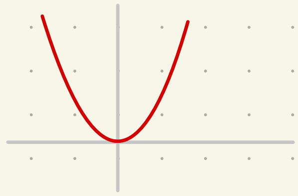
7. Projective geometry: to infinity and beyond

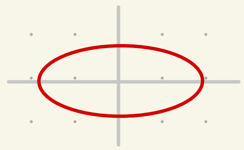
Algebraic geometry: study of spaces given by polynomial equations:

Parabola $\quad y = x^2$



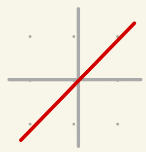
deg 2

Ellipse $\quad x^2+3y^2 = 1$



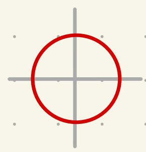
deg 2

Line $\quad y-x=0 \quad =$



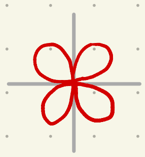
deg 1

Circle $\quad : \; x^2+y^2-1=0 \quad =$



deg 2

Flower? $\quad (x^2+y^2)^3 - 4x^2y^2=0 \quad =$



deg 6

Question: If $y = p(x)$ and p has degree 2, how many points of intersection with the x-axis can there be?
3
n?

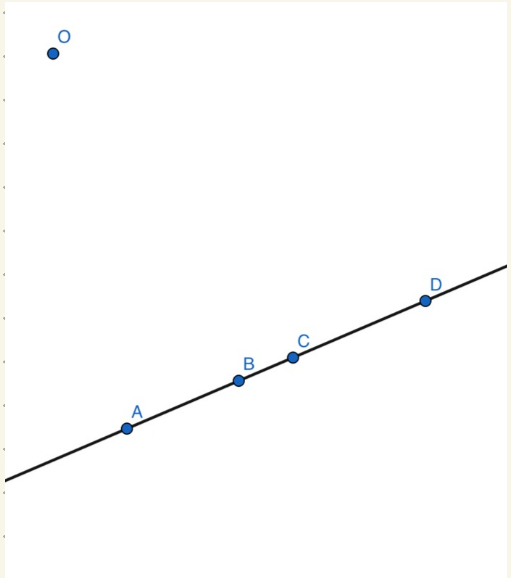
↳ Challenge: what if we allow complex numbers?

(Start video https://youtu.be/XXzhqStLG-4 , "Algebraic curves in perspective" by Bill Shillito)

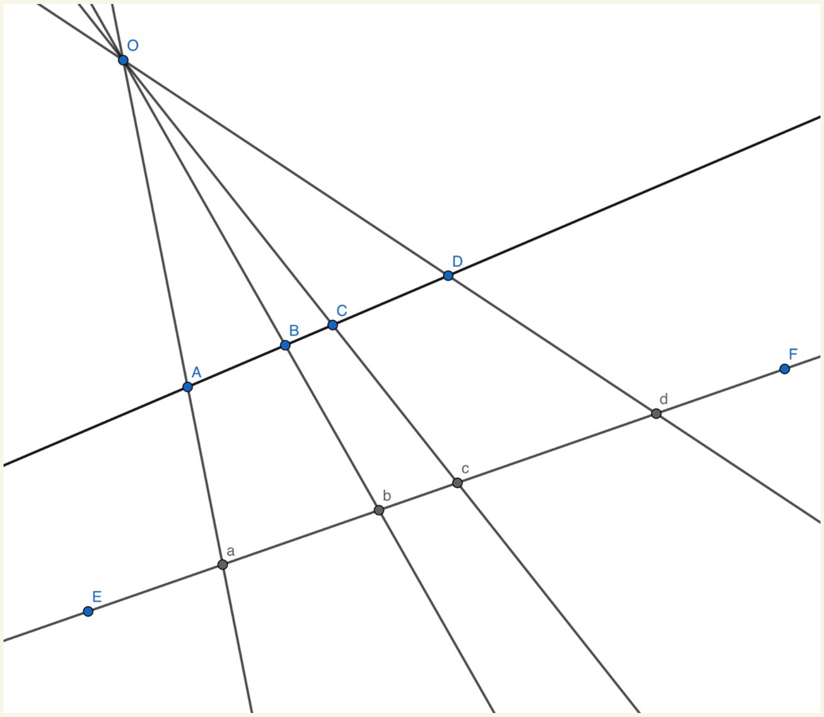
Stop at 4:25

Exploring the cross-ratio

1. Go on Geogebra - geometry and create a line with 4 points A, B, C, D on it. Create also a point O not on the line.



2. We want O to be the "center of perspective", and transport our 4 points to another line with respect to O. So create another line and join O and A, B, C, D to get points a, b, c, d on the new line (relabel them to avoid confusion)



3. Consider the distances AD, BC, AC, BD
$ad \quad bc \quad ac \quad bd$

Fact: the cross ratio is $R = AD^{\varepsilon_1} \cdot BC^{\varepsilon_2} \cdot AC^{\varepsilon_3} \cdot BD^{\varepsilon_4}$ for some signs $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4 \in \{1, -1\}$

$r = ad^{\varepsilon_1} \cdot bc^{\varepsilon_2} \cdot ac^{\varepsilon_3} \cdot bd^{\varepsilon_4}$

The key point is that $R = r$ for all choices of A, B, C, D, O, and line.

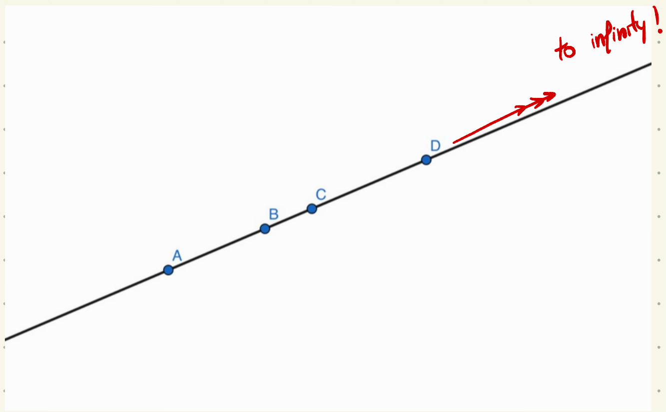
Your goal: figure out $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$ by using Geogebra. You may define AD literally using the algebra boxes (demonstrate)

(Resume video)

Pause at 6:24

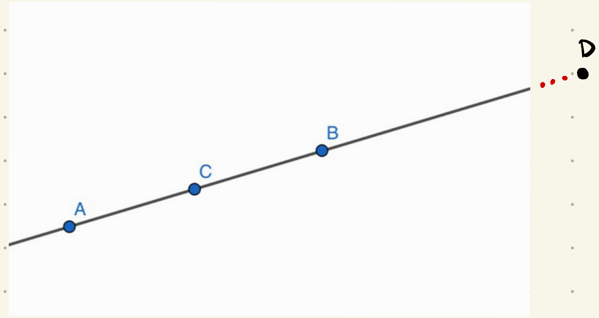
Exploring the cross-ratio when "$D \to \infty$"

Take 4 points on a line A, B, C, D and let R be their cross-ratio. Now slide D towards infinity:



1. Does R tend to a value? Can you express it in terms of A, B, C only?

2. What cross-ratio do you get if A, B, C are evenly spaced and in order A, C, B?



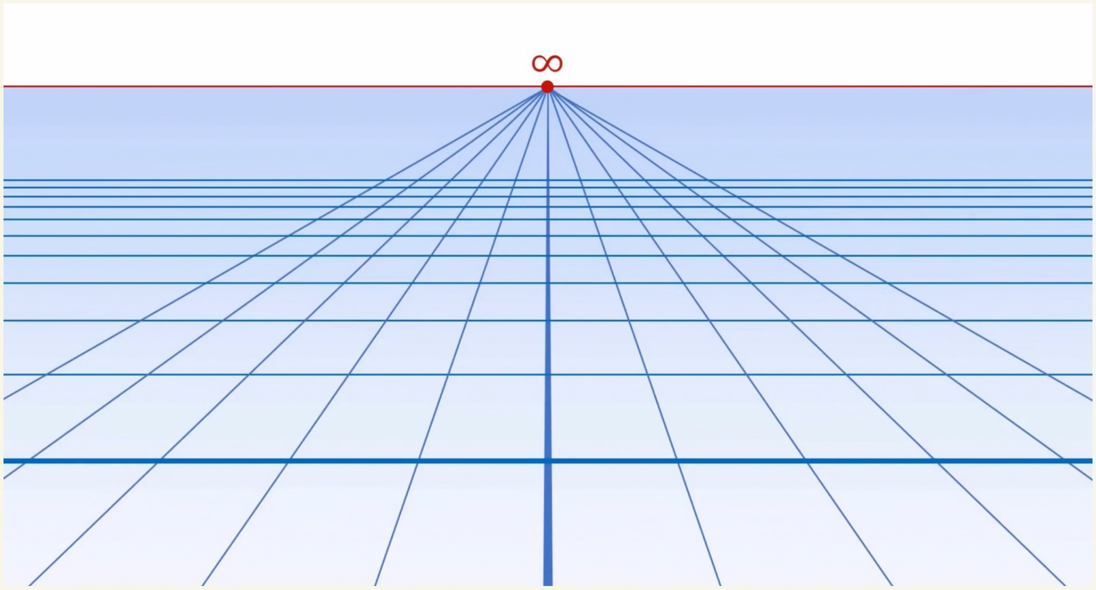
Take orientations into account! Geogebra won't do it for you!

(Resume video)

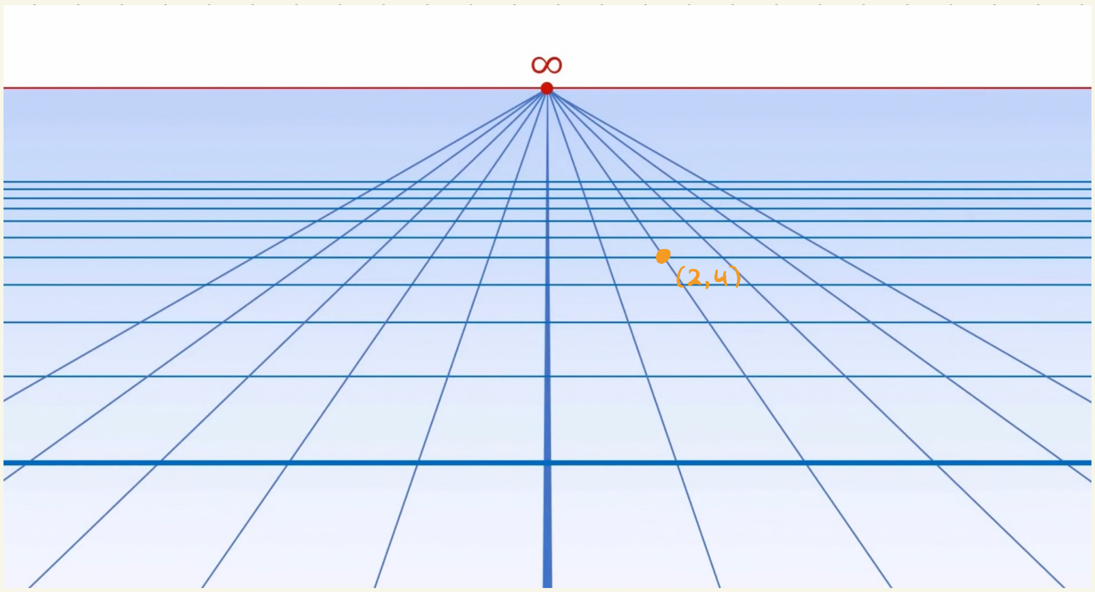
Pause at 9:10

Perspective drawing

Use the technique in the video to emulate the following picture:



Next, "plot" points on the parabola $y = x^2$. For instance, this would be the point $(2,4)$:



Try to guess what the whole plot would look like by plotting more and more points.

(Resume video)

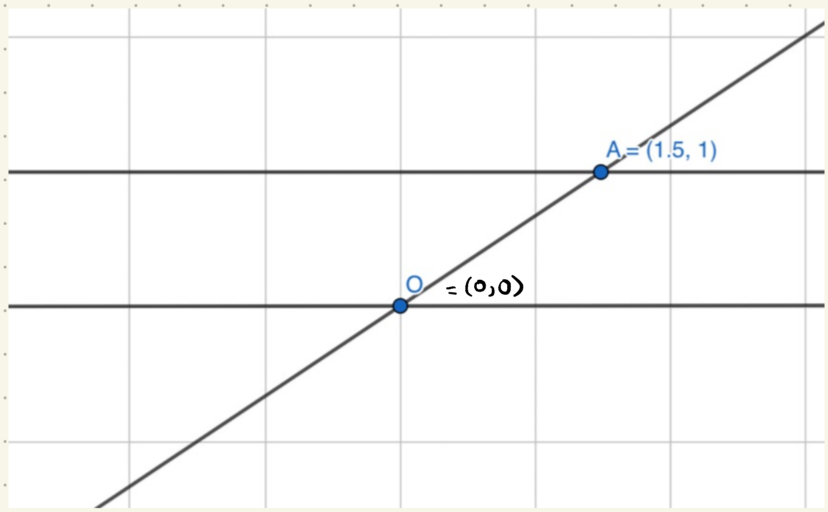
Pause at 10:15

Real projective line

We want to make sense of "the point at infinity":

∞ ... ——————————————— ... ∞

How to make this precise? Idea: Put the line in the plane at $y=1$, and associate to each point a line through O and A:



We have a correspondence $\{\text{points on the line}\} \longleftrightarrow \{\text{lines through } O\}$

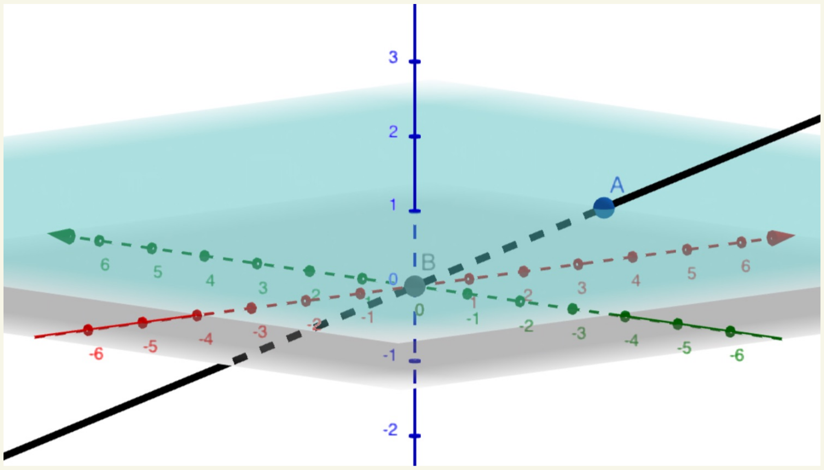
1. What line corresponds to ∞?
2. In our example, $A = (1.5, 1)$. Argue that $(3,2)$ gives the same line and therefore should be considered "the same" as $(1.5, 1)$.

(Resume video)

Pause at 11:37

Real projective plane

Repeat the discovery of the projective line with the projective plane: put a plane at $z=1$ and a point A on it, and associate to it the line through OA. Explore the points at infinity. What should the homogeneous coordinates look like?



(Resume video)

Pause at 15:13 (Old friend $\mathbb{P}^2$) (Resume)

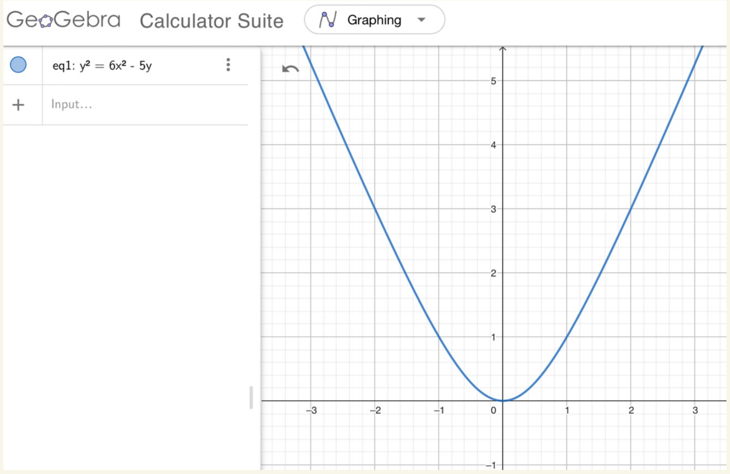
Pause at 16:50

Homogenizing equations

Take now the hyperbola $y^2 = 6x^2 - 5y$, and homogenize it to find its points at ∞.

1. What points do you get?

2. Where do those point lead to?



3. What about the circle $x^2+y^2=1$?

(Finish video)

Extra: Elliptic curves $y^2 = x^3 + ax + b$, Bézout $\rightsquigarrow$ define $+$ on it.

(known)

$x P = X$ (Explain why xP is easy)

private key   public key

Exercise:

1. Let E be the elliptic curve given by the affine equation

$$y^2 = x^3 + 5x^2 + 5x + 5$$

with the point at infinity $(0 : 1 : 0)$ as the zero element of the group law. Let $A = (-1, 2)$, $B = (1, 4)$. Calculate $A + B$, $A - B$ and $2A$ on E.