# Lecture 22.

## 1) Hilbert's Nullstellensatz.

References: [E], Sections 1.6, 4.5, 13.2; [V] Section 9.4.

## BONUS: Why Hilbert cared.

### 1) Hilbert's Nullstellensatz.

$\mathbb{F}$ infinite field, then $f \in \mathbb{F}[x_1 \dots x_n]$ can be viewed as a function $\mathbb{F}^n \to \mathbb{F}$; $f_1 \dots f_k \in \mathbb{F}[x_1, \dots x_n] \rightsquigarrow V(f_1, \dots f_k) := \{\alpha \in \mathbb{F}^n \mid f_i(\alpha) = 0\}$

### 1.1) Main result.

Q: for which $f \in \mathbb{F}[x_1, \dots x_n]$ do we have $f|_{V(f_1, \dots f_k)} = 0$?

Recall: For $A$ a commutative ring, $I \subset A$ an ideal $\rightsquigarrow$
$\sqrt{I} = \{a \in A \mid a^m \in I \text{ for some } m > 0\}$ - ideal in $A$ containing $I$.

Lemma: If $f \in \sqrt{(f_1, \dots f_k)} \Rightarrow f$ is zero on $V(f_1, \dots f_k)$.

Proof: $f^m = g_1 f_1 + \dots + g_k f_k$ is zero on $V(f_1, \dots f_k)$ for some $m \Rightarrow$ $f$ is also zero on $V(f_1, \dots f_k)$. □

If $\mathbb{F}$ is not alg. closed, "$\Leftarrow$" may fail to be true: $f_1 \in \mathbb{R}[x]$, $f_1 = x^2 + 1 \Rightarrow V(f_1) = \emptyset$, $1 \notin \sqrt{(x^2+1)}$ is zero on $V(f_1)$.

Thm (Hilbert's Nullstellensatz) Let $\mathbb{F}$ be alg. closed, $f_1, \dots f_k, f \in \mathbb{F}[x_1, \dots x_n]$. If $f$ is 0 on $V(f_1, \dots f_k)$, then $f \in \sqrt{(f_1, \dots, f_k)}$.

## 1.2) Noether normalization lemma

The proof is based on a number of auxiliary statements. This is the most important one.

Theorem (Noether). Let $\mathbb{F}$ be a field, $A$ a fin. generated $\mathbb{F}$-algebra. Then $\exists$ inclusion $\mathbb{F}[x_1, \dots x_m] \hookrightarrow A$ s.t. $A$ is finite over $\mathbb{F}[x_1, \dots x_m]$ (for some $m \geq 0$).

We'll only prove this when $\mathbb{F}$ is infinite, where a proof is easier. For a general case, see [E], Lemma 13.2 & Theorem 13.3.

Key lemma: Assume $\mathbb{F}$ is infinite, $F \in \mathbb{F}[x_1, \dots x_n]$ be nonzero. The $\exists$ $\mathbb{F}$-linear combinations $y_1, \dots, y_{n-1}$ of variables $x_1 \dots x_n$ s.t. $\mathbb{F}[x_1, \dots x_n]/(F)$ is finite over $\mathbb{F}[y_1, \dots, y_{n-1}]$.

Proof of lemma:

$F = f_0 + \dots + f_k$, $f_i$ is homogeneous of deg $= i$, $f_k \neq 0$.

Special case: $f_k(0, \dots, 0, 1) \neq 0 \iff x_n^k$ appears in $f_k$ w. nonzero coeff't. Now view $F \in \mathbb{F}[x_1, \dots x_{n-1}][x_n]$, has leading coeff't $\neq 0$ i.e. invertible in $\mathbb{F}[x_1, \dots x_{n-1}] \Rightarrow$ class of $x_n$ in $\mathbb{F}[x_1, \dots x_n]/(F)$ is integral over $\mathbb{F}[x_1, \dots x_{n-1}]$. By the theorem in Sect. 1.2) of

Lecture 9, $\mathbb{F}[x_1,\dots x_n]/(F)$ is finite over $\mathbb{F}[x_1,\dots x_{n-1}]$. Set $y_i := x_i$.

General case: $f_k \neq 0$ & $\mathbb{F}$ is infinite $\Rightarrow f_k(a_1,\dots a_n) \neq 0$ for some $a_i \in \mathbb{F}$. Pick invertible $\varphi \in Mat_{n\times n}(\mathbb{F})$ s.t.

$\varphi\begin{pmatrix}0\\ \vdots\\ 0\\ 1\end{pmatrix} = \begin{pmatrix}a_1\\ \vdots\\ a_n\end{pmatrix}$. Consider $F^{\varphi} = F\circ\varphi$ as a function $\mathbb{F}^n \to \mathbb{F}$ (polynomial obtained from $F$ by linear change of variables). Then $f_k^{\varphi}(0,\dots,0,1) = f_k(a_1,\dots a_n) \neq 0$. So

$\mathbb{F}[x_1,\dots x_n]/(F^{\varphi})$ is finite over $\mathbb{F}[x_1,\dots x_{n-1}]$, hence

$\uparrow \varphi^{-1}$

$\mathbb{F}[x_1,\dots x_n]/(F)$ is finite over $\mathbb{F}[y_1,\dots y_{n-1}]$ w.

$\begin{pmatrix}y_1\\ \vdots\\ y_n\end{pmatrix} := \varphi^{-1}\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$ □

Proof of Thm: Let $X = \{n \in \mathbb{Z}_{\geq 0} \mid \exists\ \mathbb{F}\text{-algebra homom'm } \mathbb{F}[x_1,\dots x_n] \longrightarrow A$ s.t. $A$ is finite over $\mathbb{F}[x_1,\dots x_n]\}$; $X \neq \emptyset$ b/c $A$ is finitely generated & so $\mathbb{F}[x_1,\dots x_n] \twoheadrightarrow A$ for some $n$.

Set $m := \min X \rightsquigarrow \varphi: \mathbb{F}[x_1,\dots x_m] \longrightarrow A$ s.t. $A$ is finite over $\mathbb{F}[x_1,\dots,x_m]$.

Claim: $\varphi$ is injective.

Assume the contrary: $\exists\ F \in \ker\varphi$, $F \neq 0$. By Key Lemma $\mathbb{F}[x_1,\dots x_m]/(F)$ is finite over $\mathbb{F}[y_1,\dots y_{m-1}]$ &

$A$ is finite over $\mathbb{F}[x_1,\dots x_m]/(F)$ (b/c $\varphi$ factors through $\mathbb{F}[x_1,\dots x_m]/(F)$). By Lemma 1 of Section 1.2 in Lecture 9 $A$ is finite over $\mathbb{F}[y_1,\dots,y_{m-1}]$. Contradiction w. choice of $m$. $\square$

*Important corollary:* Let $\mathbb{F}$ be an infinite field, let $A$ be a fin. gen'd $\mathbb{F}$-algebra. If $A$ is a field, then $\dim_{\mathbb{F}} A < \infty$.

*Proof:* By Thm, $\mathbb{F}[x_1,\dots x_m] \hookrightarrow A$ s.t $A$ is finite over $\mathbb{F}[x_1,\dots x_m]$. Need to show $m=0$. Assume the contrary. Since $A$ is a field, the image of $x_1$ is invertible, so $\mathbb{F}[x_1,\dots x_m] \hookrightarrow A$ extends to $\mathbb{F}[x_1,x_2,\dots x_m][x_1^{-1}] = \mathbb{F}[x_1^{\pm 1},\dots x_n] \hookrightarrow A$:

$$\mathbb{F}[x_1,\dots x_m] \hookrightarrow \mathbb{F}[x_1^{\pm 1}, x_2,\dots, x_m] \hookrightarrow A.$$

$A$ is fin. gen'd over $\mathbb{F}[x_1,\dots,x_m]$ & $\mathbb{F}[x_1,\dots,x_m]$ is Noetherian $\Rightarrow$ $\mathbb{F}[x_1^{\pm 1}, x_2,\dots x_m]$ is a finitely generated $\mathbb{F}[x_1,\dots x_m]$-module.

But this is not true: the $\mathbb{F}[x_1,\dots,x_m]$-submodule generated by $x_1^{-d_i}F_i$, $i=1,\dots,l$ is contained in $x_1^{-d}\mathbb{F}[x_1,\dots x_m]$, w. $d = \max(d_i)$. Contradiction w. $m>0$. $\square$

## 1.3) Proof of Nullstellensatz

*Proposition:* $\mathbb{F}$ is alg. closed, $A$ is fin. gen'd comm've $\mathbb{F}$-algebra. If $a \in A$ isn't nilpotent ($a^m \neq 0$ $\forall m$), then $\exists$ $\mathbb{F}$-alg. homom'm $\varphi: A \to \mathbb{F}$ s.t. $\varphi(a) \neq 0$.

*Proof:* $a$ isn't nilpotent: $0 \notin \{a^n\} \Rightarrow$ localization $A[a^{-1}] \neq \{0\}$

$A$ is fin. gen'd $\mathbb{F}$-algebra $\Rightarrow A[a^{-1}]$ is also fin. gen'd. Since $A[a^{-1}] \neq \{0\}$, by Section 2.2 in Lec 2, $A[a^{-1}]$ has a max. ideal, $\mathfrak{m}$, $\rightsquigarrow A[a^{-1}]/\mathfrak{m}$ is a field & is fin. gen'd over $\mathbb{F}$ (b/c $A[a^{-1}]$ is)
The important corollary implies that $A[a^{-1}]/\mathfrak{m}$ is a finite extension of $\mathbb{F}$. Since $\mathbb{F}$ is alg. closed, $A[a^{-1}]/\mathfrak{m} \simeq \mathbb{F}$.
$\varphi :=$ the composition $A \longrightarrow A[a^{-1}] \twoheadrightarrow A[a^{-1}]/\mathfrak{m} \xrightarrow{\sim} \mathbb{F}$
$\varphi(a) \neq 0$ b/c $\frac{a}{1} \in A[a^{-1}]$ is invertible and so $\frac{a}{1} \notin \mathfrak{m}$ □

Proof of Nullstellensatz: $A := \mathbb{F}[x_1, \dots x_n]/(f_1, \dots f_k)$, $\pi : \mathbb{F}[x_1, \dots x_n] \twoheadrightarrow A$, $a := \pi(f)$. Thm $\Leftrightarrow$ $a$ is nilpotent. Assume $a$ isn't nilpotent.
By Prop'n, $\exists\ \varphi : A \to \mathbb{F} \mid \varphi(a) \neq 0$; set $\tilde{\varphi} := \varphi \circ \pi : \mathbb{F}[x_1, \dots x_n] \to \mathbb{F}$, $\tilde{\varphi}(f) = \varphi(a) \neq 0$. Set $\alpha_i = \tilde{\varphi}(x_i) \rightsquigarrow \alpha := (\alpha_1, \dots \alpha_n) \in \mathbb{F}^n$ so that $\tilde{\varphi}(f) = f(\alpha)$. But $\tilde{\varphi}(f_i) = 0$ b/c $f_i \in \ker \pi \Rightarrow \alpha \in V(f_1, \dots f_k)$.
$\Rightarrow \tilde{\varphi}(f) = f(\alpha) = 0$. Contradiction. □

## 1.4) Corollaries.

**Corollary** of Prop'n in Sec. 1.3: If $A$ is a fin. gen'd $\mathbb{F}$-algebra, then $\sqrt{\{0\}} = \bigcap$ of all max. ideals in $A$.

**Corollary** of the proof of Thm & of Important corollary:
Let $A := \mathbb{F}[x_1, \dots x_n]/(f_1, \dots f_k)$. Suppose $\mathbb{F}$ is algebraically closed.
Then there are bijections between:
(i) $V(f_1, \dots f_k)$
(ii) $\{\mathbb{F}\text{-algebra homom'sm } A \to \mathbb{F}\}$

(iii) {maximal ideals of $A$}

(i) $\to$ (ii): $a \in V(f_1, \dots f_k) \rightsquigarrow \varphi_a : A \to \mathbb{F}$ given by $\varphi_a(f) := f(a)$.

(ii) $\to$ (iii): $\varphi \mapsto \ker\varphi$

Exercise: For $f_1, \dots f_k \in \mathbb{F}[x_1, \dots x_n]$ TFAE:

(1) $V(f_1, \dots f_k) = \emptyset$.

(2) Ideal $(f_1, \dots f_k)$ coincides with $\mathbb{F}[x_1, \dots x_n]$.

BONUS: Why Hilbert cared?

This is a continuation of a bonus from Lecture 5. Nullstellensatz was an auxiliary result in the 2nd paper by Hilbert on Invariant theory. We now discuss the main result there. Let $G$ be a "nice" group acting on a vector space $U$ by linear transformations.

Important example: $U$ is the space of homogeneous degree $n$ polynomials in variables $x, y$ (so that $\dim V = n+1$). For $G$ we take $SL_2(\mathbb{C})$, the group of $2\times 2$ matrices w. $\det = 1$, that acts on $V$ by linear changes of the variables.

The algebra of invariants $\mathbb{C}[U]^G$ is graded. So it has finitely many homogeneous generators. And every minimal collection of generators has the same number of elements (exercise)

Example: for $n=2$, $V = \{ax^2 + 2bxy + cy^2\}$. We can represent an element of $U$ as a matrix $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$, then $g \in SL_2(\mathbb{C})$ acts by $g.\begin{pmatrix} a & b \\ b & c \end{pmatrix} = g\begin{pmatrix} a & b \\ b & c \end{pmatrix} g^T$. The algebra of invariants is generated by

a single degree 2 polynomial $ac-b^2$, the determinant - or essentially the discriminant.

Example*: for $n=3$, we still have a single generator - also the discriminant.

And, as $n$ grows, the situation becomes more and more complicated. In general, very little is known about homogeneous generators. What is known, after Hilbert, is their set of common zeroes. The following theorem is a consequence of a much more general result due to Hilbert. Note that any $f \in U$ decomposes as the product of $n$ linear factors.

Theorem: For $f \in U$ (the space of homog. deg $n$ polynomials in $x, y$) TFAE:

- $f$ lies in the common set of zeroes of homogeneous generators of $\mathbb{C}[U]^G$
- $f$ has a linear factor of multiplicity $> \frac{n}{2}$.

Note that for $n=2,3$ we recover the zero locus of the discriminant.

The general result of Hilbert was way ahead of his time. Oversimplifying a bit, the first person who really appreciated this result of Hilbert was David Mumford who used a similar constructions to parameterize algebraic curves and other algebro geometric objects in the 60's - which brought him a Fields medal.