Contents

ALGEBRAIC GEOMETRY

VLADIMIR HINICH

1. Introduction

Algebraic geometry studies algebraic varieties that can be described, loosely, as sets of solutions of systems of polynomial equations. This description can be made precise in different ways, at different levels of generality. In this introductory lecture we will give the most elementary version; it will be enough to demonstrate the richness of questions one can ask about the objects as well as to present some very classical results.

1.1. **Affine varieties.** Fix an algebraically closed field k, a number n and a collection f_i of polynomials over k in n indeterminants.

An affine algebraic variety X in k^n defined by f_i is, by definition, the set of common zeroes of f_i. For instance, for $n = 1$ X is just a finite number of points in k, the roots of the greatest common divisor of all f_i. For $n = 2$ and one equation $f = 0$ we get an *affine plane algebraic curve*, for instance, a straight

line if $f(x,y)=ax+by+c$ or an elliptic curve if $f(x,y)=y^2-x^3-ax-b$. The space k^n corresponds to the empty set of equations; is called the affine space and denoted $\mathbb{A}^n_k$.

One defines a topology on $\mathbb{A}^n_k$ (Zariski topology) declaring the affine varieties to be the closed sets. This topology has quite a few open/closed sets, but it is enough for a big part of algebraic geometry.

1.1.1. *Exercise.* Verify that the above definition yields a topology on the set k^n. Denote by $V(I)$, $I\subset k[x_1,\dots,x_n]$, the affine variety defined by the equations $f=0$ for all $f\in I$. Prove that $V(I)\cup V(J)=V(IJ)$ where $IJ=\{fg|f\in I,\ f\in J\}$. Prove that $\cap V(I_i)=V(\cup I_i)$.

1.1.2. *Affine line* $\mathbb{A}^1$. As a set, $\mathbb{A}^1$ is just k, the algebraically closed field. Zariski closed subsets are

- $\mathbb{A}^1$
- Finite subsets of $\mathbb{A}^1$.

1.1.3. Zariski topology induces a topology at any affine variety. As we see from the example, Zariski topology of an affine variety is very poor so we sould expect that completely different varieties with be isomorphic as topological spaces.

But, first of all, to talk about isomorphic or nonisomorphic algebraic varieties, we have to define a morphism between (affine) varieties. We start with the notion of regular function on X that will be the same as a morphism $X\to\mathbb{A}^1$.

1.1.4. *Regular functions.* By definition, a regular function on an affine variety $X\subset\mathbb{A}^n$ is a function $f:X\to k$ that can be presented by a polynomial of n variables. So, regular functions on $\mathbb{A}^n$ for the ring $k[x_1,\dots,x_n]$; Regular functions on an affine variety X defined in $\mathbb{A}^n$ by the equations $f_i=0$, are also represented by polynomials; but this representation is not unique; for instance, f and $f+\sum a_if_i$ define the same function on X.

Interesting question: describe the set of polynomials vanishing at X. It is easy to see that this is an ideal in $k[x_1,\dots,x_n]$. We denote it by $I(X)$. Then, obviously, the ring of regular functions on X, denoted $k[X]$, can be described as $k[x_1,\dots,x_n]/I(X)=k[\mathbb{A}^n]/I(X)$. Assume that X is given by the equations $f_i=0$. Denote by I the ideal generated by f_i. Then obviously $I\subset I(X)$.

1.1.5. *Nilpotents.* An element $a\in A$ in a commutative ring A is called nilpotent if $a^n=0$ for some n. The ring having no nonzero nilpotents is called *reduced*. Obviously $k[X]$ is always reduced as it is a subset if the ring of functions. Thus, it is not always true that $I(X)=I$: it is enough to take $I=(f^2)$ and then $I(X)$ will contain f.

1.1.6. *Exercise.* Given an ideal I in a commutative ring A, one defines

$$\sqrt{I} = \{x \in A | \exists n : x^n \in I\}.$$

Prove that $\sqrt{I}$ is an ideal. Prove that it is smallest among the ideals $J \supset I$ such that A/J is reduced.

Show that the claim does not necessarily hold if A is not commutative.

1.1.7. *Advertisement.* We will prove soon that if k is algebraically closed, $I \subset k[x_1, \ldots, x_n]$ and $X = V(I)$ then $I(X) = \sqrt{I}$, see *Nullstellensatz*.

1.1.8. *Size of the set of solutions.* How can one think about the size of X? Similarly to what one does in Linear algebra, one could try to parametrize the set of solutions (and define $\dim(X)$ as the number of parameters).

This approach seldom works, but it is still interesting to give an example.

We skip the trivial example of $X \subset \mathbb{A}^2$ given by the equation $y - x^2 = 0$, and look at something more interesting.

Let $X \subset \mathbb{A}^2$ be given by the equation $x^2 + y^2 = 1$. Choose an obvious solution $x = 1, y = 0$. Let us look for a solution satisfying the condition

$$t = \frac{y}{x - 1}$$

for a given t. We get the equation

$$x^2 + t^2(x - 1)^2 = 1,$$

that is

$$x^2(1 + t^2) - 2t^2x + (t^2 - 1) = 0.$$

This is a quadratic equation with respect to x that has a solution $x = 1$. By Vieta theorem the second root is $x = \frac{t^2-1}{t^2+1}$ and therefore $y = t(x - 1) = -\frac{2t}{t^2+1}$. We get a one-to one correspondence (almost) between the points of X and $\mathbb{A}^1$, carrying $t \in \mathbb{A}^1$ to the pair $(\frac{t^2-1}{t^2+1}, -\frac{2t}{t^2+1})$ and, in the opposite direction, carrying (x, y) to $\frac{y}{x-1}$.

1.1.9. *Exercise.* Describe precisely the one-to-one correspondence:

- what subsets of X and of $\mathbb{A}^1$ correspond to each other?
- Does the above analysis work when k is a field of characteristic 2?

1.1.10. Going back to linear algebra, there is another way to define the dimension of a vector space. $\dim V$ can be defined as the maximal length of the sequence of vector subspaces

$$V = V_n \supset V_{n-1} \supset \ldots \supset V_0 = 0.$$

One can try to mimic this definition in our context.

We can safely expect to have $\dim \mathbb{A}^1 = 1$. However, there are very long sequences of proper closed subvarieties, consisting of a different number of points.

To get a reasonable answer, we should allow one-point closed subset, but sould not allow many-point subsets. The first idea could be to require subvarieties used to be connected, but here is a better notion.

1.1.11. **Definition.** A topological space X is called irreducible if it cannot be presented as a union $X = X_1 \cup X_2$ of two closed smaller subsets.

Not that the above definition makes only sense for very strange topologies, such as Zariski topology.

Now we are ready to give a formal definition.

1.1.12. **Definition.** The dimension of an affine variety X is the maximal length of the sequence

$$X = X_n \supset X_{n-1} \supset \ldots \supset X_0$$

of closed irreducible subsets.

Meanwhile it is not even obvious that $\dim \mathbb{A}^n = n$ (but this is a correct statement).

We have easily

1.1.13. **Lemma.** *An affine algebraic variety X is irreducible iff the ring of regular functions $k[X]$ is integral domain.*

The notion of dimension presented above is compatible with the following notion of dimension of commutative rings.

An ideal $\mathfrak{p} \subset A$ is called prime if $A/\mathfrak{p}$ is a domain. The dimension of A is defined as the maximal length of the chain

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n$$

of prime ideals of A.

1.2. **Projective varieties.** Recall that the projective space $\mathbb{P}^n_k$ is the set of lines passing through 0 in k^{n+1}. Otherwise, it can be defined as the quotient of the set $k^{n+1}\backslash\{0\}$ modulo the equivalence relation $x \sim \lambda x$ for $\lambda \in k^* = k\backslash\{0\}$. It is worth thinking of $\mathbb{P}^n$ as the space glued from $n+1$ copies of the affine n-dimensional space.

Any $k+1$-dimensional subspace in k^{n+1} gives rise to a copy of $\mathbb{P}^k$ inside $\mathbb{P}^n$. For instance, two lines in $\mathbb{P}^2$ always meet, the same hold for any pair of $\mathbb{P}^k$ and $\mathbb{P}^{n-k}$ in $\mathbb{P}^n$ etc.

Here are the formulas. For each $i = 0, \ldots, n$ we define a subset

$$U_i = \{(x_0 : x_1 : \ldots : x_n) | x_i \neq 0\}.$$

There is a one-to-one correspondence between the points of U_i and the points of $\mathbb{A}^n$, given by the formula

$$(x_0 : \ldots : x_n) \in U_i \mapsto (\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}).$$

This formulas allow one to see $\mathbb{P}^n$ as covered by $(n+1)$ affine spaces.

There are no polynomials $f \in k[x_0, \dots, x_n]$, except for the constants, satisfying the equation $f(x) = f(\lambda x)$ for all $\lambda \in k^*$ and all x. But the equation $f(x) = 0$ has the same roots as $f(\lambda x) = 0$ in case f is a homogeneous polynomial.

This justifies the following definition.

1.2.1. **Definition.** A projective variety $X \subset \mathbb{P}^n_k$ defined by a collection of homogeneous polynomials $f_i \in k[x_0, \dots, x_n]$ is the set of their common zeroes.

If an affine curve X is given by an equation $f(x, y) = 0$, here is how one describes its closure in $\mathbb{P}^2$. We write $f(\frac{x_1}{x_0}, \frac{x_2}{x_0})$ and multiply the rational expression by the minimal power of x_0 to get rid of the denominator. For instance, the circle defined by the equation $x^2 + y^2 = 1$ converts first to $\frac{x_1^2}{x_0^2} + \frac{x_2^2}{x_0^2} = 1$ and then to

$$x_1^2 + x_2^2 = x_0^2. \tag{1}$$

Any projective variety X, that is, a closed subset of $\mathbb{P}^n$, is covered by the affine spaces mentioned above. The intersections are open in X and closed in the affine spaces. That is, a projective variety as we define it is covered by affine varieties. See the example of (1).

A regular function on a projective variety can be defined as a collection of compatible regular functions on each affine open subvariety. Typically, there are no nonconstant regular functions on projective varieties

1.2.2. *Exercise.* Prove that the only regular functions on $\mathbb{P}^n$ are the constants.

1.3. **Bézout theorem.** Bézout theorem claims that, given two plane curves without common components of degrees m and n respectively, the number of their intersection points is precisely $m \cdot n$. To get this answer, one should be careful twice:

- Count the intersection points with their multiplicites.
- Not to forget the "points at infinity".

One should also understand that plane algebraic curves decompose into components.

The first condition is widely well-known: we understand that a degree n polynomial has n complex roots if we take into account their multiplicities. The second condition is also quite transparent: two parallel lines have one intersection point "at infinity".

Make this explicit! This should persuade us that it is often better to work with projective rather than affine varieties.

It is very easy to verify the claim if one of the curves decomposes into a union of straight lines.

1.3.1. *Common components.* One of the topic studied is the decomposition of an algebraic variety into irreducible components. This is much easier for plane curves as they are given by a unique equation and its components correspond to factors of the equation.

Let us mention

1.3.2. **Theorem.** *The ring of polynomials $k[x_1,\dots,x_n]$ has a unique decomposition into primes (in other words, the ring is factorial, or UFD).*

Proof. For $n=1$ the ring is PID, the rest follows by induction from the Gauss lemma formulated below. □

1.3.3. **Lemma** (Gauss lemma)**.** *Let A be factorial. Then $A[x]$ is factorial.*

□

1.3.4. *Exercise.* Let A be factorial and $a\in A$. Prove that the ideal (a) is prime iff a is irreducible.

Thus, irreducibility of a hypersurface $X=V(f)\subset\mathbb{A}^n$ is equivalent to irreducibility of the polynomial $f\in k[x_1,\dots,x_n]$.

1.4. **27 lines.** Here is a classical result of AG of the 19 century that contains a lot of ideas relevant till today. Let X be a smooth cubic surface in $\mathbb{P}^3$. This is the set of points $(x_0:x_1:x_2:x_3)\in\mathbb{P}^3$ satisfying a cubic (homogeneous) equation

$$f(x_0,x_1,x_2,x_3)=0$$

so that the differential $(\frac{\partial f}{\partial x_0},\frac{\partial f}{\partial x_1},\frac{\partial f}{\partial x_2},\frac{\partial f}{\partial x_3})$ does not vanish at the points of X (smoothness).

One equation in 3-dimensional space typically gives a two-dimensional variety.

.

We study the projective lines lying in X. A classical result due to Arthur Cayley and George Salmon (1849) says that there are precisely 27 lines on each smooth cubic surface. Here are the steps of the proof.

- All cubic surfaces are parametrized by their coefficients, up to a scalar. In the general form

$$f(x_0,x_1,x_2,x_3)=\sum_{i+j+k+l=3} c_{ijkl}x_0^ix_1^jx_2^kx_3^l$$

there are $\frac{6!}{3!3!}=20$ coefficients, so cubic surfaces are parametrized by $\mathcal{C}=\mathbb{P}^{19}$.
- A projective line in $\mathbb{P}^3=\mathbb{P}(V)$ with $\dim V=4$ is defined by a two-dimensional subspace of V. The collection of such is called a Grassmannian ($Gr(4,2)$, the collection of 2-dimensional vector subspaces in a 4-dimensional space) and is given by one equation (Plucker equations) in

$\mathbb{P}(\wedge^2 V) = \mathbb{P}^5$. Here is the description of the Plucker embedding. Given a vector space V, one defines its second exterior power $\wedge^2 V$ as the receptacle of the universal antisymmetric bilinear map $V \times V \to \wedge^2 V$ (we will discuss this later). If V has a basis $e_1, \dots, e_n$, $\wedge^2 V$ has a basis e_{ij} such that $e_{ii} = 0$ and $e_{ij} = -e_{ji}$. In particular, $\dim \wedge^2 V = \binom{n}{2}$. Furthermore, the operation $\wedge^2$ is functorial, which means that any linear map $W \to V$ gives rise to a linear map $\wedge^2 W \to \wedge^2 V$. In particular, for $\dim V = 4$, any subspace W of dimension 2 gives rise to a line $\wedge^2 W$ in $\wedge^2 V$ (it is worth to write down explicit formulas for the Pl'ucker embedding). The image of the grassmannian in $\mathbb{P}^5$ is given by one equation

$$x_{01}x_{23} + x_{02}x_{13} + x_{03}x_{12} = 0,$$

where x_{ij} are the coordinates of a vector in the vector space $\wedge^2 V$ with the basis e_{ij}.

Thus, the space of lines $\mathcal{L}$ in $\mathbb{P}^3$ has dimension $4 = 5 - 1$.

- We define $\mathcal{P} \subset \mathcal{L} \times \mathcal{C}$ as the set of pairs $(L, C) \in \mathcal{L} \times \mathcal{C}$ such that the line L lies in the surface C. We have two canonical projections, $p : \mathcal{P} \to \mathcal{L}$ and $q : \mathcal{P} \to \mathcal{C}$,
- Let us describe the space of cubics passing through a given line $L \in \mathcal{L}$. This is the fiber $\mathcal{P}_L := p^{-1}(L)$ of p. We claim that $\mathcal{P}_L$ is isomorphic to $\mathbb{P}^{15}$. In fact, the result obviously is independent of the choice of the line L. If L is given by the equations $x_2 = x_3 = 0$, a cubic form $F = \sum c_{ijkl} x^i y^j z^k t^l$ contains L iff $c_{3000} = c_{2100} = c_{1200} = c_{0300} = 0$. The remaining 16 parameters form $\mathbb{P}^{15}$.
- Since $p : \mathcal{P} \to \mathcal{L}$ has all fibers of dimension 4, we can easily deduce (knowing some good properties of the dimension function) that $\mathcal{P}$ has dimension $15 + 4 = 19$. Of course, we should know that $\mathcal{P}$ is a projective variety and that dimention behaves well.
- Finally, we have a projection $\mathcal{P} \to \mathcal{C}$ of two varieties of dimension 19. Its image is closed in $\mathcal{C}$ (this is because $\mathcal{P}$ is projective; the claim is similar to the claim in general topology saying that the image of compact topological space is always closed). If it were not surjective, the image would have dimension smaller than 19 and then the minimal dimension of a (nonempty) fiber would be positive. Here we use that if there is a surjective map $f : X \to Y$ with $\dim(X) = n$, $\dim(Y) = m$ that the dimension of fiber $f^{-1}(y)$ is $\geq n - m$. Therefore, to deduce that q is surjectivem it is enough to find $C \in \mathcal{C}$ for which the fiber $q^{-1}(C)$ is zero-dimensional. In other words, it is enough to find a cubic surface C thaht has only finite number of lines on it.

Take, for instance, $F=\sum_{i=0}^3 x_i^3$ (this surface is called Fermat cubic). An explicit calculation gives the following description of the lines on F. These are the lines $\{(x:\alpha x:y:\beta y)|x,y\in\mathbb{C}\}$ with $\alpha^3=\beta^3=1$ as well as the lines conjugate to the above with respect to permutation of the variables. This set being finite, this implies that the projection $q:\mathcal{P}\to\mathcal{C}$ is surjective.

Thus, any cubic surface (even a singular one) contains at least one line.

- Let now C be a smooth cubic surface. Let $L\subset C$. Look at a plane H passing through $L\subset C$. The intersection $H\cap C$ is a plane cubic curve in H containing L. Thus L is one of its components. Thus, $H\cap X=L\cup Q$ where Q is a quadric (irreducible or union of two lines). The planes H are parametrized by the projective line $\mathbb{P}^1$, and the smoothness condition on Q in terms of H is equivalent to an equation of degree 5 on the value of parameter This is verified by an explicit calculation: choose the same convenient line $x_2=x_3=0$, so that $\alpha=(a_0:a_1)\in\mathbb{P}^1$ defines $H_\alpha=\{(x_0:x_1:a_0x_2:a_1x_2)\}$. Then $H\cap C$ is given by the equations
$$\sum c_{ijkl}a_0^k a_1^l x_0^i x_1^j x_2^{3-i-j},$$
so that Q is given by the equation
$$\sum c_{ijkl}a_0^k a_1^l x_0^i x_1^j x_2^{2-i-j}.$$
This quadric decomposes iff its discriminant that is a degree 5 polynomial of a_0,a_1, vanishes. Here is the explanation: a quadratic form can be diagonalized, and the expression $\sum a_i x_i^2$ decomposes iff its rank is ≤ 2.

  It turns out that, if C is smooth, this polynomial has no multiple roots and, for α root of the polynomial, $H_\alpha\cap C$ is a union of three different lines.

  Thus, there are 5 planes H_α passing through L so that Q is degenerate, that gives that L intersects 10 other lines on C.
- Choose three lines, L_1,L_2,L_3 that are components of $C\cap H$. Any other line L on C intersects with H, so that the intersection point lies on one of the L_i. Three lines L,L_i,L_j cannot intersect at one point of C as otherwise this point would not be smooth (they do not belong to one plane). Therefore, each one of L_i has 8 more lines to meet. This gives $27=3+3\cdot 8$ lines overall.

2. Spaces with functions

The contemporary way of describing non-affine varieties is via gluing. The most appropriate language to describe gluing is the language of sheaves which

is not very elementary for one who sees it for the first time. The language of "spaces with functions" is less general, but it is much easier for understanding. A considerable part of ideas of algebraic geometry can be explained in this language. This is what we will do in this course.

2.1. **Basic definitions.** Fix a field k.

2.1.1. **Definition.** A space with functions is a pair $(X, \mathcal{O})$ where X is a topological space and $\mathcal{O}$ assigns to each open subset U of X a k-subalgebra $\mathcal{O}(U)$ of the set of k-valued functions on U. The assignment $U \mapsto \mathcal{O}(U) \subset \mathrm{Map}(U, k)$ should satisfy the following properties.

1. If $f \in \mathcal{O}(U)$ and $V \subset U$ then $f|_V \in \mathcal{O}(V)$.
2. If $U = \cup U_\alpha$, $f \in \mathrm{Map}(U, k)$ such that $f|_{U_\alpha} \in \mathcal{O}(U_\alpha)$ then $f \in \mathcal{O}(U)$.
3. If $f \in \mathcal{O}(U)$ then $D(f) = \{x \in U | f(x) \neq 0\}$ is open and $\frac{1}{f} \in \mathcal{O}(D(f))$.

We add immediately another definition.

2.1.2. **Definition.** A morphism of spaces with functions $\phi : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is a continuous map $\phi : X \to Y$ such that for any open set $V \subset Y$ and $f \in \mathcal{O}_Y(V)$ the composition $f \circ \phi : \phi^{-1}(V) \to k$ is in $\mathcal{O}_X(\phi^{-1}(V))$.

The spaces with functions and their morphisms form *the category of spaces with functions* denoted `Spfu`.

Any category $\mathcal{C}$ has objects (in this case spaces with functions). For any pair of objects (spaces with functions) a set of morphism from one to the other is given. Morphisms can be composed and the composition is associative. For any object there is the identity morphism from the object to itself.

We need one more very basic definition.

2.1.3. **Definition.** Let $(X, \mathcal{O})$ be a space with functions and let U be an open subset of X. Then a natural (obvious) structure of a space with functions is induced on U: for $V \subset U$ we set $\mathcal{O}_U(V) = \mathcal{O}(V)$. The map $(U, \mathcal{O}_U) \to (X, \mathcal{O})$ is called the open embedding.

Let us show how the formalism of spaces with functions works outside of algebraic geometry.

2.1.4. *Example.* Let $k = \mathbb{R}$, X be a topological space and $\mathcal{O}(U)$ is the space of continuous functions on U. `Verify the axioms; one uses that the set of zeroes of a continuous function is closed.`

This is a space with functions. It is not very interesting as it contains the same information as the topological space X.

2.1.5. *Example: smooth manifold.* First of all, we have a *local model*: this is the standard open disc $D = \{x \in \mathbb{R}^n |\ ||x|| < 1\}$, with $\mathcal{O}_D(U)$ defined as the algebra of smooth functions on U. Now, $(X, \mathcal{O})$ is a manifold if it is locally isomorphic to $(D, \mathcal{O}_D)$. In more detail, $(X, \mathcal{O})$ is a smooth manifold if for any $x \in X$ there exists an open neighborhood U of x such that the space with function defined by U is isomorphic to $(D, \mathcal{O}_D)$.

One can define in the same manner C^k-manifolds, complex manifolds ($k = \mathbb{C}$) or real-analytic manifolds.

2.1.6. Traditionally, the standard definition of a smooth manifold is given in terms of charts and atlases. It is easy to see that our definition is equivalent to the standard one; I think it is better as it does not require a choice of the atlas.

2.1.7. *Example: a point.* Let $X = \mathtt{pt}$ be a point. There is only one structure of a space with functions on $\mathtt{pt}$, for a given k: the functions on X should be a subset of $\mathrm{Map}(X, k) = k$ and, if it is a k-algebra, it should contain k. Thus, $\mathcal{O}_{\mathtt{pt}}(\mathtt{pt}) = k$ is the only choice.

One can easily verify that for any space with functions X one has $\mathrm{Hom}_{\mathtt{Spfu}}(\mathtt{pt}, X) = X$, considered as a set.

2.1.8. By definition of a morphism, any morphism $\phi : (Y, \mathcal{O}_Y) \to (X, \mathcal{O}_X)$ gives rise to map $\mathcal{O}_X(X) \to \mathcal{O}_Y(Y)$. Thus, we have a map

$$\mathrm{Hom}_{\mathtt{Spfu}}(Y, X) \to \mathrm{Hom}_{\mathtt{Alg}(k)}(\mathcal{O}_X(X), \mathcal{O}_Y(Y)). \tag{2}$$

In what follows we assume that k is an algebraically closed field.

2.1.9. **Definition.** A space with functions $(X, \mathcal{O}_X)$ is called an affine variety if for any space with functions $(Y, \mathcal{O}_Y)$ the natural map $\mathrm{Hom}_{\mathtt{Spfu}}(Y, X) \to \mathrm{Hom}_{\mathtt{Alg}}(\mathcal{O}_X(X), \mathcal{O}_Y(Y))$ is a bijection.

2.2. **Existence of affine varieties.** Note from the very beginning that if an affine variety X with $\mathcal{O}_X(X) = A$ exists for a certain k-algebra A, then it is unique up to a unique isomorphism (Spinoza principle).

''Spinoza principle'' is the following very general claim of categorical nature. Instead of trying to describe it in full generality, we will present how it works in our specific case.

Let $(X, \mathcal{O}_X)$ and $(X', \mathcal{O}_{X'})$ be two affine varieties with $\mathcal{O}_X(X) = \mathcal{O}_{X'}(X') = A$. This gives a specific element (isomorphism) in $\mathrm{Hom}_{\mathtt{Alg}(k)}(\mathcal{O}_X(X), \mathcal{O}_{X'}(X'))$ and, therefore, by assumption, a corresponding $\phi : (X', \mathcal{O}_{X'}) \to (X, \mathcal{O}_X)$. Replacing X with X' we get a canonical map $\psi : (X, \mathcal{O}_X) \to (X', \mathcal{O}_{X'})$. Now, the composition $\phi \circ \psi : (X, \mathcal{O}_X) \to (X, \mathcal{O}_X)$ should be the unique map corresponding to $\mathrm{id} : \mathcal{O}_X \to \mathcal{O}_X$. Therefore, $\phi \circ \psi = \mathrm{id}$. The same hold for the composition $\psi \circ \phi$. Thus, affine variety, if exists, is unique up to unique isomorphism.

We will prove the following result.

2.2.1. **Theorem.** *Let k be an algebraically closed field and let A be a k-algebra of finite type with no nilpotents (such algebras are called reduced). Then there exists an affine variety $(X, \mathcal{O})$ with $\mathcal{O}(X) = A$.*

Proof. For given k and A, we define the set X as $\mathrm{Hom}_{\mathtt{Alg}}(A, k)$ (we have no choice by 2.1.7). We define the topology on X in the "minimal possible way": for any $S \subset A$ we define $V(S) = \{x \in X | S \subset \mathrm{Ker}(x)\}$ and $D(S) = X \setminus V(S)$, and we declare the set of $D(S)$ for varying S to be the basis of topology of X. Note that $D(S) = \cup_{s\in S} D(s)$ and $V(S) = \cap_{s\in S} V(s)$, so the collection of $D(S)$ defines a topology on X.

By definition there is an evaluation map $ev : A \times X \to k$ that carries a pair (f, x) to $ev_x(f)$. We will determine $\mathcal{O}(U)$ "in a most minimal way". This means that a function $\phi : U \to k$ will be called regular for a certain open covering $U = \cup U_i$ there exist $s_i, t_i \in A$ such t_i does not vanish in U_i [$U_i \subset D(t_i)$] and $\phi(x) = ev_x(s_i)/ev_x(t_i)$ for all $x \in U_i$.

The pair $(X, \mathcal{O})$ is automatically a space with functions. In the next section we will prove that the map $ev : A \to \mathcal{O}(X)$ is bijective. This will follow from Nullstellensatz. This explains why did we have to restrict ourselves to algebras of finite type over the algebraically closed fields.

Let us now verify that for any ring homomorphism $f : \mathcal{O}_X(X) \to \mathcal{O}_Y(Y)$ there exists a unique map $F : Y \to X$ of spaces with functions inducing f on the algebras of regular functions.

Given $y \in Y$, a map

$$ev_y \circ f : \mathcal{O}_X(X) \to \mathcal{O}_Y(Y) \overset{ev_y}{\to} k$$

is, by definition, a point in X. This defines a map $F : Y \to X$. Let us verify that F is continuous. In fact, for any $s \in A$ the preimage of $D(s)$ is the collection of $y \in Y$ such that $f(s)(y) \neq 0$. By definition of a space with function, this is an open set in Y.

Finally, we have to make sure that for any open $U \subset X$, $V = F^{-1}(U)$, and any $\phi \in \mathcal{O}_X(U)$ the composition

$$V \overset{F}{\to} U \overset{\phi}{\to} k$$

belongs to $\mathcal{O}_Y(V)$. By definition, there is a covering $U = \cup U_i$ and $s_i, t_i \in A$ such that t_i does not vanish at U_i and $\phi(x) = s_i(x)/t_i(x)$ for $x \in U_i$. The open spaces $V_i = F^{-1}(U_i)$ cover V, the functions $f(t_i)$ do not valish on V_i, so $f(s_i)/f(t_i) \in \mathcal{O}_Y(V_i)$. This implies that $\phi \circ F$ is regular at V.

□

Notation: the affine variety with the k-algebra A of regular functions will be denoted by $\mathtt{spec}_k(A)$ or simply $\mathtt{spec}(A)$.

We are now ready to define general algebraic varieties.

2.2.2. **Definition.** A space with functions $(X, \mathcal{O})$ is called an algebraic variety if it admits a finite open covering with affine varieties.

2.3. **Examples.**

2.3.1. $\mathbb{A}^1$ *and* $\mathbb{P}^1$. Let us describe two simplest algebraic varieties: the affine line $\mathbb{A}^1$ and the projective line $\mathbb{P}^1$.

We fix an algebraically closed field k.

The affine line $\mathbb{A}^1$ is defined as $\mathtt{spec}(k[x])$.

The set of points of $\mathbb{A}^1$ is just k, and the topology is defined by declaring that k as well as all finite subsets of k are the closed sets. Open subsets are, therefore, the empty set and the complements to a finite number of points.

A regular function on $U = \mathbb{A}^1 \setminus \{a_1, \dots, a_n\}$ is $k[x, (x-a_1)^{-1}, \dots, (x-a_n)^{-1}] \subset k(x)$.

The projective space $\mathbb{P}^1$ consists of $\mathbb{A}^1$ and an extra point ∞. An open set in $\mathbb{P}^1$ is either empty or a complement to a finite collection of points. A regular function on $U_0 = \mathbb{P}^1 \setminus \{\infty\}$ is just $k[x] \subset k(x)$ as above. A regular function on $U_1 = \mathbb{P}^1 \setminus \{0\}$ is $k[x^{-1}] \subset k(x)$. This also defines regular functions on each open subset of U_0 and of U_1. A function on U is regular if its restrictions to $U \cap U_i$ are regular. Another descrption of projective space is presented below.

Note that in the examples above intersection of two nonempty open subsets is nonempty. This means that $\mathbb{A}^1$ and $\mathbb{P}^1$ are irreducible.

2.3.2. $\mathbb{P}^n$ *as the space of lines.* We will now present $\mathbb{P}^n$ as a space with functions and show that it is an algebraic variety in the sense of Definition 2.2.2.

As a topological space, $\mathbb{P}^n$ is the quotient of $\mathbb{A}^{n+1} \setminus \{0\}$ modulo the equivalence relation $v \sim \lambda v$ for $\lambda \in k^*$. Recall that the latter means that a subset of $\mathbb{P}^n$ is open if and only if its preimage under the factor map $\mathbb{A}^{n+1} \setminus \{0\} \to \mathbb{P}^n$ is open. One can easily verify that this yields precisely the Zariski topology on $\mathbb{P}^n$ as defined in Section 1 (this is an exercise). Finally, to define a structure of a space with functions on $\mathbb{P}^n$, we have to determine the algebra of regular functions $\mathcal{O}(U)$ on any open subset U of $\mathbb{P}^n$. There is only one way to do this, if we require that the open embeddings $U_i \to \mathbb{P}^n$, where $U_i = \{x \in \mathbb{P}^n | x_i \neq 0\}$, is an open embedding as defined in 2.1.3.

2.3.3. *Principal open sets.* Let $X = \mathtt{spec}_k(A)$ be an affine variety and let $f \in A$. The open set

$$D(f) = X \setminus V(f)$$

is called a principal open set. Principal open sets form a basis of Zariski topology. Let us show that principal open sets define affine open subvarieties of X.

Denote $A_f := A[x]/(xf - 1)$. If A is reduced, A_f is also reduced (for the proof of this fact see ??. For the current proof we can just replace A_f with $A_f/N(A_f)$ to get a reduced algebra). The algebra A_f enjoys a

very nice "universal" property (we will discuss later the word "universal" in the previous sentence). The obvious map $i : A \to A_f$ induces, for any k-algebra B, an embedding

$$\mathrm{Hom}_{\mathtt{Alg}_k}(A_f, B) \to \mathrm{Hom}_{\mathtt{Alg}_k}(A, B)$$

whose image consists of homomorphisms $\phi : A \to B$ for which $\phi(f) \in B$ is invertible. Finally, A_f is an algebra of finite type over k.

Thus, we have a map

$$\mathtt{spec}_k(A_f) \to \mathtt{spec}_k(A)$$

that is injective as a map of sets and whose image identifies with $D(f)$. It is easy to verify that this is an open embedding, that is that $D(f)$ is isomorphic, as a space with functions, to $\mathtt{spec}A_f$.

2.3.4. *Quasi-affine varieties.* There exist, however, open subsets of $\mathtt{spec}(A)$ that are not affine. Here is an example. Let $A = k[x_1, \dots, x_n]$ and let $U = \mathbb{A}^n \setminus \{0\}$. If $n = 1$, U is affine, but this fails to be true for $n > 1$. In fact, let us describe the restriction homomorphism $A \to \mathcal{O}(U)$. We can present U as the union of affine varieties $U_i = \mathtt{spec}(A_{x_i})$, $i = 1, \dots, n$. A regular function on U is given by a collection of compatible regular functions $f_i \in A_{x_i}$. Each of the rings A_{x_i} identifies with a subring in the field of rational functions in $x_1, \dots, x_n$. Their compatibility means that their images in this field coincide. This is only possible if $f_i \in A$ coincide for all i. Therefore, the restriction map $A \to \mathcal{O}(U)$ is bijective. This means that if U were affine, it would coincide with $\mathbb{A}^n$.

Definition. An algebraic variety is called quasi-affine if it is isomorphic to an open subvariety of an affine variety.

2.4. **Language of category theory.** We have already used the word "category". We will need more and more the language of categories, so let us start.

2.4.1. *Definition of a category.* A category $\mathcal{C}$ is a collection of the following data:

- a class of *objects* of $\mathcal{C}$ denoted by $\mathrm{Ob}(\mathcal{C})$.
- for any pair X, Y of objects, a set $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ of *morphisms* from X to Y.
- for any triple X, Y, Z of object, a *composition map*

$$\mathrm{Hom}_{\mathcal{C}}(Y, Z) \times \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}}(X, Z).$$

The composition is required to be associative, any $\mathrm{Hom}_{\mathcal{C}}(X, X)$ is required to have the identity morphism id_X that is a unit with respect to compositions.

2.4.2. *Examples.* Categories are everywhere in mathematics. These include

- The category of sets $\mathtt{Set}$.
- The category of vector spaces over a given field k. The category of groups, of abelian groups. The category $\mathtt{Alg}_k$ of commutative algebras over k.
- The category of topological spaces (and continuous maps).

- The category of smooth manifolds.
- The category $\mathtt{Var}_k$ of algebraic varieties over an algebraically closed field k.

A morphism $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$ is called an isomorphism of there exists $g \in \mathrm{Hom}_{\mathcal{C}}(Y,X)$ (we also write $g: Y \to X$) such that $f \circ g = \mathrm{id}_Y$ and $g \circ d = \mathrm{id}_X$.

2.4.3. *Initial object.* An object $X \in \mathcal{C}$ is called *initial* if $\mathrm{Hom}(X,Y)$ consists of one element for any $Y \in \mathrm{Ob}(\mathcal{C})$. In particular, $\mathrm{Hom}(X,X) = \{\mathrm{id}_X\}$.

Here are some trivial examples.

- $\emptyset$ is an initial object of $\mathtt{Set}$, the category of sets.
- 0 is an initial object in $\mathtt{Vect}$, the category of vector spaces over a fixed field.
- $\mathbb{Z}$ is the initial object in the category of commutative rings (the are assumed to have unit).

Here is the most general form of "Spinoza principle":

Lemma. *If $\mathcal{C}$ admits an initial object, it is unique up to a unique isomorphism.*

Proof. If both X and X' are initial, $\mathrm{Hom}(X,Y) = \{f\}$ and $\mathrm{Hom}(Y,X) = \{g\}$, one has $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$. □

To apply this result "in real life", that is to deduce uniqueness of a certain construction, one has to present this construction as an initial object in a certain category. For example, given a commutative ring A and an element f, let us define the category $\mathcal{C}$ whose objects are ring homomorphisms $\phi: A \to B$ carrying $f \in A$ to an invertible element in B. A morphism from $\phi: A \to B$ to $\psi: A \to C$ is a ring homomorphism $t: B \to C$ such that $\psi = t \circ \phi$.

It is easy to see that $\mathcal{C}$ has the ring homomorphism $A \to A[x]/(xf-1)$ is initial in $\mathcal{C}$.

In a similar way we proved uniqueness of affine varieties.

First of all, a next piece of abstract nonsense: given a category $\mathcal{C}$, we define the opposite category $\mathcal{C}^{\mathrm{op}}$ as the one having the same objects as $\mathcal{C}$, with "inverted arrows" $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(X,Y) = \mathrm{Hom}_{\mathcal{C}}(Y,X)$. A *terminal* object in $\mathcal{C}$ is defined as an initial object in $\mathcal{C}^{\mathrm{op}}$.

Here are some elementary examples of terminal objects in categories.

- a singleton is a terminal object in $\mathtt{Set}$ (we see that there is a unique isomorphism between any two singletons).
- 0 is also a terminal object in $\mathtt{Vect}$.
- The category of commutative rings has a terminal object, a ring that we seldom remember of its existence. This is the zero ring, the only ring (up to unique isomorphism) that satisfies the condition $0 = 1$ (proof: $0 = 1$ implies $0 = 0 \cdot x = 1 \cdot x = x$.) This ring has no prime ideals, so this is

definitely an exception to the theorem saying that any commutative ring admits prime ideals.

Affine varieties can also be defined as terminal objects in specially designed categories.

Given a reduced algebra A of finite type over an algebraically closed field k, we define the category $\mathcal{C}$ whose objects are pairs (X, f) where X is a space with functions and $f : A \to \mathcal{O}_X(X)$ an algebra homomorphism. A morphism $\phi : (X, f) \to (Y, g)$ is a morphism $\phi : X \to Y$ of spaces with functions such that $f = \phi^* \circ g$. A terminal object in $\mathcal{C}$ is a space with functions X endowed with a homomorphism $f : A \to \mathcal{O}_X(X)$ such that any $g : A \to \mathcal{O}_Y(Y)$ is presented as $g - \phi^* \circ f$ for a unique $\phi : (Y, \mathcal{O}_Y) \to (X, \mathcal{O}_X)$. Thus, $\mathtt{spec}_k(A)$ is the terminal object of the catgeory $\mathcal{C}$ defined above.

2.5. **Irreducible components.** A topological space is called noetherian (Emmy Noether, 1882–1935) if any descending system of its closed subsets $Y_0 \supset Y_1 \supset \dots$ stabilizes, that is $Y_{n+k} = Y_n$ for some n and all $k > 0$.

2.5.1. **Lemma.** *The topological space underlying an algebraic veriety is noetherian.*

Proof. A topological space that is a finite union of its open noetherian subspaces is noetherian. For any descending chain of closed subsets its intersection with each U_i stabilizes, to the whole thing should stabilize. This reduces the claim to an affine variety. A descending chain of closed subsets in an affine variety corresponds to an ascending chain of ideals in the corresponding ring of regular functions. By Hilbert basis theorem (see the next section) any such chain stabilizes. □

2.5.2. **Remark.** A commutative ring A is called noetherian if the following equivalent conditions hold.

- Any ideal of A is finitely generated.
- Any increasing chain of ideals in A stabilizes.

By Hilbert basis theorem the ring $k[x_1, \dots, x_n]$ is noetherian. This obviously implies that $\mathbb{A}^n$ as well as any Zariski closed subset of $\mathbb{A}^n$ is noetherian.

2.5.3. **Proposition.** *Any closed subset of a noetherian topological space X can be presented as a finite union of irreducible closed subsets. This presentation is unique if we require that none of components lies in another.*

Proof. Let Φ be the set of all closed subsets of X that cannot be presented as a finite union of irreducible closed subsets. This is a poset and, since X is noetherian, if Φ is nonempty, it has a minimal element. Let Z be a minimal element. It is not irreducible so $Z = Z_1 \cup Z_2$, so at least on of Z_i belongs to Φ, – contradiction. Uniqueness is obvious as the components are uniquely defined by the property that they are the maximal irreducible closed subsets.

Once more, irreducible components of a noetherian topological space are the maximal irreducible closed subsets. □

2.6. **Commutative algebra language.** Prime ideals in the algebra of regular functions on an affine variety correspond to irreducible closed subsets. Thus, decomposition of a variety into irreducible components can be formulated in terms of commutative algebra.

2.6.1. **Proposition.** *Let A be the ring of regular functions on an affine variety. Then A has a finite number of minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_k$. Moreover, one has $\cap \mathfrak{p}_i = 0$.*

The result, with a basically same proof, holds for any noetherian commutative ring.

2.6.2. **Proposition.** *Let A be a noetherian commutative ring. Then A has a finite number of minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_k$. Moreover, one has $\cap \mathfrak{p}_i = N(A)$.*

2.6.3. *Proof of the propositions.* Let us show that $N(A)$ is the intersection of all prime ideals in A. In fact, for any prime $\mathfrak{p} \subset A$ $N(A) \subset \mathfrak{p}$. In the opposite direction, if f is not nilpotent, let $\mathcal{I}$ the the set of ideals that do not contain f^n for all n. It satisfies Zorn lemma, so $\mathcal{I}$ has a maximal element. Let us call it $\mathfrak{p}$. It is prime: if $a, b \notin \mathfrak{p}$ then $f^n \in (a)+\mathfrak{p}$, $f^m \in (b)+\mathfrak{p}$ so $f^{m+n} \in ((a)+\mathfrak{p})((b)+\mathfrak{p}) \subset \mathfrak{p}$.

We deduce that $N(A)$ is the intersection of the minimal primes in $\mathfrak{p}$. The fact that there is only a finite number of them follows from the noetherian property of $\mathtt{spec}_k(A)$ (in the setup of Proposition 2.6.1).

In the more general setup of 2.6.2 one should replace $\mathtt{spec}_k(A)$ with another topological space that plays the same role in Grothendieck's approach to algebraic geometry. We present below the definition.

2.6.4. **Definition.** Let A be a commutative ring. The spectrum of A, $\mathtt{Spec}(A)$ is the topological space whose underlying set is the set of prime ideals of A. Closed subsets of $\mathtt{Spec}(A)$ are of form

$$V(I) = \{\mathfrak{p} \in \mathtt{Spec}(A) | \mathfrak{p} \supset I\}$$

where I is an ideal of A.

When both notions are defined, $\mathtt{spec}_k(A) \subset \mathtt{Spec}(A)$. We will discuss the relation between the two later on. If A is a noetherian ring, $\mathtt{Spec}(A)$ is a noetherian topological space. That concludes the proof of 2.6.2.

3. Hilbert's theorems. Normalization lemma

In two papers on invariant theory published in 1890 and in 1893, Hilbert proved three famous results that bear his name. We will present here two of them. The third one (theorem on syzygies) will be mentioned later.

3.1. **Noetherian rings. Noetherian modules. Hilbert basis theorem.** A ring A is called noetherian (Emmy Noether, 1882–1935) if every its ideal is finitely generated. Examples include fields (no nontrivial ideals) and PID's (all ideals are generated by one element).

Equivalently, A is noetherian iff any ascending chain of ideals

$$I_1 \subset I_2 \subset \dots$$

stabilizes: $\exists n : I_{n+k} = I_n$ for any $k > 0$.

3.1.1. **Theorem** (Hilbert's basis theorem)**.** *Assume A is noetherian. Then $A[x]$ is also noetherian.*

Proof. Let $I \subset A[x]$ be an ideal. We define J_k as the set of $a \in A$ that appear as a leading coefficient of a degree k polynomial in I. It is easy to see that J_k is an ideal in A and that $J_k \subset J_{k+1}$. We denote $J = \cup J_k$. This is an ideal in A and $J = J_n$ for some n. The ideals J_k, $k = 0, \dots, n$ are finitely generated. Let $a_{k,1}, \dots, a_{k,m_k}$ be generators of J_k. We choose $f_{k,l}$ a degree k polynomial from I with the leading term $a_{k,l}$. We will now prove that the polynomials $f_{k,l}$ generate I. Let $f \in I$ be a degree d polynomial. We will prove, by induction in d, that f belongs to the ideal generated by $f_{r,s}$. If $d > n$, $J_d = J_n$, so there are $a_1, \dots, a_{m_n}$ such that $f - x^{d-n} \sum a_j f_{n,j}$ is in I and has a smaller degree.

If $d < n$, there are $a_1, \dots, a_{m_d}$ such that $f - \sum a_j f_{d,j}$ is in I and has a smaller degree. This proves the theorem. □

3.2. **Chain properties for modules.** Apart of rings, it is worth studying modules over them. A module over a ring A would be just a vector space, if A were a field.

Here is the definition.

3.2.1. **Definition.** Given a ring A, an A-module M is an abelian group endowed with a (left) multiplication by elements of A so that

1. $a(m + m') = am + am'$.
2. $(a + a')m = am + a'm$.
3. $a(bm) = (ab)m$.
4. $1m = m$.

3.2.2. **Example.** A is a module over A. We call it *a free rank one module*, the name will become clearer later.

The notions of submodule or of homomorphism of modules are quite clear.

The modules over a given ring A form a category, called the category of A-modules, denoted $\mathtt{Mod}_A$.

3.2.3. **Definition.** 1. A module M is said to satisfy ascending chain condition (acc) if any increasing chain of its submodules stabilizes.

2. A module M is said to satisfy descending chain condition (dcc) if any decreasing chain of its submodules stabilizes.

Another name for acc and dcc modules: noetherian and artinian (Emil Artin, 1898–1962). A ring is called noetherian (artinian) if it is noetherian (artinian) as a module over itself.

The following very easy property is left as an exercise.

3.2.4. **Proposition.** *Let M be a module, M' a submodule and $M' = M/M'$ the factor module. Then M satisfies acc (resp., dcc) iff M' and M'' satisfy this property.*

3.2.5. **Corollary.** *Any algebra of finite type over a field is noetherian. Any algebra of finite type over $\mathbb{Z}$ is noetherian.*

3.3. **Nullstellensatz.** The name Nullstellensatz means in German *theorem on zeroes.* As we have already seen, it implies that any meaningful system of equations over an algebraically closed field has a solution.

We will deduce the theorem from the following Zariski lemma.

3.3.1. **Theorem** (Zariski lemma)**.** *Let k be a field, $K \supset k$ a field extension that is finitely generated as k-algebra. Then K is a finite algebraic extension.*

We will present a very easy proof that only works when k is not countable. A proof for arbitrary k is based on different ideas that we postpone till **??**.

Proof. The fact that K is finitely generated as k-algebra means that $K = k[x_1, \dots, x_n]/\mathfrak{m}$ for some ideal $\mathfrak{m}$. Let $t \in K \setminus k$. The dimension of K as a vector space over k is at most countable as the dimension of $k[x_1, \dots, x_n]$ is at most countable. The elements $\frac{1}{t-a}$ cannot be linearly independent over k for different $a \in k$ as by the assumption k is not countable. Therefore, there is a finite number of them, linearly dependent,

$$\sum_{i=1}^{n} \frac{c_i}{t - a_i} = 0.$$

Multiplying the left-hand side by $\prod(t-a_i)$, we get a polynomial equation satisfied by t. This equation is nonzero as all its summands, except for the first one, are divisible by $t - a_1$, whereas the first summand is not divisible by $t - a_1$. Thus, we have verified that any element $t \in K$ is algebraic over k. Since $x_1, \dots, x_n$ are algebraic, they generate a finite field extension. □

Zariski lemma easily implies the following result called *the weak Nullstellensatz.*

3.3.2. **Corollary** (weak Nullstellensatz)**.** *Let k be an algebraically closed field, $I \neq k[x_1, \dots, x_n]$ be a proper ideal. Then the solution set $V(I)$ is nonempty.*

Proof. Let $\mathfrak{m}$ be a maximal ideal containing I (its existence is guaranteed by Zorn lemma). The factor ring $K = k[x_1, \dots, x_n]/\mathfrak{m}$ is a field finitely generated as algebra over k. Therefore, by Zariski lemma it is an algebraic extension of k. Since k is algebraically closed, $K = k$ and this proves that $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$ for some $a = (a_1, \dots, a_n) \in k^n$. □

Note the following reformulation of the same result.

3.3.3. **Corollary.** *Let $\mathfrak{m}$ be a maximal ideal of $k[x_1, \dots, x_n]$. Then the field $K = k[x_1, \dots, x_n]/\mathfrak{m}$ is a finite extension of k.*

We will now prove

3.3.4. **Theorem** (Nullstellensatz)**.** *Let k be an algebraically closed field, $I \subset k[x_1, \dots, x_n]$. Then $I(V(I)) = \sqrt{I}$. In other words, if a polynomial f vanishes at $V(I)$ then $f^n \in I$ for some n.*

The theorem can be deduced from the weak Nullstellensatz using the following *Rabinovitsch trick*.

Proof. Let $I = (f_1, \dots, f_m)$. Define a new ideal $J \subset k[x_0, x_1, \dots, x_n]$ generated by the polynomials $f_1, \dots, f_m$, and $x_0 f - 1$. By the assumption $V(J) = \emptyset$, as the assumption $(a_0, \dots, a_n) \in V(J)$ means that $(a_1, \dots, a_n) \in V(I)$ and $f(a_1, \dots, a_n)a_0 = 1$. Therefore, by the weak Nullstellensatz, $J = k[x_0, \dots, x_n]$, that is,

$$h_0(x_0 f - 1) + \sum h_i f_i = 1$$

for some $h_i \in k[x_0, \dots, x_n]$. Define the ring homomorphism

$$\alpha : k[x_0, \dots, x_n] \to K$$

to the field of rational functions $K := k(x_1, \dots, x_n)$ by the formula $\alpha(x_0) = \frac{1}{f}$, $\alpha(x_i) = x_i$ for $i > 0$. We get

$$\sum_{i=1}^{m} \alpha(h_i) f_i = 1.$$

The elements $\alpha(h_i)$ may have only a power of f in the denominator. So, multiplying both sides of the last equation by a power of f, we dedince that a power of f lies in $I = (f_1, \dots, f_m)$. This proves the theorem. □

3.3.5. *Quasicompactness.* A topological space X is called quasicompact if for any open cover $X = \cup U_i$ there is a finite subcover.

To avoid confusion: a compact topological space is one that is quasicompact and Hausdorff.

Let us show that if A is a reduced algebra of finite type over $k = \bar{k}$, $\mathtt{spec}_k(A)$ is quasicompact. Since $D(s)$, $s \in A$, form a base of the Zariski topology, it is enough to assume that we have an open covering of $X = \mathtt{spec}_k(A)$ by the

open sets $D(s)$, $s \in S$. Thus, $D(S) = X$ and we have to find a finite subset $S_0 \subset S$ such that $D(S_0) = X$. Equivalently, $D(S) = X$ means that $V(S) = \emptyset$. By the weak Nullstellensatz, this means that S generates the whole A, that is $1 = \sum_{i=1}^{n} a_i s_i$ for some finite set of $s_i \in S$. We can now put $S_0 = \{s_1, \dots, s_n\}$.

3.3.6. *Existence of affine varieties.* We promised to complete the proof of existence of affine varieties using Hilbert Nullstellensatz. Let A be a reduced algebra of finite type over $k = \bar{k}$ and let $X = \mathtt{spec}_k(A)$. We are now ready to prove that the evaluation map $ev : A \to \mathcal{O}_X(X)$ is a bijection.

3.3.7. **Proposition.** *The evaluation map $ev : A \to \mathcal{O}_X(X)$ is a bijection.*

Proof. Let $A = k[x_1, \dots, x_n]/I$ where $I = \sqrt{I}$. Then X identifies with $V(I)$. Evaluation map ev_x, $x \in X$, assigns to $f \in k[x_1, \dots, x_n]$ the value $f(x) \in k$. By Nullstellensatz, any polynomial vanishing at X belongs to I, so $\mathrm{Ker}(ev) = 0$. It remains to prove that any function in $\mathcal{O}_X(X)$ is represented by an element of A. Let $f \in \mathcal{O}_X(X)$, By definition, there is an open covering $X = \cup D(h_i)$ such that f is represented in $D(h_i)$ by a fraction $\frac{f_i}{g_i}$ for a collection of $f_i, g_i \in A$ such that $g_i(x) \neq 0$ for $x \in U(h_i)$. Since $D(h_i) = D(h_i g_i)$, we can assume that $h_i = g_i$ so f is presented by $\frac{f_i}{g_i}$ on $D(g_i)$. This implies that the function $g_i^2 f$ is represented by $g_i f_i$ on $D(g_i)$. Since both vanish outside of $D(g_i)$, $g_i^2 f$ is everywhere represented by $g_i f_i \in A$. Since $D(g_i) = D(g_i^2)$ cover the whole X, there exist a presentation $1 = \sum a_i g_i^2$. Then $f = 1 \cdot f = \sum a_i g_i^2 f = \sum a_i g_i f_i$ is represented by an element of A. □

3.4. **Noether normalization lemma.**

3.4.1. **Theorem.** *Let A be a finitely generated algebra over a field k. Then there exists a subring B of A isomorphic to a polynomial ring $k[x_1, \dots, x_d]$ such that A is a finitely generated B-module.*

We will only prove the result in the case k is infinite. It remain equally correct for finite fields, but the proof for finite fields is slightly more difficult.

We start with some simple general assertions about infinite fields.

3.4.2. **Lemma.** *Let k be an infinite field and let $f \in k[x_1, \dots, x_m]$ be a nonzero polynomial. The there exist $c_1, \dots, c_m \in k$ such that $f(c_1, \dots, c_m) \neq 0$.*

Proof. Induction in m. For $m = 0$ the claim is vacuous. If $m > 0$, write $f = \sum g_k x_m^k$ where g_k are polynomials in $x_1, \dots x_{m-1}$. There exist k such that $g_k \neq 0$ so there exist $c_1, \dots, c_{n-1}$ such that $f(c_1, \dots, c_{m-1}, x_n)$ is a nonzero polynomial of x_m. Since k is infinite, there exists c_m such that it does not vanish at $x_m = c_m$. □

3.4.3. **Corollary** (Preparation lemma)**.** *Let k be an infinite field and let $f \in k[x_1, \dots, x_n]$ be a nonconstant polynomial. Then there exists a change of variables*

$y_i = x_i - c_i x_n$, $i = 1, \dots, n-1$, $y_n = x_n$ *that presents* f *in the form*

$$f = c y_n^d + \sum_{i=0}^{d-1} f_i y_n^i \tag{3}$$

where $f_i \in k[y_1, \dots, y_{n-1}]$ *and* $c \neq 0$.

Proof. Let $f = \sum_{i=0}^{d} F_i$ where F_i is homogeneous of degree i and $F_d \neq 0$. Since the change of variables is homogeneous, we can safely assume that $f = F_d$ is homogeneous of degree $d > 0$. Then f/x_n^d is a polynomial $\phi(x_1/x_n, \dots, x_{n-1}/x_n)$. The claim follows by applying the previous lemma to ϕ. We get $\phi(c_1, \dots, c_{n-1}) \neq 0$ that implies (3). In fact, define the polynomial g so that $f(x_1, \dots, x_{n-1}, x_n) = g(x_1 - c_1 x_n, \dots, x_{n-1} - c_{n-1} x_n, x_n)$. The condition (3) means that $g(0, \dots, 0, 1) = c$ that is $f(c_1, \dots, c_{n-1}, 1) = \phi(c_1, \dots, -c_{n-1}) = c$.

□

Here is one more easy lemma.

3.4.4. **Lemma.** *Let $A \subset B \subset C$ be commutative rings. If B is a finitely generated A-module and C is a finitely generated B-module then A is finitely generated as an A-module.*

Proof. If $b_1, \dots, b_n$ generate B as A-module and $c_1, \dots, c_m$ generate C as B-module then $b_i c_j$ generate C as an A-module. □

Proof of the theorem. Let A be generated over k by $a_1, \dots, a_n$.

Here is an example of why this theorem is not obvious. We could try to define the algebra B as generated over k by a maximal set of algebraically independent generators among a_i. Let, for instance, $A = k[x, y]/(xy)$. The elements x, y generate A, x is algebraically independent (that is, there is no polynomial p in one variable such that $p(x) = 0$ in A), and y is dependent, since $xy = 0$. But y is not integral over $k[x]$ as the xy considered as a polynomial in y is not monic. So, one has to find a clever way of choosing the generators for B.

We will prove the assertion by induction in n. If all a_i are algebraically independent, A is a polynomial ring and there is nothing to prove. Otherwise $a_1, \dots, a_n$ satisfy some nontrivial polynomial equation $f(a_1, \dots, a_n) = 0$, where $0 \neq f \in k[x_1, \dots, x_n]$.

Using Preparation lemma, we can make a change of variables $a'_n = a_n, a'_i = a_i - c_i a_n$ so that a'_n is satisfies a polynomial equation of form (3). This implies that A is generated by $1, a'_n, \dots, (a'_n)^{d-1}$ for certain d, over $k[a'_1, \dots, a'_{n-1}]$. By the inductive hypothesis the latter ring is finitely generated as a module over a polynomial subring. By transitivity, A is finitely generated module over the same polynomial subring. □

References

[AM] M. Atiyah, I. Macdonald, Introduction to commutative algebra, Addison-Wesley, 1969

[H] R. Hartshorne, Algebraic geometry, Springer, GTM, 1977.

[K] G. Kempf, Algebraic varieties, Cambridge UP, 1993.

[M] Y. Manin, Introduction to the theory of schemes, Springer, 2018.

Email address: vhinich@gmail.com