Lecture 22

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

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

If $F$ infinite field, then $f \in \mathbb{F}[x_1, \ldots, x_n]$ can be viewed as a function \[ F^n \to F; \quad \mathbf{f} \mapsto f \in \mathbb{F}[x_1, \ldots, x_n] \mapsto V(\mathbf{f}) = \{ x \in F^n \mid f_i(x) = 0 \} \]

1.1) Main result.

Q: for which $f \in \mathbb{F}[x_1, \ldots, x_n]$ do we have \( \frac{f}{V(\mathbf{f})} = 0 \)?

Recall: For $A$ a commutative ring, \( I \subset A \) an ideal \( \implies \sqrt{I} = \{ a \in A \mid a^n \in I \text{ for some } n > 0 \} \) — ideal in $A$ containing $I$.

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

Proof: $f^m = g_1 f_1^m + \ldots + g_k f_k^m$ is zero on $V(f_1, \ldots, f_k)$ for some $m \implies f$ is also zero on $V(f_1, \ldots, f_k)$ \( \square \)

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

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

Thm (Hilbert's Nullstellensatz) Let \( F \) be alg. closed, \( f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n] \). If $f$ is zero on $V(f_1, \ldots, f_k) = \{ x \in F^n \mid f_i(x) = 0 \forall i \}$, then $f \in \sqrt{(f_1, \ldots, f_k)}$. 


1.2) Proof

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

Proof: $a$ isn't nilpotent $\Rightarrow$ localization $A[a^{-1}] \cong \{\frac{1}{f} : f \in A, f \neq 0\}$.
$A$ 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 $\mathfrak{m}$.
$\sim A[a^{-1}]/\mathfrak{m}$ is a field & is fin. gen'd over $F$ (by $A[a^{-1}]$ is)

The last corollary in Lec 21 implies that $A[a^{-1}]/\mathfrak{m}$ is a finite ext'n of $F$.
Since $F$ is alg. closed, $A[a^{-1}]/\mathfrak{m} \cong \bar{F}$.

$\varphi : \text{the composition } A \to A[a^{-1}] \to A[a^{-1}]/\mathfrak{m} \sim \bar{F}$.
$\varphi(a) \neq 0$ b/c $\frac{1}{a} \in A[a^{-1}]$ is invertible $\Rightarrow \frac{a}{a} \not\in \mathfrak{m}$

Proof of Thm: $A = \bar{F}[x_1, \ldots, x_n]/(f_1, \ldots, f_k)$, $\varphi : \bar{F}[x_1, \ldots, x_n] \to A$
$a : = \varphi(f)$. Thm $\iff a$ is nilpotent. Assume the contrary.

By Prop'n, $\exists \varphi : A \to \bar{F}$ s.t. $\varphi(a) \neq 0$.
Set $\tilde{\varphi} : = \varphi \varphi : \bar{F}[x_1, \ldots, x_n] \to \bar{F}$.
$\tilde{\varphi}(f) = \varphi(a) \neq 0$.
Set $a_i = \tilde{\varphi}(x_i) \sim a_i = (x_1, \ldots, x_n) \in \bar{F}^n$ so that
$\tilde{\varphi}(f) = f(a)$. But $\tilde{\varphi}(f_i) = 0$ b/c $f_i \in \ker \varphi \Rightarrow a \in V(f_1, \ldots, f_k)$.
$\Rightarrow \tilde{\varphi}(f) = f(a) = 0$. Contradiction.

1.3) Corollaries.

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

Corollary of the proof of Thm: There are bijections between:

2}
(i) \( V(f_1, \ldots, f_k) \)

(ii) \( \{ F\text{-algebra homomorphism} A \rightarrow \mathbb{F}^n, A = \mathbb{F}[x_1, \ldots, x_n]/(f_1, \ldots, f_k) \} \)

(iii) \( \{ \text{maximal ideals of } A \mathbb{F}^n \} \)

e.g. \( \alpha \in V(f_1, \ldots, f_k) \sim \varphi_{\alpha}: A \rightarrow \mathbb{F} \) given by \( \varphi_{\alpha}(f) = f(\alpha) \).

Exer. For \( f_1, \ldots, f_k \subseteq \mathbb{F}[x_1, \ldots, x_n] \) TFAE:

1. \( V(f_1, \ldots, f_k) = \emptyset \).
2. Ideal \( (f_1, \ldots, f_k) \) coincides with \( \mathbb{F}[x_1, \ldots, x_n] \).

2) Algebraic subsets vs radical ideals

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

Defn: A is a commutative ring. An ideal \( I \subseteq A \) is radical if \( I = \sqrt{I} \).

Defn: For \( I \subseteq \mathbb{F}[x_1, \ldots, x_n] \) ideal, define \( V(I) = \{ \alpha \in \mathbb{F}^n \mid f(\alpha) = 0 \text{ for all } f \in I \} \).

Note: if \( I = (f_1, \ldots, f_k) \) and any ideal has this form \( I \subseteq \mathbb{F}[x_1, \ldots, x_n] \) is Noetherian then \( V(I) = V(f_1, \ldots, f_k) \).

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

Defn: \( \text{Subset } X \subseteq \mathbb{F}^n \) is algebraic if \( X = V(I) \) for some ideal \( I \subseteq \mathbb{F}[x_1, \ldots, x_n] \), equiv. \( X = V(f_1, \ldots, f_k) \) for some \( f_1, \ldots, f_k \subseteq \mathbb{F}[x_1, \ldots, x_n] \).

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

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

Gr: \( \mathbb{F}[x_1, \ldots, x_n] \rightarrow \mathbb{F}[x_1, \ldots, x_n]/I(X), f \mapsto f|_X \).

An element of \( \mathbb{F}[X] \) can be viewed as a function \( X \rightarrow \mathbb{F} \).
22) Basic properties:

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

\[
\begin{align*}
&\text{[radical ideals in } \mathbb{F}[x_1, ..., x_n]\text{]} \\
&\text{[algebraic subsets in } \mathbb{F}^n\text{]}.
\end{align*}
\]

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

- \( \forall \text{ radical } I \Rightarrow I = I(V(I)) \) - by Nullstellensatz
- \( \forall \text{ algebraic subsets } X \subseteq \mathbb{F}^n \Rightarrow X = V(I(X)) \): note \( X = V(J) \) for some radical ideal \( J \). So we get,
  \( V(I(V(J))) = V(J) \) 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. 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)
Since \( (f_i g_j \mid i = 1, \ldots, k, j = 1, \ldots, l) = IJ \Rightarrow XUY = V(IJ) \)

\[(I \cap J)^2 \subset IJ \cap I \cap J, \text{ so } V(IJ) = V(I \cap J).\]

\((b) \ X \cap Y = V(t_1, \ldots, t_k, q_1, \ldots, q_l) = I + J \quad \text{so} \quad X \cap Y = V(I + J) \Rightarrow I(X \cap Y) = \sqrt{I + J} \quad \Box \]

**Exercise:** If \( X \cap Y = \emptyset \), then \( \mathcal{F}[X \cup Y] = \mathcal{F}[X] \oplus \mathcal{F}[Y] \).

**Products:**

**Proposition:** Let \( X \subset \mathcal{F}^n \), \( Y \subset \mathcal{F}^m \) be algebraic subsets. Then \( X \times Y \subset \mathcal{F}^{n+m} \) is algebraic subset & \( \mathcal{F}[X \times Y] = \mathcal{F}[X] \otimes \mathcal{F}[Y] \).

**Proof:** \( I(X) = (t_1, \ldots, t_k) \subset \mathcal{F}[x_1, \ldots, x_n] \), \( I(Y) = (y_1, \ldots, y_l) \subset \mathcal{F}[y_1, \ldots, y_m] \).

\( X \times Y = \{(x, y) \in \mathcal{F}^n \times \mathcal{F}^m \mid f(x) = 0, g(y) = 0 \} \) - alg subset.

Recall (Example in Section 1 of Lecture 7):

\( \mathcal{F}[X] \otimes \mathcal{F}[Y] = \mathcal{F}[x_1, \ldots, x_n, y_1, \ldots, y_m]/(t_1, \ldots, t_k, q_1, \ldots, q_l) \)

**Claim:** \( \exists \) natural \( \Theta: \mathcal{F}[X] \otimes \mathcal{F}[Y] \longrightarrow \mathcal{F}[X \times Y] \), \( \Theta \) is constructed from the following commutative diagram:

\[
\begin{array}{ccc}
\mathcal{F}[x_1, \ldots, x_n] \otimes \mathcal{F}[y_1, \ldots, y_m] & \xrightarrow{\sim} & \mathcal{F}[x_1, \ldots, x_n, y_1, \ldots, y_m] \\
\downarrow \text{by } (t_1, \ldots, t_k, q_1, \ldots, q_l) & & \downarrow \text{by } I(X \times Y) \oplus f_i, g_j \\
\mathcal{F}[X] \otimes \mathcal{F}[Y] & \xrightarrow{\Theta} & \mathcal{F}[X \times Y]
\end{array}
\]

horizontal map
\[ \mathcal{D}(F \otimes G)(\alpha, \beta) = F(\alpha) G(\beta). \]

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

\[ \mathcal{D}\left( \sum_{r,s} a_{rs} F_r \otimes G_s \right) = 0 \implies a_{rs} = 0. \]

is a function \( \times \times Y \rightarrow \mathbb{F} \).

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

\[ \sum_{r,s} a_{rs} G_s(\beta) F_r \in F[X] \implies \forall \ r \ \sum_{s} a_{rs} G_s(\beta) = 0 \]

basis \( C \) \( \mathcal{D}_r G_s \) form a basis in \( F[Y] \).

Can vary \( \beta : \sum_{s} a_{rs} G_s = 0 \implies a_{rs} = 0 \)

\[ \square \]

**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 \( 2 \times 2 \) 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 $n=2$, $V = \{a x^2 + b x y + c y^2\}$. We can represent
an element of $U$ as a matrix $(a \ b \ c)$, then $g \in S_2(\mathbb{C})$ acts by
$g \cdot (a \ b \ c) = g(a \ b \ c) g^T$. 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 $\mathbb{C}[U]$.
- $f$ 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 algebraic geometric...
objects in the 60's - which brought him a Fields medal.