Définitions

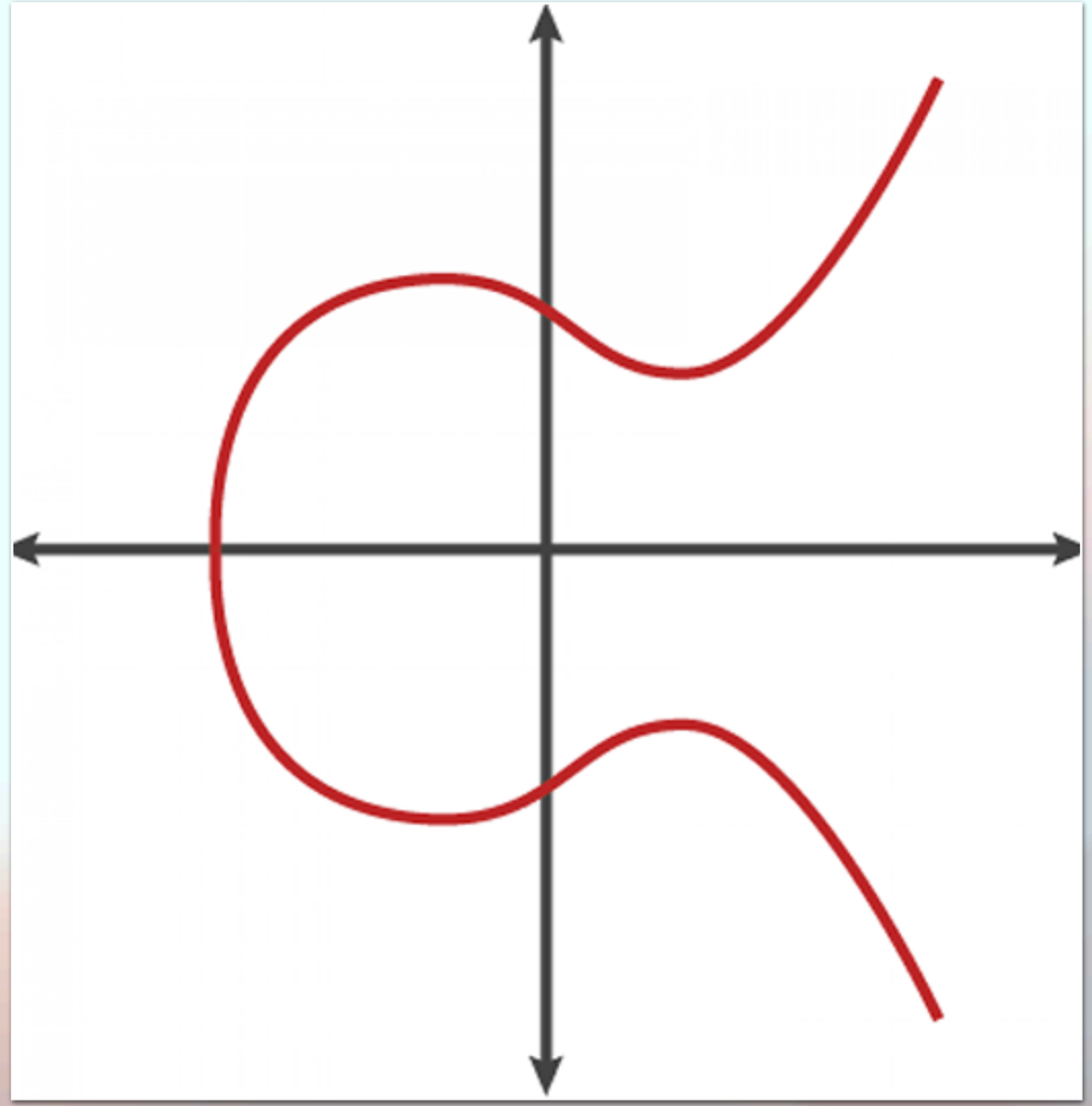
Courbe elliptique

Soient un corps $\mathbb{K}$, et des scalaires $a, b \in \mathbb{K}$, une **courbe elliptique** $\mathscr{C}$ est l'ensemble des points $(x, y) \in \mathbb{K}^2$ tels que:

$$y^2 = x^3 + ax + b$$

ainsi qu'un **point à l'infini** noté $\mathcal{O}$

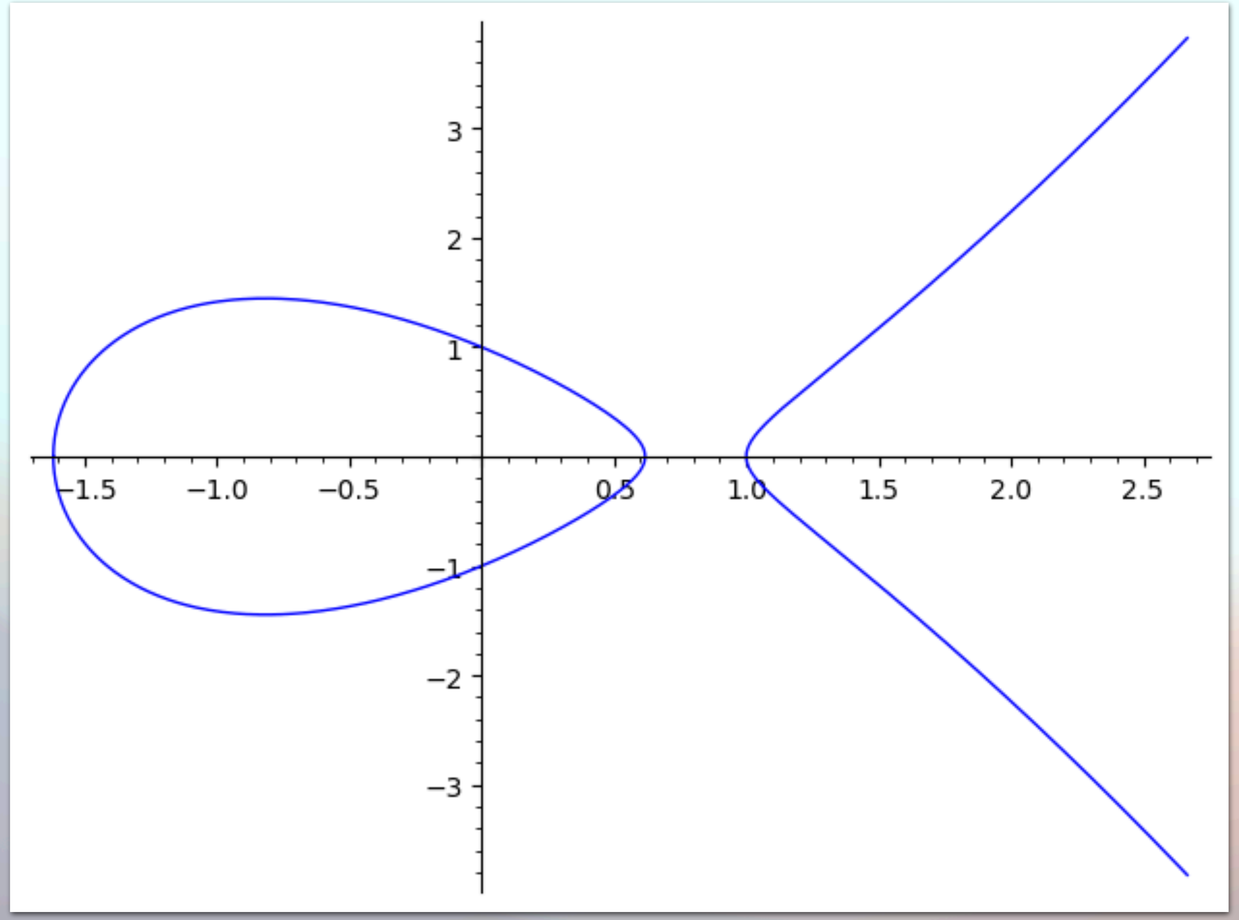
Notons que la courbe est symétrique par rapport à l'axe des abscisses



Courbes sur différents corps

Avec a = -2, b = 1**, on a la courbe** $y^2 = x^3 - 2x + 1$

Sur les réels $(\mathbb{K} = \mathbb{R})$



Sur un corps fini $(\mathbb{K} = \mathbb{F}_{61})$