Lecture 22.

1) **Hilbert’s Nullstellensatz.**

References: [E], Sections 1.6, 4.5, 13.2; [V] Section 94.

**BONUS: Why Hilbert cared.**

1) **Hilbert’s Nullstellensatz.**

If $F$ is an infinite field, then $f \in [F[x_1, \ldots, x_n]]$ can be viewed as a function $F^n \to F$; $f_{x_1, \ldots, x_n} \in [F[x_1, \ldots, x_n]] \mapsto V(f_{x_1, \ldots, x_n}):= \{ \alpha \in F^n | f_i(\alpha) = 0 \}$

11) **Main result.**

Q: For which $f \in [F[x_1, \ldots, x_n]]$ do we have $f|_{V(f_{x_1, \ldots, x_n})} = 0$?

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

**Lemma:** If $f \in \sqrt{f_{x_1, \ldots, x_n}} \implies f$ is zero on $V(f_{x_1, \ldots, x_n})$.

**Proof:** $f^n = g_1f_{x_1, \ldots, x_n} + \cdots + g_kf_{x_1, \ldots, x_n}$ is zero on $V(f_{x_1, \ldots, x_n})$ for some $m \implies f$ is also zero on $V(f_{x_1, \ldots, x_n})$. $\square$

If $F$ is not alg. closed, “$\implies$” may fail to be true: $f \in [R[x_1]]$, $f = x^2 + 1 \implies V(f) = \emptyset$, $1 \notin \sqrt{\langle x^2 + 1 \rangle}$ is zero on $V(f)$. 

1
Theorem (Hilbert's Nullstellensatz). Let $\mathbb{F}$ be algebraically closed, $f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$. If $f$ is 0 on $V(f_1, \ldots, f_k)$, then $f \in (f_1, \ldots, f_k)$.

1.2) Noether normalization lemma

The proof is based on a number of auxiliary statements. This is the most important one.

Theorem (Noether). Let $\mathbb{F}$ be a field, $A$ a finitely generated $\mathbb{F}$-algebra. Then $\exists$ inclusion $\mathbb{F}[x_1, \ldots, x_m] \hookrightarrow A$ s.t. $A$ is finite over $\mathbb{F}[x_1, \ldots, x_m]$ (for some $m \geq 0$).

We'll only prove this when $\mathbb{F}$ is infinite, where a proof is easier. For a general case, see [E], Lemma 13.2 & Theorem 13.3.

Key lemma: Assume $\mathbb{F}$ is infinite, $F \in \mathbb{F}[x_1, \ldots, x_n]$ be nonzero. Then $\exists \mathbb{F}$-linear combinations $y_1, \ldots, y_{n-1}$ of variables $x_1, \ldots, x_n$ s.t. $\mathbb{F}[x_1, \ldots, x_n]/(F)$ is finite over $\mathbb{F}[y_1, \ldots, y_{n-1}]$.

Proof of lemma:

$F = f_0 + \cdots + f_k$, $f_i$ is homogeneous of degree $i$, $f_k \neq 0$.
Special case: $f_k(0, \ldots, 0, 1) \neq 0 \iff x_k$ appears in $f_k$ w. nonzero coeff. Now view $F \in \mathbb{F}[x_1, \ldots, x_n, x_n]/[x_n]$, has leading coeff. $\neq 0$ i.e. invertible in $\mathbb{F}[x_1, \ldots, x_n]/(F)$ is integral over $\mathbb{F}[x_1, \ldots, x_n, x_n]/[x_n]$. By the theorem in Sect. 1.2) of
Lecture 9, \( \mathbb{F}[x_1, \ldots, x_n]/(\mathbb{F}) \) is finite over \( \mathbb{F}[x_1, \ldots, x_n] \). Set \( y_i := x_i \).

General case: \( f_k \neq 0 \) & \( \mathbb{F} \) is infinite \( \Rightarrow f_k(a_1, \ldots, a_n) \neq 0 \) for some \( a_i \in \mathbb{F} \). Pick invertible \( \Phi \in \text{Mat}_{n \times n}(\mathbb{F}) \) s.t.

\[
\Phi \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.
\]

Consider \( F^\Phi = F \circ \Phi \) as a function \( \mathbb{F}^n \to \mathbb{F} \) (polynomial obtained from \( F \) by linear change of variables). Then \( f_k^\Phi(0, \ldots, 0, 1) = f_k(a_1, \ldots, a_n) \neq 0 \) So

\[
\mathbb{F}[x_1, \ldots, x_n]/(\mathbb{F}^\Phi) \text{ is finite over } \mathbb{F}[x_1, \ldots, x_n], \text{ hence } \]

\[
I \uparrow \Phi^{-1}
\]

\[
\mathbb{F}[x_1, \ldots, x_n]/(\mathbb{F}) \text{ is finite over } \mathbb{F}[y_1, \ldots, y_n] \text{ w.r. to } \]

\[
\left( \begin{array}{c} y_1 \\ \vdots \\ y_n \end{array} \right) := \Phi^{-1} \left( \begin{array}{c} x_1 \\ \vdots \\ x_n \end{array} \right)
\]

\[ \square \]

Proof of Thm: Let \( X = \{ n \in \mathbb{Z}_{\geq 0} \} \) \( \exists \mathbb{F} \)-algebra homomorphism \( \mathbb{F}[x_1, \ldots, x_n] \to A \) s.t. \( A \) is finite over \( \mathbb{F}[x_1, \ldots, x_n] \); \( X \neq \emptyset \).

\( \text{b/c } A \text{ is finitely generated & so } \mathbb{F}[x_1, \ldots, x_n] \to A \) for some \( n \).

Set \( m = \min X \) \( \Rightarrow y : \mathbb{F}[x_1, \ldots, x_m] \to A \) s.t. \( A \) is finite over \( \mathbb{F}[x_1, \ldots, x_m] \).

Claim: \( y \) is injective.

Assume the contrary: \( \exists F \in \ker y, F \neq 0 \). By Key Lemma

\[
\mathbb{F}[x_1, \ldots, x_m]/(\mathbb{F}) \text{ is finite over } \mathbb{F}[y_1, \ldots, y_m] \text{ &}
\]

[3]
A is finite over \([F[x_1, \ldots, x_m]]/(F)\) (i.e., \(y\) factors through \([F[x_1, \ldots, x_m]]/(F)\)). By Lemma 1 of Section 1.2 in Lecture 9, A is finite over \([F[y_1, \ldots, y_m]]\), contradiction with choice of m. □

Important corollary: Let \(F\) be an infinite field, let \(A\) be a fin gen'd \(F\)-algebra. If \(A\) is a field, then \(\dim_F A < \infty\).

Proof: By Thm, \([F[x_1, \ldots, x_m]] \hookrightarrow A\) s.t. \(A\) is finite over \([F[x_1, \ldots, x_m]]\). Need to show \(m = 0\). Assume the contrary. Since \(A\) is a field, the image of \(x_i\) is invertible, so \([F[x_1, \ldots, x_m]] \hookrightarrow A\) extends to \([F[x_1, x_2, \ldots, x_m]] [x_i^{-1}] \subseteq [F[x_1, x_2, \ldots, x_m]] \hookrightarrow A\):
\[
[F[x_1, \ldots, x_m]] \hookrightarrow [F[x_1, x_2, \ldots, x_m]] \hookrightarrow A.
\]
\(A\) is fin gen'd over \([F[x_1, \ldots, x_m]]\) & \([F[x_1, \ldots, x_m]]\) is Noetherian ⇒ \([F[x_1, x_2, \ldots, x_m]]\) is a finitely generated \([F[x_1, \ldots, x_m]]\)-module.

But this is not true: the \([F[x_1, \ldots, x_m]]\)-submodule generated by \(x_i^{-d_i} F_i, i = 1, \ldots, l\) is contained in \(x_i^{-d}[F[x_1, \ldots, x_m]]\) with \(d = \max \{d_i\}\). Contradiction with \(m > 0\). □

1.3) Proof of Nullstellensatz

Proposition: \(F\) is alg. closed, \(A\) is fin gen'd commutative \(F\)-algebra. If \(a \in A\) isn’t nilpotent (\(a^m \neq 0\) for \(m\)), then \(\exists F\)-alg. homom \(\phi: A \rightarrow F\) s.t. \(\phi(a) \neq 0\).

Proof: \(a\) isn’t nilpotent: \(0 \neq \{a^n\} \Rightarrow\) localization \(A[a^{-1}] \neq \{0\}/A\)
A is fin. gen'd $F$-algebra $\Rightarrow A[a^{-1}]$ is also fin. gen'd. Since $A[a^{-1}] \neq \{0\}$, by Section 2.2 in Sec. 2, $A[a^{-1}]$ has a max. ideal, $\mathfrak{m}$, and $A[a^{-1}]/\mathfrak{m}$ is a field & is fin. gen'd over $F$ (b/c $A[a^{-1}]$ is)

The important corollary implies that $A[a^{-1}]/\mathfrak{m}$ is a finite extension of $F$. Since $F$ is alg. closed, $A[a^{-1}]/\mathfrak{m} \cong F$.

$g: = \text{the composition } A \rightarrow A[a^{-1}] \rightarrow A[a^{-1}]/\mathfrak{m} \rightarrow F$

$\quad g(a) \neq 0$ b/c $\frac{a}{f} \in A[a^{-1}]$ is invertible and so $\frac{a}{f} \notin \mathfrak{m}$ \quad \square

Proof of Nullstellensatz: $A := \mathbb{F}[x_1, \ldots, x_n]/(f_1, \ldots, f_k)$, $\varpi: \mathbb{F}[x_1, \ldots, x_n] \rightarrow A$, $a := \varpi(f)$. Thm $\iff a$ is nilpotent. Assume $a$ isn't nilpotent.

By Prop'n, $\exists \varphi: A \rightarrow [F | g(a) \neq 0$; set $\tilde{\varphi} := \varphi \circ \varpi: \mathbb{F}[x_1, \ldots, x_n] \rightarrow \mathbb{F}$, $\tilde{\varphi}(f) = \varphi(a) \neq 0$. Set $d_i = \tilde{\varphi}(x_i) \rightarrow \tilde{a} := (d_1, \ldots, d_n) \in \mathbb{F}^n$ so that $\tilde{\varphi}(f) = f(\tilde{a})$. But $\tilde{\varphi}(f_i) = 0$ b/c $f_i \in \ker \tilde{\varphi} \Rightarrow a \in V(f_1, \ldots, f_k)$.

$\Rightarrow \tilde{\varphi}(f) = f(\tilde{a}) = 0$. Contradiction \quad \square

1.4) Corollaries

Corollary of Prop'n in Sec. 1.3: If $A$ is a fin. gen'd $F$-algebra, then $\sqrt{\{0\}} = \bigcap$ of all max. ideals in $A$.

Corollary of the proof of Thm & of Important corollary:

Let $A := \mathbb{F}[x_1, \ldots, x_n]/(f_1, \ldots, f_k)$. Suppose $F$ is algebraically closed.

Then there are bijections between:

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

(ii) $\{F$-algebra homomorphism $A \rightarrow F \}$
(iii) \{ \text{maximal ideals of } A^g \}

(i) \rightarrow (ii): \alpha \in V(f_1, \ldots, f_k) \rightarrow \varphi_\alpha: A \to \mathbb{F} \text{ given by } \varphi_\alpha(f) = f(\alpha).

(ii) \rightarrow (iii): \varphi \mapsto \ker \varphi

Exercise: For \(f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n] \) TFAE:

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

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 \(S_2(\mathbb{C})\), the group of \(2 \times 2\) matrices \(w\) \(\det w = 1\), 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 \((a \ b)\), then \(g \in S_2(\mathbb{C})\) acts by \(g \cdot (a/bc) = g (a/bc) g^T\). The algebra of invariants is generated by 

\[g \cdot (a/bc) g^T\]
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:**

1. \( f \) lies in the common set of zeroes of homogeneous generators of \( C[U]^5 \).
2. \( f \) has a linear factor of multiplicity \( \geq \frac{n}{2} \).

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 algebra geometric objects in the 60's – which brought him a Fields medal.