LECTURE 9: PROOF OF HILBERT'S NULLSTELLENSATZ

1. Preliminary lemmas

I state without proof two lemmas from commutative algebra that we will need.

The first is the exercise (7) from **Homework 2**; see also exercise (5) from **Problems class 8**.

Lemma 1.1. *Let R be any commutative ring with unity, and let $I \leq R$. Then,*

$$\operatorname{rad}(I) = \bigcap_{\substack{P \geq I \\ P \in \operatorname{Spec}(R)}} P. \tag{1.1}$$

The second is a result about field extensions due to Oscar Zariski. The proof can be found in Atiyah and MacDonald's *Introduction to Commutative Algebra* or (presented rather tersely) on Wikipedia. I may update these notes to include a proof (although you will not need to know it for the exam).

Lemma 1.2 (Zariski's lemma)**.** *Let L be a field extension of a field K. Suppose that L is finitely generated as a K-algebra (that is, there is a surjective map $K[x_1, \ldots, x_n] \twoheadrightarrow L$ for some L). Then, L is a finite extension of K (that is, finitely generated as a K-module).*

For example, the field $K = \mathbb{C}$ is algebraically closed (by the Fundamental Theorem of Algebra), so it has no finite extensions. Zariski's lemma implies a stronger-looking condition—that any field extension of $\mathbb{C}$ that is finitely generated as a $\mathbb{C}$-algebra is equal to $\mathbb{C}$ itself. It's worth noting that $\mathbb{C}(t)$ is *not* finitely generated as a $\mathbb{C}$-algebra.

2. Proof of the Nullstellensatz

Let $R = \mathbb{C}[x_1, \ldots, x_n]$, J an ideal of R, and $X = \mathbb{V}(J) \subseteq \mathbb{A}^n$. We have

$$\operatorname{rad}(J) = \{f \in R : f^k \in R \text{ for some } k\} \leq \mathbb{I}(X) = \{f \in R : f(a) = 0 \text{ for all } a \in \mathbb{V}(J) \tag{2.1}$$

because $f^k(a) = 0 \implies f(a) = 0$.

Now consider $f \in R$ such that $f \notin \operatorname{rad}(J)$. By lemma 1.1,

$$\operatorname{rad}(J) = \bigcap_{\substack{P \geq J \\ P \in \operatorname{Spec}(R)}} P. \tag{2.2}$$

Choose some particular prime ideal $P \geq J$ such that $f \notin P$. Then, R/P is a domain.

Consider the image $\overline{f}$ of f in R/P; since $f \notin P$, $\overline{f} \neq 0$. Taking $S = (R/P)[\overline{f}^{-1}]$, the inclusion map $R/P \to S$ is injective. Let $\mathfrak{m}$ be any maximal ideal of S, so $S/\mathfrak{m}$ is a field. Let ψ be the composition of the maps

$$R \twoheadrightarrow R/P \hookrightarrow S \twoheadrightarrow S/\mathfrak{m}; \tag{2.3}$$

then, the $n+1$ elements $\psi(x_1), \ldots, \psi(x_n), \psi(f)^{-1}$ generate $s/\mathfrak{m}$ as a $\mathbb{C}$-algebra. By Zariski's lemma, $S/\mathfrak{m}$ is a finite extension of $\mathbb{C}$; but $\mathbb{C}$ is algebraically closed, so in fact $S/\mathfrak{m} \cong \mathbb{C}$ in such a way that the composition of the maps

$$\mathbb{C} \hookrightarrow \mathbb{C}[x_1, \dots, x_n] = R \xrightarrow{\psi} S/\mathfrak{m} \cong \mathbb{C} \tag{2.4}$$

is the identity map. Let φ be the composition of the isomorphism $S/\mathfrak{m} \cong \mathbb{C}$ with φ.

Let $a_j = \varphi(x_j)$. Then, $\varphi(f) = f(a_1, \dots, a_n) \in \mathbb{C}$. But $\overline{f}$ is invertible in S, so $\overline{f} \notin \mathfrak{m}$, and thus $\varphi(f) \neq 0$. So $f(a_1, \dots, a_n) \neq 0$.

On the other hand, if $g \in P$, then $g(a_1, \dots, a_n) = \varphi(g) = 0$. Thus, the point $(a_1, \dots, a_n) \in \mathbb{V}(P) \subseteq \mathbb{V}(J)$, even though $f(a_1, \dots, a_n) \neq 0$. Hence $f \notin \mathbb{I}(J)$.

We've shown that $f \notin \operatorname{rad}(J) \implies f \notin \mathbb{I}(J)$, that is, $\mathbb{I}(J) \leq \operatorname{rad}(J)$. We already proved the reverse inclusion, so $\mathbb{I}(J) = \operatorname{rad}(J)$.