Today: Hilbert's Nullstellensatz.

Original context was the theory of invariants, i.e., (homogeneous) polynomials invariant under a fixed subgroup of $GL_n(\mathbb{F})$. Hilbert's first major theorem was to prove that such a ring of invariants is always finitely generated. By solving the major open problem, he drained the energy from the subject for a time...

Hilberts NSS: Let $\mathbb{F}$ be alg closed, consider an intersection of hypersurfaces:

$$V = V_{f_1} \cap V_{f_2} \cap \cdots \cap V_{f_m}.$$

(Weak NSS): If $V = \emptyset$ then

$\exists\, \tilde{f}_1, \ldots, \tilde{f}_n$ s.t. $1 = f_1 \tilde{f}_1 + \cdots + f_m f_m$.

(Strong NSS): If g vanishes on V then $\exists\ \tilde{f}_1, \ldots, \tilde{f}_m$ & $r \geq 0$ s.t.

$$g^r = f_1 \tilde{f}_1 + \cdots + f_m \tilde{f}_m .$$

///

Remarks:

- Strong $\Rightarrow$ Weak: $g = 1$ vanishes on the empty set.
- But also Weak $\Rightarrow$ Strong, by the trick of Rabinowitsch (1929).
- Compare to Study's Lemma.

If g vanishes on V_f then the square-free part divides g: $\sqrt{f} \mid g$.
Equivalently: $f \mid g^r$ for some $r \geq 1$.

Proof: Weak: Define the ideal

$$I = f_1 \mathbb{F}[\vec{x}] + \cdots + f_m \mathbb{F}[\vec{x}] .$$

Observe $p \in V \iff f(\vec{p}) = 0 \ \forall f \in I$.

If $V = \emptyset$ will will prove $1 \in I$, equivalently $I = \mathbb{F}[\vec{x}]$. Will use induction on # variables n.

$(n=1)$: $\mathbb{F}[x]$ is a PID, hence

$I = f(x)\mathbb{F}[x]$ for some f. If $I \neq \mathbb{F}[x]$ then f is not constant, hence $f(p) = 0$ for some $p \in \mathbb{F}$, which implies $p \in V$.

$(n \geq 2)$: Now $\mathbb{F}[\vec{x}] = \mathbb{F}[x_1, \dots, x_n]$ is not a PID :(.

Normalization: For any $A \in GL_n(\mathbb{F})$, $AV \subseteq \mathbb{F}^n$ equals the intersection of hypersurfaces $AV_{f_i} : f_i(A^{-1}\vec{x}) = 0$.

Since A invertible:

$$AV = \emptyset \iff V = \emptyset$$

Since A is a ring automorphism

$\mathbb{F}[\vec{x}] \to \mathbb{F}[\vec{x}]$ we have

$$AI = \{ f(A^{-1}\vec{x}) : f \in I \} = \mathbb{F}[\vec{x}]$$

$\iff I = \mathbb{F}[\vec{x}]$. From Normalization Lemma we may choose A & $f \in I$ so $f(A^{-1}\vec{x}) = c x_n^d +$ lower terms.

Summary: We may assume $\exists f \in I$ with $f = c x_n^d +$ lower terms. ///

Elimination Step:

Let $\vec{x}' = (x_1, \ldots, x_{n-1})$, $I' = I \cap \mathbb{F}[\vec{x}']$.

Since $1 \notin I$, have $1 \notin I'$, hence by induction $\exists \vec{p}' = (p_1, \ldots, p_{n-1}) \in \mathbb{F}^{n-1}$ such that $f(\vec{p}') = 0 \ \forall f \in I'$.

Now consider the set

$$J = \{ f(\vec{p}', x_n) : f \in I \} \subseteq \mathbb{F}[x_n],$$

which is an ideal. If $1 \notin J$ then from base case $\exists p_n \in \mathbb{F}$

so that $f(\vec{p}) = f(\vec{p}\,', p_n) = 0$ for all $f \in I$, hence $\vec{p} \in V$, i.e. $V \neq \emptyset$. Done.

Assume for contradiction $1 \in J$.

Hence $1 = g(\vec{p}\,', x_n)$ for some $g \in I$.

Expand $g(\vec{x})$ in powers of x_n:

$$g = b_0(\vec{x}\,')x_n^e + \cdots + b_{e-1}(\vec{x}\,')x_n + b_e(\vec{x}\,')$$

$$1 = g(\vec{p}\,', x_n) = b_0(\vec{p}\,')x_n^e + \cdots + b_e(\vec{p}\,') \in \mathbb{F}[x_n]$$

$$\Rightarrow \quad b_0(\vec{p}\,') = \cdots = b_{e-1}(\vec{p}\,') = 0$$

$$b_e(\vec{p}\,') = 1.$$

Recall: From normalization we have some $f \in I$ of the form

$$f(\vec{x}) = cx_n^d + a_1(\vec{x}\,')x_n^{d-1} + \cdots + a_d(\vec{x}\,').$$

$$f(\vec{p}\,', x_n) = cx_n^d + a_1(\vec{p}\,')x_n^{d-1} + \cdots + a_d(\vec{p}\,').$$

We will obtain a contradiction by

considering the resultant

$$\mathrm{Res}_{x_n}(f, g) \in \mathbb{F}[\vec{x}'].$$

- Since $\mathrm{Res}_{x_n}(f,g)$ is an $\mathbb{F}[\vec{x}]$-linear combination of f & g, have $\mathrm{Res}_{x_n}(f,g) \in I \cap \mathbb{F}[\vec{x}'] = I'$, hence by definition of $\vec{p}' \in \mathbb{F}^{n-1}$,

$$\mathrm{Res}_{x_n}(f,g)(\vec{p}') = 0.$$

- On the other hand:

$$\mathrm{Res}_{x_n}(f,g)(\vec{p}')$$

$$= \pm \det \begin{pmatrix} c & a_1(\vec{p}') & \cdots & a_d(\vec{p}') & & \\ & \ddots & & & \ddots & \\ & & c & a_1(\vec{p}') & \cdots & a_d(\vec{p}') \\ & & & 1 & & \\ & 0 & & & \ddots & \\ & & & & & 1 \end{pmatrix}$$

$$= \pm c^e \neq 0.$$

///

(Strong): Assume g vanishes on

$$V = V_{f_1} \cap \cdots \cap V_{f_m} \subseteq \mathbb{F}^n.$$

i.e. $f_1(\vec{p}) = \cdots = f_m(\vec{p}) = 0 \implies g(\vec{p}) = 0.$

TRICK: Introduce new variable y & consider polynomials

$$f_1, f_2, \dots, f_m, 1 - yg \in \mathbb{F}[\vec{x}, y],$$

consider intersection of hyp. surfaces one dimension higher:

$$V^+ = V_{f_1} \cap \cdots \cap V_{f_m} \cap V_{1-yg} \subseteq \mathbb{F}^{n+1}.$$

By construction, $V^+ = \emptyset$ since

$(\vec{p}, q) \in V_{f_1} \cap \cdots \cap V_{f_m} \Rightarrow f_1(\vec{p}) = \cdots = 0.$

$\Rightarrow 1 - yg(\vec{x}) \rightsquigarrow 1 - qg(\vec{p}) = 1 \neq 0.$

$\Rightarrow (\vec{p}, q) \notin V_{1-yg}.$

Weak NSS $\implies \exists\ \tilde{h}_1, \dots, \tilde{h}_m, \tilde{s}$

in $\mathbb{F}[\vec{x}, y]$ s.t.

$$1 = f_1(\vec{x})\, h_1(\vec{x}, y) + \cdots + f_m(\vec{x})\, \widetilde{h}_m(\vec{x}, y)$$
$$+ \left(1 - y\, g(\vec{x})\right) \tilde{g}(\vec{x}, y).$$

Finally subs $y = 1/g(\vec{x}) \in \mathbb{F}(\vec{x})$

to get identity in field of fractions:

$$1 = f_1 \tilde{h}_1(\vec{x}, \tfrac{1}{g}) + \cdots + f_m h_m(\vec{x}, \tfrac{1}{g}) + 0.$$

$$1 = \left(f_1 \tilde{f}_1 + \cdots + f_m \tilde{f}_m\right) / g^r$$

for some $r \geq 0$, hence

$$g^r = f_1 \tilde{f}_1 + \cdots + f_m \tilde{f}_m.$$

QED.

Next time: The modern form of NSS

$$\text{Varieties} \;\underset{V}{\overset{I}{\rightleftarrows}}\; \text{Ideals}$$