Hilbert Nullstellensatz for ideals $I \hookrightarrow \mathcal{P} := K[x]$ or $\mathbb{Z}[x]$, $x := (x_1, \ldots, x_n)$ and K a field, called geometric or arithmetic case.

Viktoriya Baydina

MAT 477

March 11, 2014

Below $F := \mathcal{P}/m$ is a field, sets $Spec(A)$, $Specm(A)$ are

prime, resp. maximal ideals of $A := \mathcal{P}/I$ and $\mathcal{M}_A(I) := \bigcap_{I \subseteq m \in Specm(A)} m$

Main Thm: (1) $\sqrt{I} := \{f \in \mathcal{P} \mid f^N \in I\} = \mathcal{M}(I) := \mathcal{M}_{\mathcal{P}}(I)$;

(2) $F = \mathcal{P}/m \Rightarrow$ geom case $[F : K] := \dim_K F < \infty$, arith $\#(F) < \infty$;

(3) $\exists\ F$ as in (2) s.th. $\mathcal{V}_F(I) := \{\xi \in F^n : f(\xi) = 0, \forall f \in I\} \neq \emptyset$;

Classical: $\mathcal{P} = K[x]$ and algebraic closure $\overline{K} = K$. Let $\mathcal{V}(I) := \mathcal{V}_{\overline{K}}(I)$.

(4) $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$ for $\mathcal{I}(\mathcal{V}) := \{f \in \mathcal{P} : f_{|\mathcal{V}} = 0\} \Rightarrow \mathcal{V}(\mathcal{I}(\mathcal{V}(I))) = \mathcal{V}(I)$

Easy Thm: $\mathcal{P}_R(I) := \bigcap_{I \subseteq P \in Spec(R)} P = \sqrt{I}$ for ideals I in arbitrary rings R

Indeed, $f \in \mathcal{P}_R(I)/I \subset B := R/I \Rightarrow f \in \sqrt{0} \hookrightarrow B$: using $f \in \mathcal{M}_{B[x_0]}(0)$

$\Rightarrow \exists\ (1 + f\ x_0)^{-1} = \sum_{0 \le j \le d} c_j x_0^j \in B[x_0] \Rightarrow c_j = (-f)^j$, i.e. $f^{d+1} = 0$ ■

Def: domains are rings without zero divisors and $A \hookleftarrow K$ is K-algebraic

when every $a \in A \setminus \{0\}$ is, i.e. $\exists\ f \in K[z] \setminus \{0\}$ with $f(a) = 0$.

Lemma 1: K-algebraic domains $A \hookleftarrow K$ are fields. $\Rightarrow$ With F as in (2)

Corollary 1: for $\xi \in F^n$ ideals $m_\xi := \{f \in \mathcal{P} : f(\xi) = 0\}$ are maximal.

Proof of L1: $K[z]$ is a PID $\Rightarrow \forall\ a \in A \setminus \{0\}\ \exists$ irreducible f s.th. $m_a :=$

$\{g \in K[z] : g(a) = 0\} = (f)$ $\Rightarrow$ m_a maximal, $K[a]$ field. For $\phi : \mathcal{P} \to A$,

$a_i := \phi(x_i)$ ring $A = K[a_1, ...a_n]$ $\Rightarrow$ all $K[a_1, ...a_k]$ fields, by induction. ■

Key to HN. Lemma 2: Fields $F = K[x]/I$ are K-algebraic.

Remarks: $[A : K] < \infty$ for fields A from Lemma 1. Hence Lemma 2 proves geometric case of Main Thm (2) $\Rightarrow$ all $m \in Specm(\mathcal{P})$ are as in Cor. 1 with $\xi := (\phi(x_1), ..., \phi(x_n))$ and $\phi : \mathcal{P} \to F := \mathcal{P}/m$. So (3) follows with $F = \mathcal{P}/m$, $\xi \in \mathcal{V}_F(I)$ and $m_\xi = m$ being maximal among ideals $J \neq \mathcal{P}$ s.th. $J \supset I$ (via Zorn's lemma). Of course then also (1) $\Rightarrow$ (4).

Plan: We'll show how (2) $\Rightarrow$ (1) , then Lemma 2, then arithm case of (2).

Detour: $\overline{K} = K \Rightarrow \mathcal{V}(I) \to \{m \in Specm(K[x]) : I \subset m\}$ is bijective: let

$\xi := (\phi(x_1), ..., \phi(x_n)) \in \mathcal{V}(I)$ then $m = m_\xi = (x_1 - \xi_1, \ldots, x_n - \xi_n)$. ■

Lemma4 '(2) ⇒ (1)': $M \in Specm(\mathcal{P}[x_0]) \Rightarrow m := M \cap \mathcal{P} \in Specm(\mathcal{P})$

Proof: With $k := K$ in geometric and $k := \phi(\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$ in arithmetic

case field $F := \mathcal{P}[x_0]/M = k[a_0,\ a_1, ...,\ a_n] \hookleftarrow R := \mathcal{P}/m = k[a_1, ...,\ a_n]$,

where a_i's are the classes of x_i's in F . So, as in Lemma 1, R is a field. ■

Prf(2) ⇒ (1)**:** Suffices to show $f \in \mathcal{M}(I)/I \subset \mathcal{P}/I =: A \ \Rightarrow\ f \in \sqrt{0} \hookrightarrow A$

But f , due to Lemma4, is in every maximal ideal of $A[x_0]$ implying exists

$(1 + f\ x_0)^{-1} = \sum_{0 \leq j \leq d} c_j x_0^j \in A[x_0] \ \Rightarrow\ c_j = (-f)^j$, i.e. $f^{d+1} = 0$. ■

Proof of Lemma 2: Fields $F = K[x]/I$ are K-algebraic.

Proof: Let $\vec{\mathbf{a}}_j := (a_1, \ldots, a_j)$, $j \leq n$, where a_i's are the images of x_i's in $F = K[\vec{\mathbf{a}}_n]$. If F is not K-algebraic then not all of a_i's are. Then reorder a_i's and choose maximal $r \leq n$ so that a_j is not $K[\vec{\mathbf{a}}_{j-1}]$-algebraic for $j \leq r$. Then $K[x_1, ..., x_r] \to R := K[\vec{\mathbf{a}}_r]$ is an isomorphism, i.e. R is UFD with ∞ many irreducible elements and a_j's for $r < j \leq n$ are R-algebraic (and (R)-integral) $\Rightarrow$ $m = [F : L] := dim_L F < \infty$ $(L := K(\vec{\mathbf{a}}_r) = (R)$ $\hookrightarrow F = K[\vec{\mathbf{a}}_n]$). Pick an L-basis of F and $\phi : F \ni b \mapsto$ the matrix of the

L-linear endomorphism of multiplication by b in F . Let $g \in R$ be common denominator of all matrix entries of all $\phi(a_i) \in L^{m \times m}$, $i \leq n$ (for $i \leq r$ matrix $\phi(a_i)$ is diagonal with a_i on diagonal). So $\phi(a_i) \in R[g^{-1}]^{m \times m}$ $\Rightarrow$ for each $b \in F$ $\exists$ $s \in \mathbb{Z}^+$ s.th. $\phi(b) \in g^{-s} R^{m \times m}$. R is UFD, so let p_j , $j \leq k$, be the irreducible factors of g in R and $p \in R \hookrightarrow L$ any irreducible element. Then $\phi(p^{-1})$ is diagonal with all entries p^{-1} and exists $d \in \mathbb{Z}^+$, $f \in R$ s.th. $p^{-1} = g^{-d} f$ or $g^d = pf$ $\Rightarrow$ irreducible p is one of the p_i's, but there are ∞ many choices for irreducible $p \in R := K[\vec{\mathbf{a}}_r]$, ?! ■

Proof of (2) in the arithmetic case:

then $F := A = B[x]/J$ with $B := \phi(\mathbb{Z})$, where $\phi : \mathcal{P} \to A := \mathcal{P}/I$, $\Rightarrow$

either $p :=$char$F < \infty$, $[F : \mathbb{Z}/p\mathbb{Z}] < \infty$ (then $\#(F) < \infty$ and done) or

$B = \mathbb{Z}$, $A = \mathbb{Q}[x]/J\mathbb{Q}[x]$ $\Rightarrow$ each $a_j := \phi(x_j)$ is algebraic over $\mathbb{Q}$

and is integral over $R := \mathbb{Z}[\frac{1}{N}]$ for an $N \in \mathbb{Z}$. Then (using **Claim** that

integral elements form a ring) $A := \mathbb{Z}[a_1, ..., a_n]$ is integral over R and

$\forall\ r \in \mathbb{Z} \setminus \{0\}$ exist $b_i \in \mathbb{Z}[\frac{1}{N}]$ s.th. $(\frac{1}{r})^d = b_1(\frac{1}{r})^{d-1} + \ldots + b_d$ $\Rightarrow$

$\frac{1}{r} \in \mathbb{Z}[\frac{1}{N}]$ $\Rightarrow$ $\exists\ s$ s.th. $\frac{N^s}{r} \in \mathbb{Z}$, but $\exists\ \infty$ many primes $r \in \mathbb{Z}$, ?! ■

Claim: Integral closure $\overline{R}$ of a noetherian $R \hookrightarrow S$

in domain S is a subring. Lemma below implies Claim since both

$R[f+g]$ and $R[f \cdot g]$ are R-submodules of $Span_R(R[f] \cdot R[g])$.

Lemma: $f \in S$ is integ. over $R \hookrightarrow S$ iff $R[f] \subset S$ is a fin. gen. R-module.

Proof of Lemma: "only if" is straightforward. To show " $\Rightarrow$ " let

$R[f] = \sum_{1 \le j \le m} R \cdot e_j$, $e_j \in R[f]$. Then $f \cdot e_i = \sum_{1 \le j \le m} a_{ij} \cdot e_j$ with

entries a_{ij} of matrix $\mathcal{A}$ in R $\Rightarrow$ $\forall\ i$ holds $\det(f \cdot I - \mathcal{A}) \cdot e_i = 0$ $\Rightarrow$

$\det(f \cdot I - \mathcal{A}) = 0$, i.e. $R[z] \ni P(z) := \det(z \cdot I - \mathcal{A}) = z^m +$ lower order

terms and $P(f) = 0$, as required. ■ We use $T^{adj} \cdot T = \det T \cdot I$!

Claim Rab: $\sqrt{I} = \sqrt{I}^{Rab} := \bigcap_{P \in Spec_{Rab}(R) \,:\, I \subseteq P} P$, where

I ideal in R and $Spec_{Rab}(R) := \{R \cap m \mid m \in Specm(R[z])\} \subseteq Spec(R)$.

Proof: $\sqrt{I} \subseteq \mathcal{P}(I) := \bigcap_{S\mathcal{P}(I)} P$ if $S\mathcal{P}(I) := \{P \in Spec(R) : \; I \subseteq P\} \neq \emptyset$

So, suffices to show "$\supseteq$". Say $a \in \sqrt{I}^{Rab}$ and ideal J in $R[z]$ is generated

by $(I \cup \{az - 1\})$. If $J \neq R[z] \;\Rightarrow\; J \subset m \in Specm(R[z]) \;\Rightarrow$

$I \subseteq R \cap J \subseteq R \cap m \in Spec_{Rab}(R) \;\Rightarrow\; a \in m$ and, since

$(az - 1) \in J \subset m$, $\Rightarrow\; 1 \in m \neq R[z]$?! Therefore $J = R[z]$. Then

$(\bigstar)$ $1 = \sum_{j=1}^{N} g_j b_j + g_0(az - 1)$ for some $g_j \in R[z]$ and $b_j \in I$.

Applying map $\phi : R[z] \ni f \mapsto f(z^{-1}) \in R[z, z^{-1}]$ to both sides of $\bigstar \;\Rightarrow$

$(\Diamond) \qquad 1 = \sum_{j=1}^{N} \phi(g_j) b_j + \phi(g_0)(a\frac{1}{z} - 1)$.

Say $k \geq \max\{\deg(g_1), \ldots, \deg(g_n), \deg(g_0) + 1\}$. Then multiplying $(\Diamond)$

by z^k yields $z^k = \sum_{j=1}^{N} h_j(z) b_j + z^{k-1}\phi(g_0)(a - z)$ with $h_j(z) := z^k \phi(g_j)$,

and $z^{k-1}\phi(g_0)$ in $R[z] \;\Rightarrow\; a^k = \sum_{j=1}^{N} h_j(a) b_j \in I \;\Rightarrow\; a \in \sqrt{I}$. $\blacksquare$

$\Rightarrow$ **Easy Thm:** $\sqrt{I} \subseteq \mathcal{P}(I) \subseteq \sqrt{I}^{Rab} \subseteq \sqrt{I}$. $\blacksquare$

Proposition 1: If $\phi : K \hookrightarrow B \to A = K[x]/I$ is a ring homomorphism

linear over K and $m \in Specm(A)$ then $n := \phi^{-1}(m) \in Specm(B)$.

Proof of Prop. 1 : Kernel of map $\psi : B/n \to A/m$ induced by ϕ is $\{0\}$

$\Rightarrow$ B/n is isomorphic to K-subalgebra $R := \psi(B/n)$ of A/m . Then field

A/m is K-algebraic (Lemma 2) and R being K-algebraic domain $\Rightarrow$

(Lemma 1) R and with it B/n are fields. So $n \in Specm(B)$. ■

Hilbert Nullstellensatz revisited: $\sqrt{I} = \mathcal{M}(I) := \bigcap_{m \in Specm(A) \,:\, I \subseteq m} m$.

Proof: Suffices to show "$\supseteq$". Say $P \in Spec_{Rab}(A)$, i.e. $P = A \cap m$ with

$m \in Specm(A[z])$. Applying Proposition 1 $\Rightarrow$ $P \in Specm(A)$ and

$Spec_{Rab}(A) \subseteq Specm(A)$. Hence $\sqrt{I} \supseteq = \sqrt{I}^{Rab} \supseteq \mathcal{M}(I)$. ■