Midterm 3: this Thurs. 7:00-8:30 Loomis Lab. 144

Topics: everything through Galois theory

Practice problems + policies: see email

No problem session tomorrow

Instead: problem session will be Thurs. 10am-12pm, 3rd floor of Altgeld (345 or 347)

Algebraic geometry (roughly) studies sol'ns to sets of (multivariate) polynomial eq'ns

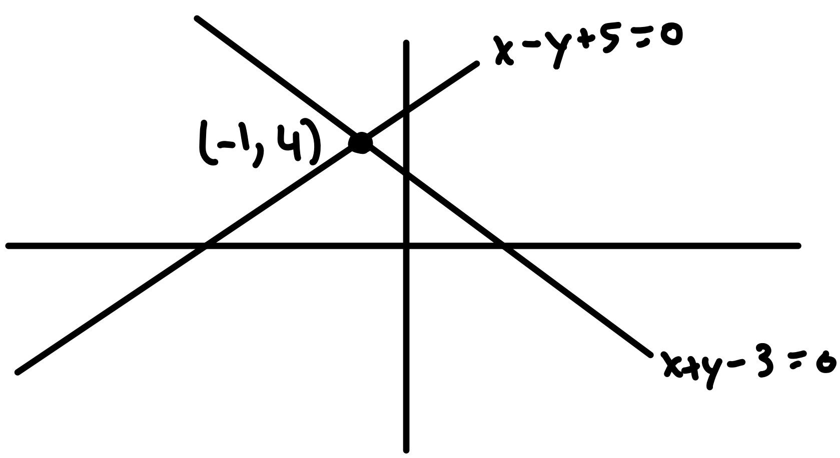
a) does a solution exist?

b) what is the "shape" of the set of sol'ns

Examples in $\mathbb{C}[x,y]$:

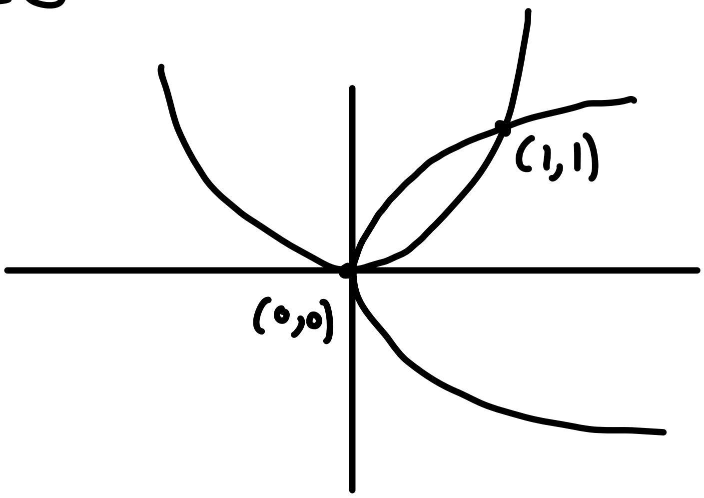
$x+y=3 \rightsquigarrow f(x,y) := x+y-3=0$

$x-y=5 \rightsquigarrow g(x,y) := x-y+5=0$



$y - x^2 = 0$

$x - y^2 = 0$



& (ζ_3, ζ_3^2)

(ζ_3^2, ζ_3)

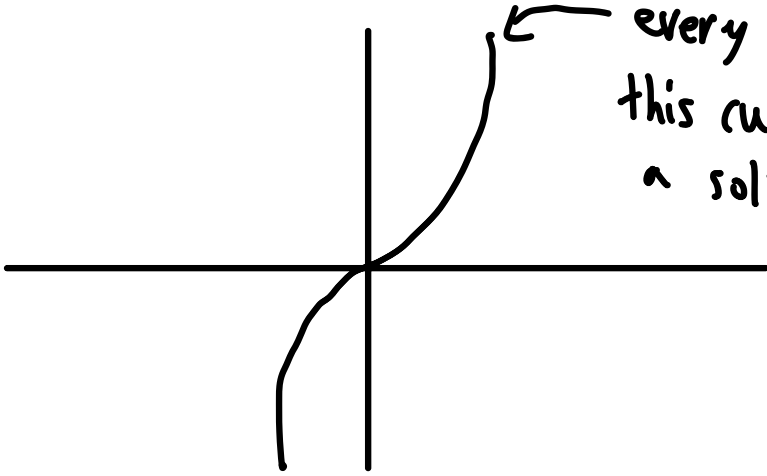
Aside:

Bézout's Thm: The "usual" situation is that two poly. in $\mathbb{C}[x,y]$ of degrees m and n have $m \cdot n$ intersection points in $\mathbb{C}$

Starting point for "intersection (co)homology"

$y - x^3 = 0$

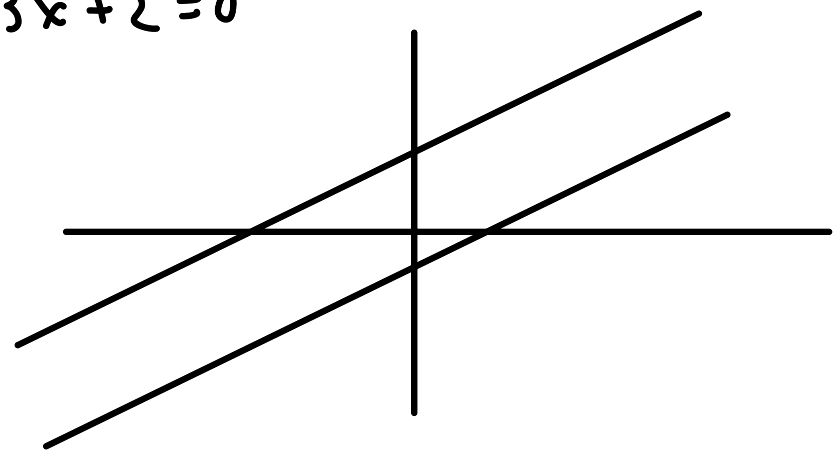
$2y - 2x^3 = 0$



every pt. on this curve is a sol'n

$f(x,y) = 4y - 2x - 6 = 0$

$g(x,y) = -6y + 3x + 2 = 0$



no soln's

Why not?

$$3f - 2g = 12y - 6x - 18 + 12y - 6x - 4 = -22$$

Hilbert's Nullstellensatz (weak form, first version):

Let $f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$

Then the system of equations

$$f_1(x_1, \dots, x_n) = \dots = f_m(x_1, \dots, x_n) = 0$$

has <u>no</u> solution in $\mathbb{C}^n$ if and only if

$\exists\, g_1, \dots, g_m \in \mathbb{C}[x_1, \dots, x_n]$ s.t. $f_1 g_1 + \dots + f_m g_m = 1 \in \mathbb{C}[x_1, \dots x_n]$

Def:

a) An ideal of a (comm, unital) ring R is a subset $I \subseteq R$ s.t. $a, b \in I$, $r \in R \Rightarrow a+b,\ ra \in I$.

b) The radical of an ideal I is the ideal

$$\sqrt{I} = \{ r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}_{\geq 0} \}$$

If $\sqrt{I} = I$, we call it a radical ideal

Remark: $\sqrt{\sqrt{I}} = \sqrt{I}$

Examples:

$R = \mathbb{Z}$, $I = \langle 8 \rangle$, $\sqrt{I} = \langle 2 \rangle$

$R = \mathbb{C}[x]$, $I = \langle x^2(x+1) \rangle$, $\sqrt{I} = \langle x(x+1) \rangle$

Unless otherwise stated, let k be an alg. closed field

Def: An (affine) algebraic variety (or algebraic set) is a subset $V \subseteq k^n$ of the form

$$V = V(I) := \{ f_i(x_1, .., x_n) = 0 \mid \forall i \in I \}$$

for some subset $I \subseteq k[x_1, .., x_n]$

(*Note*: D&F require "irreducibility")

All of our original examples were varieties

Remark: Can (and will!) take I to be an ideal since

$$f(x_1,..,x_n) = g(x_1,..,x_n) = 0 \Rightarrow (f+g)(x_1,..,x_n) = 0$$

$$f(x_1,..,x_n) = 0 \Rightarrow (f \cdot h)(x_1,..,x_n) = 0 \quad \forall h \in k[x_1,..,x_n]$$

Prop: I, J : ideals

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

b) $V(I) \cap V(J) = V(I \cup J) = V(I + J)$

c) $V(I) \cup V(J) = V(I \cap J) = V(IJ)$

d) $V(0) = k^n$ and $V(\langle 1 \rangle) = \phi$

Def: V: alg. variety. Then set

$$I(V) = \{ f \in k[x_1,..,x_n] \mid f(a) = 0 \ \forall a \in V \}$$

$= (a_1,..,a_n)$

Prop: U, V: varieties

a) $U \subseteq V \Rightarrow I(U) \supseteq I(V)$

b) $I(U \cup V) = I(U) \cap I(V)$

c) $I(U \cap V) \supseteq I(U) + I(V)$

Prop:

a) $V = V(I(V))$

b) $I \subseteq I(V(I))$

Pf of a): If $a \in V$, then $\forall f \in I(V)$, $f(a) = 0$, so $a \in V(I(V))$.
Since V is a variety, $V = V(J)$ for some ideal J.
We must have $J \subseteq I(V)$, but then $V(J) \supseteq V(I(V))$, so
$V(I(V)) = V(J) = V$. $\square$

i.e. a) is an equality because we already know that every variety V is of the form $V = V(J)$. If we know that $I = I(U)$, then $I(V(I)) = I$ by the same argument.

Hilbert's Nullstellensatz (strong form): $I(V(I)) = \sqrt{I}$.
Moreover, we have inverse bijections

$$\begin{array}{ccc} \text{alg. varieties} & \xrightarrow{\quad I \quad} & \text{radical ideals} \\ V \subseteq k^n & \xleftarrow[\quad V \quad]{} & I \subseteq k[x_1, \dots, x_n] \end{array}$$

Cor: Hilbert's Nullstellensatz (weak form, second version)

Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. Then $V(I) = \emptyset$ if and only if $1 \in I$ (and so $I = k[x_1, \ldots, x_n]$)

Pf: By the strong form,

$$\sqrt{I} = I(V(I)) = I(\emptyset) = k[x_1, \ldots, x_n],$$

so $1 \in \sqrt{I}$. This means that $1^n \in I$ for some n,

so $1 = 1^n \in I$ $\square$