Lecture 23: Connections to Algebraic geometry, I.

1) Hilbert's Nullstellensatz.

2) Algebraic subsets & their vanishing ideals.

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

BONUSES: 1) Why Hilbert cared.

2) Is this ideal radical?

1) Hilbert's Nullstellensatz.

Let $\mathbb{F}$ be an 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 is uniquely recovered from this function.

To $\Psi\subset\mathbb{F}[x_1,\dots,x_n]$ we assign $V(\Psi):=\{\alpha\in\mathbb{F}^n \mid f(\alpha)=0, \forall f\in\Psi\}$ (solutions to the system Ψ of polynomial equations) and $I_\Psi = \operatorname{Span}_{\mathbb{F}[x_1,\dots,x_n]}(\Psi)$, an ideal in $\mathbb{F}[x_1,\dots,x_n]$.

Exercise: $\Psi_1\subset\Psi_2 \Rightarrow V(\Psi_2)\subset V(\Psi_1)$.

1.1) Main result.

Q: For $\Psi_1,\Psi_2\subset\mathbb{F}[x_1,\dots,x_n]$ find necessary & suff't cond'n for $V(\Psi_1)=V(\Psi_2)$

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: $V(\Psi)=V(\sqrt{I_\Psi})$.

Proof: $\Psi\subset\sqrt{I_\Psi} \Rightarrow V(\sqrt{I_\Psi})\subset V(\Psi)=:X$. To prove "=", take $f\in\sqrt{I_\Psi}$

We need to show $f|_X=0$: $\exists m \mid f^m = g_1 f_1 + \ldots + g_k f_k$ for $f_i \in \Psi$. Since $f_i|_X = 0 \Rightarrow f^m|_X = 0 \Rightarrow f|_X = 0$ $\square$

Thm (Nullstellensatz) Let $\mathbb{F}$ be alg. closed, $\Psi \subset \mathbb{F}[x_1, \ldots x_n]$, $f \in \mathbb{F}[x_1, \ldots x_n]$. If f is 0 on $V(\Psi)$, then $f \in \sqrt{I_\Psi}$

Cor: If $\mathbb{F}$ is alg. closed, then $V(\Psi_1) = V(\Psi_2) \Leftrightarrow \sqrt{I_{\Psi_1}} = \sqrt{I_{\Psi_2}}$

Remarks: 1) The conclusion of Thm is false over $\mathbb{R}$: Take $\Psi = \{x^2+1\}$, $\Rightarrow V(\Psi) = \emptyset$ & $f=1$. But $\sqrt{I_\Psi} = I_\Psi \not\ni 1$.

2) Nullstellensatz connects an algebraic object, $\sqrt{I_\Psi}$, and a geometric object, $V(\Psi)$. As such it provides the first connection between Commutative Algebra and Algebraic Geometry.

Exercise: Suppose $\mathbb{F}$ is alg. closed. Show $V(\Psi) = \emptyset \Leftrightarrow I_\Psi = \mathbb{F}[x_1, \ldots x_n]$.

1.2) Proof of Nullstellensatz

Let $X := V(\Psi)$, $I := I_\Psi$, $A := \mathbb{F}[x_1, \ldots x_n]/I$, $a := f + I \subset A$. Our job is to show that $\exists\, n \mid a^n = 0$. The proof is in 4 steps.

1) We establish a bijection $X \xrightarrow{\sim} \mathrm{Hom}(A, \mathbb{F})$ (w. $\mathrm{Hom} := \mathrm{Hom}_{\mathbb{F}\text{-Alg}}$)
2) From here we deduce $\mathrm{Hom}_{\mathbb{F}\text{-Alg}}(A[a^{-1}], \mathbb{F}) = \emptyset$
3) We deduce $A[a^{-1}] = \{0\}$ (using Important Cor from Sec 2 of Lec 22)
4) We deduce $0 \in \{a^n \mid n \geq 0\}$ finishing the proof.

1) $\alpha \in X \rightsquigarrow ev_\alpha : \mathbb{F}[x_1, \dots x_n] \to \mathbb{F}$, $f \mapsto f(\alpha)$, then $ev_\alpha \in Hom(A, \mathbb{F})$. Since $f(\alpha) = 0 \ \forall f \in I$, ev_α factors through $A \to \mathbb{F}$. The resulting homomorphism is also denoted by ev_α.

Conversely, let $\varphi : A \to \mathbb{F}$ be an algebra homomorphism. Set $\bar{x}_i := x_i + I \in A$. Set $\alpha_\varphi := (\varphi(\bar{x}_1), \dots, \varphi(\bar{x}_n)) \in \mathbb{F}^n$.

Exercise: $\alpha_\varphi \in X$ & $\alpha \mapsto ev_\alpha$, $\varphi \mapsto \alpha_\varphi$ are mutually inverse maps $X \rightleftarrows Hom(A, \mathbb{F})$.

2) $Hom(A[a^{-1}], \mathbb{F}) \xleftrightarrow{\sim}$ [univ. property of localization] $\{\varphi \in Hom(A, \mathbb{F}) \mid \varphi(a)$ is invertible $\Leftrightarrow \neq 0\} \xleftrightarrow{\sim}$ [Step 1] $\{\alpha \in X \mid 0 \neq ev_\alpha(a) = ev_\alpha(f) = f(\alpha)\} = \emptyset$ b/c $f|_X = 0$.

3) Suppose $A[a^{-1}] \neq \{0\}$. Note that $A[a^{-1}]$ is fin. gen'd (by $\frac{\bar{x}_i}{1}$ & $\frac{1}{a}$). Let $\mathfrak{m} \subset A[a^{-1}]$ be a max. ideal. Then $A[a^{-1}]/\mathfrak{m}$ is fin. gen'd $\mathbb{F}$-algebra that is also a field. By Important Corollary in Sec 2 of Lec 22, $A[a^{-1}]/\mathfrak{m}$ is finite field extension of $\mathbb{F}$. Since $\mathbb{F}$ is alg. closed, $A[a^{-1}]/\mathfrak{m} \simeq \mathbb{F}$. We've got an $\mathbb{F}$-algebra homomorphism $A \to A[a^{-1}]/\mathfrak{m} \xrightarrow{\sim} \mathbb{F}$. Contradiction w. Step 2.

4) Recall, Exer. in Sec 2 of Lec 8, that for $S \subset A$, a multiplicative subset, $A[S^{-1}] = \{0\} \Leftrightarrow 0 \in S$. Apply this to $S = \{a^n \mid n \geqslant 0\}$ so that $A[S^{-1}] = A[a^{-1}]$ and get $0 \in \{a^n\}$, which is what we need to prove. $\square$

Corollary: $\mathbb{F}$ is alg. closed, $A := \mathbb{F}[x_1, \dots x_n]/I_\Psi$, $X = V(\Psi)$. The following sets are in bijection.

(i) X.

(ii) $\mathrm{Hom}_{\mathbb{F}\text{-Alg}}(A, \mathbb{F})$

(iii) $\{$max. ideals $\mathfrak{m} \subset A\}$

Proof:

Bijections (i) $\xleftrightarrow{\sim}$ (ii) are constructed in Step 1.

(ii) $\to$ (iii): $\varphi \mapsto \ker \varphi$ – maximal b/c $A/\ker\varphi \xrightarrow{\sim} \mathrm{im}\,\varphi = [\varphi$ is an $\mathbb{F}$-algebra homomorphism$] = \mathbb{F}$, a field.

(iii) $\to$ (ii): As in Step 3, $A/\mathfrak{m} \simeq \mathbb{F}$ ($\mathbb{F}$-algebra iso, unique b/c $1 \leftrightarrow 1$)

We send $\mathfrak{m}$ to $A \twoheadrightarrow A/\mathfrak{m} \xrightarrow{\sim} \mathbb{F}$

Exercise: Prove (ii) $\rightleftarrows$ (iii) are inverse to each other. $\square$

Exercise: If A is a finitely generated $\mathbb{F}$-algebra, then $\sqrt{\{0\}} = \bigcap$ of all max. ideals in A.

2) Algebraic subsets & their vanishing ideals.

2.1) Definitions.

Below $\mathbb{F}$ denotes an alg. closed field. Let A be a commutative ring.

Definition • An ideal $I \subset A$ is **radical** if $I = \sqrt{I}$.

• A subset $X \subset \mathbb{F}^n$ is **algebraic** if $X = V(\Psi)$ for some $\Psi \subset \mathbb{F}[x_1, \dots x_n]$.

• For $X \subset \mathbb{F}^n$ algebraic, consider its vanishing ideal $I(X)=\{f\in \mathbb{F}[x_1,\dots,x_n] \mid f|_X=0\}$ & its algebra of polynomial functions $\mathbb{F}[X]:=\mathbb{F}[x_1,\dots x_n]/I(X)$.

Remarks: 1) By Lemma in Sec 1.1, $X=V(\sqrt{I_\Psi})$; $\sqrt{I_\Psi}$ is a finitely generated ideal (b/c $\mathbb{F}[x_1,\dots x_n]$ is Noetherian). If $f_1,\dots f_k$ are generators, then $X=V(f_1,\dots f_k)$. In particular, in the study of algebraic subsets $V(\Psi)$, it's enough to assume Ψ is finite.
2) $I(X)$ is a radical ideal (exercise). Elements of $\mathbb{F}[X]$ can be viewed as functions on X: for $\alpha\in X$ & $f\in\mathbb{F}[x_1,\dots,x_n]$, the value $f(\alpha)$ only depends on $f+I(X)$ – by def'n of $I(X)$. Hence the name for $\mathbb{F}[X]$.

2.2) Basic properties.

Corollary (of Nullstellensatz): the maps $I\mapsto V(I)$ & $X\mapsto I(X)$ are inclusion-reversing & mutually inverse bijections between:

$\{$radical ideals in $\mathbb{F}[x_1,\dots x_n]\}$
$\{$algebraic subsets in $\mathbb{F}^n\}$

Proof: Both $I\mapsto V(I)$ & $X\mapsto I(X)$ reverse inclusions (Sec 1 for the former & exercise for the latter. It remains to check that

i) $I=I(V(I))$: $I(V(I))=\{f \mid f$ is 0 on $V(I)\}$ $=$[Nullstellensatz]$=\sqrt{I}=$[I is radical]$=I$.

ii) $\forall$ algebraic subset $X \subseteq \mathbb{F}^n \Rightarrow X = V(I(X))$: by Lemma in Sec 1.1 $X = V(J)$ for a radical ideal J. Hence $V(I(V(J)) = [$by i), $I(V(J)) = J\,] = V(J)$. This finishes the proof $\square$

Now we discuss the behavior of the bijections in the corollary under intersections (of ideals & of algebraic subsets)

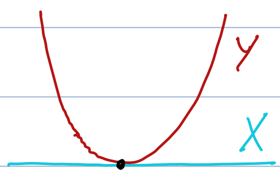
Lemma: Let $X, Y \subseteq \mathbb{F}^n$ be algebraic subsets.

(a) $X \cup Y$ is algebraic w. $I(X \cup Y) = I(X) \cap I(Y)$.

(b) $X \cap Y$ is algebraic with $I(X \cap Y) = \sqrt{I(X) + I(Y)}$

Example: $n=2$, $X = V(y)$, $Y = V(y-x^2)$, $I(X) = (y)$, $I(Y) = (y-x^2)$ (exer),
$X \cap Y = \{(0,0)\}$, $I(X) + I(Y) = (y-x^2, y) = (x^2, y)$ - not radical

but $\sqrt{(x^2,y)} = (x,y)$.



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

(a) $I := I(X)$, $J := I(Y)$ - radical ideals. Observe that:

- $I \cap J$ is radical (exercise).
- for $I = (f_1, \dots f_k)$, $J = (g_1, \dots g_\ell) \Rightarrow X \cup Y = \{a \in \mathbb{F}^n \mid f_i g_j (a) = 0 \; \forall i, j\}$

Since $(f_i g_j \mid i=1,\dots,k,\ j=1,\dots,\ell) = IJ \Rightarrow X\cup Y = V(IJ)$.
$\cdot\ (I\cap J)^2 \subset IJ \subset I\cap J$, so $\sqrt{IJ} = I\cap J$ & $V(IJ) = V(I\cap J)$.

(6) $X\cap Y = V(f_1,\dots,f_k, g_1,\dots,g_\ell)$ & $(f_1,\dots,f_k,g_1,\dots,g_\ell) = I+J$. So $X\cap Y = V(I+J) \Rightarrow I(X\cap Y) = \sqrt{I+J}$ $\square$

Exercise: if $X\cap Y = \varnothing$, then $\mathbb{F}[X\amalg Y] = \mathbb{F}[X]\times\mathbb{F}[Y]$.

BONUS 1: 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.

BONUS 2: Is this ideal radical?

We've talked about various properties of ideals (being radical/prime) and rings (being a normal domain). We work w. the ring $\mathbb{F}[x_1, \dots x_n]$, where $\mathbb{F}$ is a field, its ideals & quotients.

Usually, the ideals are specified by their generators. So we can ask the following questions:

I) Given $F_1, \dots F_k \in \mathbb{F}[x_1, \dots x_n]$, can we determine whether $(F_1, \dots F_k)$ is radical or prime?

As usual, the answer is both Yes & No.

Yes: for given n, k (& $F_1, \dots F_k$) there are algorithms (often implemented in Computer Algebra software) that allow to answer these and related questions. The main approach is via Gröbner bases. For more on them, see [E], Chapter 15.

No: if we care about the situation where we have a family of ideals with varying n, k.

Here's a famous example. Consider the space of pairs of square matrices, $\mathrm{Mat}_n(\mathbb{C})^2 \simeq \mathbb{C}^{2n^2}$. We have n^2 quadratic polynomials in these $2n^2$ variables – the entries of the matrix commutator $[A,B] = AB - BA$. For example, for $n=2$ we have

$$\left[\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}, \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}\right] = \begin{pmatrix} x_{12}y_{21} - y_{12}x_{21} & x_{11}y_{12} + x_{12}y_{22} - y_{11}x_{12} - y_{12}x_{22} \\ x_{21}y_{11} + x_{22}y_{21} - y_{21}x_{11} - y_{22}x_{21} & y_{12}x_{21} - x_{12}y_{21} \end{pmatrix}$$

In fact, as this example indicates, the n^2 polynomials we get are linearly dependent – $\mathrm{tr}[A,B]=0$. In any case, let I be the ideal generated by these polynomials so that $V(I) = \{(A,B) \in \mathrm{Mat}_n(\mathbb{C})^2 \mid AB = BA\}$, a.k.a the commuting variety.

Open problem: is I radical?