Theorem 9.7 (Strong Nullstellensatz)

Let k be algebraically closed and $I \subset k[x_1, \ldots, x_n]$ 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 $I \subset k[x_1, \ldots, x_n]$ 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 $p \in I$. $\square$

Theorem 9.9. (Ideal-Variety correspondence)

Let K be any field.

(i) The maps

I: variety $W \longmapsto$ ideal $I(W)$ and

V: ideal $J \longmapsto$ variety $V(J)$

are inclusion reversing, i.e.,

$J_1 \subset J_2 \Rightarrow V(J_1) \supset V(J_2)$ and

$W_1 \subset W_2 \Rightarrow I(W_1) \supset I(W_2)$

(ii) For any variety W

$$V(I(W)) = W \qquad \text{(so } I \text{ is injective)}$$

For any ideal J

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

(iii) If K is algebraically closed, then

I: {varieties} $\to$ {radical ideals} and

V: {radical ideals} $\to$ {varieties}

are inclusion-reversing bijections and

$$I^{-1} = V, \qquad V^{-1} = I$$

Proof

(i) Let $J_1 \subset J_2 \subset k[x_1, \ldots, x_n]$ ideals. Then

$$V(J_2) = \{a \in k^n : p(a) = 0 \ \forall p \in J_2\}$$
$$\subset \{a \in k^n : p(a) = 0 \ \forall p \in J_1 \subset J_2\} = V(J_1)$$

Let $W_1 \subset W_2 \subset k^n$ varieties. Then

$$I(W_2) = \{p \in k[x_1, \ldots, x_n] : p(a) = 0 \ \forall a \in W_2\}$$
$$\subset \{p \in k[x_1, \ldots, x_n] : p(a) = 0 \ \forall a \in W_1 \subset W_2\} = I(W_1)$$

(ii) Let $W = V(p_1, \ldots, p_s) \subset k^n$ be a variety.

If $a \in W$, then $p(a) = 0 \ \forall p \in I(W) \Rightarrow a \in V(I(W))$

If $a \in V(I(W))$, then $p(a) = 0 \ \forall p \in I(W)$, so in particular $p_1(a) = \ldots = p_s(a) = 0 \Rightarrow a \in W$.

Let $J \subset k[x_1, \ldots, x_n]$ be an ideal. Then

$$V(\sqrt{J}) = \{a \in k^n : \forall p \in J \ \exists m \in \mathbb{N} \ p^m(a) = 0\}$$
$$= \{a \in k^n : \forall p \in J \ \ p(a) = 0\} = V(J)$$

since $p^m(a) = 0 \Leftrightarrow p(a) = 0$

(iii) Lemma 9.6 $\Rightarrow$ $I(W)$ is a radical ideal for any variety W, so

$$I : \{\text{varieties}\} \to \{\text{radical ideals}\}$$

is well defined. The map

$$V : \{\text{radical ideals}\} \to \{\text{varieties}\}$$

is well defined as a restriction map (ie. only the domain changes from $\{\text{ideals}\}$ to $\{\text{radical ideals}\}$)

By (ii), $V(I(W)) = W$ for all varieties W, so

- I is injective,
- V is surjective,
- V is the left-inverse of I,
- I is the right-inverse of V

It remains to show $I(V(J)) = J$ for radical ideals J.

Here we need the algebraically closed field assumption.

Nullstellensatz (Theorem 9.7) $\Rightarrow$ $I(V(J)) = \sqrt{J}$.

Lemma 9.8 $\Rightarrow$ $\sqrt{J} = J$. $\square$

<u>Proposition 9.10</u> (Radical membership)

Let k be an arbitrary field.

Let $I = \langle p_1, \ldots, p_s \rangle \subset k[x_1, \ldots, x_n]$ be an ideal. Then

$$f \in \sqrt{I} \iff 1 \in \langle p_1, \ldots, p_s, 1 - yf \rangle \subset k[x_1, \ldots, x_n, y]$$

<u>Proof</u>

"$\Leftarrow$" Repeat the latter half of the proof of Hilbert's Nullstellensatz (note algebraically closed is not required):

$$1 \in \langle p_1, \ldots, p_s, 1 - yf \rangle$$

$$\Rightarrow 1 = q_1 p_1 + \cdots + q_s p_s + q(1 - yf), \quad q_i \in k[x_1, \ldots, x_n, y]$$

$$\Rightarrow f^m = \tilde{q}_1 p_1 + \cdots + \tilde{q}_s p_s, \quad \tilde{q}_i \in k[x_1, \ldots, x_n]$$

$$\Rightarrow f \in \sqrt{I}$$

"$\Rightarrow$" Let $f \in \sqrt{I}$, so $f^m \in I$ for some $m \in \mathbb{N}$.

Since $I \subset \langle p_1, \dots, p_s, 1-yf \rangle \subset k[x_1, \dots, x_n, y]$, we get

$$\begin{aligned} 1 &= y^m f^m + 1 - y^m f^m \\ &= y^m f^m + (1-yf)(1 + yf + y^2 f^2 + \dots + y^{m-1} f^{m-1}) \\ &\in \langle p_1, \dots, p_s, 1-yf \rangle \quad \square \end{aligned}$$

<u>Example 9.11</u>

Let $I = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle \subset \mathbb{C}[x,y]$.

(1) Question: is $f = y - x^2 + 1$ contained in $\sqrt{I}$?

<u>Algebraic solution:</u>

Computing a reduced Gröbner basis of

$$J = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 - z(y - x^2 + 1) \rangle \subset K[x,y,z]$$

we find $1 \in J$.

(Applying Buchberger's algorithm for example in lex order requires 6 S-polynomial computations, and then reducing the resulting Gröbner basis)

Geometric solution:

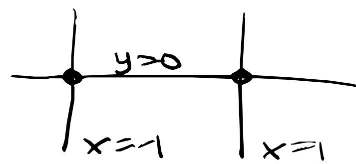
Consider the factorizations

$$xy^2+2y^2 = y^2(x+2), \quad x^4-2x^2+1 = (x^2-1)^2$$

If $x^2-1=0$ for $x\in\mathbb{C}$, then $x+2\neq 0$

Hence (not true in all fields!)

$$V(xy^2+2y^2,\ x^4-2x^2+1) = V((x+2)y^2)\cap V((x^2-1)^2)$$
$$= \left(V(x+2)\cup V(y^2)\right)\cap V((x^2-1)^2)$$
$$= V(y^2)\cap V((x^2-1)^2)$$
$$= V(y)\cap V(x^2-1)$$
$$= V(y,\ x^2-1)$$



and $f = y-x^2+1$ vanishes on $V(y,x^2-1)$ so

$$f\in I(V(y,x^2-1)) = I(V(I)) = \sqrt{I}.$$

(2) Question: what is the minimal $m\in\mathbb{N}$ s.t. $f^m\in I$?

Algebraic solution:

I has a Gröbner basis $G=\{y^2,\ x^4-2x^2+1\}$ in lex.

By polynomial division we can compute

$$\overline{f}^G = f$$
$$\overline{f^2}^G = -2x^2y+2y$$
$$\overline{f^3}^G = 0$$

So the minimal exponent is $m=3$.

Geometric heuristic (not a rigorous argument!)

We observed

$$V(I) = V(y, x^2-1) = \{(\pm 1, 0)\} \subset \mathbb{C}^2$$

However the (univariate) generators

$$p_1 = y^2 \quad \text{and} \quad p_2 = (x^2-1)^2 \quad \text{of } I$$

vanish to order 2 at $(\pm 1, 0)$, i.e.

$$p_2(\pm 1) = p_2'(\pm 1) = 0, \quad p_2''(\pm 1) \neq 0$$

$$p_1(0) = p_1'(0) = 0, \quad p_1''(0) \neq 0$$

Heuristic: therefore all polynomials of I (also multivariate) vanish to order ≥ 2 at $(\pm 1, 0)$ in x or in y

Then we consider how powers of f vanish at $(\pm 1, 0)$:

$$f = \underbrace{y} - \underbrace{(x-1)(x+1)}$$

vanish with order 1

$$f^2 = \underbrace{y^2}_{\text{order 2}} - 2\underbrace{y}_{\text{order 1}}\underbrace{(x-1)(x+1)}_{\text{order 1}} + \underbrace{(x-1)^2(x+1)^2}_{\text{order 2}}$$

$$f^3 = \underbrace{y^3}_{\text{order 3}} - 3\underbrace{y^2}_{\text{order 2}}(x-1)(x+1) + 3y\underbrace{(x-1)^2(x+1)^2}_{\text{order 2}} - \underbrace{(x-1)^3(x+1)^3}_{\text{order 3}}$$

so we should expect $f^3 \in I$.

How to compute a basis for $\sqrt{I}$?
We will postpone the general case for later, but solve the simpler case $I = \langle p \rangle$ now.

Proposition 9.12

Let $p \in k[x_1, \ldots, x_n]$ and $I = \langle p \rangle$. Let
$$p = c \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_n}, \quad c \in k, \quad \alpha_i \geq 1, \quad p_i \in k[x_1, \ldots, x_n]$$
be the factorization of p into distinct irreducible polynomials.
Then $\sqrt{I} = \langle p_1 \cdot \ldots \cdot p_m \rangle$.

Proof

$p_1 \cdots p_m \in \sqrt{I}$ since $p \mid (p_1 \cdots p_m)^{\max\{\alpha_1 \ldots \alpha_n\}}$,
so $\langle p_1 \cdots p_m \rangle \subset \sqrt{I}$.
For the converse, let $f \in \sqrt{I}$, so $f^m \in I$.
Then $f^m = q \cdot p$, so each irreducible factor p_i divides f^m $\Rightarrow$ $p_i \mid f$ for all i $\Rightarrow p_1 \cdots p_m \mid f$ $\square$

Definition 9.13

- Let $p \in k[x_1, \ldots, x_n]$. A <u>reduction</u> or <u>square-free part</u> of p is a polynomial $p_{red} \in k[x_1, \ldots, x_n]$ such that
$$\sqrt{\langle p \rangle} = \langle p_{red} \rangle \quad \text{(only unique up to a constant)}$$
- A polynomial p is square-free if $\sqrt{\langle p \rangle} = \langle p \rangle$.

Definition 9.14

Let $p, q \in k[x_1, \dots, x_n]$. A polynomial $h \in k[x_1, \dots, x_n]$ is a <u>greatest common divisor</u> of p and q, if

(i) $h \mid p$ and $h \mid q$

(ii) if $f \mid p$ and $f \mid q$, then $p \mid h$

We will denote $h = \gcd(p, q)$.

Note: $\gcd(p,q)$ is only unique up to a constant factor.

Proposition 9.15

Let k be a field of characteristic 0 (i.e. $\mathbb{Q} \subset k$). Then for any $I = \langle p \rangle$, $p \in k[x_1, \dots, x_n]$,

$$p_{red} = \frac{p}{\gcd\left(p, \frac{\partial p}{\partial x_1}, \dots, \frac{\partial p}{\partial x_n}\right)}$$