Hilbert's Nullstellenstaz

John Fleming

November 25, 2011

Notations: k is a field (geom) or k = $\mathbb{Z}$ (arithm)

$\mathbb{K}$ is a field with $[\mathbb{K} : k] < \infty$ geom., $\#\mathbb{K} < \infty$ arithm. cases.

$g, f_1, ..., f_m \in k[\vec{x}] := k[x_1, .., x_n]$, $I = (f_1, ...f_m)$ ideal in $k[\vec{x}]$.

$\sqrt{I} := \{h \in k[\vec{x}] : h^n \in I$ for some n$\}$.

$V_{\mathbb{K}}(I) := \{\forall a \in \mathbb{K}^n \, (f(a) = 0 : \forall f \in I)\}$, $V(I) := \bigcup_{\mathbb{K}} V_{\mathbb{K}}(I)$.

$Spec(R) := \{\mathfrak{p} \subset R : \mathfrak{p}$ is a prime ideal$\}$.

$Specm(R) := \{\mathfrak{m} \subset R : \mathfrak{m}$ is a maximal ideal$\}$.

$\mathfrak{m}_a := \{h \in k[\vec{x}] : h(a) = 0, a \in \mathbb{K}^n\}$.

HN Thm: $V(g) \supset V(I) \Rightarrow g \in \sqrt{I}$. $\mathfrak{p} \in Spec(R)$ and $b \in R/\mathfrak{p}$:

1^R. $R/\mathfrak{p}[b^{-1}]$ a field $\Rightarrow$ $\mathfrak{p} \in Specm(R)$ (true if R field or $\mathbb{Z}$).

1. Abstract HN (AHN) $S := R[\gamma]$. i) $1^R \Rightarrow 1^S$.

ii) $S/\mathfrak{n}$ field $\Rightarrow m := n \bigcap R \in Specm(R)$; iii) $[S/\mathfrak{n} : R/\mathfrak{m}] < \infty$.

2. $\mathfrak{m} \in Specm(k[\vec{x}]) \Leftrightarrow \mathfrak{m} = \mathfrak{m}_a$ for some $a \in \mathbb{K}^n$.

3. $\bigcap_{\mathfrak{m} \supset I : \mathfrak{m} \in Specm(k[\vec{x}])} \mathfrak{m} = \bigcap_{\mathfrak{p} \supset I : \mathfrak{p} \in Spec(k[\vec{x}])} \mathfrak{p}$.

4. $\bigcap_{\mathfrak{p} \supset I : \mathfrak{p} \in Spec(k[\vec{x}])} \mathfrak{p} = \sqrt{I}$.

Proof of AHN. $\bar{\gamma} \in B := S/\mathfrak{p}$, $\mathfrak{p} \in Spec(S)$.

We prove i) $b \in B \backslash \{0\}$, $B[b^{-1}]$ a field $\Rightarrow$ B is a field.

ii) A := R/($\mathfrak{p} \bigcap R$) is a field. iii) $[B : A] < \infty$.

Proof. $B = A[\bar{\gamma}] \Rightarrow B = A[x]/\mathfrak{q}$, $\mathfrak{q} \in Spec(A[x])$.

$\mathfrak{q} \neq 0$! Otherwise, $A[x][b^{-1}]$ is field $\Rightarrow$ $(A)[x][b^{-1}]$ is field

$\Rightarrow \forall f \in (A)[x] \backslash \{0\}$, $\exists f^{-1} = \dfrac{g}{b^n}$, $g \in (A)[x]$, $n \in \mathbb{Z}_+$.

Using (A)[x] UFD $\Rightarrow$?! So, $\mathfrak{q} \neq 0$.

Reduction to a "detour".

$\exists\ P(x) \in \mathfrak{q}\backslash\{0\}$, $P(\bar{\gamma}) = 0 \ \Rightarrow\ (A)[\bar{\gamma}]$ is field.

$(B) = B[b^{-1}] = (A[\bar{\gamma}]) = (A)[\bar{\gamma}] \ \Rightarrow\ [(B) : (A)] < \infty$.

$\alpha \in R'$ is integral over $R \subset R'$ iff $P(\alpha) = 0$, monic $P \in R[x]$

Detour: $\bar{R} := \{\alpha \in R' : \alpha$ integral over R$\}$ is a ring.

Prop. $\bar{R} \supset S$ is field $\ \Rightarrow\$ R is field ($\Leftarrow$ is clear for $S = R[\alpha]$) .

Conclusion of Step 1.

Say $P(x) = p_n x^n + \ldots$, $Q(x) = q_m x^m + \ldots$, $Q(b^{-1}) = 0$

and $p_n \cdot q_m \neq 0$, $P(x)$ and $Q(x) \in A[x]$

$\Rightarrow$ $B[b^{-1}] = A[\bar{\gamma}, b^{-1}]$ is integral over $A[(p_m q_m)^{-1}] =: K$

$\Rightarrow K$ is field $\Rightarrow A$ is field (see (i)) $\Rightarrow B$ is field,

directly from Proposition. $\square$

Proof of ‘Detour’ $\Rightarrow$ Proposition.

Hint: to show that α , β integral $\Rightarrow$ $\alpha \cdot \beta$ and $\alpha + \beta$ are integral

use symmetric polynomials evaluated on ‘conjugates’ of α , β .

Proof of Proposition: S is a field $\Rightarrow$ R is a field.

Say $a \in R$, $a \cdot \gamma = 1$, $\gamma \in S$, $f \in R[x]$ monic minimal s. th.

$f(\gamma) = 0$, $f(x) =: x^n + b_{n-1}x^{n-1} + \cdots + b_0$ $\Rightarrow$ $0 = a \cdot f(\gamma) =$

$\gamma^{n-1} + b_{n-1}\gamma^{n-2} + \cdots + b_1 + a \cdot b_0$ $\Rightarrow$ $n = 1$ $\Rightarrow$ $\gamma = b \in R$. $\square$

AHN (many generators) via induction on their $\#$

Assume AHN with $S := R[\gamma_0, ..., \gamma_{n-1}]$.

To show AHN with $S' := S[\gamma_n]$ pick $\mathfrak{n} \in Specm(S')$

$\Rightarrow \ \mathfrak{m} := \mathfrak{n} \bigcap S \in Specm(S) \ \Rightarrow \ \mathfrak{n} \bigcap R \in Specm(R)$.

Also, $[S'/\mathfrak{n} : S/\mathfrak{m}] < \infty$ and $[S/\mathfrak{m} : R/(\mathfrak{n} \bigcap R)] < \infty$

$\Rightarrow \ [S'/\mathfrak{n} : R/(\mathfrak{n} \bigcap R)] < \infty$. Finally, $1^R \Rightarrow 1^S \Rightarrow 1^{S'}$. $\square$

HN 2: $\mathfrak{m} \in Specm(k[\vec{x}]) \Leftrightarrow \mathfrak{m} = \mathfrak{m}_a$, $a \in \mathbb{K}^n$

Proof "$\Leftarrow$". $\mathbb{K}[\vec{x}]$ is finitely generated over $k[\vec{x}]$ ($\mathbb{Z}_p[\vec{x}]$ if $k = \mathbb{Z}$) .

$\mathfrak{n} := \{h \in \mathbb{K}[x] : h(a) = 0\} \;\Rightarrow\; \mathbb{K}[x]/\mathfrak{n} = \mathbb{K}$, $m_a := \mathfrak{n} \bigcap k[\vec{x}]$.

This completes proof in geometric case, i.e. when k is a field.

For $k = \mathbb{Z}$ set $\phi : \mathbb{Z}[\vec{x}] \to \mathbb{Z}_p[\vec{x}]$.

$\mathfrak{m}_a = \phi^{-1}(\mathfrak{n} \bigcap k[\vec{x}]) \in Spec(\mathbb{Z}[\vec{x}])$, which completes the proof.

Continuation of Proof "$\Rightarrow$" with k a field or $\mathbb{Z}$.

$\mathfrak{m} \in Specm(k[\vec{x}]) \ \Rightarrow \ [k[\vec{x}]/\mathfrak{m} : k/(\mathfrak{m} \cap k)] < \infty$.

$\mathfrak{m} \cap k = \{0\}$ for k field and $k/(\mathfrak{m} \cap k) = \mathbb{Z}_p$ for $k = \mathbb{Z}$ (AHN).

With $\phi : k[\vec{x}] \to k[\vec{x}]/\mathfrak{m}$ let $\bar{x}_i := \phi(x_i)$, $a := (\bar{x}_1, ..., \bar{x}_n)$.

$P(x) \in \mathfrak{m} \iff P(a) = 0 \Rightarrow \mathfrak{m} = \mathfrak{m}_a$,

which completes the proof of HN 2.

HN 3: $\bigcap_{\mathfrak{m} \supset I : \mathfrak{m} \in Specm(k[\vec{x}])} \mathfrak{m} = \bigcap_{\mathfrak{p} \supset I : \mathfrak{p} \in Spec(k[\vec{x}])} \mathfrak{p}$

To prove it is sufficient to show that:

$1^R \Rightarrow \forall\, \mathfrak{p} \in Spec(R) : \mathfrak{p} = \bigcap_{\mathfrak{m} \supset \mathfrak{p} : \mathfrak{m} \in Specm(R)} \mathfrak{m}$.

Proof: Pick $\mathfrak{p} \in Spec(R)$ and $M = \bigcap_{\mathfrak{m} \in Specm(R) : \mathfrak{m} \supset \mathfrak{p}} \mathfrak{m}$.

Then $M = \mathfrak{p}$. Otherwise, letting $h \in M - \mathfrak{p}$ and

$X = \{\mathfrak{b} : \mathfrak{p} \subset \mathfrak{b} \in Spec(R)\ ,\ h \notin \mathfrak{b}\}$ choose $\mathfrak{b}_0$ maximal in X .

$h \notin \mathfrak{b}_0 \Rightarrow \mathfrak{b}_0 \notin Specm(R) \Rightarrow S := R/\mathfrak{b}_0$ is no field.

Step 3 continued

$a \notin \mathfrak{b}_0 \Rightarrow \mathfrak{b}_0 \notin Specm(R) \Rightarrow S := R/\mathfrak{b}_0$ is not a field.

Let H be the class of h in S . Then $S[H^{-1}]$ is a field.

Otherwise, $\exists \, \{0\} \neq \mathfrak{c} \in Spec(S[H^{-1}])$

$$\Rightarrow \ \exists \, 0 \neq \frac{b}{H^n} \in \mathfrak{c} \, , \ b \in S \, , \ n \in \mathbb{Z}_+ \Rightarrow b \in \mathfrak{c} \bigcap S \neq \{0\}$$

$\Rightarrow \mathfrak{b}_0$ not maximal in X ?! So $S[H^{-1}]$ is a field.

S not field and $S[H^{-1}]$ is field $\Rightarrow$?! with 1^R, so $M = \mathfrak{p}$. □

Lemma: $\bigcap_{\mathfrak{p} \in Spec(R)} \mathfrak{p} = nil(R)$.

Def: $nil(R) := \{r \in R : r^n = 0 \text{ for some n}\}$.

Show $nil(R) \subset \bigcap_{\mathfrak{p} \in Spec(R)} \mathfrak{p}$.

Proof: $x^n = 0$ and $0 \in \mathfrak{p}$ prime $\Rightarrow x$ or $x^{n-1} \in \mathfrak{p}$.

Next show $\bigcap_{\mathfrak{p} \in Spec(R)} \mathfrak{p} \subset nil(R)$.

Proof: $f \in \bigcap_{\mathfrak{p} \in Spec(R)}$, $f \in nil(A)$ otherwise,

$X := \{I \text{ ideals of } R : \forall\, n : f^n \notin I\}$. (Note: $0 \in S$.)

Proof of Lemma continued

$\mathcal{C}(chain) \subset X, \Rightarrow \bigcup_{I \in \mathcal{C}} I \in X$

$\Rightarrow \exists\, \mathfrak{p} \in X : \mathfrak{p}$ is maximal in X (Zorn's Lemma).

Then $\mathfrak{p} \in Spec(R)$. otherwise $\exists\, a \cdot b \in \mathfrak{p}$ with $a, b \notin \mathfrak{p}$

$\Rightarrow f^n \in (a, \mathfrak{p}) \notin X$ and $f^m \in (b, \mathfrak{p}) \notin X$

$\Rightarrow f^{m+n} \in (a \cdot b, \mathfrak{p}) = \mathfrak{p} \Rightarrow \mathfrak{p} \notin X \Rightarrow$?! So, $\mathfrak{p} \in Spec(R)$.

Since $f \notin \mathfrak{p}$ (Definition of X) and $\forall\, \mathfrak{q} \in Spec(R) \Rightarrow f \in \mathfrak{q}$?!

So $f \in nil(R)$. Which complete the lemma.

Proof HN 4: $\bigcap_{\mathfrak{p}\supset I:\mathfrak{p}\in Spec(k[\vec{x}])} \mathfrak{p} = \sqrt{I}$.

$(\bigcap_{\mathfrak{p}\supset I:\mathfrak{p}\in Spec(k[\vec{x}])} \mathfrak{p})/I = \bigcap_{\mathfrak{p}\in Spec(k[\vec{x}]/I)} \mathfrak{p} = nil(k[\vec{x}]/I) = \sqrt{I}/I$.

$I \subset \bigcap_{\mathfrak{p}\supset I:\mathfrak{p}\in Spec(k[\vec{x}])} \mathfrak{p}$ and $I \subset \sqrt{I}$, as required in HN 4.

Proofs of HN parts 1,2,3 and 4 complete.