Commutative Algebra: Hilbert's Nullstellensatz

Dr. Zvi Rosen

Department of Mathematical Sciences,
Florida Atlantic University

Outline

Radical Ideals & Algebraic Varieties

Weak $\implies$ Strong

Proof 2: Noether Normalization

Proof 3: Jacobson Rings

Def: Affine Variety

- Let $A = k[x_1, \dots, x_n]$, k field.

  Let $S \subseteq A$. Define $V(S) =$

  $\{(p_1, \dots, p_n) \in k^n : f(p_1, \dots, p_n) = 0 \ \forall f \in S\}$.

  The affine algebraic variety (vanishing set) of S,

- Let $X \subseteq k^n$. Define $I(X) =$

  $\{f \in A : f(p_1, \dots, p_n) = 0 \ \forall p \in X\}$.

  the vanishing ideal of X.

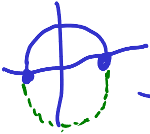
Examples

1) Let $p(x) \in k[x]$ be a polynomial in one variable, then

$$V(\{p(x)\}) = \{\alpha_i : p(\alpha_i) = 0, \alpha_i \in k\}.$$

2) Let $X = [0,1] \subseteq \mathbb{R}^1$. Any polynomial satisfying $p(x) = 0$ $\forall x \in [0,1]$

$$\Rightarrow I(X) = (0) \subset \mathbb{R}[x].$$

3)  $X = \{(x,y) : x^2 + y^2 = 1, y \geq 0\}$

$$I(X) = \langle x^2 + y^2 - 1 \rangle.$$

Some Properties

- Given $V \subset W \subset k^n$, then $I(W) \subset I(V)$. Given f s.t. $f(p) = 0 \ \forall p \in W \Rightarrow$ also true for $p \in V$.
- Given $I \subset J \subset k[x_1, \ldots, x_n]$. then $V(J) \subset V(I)$. Take $p \in V(J)$, $\Rightarrow f(p) = 0 \ \forall f \in J \Rightarrow$ also true for any $f \in I$.

Hilbert's Nullstellensatz

Let k be an algebraically closed field, and $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. Then $\mathbf{I}(\mathbf{V}(I)) = \mathfrak{r}(I)$.

e.g. k not alg. closed

$I = \langle x^2 + y^2 + 1 \rangle \subset \mathbb{R}[x, y]$

$V(I) = \emptyset$. $I(V(I)) = (1)$.

Consequence: 1-1 correspondence between radical ideals and alg varieties.

David Hilbert (1862 - 1943)

Wait a minute...

Version from last lecture: Let k be a field, B a finitely-generated k-algebra. If B is a field, then it is a finite algebraic extension of k.

Recall: proved using results on valuation rings, extending homom's into alg. closed fields.

Weak Nullstellensatz

Let k be an algebraically closed field, and $I \subseteq k[x_1, \dots, x_n]$ be an ideal satisfying $V(I) = \varnothing$. Then $I = k[x_1, \dots, x_n]$.

Suppose not. Then, $I \subseteq \mathfrak{m}$ maximal.

$B = k[x_1, \dots, x_n]/\mathfrak{m} \leftarrow$ extension field of k.

$\Rightarrow B$ finite extension of k.

$\Rightarrow B \simeq k$. Quotient map has kernel $\mathfrak{m}$.

$x_i \to t_i \in k \Rightarrow \mathfrak{m} \supseteq (x_1 - t_1, \dots, x_n - t_n) \leftarrow$ max

$\Rightarrow (t_1, \dots, t_n) \in V(I) = \varnothing$. $\Rightarrow\!\Leftarrow$.

"The Rabinowitsch Trick"

If $V(I) = \emptyset \Rightarrow I = k[x_1, \dots, x_n]$

WTS: $I(V(I)) = r(I) \quad \forall I \subseteq k[x_1, \dots, x_n]$.

Take $f \in I(V(I)) \Rightarrow f(p) = 0$ at all points $p \in V(I)$. Suppose we extend

$$I' = I + \langle fy - 1 \rangle \subseteq k[x_1, \dots, x_n, y].$$

$V(I') = \emptyset$. Why? $(p_1, \dots, p_n) \in V(I)$

$\Rightarrow f(p_1, \dots, p_n) = 0 \Rightarrow fy - 1 \neq 0$.

$(p_1, \dots, p_n) \notin V(I) \Rightarrow \exists g \in I$ s.t. $g(p, y) \neq 0$. $\forall y$.

"The Rabinowitsch Trick"

$\Rightarrow I' = k[x_1, \dots, x_n, y]$.

$$1 = \sum_{i=1}^{k} p(x_1, \dots, x_n, y) f_i(x_1, \dots, x_n) + q(x_1, \dots, x_n, y)(fy - 1)$$

Specialize $y = \frac{1}{f}$.

Emmy Noether (1882 - 1935)

Noether Normalization Lemma

Let k be a $\overbrace{\text{(infinite)}}^{\text{not necessary except for this proof}}$ field, $A \neq 0$ a finitely-generated k-algebra. Then, there exist elements $y_1, \ldots, y_r \in A$ which are algebraically independent over k and such that A is integral over $k[y_1, \ldots, y_r]$.

$$\begin{tikzcd} A \arrow[d, dash, "\text{integral ext}"'] \\ k[y_1,\ldots,y_r] \arrow[d, dash, "\text{transc. ext.}"'] \\ k \end{tikzcd}$$

Proof

Suppose $A = k[x_1, \dots, x_n]$.

Renumber $x_1, \dots, x_n$ so that $x_1, \dots, x_r$ are alg. independent, and x_k is alg over $k[x_1, \dots, x_r]$ $\forall k > r$.

Induction on $n-r$. $n-r=0 \Rightarrow$ Done.

Suppose true for $n-r=k$. WTS:

true for $n-r=k+1$.

Proof

By ind hyp, $k[x_1,\dots,x_{n-1}]$ is integral over $k[x_1,\dots,x_r]$. x_n must satisfy a polynomial relation

$$f(x_1,\dots,x_n)=0. \leftarrow \text{deg } m$$

Take the degree m part of f, called f_m.

Take $f_m(\lambda_1,\dots,\lambda_{n-1},1)\neq 0$. (infinite field $\Rightarrow$ okay)

Set $x_i' = x_i - \lambda_i x_n \quad \forall i \leq n-1$.

Proof

Then x_n integral over $k[x'_1, \ldots, x'_{n-1}]$.

$\Rightarrow f(x_1, \ldots, x_n) = 0 \Longrightarrow f(x'_1 + \lambda_1 x_n, \ldots, x'_{n-1} + \lambda_{n-1} x_n, x_n) = 0$.

$\Rightarrow$ highest power of x_n appears on its own without coefficient.

$A := k[x_1, \ldots, x_n]$ integral over $A' = k[x'_1, \ldots, x'_{n-1}]$

$\Rightarrow \exists\, y_1, \ldots, y_{n-1}$ $A' = k[y_1, \ldots, y_{n-1}]$ integral over $k[y_1, \ldots, y_r]$. $\Longrightarrow$ A integral over $k[y_1, \ldots, y_r]$

Geometric Interpretation

Integral extensions $\longleftrightarrow$ surjective maps w/ finite fibers.

There is an r-dim subspace L of k^n s.t. the affine variety V with coordinate ring $A = k[x_1, \dots, x_n]/I(V)$ surjects onto L.

Example: k[x,y]/(xy-1)

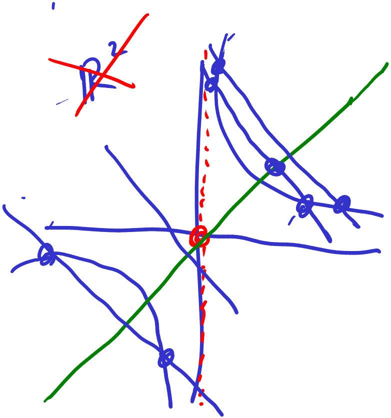
$\mathbb{C}$

$k[x, \quad y]$

alg ind $\qquad$ alg dep on $k[x]$

$xy - 1 \qquad \lambda_1 = 1$

$xy|_{(1,1)} \neq 0.$



$x' = x - y.$

$k[x', y] \qquad xy - 1 = 0 \Rightarrow (x'+y)y - 1 = 0$

integral over $k[x']$. $\quad y^2 + x'y - 1 = 0.$

Noether Nrmlz $\implies$ Weak Nlstlnsatz

Recall

Weak Nullstellensatz: Let k be an algebraically closed field, and $I \subseteq k[x_1, \ldots, x_n]$ be an ideal satisfying $\mathrm{V}(I) = \varnothing$. Then $I = k[x_1, \ldots, x_n]$.

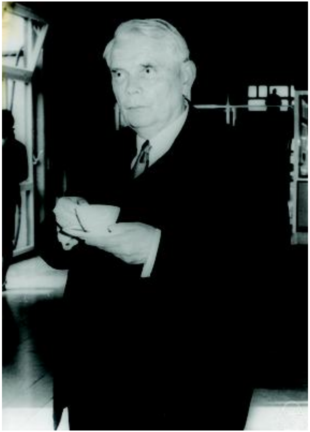
Suppose not. $\exists\, \mathfrak{m}$ maximal, $I \subseteq \mathfrak{m}$.

$A = k[x_1, \ldots, x_n]/\mathfrak{m} = k[y_1, \ldots, y_n] \Rightarrow$.

$y_1, \ldots, y_n$ integral over k. $\Rightarrow$ $y_i \to \alpha_i$ a root of its defining polynomial over k.

$\Rightarrow \exists$ point where all poly's in $\mathfrak{m}$ vanish. $\divideontimes$.

Krull & Jacobson



Def: Jacobson Ring

Let A be a ring.

A is Jacobson if every prime ideal is the intersection of the maximal ideals containing it.

$\iff$ Every non-maximal prime is the intersection of primes strictly containing it.

Jacobson version of Nullstellensatz

Let A be Jacobson, B a f.g. A-algebra, then B is Jacobson.
If $\mathfrak{n} \subseteq B$ maximal, then $\mathfrak{m} = \mathfrak{n} \cap A$ is maximal and $B/\mathfrak{n}$ is a finite extension of $A/\mathfrak{m}$.

Lemma

TFAE: 1) A Jacobson
2) For $\mathfrak{p} \subset A$ prime, if $b \neq 0 \in B = A/\mathfrak{p}$ has $B[b^{-1}]$ a field, then B is a field.

1) $\Rightarrow$ 2). Take $\mathfrak{p} \subset A$ prime. $A/\mathfrak{p}$ integral domain, and Jacobson.
(0) prime $= \bigcap$ maximal ideals.
$b \neq 0 \in B = A/\mathfrak{p}$. with $B[b^{-1}]$ field
Any nonzero max ideal contains $b \Rightarrow b \in (0)$ $\Rightarrow\!\Leftarrow$.
$\Rightarrow$ no nonzero maximal ideals. $\blacksquare$

Lemma

TFAE: 1) A Jacobson
2) For $\mathfrak{p} \subset A$ prime, if $b \neq 0 \in B = A/\mathfrak{p}$ has $B[b^{-1}]$ a field, then B is a field.

2) $\Rightarrow$ 1) $\forall \mathfrak{p} \subset A$ prime. WTS: $\mathfrak{p} = \bigcap_{\substack{\mathfrak{p} \subset \mathfrak{m} \\ \max.}} \mathfrak{m}$

Suppose not. $Q = \bigcap_{\mathfrak{m}\ \max} \mathfrak{m} \neq \mathfrak{p}$.

$\exists f \in Q \setminus \mathfrak{p}$. Construct maximal prime ideal P containing $\mathfrak{p}$ and not f. (Zorn)

P not maximal. $\Rightarrow A/P$ not a field.

But P maximal in $A[f^{-1}] \Rightarrow A/P[f^{-1}]$ field.

$\Rightarrow\Leftarrow$.

Proof: Case $B = A[x]$, A field, x transc

WTS: B Jacobson, $B/\mathfrak{n}$ finite over $A/\mathfrak{m}$.

Primes of this ring are (0) and ideals gen'd by monic irred. polynomial.

Every nonzero prime is max'l.

If $\{\mathfrak{m} \text{ max'l}\}$ is infinite, then $(0) = \bigcap \mathfrak{m}$.

Euclid: Suppose $f_1, \dots, f_n$ irred. $g = f_1 \cdots f_n + 1$.

g has a diff. irred factor.

$\mathfrak{m} = \mathfrak{n} \cap A = (0)$. $B/\mathfrak{n}$ is a finite alg. ext of A.

Proof: Case $B = A[x]$, A Jacobson, x transc

WTS: B Jacobson, B/n finite over A/m.

Take any $b \in B$, $b \neq 0$. Suppose $B[b^{-1}]$ is a field. Then $A[x][b^{-1}]$ is a field.

$K = \mathrm{Frac}(A) \Rightarrow K[x][b^{-1}]$ field.

$K[x]$ Jacobson $\Rightarrow K[x]$ field. $\Rightarrow \Leftarrow$.

$\Rightarrow B[b^{-1}]$ not a field. $\Rightarrow B$ Jacobson.

Proof: $B = A[x]/q$, A Jacobson

WTS: B Jacobson, B/n finite over A/m.

$B = A[x]/q$. (Lemma) Take $b \in B$, $b \neq 0$.

Suppose $B[b^{-1}]$ field, then consider

$$B[b^{-1}] = A[x]/qA[x]\,[b^{-1}]$$

extension of $K[x]/qK[x]$. (field)

$$p_n x^n + p_{n-1}x^{n-1} + \dots + p_0 = 0$$

$B[p_n^{-1}]$ integral over $A[p_n^{-1}]$.

Proof: $B = A[x]/\mathfrak{q}$, A Jacobson

$b \in B \Rightarrow \quad q_m b^m + q_m b^{m-1} + \dots + q_0 = 0$

$\Rightarrow \quad (b^{-1})^m + \frac{q_1}{q_0}(b^{-1})^{m-1} + \dots + \frac{q_m}{q_0} = 0.$

$\Rightarrow b^{-1}$ integral over $A[(p_n q_0)^{-1}]$.

$B[b^{-1}]$ field $\Rightarrow A[(p_n q_0)^{-1}]$ Field.

$\Rightarrow$ A field $\Rightarrow B = A[x]/\mathfrak{q}$ integral extension of a field $\Rightarrow B$ field.

Proof: $B = A[x_1, \dots, x_n]$, A Jacobson

$A' = A[x_1, \dots, x_{n-1}]$ Jacobson by ind hyp.

$A'[x_n]$ Jacobson by base case.

$\mathfrak{n} \subset A[x_1, \dots, x_n] \Rightarrow \mathfrak{n} \cap A[x_1, \dots, x_{n-1}] = \mathfrak{m}$

$B/\mathfrak{n}$ finite over $A'/\mathfrak{m}$. $A'/\mathfrak{m}$ finite over $A/\mathfrak{p}$ $\Rightarrow$ $B/\mathfrak{n}$ finite over $A/\mathfrak{p}$.

$\Rightarrow$ B Jacobson, $B/\mathfrak{n}$ finite over $A/\mathfrak{p}$. $\blacksquare$

Jacobson Version implies Nullstellensatz

A Jacobson, B f.g. A-algebra.

$\Rightarrow$ B Jacobson. B/n finite ext of A/m.

WTS: k alg. closed field. $I \subset k[x_1, \ldots, x_n]$

then $I(V(I)) = r(I)$.

Proof: $k[x_1, \ldots, x_n]$ Jacobson.

k alg. closed $\Rightarrow$ $V(I)$ = set of max ideals containing I.

$\Rightarrow$ $I(V(I)) = \bigcap$ max ideals

$= \bigcap$ prime ideals $= r(I)$. $\blacksquare$