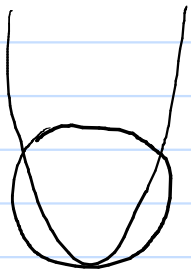
(1) Intersections of curves & Resultants



i) $\begin{cases} f = x^2 - y = 0 \iff -y + x^2 = 0 \\ g = x^2 + (y-1)^2 - 1 = 0 \end{cases}$

$= y^2 - 2y + x^2 = 0$

$$\mathrm{Res}(f, g ; y) = \det \begin{pmatrix} -1 & 0 & 1 \\ x^2 & -1 & -2 \\ 0 & x^2 & x^2 \end{pmatrix}$$

$= x^2(x+1)(x-1)$ $\qquad x^2(x+1)(x-1)$

So the solutions are $(0,0)$, $(-1,1)$, $(1,1)$

Since x has power 2, it is a "double" pt

i.e.  not transverse

Instead from f, we parametrise by (t, t^2):

$t^2 + (t^2-1)^2 - 1 = 0$

$t^4 - t^2 = 0$

$t^2(t^2-1) = 0$

ii) $\begin{cases} f = x^3 - 2xy = 0 \\ g = x^2 y + x - 2y^2 = 0 \end{cases}$

$$\mathrm{Res}(f, g ; x) = \det \begin{pmatrix} 1 & 0 & y & 0 & 0 \\ 0 & 1 & 0 & y & 0 \\ -2y & 0 & -2y^2 & 1 & 0 \\ 0 & -2y & 0 & -2y^2 & 1 \\ 0 & 0 & 0 & 0 & -2y^2 \end{pmatrix}$$

$= 4y^3$

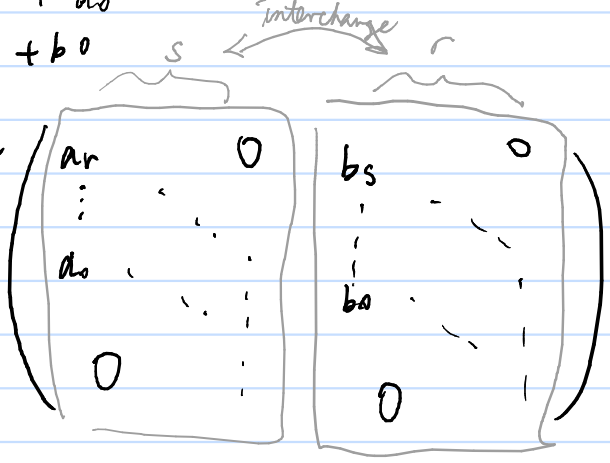
So for $y=0$, $f(x,0)$ and $g(x,0)$ has common root $(0,0)$.

More on resultants

i) Show $\mathrm{Res}(f,g) = (-1)^{rs}\,\mathrm{Res}(g,f)$

for $f = a_r x^r + \cdots + a_0$

$g = b_s x^s + \cdots + b_0$



Pf. $\mathrm{Res}(f,g) = \det$

△ △ △ △

ii) Last time in our proof of equation relating Disc with Res, we proved:

for monic h, k,

$$\mathrm{Res}(h,k) = \prod_{\substack{\gamma \\ \text{roots of } h}} k(\gamma)$$

Indeed, we can show in general:

$$\mathrm{Res}(f,g) = a_r \prod_{\substack{\alpha \\ \text{roots of } f}} g(\alpha)$$

Pf. We know

$$\mathrm{Res}(f,g) = a_r^s b_s^r \prod_{i,j} (\alpha_i - \beta_j)$$

where α are roots of f and β are roots of g

And $g(x) = b_s \prod (x - \beta_j)$

$\Rightarrow g(\alpha_i) = b_s \prod_j (\alpha_i - \beta_j)$

So, $a_r^s \prod_i g(\alpha_i)$

$= a_r^s \prod_i b_s \prod_j (\alpha_i - \beta_j)$

$= a_r^s b_s^r \prod_{i,j} (\alpha_i - \beta_j) = \mathrm{Res}(f,g)$

② Radical ideals

Recall:

R comm ring (unital), $I \subseteq R$.

$$\sqrt{I} := \{r \in R : \exists n \in \mathbb{N}_{>0} : r^n \in I\}$$

I) $\sqrt{I}$ is an ideal of R

Pf. $r, s \in \sqrt{I}$

$\Rightarrow r^m, s^n \in I$

$$(r+s)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} r^i s^{m+n-i}$$

If $i \geq m$, $r^m \mid \binom{m+n}{i} r^i s^{m+n-i}$

If $i \leq m \Leftrightarrow m+n-i \geq n$, $s^n \mid \binom{m+n}{i} r^i s^{m+n-i}$

$k \in R$, $(ks)^m = k^m s^m \in I$.

ii) ✗ prime ideal P is radical

i.e. $\sqrt{P} = P$.

Pf. Obviously we have $P \subseteq \sqrt{P}$

Conversely, suppose $r \in \sqrt{P}$

i.e. $r^m \in P$

WLOG, m is the minimal no. s.t. $r^m \in \sqrt{P}$

if $m > 1$, then $r^{m-1} \in P$ or $r \in P$

$\because m$ is min, $r \in P$

iii) Reduced ring — no non-zero nilpotent element

We know that for a prime ideal P

the quotient ring R/P is an integral domain.

Indeed, there is an analog for radical ideal J

i.e. R/J is a reduced ring.

Pf. J radical.

Suppose $(r+J)^n = 0$ in R/J

$\Rightarrow r^n + J = 0$

$\Rightarrow r^n \in J \Rightarrow r \in J$ $\because J$ radical

$\Rightarrow r + J = 0$ in R/J

Conversely, suppose R/J is reduced ring

$r^n \in J$

$$0 + J = r^n + J = (r+J)^n$$
$$\Rightarrow r + J = 0$$
$$\Rightarrow r \in J$$
$$\therefore J \text{ is radical}$$

iv) In UFD, describe the radicals of a principal ideal:

Let (g) be a principal ideal.
Write $g = g_1^{k_1} \cdots g_n^{k_n}$ as irreducible decomposition

Claim: $\sqrt{(g)} = (g_1 \cdots g_n)$

$(g_1 \cdots g_n)$ all primes

Obviously $(g_1 \cdots g_n) \subseteq \sqrt{(g)}$

$$f \in \sqrt{(g)} \Rightarrow f^m \in (g) = (g_1^{k_1} \cdots g_n^{k_n})$$
$$\Rightarrow g_1^{k_1} \cdots g_n^{k_n} \mid f^m$$
$$\Rightarrow g_1^{k_1} \mid f^m, \quad g_2^{k_2} \mid f^m, \cdots$$

$I \subseteq \sqrt{I}$ as always (take $n=1$)

irr = prime

$$\Rightarrow g_1 \mid f^m, \cdots, g_n \mid f^m$$
$$\Rightarrow f^m \in (g_1 \cdots g_n)$$

v) $\sqrt{\sqrt{I}} = \sqrt{I}$:

pf. $r \in \sqrt{\sqrt{I}} \Rightarrow \exists n, \ r^n \in \sqrt{I} \Rightarrow \exists m, \ (r^n)^m \in I$
$$\Rightarrow r^k \in I, \quad k = mn$$

vi) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} = \sqrt{I \cdot J}$

pf. $r^n \in I \cap J \Leftrightarrow r^n \in I \wedge r^n \in J$

def of ideal

$r^n \in I \cdot J \Leftrightarrow r^n = i \cdot j \Leftrightarrow r^n \in I \wedge r^n \in J$

vii) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$

pf. $r^n \in I + J \Leftrightarrow r^n = i + j \Rightarrow r^n \in r(I) + r(J)$ since $i \in \sqrt{I}$ and $j \in \sqrt{J}$

$r^n \in \sqrt{I} + \sqrt{J} \Leftrightarrow r^n = r_i + r_j$ where $r_i^a \in I$, $r_j^b \in J$

then $r^{n(a+b)} = (r_i + r_j)^{(a+b)}$

WTS: $r^k \in I + J$

$$= r_i^{a+b} r_j^0 + \binom{a+b}{1} r_i^{a+b-1} r_j^1 + \cdots + r_i^0 r_j^{a+b}$$
$$= \sum_{k=0}^{a+b} \binom{a+b}{k} r_i^k r_j^{a+b-k}$$

If $k \geq a$, $r_i^a \mid$ the term

If $k \leq a \Leftrightarrow a+b-k > b$, $r_j^b \mid$ the term

③ Affine varieties & Vanishing ideals:

i) Show the following:

1. $V(0) = \mathbb{A}^n$, $V(1) = \emptyset$

2. If $I \subseteq J$, then $V(I) \supseteq V(J)$

3. Intersection of any collection of affine varieties is affine variety

(Hint: $\{I_\alpha\}$, $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$)

4. Finite union of affine varieties is affine variety

(Hint: $V(I) \cup V(J) = V(I \cap J)$)

Pf. 1. $\forall p \in \mathbb{A}^n$, $0(p) = 0$

$\forall p \in \mathbb{A}^n$, $1(p) = 1 \neq 0$

2. $F(p) = 0 \quad \forall F \in J$

$\Rightarrow F(p) = 0 \quad \forall F \in I \subseteq J$

3. $V(\bigcup_\alpha I_\alpha) \subseteq V(I_\alpha)$ by 2.

$\Rightarrow V(\bigcup_\alpha I_\alpha) \subseteq \bigcap_\alpha V(I_\alpha)$

Conversely, $p \in \bigcap_\alpha V(I_\alpha)$

$\Rightarrow F(p) = 0 \quad \forall F \in I_\alpha$, $\forall \alpha$

$\Rightarrow F(p) = 0 \quad \forall F \in \bigcup_\alpha I_\alpha$

$\Rightarrow \bigcap_\alpha V(I_\alpha) \subseteq V(\bigcup_\alpha I_\alpha)$

4. $V(I) \supseteq V(I \cap J)$, $V(J) \supseteq V(I \cap J)$ by 2.

$\Rightarrow V(I) \cap V(J) \supseteq V(I \cap J)$

Conversely, $p \notin V(I) \cup V(J)$

$\exists F \in I$, $G \in J$; $F(p) \neq 0$, $G(p) \neq 0$

$\Rightarrow FG(p) \neq 0$

$FG \in I \cap J$, so $p \notin V(I \cap J)$

ii) Show the following:

1. If $\inf$, $I(\mathbb{A}^n) = (0)$ and $I(\phi) = (1)$

2. If $X \subset Y$, then $I(X) \supset I(Y)$

Pf. 1. $F(p) = 0(p)$ $\forall p \in \mathbb{A}^n$
$\Rightarrow F \equiv 0$ since k is inf
$\forall p \in \phi$, $F(p) = 0$ $\forall F$

2. $F(p) = 0$ $\forall p \in Y$
$\Rightarrow F(p) = 0$ $\forall p \in X \subset Y$

iii) Show that there is a Galois connection:

1. $J \subseteq I(V(J))$ $\forall J \subseteq k[x_1, \dots, x_n]$

2. $X \subseteq V(I(X))$ $\forall X \subseteq \mathbb{A}^n$

3. $V(J) = V(I(V(J)))$

4. $I(X) = I(V(I(X)))$

so we have a Galois correspondence

$$\{\text{ideals of } k[x_1 \dots]\} \underset{I}{\overset{V}{\rightleftarrows}} \{\text{affine varieties of } \mathbb{A}^n\}$$

Pf. 1. Suppose $p \in V(J)$
then $\forall H \in J$, $H(p) = 0$ $\forall p \in V(J)$
$\Rightarrow H \in I(V(J))$

2. Suppose $F \in I(X)$
then $\forall x \in X$, $F(x) = 0$ $\forall F \in I(X)$
$\Rightarrow x \in V(I(X))$

3. $J \subseteq I(V(J))$

$\Rightarrow V(I(V(J))) \subseteq V(J)$ by (i) 2.

But $X = V(J)$ in (iii) 2.

$\Rightarrow V(J) \subseteq V(I(V(J)))$

4. $X \subseteq V(I(X))$

$\Rightarrow I(V(I(X))) \subseteq I(X)$ by (ii) 2.

But $J = I(X)$ in (iv) 1.

$\Rightarrow I(X) \subseteq I(V(I(X)))$

The center of class AG is the correspondence between poly and the points on a space representing the roots.

Examples:

iv) { quadratic poly up to scalar mult } $\longleftrightarrow$ { zero set of quadratic poly } (affine variety):

Pf. Suppose 2 quad poly f, g have same zero set (affine variety)

Then by the theory of resultant,

f, g have common factor

Case I: common factor is of degree 2

then $f = hg$ where $\deg h = 0 \Rightarrow$ scalar

Case II: common factor is of degree 1

Divide f and g by this linear common factor

Then f', g' also have same zero set,

by the theory of resultant again

f', g' have common factor.

So $f' = h g' \Rightarrow h$ is scalar

then

$f = hg$ for scalar h

The other direction is obvious.

Rk. cubic poly is not the same: fg^2 and $f^2 g$ have same zero set but they are not scalar multiple of each other

④ A glance of Zariski topology

Idea:

Zariski topology defines closed sets as subvarieties of affine varieties.

i.e. closed sets are of the form $V(S)$

i) How does the Zariski top look like in $\mathbb{A}^1$?

In $\mathbb{A}^1$,

irreducible poly is linear poly

Either $f \equiv 0$, or we decompose f into finite linear factors

$\Rightarrow$ a finite set of points is closed as they are the roots of f.