Quelques liens entre géométrie algébrique et codage

Hugues Randriam

Journée LTCI
2018-10-11

Géométrie algébrique

C'est l'étude des objets géométriques (courbes, surfaces...) qui peuvent être définis de façon algébrique (par des polynômes).

Historique succint

- Apollonius (III^{e} s. AEC) : *Traité des sections coniques*
- Omar Khayyam (1070) : résolution des équations de degré 3 par intersection de coniques
- Descartes (1637) : *La Géométrie* (analytique/algébrique)
- Newton (fin XVII^{e} s.) : classification (presque complète) des cubiques planes réelles
- ...

Historique succint

- Apollonius (III^{e} s. AEC) : *Traité des sections coniques*
- Omar Khayyam (1070) : résolution des équations de degré 3 par intersection de coniques
- Descartes (1637) : *La Géométrie* (analytique/algébrique)
- Newton (fin XVII^{e} s.) : classification (presque complète) des cubiques planes réelles
- ...
- XIX^{e} s., première moitié XX^{e} s. : écoles allemande, italienne, américaine

Historique succint

- Apollonius (III^{e} s. AEC) : *Traité des sections coniques*
- Omar Khayyam (1070) : résolution des équations de degré 3 par intersection de coniques
- Descartes (1637) : *La Géométrie* (analytique/algébrique)
- Newton (fin XVII^{e} s.) : classification (presque complète) des cubiques planes réelles
- ...
- XIX^{e} s., première moitié XX^{e} s. : écoles allemande, italienne, américaine
- seconde moitié XX^{e} s. : école française (Grothendieck, Serre) $\rightarrow$ schémas, faisceaux, cohomologie...

On peut travailler sur $\mathbb{C}$ (le plus simple en général), sur $\mathbb{R}$, sur un corps fini $\mathbb{F}_q$ (pour les applications codage/crypto), ou sur $\mathbb{Q}$, $\mathbb{Z}$ (problèmes diophantiens).

Il est naturel aussi de se placer dans le cadre de la géométrie projective (Pappus, Desargues...), en ajoutant des points à l'infini.
Ex. : théorème de Bézout, dans le plan, deux courbes définies par des polynômes de degré m et n ont mn points d'intersection.

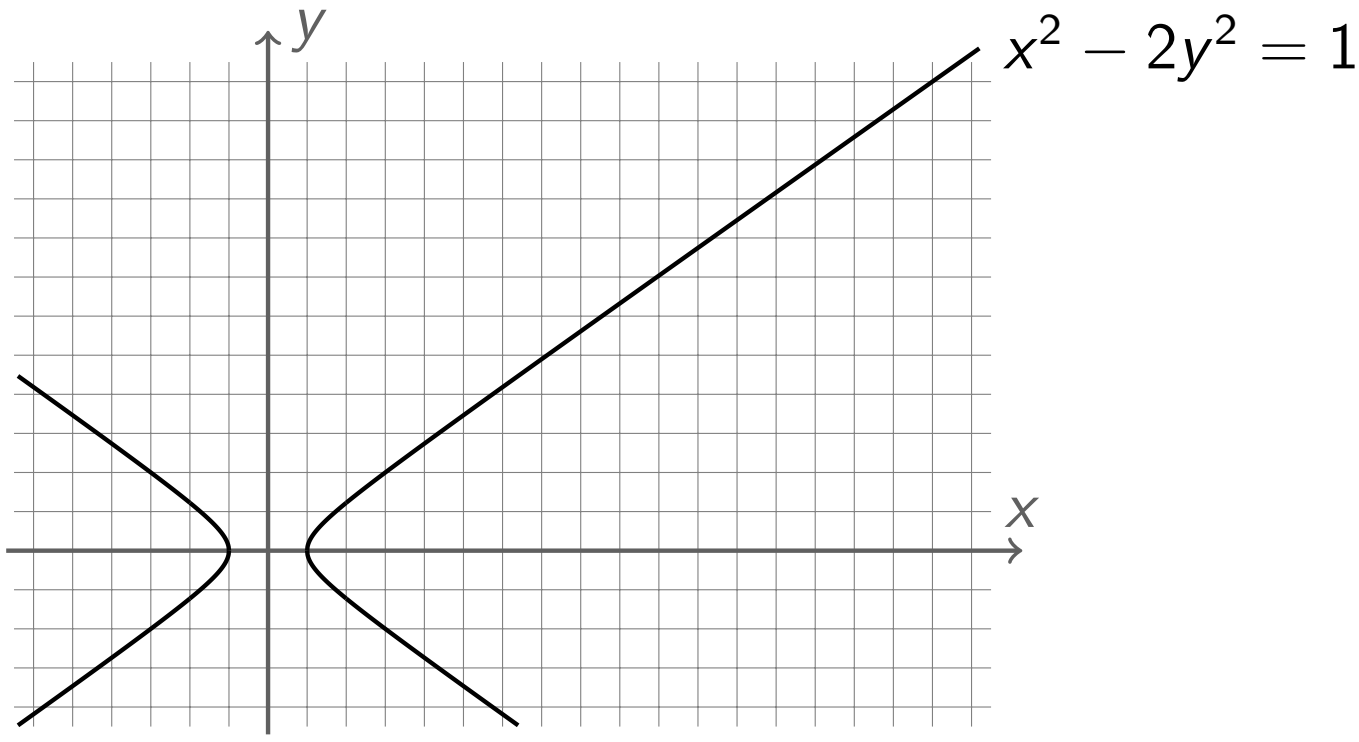
Ici on va motiver notre approche par les équations diophantiennes.
Déjà en dimension 1 (courbes) la théorie est très riche.

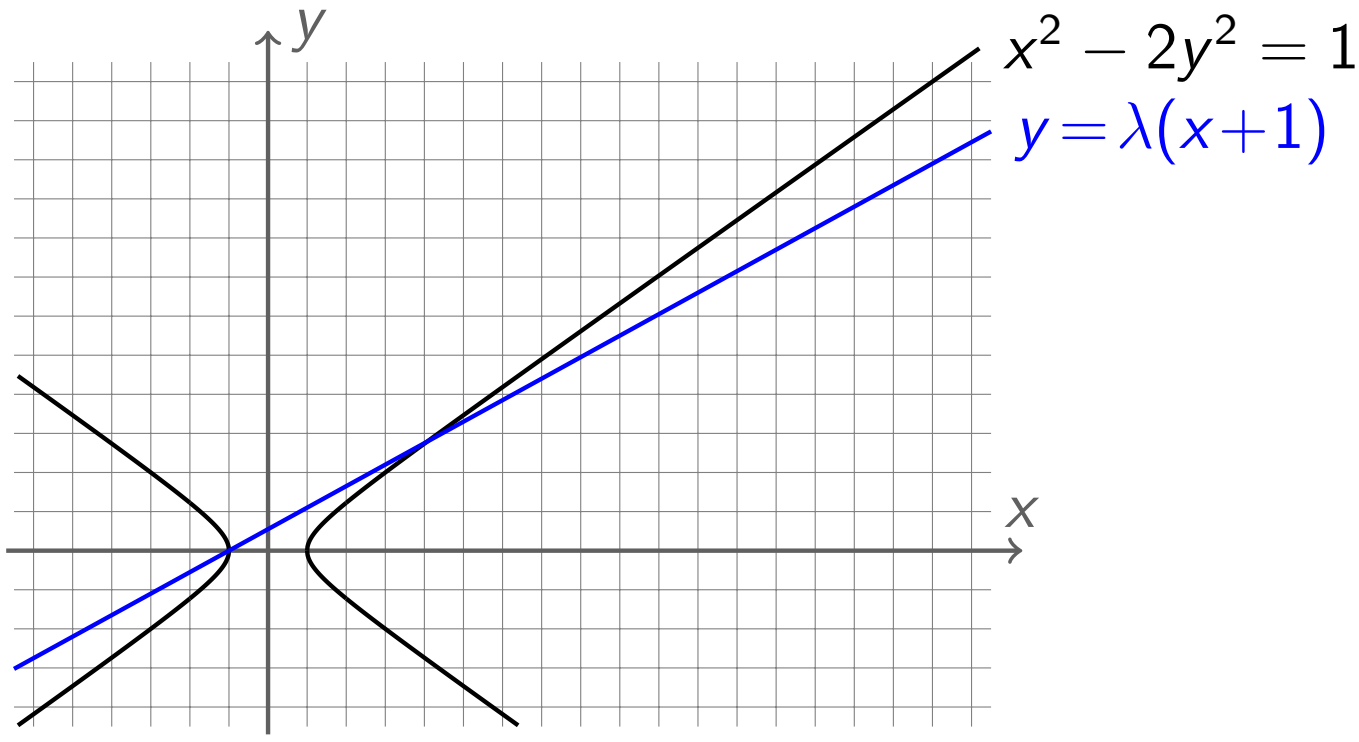
Slogan : “la géométrie gouverne l’arithmétique”.

Genre 0

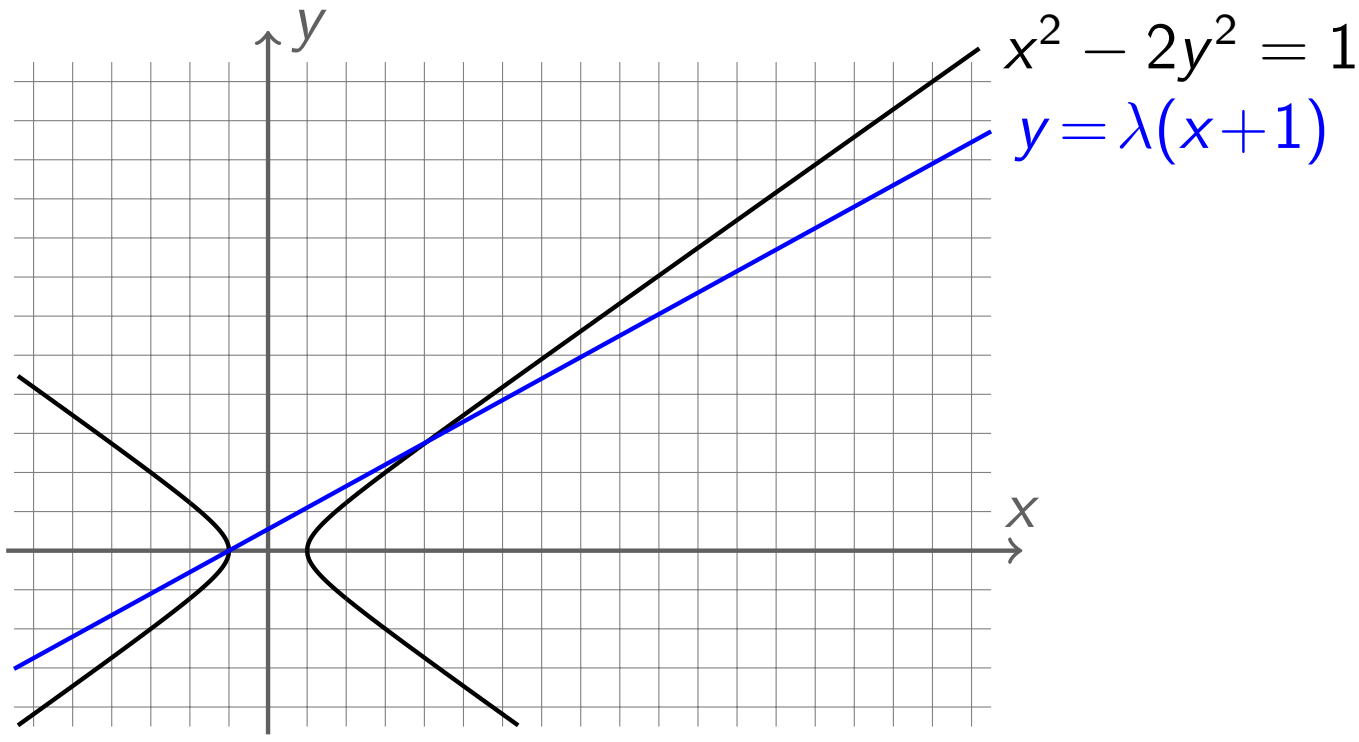
Pell-Fermat : trouver les solutions (entières) de

$$x^2 - Ny^2 = c.$$

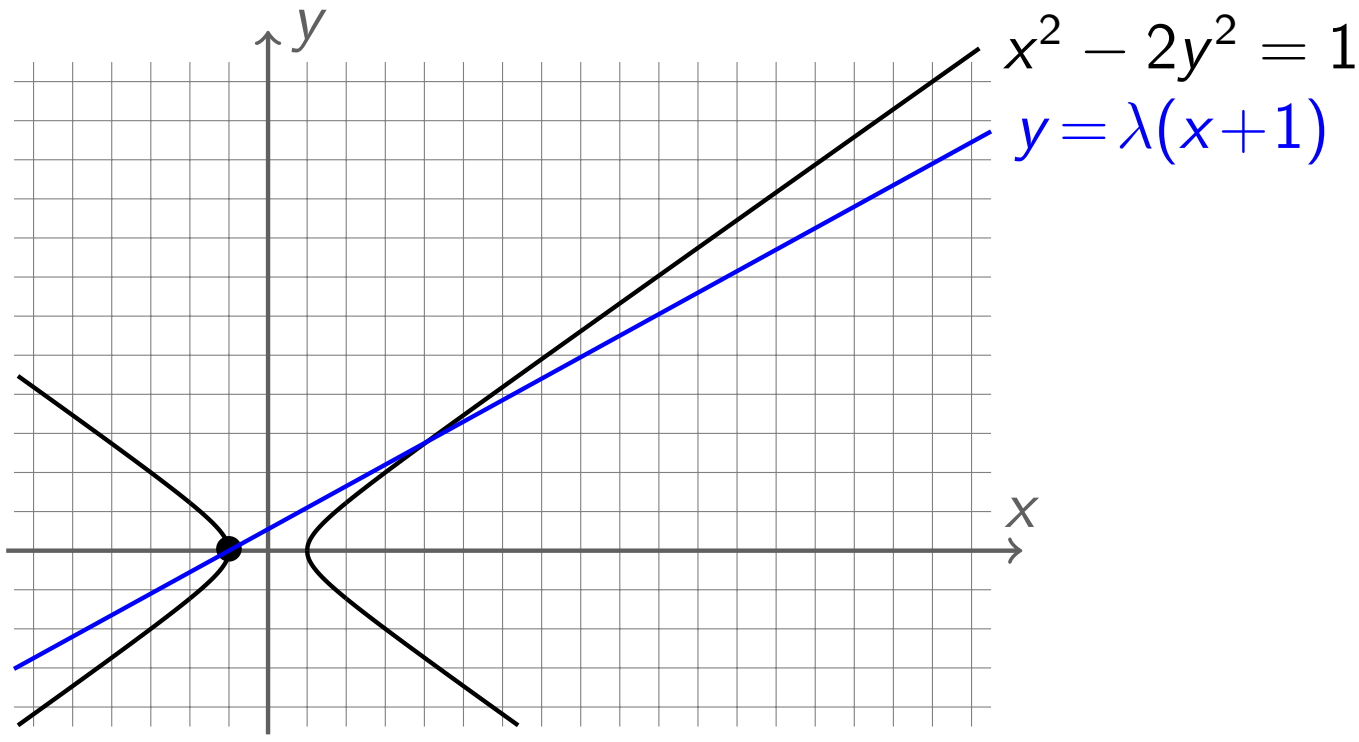

y
x
$x^2 - 2y^2 = 1$



Paramétrisation : on intersecte avec la droite $y = \lambda(x + 1)$

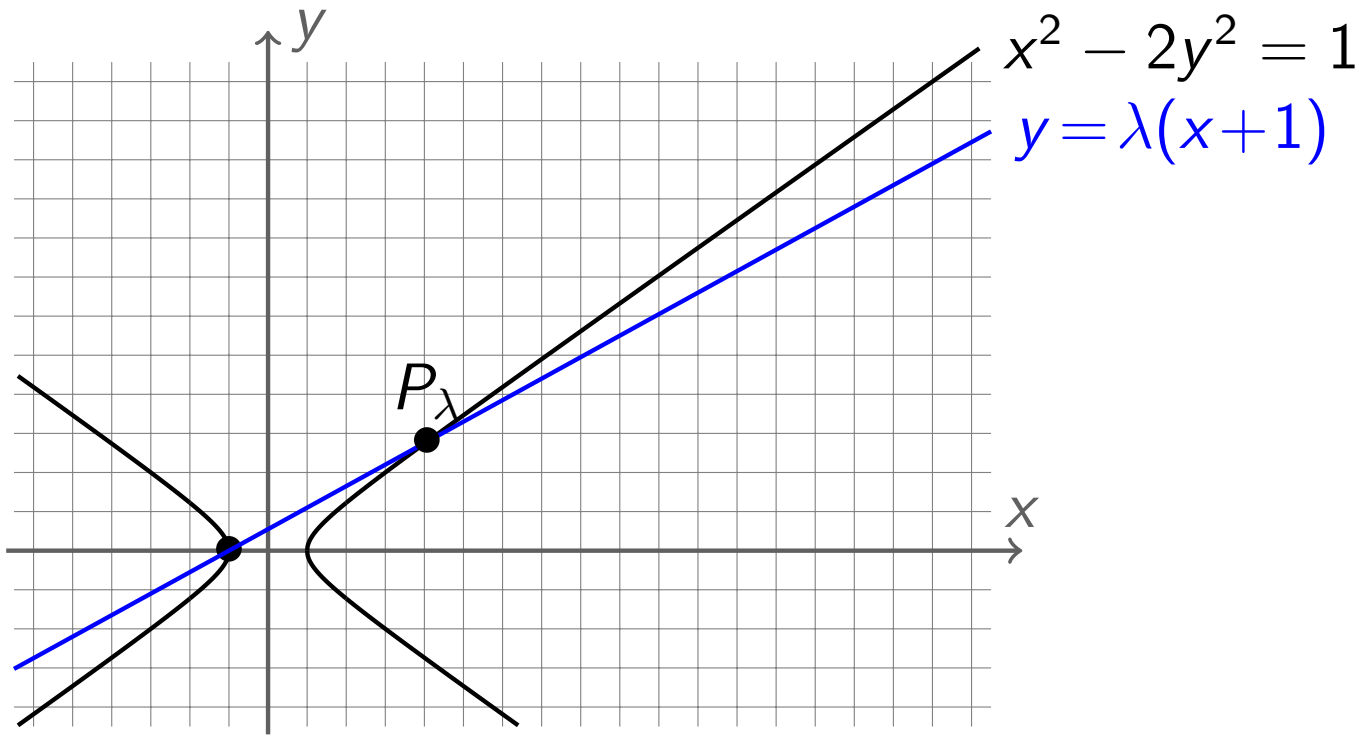


Paramétrisation : on intersecte avec la droite $y = \lambda(x+1)$
$\rightarrow x^2 - 2\lambda^2(x+1)^2 = 1,$



Paramétrisation : on intersecte avec la droite $y = \lambda(x+1)$

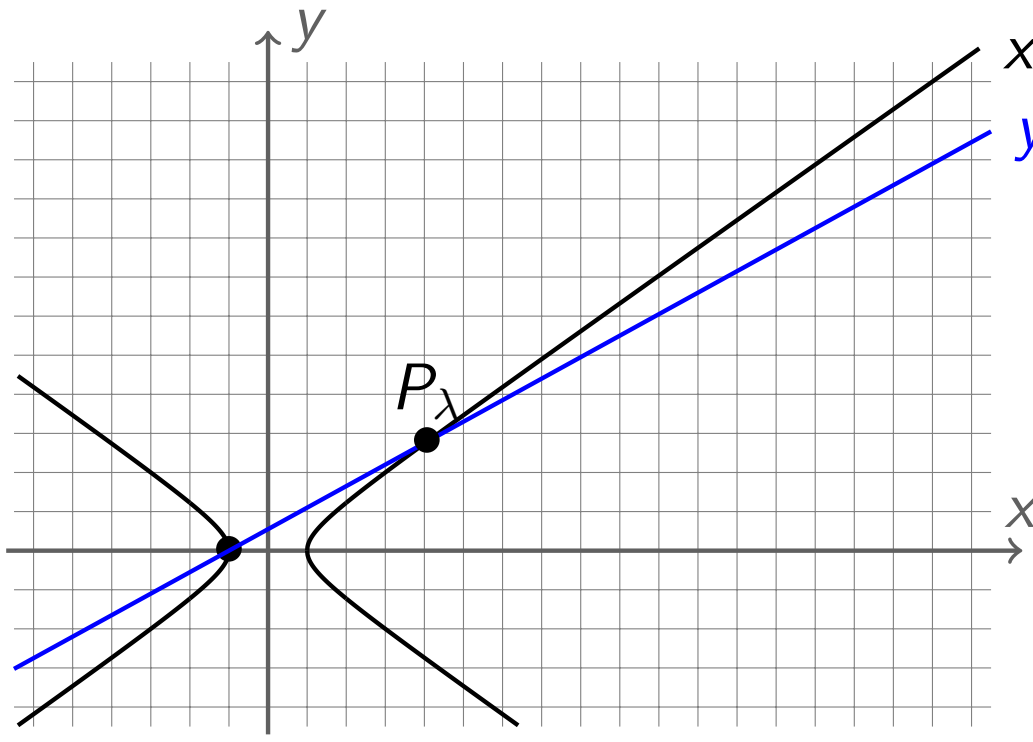
$\rightarrow x^2 - 2\lambda^2(x+1)^2 = 1$, i.e. $(x+1)((x-1) - 2\lambda^2(x+1)) = 0$



Paramétrisation : on intersecte avec la droite $y = \lambda(x+1)$

$\rightarrow x^2 - 2\lambda^2(x+1)^2 = 1$, i.e. $(x+1)((x-1) - 2\lambda^2(x+1)) = 0$

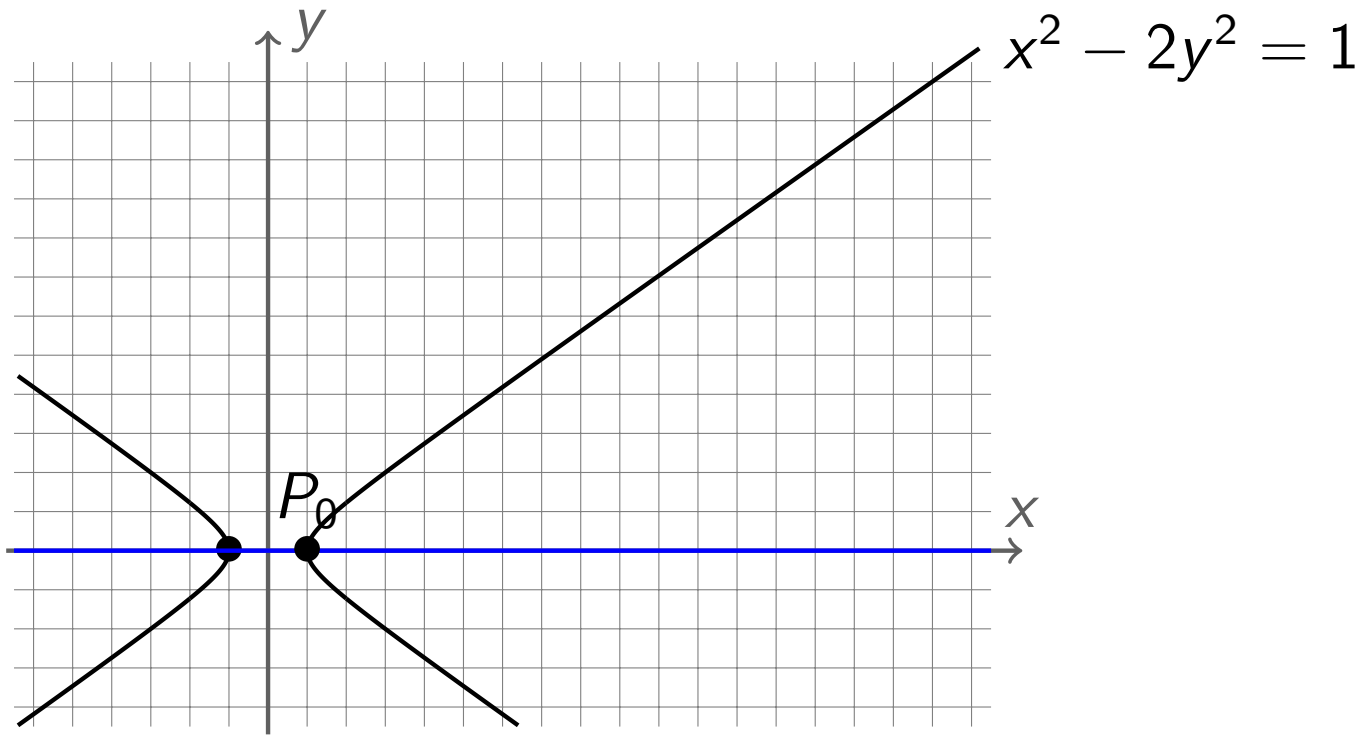
$\rightarrow P_\lambda = \begin{vmatrix} x_\lambda \\ y_\lambda \end{vmatrix}$ où $\quad x_\lambda = \frac{1+2\lambda^2}{1-2\lambda^2}$



Paramétrisation : on intersecte avec la droite $y = \lambda(x+1)$

$\rightarrow x^2 - 2\lambda^2(x+1)^2 = 1$, i.e. $(x+1)((x-1) - 2\lambda^2(x+1)) = 0$

$\rightarrow P_\lambda = \begin{vmatrix} x_\lambda \\ y_\lambda \end{vmatrix}$ où $x_\lambda = \frac{1+2\lambda^2}{1-2\lambda^2}$ et $y_\lambda = \frac{2\lambda}{1-2\lambda^2}$

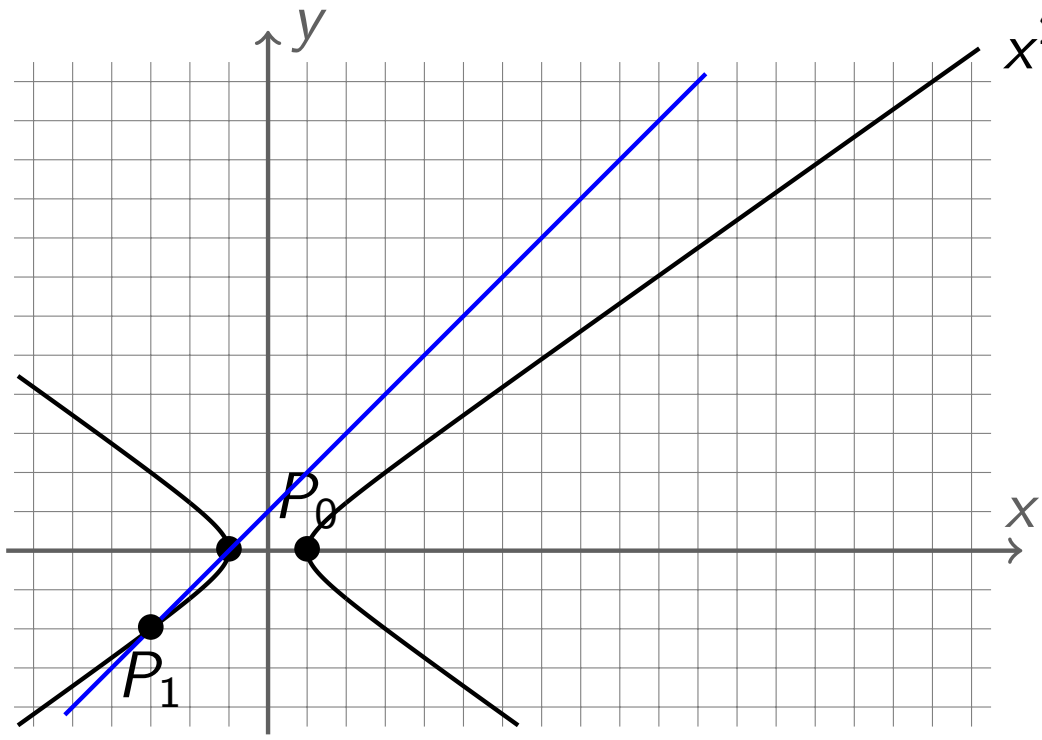


Paramétrisation : on intersecte avec la droite $y = \lambda(x+1)$

$\rightarrow x^2 - 2\lambda^2(x+1)^2 = 1$, i.e. $(x+1)((x-1) - 2\lambda^2(x+1)) = 0$

$\rightarrow P_\lambda = \begin{vmatrix} x_\lambda \\ y_\lambda \end{vmatrix}$ où $x_\lambda = \frac{1+2\lambda^2}{1-2\lambda^2}$ et $y_\lambda = \frac{2\lambda}{1-2\lambda^2}$

ex. : $P_0 = \begin{vmatrix} 1 \\ 0 \end{vmatrix}$

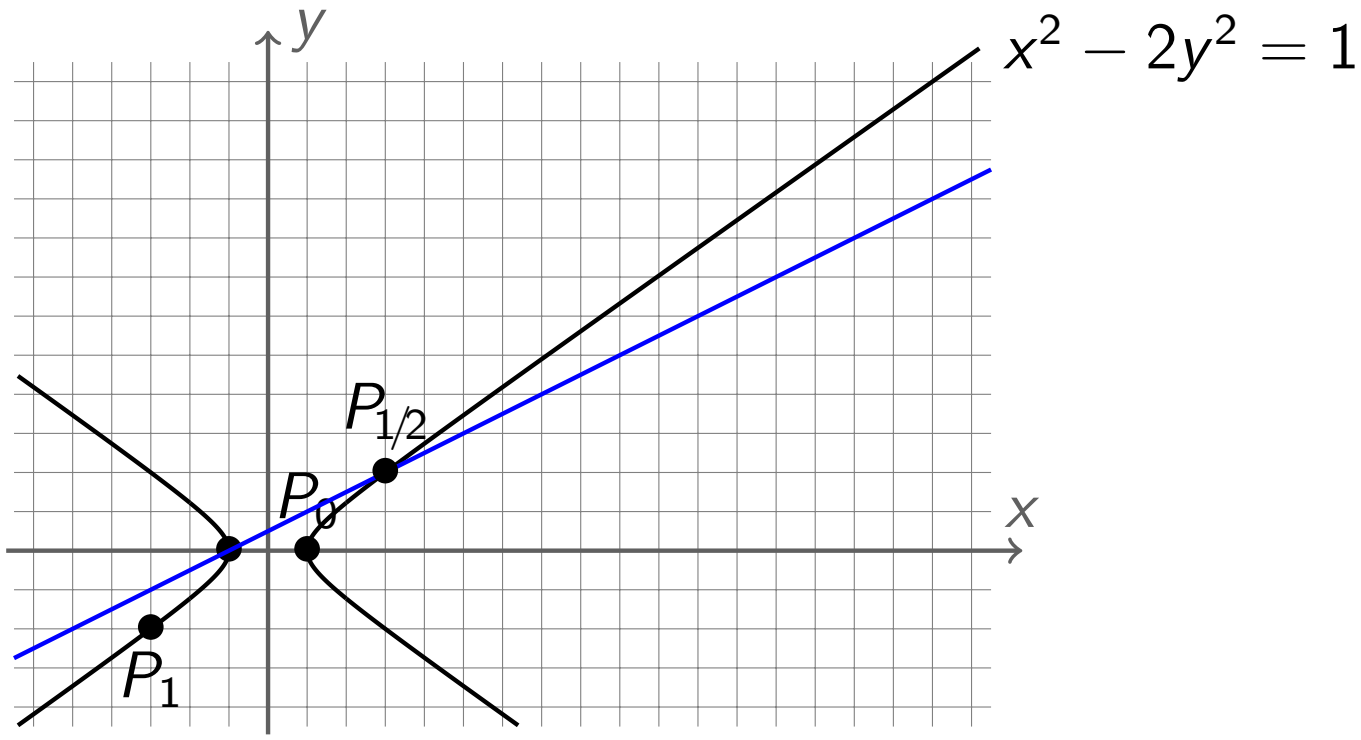


Paramétrisation : on intersecte avec la droite $y = \lambda(x+1)$

$\rightarrow x^2 - 2\lambda^2(x+1)^2 = 1$, i.e. $(x+1)((x-1) - 2\lambda^2(x+1)) = 0$

$\rightarrow P_\lambda = \begin{vmatrix} x_\lambda \\ y_\lambda \end{vmatrix}$ où $x_\lambda = \frac{1+2\lambda^2}{1-2\lambda^2}$ et $y_\lambda = \frac{2\lambda}{1-2\lambda^2}$

ex. : $P_0 = \begin{vmatrix} 1 \\ 0 \end{vmatrix}$ $P_1 = \begin{vmatrix} -3 \\ -2 \end{vmatrix}$

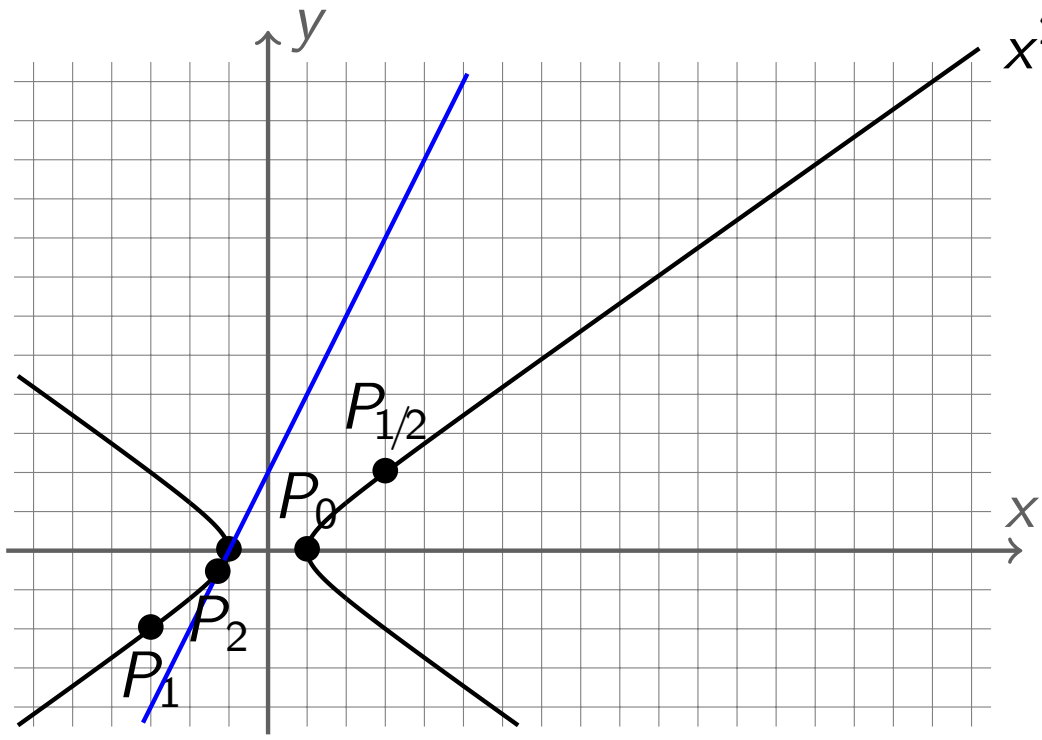


Paramétrisation : on intersecte avec la droite $y = \lambda(x+1)$

$\rightarrow x^2 - 2\lambda^2(x+1)^2 = 1$, i.e. $(x+1)((x-1) - 2\lambda^2(x+1)) = 0$

$\rightarrow P_\lambda = \begin{vmatrix} x_\lambda \\ y_\lambda \end{vmatrix}$ où $x_\lambda = \frac{1+2\lambda^2}{1-2\lambda^2}$ et $y_\lambda = \frac{2\lambda}{1-2\lambda^2}$

ex. : $P_0 = \begin{vmatrix} 1 \\ 0 \end{vmatrix}$ $P_1 = \begin{vmatrix} -3 \\ -2 \end{vmatrix}$ $P_{1/2} = \begin{vmatrix} 3 \\ 2 \end{vmatrix}$

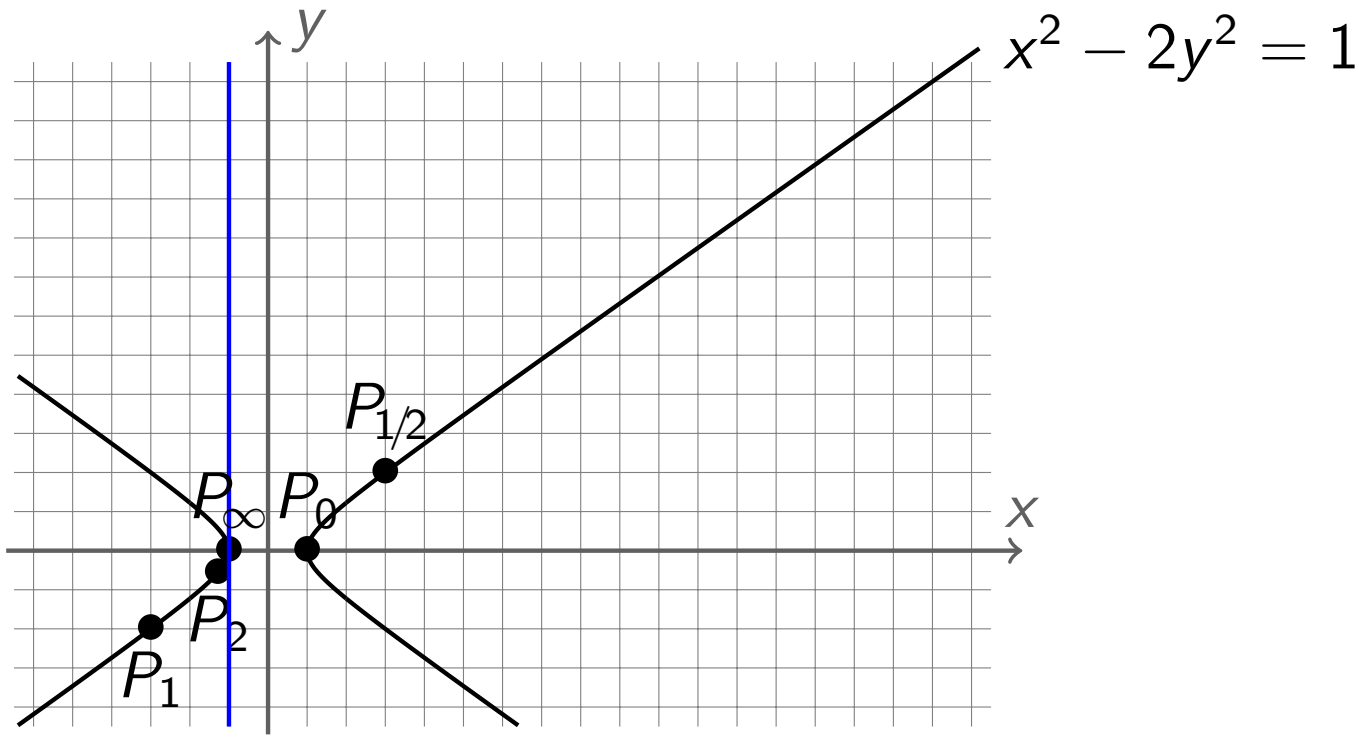


Paramétrisation : on intersecte avec la droite $y = \lambda(x+1)$

$\rightarrow x^2 - 2\lambda^2(x+1)^2 = 1$, i.e. $(x+1)((x-1) - 2\lambda^2(x+1)) = 0$

$\rightarrow P_\lambda = \begin{vmatrix} x_\lambda \\ y_\lambda \end{vmatrix}$ où $x_\lambda = \frac{1+2\lambda^2}{1-2\lambda^2}$ et $y_\lambda = \frac{2\lambda}{1-2\lambda^2}$

ex. : $P_0 = \begin{vmatrix} 1 \\ 0 \end{vmatrix}$ $P_1 = \begin{vmatrix} -3 \\ -2 \end{vmatrix}$ $P_{1/2} = \begin{vmatrix} 3 \\ 2 \end{vmatrix}$ $P_2 = \begin{vmatrix} -9/7 \\ -4/7 \end{vmatrix}$

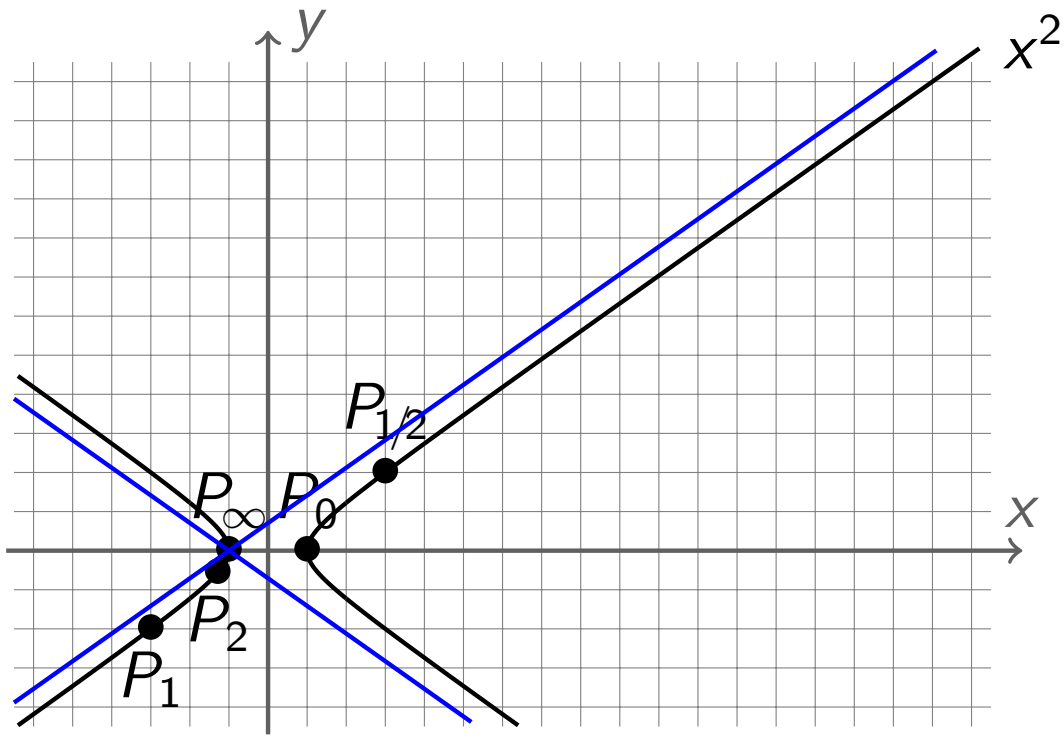


Paramétrisation : on intersecte avec la droite $y = \lambda(x+1)$

$\to x^2 - 2\lambda^2(x+1)^2 = 1$, i.e. $(x+1)((x-1) - 2\lambda^2(x+1)) = 0$

$\to P_\lambda = \begin{vmatrix} x_\lambda \\ y_\lambda \end{vmatrix}$ où $x_\lambda = \frac{1+2\lambda^2}{1-2\lambda^2}$ et $y_\lambda = \frac{2\lambda}{1-2\lambda^2}$

ex. : $P_\infty = \begin{vmatrix} -1 \\ 0 \end{vmatrix}$

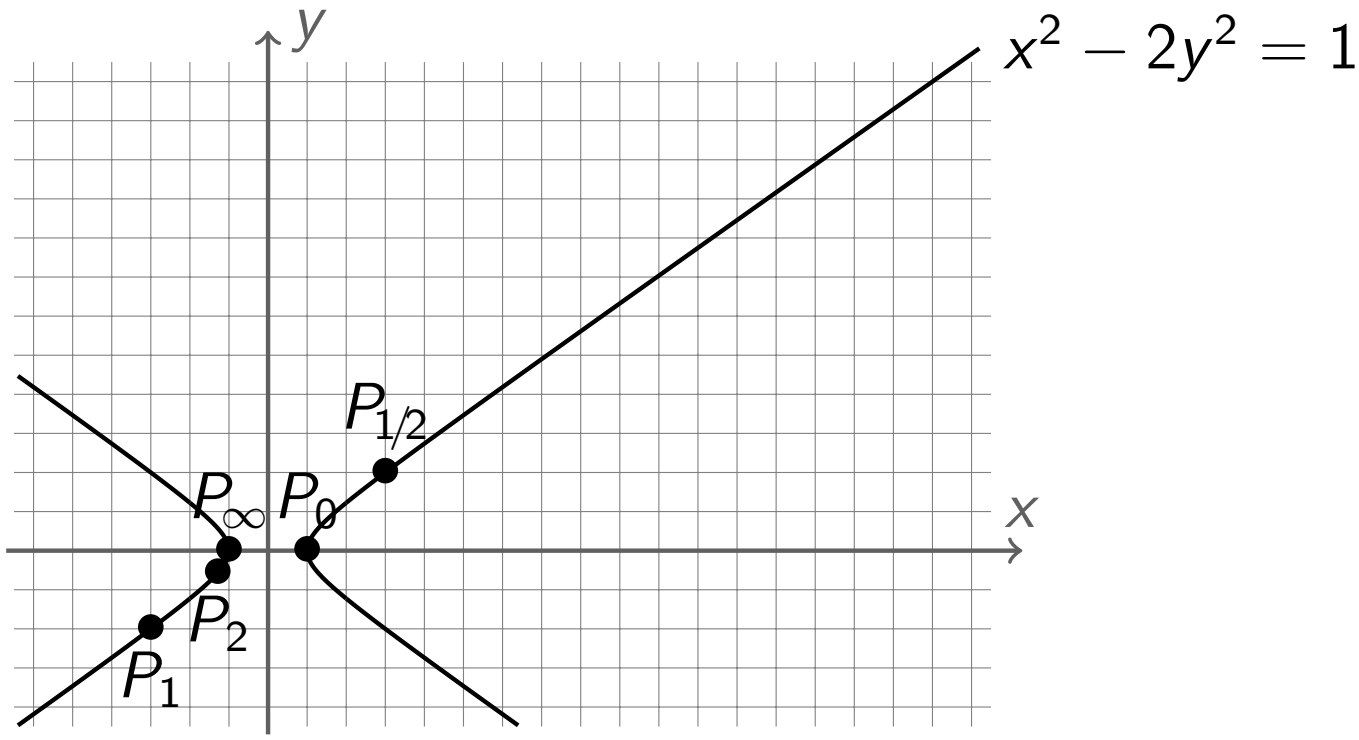


Paramétrisation : on intersecte avec la droite $y = \lambda(x+1)$

$\to x^2 - 2\lambda^2(x+1)^2 = 1$, i.e. $(x+1)((x-1) - 2\lambda^2(x+1)) = 0$

$\to P_\lambda = \begin{vmatrix} x_\lambda \\ y_\lambda \end{vmatrix}$ où $x_\lambda = \frac{1+2\lambda^2}{1-2\lambda^2}$ et $y_\lambda = \frac{2\lambda}{1-2\lambda^2}$

ex. : $P_\infty = \begin{vmatrix} -1 \\ 0 \end{vmatrix}$ $P_{\sqrt{2}/2}, P_{-\sqrt{2}/2}$ à l'infini.

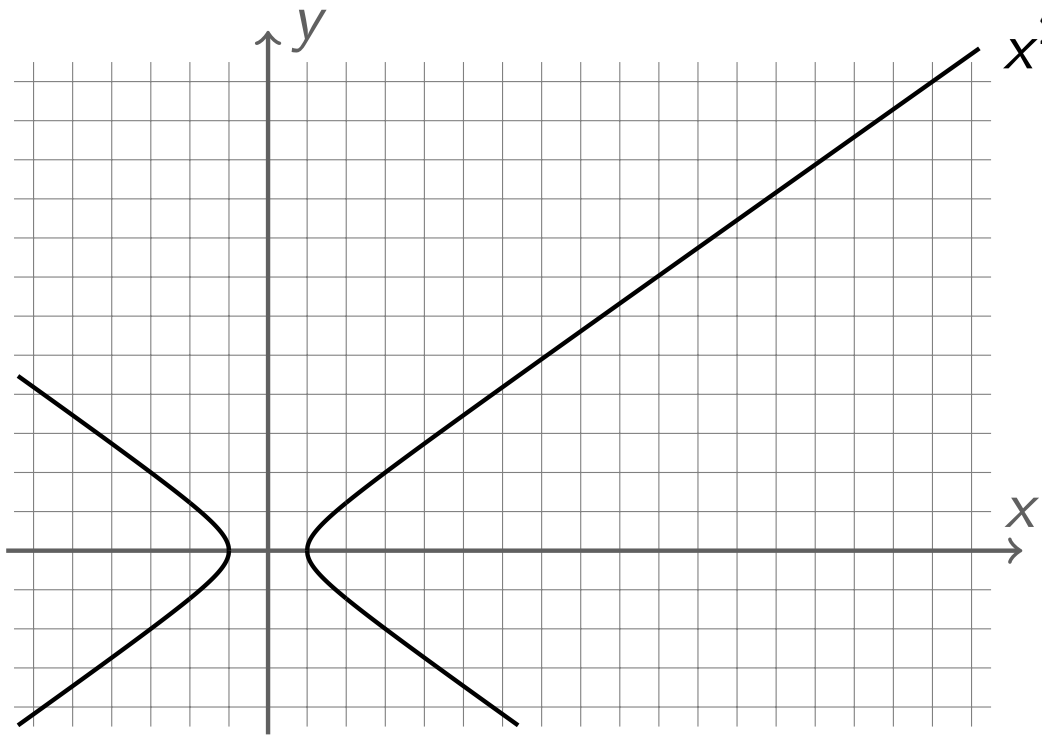


Paramétrisation : on intersecte avec la droite $y = \lambda(x+1)$

$\to x^2 - 2\lambda^2(x+1)^2 = 1$, i.e. $(x+1)((x-1) - 2\lambda^2(x+1)) = 0$

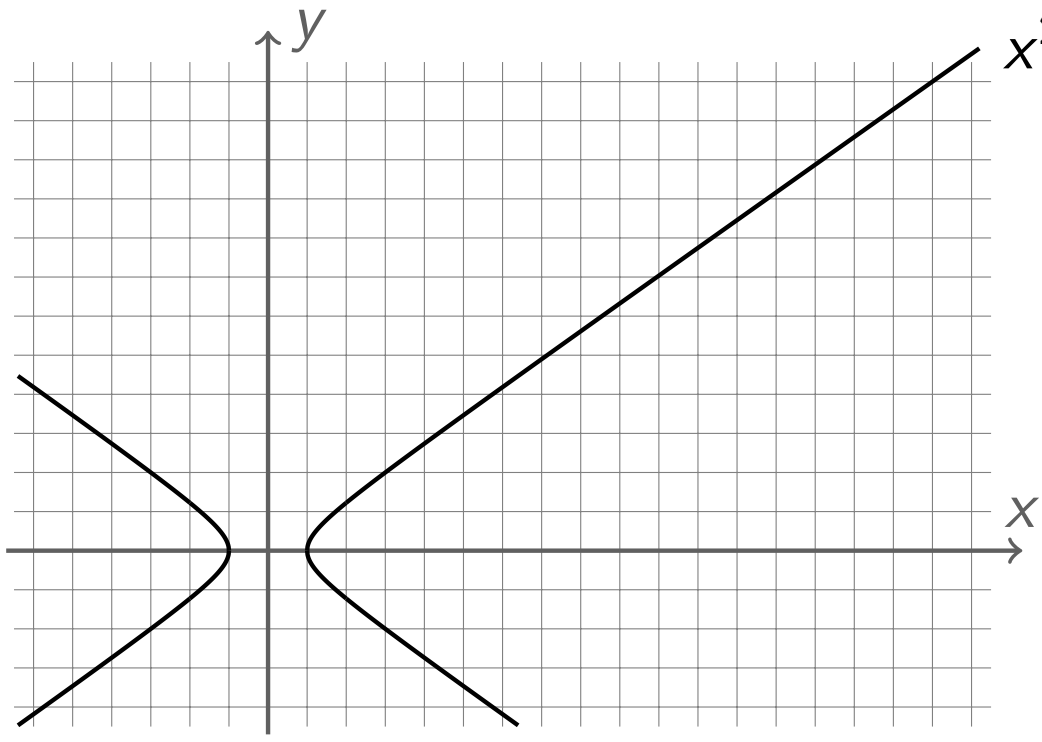
$\to P_\lambda = \begin{vmatrix} x_\lambda \\ y_\lambda \end{vmatrix}$ où $x_\lambda = \frac{1+2\lambda^2}{1-2\lambda^2}$ et $y_\lambda = \frac{2\lambda}{1-2\lambda^2}$

ex. : $P_0 = \begin{vmatrix} 1 \\ 0 \end{vmatrix}$ $P_1 = \begin{vmatrix} -3 \\ -2 \end{vmatrix}$ $P_{1/2} = \begin{vmatrix} 3 \\ 2 \end{vmatrix}$ $P_2 = \begin{vmatrix} -9/7 \\ -4/7 \end{vmatrix}$



Brahmagupta (VII$^{\text{e}}$ s.) : On peut “multiplier” deux points.

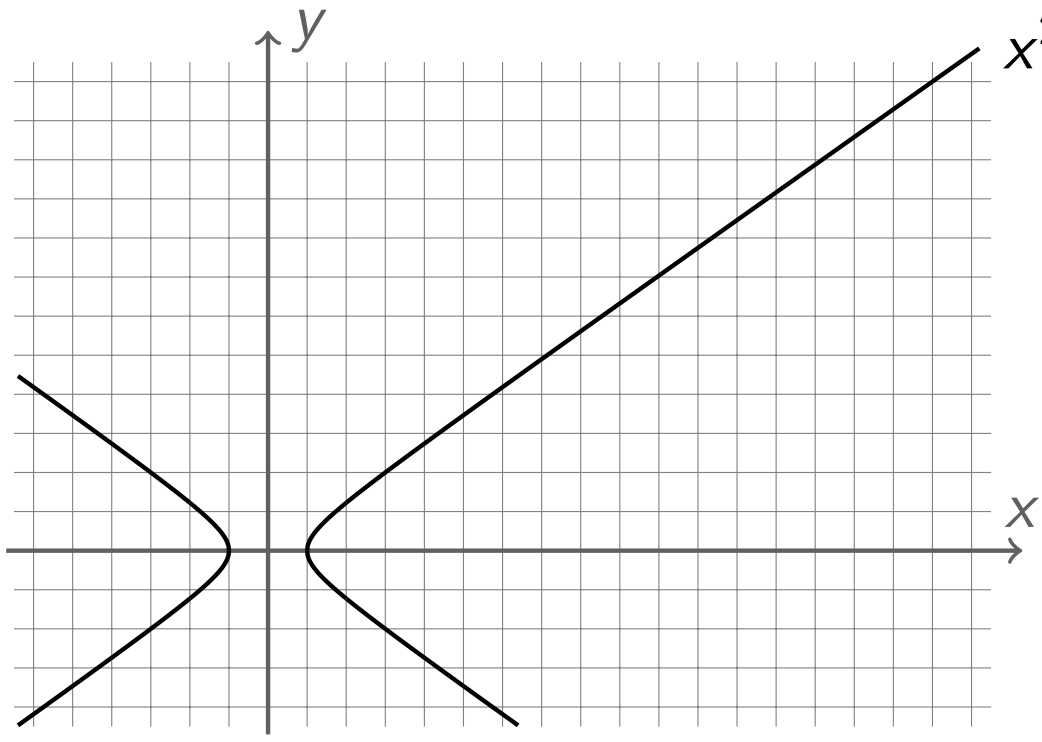
$$P = \begin{vmatrix} x_P \\ y_P \end{vmatrix} \quad Q = \begin{vmatrix} x_Q \\ y_Q \end{vmatrix} \qquad \rightarrow \qquad P \bullet Q = \begin{vmatrix} x_P x_Q + 2 y_P y_Q \\ x_P y_Q + x_Q y_P \end{vmatrix}$$



Brahmagupta (VII$^{\text{e}}$ s.) : On peut “multiplier” deux points.

$$P = \begin{vmatrix} x_P \\ y_P \end{vmatrix} \quad Q = \begin{vmatrix} x_Q \\ y_Q \end{vmatrix} \qquad \rightarrow \qquad P \bullet Q = \begin{vmatrix} x_P x_Q + 2 y_P y_Q \\ x_P y_Q + x_Q y_P \end{vmatrix}$$

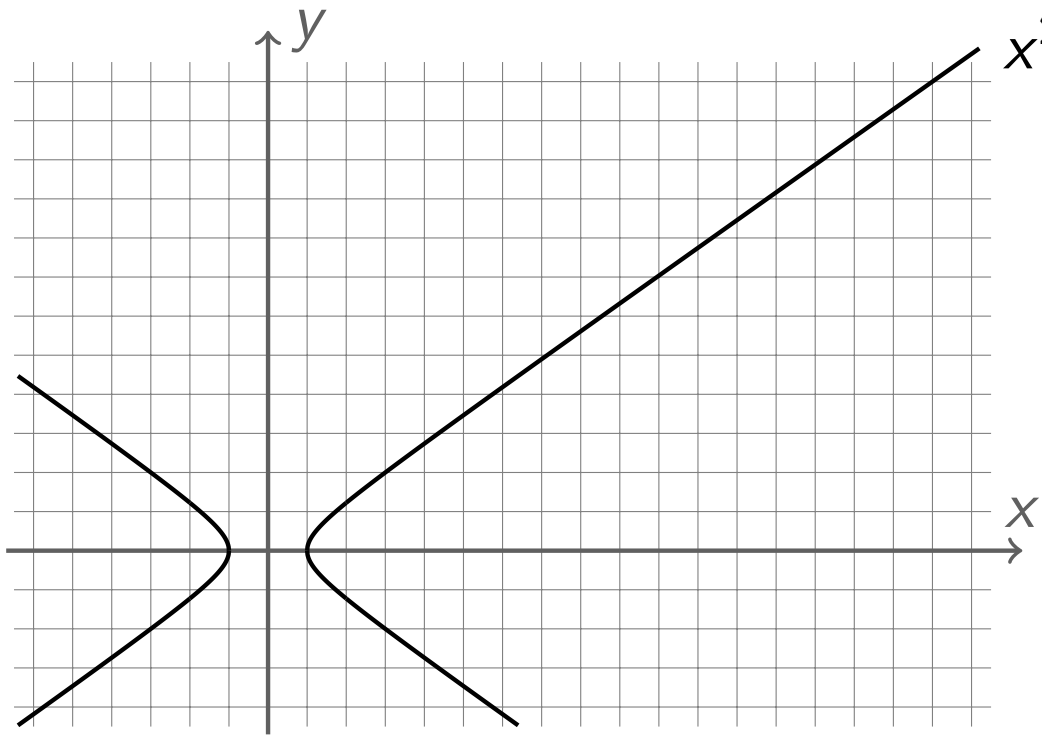
$$(x_P x_Q + 2 y_P y_Q)^2 - 2(x_P y_Q + x_Q y_P)^2 = (x_P^2 - 2 y_P^2)(x_Q^2 - 2 y_Q^2)$$



Brahmagupta (VII$^{\text{e}}$ s.) : On peut “multiplier” deux points.

$$P = \begin{vmatrix} x_P \\ y_P \end{vmatrix} \quad Q = \begin{vmatrix} x_Q \\ y_Q \end{vmatrix} \qquad \rightarrow \qquad P \bullet Q = \begin{vmatrix} x_P x_Q + 2 y_P y_Q \\ x_P y_Q + x_Q y_P \end{vmatrix}$$

$$(x_P x_Q + 2 y_P y_Q)^2 - 2(x_P y_Q + x_Q y_P)^2 = (x_P^2 - 2 y_P^2)(x_Q^2 - 2 y_Q^2) = 1$$

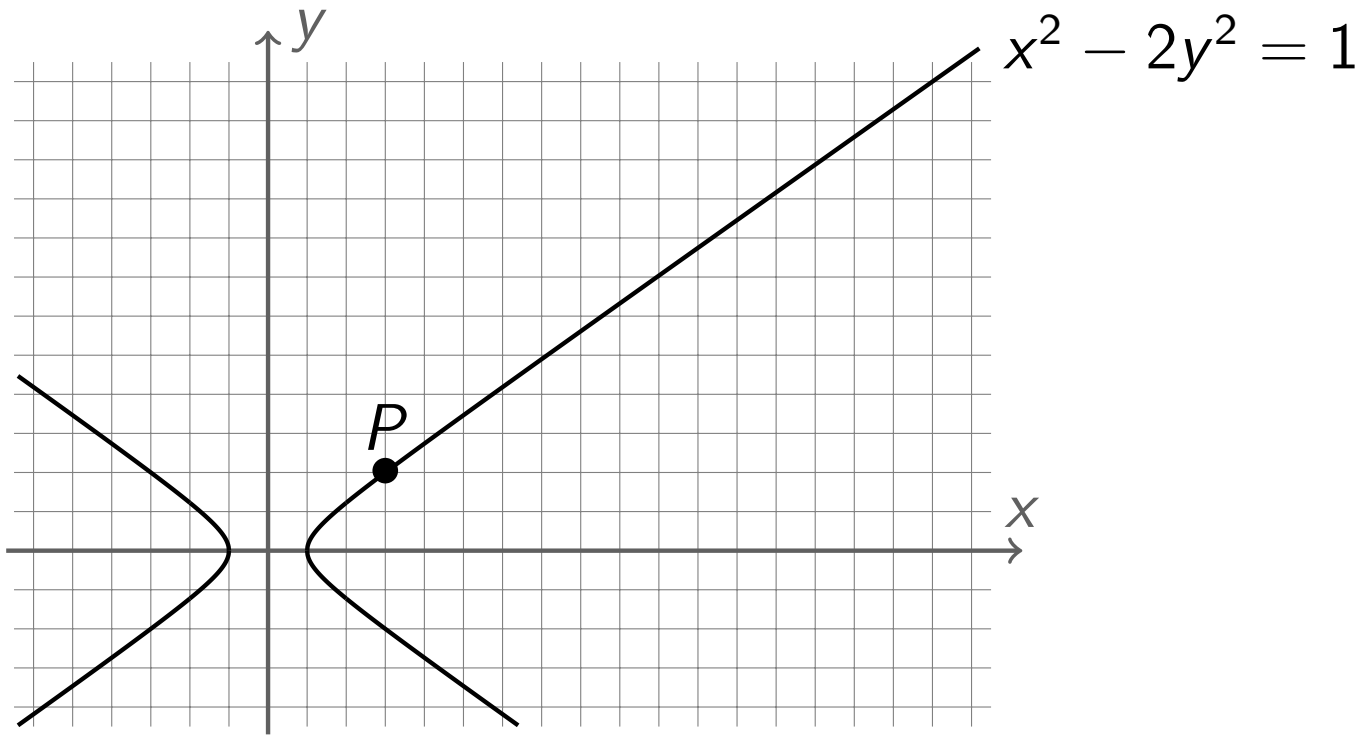


Brahmagupta (VII$^{\text{e}}$ s.) : On peut “multiplier” deux points.

$$P = \begin{vmatrix} x_P \\ y_P \end{vmatrix} \quad Q = \begin{vmatrix} x_Q \\ y_Q \end{vmatrix} \qquad \rightarrow \qquad P \bullet Q = \begin{vmatrix} x_P x_Q + 2y_P y_Q \\ x_P y_Q + x_Q y_P \end{vmatrix}$$

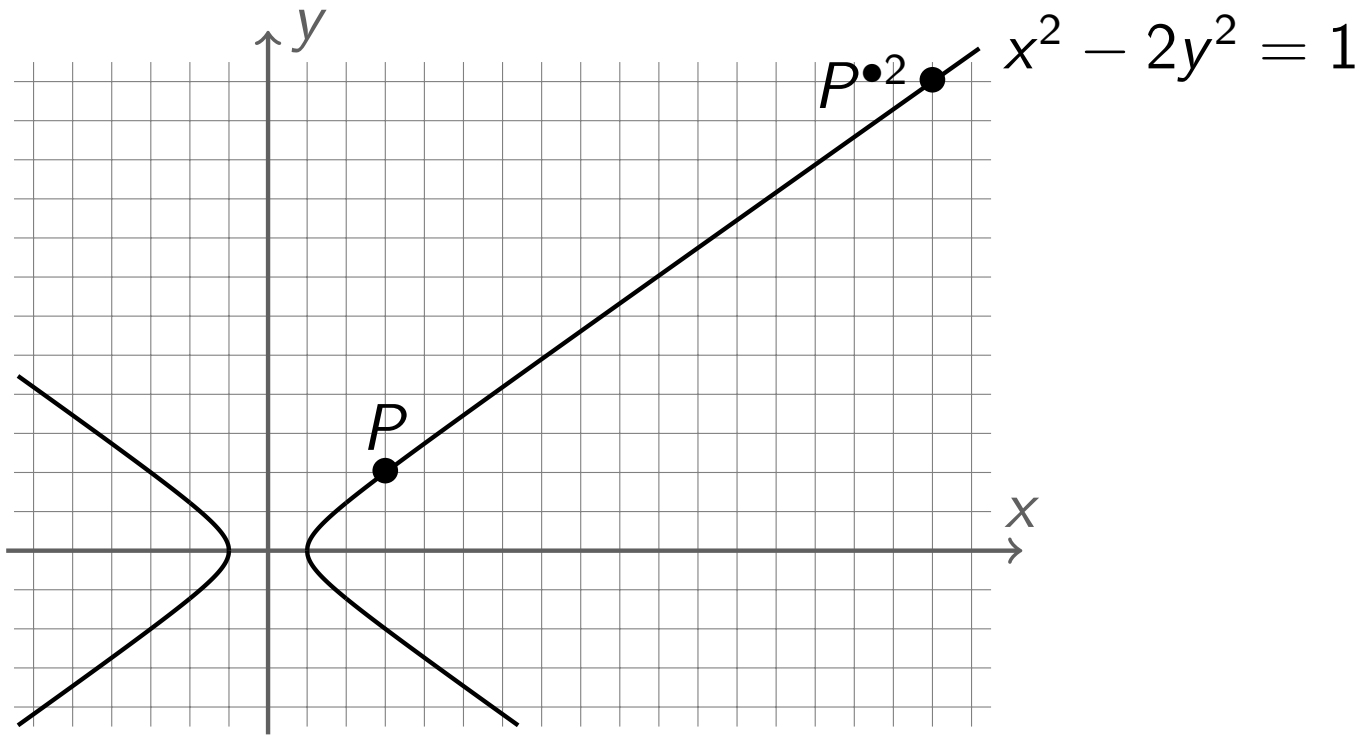
$$(x_P x_Q + 2y_P y_Q)^2 - 2(x_P y_Q + x_Q y_P)^2 = (x_P^2 - 2y_P^2)(x_Q^2 - 2y_Q^2)$$

$$(x_P + y_P\sqrt{2})(x_Q + y_Q\sqrt{2}) = (x_P x_Q + 2y_P y_Q) + (x_P y_Q + x_Q y_P)\sqrt{2}$$



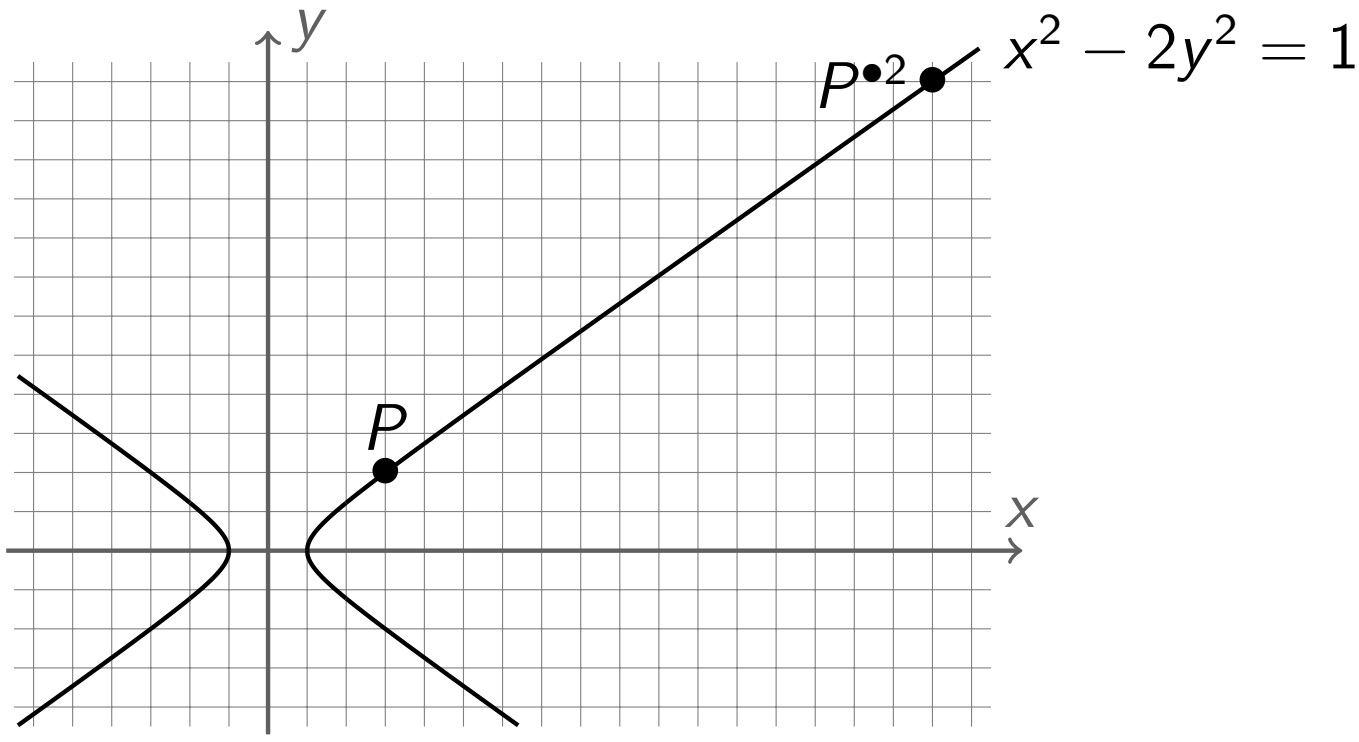
Brahmagupta (VII$^{\text{e}}$ s.) : On peut “multiplier” deux points.

ex : $P = \begin{vmatrix} 3 \\ 2 \end{vmatrix}$



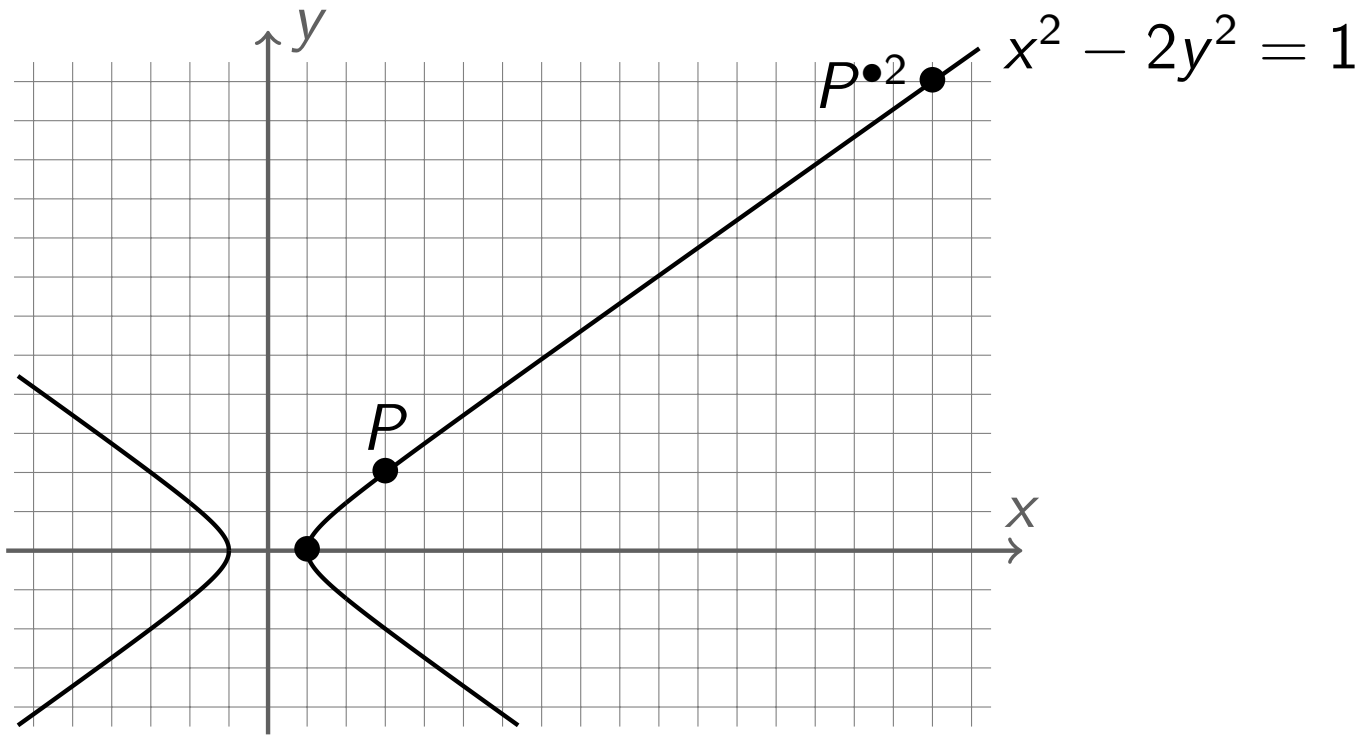
Brahmagupta (VII$^{\text{e}}$ s.) : On peut “multiplier” deux points.

ex : $P = \begin{vmatrix} 3 \\ 2 \end{vmatrix}$ $\qquad P^{\bullet 2} = P \bullet P = \begin{vmatrix} 17 \\ 12 \end{vmatrix}$



Brahmagupta (VII$^{\text{e}}$ s.) : On peut “multiplier” deux points.

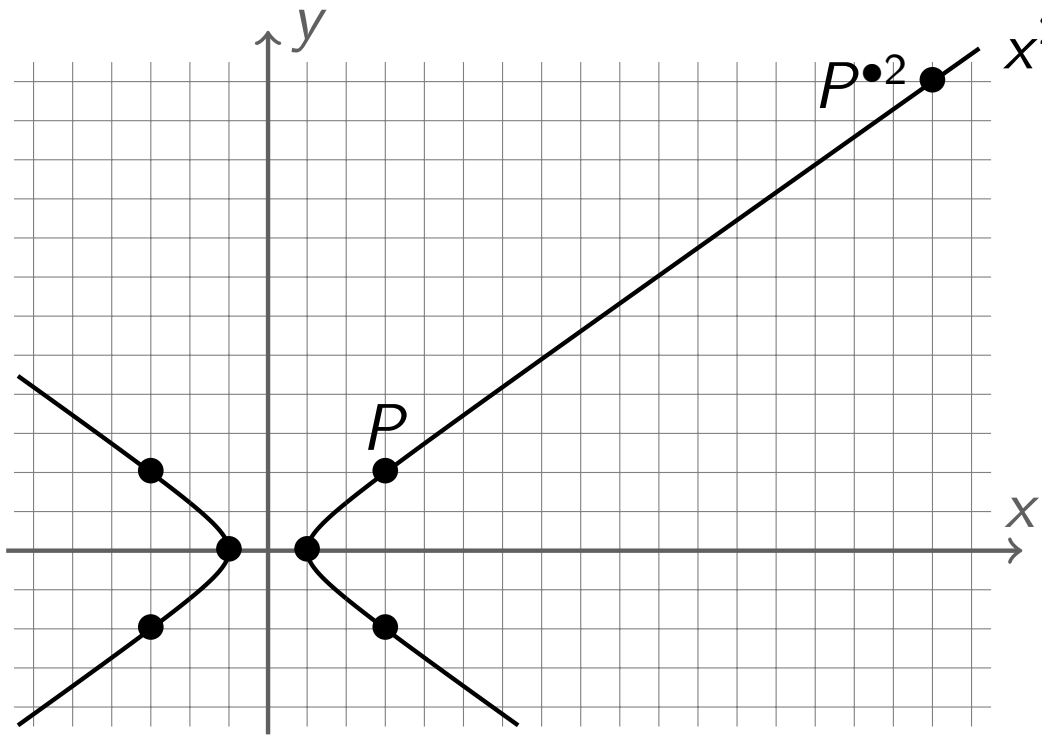
ex : $P = \begin{vmatrix} 3 \\ 2 \end{vmatrix}$ $\quad P^{\bullet 2} = P \bullet P = \begin{vmatrix} 17 \\ 12 \end{vmatrix}$ $\quad P^{\bullet 3} = \begin{vmatrix} 99 \\ 70 \end{vmatrix}$ etc.



Brahmagupta (VII$^{\text{e}}$ s.) : On peut “multiplier” deux points.

ex : $P = \begin{vmatrix} 3 \\ 2 \end{vmatrix}$ $\quad P^{\bullet 2} = P \bullet P = \begin{vmatrix} 17 \\ 12 \end{vmatrix}$ $\quad P^{\bullet 3} = \begin{vmatrix} 99 \\ 70 \end{vmatrix}$ etc.

$P^{\bullet 0} = \begin{vmatrix} 1 \\ 0 \end{vmatrix}$



Brahmagupta (VII$^{\text{e}}$ s.) : On peut “multiplier” deux points.

ex : $P = \begin{vmatrix} 3 \\ 2 \end{vmatrix}$ $\quad P^{\bullet 2} = P \bullet P = \begin{vmatrix} 17 \\ 12 \end{vmatrix}$ $\quad P^{\bullet 3} = \begin{vmatrix} 99 \\ 70 \end{vmatrix}$ etc.

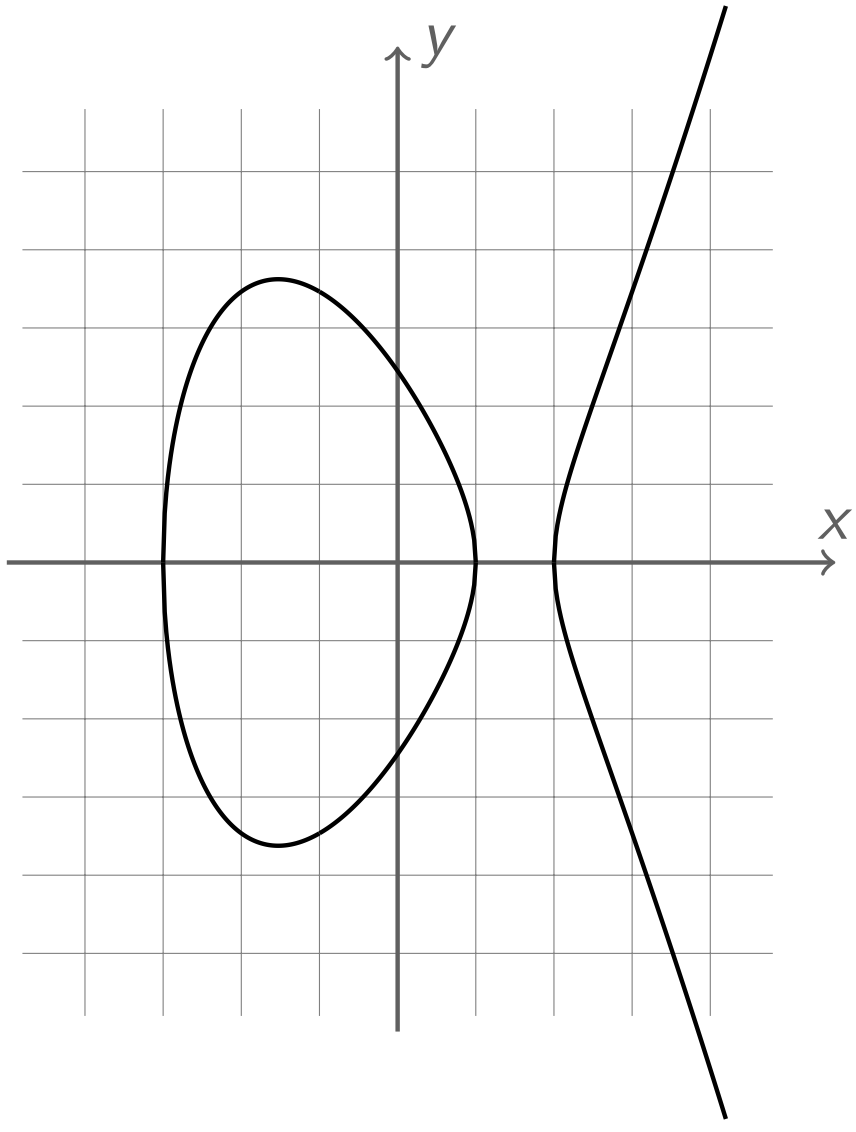
$P^{\bullet 0} = \begin{vmatrix} 1 \\ 0 \end{vmatrix}$ et on montre qu’au signe des coordonnées près on obtient ainsi toutes les solutions entières.

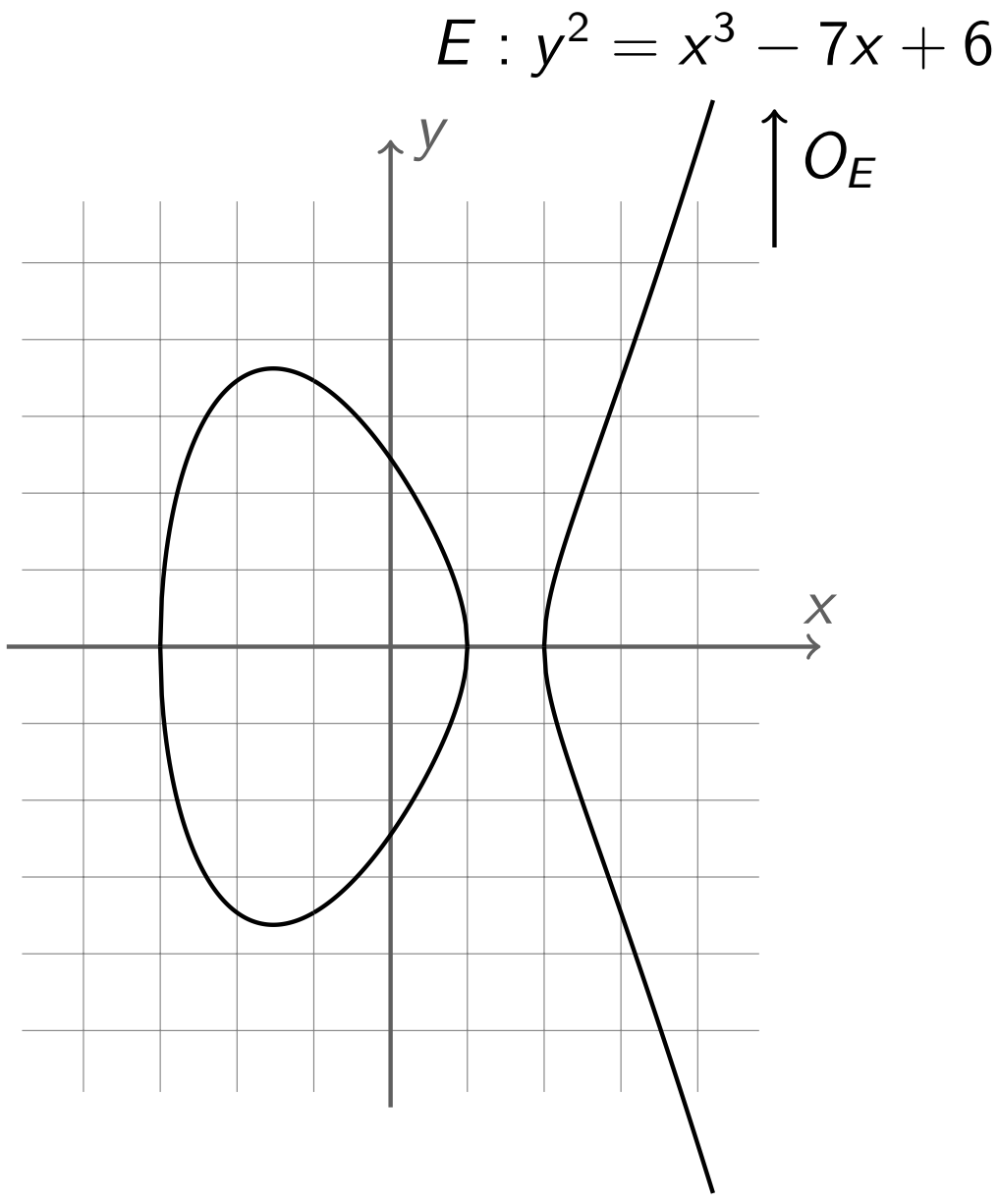
Genre 1

Courbes elliptiques.
Motivation : "grand théorème de Fermat" $x^N + y^N = z^N$

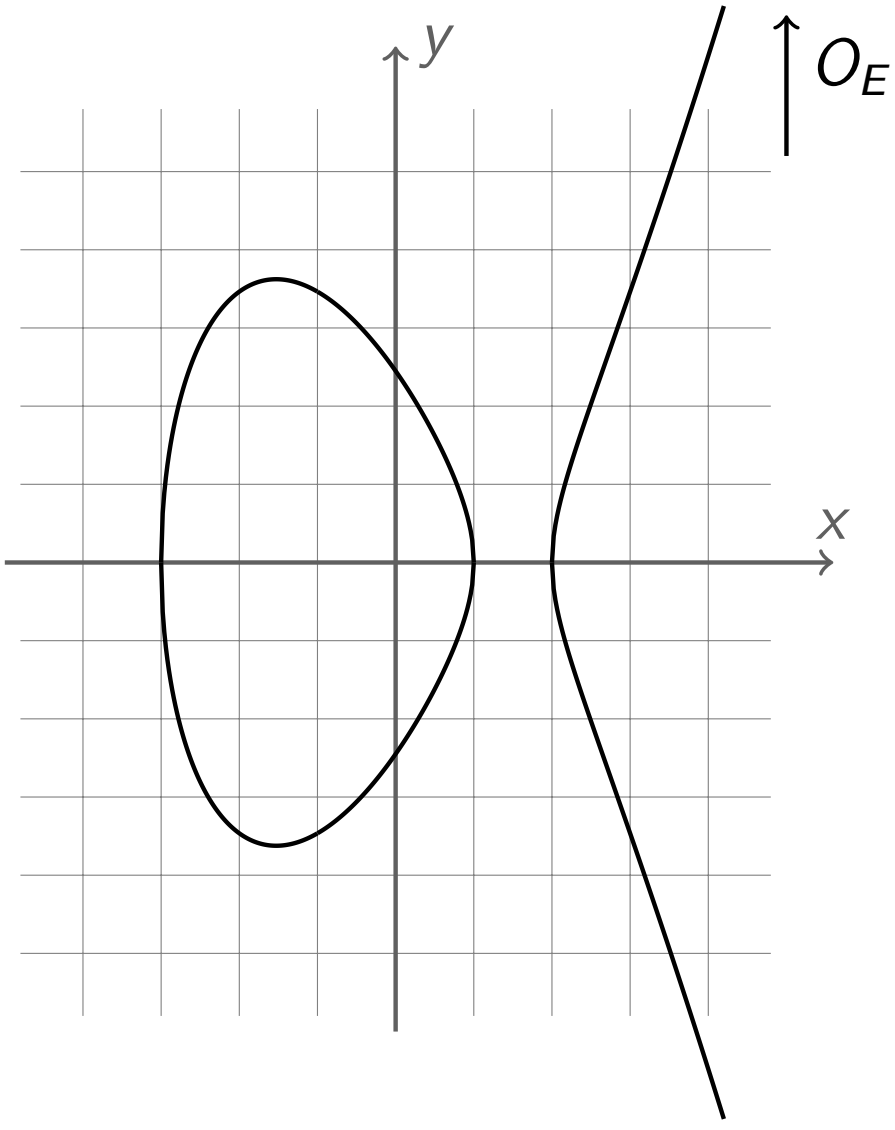
- Fermat pour $N = 4$
- Wiles, etc. pour le cas général

$$E : y^2 = x^3 - 7x + 6$$



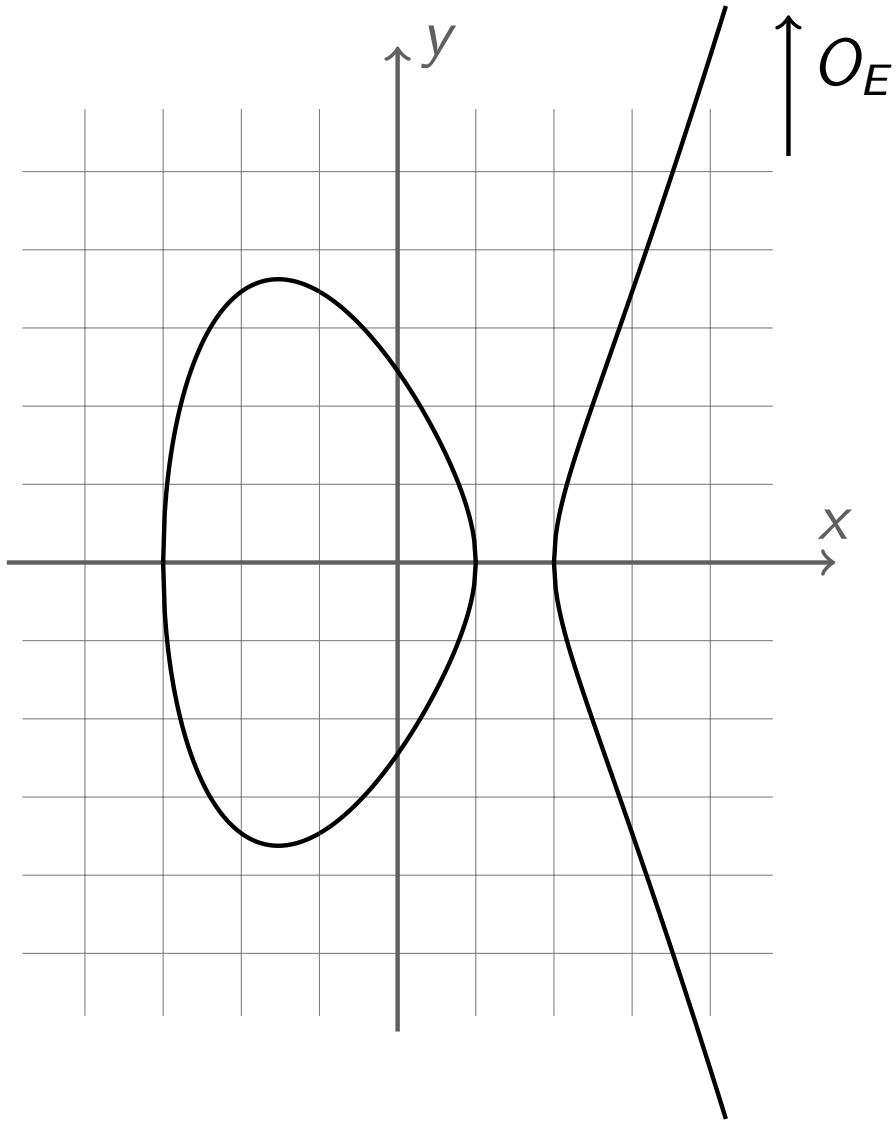

$E : y^2 = x^3 - 7x + 6$
O_E
y
x

$$E : y^2 = x^3 - 7x + 6$$



On va munir E d'une loi d'addition (qui va en faire un groupe abélien).

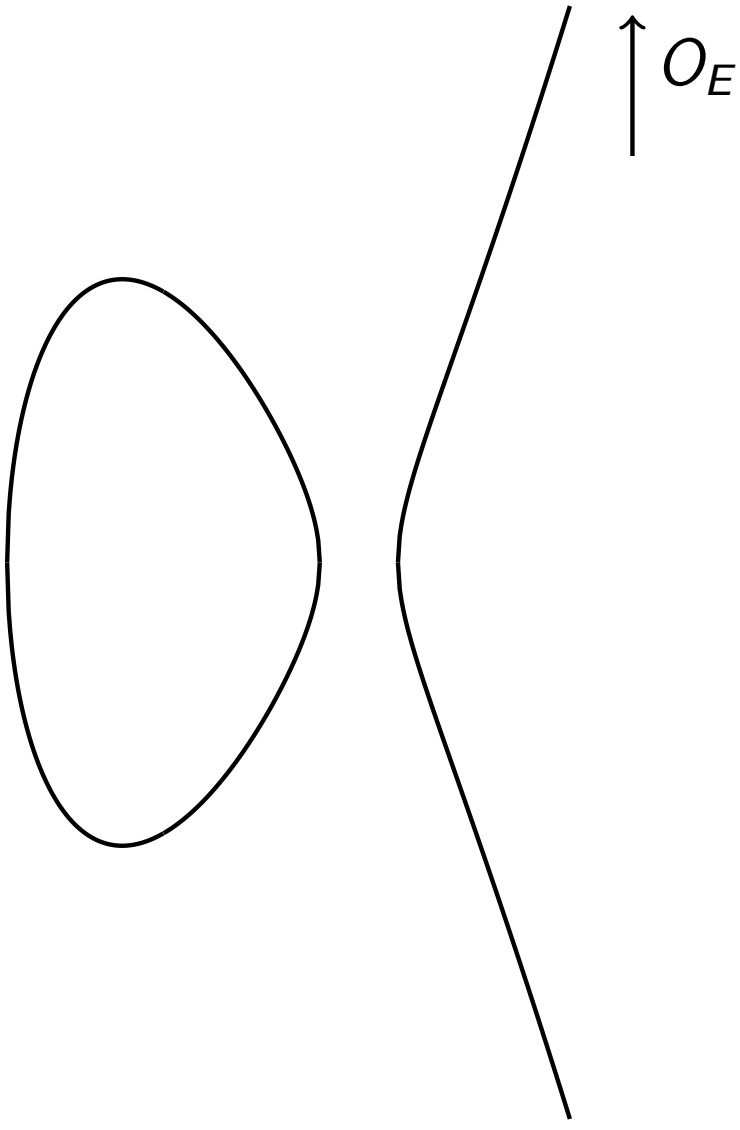
$$E : y^2 = x^3 - 7x + 6$$



On va munir E d'une loi d'addition (qui va en faire un groupe abélien).

Règles :

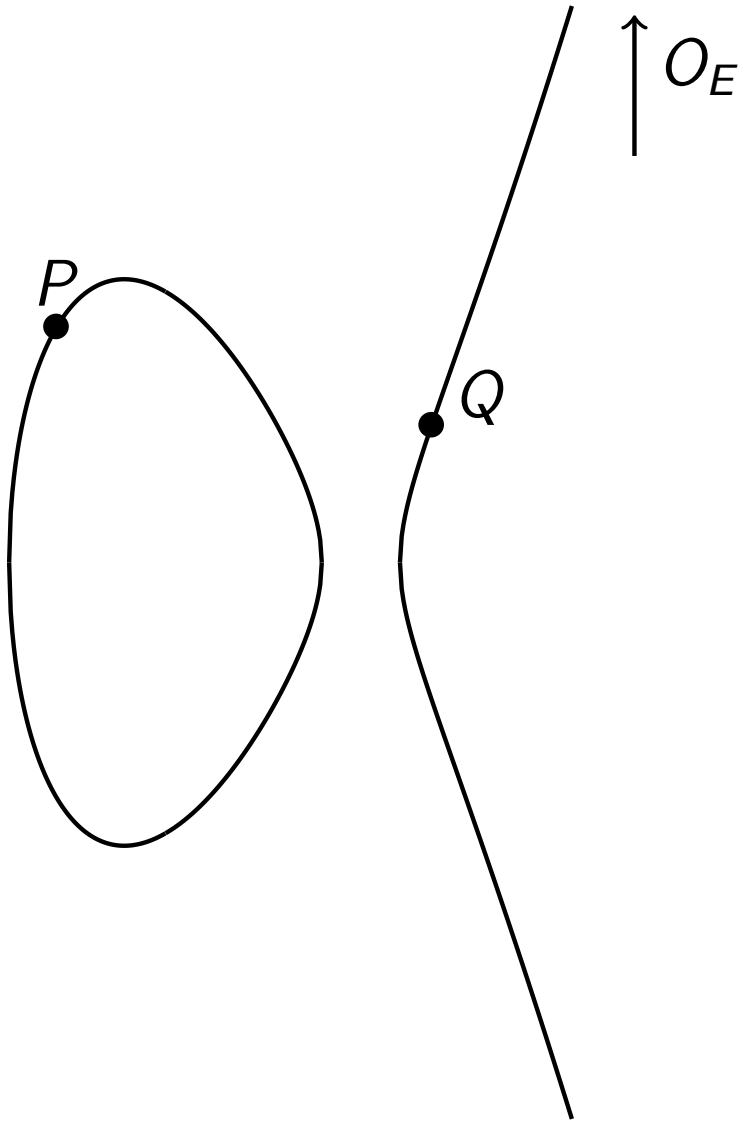
- O_E est l'élément neutre
- $P + Q + R = O_E$ ssi $\{P, Q, R\} = E \cap D$.



On va munir E d'une loi d'addition (qui va en faire un groupe abélien).

Règles :

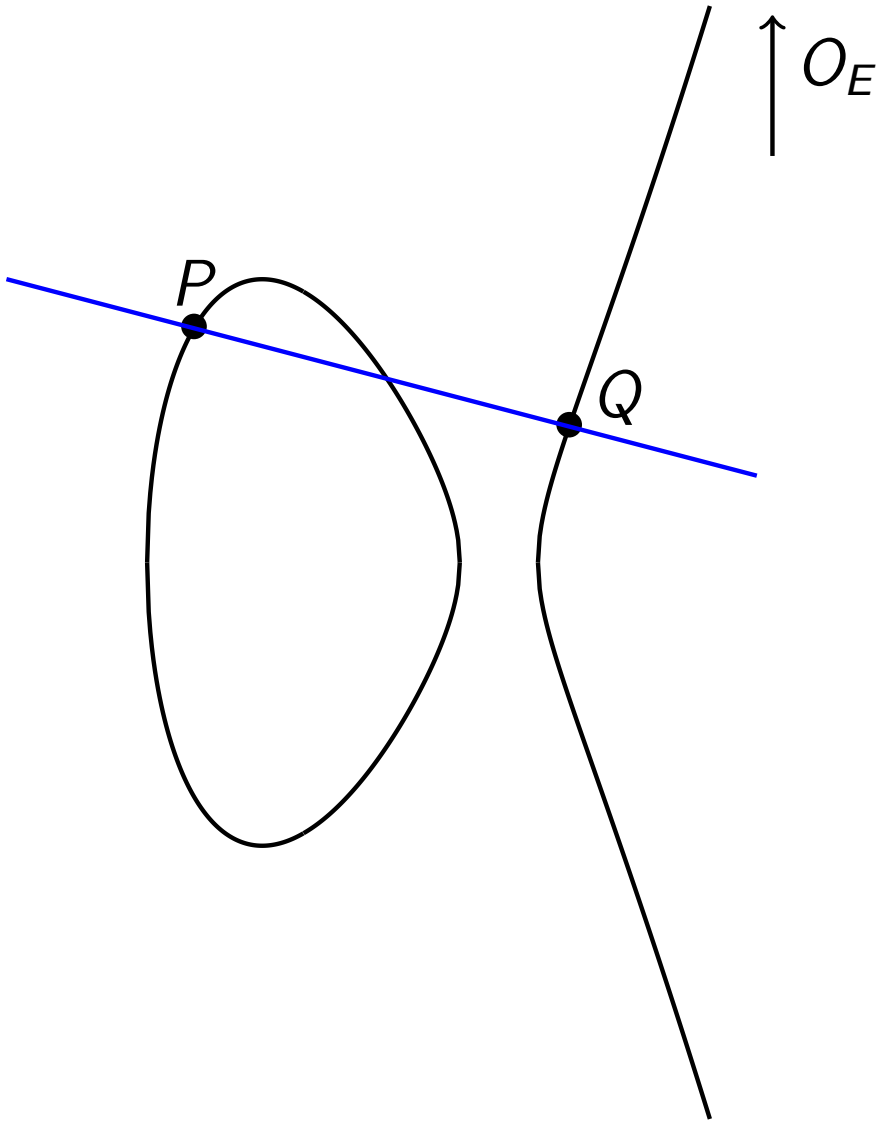
- O_E est l'élément neutre
- $P + Q + R = O_E$ ssi $\{P, Q, R\} = E \cap D$.



On va munir E d'une loi d'addition (qui va en faire un groupe abélien).

Règles :

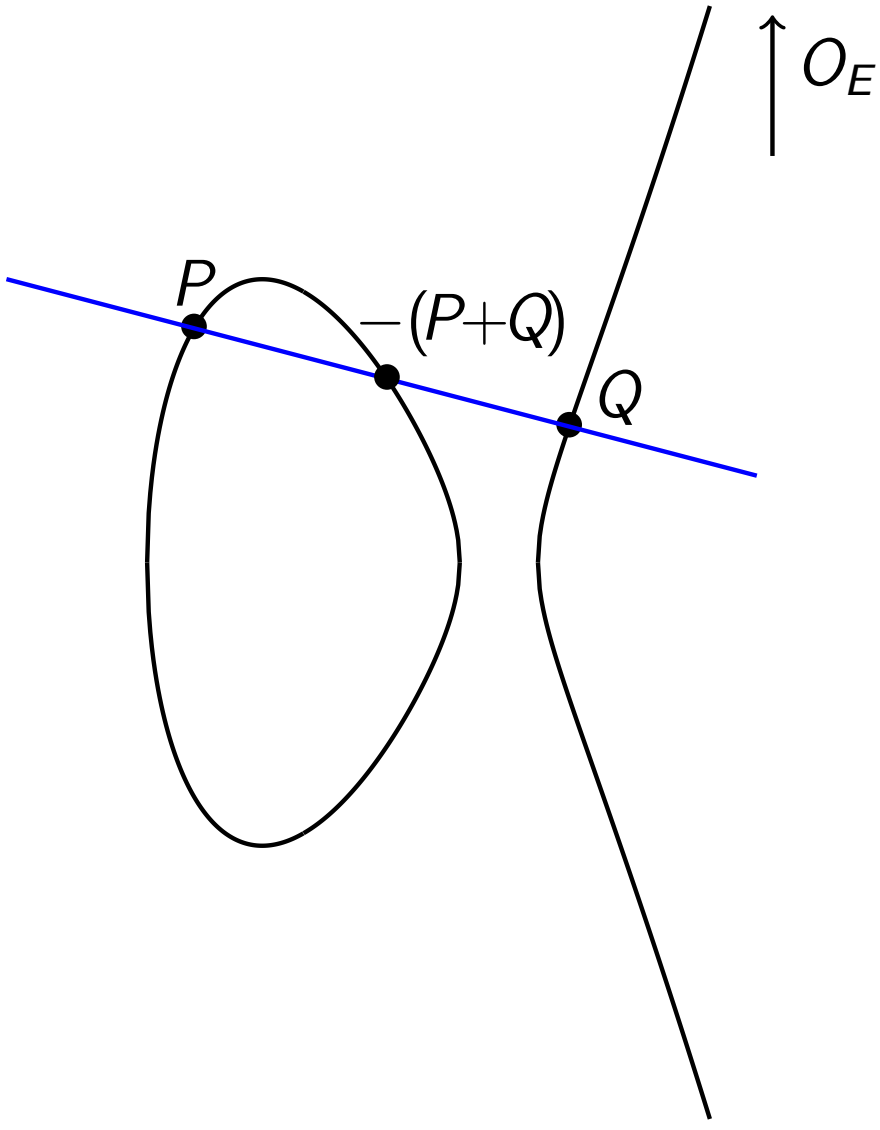
- O_E est l'élément neutre
- $P + Q + R = O_E$ ssi $\{P, Q, R\} = E \cap D$.



On va munir E d'une loi d'addition (qui va en faire un groupe abélien).

Règles :

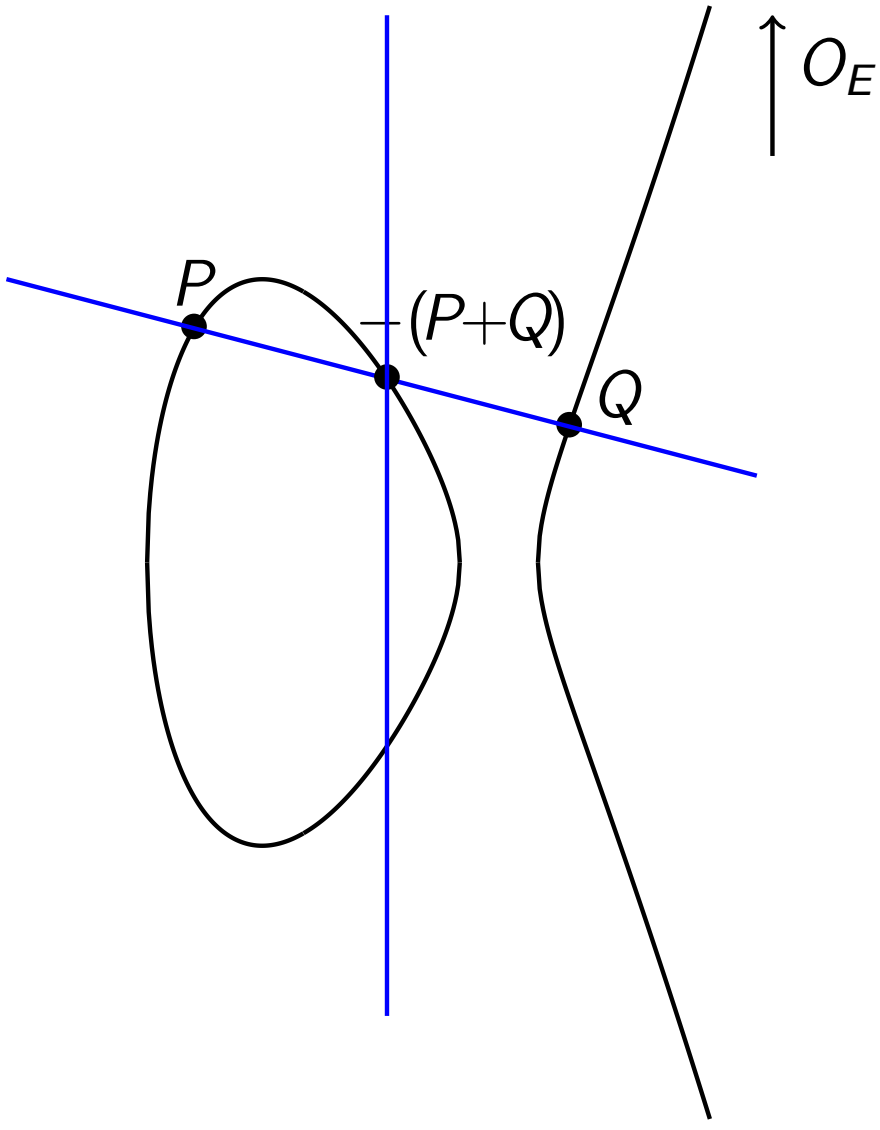
- O_E est l'élément neutre
- $P + Q + R = O_E$ ssi $\{P, Q, R\} = E \cap D$.



On va munir E d'une loi d'addition (qui va en faire un groupe abélien).

Règles :

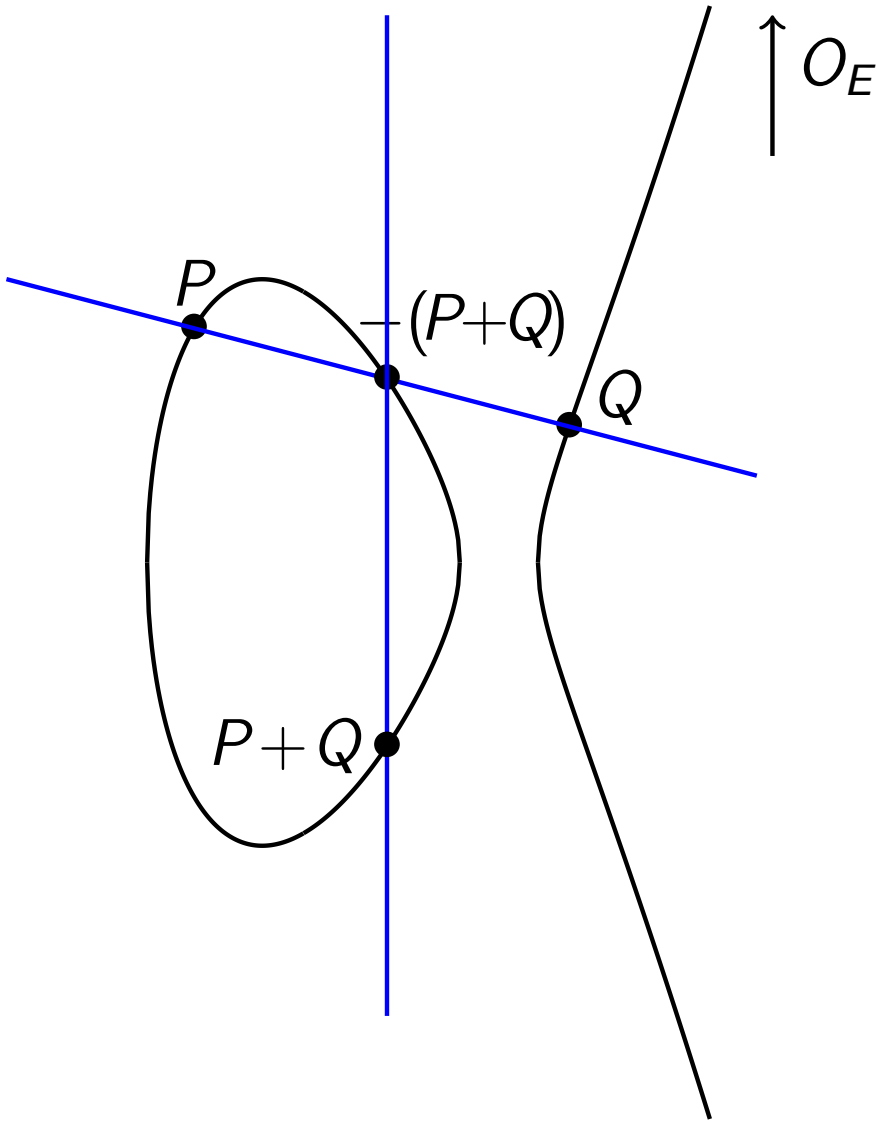
- O_E est l'élément neutre
- $P + Q + R = O_E$ ssi $\{P, Q, R\} = E \cap D$.



On va munir E d'une loi d'addition (qui va en faire un groupe abélien).

Règles :

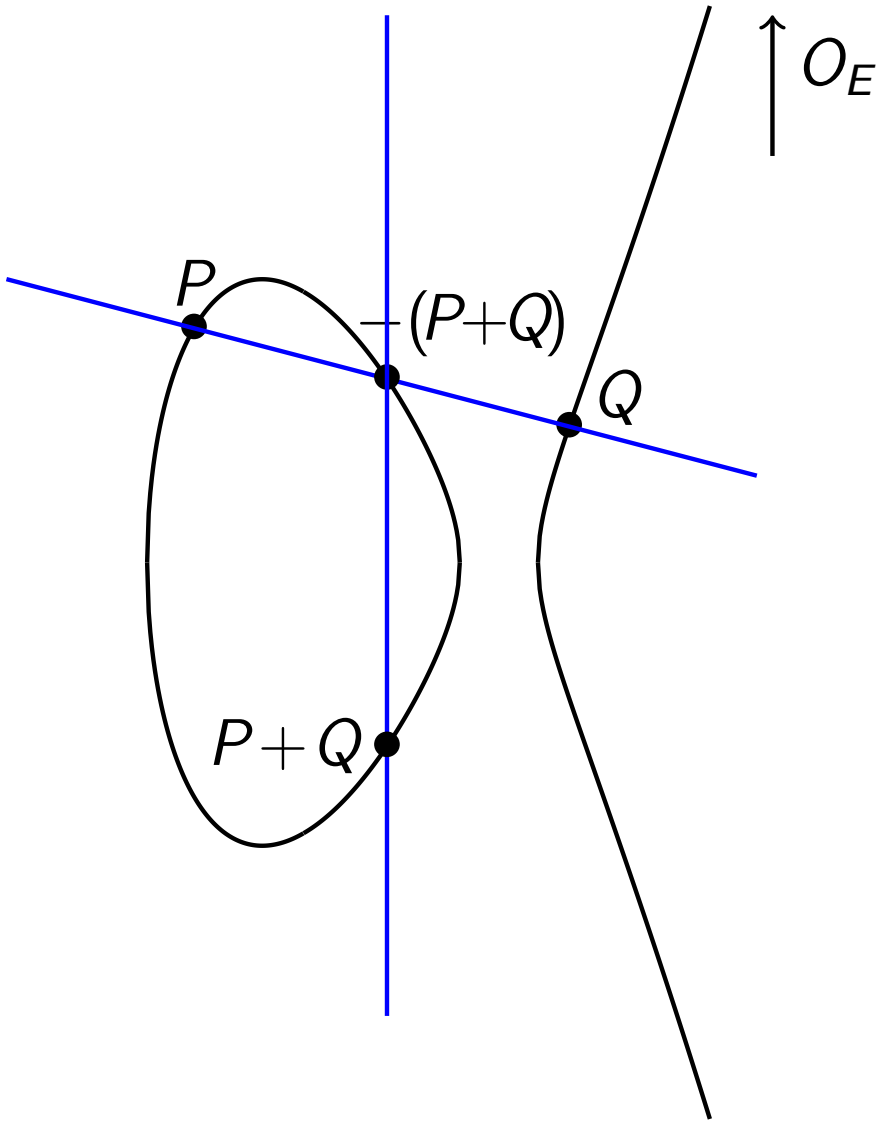
- O_E est l'élément neutre
- $P + Q + R = O_E$ ssi $\{P, Q, R\} = E \cap D$.



On va munir E d'une loi d'addition (qui va en faire un groupe abélien).

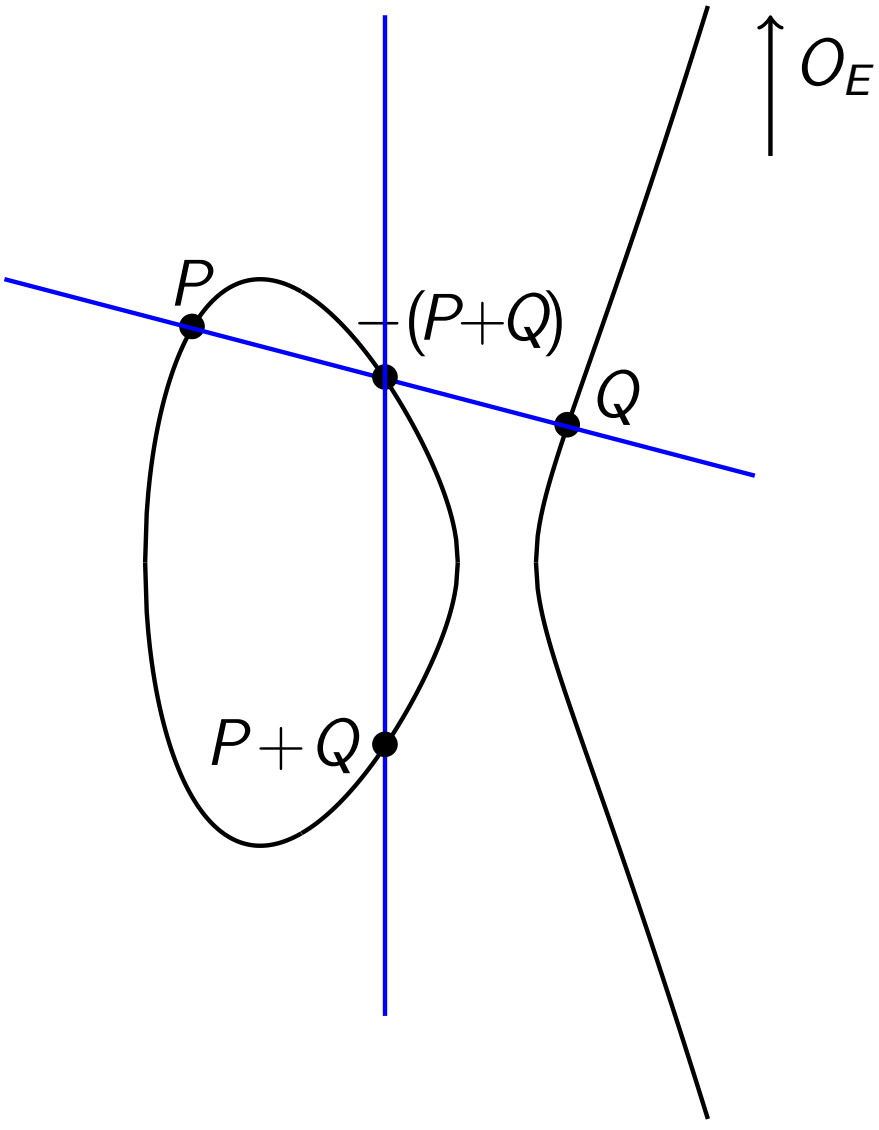
Règles :

- O_E est l'élément neutre
- $P + Q + R = O_E$ ssi $\{P, Q, R\} = E \cap D$.



Formules explicites :

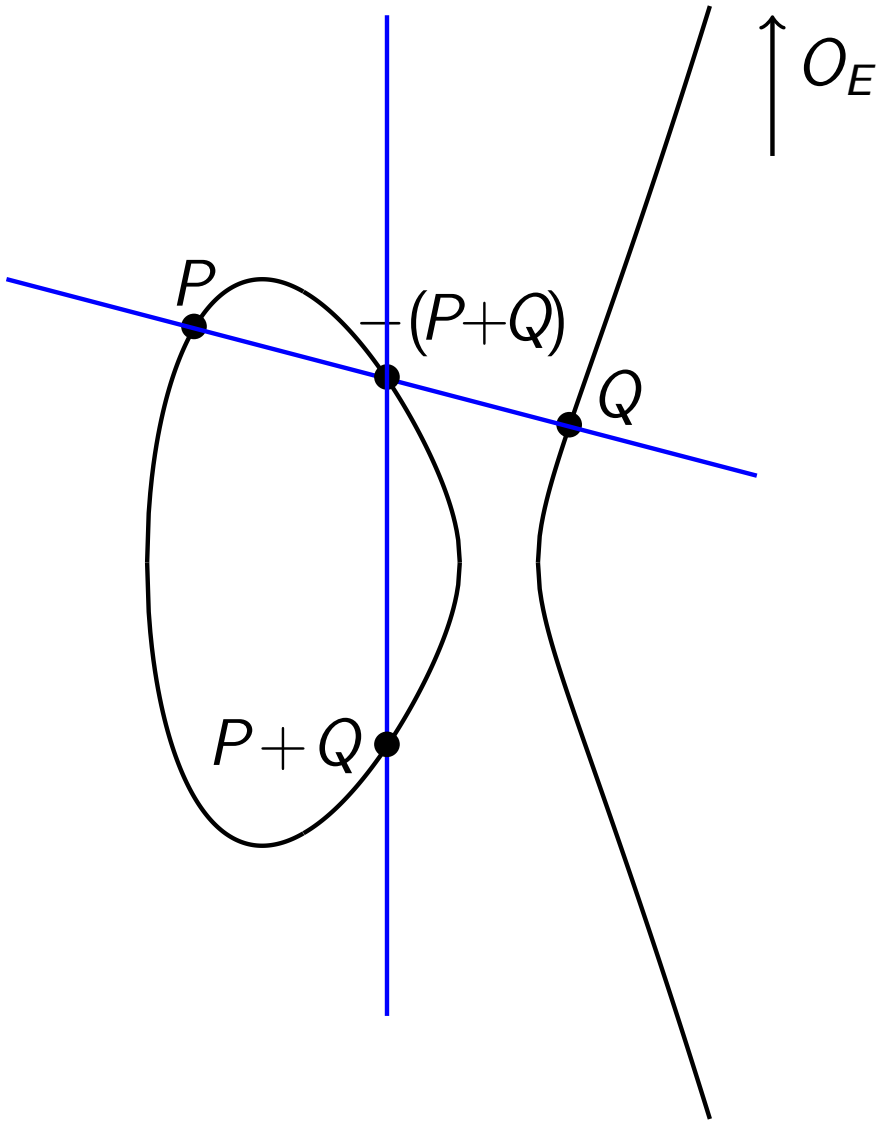
$$P = \begin{vmatrix} x_P \\ y_P \end{vmatrix} \qquad Q = \begin{vmatrix} x_Q \\ y_Q \end{vmatrix}$$



Formules explicites :

$$P = \begin{vmatrix} x_P \\ y_P \end{vmatrix} \qquad Q = \begin{vmatrix} x_Q \\ y_Q \end{vmatrix}$$

$(PQ) : y = \lambda(x - x_P) + y_P$
où $\lambda = (y_Q - y_P)/(x_Q - x_P)$



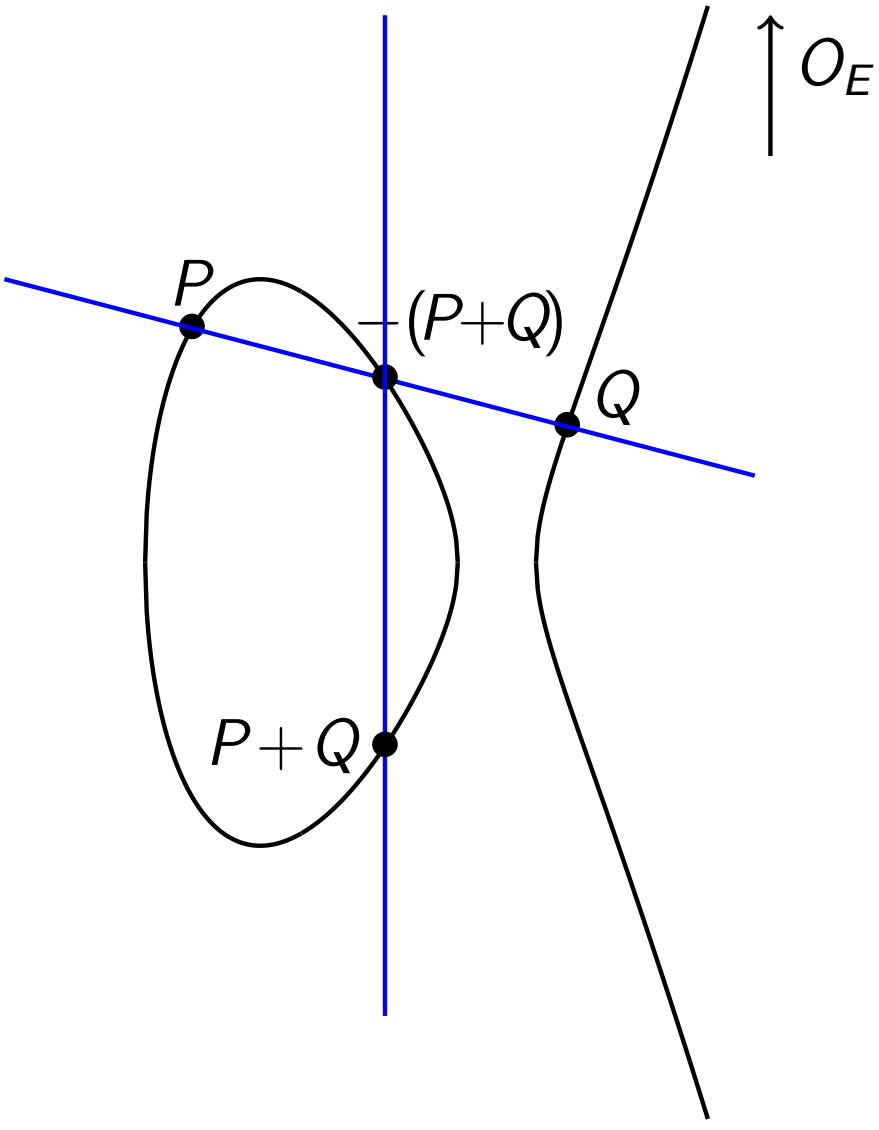
Formules explicites :

$$P = \begin{vmatrix} x_P \\ y_P \end{vmatrix} \qquad Q = \begin{vmatrix} x_Q \\ y_Q \end{vmatrix}$$

$(PQ) : y = \lambda(x - x_P) + y_P$
où $\lambda = (y_Q - y_P)/(x_Q - x_P)$

$E \cap (PQ)$:

$E : y^2 = x^3 - 7x + 6$



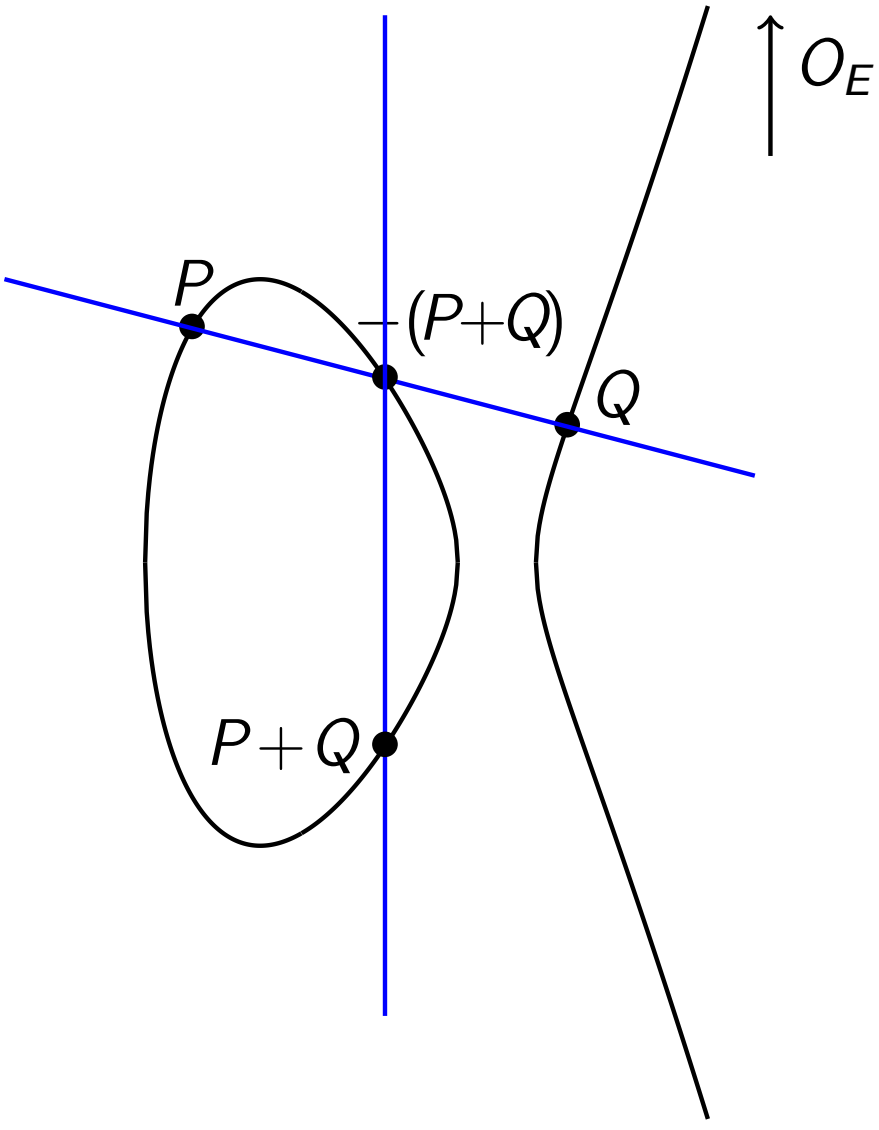
Formules explicites :

$$P = \begin{vmatrix} x_P \\ y_P \end{vmatrix} \qquad Q = \begin{vmatrix} x_Q \\ y_Q \end{vmatrix}$$

$(PQ) : y = \lambda(x - x_P) + y_P$
où $\lambda = (y_Q - y_P)/(x_Q - x_P)$

$E \cap (PQ)$:

$E : y^2 = x^3 - 7x + 6$



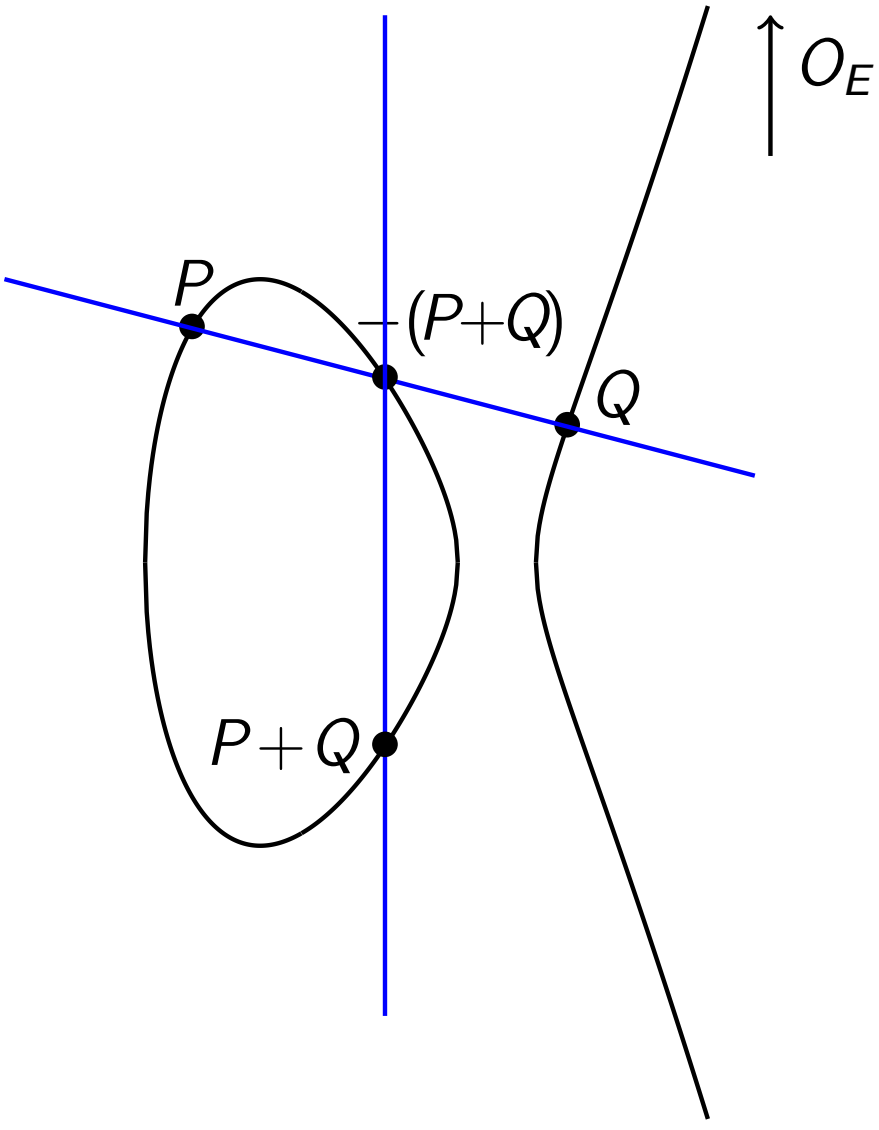
Formules explicites :

$$P = \begin{vmatrix} x_P \\ y_P \end{vmatrix} \qquad Q = \begin{vmatrix} x_Q \\ y_Q \end{vmatrix}$$

$(PQ) : y = \lambda(x - x_P) + y_P$
où $\lambda = (y_Q - y_P)/(x_Q - x_P)$

$E \cap (PQ)$:
$\rightarrow \quad x^3 - \lambda^2 x^2 + \cdots = 0$

$$E : y^2 = x^3 - 7x + 6$$



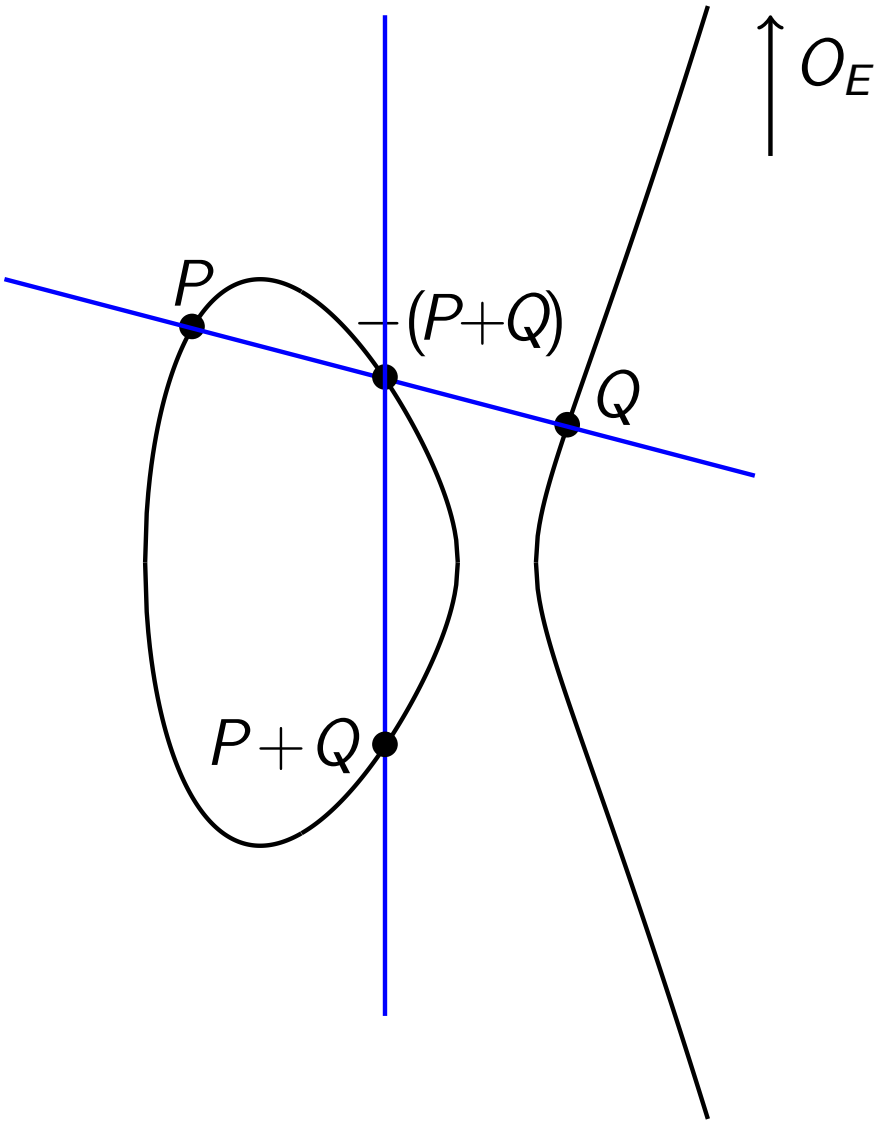
Formules explicites :

$$P = \begin{vmatrix} x_P \\ y_P \end{vmatrix} \qquad Q = \begin{vmatrix} x_Q \\ y_Q \end{vmatrix}$$

$(PQ) : y = \lambda(x - x_P) + y_P$
où $\lambda = (y_Q - y_P)/(x_Q - x_P)$

$E \cap (PQ)$:
$\rightarrow \quad x^3 - \lambda^2 x^2 + \cdots = 0$
racines x_P, x_Q, x_{P+Q}

$$E : y^2 = x^3 - 7x + 6$$



Formules explicites :

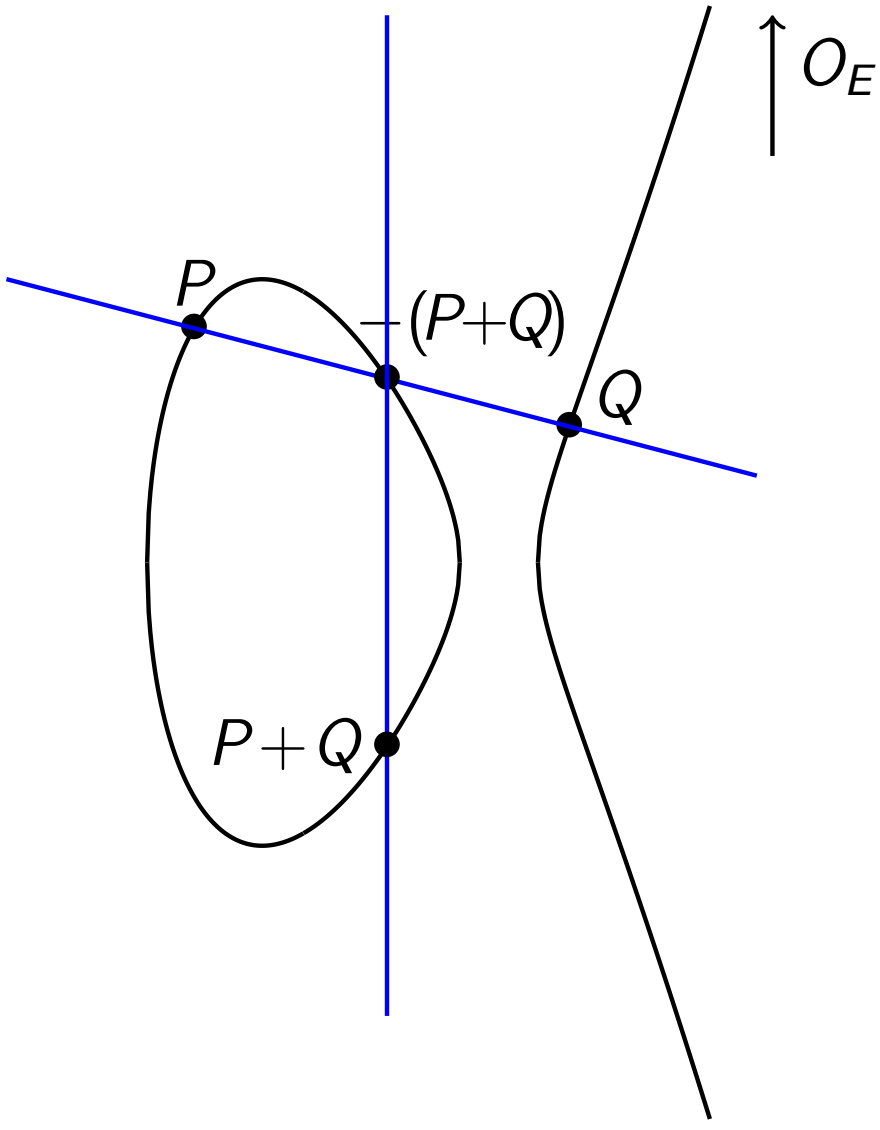
$$P = \begin{vmatrix} x_P \\ y_P \end{vmatrix} \qquad Q = \begin{vmatrix} x_Q \\ y_Q \end{vmatrix}$$

$(PQ) : y = \lambda(x - x_P) + y_P$
où $\lambda = (y_Q - y_P)/(x_Q - x_P)$

$E \cap (PQ)$:
$\rightarrow \quad x^3 - \lambda^2 x^2 + \cdots = 0$
racines x_P, x_Q, x_{P+Q}

$$x_{P+Q} = \lambda^2 - x_P - x_Q$$

$$E : y^2 = x^3 - 7x + 6$$



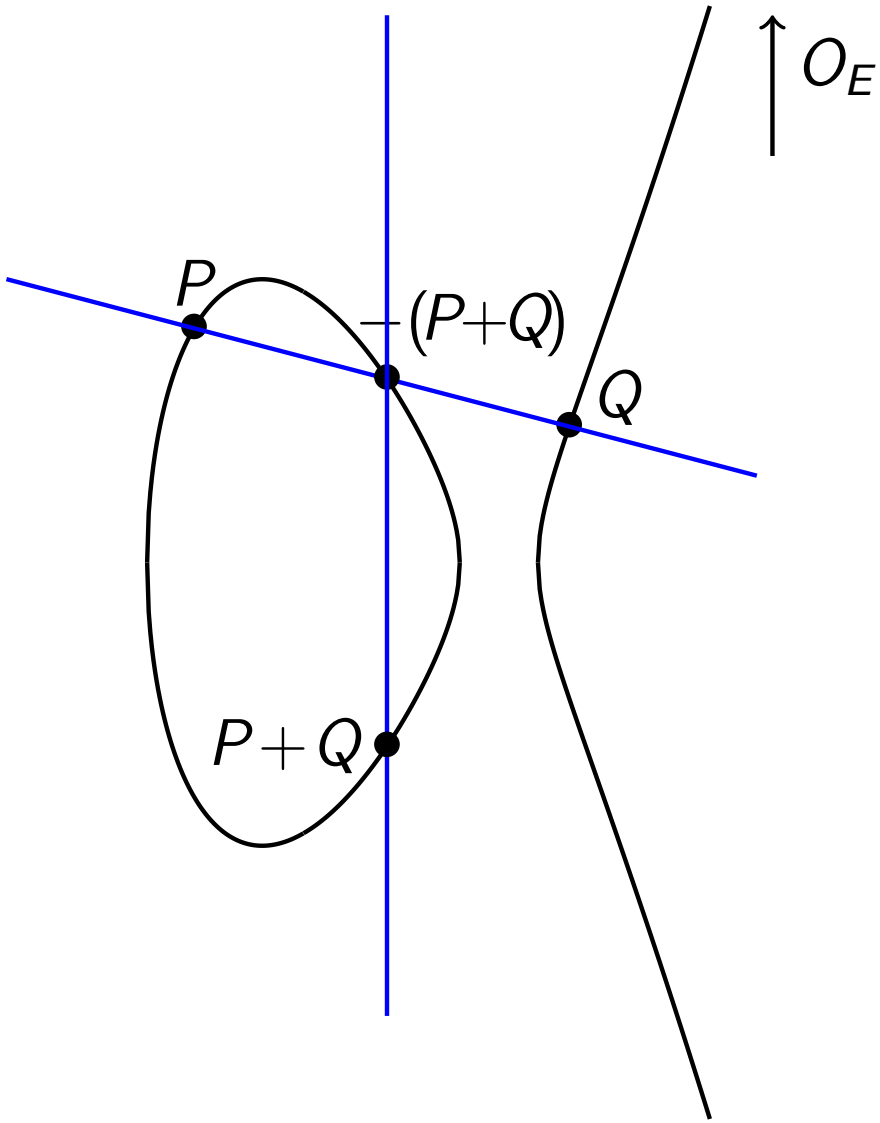
Formules explicites :

$$P = \begin{vmatrix} x_P \\ y_P \end{vmatrix} \qquad Q = \begin{vmatrix} x_Q \\ y_Q \end{vmatrix}$$

$(PQ) : y = \lambda(x - x_P) + y_P$
où $\lambda = (y_Q - y_P)/(x_Q - x_P)$

$E \cap (PQ)$:
$\rightarrow \quad x^3 - \lambda^2 x^2 + \cdots = 0$
racines x_P, x_Q, x_{P+Q}

$x_{P+Q} = \lambda^2 - x_P - x_Q$
$y_{P+Q} = -\lambda(x_{P+Q} - x_P) - y_P$



Groupe abélien :

- neutre O_E
- opposé

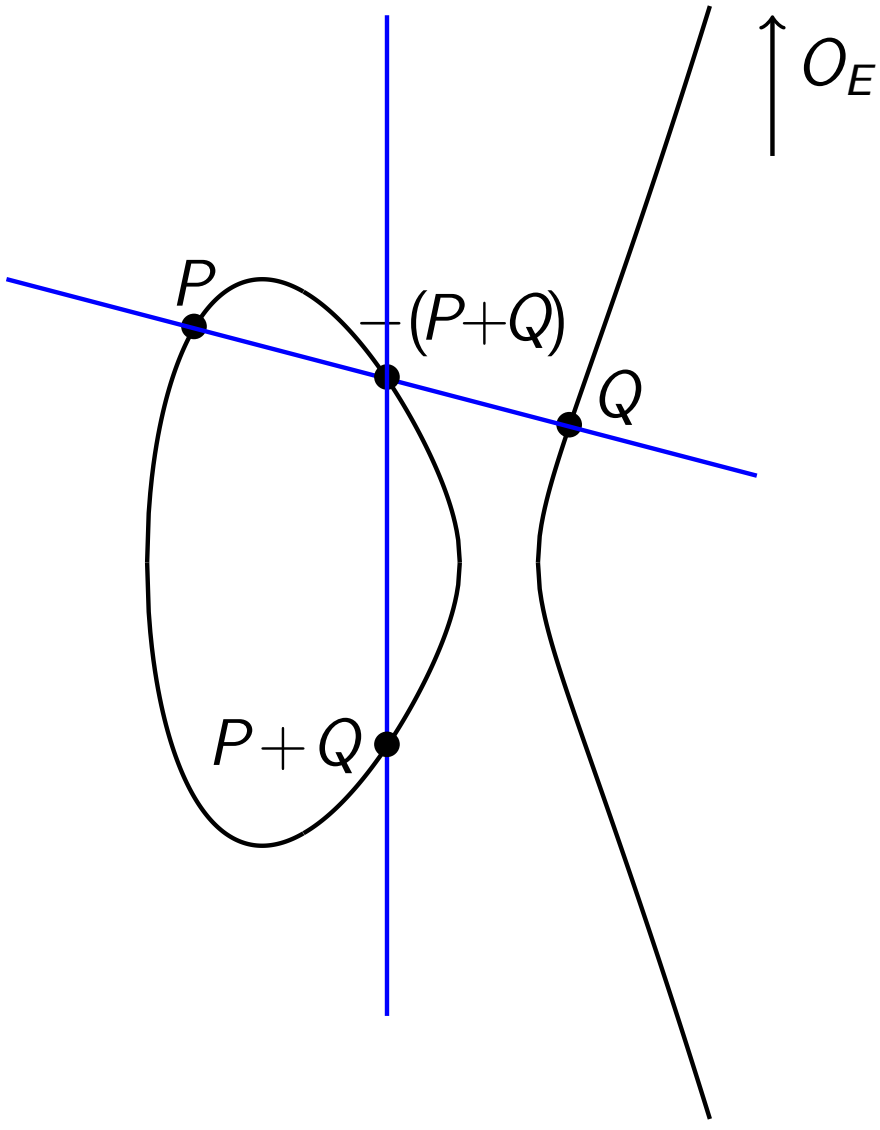
$$-\begin{vmatrix} x \\ y \end{vmatrix} = \begin{vmatrix} x \\ -y \end{vmatrix}$$

- commutativité

$$P + Q = Q + P$$

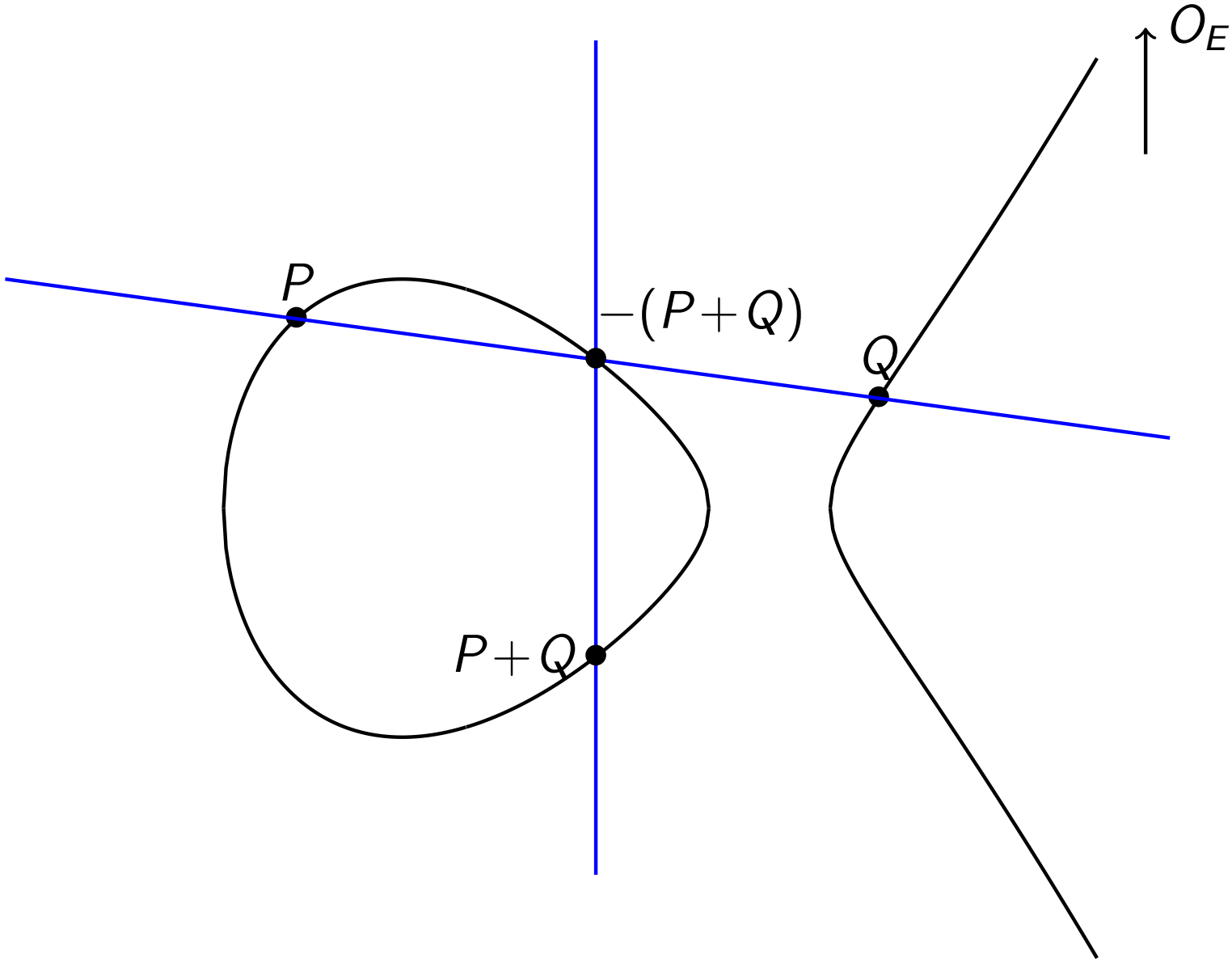
- associativité

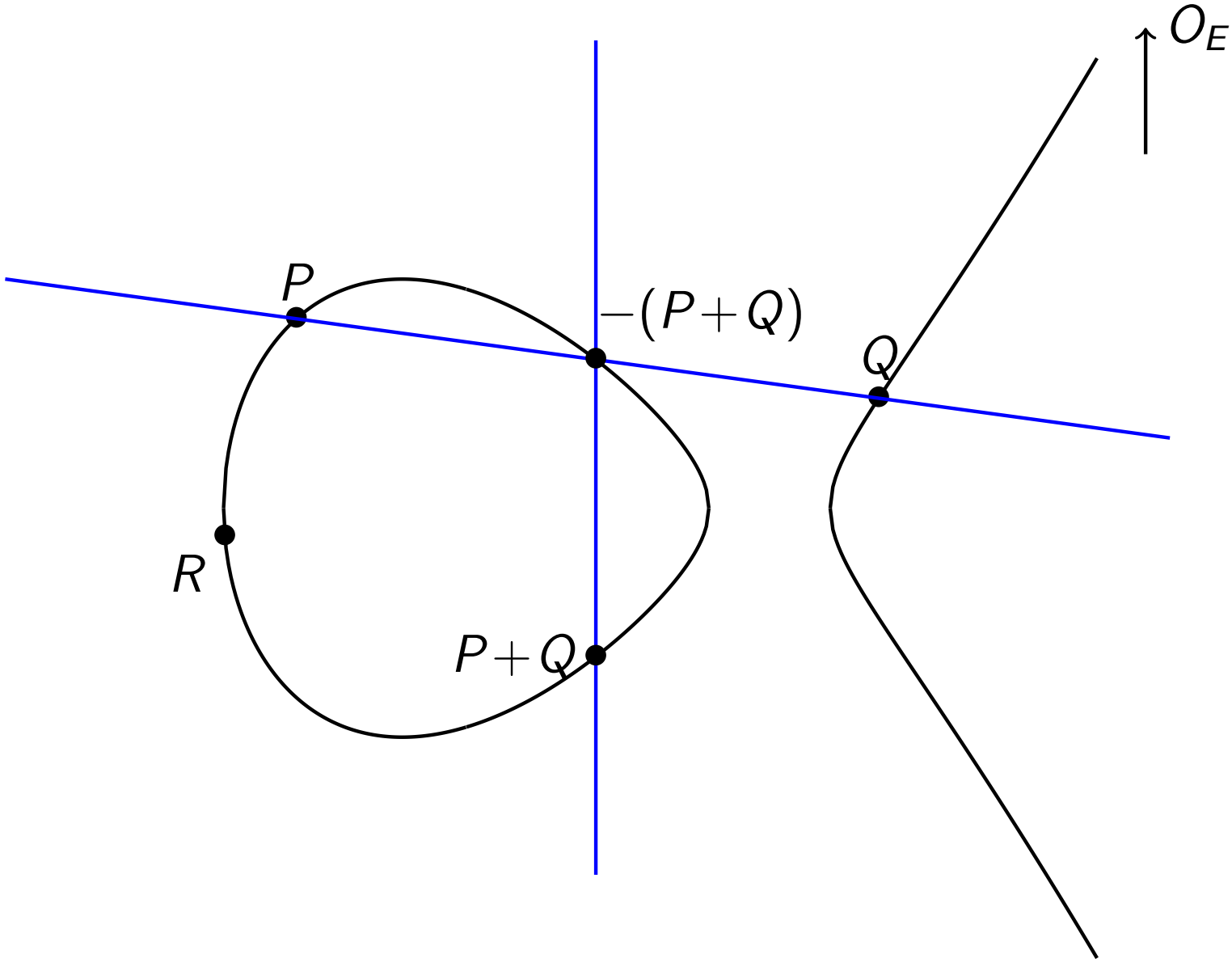
$$(P+Q)+R = P+(Q+R)$$

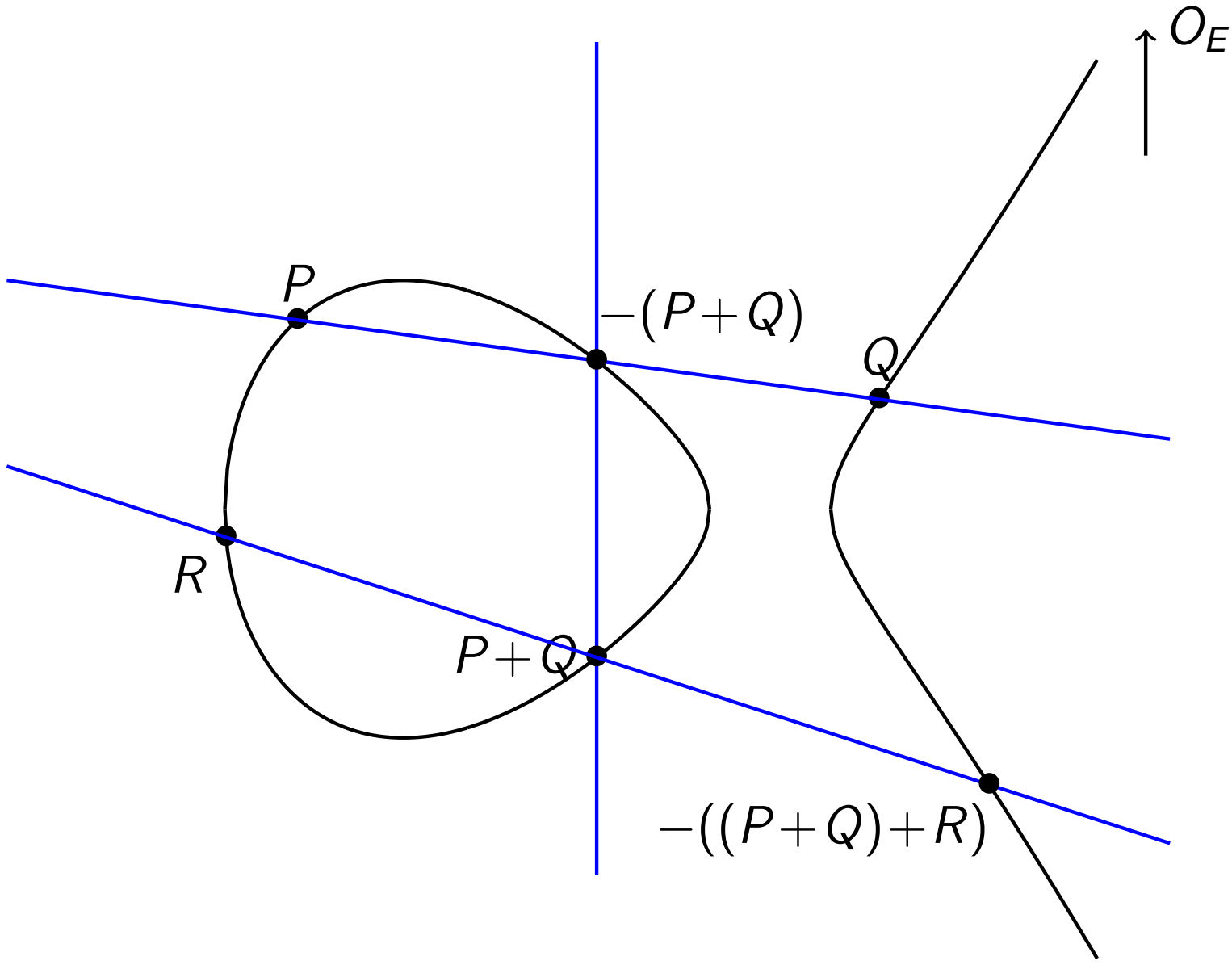


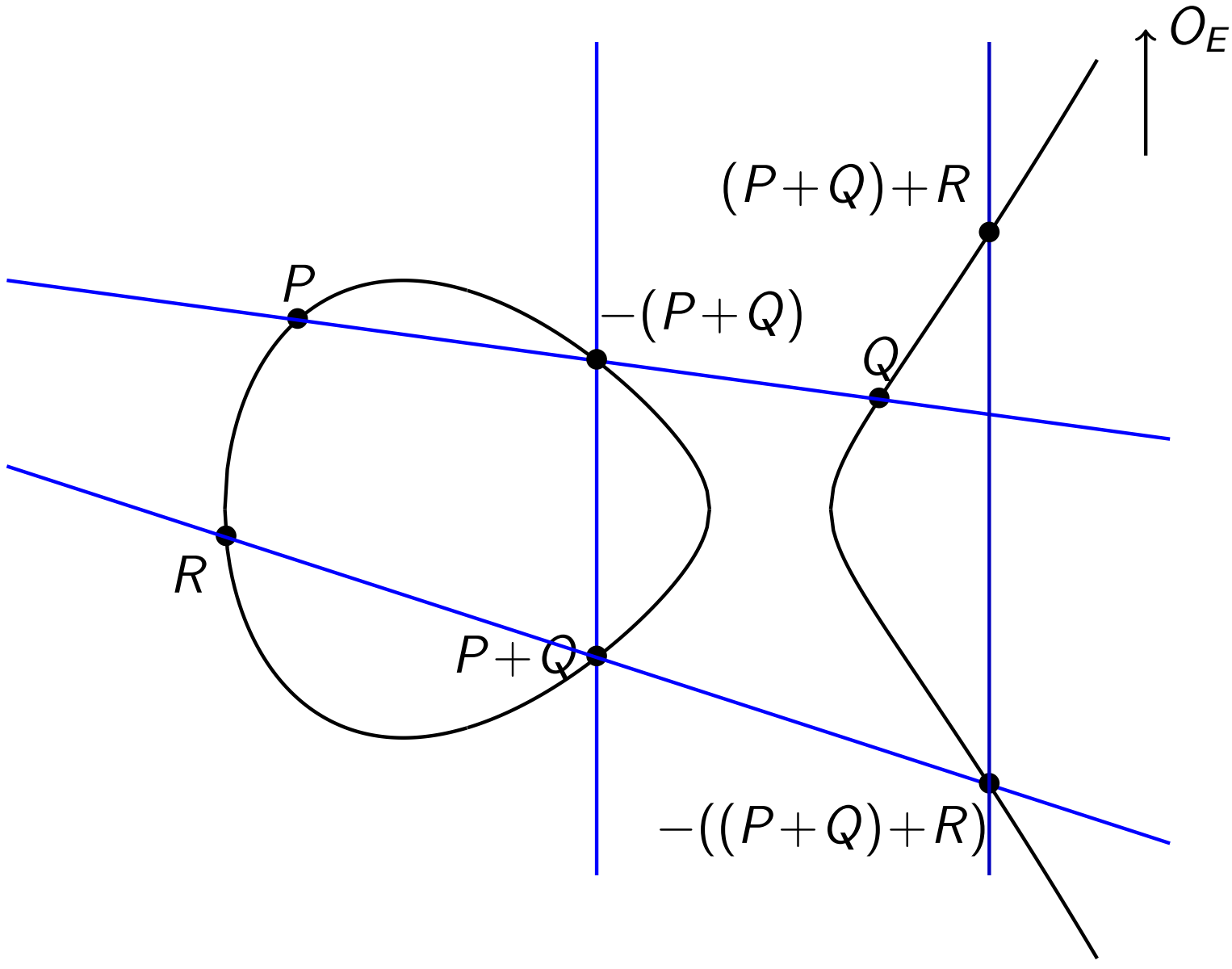
- associativité

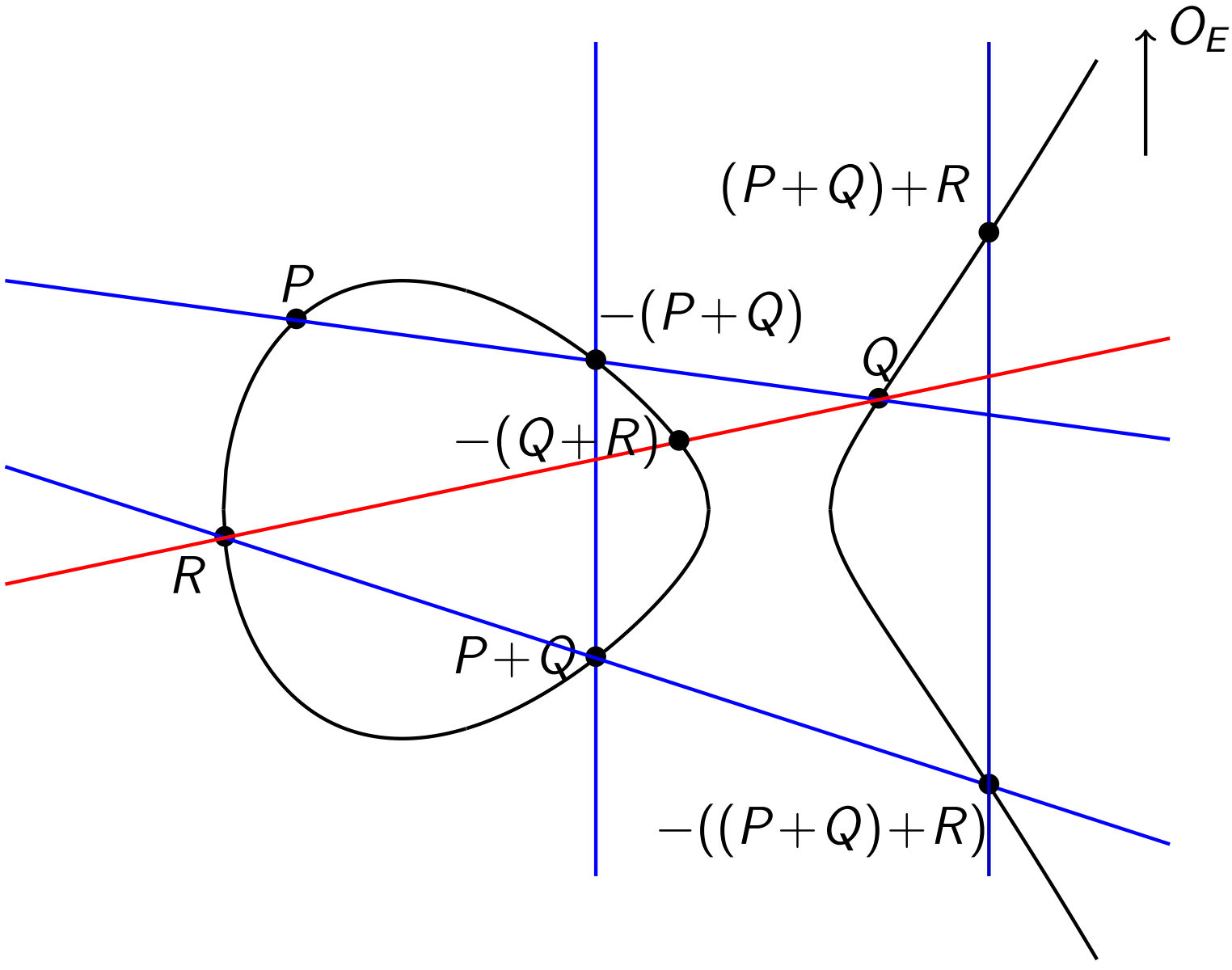
$$(P+Q)+R \overset{???}{=} P+(Q+R)$$

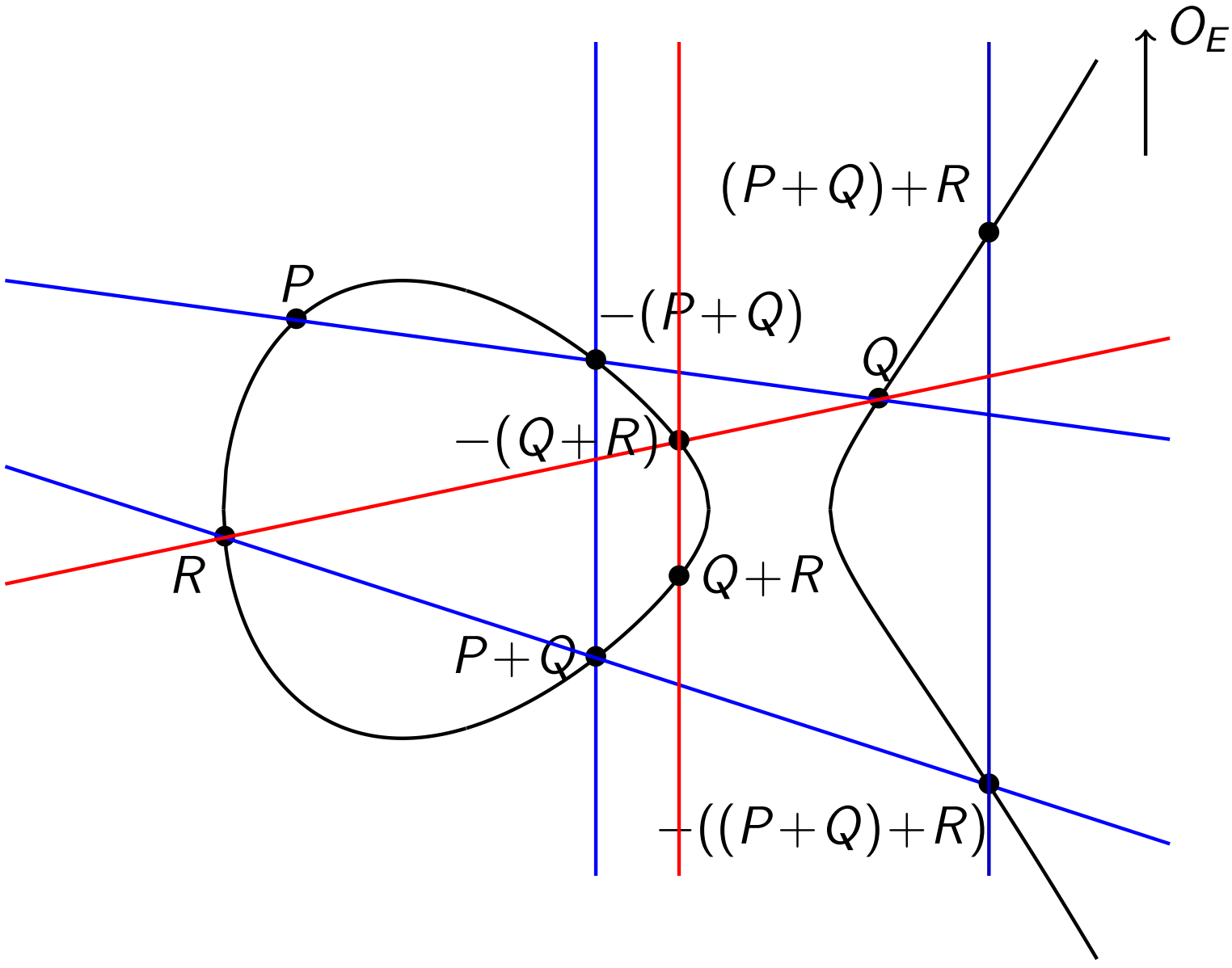

O_E
P
$-(P+Q)$
Q
$P+Q$

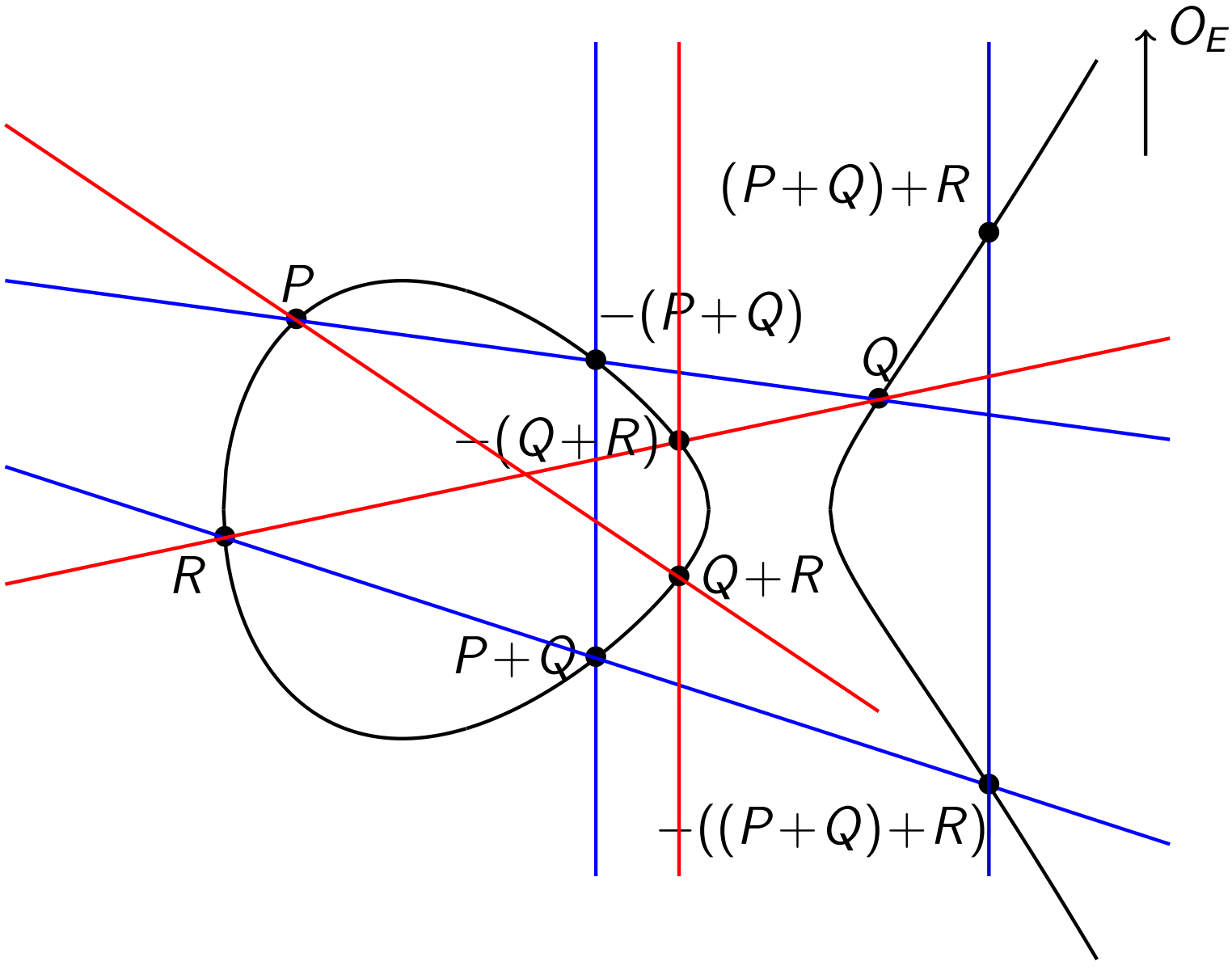

O_E
P
$-(P+Q)$
Q
R
$P+Q$

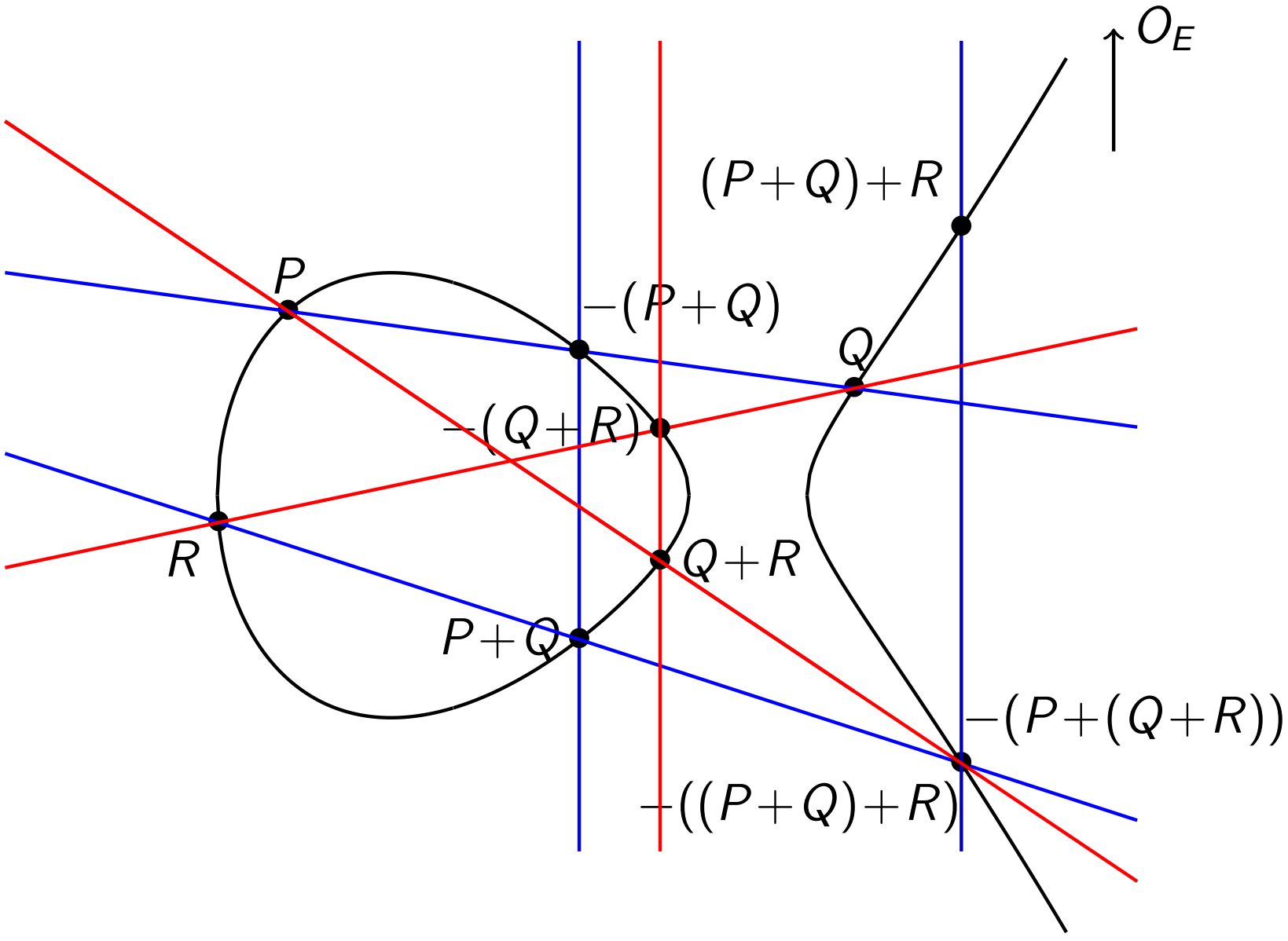

O_E
P
$-(P+Q)$
Q
R
$P+Q$
$-((P+Q)+R)$

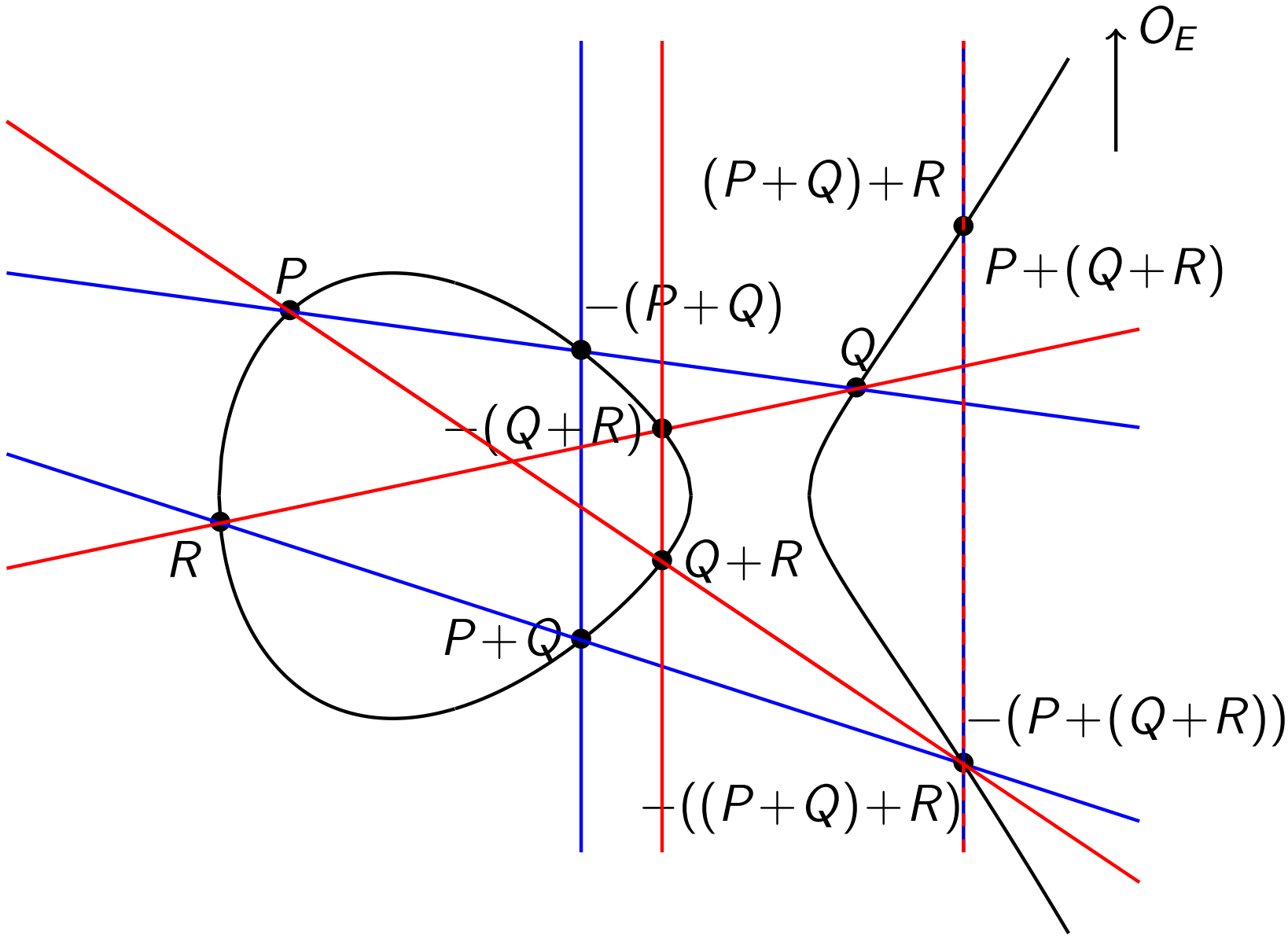

O_E
$(P+Q)+R$
P
$-(P+Q)$
Q
R
$P+Q$
$-((P+Q)+R)$

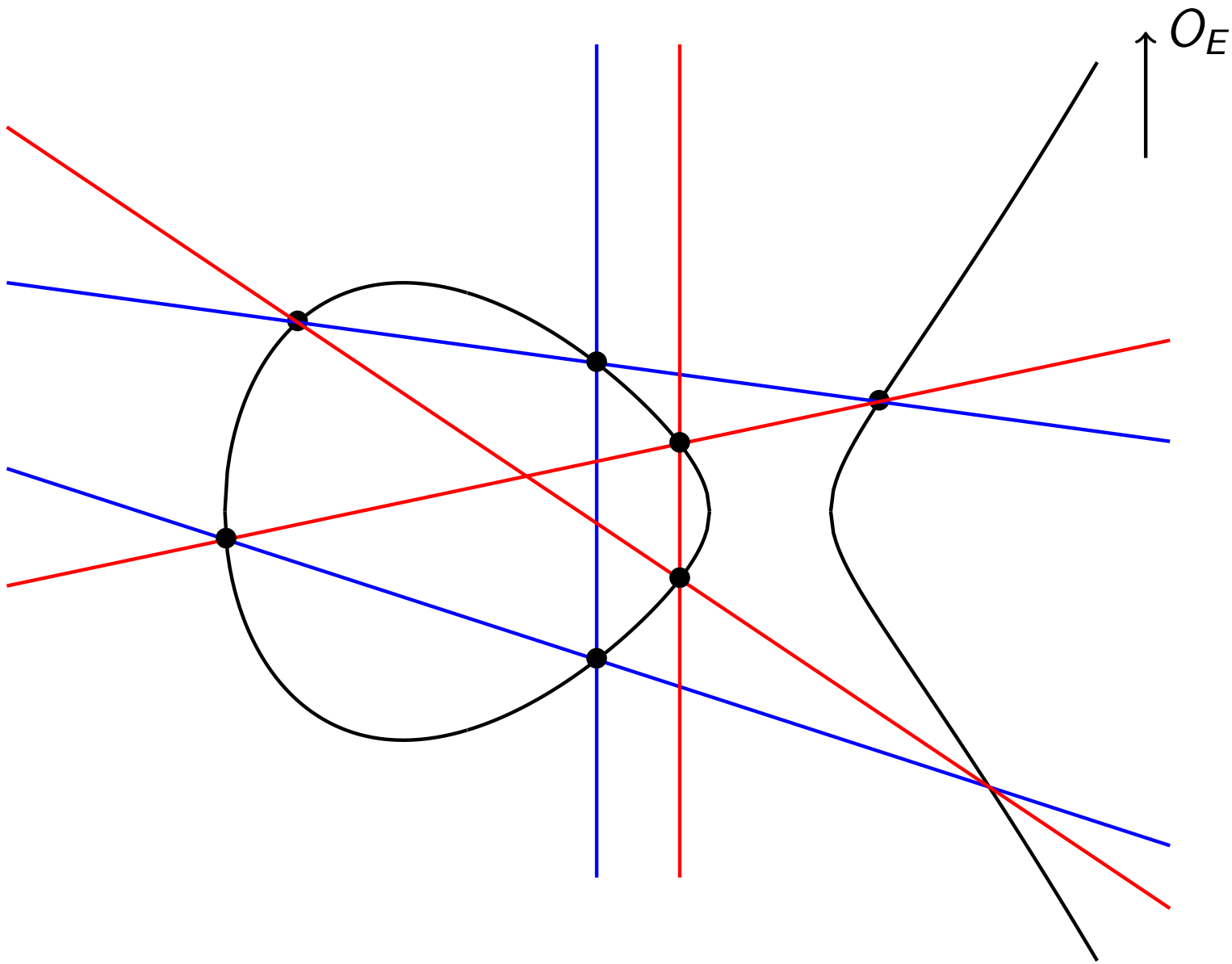

O_E
$(P+Q)+R$
P
$-(P+Q)$
Q
$-(Q+R)$
R
$P+Q$
$-((P+Q)+R)$

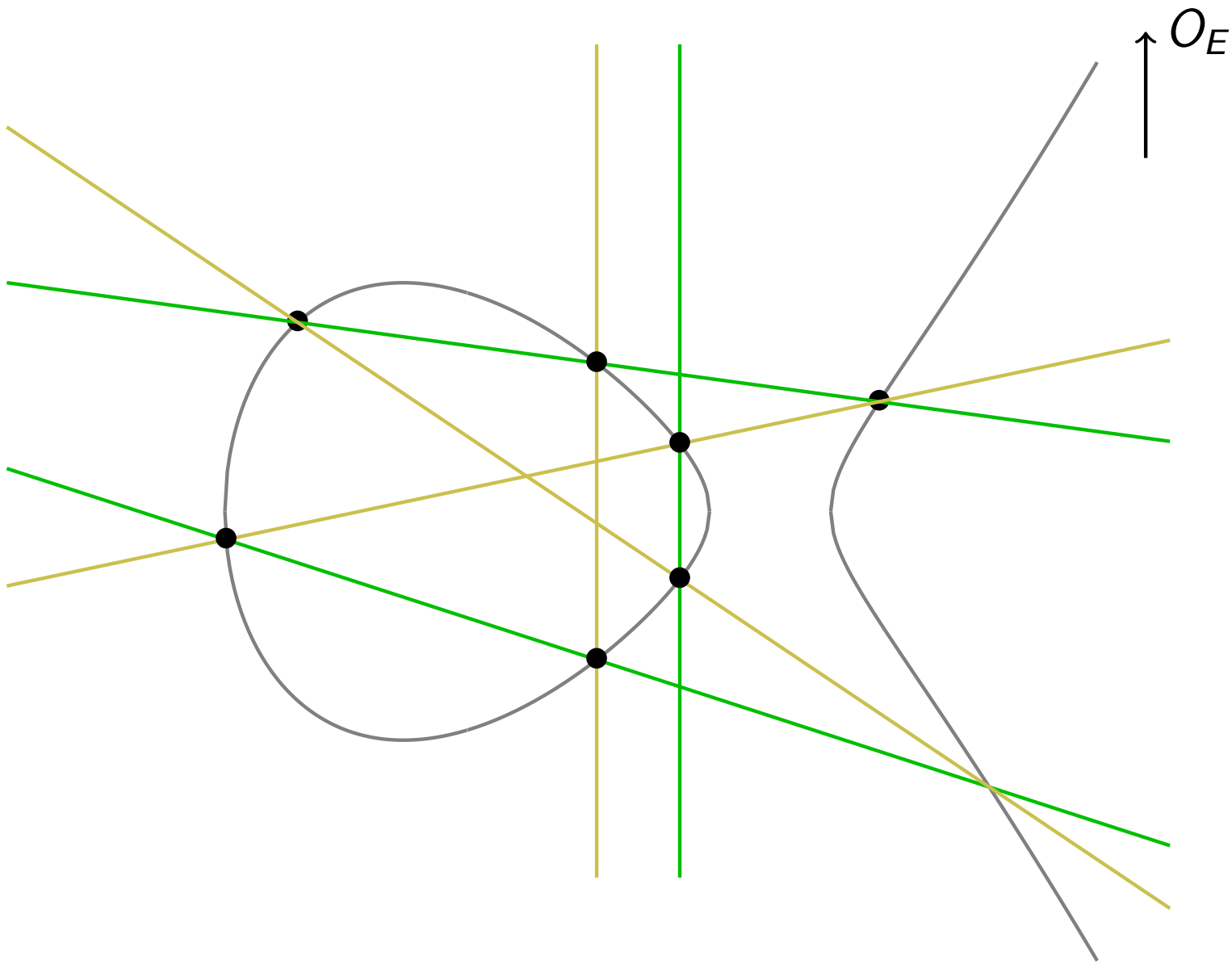

O_E
$(P+Q)+R$
P
$-(P+Q)$
Q
$-(Q+R)$
R
$Q+R$
$P+Q$
$-((P+Q)+R)$

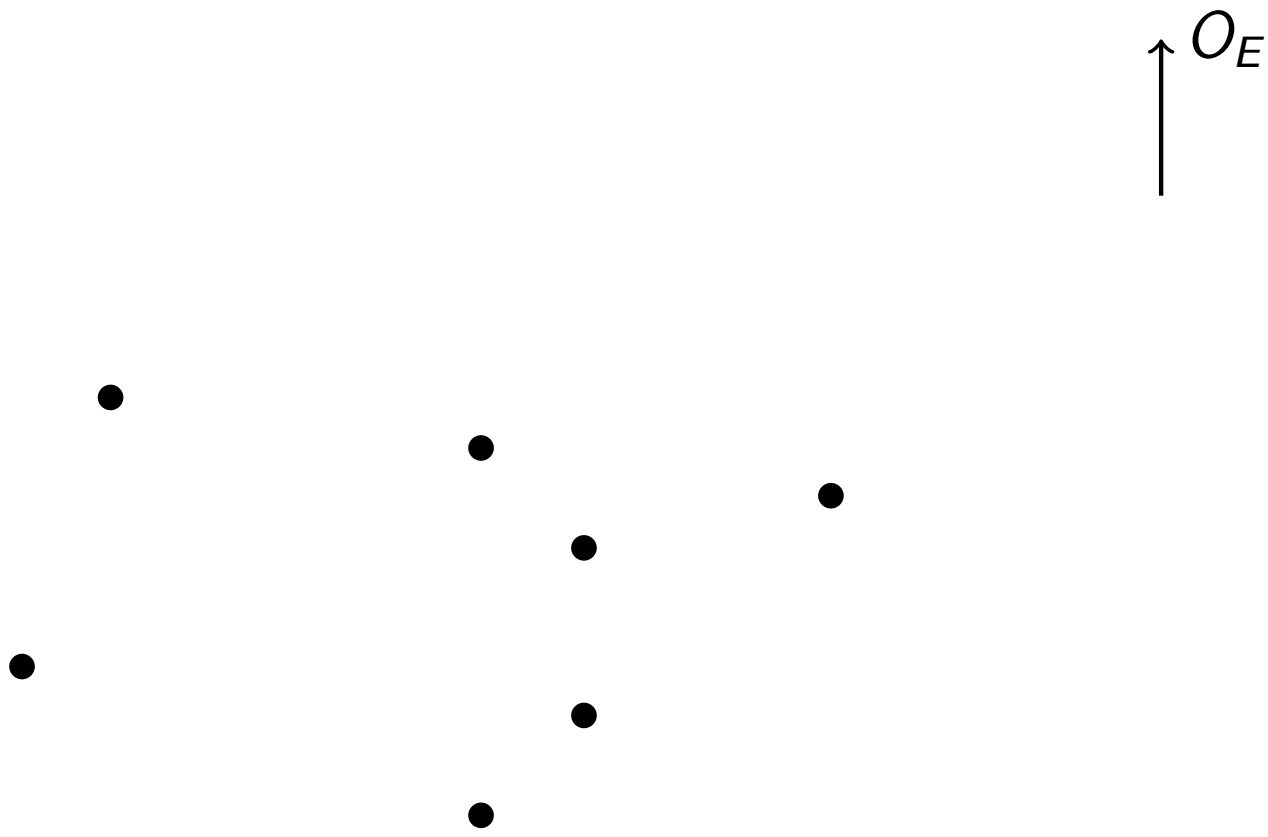

O_E
$(P+Q)+R$
P
$-(P+Q)$
Q
$-(Q+R)$
R
$Q+R$
$P+Q$
$-((P+Q)+R)$

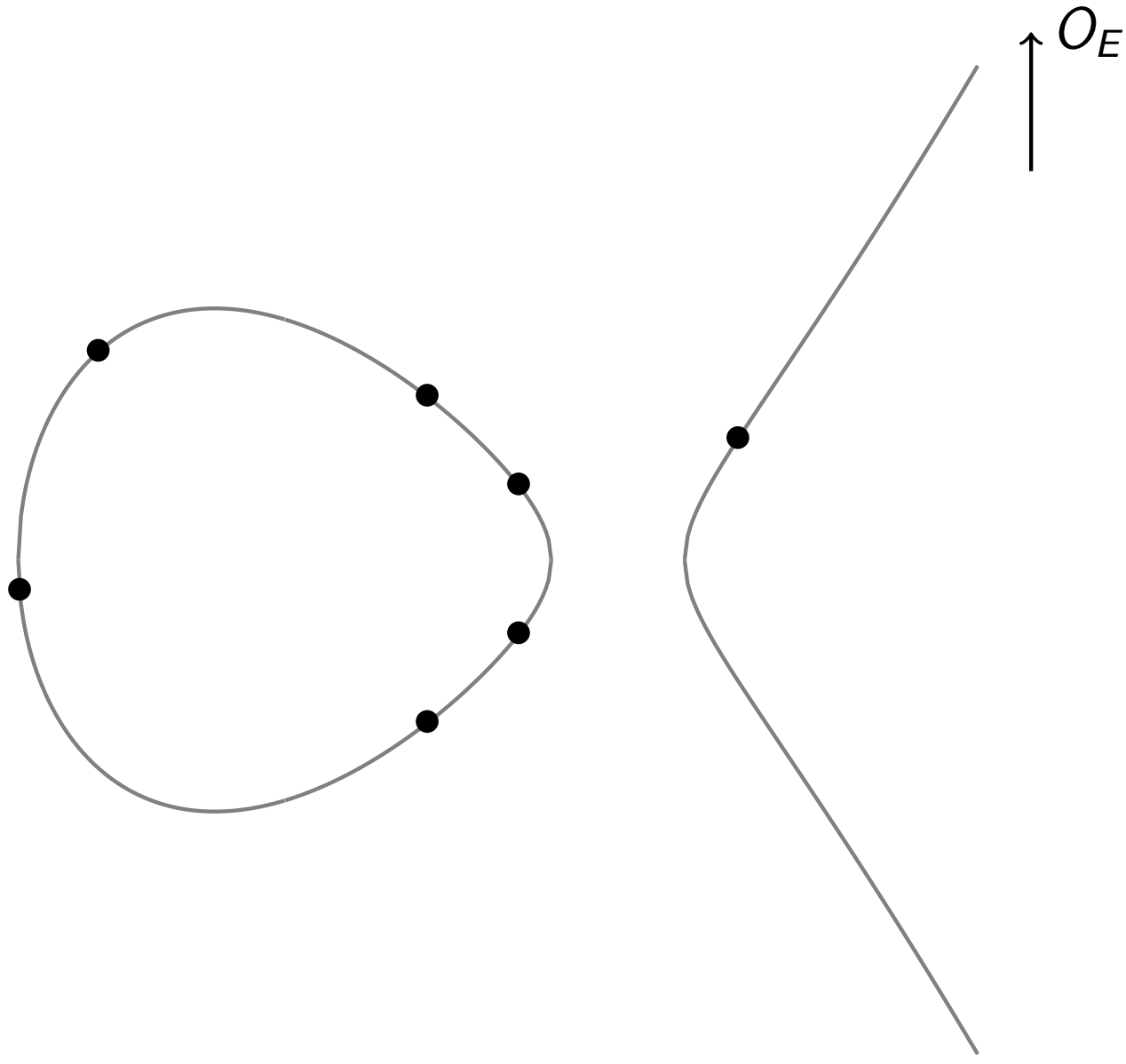

O_E
$(P+Q)+R$
P
$-(P+Q)$
Q
$-(Q+R)$
R
$Q+R$
$P+Q$
$-(P+(Q+R))$
$-((P+Q)+R)$

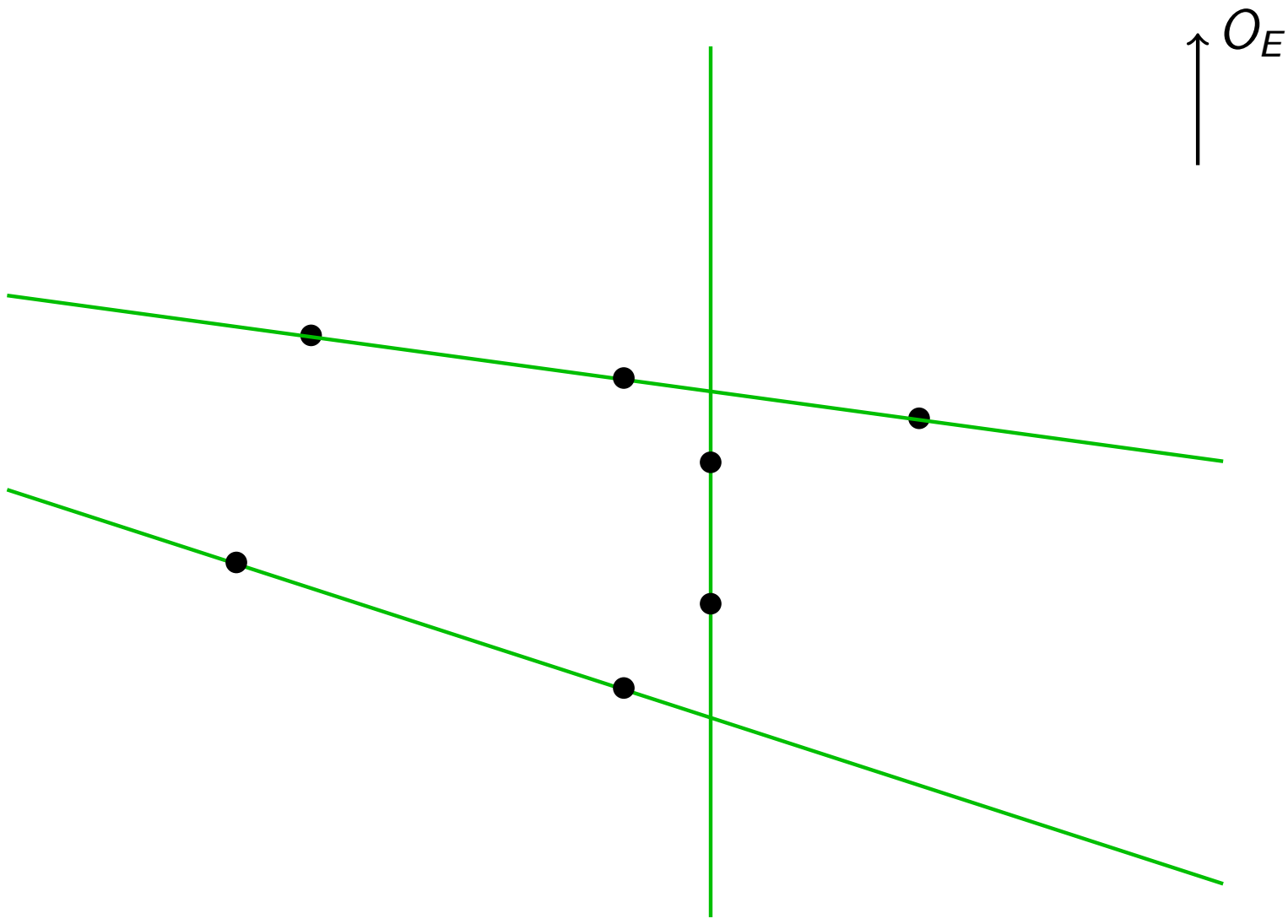

O_E
$(P+Q)+R$
$P+(Q+R)$
P
$-(P+Q)$
Q
$-(Q+R)$
R
$Q+R$
$P+Q$
$-(P+(Q+R))$
$-((P+Q)+R)$

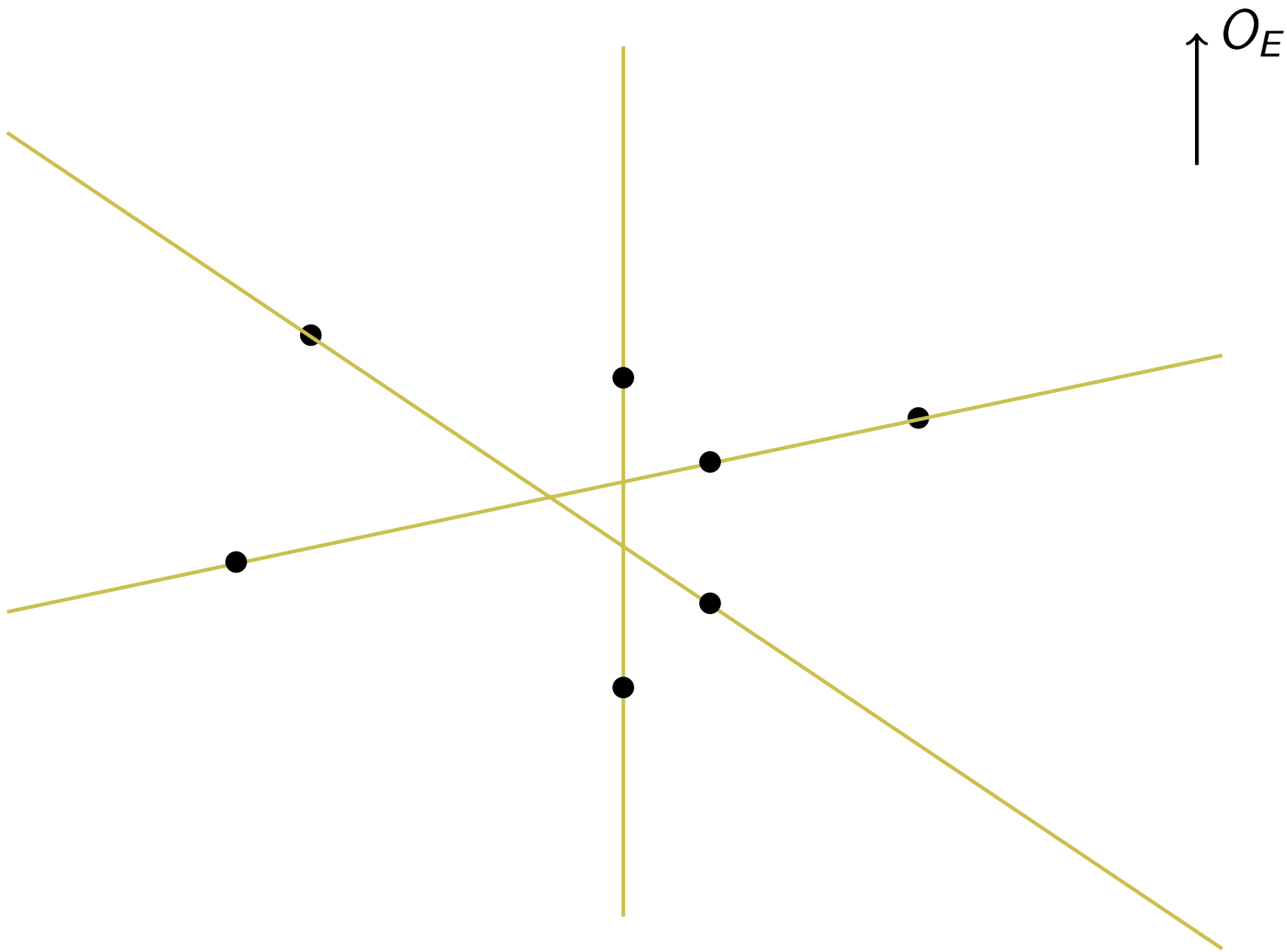

O_E

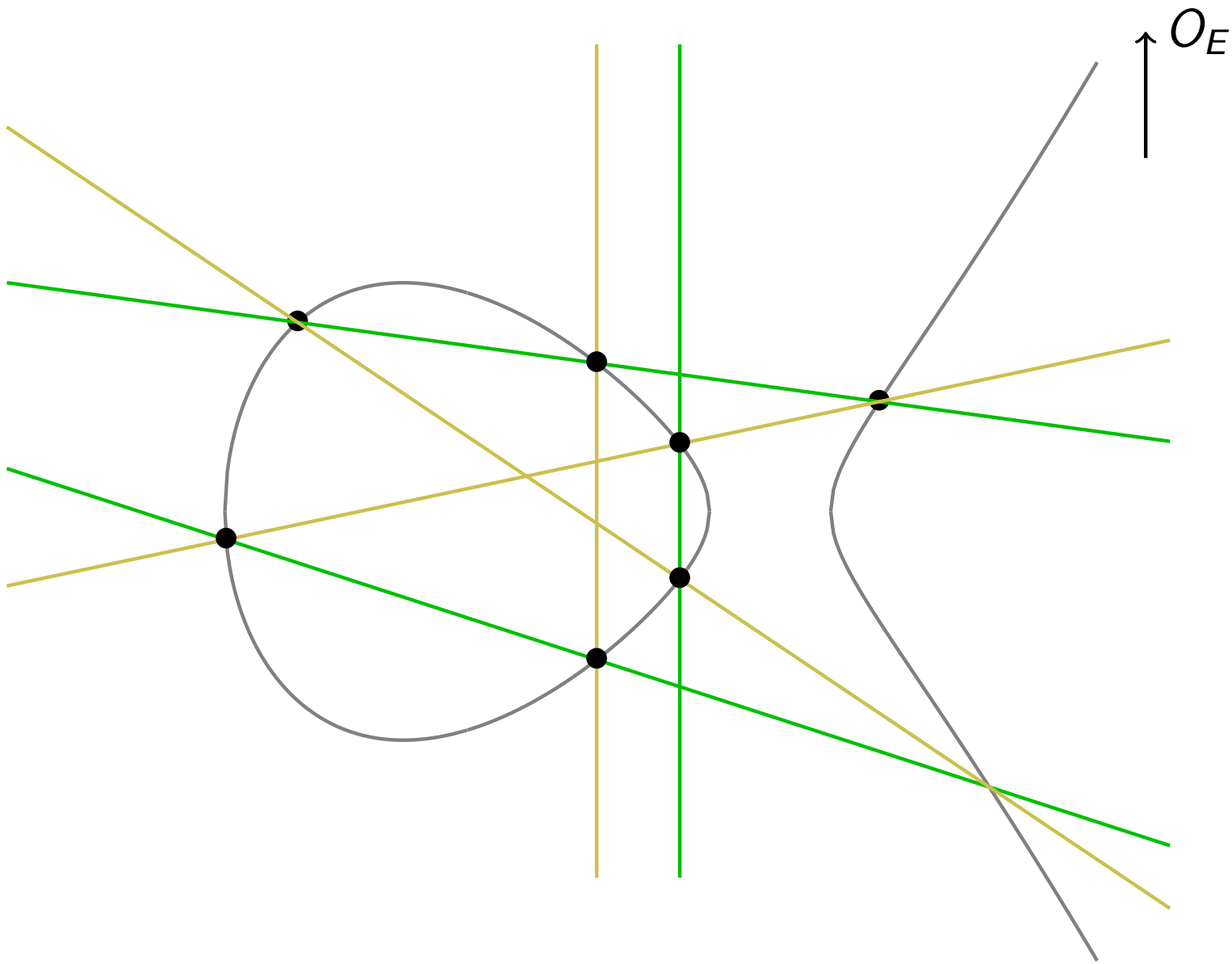

O_E


O_E


O_E


O_E


O_E


O_E

Dans le plan :

(1) la courbe E

(2) la réunion des trois droites vertes

(3) la réunion des trois droites kaki

Dans le plan :

(1) la courbe E

(2) la réunion des trois droites vertes

(3) la réunion des trois droites kaki

sont chacune définie par l'annulation d'un polynôme P_1, P_2, P_3 de degré 3 en deux variables, soit de la forme

$$\begin{aligned} & a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3 \\ & +a_5x^2 + a_6xy + a_7y^2 \\ & +a_8x + a_9y \\ & +a_{10}. \end{aligned}$$

Dans le plan :

(1) la courbe E

(2) la réunion des trois droites vertes

(3) la réunion des trois droites kaki

sont chacune définie par l'annulation d'un polynôme P_1, P_2, P_3 de degré 3 en deux variables, soit de la forme

$$\begin{gathered} a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3 \\ +a_5x^2 + a_6xy + a_7y^2 \\ +a_8x + a_9y \\ +a_{10}. \end{gathered}$$

La condition de passer par les huit points marqués (y compris O_E) donne huit relations linéaires sur $a_1, a_2, \ldots, a_{10}$.

Dans le plan :

(1) la courbe E

(2) la réunion des trois droites vertes

(3) la réunion des trois droites kaki

sont chacune définie par l'annulation d'un polynôme P_1, P_2, P_3 de degré 3 en deux variables, soit de la forme

$$\begin{aligned} & a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3 \\ & +a_5x^2 + a_6xy + a_7y^2 \\ & +a_8x + a_9y \\ & +a_{10}. \end{aligned}$$

La condition de passer par les huit points marqués (y compris O_E) donne huit relations linéaires sur $a_1, a_2, \ldots, a_{10}$.

- P_1, P_2, P_3 vivent dans un sous-espace de dimension 2.

Dans le plan :

(1) la courbe E

(2) la réunion des trois droites vertes

(3) la réunion des trois droites kaki

sont chacune définie par l'annulation d'un polynôme P_1, P_2, P_3 de degré 3 en deux variables, soit de la forme

$$\begin{gathered} a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3 \\ +a_5x^2 + a_6xy + a_7y^2 \\ +a_8x + a_9y \\ +a_{10}. \end{gathered}$$

La condition de passer par les huit points marqués (y compris O_E) donne huit relations linéaires sur $a_1, a_2, \ldots, a_{10}$.

- P_1, P_2, P_3 vivent dans un sous-espace de dimension 2.
- Ils sont liés.

Dans le plan :

(1) la courbe E

(2) la réunion des trois droites vertes

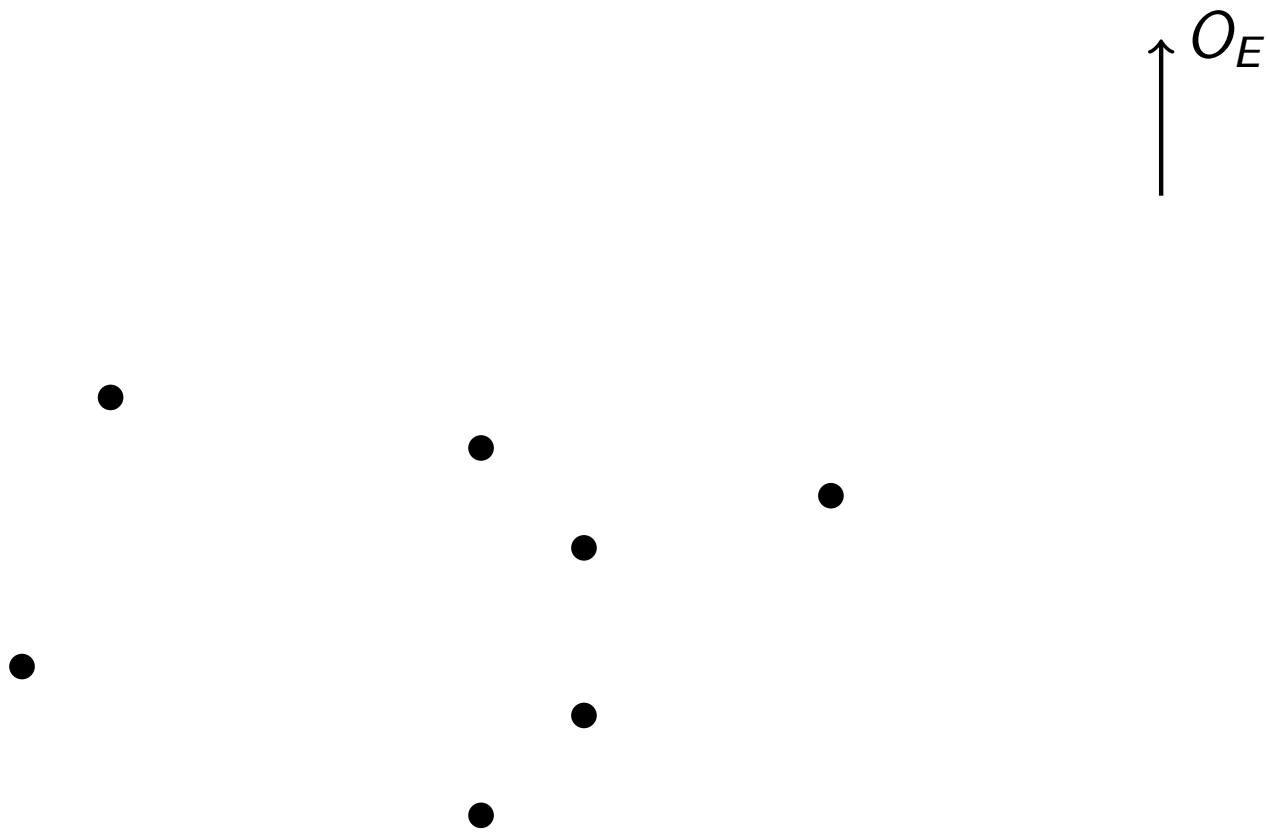
(3) la réunion des trois droites kaki

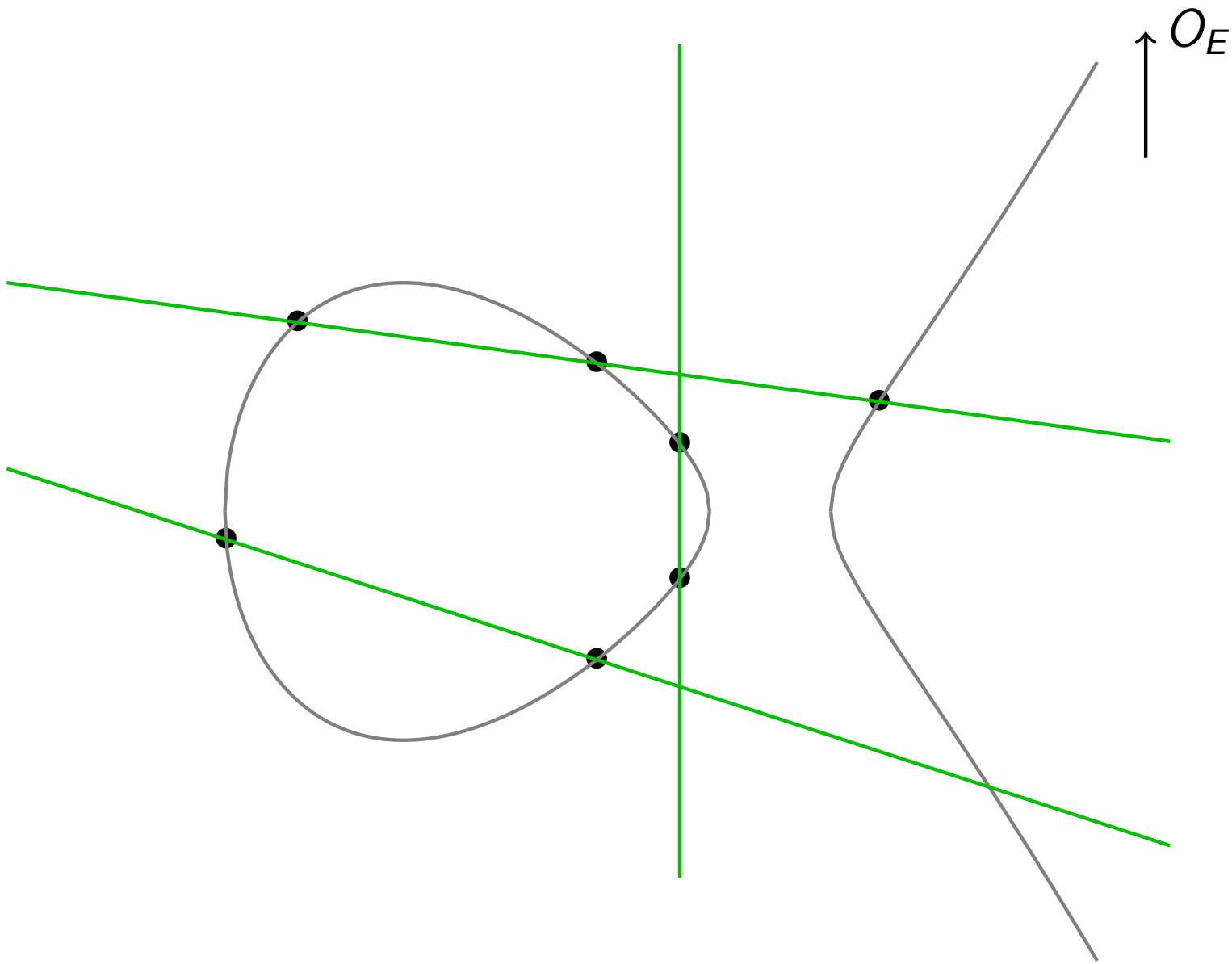
sont chacune définie par l'annulation d'un polynôme P_1, P_2, P_3 de degré 3 en deux variables, soit de la forme

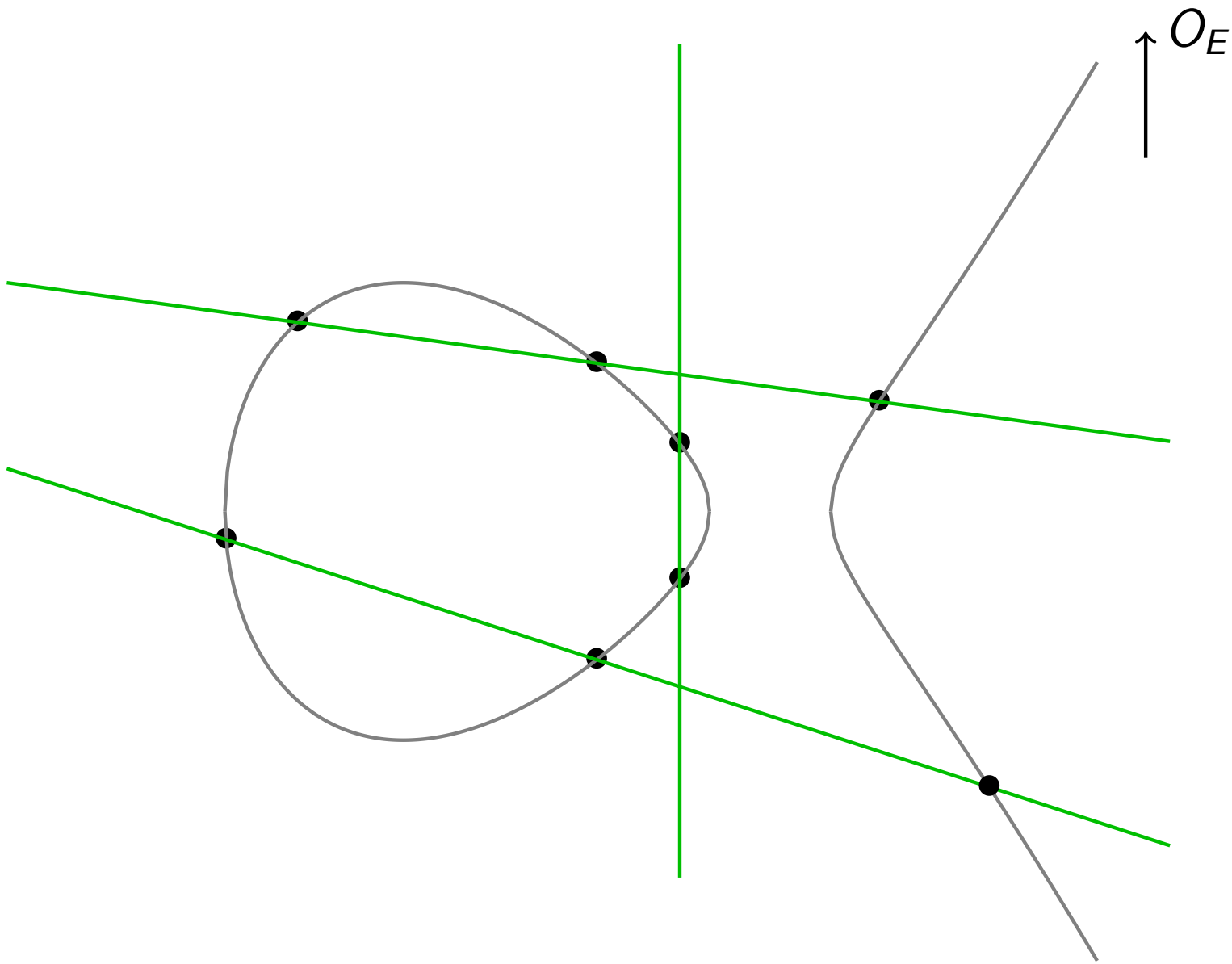
$$\begin{gathered} a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3 \\ +a_5x^2 + a_6xy + a_7y^2 \\ +a_8x + a_9y \\ +a_{10}. \end{gathered}$$

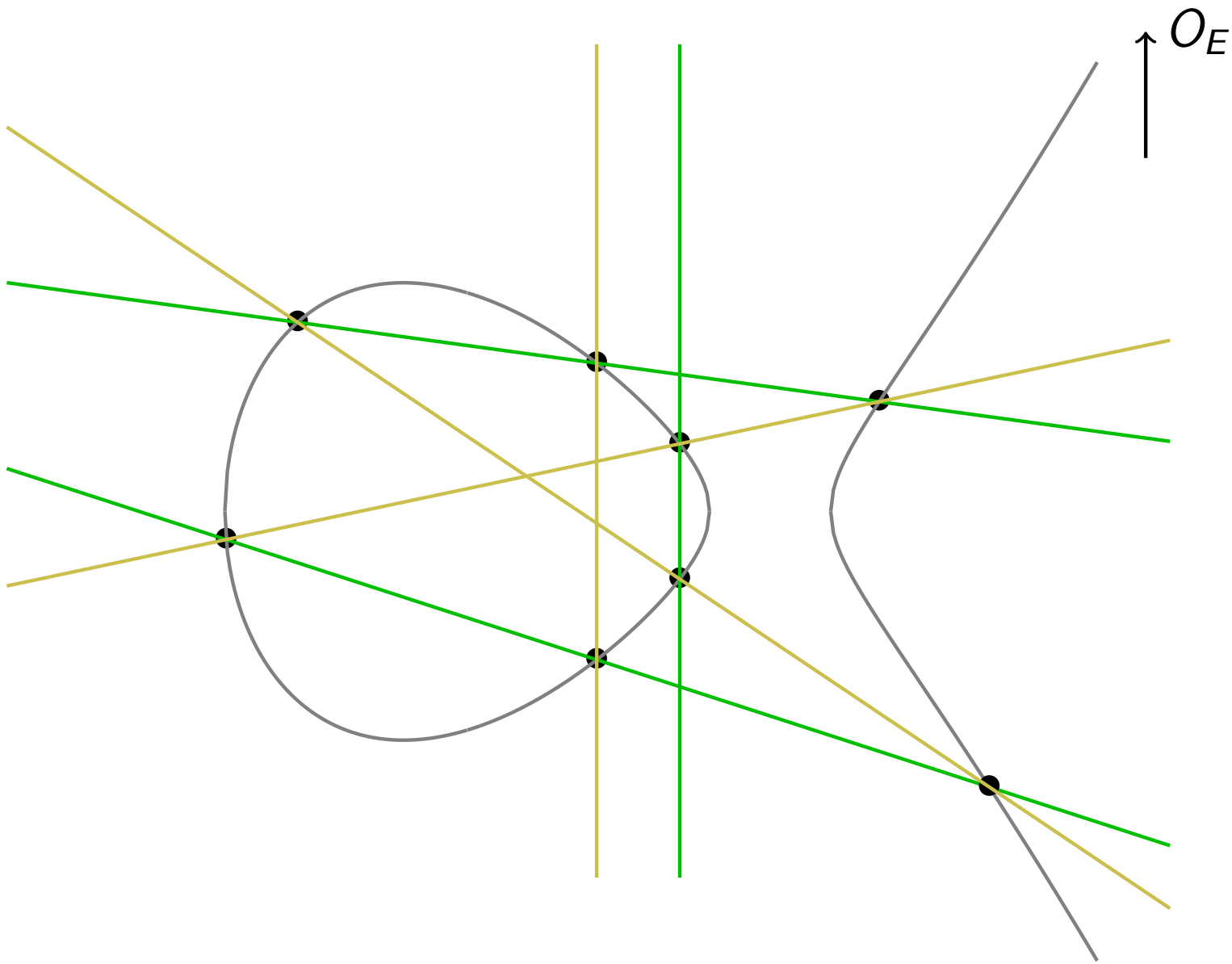
La condition de passer par les huit points marqués (y compris O_E) donne huit relations linéaires sur $a_1, a_2, \ldots, a_{10}$.

- P_1, P_2, P_3 vivent dans un sous-espace de dimension 2.
- Ils sont liés.
- Si P_1, P_2 ont un neuvième point d'annulation commun, alors P_3 aussi.


O_E


O_E


O_E


O_E

Codage

Dans cet exposé : codes correcteurs d'erreurs (linéaires).

Un code $[n, k, d]_{\mathbb{K}}$ est un sous-$\mathbb{K}$-espace vectoriel de $\mathbb{K}^n$ de dimension k, dont deux éléments distincts quelconques diffèrent toujours en au moins d positions.

Paramètres :

- longueur n
- dimension k
- rendement $R = k/n$
- distance minimale d
- capacité de correction $(d-1)/2$
- alphabet $\mathbb{K}$ (corps, e.g. $\mathbb{K} = \mathbb{F}_q$ fini)

Code de Hamming $[7,4,3]_{\mathbb{F}_2}$ = le sous-espace $\mathcal{C} \subseteq (\mathbb{F}_2)^7$ engendré par les lignes de la matrice

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\mathcal{C} = \{0000000,\ 1000110,\ 0100101,\ 1100011,\ 0010011,$$
$$1010101,\ 0110110,\ 1110000,\ 0001111,\ 1001001,\ 0101010,$$
$$1101100,\ 0011100,\ 1011010,\ 0111001,\ 1111111\}$$

Code de Hamming $[7,4,3]_{\mathbb{F}_2}$ = le sous-espace $\mathcal{C} \subseteq (\mathbb{F}_2)^7$ engendré par les lignes de la matrice

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\mathcal{C} = \{0000000,\ 1000110,\ 0100101,\ 1100011,\ 0010011,\ 1010101,\ 0110110,\ 1110000,\ 0001111,\ 1001001,\ 0101010,\ 1101100,\ 0011100,\ 1011010,\ 0111001,\ 1111111\}$$

Alice veut envoyer un message $\mathbf{m} \in (\mathbb{F}_2)^4$, elle calcule $\mathbf{c} = \mathbf{mG}$ et l'envoie à Bob.

Code de Hamming $[7,4,3]_{\mathbb{F}_2}$ = le sous-espace $\mathcal{C} \subseteq (\mathbb{F}_2)^7$ engendré par les lignes de la matrice

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\mathcal{C} = \{0000000,\ 1000110,\ 0100101,\ 1100011,\ 0010011,\ 1010101,\ 0110110,\ 1110000,\ 0001111,\ 1001001,\ 0101010,\ 1101100,\ 0011100,\ 1011010,\ 0111001,\ 1111111\}$$

Alice veut envoyer un message $\mathbf{m} \in (\mathbb{F}_2)^4$, elle calcule $\mathbf{c} = \mathbf{mG}$ et l'envoie à Bob.
Bob reçoit un mot bruité $\mathbf{c}' = (1001010)$.

Code de Hamming $[7,4,3]_{\mathbb{F}_2}$ = le sous-espace $\mathcal{C} \subseteq (\mathbb{F}_2)^7$ engendré par les lignes de la matrice

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\mathcal{C} = \{0000000,\ 1000110,\ 0100101,\ 1100011,\ 0010011,\ 1010101,\ 0110110,\ 1110000,\ 0001111,\ 1001001,\ 0101010,\ 1101100,\ 0011100,\ 1011010,\ 0111001,\ 1111111\}$$

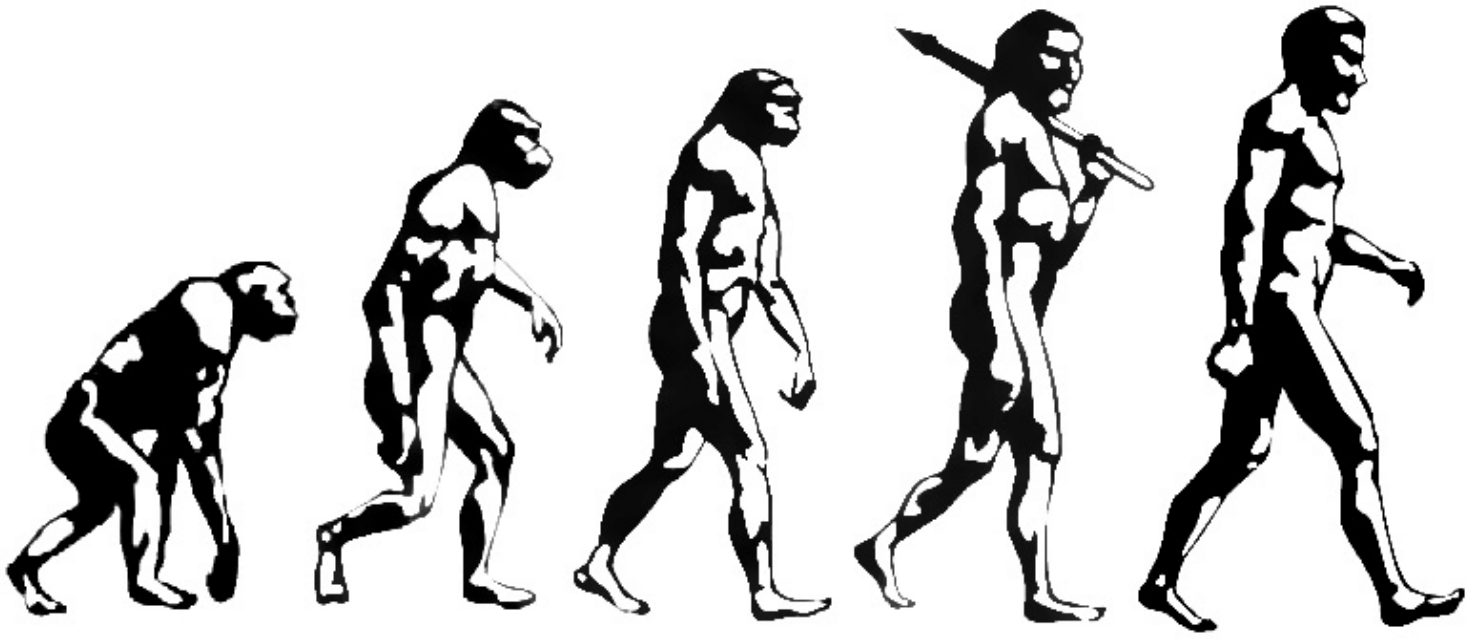
Alice veut envoyer un message $\mathbf{m} \in (\mathbb{F}_2)^4$, elle calcule $\mathbf{c} = \mathbf{mG}$ et l'envoie à Bob.
Bob reçoit un mot bruité $\mathbf{c}' = (1001010)$.
Dans $\mathcal{C}$ il y a un unique mot à distance 1 de $\mathbf{c}'$, Bob le retrouve et en déduit $\mathbf{m} = (1011)$.

Historique succint

- Shannon (1948) $\leftarrow$ probabilités
- Hamming, Golay (1948-1950), ... MacWilliams (1960's), ... $\leftarrow$ algèbre et combinatoire
- Manin, Goppa (1970's), Vladut, Tsfasman (1980's), ... $\leftarrow$ arithmétique et géométrie algébrique

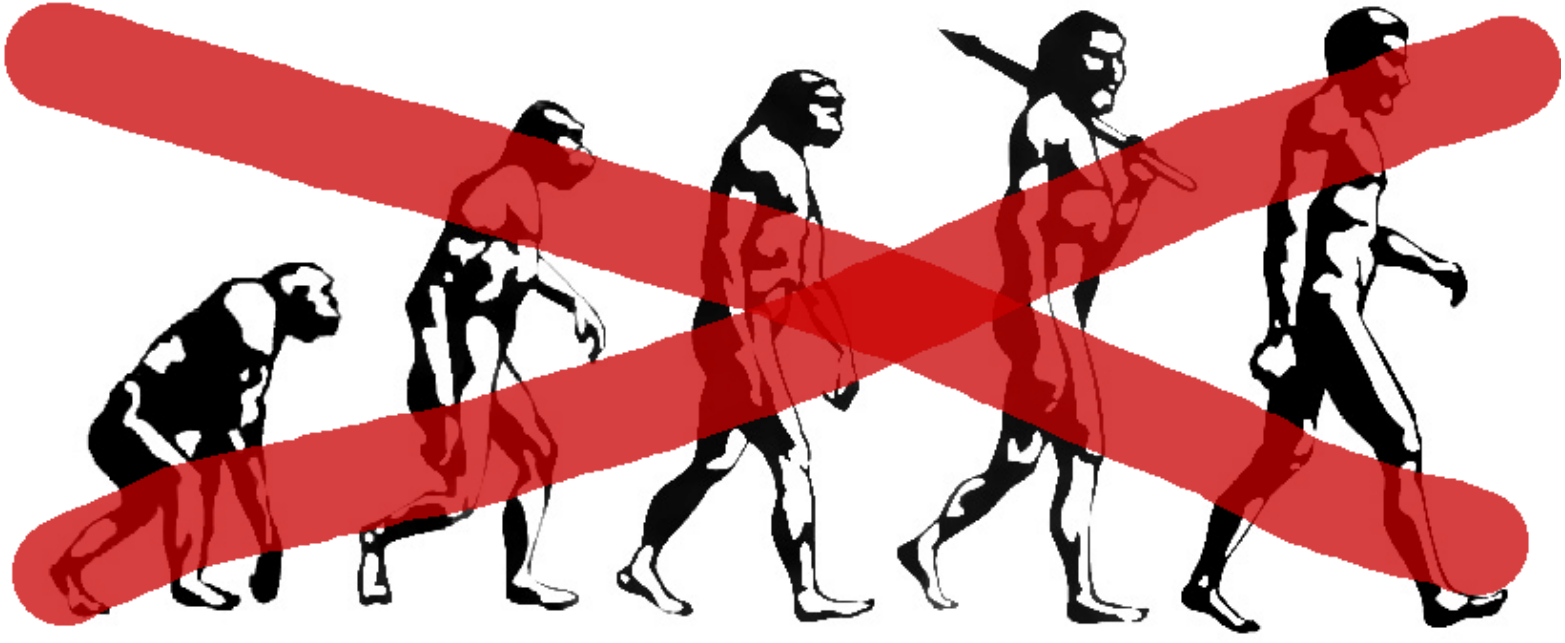
Historique succint

- Shannon (1948) $\leftarrow$ probabilités
- Hamming, Golay (1948-1950), ... MacWilliams (1960's), ... $\leftarrow$ algèbre et combinatoire
- Manin, Goppa (1970's), Vladut, Tsfasman (1980's), ... $\leftarrow$ arithmétique et géométrie algébrique



Historique succint

- Shannon (1948) $\leftarrow$ probabilités
- Hamming, Golay (1948-1950), ... MacWilliams (1960's), ... $\leftarrow$ algèbre et combinatoire
- Manin, Goppa (1970's), Vladut, Tsfasman (1980's), ... $\leftarrow$ arithmétique et géométrie algébrique



Problème fondamental : n donné, on voudrait avoir à la fois k et d grands.

Shannon, Gilbert-Varshamov : pour $n \to \infty$, on obtient de très bons codes en les tirant au hasard.

Pour n petit, on a de bonnes constructions algébriques.
Reed-Solomon : soient $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ distincts,

$$\begin{array}{ccc} \mathbb{K}[X]_{\leq k-1} & \longrightarrow & \mathbb{K}^n \\ P & \mapsto & (P(\alpha_1), \ldots, P(\alpha_n)). \end{array}$$

L'image de cette application est un code $[n, k, d = n-k+1]$ (preuve : un polynôme de degré $\leq k-1$ admet $\leq k-1$ racines).

C'est optimal ! (borne de Singleton)

Problème : si $\mathbb{K} = \mathbb{F}_q$ corps fini, ne fonctionne que pour $n \leq q$ (ou plutôt $n \leq q+1$).

Solution : au lieu d'évaluer des polynômes sur $\mathbb{P}^1$, on évalue des fonctions sur une courbe de genre plus élevé (Goppa).

Donnés :

- X une courbe sur $\mathbb{F}_q$ de genre g
- $\mathcal{P} = \{P_1, \ldots, P_n\}$ n points de X sur $\mathbb{F}_q$
- D un diviseur de degré m sur X

avec $g \leq m < n$.

Soient $\mathcal{L}(D)$ l'espace des fonctions sur X de pôles au plus D, et $\mathcal{C}(D, \mathcal{P})$ l'image de l'application d'évaluation

$$\begin{array}{ccc} \mathcal{L}(D) & \to & (\mathbb{F}_q)^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)). \end{array}$$

Alors $\mathcal{C}(D, \mathcal{P})$ est un code de paramètres

- $k = \dim \mathcal{L}(D) \geq m + 1 - g$ (Riemann-Roch)
- $d \geq n - m$.

Remarque : on est à g de la borne de Singleton

$$n + 1 - g \leq k + d \leq n + 1.$$

Par des résultats profonds d'arithmétique, on montre qu'il existe des courbes ayant un nombre de points qui croît linéairement avec g.
P.ex. $n \approx (p-1)g$ si $q = p^2$, ce qui permet de battre la borne probabiliste dès que $p \geq 7$.

Algorithmes de multiplication

(et calcul réparti / partage de secret arithmétique)

$$
\begin{array}{rrrrr}
 & & 2 & 0 & 1 & 8 \\
\times & & 1 & 7 & 2 & 9 \\
\hline
 & & & & & \\
 & & & & & \\
 & & & & & \\
\hline
\end{array}
$$

$$
\begin{array}{rcccc}
 & 2 & 0 & 1 & \mathbf{8} \\
\times & 1 & 7 & 2 & \mathbf{9} \\
\hline
 & & & 7 & 2 \\
 & & & & \\
 & & & & \\
\hline
\end{array}
$$

$8 \bullet 9 = 72,$

$$
\begin{array}{rcccc}
 & 2 & 0 & \mathbf{1} & 8 \\
\times & 1 & 7 & 2 & \mathbf{9} \\
\hline
 & & 1 & 6 & 2 \\
 & & & & \\
 & & & & \\
\hline
\end{array}
$$

$8 \bullet 9 = 72, \quad 1 \bullet 9 = 9,$

$$
\begin{array}{rcccc}
 & 2 & \mathbf{0} & 1 & 8 \\
\times & 1 & 7 & 2 & \mathbf{9} \\
\hline
 & & 1 & 6 & 2 \\
 & & & & \\
 & & & & \\
\hline
\end{array}
$$

$8 \bullet 9 = 72, \quad 1 \bullet 9 = 9, \quad 0 \bullet 9 = 0,$

$$
\begin{array}{rcccc}
 & & \mathbf{2} & 0 & 1 & 8 \\
\times & & 1 & 7 & 2 & \mathbf{9} \\
\hline
 & 1 & 8 & 1 & 6 & 2 \\
 & & & & & \\
 & & & & & \\
\hline
\end{array}
$$

$8 \bullet 9 = 72, \quad 1 \bullet 9 = 9, \quad 0 \bullet 9 = 0, \quad 2 \bullet 9 = 18$

$$
\begin{array}{rrrrrr}
 & & & 2 & 0 & 1 & \mathbf{8} \\
\times & & & 1 & 7 & \mathbf{2} & 9 \\
\hline
 & & 1 & 8 & 1 & 6 & 2 \\
 & & & & 1 & 6 & \\
 & & & & & & \\
 & & & & & & \\
\hline
\end{array}
$$

$8 \bullet 9 = 72, \quad 1 \bullet 9 = 9, \quad 0 \bullet 9 = 0, \quad 2 \bullet 9 = 18$
$8 \bullet 2 = 16,$

$$
\begin{array}{rcccc}
 & 2 & 0 & \mathbf{1} & 8 \\
\times & 1 & 7 & \mathbf{2} & 9 \\
\hline
1 & 8 & 1 & 6 & 2 \\
 & & 3 & 6 & \\
 & & & & \\
 & & & & \\
\hline
\end{array}
$$

$8 \bullet 9 = 72, \quad 1 \bullet 9 = 9, \quad 0 \bullet 9 = 0, \quad 2 \bullet 9 = 18$
$8 \bullet 2 = 16, \quad 1 \bullet 2 = 2,$

$$
\begin{array}{rrrrr}
 & & 2 & \mathbf{0} & 1 & 8 \\
\times & & 1 & 7 & \mathbf{2} & 9 \\
\hline
 & 1 & 8 & 1 & 6 & 2 \\
 & & 0 & 3 & 6 & \\
 & & & & & \\
 & & & & & \\
\hline
\end{array}
$$

$8 \bullet 9 = 72, \quad 1 \bullet 9 = 9, \quad 0 \bullet 9 = 0, \quad 2 \bullet 9 = 18$

$8 \bullet 2 = 16, \quad 1 \bullet 2 = 2, \quad 0 \bullet 2 = 0,$

$$
\begin{array}{rcccc}
 & & \mathbf{2} & 0 & 1 & 8 \\
\times & & 1 & 7 & \mathbf{2} & 9 \\
\hline
 & 1 & 8 & 1 & 6 & 2 \\
 & 4 & 0 & 3 & 6 & \\
 & & & & & \\
 & & & & & \\
\hline
\end{array}
$$

$8 \bullet 9 = 72, \quad 1 \bullet 9 = 9, \quad 0 \bullet 9 = 0, \quad 2 \bullet 9 = 18$

$8 \bullet 2 = 16, \quad 1 \bullet 2 = 2, \quad 0 \bullet 2 = 0, \quad 2 \bullet 2 = 4$

$$
\begin{array}{cccccc}
 & & & 2 & 0 & 1 & \mathbf{8} \\
\times & & & 1 & \mathbf{7} & 2 & 9 \\
\hline
 & & 1 & 8 & 1 & 6 & 2 \\
 & & 4 & 0 & 3 & 6 & \\
 & & & 5 & 6 & & \\
 & & & & & & \\
\hline
\end{array}
$$

$8 \bullet 9 = 72, \quad 1 \bullet 9 = 9, \quad 0 \bullet 9 = 0, \quad 2 \bullet 9 = 18$

$8 \bullet 2 = 16, \quad 1 \bullet 2 = 2, \quad 0 \bullet 2 = 0, \quad 2 \bullet 2 = 4$

$8 \bullet 7 = 56,$

$$
\begin{array}{rcccc}
 & 2 & 0 & \mathbf{1} & 8 \\
\times & 1 & \mathbf{7} & 2 & 9 \\
\hline
1 & 8 & 1 & 6 & 2 \\
4 & 0 & 3 & 6 & \\
1 & 2 & 6 & & \\
\hline
\end{array}
$$

$8 \bullet 9 = 72, \quad 1 \bullet 9 = 9, \quad 0 \bullet 9 = 0, \quad 2 \bullet 9 = 18$

$8 \bullet 2 = 16, \quad 1 \bullet 2 = 2, \quad 0 \bullet 2 = 0, \quad 2 \bullet 2 = 4$

$8 \bullet 7 = 56, \quad 1 \bullet 7 = 7,$

$$
\begin{array}{rrrrrr}
 & & & 2 & \mathbf{0} & 1 & 8 \\
\times & & & 1 & \mathbf{7} & 2 & 9 \\
\hline
 & & 1 & 8 & 1 & 6 & 2 \\
 & & 4 & 0 & 3 & 6 & \\
 & & 1 & 2 & 6 & & \\
 & & & & & & \\
\hline
\end{array}
$$

$8 \bullet 9 = 72, \quad 1 \bullet 9 = 9, \quad 0 \bullet 9 = 0, \quad 2 \bullet 9 = 18$

$8 \bullet 2 = 16, \quad 1 \bullet 2 = 2, \quad 0 \bullet 2 = 0, \quad 2 \bullet 2 = 4$

$8 \bullet 7 = 56, \quad 1 \bullet 7 = 7, \quad 0 \bullet 7 = 0,$

$$
\begin{array}{rrrrrrr}
 & & & & \mathbf{2} & 0 & 1 & 8 \\
\times & & & & 1 & \mathbf{7} & 2 & 9 \\
\hline
 & & & 1 & 8 & 1 & 6 & 2 \\
 & & & 4 & 0 & 3 & 6 & \\
 & 1 & 4 & 1 & 2 & 6 & & \\
\hline
\end{array}
$$

$$
\begin{array}{llll}
8 \bullet 9 = 72, & 1 \bullet 9 = 9, & 0 \bullet 9 = 0, & 2 \bullet 9 = 18 \\
8 \bullet 2 = 16, & 1 \bullet 2 = 2, & 0 \bullet 2 = 0, & 2 \bullet 2 = 4 \\
8 \bullet 7 = 56, & 1 \bullet 7 = 7, & 0 \bullet 7 = 0, & 2 \bullet 7 = 14
\end{array}
$$

$$
\begin{array}{cccccccc}
 & & & & 2 & 0 & 1 & \mathbf{8} \\
\times & & & & \mathbf{1} & 7 & 2 & 9 \\
\hline
 & & & 1 & 8 & 1 & 6 & 2 \\
 & & & 4 & 0 & 3 & 6 & \\
 & 1 & 4 & 1 & 2 & 6 & & \\
 & & & & 8 & & & \\
\hline
\end{array}
$$

$8 \bullet 9 = 72$, $1 \bullet 9 = 9$, $0 \bullet 9 = 0$, $2 \bullet 9 = 18$

$8 \bullet 2 = 16$, $1 \bullet 2 = 2$, $0 \bullet 2 = 0$, $2 \bullet 2 = 4$

$8 \bullet 7 = 56$, $1 \bullet 7 = 7$, $0 \bullet 7 = 0$, $2 \bullet 7 = 14$

$8 \bullet 1 = 8$,

$$
\begin{array}{cccccccc}
 & & & & 2 & 0 & \mathbf{1} & 8 \\
\times & & & & \mathbf{1} & 7 & 2 & 9 \\
\hline
 & & & 1 & 8 & 1 & 6 & 2 \\
 & & & 4 & 0 & 3 & 6 & \\
 & 1 & 4 & 1 & 2 & 6 & & \\
 & & & 1 & 8 & & & \\
\hline
\end{array}
$$

$8 \bullet 9 = 72$, $1 \bullet 9 = 9$, $0 \bullet 9 = 0$, $2 \bullet 9 = 18$

$8 \bullet 2 = 16$, $1 \bullet 2 = 2$, $0 \bullet 2 = 0$, $2 \bullet 2 = 4$

$8 \bullet 7 = 56$, $1 \bullet 7 = 7$, $0 \bullet 7 = 0$, $2 \bullet 7 = 14$

$8 \bullet 1 = 8$, $1 \bullet 1 = 1$,

$$
\begin{array}{cccccccc}
 & & & & 2 & \mathbf{0} & 1 & 8 \\
\times & & & & \mathbf{1} & 7 & 2 & 9 \\
\hline
 & & & 1 & 8 & 1 & 6 & 2 \\
 & & & 4 & 0 & 3 & 6 & \\
 & 1 & 4 & 1 & 2 & 6 & & \\
 & & 0 & 1 & 8 & & & \\
\hline
\end{array}
$$

$$
\begin{array}{llll}
8 \bullet 9 = 72, & 1 \bullet 9 = 9, & 0 \bullet 9 = 0, & 2 \bullet 9 = 18 \\
8 \bullet 2 = 16, & 1 \bullet 2 = 2, & 0 \bullet 2 = 0, & 2 \bullet 2 = 4 \\
8 \bullet 7 = 56, & 1 \bullet 7 = 7, & 0 \bullet 7 = 0, & 2 \bullet 7 = 14 \\
8 \bullet 1 = 8, & 1 \bullet 1 = 1, & 0 \bullet 1 = 0, &
\end{array}
$$

$$
\begin{array}{cccccccc}
 & & & & \mathbf{2} & 0 & 1 & 8 \\
\times & & & & \mathbf{1} & 7 & 2 & 9 \\
\hline
 & & & 1 & 8 & 1 & 6 & 2 \\
 & & & 4 & 0 & 3 & 6 & \\
 & 1 & 4 & 1 & 2 & 6 & & \\
 & 2 & 0 & 1 & 8 & & & \\
\hline
\end{array}
$$

$$
\begin{array}{llll}
8 \bullet 9 = 72, & 1 \bullet 9 = 9, & 0 \bullet 9 = 0, & 2 \bullet 9 = 18 \\
8 \bullet 2 = 16, & 1 \bullet 2 = 2, & 0 \bullet 2 = 0, & 2 \bullet 2 = 4 \\
8 \bullet 7 = 56, & 1 \bullet 7 = 7, & 0 \bullet 7 = 0, & 2 \bullet 7 = 14 \\
8 \bullet 1 = 8, & 1 \bullet 1 = 1, & 0 \bullet 1 = 0, & 2 \bullet 1 = 2
\end{array}
$$

$$
\begin{array}{cccccccc}
 & & & & 2 & 0 & 1 & 8 \\
\times & & & & 1 & 7 & 2 & 9 \\
\hline
 & & & 1 & 8 & 1 & 6 & 2 \\
 & & & 4 & 0 & 3 & 6 & \\
 & & 1 & 4 & 1 & 2 & 6 & \\
 & & 2 & 0 & 1 & 8 & & \\
\hline
 & & 3 & 4 & 8 & 9 & 1 & 2 & 2
\end{array}
$$

$$
\begin{array}{llll}
8 \bullet 9 = 72, & 1 \bullet 9 = 9, & 0 \bullet 9 = 0, & 2 \bullet 9 = 18 \\
8 \bullet 2 = 16, & 1 \bullet 2 = 2, & 0 \bullet 2 = 0, & 2 \bullet 2 = 4 \\
8 \bullet 7 = 56, & 1 \bullet 7 = 7, & 0 \bullet 7 = 0, & 2 \bullet 7 = 14 \\
8 \bullet 1 = 8, & 1 \bullet 1 = 1, & 0 \bullet 1 = 0, & 2 \bullet 1 = 2
\end{array}
$$

$$
\begin{array}{cccccccc}
 & & & & \mathbf{2} & \mathbf{0} & \mathbf{1} & \mathbf{8} \\
\times & & & & \mathbf{1} & \mathbf{7} & \mathbf{2} & \mathbf{9} \\
\hline
 & & & 1 & 8 & 1 & 6 & 2 \\
 & & & 4 & 0 & 3 & 6 & \\
 & 1 & 4 & 1 & 2 & 6 & & \\
 & 2 & 0 & 1 & 8 & & & \\
\hline
 & 3 & 4 & 8 & 9 & 1 & 2 & 2
\end{array}
$$

$$
\begin{array}{llll}
8 \bullet 9 = 72, & 1 \bullet 9 = 9, & 0 \bullet 9 = 0, & 2 \bullet 9 = 18 \\
8 \bullet 2 = 16, & 1 \bullet 2 = 2, & 0 \bullet 2 = 0, & 2 \bullet 2 = 4 \\
8 \bullet 7 = 56, & 1 \bullet 7 = 7, & 0 \bullet 7 = 0, & 2 \bullet 7 = 14 \\
8 \bullet 1 = 8, & 1 \bullet 1 = 1, & 0 \bullet 1 = 0, & 2 \bullet 1 = 2
\end{array}
$$

$$(\mathbf{2}X^3 + \mathbf{0}X^2 + \mathbf{1}X + \mathbf{8})(\mathbf{1}X^3 + \mathbf{7}X^2 + \mathbf{2}X + \mathbf{9})$$

Multiplier deux polynômes de degré $k-1$ demande k^2 multiplications bilinéaires $\bullet$. Peut-on faire mieux ?

Karatsuba (1962)

$$(u_0+u_1X)(v_0+v_1X) = u_0 \bullet v_0 + (u_0 \bullet v_1 + u_1 \bullet v_0)X + u_1 \bullet v_1 X^2$$

Karatsuba (1962)

$$\begin{aligned}(u_0+u_1X)(v_0+v_1X) &= u_0\bullet v_0 + (u_0\bullet v_1 + u_1\bullet v_0)X + u_1\bullet v_1X^2\\ &= u_0\bullet v_0(1-X) + (u_0+u_1)\bullet(v_0+v_1)X + u_1\bullet v_1(X^2-X)\end{aligned}$$

permet de multiplier deux polynômes de degré 1 avec trois $\bullet$ au lieu de quatre.

Karatsuba (1962)

$$(u_0+u_1X)(v_0+v_1X)$$
$$= u_0 \bullet v_0(1-X) + (u_0+u_1) \bullet (v_0+v_1)X + u_1 \bullet v_1(X^2-X)$$

permet de multiplier deux polynômes de degré 1 avec trois $\bullet$ au lieu de quatre.

Peut s'appliquer itérativement, par exemple en degré 3 on écrit

$$u_0 + u_1X + u_2X^2 + u_3X^3 = (u_0+u_1X) + (u_2+u_3X)X^2$$
$$v_0 + v_1X + v_2X^2 + v_3X^3 = (v_0+v_1X) + (v_2+v_3X)X^2$$

et on les multiplie avec 9 $\bullet$ au lieu de 16.

Karatsuba (1962)

$$(u_0+u_1X)(v_0+v_1X)$$
$$= u_0 \bullet v_0(1-X) + (u_0+u_1) \bullet (v_0+v_1)X + u_1 \bullet v_1(X^2-X)$$

permet de multiplier deux polynômes de degré 1 avec trois $\bullet$ au lieu de quatre.

Peut s'appliquer itérativement, par exemple en degré 3 on écrit

$$u_0 + u_1X + u_2X^2 + u_3X^3 = (u_0+u_1X) + (u_2+u_3X)X^2$$
$$v_0 + v_1X + v_2X^2 + v_3X^3 = (v_0+v_1X) + (v_2+v_3X)X^2$$

et on les multiplie avec 9 $\bullet$ au lieu de 16.

Plus généralement on multiplie deux polynômes de degré $k-1$ avec $\approx k^{\log_2(3)} \approx k^{1,585}$ $\bullet$ au lieu de k^2.

On va s'intéresser plus particulièrement à la multiplication dans les corps finis.

Rappel :

- tout corps fini est de la forme $\mathbb{F}_q$ pour q une puissance d'un nombre premier
- si $q = p$ premier, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$ avec $+, \times$ modulo p
- $\mathbb{F}_{q^k} = \mathbb{F}_q[X]/(P)$ où P polynôme irréductible de degré k sur $\mathbb{F}_q$, i.e. $\mathbb{F}_{q^k} = \mathbb{F}_q[\alpha]$ où $P(\alpha) = 0$.

But : effectuer une multiplication dans $\mathbb{F}_{q^k}$ en minimisant le nombre de $\bullet$ dans $\mathbb{F}_q$.

On va s'intéresser plus particulièrement à la multiplication dans les corps finis.

Rappel :

- tout corps fini est de la forme $\mathbb{F}_q$ pour q une puissance d'un nombre premier
- si $q = p$ premier, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$ avec $+, \times$ modulo p
- $\mathbb{F}_{q^k} = \mathbb{F}_q[X]/(P)$ où P polynôme irréductible de degré k sur $\mathbb{F}_q$, i.e. $\mathbb{F}_{q^k} = \mathbb{F}_q[\alpha]$ où $P(\alpha) = 0$.

But : effectuer une multiplication dans $\mathbb{F}_{q^k}$ en minimisant le nombre de $\bullet$ dans $\mathbb{F}_q$.

P.ex. Karatsuba s'applique pour $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ où $\alpha^2 = 1 + \alpha$:

$$\begin{aligned}(u_0+u_1X)(v_0+v_1X) \\ = u_0 \bullet v_0(1-X) + (u_0+u_1) \bullet (v_0+v_1)X + u_1 \bullet v_1(X^2-X)\end{aligned}$$

On va s'intéresser plus particulièrement à la multiplication dans les corps finis.

Rappel :

- tout corps fini est de la forme $\mathbb{F}_q$ pour q une puissance d'un nombre premier
- si $q = p$ premier, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$ avec $+, \times$ modulo p
- $\mathbb{F}_{q^k} = \mathbb{F}_q[X]/(P)$ où P polynôme irréductible de degré k sur $\mathbb{F}_q$, i.e. $\mathbb{F}_{q^k} = \mathbb{F}_q[\alpha]$ où $P(\alpha) = 0$.

But : effectuer une multiplication dans $\mathbb{F}_{q^k}$ en minimisant le nombre de $\bullet$ dans $\mathbb{F}_q$.

P.ex. Karatsuba s'applique pour $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ où $\alpha^2 = 1 + \alpha$:

$$\begin{aligned}(u_0+u_1\alpha)(v_0+v_1\alpha) \\ &= u_0 \bullet v_0(1+\alpha) + (u_0+u_1)\bullet(v_0+v_1)\alpha + u_1 \bullet v_1\end{aligned}$$

En termes de codes, on cherche une décomposition

$$\begin{array}{ccc} \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} & \xrightarrow{\times} & \mathbb{F}_{q^k} \\ \Big\downarrow{\scriptstyle \varphi\times\varphi} & & \Big\uparrow{\scriptstyle \theta} \\ (\mathbb{F}_q)^n \times (\mathbb{F}_q)^n & \xrightarrow{*} & (\mathbb{F}_q)^n \end{array}$$

où :

- $\varphi : \mathbb{F}_{q^k} \to (\mathbb{F}_q)^n$ application d'encodage, $\mathbb{F}_q$-linéaire
- $*$ est la multiplication coordonnée par coordonnée

$$(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_1 \bullet b_1, \ldots, a_n \bullet b_n).$$

- $\theta : (\mathbb{F}_q)^n \to \mathbb{F}_{q^k}$ application de décodage, $\mathbb{F}_q$-linéaire.

Permet de faire une multiplication dans $\mathbb{F}_{q^k}$ avec n $\bullet$ dans $\mathbb{F}_q$.

Attention : θ ne décode pas le code $\mathcal{C}$ image de φ, mais le code $\mathcal{C} * \mathcal{C}$.

$$\begin{array}{ccc} \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} & \xrightarrow{\times} & \mathbb{F}_{q^k} \\ {\scriptstyle \varphi\times\varphi}\downarrow & & \uparrow{\scriptstyle \theta} \\ (\mathbb{F}_q)^n \times (\mathbb{F}_q)^n & \xrightarrow{*} & (\mathbb{F}_q)^n \end{array}$$

Exemple : $q = 2$, $k = 2$, $n = 3$, Karatsuba

$$(u_0+u_1\alpha)(v_0+v_1\alpha) = u_0 \bullet v_0(1+\alpha) + (u_0+u_1)\bullet(v_0+v_1)\alpha + u_1 \bullet v_1$$

s'écrit bien $\mathbf{uv} = \theta(\varphi(\mathbf{u}) * \varphi(\mathbf{v}))$

où
$\varphi : \mathbf{u} = u_0 + u_1\alpha \mapsto \varphi(\mathbf{u}) = (u_0,\ u_0+u_1,\ u_1)$
$\theta : (c_1, c_2, c_3) \mapsto c_1(1+\alpha) + c_2\alpha + c_3.$

$$\begin{array}{ccc} \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} & \xrightarrow{\times} & \mathbb{F}_{q^k} \\ \Big\downarrow{\scriptstyle \varphi\times\varphi} & & \Big\uparrow{\scriptstyle \theta} \\ (\mathbb{F}_q)^n \times (\mathbb{F}_q)^n & \xrightarrow{*} & (\mathbb{F}_q)^n \end{array}$$

Plusieurs points de vue :

- complexité / algèbre bilinéaire $\rightarrow$ k donné, minimiser n $\rightarrow$ rang du tenseur de multiplication dans $\mathbb{F}_{q^k}$
- calcul réparti $\rightarrow$ $\mathbf{u} \in \mathbb{F}_{q^k}$ scindé en n parts $(a_1, \ldots, a_n)$ distribuées à n entités distantes, idem pour $\mathbf{v}$ en $(b_1, \ldots, b_n)$; calculer $\mathbf{u} + \mathbf{v}$ revient à faire les opérations locales $a_i + b_i$ ou $a_i \bullet b_i$; tolérance aux fautes $= d(\mathcal{C} * \mathcal{C})$
- partage de secret à seuil $\rightarrow$ idem en exigeant qu'il soit difficile de retrouver $\mathbf{u}$ à partir d'un nombre limité des a_i $\rightarrow$ $d(\mathcal{C}^\perp)$

Comment construire une telle décomposition ?

Karatsuba pour $\mathbb{F}_4$ fonctionne par évaluation-interpolation.

Donnés $\mathbf{u} = P_{\mathbf{u}}(\alpha)$ avec $P_{\mathbf{u}} = u_0 + u_1 X$
et $\mathbf{v} = P_{\mathbf{v}}(\alpha)$ avec $P_{\mathbf{v}} = v_0 + v_1 X$.

Évaluation (en $0, 1, \infty$)

$$\begin{array}{lll} u_0 = P_{\mathbf{u}}(0), & u_0+u_1 = P_{\mathbf{u}}(1), & u_1 = P_{\mathbf{u}}(\infty) \\ v_0 = P_{\mathbf{v}}(0), & v_0+v_1 = P_{\mathbf{v}}(1), & v_1 = P_{\mathbf{v}}(\infty) \end{array}$$

Puis on calcule $c_1 = u_0 \bullet v_0$, $c_2 = (u_0+u_1) \bullet (v_0+v_1)$, $c_3 = u_1 \bullet v_1$.

Interpolation

Par interpolation de Lagrange on trouve un (unique) polynôme de degré 2 tel que $Q(0) = c_1$, $Q(1) = c_2$, $Q(\infty) = c_3$.

Mais le polynôme produit $P_{\mathbf{u}} P_{\mathbf{v}}$ vérifie aussi ces conditions. On en déduit $P_{\mathbf{u}} P_{\mathbf{v}} = Q$, puis en évaluant en α, on trouve

$$\mathbf{uv} = Q(\alpha).$$

Généralisation à une extension de degré k :

- Les éléments de l'extension sont représentés par des polynômes de degré $k-1$.
- Le produit de deux tels polynômes est de degré $2k-2$.
- Pour retrouver ce polynôme produit par interpolation de Lagrange, on a besoin de ses valeurs en $2k-1$ points.

Problème : on travaille sur un corps de base $\mathbb{F}_q$ fixé, on ne peut pas prendre k arbitrairement grand.
Par exemple sur $\mathbb{F}_2$, on a déjà utilisé les points $\{0, 1, \infty\}$ de $\mathbb{P}^1$... il n'y en a pas d'autres !

Généralisation à une extension de degré k :

- Les éléments de l'extension sont représentés par des polynômes de degré $k-1$.
- Le produit de deux tels polynômes est de degré $2k-2$.
- Pour retrouver ce polynôme produit par interpolation de Lagrange, on a besoin de ses valeurs en $2k-1$ points.

Problème : on travaille sur un corps de base $\mathbb{F}_q$ fixé, on ne peut pas prendre k arbitrairement grand.
Par exemple sur $\mathbb{F}_2$, on a déjà utilisé les points $\{0, 1, \infty\}$ de $\mathbb{P}^1$... il n'y en a pas d'autres !

Solution (Chudnovsky-Chudnovsky) : évaluation-interpolation sur une courbe de genre plus élevé.

Supposons donnés :

- X une courbe sur $\mathbb{F}_q$ de genre g
- $P_1, \ldots, P_n$ points de X sur $\mathbb{F}_q$
- Q un point de X sur $\mathbb{F}_{q^k}$
- D un diviseur sur X

tels que

- l'évaluation $\mathcal{L}(D) \to \mathbb{F}_{q^k}$, $f \mapsto f(Q)$ soit surjective
- l'évaluation $\mathcal{L}(2D) \to (\mathbb{F}_q)^n$, $h \mapsto (h(P_1), \ldots, h(P_n))$ soit injective.

Alors par évaluation-interpolation on en déduit un algorithme de multiplication dans $\mathbb{F}_{q^k}$ avec n • dans $\mathbb{F}_q$.

Supposons donnés :

- X une courbe sur $\mathbb{F}_q$ de genre g
- $P_1, \ldots, P_n$ points de X sur $\mathbb{F}_q$
- Q un point de X sur $\mathbb{F}_{q^k}$
- D un diviseur sur X

tels que

- l'évaluation $\mathcal{L}(D) \to \mathbb{F}_{q^k}$, $f \mapsto f(Q)$ soit surjective
- l'évaluation $\mathcal{L}(2D) \to (\mathbb{F}_q)^n$, $h \mapsto (h(P_1), \ldots, h(P_n))$ soit injective.

Alors par évaluation-interpolation on en déduit un algorithme de multiplication dans $\mathbb{F}_{q^k}$ avec n • dans $\mathbb{F}_q$.

Résultat (Chudnovsky-Chudnovsky) : on sait construire de tels objets avec g, n linéaires en $k \to$ complexité linéaire en k !

Supposons donnés :

- X une courbe sur $\mathbb{F}_q$ de genre g
- $P_1, \ldots, P_n$ points de X sur $\mathbb{F}_q$
- Q un point de X sur $\mathbb{F}_{q^k}$
- D un diviseur sur X

tels que

- l'évaluation $\mathcal{L}(D) \to \mathbb{F}_{q^k}$, $f \mapsto f(Q)$ soit surjective
- l'évaluation $\mathcal{L}(2D) \to (\mathbb{F}_q)^n$, $h \mapsto (h(P_1), \ldots, h(P_n))$ soit injective.

Alors par évaluation-interpolation on en déduit un algorithme de multiplication dans $\mathbb{F}_{q^k}$ avec n • dans $\mathbb{F}_q$.

Cas particulier $q = p^2$, $p \geq 5$ (Shparlinski-Tsfasman-Vladut, H.R.) on y arrive avec $2k + 1 - g = n \approx (p-1)g$, d'où une complexité $n \approx 2(1 + \frac{1}{p-2})k$.

Analogie entre fibrés vectoriels, réseaux euclidiens, et codes