Hilbert's Nullstellensatz

Jia Ji

January 15, 2010

General Statement of Hilbert's Nullstellensatz

k - **field (geometric) or** $\mathbb{Z}$ **(arithmetic)**

$$g, f_1, \cdots, f_m \in k[x_1, \cdots, x_n] =: P_n, \quad I = \langle f_1, \cdots, f_m \rangle$$

IF: $\forall F : \dim_k F < \infty$ (**For** $k = \mathbb{Z}$, $|F| < \infty$) $\forall a \in F^n$:

$$(\forall i, f_i(a) = 0) \Rightarrow g(a) = 0$$

THEN (BY H.N.): $\exists N \in \mathbb{Z}_{>0}$ **s.t.** $g^N \in I$

Remark: If $k = \mathbb{C}$**, by Fund Thm of Alg,** $\dim_{\mathbb{C}} F < \infty \Rightarrow F = \mathbb{C}$

Ideas of the Proof of HN

$$a \in F^n, \quad k \subset k[a_1, \cdots, a_n] =: K \subset F \text{ field} \Rightarrow K \text{ field}$$

$$M_a := \{h \in P_n : h(a) = 0\} \Rightarrow M_a \in \mathrm{Specm} P_n$$

$$\text{HN-B} \Rightarrow \forall m \in \mathrm{Specm} P_n, m \text{ is like some } M_a$$

$$g \in \cap_{a\text{-common zero}} M_a = \cap_{m \supset I, m \in \mathrm{Specm} P_n} m$$

$$\text{HN-A} \Rightarrow g \in \cap_{m \supset I, m \in \mathrm{Specm} P_n} m = \cap_{p \supset I, p \in \mathrm{Spec} P_n} p = \sqrt{I}$$

$$\exists N \in \mathbb{Z}_{>0} \text{ s.t. } g^N \in I. \text{ Done!}$$

$\cap_{p\in \mathrm{Spec}A} p = \mathrm{nil}A$. **(i)** $\cdots \supset \cdots$ **easy.**

(ii) $f \in \cap_{p\in \mathrm{Spec}A} p$. **If** $f \notin \mathrm{nil}A$: $0 \in S := \left\{\textbf{ideals } I \neq A : \forall k, f^k \notin I\right\}$

$\left(\cup_{I\in \textbf{chain}} I\right) \in S$. $\exists$**maximal** $P \in S \Rightarrow P$ **is prime. If** $xy \in P, x, y \notin P$:

$f^n \in \langle x\rangle + P \notin S, \quad f^m \in \langle y\rangle + P \notin S \Rightarrow f^{n+m} \in \langle xy\rangle + P = P$ **?!**

$\Rightarrow \exists P \in \mathrm{Spec}A$ **s.t.** $f \notin P$ **?!** $\Rightarrow \cdots \subset \cdots$ **Done.**

$$\cap_{p\in \mathrm{Spec}P_n/I} p = \left(\cap_{p\supset I, p\in \mathrm{Spec}P_n} p\right)/I = \mathrm{nil}\left(P_n/I\right) = \sqrt{I}/I$$

$$\Rightarrow \cap_{p\supset I, p\in \mathrm{Spec}P_n} p = \sqrt{I}$$

Proof of HN-B (1/5): Field-Case (geometric):

HN-B: $A := {}^{P_n}/_{I}, \quad m \in \mathrm{Specm} A, \quad F := {}^{A}/_{m} \Rightarrow$

k**-field:** $\dim_k F < \infty; \quad k = \mathbb{Z}$**:** $|F| < \infty$

Pf: Field-Case: $n = 1$**:** $\pi : k[x_1] \to A, \widetilde{m} = \pi^{-1}(m), F = {}^{k[x_1]}/_{\widetilde{m}}$

$k[x_1]$**-PID** $\Rightarrow \widetilde{m} = \langle g \rangle \Rightarrow \overline{x_1}$**-algebraic over** $k \Rightarrow \dim_k F < \infty$

Assume HN-B for $n-1$**. Prove for** n**: Now** $F = k[\overline{x_1}, \cdots, \overline{x_n}]$**.**

If all $\overline{x_i}$ **alg over** k**,** $k \subset k[\overline{x_1}] \subset \cdots \subset k[\overline{x_1}, \cdots, \overline{x_n}]$ **fin. ext. Done.**

Proof of HN-B (2/5)

If one $\overline{x_i}$, say $\overline{x_1}$, transcendental/k, i.e. $k[\overline{x_1}] \cong k[x_1]$, prove $\Rightarrow$?!

$$K := k(\overline{x_1}) \cong k(x_1), \quad F := {}^{A}/_{m} = K[\overline{x_2}, \cdots, \overline{x_n}]$$

By Ind. Hyp. $\Rightarrow \dim_K K[\overline{x_2}, \cdots, \overline{x_n}] < \infty \Rightarrow \overline{x_2}, \cdots, \overline{x_n}$ **alg**/K

$$\Rightarrow \exists f_i \in k[\overline{x_1}], f_i \neq 0, f_i \overline{x_i} \text{ integral}/k[\overline{x_1}] \Rightarrow f\overline{x_i} \text{ int}/k[\overline{x_1}], f = f_1 \cdots f_n$$

$$R_f := \left\{ \frac{h}{f^l} : h \in R, l \in \mathbb{Z}_{\geq 0} \right\}: \text{ Then all } \overline{x_i} \text{ int}/k[\overline{x_1}]_f$$

Proof of HN-B (3/5)

Fact 1: Integral closure $\overline{R}$ in S of a subring $R \subset S$ is a subring. $\Rightarrow$

$$(K \supset k\left[\overline{x_1}\right]_f \supset k\left[\overline{x_1}\right]) \quad \forall G \in F = k\left[\overline{x_1}\right]_f\left[\overline{x_2}, \cdots, \overline{x_n}\right], G \text{ int}/k\left[\overline{x_1}\right]_f$$

$$\Rightarrow \exists N \in \mathbb{Z}_{>0} \text{ s.t. } f^N G \text{ int}/k\left[\overline{x_1}\right]$$

Fact 2: R-UFD, $K :=$ field of fractions of $R \Rightarrow$ in K, $\overline{R} = R \Rightarrow$

$$\forall \text{irred } q \in k\left[\overline{x_1}\right] \cong k\left[x_1\right] \quad \exists N \in \mathbb{Z}_{>0} \text{ s.t. } f^N \cdot \frac{1}{q} \in K \text{ int}/k\left[\overline{x_1}\right] \Rightarrow$$

$$\frac{f^N}{q} \in k\left[\overline{x_1}\right] \Rightarrow q | f \text{ but } f \neq 0. \text{ ?! } \therefore \textbf{Field-Case proved.}$$

Note: Need, $k\left[x_1\right]$ has ∞ many irreducible polynomials.

Proof of HN-B (4/5): $\mathbb{Z}$-Case (arithmetic)

$k = \mathbb{Z}$: $F = \mathbb{Z}[\overline{x_1}, \cdots, \overline{x_n}]$. **(i) If** $p := \mathrm{char} F \neq 0$

then $F = \mathbb{Z}/p[\overline{x_1}, \cdots, \overline{x_n}]$. **By Field-Case,** $\dim_{\mathbb{Z}/p} F < \infty$

$\Leftrightarrow |F| < \infty$. **Done.**

(ii) Want to show $\mathrm{char} F = 0$ **leads to ?!.**

Say $\mathbb{Q} \subset F \Rightarrow F = \mathbb{Q}[\overline{x_1}, \cdots, \overline{x_n}]$

By Field-Case, $\dim_{\mathbb{Q}} F < \infty \Rightarrow$ **all** $\overline{x_i}$ **alg**/$\mathbb{Q}$

Proof of HN-B (5/5)

$$\Rightarrow \exists f \in \mathbb{Z}, \quad f \neq 0, \quad f\overline{x_i} \text{ int}/\mathbb{Z} \Rightarrow \text{all } \overline{x_i} \text{ int}/\mathbb{Z}_f$$

$$\Rightarrow \text{If } G \in \mathbb{Z}_f\,[\overline{x_1}, \cdots, \overline{x_n}] = F, \text{ then } G \text{ int}/\mathbb{Z}_f$$

$$\Rightarrow \exists N \in \mathbb{Z}_{>0} \text{ s.t. } f^N G \text{ int}/\mathbb{Z}$$

$$\forall \text{prime } q \in \mathbb{Z} \quad \exists N \in \mathbb{Z}_{>0} \text{ s.t. } f^N \cdot \frac{1}{q} \in \mathbb{Q} \text{ is int}/\mathbb{Z} \Rightarrow$$

$$\text{by Fact 2, } \frac{f^N}{q} \in \mathbb{Z} \Rightarrow q|f. \text{ But } f \neq 0. \text{ ?! } \mathrm{char}F \neq 0.$$

$\mathbb{Z}$-Case and thus HN-B proved!

Auxiliary Theorem (Prepared for HN-A)

$$A := {}^{k[x_1,\cdots,x_n]}/_{I},\ M \in \mathrm{Specm}A\,[t]\,,\ m := M \cap A \Rightarrow m \in \mathrm{Specm}A$$

Pf: (**clearly** $m \in \mathrm{Spec}A$). **Note** ${}^{A}/_{m} \subset {}^{A[t]}/_{M}$ **embedding**

$$A\,[t] = {}^{k[x_1,\cdots,x_n,t]}/_{\langle I\rangle},\ {}^{A}/_{m} = k\,[\overline{x_1},\cdots,\overline{x_n}]\,,\ F := {}^{A[t]}/_{M} = k\,[\overline{x_1},\cdots,\overline{x_n},\overline{t}]$$

F **is a field. (i) If** $k =$ **field:** $\dim_k F < \infty \Rightarrow \overline{x_i}, \overline{t}$ **alg**$/k \Rightarrow {}^{A}/_{m}$ **field.**

(ii) If $k = \mathbb{Z}$**:** $|F| < \infty, \quad p := \mathrm{char}F \Rightarrow \overline{x_i}, \overline{t}$ **alg**$/{}^{\mathbb{Z}}/_{p}$ **and**

$$F = {}^{\mathbb{Z}}/_{p}\,[\overline{x_1},\cdots,\overline{x_n},\overline{t}] \Rightarrow {}^{\mathbb{Z}}/_{p}\,[\overline{x_1},\cdots,\overline{x_n}] = {}^{A}/_{m}\ \textbf{field. Done.}$$

HN-A: $\bigcap_{m\in \mathrm{Specm}A} m = \bigcap_{p\in \mathrm{Spec}A} p$ (clearly $\cdots \supset \cdots$)

Pf: $f \in \bigcap_{m\in \mathrm{Specm}A} m \Rightarrow$ **If** $M \in \mathrm{Specm}A[t]$, **then** $f \in M \cap A$

$$\Rightarrow f \cdot t \in \bigcap_{M\in \mathrm{Specm}A[t]} M \Rightarrow \forall M \in \mathrm{Specm}A[t], 1 + f \cdot t \notin M$$

$$\Rightarrow 1 + f \cdot t \textbf{ invertible}$$

$$\Rightarrow (1 + f \cdot t)\left(c_0 + c_1 t + \cdots + c_N t^N\right) = 1$$

$$\Rightarrow c_0 = 1, \quad c_1 = -f, \quad \cdots, \quad c_N = (-f)^N, \quad c_N \cdot f = 0$$

$$\Rightarrow f^{N+1} = 0 \Rightarrow f \in \mathrm{nil}A \Rightarrow f \in \bigcap_{p\in \mathrm{Spec}A} p$$

Further Elaborations (in anticipation of questions) (1/3)

1. **Say,** $a \in F^n, M_a := \{h \in P_n : h(a) = 0\} \in \mathrm{Specm} P_n$. **Why?**

Say $\mathrm{ev}_a : P_n \to F$, **then** $\mathrm{Ker}(\mathrm{ev}_a) = M_a$. **So,** $k \subset K := {}^{P_n}/_{M_a} \subset F$

$$\dim_k F < \infty \Rightarrow K \text{ finite}/k. \quad \forall t \in K, \quad \mathrm{ev}_t : k[T] \to K \Rightarrow$$

$$\exists \langle f \rangle = \mathrm{Ker}(\mathrm{ev}_t). \quad k[T] \text{ is PID} \Rightarrow \mathrm{Ker}(\mathrm{ev}_t) \in \mathrm{Specm} k[T] \Rightarrow$$

$$\mathrm{Im}(\mathrm{ev}_t) = k[t] = {}^{k[T]}/_{\mathrm{Ker}(\mathrm{ev}_t)} \Rightarrow k[t] \text{ field} \Rightarrow t^{-1} \in k[t] \subset K$$

$\Rightarrow K$ **field.** (**If** $k = \mathbb{Z}$, **essentially the same, just replace** k **by** ${}^{\mathbb{Z}}/_{p}$)

Further Elaborations (in anticipation of questions) (2/3)

2. From HN-B: $m \in \mathrm{Specm} P_n, \pi : P_n \to {}^{P_n}/_{m}; \quad x_i \mapsto a_i =: \overline{x_i} \in F$

$$\Rightarrow p \in m \Leftrightarrow p(a) = 0 \Rightarrow m = M_a$$

3. $\cap_{m \in \mathrm{Specm} P_n/I} m = \cap_{p \in \mathrm{Spec} P_n/I} p \Leftrightarrow$

$$\left(\cap_{m \supset I, m \in \mathrm{Specm} P_n} m\right)/I = \left(\cap_{p \supset I, p \in \mathrm{Spec} P_n} p\right)/I$$

Further Elaborations (in anticipation of questions) (3/3)

4. Proof of Fact 1: Our instrument is

Lemma: $f \in S$ **is int over** $R \subset S$ **iff**

$R[f] \subset S$ **is finite generated** $R-\text{module}$. $(\Rightarrow$ **clear**$)$

Pf: $f \in S, \quad R \subset S, \quad R[f]$ **fin.gen.**R**-mod** $\Rightarrow R[f] = \sum_{i=1}^{m} Re_i$

$$f \cdot e_i = \sum_{j=1}^{m} a_{ij} e_j, \quad \det(f \cdot I - A) \cdot I = (f \cdot I - A)^* (f \cdot I - A)$$

$$\Rightarrow \det(f \cdot I - A) \cdot e_i = 0 \Rightarrow \det(f \cdot I - A) = 0$$

Epilogue: The Complex World

If $k = \mathbb{C}$: $a \in \mathbb{C}^n, M_a = \langle x_1 - a_1, \cdots, x_n - a_n \rangle$. **Why?**

$$f \in P_n, \quad q\left(\overrightarrow{y}\right) := f\left(\overrightarrow{y} + a\right) \Rightarrow f\left(\overrightarrow{x}\right) = q\left(\overrightarrow{x} - a\right)$$

$$f(a) = 0 \Leftrightarrow q(0) = 0 \Leftrightarrow q \in \langle y_1, \cdots, y_n \rangle$$

$$\Leftrightarrow f \in \langle x_1 - a_1, \cdots, x_n - a_n \rangle$$

$$\therefore m \in \mathrm{Specm}\mathbb{C}[x_1, \cdots, x_n] \Leftrightarrow \exists a \in \mathbb{C}^n, m = \langle x_1 - a_1, \cdots, x_n - a_n \rangle$$