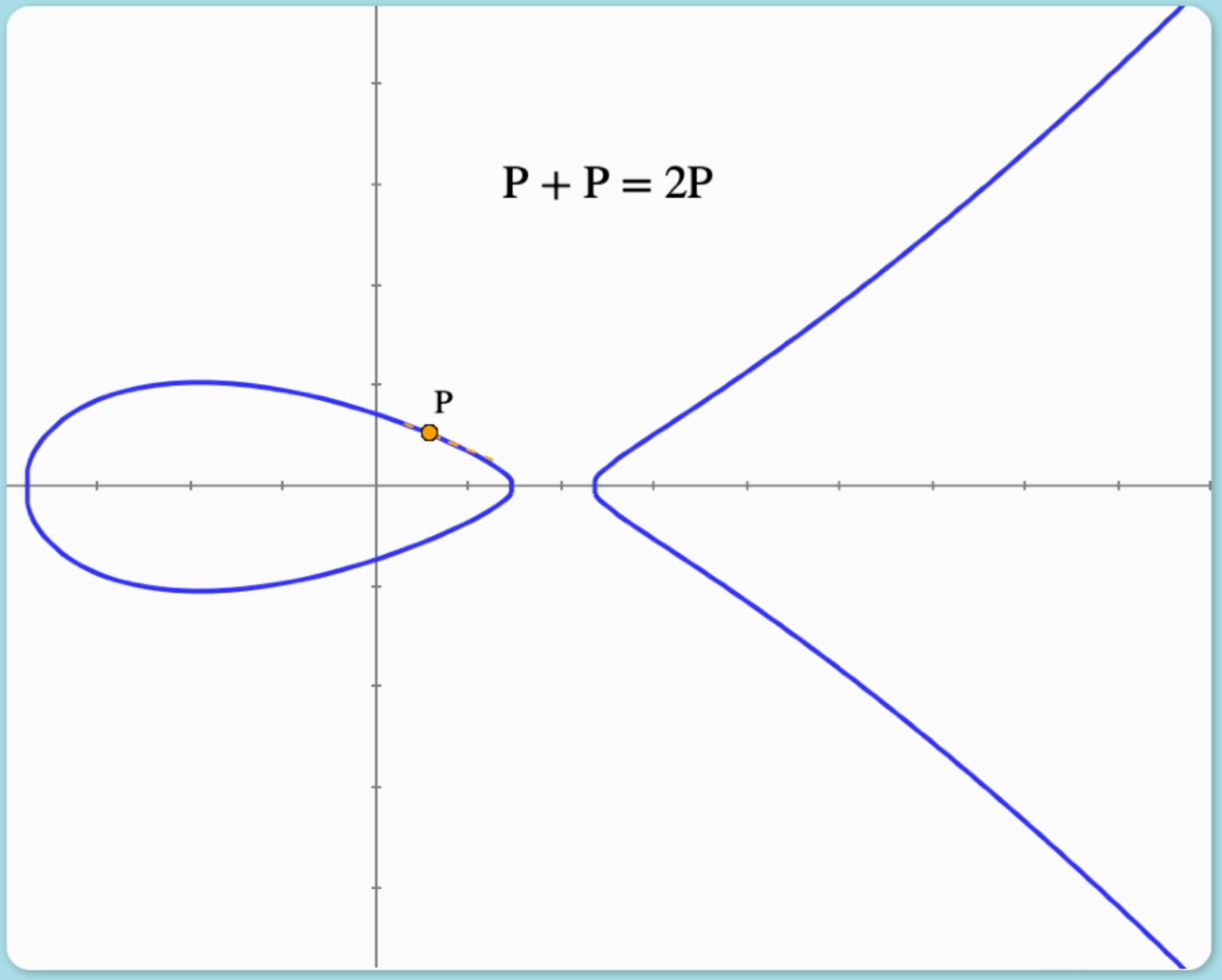
Noté $+ : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$

1. Tracer la ligne
    A. Tangente au point **ou**
    B. Passant par les deux points
2. Trouver où la ligne croise la courbe
3. Renverser le point verticalement

On en déduit la multiplication par un entier:

$$\mathbb{Z} \times \mathscr{C} \to \mathscr{C}$$

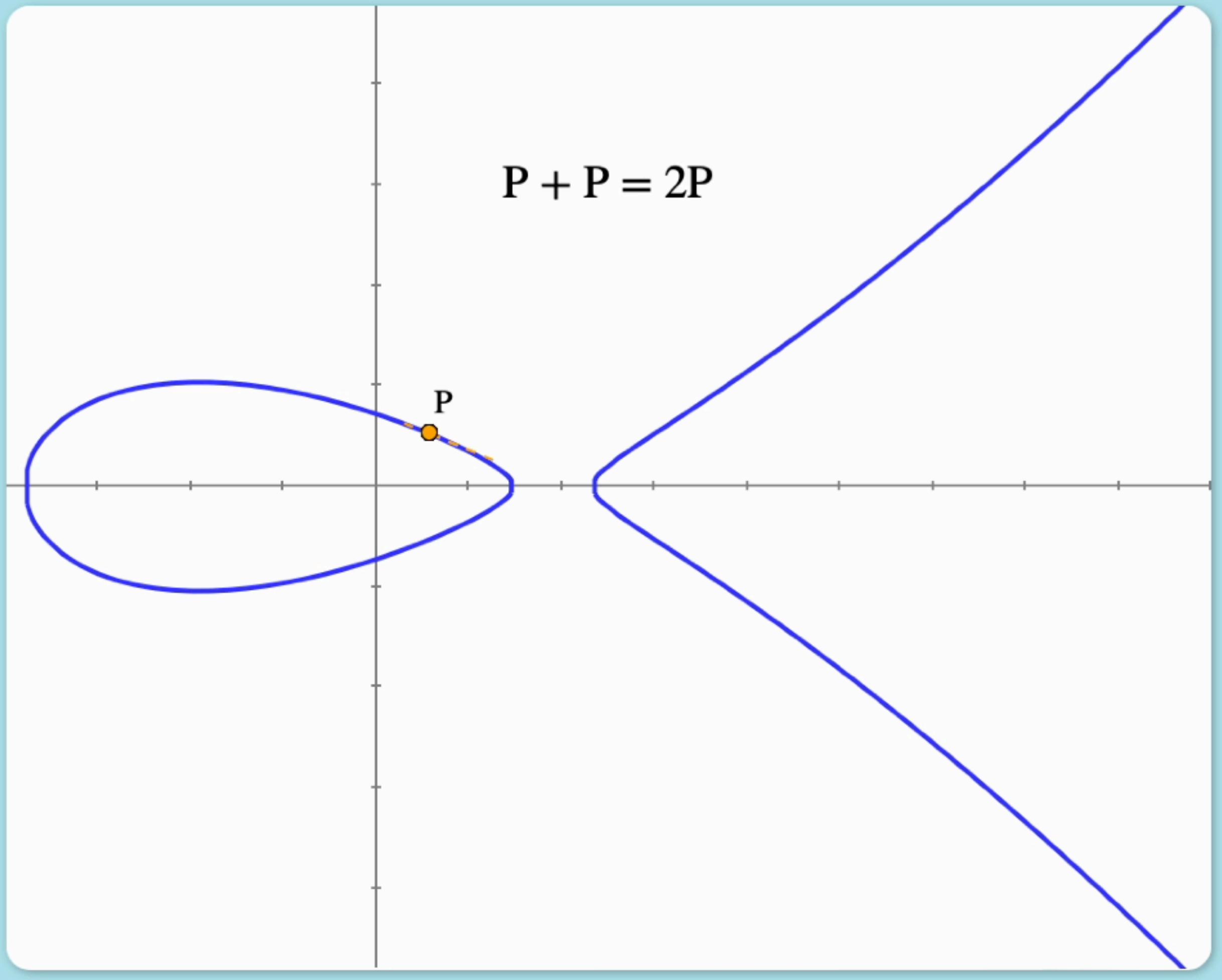
$$nP = \underbrace{P + P + \cdots + P}_{n \text{ fois}}$$



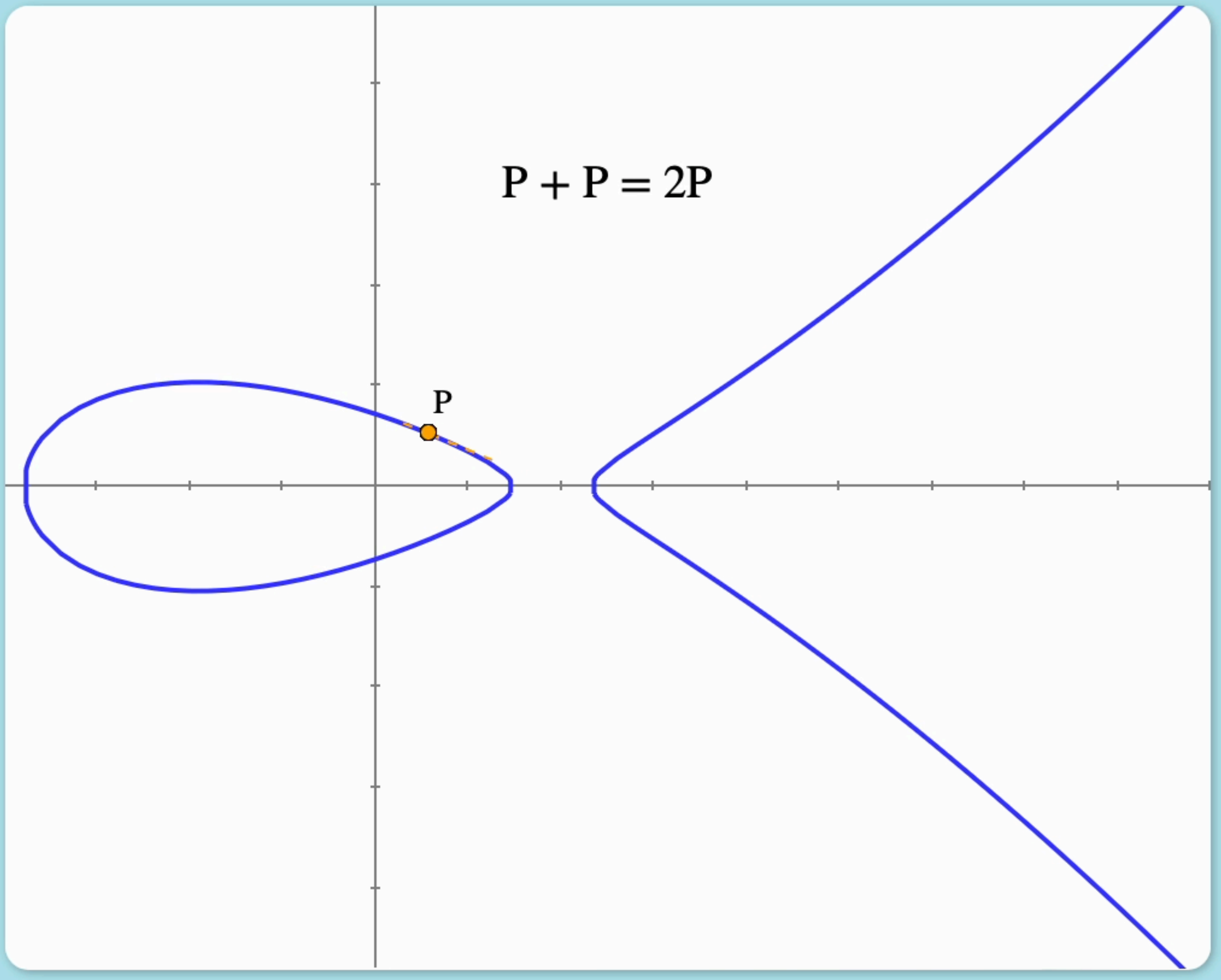
Repeated addition of a point P

Addition de points

5



Repeated addition of a point P



Repeated addition of a point P

Addition de points

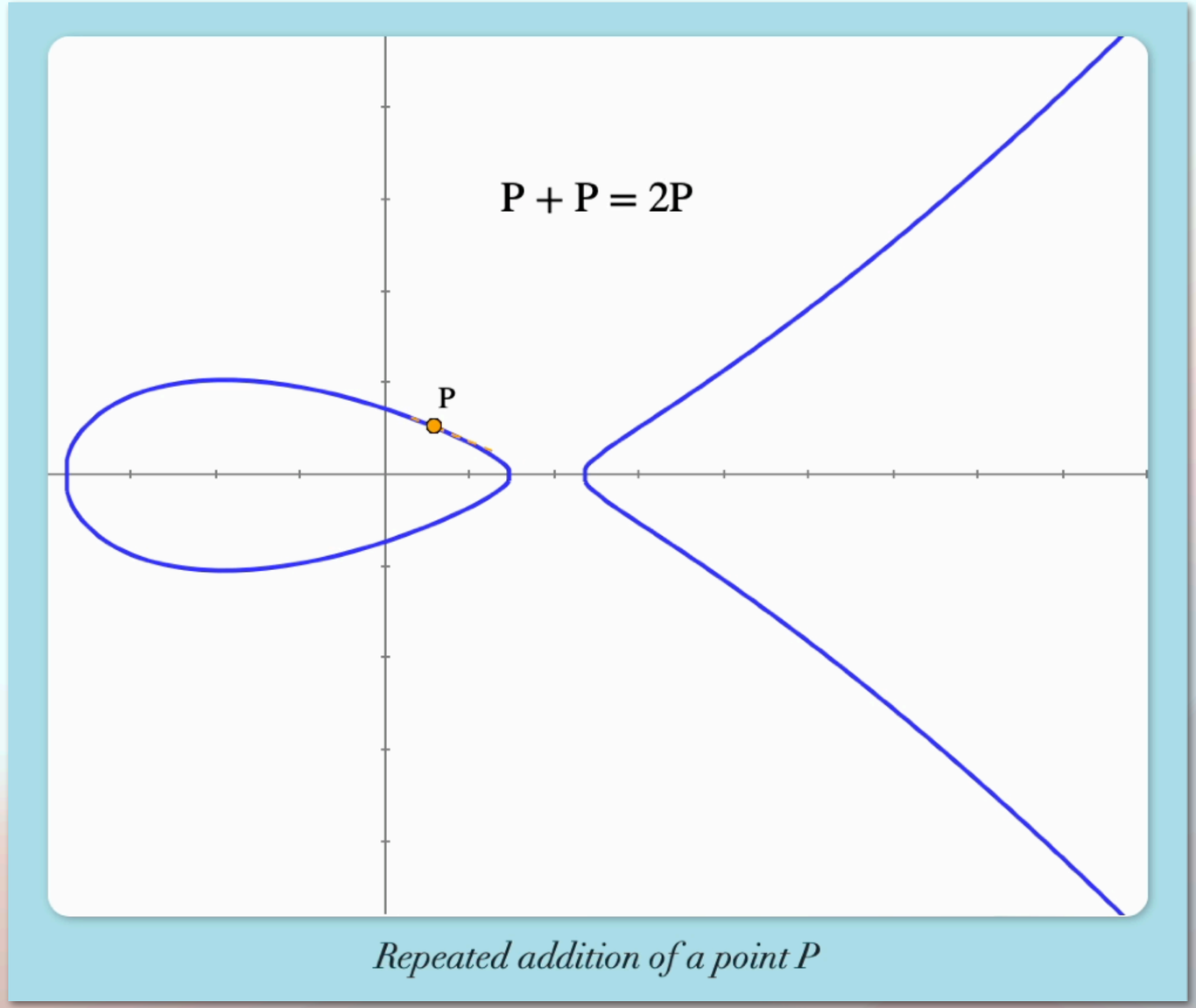
Noté $+ : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$

1. Tracer la ligne
    A. Tangente au point **ou**
    B. Passant par les deux points
2. Trouver où la ligne croise la courbe
3. Renverser le point verticalement

On en déduit la multiplication par un entier:

$$\mathbb{Z} \times \mathscr{C} \to \mathscr{C}$$

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ fois}}$$



Repeated addition of a point P

Structure de groupe

$(\mathscr{C}, +)$ a les propriétés suivantes

- Fermeture $\forall P, Q \in \mathscr{C}$

  $$P + Q \in \mathscr{C}$$

- Associativité $\forall P, Q, R \in \mathscr{C}$

  $$(P + Q) + R = P + (Q + R)$$

- Identité $\forall P \in \mathscr{C}$

  $$\mathcal{O} + P = P = P + \mathcal{O}$$

- Inverse $\forall P \in \mathscr{C}, \exists Q \in \mathscr{C}$

  $$P + Q = \mathcal{O}$$