Model Theory of Fields with Operators

Piotr Kowalski

Instytut Matematyczny
Uniwersytetu Wrocławskiego

PhDs in Logic VIII, Darmstadt, May 9-11, 2016

Beginnings

Initial setting

- A first-order language L;
- First order L-formulas, L-sentences and L-theories T;
- L-structures $\mathcal{M}$ which may be models of T, denoted $\mathcal{M} \models T$.

Example (Groups)

- $L = \{\cdot, e\}$ (or $L = \{\cdot\}$, or $L = \{\cdot, ^{-1}, e\}$);
- An L-structure $\mathcal{M} = (M, \cdot_M, e_M)$ is a set with one binary function $\cdot_M$ and one constant e_M;
- T: the theory of groups, e.g. the sentence below is in T

$$\forall x, y, z \qquad (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

- Models of T: groups.

Beginnings ct.

Example (Fields)

- $L = \{\cdot, +, 0, 1\}$;
- An L-structure $\mathcal{M} = (M, +_M, \cdot_M, 0_M, 1_M)$ is a set M with two binary functions $+_M, \cdot_M$ and two constants $0_M, 1_M$;
- T: the theory of fields, e.g. T contains the sentence $\forall x \ \ (x \neq 0 \ \rightarrow \ \exists y \ x \cdot y = 1)$
- Models of T: fields.

Example (Linear orders)

- $L = \{\leqslant\}$ and an L-structure $\mathcal{M} = (M, \leqslant_M)$ is a set M with a binary relation $\leqslant_M$;
- T: the theory of linear orders, e.g. T contains the sentence $\forall x, y \quad x \leqslant y \ \vee \ y \leqslant x$
- Models of T: linear orders.

Consistent theories and Compactness Theorem

Definition

A theory T is consistent if every finite subset of T has a model.

Compactness Theorem

Every consistent L-theory T has a model $\mathcal{M}$ (s.t. $|M| \leqslant |L| + |T|$).

Example (Fields of characteristic 0)

Let T be the theory of fields of characteristic 0 and T' a finite subset of T. Let n be the biggest number such that the sentence $1 + \ldots + 1 \neq 0$ (addition taken n times) is in T. Then $\mathbb{F}_p \models T'$, for any prime number p greater than n. By Compactness Theorem, *there is a field of characteristic* 0.

Of course, we know particular models of T as $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ etc. But the argument above also shows that fields of characteristic zero are kind of "logical limits" of fields of finite characteristic.

Elementary extensions

Definitions

Let $\mathcal{M}$ be an L-substructure of an L-structure $\mathcal{N}$. We say that $\mathcal{N}$ is elementary extension of $\mathcal{M}$ (denoted $\mathcal{M} \preccurlyeq \mathcal{N}$), if for every L-sentence φ with parameters from M, we have that:

$$\mathcal{M} \models \varphi \quad \text{iff} \quad \mathcal{N} \models \varphi.$$

Löwenheim-Skolem (upward) Theorem

For any infinite L-structure $\mathcal{M}$ and any cardinal number $\kappa \geqslant |M|$, there is an elementary extension $\mathcal{M} \preccurlyeq \mathcal{N}$ such that $|N| = \kappa$.

Proof of Löwenheim-Skolem

Compactness Theorem for $T := \mathrm{Th}_M(\mathcal{M}) \cup \{c_i \neq c_j \mid i < j < \kappa\}$.

The theory ACF

Definitions

- Let ACF denote the theory of algebraically closed fields. Note that ACF has infinitely many axioms.
- For p being a prime number or $p = 0$, let ACF_p denote the theory of algebraically closed fields of characteristic p.

Theorem (ACF is model complete)

Any extension of models of ACF is elementary.

Theorem (Completions of ACF)

The theories ACF_p are complete, i.e. for any two models K, L of ACF_p and any sentence φ, we have $K \models \varphi$ iff $L \models \varphi$.

Lefschetz Principle

L. P. is often used informally in algebraic geometry in the form: *"If something is true for algebraically closed fields of arbitrarily large characteristic, then it is also true for $\mathbb{C}$."*

A formal version is below. Let φ be a sentence in the language of rings. Then the following are equivalent:

1. For all algebraically closed fields K of characteristic 0, we have $K \models \varphi$.
2. For infinitely many primes p and all algebraically closed fields K of characteristic p, we have $K \models \varphi$.
3. For almost all primes p and all algebraically closed fields K of characteristic p, we have $K \models \varphi$.

Ax's Theorem

One of the applications of Lefschetz Principle (so, in fact, of Compactness Theorem) is the following result.

Theorem (Ax)

Suppose that K is an algebraically closed field and $W : K^n \to K^n$ is a polynomial function. If W is one-to-one, then W is onto.

Similar results are true in the contexts of: finite sets, finite dimensional vector spaces or (more generally) Noetherian modules. Note that for each $n, N > 0$, Ax's theorem for W of total degree smaller than N is a first-order sentence $\varphi = \varphi_{n,N}$. Hence:

1. By Lefschetz Principle for φ, we can assume that $K = \mathbb{F}_p^{\mathrm{alg}}$.
2. Since $\mathbb{F}_p^{\mathrm{alg}} = \bigcup_n \mathbb{F}_{p^n}$, we can assume that K is finite, OK.

Quantifier elimination

Let T be an arbitrary L-theory.

Definition

T has Quantifier Elimination, if for any L-formula $\varphi(x_1, \ldots, x_n)$ there is an L-formula without quantifiers $\psi(x_1, \ldots, x_n)$ such that for any $\mathcal{M} \models T$ we have

$$\mathcal{M} \models \forall x_1, \ldots, x_n\ \varphi(x_1, \ldots, x_n) \leftrightarrow \psi(x_1, \ldots, x_n).$$

Remark

Note that for any L-extension $\mathcal{M} \subseteq \mathcal{N}$ and any quantifier-free L-sentence ψ we have

$$\mathcal{M} \models \psi \quad \text{iff} \quad \mathcal{N} \models \psi.$$

Hence Quantifier Elimination implies Model Completeness.

Definable sets

In different branches of mathematic, we are interested in sets of different types (and with possible extra structures), e.g.:

- set theory: just sets
- topology: topological spaces
- differential geometry: manifolds
- algebraic geometry: algebraic varieties

In model theory, we are interested in definable sets. Let $\mathcal{M}$ be an L-structure and $V \subseteq M^n$ ($A \subset M$).

Definition

V is definable in $\mathcal{M}$ (over parameters A), if there is an L-formula $\varphi(x_1, \ldots, x_n)$ (with parameters from A) such that

$$V = \{(m_1, \ldots, m_n) \in M^n \mid \mathcal{M} \models \varphi(m_1, \ldots, m_n)\}.$$

Examples of definable sets

- If V is finite or cofinite, then V is clearly definable (over the parameters coming from V or its complement).
- If K is a field and $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$, then the set of solutions of the system of equations:

$$f_1(\overline{v}) = 0 \ \wedge \ \ldots \ \wedge \ f_m(\overline{v}) = 0$$

  is definable. Such definable sets are called Zariski closed.
- The formula $\exists z \ x - y = z \cdot z$ defines the order in $(\mathbb{R}, +, \cdot)$.
- It can be shown that $\mathbb{N}$ is definable in $(\mathbb{Z}, +, \cdot)$ (Lagrange's four-square theorem) and that $\mathbb{Z}$ is definable in $(\mathbb{Q}, +, \cdot)$ (this is more difficult).
- It can be also shown that neither $\mathbb{Z}$ nor $\mathbb{Q}$ is definable in $(\mathbb{C}, +, \cdot)$. Actually, only finite and cofinite subsets of $\mathbb{C}$ are definable (this follows from quantifier elimination for ACF).

Quantifier-free definable sets

A subset $V \subseteq M^n$ is quantifier-free definable, if there is a formula without quantifiers $\varphi(x_1, \ldots, x_n)$ such that

$$V = \{(m_1, \ldots, m_n) \in M^n \mid \mathcal{M} \models \varphi(m_1, \ldots, m_n)\}.$$

Quantifier-free definable sets in fields

Suppose that K is a field

- If $V \subseteq K$ is quantifier-free definable, then V is finite or cofinite (a non-zero polynomial has finitely many roots).
- More generally, if $V \subseteq K^n$ is Zariski closed, then V is quantifier-free definable, and any quantifier-free definable subset of K^n is Boolean combination of Zariski closed sets.

Quantifier Elimination for ACF

Theorem (Tarski)

The theory ACF has quantifier elimination.

Reason: quantifier-free formulas determine the isomorphism type

Let $\bar{a}, \bar{b} \in K^n$ ($K \models ACF$) and F be a subfield of K. Then TFAE:

1. There is an F-isomorphism between $F(\bar{a})$ and $F(\bar{b})$ which takes $\bar{a}$ to $\bar{b}$.
2. $I_F(\bar{a}) = I_F(\bar{b})$, where

$$I_F(\bar{a}) = \{W \in F[X_1, \ldots, X_n] \mid W(\bar{a}) = 0\}.$$

The second condition is quantifier-free and any F-isomorphism between $F(\bar{a})$ and $F(\bar{b})$ extends to an F-automorphism of K.

Chevalley constructibility theorem

Definition

Let X be a topological space. A subset $V \subseteq X$ is constructible, if it is a finite union of locally closed sets.

Let K be a field

- On each $X = K^n$, Zariski closed sets are closed sets of a topology called Zariski topology (Hilbertscher Basissatz).
- Quantifier-free definable subsets of K^n are exactly Zariski constructible sets.

Theorem (Chevalley)

Let K be an algebraically closed field, $F : K^n \to K^m$ be a polynomial function and $V \subseteq K^n$ be a constructible set. Then the set $F(V)$ is constructible.

Chevalley constructibility theorem: examples

Example

- Let $V \subset K \times K$ be given by the equation $XY = 1$ (hyperbola).
- Let $F : K \times K \to K$ be the projection on the x-axis.
- Then $F(V) = K \setminus \{0\}$, so $F(V)$ is *not* Zariski closed.
- Clearly, $F(V)$ is constructible.

Example

- Let $V \subset \mathbb{R} \times \mathbb{R}$ be given by the equation $X = Y^2$ (parabola).
- Let $F : K \times K \to K$ be the projection on the x-axis.
- Then $F(V) = [0, \infty)$, so $F(V)$ is *not* Zariski constructible (since constructible subsets of a field are finite or cofinite).
- Clearly, the field $\mathbb{R}$ is not algebraically closed.

Chevalley constructibility theorem: proof

It follows immediately from Quantifier Elimination for ACF:

1. Any constructible set V is definable.
2. The image $F(V)$ of a definable set is again definable (plugging the existential quantifier).
3. By Quantifer Elimination for ACF, the set $F(V)$ is quantifier-free definable.
4. We know that quantifier-free definable sets (in fields) are constructible.

Hilbert's Tenth Problem

Hilbert's 10

Find a general algorithm for deciding, given $n > 0$ an $f \in \mathbb{Z}[X_1, \ldots, X_n]$, whether or not f has a zero in $\mathbb{Z}^n$.

Theorem (Matiyasevich, 1970)

No such algorithm exists. In particular, the existential theory of $(\mathbb{Z}, +, \cdot)$ *is undecidable.*

Hilbert's 10 for $\mathbb{Q}$

Is the existential theory of $(\mathbb{Q}, +, \cdot)$ decidable?

This is still an open problem.

Hilbert's Tenth Problem and definability of $\mathbb{Z}$ in $\mathbb{Q}$

- By Matiyasevich theorem, IF $\mathbb{Z}$ is existentially definable in $(\mathbb{Q}, +, \cdot)$, THEN the answer to Hilbert's 10 for $\mathbb{Q}$ is "NO".
- It is still an open problem whether $\mathbb{Z}$ is existentially definable in $(\mathbb{Q}, +, \cdot)$.
- It is easy to see that if $\mathbb{Z}$ is existentially definable in $(\mathbb{Q}, +, \cdot)$, then $\mathbb{Z}$ is universally definable in $(\mathbb{Q}, +, \cdot)$.
- Julia Robinson showed that $\mathbb{Z}$ is "$\forall x_1, x_2 \exists y_1, \ldots, y_7 \forall z_1, \ldots, z_6$"-definable in $(\mathbb{Q}, +, \cdot)$
- Bjorn Poonen showed that $\mathbb{Z}$ is "$\forall x_1, x_2 \exists y_1, \ldots, y_7$"-definable in $(\mathbb{Q}, +, \cdot)$
- Koeningsmann showed that $\mathbb{Z}$ is universally definable in $(\mathbb{Q}, +, \cdot)$ (as I already said on Monday).

Definability of $\mathbb{Z}$ in $\mathbb{Q}$ ct.

Koeningsmann's result has a following geometric formulation.

Theorem

There is a Zariski closed set $V \subseteq \mathbb{Q}^N$ and a $\mathbb{Q}$-polynomial map $\pi : \mathbb{Q}^N \to \mathbb{Q}$ such that $\pi(V) = \mathbb{Q} \setminus \mathbb{Z}$.

It is expected that $\mathbb{Z}$ is *not* existentially definable in $(\mathbb{Q}, +, \cdot)$.

Theorem (Koeningsmann)

The Bombieri-Lang conjecture (an open problem in diophantine geometry) implies that $\mathbb{Z}$ is not existentially definable in $(\mathbb{Q}, +, \cdot)$.

However, Hilbert's 10 for $\mathbb{Q}$ may have the negative answer for other reasons...

Differential fields

We will consider fields with extra unary functions of special kinds (operators). Main examples of such functions are derivations and endomorphisms. Let us start with derivations. We fix:

- The language $L = \{+, \cdot, \partial, 0, 1\}$;
- A field K.

Definition

A function $\partial_K : K \to K$ is called derivation, if for all $a, b \in K$:

- $\partial_K(a + b) = \partial_K(a) + \partial_K(b)$;
- $\partial_K(ab) = \partial_K(a)b + \partial_K(b)a$.

A pair (K, ∂_K) consisting of a field and a derivation is called differential field.

We will write just (K, ∂) for a differential field.

Examples of differential rings and fields

There is a corresponding notion of a differential ring.

Example

1. Let $C^\infty(\mathbb{R})$ be the ring of infinitely differentiable functions from $\mathbb{R}$ to $\mathbb{R}$. Then it becomes a differential ring with the standard derivation $\partial(f) = f'$.
2. Let k be an arbitrary ring and $R := k[X]$. Let
$$\partial(\alpha_n X^n + \ldots + \alpha_1 X + \alpha_0) := n\alpha_n X^{n-1} + \ldots + \alpha_1.$$
(R, ∂) is a differential ring. For $k = \mathbb{R}$ it may be understood as a differential subring of the differential ring from (1).
3. Let $K = \mathbb{R}(X)$. We extend the derivation from $\mathbb{R}[X]$ to $\mathbb{R}(X)$ by the formula: $\partial(F/W) = (\partial(F)W - \partial(W)F)/W^2$. Then (K, ∂) is a differential field.

Differential closed fields: idea

We need a notion of a special differential field which among the class of differential fields will play the same role as algebraically closed fields play among the class of (pure) fields. In other words, in such differential fields, we want to be able to solve all the "solvable polynomial differential equations".

Polynomial differential equations

1. Let (K, ∂) be a differential field and $W \in K[X_0, \ldots, X_n]$.
2. By polynomial differential equations, we mean an L-term of the form $\mathcal{W}(x) = 0$, where

$$\mathcal{W}(x) := W(x, \partial(x), \partial(\partial(x)), \ldots, \partial^{(n)}(x)),$$

and $\partial^{(n)}$ denotes $\partial \circ \ldots \circ \partial$ (composition taken n times). It is of order n, if $W \notin K[X_0, \ldots, X_{n-1}]$.

Differential closed fields: axioms

In the language L of differential fields, we define the following theory (of differentially closed fields of characteristic 0).

The theory DCF_0

An L-structure (K, ∂) is a model of DCF_0, if:

1. (K, ∂) is a differential field of characteristic 0;
2. For any $n > 0$, and any differential equation $\mathcal{W}(x) = 0$ of order n, and any differential equation $\mathcal{F}(x) = 0$ of order smaller that n, there is $a \in K$ such that

$$\mathcal{W}(a) = 0 \quad \wedge \quad \mathcal{F}(a) \neq 0.$$

Common context for ACF and DCF_0

Let T be now an arbitrary theory and $\mathcal{M} \models T$.

Definition

$\mathcal{M}$ is existentially closed model of T, if for any

- extension $\mathcal{M} \subseteq \mathcal{N}$ of models of T;
- quantifier free formula $\varphi(\bar{x})$ with parameters from M;

IF there is $\bar{b} \in N^n$ such that $\mathcal{N} \models \varphi(\bar{b})$,
THEN there is $\bar{a} \in M^n$ such that $\mathcal{M} \models \varphi(\bar{a})$.

"All solvable equations over M can be solved in $\mathcal{M}$."

Definition

A theory T^* is model companion of T, if the models of T^* are exactly the existentially closed models of T.

Common context for ACF and DCF_0 ct.

Model companion of T may exist or not. If T^* is a model companion of T, then T^* is model complete (Robinson's test).

Example

- ACF is a model companion of the theory of fields.
- DCF_0 is a model companion of the theory of differential fields of characteristic 0.
- There is a model companion (called ACFA) of the theory of fields with an automorphism.
- There is *no* model companion of the theory of fields with two commuting automorphisms (Hrushovski).

Properties of DCF_0

The theory DCF_0 shares many nice properties of ACF_0, but it is model-theoretically much richer, i.e. we have more interesting definable sets. Some properties are below:

- DCF_0 has quantifier elimination.
- DCF_0 is complete.
- Any differential field (F, ∂) has differential closure, which is unique up to a differential isomorphism fixing F.
- However, unlike in the case of ACF, this differential closure is not minimal (Rosenlicht).

Strongly minimal theories

We consider again a general case. Let T be any theory.

Definition

T is strongly minimal, if for any $\mathcal{M} \models T$ each definable subset of M is finite or cofinite.

Remarks

1. The theory ACF is strongly minimal.
2. The theory of vector spaces (over a fixed field) is strongly minimal.
3. The theory of "nothing" or of pure sets is strongly minimal.
4. The theory DCF_0 is not strongly minimal, consider the constant field
$$C = \{a \in K \mid \partial(a) = 0\}.$$

Podewski's conjecture

Definition

- A structure is strongly minimal, if its theory is strongly minimal.
- A structure $\mathcal{M}$ is minimal, if all definable subsets of M are finite or cofinite.

- Note that being minimal is a weaker (and "less logical"!) condition than being strongly minimal.
- We know that algebraically closed fields are strongly minimal (quantifier elimination). Macintyre proved the converse: any strongly minimal field is algebraically closed (much more is true).
- Podewski conjectured in 1973 that any minimal field is algebraically closed. Surprisingly, this is still an open problem. Wagner proved it for fields of positive characteristic.

Strongly minimal formulas

We still consider a general case. Let T be a theory and $\varphi(x_1, \ldots, x_n)$ a formula.

Definition

The formula $\varphi(x_1, \ldots, x_n)$ is strongly minimal (relative to T) if for each $\mathcal{M} \models T$ the only definable subsets of the set defined in $\mathcal{M}$ by $\varphi(x_1, \ldots, x_n)$ are finite or cofinite.

Example

1. A theory T is strongly minimal iff the formula "$x = x$" is strongly minimal.
2. If $T = \mathrm{DCF}_0$, then the formula "$\partial(x) = 0$" (defining the field of constants) is strongly minimal.

Richness of DCF_0

In differentially closed fields, we can find strongly minimal sets (i.e. sets defined by strongly minimal formulas) "looking like":

1. Fields: given by differential equation $\partial(X) = 0$.
2. Pure sets: given by Painlevé equations (Nagloo-Pillay), e.g.

$$\partial(\partial(X)) = 6X^2 + t,$$

   where t is transcendental over $\mathbb{Q}$.
3. Vector spaces: given by certain natural differential equations coming from elliptic curves.

The above "looking like" may be understood as having "as much as" definable subsets of M^2. E.g. a field has a lot of them (all plane curves), a vector space has less (affine subspaces) and a pure set has almost none (diagonal, vertical and horizontal lines).

Zilber's Trichotomy Conjecture

Zilber's conjecture (1970's)

Let $\mathcal{M}$ be a strongly minimal structure which does not "look like" neither a vector space nor a pure set. Then there is an infinite field definable in $\mathcal{M}$ (necessarily algebraically closed).

In other words, Zilber conjectured that *any* strongly minimal structure "looks like" a pure set or a vector space or an algebraically closed field.

Theorem (Hrushovski)

There is a strongly minimal structure $\mathcal{M}$ which does not "look like" neither a pure set nor a vector space and such that there are no infinite groups definable in $\mathcal{M}$.

This theorem means that Hrushovski provided a strong counterexample for Zilber's conjecture.

Zilber's Trichotomy for DCF_0 and its application

Zilber's conjecture (even being false) is still very important and influential, since it is often true in important classes of structures.

Theorem (Hrushovski-Sokolović)

Strongly minimal sets definable in models of DCF_0 satisfy Zilber's conjecture in a strong form: any such set which does not "look like" neither a pure set nor a vector space can be identified with an algebraic curve over the field of constants.

1. Using Zilber's conjecture for DCF_0, Hrushovski gave a proof of a function field version of Mordell-Lang conjecture in characteristic 0. This result was already known.
2. Using the truth of Zilber's conjecture for "positive characteristic version of DCF_0", Hrushovski showed a function field version of Mordell-Lang conjecture in positive characteristic. This was an open problem.

The theory ACFA

Recall that ACFA denotes the model companion of the theory of fields with an automorphism.

Theorem (Chatzidakis-Hrushovski-Peterzil)

Strongly minimal sets definable in models of ACFA satisfy Zilber's conjecture in a strong form, similarly as for DCF_0 (however, in the positive characteristic case there are more constant fields).

This theorem again has important applications.

1. Results of the type of Manin-Mumford conjecture.
2. Results about algebraic dynamics.

Nonstandard Frobenius

Hrushovski has proved an amazing result saying that "a non-standard Frobenius is a generic automorphism".

Theorem (Hrushovski)

Let $\mathcal{U}$ be a non-principal ultrafilter on the set $\mathbb{P}$ of prime numbers. Then the following ultraproduct

$$\prod_{p\in\mathbb{P}}(\mathbb{F}_p^{\mathrm{alg}}, x\mapsto x^p)/\mathcal{U}$$

is a model of ACFA

This theorem also has important applications and for its proof (the paper has 149 pages) Hrushovski needed to invent difference intersection theory generalizing (already difficult) intersection theory from algebraic geometry.

Some things I did not say

There are lots of interesting recent developments in model theory (of fields or in general) which I had no time to mention. They include:

- The theory of o-minimal fields (like $\mathbb{R}$) and its applications to diophantine geometry as André-Oort conjecture (Pila-Wilkie).
- The model theory of fields with valuation and its applications to the theory of Berkovich spaces (Loeser-Hrushovski) and to the theory of motivic integration (Hrushovski-Kazhdan).
- Applications of model theory to additive combinatorics (Hrushovski, Breuillard-Green-Tao).

That's all, thanks!