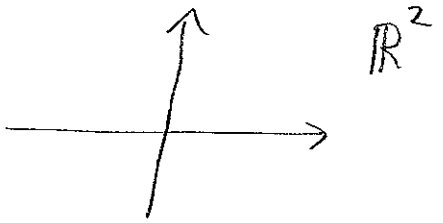
Lecture 31: Toward Algebraic Geometry.

The focus of the rest of the course will be *algebraic geometry*. Roughly, solutions to systems of polynomial equations.

Fix a field k $(= \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_p, \ldots)$

Affine space: $k^n = \mathbb{A}^n_k$



Algebraic Variety: $I \subseteq k[x_1, x_2, \ldots, x_n]$

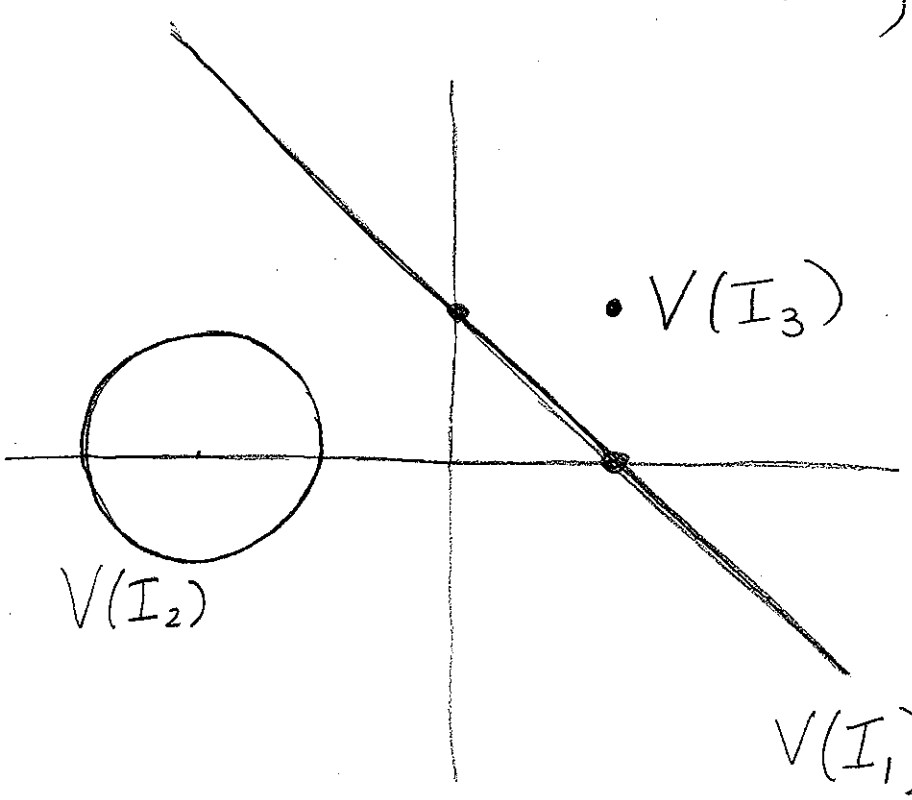
$$V(I) = \{(a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}$$

Ex: $k = \mathbb{R}$, $n = 2$

$I_1 = \{x + y - 1\}$

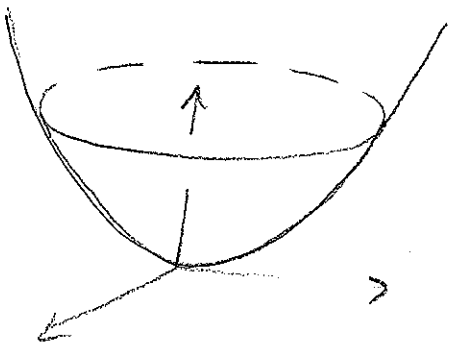
$I_2 = \{(x+2)^2 + y^2 - 1\}$

$I_3 = \{x - y, x + y - 2\}$



Ex: $k = \mathbb{R}$, $n = 3$

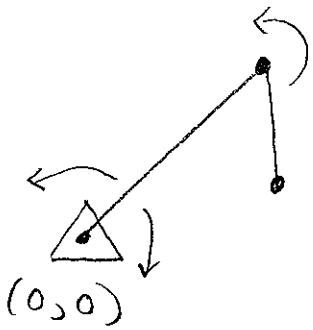
$I = \{z - x^2 - y^2\}$



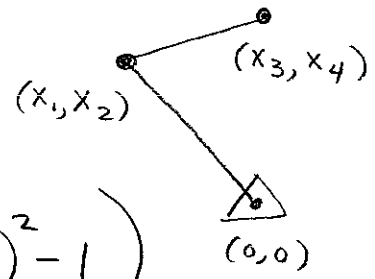
Places where such equations arise:

Robotics: Simplified robot arm in $\mathbb{R}^2$:

Joints move freely, segments have lengths 3 and 1.

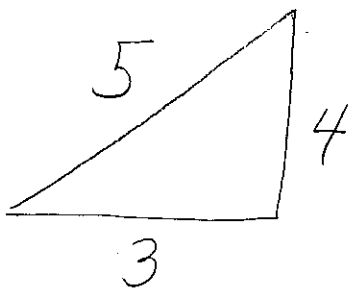


A configuration of the arm can be tracked via a point in $\mathbb{R}^4$



Space of all configs $= V\left(x_1^2 + x_2^2 - 9,\ (x_1 - x_3)^2 + (x_2 - x_4)^2 - 1\right)$

Number Theory: Find all integers with $a^2 + b^2 = c^2$



Equivalently, $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$,

i.e. solving $x^2 + y^2 = 1$ for $x, y \in \mathbb{Q}$.

F.L.T. in $\mathbb{Q}^2$, $V(x^n + y^n - 1) = \emptyset$ for $n > 2$.

Cryptography:

Elliptic curve:

$$C = V(y^2 - (x^2+x+1)) \subseteq \mathbb{F}_5^2$$

Has nine pts; have a group str. $\cong \mathbb{Z}_9$.

For much larger $\mathbb{F}_p$, used for pub. key cryptosystems.

Algebra: Let $S \subseteq k[x_1, \ldots, x_n] = R$

If I is the ideal generated by S

then

$$V(S) = V(I)$$

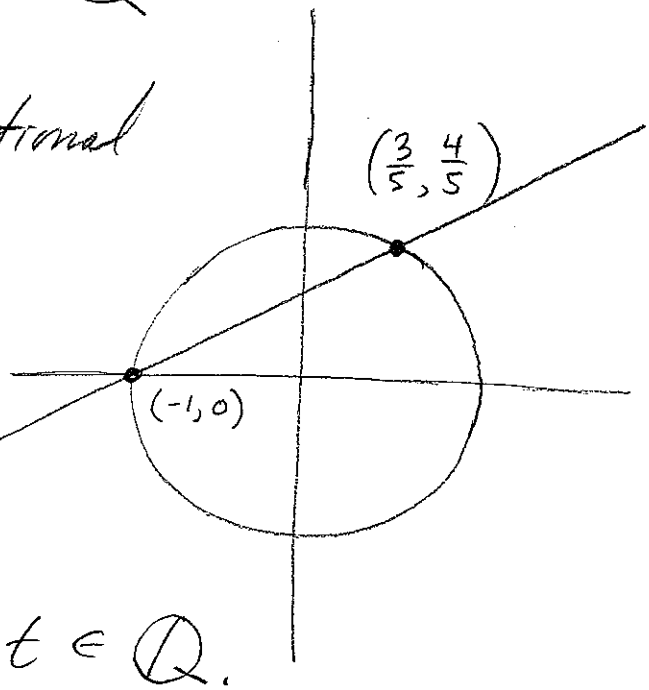
Pf: Clearly $V(I) \subseteq V(S)$. If $f \in I$, then $f = \sum g_i s_i$ for $s_i \in S$, $g_i \in R$

So if $a \in k^n$ is in $V(S)$,

we have $f(a) = \sum g_i(a) s_i(a) = 0$. So $a \in V(I)$.

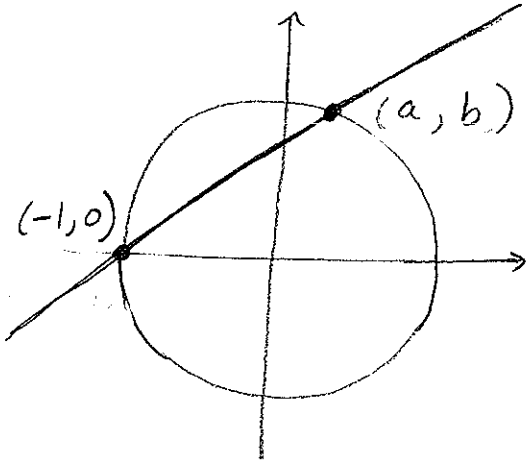
Geometry: Consider

$$C = V(x^2+y^2-1) \subseteq \mathbb{Q}^2$$



The line shown has rational slope t. Flip around: find other solutions by starting with the line

$$y = t(x+1) \text{ for some } t \in \mathbb{Q}.$$



We have

$$a^2 + t^2(a+1)^2 = 1$$

and hence

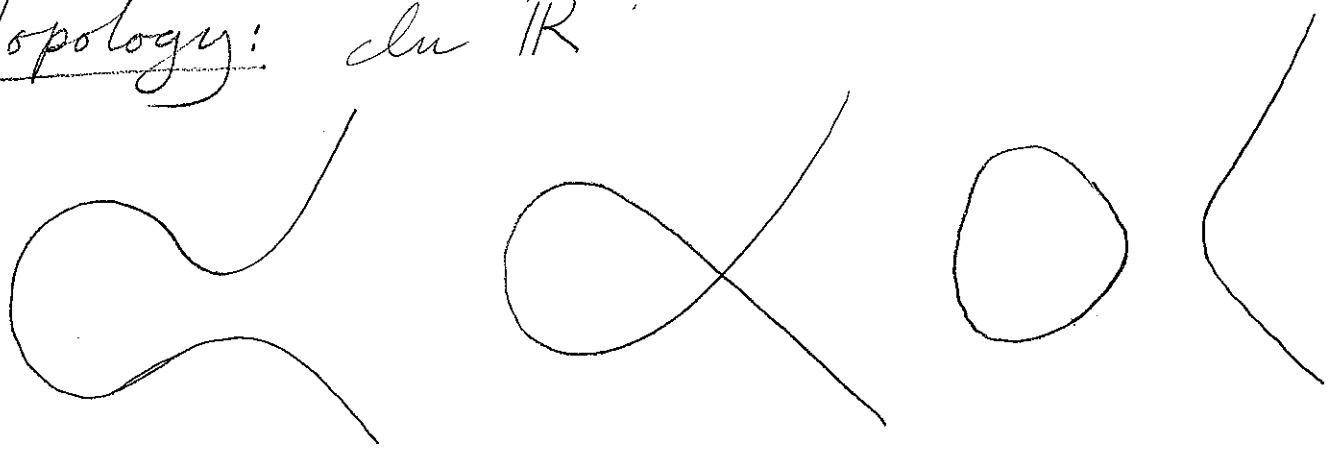
$$t^2(a+1)^2 = 1-a^2$$

$$\Rightarrow t^2(a+1) = (1-a)$$

$$\Rightarrow a = \frac{1-t^2}{1+t^2} \qquad b = \frac{2t}{1+t^2}$$

Thm: Except for interchanging x, y all solutions in $\mathbb{Z}$ to $X^2+Y^2=Z^2$ are $X = m(p^2-q^2)$, $Y = 2pq$, $Z = m(p^2+q^2)$

Topology: on $\mathbb{R}^2$.



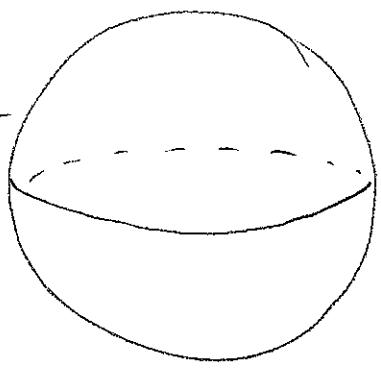
$y^2 = (x+1)(x^2+\varepsilon)$ $\quad$ $y^2 = (x+1)x^2$ $\quad$ $y^2 = (x+1)(x^2-\varepsilon)$

Over $\mathbb{C}$, 1st and 3rd are the same,

$= $  $= S^1 \times S^1$

where $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$, a group under mult.

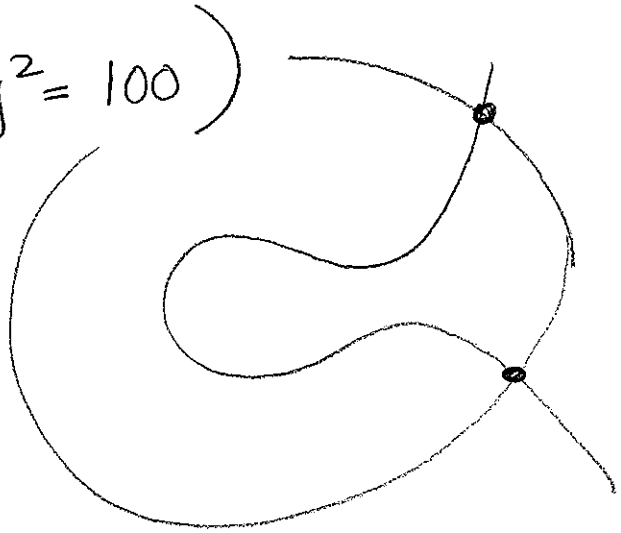
Back to Robotics: $V =$ 

Compare 

Discuss combing hair and control systems.

Computation: in $\mathbb{R}^2$

$V = V\left(y^2 - (x+1)(x^2+1/10),\ x^2+y^2 = 100\right)$



do two pts, with

algebraic coordinates

(cf. constructable #s)

How can we find them?

Resultants, Gröbner basis, homotopy continuation, ...

Galois Theory: Can understand V

in terms of functions on it, e.g. polynomial

fns $= k[x_1, \ldots, x_n]/I$.

$\mathbb{C}(t)$ = ratl fns on $\mathbb{P}^1(\mathbb{C})$

Thm: Every finite gp occurs as

$Gal(K/\mathbb{C}(t))$

Applications to biology, etc...

References:

D+F: Chapter 15.

Cox, Little, and O'Shea ← see web page for more.

Reid ←

PDFs of first book avail. from library.