MODEL THEORY OF DIFFERENTIAL FIELDS

MOSHE KAMENSKY

1. Introduction

Consider a finite system X of equations $p_i(x_1,\dots,x_k)=0$, for $1\le i\le n$, where p_i are polynomials over $\mathbb{Q}$. What can be said about the set S of solutions of X whose coordinates are all roots of unity? For example, in what cases is S infinite?

To make the question more precise, one needs in particular to specify where the solutions to X are taken to begin with. However, all roots of unity are contained in the algebraic closure of $\mathbb{Q}$, so we are free to choose any field that contains it, for example $\mathbb{C}$. In this case, the set $X(\mathbb{C})$ of complex valued solutions has a geometric structure (essentially a complex analytic manifold, though it may have some "corners"). Without choosing $\mathbb{C}$, we may still view X as a geometric object: it is an example of an *affine algebraic variety.* The set S we would like to study is the intersection $X(\mathbb{C})\cap T$, where T is the set of all n-tuples of roots of unity.

If T was also an algebraic variety, i.e., if $T=Y(\mathbb{C})$ for some system of polynomial equations, it would be possible to study such questions via geometry: algebraic varieties admit a good notion of dimension, and a well developed theory of intersection, predicting the dimension and number of points in the intersection. However, no such system Y exists: it is easy to check that the set T does not (collectively) satisfy any non-trivial polynomial relation.

A fundamental idea then is to enlarge the class of possible equations, in a manner that will provide non-trivial information on the set T, while keeping the structure of such equations manageable. There are a number of useful choices for such structures, and in this course we will concentrate on a differential one.

In place of the field $\mathbb{C}$ we chose above, we consider for instance the field K of meromorphic functions on an open disc D in the complex plane. K is equipped with a natural additional structure: the derivative $'$ on meromorphic functions. Using this additional structure, we may form new equations, on top of the polynomial ones we had before. In particular, the set of all roots of unity is contained in the set of solutions of the equation $p(x)=0$, where $p(x)=x'$ is now a *differential polynomial.* This follows from the fact that the set of solutions to this equation is $\mathbb{C}$, an algebraically closed field, but a more conceptual approach is replace the above equation by the equation $l(x)=0$, where $l(x)=\frac{x'}{x}$. The point is that $l_K:K^*\to K$ is a group homomorphism from the multiplicative group to the additive one, and roots of unity are precisely the torsion points for the multiplicative structure, so must go to 0 in the additive one (which is torsion free).

As above, the full kernel of l is $\mathbb{C}^*$, so much "smaller" than K. With the theory of dimension that we will present, this will be one of the main examples of (the points of) a set of dimension 1. This example is in fact not very useful: after passing to the kernel, we no longer see the differential structure, and we are back to usual commutative algebra over $\mathbb{C}$. However, an analogous consideration for a different class of groups plays a role in one of the main applications of the model theory of differential fields to arithmetic, namely the proof (by Hrushovski) of the relative Mordell–Lang conjecture. We will explain elements of this proof, following the book [1], which is dedicated to it.

As another example, there is a classical function, the j-function, which is a holomorphic function on the upper-half plane $\mathbb{H} = \{z \in \mathbb{C} | \Im z > 0\}$. This function admits (and almost characterised by) the property that $j(z) = j(m(z))$ whenever $m : \mathbb{H} \to \mathbb{H}$ is an *integral Möbius transformation*, i.e., $m(z) = \frac{az+b}{cz+d}$, where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$. In other words, if $W_m = \{\langle z, m(z)\rangle | z \in \mathbb{H}\} \subseteq \mathbb{H} \times \mathbb{H}$ is the graph of m, then $j(W_m) \subseteq \Delta \subseteq \mathbb{A}^2$, so an algebraic subvariety W_m of $\mathbb{H}^2$ is mapped into a (proper) algebraic subvariety of $\mathbb{A}^2$. Since j is far from being a polynomial map, it is interesting to ask if there are other non-trivial algebraic relations among the values of j. It turns out that the answer is "no", even if one includes first and second derivatives of j (and also for generalisations of j). A crucial point in the proof (by Casale–Freitag–Nagloo, [2]) is that j satisfies a particular algebraic differential equation (of order 3). The proof proceeds by analysing the structure of this equation.

A fundamental observation is that the properties we are interested in are *algebraic* properties of the solutions, and thus one can expect to derive them from algebraic properties of the equations themselves. There is a number of approaches to formalising this idea, our basic notion will be that of a *differential field*:

derivation

Definition 1.0.1. Let A be a commutative ring. A *derivation* of A is an additive function $\partial : A \to A$ satisfying the Leibniz rule: $\partial(ab) = \partial(a)b + a\partial(b)$ for all $a, b \in A$.

differential ring

A *differential ring* is a pair $\langle A, \partial\rangle$ with A and ∂ as above.

Starting with a differential ring $A = \langle A, \partial\rangle$, it is possible to consider polynomial differential equations with coefficients in A, and their solutions (in a differential ring extending A). This way, algebraic properties of differential equations can be studied without reference to any analytic properties of their solutions. One expects to have a theory similar the theory of polynomial equations and their solutions, and such a theory, *differential algebra* and *differential algebraic geometry* indeed exists, but we will see that it is substantially more complicated than the algebraic situation. In particular, algebraically defined dimension is difficult to work with, there are no analogs of Noetherianity and primary decomposition, and so on.

Better tools are obtained via model theory. The relevant first order theory DCF belongs to the well-behaved class of ω-stable theories. Model theory provides good notions of rank for systems of equations (definable sets) in such a theory, and these turn out to be very useful in this setting. A central result is a detailed classification of definable sets of rank 1, which is the basis to the applications mentioned above. From a different point of view, DCF provides a non-degenerate example of an ω-stable theory, and examples of interesting model theoretic phenomena (for instance, distinction between Morley and Lascar ranks).

1.1. **More bibliography.** In addition to the references mentioned above, relevant information is contained in [5] and in [3]. For general model theory, [4] and [6] are useful.

1.2. **Tentative outline.**

- Review of first order logic (structures, models, formulas, theories, compactness) (1)
- The theory of fields, affine algebraic varieties (2)
- Quantifier elimination, model companions, ACF (3-4)
- More varieties, prolongations, DCF (5-6)
- Imaginaries (7)
- Morley rank, strong minimality, ω-stability (8-9)
- General properties of strongly minimal sets, orthogonality, Zilber trichotomy (abstract geometries?) (10-12)
- Abelian varieties, Isogenies, Manin kernels (13-14)
- Strong minimality of Fuchsian equations (CFN §3,4) (15-16)
- Zil'ber trichotomy in DCF (Zariski geometries/Jet spaces) (17-18)
- Geometric triviality of Fuchsian equations (CFN 5) (19)

2. Preliminaries

2.1. **Review of first order logic.** For completeness we recall the basic definitions. You might prefer to look in a basic logic book, or jump directly to Example 2.1.8.

Definition 2.1.1. A (1-sorted) *first order structure* is given by: **first order structure**

(1) A set M ("the universe")
(2) For every finite set J, a boolean sub-algebra D_J of $\mathcal{P}(M^J)$ ("definable subsets")

satisfying:

(1) If $X \in D_I$ and $Y \in D_J$ where I, J are disjoint, then $X \times Y \in D_{I \cup J}$
(2) For any function $t : I \to J$, for all $X \in D_J$, $t^*X = \{f \circ t | f \in X\} \in D_I$

Less formally, if $f \in M^J$ and $t : I \to J$, then $f \circ t \in M^I$ is the point obtained from f by picking the coordinates as dictated by t, and t^*X is the image of X under this map. In particular:

- If t is a permutation of J, then $f \circ t$ is a tuple obtained by permuting the coordinates
- If t is the inclusion of a subset I, t^* is the projection to the coordinates in I
- If J is a singleton (and t is the unique function from I), then t^* is the diagonal map from $M^J = M$ to M^I.

All other cases are determined as combinations of these ones. The definition for the general (multi-sorted) case is similar, and we will review it later. It is clear that given an arbitrary collection D of subsets of M^I, for various I, there is a smallest structure with universe M where all these subsets are definable. We will call it the structure generated by D.

Exercise 2.1.2. Assume $X \in D_I(M)$ and $Y \in D_J(M)$ for some structure M. Show that $\{f \in M^{I\cup J} | f_I \in X, f_J \in Y\} \in D_{I\cup J}(M)$, where f_I is the restriction of f to I. □

For X, Y definable in a structure M, we say that a function $f : X \to Y$ is definable if its graph $\Gamma_f = \{\langle x, y\rangle \in X \times Y | y = f(x)\}$ is definable.

Exercise 2.1.3. For each $t : I \to J$ and $X \in D_J$, the function $f \mapsto f \circ t$ is definable □

Exercise 2.1.4. If X, Y, Z are definable in M, and $f : X \to Z$, $g : Y \to Z$ are definable, then $X \times_Z Y = \{\langle x, y\rangle \in X \times Y | f(x) = g(y)\}$ is definable. □

The notion of a structure is important, but for us it will be more useful to have a more syntactic description, for a number of reasons. First, as will be seen below, it is a convenient and natural way to describe definable sets. More importantly, the syntax provides a way to relate "the same" definable subset of two different structures. Our variant of syntax is given as follows:

first order language

Definition 2.1.5. A (relational, 1-sorted) *first order language* is given by a set $\mathcal{F}_I$ of "formulas in the variables I", for every finite set I, along with:

(1) Functorial[1] maps $t_* : \mathcal{F}_I \to \mathcal{F}_J$ for every function $t : I \to J$.
(2) Operations $\to: \mathcal{F}_I \times \mathcal{F}_I \to \mathcal{F}_I$ and $\exists i : F_I \to \mathcal{F}_{I\setminus\{i\}}$ for all i.
(3) Prescribed elements $\mathbf{0} \in \mathcal{F}_\emptyset$ and $= \in \mathcal{F}_{\mathbf{2}}$

The sets I should be thought of as variables. If $I = \{x, y, z, \dots\}$, we write $\phi(x, y, z, \dots)$ for a typical element of $\mathcal{F}_I$, and call it "a formula in the free variables I". We write $\phi \to \psi$ in place of $\to (\phi, \psi)$, reading "ϕ implies ψ", etc. The operations t_* correspond to variable substitution.

We make the following abbreviations:

- $\neg\phi := \phi \to \mathbf{0}$ ("not ϕ"). We set $\mathbf{1} := \neg\mathbf{0}$

[1]This means that $(t \circ s)_* = t_* \circ s_*$ for all t, s, and t_* is the identity map whenever t is

- $\phi \vee \psi := (\neg\phi) \to \psi$, $\phi \wedge \psi := \neg((\neg\phi) \vee (\neg\psi))$
- $\forall x\phi := \neg\exists x(\neg\phi)$
- $\exists! x\phi := \exists x\phi \wedge \forall y, z(t_*\phi \wedge s_*\phi \to y = z)$, where $t, s : \{x\} \to \{y, z\}$ send x to y and to z, respectively.

We note that our definition of the syntax is somewhat more general than usual, but this will not make a substantial difference.

The relation between the syntax and the semantics is given by the following definition:

Definition 2.1.6. Let $\mathcal{F} = (\mathcal{F}_I)_I$ be a language. An $\mathcal{F}$*-structure* consists of a set M and an assignment $\phi \mapsto \phi(M) \subseteq M^I$ for each $\phi \in \mathcal{F}_I$, such that: **$\mathcal{F}$-structure**

- For each $t : I \to J$ and each $\phi \in F_I$, $(t_*\phi)(M) = \{f \in M^J | f \circ t \in \phi(M)\}$
- $\mathbf{0}(M) = \emptyset$, $=(M) = \{\langle m, m\rangle | m \in M\}$
- $(\phi \to \psi)(M) = \phi(M)^c \cup \psi(M)$
- $(\exists x\phi)(M) = t^*\phi(M)$, where $t : I \setminus \{x\} \to I$ is the inclusion map

Exercise 2.1.7. If $\mathcal{F}$ is a first order language and M is an $\mathcal{F}$-structure, then, with the collection of subsets $D_I = \{\phi(M) | \phi \in \mathcal{F}_I\}$ it is a first order structure.

Conversely, every first-order structure is an $\mathcal{F}$-structure, for a canonically defined $\mathcal{F}$. $\square$

Given a first order language $\mathcal{F}$, and collection of subsets $R_I \subseteq \mathcal{F}_I$ for each I, it is easy to see that there is a smallest sub-language $\mathcal{F}' \subseteq \mathcal{F}$ containing the R_I. If $\mathcal{F}' = \mathcal{F}$, we say that $\mathcal{F}$ is generated by the R_I, and often describe only the R_I. Any $\mathcal{F}$ structure is determined by its restriction to R_I.

Furthermore, given a set R_I for each I, it is possible to construct a "free" language generated by the R_I, and in practice one restricts to languages of this form (the R_I are called a *signature*). The freeness implies that any assignment of subsets (of the correct arity) to the elements of R_I extends to and $\mathcal{F}$ structure. **signature**

Example 2.1.8. Let A be a commutative ring. We consider the first order language $\mathcal{F}$ generated by the formulas $R_I = \{p = 0 | p \in A[I]\}$, where $A[I]$ is the algebra of polynomials in the variables I, with coefficients in A. We will call this the language of (commutative) A-algebras.

Any commutative A-algebra B determines a structure for this language, by assigning to $p = 0$ the set of solutions of this equation in B. $\square$

So far, we did not consider any substantial way of restricting the structures. For instance, in the last example, there are many more $\mathcal{F}$-structures than commutative A-algebras. This can be fixed by noting that the language considered above can be used to describe those structure that are commutative A-algebras.

To make this precise, we note that by definition, for an element $\phi \in \mathcal{F}_\emptyset$ and an $\mathcal{F}$-structure M, $\phi(M) \subseteq \mathbf{1} = \{\emptyset\} = M^\emptyset$. Such a ϕ is called a *sentence*, and we say that ϕ holds in M, or that M is a *model of* ϕ, if $\phi(M) = \mathbf{1}$. Similarly, if T is a set of sentences, we say that M is a *model of* T if it is a model of every element of T. We denote by $\mathcal{Mod}(T)$ the class of models of T, and say that a class of this form (for some T) is an *elementary class*.

sentence
model of ϕ
model of T
elementary class

Conversely, if C is a class of $\mathcal{F}$-structures, the *theory of* C, denoted by $\mathcal{Th}(C)$, is the set of sentences that hold in all members of C. A sentence ϕ *logically follows* from a set of sentences T if $\phi \in \mathcal{Th}(\mathcal{Mod}(T))$. A set of the form $\mathcal{Th}(C)$ for some class C is called a *theory*. Thus, a theory is a set of sentences closed under implication. Given a set of sentences T_0, there is a smallest theory that contains it (namely, $T = \mathcal{Th}(\mathcal{Mod}(T_0))$), and we normally do not distinguish between T and T_0 (one says that T_0 *axiomatises* T).

theory of C
logically follows
theory
axiomatises

A theory T is said to be *consistent* if it has a model, i.e., if $\mathcal{Mod}(T)$ is non-empty.

consistent

Example 2.1.9. The class of commutative A-algebras is elementary (in the language of A-algebras). Some examples of sentences that axiomatise the theory that shows it are:

(1) $\forall x \forall y \exists ! z (x + y - z = 0)$
(2) $\forall x \forall y \exists ! z (x * y - z = 0)$
(3) $\forall x, y (x - y = 0 \to x{=}y)$
(4) $\forall x, y, z, w (x + y - z = 0 \wedge y + x - w = 0 \to z{=}w)$
(5) ...

□

What is an example of a non-elementary class? A little experimenting shows that if A is finite (for example, $A = \mathbb{F}_p$), there is no theory axiomatising the class of finite A-algebras. To prove this, we recall:

Theorem 2.1.10 (The Compactness Theorem)**.** *If every finite subset of a theory T is consistent, then T is consistent.*

This theorem can be reformulated in many ways. For example:

Exercise 2.1.11. If a theory T implies a sentence ϕ, then a finite subset of T implies ϕ as well. □

As an application, we show that indeed the class of finite $\mathbb{F}_p$-algebras is not axiomatisable:

Corollary 2.1.12. *If T is a theory that has finite models of unbounded size, then it has an infinite model.*

Proof. We first note that for each $n \in \mathbb{N}$, there is a sentence ϕ_n whose models are structures of size at least n. Namely, ϕ_n is given by

$$\exists x_1, \dots, x_n (\bigwedge_{i<j\leq n} x_i \not= x_j)$$

Now, assume that T has arbitrary large models. Then every finite finite subset of $T_1 = T \cup \{\phi_n | n \in \mathbb{N}\}$ is consistent, since it has only finitely many

ϕ_i. By compactness, T_1 is also consistent, and each model of T_1 is an infinite model of T. □

End of lecture 1, Mar 22

References

[1] Elisabeth Bouscaren, ed. *Model theory and algebraic geometry.* Lecture Notes in Mathematics 1696. An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture. Berlin: Springer-Verlag, 1998. ISBN: 3-540-64863-1 (cit. on p. 2).

[2] Guy Casale, James Freitag, and Joel Nagloo. "Ax-Lindemann-Weierstrass with derivatives and the genus 0 Fuchsian groups". In: (2018). DOI: 10.48550/ARXIV.1811.06583. arXiv: 1811.06583 (cit. on p. 2).

[3] Deirdre Haskell, Anand Pillay, and Charles Steinhorn, eds. *Model theory, algebra, and geometry.* Mathematical Sciences Research Institute Publications 39. Cambridge: Cambridge University Press, 2000. ISBN: 0-521-78068-3. URL: http://www.msri.org/communications/books/Book39/contents.html (cit. on p. 3).

[4] David Marker. *Model theory: An introduction.* Graduate Texts in Mathematics 217. New York: Springer-Verlag, 2002. ISBN: 0-387-98760-6 (cit. on p. 3).

[5] David Marker, Margit Messmer, and Anand Pillay. *Model theory of fields.* 2nd ed. Lecture Notes in Logic 5. La Jolla, CA: Association for Symbolic Logic, 2006. ISBN: 978-1-56881-282-3; 1-56881-282-5 (cit. on p. 3).

[6] Katrin Tent and Martin Ziegler. *A Course in Model Theory.* Lecture Notes in Logic. Cambridge University Press, 2012. DOI: 10.1017/CBO9781139015417 (cit. on p. 3).

Department of Math, Ben-Gurion University, Be'er-Sheva, Israel
Email address: mailto:kamenskm@bgu.ac.il
URL: https://www.math.bgu.ac.il/~kamenskm