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.

January, 2016

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

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

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

(2) $[F : K] := \dim_K F < \infty$ and $\#(F) < \infty$ in arithmetic case;

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

Classical case: $\mathcal{P} = K[x]$ and $K =$ its alg. closure $\overline{K}$ then

(4) $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$ and $\mathcal{V}(\mathcal{I}(\mathcal{V}(I))) = \mathcal{V}(I) := \mathcal{V}_{\overline{K}}(I)$, where

$\mathcal{I}(\mathcal{V}) := \{f \in \mathcal{P} : \ f_{|\mathcal{V}} = 0\}$.

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

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

$(1 + f\ x_0)^{-1} = \sum_{j<d} c_j x_0^j \in B[x_0] \Rightarrow c_j = (-f)^j$ and $f^d = 0$ ■

Defs: R is domain when $\{0\} \in Spec(R)$. Ring $A \hookleftarrow K$ is

K-algebraic: $\forall a \in A \setminus \{0\}\ \exists\ f \in K[z] \setminus \{0\}$ with $f(a) = 0$

Lemma 1: K-algeb. domains $A \hookleftarrow K$ are fields. If F is from (2)

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

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 $A = K[a_1, ...a_n]$, $a_i := [x_i] \ \Rightarrow$ all $K[a_1, ...a_k]$ are fields. ■

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

Remarks: $[A : K] < \infty$ for fields A from L1. Hence Lemma 2

$\Rightarrow$ geom. case of Main Thm (2) $\Rightarrow$ each $m \in Specm(\mathcal{P})$ is m_ξ

from Cor. 1 with $\xi := ([x_1], ..., [x_n])$ and $[x_i] \in F := \mathcal{P}/m$.

So (3) follows with $F = \mathcal{P}/m$ and m maximal among ideals

$J \neq \mathcal{P}$ s.th. $J \supset I$ (via Zorn's lemma). So, then also (1) $\Rightarrow$ (4).

Plan: We'll prove (2) $\Rightarrow$ (1) , then L2, then arithm case of (2).

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

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

Lemma 4 : $M \in Specm(\mathcal{P}[x_0]) \Rightarrow m := M \cap \mathcal{P} \in Specm(\mathcal{P})$

Prf: With $k := K$ in geom. and $\phi(\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$ in arith. case

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

where $a_i := [x_i] \in F$. So, as in Lemma 1, R is a field. ■

Prf $(2) \Rightarrow (1)$**:** $f \in \mathcal{M}(I)/I \subset A \ \Rightarrow\ f \in \sqrt{0} \hookrightarrow A$ suffices

But f , due to L4, is in every maximal ideal of $A[x_0]$ implying exists

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

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

Prf: Let $\vec{\mathbf{a}}_j := (a_1, \ldots, a_j)$, $j \leq n$, where $a_i := [x_i] \in F = K[\vec{\mathbf{a}}_n]$

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

$j \leq r \;\Rightarrow\; K[x_1, ..., x_r]$ isomorphic $R := K[\vec{\mathbf{a}}_r] \;\Rightarrow$ is UFD with

∞ many irreducible elements and a_j's for $r < j$ are R-algebraic

$\Rightarrow\; m = [F : L] := dim_L F < \infty$, where $L := K(\vec{\mathbf{a}}_r) = (R) \hookrightarrow$

$F = K[\vec{\mathbf{a}}_n]$. Let $\phi : F \ni b \mapsto$ the matrix of the L-linear maps

of multiplication by b in F in a fixed L-basis of F . Let $g \in R$ be common denominator of matrix entries of $\phi(a_i) \in L^{m\times m}$ (for $i \leq r$ matrix $\phi(a_i) = a_i \cdot I$ is diagonal) $\Rightarrow \phi(a_i) \in R[g^{-1}]^{m\times m}$ $\Rightarrow \forall b \in F \ \exists\ s \in \mathbb{Z}^+$ s.th. $\phi(b) \in g^{-s}R^{m\times m}$. Let p_j , $j \leq k$, be the irred. factors of g in R and $p \in R \hookrightarrow L$ any irreducible element $\Rightarrow$ matrix $\phi(p^{-1}) = p^{-1} \cdot I$ and $\exists\ d \in \mathbb{Z}^+$ and $f \in R$ s.th. $p^{-1} = g^{-d} \cdot f$ or $g^d = p \cdot f \ \Rightarrow$ p is one of the p_i's , but $\exists\ \infty$ many choices for irreducible $p \in R := K[\vec{\mathbf{a}}_r]$?! ■

Proof of (2) in the arithmetic case: then $F = B[x]/J$

with $B := \phi(\mathbb{Z})$ and $\phi : \mathcal{P} \to F = \mathcal{P}/I \;\Rightarrow$ either

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

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

$\mathbb{Q}$ and integral over $R := \mathbb{Z}[\frac{1}{N}]$ for an $N \in \mathbb{Z}$. Integral elements

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

$\forall\ r \in \mathbb{Z} \setminus \{0\}\ \exists\ b_i \in \mathbb{Z}[\frac{1}{N}]$ 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 $\#\{$ primes $\in \mathbb{Z}\} = \infty$?! ■

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

domain S is a subring. Follows using $R[f+g]$ and $R[f \cdot g]$ are

R-submodules of $Span_R(R[f] \cdot R[g])$ and **Lemma:**

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

Proof of 'if': Let $R[f] = \sum_{1 \le j \le m} R \cdot e_j$, $e_j \in R[f] \Rightarrow$ $f \cdot e_i =$

$\sum_{1 \le j \le m} a_{ij} \cdot e_j$ with $a_{ij} \in R$. Using $T^{adj} \cdot T = \det T \cdot I \Rightarrow$

$\det(f \cdot I - \mathcal{A}) \cdot e_i = 0 \ \ \forall \ i$, where matrix $\mathcal{A} := \{a_{ij}\} \Rightarrow$

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

lower order terms and $P(f) = 0$. 'Only if' is obvious. ■