MODEL THEORY OF DIFFERENTIAL FIELDS

MOSHE KAMENSKY

1. Introduction

Consider a finite system X of equations $p_i(x_1, \ldots, x_k) = 0$, for $1 \leq i \leq n$, 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 $\mathcal{F}$. □

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. □

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 $\mathcal{M}od(T)$ 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 $\mathcal{T}h(C)$, is the set of sentences that hold in all members of C. A sentence ϕ *logically follows* from a set of sentences T if $\phi \in \mathcal{T}h(\mathcal{M}od(T))$. A set of the form $\mathcal{T}h(C)$ 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, $T = \mathcal{T}h(\mathcal{M}od(T_0))$, 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 $\mathcal{M}od(T)$ 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) $\dots$

□

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

$$\exists x_1, \dots, x_n(\bigwedge_{i<j\leq n} x_i \neq x_j)$$

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

2.2. **Expansion by constants.** There is a well defined notion of homomorphism for A-algebras. We discuss a variant of it for structures.

We fix a first-order language $\mathcal{F}$ and a subset $R_I \subseteq \mathcal{F}_I$ for each I, that freely generate $\mathcal{F}$, so that each R-structure extends uniquely to an $\mathcal{F}$-structure. We may say R-structures in place of $\mathcal{F}$-structures to stress when properties depend on R rather than $\mathcal{F}$. The elements of R_I are called *basic* (or *quantifier free*), and we assume they include $\mathbf{0}$ and $=$. **quantifier free**

Example 2.2.1. We modify Example 2.1.8 so that $R_{x,y}$ includes $\exists! z(x+y-z=0)$ and $\exists! z(xy-z=0)$, in addition to all polynomial equations. This will be our typical example. □

Definition 2.2.2. Let M and N be two R-structures. A *homomorphism* from M to N is a function $f : M \to N$ such that for all $\phi \in R_I$ and all $x \in M^I$, if $x \in \phi(M)$ then $f \circ x \in \phi(N)$. **homomorphism**

A subset M of a structure N such that the inclusion is a homomorphism is called a *substructure* of N. Note that a formula $\phi(x, y)$ defines (the graph of) a function on the set $\exists! y\phi(x, y)$, so if such a formula is included in R_I, a substructure is closed under the function defined by ϕ. **substructure**

Exercise 2.2.3. Show that in the setting of Example 2.2.1, when M and N are two structures viewed as A-algebras, a homomorphism from M to N is the same as a map of A-algebras. Show also that such a homomorphism need not satisfy the condition in the definition for an arbitrary formula ϕ. □

For a commutative A, the class of A-algebras can be described as follows: We start with the (elementary) class C of all commutative rings, fix a structure A, and consider the class of pairs (M, f), where M is in C and $f : A \to M$ is a homomorphism. We may repeat the same procedure with an arbitrary class of structures C and an arbitrary structure A, and obtain the class of structure in C over A, denoted $C_{A/}$.

In the case of commutative rings, we saw that the class obtained in this manner is elementary. The same is true in general, with a similar construction:

Definition 2.2.4. Let $\mathcal{F}$ be a language, and A a set. By the *expansion by constants* of $\mathcal{F}$ we mean the language $\mathcal{F}^A$ given by ${\mathcal{F}^A}_I = \bigcup_{A_0 \subseteq A} \mathcal{F}_{I \cup A_0}$, where the union is over all finite subsets A_0 of A. **expansion by constants**

If M is an $\mathcal{F}$-structure and $A \subseteq M$ (or, more generally, we are given an injective map from A to M), we view M as an $\mathcal{F}^A$-structure in the obvious way.

If T is a theory in $\mathcal{F}$ and A is an $\mathcal{F}$-structure, we let T_A be the theory obtained from T by adding all $\phi(a)$ for $\phi \in R_I$ such that $a \in \phi(A)$.

Exercise 2.2.5. The models of T_A are (naturally identified with) models M of T along with a homomorphism from A to M. □

universal formula
universal sentence

We may now show another application of the compactness theorem. By a *universal formula* we mean one of the form $\forall x \phi(x, y)$, where $\phi(x, y) \in R_I$ (so $(x, y) \in I$ are tuples of any length). A *universal sentence* is a sentence which is a universal formula. For a theory T, we denote by $T_\forall$ the set of universal sentences implied by T. Clearly, if M satisfies a given universal sentence ϕ, then any substructure satisfies ϕ. We claim that the converse also holds:

Proposition 2.2.6. *If T is any theory, then $\mathcal{M}od(T_\forall)$ is the class of substructures of models of T (in particular, this class is elementary)*

Proof. We already mentioned one direction, so we need to prove: if M is a model of $T_\forall$, then M is a substructure of a model of T. We have seen above that such a model is the same as a model of T_M, so we need to show that T_M is consistent.

Assuming not, by compactness a finite subset T_0 of T_M is inconsistent, and by taking conjunction, we may assume that $T_0 = \{\phi_0 \wedge \phi_1\}$, where ϕ_0 is in the language $\mathcal{F}$ of T, and $\phi_1 = \psi(m)$, with $\psi \in R$ and $m \in M$. So T implies $\neg\psi(m)$ for arbitrary m, but then T implies $\forall x \neg\psi(x)$, an element of $T_\forall$, contradicting that M was a model of it. □

Example 2.2.7. Let $\mathbb{F}$ be the theory of fields, in the language of Example 2.2.1 (so that a structure is a set along with binary functions $+$ and $\cdot$). The standard axiomatisation of $\mathbb{F}$ involves a non-universal sentence $\forall x \exists y (x = 0 \vee xy = 1)$. One could ask if this axiom can be replaced by a universal one. According to the proposition, the answer is no: a substructure of a field need not be a field.

Can we describe $\mathbb{F}_\forall$? An element of this theory is the sentence $\forall x, y (xy = 0 \to x = 0 \vee y = 0)$, i.e., there are no zero-divisors. This is the full theory, again according to the last proposition, since every integral domain is the substructure of a field (its field of fractions).

We note the dependence of these notions on the collection of quantifier free formulas: If we include the set $\phi(x) = \exists y (xy = 1)$ of invertible elements as "quantifier free", fields are axiomatised by the universal sentence $\forall x (x = 0 \vee \phi(x))$. □

2.3. **Quantifier free sets in the theory of fields.** We now completely specialize to the setup of Example 2.2.1, and the theory $\mathbb{F}$ of fields from the last example (possibly over a given ring A).

Our goal is to describe some of the structure of sets definable without quantifiers. This is (part of) the subject of *algebraic geometry*, and we will take a few small bites of it. We fix a field K, and denote by $S = K[x_1, \ldots, x_n]$ the polynomial ring over K in n variables. Each $p \in S$ determines a function $p : K^n \to K$.

Zariski closed subset

Definition 2.3.1. A *Zariski closed subset* of K^n is the set of solutions of a finite system of equations $p_1 = \cdots = p_m = 0$ with $\pi \in S$

Example 2.3.2. For $K = \mathbb{R}$, the equation $x^2 + y^2 - 1 = 0$ shows that the unit circle is a Zariski closed subset of $\mathbb{R}^2$. □

For a subset $I_0 \subseteq S$, we set $Z(I_0) = \{a \in K^n | p(a) = 0 \forall p \in I_0\}$. To which extent is I_0 determined by $Z(I_0)$? We consider several cases:

- If $I_0 = p, q$, then for every $r \in S$, $Z(I_0) = Z(p, rp + q)$.
- For every $p \in S$, $Z(p) = Z(p^2)$
- For $K = \mathbb{R}$, $Z(x^2 + 1) = Z(1) = \emptyset$

In the last case, there is no easily expressible algebraic relation between $x^2 + 1$ and 1 that would account for the equality, but the equality depends on the field $\mathbb{R}$: if we consider solutions in other fields (for instance, $\mathbb{C}$), the sets of solutions are no longer the same. We will return to this case later.

For the first instance, the general phenomenon is that a system of polynomials defines the same subset as the ideal it generates, so to remove the ambiguity we may restrict attention to ideals. This does not resolve the ambiguity presented in the second example, since p is (usually) not in the ideal generated by p^2. We will describe an explicit description later, but for the moment we bypass the difficulty with the following definition: For any subset $Y \subseteq K^n$, we let $I(Y) = \{p \in S | p(y) = 0 \forall y \in Y\}$.

Clearly, for all $Y \subseteq K^n$ the set $I(Y)$ is an ideal in S, and directly from the definition it follows that $I_0 \subseteq I(Z(I_0))$ and $Y \subseteq Z(I(Y))$ for all $I_0 \subseteq S$ and $Y \subseteq K^n$. The examples above show that the inclusion can be strict, even when I_0 is an ideal, but we have the following:

Exercise 2.3.3. For all $I_0 \subseteq S$, $Z(I(Z(I_0))) = Z(I_0)$ and for all $Y \subseteq K^n$, $I(Z(I(Y))) = I(Y)$ □

A priori, a subset of the form $Z(I)$ is not Zariski closed, according to our definition, since we required it to be the zero set of a *finite* number of polynomials. Of course, if I is finitely generated, as an ideal, this is not an issue. It turns out that all ideals in S are finitely generated, i.e., S is a *Noetherian ring*. This is known as

Noetherian ring

Theorem 2.3.4 (Hilbert's basis theorem)**.** *If A is a Noetherian ring, then so is the polynomial ring $A[x]$.*

By induction, every polynomial ring in finitely many variables over A is Noetherian. Hence, the Zariski closed subsets are precisely the subsets of the form $Z(I)$ for some ideal I in the polynomial algebra. One could also ask:

Question 2.3.5. what ideals are of the form $I(Y)$, for some subset $Y \subseteq K^n$? □

and we will answer this question later.

End of lecture 2, Mar 28

2.3.6. *Affine varieties.* One issue with our definition of "Zariski closed subset", is that it is only defined as a subset, rather than a standalone object. In some cases, we would like to consider them independently of the embedding into K^n. So we would like to view them as some kind of a "geometric space", where the geometry is determined by the algebra of functions on it.

k-algebra of functions

Let k be a (commutative) ring, and X a set. By a *k-algebra of functions* on X we mean a k-sub-algebra of the algebra k^X of all functions from X to k (with pointwise operations). Given such an algebra S, every element $x \in X$ determines a k-algebra homomorphism $\phi_x : S \to k$, given by $\phi_x(s) = s(x)$.

affine variety

Definition 2.3.7. An *affine variety* over a field k is a pair $\langle S, X\rangle$, where X is a set, and S is a k-algebra of functions on X. They are required to satisfy the following conditions:

(1) The k-algebra S is finitely generated
(2) The map $x \mapsto \phi_x$ (as above) is a bijection from X to the set $Hom_{k-alg}(S, k)$ of k-algebra homomorphisms from S to k.

Example 2.3.8. For any infinite field k and any natural number n, the pair $\langle k[x_1, \dots, x_n], k^n\rangle$ is an affine variety, where we identify each element p of $S = k[x_1, \dots, x_n]$ with the function it defines on k^n. Indeed, S is visibly finitely generated, and k-algebra maps from S to k are in canonical correspondence with elements of $k^{x_1,\dots,x_n} = k^n$ (via the required map). □

Exercise 2.3.9. Where did we use that k is infinite, and why is it enough? □

We remark that the datum of an affine variety is completely determined by the algebra S, since X is identifies with $Hom_{k-alg}(S, k)$. However, we do not know, at this point, which algebras occur as the algebra of an affine variety. This is related to our previous question 2.3.5[2]:

Proposition 2.3.10. *Let $Z \subseteq K^n$ be a Zariski closed subset. Then the pair $\langle K[x_1, \dots, x_n]/I(Z), Z\rangle$ is an affine variety over K.*

Proof. We first remark that $S = K[x_1, \dots, x_n]/I(Z)$ may indeed be viewed as an algebra of functions on Z: we identify the class of a polynomial p with the function on Z that the restriction of p determines. By definition of $I(Z)$ this does not depend on the choice of p, and if p determines the zero function, it is in $I(Z)$, again by definition of this ideal.

Clearly S is finitely-generated. If $z, w \in Z$ determine the same homomorphism from S to k, then they also determine the same homomorphism from the algebra of polynomials, so $z = w$ by the previous case. It remains to see that an arbitrary homomorphism $\phi : S \to k$ corresponds to a point of Z. We already know it corresponds to a point x of K^n, and by definition, $s(x) = 0$ for all $s \in I(Z)$. Since Z was Zariski closed, this implies that $x \in Z$ by Ex. 2.3.3. □

[2]We assume for convenience that the base field is infinite, but the statements are easily modified for the general case

We would like to assert that every affine variety is of the above form, but this is only true up to isomorphism, so to state this precisely, we need to define what are maps between affine varieties. Intuitively, a map from $\langle S, X\rangle$ to $\langle T, Y\rangle$ should be a function of sets from X to Y that preserves the algebra of functions, i.e.:

Definition 2.3.11. A map from the affine k-variety $\langle S, X\rangle$ to the affine k-variety $\langle T, Y\rangle$ is a function $g : X \to Y$ such that $t \circ g \in S$ for all $t \in T$.

Notice that in this case, the function $t \mapsto t \circ g$ is a k-algebra homomorphism. While the definition is reasonable (and correct) there is a simpler description:

Exercise 2.3.12. In the situation of the definition, show that every k-algebra map from T to S corresponds to a unique map of affine varieties. □

Example 2.3.13. By way of a sanity check, setting $Y = K^0$ a singleton, and $S = k$ in the last exercise, we see that the points of X correspond to maps from Y, as expected. □

It is obvious that the composition of maps of varieties is again such a map, and as usual, an isomorphism of affine varieties is a map that has an inverse with respect to composition.

We may now formulate the converse to 2.3.10:

Proposition 2.3.14. *If $\langle K[x_1, \ldots, x_n]/I, X\rangle$ is an affine variety, then $I = I(Z(I))$, and the variety is isomorphic to $\langle K[x_1, \ldots, x_n]/I, Z(I)\rangle$. Every affine variety is isomorphic to one of this form.*

Proof. Let $Z = Z(I)$, and $J = I(Z)$. We need to show that $J \subseteq I$, so let $p \in J$. We need to show that the image s of p in $S = K[x_1, \ldots, x_n]/I$ is 0, and since X is an affine variety, for that it suffices to show that $\phi(s) = 0$ for all $\phi : S \to k$. But each such ϕ is represented by some $z \in Z$, so $\phi(s) = 0$ since $J = I(Z)$.

The fact that X is isomorphic to Z follows, since they have the same algebra, and for the last part, if $\langle S, X\rangle$ is an affine variety, S is finite generated, so there is a surjective map to S from some polynomial ring, with some kernel I, which is of the form above by the first part. □

We extend the definition of Zariski closed subsets to arbitrary affine varieties: A Zariski closed subset of $\langle S, X\rangle$ is one of the form $Z = Z(I_0) = \{z \in X | s(z) = 0 \forall s \in I_0\}$. Since S is a quotient of a polynomial ring, and a quotient of a Noetherian ring is Noetherian, a finite number of elements of S suffice to define each Zariski closed subset. A map from $\langle S, X\rangle$ to $\langle T, Y\rangle$ where the algebra map $T \to S$ is surjective is called a *closed embedding* of X in Y. It identifies X with the closed subset $Z(I) \subseteq Y$, where I is the kernel of the algebra map. Note that not every embedding is closed: the subset $X = K^*$ of invertible elements in K has the structure of an affine variety, with algebra of functions given by the localisation $K[x, \frac{1}{x}] = K[x, y]/xy - 1$,

closed embedding

and the inclusion of X in K is the map of varieties that corresponds to the inclusion of $K[x]$ in $K[x, \frac{1}{x}]$, so is not closed.

2.3.15. *Dimension.* Can we prove that the circle, given by $x^2+y^2 = 1$ in $\mathbb{R}^2$, is not isomorphic to the sphere $x^2 + y^2 + z^2 = 1$ in $\mathbb{R}^3$? If p is a polynomial isomorphism from S^1 to S^2, it is in particular a diffeomorphism between them, viewed as smooth manifolds. Such a diffeomorphism does not exists, since the two manifolds have different dimensions.

We would like to make a similar argument, but without passing to the smooth category. In other words, we would like to define the dimension algebraically. The analog of smooth manifolds is difficult to define in this setting, and instead we will use a definition that is similar to the one for vector spaces.

Recall that the dimension of a finitely generated vector space V can be defined in two equivalent ways:

- It is the number of elements in each basis of V
- It is the length of the longest chain of subspaces $0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$, where all inclusions are proper.

For algebraic varieties, the situation is similar but more complicated. Starting with the second approach, a direct generalization would be the longest chain of proper Zariski closed subsets.

Example 2.3.16. The subset $\{0, 1, 2\} \subseteq \mathbb{R}$ (given inside $\mathbb{R}$ as the zero set of $x(x-1)(x-2)$) is expected to be 0-dimensional, but the chain $\{0\} \subset \{0, 1\} \subset \{0, 1, 2\}$ has length 3. □

Example 2.3.17. The subset defined by the equations $xz = yz = 0$ is the union of the plane $z = 0$ and the line $x = y = 0$ through it. Hence we expect its dimension to be 2, but the plane is a closed subset whose dimension should be 2 as well. □

The last two example are examples of reducible varieties:

reducible irreducible variety

Definition 2.3.18. An affine variety is *reducible* if it is the union of finitely many proper closed subsets. Otherwise, it is called an *irreducible variety*.

If $\langle S, X\rangle$ is an affine variety, the Noetherian property of S implies that any descending chain of closed subsets of X is finite. In particular, X is a finite union of irreducible subvarieties, called its irreducible components. We expect the dimension of X to be equal to the maximal dimension of a component, and if $\langle S, X\rangle$ is irreducible, we expect each closed subset to be of lower dimension. We arrive at the following definition:

Krull dimension

Definition 2.3.19. The *Krull dimension* of a non-empty affine variety X is the maximal length of a chain $X_0 \subset \cdots \subset X_n$ of irreducible subvarieties X_i of X. The dimension of $\emptyset$ is $-\infty$.

Algebraically, the variety $\langle S, X\rangle$ is irreducible precisely when S is an integral domain. Hence, the dimension is the maximal length of a certain

kind of chains of prime ideals (namely, those that correspond to proper subvarieties).

End of lecture 3, Mar 29

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