists y\ (x * \boldsymbol{u} + y * \boldsymbol{v} = \boldsymbol{0}\ \&\ (x \neq 0 \lor y \neq 0)) \arrow[d, dash] & & \\
& \exists y\ (x * \boldsymbol{u} + y * \boldsymbol{v} = \boldsymbol{0}\ \&\ (x \neq 0 \lor y \neq 0)) \arrow[d, dash] & & \\
& (x * \boldsymbol{u} + y * \boldsymbol{v} = \boldsymbol{0}\ \&\ (x \neq 0 \lor y \neq 0)) \arrow[dl, dash] \arrow[dr, dash] & & \\
x * \boldsymbol{u} + y * \boldsymbol{v} = \boldsymbol{0} & & (x \neq 0 \lor y \neq 0) \arrow[dl, dash] \arrow[dr, dash] & \\
& x \neq 0 & & y \neq 0
\end{tikzcd}$$

FIGURE 8

$$\begin{tikzcd}[column sep=small]
& \neg\exists x\ \varphi \arrow[dl, dash] \arrow[dr, dash] & & \\
\neg\varphi(a) & & (\neg\varphi(a) \Rightarrow \neg\exists x\ \varphi) \arrow[dl, dash] \arrow[dr, dash] & \\
& (\neg\varphi(a) \Rightarrow \neg\varphi(b)) & & ((\neg\varphi(a) \Rightarrow \neg\varphi(b)) \Rightarrow (\neg\varphi(a) \Rightarrow \neg\exists x\ \varphi))
\end{tikzcd}$$

FIGURE 9. Proof of $\neg\exists x\ \varphi$, where φ is $\neg(x = x \Rightarrow x = x)$

functions recursively on the set of theorems. These points are elaborated in the following paragraphs.

¶ 22. Let PV be a set of **propositional variables,** perhaps

$$\{P_n \colon n \in \mathbb{N}\}.$$

The set of **propositional formulas,** say PF, is the smallest set that includes PV and is closed under the operations

$$F \mapsto \neg F, \qquad\qquad (F, G) \mapsto (F\ \&\ G).$$

This just means PF satisfies induction (with respect to PV and these operations).

¶ 23. More is true: Functions can be defined recursively on PF, because there is *only one way* to construct a given formula. For example, suppose $h \colon \mathrm{PV} \to \mathbb{F}_2$ (where $\mathbb{F}_2$ is a two-element field). Then h extends uniquely to a function H on PF such that

$$H(\neg F) = 1 + H(F), \qquad H(F \mathbin{\&} G) = H(F) \cdot H(G).$$

A propositional formula F is a **tautology** if $H(F) = 1$ for all choices of h.

¶ 24. In practice, one uses abbreviations in formulas, as

$$(F \vee G) \text{ for } \neg(\neg F \mathbin{\&} \neg G),$$
$$(F \Rightarrow G) \text{ for } \neg F \vee G,$$
$$(F \Leftrightarrow G) \text{ for } ((F \Rightarrow G) \mathbin{\&} (G \Rightarrow F)).$$

¶ 25. Let us now develop first-order logic in a signature $\mathscr{L}$. For simplicity, we assume $\mathscr{L}$ is the signature of a one-sorted structure; for definiteness, we assume

$$\mathscr{L} = \{0, -, +, \|\}.$$

Fix a set X of **individual variables.** Let C be a set of **parameters**—individuals from some $\mathscr{L}$-structure $\mathfrak{V}$. The set of **terms** over C is the smallest set that includes X and is closed under

$$c, \qquad 0, \qquad t \mapsto -t, \qquad (t, u) \mapsto (t + u),$$

where c ranges over C. Call this set

$$\mathrm{Tm}_{\mathscr{L}}(C);$$

by definition, it satisfies induction with respect to X and the given operations.

¶ 26. Also, functions can be defined recursively on $\mathrm{Tm}_{\mathscr{L}}(C)$, because there is *only one way* to construct a given term. For example, if $v\colon X \to V$, then there is a unique function $\tilde{v}$ from $\mathrm{Tm}_{\mathscr{L}}(C)$ into V that extends v and satisfies

$$\tilde{v}(c) = c, \qquad \tilde{v}(0) = 0, \qquad \tilde{v}(-t) = -\tilde{v}(t), \qquad \tilde{v}(t + u) = \tilde{v}(t) + \tilde{v}(u).$$

Here, for example, $t + u$ is a string of symbols; but $\tilde{v}(t) + \tilde{v}(u)$ is the image of $(\tilde{v}(t), \tilde{v}(u))$ under the operation of $+$ on $\mathfrak{V}$.

¶ 27. We now define simultaneously the set $\mathrm{Fm}_{\mathscr{L}}(C)$ of **formulas** over C and the function assigning to each formula φ its set $FV(\varphi)$ of **free variables.**

(1) If $t, u \in \mathrm{Tm}_{\mathscr{L}}(C)$, then the strings

$$t = u, \qquad t \parallel u$$

are in $\mathrm{Fm}_{\mathscr{L}}(C)$, and both $FV(t = u)$ and $FV(t \parallel u)$ consist of the variables actually appearing in t or u.

(2) $\mathrm{Fm}_{\mathscr{L}}(C)$ is closed under $\varphi \mapsto \neg\varphi$, and

$$FV(\neg\varphi) = FV(\varphi).$$

(3) If φ is in $\mathrm{Fm}_{\mathscr{L}}(C)$, and $x \in FV(\varphi)$, then $\exists x\ \varphi$ is in $\mathrm{Fm}_{\mathscr{L}}(C)$, and

$$FV(\exists x\ \varphi) = FV(\varphi) \smallsetminus \{x\}.$$

(4) If φ and ψ are in $\mathrm{Fm}_{\mathscr{L}}(C)$, and no variable occurring *non-freely* in one of them occurs (freely or non-freely) in the other, then $(\varphi \mathbin{\&} \psi)$ is in $\mathrm{Fm}_{\mathscr{L}}(C)$, and

$$FV(\varphi \mathbin{\&} \psi) = FV(\varphi) \cup FV(\psi).$$

Then $\mathrm{Fm}_{\mathscr{L}}(C)$ satisfies a kind of induction. Moreover functions can be defined recursively on $\mathrm{Fm}_{\mathscr{L}}(C)$. Indeed, if $v \colon X \to V$ as above, and φ is a formula, let $\varphi[v]$ be the result of replacing each instance of each *free* variable x in φ with $v(x)$. Then $\varphi[v]$ is **true** in $\mathfrak{V}$, and we write

$$\mathfrak{V} \vDash \varphi[v],$$

according to the following recursive definition.

(1) $\mathfrak{V} \vDash (t = u)[v]$ if and only if

$$\tilde{v}(t) = \tilde{v}(u).$$

(2) $\mathfrak{V} \vDash (t \parallel u)[v]$ if and only if

$$\tilde{v}(t) \parallel \tilde{v}(u)$$

(3) $\mathfrak{V} \vDash \neg\varphi[v]$ if and only if

$$\mathfrak{V} \nvDash \varphi[v].$$

(4) $\mathfrak{V} \vDash \exists x\ \varphi[v]$ if and only if

$$\mathfrak{V} \vDash \varphi[v']$$

for some v' that agrees with v on $FV(\exists x\ \varphi)$.

A formula σ is a **sentence** if $FV(\sigma) = \varnothing$. In this case, $\sigma[v]$ is just σ. If σ is true in all $\mathscr{L}$-structures that include C, then σ is **logically valid,** and we may write simply

$$\vDash \sigma.$$

¶ 28. If we use sentences as propositional variables, then a propositional formula is also a sentence: if the propositional formula is a tautology, then we may refer also to the sentence as a **tautology.** If $FV(\varphi) = \{x\}$, and $c \in C$, then $\varphi(c)$ is the result of replacing each instance of x in φ with c. Now we define a sentence to be a **logical axiom** if it is:

(1) a tautology;

(2) a sentence of one of the forms

$$t = t,$$
$$(t = u \Rightarrow u = t),$$
$$((t = u \mathbin{\&} u = s) \Rightarrow t = s),$$
$$(c = d \Rightarrow (\varphi(c) \Rightarrow \varphi(d)));$$

(3) a sentence

$$(\sigma \Rightarrow \sigma'),$$

where σ and σ' are sentences, and we get σ' from σ by replacing each occurrence of x with y;

(4) a sentence

$$(\varphi(c) \Rightarrow \exists x\ \varphi(x));$$

(5) a sentence
$$((\sigma \Rightarrow \neg\varphi(c)) \Rightarrow (\sigma \Rightarrow \neg\exists x\ \varphi(x))),$$
where c does not occur in σ.

The set of **theorems** is the smallest set that contains the logical axioms and that contains τ if it contains σ and $(\sigma \Rightarrow \tau)$.

¶ 29. If σ is a theorem, we may write
$$\vdash \sigma.$$
Every theorem is valid: if $\vdash \sigma$, then $\vDash \sigma$. The converse is **Gödel's Completeness Theorem:**

Theorem (Gödel, 1930)**.** *If $\vDash \sigma$, then $\vdash \sigma$.*

A sentence σ is **provable** from a collection S of sentences, and we may write
$$S \vdash \sigma,$$
if some sentence
$$\tau_0\ \&\ \cdots\ \&\ \tau_{n-1} \Rightarrow \sigma$$
is a theorem, where $\tau_0, \ldots, \tau_{n-1}$ are in S.

Theorem (Malcev, 1936)**.** *If $S \vDash \sigma$, then $S \vdash \sigma$.*

Corollary (Compactness Theorem)**.** *If every finite subset of S has a model, then S has a model.*

Proof. If S has no model, then
$$S \vDash 0 \neq 0, \qquad S \vdash 0 \neq 0, \qquad S_0 \vdash 0 \neq 0$$
for some *finite* subset S_0 of S; but then S_0 has no model. □

Compactness *fails* in second-order logic: The Dedekind–Peano Axioms, together with
$$\{c \neq 1, c \neq S1, c \neq SS1, c \neq SSS1, \ldots\},$$
have no model, although every finite subset does.

5. Model theory of fields

¶ 30. Henceforth the logic is first-order. If $\mathfrak{A}$ is a structure (of one sort, for simplicity,) in a signature $\mathscr{L}$, and $\varphi \in \mathrm{Fm}_{\mathscr{L}}(A)$ with free variables from the list $(x_1, \ldots, x_n)$, and $(c_1, \ldots, c_n) \in A^n$, then the result of replacing each free variable x_k in φ with c_k is denoted by
$$\varphi(c_1, \ldots, c_n).$$
Then φ **defines** in $\mathfrak{A}$ the n-ary relation
$$\{(c_1, \ldots, c_n) \in A^n : \mathfrak{A} \vDash \varphi(c_1, \ldots, c_n)\},$$
which can be denoted by
$$\varphi^{\mathfrak{A}}.$$
A definable *set* is a singulary definable relation. If $FV(\psi) = \{x_1, \ldots, x_n, y\}$, then
$$(\exists y\ \psi)^{\mathfrak{A}} = \pi(\psi^{\mathfrak{A}}),$$

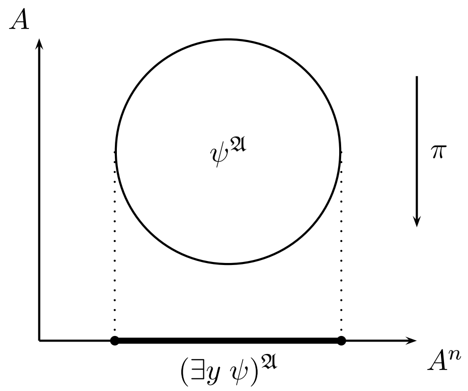

FIGURE 10

where π is the **projection** given by

$$\pi(c_1, \dots, c_n, d) = (c_1, \dots, c_n).$$

See Figure 10. A theory T admits **quantifier-elimination** (QE) if, for every model $\mathfrak{A}$ of T, the collection of relations definable by *quantifier-free* formulas is closed under projection. Having a theory with QE is a further measure of tameness.

¶ 31. Let ACF be the theory of **algebraically closed fields:** field theory, together with, for each n in $\mathbb{N}$,

$$\forall t_1 \ \cdots \forall t_n \ \exists x \ x^n + t_1 x^{n-1} + \cdots + t_{n-1} x + t_n = 0. \tag{§}$$

Let ACF_0 be the theory of algebraically closed fields of characteristic 0, namely ACF together with, for each prime p,

$$\underbrace{1 + \cdots + 1}_{p} \neq 0.$$

Let RCF be the theory of **real-closed ordered fields:** the theory of ordered fields, together with (§) for each *odd* n in $\mathbb{N}$, and also

$$\forall y \ \exists x \ (y > 0 \Rightarrow y = x^2).$$

Theorem (Tarski[1])**.** ACF *and* RCF *admit QE. In particular, the definable sets:*

(1) *in an algebraically closed field, are the finite and co-finite sets;*
(2) *in a real-closed field, are the finite unions of intervals and singletons.*

¶ 32. A structure $\mathfrak{A}$ has a **diagram,** denoted by

$$\mathrm{diag}(\mathfrak{A});$$

this is the set of quantifier-free sentences with parameters from A that are true in $\mathfrak{A}$.

Theorem. *For a theory T, the following are equivalent:*

(1) *T admits QE;*

[1]According to Hodges [6, p. 85], Tarski announced these results in 1949, publishing the proof the result on RCF in [11].

(2) *whenever* $\mathfrak{A} \subseteq \mathfrak{M}$ *for some model* $\mathfrak{M}$ *of* T*, and* $\mathfrak{A}$ *is finitely generated, the theory*

$$T \cup \operatorname{diag}(\mathfrak{A})$$

is complete.

¶ **33.** By considering prime fields, we can now conclude:

Theorem.

(1) $\operatorname{Th}(\mathbb{C}, +, \cdot)$ *is axiomatized by* ACF_0.
(2) $\operatorname{Th}(\mathbb{R}, +, \cdot, <)$ *is axiomatized by* RCF.

¶ **34.** If $T \cup \operatorname{diag}(\mathfrak{M})$ is complete whenever $\mathfrak{M} \vDash T$, then T is called **model complete.**[2] So ACF and RCF and all other theories with QE are model complete.

¶ **35.** A theory T^* is a **model companion** of a theory T (in the same signature if

(1) a model of one embeds in a model of the other, that is,

$$T_\forall = {T^*}_\forall;$$

(2) T^* is model complete.

So ACF and RCF are model companions of the theories of fields and ordered fields, respectively.

¶ **36.** model companions are useful for the following reason. Suppose T^* is a model companion of T, and

$$\mathfrak{M} \vDash T^*, \qquad \mathfrak{N} \vDash T, \qquad \mathfrak{M} \subseteq \mathfrak{N}.$$

Say φ is quantifier-free, with parameters from M, and

$$\mathfrak{N} \vDash \exists \boldsymbol{x}\ \varphi.$$

Then

$$\mathfrak{M} \vDash \exists \boldsymbol{x}\ \varphi.$$

Indeed, we have $\mathfrak{N} \subseteq \mathfrak{M}'$ for some model $\mathfrak{M}'$ of T^*. Then $\mathfrak{M}' \vDash \exists \boldsymbol{x}\ \varphi$, so

$$T^* \cup \operatorname{diag}(\mathfrak{M}) \vDash \exists \boldsymbol{x}\ \varphi.$$

6. Model theory of vector spaces

¶ **37.** Let VS_K be the theory of vector spaces *over the field* $\mathfrak{K}$, in the signature

$$\{0, -, +\} \cup \{a*\colon a \in K\}.$$

This theory admits QE.

¶ **38.** Let VS be the theory of vector spaces over an arbitrary field, in the signature

$$\{\mathbf{0}, \boldsymbol{-}, \boldsymbol{+}, 0, -, +, *\}.$$

This has a model companion, namely the theory of *one-dimensional* vector spaces over an *algebraically closed* field. In particular, every space embeds in a one-dimensional space.

[2]The definition is due to Abraham Robinson.

¶ 39. Let VS^2 be the theory of vector-spaces of dimension at least 2:

$$\mathrm{VS}^2 = \mathrm{VS} \cup \{\exists \boldsymbol{u}\ \exists \boldsymbol{v}\ \forall x\ \forall y\ (x * \boldsymbol{u} + y * \boldsymbol{v} = 0 \Rightarrow x = 0\ \&\ y = 0)\}.$$

This has the same model companion as VS, but is not *included* in a model complete theory, because the union of a **chain** of models of VS^2 need not be a model. For example, let

$$K_n = \mathbb{Q}(\pi^{1/2^n}), \qquad L = \bigcup_{n\in\mathbb{N}} K_n = \mathbb{Q}(\pi, \pi^{1/2}, \pi^{1/4}, \dots).$$

Then $(K_{n+1}, K_n) \vDash \mathrm{VS}_2$, and

$$(K_{n+1}, K_n) \subseteq (K_{n+2}, K_{n+1}),$$

but

$$\bigcup_{n\in\mathbb{N}} (K_{n+1}, K_n) = (L, L),$$

a model of VS, but not VS^2.

¶ 40. As before, let VS_2 be the theory of vector spaces of dimension at least 2 in the signature

$$\{\mathbf{0}, -, +, \|\}.$$

This has a model companion, namely the theory of 2-dimensional vector spaces over an algebraically closed field.

¶ 41. More generally, if $n \in \mathbb{N}$, let VS_n be the theory of vector spaces of dimension at least n in the signature

$$\{\mathbf{0}, -, +, \|^n\},$$

where $\|^n$ stands for the n-ary relation of linear dependence. (If we include the signature of the scalar field, then the space can have any dimension.) This has a model companion, namely the theory of n-dimensional vector spaces over an algebraically closed field. For, if again $K \subseteq L$, and $(a_1, \dots, a_n, 1)$, that is, $(\boldsymbol{a}, 1)$, is an $(n+1)$-tuple from L that is linearly independent over K, then $(K^{n+1}, \|^n_K)$ embeds in $(L^n, \|^n_L)$ under

$$\boldsymbol{x} \mapsto \boldsymbol{x} \cdot \begin{pmatrix} I_n \\ \hline -\boldsymbol{a} \end{pmatrix}.$$

¶ 42. There is an analogy with fields. Let

$$M = K(a_0, \dots, a_n),$$

where $(a_0, \dots, a_n)$ is algebraically independent over K. Then there is a field L such that $K \subseteq L$, and

$$\text{tr-deg}(ML/L) = n,$$

but if $(b_1, \dots, b_n)$ from M is algebraically independent over K, then it remains so over L. Indeed, we can take

$$L = K(x, y),$$

where x is transcendental over M, but

$$y = \sum_{k=0}^{n} a_k x^k.$$

References

[1] Richard Dedekind, *Essays on the theory of numbers. I: Continuity and irrational numbers. II: The nature and meaning of numbers*, authorized translation by Wooster Woodruff Beman, Dover Publications Inc., New York, 1963. MR MR0159773 (28 #2989)

[2] Descartes, *The geometry of René Descartes*, Dover Publications, Inc., New York, 1954, Translated from the French and Latin by David Eugene Smith and Marcia L. Latham, with a facsimile of the first edition of 1637.

[3] John Dyer-Bennet, *A theorem on partitions of the set of positive integers*, Amer. Math. Monthly **47** (1940), 152–154. MR MR0001234 (1,201b)

[4] Euclid, *Euclid's Elements*, Green Lion Press, Santa Fe, NM, 2002, All thirteen books complete in one volume, the Thomas L. Heath translation, edited by Dana Densmore. MR MR1932864 (2003j:01044)

[5] Kurt Gödel, *On formally undecidable propositions of* principia mathematica *and related systems I (1931)*, From Frege to Gödel (Jean van Heijenoort, ed.), Harvard University Press, 1976, pp. 596–616.

[6] Wilfrid Hodges, *Model theory*, Encyclopedia of Mathematics and its Applications, vol. 42, Cambridge University Press, Cambridge, 1993. MR 94e:03002

[7] Victor J. Katz (ed.), *The mathematics of Egypt, Mesopotamia, China, India, and Islam: A sourcebook*, Princeton University Press, Princeton and Oxford, 2007.

[8] Edmund Landau, *Foundations of analysis. The arithmetic of whole, rational, irrational and complex numbers*, third ed., Chelsea Publishing Company, New York, N.Y., 1966, translated by F. Steinhardt; first edition 1951; first German publication, 1929. MR 12,397m

[9] Giuseppe Peano, *The principles of arithmetic, presented by a new method (1889)*, From Frege to Gödel (Jean van Heijenoort, ed.), Harvard University Press, 1976, pp. 83–97.

[10] David Pierce, *Model-theory of vector-spaces over unspecified fields*, Arch. Math. Logic **48** (2009), no. 5, 421–436. MR MR2505433

[11] Alfred Tarski, *A decision method for elementary algebra and geometry*, University of California Press, Berkeley and Los Angeles, Calif., 1951, 2nd ed. MR MR0044472 (13,423a)

Mathematics Dept, METU, Ankara 06531, Turkey
E-mail address: dpierce@metu.edu.tr
URL: http://metu.edu.tr/~dpierce/