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 [6] and in [3]. For general model theory, [5] and [8] 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 $\mathcal{T}$ is a set of sentences, we say that M is a *model of* $\mathcal{T}$ if it is a model of every element of $\mathcal{T}$. We denote by $\mathcal{M}od(\mathcal{T})$ the class of models of $\mathcal{T}$, and say that a class of this form (for some $\mathcal{T}$) is an *elementary class*.

sentence
model of ϕ
model of $\mathcal{T}$
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 $\mathcal{T}$ if $\phi \in \mathcal{T}h(\mathcal{M}od(\mathcal{T}))$. 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 $\mathcal{T}_0$, there is a smallest theory that contains it (namely, $\mathcal{T} = \mathcal{T}h(\mathcal{M}od(\mathcal{T}_0))$, and we normally do not distinguish between $\mathcal{T}$ and $\mathcal{T}_0$ (one says that T_0 *axiomatises* $\mathcal{T}$).

theory of C
logically follows
theory
axiomatises

A theory $\mathcal{T}$ is said to be *consistent* if it has a model, i.e., if $\mathcal{M}od(\mathcal{T})$ 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 $\mathcal{T}$ is consistent, then $\mathcal{T}$ is consistent.*

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

Exercise 2.1.11. If a theory $\mathcal{T}$ implies a sentence ϕ, then a finite subset of $\mathcal{T}$ 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 $\mathcal{T}$ 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 $\mathcal{T}$ has arbitrary large models. Then every finite finite subset of $\mathcal{T}_1 = \mathcal{T} \cup \{\phi_n | n \in \mathbb{N}\}$ is consistent, since it has only finitely many

ϕ_i. By compactness, $\mathcal{T}_1$ is also consistent, and each model of $\mathcal{T}_1$ is an infinite model of $\mathcal{T}$. □

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 $\mathcal{T}$ is a theory in $\mathcal{F}$ and A is an $\mathcal{F}$-structure, we let $\mathcal{T}_A$ be the theory obtained from $\mathcal{T}$ 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 $\mathcal{T}$ 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 $\mathcal{T}$, we denote by $\mathcal{T}_\forall$ the set of universal sentences implied by $\mathcal{T}$. 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 $\mathcal{T}$ is any theory, then $\mathcal{M}od(\mathcal{T}_\forall)$ is the class of substructures of models of $\mathcal{T}$ (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 $\mathcal{T}$. 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 $\mathcal{T}$, and $\phi_1 = \psi(m)$, with $\psi \in R$ and $m \in M$. So $\mathcal{T}$ implies $\neg\psi(m)$ for arbitrary m, but then $\mathcal{T}$ 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 $p_i \in S$

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

Exercise 2.3.20. Show that a finite, non-empty variety is irreducible if and only if it consists of one point. Conclude that a variety is 0-dimensional if and only if it is finite and non-empty. □

Example 2.3.21. For each $i \leq n$, the ideal generated by $x_{i+1}, \ldots, x_n$ in $k[x_1, \ldots, x_n]$ is prime, since the quotient is $k[x_1, \ldots, x_i]$. Hence the dimension of k^n is at least n (geometrically, the corresponding subvarieties are the affine subspaces determined by the coordinate axes) □

To obtain more precise information about the dimension, we need a stronger tie between the algebra and the geometry. We will therefore work on the assumption that the correspondence between closed irreducible subsets and prime ideals is a bijection. We will later see that this assumption holds when the base field is algebraically closed. At the moment, we simply switch to algebra: the assumption is only needed to relate the algebraic results to the geometric notion of dimension. The algebraic counterpart of the definition of dimension is:

Krull dimension

Definition 2.3.22. The *Krull dimension* of a (Noetherian) non-zero ring A is the maximal length of a chain of prime ideals $p_0 \subset \ldots p_n \subset A$.

One way to compute the dimension precisely, we may use the following result (by Emmy Noether):

Theorem 2.3.23 (Noether Normalization)**.** *If A is generated by n elements as an algebra over a field k, then there is a polynomial sub-algebra $B = k[y_1, \ldots, y_m] \subseteq A$ such that A is finite over B, with $m < n$ if the n elements satisfy a relation.*

finite algebra

Recall that A is a *finite algebra* over B if it is finitely generated over B as a module. One significance of this condition (in the geometric case) to dimension is provided by the following:

Theorem 2.3.24. *If $A \subseteq B$ is a finite ring extension, the map restriction map $q \mapsto q \cap A$ from prime ideals in B to prime ideals in A is surjective and strongly inclusion preserving: if $q_1 \subset q_2$ then $q_1 \cap A \subset q_2 \cap A$*

Each point of an affine variety determines a maximal (hence prime) ideal, and if $q \subseteq A$ is of this form, the theorem asserts the fibre over that point is (at most) 0-dimensional. In fact, in the geometric case finite inclusions correspond to surjective, proper maps with finite fibres. In any case, the theorem implies that Krull dimensions of A and B are equal. Together with Noether normalization, it thus reduces the computation of Krull dimension to polynomial rings

Claim 2.3.25. *For every field k, the Krull dimension of $A = k[x_1, \ldots, x_n]$ is n.*

Proof. We already saw one direction. In the other, let $0 = p_0 \subset \cdots \subset p_m \subset A$ be a strict chain of prime ideals. Let $f \in p_1$. By Noether normalization A/f is finite over $k[y_1, \ldots, y_r]$ for $r < n$, so the dimension of A/f is r by induction. But p_i/f are a chain of primes in A/f, so $m \leq r < n$. □

Noether Normalization also provides a second way to determine the dimension of A, when A is a finitely generated integral domain over k. To explain it, we recall some definitions:

Definition 2.3.26. Let A be a k-algebra. A subset $B \subseteq A$ is *algebraically independent* over k if $p(\bar{b}) \neq 0$ for every non-zero polynomial p over k.

algebraically independent

In other words, B is independent over k if the tautological k-algebra map from $k[B]$ to A is injective. When A is a field extension of k, this is equivalent to the statement that the inclusion of B in A extends to a map of fields $k(B) \to A$.

By Zorn's lemma, each algebra A admits a maximal independent subset. If B is such a subset, every element of A is algebraic over the sub-algebra generated by B (so if A is a field, this is an algebraic field extension). It is a basic fact (that we will prove later in greater generality) that when A is a field, all maximal independent subsets have the same cardinality, which is called the *transcendence degree* of A over k. In particular, the transcendence degree is preserved by algebraic extensions.

transcendence degree

Corollary 2.3.27. *Let A be a finitely generated integral domain over a field k. Then the Krull dimension of A is equal to the transcendence degree of the fraction field $K(A)$ over k.*

Proof. Let $B \subseteq A$ be as in Noether normalization. Then $K(A)$ is a finite field extension of $K(B)$, so has the same transcendence degree. On the other hand, we saw that A and B have the same Krull dimension. So the statement reduces to the case of polynomial algebras, where it is obvious. □

2.4. **Differential algebra.** We would like to repeat some of the above ideas with *differential* polynomial equations, instead of polynomials ones. To do that, we introduce a formal notion of derivative:

Definition 2.4.1. 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 $a, b \in A$.

derivation

A *differential ring* is a pair $\langle A, \partial \rangle$ with A and ∂ as above. A map of differential rings is a map of rings that commutes with the derivation. A is a domain, a field, etc., if it so as a ring.

differential ring

If $p(x)$ is a polynomial over a commutative ring A, we considered the solutions to the equation $p(x) = 0$ in A (or extension of it). The analogous notion in the differential case is provided by differential polynomials:

Definition 2.4.2. Let A be a ring, and I a set of variables. A *differential polynomial* in I over A is a polynomial over A in the variables $x^{(i)}$, where

differential polynomial

$x \in I$ and i a natural number.

We identify $x^{(0)}$ with x, and sometimes write x', x'', etc. in place of $x^{(1)}$, $x^{(2)}$, etc. Note that the definition does not require a derivation on A. As usual, the collection $A\{I\}$ of differential polynomials is an A-algebra, and the differential structure is provided by the fact that each derivation on A extends canonically to $A\{I\}$:

Exercise 2.4.3. Let $A = \langle A, \partial \rangle$ be a differential ring and I a set. There is a unique derivation ∂ on $A\{I\}$ determined by the requirements that $\partial(x^{(i)}) = x^{(i+1)}$ for all $x \in I$ and $i \in \mathbb{N}$, and the map $A \to A\{I\}$ is a map of differential rings. It classifies functions from I to differential ring extensions of A: the restriction $Hom_{\langle A,\partial \rangle}(A\{I\}, B) \to B^I$ is a bijection for every differential ring B over A (in other words, it is the free differential A-algebra on I) $\square$

As in the algebraic situation, we will mostly be interested in sets of solutions in fields:

Definition 2.4.4. Let $\langle K, \partial \rangle$ be a differential field. A *Kolchin closed subset* of K^n is the set of solutions of a finite system of equations $p_1 = \ldots = p_m = 0$, where each $p_i \in K\{x_1, \ldots, x_n\}$. **Kolchin closed subset**

End of lecture 4, Apr 4

As with usual polynomials, we would like to remove some of the ambiguity by passing to ideals. Since the derivative of 0 is 0, we require it to be closed under the derivative:

Definition 2.4.5. A *differential ideal* in a differential ring $\langle A, \partial \rangle$ is an ideal $I \subseteq A$ such that $\partial(x) \in I$ for all $x \in I$. **differential ideal**

If $I \subseteq A$ is a differential ideal, A/I is a differential ring, uniquely determined by the property that the quotient map is a map of differential rings.

As in the algebraic case, differential polynomial equations for a language of a universal theory:

Definition 2.4.6. Let $\langle A, \partial \rangle$ be a differential ring. The language of differential fields over A consists of differential polynomial equations over A as basic (quantifier free) relations. The theory DF_A consists of the axioms for differential fields of characteristic 0 over A[3]

Where does one obtain examples of differential rings? We will soon see some constructions, but the natural source is geometry:

Example 2.4.7. The ring of smooth functions on the open interval $(0, 1)$ is a differential ring with the usual derivative (and similarly for other intervals). This example is far from being a field, it is not even a domain. $\square$

[3]Strictly speaking, setting the characteristic is not necessary, but the theory behaves very differently in positive characteristic

Example 2.4.8. To obtain a differential integral domain, replace the real interval by a complex analytic domain X (open connected subset of $\mathbb{C}$), and consider holomorphic functions on X. The fraction field is the field of meromorphic functions on X. □

Both examples can be generalised by considering a smooth (or analytic) manifold X along with a vector field on it. We will return to this later. An easy special case:

Example 2.4.9. The field $\mathbb{C}(t)$ of rational functions, with the derivative determined by sending t to 1.

In fact, it is easy to see that for every $f \in \mathbb{C}(t)$, there is a unique derivation ∂ on $\mathbb{C}(t)$ determined by the property that $\partial(t) = f$. For example, we could set $t' = t$. Analytically, this would mean that t actually represents an exponential function $t = e^s$: algebraically, there is no difference between the coordinate t and the exponential function e^s, both are algebraically transcendental over $\mathbb{C}$. But differentially, they satisfy distinct equations. □

Example 2.4.10. Each ring can be viewed as a differential ring with the 0 derivation. This means, informally, that objects of algebraic geometry can be viewed as objects of the differential world. □

Exercise 2.4.11. Let A be a commutative ring, and let $A[\epsilon] = A[x]/x^2$ (we denote by ϵ the image of x), with $\pi : A[\epsilon] \to A$ the A-algebra map that sends ϵ to 0.

(1) If $\partial : A \to A$ is a derivation, the function $t_\partial : A \to A[\epsilon]$ given by $t(a) = a + \partial(a)\epsilon$ is a map of rings. Conversely, any map of rings $t : A \to A[\epsilon]$ such $\pi \circ t$ is the identity is of the form $t = t_\partial$ for a unique ∂ (we will later discuss the geometric meaning of this)
(2) If A is a differential domain, there is a unique derivation on $K(A)$ that extends the one on A (if you know what is an étale map, show that any derivation extends uniquely along them as well)
(3) The subset $C_A = \{c \in A | \partial(c) = 0\}$ is sub-ring of A, which is a subfield if A is a field. It is called the *subring of constants* of A

subring of constants

□

Suppose that $L \subseteq K$ is an extension of differential fields, and $a \in K$. What can be said of a from the point of view of L? The element a corresponds to an L-algebra map $L\{x\} \to K$, sending x to a, and its kernel is a prime differential ideal, the ideal of differential polynomials satisfied by a. Hence, we would like to understand prime differential ideals in $L\{x\}$.

Let us first recall the analogous situation in the algebraic setting. The polynomial algebra $k[x]$ in one variable is a *principal ideal domain*: Every (prime) ideal is generated by one element. The element generating an ideal I can be found as an element of minimal degree in I. In particular, it is a unique factorisation domain: every irreducible element is prime (recall that an element a is reducible if it is a product of two non-invertible elements,

and prime if the ideal it generates is prime; it follows immediately that a prime element is irreducible, but in general the converse is false).

In the differential setting, the definition of "irreducible" remains the same, but the ideal in the definition of a being prime is replaced by the *differential* ideal $\langle a \rangle$ generated by a. With these definitions, the analogous facts to the above are false for $k\{x\}$: the polynomial $p(x) = (x'')^2 - 2x'$ is irreducible, but its derivative (which is in $\langle p \rangle$) is $2x''x''' - 2x'' = 2x''(x''' - 1)$, and neither of the factors is in $\langle p \rangle$, so the ideal is not prime.

We can still achieve a description that somewhat resembles the algebraic one. To each irreducible differential polynomial p, we will assign a prime ideal $I(p)$ containing it. We will also define a well-founded pre-order $\ll$, and will show that each prime differential ideal I is of the form $I(p)$ for $p \in I$ minimal with respect to $\ll$. We start with the definition of $\ll$:

Definition 2.4.12. The *order* $\mathrm{ord}(p)$ of non-zero differential polynomial p is the highest i such that $x^{(i)}$ appears in p. **order**

For any $p, q \in K\{x\}$, we say p is simpler than q, writing $p \ll q$, if $\mathrm{ord}(p) < \mathrm{ord}(q)$, or $\mathrm{ord}(p) = \mathrm{ord}(q) = n$, and $\deg_{x^{(n)}}(p) \leq \deg_{x^{(n)}}(q)$.

To proceed, we make the following computation, that will be used (and reinterpreted) also later: suppose that $p = p(t) = \sum_{i=0}^{m} a_i t^i$ is a (regular) polynomial over a differential ring $\langle A, \partial \rangle$, and $b \in A$. Then

$$\partial(p(b)) = \partial(\sum_{i=0}^{m} a_i b^i) = \sum_{i=0}^{m} \partial(a_i) b^i + (\sum_{i=1}^{m} i a_i b^{i-1}) \partial(b) = p^{\partial}(b) + \frac{\partial p}{\partial t}(b) \cdot \partial(b) \quad (2.1)$$

where p^{∂} is the polynomial obtained from p by applying ∂ to the coefficients. Assuming now that $p(x)$ is a differential polynomial of order n, we view it as a regular polynomial $p = p_0(x^{(n)})$ with p_0 over $k\{x\}$ (with coefficients of order at most $n-1$), and applying the above calculation we obtain

$$\partial(p) = {p_0}^{\partial}(x^{(n)}) + \frac{\partial p}{\partial x^{(n)}} \cdot x^{(n+1)} \quad (2.2)$$

the expression $\frac{\partial p}{\partial x^{(n)}}$ is called the *separant* of p, denoted s_p. In the example above, $\partial(p)$ was reducible because $s_p = 2x''$ divides the first summand (which was also $2x''$). Note that s_p is strictly simpler than p, so assuming p is minimal within a given prime ideal I, we expect the other factor to lie in I. Hence we define **separant**

$$I(p) = \{q \in k\{x\} | \exists m \in \mathbb{N}\ s_p^m q \in \langle p \rangle\} \quad (2.3)$$

This is often called the *saturation* of $\langle p \rangle$ with respect to s_p. It turns out that s_p accounts for all the non-primeness of $\langle p \rangle$:

Proposition 2.4.13. *For each irreducible $p \in k\{x\}$, $I(p)$ is a prime differential ideal containing p. Conversely, if I is a prime differential ideal in $k\{x\}$, then $I = I(p)$ for $p \in I$ minimal with respect to $\ll$.*

End of lecture 5, Apr 5

2.4.14. To prove Proposition 2.4.13, we mimic the algebraic case, with suitable modifications. We set $A = k\{x\}$, and let $A_i \subseteq A$ be the sub-ring of polynomials of order less than i (so $A_0 = k$). We fix $p \in A$ of order n (not necessarily irreducible), so $p(x) = a(x)x^{(n)^d} + p_1(x)$, where $a = a(x)$ is of order lower than p, and p_1 is simpler than p. We denote by s the separant of p.

Let $B_i = A_{i+1}/A_i$. This is a module over A_i (and therefore over A_j, for $j < i$), and since $\partial(A_i) \subseteq A_{i+1}$, we have an induced map $\partial_i : B_i \to B_{i+1}$, which is A_i-linear. The polynomial p has a non-zero image $\bar{p}$ in B_n, and applying the above observations along with formula (2.2), we see that for each $m > 0$, $\partial^m(p) = sx^{(n+m)}$ up to lower order terms. Similar arguments allow us to work up to simpler terms.

We now have the following two variants of division with remainder:

Lemma 2.4.15. *With notation as in 2.4.14, for any $q \in A$ we have*

(1) *$l, m \in \mathbb{N}$ and $r \in A$ with $r \ll p$ and $a^l s^m q - r \in \langle p \rangle$*
(2) *$m \in \mathbb{N}$ and $r \in A$ with $\mathrm{ord}(r) \leq n$ and $s^m q - r \in \langle p \rangle$*

Proof. Let j be the order of q. If $j = n$, we may take $r = q$ and $m = 0$ for the second version. For the first, we may divide by a and use regular polynomial division (for polynomials in the variable $x^{(n)}$) to find r of lower degree so that $a^l q - r$ is divisible by p (in this case, $m = 0$).

If $j > n$, we remarked above that up to simpler terms, $\partial^{j-n}(p) = sx^{(j)}$. Writing up to simpler terms $q = bx^{(j)^e}$ for some b of order lower than j and $e \in \mathbb{N}$, we see that $q_1 = b(\partial^{j-n}p)^e - s^e q$ is simpler than q, so by induction, there are l_1, m_1, r_1 as in the statement (with $l_1 = 0$ for the second version), so that $a^{l_1} s^{m_1} q_1 - r_1 \in \langle p \rangle$. Since $b(\partial^{j-n}p)^e \in \langle p \rangle$, we are done. □

We next note that for q has order n, q could only be in $I(p)$ for the obvious reason:

Lemma 2.4.16. *Notation as in 2.4.14. If $q \in I(p)$ is of order n, then $s^m q \in (p)$ for some m. If p is irreducible, we may take $m = 0$.*

Proof. By assumption, $s^m q \in \langle p \rangle$ for some m, so $s^m q \in (p, \ldots, \partial^k(p))$ for some k, which we may take minimal. Assume $k > 0$. Localising at s, we have $q \in (p, p_1, \ldots, p_k)$, where $p_i = x^{(n+i)} + r_i$ with r_i of lower order. This is true in particular for $i = k$, and since $x^{(n+k)}$ does not appear in q, we may plug $x^{(n+k)} = -r_k$ (note that the differential structure no longer plays a role), so $q \in (p, \ldots, p_{k-1})$. This contradicts the minimality of k and proves the first statement.

For the second, note that (p) is prime (the polynomial ring is a UFD), and $s \notin (p)$ since the degree is too low. Since $s^m q \in (p)$ we must have $q \in (p)$. □

proof of 2.4.13. It is obvious that for all p, $I(p)$ is an ideal. To show that it is a differential ideal, let $g \in I(p)$, so that $s^m g \in \langle p \rangle$ for some m. Then $s^{m+1} g' = (s^{m+1} g)' - (m+1) s^m g$, and both terms on the right are in $\langle p \rangle$, so $g' \in I(p)$.

To show that $I(p)$ is prime when p is irreducible, assume $fg \in I(p)$, so that $s^m fg \in \langle p \rangle$ for some m. Applying long division 2.4.15 in the second version (possibly modifying m), we may assume that f, g have order at most n. But then p divides $s^m fg$ by Lemma 2.4.16. Since it is irreducible, it must divide one of the factors f, g (it cannot divide s, since it is simpler). Hence f or g are in $I(p)$.

Conversely, assume that I is a prime (differential) ideal, and let p be simplest non-zero in I (p need not be unique). Note that p is irreducible, since a factor would be in I and simpler. If $g \in I(p)$, then $s^m g \in \langle p \rangle \subseteq I$ for some m. Since I is prime, s^m or g is in I. It cannot be s^m since it is simpler than p. This shows that $I(p) \subseteq I$.

Assume that $q \in I$. Applying long division, we find $a^l s^m q - r \in \langle p \rangle \subseteq I$ for some l, m and some r simpler than p, so that $r \in I$ as well. Since p was assumed to be simplest non-zero in I, we have $r = 0$. Hence $a^l s^m q \in \langle p \rangle$, so $a^l q \in I(p)$. We already saw that $I(p)$ is prime, so $a^l \in I(p)$ or $q \in I(p)$. The former is impossible by simplicity. □

The direct analogue of Hilbert's basis theorem fails: there is no ascending chain condition on differential ideals in $k\{x\}$. For example, the sequence $I_0 = 0$ and $I_{k+1} = \langle I_k \cup \{(x^{(k)})^2\} \rangle$ is a strictly increasing chain (this is not trivial). However, we are interested in the geometry of the sets determined by these ideals, and we have, for example, $Z(I_1) = Z(x)$. Recall that the *radical* of an ideal I is the ideal $\sqrt{I} = \{b | \exists k \in \mathbb{N}\ b^k \in I\}$. It is clear that $Z(I) = Z(\sqrt{I})$. Furthermore,

radical

Exercise 2.4.17. If I is a differential ideal (in any differential ring), then $\sqrt{I}$ is also a differential ideal. □

An ideal I is called a *radical ideal* if $I = \sqrt{I}$ (this is an algebraic notion). A differential ideal I is *well-mixed* if $ab \in I$ implies $ab' \in I$. Of course, if I is prime then it is well-mixed, but also

radical ideal

well-mixed

Exercise 2.4.18. Any radical differential ideal is well-mixed □

It turns out that the analogue of the Hilbert basis theorem is true for *radical* differential ideals. Let us say that a differential ring A is *differentially Noetherian* if every strictly ascending chain of radical differential ideals stabilizes.

differentially Noetherian

Theorem 2.4.19 (Ritt–Raudenbush basis theorem)**.** *If A is a differentially Noetherian differential ring (in characteristic 0), then so is $A\{x\}$.*

We skip the proof, see [6] or [4]. We recall again that geometrically, this means that every strictly descending chain of Kolchin closed subsets stabilises, and that every Kolchin closed subset can be given by a *finite* number of equations.

End of lecture 6, Apr 11

3. The theory of differentially closed fields

3.1. **Quantifier Elimination.** We saw above that we have some understanding of *quantifier free* definable subsets in fields, and even in differential fields. However, model theoretic notions are normally described via the collection of *all* definable sets, including quantifiers. These could be vastly more complicated:

Example 3.1.1. Consider the field $\mathbb{Q}$ of rational numbers. Julia Robinson showed (in her thesis, see [7] for example) that the subset of integers is definable: there is a formula $\phi(x)$ such that $\phi(q)$ holds for a rational q if and only if q is an integer (of course, ϕ must have quantifiers, but it turns out that just a few quantifiers suffice). Once this is known, the definable sets are essentially the same as the ones definable in $\mathbb{Z}$, the structure studied by Gödel in his incompleteness theorem. The proof of this theorem shows that this structure is extremely rich and "unmanageable". In particular, there is a definable bijection between any two Cartesian powers, so no reasonable theory of dimension for definable sets can exist. □

constructible

The situation is rather different with the field $\mathbb{C}$ of complex numbers. We will call a subset of $\mathbb{C}^n$ *constructible* if it can be defined by a quantifier-free formula (in the language of fields). In other words, it is a finite boolean combination of Zariski closed subsets. We will prove below:

Proposition 3.1.2. *Every definable subset of $\mathbb{C}^n$ is constructible*

A similar kind of statement is usually required to have any hope of understanding model-theoretically a structure, so there is some machinery in place to prove them. First, we note that this statement is really about the *theory* $\mathcal{T}$ of $\mathbb{C}$: for every formula $\phi(x)$ there is a quantifier free formula ψ with $\forall x(\phi \leftrightarrow \psi) \in \mathcal{T}$. This has a name:

quantifier elimination

Definition 3.1.3. A theory $\mathcal{T}$ admit *quantifier elimination* if for every formula $\phi(x)$ there is a quantifier free formula ψ with $\forall x(\phi \leftrightarrow \psi) \in \mathcal{T}$.

One tool to prove quantifier elimination is the following:

Proposition 3.1.4. *Let $\mathcal{T}$ be a theory, and let $\phi(x)$ be formula. Then ϕ is equivalent (with respect to $\mathcal{T}$) to a quantifier-free formula if and only if for all models M of $\mathcal{T}$ and any $a \in \phi(M)$, $\mathcal{T}_a$ implies $\phi(a)$*

Proof. We may assume ϕ is consistent with $\mathcal{T}$. If ϕ is equivalent to a quantifier-free formula, we may assume it itself is already quantifier-free, and then $\phi(a) \in \mathcal{T}_a$.

Conversely, let Γ be the set of quantifier-free formulas implied by ϕ. We claim that Γ implies ϕ (with respect to $\mathcal{T}$). If not, let N be a model with an element $a \in N$ such that $a \in \neg\phi(N)$ but $a \in \psi(M)$ hold for all $\psi \in \Gamma$.

We claim that $\mathcal{T}_a$ is consistent with $\phi(a)$: otherwise, $\Gamma \cup \{\phi\}$ is inconsistent with $\mathcal{T}$, so by compactness, ϕ is inconsistent with some $\psi \in \Gamma$. But then ϕ implies both ψ and $\neg\psi$, contradicting its consistency.

Since $\mathcal{T}_a$ is consistent with $\phi(a)$, there is a model M of $\mathcal{T}_a$ for which $a \in \phi(M)$. By assumption, this means that $\mathcal{T}_a$ implies $\phi(a)$, contradicting the existence of N.

We proved that Γ implies ϕ. Again by compactness, some $\psi \in \Gamma$ implies it. Since by definition $\phi \to \psi$, we are done. □

The above result provides a way of checking that a particular formula is quantifier-free, but for an arbitrary formula it might still be difficult to check this condition. If we wish to prove that *all* formulas are equivalent to quantifier-free ones, we have the following observation:

Exercise 3.1.5. If $\mathcal{T}$ is a theory, and for each quantifier-free formula $\phi(x, y)$, where y is one variable, the formula $\exists y(\phi(x, y))$ is equivalent to a quantifier-free one, then $\mathcal{T}$ admits quantifier-elimination. □

We may now prove the statement we started with, in slightly greater generality:

Proposition 3.1.6. *Let K be an algebraically closed field, and let $\mathcal{T}$ be its theory (in the language of fields). Then $\mathcal{T}$ admit quantifier-elimination.*

Proof. By the last exercise, it suffice to show that each formula of the form $\exists y\phi(x, y)$, where ϕ is quantifier-free, is equivalent to a quantifier-free one. By the criterion 3.1.4, we need to show that if L is a model of $\mathcal{T}$ and a is a tuple in L for which $\phi(a, y)$ has a solution in L, then $\phi(a, y)$ also has a solution in any other field E satisfying $\mathcal{T}$ and containing a.

Note that $\phi(a, y)$ is boolean combination of polynomial equations in y (a single variable), with coefficients in the subfield L_0 generated by a. In fact, we may assume that $\phi(a, y)$ has the form $p_1 = 0 \wedge \cdots \wedge p_k = 0 \wedge q \neq 0$ for some polynomials p_i and q. Since $L_0[x]$ is a pid, this system is implied by one equation $p = 0$ with p a non-unit polynomial over L_0, $p_a(x) = x^n + \sum a_i x^i$. Since K is algebraically closed, $\mathcal{T}$ includes the sentence $\forall y \exists x(p_y(x) = 0)$, so it is true in E. Speciallising to $y = a$, we see that p_a has a solution in E. □

Tracing through the proof, we see explicitly that we proved the follow stronger fact:

Corollary 3.1.7. *There is a first order theory ACF in the language of fields, whose models are precisely the algebraically closed fields. This theory admits quantifier-elimination.*

Since $\mathbb{C}$ is an algebraically closed field, we have $ACF \subseteq \mathcal{T}h(\mathbb{C})$. Is there anything else we can say in a first order manner about $\mathbb{C}$? The following result is often obtained via the Löwenheim–Skolem theorems, using the

uniqueness of models in a fixed uncountable cardinality. For each ideal I in $\mathbb{Z}$, write $ACF_I = ACF \cup \{\underline{n} = 0 | n \in I\} \cup \underline{m} \neq 0 m \notin I$, where $\underline{n} = 1 + \cdots + 1$ ($|n|$ times). We write ACF_p in place of $ACF_{(p)}$.

Corollary 3.1.8. *The theories ACF_p are complete when p is prime. In particular, $ACF_0 = \mathcal{Th}(\mathbb{C})$.*

Proof. Let ψ be a sentence. According the quantifier-elimination in ACF, it is equivalent there to a quantifier-free one, so we may assume it is quantifier-free. Every such sentence is a statement about the field structure of the prime field, which is uniquely determined by p. □

We next would like to finish describing the relation between algebra and geometry for affine varieties. To do that, we use the following definition, which will also be important later:

existentially closed

Definition 3.1.9. Let M be a model of a theory $\mathcal{T}$. We say that M is *existentially closed* if any quantifier-free formula $\phi(x)$ in $\mathcal{T}_M$ that is consistent with $\mathcal{T}_M$ has a point $m \in \phi(M)$.

Exercise 3.1.10. In the definition, it doesn't matter if x is a variable or a tuple of variables. □

Exercise 3.1.11. If $\mathcal{T}$ admit quantifier-elimination, then every model of $\mathcal{T}$ is existentially closed. □

For example, $\mathbb{C}$ is existentially closed (with respect to the theory of algebraically closed fields, or of fields). In the case of one variable, it says that if a polynomial has a root in some field extension, then it has a root in $\mathbb{C}$. In the case of several variables, it can be thought of as a form of Hilbert's Nullstellensatz:

Corollary 3.1.12. *Let K be an algebraically closed field, I a prime ideal in $A = K[x_1, \ldots, x_n]$ and $g \in A \setminus I$. Then $Z(I) \setminus Z(g) \subseteq K^n$ is non-empty.*

Proof. Let L be the fraction field field of the domain A/I. The canonical map $p : A \to L$ determines a point of $Z(I)$ as in Proposition 2.3.10, and since the kernel of p is precisely I, this point is not in $Z(g)$.

Let $p_1, \ldots, p_k$ be generators for I. We just showed that $p_1 = 0 \wedge \cdots \wedge p_k = 0 \wedge g \neq 0$ is satisfied in an extension of K. Since K is existentially closed, it is satisfied in K. □

A standard way to state the Nullstellensatz is as follows:

Corollary 3.1.13 (Hilbert's Nullstellensatz)**.** *If K is algebraically closed, and I, J are two distinct radical ideals in $K[x_1, \ldots, x_n]$, then $Z(I) \neq Z(J)$. For any ideal I, $I(Z(I)) = \sqrt{I}$. Any finitely generated reduced K algebra is affine (i.e., the ring of functions on an affine variety).*

We outline the argument: We may assume there is $g \in J \setminus I$. Any radical ideal is the intersection of the prime ideals that contain it (this is essentially

the algebraic counterpart of irreducible components), so there is a prime ideal I_1 containing I and not g. We have $Z(I_1) \subseteq Z(I)$ and $Z(J) \subseteq Z(g)$, so to show that $Z(I)$ is different from $Z(J)$, it suffices to find a point in $Z(I_1)$ which is not in $Z(g)$. This is provided by 3.1.12. The second statement follows since both sides are radical ideals that define the same Zariski closed subset, and the last statement is the translation via Proposition 2.3.10. End of lecture 7, Apr 12

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] I. Kaplansky. *An Introduction to Differential Algebra*. 2nd ed. Paris: Hermann, 1976 (cit. on p. 20).

[5] 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).

[6] 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: 1-56881-282-5 (cit. on pp. 3, 20).

[7] J. Robinson and S. Feferman. *The Collected Works of Julia Robinson*. Collected works series. American Mathematical Society, 1996. ISBN: 9780821805756. URL: https://books.google.co.il/books?id=%5C_33D84OENIAC (cit. on p. 20).

[8] 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:kamensky.bgu@gmail.com
URL: https://www.math.bgu.ac.il/~kamenskm