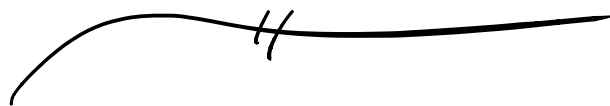


Today: Hilbert's Nullstellensatz.

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...



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

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

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

$$\exists \hat{f}_1, \dots, \hat{f}_m \text{ s.t. } 1 = f_1 \hat{f}_1 + \dots + f_m \hat{f}_m.$$

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

$$g^r = \sum_1 \tilde{f}_1 + \dots + \sum_m \tilde{f}_m. \quad \text{//}$$

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  $V_S$  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

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

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

If  $V = \emptyset$  will will prove  $1 \in \mathcal{I}$ ,

equivalently  $\mathcal{I} = \mathbb{F}[\vec{x}]$ . Will use induction on # variables  $n$ .

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

$\mathcal{I} = f(x)\mathbb{F}[x]$  for some  $f$ . If

$\mathcal{I} \neq \mathbb{F}[x]$  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  $\smile$ .

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:

$$AV = \emptyset \Leftrightarrow V = \emptyset$$

Since  $A$  is a ring automorphism

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

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

$\Leftrightarrow \mathbb{I} = \mathbb{F}[\vec{x}']$ . From Normalization

Lemma we may choose  $A$  &  $f \in \mathbb{I}$

so  $f(A^{-1}\vec{x}) = cx_n^d + \text{lower terms}$ .

Summary: We may assume  $\exists f \in \mathbb{I}$   
with  $f = cx_n^d + \text{lower terms}$ . ///

Elimination Step:

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

Since  $1 \notin \mathbb{I}$ , have  $1 \notin \mathbb{I}'$ , hence by

induction  $\exists \vec{p}' = (p_1, \dots, p_{n-1}) \in \mathbb{F}^{n-1}$

such that  $f(\vec{p}') = 0 \quad \forall f \in \mathbb{I}'$ .

Now consider the set

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

which is an ideal. If  $1 \notin \mathbb{J}$

then from base case  $\exists p_n \in \overline{\mathbb{F}}$

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  $g \in \underline{I}$ .

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

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

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

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

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

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

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

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

We will obtain a contradiction by

considering the resultant

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

- Since  $\text{Res}_{x_n}(f, g)$  is an  $\mathbb{F}[\vec{x}']$ -linear combination of  $f$  &  $g$ , have

$$\text{Res}_{x_n}(f, g) \in I \cap \mathbb{F}[\vec{x}'] = I',$$

hence by definition of  $\vec{p}' \in \mathbb{F}^{n-1}$ ,

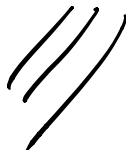
$$\text{Res}_{x_n}(f, g)(\vec{p}') = 0.$$

• On the other hand:

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

$$= \pm \det \begin{pmatrix} c & a_1(\vec{p}') & \dots & a_\lambda(\vec{p}') \\ & \ddots & & \ddots \\ & & c & a_1(\vec{p}') & \dots & a_\lambda(\vec{p}') \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}$$

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



(Strong): Assume  $g$  vanishes on

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

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

TRICK: Introduce new variable  $y$   
& consider polynomials

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

consider intersection of hyp. surfaces  
one dimension higher:

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

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

$$(\vec{p}, g) \in V_{f_1} \cap \dots \cap V_{f_m} \implies f_1(\vec{p}) = \dots = 0.$$

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

$$\implies (\vec{p}, g) \in V_{1-yg}.$$

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

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

$$1 = f_1(\vec{x}) h_1(\vec{x}, y) + \dots + f_m(\vec{x}) \hat{h}_m(\vec{x}, y) \\ + (1 - y g(\vec{x})) \tilde{g}(\vec{x}, y).$$

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

to get identity in field of fractions:

$$1 = f_1 \tilde{h}_1(\vec{x}, \frac{1}{g}) + \dots + f_m \tilde{h}_m(\vec{x}, \frac{1}{g}) + 0.$$

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

for some  $r \geq 0$ , hence

$$g^r = f_1 \tilde{f}_1 + \dots + f_m \tilde{f}_m. \quad \text{QED.}$$



Next time: The modern form of NSS

