1) **Hilbert’s Nullstellensatz.**

Let \( F \) be an infinite field, then \( f \in [F[x_1, \ldots, x_n]] \) can be viewed as a function \( \mathbb{F}^n \rightarrow \mathbb{F} \) & \( f \) is uniquely recovered from this function.

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

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

1.1) **Main result.**

Q: For \( \Psi_1, \Psi_2 \subset [F[x_1, \ldots, x_n]] \) find necessary & sufficient cond. for \( V(\Psi_1) = V(\Psi_2) \)

Recall: For \( A \) a commutative ring, \( I \subset A \) an ideal \( \Rightarrow \sqrt{I} = \{ a \in A | a^m \in I \text{ for some } m > 0 \} \) - 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 $f_i|_X = 0 \Rightarrow f^m|_X = 0 \Rightarrow f|_X = 0 \quad \square$

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

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

**Remarks:**
1) The conclusion of Thm is false over $\mathbb{R}$: Take $\Psi = \{x^2 + 1\}$, $\Rightarrow V(\Psi) = \emptyset$ & $f = 1$. But $\sqrt{I_\Psi} = I_\Psi \neq 1$.
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 $F$ is alg. closed. Show $V(\Psi) = \emptyset \iff I_\Psi = F[x_1, \ldots, x_n]$.

1.2) **Proof of Nullstellensatz**

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

1) We establish a bijection $X \cong \text{Hom}(A, F)$ (w. Hom := Hom$_{F-\text{Alg}}$)
2) From here we deduce $\text{Hom}_{F-\text{Alg}}(A[a^{-1}], F) = \emptyset$
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) \( x \in X \mapsto \text{ev}_x : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}, f \mapsto f(x) \), then \( \text{ev}_x \in \text{Hom}(\mathbb{F}, \mathbb{F}) \). Since \( f(x) = 0 \nRightarrow f \in I \), \( \text{ev}_x \) factors through \( A \to \mathbb{F} \). The resulting homomorphism is also denoted by \( \text{ev}_x \).

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

**Exercise:** \( a_{\varphi} \in X \) \& \( \varphi \mapsto a_{\varphi} \) are mutually inverse maps \( X \leftrightarrow \text{Hom}(A, \mathbb{F}) \).

2) \( \text{Hom}(A[\alpha^{-1}], \mathbb{F}) \leftrightarrow [\text{univ. property of localization}] \{ \varphi \in \text{Hom}(A, \mathbb{F}) \mid \varphi(\alpha) \text{ is invertible} \} \leftrightarrow [\text{Step 1}] \{ x \in X \mid 0 \neq \text{ev}_x(\alpha) = \text{ev}_x(f) = f(\alpha) \} = \emptyset \)

b/c \( f|_X = 0 \).

3) Suppose \( A[\alpha^{-1}] \neq \{0\} \). Note that \( A[\alpha^{-1}] \) is fin.gen'd (by \( \overline{x}_i \) \& \( \frac{1}{\alpha} \))

Let \( \mathfrak{m} \subseteq A[\alpha^{-1}] \) be a max ideal. Then \( A[\alpha^{-1}]/\mathfrak{m} \) is fin.gen'd \( \mathbb{F} \)-algebra that is also a field. By Important Corollary in Sec 2 of Lec22, \( A[\alpha^{-1}]/\mathfrak{m} \) is finite field extension of \( \mathbb{F} \). Since \( \mathbb{F} \) is alg. closed, \( A[\alpha^{-1}]/\mathfrak{m} \cong \mathbb{F} \). We've got an \( \mathbb{F} \)-algebra homomorphism \( A \to A[\alpha^{-1}]/\mathfrak{m} \)

\( \cong \mathbb{F} \). Contradiction w. Step 2.

4) Recall, Exer. in Sec 2 of Lec8, that for \( S \subseteq A \), a multiplicative subset, \( A[S^{-1}] = \{0\} \iff 0 \in S \). Apply this to \( S = \{\alpha \mid \alpha \neq 0, 3 \} \) so that \( A[S^{-1}] = A[\alpha^{-1}] \) and get \( 0 \in \{3^{-1}\} \), which is what we need to prove. \( \square \)
Corollary: \( \mathbb{F} \) is alg. closed, \( A := \mathbb{F}[x_1, \ldots, x_n]/I \Phi, \ X = V(\Phi) \). The following sets are in bijection.

(i) \( X \).

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

(iii) \( \{ \text{max. ideals } \mathfrak{m} \in A \} \).

Proof:

Bijections (i) \( \leftrightarrow \) (ii) are constructed in Step 1.

(ii) \( \rightarrow \) (iii): \( \Phi \mapsto \ker \Phi \) is maximal b/c \( A/\ker \Phi \) \( \cong \text{im} \Phi = [\Phi \text{ is an } \mathbb{F} \text{-alg. homomorphism}] = \mathbb{F} \), a field.

(iii) \( \rightarrow \) (ii): As in Step 3, \( A/\mathfrak{m} \cong \mathbb{F} \) (\( \mathbb{F} \)-alg. iso, unique b/c \( 1 \mapsto 1 \)).

We send \( \mathfrak{m} \) to \( A \mapsto A/\mathfrak{m} \mapsto \mathbb{F} \).

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

Exercise: If \( A \) is a finitely generated \( \mathbb{F} \)-alg, then \( \sqrt{0} = \cap \) 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 \( I = \sqrt{I} \).

\[ \cdot \] A subset \( X \subset \mathbb{F}^n \) is algebraic if \( X = V(\Psi) \) for some \( \Psi \subset \mathbb{F}[x_1, \ldots, x_n] \).
· For \( X \subset \mathbb{F}^n \) algebraic, consider its vanishing ideal \( I(X) = \{ f \in \mathbb{F}[x_1, \ldots, x_n] \mid f_x = 0 \} \) and its algebra of polynomial functions \( \mathbb{F}[x] = \mathbb{F}[x_1, \ldots, x_n]/I(X) \).

Remarks: 1) By Lemma in Sec 1.1, \( X = V(\sqrt{I(Y)}) \) is a finitely generated ideal (since \( \mathbb{F}[x_1, \ldots, x_n] \) is Noetherian). If \( f_1, \ldots, f_k \) are generators, then \( X = V(f_1, \ldots, f_k) \). In particular, in the study of algebraic subsets \( V(Y) \), it’s enough to assume \( Y \) is finite.

2) \( I(X) \) is a radical ideal (exercise). Elements of \( \mathbb{F}[x] \) can be viewed as functions on \( X \) for \( x \in X \) & \( f \in \mathbb{F}[x_1, \ldots, x_n] \), the value \( f(x) \) only depends on \( f + I(X) \) - by defn 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:

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

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) \( I = I(V(I)) \): \( I(V(I)) = \{ f \mid f \text{ is 0 on } V(I) \} \)

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

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 with $I(X \cup Y) = I(X) \cap I(Y)$.
(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 $I = (f_1, \ldots, f_k), J = (g_1, \ldots, g_l) \Rightarrow X \cap Y = \{a \in \mathbb{F}^n | f_j(a) = 0 \neq i, j \leq k \}$
Since \((f_i g_j | i=1...k, j=1...l) = IJ \Rightarrow XVY = V(IJ)\)

\cdot (IJ)^2 \subset IJ \subset I\Lambda J, so \sqrt{IJ} = I\Lambda J \& V(IJ) = V(I\Lambda J).

(6) \(XNY = V(f_1...f_k, g_1...ge) \& (f_1...f_k, g_1...ge) = I+J\) So

\(XNY = V(I+J) \Rightarrow I(XNY) = \sqrt{I+J} \)

\(\Box\)

Exercise: if \(XNY = \emptyset\), then \([F[X \cup Y]] = [F[X]] \times [F[Y]]\).

**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 \(SL_2(C)\), the group of \(2 \times 2\) matrices \(w. det = 1\), that acts on \(V\) by linear changes of the variables.

The algebra of invariants \([C[U]]^G\) is graded. So it has finitely many homogeneous generators and every minimal collection of generators has the same number of elements (Exercise).

Example: for \(n=2\), \(V = \{ax^2 + 2bx + cy^2\} \). We can represent an
element of \( U \) as a matrix \((\begin{smallmatrix} a & b \\ c & d \end{smallmatrix})\), then \( g \in S_2(\mathbb{C}) \) acts by 
\[ g \cdot (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) = g'(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix})g^{\top}. \]
The algebra of invariants is generated by a single degree 2 polynomial \( ac - bd \), 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. degree 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 algebraic geometric objects in the 60s - 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 in the ring $\mathbb{F}[x_1, \ldots, x_n]$, 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 $F_1, \ldots, F_k \in \mathbb{F}[x_1, \ldots, x_n]$, can we determine whether $(F_1, \ldots, F_k)$ is radical or prime?

As usual, the answer is both Yes & No.

Yes: for given $n, k$ ($\& F_1, \ldots, F_k$) 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 [EJ], 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, $\text{Mat}_n(\mathbb{C})^2 \approx \mathbb{C}^{2n^2}$. 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
\[
\begin{pmatrix}
  x_{11} & x_{12} \\
  x_{21} & x_{22}
\end{pmatrix}
\begin{pmatrix}
  y_{11} & y_{12} \\
  y_{21} & y_{22}
\end{pmatrix}
= 
\begin{pmatrix}
  x_{11} y_{11} - y_{12} x_{11} & x_{11} y_{12} + x_{12} y_{12} - y_{11} x_{22} \\
  x_{21} y_{11} + x_{22} y_{12} - y_{21} x_{11} & x_{22} y_{12} - x_{21} y_{11}
\end{pmatrix}
\]

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

Open problem: is $I$ radical?