Lecture 14

In this final lecture of the course we shall prove the Nullstellensatz and some facts about primary decompositions of ideals on Noetherian rings.

1 Nullstellensatz

Let K be an algebraic closed field. For $c_1, \cdots, c_n \in K$ denote by $m_{c_1,\cdots,c_n} \subset K[x_1, \cdots, x_n]$ denote the ideal $(x_1 - c_1, \cdots, x_n - c_n)$.

Proposition 1 (Weak Nullstellensatz)**.** *Every maximal ideal of $K[x_1, \cdots, x_n]$ is of the form $m_{c_1,\cdots,c_n}$ for some $c_i \in K$.*

Proof. Clearly, every ideal of the form $m_{c_1,\cdots,c_n}$ is maximal (this holds true in general, even if K is not algebraically closed). Now, let $m \subset K[x_1, \cdots, x_n]$ be a maximal ideal. Then $K[x_1, \cdots, x_n]/m$ is a field. Hence, we know from previous lectures that $K[x_1, \cdots, x_n]/m$ must be a finite extension of K, hence it must be isomorphic to K itself since K is algebraically closed. So the composition $K \to K[x_1, \cdots, x_n] \xrightarrow{\pi} K[x_1, \cdots, x_n]/m$ must be an isomorphism, and we can use it to identify K with $K[x_1, \cdots, x_n]/m$ in a natural way. Let now $c_i := \pi(x_i)$, so $c_i \in K$ due to the identification from before. Note that $x_i - c_i \in m$ since $m = \ker(\pi)$ and $\pi(x_i - c_i) = c_i - c_i = 0$. This implies that $m_{c_1,\cdots,c_n} \subset m$ and since the former is maximal we conlcude that $m_{c_1,\cdots,c_n} = m$. ☐

Note that the main ingredient needed to prove the weak Nullstellensatz is Noether normalization (together with the fact that if $R \subset S$ is an integral extension of domains, then R is a field if and only if S is a field).

Let now $I \subset K[x_1, \cdots, x_n]$ be an ideal. Recall that $V(I) \subset K^n$ denotes the vanishing locus of I, that is, $V(I)$ is the Zariski closed subset

$$V(I) = \{(c_1, \cdots, c_n) \in K^n \colon f(c_1, \cdots, c_n) = 0 \text{ for every } f \in I\}.$$

Since $K[x_1, \cdots, x_n]$ is Noetherian we know that I is finitely generated, so we can write $I = (f_1, \cdots f_k)$ for some $f_i \in K[x_1, \cdots, x_n]$ and therefore

$$V(I) = \{(c_1, \cdots, c_n) \in K^n \colon f_i(c_1, \cdots, c_n) = 0 \text{ for } i = 1, \cdots, k\}.$$

Given any subset $Z \subset K^n$ one denotes by $I(Z) \subset K[x_1, \cdots, x_n]$ the ideal given by $\{f \in K[x_1, \cdots, x_n] \colon f(z) = 0 \text{ for every } z \in Z\}$. Note that $I(Z)$ is always a radical ideal (why?).

Lemma 2. *For an ideal $I \subset K[x_1, \cdots, x_n]$, we have $I = (1)$ if and only if $V(I) = \emptyset$.*

Proof. Clearly $V(1) = \emptyset$. Now, assume that $V(I) = \emptyset$ and assume that $I \neq (1)$. Then there is a maximal ideal $m_{c_1,\cdots,c_n}$ containing I, which implies that $(c_1, \cdots, c_n) \in V(I)$, absurd. $\square$

Theorem 3 (Nullstellensatz)**.** *Let K be an algebraically closed field and let $I \subset K[x_1, \cdots, x_n]$ be an ideal. Then $I(V(I)) = \sqrt{I}$.*

Proof. The inclusion $\sqrt{I} \subset I(V(I))$ is clear, so we only need to prove that $I(V(I)) \subset \sqrt{I}$. Take $g \in I(V(I))$. We want to show that there is some $n > 0$ such that $g^n \in I$. Equivalently, we want to show that $\bar{g} \in R \coloneqq K[x_1, \cdots, x_n]/I$ is nilpotent, where as usual $\bar{g}$ denotes the image of g under the quotient map.

Note that for a commutative ring R and an element $r \in R$, we have that the localization R_r is the zero ring if and only if r is nilpotent (check this). So, it is enough to show that $R_{\bar{g}} = 0$ in our case.

We know how to explicitly construct the locazitaion of a ring at one element: $R_{\bar{g}} = R[x_{n+1}]/(x_{n+1}\bar{g} - 1)$. Using the correspondence theorem, if we write $I = (f_1, \cdots, f_k)$, we also have

$$R_{\bar{g}} = K[x_1, \cdots, x_n, x_{n+1}]/(f_1, \cdots, f_k, x_{n+1}g - 1).$$

So our aim is to show that $J \coloneqq (f_1, \cdots, f_k, x_{n+1}g - 1) = (1)$, i.e., that $V(J) = \emptyset$ due to the Lemma before.

So, assume that $(c_1, \cdots, c_n, c_{n+1}) \in V(J)$. This implies in particular that $(c_1, \cdots, c_n) \in V(I)$ by construction. But then $g(c_1, \cdots, c_n) = 0$ as well, because $g \in I(V(I))$. Finally, we have the contradiction

$$0 = c_{n+1}g(c_1, \cdots, c_n) - 1 = -1.$$

$\square$

2 Primary decomposition

Let again K be an algebraically closed field and consider an ideal $I \subset K[x_1, \cdots, x_n]$. We claimed that the associated Zariski closed subset (or algebraic variety) $V(I) \subset K^n$ can be decomposed into irreducible Zariski closed subsets. We recall that a topological space V is irreducible if when we write $V = V_1 \cup V_2$ with $V_1, V_2 \subset V$ closed, then necessarily $V_1 = V$ or $V_2 = V$. In a previous lecture, we proved that $V(I)$ is irreducible if and only if I is a prime ideal. Using the Nullstellensatz, it also follows that a Zariski closed $V \subset K^n$ is irreducible if and only if $I(V)$ is prime.

Now, if $V(I) = \cup V_i$ is a decomposition into irreducible components, then

$$I(V(I)) = \sqrt{I} = \bigcap_i I(V_i).$$

Hence, the existence of the decomposition into irreducible components translates to algebra into: every radical ideal of $K[x_1, \cdots, x_n]$ can be written as an intersection of prime ideals (this is, in fact, true in general for every Noetherian ring).

The primary decomposition of ideals is a stronger statement which works for any ideal (not necessarily radical) in any Noetherian ring.

Definition 4. Let R be a ring. An ideal $I \subset R$ is primary if for every $x, y \in R$ such that $xy \in I$, if $x \notin I$ then $y^n \in I$ for some $n > 0$.

In other words: an ideal $I \subset R$ is primary if every zero-divisor of R/I is nilpotent.

Proposition 5. *If $I \subset R$ is primary, then $\sqrt{I}$ is prime, and is the smallest prime ideal containing I.*

Proof. Let $x, y \in R$ be such that $xy \in \sqrt{I}$ and assume that $x \notin \sqrt{I}$. For some $n > 0$ we have $x^n y^n \in I$, and since $x \notin \sqrt{I}$ we also have $x^n \notin I$. Since I is primary, there is some $m > 0$ such that $(y^n)^m \in I$. But then $y \in \sqrt{I}$, so $\sqrt{I}$ is prime.

The fact that $\sqrt{I}$ is the smallest prime containing I is obvious, since for any prime ideal q such that $I \subset q$ we have $\sqrt{I} \subset q$. □

If I is primary and $p = \sqrt{I}$, we say that I is p-primary.

Example.

1. If an ideal I is such that $\sqrt{I}$ is prime, then I is not necessarily primary. As an example one can take the ideal $I = (xy, y^2) \subset K[x, y]$ for K any field. Since $(y)^2 \subset I \subset (y)$ we have that $\sqrt{I} = (y)$, which is prime. On the other hand, I is not primary, because $xy \in I$, $y \notin I$ and $x^n \notin I$ for any $n > 0$.

2. If $p \subset R$ is a prime ideal, then p^n is not necessarily p-primary. Consider $R = K[x, y, z]/(xy - z^2)$, and denote by $\bar{x}, \bar{y}, \bar{z}$ the images of the variables in R. Let $I = (\bar{x}, \bar{z}) \subset R$. Now $R/I = K[x, y, z]/(xy - z^2, x, z) = K[y]$, so I is prime. We want to show that I^2 is not primary. But $I^2 = (\bar{x}^2, \bar{z}^2, \bar{x}\bar{z}) = (\bar{x}^2, \bar{x}\bar{y}, \bar{x}\bar{z})$. So $\bar{x}\bar{y} \in I^2$ but $\bar{x} \notin I^2$ and $\bar{y}^n \notin I^2$ for any $n > 0$, for otherwise $\bar{y} \in \sqrt{I^2} = I$, which is impossible since $R/I \cong K[y]$.

3. If I is p-primary, then I is not necessarily a power of p. To check this, simply consider $I = (x, y^2) \subset K[x, y]$. The fact that I is (x, y)-primary will follow from Proposition 6. But $(x, y)^2 \subsetneq I \subsetneq (x, y)$, and it is easy to verify that all the inclusions are strict.

4. Finally, this last example shows that primary ideals are hard if not impossible to classify. Consider the ideal $I_a = (x^2, y^2, xy, ax + y) \subset K[x, y]$, where $a \in K$. This is (x, y)-primary again due to Proposition 6, and we also have $(x, y)^2 \subset I_a \subset (x, y)$. We now show that if $a \neq b$ then $I_a \neq I_b$. In fact, if $\alpha x + \beta y \in I_a$ for some $\alpha, \beta \in K$ then $\alpha x + \beta y = k \cdots (ax + y)$ for some $k \in K$ necessarily. But then $k\beta$ and hence $\beta \neq 0$ and $\alpha/\beta = a$.

On the other hand, we have

Proposition 6. *Let $I \subset R$ be an ideal such that $\sqrt{I} = m$ is a maximal ideal. Then I is m-primary.*

Proof. We prove that every zero-divisor in R/I is nilpotent. The nilradical of R/I is $n = \sqrt{I}/I$, which is also a maximal ideal, because its contraction under the quotient map $R \to R/I$ is maximal. Since every prime ideal contains the nilradical this shows that n is also the only prime ideal of R/I. But then every element of $R/I \setminus n$ is a unit for otherwise it would be contained in some maximal ideal. Finally, take a zero-divisor $x \in R/I$. Then x cannot be a unit, hence $x \in n$, hence it is nilpotent. □

All ideals now are considered to be proper ideals.

Definition 7. Let R be a ring.

- An ideal $I \subset R$ is irreducible if $I = I_1 \cap I_2$ then either $I = I_1$ or $I = I_2$.
- An ideal I is decomposable if we can write $I = \bigcap_{j=1}^{n} I_j$ where each I_j is irreducible.

Note in particular that every irreducible ideal is decomposable. The next two propositions show two very interesting consequences of the Noetherianity assumption:

Proposition 8. *In a Noetherian ring every ideal is decomposable.*

Proof. Consider the set S of all ideals of R which are not decomposable, ordered by inclusion. Take a maximal element $I \in S$, which exists because R is Noetherian. Since I is not decomposable it cannot be irreducible and we can write $I = I_1 \cap I_2$ for $I \subsetneq I_1, I_2 \subsetneq R$. But then $I_1, I_2 \notin S$ due to the maximality of I, so they are both decomposable. But then both I_1 and I_2 can be written as a finite intersection of irreducible ideals, and hence also I, which is a contradiction. □

The connection between irreducibility and being primary also works in general only for Noetherian rings:

Proposition 9. *Let R be Noetherian and let $I \subset R$ be irreducible. Then I is primary.*

Proof. By passing to the quotient it is enough to prove this for the zero ideal, that is: if (0) is irreducible, then (0) is primary. Take $x, y \in R$ such that $xy = 0$ and assume that $y \neq 0$. We therefore need to show that $x^n = 0$ for some $n > 0$. Consider the chain of annilhators

$$\mathrm{Ann}(x) \subset \mathrm{Ann}(x^2) \subset \cdots \subset \mathrm{Ann}(x^n) \subset \cdots$$

Since R is Noetherian this chain is stationary, so in particular there is some $n > 0$ such that $\mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1})$. Now we claim that $(x^n) \cap (y) = (0)$. Take $z \in (x^n) \cap (y)$, then $zx = 0$ because $z \in (y)$ and $xy = 0$. Also, $z = x^n a$ for some $a \in R$, because $z \in (x^n)$. But then $zx = ax^{n+1} = 0$ so $a \in \mathrm{Ann}(x^{n+1})$ and hence $a \in \mathrm{Ann}(x^n)$, so that $z = 0$. Now $(y) \neq (0)$ because $y \neq 0$; since (0) is irreducible, this finally shows that $(x^n) = (0)$. □

Note that the previous two propositions combined show that every ideal in a Noetherian ring can be written as a finite intersection of primary ideals. Before saying more, let us show that primary ideals are not in general irreducible:

Proposition 10. *If I_1, I_2 are p-primary ideals, then also $I_1 \cap I_2$ is p-primary.*

Proof. Let $x, y \in R$ be such that $xy \in I_1 \cap I_2$ and $x \notin I_1 \cap I_2$. We can assume wlog that $x \notin I_1$. Since I_1 is primary we then have $y^n \in I_1$ for some $n > 0$. Hence $y \in p = \sqrt{I_1}$. But since $\sqrt{I_2} = p$ as well, there must be some $m > 0$ such that $y^m \in I_2$ as well, hence $y^{nm} \in I_1 \cap I_2$.

Finally, $\sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2} = p$. □

Using this last proposition, we can group all the primary ideals having the same radical in a primary decomposition together, thus obtaining:

Theorem 11. *Let R be a Noetherian ring and let $I \subset R$ be an ideal. Then we can write*

$$I = \bigcap_{i=1}^{n} I_i$$

such that each I_i is primary and $p_i = \sqrt{I_i}$ are all distinct prime ideals.

We can also asssume that for every i we have $\bigcap_{j \neq i}^{n} I_j \subsetneq I_i$, for otherwise taking out I_i would still yield a primary decomposition of I. If a primary decomposition satisfies this last condition then we call the primary decomposition minimal.

In general a minimal primary decomposition is never unique:

Example. Consider the ideal $I = (xy, y^2) \subset K[x, y]$. Then we can write $I = (y) \cap (x, y^2) = (y) \cap (x + y, y^2)$. The first equality is clear, so let us show the second. Clearly $xy \in (x + y, y^2)$ so $I \subset (y) \cap (x + y, y^2)$. Now, take $f = (x + y)h_1 + y^2 h_2 \in (y) \cap (x + y, y^2)$. Then y divides h_1 necessarily so we can write $h_1 = y\tilde{h}_1$ and $f = (x + y)y\tilde{h}_1 + y^2 h_2 = (xy)\tilde{h}_1 + y^2(h_2 + \tilde{h}_1)$ which shows the other containment. The fact that $(x + y, y^2)$ is primary follows from Proposition 6, since $(x, y)^2 \subset (x + y, y^2) \subset (x, y)$, where the former inclusion comes from the fact that $xy \in (x + y, y^2)$ and therefore $x^2 \in (x + y, y^2)$ too. But clearly $(x, y^2) \neq (x + y, y^2)$ because $x + y \notin (x, y^2)$ for otherwise $y \in (x, y^2)$ too.

On the other hand, with some more work, one can make the following improvements towards a unicity statement:

- If $I = \bigcap_{i=1}^{n} I_i$ is a minimal prime decomposition as in Theorem 11, then the prime ideals $p_i = \sqrt{I_i}$ are, up to reordering, always the same (they are called the associated primes of I, see later);

- If $I = \bigcap_{i=1}^{n} I_i$ is a minimal prime decomposition, then the primary ideals I_i such that $p_j \subsetneq p_i$ for every $j \neq 1$ are, up to reordering, always the same.

The definition of associated primes works in general for modules, and it is the following:

Definition 12. Let M be a R-module: a prime ideal $p \subset R$ is an associated prime of M if there is some $m \in M$ such that $p = \mathrm{Ann}(m)$. If $I \subset R$ is an ideal, then the associated primes of I are the associated primes of the module R/I.

For a proof of these statements see for instance Patakfalvi's notes or any book of commutative algebra, e.g., Atiyah-MacDonald's. Note in particular that the first uniqueness statement yield the following corollary, whose geometric counterpart is the (unique) decomposition of algebraic subsets into irreducible components:

Corollary 13. *Any radical ideal in a Noetherian ring can be written uniquely as an intersection of prime ideals.*