Lecture 14: Connections to Algebraic geometry, I.

1) Hilbert's Nullstellensatz & consequences

References: [E], Sections 1.6, 4.5, [V] Sec 9.4

BONUS: Why Hilbert cared.

1.1) Main result

Let $\mathbb{F}$ be an infinite field

Consider a system of polynomial equations $f_i(x_1,..x_n)=0$, $i=0,...m$. A basic question is when the last m equations imply the first one. It turns out that there's answer to this question in terms of algebra when $\mathbb{F}$ is algebraically closed ($\mathbb{F}=\overline{\mathbb{F}}$).

Thm (Nullstellensatz) Let $\mathbb{F}=\overline{\mathbb{F}}$ & $f_i \in \mathbb{F}[x_1,..x_n]$, $i=0,...m$. TFAE

a) $\exists\, k \in \mathbb{Z}_{\geq 0} \mid f_0^k \in (f_1,..f_n)$.

b) $f_i(\alpha)=0\ \forall\, i=1,...m, \Rightarrow f_0(\alpha)=0$ $(\forall\, \alpha \in \mathbb{F}^n)$

Proof of a) $\Rightarrow$ b) (for any $\mathbb{F}$): if $f_0^k=\sum_{i=1}^n g_i f_i$ & $f_i(\alpha)=0$, $i=1,..m$, then $f_0(\alpha)^k=\sum_{i=1}^n g_i(\alpha)f_i(\alpha)=0 \Rightarrow f_0(\alpha)=0$. $\square$

Exercise: 1) Assume $\mathbb{F}=\overline{\mathbb{F}}$. Then the system $f_i(\alpha)=0$, $i=1,...m$, has no solutions $\Leftrightarrow 1 \in (f_1,..f_m)$ (hint: apply Thm w. $f_0=1$).

2) Give a counterexample to "$\Rightarrow$" in 1) for $\mathbb{F}=\mathbb{R}$, $n,m=1$.

The proof of b) $\Rightarrow$ a) requires two different ingredients: the "weak Nullstellensatz" & a manipulation w. localizations.

1.2) Weak Nullstellensatz.

Proposition: Let $\mathbb{F}$ be a field & K be a field extension of $\mathbb{F}$, finitely generated as an $\mathbb{F}$-algebra. Then $\dim_{\mathbb{F}} K < \infty$.

Proof (using Noether's normalization lemma that we've only proved for infinite $\mathbb{F}$)

By that lemma (Thm in Sec 2 of Lec 13) $\exists\, m \mid \mathbb{F}[x_1,\dots x_m] \hookrightarrow K$ s.t. K is finite/ $\mathbb{F}[x_1,\dots,x_m]$. WTS $m=0$. If $m>0$, then since K is a field, $\exists\, x_1^{-1} \in K$. It's integral/ $\mathbb{F}[x_1,\dots x_m]$ (b/c K is finite $\Rightarrow$ integral) $\Rightarrow \ell>0,\ g_0,\dots g_{\ell-1} \in \mathbb{F}[x_1,\dots,x_m]$ s.t. $x_1^{-\ell} + g_{\ell-1}x_1^{1-\ell} + \dots + g_0 = 0$ (in K) $\Rightarrow$ [multiply by x_1^{ℓ}] $1 + g_{\ell-1}x_1 + \dots + g_0 x_1^{\ell} = 0$ (in K & hence in $\mathbb{F}[x_1,\dots x_m]$). But the constant term is 1, so we arrive at contradiction $\square$

Proposition has the following corollary that we'll use to prove Thm.

Corollary: Suppose $\mathbb{F} = \overline{\mathbb{F}}$. Let $G_1,\dots G_\ell \in \mathbb{F}[x_1,\dots x_k]$, $I = (G_1,\dots G_\ell)$, $B := \mathbb{F}[x_1,\dots x_k]/I$. The following sets are in bijection.

- $X_1 := \{$the maximal ideals $\mathfrak{m} \subset B\}$
- $X_2 := \{\alpha = (\alpha_1,\dots \alpha_k) \in \mathbb{F} \mid G_1(\alpha) = \dots = G_\ell(\alpha) = 0\}$

Proof: write $\bar{x}_i$ for $x_i + I \in B$.

- Map $X_1 \to X_2$: Note $K = B/\mathfrak{m}$ is a field & finitely generated $\mathbb{F}$-

algebra. By Proposition, $\dim_{\mathbb{F}} K<\infty$ and, since $\mathbb{F}$ is algebraically closed, $K=\mathbb{F}$. Let $\alpha_i^{\mathfrak{m}}:=$ image of $\bar{x}_i$ in $B/\mathfrak{m}=\mathbb{F}$ & $\alpha^{\mathfrak{m}}:=(\alpha_1^{\mathfrak{m}},\dots \alpha_k^{\mathfrak{m}})$
Since $G_j(\bar{x}_1,\dots \bar{x}_k)=0 \Rightarrow G_j(\alpha^{\mathfrak{m}})=0\ \forall j \Rightarrow \alpha^{\mathfrak{m}}\in X_2$.

• map $X_2\to X_1$: For $\alpha\in X_2$, the assigment $f+I\mapsto f(\alpha)$ is a well-defined homomorphism $B\to\mathbb{F}$ b/c $G_i(\alpha_1,\dots \alpha_k)=0$. It's surjective b/c $a+(G_1,\dots G_e)\mapsto a$. So its kernel $\mathfrak{m}_\alpha$ is a max. ideal, i.e. $\mathfrak{m}_\alpha\in X_1$.
Explicitly, $\mathfrak{m}_\alpha=\{f+I \mid f(\alpha_1,\dots \alpha_k)=0\}$

• $\alpha\mapsto\alpha^{\mathfrak{m}}$ & $\mathfrak{m}\mapsto\mathfrak{m}_\alpha$ are mutually inverse:
$\alpha^{\mathfrak{m}_\alpha}=(\text{image of } \bar{x}_i \text{ in } B/\mathfrak{m}_\alpha)_{i=1,\dots k}=(x_1(\alpha),\dots,x_k(\alpha))=(\alpha_1,\dots \alpha_k)=\alpha$.
$\mathfrak{m}_{\alpha^{\mathfrak{m}}}=\{f+I \text{ w. } f\in\mathbb{F}[x_1,\dots x_k] \mid f(\alpha_1^{\mathfrak{m}},\dots \alpha_k^{\mathfrak{m}})=0 \Leftrightarrow [\alpha_i^{\mathfrak{m}}=\text{image of } \bar{x}_i \text{ in } B/\mathfrak{m}]$
image of $f+I$ in $B/\mathfrak{m}$ is $0 \Leftrightarrow f+I\in\mathfrak{m}\}=\mathfrak{m}$. □

Exercise: Prove that X_1, X_2 are also in bijection w.
$X_3:=\{\mathbb{F}\text{-algebra homomorphisms } B\to\mathbb{F}\}$

1.3) Proof of b) ⇒ a) of Thm

Set $A=\mathbb{F}[x_1,\dots x_n]/(f_1,\dots f_m)$, $a:=f_0+(f_1,\dots f_m)\in A$, $B:=A[a^{-1}]$
WTS: $0\in\{a^\ell \mid \ell\geqslant 0\}\Leftrightarrow$[Rem 1) in Sec 2.2 of Lec 8] $\Leftrightarrow B=\{0\}$.
Every nonzero ring has a maximal ideal (we proved this in the Noetherian case & B is Noetherian as localization of such, Corollary in Sec 2.3 of Lec 9). So $B=\{0\}\Leftrightarrow X_1=\emptyset$. But $B\simeq$[Lem in Lec 9, Sec 1.1]$\simeq A[x_0]/(1-x_0a)\simeq\mathbb{F}[x_0,\dots x_n]/(f_1,\dots f_m, 1-x_0f_0)$

$X_2=\{(\alpha_0,\dots\alpha_n)\in\mathbb{F}^{n+1}\mid f_i(\alpha_1,\dots\alpha_n)=0\ \forall\ i=1,\dots m\ \&\ \alpha_0 f_0(\alpha_1,\dots\alpha_n)=1\}$
But $f_i(\alpha_1,\dots\alpha_n)=0\Rightarrow f_0(\alpha_1,\dots\alpha_n)=0\Rightarrow\alpha_0f_0(\alpha_1,\dots\alpha_n)=0$. So $X_2=\emptyset\Leftrightarrow$ [Corollary in Sec 1.2] $\Leftrightarrow X_1=\emptyset\Leftrightarrow 0\in\{\alpha^\ell\mid\ell\geqslant 0\}$. $\square$

1.4) Algebraic subsets vs radical ideals.

Until the end of the lecture, $\mathbb{F}=\overline{\mathbb{F}}$.

We now turning to understanding Nullstellensatz more conceptually. Recall (Sec 1 of Lec 2) that for ideal I in a commutative ring A, the radical $\sqrt{I}:=\{a\in A\mid a^\ell\in I$ for some $\ell>0\}$ is an ideal in A.

Definitions: 1) An ideal $I\subset A$ is radical if $I=\sqrt{I}$.

2) A subset $X\subset\mathbb{F}^n$ is called algebraic if $\exists$ $f_1,\dots f_m\in\mathbb{F}[x_1,\dots x_n]\mid X=\{\alpha\in\mathbb{F}^n\mid f_i(\alpha)=0\ \forall\ i=1,\dots m\}$. We say that X is defined by the polynomials $f_1,\dots f_m$ and write $X=V(f_1,\dots f_m)$.

Our goal is to relate algebraic subsets of $\mathbb{F}^n$ to radical ideals in $\mathbb{F}[x_1,\dots x_n]$. To any subset $X\subset\mathbb{F}^n$ we assign

$$I(X)=\{f\in\mathbb{F}[x_1,\dots x_n]\mid f(\alpha)=0\ \ \forall\ \alpha\in X\}$$

In the other direction, if $I\subset\mathbb{F}[x_1,\dots x_n]$ is any ideal, then we can consider the subset

$$V(I)=\{\alpha\in\mathbb{F}^n\mid f(\alpha)=0\ \ \forall\ f\in I\}$$

The computation in the proof of a) $\Rightarrow$ b) of Nullstellensatz shows that:

i) $I(X)$ is a radical ideal.

ii) If $I=(f_1,..f_m)$ ($\mathbb{F}[x_1,..x_n]$ is Noetherian so any ideal has this form), then $V(I)=V(f_1,..f_m)$.
iii) and $V(I)=V(\sqrt{I})$.

Proposition: The assignments $X\mapsto I(X)$, $I\mapsto V(I)$ are mutually inverse bijections between
- Algebraic subsets of $\mathbb{F}^n$
- Radical ideals in $\mathbb{F}[x_1,..x_n]$

Proof: i) & ii) ensure that the maps are between speeified sets.

Let $X=V(f_1,..f_m)$. b) $\Rightarrow$ a) of Nullstellensatz means $I(X)=\sqrt{(f_1,\dots,f_m)}$. ii) & iii) show $V(I(X))=X$.

Now let $I=(f_1,..f_m)$ be radical. Then $V(I)=V(f_1,..f_m)$, so $I(V(I))=\sqrt{(f_1,..f_m)}=\sqrt{I}=I$ $\square$

Examples: 1) $V(\{0\})=\mathbb{F}^n$ & $V(\mathbb{F}[x_1,..x_n])=\emptyset$.
2) If $\mathfrak{m}\subset\mathbb{F}[x_1,..x_n]$ is maximal, then $V(\mathfrak{m})$ is a single point.

Exercise: Correspondences in Proposition reverse inclusions:
1) For ideals $I_1\subset I_2\subset\mathbb{F}[x_1,..x_n]$, have $V(I_1)\supset V(I_2)$
2) For algebraic subsets $X_1\subset X_2\subset\mathbb{F}^n$, have $I(X_1)\supset I(X_2)$.

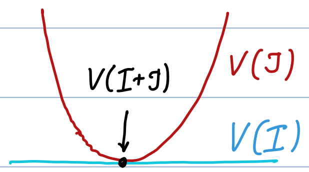
Now we discuss how operations w. ideals translate to those w. algebraic subsets.

Lemma: Let $I, J \subset \mathbb{F}[x_1, \dots x_n]$ be ideals. Then

1) $V(I+J) = V(I) \cap V(J)$
2) $V(I \cap J) = V(IJ) = V(I) \cup V(J)$

In particular, intersections & unions of two algebraic subsets are again algebraic.

Example: $n=2$, $I=(x_2)$, $J=(x_2-x_1^2)$ (radical – exercise; see also Lec 15)
$I+J=(x_2-x_1^2, x_2) = (x_1^2, x_2)$ – not radical, $\sqrt{I+J} = (x_1, x_2)$,
$V(I) = \{(x_1,x_2) \mid x_2 = 0\}$, $V(J) = \{(x_1,x_2) \mid x_2 = x_1^2\}$, $V(I+J) = \{(0,0)\}$.



This example indicates that non-radical ideals have geometric significance too: in this example, they reflect that intersections of algebraic subsets is not transversal.

Proof of Lemma:

Let $I=(f_1, \dots f_n)$, $J=(g_1, \dots g_m)$. Then $I+J = (f_1, \dots f_n, g_1, \dots g_m)$ & $IJ = (f_i g_j \mid i=1,\dots k, j=1,\dots,\ell)$ (Sec 1 of Lec 2).

$V(I) \cap V(J) = \{\alpha \in \mathbb{F}^n \mid f_i(\alpha) = 0\} \cap \{\alpha \in \mathbb{F}^n \mid g_j(\alpha) = 0\} = \{\alpha \in \mathbb{F}^n \mid f_i(\alpha) = 0 \ \& \ g_j(\alpha) = 0\} = V(I+J)$

$V(I) \cup V(J) = \{\alpha \in \mathbb{F}^n \mid f_i(\alpha) = 0 \ \forall i \text{ or } g_j(\alpha) = 0 \ \forall j \Leftrightarrow [f_i g_j](\alpha) = 0 \ \forall i,j\} = V(IJ)$

To see $V(I \cap J) = V(IJ)$, note $I \cap J \supset IJ \supset (I \cap J)^2 \Rightarrow \sqrt{IJ} = \sqrt{I \cap J}$. $\square$

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 2×2 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.