9. Lecture 19 – Hilbert's nullstellensatz and primary decomposition in Noetherian rings

Recall that a field extension $k \subseteq k'$ is finite if k' is a finite-dimensional k-vector space.

Proposition (Zariski's lemma)**.** *Let k be a field, and let A be a finitely generated k-algebra. If A is a field, then A is a finite field extension of k.*

Remark. Clearly, if A is a finite field extension of k, then it is finitely generated as a k-algebra, since then A has a k-basis $a_1, \ldots, a_n$ which generates A as a module over k. These must therefore also generate A as a k-algebra.

Example. The field extension $k \subset k(x)$ is not finite, so the lemma says in this case that $k(x)$ is not a finitely generated k-algebra.

Corollary (Weak nullstellensatz)**.** *Let $\mathfrak{m} \subseteq k[x_1, \ldots, x_n]$ be a maximal ideal. Then $k[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite field extension of k.*

If k is algebraically closed, then $k[x_1, \ldots, x_n]/\mathfrak{m} \cong k$, and $\mathfrak{m}$ has the form

$$\mathfrak{m} = (x - a_1, x - a_2, \ldots, x - a_n)$$

for some $a_1, \ldots, a_n \in k$.

Proof. The ring $k[x_1, \ldots, x_n]/\mathfrak{m}$ is a field, so Zariski's lemma applies.

If k is algebraically closed, then it has no non-trivial finite field extension, so we must get $k[x_1, \ldots, x_n]/\mathfrak{m} \cong k$. The homomorphism

$$\phi\colon k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]/\mathfrak{m} \to k$$

has

$$(x_1 - \phi(x_1), \ldots, x_n - \phi(x_n)) \subseteq \ker \phi = \mathfrak{m}.$$

It's easy to see that the ideal on the left hand side is maximal, so we have an equality. □

Proof of Zariski's lemma, cheap version. Assume that k is uncountable, (e.g. $k = \mathbb{C}, \mathbb{R}$, not $k = \mathbb{Q}, \overline{\mathbb{Q}}$). Let A be a k-algebra generated by $a_1, \ldots, a_n \in A$, and assume that A is a field.

We claim that each of the a_i are algebraic. If a_i is not algebraic over k, so that $f(a_i) \neq 0$ for all $0 \neq f \in k[x]$, we have an inclusion of fields

$$k \subseteq k(x) \overset{x \mapsto a_i}{\to} A.$$

Now A is generated as a k-module by the elements $a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n}$, of which there are countably many, so that A has countable dimension as a k-module.

Claim: The dimension of $k(x)$ as a k-module is greater than or equal to the cardinality of k.

Proof. For each $\alpha \in k$, we have an element $(x - \alpha)^{-1} \in k(x)$. These are all linearly independent. Suppose we have a linear relation

$$\sum_{i=1}^{n} \beta_i (x - \alpha_i)^{-1} = 0$$

between some of them with α_i distinct. Multiplying by $f \prod_{i=1}^n (x - \alpha_i)$ gives a relation between polynomials

$$0 = \sum_{i=1}^n \beta_i \frac{f}{(x - \alpha_i)} \in k[x].$$

Evaluating this polynomial in α_i proves $0 = \beta_i$, so the elements $(x - \alpha_i)^{-1}$ are linearly independent. □

Now since $k(x) \cong k(a_i) \subseteq A$, we have a relation between the dimensions

$$|k| \leq \dim k(x) = \dim k(a_i) \leq \dim A = |\mathbb{Z}|,$$

contradicting our assumption that k was uncountable. □

Primary decompositions in Noetherian rings

Theorem (Lasker–Noether theorem)**.** *Let A be a Noetherian ring, and let $\mathfrak{a} \subseteq A$ be an ideal. Then $\mathfrak{a}$ admits a primary decomposition, i.e. we can write*

$$\mathfrak{a} = \cap_{i=1}^n \mathfrak{q}_i$$

with $\mathfrak{q}_i$ primary ideals.

We prove this in two steps. We say an ideal is **irreducible** if it cannot be written as a finite intersection of strictly bigger ideals. The first step is

Lemma. *Let A be a Noetherian ring, and let $\mathfrak{a} \subseteq A$ be an ideal. Then we can write $\mathfrak{a}$ as a finite intersection of irreducible ideals.*

Proof. Assume there is an ideal which is not an intersection of finitely many irreducible ideals. Since A is Noetherian we can take a maximal such ideal, call it $\mathfrak{a}$. The ideal $\mathfrak{a}$ is not itself irreducible, hence we can write $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ with $\mathfrak{a} \subsetneq \mathfrak{b}, \mathfrak{c}$. But now since $\mathfrak{a}$ is maximal, we can write $\mathfrak{b}$ and $\mathfrak{c}$ as finite intersections of irreducible ideals, so the same holds for $\mathfrak{a}$, a contradiction. □

Lemma. *Let A be a Noetherian ring, and let $\mathfrak{a}$ be irreducible. Then $\mathfrak{a}$ is primary.*

Proof. Passing to $A/\mathfrak{a}$, we may assume that $\mathfrak{a} = (0)$, and we want to show that (0) is primary.

We will assume that (0) is not primary, and then show that it is not irreducible. Since (0) is not primary, there exist $x, y \in A$ such that $xy = 0$, but $x \neq 0$ and y is not nilpotent. Consider then the sequence of ideals in A given by

$$\mathrm{Ann}(y) \subseteq \mathrm{Ann}(y^2) \subseteq \cdots.$$

Since A is Noetherian, this stabilises, so there is an N such that for $n \geq N$, we have $\mathrm{Ann}(y^n) = \mathrm{Ann}(y^N)$. Consider now the ideals (y^N) and $\mathrm{Ann}(y^N)$. Since y is not nilpotent, we have $(y^N) \neq (0)$. And since $x \in \mathrm{Ann}(y) \subseteq \mathrm{Ann}(y^N)$, we have $\mathrm{Ann}(y^N) \neq (0)$.

Main claim: $(y^N) \cap \mathrm{Ann}(y^N) = (0)$, which contradicts (0) being irreducible. *Proof of claim:* An element in the intersection has the form ay^N for some $a \in A$. It further satisfies

$$ay^N y^N = ay^{2N} = 0.$$

But then $a \in \mathrm{Ann}(y^{2N}) = \mathrm{Ann}(y^N)$, so $ay^N = 0$. □

Corollary. *Let A be a Noetherian ring, and let $\mathfrak{a} \subseteq A$ be an ideal.*

- *There is a primary decomposition of* $\mathfrak{a}$.
- *The set of prime ideals of the form* $\sqrt{(\mathfrak{a} : x)}$ *with* $x \in A$ *is finite, and contains all the minimal prime ideals containing* $\mathfrak{a}$.
- *If* $\mathfrak{a} = \sqrt{\mathfrak{a}}$, *then*
$$\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{p}_i,$$
where $\mathfrak{p}_i$ *are the minimal prime ideals containing* $\mathfrak{a}$.
- *The set of 0-divisors in* A *is the union of the (finitely many) minimal prime ideals in* A.