Lecture 13

1. Noether Normalization and Nullstellensatz

Let R be a ring and $0 \neq f \in R[x]$ be a polynomial. We say that f is essentially monic if its leading coefficient is invertible in R. If $0 \neq f \in R[x_1, ..., x_n]$ then we say that f is essentially monic in x_n if it is essentially monic as an element of $A[x_n]$ where $A = R[x_1, ..., x_{n-1}]$.

Theorem 1.1 (Noether's normalization). *Let A be a finitely generated k-algebra where k is a field. Then there exists $x_1, ..., x_n$ in A such that $x_1, ..., x_n$ are algebraically independent over k and $k[x_1, \dots, x_n] \subseteq A$ is module-finite.*

Proof. Let $A = k[y_1, \dots, y_m]$. If $m = 0$ we are done. Assume $m > 0$. We will prove the statement by induction on m.

If $y_1, \dots, y_m$ are algebraically independent over k we are done. Assume that there exists a polynomial $f \in k[Y_1, \dots, Y_m]$ such that $f(y_1, ..., y_m) = 0$.

Let $z_i = y_i - y_1^{r_1}$ for $i = 2, ..., m$. Then $f(y_1, z_2 + y_1^{r_2}, \dots, z_m + y_1^{r_m}) = 0$.

If we take $r_2 < r_3 < \cdots < r_m$ sufficiently large then there exists $g \in k[z_2, \dots, z_m][y_1]$ essentially monic such that

$$0 = f(y_1, z_2 + y_1^{r_2}, \dots, z_m + y_1^{r_m}) = g(y_1).$$

This implies that y_1 is integral over $R = k[z_2, \dots, z_m]$ and since $y_i = z_i + y_1^{r_i}, i = 2, \cdots, m$, we get that A is integral over R. Since A is a finitely generated R-algebra we get that A is module-finite over R.

But R has $m - 1$ k-algebra generators so there exists $x_1, ..., x_n$ in R such that $x_1, ..., x_n$ are algebraically independent over k and $k[x_1, \dots, x_n] \subseteq R$ is module-finite.

But since A is module-finite over R we get, by transitivity, that A is module-finite over $k[x_1, \dots, x_n]$.

$\square$

2. Hilbert Nulstellensatz

Theorem 2.1. *(Zariski's Lemma) If $k \subseteq R$ is a finitely generated k-algebra with R a field, then $k \subseteq R$ is a finite algebraic extension. Furthermore, if $k = \overline{k}$, then $k = R$.*

Proof. Using Noether normalization, let $\theta_1, ..., \theta_n$, algebraically independent over k, be such that $A = k[\theta_1, ..., \theta_n] \hookrightarrow R$ is module-finite. But $A \hookrightarrow R$ is integral, so $\{\theta_1, ..., \theta_n\} = \emptyset$, since $\dim(A) = \dim(R) = 0$. This implies $A = k$, so $k \hookrightarrow R$ is module-finite, and thus algebraic. □

Remark 2.2. *Let $R = k[x_1, ..., x_n]$, and $\lambda = (\lambda_1, ..., \lambda_n) \in k^n$. Then there is a surjective homomorphism $f_\lambda : k[x_1, ..., x_n] \to k$ that takes $x_i \mapsto \lambda_i$. Then $\ker f_\lambda = \{f \in R \mid f(\lambda) = 0\}$ is a maximal ideal, and if $m_\lambda = (x_1 - \lambda_1, ..., x_n - \lambda_n)$, then $m_\lambda \subseteq \ker f_\lambda$. In fact, $m_\lambda \subseteq \ker f_\lambda$ as the following argument shows it.*

By letting $y_i = x_i - \lambda_i$, we see that $f(x_1, \ldots, x_n) = f(y_1 + \lambda_1, \ldots, y_n + \lambda_n) = g(y_1, \ldots, y_n) + f(\lambda_1, \ldots, \lambda_n)$ with g a polynomial with zero constant coefficient; if $f \in \ker f_\lambda$, then $f(x_1, \ldots, x_n) = g(y_1, \ldots, y_n) \in m_\lambda$.

Theorem 2.3. *Let $R = k[x_1, ..., x_n]$, where $k = \overline{k}$ and let $f_1, ..., f_m \in R$. Then either $(f_1, ..., f_m) = R$ or $\exists\, \lambda \in k^n$ such that $f_i(\lambda) = 0$ for all i.*

Proof. Assume $(f_1, ..., f_m) \neq R$. Then $\exists \mathfrak{m} \in \mathrm{Max}(R)$ such that $(f_1, ..., f_m) \subseteq \mathfrak{m}$. Then $k \hookrightarrow R/\mathfrak{m}$ and $R/\mathfrak{m}$ is a finitely generated k-algebra. Then by the Zariski's Lemma, and because k is algebraically closed, $k = R/\mathfrak{m}$. So $\overline{x_i} \in R/\mathfrak{m} = k$ and hence $\exists\, \lambda_i \in k$ such that $\overline{x_i} = \lambda_i \in R/\mathfrak{m}$. This implies $\lambda_i - x_i \in \mathfrak{m}$, so $\mathfrak{m} = (x_1 - \lambda_1, ..., x_n - \lambda_n) = m_\lambda$, because $m_\lambda \in \mathrm{Max}(R)$. But $(f_1, ..., f_m) \subseteq \mathfrak{m} = m_\lambda$, which implies $f_i(\lambda) = 0$ for all i. □

Remark 2.4. *If $k = \overline{k}$ then all $\mathfrak{m} \in Max(R)$ are of the form m_λ for some $\lambda \in k^n$. So, there is a one-to-one correspondence between $Max(R)$ and the points of k^n.*

Theorem 2.5. *Let $R = k[x_1, ..., x_n]$, with $k = \overline{k}$, then there is a one-to-one correspondence between algebraic sets in k^n and radical ideals of R, where $X \mapsto I(X)$ and $Z(J) \mapsto J$.*

Proof. Let $J \leq k[x_1, ..., x_n]$ with $k = \overline{k}$. Then $Z(J) = \{x \in k^n \ : f(x) = 0, \ \forall f \in J\}$. If $Y \subseteq k^n$, then $I(Y) = \{f \in k[x_1, ..., x_n] \ : f|_Y = 0\}$. We can assume that $J = \mathrm{Rad}(J)$

since $I(Z(J)) = I(Z(\text{Rad}(J))$. Let $J = (f_1, ..., f_m)$, then $I(Z(J)) = \{f \ : f|_{Z(J)} = 0\}$. We would like to show that if $f \in I(Z(J))$ then $f \in \text{Rad}(J)$. We claim that if f vanishes where all of the $f_1, ..., f_m$ do, then $\exists\ n$ such that $f^n \in J = (f_1, ..., f_m)$. Let $R = k[x_1, ..., x_n]$, and $S = R[z]$. Let $f_0 = 1 - zf \in S$. Then $f_0, ..., f_m$ do not vanish simultaneously. By the weak Hilbert Nullstellensatz, $\exists\ G_0, ..., G_m \in S$ such that $1 = G_0(x,z)f_0 + \cdots + G_m(x,z)f_m$. Let $z = \frac{1}{f}$. Then

$$1 = G_1(x, \frac{1}{f})f_1 + \cdots + G_m(x, \frac{1}{f})f_m = \frac{g_1(x)}{f^{N_1}} + \cdots + \frac{g_m(x)}{f^{N_m}}.$$

We can amplify the fractions to have the same power of f in the denominators, and obtain $1 = \left(\sum \lambda_i g_i f_i\right) f^{-N}$, which implies $f^N = \sum \lambda_i g_i f_i \in J$. □

Theorem 2.6 (Going-down Theorem)**.** *Let $R \subset S$ be an integral extension of domains such that R is normal. Let*

$$P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq Pn$$

be a chain of prime ideals in R. Let Q_n be a prime ideal of S lying over P_n. Then there exists a chain of prime ideals in S

$$Q_1 \subsetneq \cdots \subsetneq Q_n$$

such that $Q_i \cap R = P_i$ for all $i = 0, \ldots, n$.