INTRODUCTION TO ALGEBRAIC GEOMETRY

Notes of the course

Advanced Geometry 3

A.A. 2018/19

Emilia Mezzetti

Dipartimento di Matematica e Geoscienze
Università degli Studi di Trieste
Via Valerio 12/1
34127 Trieste, ITALY
e-mail: mezzette@units.it

Introduction

Algebraic Geometry is the field of mathematics that studies the sets of solutions of systems of algebraic equations, i.e. of equations given by polynomials. The origins of Algebraic Geometry go back to the Ancient Babylonians and Greeks and, since them, this fascinating subject has attracted mathematicians of every times and countries. During the 19^{th} and the beginning of last century, important progress has been made, mainly by the so-called Italian School of Algebraic Geometry. Then, starting from 1950, the subject was completely refounded, taking into account the advent of Modern Algebra. This work was initiated by Oscar Zariski (1899-1986), a mathematician of Russian origin, who studied in Italy and then moved to the USA, and pushed on mainly by the French mathematician Alexander Grothendieck (1928-2014). In the last fifty years, important results and answers to classical problems have been given.

An asterisk * near an exercise denotes that it is quoted in the text.

1. Affine and projective space.

Let K be a field. By definition, the *affine space* of dimension n over K is simply the set K^n : on it, the additive group of K^n acts naturally by translation. The affine space will be denoted $\mathbb{A}^n_K$ or simply $\mathbb{A}^n$. So the points of $\mathbb{A}^n_K$ are $n-$tuples $(a_1, \ldots, a_n)$, where $a_i \in K$ for $i = 1, \ldots, n$.

The natural *action* of K^n on $\mathbb{A}^n_K$, is the map t defined by

$$t : K^n \times \mathbb{A}^n_K \longrightarrow \mathbb{A}^n_K$$

$$((x_1, \ldots, x_n), (a_1, \ldots, a_n)) \longrightarrow (x_1 + a_1, \ldots, x_n + a_n).$$

Note that: $t(0, P) = P$, where 0 is the zero vector of K^n and $P \in \mathbb{A}^n_K$, and $t(w, t(v, P)) = t(v + w, P)$, for $v, w \in K^n$ and $P \in \mathbb{A}^n_K$.

The action of a vector v on a point P is "by translation". The point $t(v, P)$ will be denoted $P + v$. The action t is *faithful* and *transitive*: this means that, for any choice of $P, Q \in \mathbb{A}^n_K$, there exists one and only one $v \in V$ such that $Q = t(v, P)$: for this vector, the notation $Q - P$ will be sometimes used.

Let $Q \in \mathbb{A}^n_K$ be a point, and $W \subset K^n$ be a vector subspace. We define the *affine subspace* of $\mathbb{A}^n_K$ passing through Q with orienting space W (or of direction W) as follows:

$$S = \{P \in \mathbb{A}^n_K \mid P = Q + w, w \in W\}.$$

S can be seen as "W translated in Q". Note that affine subspaces of $\mathbb{A}^n_K$ do not necessarily pass through the origin. Two affine subspaces of $\mathbb{A}^n$ with a common orienting space are called parallel. If $\dim W = m$, we also define $\dim S = m$. The subspaces of dimension 1 are called *lines*, those of dimension 2 *planes*, those of dimension $n - 1$ (or of codimension 1) *hyperplanes*.

The points of an affine subspace of $\mathbb{A}^n$ can be characterized as solutions of a system of equations. These are of two types:

a) Parametric equations of a subspace.

Let S be the subspace passing through $Q(y_1, \ldots, y_n)$ with orienting space W, and let $w_1, \ldots, w_s$ be a basis of W, with $w_i = (w_{i1}, \ldots, w_{in})$. Then $P(x_1, \ldots, x_n) \in S$ if and only if there exist $t_1, \ldots, t_s \in K$ such that

$$(x_1, \ldots, x_n) = (y_1, \ldots, y_n) + t_1 w_1 + \ldots + t_s w_s,$$

or equivalently

$$\begin{cases} x_1 = y_1 + t_1 w_{11} + \ldots + t_s w_{s1} \\ x_2 = y_2 + t_1 w_{12} + \ldots + t_s w_{s2} \\ \ldots \\ \ldots \end{cases}$$

As $(t_1, \ldots, t_s)$ varies in K^s we get in this way all points of S.

For example, if S is the line through Q of direction $W = \langle w \rangle$, with $w = (b_1, \ldots, b_n)$, then

$$\begin{cases} x_1 = y_1 + tb_1 \\ x_2 = y_2 + tb_2 \\ \ldots \\ x_n = y_n + tb_n \end{cases}$$

are parametric equations of S.

b) Cartesian equations of a subspace.

Let $s = \dim W$, $W \subset K^n$, a vector subspace. Then W is the set of vectors whose coordinates are solutions of a homogeneous linear system of rank $n - s$ in n indeterminates $z_1, \ldots, z_n$:

$$\begin{cases} a_{11}z_1 + \ldots + a_{1n}z_n = 0 \\ \ldots \\ a_{n-s,1}z_1 + \ldots + a_{n-s,n}z_n = 0. \end{cases}$$

Hence $P(x_1, \ldots, x_n)$ belongs to S if and only if $P = Q + w$, where w is a solution of the previous system, i.e. if and only if the following equations are satisfied:

$$\begin{cases} a_{11}(x_1 - y_1) + \ldots + a_{1n}(x_n - y_n) = 0 \\ \ldots \\ a_{n-s,1}(x_1 - y_1) + \ldots + a_{n-s,n}(x_n - y_n) = 0 \end{cases}$$

i.e. $(x_1, \ldots, x_n)$ is a solution of the system:

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n + b_1 = 0 \\ \ldots \\ a_{n-s,1}x_1 + \ldots + a_{n-s,n}x_n + b_n \end{cases} = 0$$

where we have put $b_i = -(a_{i1}y_1 + \ldots + a_{in}y_n)$, for $i = 1, \ldots, n - s$. For example a hyperplane is represented by a unique linear equation of the form:

$$a_1x_1 + \ldots + a_nx_n + b = 0.$$

Let V be a $K-$vector space, of dimension $n + 1$. Let $V^* = V \setminus \{0\}$ be the subset of non–zero vectors. The following relation in V^* is an equivalence relation (relation of proportionality):

$v \sim v'$ if and only if $\exists \lambda \neq 0, \lambda \in K$ such that $v' = \lambda v$.

The quotient set $V^*/\sim$ is called the *projective space* associated to V and denoted $\mathbb{P}(V)$. The points of $\mathbb{P}(V)$ are the lines of V (through the origin) deprived of the origin. In particular, $\mathbb{P}(K^{n+1})$ is denoted $\mathbb{P}^n_K$ (or simply $\mathbb{P}^n$) and called the *numerical projective n-space*. By definition, the dimension of $\mathbb{P}(V)$ is equal to $\dim V - 1$.

There is a canonical surjection $p : V^* \to \mathbb{P}(V)$ which takes a vector v to its equivalence class $[v]$. If $(x_0, \ldots, x_n) \in (K^{n+1})^*$, then the corresponding point of $\mathbb{P}^n$ is denoted $[x_0, \ldots, x_n]$. So $[x_0, \ldots, x_n]$=$[x'_0, \ldots, x'_n]$ if and only if $\exists \lambda \in K^*$ such that $x'_0 = \lambda x_0, \ldots, x'_n = \lambda x_n$.

If a basis $e_0, \ldots, e_n$ of V is fixed, then a system of *homogeneous coordinates* is introduced in V, in the following way: if $v = x_0 e_0 + \ldots + x_n e_n$, then $x_0, \ldots, x_n$ are called homogeneous coordinates of the corresponding point $P = [v] = p(v)$ in $\mathbb{P}(V)$. We also write $P[x_0, \ldots, x_n]$. Note that homogeneous coordinates of a point P are not uniquely determined by P, but are defined only up to multiplication by a non–zero constant. If $\dim V = n + 1$, a system of homogeneous coordinates allows to define a *bijection*

$$\mathbb{P}(V) \longrightarrow \mathbb{P}^n$$

$$P = [v] \longrightarrow [x_0, \ldots, x_n]$$

where $v = x_0 e_0 + \ldots + x_n e_n$.

The points $E_0[1, 0, \ldots, 0], \ldots, E_n[0, 0, \ldots, 1]$ are called the fundamental points and $U[1, \ldots, 1]$ the unit point for the given system of coordinates.

A *projective* (or *linear*) *subspace* of $\mathbb{P}(V)$ is a subset of the form $\mathbb{P}(W)$, where $W \subset V$ is a subspace.

Assume that $\dim W = s + 1$ and that W is represented by a linear homogeneous system

$$(*) \begin{cases} a_{10}x_0 + \ldots + a_{1n}x_n = 0 \\ \ldots \\ a_{n-s,0}x_0 + \ldots + a_{n-s,n}x_n = 0. \end{cases}$$

Note that a $(n + 1)$-tuple $(\bar{x}_0, \ldots, \bar{x}_n)$ is a solution of the system if and only if $(\lambda\bar{x}_0, \ldots, \lambda\bar{x}_n)$ is, with $\lambda \neq 0$. So these solutions can also be interpreted as representing the points of $\mathbb{P}(W)$ and the equations (*) as a system of Cartesian equations of $\mathbb{P}(W)$. To write down parametric equations of $\mathbb{P}(W)$ it is enough to fix a basis of W, formed by vectors $w_0, \ldots, w_s$. Then a general point of $\mathbb{P}(W)$ is parametrically represented by $[\lambda_0 w_0 + \ldots + \lambda_s w_s]$, as $\lambda_0, \ldots, \lambda_s$ vary in $\mathbb{P}^s$.

If W, U are vector subspaces of V, the following *Grassmann relation* holds:

$$\dim U + \dim W = \dim(U \cap W) + \dim(U + W).$$

From this relation, observing that $\mathbb{P}(U \cap W) = \mathbb{P}(U) \cap \mathbb{P}(W)$, we get in $\mathbb{P}(V)$:

$$\dim \mathbb{P}(U) + \dim \mathbb{P}(W) = \dim(\mathbb{P}(U) \cap \mathbb{P}(W)) + \dim \mathbb{P}(U + W).$$

Note that $\mathbb{P}(U + W)$ is the minimal linear subspace of $\mathbb{P}(V)$ containing both $\mathbb{P}(U)$ and $\mathbb{P}(W)$: it is denoted $\mathbb{P}(U) + \mathbb{P}(W)$.

1.1. Example. Let $V = K^3$, $\mathbb{P}(V) = \mathbb{P}^2$, $U, W \subset K^3$ subspaces of dimension 2. Then $\mathbb{P}(U), \mathbb{P}(V)$ are lines in the projective plane. There are two cases:

(i) $U = W = U + W = U \cap W$;
(ii) $U \neq W$, $\dim U \cap W = 1$, $U + W = K^3$.
In case (i) the two lines in $\mathbb{P}^3$ coincide; in case (ii) $\mathbb{P}(U) \cap \mathbb{P}(W) = \mathbb{P}(U \cap W) = [v]$, if $v \neq 0$ is a vector generating $U \cap W$. Observe that *never* $\mathbb{P}(U) \cap \mathbb{P}(W) = \emptyset$.

Let $T \subset \mathbb{P}(V)$ be a non–empty set. The linear span $\langle T \rangle$ of T is the intersection of the projective subspaces of $\mathbb{P}(V)$ containing T, i.e. the minimum subspace containing T. For example, if $T = \{P_1, \ldots, P_t\}$, a finite set, then $\langle P_1, \ldots, P_t \rangle = \mathbb{P}(W)$, where W is the vector subspace of V generated by vectors $v_1, \ldots, v_t$ such that $P_1 = [v_1], \ldots, P_t = [v_t]$. So $\dim\langle P_1, \ldots, P_t \rangle \leq t - 1$ and equality holds if and only if $v_1, \ldots, v_t$ are linearly independent; in this case, also the points $P_1, \ldots, P_t$ are called *linearly independent*. In particular, for $t = 2$, two points are linearly independent if they generate a line, for $t = 3$, three points are linearly independent if they generate a plane, etc. It is clear that, if $P_1, \ldots, P_t$ are linearly independent, then $t \leq n + 1$, and any subset of $\{P_1, \ldots, P_t\}$ is formed by linearly independent points.

$P_1, \ldots, P_t$ are said to be *in general position* if either $t \leq n + 1$ and they are linearly independent or $t > n + 1$ and any $n + 1$ points among them are linearly independent.

1.2. Proposition. *The fundamental points $E_0, \ldots, E_n$ and the unit point U of a system of homogeneous coordinates on $\mathbb{P}^n$ are $n + 2$ points in general position. Conversely, if $P_0, \ldots, P_n, P_{n+1}$ are $n + 2$ points in general position, then there exists a system of homogeneous coordinates in which $P_0, \ldots, P_n$ are the fundamental points and P_{n+1} is the unit point.*

Proof. If $e_0, \ldots, e_n$ is a basis, then clearly the $n+1$ vectors $e_0, \ldots, \hat{e_i}, \ldots, e_n, e_0 + \ldots + e_n$ are linearly independent: this proves the first claim. To prove the second claim, we fix vectors $v_0, \ldots, v_{n+1}$ such that $P_i = [v_i]$ for all i. So $v_0, \ldots, v_n$ is a basis and there exist $\lambda_0, \ldots, \lambda_n$ in K such that $v_{n+1} = \lambda_0 v_0 + \ldots + \lambda_n v_n$. The assumption of general position easily implies that $\lambda_0, \ldots, \lambda_n$ are all different from 0, hence $\lambda_0 v_0, \ldots, \lambda_n v_n$ is a new basis such $[\lambda_i v_i] = P_i$ and P_{n+1} is the corresponding unit point. □

Let $H_0 = \langle E_1, \ldots, E_n \rangle, H_1 = \langle E_0, E_2, \ldots, E_n \rangle, \ldots, H_n = \langle E_0, \ldots, E_{n-1} \rangle$ be $n+1$ hyperplanes in $\mathbb{P}^n$. Note that the equation of H_i is simply $x_i = 0$. These hyperplanes are called the *fundamental hyperplanes*. Let $U_i = \mathbb{P}^n \setminus H_i = \{P[x_0, \ldots, x_n] \mid x_i \neq 0\}$. Note that $\mathbb{P}^n = U_0 \cup U_1 \cup \ldots \cup U_n$, because no point in $\mathbb{P}^n$ has all coordinates equal to zero. There is a map $\phi_0 : U_0 \longrightarrow \mathbb{A}^n (= K^n)$ defined by $\phi_0([x_0, \ldots, x_n]) = (\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})$. ϕ_0 is bijective and the inverse map is $j_0 : \mathbb{A}^n \longrightarrow U_0$ such that $j_0(y_1, \ldots, y_n) = [1, y_1, \ldots, y_n]$.

So ϕ_0 and j_0 establish a bijection between the affine space $\mathbb{A}^n$ and the subset U_0 of the projective space $\mathbb{P}^n$. There are other similar maps ϕ_i and j_i for $i = 1, \ldots, n$. So $\mathbb{P}^n$ is covered by $n + 1$ subsets, each one in natural bijection with $\mathbb{A}^n$.

There is a natural way of thinking of $\mathbb{P}^n$ as a completion of $\mathbb{A}^n$; this is done by identifying $\mathbb{A}^n$ with U_i via ϕ_i, and by interpreting the points of $H_i(= \mathbb{P}^n \setminus U_i)$ as *points at infinity* of $\mathbb{A}^n$, or directions in $\mathbb{A}^n$. We do this explicity for $i = 0$. First of all we identify $\mathbb{A}^n$ with U_0 via ϕ_0 and j_0. So if $P[a_0, \ldots, a_n] \in \mathbb{P}^n$, either $a_0 \neq 0$ and $P \in \mathbb{A}^n$, or $a_0 = 0$ and $P[0, a_1, \ldots, a_n] \notin \mathbb{A}^n$. Then we consider in $\mathbb{A}^n$ the line L, passing through $O(0, \ldots, 0)$ and of direction given by the vector $(a_1, \ldots, a_n)$. Parametric equations for L are the following:

$$\begin{cases} x_1 = a_1 t \\ x_2 = a_2 t \\ \ldots \\ x_n = a_n t \end{cases}$$

with $t \in K$. The points of L are identified with points of U_0 (via j_0) with homogeneous coordinates $x_0, \ldots, x_n$ given by:

$$\begin{cases} x_0 = 1 \\ x_1 = a_1 t \\ x_2 = a_2 t \\ \ldots \end{cases}$$

or equivalently, if $t \neq 0$, by:

$$\begin{cases} x_0 = \frac{1}{t} \\ x_1 = a_1 \\ x_2 = a_2 \\ \ldots \end{cases}.$$

Now, roughly speaking, if t *tends to infinity*, this point goes to $P[0, a_1, \ldots, a_n]$. Clearly this is not a rigorous argument, but just a hint to the intuition.

In this way $\mathbb{P}^n$ can be interpreted as $\mathbb{A}^n$ with the points at infinity added, each point at infinity corresponding to one direction in $\mathbb{A}^n$.

Exercise to §1.

1*. Let V be a vector space of finite dimension over a field K. Let $\check{V}$ denote the dual of V. Prove that $\mathbb{P}(\check{V})$ can be put in bijection with the set of the hyperplanes of $\mathbb{P}(V)$ (hint: the kernel of a non-zero linear form on V is a subvector space of V of codimension one).

2. Algebraic sets.

Roughly speaking, algebraic subsets of the affine or of the projective space are sets of solutions of systems of algebraic equations, i.e. common roots of sets of polynomials.

Examples of algebraic sets are: linear subspaces of both the affine and the projective space, plane algebraic curves, quadrics, graphics of polynomials functions, ...

Algebraic geometry is the branch of mathematics which studies algebraic sets (and their generalizations). Our first aim is *to give a formal definition of algebraic sets*.

Let $K[x_1, \ldots, x_n]$ be the polynomial ring in n variables over the field K. If $P(a_1, \ldots, a_n) \in \mathbb{A}^n$, and $F = F(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, we can consider the value of F at P, i.e. $F(P) = F(a_1, \ldots, a_n) \in K$. We say that P is a *zero of* F if $F(P) = 0$.

For example the points $P_1(1, 0)$, $P_2(-1, 0)$, $P_3(0, 1)$ are zeroes of $F = x_1^2 + x_2^2 - 1$ over any field. If $G = x_1^2 + x_2^2 + 1$ then G has no zeroes in $\mathbb{A}^2_{\mathbb{R}}$, but it does have zeroes in $\mathbb{A}^2_{\mathbb{C}}$.

2.1. Definition. A subset X of $\mathbb{A}^n_K$ is an *affine algebraic set* if X is the set of common zeroes of a family of polynomials of $K[x_1, \ldots, x_n]$.

This means that there exists a subset $S \subset K[x_1, \ldots, x_n]$ such that

$$X = \{P \in \mathbb{A}^n \mid F(P) = 0 \ \forall \ F \in S\}.$$

In this case X is called the zero set of S and is denoted $V(S)$ (or in some books $Z(S)$, e.g. this is the notation of Hartshorne's book). In particular, if $S = \{F\}$, then $V(S)$ will be simply denoted by $V(F)$.

2.2. Examples and remarks.

1. $S = K[x_1, \ldots, x_n]$: then $V(S) = \emptyset$, because S contains non–zero constants.
2. $S = \{0\}$: then $V(S) = \mathbb{A}^n$.
3. $S = \{xy - 1\}$: then $V(xy - 1)$ is the hyperbola.
4. If $S \subset T$, then $V(S) \supset V(T)$.

Let $S \subset K[x_1, \ldots, x_n]$ be a set of polynomials, let $\alpha := \langle S \rangle$ be the ideal generated by S. Recall that $\alpha = \{$finite sums of products of the form HF where $F \in S$, $H \in K[x_1, \ldots, x_n]\}$.

2.3. Proposition. $V(S) = V(\alpha)$.

Proof. If $P \in V(\alpha)$, then $F(P) = 0$ for any $F \in \alpha$; in particular for any $F \in S$ because $S \subset \alpha$.

Conversely, if $P \in V(S)$, let $G = \sum_i H_i F_i$ be a polynomial of α ($F_i \in S \ \forall \ i$). Then $G(P) = (\sum H_i F_i)(P) = \sum H_i(P) F_i(P) = 0$. □

The above Proposition is important in view of the following:

Hilbert' Basis Theorem. *If R is a Noetherian ring, then the polynomial ring $R[x]$ is Noetherian.*

Proof. Assume by contradiction that $R[x]$ is not Noetherian. Let $I \subset R[x]$ be a not finitely generated ideal. Let $f_1 \in I$ be a non-zero polynomial of minimum degree. We define by induction as follows a sequence $\{f_k\}_{k \in \mathbb{N}}$ of polynomials: if

f_k ($k \geq 1$) has already been chosen, let f_{k+1} be a polynomial of minimum degree in $I \setminus \langle f_1, \ldots, f_k \rangle$. Let n_k be the degree of f_k and a_k be its leading coefficient. Note that, by the very choice of f_k, the chain of the degrees is increasing: $n_1 \leq n_2 \leq \ldots$.

We will prove now that $\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \ldots$ is a chain of ideals, that does not become stationary: this will give the required contradiction. Indeed, if $\langle a_1, \ldots, a_r \rangle = \langle a_1, \ldots, a_r, a_{r+1} \rangle$, then $a_{r+1} = \sum_{i=1}^{r} b_i a_i$, for suitable $b_i \in R$. In this case, we consider the element $g := f_{r+1} - \sum_{i=1}^{r} b_i x^{n_{r+1}-n_i} f_i$: g belongs to I, but $g \notin \langle f_1, \ldots, f_r \rangle$, and its degree is strictly lower than the degree of f_{r+1}: contradiction. □

2.4. Corollary. *Any affine algebraic set $X \subset \mathbb{A}^n$ is the zero set of a finite number of polynomials, i.e. there exist $F_1, \ldots, F_r \in K[x_1, \ldots, x_n]$ such that $X = V(F_1, \ldots, F_r)$.*

□

Note that $V(F_1, \ldots, F_r) = V(F_1) \cap \ldots \cap V(F_r)$, so every algebraic set is a finite intersection of algebraic sets of the form $V(F)$, i.e. zeroes of a unique polynomial F. If $F = 0$, then $V(0) = \mathbb{A}^n$; if $F = c \in K \setminus \{0\}$, then $V(c) = \emptyset$; if *deg* $F > 0$, then $V(F)$ is called a *hypersurface*.

2.5. Proposition. *The affine algebraic sets of $\mathbb{A}^n$ satisfy the axioms of the closed sets of a topology, called the Zariski topology.*

Proof. It is enough to check that finite unions and arbitrary intersections of algebraic sets are again algebraic sets.

Let $V(\alpha), V(\beta)$ be two algebraic sets, with α, β ideals of $K[x_1, \ldots, x_n]$. Then $V(\alpha) \cup V(\beta) = V(\alpha \cap \beta) = V(\alpha\beta)$, where $\alpha\beta$ is the product ideal, defined by:

$$\alpha\beta = \{\sum_{\text{fin}} a_i b_i \mid a_i \in \alpha, b_i \in \beta\}.$$

In fact: $\alpha\beta \subset \alpha \cap \beta$ so $V(\alpha \cap \beta) \subset V(\alpha\beta)$, and both $\alpha \cap \beta \subset \alpha$ and $\alpha \cap \beta \subset \beta$ so $V(\alpha) \cup V(\beta) \subset V(\alpha \cap \beta)$. Assume now that $P \in V(\alpha\beta)$ and $P \notin V(\alpha)$: hence $\exists F \in \alpha$ such that $F(P) \neq 0$; on the other hand, if $G \in \beta$ then $FG \in \alpha\beta$ so $(FG)(P) = 0 = F(P)G(P)$, which implies $G(P) = 0$.

Let $V(\alpha_i), i \in I$, be a family of algebraic sets, $\alpha_i \subset K[x_1, \ldots, x_n]$. Then $\cap_{i \in I} V(\alpha_i) = V(\sum_{i \in I} \alpha_i)$, where $\sum_{i \in I} \alpha_i$ is the sum ideal of α_i's. In fact $\alpha_i \subset \sum_{i \in I} \alpha_i \ \forall i$, hence $V(\sum_i \alpha_i) \subset V(\alpha_i) \ \forall i$ and $V(\sum_i \alpha_i) \subset \cap_i V(\alpha_i)$. Conversely, if $P \in V(\alpha_i) \ \forall i$, and $F \in \sum_i \alpha_i$, then $F = \sum_i F_i$; therefore $F(P) = \sum F_i(P) = 0$.

□

2.6. Examples.

1. The Zariski topology of the affine line $\mathbb{A}^1$.

Let us recall that the polynomial ring $K[x]$ in one variable is a PID (principal ideal domain), so every ideal $I \subset K[x]$ is of the form $I = \langle F \rangle$. Hence every closed subset of $\mathbb{A}^1$ is of the form $X = V(F)$, the set of zeroes of a unique polynomial $F(x)$. If $F = 0$, then $V(F) = \mathbb{A}^1$, if $F = c \in K^*$, then $V(F) = \emptyset$, if $\deg F = d > 0$, then F can be decomposed in linear factors in polynomial ring over the algebraic closure of K; it follows that $V(F)$ has at most d points.

We conclude that the closed sets in the Zariski topology of $\mathbb{A}^1$ are: $\mathbb{A}^1$, $\emptyset$ and the finite sets.

2. If $K = \mathbb{R}$ or $\mathbb{C}$, then the Zariski topology and the Euclidean topology on $\mathbb{A}^n$ can be compared, and it results that the Zariski topology is coarser. Indeed every open set in the Zariski topology is open also in the usual topology. Let $X = V(F_1, \ldots, F_r)$ be a closed set in the Zariski topology, and $U := \mathbb{A}^n \setminus X$; if $P \in U$, then $\exists\ F_i$ such that $F_i(P) \neq 0$, so there exists an open neighbourhood of P in the usual topology in which F_i does not vanish.

Conversely, there exist closed sets in the usual topology which are not Zariski closed, for example the balls. The first case, of an interval in the real affine line, follows from part 1.

We want to define now the projective algebraic sets in $\mathbb{P}^n$. Let $K[x_0, x_1, \ldots, x_n]$ be the polynomial ring in $n+1$ variables. Fix a polynomial $G(x_0, x_1, \ldots, x_n) \in K[x_0, x_1, \ldots, x_n]$ and a point $P[a_0, a_1, \ldots, a_n] \in \mathbb{P}^n$: then, in general,

$$G(a_0, \ldots, a_n) \neq G(\lambda a_0, \ldots, \lambda a_n),$$

so the value of G at P is not defined.

2.7. Example. Let $G = x_1 + x_0 x_1 + x_2^2$, $P[0,1,2] = [0,2,4] \in \mathbb{P}^2_{\mathbb{R}}$. So $G(0,1,2) = 1 + 4 \neq G(0,2,4) = 2 + 16$. But if $Q = [1,0,0] = [\lambda, 0, 0]$, then $G(1,0,0) = G(\lambda, 0, 0) = 0$ for all λ.

2.8. Definition. Let $G \in K[x_0, x_1, \ldots, x_n]$: G is *homogeneous of degree* d, or G is *a form* of degree d, if G is a linear combination of monomials of degree d.

2.9. Lemma. *If G is homogeneous of degree d, $G \in K[x_0, x_1, \ldots, x_n]$, and t is a new variable, then $G(tx_0, \ldots, tx_n) = t^d G(x_0, \ldots, x_n)$.*

Proof. It is enough to prove the equality for monomials, i.e. for

$$G = a x_0^{i_0} x_1^{i_1} \ldots x_n^{i_n} \text{ with } i_0 + i_1 + \ldots + i_n = d :$$

$G(tx_0, \ldots, tx_n) = a(tx_0)^{i_0}(tx_1)^{i_1} \ldots (tx_n)^{i_n} = a t^{i_0 + i_1 + \ldots + i_n} x_0^{i_0} x_1^{i_1} \ldots x_n^{i_n} =$
$= t^d G(x_0, \ldots, x_n)$.

□

2.10. Definition. Let G be a homogeneous polynomial of $K[x_0, x_1, \ldots, x_n]$. A point $P[a_0, \ldots, a_n] \in \mathbb{P}^n$ is a *zero of* G if $G(a_0, \ldots, a_n) = 0$. In this case we write $G(P) = 0$.

Note that by Lemma 2.9 if $G(a_0, \ldots, a_n) = 0$, then

$$G(\lambda a_0, \ldots, \lambda a_n) = \lambda^{\deg G} G(a_0, \ldots, a_n) = 0$$

for every choice of $\lambda \in K^*$.

2.11. Definition. A subset Z of $\mathbb{P}^n$ is a *projective algebraic set* if Z is the set of common zeroes of a set of homogeneous polynomials of $K[x_0, x_1, \ldots, x_n]$.

If T is such a subset of $K[x_0, x_1, \ldots, x_n]$, then the corresponding algebraic set will be denoted by $V_P(T)$.

Let $\alpha = \langle T \rangle$ be the ideal generated by the (homogeneous) polynomials of T. If $F \in \alpha$, then $F = \sum_i H_i F_i$, $F_i \in T$: if $P \in V_P(T)$, and $P[a_0, \ldots, a_n]$, then $F(a_0, \ldots, a_n) = \sum H_i(a_0, \ldots, a_n) F_i(a_0, \ldots, a_n) = 0$, for any choice of coordinates of P, regardless if F is homogeneous or not. We say that P is a *projective zero* of F.

If F is a polynomial, then F can be written *in a unique way* as a sum of homogeneous polynomials, called the homogeneous components of F: $F = F_0 + F_1 + \ldots + F_d$. More in general, we give the following:

2.12. Definition. Let A be a ring. A is called *a graded ring over* $\mathbb{Z}$ if there exists a family of additive subgroups $\{A_i\}_{i \in \mathbb{Z}}$ such that $A = \oplus_{i \in \mathbb{Z}} A_i$ and $A_i A_j \subset A_{i+j}$ for all pair of indices.

The elements of A_i are called *homogeneous of degree* i and A_i is the homogeneous component of degree i. The standard example of graded ring is the polynomial ring with coefficients in a ring R. In this case the homogeneous components of negative degrees are all zero.

2.13 Proposition - Definition. *Let $I \subset A$ be an ideal of a graded ring. I is called* **homogeneous** *if the following equivalent conditions are fulfilled:*
(i) I is generated by homogeneous elements;
(ii) $I = \oplus_{k \in \mathbb{Z}} (I \cap A_k)$, i.e. if $F = \Sigma_{k \in \mathbb{Z}} F_k \in I$, then all homogeneous components F_k of F belong to I.

Proof of the equivalence.

"(ii)⇒(i)": given a system of generators of I, write each of them as sum of its homogeneous components: $F_i = \Sigma_{k \in \mathbb{Z}} F_{ik}$. Then a set of homogeneous generators of I is formed by all the elements F_{ik}.

"(i)⇒(ii)": let I be generated by a family of homogeneous elements $\{G_\alpha\}$, with $\deg G_\alpha = d_\alpha$. If $F \in I$, then F is a combination of the elements G_α with suitable coefficients H_α; write each H_α as sum of its homogeneous components: $H_\alpha = \Sigma H_{\alpha k}$. Note that the product $H_{\alpha k} G_\alpha$ is homogeneous of degree $k + d_\alpha$. By

the unicity of the expression of F as sum of homogeneous elements, it follows that all of them are combinations of the generators $\{G_\alpha\}$ and therefore they belong to I. □

Let $I \subset K[x_0, x_1, \ldots, x_n]$ be a homogeneous ideal. Note that, by the noetherianity, I admits a finite set of homogeneous generators.

Let $P[a_0, \ldots, a_n] \in \mathbb{P}^n$. If $F \in I$, $F = F_0 + \ldots + F_d$, then $F_0 \in I, \ldots, F_d \in I$. We say that P *is a zero of* I if P is a projective zero of any polynomial of I or, equivalently, of any homogeneous polynomial of I. This also means that P is a zero of any homogeneous polynomial of a set generating I. The set of zeroes of I will be denoted $V_P(I)$: all projective algebraic subsets of $\mathbb{P}^n$ are of this form.

As in the affine case, the projective algebraic subsets of $\mathbb{P}^n$ satisfy the axioms of the closed sets of a topology called the Zariski topology of $\mathbb{P}^n$ (see also Exercise 3).

Note that also all subsets of $\mathbb{A}^n$ and $\mathbb{P}^n$ have a structure of topological space, with the induced topology, which is still called the Zariski topology.

Exercises to §2.

1. Let $F \in K[x_1, \ldots, x_n]$ be a non–constant polynomial. The set $\mathbb{A}^n \setminus V(F)$ will be denoted $\mathbb{A}^n_F$. Prove that $\{\mathbb{A}^n_F | F \in K[x_1, \ldots, x_n] \setminus K\}$ is a topology basis for the Zariski topology.

2. Let $B \subset \mathbb{R}^n$ be a ball. Prove that B is not Zariski closed.

3*. Let I, J be homogeneous ideals of $K[x_0, x_1, \ldots, x_n]$. Prove that $I + J$, IJ and $I \cap J$ are homogeneous ideals.

4*. Prove that the map $\phi : \mathbb{A}^1 \to \mathbb{A}^3$ defined by $t \to (t, t^2, t^3)$ is a homeomorphism between $\mathbb{A}^1$ and its image, for the Zariski topology.

5. Let $X \subset \mathbb{A}^2_{\mathbb{R}}$ be the graph of the map $\mathbb{R} \to \mathbb{R}$ such that $x \to \sin x$. Is X closed in the Zariski topology? (hint: intersect X with a line....)

3. Examples of algebraic sets.

a) In the Zariski topology both of $\mathbb{A}^n$ and of $\mathbb{P}^n$ all points are closed.

If $P(a_1, \ldots, a_n) \in \mathbb{A}^n$: $P = V(x_1 - a_1, \ldots, x_n - a_n)$. If $P[a_0, \ldots, a_n] \in \mathbb{P}^n$: $P = V_P(\langle a_i x_j - a_j x_i \rangle_{i,j=0,\ldots,n})$.

Note that in the projective case the polynomials defining P as closed set are homogeneous. They can be seen as minors of order 2 of the matrix

$$\begin{pmatrix} a_0 & a_1 & \ldots & a_n \\ x_0 & x_1 & \ldots & x_n \end{pmatrix}$$

with entries in $K[x_0, x_1, \ldots, x_n]$.

b) Hypersurfaces.

Let us recall that the polynomial ring $K[x_1, \ldots, x_n]$ is a UFD (unique factorization domain), i. e. every non-constant polynomial F can be expressed in a unique way (up to the order and up to units) as $F = F_1^{r_1} F_2^{r_2} \ldots F_s^{r_s}$, where $F_1, \ldots, F_s$ are irreducible polynomials, two by two distinct, and $r_i \geq 1 \forall\ i = 1, \ldots, s$. Hence the hypersurface of $\mathbb{A}^n$ defined by F is

$$X := V(F) = V(F_1^{r_1} F_2^{r_2} \ldots F_s^{r_s}) = V(F_1 F_2 \ldots F_s) = V(F_1) \cup V(F_2) \cup \ldots \cup V(F_s).$$

The equation $F_1 F_2 \ldots F_s = 0$ is called the reduced equation of X. Note that $F_1 F_2 \ldots F_s$ generates the radical $\sqrt{F}$. If $s = 1$, X is called an irreducible hypersurface; by definition its degree is the degree of its reduced equation. Any hypersurface is a finite union of irreducible hypersurfaces.

In a similar way one defines hypersurfaces of $\mathbb{P}^n$, i. e. projective algebraic sets of the form $Z = V_P(G)$, with $G \in K[x_0, x_1, \ldots, x_n]$, G homogeneous. Since the irreducible factors of G are homogeneous (see Exercise 3.6), any projective hypersurface Z has a reduced equation (whose degree is, by definition, the degree of Z) and Z is a finite union of irreducible hypersurfaces. The degree of a projective hypersurface has the following important geometrical meaning.

3.1. Proposition. *Let K be an algebraically closed field. Let $Z \subset \mathbb{P}^n$ be a projective hypersurface of degree d. Then a line of $\mathbb{P}^n$, not contained in Z, meets Z at exactly d points, counting multiplicities.*

Proof. Let G be the reduced equation of Z and $L \subset \mathbb{P}^n$ be any line.

We fix two points on L: $A = [a_0, \ldots, a_n], B = [b_0, \ldots, b_n]$. So L admits parametric equations of the form

$$\begin{cases} x_0 = \lambda a_0 + \mu b_0 \\ x_1 = \lambda a_1 + \mu b_1 \\ \ldots \\ x_n = \lambda a_n + \mu b_n \end{cases}$$

The points of $Z \cap L$ are obtained from the homogeneous pairs $[\lambda, \mu]$ which are solutions of the equation $G(\lambda a_0 + \mu b_0, \ldots, \lambda a_n + \mu b_n) = 0$. If $L \subset Z$, then this equation is identical. Otherwise, $G(\lambda a_0 + \mu b_0, \ldots, \lambda a_n + \mu b_n)$ is a non-zero homogeneous polynomial of degree d in two variables. Being K algebraically closed, it can be factorized in linear factors:

$$G(\lambda a_0 + \mu b_0, \ldots, \lambda a_n + \mu b_n) = (\mu_1 \lambda - \lambda_1 \mu)^{d_1} (\mu_2 \lambda - \lambda_2 \mu)^{d_2} \ldots (\mu_r \lambda - \lambda_r \mu)^{d_r}$$

with $d_1 + d_2 + \ldots + d_r = d$. Every factor corresponds to a point in $Z \cap L$, to be counted with the same multiplicity as the factor. □

If K is not algebraically closed, considering the algebraic closure of K and using Proposition 3.1, we get that d is un upper bound on the number of points of $Z \cap L$.

c) Affine and projective subspaces.

The subspaces introduced in §1, both in the affine and in the projective case, are examples of algebraic sets.

d) Product of affine spaces.

Let $\mathbb{A}^n$, $\mathbb{A}^m$ be two affine spaces over the field K. The cartesian product $\mathbb{A}^n \times \mathbb{A}^m$ is the set of pairs (P, Q), $P \in \mathbb{A}^n$, $Q \in \mathbb{A}^m$: it is in natural bijection with $\mathbb{A}^{n+m}$ via the map

$$\phi : \mathbb{A}^n \times \mathbb{A}^m \longrightarrow \mathbb{A}^{n+m}$$

such that $\phi((a_1, \ldots, a_n), (b_1, \ldots, b_m)) = (a_1, \ldots, a_n, b_1, \ldots, b_m)$.

From now on we will always identify $\mathbb{A}^n \times \mathbb{A}^m$ with $\mathbb{A}^{n+m}$. We get two topologies on $\mathbb{A}^n \times \mathbb{A}^m$: the Zariski topology and the product topology.

3.1. Proposition. *The Zariski topology is strictly finer than the product topology.*

Proof. If $X = V(\alpha) \subset \mathbb{A}^n$, $\alpha \subset K[x_1, \ldots, x_n]$ and $Y = V(\beta) \subset \mathbb{A}^m$, $\beta \subset K[y_1, \ldots, y_m]$, then $X \times Y \subset \mathbb{A}^n \times \mathbb{A}^m$ is Zariski closed, precisely $X \times Y = V(\alpha \cup \beta)$ where the union is made in the polynomial ring in $n + m$ variables $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$. Hence, if $U = \mathbb{A}^n \setminus X$, $V = \mathbb{A}^m \setminus Y$ are open subsets of $\mathbb{A}^n$ and $\mathbb{A}^m$ in the Zariski topology, then $U \times V = \mathbb{A}^n \times \mathbb{A}^m \setminus ((\mathbb{A}^n \times Y) \cup (X \times \mathbb{A}^m))$ is open in $\mathbb{A}^n \times \mathbb{A}^m$ in the Zariski topology.

Conversely, we prove that $\mathbb{A}^1 \times \mathbb{A}^1 = \mathbb{A}^2$ contains some subsets which are Zariski open but are not open in the product topology. The proper open subsets in the product topology are of the form $\mathbb{A}^1 \times \mathbb{A}^1 \setminus \{$ finite unions of "vertical" and "horizontal" lines$\}$.

– Fig. 1 –

Let $X = \mathbb{A}^2 \setminus V(x-y)$: it is Zariski open but does not contain any non-empty subset of the above form, so it is not open in the product topology. There are similar examples in $\mathbb{A}^n \times \mathbb{A}^m$ for any n, m. □

Note that there is no similar construction for $\mathbb{P}^n \times \mathbb{P}^m$.

e) Embedding of $\mathbb{A}^n$ in $\mathbb{P}^n$.

Let H_i be the hyperplane of $\mathbb{P}^n$ of equation $x_i = 0$, $i = 0, \dots, n$; it is closed in the Zariski topology, and the complementar set U_i is open. So we have an open covering of $\mathbb{P}^n$: $\mathbb{P}^n = U_0 \cup U_1 \cup \dots \cup U_n$. Let us recall that for all i there is a bijection $\phi_i : U_i \to \mathbb{A}^n$ such that $\phi_i([x_0, \dots, x_i, \dots, x_n]) = (\frac{x_0}{x_i}, \dots, \hat{1}, \dots, \frac{x_n}{x_i})$. The inverse map is $j_i : \mathbb{A}^n \to U_i$ such that $j_i(y_1, \dots, y_n) = [y_1, \dots, 1, \dots, y_n]$.

3.2. Proposition. *The map ϕ_i is a homeomorphism, for $i = 0, \dots, n$.*

Proof. Assume $i = 0$ (the other cases are similar).

We introduce two maps:

(i) *dehomogeneization* of polynomials with respect to x_0.

It is a map ${}^a : K[x_0, x_1, \dots, x_n] \to K[y_1, \dots, y_n]$ such that

$$ {}^a(F(x_0, \dots, x_n)) = {}^aF(y_1, \dots, y_n) := F(1, y_1, \dots, y_n). $$

Note that ^{a} is a ring homomorphism.

(ii) *homogeneization* of polynomials with respect to x_0.

It is a map ${}^h : K[y_1, \dots, y_n] \to K[x_0, x_1, \dots, x_n]$ defined by

$$ {}^h(G(y_1, \dots, y_n)) = {}^hG(x_0, \dots, x_n) := x_0^{\deg G} G(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}) $$

.

${}^hG$ is always a homogeneous polynomial of the same degree as G. The map ^{h} is clearly not a ring homomorphism. Note that always ${}^a({}^hG) = G$ but in general ${}^h({}^aF) \neq F$; what we can say is that, if $F(x_0, \dots, x_n)$ is homogeneous, then $\exists r \geq 0$ such that $F = x_0^r({}^h({}^aF))$.

Let $X \subset U_0$ be closed in the topology induced by the Zariski topology of the projective space, i.e. $X = U_0 \cap V_P(I)$ where I is a homogeneous ideal of $K[x_0, x_1, \dots, x_n]$. Define ${}^aI = \{{}^aF \mid F \in I\}$: it is an ideal of $K[y_1, \dots, y_n]$ (because ^{a} is a ring homomorphism). We prove that $\phi_0(X) = V({}^aI)$. For: let $P[x_0, \dots, x_n]$ be a point of U_0; then $\phi_0(P) = (\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}) \in \phi_0(X) \iff P[x_0, \dots, x_n] = [1, \frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}] \in X = V_P(I) \iff F(1, \frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}) = 0 \ \forall \ {}^aF \in {}^aI \iff \phi_0(P) \in V({}^aI)$.

Conversely: let $Y = V(\alpha)$, α ideal of $K[y_1, \dots, y_n]$, be a Zariski closed set of $\mathbb{A}^n$. Let ${}^h\alpha$ be the homogeneous ideal of $K[x_0, x_1, \dots, x_n]$ generated by the set $\{{}^hG \mid G \in \alpha\}$. We prove that $\phi_0^{-1}(Y) = V_P({}^h\alpha) \cap U_0$. In fact: $[1, x_0, \dots, x_n] \in \phi_0^{-1}(Y) \iff (x_1, \dots, x_n) \in Y \iff G(x_1, \dots, x_n) = {}^hG(1, x_1, \dots, x_n) = 0 \ \forall \ G \in \alpha \iff [1, x_1, \dots, x_n] \in V_P({}^h\alpha)$. □

From now on we will often identify $\mathbb{A}^n$ with U_0 via ϕ_0 (and similarly with U_i via ϕ_i). So if $P[x_0,\dots,x_n] \in U_0$, we will refer to $x_0,\dots,x_n$ as the homogeneous coordinates of P and to $\frac{x_1}{x_0},\dots,\frac{x_n}{x_0}$ as the non–homogeneous or affine coordinates of P.

Exercises to §3.

1*. Let $n \geq 2$. Prove that, if K is an algebraically closed field, then in $\mathbb{A}^n_K$ both any hypersurface and any complementar set of a hypersurface have infinitely many points.

2. Prove that the Zariski topology on $\mathbb{A}^n$ is T_1.

3*. Let $F \in K[x_0,x_1,\dots,x_n]$ be a homogeneous polynomial. Check that its irreducible factors are homogeneous. (hint: consider a product of two polynomials not both homogeneous...)

4. The ideal of an algebraic set and the Hilbert Nullstellensatz.

Let $X \subset \mathbb{A}^n$ be an algebraic set, $X = V(\alpha)$, $\alpha \subset K[x_1,\dots,x_n]$. The ideal α defining X is not unique: for example, let $X = \{0\} \subset \mathbb{A}^2$; then $0 = V(x_1,x_2) = V(x_1^2,x_2) = V(x_1^2,x_2^3) = V(x_1^2,x_1,x_2,x_2^2) = \dots$ Nevertheless, there is an ideal we can canonically associate to X, i.e. the biggest one. Precisely:

4.1. Definition. Let $Y \subset \mathbb{A}^n$ be any set.

The *ideal of* Y is $I(Y) = \{F \in K[x_1,\dots,x_n] \mid F(P) = 0 \text{ for any } P \in Y\} = \{F \in K[x_1,\dots,x_n] \mid Y \subset V(F)\}$: it is formed by all polynomials vanishing on Y. Note that $I(Y)$ is in fact an ideal.

For instance, if $P(a_1,\dots,a_n)$ is a point, then $I(P) = \langle x_1 - a_1,\dots,x_n - a_n\rangle$. Indeed all its polynomials vanish on P, and, on the other side, it is maximal.

The following relations follow immediately by the definition:

(i) if $Y \subset Y'$, then $I(Y) \supset I(Y')$;
(ii) $I(Y \cup Y') = I(Y) \cap I(Y')$;
(iii) $I(Y \cap Y') \supset I(Y) + I(Y')$.

Similarly, if $Z \subset \mathbb{P}^n$ is any set, the *homogeneous ideal of* Z is, by definition, the homogeneous ideal of $K[x_0,x_1,\dots,x_n]$ generated by the set $\{G \in K[x_0,x_1,\dots,x_n] \mid G \text{ is homogeneous and } V_P(G) \supset Z\}$. It is denoted $I_h(Z)$.

Relations similar to (i),(ii),(iii) are satisfied. $I_h(Z)$ is also the set of polynomials $F(x_0,\dots,x_n)$ such that every point of Z is a projective zero of F.

Let $\alpha \subset K[x_1,\dots,x_n]$ be an ideal. Let $\sqrt{\alpha}$ denote the radical of α, i.e. the ideal $\{F \in K[x_1,\dots,x_n] \mid \exists r \geq 1 \text{ s.t. } F^r \in \alpha\}$. Note that always $\alpha \subset \sqrt{\alpha}$; if equality holds, then α is called a *radical ideal*.

4.2. Proposition.

1) For any $X \subset \mathbb{A}^n$, $I(X)$ is a radical ideal.
2) For any $Z \subset \mathbb{P}^n$, $I_h(Z)$ is a homogeneous radical ideal.

Proof. 1) If $F \in \sqrt{I(X)}$, let $r \geq 1$ such that $F^r \in I(X)$: hence if $P \in X$, then $(F^r)(P) = 0 = (F(P))^r$ in the base field K. Therefore $F(P) = 0$.

2) is similar, taking into account that $I_h(Z)$ is a homogeneous ideal (see Exercise 4.7.). □

We can interpret I as a map from $\mathcal{P}(\mathbb{A}^n)$, the set of subsets of the affine space, to $\mathcal{P}(K[x_1, \ldots, x_n])$. On the other hand, V can be seen as a map in the opposite sense. We have:

4.3. Proposition. *Let $\alpha \subset K[x_1, \ldots, x_n]$ be an ideal, $Y \subset \mathbb{A}^n$ be any subset. Then:*
(i) $\alpha \subset I(V(\alpha))$;
(ii) $Y \subset V(I(Y))$;
(iii) $V(I(Y)) = \overline{Y}$: the closure of Y in the Zariski topology of $\mathbb{A}^n$.

Proof. (i) If $F \in \alpha$ and $P \in V(\alpha)$, then $F(P) = 0$, so $F \in I(V(\alpha))$.

(ii) If $P \in Y$ and $F \in I(Y)$, then $F(P) = 0$, so $P \in V(I(Y))$.

(iii) Taking closures in (ii), we get: $\overline{Y} \subset \overline{V(I(Y))} = V(I(Y))$. Conversely, let $X = V(\beta)$ be any closed set containing Y: $X = V(\beta) \supset Y$. Then $I(Y) \supset I(V(\beta)) \supset \beta$ by (i); we apply V again: $V(\beta) = X \supset V(I(Y))$ so any closed set containing Y contains $V(I(Y))$ so $\overline{Y} \supset V(I(Y))$. □

Similar properties relate homogeneous ideals of $K[x_0, x_1, \ldots, x_n]$ and subsets of $\mathbb{P}^n$; in particular, if $Z \subset \mathbb{P}^n$, then $V_P(I_h(Z)) = \overline{Z}$, the closure of Z in the Zariski topology of $\mathbb{P}^n$.

There does not exist any characterization of $I(V(\alpha))$ *in general.* We can only say that it is a radical ideal containing α, so it contains also $\sqrt{\alpha}$. To characterize $I(V(\alpha))$ we need some extra assumption on the base field.

4.4. Hilbert Nullstellensatz (Theorem of zeroes). *Let K be an algebraically closed field. Let $\alpha \subset K[x_1, \ldots, x_n]$ be an ideal. Then $I(V(\alpha)) = \sqrt{\alpha}$.*

Remark. The assumption on K is necessary. Let me recall that K is algebraically closed if any non–constant polynomial of $K[x]$ has at least one root in K, or, equivalently, if any irreducible polynomial of $K[x]$ has degree 1. So if K is not algebraically closed, there exists $F \in K[x]$, irreducible of degree $d > 1$. Therefore F has no zero in K, hence $V(F) \subset \mathbb{A}^1_K$ is empty. So $I(V(F)) = I(\emptyset) = \{G \in K[x] \mid \emptyset \subset V(G)\} = K[x]$. But $\langle F \rangle$ is a maximal ideal of $K[x]$, and $\langle F \rangle \subset \sqrt{\langle F \rangle}$. If $\langle F \rangle \neq \sqrt{\langle F \rangle}$, by the maximality $\sqrt{\langle F \rangle} = \langle 1 \rangle$, so $\exists r \geq 1$ such that $1^r = 1 \in \langle F \rangle$, which is false. Hence $\sqrt{\langle F \rangle} = \langle F \rangle \neq K[x] = I(V(F))$.

We will deduce the proof of Hilbert Nullestellensatz, after several steps, from another very important theorem, known as the "Emmy Noether normalization Lemma".

We start with some definitions.

Let $K \subset E$ be fields, K a subfield of E. Let $\{z_i\}_{i\in I}$ be a family of elements of E.

4.5.Definition. The family $\{z_i\}_{i\in I}$ is *algebraically free* over K or, equivalently, the elements z_i's are *algebraically independent* over K if there does not exist any non–zero polynomial $F \in K[x_i]_{i\in I}$, the polynomial ring in a set of variables indexed on I, such that F vanishes in the elements of the family $\{z_i\}$.

For example: if the family is formed by one element z, $\{z\}$ is algebraically free over K if and only if z is transcendental over K. The family $\{\pi, \sqrt{\pi}\}$ is not algebraically free over $\mathbb{Q}$: it satisfies the non–trivial relation $x_1^2 - x_2 = 0$.

By convention, the empty family is free over any field K.

Let $\mathcal{S}$ be the set of the families of elements of E, which are algebraically free over K. $\mathcal{S}$ is a non–empty set, partially ordered by inclusion and inductive. By Zorn's lemma, there exist in $\mathcal{S}$ maximal elements, i.e. algebraically free families such that they do not remain free if any element of E is added. Any such maximal algebraically free family is called a *transcendence basis* of E over K. It can be proved that, if B, B' are two transcendence bases, then they have the same cardinality, called the *transcendence degree* of E over K. It is denoted $tr.d.E/K$.

4.6. Definition. A *K–algebra* is a ring A containing (a subfield isomorphic to) K.

Let $y_1, \ldots, y_n$ be elements of E: the *K–algebra generated by $y_1, \ldots, y_n$* is, by definition, the minimum subring of E containing $K, y_1, \ldots, y_n$: it is denoted $K[y_1, \ldots, y_n]$ and its elements are polynomials in the elements $y_1, \ldots, y_n$ with coefficients in K. Its quotient field $K(y_1, \ldots, y_n)$ is the minimum subfield of E containing $K, y_1, \ldots, y_n$.

A *finitely generated K–algebra A* is a K–algebra such that there exist elements of A $y_1, \ldots, y_r$ which verify the condition $A = K[y_1, \ldots, y_r]$.

4.7. Proposition. *There exists a transcendence basis of $K(y_1, \ldots, y_n)$ over K contained in the set $\{y_1, \ldots, y_n\}$.*

Proof. Let $\mathcal{S}$ be the set of the subfamilies of $\{y_1, \ldots, y_n\}$ formed by algebraically independent elements: $\mathcal{S}$ is a finite set so it possesses maximal elements with respect to the inclusion. We can assume that $\{y_1, \ldots, y_r\}$ is such a maximal family. Then $y_{r+1}, \ldots, y_n$ are each one algebraic over $K(y_1, \ldots, y_r)$ so $K(y_1, \ldots, y_n)$ is an algebraic extension of $K(y_1, \ldots, y_r)$. If $z \in K(y_1, \ldots, y_n)$ is any element, then z is algebraic over $K(y_1, \ldots, y_r)$, so the family $\{y_1, \ldots, y_r, z\}$ is not algebraically free.

□

4.8. Corollary. *tr.d.*$K(y_1, \ldots, y_n)/K \leq n$. □

Let now $A \subset B$ be rings, A a subring of B. Let $b \in B$: b is *integral over* A if it is a root of a monic polynomial of $A[x]$, i.e. there exist $a_1, \ldots, a_n \in A$ such that

$$b^n + a_1 b^{n-1} + a_2 b^{n-2} + \ldots + a_n = 0.$$

Such a relation is called an integral equation for b over A.

Note that, if A is a field, then b is integral over A if and only if b is algebraic over A.

B is called *integral over* A, or an integral extension of A, if and only if b is integral over A for every $b \in B$.

We can state now the

4.9. Normalization Lemma. *Let A be a finitely generated K–algebra and an integral domain. Let $r :=$ tr.d.$K(y_1, \ldots, y_n)/K$. Then there exist elements $z_1, \ldots, z_r \in A$, algebraically independent over K, such that A is integral over $K[z_1, \ldots, z_r]$.*

Proof. See, for instance, Lang [6]. □

We start now the proof of the Nullstellensatz.

1^{st} **Step.**

Let K be an algebraically closed field, let $\mathcal{M} \subset K[x_1, \ldots, x_n]$ be a maximal ideal. Then, there exist $a_1, \ldots, a_n \in K$ such that $\mathcal{M} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$.

Proof. Let K' be the quotient ring $\frac{K[x_1,\ldots,x_n]}{\mathcal{M}}$: it is a field because $\mathcal{M}$ is maximal, and a finitely generated K–algebra (by the residues in K' of $x_1, \ldots, x_n$). By the Normalization Lemma, there exist $z_1, \ldots, z_r \in K'$, algebraically independent over K', such that K' is integral over $A := K[z_1, \ldots, z_r]$. We claim that A *is a field*: let $f \in A$, $f \neq 0$; $f \in K'$ so there exists $f^{-1} \in K'$, and f^{-1} is integral over A; we fix an integral equation for f^{-1} over A:

$$(f^{-1})^s + a_{s-1}(f^{-1})^{s-1} + \ldots + a_0 = 0$$

where $a_0, \ldots, a_{s-1} \in A$. We multiply this equation by f^{s-1}:

$$f^{-1} + a_{s-1} + \ldots + a_0 f^{s-1} = 0$$

hence $f^{-1} \in A$. So A is both a field and a polynomial ring over K, so $r = 0$ and $A = K$. Therefore K' is an algebraic extension of K, which is algebraically closed, so $K' \simeq K$. Let us fix an isomorphism $\psi : \frac{K[x_1,\ldots,x_n]}{\mathcal{M}} \xrightarrow{\sim} K$ and let $p : K[x_1, \ldots, x_n] \to \frac{K[x_1,\ldots,x_n]}{\mathcal{M}}$ be the canonical epimorphism.

Let $a_i = \psi(p(x_i))$, $i = 1, \ldots, n$. The kernel of $\psi \circ p$ is $\mathcal{M}$, and $x_i - a_i \in \ker(\psi \circ p)$ for any i. So $\langle x_1 - a_1, \ldots, x_n - a_n \rangle \subset \ker(\psi \circ p) = \mathcal{M}$. Since $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is maximal (see Exercise 4.5.), we conclude the proof of the 1^{st} Step.

2^{nd} **Step** (Weak Nullstellensatz).

Let K be an algebraically closed field, let $\alpha \subset K[x_1, \ldots, x_n]$ be a *proper* ideal. Then $V(\alpha) \neq \emptyset$ i.e. the polynomials of α have at least one common zero in $\mathbb{A}^n_K$.

Proof. Since α is proper, there exists a maximal ideal $\mathcal{M}$ containing α. Then $V(\alpha) \supset V(\mathcal{M})$. By 1^{st} Step, $\mathcal{M} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$, so $V(\mathcal{M}) = \{P\}$ with $P(a_1, \ldots, a_n)$, hence $P \in V(\alpha)$.

3^{rd} **Step** (Rabinowitch method).

Let K be an algebraically closed field: we will prove that $I(V(\alpha)) \subset \sqrt{\alpha}$. Since the reverse inclusion always holds, this will conclude the proof.

Let $F \in I(V(\alpha))$, $F \neq 0$ and let $\alpha = \langle G_1, \ldots, G_r \rangle$. The assumption on F means: if $G_1(P) = \ldots = G_r(P) = 0$, then $F(P) = 0$. Let us consider the polynomial ring in $n+1$ variables $K[x_1, \ldots, x_{n+1}]$ and let β be the ideal $\beta = \langle G_1, \ldots, G_r, x_{n+1}F - 1 \rangle$: β has no zeroes in $\mathbb{A}^{n+1}$, hence, by Step 1, $1 \in \beta$, i.e. there exist $H_1, \ldots, H_{r+1} \in K[x_1, \ldots, x_{n+1}]$ such that

$$1 = H_1 G_1 + \ldots + H_r G_r + H_{r+1}(x_{n+1}F - 1).$$

We introduce the K-homomorphism $\psi : K[x_1, \ldots, x_{n+1}] \to K(x_1, \ldots, x_n)$ defined by $H(x_1, \ldots, x_{n+1}) \to H(x_1, \ldots, x_n, \frac{1}{F})$.

The polynomials $G_1, \ldots, G_r$ do not contain x_{n+1} so $\psi(G_i) = G_i \; \forall \, i = 1, \ldots, r$. Moreover $\psi(x_{n+1}F - 1) = 0$, $\psi(1) = 1$. Therefore

$$1 = \psi(H_1 G_1 + \ldots + H_r G_r + H_{r+1}(x_{n+1}F - 1)) = \psi(H_1)G_1 + \ldots + \psi(H_r)G_r$$

where $\psi(H_i)$ is a rational function with denominator a power of F. By multiplying this relation by a common denominator, we get an expression of the form:

$$F^m = H'_1 G_1 + \ldots + H'_r G_r,$$

so $F \in \sqrt{\alpha}$. □

4.10. Corollaries. *Let K be an algebraically closed field.*
1. There is a bijection between algebraic subsets of $\mathbb{A}^n$ and radical ideals of $K[x_1, \ldots, x_n]$. The bijection is given by $\alpha \to V(\alpha)$ and $X \to I(X)$. In fact, if X is closed in the Zariski topology, then $V(I(X)) = X$; if α is a radical ideal, then $I(V(\alpha)) = \alpha$.
2. Let $X, Y \subset \mathbb{A}^n$ be closed sets. Then
(i) $I(X \cap Y) = \sqrt{I(X) + I(Y)}$;
(ii) $I(X \cup Y) = I(X) \cap I(Y) = \sqrt{I(X)I(Y)}$.

Proof. 2. follows from next lemma, using the Nullstellensatz.

4.11. Lemma. *Let α, β be ideals of $K[x_1, \ldots, x_n]$. Then*
a) $\sqrt{\sqrt{\alpha}} = \sqrt{\alpha}$;
b) $\sqrt{\alpha + \beta} = \sqrt{\sqrt{\alpha} + \sqrt{\beta}}$;
c) $\sqrt{\alpha \cap \beta} = \sqrt{\alpha\beta} = \sqrt{\alpha} \cap \sqrt{\beta}$.

Proof.
a) if $F \in \sqrt{\sqrt{\alpha}}$, there exists $r \geq 1$ such that $F^r \in \sqrt{\alpha}$, hence there exists $s \geq 1$ such that $F^{rs} \in \alpha$.
b) $\alpha \subset \sqrt{\alpha}$, $\beta \subset \sqrt{\beta}$ imply $\alpha + \beta \subset \sqrt{\alpha} + \sqrt{\beta}$ hence $\sqrt{\alpha + \beta} \subset \sqrt{\sqrt{\alpha} + \sqrt{\beta}}$.

Conversely, $\alpha \subset \alpha + \beta$, $\beta \subset \alpha + \beta$ imply $\sqrt{\alpha} \subset \sqrt{\alpha + \beta}$, $\sqrt{\beta} \subset \sqrt{\alpha + \beta}$, hence $\sqrt{\alpha} + \sqrt{\beta} \subset \sqrt{\alpha + \beta}$ so $\sqrt{\sqrt{\alpha} + \sqrt{\beta}} \subset \sqrt{\sqrt{\alpha + \beta}} = \sqrt{\alpha + \beta}$.
c) $\alpha\beta \subset \alpha \cap \beta \subset \alpha$ (resp. $\subset \beta$) therefore $\sqrt{\alpha\beta} \subset \sqrt{\alpha \cap \beta} \subset \sqrt{\alpha} \cap \sqrt{\beta}$. If $F \in \sqrt{\alpha} \cap \sqrt{\beta}$, then $F^r \in \alpha$, $F^s \in \beta$ for suitable $r, s \geq 1$, hence $F^{r+s} \in \alpha\beta$, so $F \in \sqrt{\alpha\beta}$. □

Part 2.*(i)* of 4.10. implies that, i$I(X \cap Y) \neq I(X) + I(Y)$, if and only if $I(X) + I(Y)$ is not radical.

We move now to projective space. There exist *proper* homogeneous ideals of $K[x_0, x_1, \ldots, x_n]$ without zeroes in $\mathbb{P}^n$, also assuming K algebraically closed: for example the maximal ideal $\langle x_0, x_1, \ldots, x_n \rangle$. The following characterization holds:

4.12. Proposition. *Let K be an algebraically closed field and let I be a homogeneous ideal of $K[x_0, x_1, \ldots, x_n]$.*

The following are equivalent:
(i) $V_P(I) = \emptyset$;
(ii) either $I = K[x_0, x_1, \ldots, x_n]$ *or* $\sqrt{I} = \langle x_0, x_1, \ldots, x_n \rangle$;
(iii) $\exists d \geq 1$ *such that* $I \supset K[x_0, x_1, \ldots, x_n]_d$, *the subgroup of* $K[x_0, x_1, \ldots, x_n]$ *formed by the homogeneous polynomials of degree* d.

Proof.
(i)⇒(ii) Let $p : \mathbb{A}^{n+1} - \{0\} \to \mathbb{P}^n$ be the canonical surjection. We have: $V_P(I) = p(V(I) - \{0\})$, where $V(I) \subset \mathbb{A}^{n+1}$. So if $V_P(I) = \emptyset$, then either $V(I) = \emptyset$ or $V(I) = \{0\}$. If $V(I) = \emptyset$ then $I(V(I)) = I(\emptyset) = K[x_0, x_1, \ldots, x_n]$; if $V(I) = \{0\}$, then $I(V(I)) = \langle x_0, x_1, \ldots, x_n \rangle = \sqrt{I}$ by the Nullstellensatz.
(ii)⇒(iii) Let $\sqrt{I} = K[x_0, x_1, \ldots, x_n]$, then $1 \in \sqrt{I}$ so $1^r = 1 \in I (r \geq 1)$. If $\sqrt{I} = \langle x_0, x_1, \ldots, x_n \rangle$, then for any variable x_k there exists an index $i_k \geq 1$ such that $x_k^{i_k} \in I$. If $d \geq i_0 + i_1 + \ldots + i_n$, then any monomial of degree d is in I, so $K[x_0, x_1, \ldots, x_n]_d \subset I$.
(iii)⇒(i) because no point in $\mathbb{P}^n$ has all coordinates equal to 0. □

4.13. Theorem. *Let K be an algebraically closed field and I be a homogeneous*

ideal of $K[x_0, x_1, \ldots, x_n]$. *If* F *is a homogeneous non–constant polynomial such that* $V_P(F) \supset V_P(I)$ *(i.e.* F *vanishes on* $V_P(I)$*, then* $F \in \sqrt{I}$.

Proof. We have $p(V(I) - \{0\}) = V_P(I) \subset V_P(F)$. Since F is non–constant, we have also $V(F) = p^{-1}(V_P(F)) \cup \{0\}$, so $V(F) \supset V(I)$; by the Nullstellensatz $I(V(I)) = \sqrt{I} \supset I(V(F)) = \sqrt{(F)} \ni F$. □

4.14. Corollary (homogeneous Nullstellensatz). *Let* I *be a homogeneous ideal of* $K[x_0, x_1, \ldots, x_n]$ *such that* $V_P(I) \neq \emptyset$, K *algebraically closed. Then* $\sqrt{I} = I_h(V_P(I))$. □

4.15. Definition. A homogeneous ideal of $K[x_0, x_1, \ldots, x_n]$ such that $\sqrt{I} = \langle x_0, x_1, \ldots, x_n \rangle$ is called *irrelevant*.

4.16. Corollary. *Let* K *be an algebraically closed field. There is a bijection between the set of projective algebraic subsets of* $\mathbb{P}^n$ *and the set of radical homogeneous non–irrelevant ideals of* $K[x_0, x_1, \ldots, x_n]$. □

Remark. Let $X \subset \mathbb{P}^n$ be an algebraic set, $X \neq \emptyset$. The affine cone of X, denoted $C(X)$, is the following subset of $\mathbb{A}^{n+1}$: $C(X) = p^{-1}(X) \cup \{0\}$. If $X = V_P(F_1, \ldots, F_r)$, with $F_1, \ldots, F_r$ homogeneous, then $C(X) = V(F_1, \ldots, F_r)$. By the Nullstellensatz, if K is algebraically closed, $I(C(X)) = I_h(X)$.

Exercises to §4.

1. Give a non-trivial example of an ideal α of $K[x_1, \ldots, x_n]$ such that $\alpha \neq \sqrt{\alpha}$.

2. Show that the following closed subsets of the affine plane $Y = V(x^2+y^2-1)$ and $Y' = V(y-1)$ are such that equality does not hold in the following relation: $I(Y \cap Y') \supset I(Y) + I(Y')$.

3. Let $\alpha \subset K[x_1, \ldots, x_n]$ be an ideal. Prove that $\alpha = \sqrt{\alpha}$ if and only if the quotient ring $K[x_1, \ldots, x_n]/\alpha$ does not contain any non–zero nilpotent.

4. Consider $\mathbb{Z} \subset \mathbb{Q}$. Prove that if an element $y \in \mathbb{Q}$ is integral over $\mathbb{Z}$, then $y \in \mathbb{Z}$.

5. Let $a_1, \ldots a_n \in K$ (K any field). Prove that the ideal

$$I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$$

is maximal. (Hint: every polynomial F can be written in the form

$$F = F(a_1, \ldots, a_n) + \sum F_i(a_1, \ldots, a_n)(x_i - a_i) + \ldots,$$

where F_i is the i-th partial derivative of F. If $F \notin I \ldots$

Remember that it makes sense to consider derivatives of polynomials over any field.)

6. Let us recall that a prime ideal of a ring R is an ideal $\mathcal{P}$ such that $a \notin \mathcal{P}$, $b \notin \mathcal{P}$ implies $ab \notin \mathcal{P}$. Prove that any prime ideal is a radical ideal.

7*. Let I be a homogeneous ideal of $K[x_1, \ldots, x_n]$ satisfying the following condition: *if F is a homogeneous polynomial such that $F^r \in I$ for some positive integer r, then $F \in I$*. Prove that I is a radical ideal.

5. The projective closure of an affine algebraic set.

Let $X \subset \mathbb{A}^n$ be Zariski closed. Fix an index $i \in \{0, \ldots, n\}$ and embed $\mathbb{A}^n$ into $\mathbb{P}^n$ as the open subset U_i. So $X \subset \mathbb{A}^n \overset{\phi_i}{\hookrightarrow} \mathbb{P}^n$.

5.1. Definition. The *projective closure* of X, $\overline{X}$, is the closure of X in the Zariski topology of $\mathbb{P}^n$.

Since the map ϕ_i is a homeomorphism (see Proposition 3.2.), we have: $\overline{X} \cap \mathbb{A}^n = X$ because X is closed in $\mathbb{A}^n$. The points of $\overline{X} \cap H_i$, where $H_i = V_P(x_i)$, are called the "points at infinity" of X in the fixed embedding.

Note that, if K is an infinite field, then the projective closure of $\mathbb{A}^n$ is $\mathbb{P}^n$: indeed, let F be a homogeneous polynomial vanishing along $\mathbb{A}^n = U_0$. We can write $F = F_0 x_0^d + F_1 x_0^{d-1} + \ldots + F_d$. By assumption, for every $P(a_1, \ldots, a_n) \in \mathbb{A}^n$, $P \in V_P(F)$, i.e. $F(1, a_1, \ldots, a_n) = 0 = {}^aF(a_1, \ldots, a_n)$. So ${}^aF \in I(\mathbb{A}^n)$. We claim that $I(\mathbb{A}^n) = (0)$: if $n = 1$, this follows from the principle of identity of polynomials, because K is infinite. If $n \geq 2$, assume that $F(a_1, ..., a_n) = 0$ for all $(a_1, ..., a_n) \in K^n$ and consider $F(a_1, ..., a_{n-1}, x)$: either it has positive degree in x for some choice of $(a_1, ..., a_n)$, but then it has finitely many zeroes against the assumption; or it is always constant in x, so F belongs to $K[x_1, ..., x_{n-1}]$ and we can conclude by induction. So the claim is proved. We get therefore that $F_0 = F_1 = \ldots = F_d = 0$ and $F = 0$.

5.2. Proposition. *Let $X \subset \mathbb{A}^n$ be an affine algebraic set, $\overline{X}$ be the projective closure of X. Then*

$$I_h(\overline{X}) = {}^hI(X) := \langle {}^hF | F \in I(X) \rangle.$$

Proof. Assume $\mathbb{A}^n = U_0 \subset \mathbb{P}^n$.

Let $F \in I_h(\overline{X})$ be a homogeneous polynomial. If $P(a_1, \ldots, a_n) \in X$, then $[1, a_1, \ldots, a_n] \in \overline{X}$, so $F(1, a_1, \ldots, a_n) = 0 = {}^aF(a_1, \ldots, a_n)$. Hence ${}^aF \in X$. There exists $k \geq 0$ such that $F = (x_0^k)^h({}^aF)$ (see Proposition 3.2), so $F \in {}^hI(X)$. Hence $I_h(\overline{X}) \subset {}^hI(X)$.

Conversely, if $G \in I(X)$ and $P(a_1, \dots, a_n) \in X$, then $G(a_1, \dots, a_n) = 0 = {}^hG(1, a_1, \dots, a_n)$, so ${}^hG \in I_h(X)$ (here X is seen as a subset of $\mathbb{P}^n$). So ${}^hI(X) \subset I_h(X)$. Since $I_h(X) = I_h(\overline{X})$ (see Exercise 5.1), we have the claim.

□

In particular, if X is a hypersurface and $I(X) = \langle F \rangle$, then $I_h(\overline{X}) = \langle {}^hF \rangle$.

Next example will show that, *in general*, it is not true that, if $I(X) = \langle F_1, \dots, F_r \rangle$, then ${}^hI(X) = \langle {}^hF_1, \dots, {}^hF_r \rangle$. Only in the last twenty years, thanks to the development of symbolic algebra and in particular of the theory of Groebner bases, the problem of characterizing the systems of generators of $I(X)$, whose homogeneization generates ${}^hI(X)$, has been solved.

5.3. Example. *The skew cubic.*

Let K be an algebraically closed field. The affine skew cubic is the following closed subset of $\mathbb{A}^3$: $X = V(y - x^2, z - x^3)$ (we use variables x, y, z). X is the image of the map $\phi : \mathbb{A}^1 \to \mathbb{A}^3$ such that $\phi(t) = (t, t^2, t^3)$. Note that $\phi : \mathbb{A}^1 \to X$ is a homeomorphism (see Exercise 2.4). The ideal $\alpha = \langle y - x^2, y - x^3 \rangle$ defines X and is prime: indeed the quotient ring $K[x, y, z]/\alpha$ is isomorphic to $K[x]$, hence an integral domain. Therefore α is radical so $\alpha = I(X)$.

Let $\overline{X}$ be the projective closure of X in $\mathbb{P}^3$. We are going to prove that $\overline{X}$ is the image of the map $\psi : \mathbb{P}^1 \to \mathbb{P}^3$ such that $\psi([\lambda, \mu]) = [\lambda^3, \lambda^2\mu, \lambda\mu^2, \mu^3]$. We identify $\mathbb{A}^1$ with the open subset of $\mathbb{P}^1$ defined by $\lambda \neq 0$ i.e. U_0, and $\mathbb{A}^3$ with the open subset of $\mathbb{P}^3$ defined by $x_0 \neq 0$ (U_0 too). Note that $\psi|_{\mathbb{A}^1} = \phi$, because $\psi([1, t]) = [1, t, t^2, t^3] =$ via the identification of $\mathbb{A}^3$ with $U_0 = (t, t^2, t^3) = \phi(t)$. Moreover $\psi([0, 1]) = [0, 0, 0, 1]$. So $\psi(\mathbb{P}^1) = X \cup \{[0, 0, 0, 1]\}$.

If G is a homogeneous polynomial of $K[x_0, x_1, \dots, x_3]$ such that $X \subset V_P(G)$, then $G(1, t, t^2, t^3) = 0 \ \forall t \in K$, so $G(\lambda^3, \lambda^2\mu, \lambda\mu^2, \mu^3) = 0 \ \forall \mu \in K, \ \forall \lambda \in K^*$. Since K is infinite, then $G(\lambda^3, \lambda^2\mu, \lambda\mu^2, \mu^3)$ is the zero polynomial in λ and μ, so $G(0, 0, 0, 1) = 0$ and $V_P(G) \supset \psi(\mathbb{P}^1)$, therefore $\overline{X} \supset \psi(\mathbb{P}^1)$.

Conversely, it is easy to prove that $\psi(\mathbb{P}^1)$ is Zariski closed, in fact that $\psi(\mathbb{P}^1) = V_P(x_1^2 - x_0x_2, x_1x_2 - x_0x_3, x_2^2 - x_1x_3)$. So $\psi(\mathbb{P}^1) = \overline{X}$.

The three polynomials $F_0 := x_1x_3 - x_2^2$, $F_1 := x_1x_2 - x_0x_3$, $F_2 := x_0x_2 - x_1^2$ are the 2×2 minors of the matrix

$$M = \begin{pmatrix} x_0 & x_1 & x_2 \\ x_1 & x_2 & x_3 \end{pmatrix}$$

with entries in $K[x_0, x_1, \dots, x_3]$. Let $F = y - x^2$, $G = z - x^3$ be the two generators of $I(X)$; ${}^hF = x_0x_2 - x_1^2$, ${}^hG = x_0^2x_3 - x_1^3$, hence $V_P({}^hF, {}^hG) = V_P(x_0x_2 - x_1^2, x_0^2x_3 - x_1^3) \neq \overline{X}$, because $V_P({}^hF, {}^hG)$ contains the whole line $V_P(x_0, x_1)$.

We shall prove now the non-trivial fact:

5.4. Proposition. $I_h(\overline{X}) = \langle F_0, F_1, F_2 \rangle$.

Proof. For all integer number $d \geq 0$, let $I_h(\overline{X})_d := I_h(\overline{X}) \cap K[x_0, x_1, \ldots, x_3]_d$: it is a K-vector space of dimension $\leq \binom{d+3}{3}$. We define a K-linear map ρ_d having $I_h(\overline{X})_d$ as kernel:

$$\rho_d : K[x_0, x_1, \ldots, x_3]_d \to K[\lambda, \mu]_{3d}$$

such that $\rho_d(F) = F(\lambda^3, \lambda^2\mu, \lambda^2\mu^2, \mu^3)$. Since ρ_d is clearly surjective, we compute

$$\dim I_h(\overline{X})_d = \binom{d+3}{3} - (3d+1) = (d^3 + 6d^2 - 7d)/6.$$

For $d \geq 2$, we define now a second K-linear map

$$\phi_d : K[x_0, x_1, \ldots, x_3]_{d-2} \oplus K[x_0, x_1, \ldots, x_3]_{d-2} \oplus K[x_0, x_1, \ldots, x_3]_{d-2} \to I_h(\overline{X})_d$$

such that $\phi_d(G_0, G_1, G_2) = G_0F_0 + G_1F_1 + G_2F_2$. Our aim is to prove that ϕ_d is surjective. The elements of its kernel are called the *syzygies of degree d* among the polynomials F_0, F_1, F_2. Two obvious syzygies of degree 3 are constructed by developing, according to the Laplace rule, the determinant of the matrix obtained repeating one of the rows of M, for example

$$\begin{pmatrix} x_0 & x_1 & x_2 \\ x_0 & x_1 & x_2 \\ x_1 & x_2 & x_3 \end{pmatrix}$$

We put $H_1 = (x_0, x_1, x_2)$ and $H_2 = (x_1, x_2, x_3)$, they both belong to $\ker \phi_3$. Note that H_1 and H_2 give raise to syzygies of all degrees ≥ 3, in fact we can construct a third linear map

$$\psi_d : K[x_0, x_1, \ldots, x_3]_{d-3} \oplus K[x_0, x_1, \ldots, x_3]_{d-3} \to \ker \phi_d$$

putting $\psi_d(A, B) = H_1A + H_2B = (x_0, x_1, x_2)A + (x_1, x_2, x_3)B = (x_0A + x_1B, x_1A + x_2B, x_2A + x_3B)$.

Claim. ψ_d is an isomorphism.
Assuming the claim, we are able to compute $\dim \ker \phi_d = 2\binom{d}{3}$, therefore

$$\dim Im\ \phi_d = 3\binom{d+1}{3} - 2\binom{d}{3}$$

which coincides with the dimension of $I_h(\overline{X})_d$ previously computed. This proves that ϕ_d is surjective for all d and concludes the proof of the Proposition.

Proof of the Claim. Let (G_0, G_1, G_2) belong to $\ker \phi_d$. This means that the following matrix N with entries in $K[x_0, x_1, \ldots, x_3]$ is degenerate:

$$N := \begin{pmatrix} G_0 & G_1 & G_2 \\ x_0 & x_1 & x_2 \\ x_1 & x_2 & x_3 \end{pmatrix}$$

Therefore, the rows of N are linearly dependent over the quotient field of the polynomial ring $K(x_0, \dots, x_3)$. Since the last two rows are independent, there exist reduced rational functions $\frac{a_1}{a_0}, \frac{b_1}{b_0} \in K(x_0, x_1, x_2, x_3)$, such that

$$G_0 = \frac{a_1}{a_0}x_0 + \frac{b_1}{b_0}x_1 = \frac{a_1b_0x_0 + a_0b_1x_1}{a_0b_0}$$

and similarly

$$G_1 = \frac{a_1b_0x_1 + a_0b_1x_2}{a_0b_0}, G_2 = \frac{a_1b_0x_2 + a_0b_1x_3}{a_0b_0}$$

The G_i's are polynomials, therefore the denominator a_0b_0 divides the numerator in each of the three expressions on the right hand side. Moreover, if p is a prime factor of a_0, then p divides the three products b_0x_0, b_0x_1, b_0x_2, hence p divides b_0. We can repeat the reasoning for a prime divisor of b_0, so obtaining that $a_0 = b_0$ (up to invertible constants). We get:

$$G_0 = \frac{a_1x_0 + b_1x_1}{b_0}, G_1 = \frac{a_1x_1 + b_1x_2}{b_0}, G_2 = \frac{a_1x_2 + b_1x_3}{b_0},$$

therefore b_0 divides the numerators

$$c_0 := a_1x_0 + b_1x_1, c_1 := a_1x_1 + b_1x_2, c_2 := a_1x_2 + b_1x_3.$$

Hence b_0 divides also $x_1c_0 - x_0c_1 = b_1(x_1^2 - x_0x_1) = -b_1F_2$, and similarly $x_2c_0 - x_0c_2 = b_1F_1$, $x_2c_1 - x_1c_2 = -b_1F_0$. But F_0, F_1, F_2 are irreducible and coprime, so we conclude that $b_0 \mid b_1$. But b_0 and b_1 are coprime, so finally we get $b_0 = a_0 = 1$. □

As a by-product of the proof of Proposition 5.4 we have the minimal free resolution of the R-module $I_h(\overline{X})$, where $R = K[x_0, x_1, \dots, x_3]$:

$$0 \to R^{\oplus 2} \xrightarrow{\psi} R^{\oplus 3} \xrightarrow{\phi} I_h(\overline{X}) \to 0$$

where ψ is represented by the transposed of the matrix M and ϕ by the triple of polynomials (F_0, F_1, F_2).

Exercises to §5.

1*. Let $X \subset \mathbb{A}^n$ be a closed subset, $\overline{X}$ be its projective closure in $\mathbb{P}^n$. Prove that $I_h(X) = I_h(\overline{X})$.

2. Find a system of generators of the ideal of the affine skew cubic X, such that, if you homogeneize them, you get a system of generators for $I_h(\overline{X})$.

6. Irreducible components.

6.1. Definition. Let $X \neq \emptyset$ be a topological space. X is *irreducible* if the following condition holds: if X_1, X_2 are closed subsets of X such that $X = X_1 \cup X_2$, then either $X = X_1$ or $X = X_2$. Equivalently, X is irreducible if for all pair of non–empty open subsets U, V we have $U \cap V \neq \emptyset$. By definition, $\emptyset$ is not irreducible.

6.2. Proposition. *X is irreducible if and only if any non–empty open subset U of X is dense.*

Proof. Let X be irreducible, let P be a point of X and I_P be an open neighbourhood of P in X. I_P and U are non–empty and open, so $I_P \cap U \neq \emptyset$, therefore $P \in \overline{U}$. This proves that $\overline{U} = X$.

Conversely, assume that open subsets are dense. Let U, $V \neq \emptyset$ be open subsets. Let $P \in U$ be a point. By assumption $P \in \overline{V} = X$, so $V \cap U \neq \emptyset$ (U is an open neighbourhood of P). □

Examples.

1. If $X = \{P\}$ a unique point, then X is irreducible.

2. Let K be an infinite field. Then $\mathbb{A}^1$ is irreducible, because proper closed subsets are finite sets. The same holds for $\mathbb{P}^1$.

3. Let $f : X \to Y$ be a continuous map of topological spaces. If X is irreducible and f is surjective, then Y is irreducible.

4. Let $Y \subset X$ be a subset, give it the induced topology. Then Y is irreducible if and only if the following holds: if $Y \subset Z_1 \cup Z_2$, with Z_1 and Z_2 closed in X, then either $Y \subset Z_1$ or $Y \subset Z_2$; equivalently: if $Y \cap U \neq \emptyset$, $Y \cap V \neq \emptyset$, with U, V open subsets of X, then $Y \cap U \cap V \neq \emptyset$.

6.3. Proposition. *Let X be a topological space, Y a subset of X. Y is irreducible if and only if $\overline{Y}$ is irreducible.*

Proof. Note first that if $U \subset X$ is open and $U \cap Y = \emptyset$ then $\overline{U} \cap \overline{Y} = \emptyset$. Otherwise, if $P \in U \cap \overline{Y}$, let A be an open neighbourhood of P: then $A \cap Y \neq \emptyset$. In particular, U is an open neighbourhood of P so $U \cap Y \neq \emptyset$.

Let Y be irreducible. If U and V are open subsets of X such that $U \cap \overline{Y} \neq \emptyset$, $V \cap \overline{Y} \neq \emptyset$, then $U \cap Y \neq \emptyset$ and $V \cap Y \neq \emptyset$ so $Y \cap U \cap V \neq \emptyset$ by irreducibility of Y. Hence $\overline{Y} \cap (U \cap V) \neq \emptyset$. So $\overline{Y}$ is irreducible. If $\overline{Y}$ is irreducible, we get the irreducibility of Y in a completely analogous way. □

6.4. Corollary. *Let X be an irreducible topological space and U be a non–empty open subset of X. Then U is irreducible.*

Proof. By Proposition 6.2 $\overline{U} = X$ which is irreducible. By Proposition 6.3 U is irreducible. □

For algebraic sets (both affine and projective) irreducibility can be expressed

in a purely algebraic way.

6.5. Proposition. *Let $X \subset \mathbb{A}^n$ (resp. $\mathbb{P}^n$) be an algebraic set. X is irreducible if and only if $I(X)$ (resp. $I_h(X)$) is prime.*

Proof. Assume first that X is irreducible, $X \subset \mathbb{A}^n$. Let F, G polynomials of $K[x_1, \ldots, x_n]$ such that $FG \in I(X)$: then

$$V(F) \cup V(G) = V(FG) \supset V(I(X)) = X$$

hence either $X \subset V(F)$ or $X \subset V(G)$. In the former case, if $P \in X$ then $F(P) = 0$, so $F \in I(X)$, in the second case $G \in I(X)$; hence $I(X)$ is prime.

Assume now that $I(X)$ is prime. Let $X = X_1 \cup X_2$ be the union of two closed subsets. Then $I(X) = I(X_1) \cap I(X_2)$ (see §4). Assume that $X_1 \neq X$, then $I(X_1)$ strictly contains $I(X)$ (otherwise $V(I(X_1)) = V(I(X))$. So there exists $F \in I(X_1)$ such that $F \notin I(X)$. But for every $G \in I(X_2)$, $FG \in I(X_1) \cap I(X_2) = I(X)$ prime: since $F \notin I(X)$, then $G \in I(X)$. So $I(X_2) \subset I(X)$ hence $I(X_2) = I(X)$.

If $X \subset \mathbb{P}^n$, the proof is similar, taking into account the following:

6.6. Lemma *Let $\mathcal{P} \subset K[x_0, x_1, \ldots, x_n]$ be a homogeneous ideal. Then $\mathcal{P}$ is prime if and only if, for every pair of homogeneous polynomials F, G such that $FG \in \mathcal{P}$, either $F \in \mathcal{P}$ or $G \in \mathcal{P}$.*

Proof of the Lemma. Let H, K be any polynomials such that $HK \in \mathcal{P}$. Let $H = H_0 + H_1 + \ldots + H_d$, $K = K_0 + K_1 + \ldots + K_e$ (with $H_d \neq 0 \neq K_e$) be their expressions as sums of homogeneous polynomials. Then $HK = H_0K_0 + (H_0K_1 + H_1K_0) + \ldots + H_dK_e$: the last product is the homogeneous component of degree $d + e$ of HK. $\mathcal{P}$ being homogeneous, $H_dK_e \in \mathcal{P}$; by assumption either $H_d \in \mathcal{P}$ or $K_e \in \mathcal{P}$. In the former case, $HK - H_dK = (H - H_d)K$ belongs to $\mathcal{P}$ while in the second one $H(K - K_e) \in \mathcal{P}$. So in both cases we can proceed by induction. □

We list now some consequences of the previous Proposition.

1. Let K be an infinite field. Then $\mathbb{A}^n$ and $\mathbb{P}^n$ are irreducible, because $I(\mathbb{A}^n) = I_h(\mathbb{P}^n) = (0)$.

2. Let $Y \subset \mathbb{P}^n$ be closed. Y is irreducible if and only if its affine cone $C(Y)$ is irreducible.

3. Let $Y = V(F) \subset \mathbb{A}^n$, be a hypersurface over an algebraically closed field K. If F is irreducible, then Y is irreducible.

4. Let K be algebraically closed. There is a bijection between prime ideals of $K[x_1, \ldots, x_n]$ and irreducible algebraic subsets of $\mathbb{A}^n$. In particular, the maximal ideals correspond to the points. Similarly, there is a bijection between homogeneous non–irrelevant prime ideals of $K[x_0, x_1, \ldots, x_n]$ and irreducible algebraic subsets of $\mathbb{P}^n$.

6.7. Definition. A topological space X is called *noetherian* if it satisfies the following equivalent conditions:

(i) the ascending chain condition for open subsets;

(ii) the descending chain condition for closed subsets;

(iii) any non–empty set of open subsets of X has maximal elements;

(iv) any non–empty set of closed subsets of X has minimal elements.

The proof of the equivalence is standard.

Example. $\mathbb{A}^n$ is noetherian: if the following is a descending chain of closed subsets

$$Y_1 \supset Y_2 \supset \ldots \supset Y_k \supset \ldots,$$

then

$$I(Y_1) \subset I(Y_2) \subset \ldots \subset I(Y_k) \subset \ldots$$

is an ascending chain of ideals of $K[x_1, \ldots, x_n]$ hence stationary from a suitable m on; therefore $V(I(Y_m)) = Y_m = V(I(Y_m)) = Y_{m+1} = \ldots$.

6.8. Proposition. *Let X be a noetherian topological space and Y be a non–empty closed subset of X. Then Y can be written as a finite union $Y = Y_1 \cup \ldots \cup Y_r$ of irreducible closed subsets. The maximal Y_i's in the union are uniquely determined by Y and called the "irreducible components" of Y. They are the maximal irreducible subsets of Y.*

Proof. By contradiction. Let S be the set of the non–empty closed subsets of X which are not a finite union of irreducible closed subsets: assume $S \neq \emptyset$. By noetherianity S has minimal elements, fix one of them Z. Z is not irreducible, so $Z = Z_1 \cup Z_2$, $Z_i \neq Z$ for $i = 1, 2$. So $Z_1, Z_2 \notin S$, hence Z_1, Z_2 are both finite unions of irreducible closed subsets, so such is Z: a contradiction.

Now assume that $Y = Y_1 \cup \ldots \cup Y_r$, with $Y_i \not\subseteq Y_j$ if $i \neq j$ and Y_i irreducible closed for all i. If there is another similar expression $Y = Y_1' \cup \ldots \cup Y_s'$, $Y_i' \not\subseteq Y_j'$ for $i \neq j$, then $Y_1' \subset Y_1 \cup \ldots Y_r$, so $Y_1' = \bigcup_{i=1}^r (Y_1' \cup Y_i)$, hence $Y_1' \subset Y_i$ for some i, and we can assume $i = 1$. Similarly, $Y_1 \subset Y_j'$, for some j, so $Y_1' \subset Y_1 \subset Y_j'$, so $j = 1$ and $Y_1 = Y_1'$. Now let $Z = \overline{Y - Y_1} = Y_2 \cup \ldots \cup Y_r = Y_2' \cup \ldots \cup Y_s'$ and proceed by induction.

□

6.9. Corollary. *Any algebraic subset of $\mathbb{A}^n$ (resp. of $\mathbb{P}^n$) is in a unique way the finite union of its irreducible components.* □

Note that the irreducible components of X are its maximal algebraic subsets. They correspond to the minimal prime ideals over $I(X)$. Since $I(X)$ is radical, these minimal prime ideals coincide with the primary ideals appearing in the primary decomposition of $I(X)$.

6.10. Definition. An irreducible closed subset of $\mathbb{A}^n$ is called an *affine variety*. Similarly, an irreducible closed subset of $\mathbb{P}^n$ is a *projective variety*. A locally closed subset in $\mathbb{P}^n$ is the intersection of an open and a closed subset. An irreducible locally closed subset of $\mathbb{P}^n$ is a *quasi–projective variety*.

6.11. Proposition. *Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be affine varieties. Then $X \times Y$ is irreducible, i.e. a subvariety of $\mathbb{A}^{n+m}$.*

Proof. Let $X \times Y = W_1 \cup W_2$, with W_1, W_2 closed. For all $P \in X$ the map $\{P\} \times Y \to Y$ which takes (P, Q) to Q is a homeomorphism, so $\{P\} \times Y$ is irreducible. $\{P\} \times Y = (W_1 \cap (\{P\} \times Y)) \cup (W_2 \cap (\{P\} \times Y))$, so $\exists i \in \{1, 2\}$ such that $\{P\} \times Y \subset W_i$. Let $X_i = \{P \in X \mid \{P\} \times Y \subset W_i\}$, $i = 1, 2$. Note that $X = X_1 \cup X_2$.

Claim. X_i is closed in X.
Let $X^i(Q) = \{P \in X \mid (P, Q) \in W_i\}$, $Q \in Y$. We have: $(X \times \{Q\}) \cap W_i = X^i(Q) \times \{Q\} \simeq X^i(Q)$; $X \times \{Q\}$ and W_i are closed in $X \times Y$, so $X^i(Q) \times \{Q\}$ is closed in $X \times Y$ and also in $X \times \{Q\}$, so $X^i(Q)$ is closed in X. Note that $X_i = \bigcap_{Q \in Y} X^i(Q)$, hence X_i is closed, which proves the Claim.

Since X is irreducible, $X = X_1 \cup X_2$ implies that either $X = X_1$ or $X = X_2$, so either $X \times Y = W_1$ or $X \times Y = W_2$. □

Exercises to §6.

1. Let $X \neq \emptyset$ be a topological space. Prove that X is irreducible if and only if all non–empty open subsets of X are connected.

2*. Prove that the *cuspidal cubic* $Y \subset \mathbb{A}^2_{\mathbb{C}}$ of equation $x^3 - y^2 = 0$ is irreducible. (Hint: express Y as image of $\mathbb{A}^1$ in a continuous map...)

3. Give an example of two irreducible subvarieties of $\mathbb{P}^3$ whose intersection is reducible.

4. Find the irreducible components of the following algebraic sets over the complex field:
a) $V(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3) \subset \mathbb{A}^2$;
b) $V(y^2 - xz, z^2 - y^3) \subset \mathbb{A}^3$.

5*. Let Z be a topological space and $\{U_\alpha\}_{\alpha \in I}$ be an open covering of Z such that $U_\alpha \cap U_\beta \neq \emptyset$ for $\alpha \neq \beta$ and that all U_α's are irreducible. Prove that Z is irreducible.

7. Dimension.

Let X be a topological space.