LESSON 4.

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

Let $X \subset \mathbb{A}^n$ be an affine variety, $X = V(\alpha)$, where $\alpha \subset K[x_1, \ldots, x_n]$ is an ideal.

The ideal α defining X is not unique. We have already made this observation in the case of the hypersurfaces. For another example, let $O = \{(0,0)\} \subset \mathbb{A}^2$ be the origin; then $O = V(x_1, x_2) = V(x_1^2, x_2) = V(x_1^2, x_2^3) = V(x_1^2, x_1 x_2, x_2^2) = \ldots$ Nevertheless, there is an ideal we can canonically associate to X: the biggest one among the ideals defining it.

We give the following definition:

Definition 1.1. Let $Y \subset \mathbb{A}^n$ be any set.

The *ideal of* Y is

$$I(Y) = \{F \in K[x_1, \ldots, x_n] \mid F(P) = 0 \text{ for any } P \in Y\} = \{F \in K[x_1, \ldots, x_n] \mid Y \subset V(F)\} :$$

it is the set of **all** polynomials vanishing on Y. Note that $I(Y)$ is in fact an ideal, because the sum of two polynomials vanishing along Y also vanishes along Y, and the product of any polynomial by a polynomial vanishing along Y again vanishes along Y.

Example 1.2. Maximal ideal of a point.

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

The fact that $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is maximal can be understood looking at the quotient ring $K[x_1, \ldots, x_n]/\langle x_1 - a_1, \ldots, x_n - a_n \rangle$: the idea is that in the quotient the variables $x_1, \ldots, x_n$ are replaced by the constants $a_1, \ldots, a_n$, so it has to be $K[a_1, \ldots, a_n] = K$. Since the quotient is a field, the ideal is maximal.

Another proof of the maximality of $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ can be given by exploiting the expansion in power series around $\underline{a} := (a_1, \ldots, a_n)$ of any polynomial $F(x_1, \ldots, x_n)$. I first recall that this expansion is possible for polynomials over any field, without involving any differentiation process, but using only the formal definition of derivative for polynomials. See for instance [R. Walker, Algebraic curves, Springer, pp. 21-23.]

The proof goes as follows. Assume that $F(a_1, \ldots, a_n) = 0$ and use the Taylor expansion:

$$F(x_1, \ldots, x_n) = F(\underline{a}) + \sum_{i=1}^{n}(x_i - a_i)F_{x_i}(\underline{a}) + \sum_{i,j=1}^{n}(x_i - a_i)(x_j - a_j)F_{x_i x_j}(\underline{a}) + \ldots$$

It follows that $F \in \langle x_1 - a_1, \ldots, x_n - a_n \rangle$.

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 $K[x_0, x_1, \ldots, x_n]$ generated by the set

$$\{G \in K[x_0, x_1, \ldots, x_n] \mid G \text{ is homogeneous and } V_P(G) \supset Z\}.$$

It is denoted $I_h(Z)$.

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

If $X = V(\alpha)$ we want to understand the relation between α and $I(X)$.

Let $\alpha \subset K[x_1, \ldots, x_n]$ be an ideal. Let $\sqrt{\alpha}$ denote the radical of α:

$$\sqrt{\alpha} =: \{F \in K[x_1, \ldots, x_n] \mid \exists r \geq 1 \text{ s.t. } F^r \in \alpha\}.$$

Note that $\sqrt{\alpha}$ is an ideal (why?) and that always $\alpha \subset \sqrt{\alpha}$; if equality holds, then α is called a *radical ideal*.

Proposition 1.3. *The ideal of a subset of the affine space is radical, more precisely:*

(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 $F^r \in I(X)$: 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 (6)).

$\square$

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

Proposition 1.4. *Let $\alpha \subset K[x_1, \ldots, x_n]$ be an ideal, let $Y \subset \mathbb{A}^n$ 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: $\overline{Y} \subset \overline{V(I(Y))} = V(I(Y))$, because it is already closed. 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 $\overline{Y} \supset V(I(Y))$.

$\square$

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 $\mathbb{P}^n$. In the projective case, one has to take care of the fact that any homogeneous ideal is generated by the set of its homogeneous elements, and so, to prove an inclusion between homogeneous ideals, it is enough to check it on the homogeneous elements.

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 characterise $I(V(\alpha))$ we need to put into the picture the properties of the base field K.

The following celebrated theorem gives the answer for algebraically closed fields.

Theorem 1.5 (**Hilbert's Nullstellensatz - Theorem of zeros**). *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 in $K[x]$, 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 "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.

Definition 1.6. 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 $tr.d.E/K$.

Definition 1.7. 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 $A = K[y_1, \ldots, y_r]$.

Proposition 1.8. *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. $\qquad\square$

Corollary 1.9. $tr.d.K(y_1, \ldots, y_n)/K \leq n$.

Let now $A \subset B$ be rings, A a subring of B.

Definition 1.10. 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

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

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

Theorem 1.11. 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. We postpone the proof. $\square$

We start now the proof of the Nullstellensatz.

1st 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 $K[x_1, \ldots, x_n]/\mathcal{M}$: 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:

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

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

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

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 $\psi : K[x_1, \ldots, x_n]/\mathcal{M} \overset{\sim}{\longrightarrow} K$ and let $p : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]/\mathcal{M}$ 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 Example 1.2), we conclude the proof of the 1st Step.

2nd **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 $\mathbb{A}_K^n$.

Proof. Since α is proper, there exists a maximal ideal $\mathcal{M}$ containing α. Then $V(\alpha) \supset V(\mathcal{M})$. By 1st 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 $P \in V(\alpha)$.

3rd **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 $G_1(P) = \cdots = G_r(P) = 0$, 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 2, $1 \in \beta$, i.e. there exist $H_1, \ldots, H_{r+1} \in K[x_1, \ldots, x_{n+1}]$ such that

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

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

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

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:

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

so $F \in \sqrt{\alpha}$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \square$

Corollary 1.12. *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) $I(X \cup Y) = I(X) \cap I(Y) = \sqrt{I(X)I(Y)}$.
3. *The points of a hypersurface determine its reduced equation.*

Proof. 1. is clear. 2. follows from next lemma, using the Nullstellensatz. To prove 3., assume that F, G are square-free polynomials in $K[x_1 \ldots, x_n]$ such that $V(F) = V(G)$. By

the Nullstellensatz it follows that $\sqrt{F} = I(V(F)) = I(V(G)) = \sqrt{G}$, so $\langle F \rangle = \langle G \rangle$, which means that F, G differ at most by units. $\qquad\square$

Lemma 1.13. *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 $F \in \sqrt{\alpha\beta}$.

$\qquad\square$

Part 2.*(i)* of Corollary 1.12 implies that $I(X \cap Y) \neq I(X) + I(Y)$ if and only if $I(X) + I(Y)$ is not radical.

Remark. The weak form of the Nullstellensatz says that a system of algebraic equations has at least one solution over an algebraically closed field if, and only if, the ideal generated by the corresponding polynomials is not the whole ring, or, equivalently, if it is impossible to find a linear combination of them, with coefficients in the polynomial ring, equal to the constant 1. The above proof of Nullstellensatz is not constructive, in the sense that, given polynomials $F_1, \ldots, F_r$, it does not say how to check if 1 belongs or not to the ideal $\langle F_1, \ldots, F_r \rangle$.

The problem of making the proof constructive is connected to the more general "ideal membership problem", which asks, given an ideal $\alpha \subset K[x_1 \ldots, x_n]$ and a polynomial $G \in K[x_1 \ldots, x_n]$, to decide if $G \in \alpha$ or not.

Answers to these problems can be given with the tools of computational algebra, in particular using the theory of Gröbner bases.

We move now to the 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:

Proposition 1.14. *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) there exists $d \geq 1$ such that $I \supset K[x_0, x_1, \ldots, x_n]_d$, the homogeneous components of $K[x_0, x_1, \ldots, x_n]$ of the homogeneous polynomials of degree d.

Proof.

(i)$\Rightarrow$(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)$\Rightarrow$(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 $d \geq i_0 + i_1 + \cdots + i_n$, then any monomial of degree d is in I, so $K[x_0, x_1, \ldots, x_n]_d \subset I$.

(iii)$\Rightarrow$(i) because no point in $\mathbb{P}^n$ has all coordinates equal to 0. $\square$

Theorem 1.15. *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 $I(V(I)) = \sqrt{I} \supset I(V(F)) = \sqrt{(F)} \ni F$. $\square$

Corollary 1.16 (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 $\sqrt{I} = I_h(V_P(I))$.*

Definition 1.17. 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*.

Corollary 1.18. *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 by $C(X)$, 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 1.   (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 are such that equality does not hold in the relation $I(Y \cap Y') \supset I(Y) + I(Y')$: $Y = V(x^2 + y^2 - 1)$ and $Y' = V(y - 1)$. (**Remark**: as observed by Malech, it is necessary to add the assumptions that K is algebraically closed and char $K \neq 2$.)

(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 $y \in \mathbb{Z}$. (Hint: fixed $y = a/b \in \mathbb{Q}$ integral over $\mathbb{Z}$, write an integral equation for y, then use the unique factorization in $\mathbb{Z}$.)

(5) 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.

(6) * 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. (Hint: take F non homogeneous such that for some $r \geq 1$ $F^r \in I$, then use induction on the number of non-zero homogeneous components of F to prove that $F \in I$.)