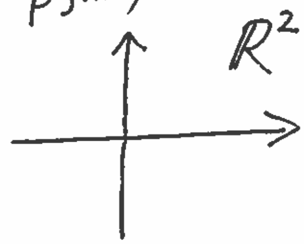
Lecture 30: Toward algebraic geometry.

Rest of course will focus on *algebraic geometry*, the study of solutions to polynomial equations.

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

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



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

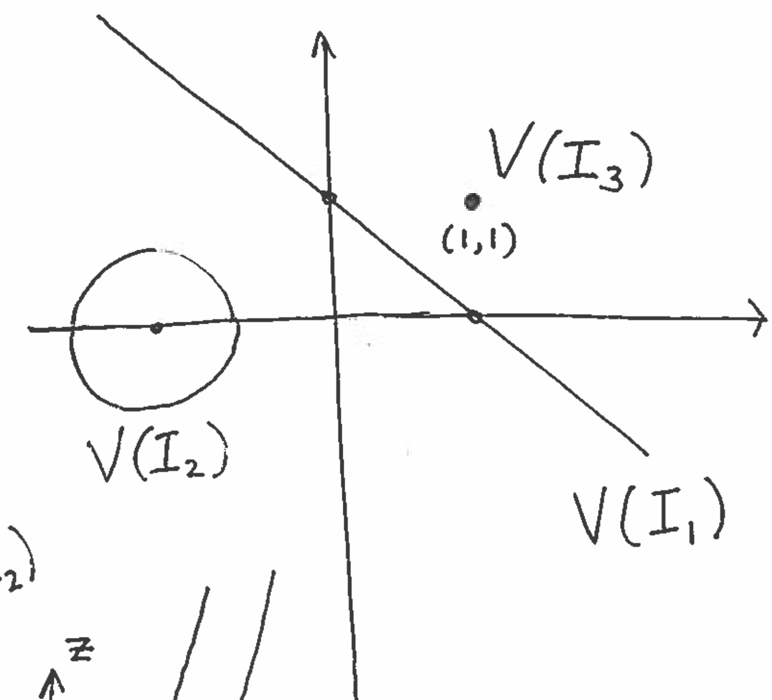
$$V(I) = \{(a_1, \dots, a_n) \in k^n \mid f(a_1, \dots, a_n) = 0 \text{ for all } f \in I\}$$

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

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

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

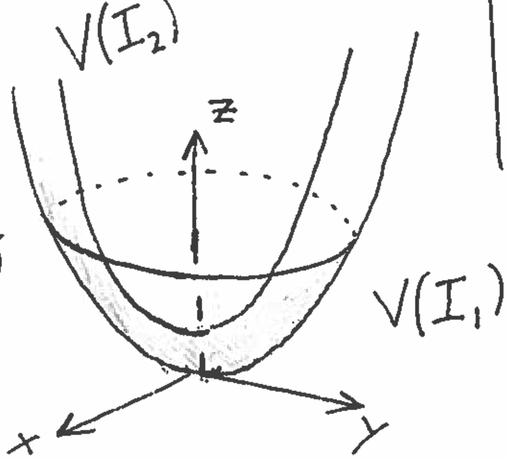
$I_3 = \{x - y, x + y - 2\}$



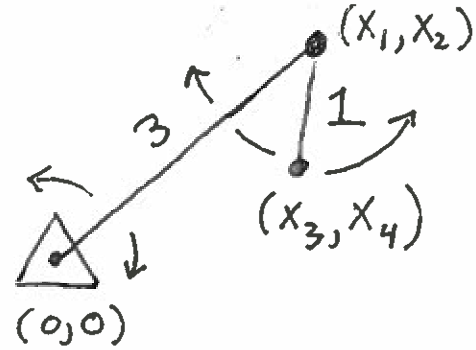
Ex: $k = \mathbb{R}^3$, $n = 3$

$I_1 = \{z - x^2 - y^2\}$

$I_2 = \{z - x^2 - y^2, x + y - 1\}$



Places where alg. varieties arise:



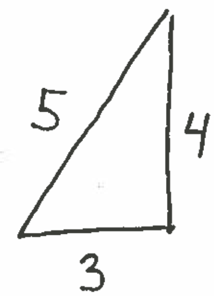
Robotics: Simplified robot arm in $\mathbb{R}^2$. Joints move freely.

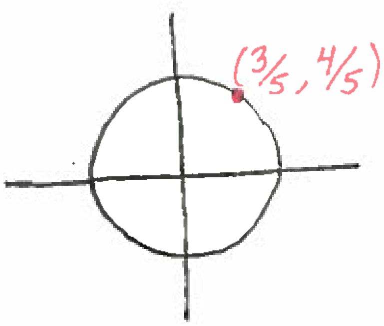
A configuration can be tracked by a point in $\mathbb{R}^4$

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

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

Equivalently $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$, so we want to find all $x, y \in \mathbb{Q}$ where $x^2 + y^2 = 1$.





Fermat's Last Thm: In $\mathbb{Q}^2$,

$$V(x^n + y^n - 1) = \emptyset \text{ for } n > 2.$$

Cryptography: One form of public key cryptosystems uses elliptic curves over $\mathbb{F}_p$.

$$C = V(x^3 + x + 1 - y^2) \subseteq \mathbb{F}_5^2$$

has nine points, which have a group str making them $\cong C_9$. For (much) larger p, things get complicated...

Algebra: Suppose $S \subseteq k[x_1, \dots, x_n] = R$.

If I is the ideal gen. by S, then

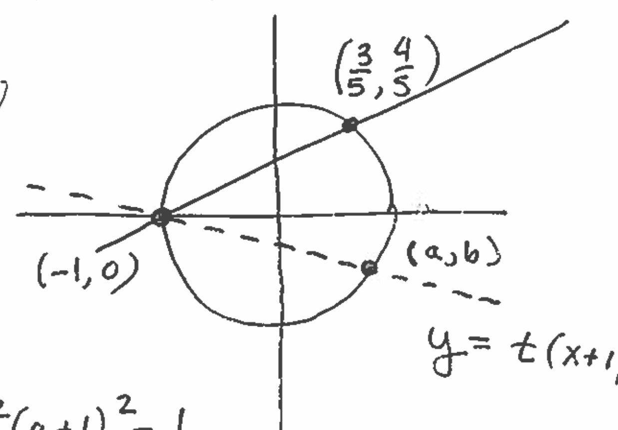
$$V(S) = V(I)$$

Pf: First, $I \supseteq S \Rightarrow V(I) \subseteq V(S)$. If $f \in I$, then $f = \sum g_i s_i$ for some $s_i \in S$ and $g_i \in R$.

So for $a \in V(S) \subseteq k^n$, we have $f(a) = \sum g_i(a) s_i(a)$

$= \sum g_i(a) \cdot 0 = 0$. So $a \in V(I)$. $\square$

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



Note the line shown has rational slope $\frac{4/5}{8/5} = \frac{1}{2}$. Flip this around: for $t \in \mathbb{Q}$, consider the line $y = t(x+1)$. We have $a^2 + t^2(a+1)^2 = 1$

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

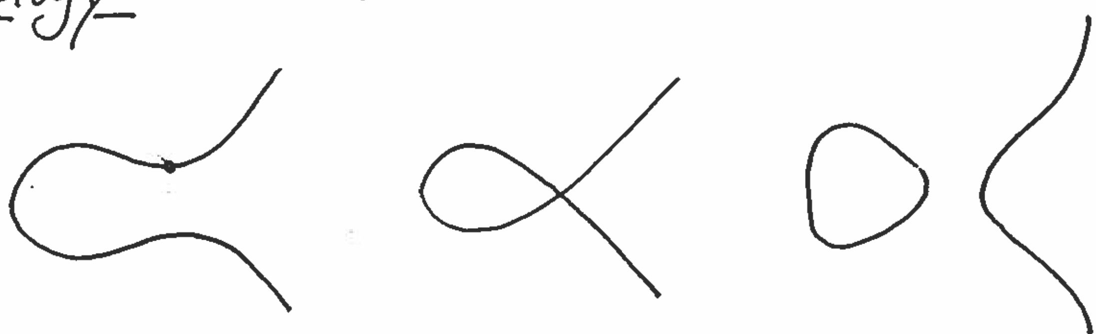
$$\Rightarrow a = \frac{1-t^2}{1+t^2} \qquad b = \frac{2t}{1+t^2}$$

Thm: Except for interchanging x, y, all solutions in $\mathbb{Z}$ to $x^2+y^2=z^2$ are

$$x = m(p^2-q^2), \quad y = 2mpq, \quad z = m(p^2+q^2)$$

with $m, p, q \in \mathbb{Z}$.

Topology: In $\mathbb{R}^2$



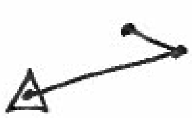
$y^2 = (x+1)(x^2+\varepsilon)$ $\qquad$ $y^2 = (x+1)x^2$ $\qquad$ $y^2 = (x+1)(x^2-\varepsilon)$

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

 $= S^1 \times S^1$ where the circle

$S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}$ is a group under multiplication.

Back to Robotics: $V =$ . Compare 

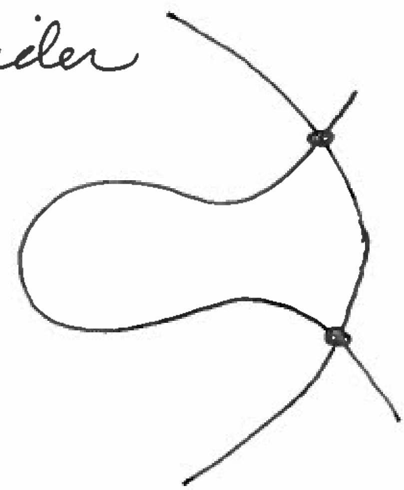
 Discuss combing hair and control systems.

<u>Galois Theory</u>: Will understand V in terms of functions on it, e.g. polynomial functions
$= k[x_1, \dots, x_n]/I$

$\mathbb{C}(t) =$ rational functions on $\mathbb{P}^1(\mathbb{C}) =$ 

<u>Thm</u> Every finite group occurs as $\mathrm{Gal}(K/\mathbb{C}(t))$.

<u>Computational aspects</u>: In $\mathbb{R}^2$, consider



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

<u>Fact</u>: These points have <u>algebraic</u> coordinates.

How can we find them? Resultants, Gröbner basis, PHC...

<u>Applications to biology...</u>

<u>References</u>: D-F, Chapter 15
Cox, Little, O'Shea
Reid

$\Big\}$ see webpage.