Algebraic Varieties

Notes by Mateusz Michałek
for the lecture on April 17, 2018, in the
IMPRS Ringvorlesung *Introduction to Nonlinear Algebra*

Algebraic varieties represent solutions of a system of polynomial equations. Given a set of k polynomials $f_1, \ldots, f_k \in K[\mathbf{x}]$, their *(algebraic) variety* is the set of common zeros:

$$\mathcal{V}(f_1, \ldots, f_k) \; := \; \{\, \mathbf{p} = (p_1, \ldots, p_n) \in K^n : f_1(\mathbf{p}) = \cdots = f_k(\mathbf{p}) = 0 \,\}.$$

Different sets of polynomials can define the same variety. For instance, $\mathcal{V}(f_1, f_2) = \mathcal{V}(f_1, f_1 + f_2)$. Thus, instead of thinking about explicit polynomials it is more reasonable to consider the ideal they generate, $I = \langle f_1, \ldots, f_k \rangle$, and to define $\mathcal{V}(I) := \mathcal{V}(f_1, \ldots, f_k)$.

Subsets of K^n of the form $\mathcal{V}(I)$ for some ideal $I \subset K[\mathbf{x}]$ are called *varieties*. Given any ideal $I \subset K[\mathbf{x}]$, by *Hilbert Basis Theorem*, we may always find a *finite* set of generators. By Exercise 1, the definition of $\mathcal{V}(I)$ does not depend on the choice of generators of the ideal I.

Remark 1. *Two distinct ideals may define the same variety, e.g.* $\mathcal{V}(u) = \mathcal{V}(u^2) = \{0\} \subset K^1$. *Our later lecture on the Nullstellensätze deals with this issue for fields K that are either algebraically closed, like the complex numbers $K = \mathbb{C}$, or real closed, like the reals $K = \mathbb{R}$.*

Algebraic geometry is the study of the geometry of varieties. As in many branches of mathematics, given a fundamental object - varieties in our case - one considers the basic, irreducible building blocks. A variety $\mathcal{V}(I)$ is called *irreducible* if it cannot be written as a union of proper subvarieties. In symbols, $\mathcal{V}(I)$ is irreducible if and only if

$$\mathcal{V}(I) = \mathcal{V}(J) \cup \mathcal{V}(J') \implies \mathcal{V}(I) = \mathcal{V}(J) \text{ or } \mathcal{V}(I) = \mathcal{V}(J') \qquad \text{for any ideals } J \text{ and } J'.$$

We can turn K^n into a topological space, using the *Zariski topology*, in which varieties are closed sets. In this setting, the definition of an irreducible variety coincides with the definition of an irreducible topological space.

Our aim is to study relations between the geometry of $\mathcal{V}(I)$ and algebraic properties of I. Consider a maximal ideal $m := \langle x_1 - p_1, \ldots, x_n - p_n \rangle \subset K[\mathbf{x}]$. Note that $(p_1, \ldots, p_n) \in \mathcal{V}(I)$ if and only if $I \subset m$. Given any subset $V \subset K^n$, we can consider the set of all polynomials that vanish on V. This set is an ideal, denoted as

$$\mathcal{I}(V) \; := \; \{\, f \in K[\mathbf{x}] \; : \; f(\mathbf{p}) = 0 \text{ for all } \mathbf{p} \in V \,\}.$$

Note that W is a variety if and only if $W = \mathcal{V}(\mathcal{I}(W))$. Furthermore, for varieties V, W, we have $V \subseteq W$ if and only if $\mathcal{I}(W) \subseteq \mathcal{I}(V)$.

Proposition 2. *A variety $W \subset K^n$ is irreducible if and only if its ideal $\mathcal{I}(W)$ is prime.*

Proof. Suppose $\mathcal{I}(W)$ is prime and $W = \mathcal{V}(J) \cup \mathcal{V}(J')$. If $W \neq \mathcal{V}(J)$ then there exists $f \in J$ and $v \in W$ such that $f(v) \neq 0$, i.e. $f \notin \mathcal{I}(W)$. For any $g \in J'$ we know that fg vanishes on $\mathcal{V}(J)$ and $\mathcal{V}(J')$, hence on W. Thus $fg \in \mathcal{I}(W)$. As $\mathcal{I}(W)$ is prime, we have $g \in \mathcal{I}(W)$, i.e. $J' \subset \mathcal{I}(W)$. By Exercise 2 this implies $W = \mathcal{V}(\mathcal{I}(W)) \subset \mathcal{V}(J')$.

Suppose now that W is irreducible and $fg \in \mathcal{I}(W)$. Hence

$$W = W \cap \mathcal{V}(fg) = W \cap (\mathcal{V}(f) \cup \mathcal{V}(g)) = (W \cap \mathcal{V}(f)) \cup (W \cap \mathcal{V}(g)).$$

Without loss of generality we may assume $W = W \cap \mathcal{V}(f)$, i.e. $W \subseteq \mathcal{V}(f)$, hence $f \in \mathcal{I}(W)$, which proves that $\mathcal{I}(W)$ is a prime ideal. □

Many examples of varieties appearing from applications are given as (closures) of images of polynomial maps. Often we think about the domain K^n as the space of *parameters* and the codomain as the space of possible (observable) outcomes – cf. Exercise 9. We note that the (Zariski) closure of the image must be irreducible.

Example 3. *Consider two independent discrete random variables X and Y each one with n states. The probability distribution of X (resp. Y) may be encoded as a point $(p_1, \ldots, p_n) \in K^n$ (resp. $(q_1, \ldots, q_n)$). The joint distribution of (X, Y) has n^2 states. The map that associates to a distribution of X and a distribution of Y the joint distribution is given as:*

$$K^n \times K^n \ni (p_1, \ldots, p_n, q_1, \ldots, q_n) \to (p_1q_1, p_1q_2, \ldots, p_1q_n, p_2q_1, \ldots, p_nq_n) \in K^{n^2}. \tag{1}$$

Further, as $\sum p_i = \sum q_i = 1$, we may in fact restrict the domain and obtain a map that we write explicitly for $n = 3$:

$$(p_1, p_2, q_1, q_2) \to \tag{2}$$
$$(p_1q_1, p_1q_2, p_1(1-q_1-q_2), p_2q_1, p_2q_2, p_2(1-q_1-q_2), (1-p_1-p_2)q_1, (1-p_1-p_2)q_2, (1-p_1-p_2)(1-q_1-q_2))$$

In Exercise 9 we ask for the description of the ideal of the closure of the image of these maps.

Prime ideals play a central role in algebraic geometry. This motivates the following definition. We now take R to be any commutative ring with unity. The primary example is the polynomial ring $R = K[\mathbf{x}]$, or its quotient $R = K[\mathbf{x}]/I$ for some ideal I.

Definition 4. The *spectrum* of the ring R is the set of all (proper) prime ideals:

$$\operatorname{Spec}(R) := \left\{ p \subsetneq R \,:\, p \text{ is a prime ideal} \right\}.$$

The set $\operatorname{Spec}(R)$ comes with an induced Zariski topology, where the closed set $\mathcal{V}(I)$ given by an (arbitrary) ideal I is defined as

$$\mathcal{V}(I) = \{p \in \operatorname{Spec} R : I \subset p\}.$$

We note that the spectrum of the ring remembers a lot of information: all prime ideals. In particular, $\operatorname{Spec} K[\mathbf{x}]$ has points corresponding to *all* irreducible subvarieties of K^n - not only to usual points $(p_1,\dots,p_n)\in K^n$, which correspond to maximal ideals of the form $\langle x_1-p_1,\dots,x_n-p_n\rangle$. One could say that K^n is a subset of $\operatorname{Spec} K[\mathbf{x}]$. In Exercise 4 you will prove that in fact the Zariski topology on K^n is the induced one from the Zariski topology on $\operatorname{Spec} K[\mathbf{x}]$.

Proposition 5. *Any variety can be uniquely represented as a finite union of irreducible varieties (pairwise not contained in each other).*

Proof. We start by proving the existence of such a decomposition. Any variety W is either irreducible or may be represented as a union $W_1\cup V_1$. We may continue presenting W_1 as a union $W_2\cup V_2$ etc. We obtain an ascending chain $\mathcal{I}(W_1)\subsetneq\mathcal{I}(W_2)\subsetneq\dots$ which stabilizes as the ring is noetherian by Hilbert Basis Theorem. Thus the decomposition procedure must finish.

Suppose we have two decompositions $V_1\cup\dots\cup V_k=W_1\cup\dots\cup W_s$. As each W_{i_0} is irreducible and covered by $\bigcup_j(V_j\cap W_{i_0})$ we have $W_{i_0}\subset V_{j_0}$. But similarly $V_{j_0}\subset W_{i_1}$ for some i_1. As we cannot have $W_{i_0}\subsetneq W_{i_1}$ it follows that $W_{i_0}=V_{j_0}$. Hence, for every component W_{i_0} there exists a (unique) component V_{j_0} equal to it. □

We recall that the ring $K[\mathbf{x}]$ represents the (polynomial) functions on K^n. We now would like to represent (polynomial) functions on a variety $W\subset K^n$. They will form a ring $K[W]$. Clearly, as we are interested in polynomial functions, we have a surjection $K[\mathbf{x}]\twoheadrightarrow K[W]$. Two functions coincide on W if and only if their difference vanishes on W. Thus the kernel of the above map equals $\mathcal{I}(W)$ and we have an isomorphism $K[W]:=K[\mathbf{x}]/\mathcal{I}(W)$, that we may consider as a definition of the ring of functions on W. The advantage of this approach is that we may consider the ring $K[W]$ as an object representing W, without referring to any embedding. As before, we identify points $\mathbf{p}=(p_1,\dots,p_n)$ in W with maximal ideals $\langle x_1-p_1,\dots,x_n-p_n\rangle\subset K[W]$. The Zariski topologies on W and $\operatorname{Spec}(K[W])$ are compatible.

We have defined our basic objects - affine varieties W and associated rings $K[W]$. Following a category theory approach, our aim is to define morphisms of varieties.

Given two geometric objects X,Y and a map $f:X\to Y$ between them, one may pull-back functions on Y. Explicitly, given $g:Y\to K$ we define the pull-back $f^*(g)=g\circ f$. As we are dealing with algebraic varieties, we would like the pull-backs of polynomials to be polynomials. Hence, given an algebraic map $f:W_1\to W_2$ between varieties, we would like the induced map $f^*:K[W_2]\to K[W_1]$ to be a well-defined ring morphism. In Exercise 5 you will show that any ring morphism $K[W_2]\to K[W_1]$ induces a map $\operatorname{Spec} K[W_1]\to\operatorname{Spec} K[W_2]$. Hence, we may think about algebraic maps between varieties as morphisms among their rings of functions in the opposite direction. Using slightly more sophisticated language there is a contravariant functor, inducing an equivalence of categories of affine irreducible varieties (over K) and finitely generated integral K-algebras. We note that (algebraic) maps between varieties are continuous in Zariski topology.

Remark 6. *One may define affine algebraic varieties more generally as* $\operatorname{Spec} R$ *for any (commutative, with unity) ring R, not only finitely generated K-algebra. However, in these lectures all affine varieties will come from zero sets of polynomials defined over K.*

In next examples we note that the dependence on the field is crucial for many properties of ideals. We start with the map $f : K[x] \to K[y]$, given by $f(x) = y^2$. This corresponds to the map $K^1 \ni \lambda \to \lambda^2 \in K^1$. If $K = \mathbb{C}$ the latter map is surjective. If $K = \mathbb{R}$ the image is the set of nonnegative real numbers. In both cases the Zariski closure is the whole space. If $K = \mathbb{F}_p$ and $p \neq 2$, the image is a proper subset of K^1 and coincides with its Zariski closure.

Another important example is the ideal $I = (x^2 + 1)$. The reader is asked to provide the description of $\mathcal{V}(I)$ in Exercise 6.

Example 7. *We consider three ideals $I_1 = (x^2 - y^2)$, $I_2 = (x^2 - 2y^2)$ and $I_3 = (x^2 + y^2)$ in $K[x, y]$. The first one is not prime for any K. The second one is not prime for $K = \mathbb{R}$ or $K = \mathbb{C}$. However, it is a prime ideal when $K = \mathbb{Q}$. The last I_3 is not prime for $K = \mathbb{C}$, but is a prime ideal for $K = \mathbb{Q}$ or $K = \mathbb{R}$. Here we only prove the last statement and leave the others as an exercise. Suppose $fg \in I_3 \subset \mathbb{R}[x, y]$. This means that $fg = (x^2 + y^2) * h$, where $f, g, h \in \mathbb{R}[x, y]$. By the fundamental theorem of algebra every homogeneous polynomial p in two variables has a unique (up to multiplication by constants) representation as a product of linear forms with complex coefficients $p = \prod l_i$. In particular, if p has real coefficients, the decomposition must be stable under conjugation, i.e. for every i, either l_i has real coefficients or $\overline{l_i}$ must also appear in the decomposition. We have $x^2 + y^2 = (x + iy)(x - iy)$. In the ring $\mathbb{C}[x, y]$, without loss of generality, we may assume $(x + iy)|f$. But then, by the above argument also $(x - iy)|f$. Thus $f = (x + iy)(x - iy) \prod_i l_i$ for $l_i \in \mathbb{C}[x, y]$. However, $\prod_i l_i$ is stable under conjugation, i.e. defines a real polynomial. Thus $x^2 + y^2|f$ in $\mathbb{R}[x, y]$.*

As we have already seen, the image of a variety does not have to be closed, even if $K = \mathbb{C}$ or dense in its Zariski closure if $K = \mathbb{R}$. The following theorem shows however that one can always provide an algebraic description of the image. We start with a definition.

Definition 8. *A subset $A \subset K^n$ is (Zariski)* constructible *if it can be described as a finite union of (set-theoretic) differences of two varieties.*

A subset $B \subset \mathbb{R}^n$ is semi-algebraic *if it can be described as a set of solutions of a finite system of polynomial (weak and strong) inequalities or a finite union of such.*

Theorem 9.
1. *(Chevalley) If K is algebraically closed, then the image of a variety is a constructible set.*
2. *(Tarski-Seidenberg) If $K = \mathbb{R}$ then the image of a variety is a semi-algebraic set.*

Proof. The first part can be found e.g. in [6.4][4] and of the second part e.g. in [1.4] [1]. □

We define the *dimension* of an irreducible variety V as the maximal length $r := \dim V$ of the chain of irreducible varieties

$$\emptyset \subsetneq V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_r = V.$$

If V is reducible then its dimension is equal to the maximum dimension of all irreducible components from Proposition 5. The dimension is a basic invariant of a variety. This invariant has very nice properties:

- the dimension of the (closure of the) image of a variety V is at most $\dim V$,
- if $V_1 \subsetneq V_2$ then $\dim V_1 \leq \dim V_2$. If V_2 is irreducible, then the inequality is strict.

So far all the geometric objects we encountered were contained in K^n. We called them *varieties*, but more precisely we should refer to them as *affine varieties*. We now change our perspective with the aim of understanding *projective algebraic varieties*. We start by recalling the construction of a projective space $\mathbb{P}(V)$ over the vector space V of dimension $n+1$. Points of $\mathbb{P}(V)$ correspond to lines in V. Hence $[a_0 : \cdots : a_n] \in \mathbb{P}(V)$ represents a line going through the point $(a_0, \dots, a_n) \in V$, where we assume that not all a_i are equal to zero. Formally, $\mathbb{P}(V)$ is the set of equivalence classes $[v]$ for $v \in V \setminus \{0\}$ modulo the relation $v_1 \sim v_2$ if and only if there exists a nonzero scalar λ such that $v_1 = \lambda v_2$. For the topological construction over $\mathbb{R}$ or $\mathbb{C}$, we note that each line in V intersects the unit sphere precisely in two points. Thus $\mathbb{P}(V)$ may be regarded as a quotient of the sphere, identifying two antipodal points. In particular, it is always compact, with respect to the usual topology.

If we look at the subset S_i of $\mathbb{P}(V)$ where $a_i \neq 0$ we may always rescale and assume $a_i = 1$. This way we may identify $S_i = K^n$. As for any $p \in \mathbb{P}(V)$ some coordinate is nonzero, the affine spaces $S_i = K^n$ cover $\mathbb{P}(V)$, as $i = 0, \dots, n$. In fact, we may start from the affine spaces $S_i = K^n$ and glue them together to obtain $\mathbb{P}(V)$.

As before we are interested in polynomial functions on $\mathbb{P}(V)$. The first problem we encounter is that for a polynomial f it does not make sense to evaluate it on $[a_0 : \cdots : a_n]$, as the result depends on the choice of the representative. It may even happen that f vanishes for some representatives, while it does not for others. Thus, from now on we focus on *homogeneous* polynomials, i.e. linear combinations of monomials of fixed degree. If f is a homogeneous polynomial of degree d in $n+1$ variables, then $f(ta_0, \dots, ta_n) = t^d f(a_0, \dots, a_n)$. In particular, f vanishes on some representative of $[a_0 : \cdots : a_n]$ if and only if it vanishes on any representative. Given homogeneous polynomials $f_1, \dots, f_k$, possibly of distinct degrees, we define the associated *projective variety*:

$$\mathcal{V}(f_1, \dots, f_k) = \{[a_0 : \cdots : a_n] \in \mathbb{P}(V) : f_1(a_0, \dots, a_n) = \cdots = f_k(a_0, \dots, a_n) = 0\}.$$

An ideal is called *homogeneous* if it may be generated by homogeneous polynomials. In analogy to the affine case we define $\mathcal{V}(I) = \mathcal{V}(f_1, \dots, f_k)$ for an ideal I generated by homogeneous polynomials f_i.

Remark 10. *We note that homogeneous ideals contain (many) nonhomogeneous polynomials. In particular, $\langle x + y^2, y \rangle$ is a homogeneous ideal. For more characterisations and examples see Exercise 11.*

In theory, instead of considering a projective variety $X \subset \mathbb{P}(V)$ one can consider the affine cone $\hat{X}$ over it, i.e. the variety defined by the same ideal, but considered in V. However, in almost all cases, if possible it is *preferable* to work with projective varieties. The reason is that projective varieties are simpler - they behave better with respect to many properties. Below we present just a few of them.

First we note that (if X is not a projective subspace) the affine cone $\hat{X}$ is always singular at the point $0 \in V$. Second, for $K = \mathbb{C}$ or $K = \mathbb{R}$ Zariski closed sets are closed in the usual topology. In particular, projective varieties are compact. Thus, the image of any projective variety X is *closed*.

Theorem 11. *Over an algebraically closed field, the image of a projective variety X is Zariski closed.*

Proof. The first idea, discussed in the next lecture, is to describe the image as a projection of the graph of the map. Then one can apply Nullstellensatz - see Lecture 5 - to turn the problem into one from linear algebra. Details can be found in e.g. [4, 7.4.6–7.4.8]. $\square$

One of the important invariants of projective varieties, just as for affine varieties, is the dimension. The second one is the *degree*. There are several ways to define it. For example, when K is algebraically closed, a general projective subspace $L \subset \mathbb{P}(V)$ of dimension equal to the codimension of $V = \mathcal{V}(I) \subset \mathbb{P}(V)$ will intersect V only in finitely many, say d, points. This is the degree of V. If $I = (f)$ is principal and radical then the degree of $\mathcal{V}(I)$ equals the degree of f.

One of the nicest properties of projective varieties over algebraically closed fields is their behavior under intersection.

Theorem 12. *[3, 6.2 Theorem 6] Let $X, Y \subset \mathbb{P}(V)$ be two projective varieties of dimensions respectively d_1 and d_2. The intersection $X \cap Y$ has dimension at least $d_1 + d_2 - \dim \mathbb{P}(V)$.*

Exercises

Exercise 1. *Prove that the definition of $\mathcal{V}(I)$ does not depend on the choice of the generators of I.*

Exercise 2.

1. *Show that $J \subseteq I$ implies $\mathcal{V}(I) \subseteq \mathcal{V}(J)$.*
2. *Show that for any subsets $A, B \subseteq K^n$ if $A \subset B$ then $\mathcal{I}(B) \subseteq \mathcal{I}(A)$.*
3. *Give counterexamples to both opposite implications.*

Exercise 3. *Prove that varieties (in K^n) satisfy the axioms of closed sets.*

Exercise 4. *By identifying the point $(p_i) \in K^n$ with the prime ideal $\langle x_1 - p_1, \ldots, x_n - p_n \rangle$ consider K^n as a subset of $\operatorname{Spec} K[\mathbf{x}]$. Show that the Zariski topology induced from $\operatorname{Spec} K[\mathbf{x}]$ to K^n is the Zariski topology on K^n.*

Exercise 5. *Show that a morphism of rings $f : R_1 \to R_2$ induces a map $f^* : \operatorname{Spec} R_2 \to \operatorname{Spec} R_1$, by proving that a pull-back of a prime ideal is prime. Show that the induced map is continuous with respect to the Zariski topology.*

Exercise 6. *Describe $\mathcal{V}(I) \subset K^1$ for $I = (x^2 + 1)$ when $K = \mathbb{C}$ and $K = \mathbb{R}$.*

Exercise 7. *Realize the set of $n \times n$ nilpotent matrices as an affine variety. What is its dimension?*

Exercise 8. *1. Consider a polynomial $f \in K[\mathbf{x}]$ (e.g. $f = x$). Let D be the (open) set $D_f = \{p \in K^n : f(p) \neq 0\}$. Construct an affine variety V and a polynomial map inducing a bijection $V \to D$.*

2. Realize nondegenerate $n \times n$ matrices as an affine variety.

Exercise 9. *1. Use (or not) your favorite computer algebra system to determine the ideal of the image of the map given by formula (2). What is the meaning of the lowest degree polynomial in this ideal?*

2. Describe the ideal of the image of the map given by formula (1).

3. Generalize the previous point to more (independent) variables possibly with different (but finite) number of states.

Exercise 10. *Determine for which prime numbers p, the ideal $I_2 = \langle x^2 - 2y^2 \rangle \subset \mathbb{F}_p[x, y]$ is prime.*

Exercise 11. *For a polynomial $f = \sum_{\mathbf{a}} c_{\mathbf{a}} x^{\mathbf{a}}$ we call the degree k part of f the homogeneous polynomial $\sum_{\mathbf{a}:|\mathbf{a}|=\mathbf{k}} c_{\mathbf{a}} x^{\mathbf{a}}$.*

1. *Provide an example of a homogeneous ideal generated by nonhomogeneous polynomials.*
2. *Prove that an ideal $I = \langle f_1, \ldots, f_j \rangle$ is homogeneous if and only if for any f_i and any k the degree k part of f_i belongs to I.*
3. *Propose an algorithm that, given a set of generators of $I \subset K[\mathbf{x}]$, decides if I is a homogeneous ideal.*

References

[1] J. Bochnak M. Coste and M.-F. Roy. *Real algebraic geometry.* Vol. 36. Springer Science & Business Media, 2013.

[2] D. Cox, J. Little and D. O'Shea: *Ideals, Varieties, and Algorithms.* An introduction to computational algebraic geometry and commutative algebra, Third edition, Undergraduate Texts in Mathematics, Springer, New York, 2007.

[3] I. Shafarevich: *Basic algebraic geometry. 1. Varieties in projective space.* Translated from the 1988 Russian edition and with notes by Miles Reid. (1994).

[4] R. Vakil: *Foundations of algebraic geometry.*