Lecture 22.

1) Hilbert's Nullstellensatz.
2) Algebraic subsets vs radical ideals.

Bonus: why Hilbert cared.

References: [E], Sections 1.6, 4.5, 13.2; Vinberg, A course in Algebra, Section 9.4.

1) $\mathbb{F}$ 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 comm've 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: $f^m=g_1f_1+\dots+g_kf_k$ is zero on $V(f_1,\dots f_k)$ for some $m\Rightarrow$ f is also zero on $V(f_1,\dots f_k)$ $\square$

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

"null" = "zero", "stellen" = "location", "satz" = "theorem."

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 zero on $V(f_1,\dots f_k)=\{\alpha\in\mathbb{F}^n\mid f_i(\alpha)=0\ \forall i\}$ then $f\in\sqrt{(f_1,\dots,f_k)}$.

1.2) Proof

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 $\rightsquigarrow$ localization $A[a^{-1}] \neq \{0\}$ $(\frac{1}{1} \neq \frac{0}{1})$

A is fin. gen'd $\Rightarrow$ $A[a^{-1}]$ 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 last corollary in Lec 21 implies that $A[a^{-1}]/\mathfrak{m}$ is a finite ext'n 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 $\Rightarrow \frac{a}{1} \notin \mathfrak{m}$ $\square$

Proof of Thm: $A := \mathbb{F}[x_1, \dots x_n]/(f_1, \dots, f_k)$, $\pi: \mathbb{F}[x_1, \dots x_n] \twoheadrightarrow A$

$a := \pi(f)$. Thm $\Leftrightarrow$ a is nilpotent. Assume the contrary.

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. $\square$

1.3) Corollaries.

Corollary of Prop'n: 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: There are bijections between:

(i) $V(f_1, \dots f_k)$

(ii) $\{\mathbb{F}\text{-algebra homom'sm } A \to \mathbb{F}\}$, $A = \mathbb{F}[x_1, \dots x_n]/(f_1, \dots f_k)$.

(iii) $\{\text{maximal ideals of } A\}$

e.g. $\alpha \in V(f_1, \dots f_k) \rightsquigarrow \varphi_\alpha : A \to \mathbb{F}$ given by $\varphi_\alpha(f) := f(\alpha)$.

Exer: 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 $\mathbb{F}[x_1, \dots x_n]$.

2) Algebraic subsets vs radical ideals

2.1) Definitions: $\mathbb{F}$ is alg. closed

Def'n: A is a comm've ring. An ideal $I \subset A$ is <u>radical</u> if $I = \sqrt{I}$.

Def'n: For $I \subset \mathbb{F}[x_1, \dots x_n]$ ideal, define $V(I) := \{\alpha \in \mathbb{F}^n \mid f(\alpha) = 0 \ \forall f \in I\}$

Note: if $I = (f_1, \dots f_k)$ - and any ideal has this form b/c $\mathbb{F}[x_1, \dots x_n]$ is Noeth'n - then $V(I) = V(f_1, \dots f_k)$.

By Lemma in Sect 1.1, $V(\sqrt{I}) = V(I)$.

Def'n: • Subset $X \subset \mathbb{F}^n$ is <u>algebraic</u> if $X = V(I)$ for some ideal $I \subset \mathbb{F}[x_1, \dots x_n]$, equiv. $X = V(f_1, \dots f_k)$ for some $f_1, \dots f_k \in \mathbb{F}[x_1, \dots x_n]$.

• $I(X) := \{f \in \mathbb{F}[x_1, \dots x_n] \mid f|_X = 0\}$ - is a radical ideal in $\mathbb{F}[x_1, \dots x_n]$.

• $\mathbb{F}[X] := \mathbb{F}[x_1, \dots x_n]/I(X)$, the algebra of polynomial functions on X.

$\pi: \mathbb{F}[x_1, \dots x_n] \twoheadrightarrow \mathbb{F}[x_1, \dots x_n]/I(X)$, $f \mapsto f|_X$.

An element of $\mathbb{F}[X]$ can be viewed as a function $X \to \mathbb{F}$.

3]

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: By construction, both $I \mapsto V(I)$ & $X \mapsto I(X)$ reverse inclusions.

- $\forall$ radical $I \Rightarrow I = I(V(I))$ – by Nullstellensatz
- $\forall$ algebraic subsets $X \subseteq \mathbb{F}^n \Rightarrow X = V(I(X))$: note

$X = V(J)$ for some radical ideal J. So we get,

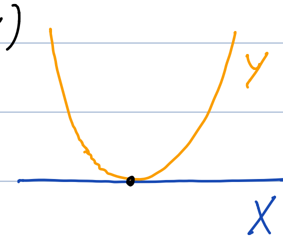
$V(\underbrace{I(V(J))}_{=J}) = V(J)$ which is what we need to prove $\square$

- Intersections.

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

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

(b) $X \cap Y$ is alg'c w. $I(X \cap Y) = \sqrt{I(X) + I(Y)}$



Example: $n=2$, $X = \{y=0\}$, $Y = \{y - x^2 = 0\}$

$I(X) = (y)$, $I(Y) = (y - x^2)$

$X \cap Y = \{(0,0)\}$, $I(X) + I(Y) = (y - x^2, y) = (x^2, y)$ – not radical

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

- $I \cap J$ is radical. (exercise)

• $I=(f_1,\dots f_k)$, $J=(g_1,\dots g_\ell) \Rightarrow X\cup Y=\{\alpha \mid f_i g_j(\alpha)=0 \ \forall i,j\}$

Since $(f_i g_j \mid i=1,\dots k,\ j=1,\dots \ell) = IJ \Rightarrow X\cup Y = V(IJ)$.

• $(I\cap J)^2 \subset IJ \subset I\cap J$, so $V(IJ)=V(I\cap J)$.

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

Exercise: If $X\cap Y=\emptyset$, then $\mathbb{F}[X\sqcup Y]=\mathbb{F}[X]\oplus\mathbb{F}[Y]$.

• Products:

Proposition: Let $X\subset\mathbb{F}^n$, $Y\subset\mathbb{F}^m$ be algebraic subsets. Then $X\times Y\subset\mathbb{F}^{n+m}$ is algebraic subset & $\mathbb{F}[X\times Y]=\mathbb{F}[X]\otimes_{\mathbb{F}}\mathbb{F}[Y]$.

Proof: $I(X)=(f_1,\dots f_k)\subset\mathbb{F}[x_1,\dots x_n]$, $I(Y)=(g_1,\dots g_\ell)\subset\mathbb{F}[y_1,\dots y_m]$.
$X\times Y=\{(\alpha,\beta)\in\mathbb{F}^n\times\mathbb{F}^m=\mathbb{F}^{n+m} \mid f_i(\alpha)=0,\ g_j(\beta)=0\}$ - alg. subset.

Recall (Example in Section 1 of Lecture 18):
$\mathbb{F}[X]\otimes_{\mathbb{F}}\mathbb{F}[Y]=\mathbb{F}[x_1,\dots x_n,y_1,\dots y_m]/(f_1,\dots f_k,g_1,\dots g_\ell)$

Claim: $\exists$ natural $\pi: \mathbb{F}[X]\otimes_{\mathbb{F}}\mathbb{F}[Y]\twoheadrightarrow\mathbb{F}[X\times Y]$, π is constructed from the following commut. diagram:

$$\begin{tikzcd}
\mathbb{F}[x_1,\dots x_n]\otimes_{\mathbb{F}}\mathbb{F}[y_1,\dots y_m] \arrow[r, "\sim"] \arrow[d, "\text{by } (f_1,\dots f_k, g_1,\dots g_\ell)"] & \mathbb{F}[x_1,\dots x_n,y_1,\dots y_m] \arrow[d, "\text{by } I(X\times Y)\ni f_i, g_j"] \\
\mathbb{F}[X]\otimes_{\mathbb{F}}\mathbb{F}[Y] \arrow[r, dashed, "\pi"] & \mathbb{F}[X\times Y]
\end{tikzcd}$$

so have bottom horizontal map

$\pi(F\otimes G)(\alpha,\beta) = F(\alpha)G(\beta)$.

Remains to show π is injective. Let F_r, $r\in R$, be an $\mathbb{F}$-basis in $\mathbb{F}[X]$; G_s, $s\in S$, $\mathbb{F}$-basis in $\mathbb{F}[Y]$, so $F_r\otimes G_s$ form an $\mathbb{F}$-basis in $\mathbb{F}[X]\otimes_{\mathbb{F}}\mathbb{F}[Y]$. Need to show

$$\underbrace{\pi\Big(\sum_{r,s} a_{rs} F_r\otimes G_s\Big)}_{\text{is a function } X\times Y\to\mathbb{F}}=0 \implies a_{rs}=0.$$

Fix $\beta\in Y$.

Then the function $\sum_{r,s} a_{rs}G_s(\beta)F_r : X\to\mathbb{F}$ is zero

$$\sum_{r,s} a_{rs}G_s(\beta)\underbrace{F_r}_{\text{basis}}\in\mathbb{F}[X] \implies \forall r\ \sum_s a_{rs}G_s(\beta)=0$$

b/c G_s form a basis in $\mathbb{F}[Y]$.

Can vary β: $\sum_s a_{rs}G_s = 0 \implies a_{rs}=0$

$\square$

BONUS: Why Hilbert cared?

This is a continuation of a bonus from Lecture 6. 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.