5 Applications of Nullstellensatz. Maximal ideals in polynomial rings. Radical ideals.

5.1 Decomposition of affine algebraic sets into affine algebraic varieties.

Proposition 5.1. *Let k be algebraically closed, let $\mathfrak{a} \lhd k[x_1, ..., x_n]$, and let*

$$\mathfrak{a} = \mathfrak{q}_1 \cdot ... \cdot \mathfrak{q}_m = \mathfrak{q}_1 \cap ... \cap \mathfrak{q}_m.$$

be the primary decomposition of $\mathfrak{a}$ with the prime ideals $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$. Then $\mathcal{Z}(\mathfrak{q}_i)$ are affine algebraic varieties.

Proof. Clearly

$$\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\mathfrak{q}_1 \cap ... \cap \mathfrak{q}_m) = \mathcal{Z}(\mathfrak{q}_1) \cup ... \cup \mathcal{Z}(\mathfrak{q}_m),$$

and $\mathcal{Z}(\mathfrak{q}_i)$ is a variety, since $\mathcal{I}(\mathcal{Z}(\mathfrak{q}_i)) = \mathrm{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$ is prime, $i \in I$. □

5.2 Maximal ideals in polynomial rings.

Lemma 5.2. *Let A be a commutative ring, let $f \in A[x_1, ..., x_n]$. If $f(a_1, ..., a_n) = 0$ for some $(a_1, ..., a_n) \in A^n$, then there exist polynomials $g_1, ..., g_n \in A[x_1, ..., x_n]$ such that*

$$f = (x_1 - a_1) g_1 + ... + (x_n - a_n) g_n.$$

Proof. If $n = 1$, consider the identity:

$$x^m - a^m = (x - a)(x^{m-1} + a x^{m-2} + ... + a^{m-2} x + a^{m-1}).$$

Say $f(x_1) = b_0 + b_1 x_1 + ... + b_l x_1^l$. Since $f(a_1) = 0$, we get

$$\begin{aligned} f(x_1) &= f(x_1) - f(a_1) \\ &= (b_0 + b_1 x_1 + ... + b_l x_1^l) - (b_0 + b_1 a_1 + ... + b_l a_1^l) \\ &= b_1(x_1 - a_1) + b_2(x_1^2 - a_1^2) + ... + b_l(x_1^l - a_1^l), \end{aligned}$$

so that $f(x_1) = (x_1 - a_1) g(x_1)$ for a suitably defined $g \in A[x_1]$.

If $n > 1$ and the Lemma is true for polynominals in $n - 1$ variables, then consider the polynomial

$$g(x_1, ..., x_{n-1}) = f(x_1, ..., x_{n-1}, a_n) \in k[x_1, ..., x_{n-1}].$$

By the inductive hypothesis:

$$g(x_1, ..., x_{n-1}) = (x_1 - a_1) g_1 + ... + (x_{n-1} - a_{n-1}) g_{n-1},$$

for some $g_1, ..., g_{n-1} \in k[x_1, ..., x_{n-1}]$. Moreover

$$\begin{aligned} f(x_1, ..., x_n) &= \underbrace{f(x_1, ..., x_n) - f(x_1, ..., x_{n-1}, a_n)}_{\in A[x_1, ..., x_{n-1}][x_n]} + \underbrace{f(x_1, ..., x_{n-1}, a_n)}_{\in A[x_1, ..., x_{n-1}]} \\ &= (x_n - a_n) g_n(x_1, ..., x_n) + (x_1 - a_1) g_1 + ... + (x_{n-1} - a_{n-1}) g_{n-1} \end{aligned}$$

by the result for $n=1$ and the inductive step. □

Proposition 5.3. *Let k be algebraically closed and let $\mathfrak{m} \lhd k[x_1, \ldots, x_n]$. Then $\mathfrak{m}$ is maximal if and only if $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$, for some $a_1, \ldots, a_n \in k$.*

Proof. The ideal $(x_1 - a_1, \ldots, x_n - a_n)$ is maximal as the kernel of the homomorphic map $k[x_1, \ldots, x_n] \to k$ given by $f \mapsto f(a_1, \ldots, a_n)$.

Conversely, let $\mathfrak{m}$ be a maximal ideal. By Lemma 4.14 the set $\mathcal{Z}(\mathfrak{m})$ is nonempty, hence it contains an element $(a_1, \ldots, a_n) \in k^n$. Consider the ideal $\mathfrak{a} = (x_1 - a_1, \ldots, x_n - a_n)$. As before, $\mathfrak{a}$ is maximal. Since

$$\mathcal{Z}(\mathfrak{a}) = \{(a_1, \ldots, a_n)\} \subseteq \mathcal{Z}(\mathfrak{m})$$

we get that

$$\mathcal{I}(\mathcal{Z}(\mathfrak{a})) \supseteq \mathcal{I}(\mathcal{Z}(\mathfrak{m})).$$

$\mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ is a propel ideal, for otherwise $(a_1, \ldots, a_n) \in \mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\mathcal{I}(\mathcal{Z}\,(\mathfrak{m}))) = \mathcal{Z}(1) = \emptyset$, which is a contradiction. A $\mathfrak{m}$ is maximal:

$$\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \mathcal{I}(\mathcal{Z}(\mathfrak{m})) = \mathfrak{m}.$$

On the other hand $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) \supseteq \mathfrak{a}$, and hence $\mathfrak{a} \subseteq \mathfrak{m}$. But as $\mathfrak{m}$ is maximal, this yields $\mathfrak{a} = \mathfrak{m}$. □

Corollary 5.4. *Let k be algebraically closed.*

1. *If $\mathfrak{m} \lhd k[x_1, \ldots, x_n]$ is a maximal ideal, then $\mathcal{Z}(\mathfrak{m})$ is a singleton.*

2. *For every $\underline{a} \in k^n$ the ideal $\mathcal{I}(\underline{a})$ is maximal.*

Proof. The first part follows directly from Proposition 5.3. For the secon one take $(a_1, \ldots, a_n) \in k^n$ and consider the maximal ideal $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n) \lhd k[x_1, \ldots, x_n]$. If $f \in \mathfrak{m}$, then $f \in \mathcal{I}(\{(a_1, \ldots, a_n)\})$, so that $\mathfrak{m} \subseteq \mathcal{I}(\{(a_1, \ldots, a_n)\})$. But then $\mathfrak{m} = \mathcal{I}(\{(a_1, \ldots, a_n)\})$. □

Proposition 5.5. *Let k be algebraically closed. The map*

$$\mathcal{I}\colon \operatorname{Var} k^n \to \operatorname{Spec} k[x_1, \ldots, x_n], \qquad V \mapsto \mathcal{I}(V)$$

is a bijection. In particular singleton sets are mapped onto maximal ideals, and the inverse map is given by

$$\mathcal{Z}\colon \operatorname{Spec} k[x_1, \ldots, x_n] \to \operatorname{Var} k^n, \qquad \mathfrak{p} \mapsto \mathcal{Z}(\mathfrak{p}).$$

Proof. For an affine algebraic variety $V \subseteq k^n$, $\mathcal{Z}(\mathcal{I}(V)) = V$, by Remark 3.6.3 and, for a prime ideal $\mathfrak{p} \lhd k[x_1, \ldots, x_n]$, $\mathcal{I}(\mathcal{Z}(\mathfrak{p})) = \operatorname{rad} \mathfrak{p} = \mathfrak{p}$, by Hilbert Nullstellensatz. Moreover, singletons are mapped onto maximal ideals, by Corollary 5.4. □

5.3 Radical ideals.

Definition 5.6. *An ideal $\mathfrak{a}$ of a ring A is called* ***radical****, if $\mathfrak{a} = \operatorname{rad}(\mathfrak{a})$.*

Lemma 5.7. *Let A be a ring. An ideal $\mathfrak{a} \lhd A$ is radical if and only if the ring $A/\mathfrak{a}$ does not have nonzero nilpotents.*

Proof. Let $\kappa: A \to A/\mathfrak{a}$ be the canonical epimorphism. We claim that

$$\operatorname{rad}\mathfrak{a} = \kappa^{-1}(\operatorname{Nil}(A/\mathfrak{a})).$$

Indeed, for $x \in A$:

$$\begin{aligned} x \in \operatorname{rad}\mathfrak{a} &\Leftrightarrow x^n \in \mathfrak{a} \text{ for some } n \in \mathbb{N} \\ &\Leftrightarrow x + \mathfrak{a} \in \operatorname{Nil}(A/\mathfrak{a}) \\ &\Leftrightarrow x \in \kappa^{-1}(\operatorname{Nil}(A/\mathfrak{a})). \end{aligned}$$

Therefore

$$\mathfrak{a} = \operatorname{rad}\mathfrak{a} \Leftrightarrow \mathfrak{a} = \kappa^{-1}(\operatorname{Nil}(A/\mathfrak{a})) \Leftrightarrow \operatorname{Nil}(A/\mathfrak{a}) = \mathfrak{a},$$

which means that $\mathfrak{a}$ is radical if and only if the only element nilpotent in $A/\mathfrak{a}$ is the zero element. □

Proposition 5.8. *Let k be algebraically closed and let $\mathfrak{a} \lhd k[x_1, \ldots, x_n]$. Then $\mathfrak{a}$ is radical if and only if $\mathfrak{a} = \mathcal{I}(V)$ for some affine algebraic set $V \subset k^n$.*

Proof. If $\mathfrak{a}$ is radical, that is $\mathfrak{a} = \operatorname{rad}\mathfrak{a}$, then by Hilbert Nullstellensatz $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \operatorname{rad}\mathfrak{a} = \mathfrak{a}$, that is $\mathfrak{a} = \mathcal{I}(V)$, where $V = \mathcal{Z}(\mathfrak{a})$.

Conversely, if $\mathfrak{a} = \mathcal{I}(V)$, then $\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\mathcal{I}(V)) = V$, so that by Hilbert Nullstellensatz

$$\operatorname{rad}\mathfrak{a} = \mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \mathcal{I}(V) = \mathfrak{a}.$$

□

Proposition 5.9. *Let k be algebraically closed and let $\mathfrak{a} \lhd k[x_1, \ldots, x_n]$ be a radical ideal. Then $\mathfrak{a}$ has a unique decomposition into prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \lhd k[x_1, \ldots, x_n]$:*

$$\mathfrak{a} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r \quad \textit{with } \mathfrak{p}_i \not\subseteq \mathfrak{p}_j, \textit{ for } i \neq j.$$

Proof. Let

$$\mathcal{Z}(\mathfrak{a}) = V_1 \cup \ldots \cup V_r$$

be the decomposition of the affine algebraic set $\mathcal{Z}(\mathfrak{a})$ into a union of pairwise incomparable affine algebraic varieties. Clearly

$$\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \mathcal{I}(V_1) \cap \ldots \cap \mathcal{I}(V_r),$$

and every ideal $\mathcal{I}(V_i)$ is prime. From the incomparability of V_i's it follows that $\mathcal{I}(V_i)$'s are also incomparable. By Hilbert Nullstellensatz $\operatorname{rad}\mathfrak{a} = \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$, so that – as $\mathfrak{a}$ is radical – we get that

$$\mathfrak{a} = \mathcal{I}(V_1) \cap \ldots \cap \mathcal{I}(V_r).$$

is a decomposition of $\mathfrak{a}$ into pairwise incomparable prime ideals of $k[x_1, \ldots, x_n]$.

In order to show that such a decomposition is unique, suppose that

$$\mathfrak{a} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s$$

are two decompositions into pairwise incomparable prime ideals. But then

$$\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\mathfrak{p}_1) \cup \ldots \cup \mathcal{Z}(\mathfrak{p}_r) = \mathcal{Z}(\mathfrak{q}_1) \cup \ldots \cup \mathcal{Z}(\mathfrak{q}_s)$$

are two decompositions of $\mathcal{Z}(\mathfrak{a})$ into affine algebraic varieties with incomparable summands. Consequently, $r = s$ and after a conceivably necessary change of labelling $\mathcal{Z}(\mathfrak{p}_i) = \mathcal{Z}(\mathfrak{q}_i)$, so that $\mathfrak{p}_i = \mathfrak{q}_i$, $i \in \{1, \ldots, r\}$. □