9. THE ALGEBRA-GEOMETRY DICTIONARY

Goal: study the correspondence

$$\begin{array}{ccc} \underline{\text{varieties}} & & \underline{\text{ideals}} \\ W & \longrightarrow & I(W) \\ & & \{p : p(a) = 0 \ \forall a \in W\} \\ & & \\ V(J) & \longleftarrow & J \\ \{a : p(a) \ \forall p \in J\} & & \end{array}$$

Example 9.1

The correspondence is not a bijection:

(1) For $I = \langle x \rangle$, $J = \langle x^2 \rangle$ in $k[x]$

$$V(I) = \{0\} = V(J)$$

More generally for any $p \in k[x_1, \dots, x_n]$ and $m \in \mathbb{N}$

$$V(p) = V(p^m) \quad \text{but} \quad \langle p^m \rangle \subsetneq \langle p \rangle$$

(2) Non-algebraically closed fields are more problematic!

In $\mathbb{R}[x]$ for $I = \langle 1 + x^2 \rangle$, $J = \langle 1 + x^2 + x^4 \rangle$

$$I \nsubseteq J, \quad J \nsubseteq I, \quad V(I) = V(J) = \emptyset$$

Similarly in $\mathbb{R}[x, y]$

$$V(1 + x^2 + y^2) = V(1 + x^2 + y^4) = V(1 + x^2 y^2) = \emptyset$$

$$\langle 1 + x^2 + y^2 \rangle \neq \langle 1 + x^2 + y^4 \rangle \neq \langle 1 + x^2 y^2 \rangle$$

(3) Suppose $I \subset K[x]$ with $V(I) = \emptyset$.

Univariate ideals are principal, so

$$I = \langle p \rangle, \quad p \in K[x] \Rightarrow V(p) = V(I) = \emptyset$$

If K algebraically closed, then

$$V(p) = \emptyset \Rightarrow p \text{ nonzero constant}$$
$$\Rightarrow I = \langle 1 \rangle = K[x]$$

<u>Theorem 9.2</u> (Weak Nullstellensatz)

Let K be algebraically closed and $I \subset K[x_1, \dots, x_n]$ an ideal. Then

$$V(I) = \emptyset \Leftrightarrow I = K[x_1, \dots, x_n]$$

<u>Proof</u>

"$\Leftarrow$" is immediate.

The nontrivial claim is $I \subsetneq K[x_1, \dots, x_n] \Rightarrow V(I) \neq \emptyset$.

This follow by induction on $n \geq 1$.

The case $n = 1$ is Example 9.1(3).

For the induction step we will prove

(*) $I \subsetneq K[x_1, \dots, x_n] \Rightarrow \exists a \in K$ s.t. $I_{x_n = a} \subsetneq K[x_1, \dots, x_{n-1}]$

where

$$I_{x_n = a} = \{ p(x_1, \dots, x_{n-1}, a) \in K[x_1, \dots, x_{n-1}] : p \in I \}.$$

The proof of (*) splits into two cases.

Case 1: $I \cap K[x_n] \neq \{0\}$.

Let $0 \neq p \in I \cap K[x_n]$.

Since K is algebraically closed, $\exists c, a_1, \ldots, a_m \in K$ s.t.

$$p = c \prod_{j=1}^{m} (x_n - a_j)$$

Note: $m \geq 1$ since otherwise $1 = \frac{1}{c} p \in I$

Claim: ⊛ holds for some $a = a_j$, $j = 1, \ldots, m$.

Proof: Suppose not. Then for each $j = 1, \ldots, m$

$I_{x_n = a_j} = K[x_1, \ldots, x_{n-1}] \Rightarrow 1 \in I_{x_n = a_j}$

$\Rightarrow \exists q_j \in I$ such that $q_j(x_1, \ldots, x_{n-1}, a_j) = 1$

Then $q_j = 1 + (x_n - a_j) \cdot h_j$ for some $h_j \in K[x_1, \ldots, x_n]$:

If $q_j = \sum_\alpha c_\alpha x^{\bar{\alpha}} x_n^{\alpha_n}$, $\alpha = (\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) = (\bar{\alpha}, \alpha_n)$

then $q_j(x_1, \ldots, x_{n-1}, a_j + x_n - a_j) = \sum_\alpha c_\alpha x^{\bar{\alpha}} (a_j + (x_n - a_j))^{\alpha_n}$

$$= \sum_\alpha c_\alpha \left(\bar{x}^{\alpha} a_j^{\alpha_n} + (x_n - a_j)(\ldots) \right)$$

It follows that

$$1 = \prod_{j=1}^{m} \left(q_j - (x_n - a_j) \cdot h_j \right) \in \prod_{j=1}^{m} \left(I + (x_n - a_j) h_j \right)$$

$$\subset \prod_{j=1}^{m} (x_n - a_j) h_j + I$$

$$= \frac{1}{c} p \cdot \prod_{j=1}^{m} h_j + I \subset I. \ ↯$$

Hence ⊛ must hold for some $j = 1, \ldots, m$

Case 2: $I \cap K[x_n] = 0$

Let $G = \{g_1, \dots, g_t\}$ Gröbner basis of I in lex.

Decompose the leading monomials as

$$LM(g_i) = x^{\alpha_i} \cdot x_n^{m_i}, \quad x^{\alpha_i} \text{ monomial in } x_1, \dots, x_{n-1}$$

and collect all terms with a x^{α_i} factor

(**) $$g_i = c_i(x_n) \cdot x^{\alpha_i} + \dots \text{terms} < x^{\alpha_i} \dots$$

where $0 \neq c_i \in K[x_n]$

Let $a \in K$ be such that $c_i(a) \neq 0 \quad \forall i = 1, \dots, t$

(Note: this exists since an algebraically closed field is infinite)

Since G is a basis of I,

$$\bar{g}_i := g_i(x_1, \dots, x_{n-1}, a) \in K[x_1, \dots, x_{n-1}], \quad i = 1, \dots, t$$

is a basis of $I_{x_n = a}$.

Claim: $\bar{G} = \{\bar{g}_1, \dots, \bar{g}_t\}$ is a Gröbner basis of $I_{x_n = a}$.

Proof: We will use the lcm-representation generalization of Buchberger's criterion.

For $1 \leq i, j \leq t$, let $x^{\gamma} = \operatorname{lcm}(x^{\alpha_i}, x^{\alpha_j})$ and consider

$$S = c_j(x_n) \cdot \frac{x^{\gamma}}{x^{\alpha_i}} g_i - c_i(x_n) \frac{x^{\gamma}}{x^{\alpha_j}} g_j$$

By (**) $LT(S) < x^{\gamma}$.

By polynomial division we get a standard representation

$$S = \sum_{l=1}^{t} q_l g_l, \qquad LT(q_l g_l) \leq LT(S)$$

Evaluating at $x_n = a$, we get

$$\bar{S} = c_j(a) \frac{x^\gamma}{x^{\alpha_i}} \bar{g}_i - c_i(a) \frac{x^\gamma}{x^{\alpha_j}} \bar{g}_j = \sum_{l=1}^{t} \bar{q}_l \bar{g}_l$$

where $\bar{q}_l = q_l(x_1, \dots, x_{n-1}, a) \in k[x_1, \dots, x_{n-1}]$

Hence we have

- $\bar{S} = c_i(a) c_j(a) \cdot S(\bar{g}_i, \bar{g}_j)$
- $LT(\bar{q}_l \bar{g}_l) \leq LT(q_l g_l) \leq LT(S) < x^\gamma$
- $x^\gamma = lcm(x^{\alpha_i}, x^{\alpha_j}) = lcm(LM(\bar{g}_i), LM(\bar{g}_j))$

So each S-polynomial $S(\bar{g}_i, \bar{g}_j) \in k[x_1, \dots, x_{n-1}]$ has a lcm-representation $\Rightarrow$ $\bar{G}$ Gröbner basis.

To conclude the proof, observe that

$$LT(\bar{g}_i) = c_i(a) x^{\alpha_i}$$

is not a constant since otherwise

$$LM(g_i) = x^{\alpha_i} x_n^{m_i} = x_n^{m_i} \quad \Rightarrow g_i \in k[x_n]$$

and then $I \cap k[x_n] = 0 \Rightarrow g_i = 0$.

Hence $LT(\bar{g}_i) \nmid 1$ for all $i = 1, \dots, t$

so $1 \notin I_{x_n = a}$. $\square$

Fundamental Theorem of algebra:

$$p \in \mathbb{C}[t] \ \& \ 1 \notin \langle p \rangle \implies \exists \text{ solution to } p = 0$$

Weak Nullstellensatz:

$$p_1, \ldots, p_m \in \mathbb{C}[x_1, \ldots, x_n] \ \& \ 1 \notin \langle p_1, \ldots, p_n \rangle$$
$$\implies \exists \text{ solution to } p_1 = \ldots = p_n = 0$$

<u>Theorem 9.3</u> (Hilbert's Nullstellensatz)

Let K be an algebraically closed field and $I = \langle p_1, \ldots, p_s \rangle < K[x_1, \ldots, x_n]$. Then

$$f \in I(V(I)) \iff f^m \in I \text{ for some } m \in \mathbb{N}$$

<u>Proof</u>

"$\Leftarrow$" If $f^m \in I$, then $f^m(c) = 0 \ \forall c \in V(I)$

so also $f(a) = 0 \quad \forall a \in V(I)$.

"$\Rightarrow$" Rabinowitsch's trick: Consider the ideal

$$J := \langle p_1, \ldots, p_s, 1 - yf \rangle < K[x_1, \ldots, x_n, y]$$

<u>Claim</u>: $V(J) = \emptyset$

Proof: Let $(a,b) \in K^n \times K$. Either $a \in V(I)$ or $a \notin V(I)$.

If $a \in V(I)$ then by assumption $f(a) = 0$, so

$$(1 - yf)(a,b) = 1 - b \cdot f(a) = 1 \neq 0 \implies (a,b) \notin V(J).$$

If $a \notin V(I)$ then $p_i(a,b) = p_i(a) \neq 0$ for some $i = 1, \ldots, s$

so again $(a,b) \in V(J)$.

Apply the weak Nullstellensatz to obtain $1 \in J$, so

$$1 = \sum_{i=1}^{s} q_i p_i + q(1 - yf)$$

for some $q_1, \ldots, q_n, q \in k[x_1, \ldots, x_n, y]$

Formally substituting $y = 1/f(x_1, \ldots, x_n)$ we get a rational expression in $x_1, \ldots, x_n$

$$1 = \sum_{i=1}^{s} q_i\left(x_1, \ldots, x_n, \frac{1}{f}\right) p_i(x_1, \ldots, x_n)$$

Clearing denominators, we obtain a polynomial identity

$$f^m = \sum_{i=1}^{s} \tilde{q}_i \, p_i \implies f^m \in I. \quad \square$$

$I(V)$ is a special type of ideal:

$$f^m \in I(V) \implies f \in I(V)$$

Definition 9.4

(1) An ideal I is <u>radical</u> if $f^m \in I \Rightarrow f \in I$.

(2) The radical of an ideal I is the set

$$\sqrt{I} = \{ f : f^m \in I \text{ for some } m \in \mathbb{N} \}$$

Example 9.5

Let $I = \langle x^2, y^3 \rangle \subset k[x,y]$, so

$x \in \sqrt{I}$ and $y \in \sqrt{I}$

Then also

$$xy \in \sqrt{I} \text{ since } (xy)^2 = \overset{\in I}{x^2} \cdot y^2$$

and by the binomial formula $x+y \in \sqrt{I}$ since

$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \in I$$

multiples of x^2 multiples of y^3

Lemma 9.6

If $I \subset k[x_1, \dots, x_n]$ is an ideal, then $\sqrt{I}$ is a radical ideal with $I \subset \sqrt{I}$.

Proof

$I \subset \sqrt{I}$ is immediate (take $m=1$)

That $\sqrt{I}$ is an ideal follows by the argument of Example 9.5:

$$p \in \sqrt{I} \Rightarrow p^m \in I \Rightarrow (pq)^m \in I \text{ for all } q$$

$$p, q \in \sqrt{I} \Rightarrow p^m \in I \text{ and } q^l \in I$$

$$\Rightarrow (p+q)^{m+l-1} = \sum_{i=0}^{m+l-1} \binom{m+l-1}{i} p^i q^{m+l-1-i} \in I$$

since each summand has either $i \geq m$ or $i \leq m-1 \Rightarrow m+l-1-i \geq l$.

Finally, $f^m \in \sqrt{I} \Rightarrow f^{ml} \in I \Rightarrow f \in \sqrt{I}$ so $\sqrt{I}$ is radical $\square$

Theorem 9.7 (Strong Nullstellensatz)

Let k be algebraically closed and $I \subset k[x_1, \dots, x_n]$ an ideal. Then

$$I(V(I)) = \sqrt{I}$$

Proof

Hilbert's Nullstellensatz $\Rightarrow$ $I(V(I)) \subset \sqrt{I}$.

For the converse, let $f \in \sqrt{I}$, so $f^m \in I$.

Then $f^m(a) = 0$ $\forall a \in V(I)$ so also $f(a) = 0$ $\forall a \in V(I)$ and $f \in I(V(I))$. $\square$

Convention: If we don't specify otherwise, then "Nullstellensatz" = Strong Nullstellensatz

Lemma 9.8

If $I \subset k[x_1, \dots, x_n]$ radical ideal, then $\sqrt{I} = I$.

Proof

Lemma 9.6 $\Rightarrow$ $I \subset \sqrt{I}$.

Conversely, if $p \in \sqrt{I}$, then $p^m \in I$ for some I.

Since I is radical, we get $p \in I$. $\square$