Courbes elliptiques

Cédric Bonnafé

CNRS (UMR 5149) - Université de Montpellier

Montpellier, Lycée Joffre, Mars 2016

- Coniques : $ax^2 + bxy + cy^2 + dx + ey + f = 0$

- Coniques : $ax^2 + bxy + cy^2 + dx + ey + f = 0$
- Cubiques :
  $\alpha x^3 + \beta x^2 y + \gamma x y^2 + \delta y^3$

- Coniques : $ax^2 + bxy + cy^2 + dx + ey + f = 0$
- Cubiques :
  $\alpha x^3 + \beta x^2 y + \gamma x y^2 + \delta y^3 + ax^2 + bxy + cy^2 + dx + ey + f = 0$

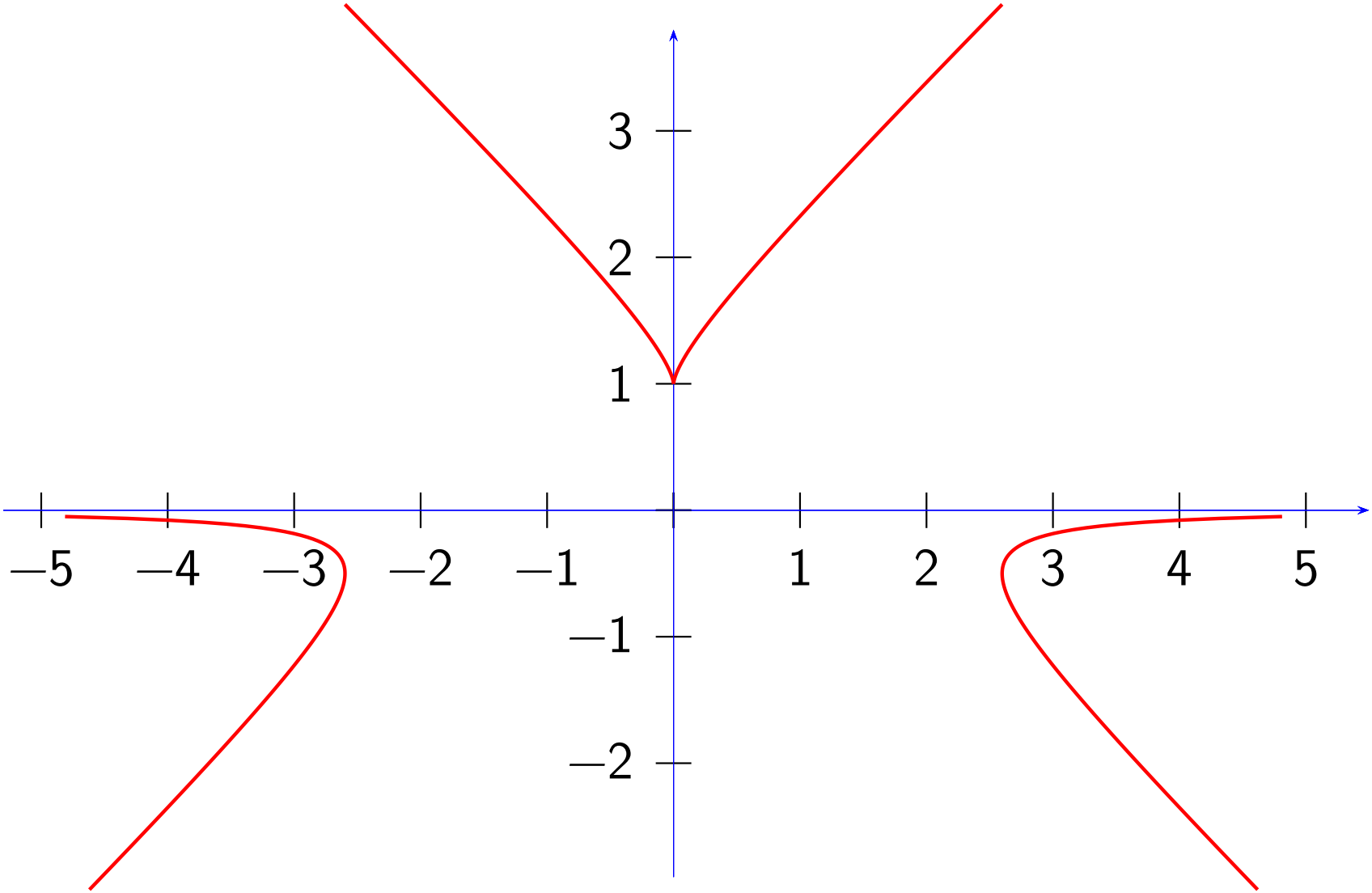
- Coniques : $ax^2 + bxy + cy^2 + dx + ey + f = 0$
- Cubiques :
  $\alpha x^3 + \beta x^2 y + \gamma x y^2 + \delta y^3 + ax^2 + bxy + cy^2 + dx + ey + f = 0$
- Courbes elliptiques : cubiques sans points singuliers
- 19ème siècle : Abel, Gauss, Jacobi, Legendre...

- Coniques : $ax^2 + bxy + cy^2 + dx + ey + f = 0$
- Cubiques :
  $\alpha x^3 + \beta x^2 y + \gamma x y^2 + \delta y^3 + ax^2 + bxy + cy^2 + dx + ey + f = 0$
- Courbes elliptiques : cubiques sans points singuliers
- 19ème siècle : Abel, Gauss, Jacobi, Legendre...
- 1920 : Mordell
- 1970-1995 : Hellegouarch, Frey, Ribet, Taylor/Wiles : preuve du théorème de Fermat

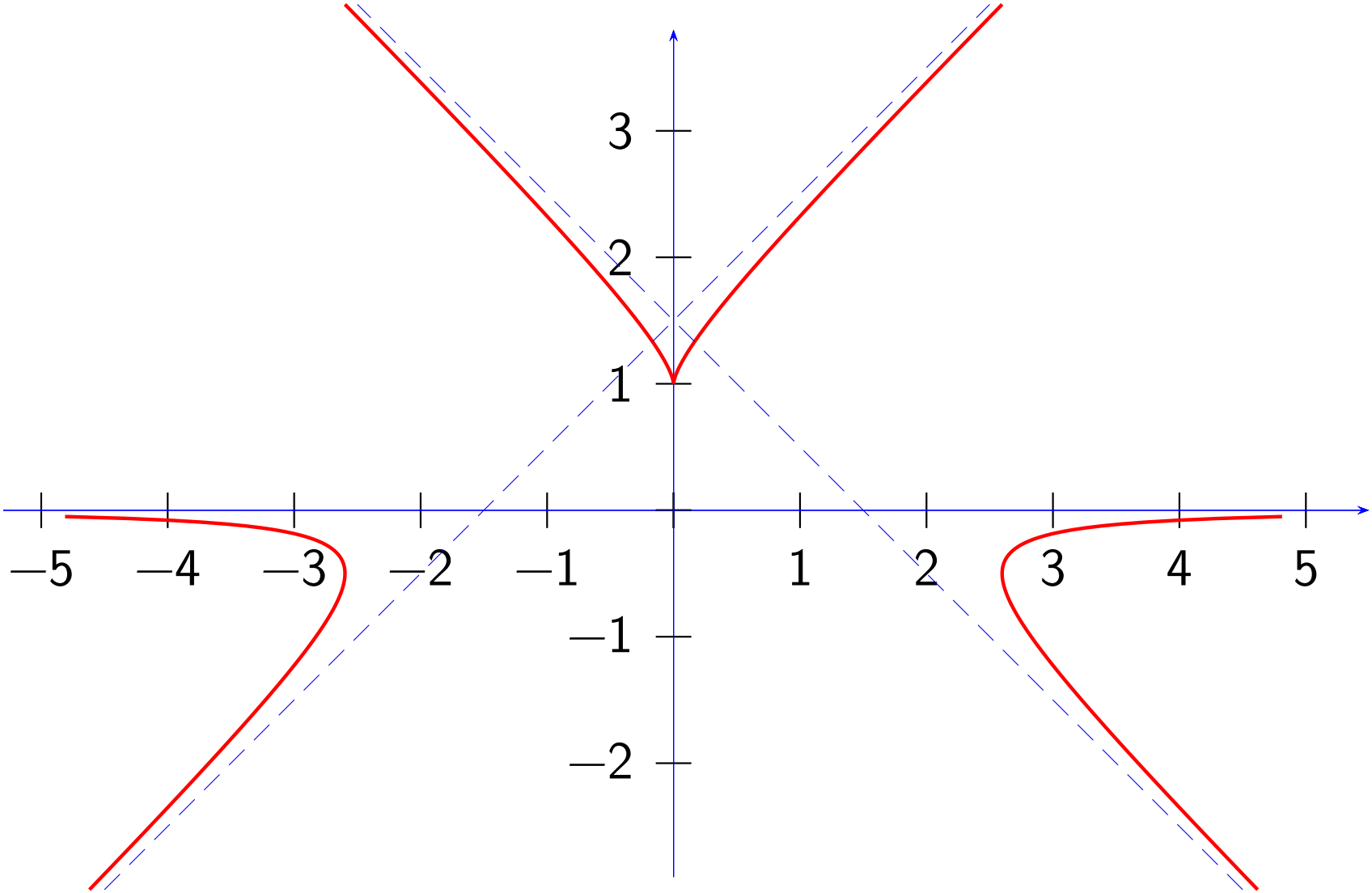
- Coniques : $ax^2 + bxy + cy^2 + dx + ey + f = 0$
- Cubiques :
  $\alpha x^3 + \beta x^2 y + \gamma x y^2 + \delta y^3 + ax^2 + bxy + cy^2 + dx + ey + f = 0$
- Courbes elliptiques : cubiques sans points singuliers
- 19ème siècle : Abel, Gauss, Jacobi, Legendre...
- 1920 : Mordell
- 1970-1995 : Hellegouarch, Frey, Ribet, Taylor/Wiles : preuve du théorème de Fermat

Une référence : *Elliptic curves*, H. McKean & V. Moll, Cambridge University Press (1997).

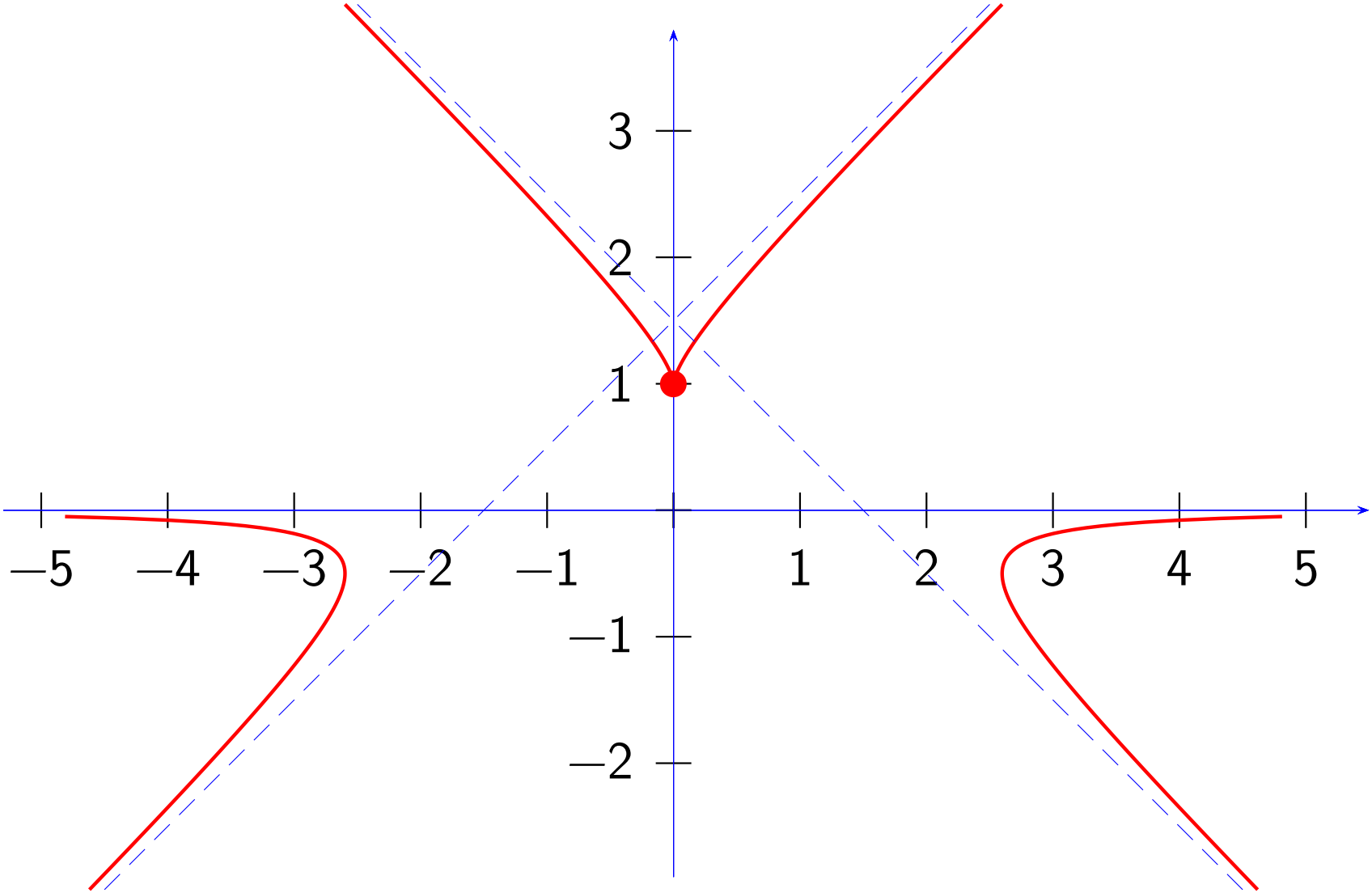
$x^2y = (y-1)^3$



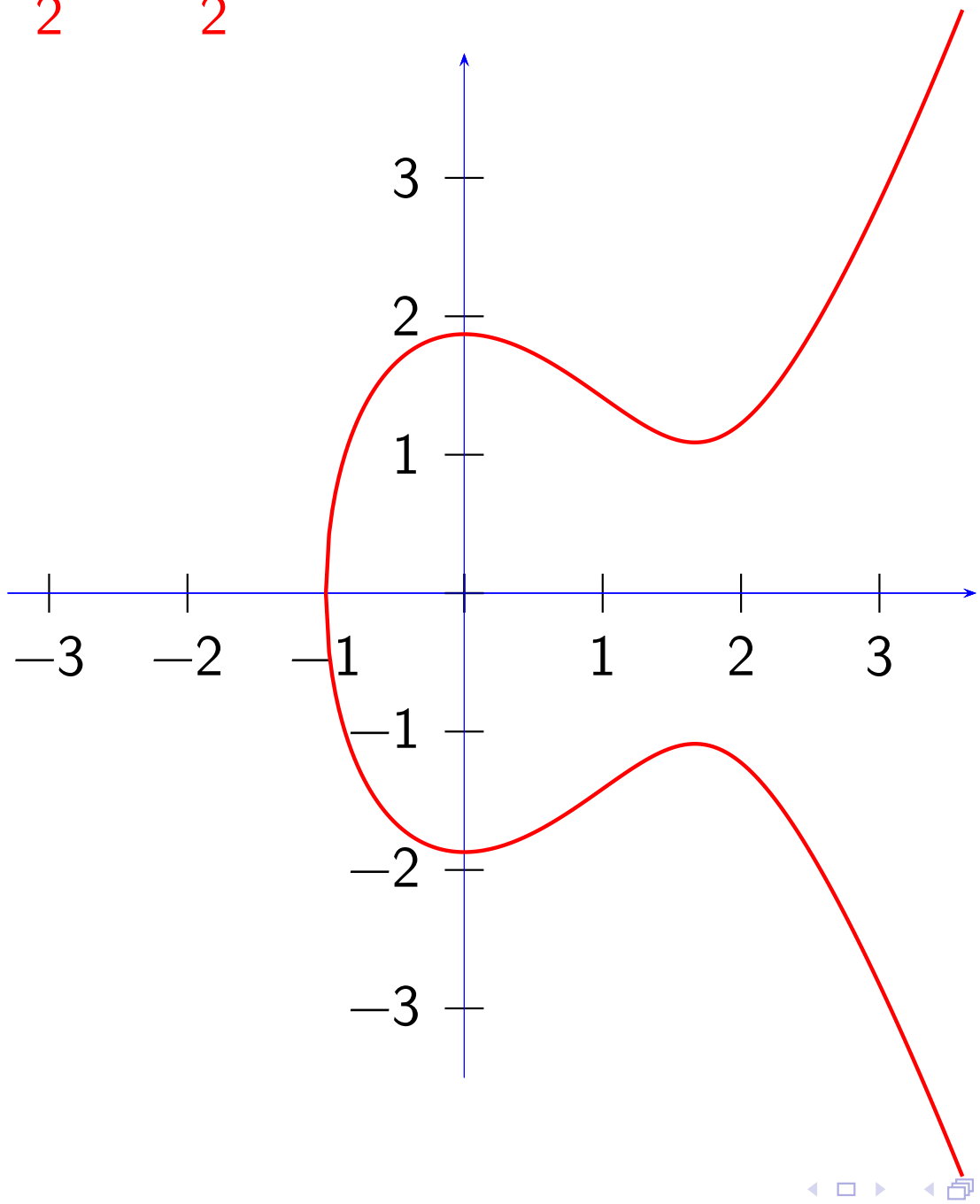
$x^2y = (y-1)^3$



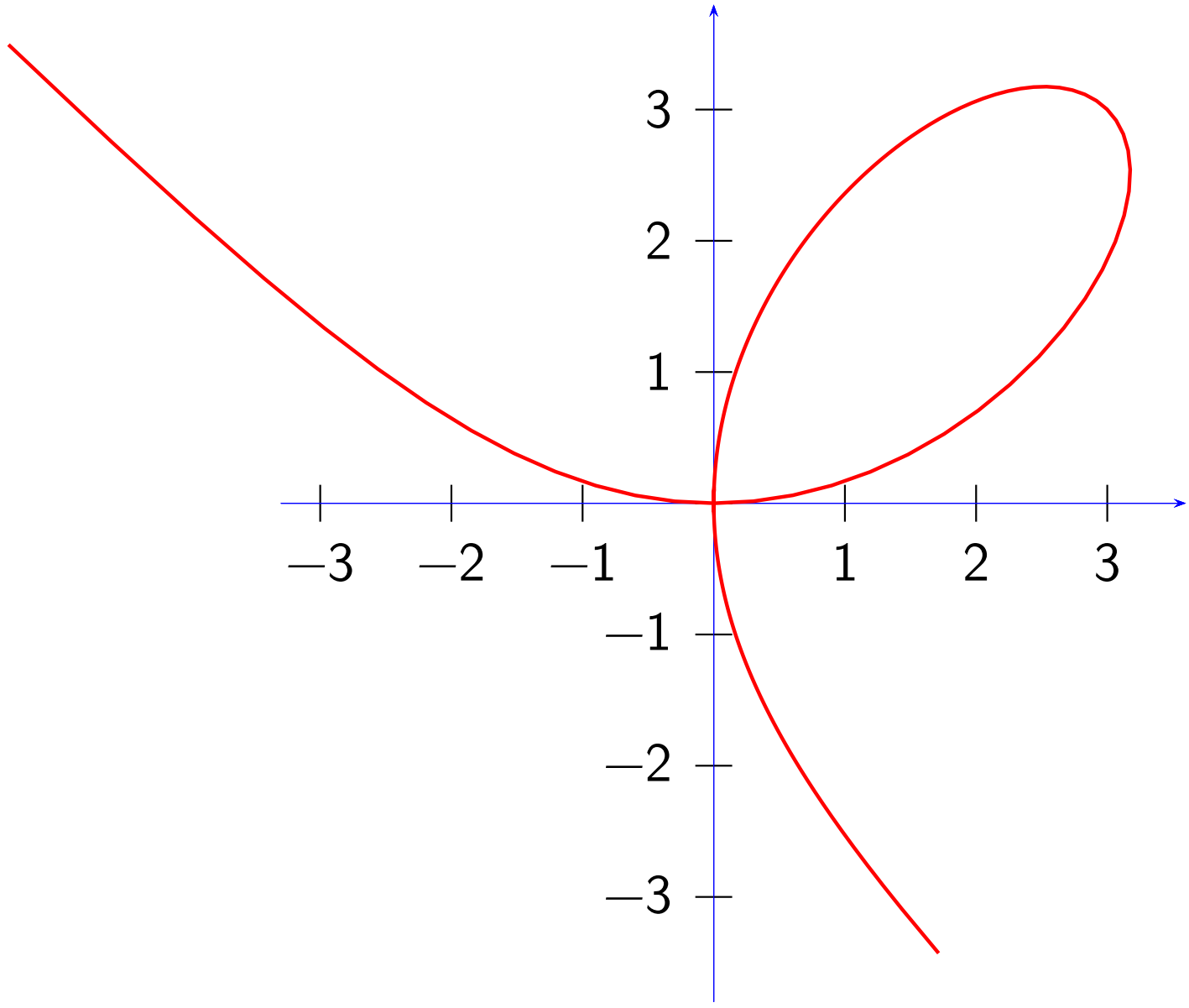
$x^2y = (y-1)^3$



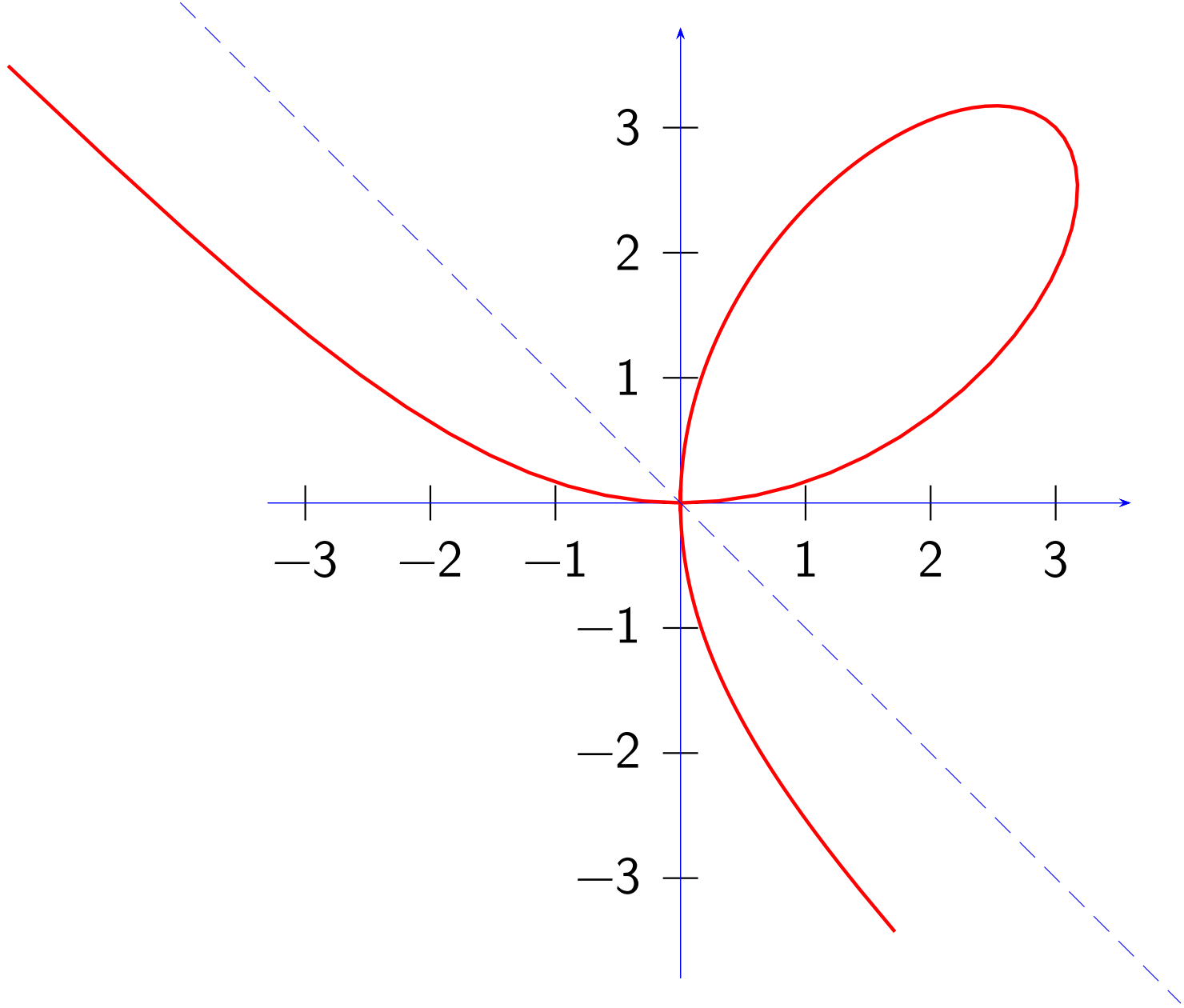
$$y^2 = x^3 - \frac{5}{2}x^2 + \frac{7}{2}$$



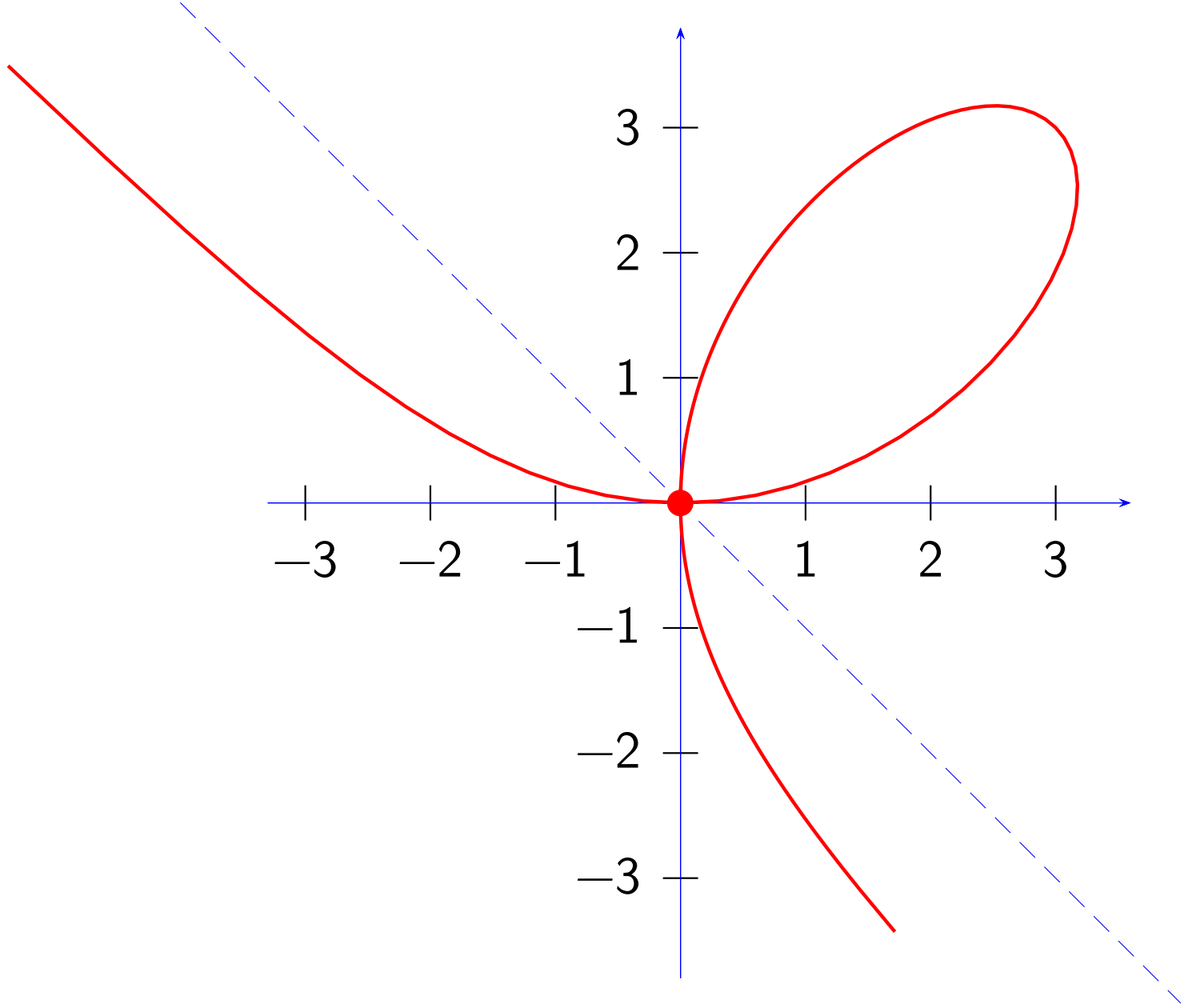
$x^3 + y^3 - 6xy = 0$



$x^3 + y^3 - 6xy = 0$

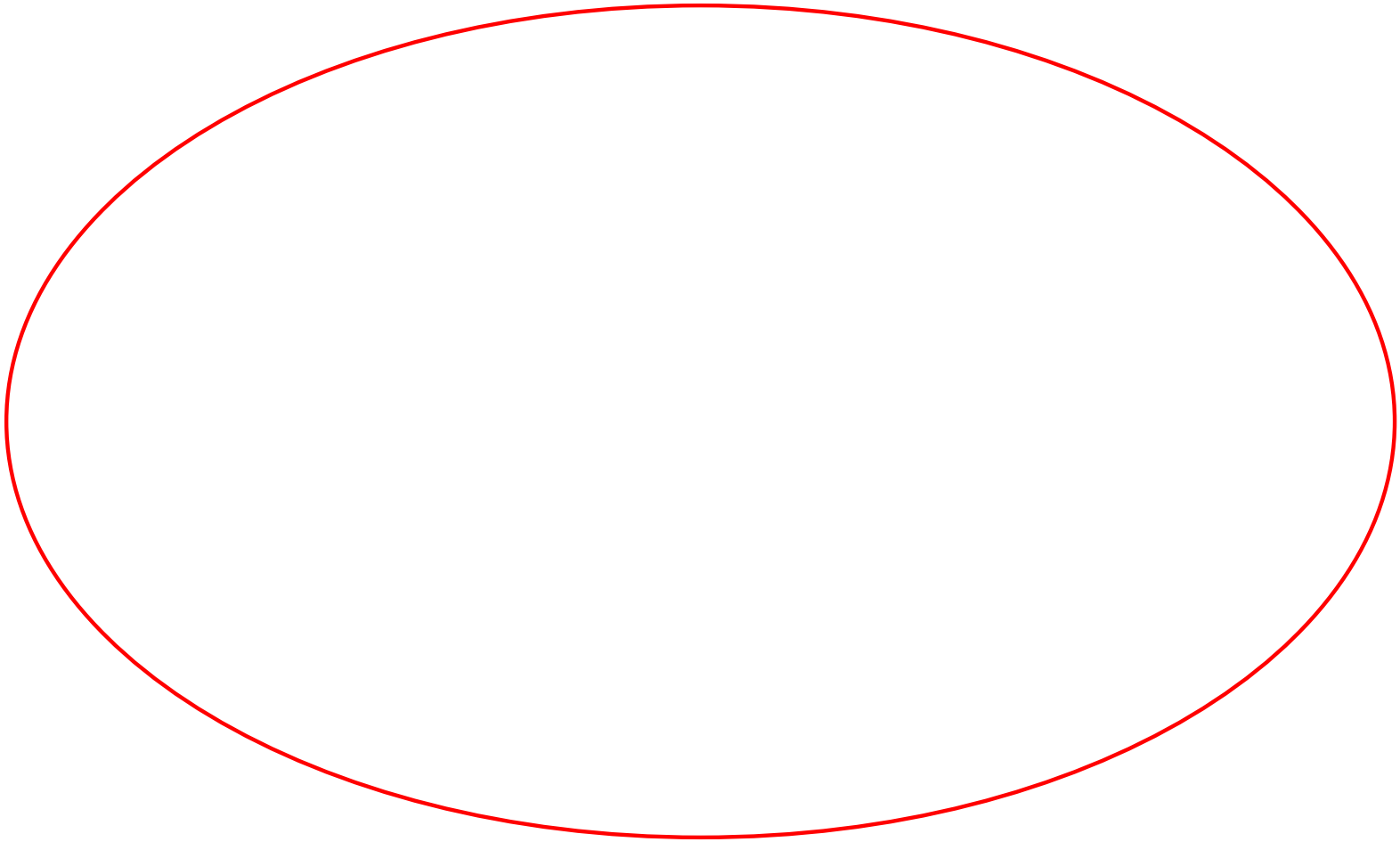


$x^3 + y^3 - 6xy = 0$

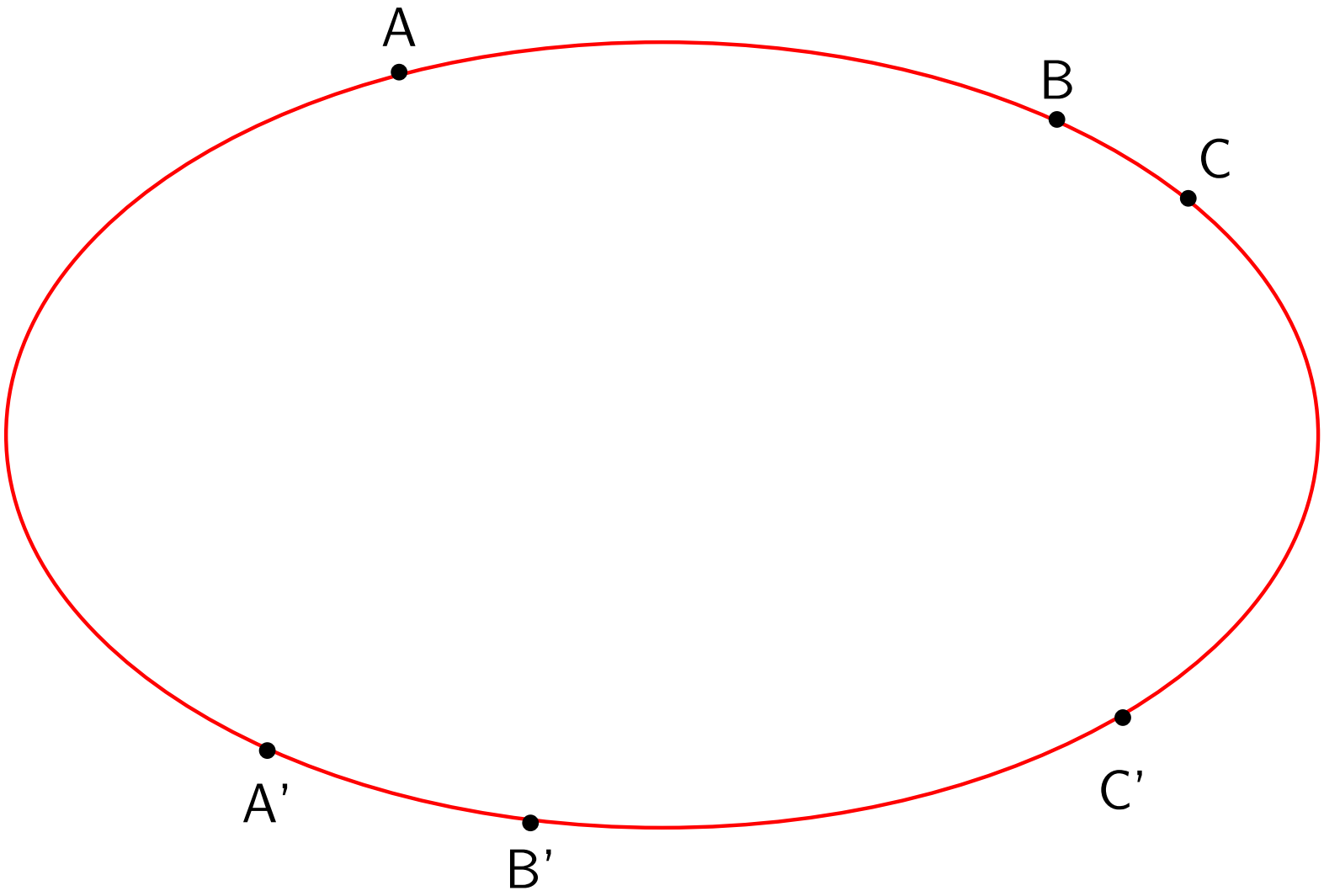


Théorème de Pascal

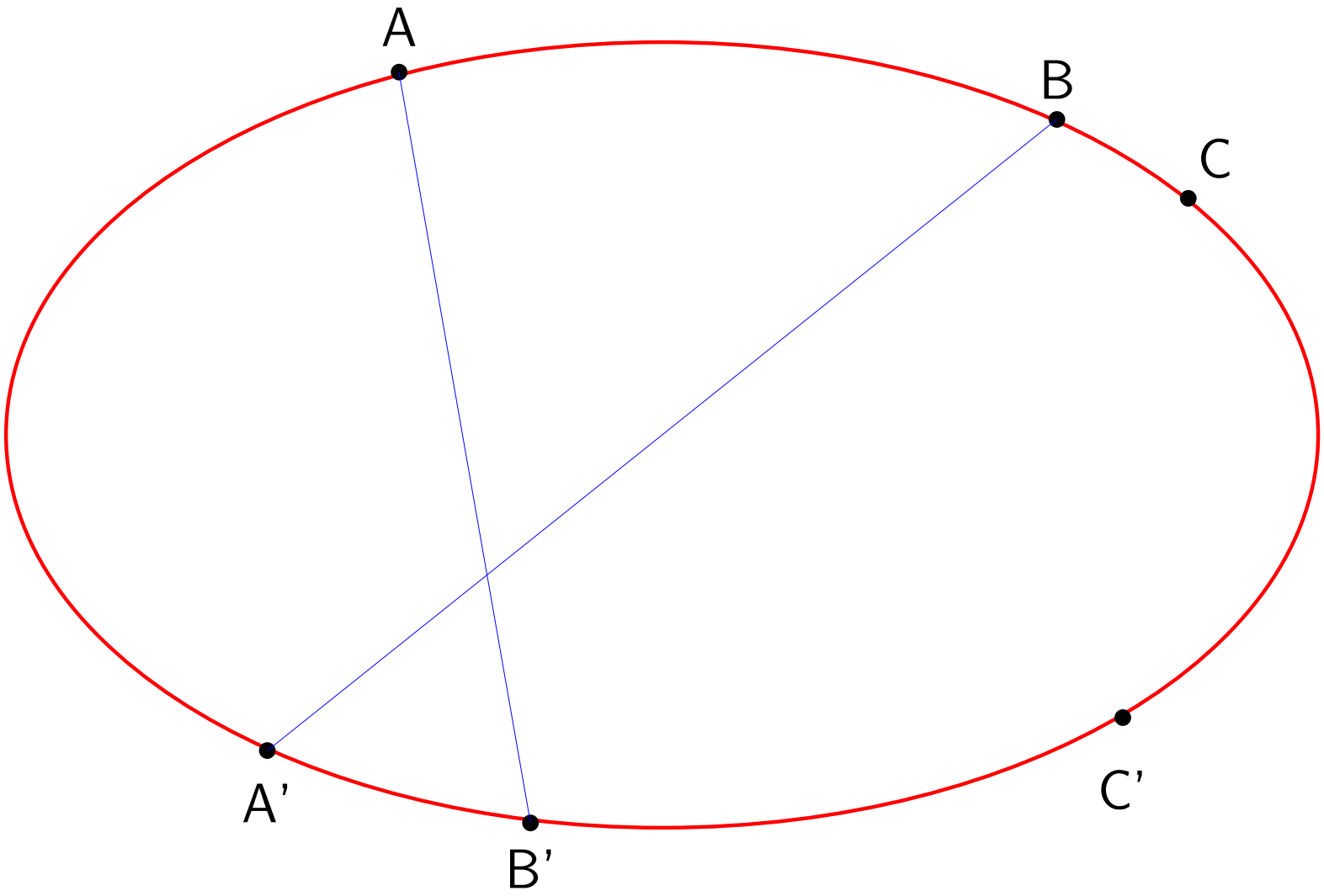
Théorème de Pascal



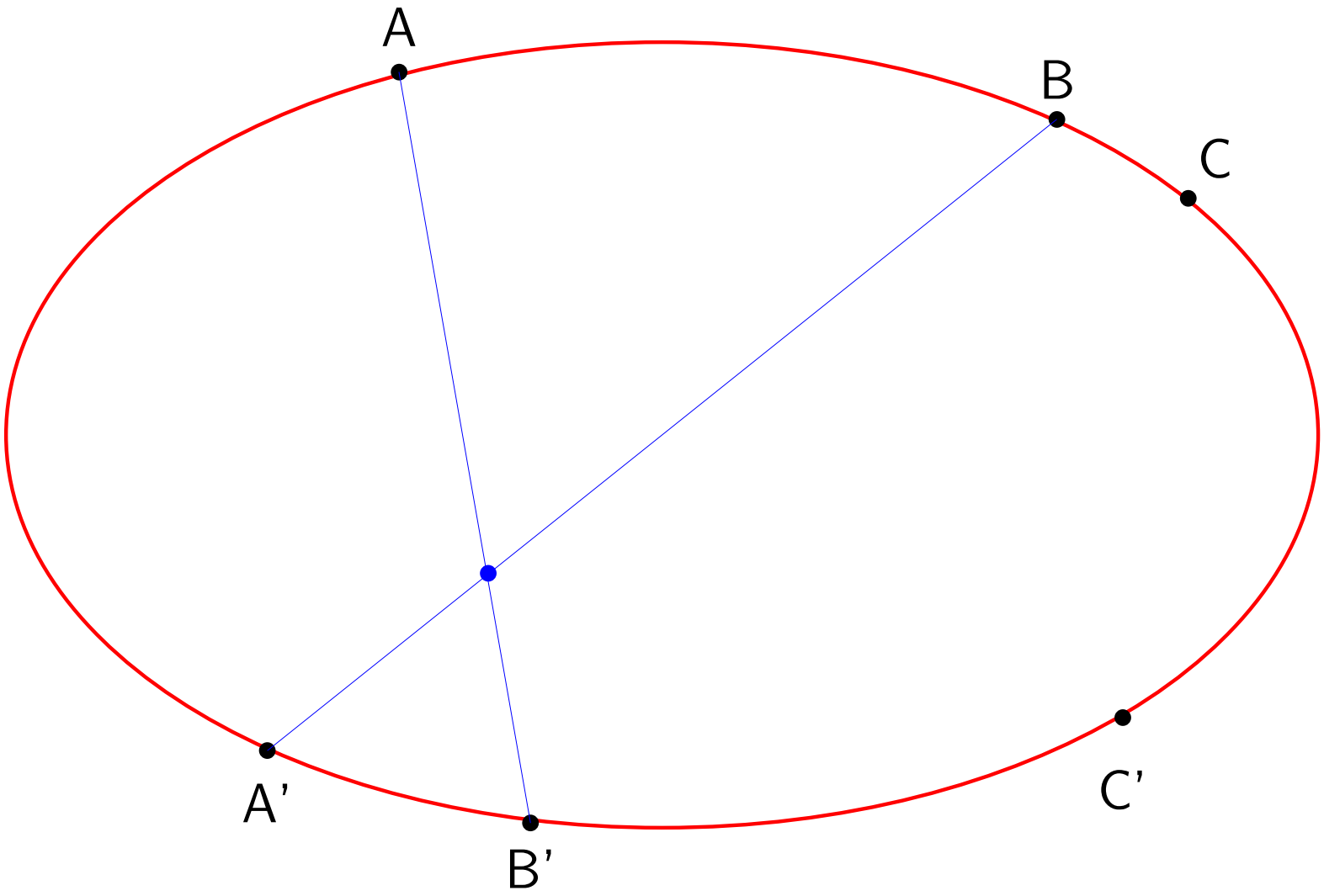
Théorème de Pascal



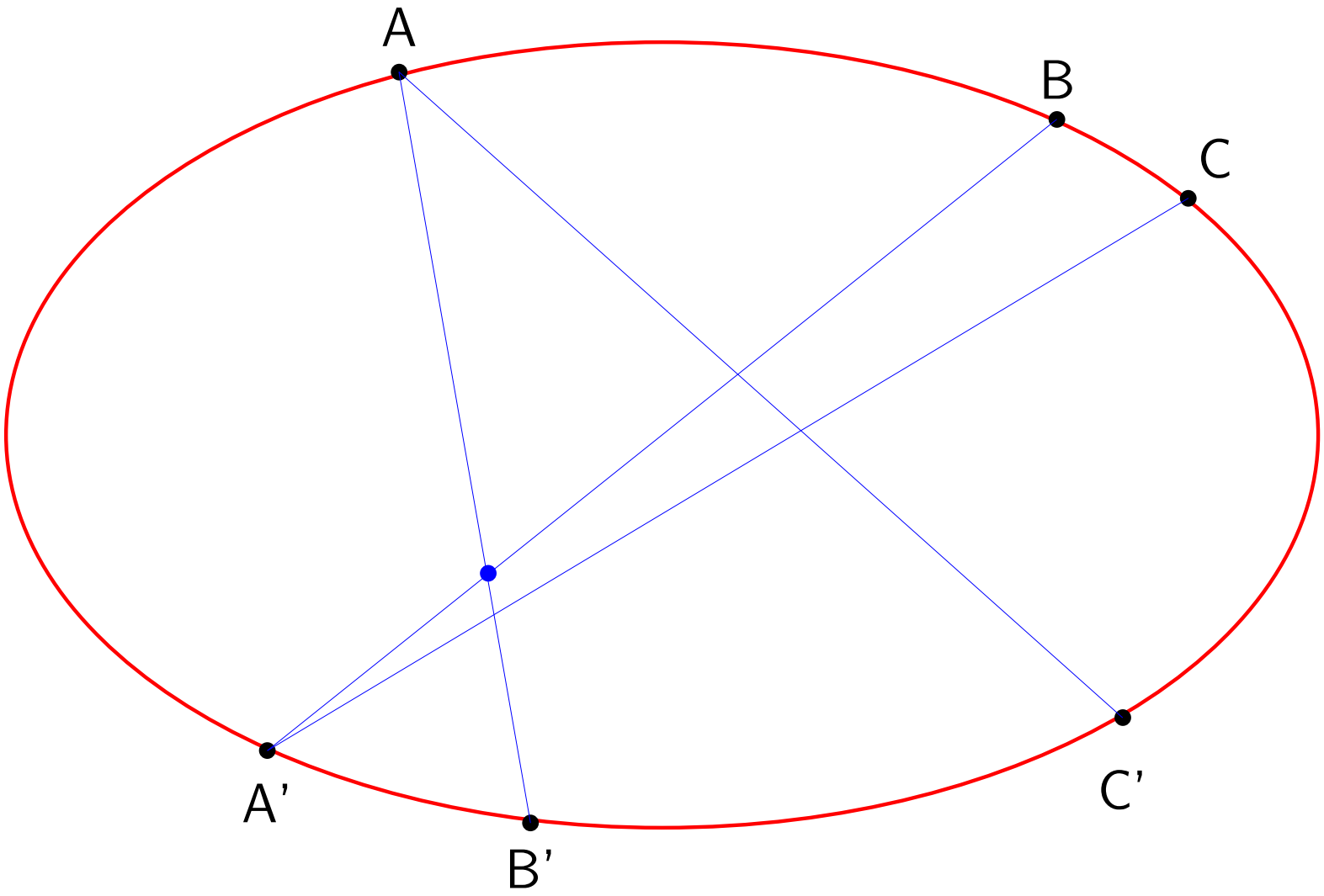
Théorème de Pascal



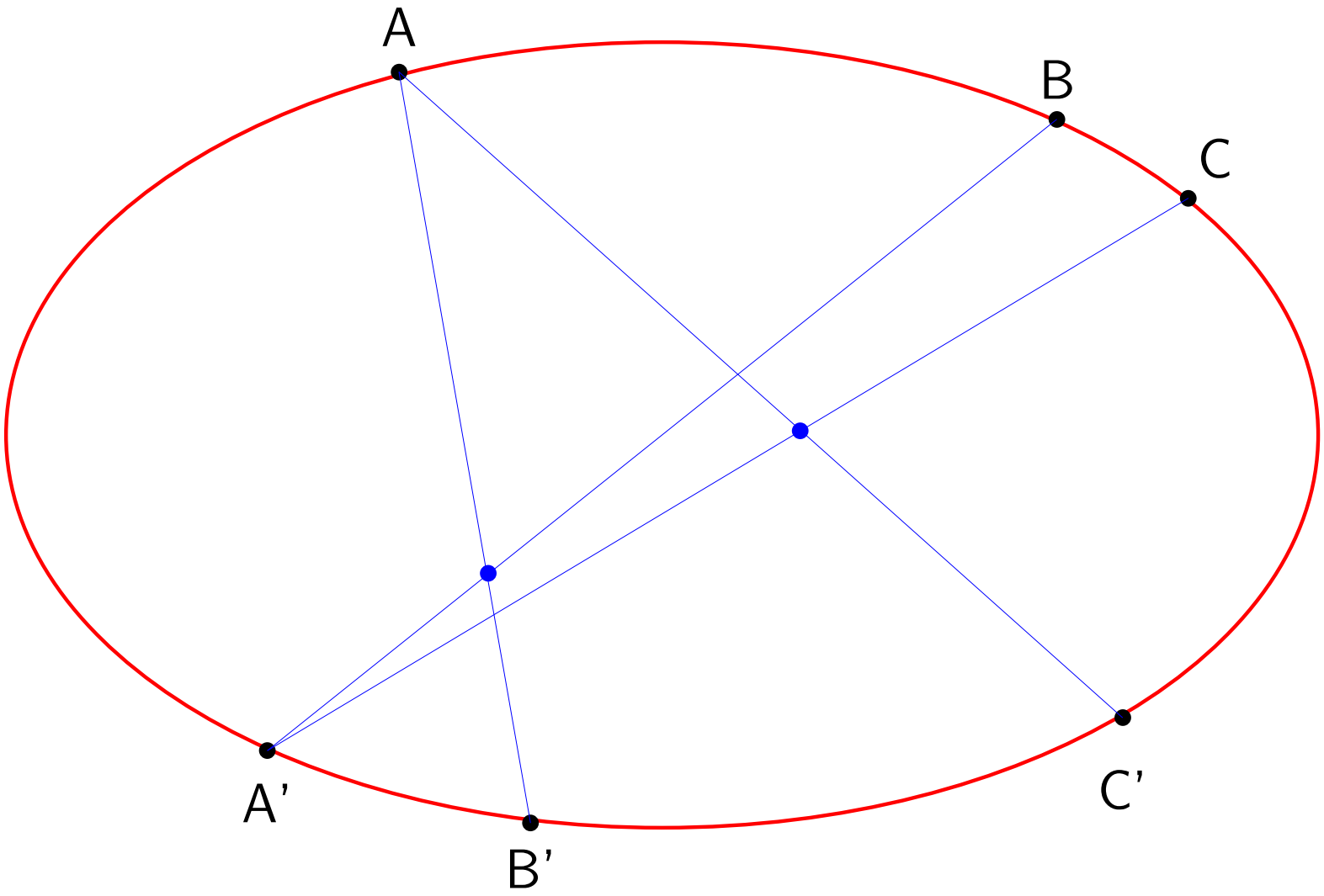
Théorème de Pascal



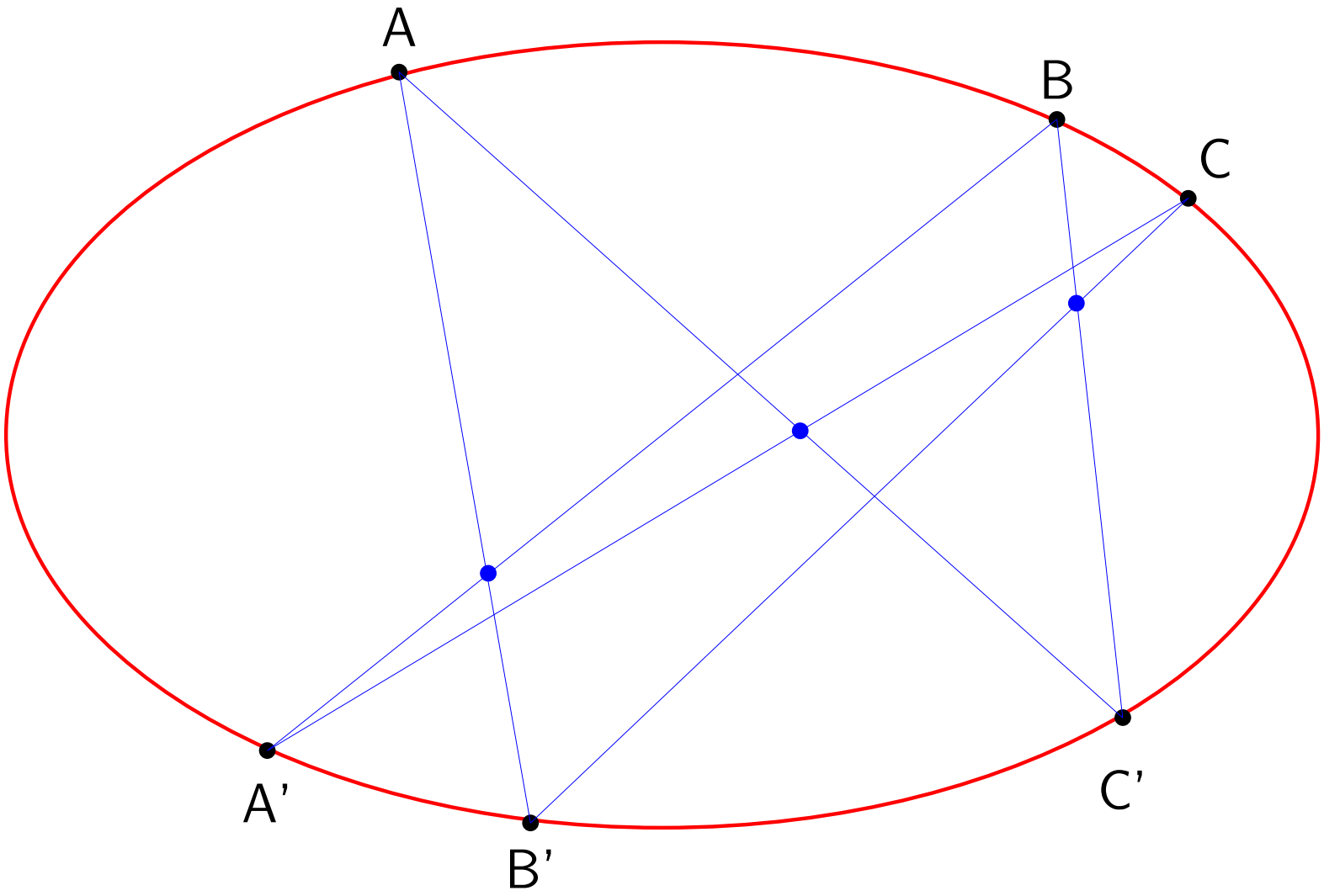
Théorème de Pascal



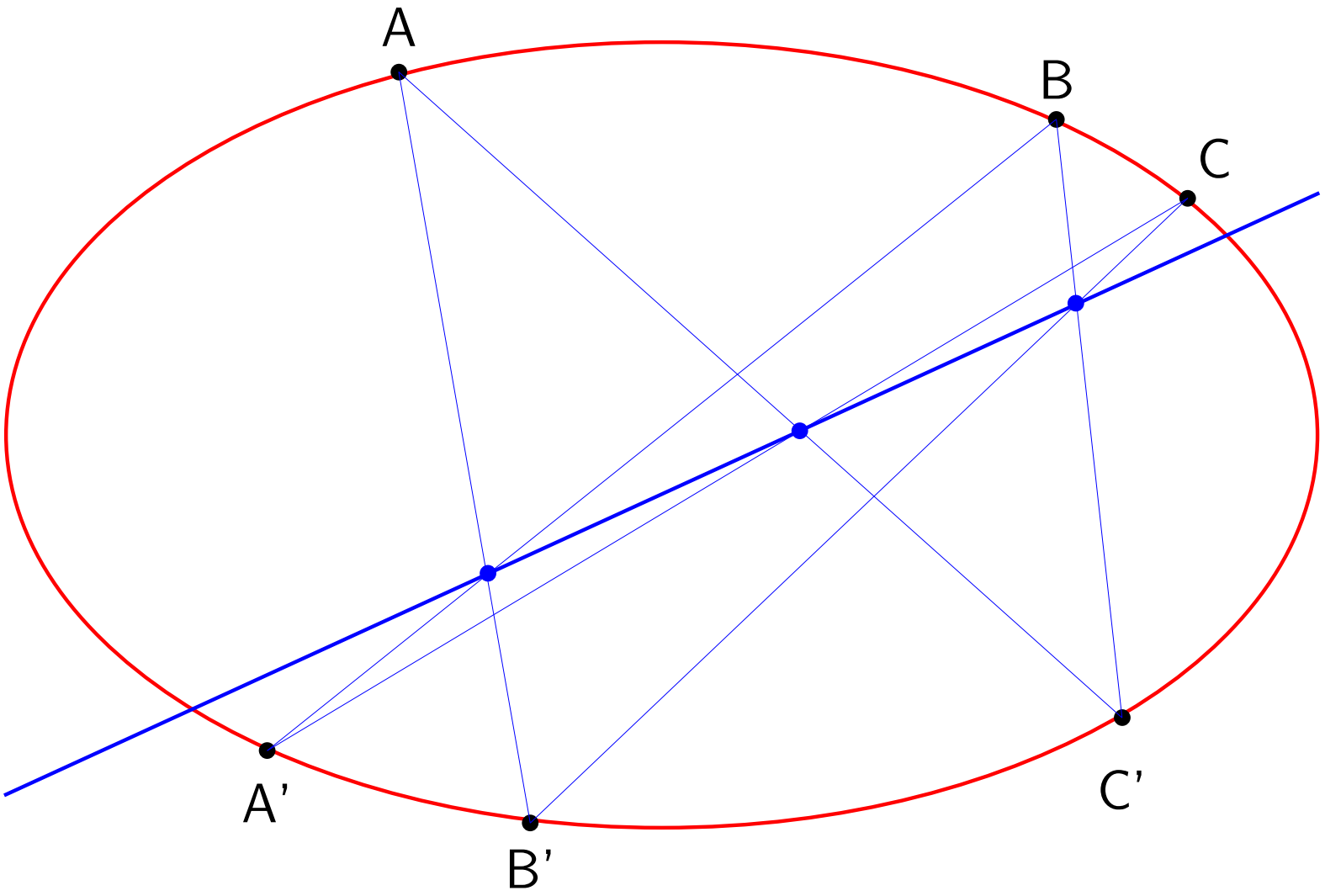
Théorème de Pascal

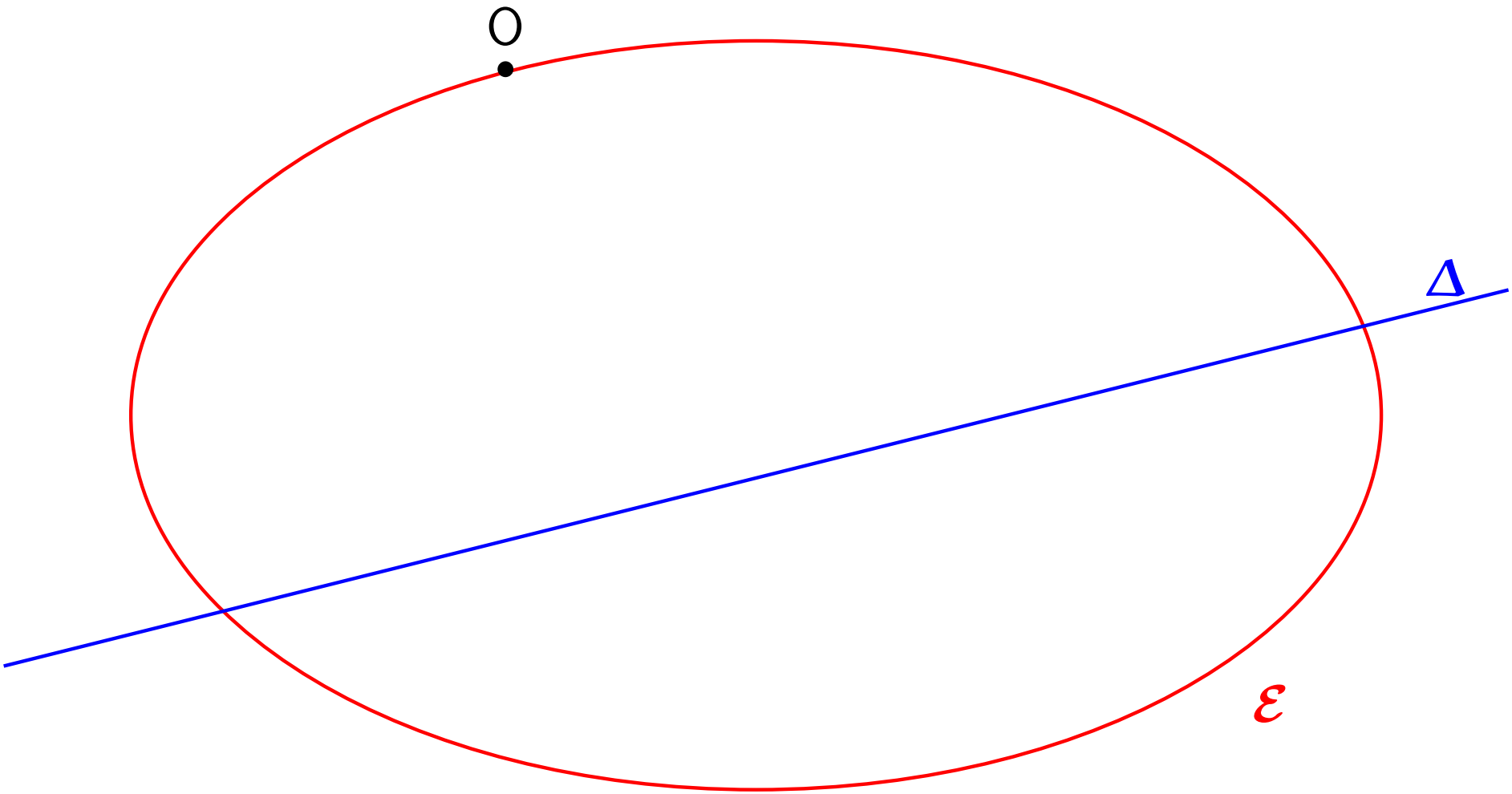


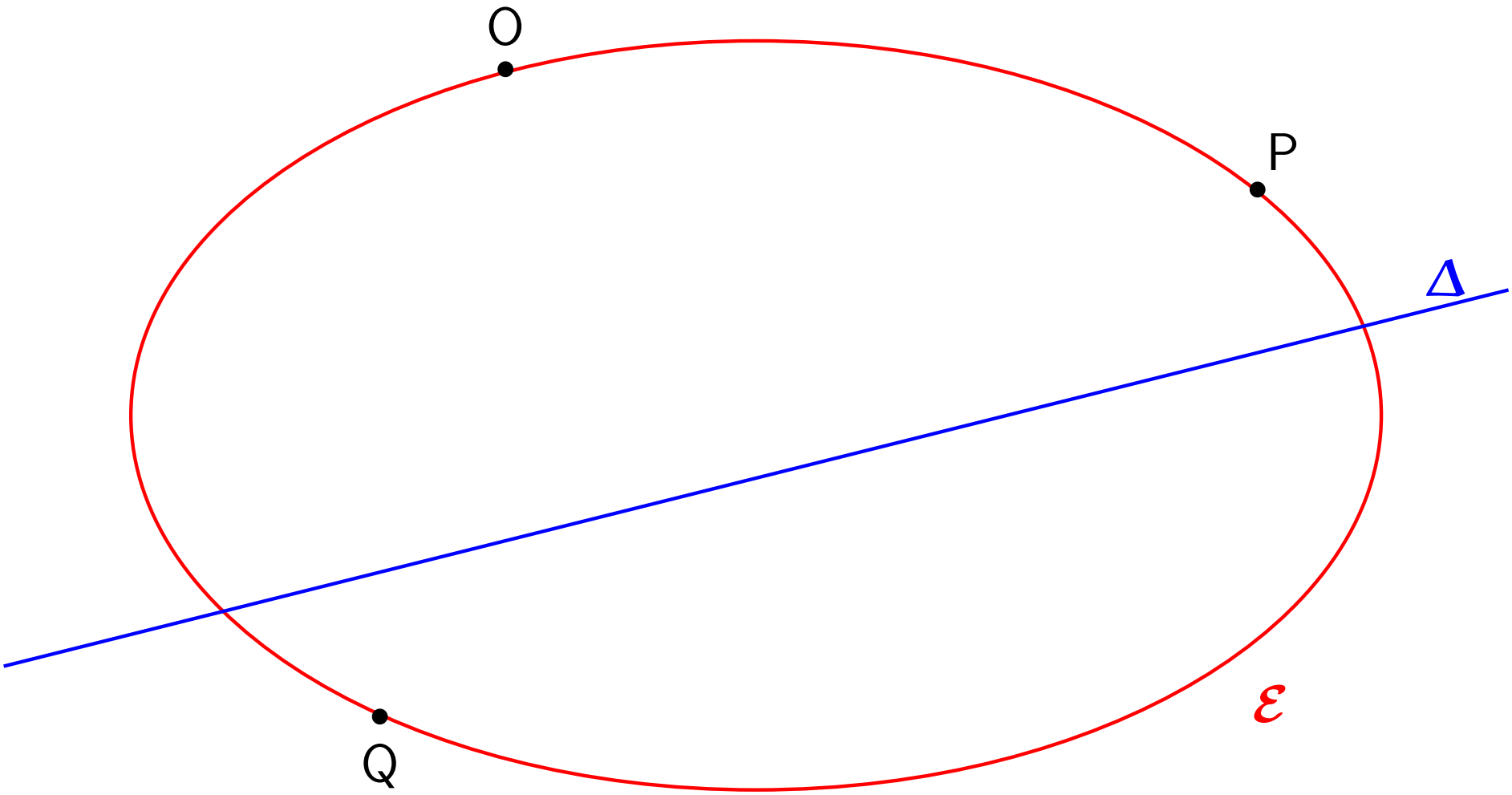
Théorème de Pascal

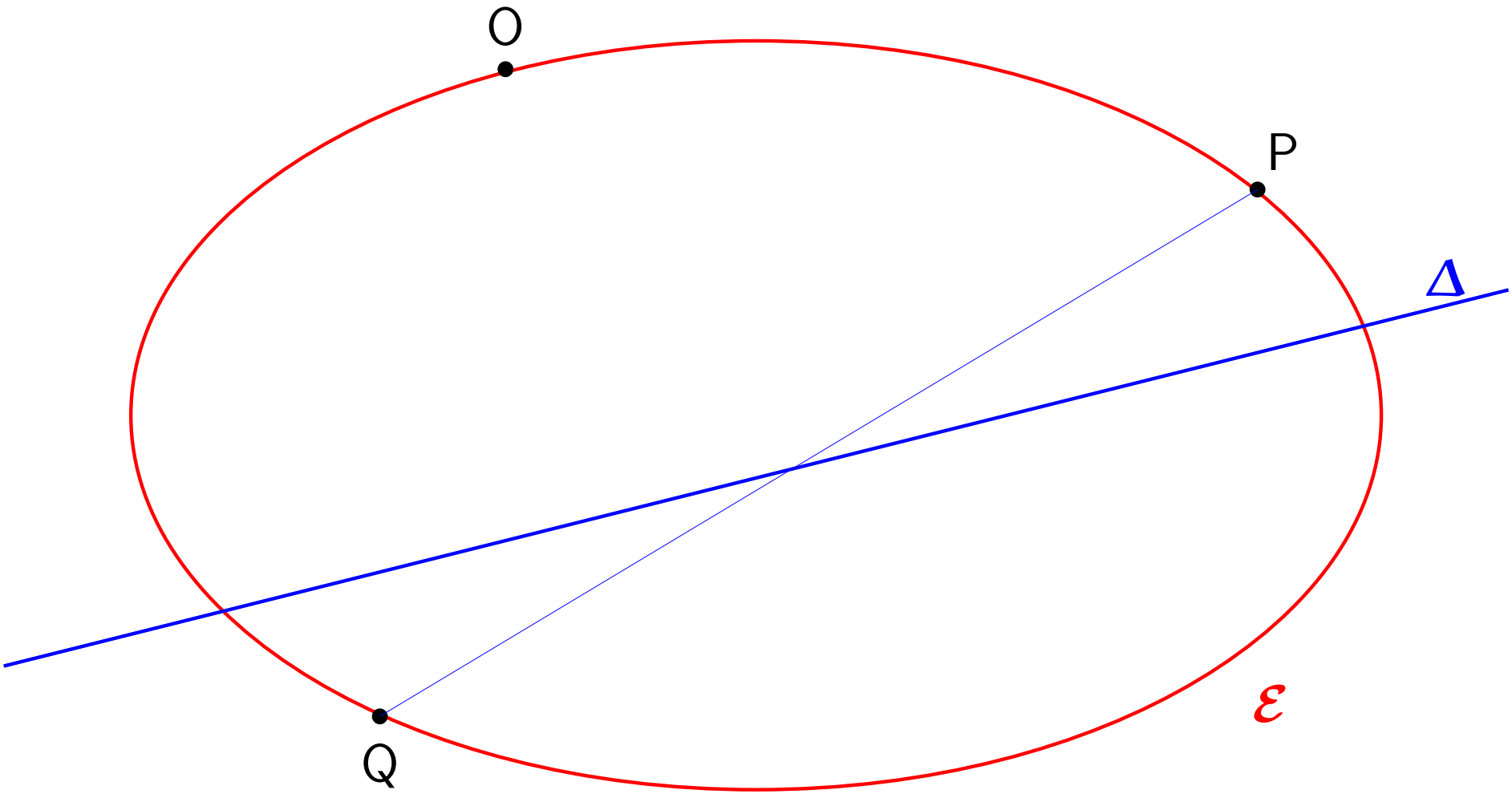


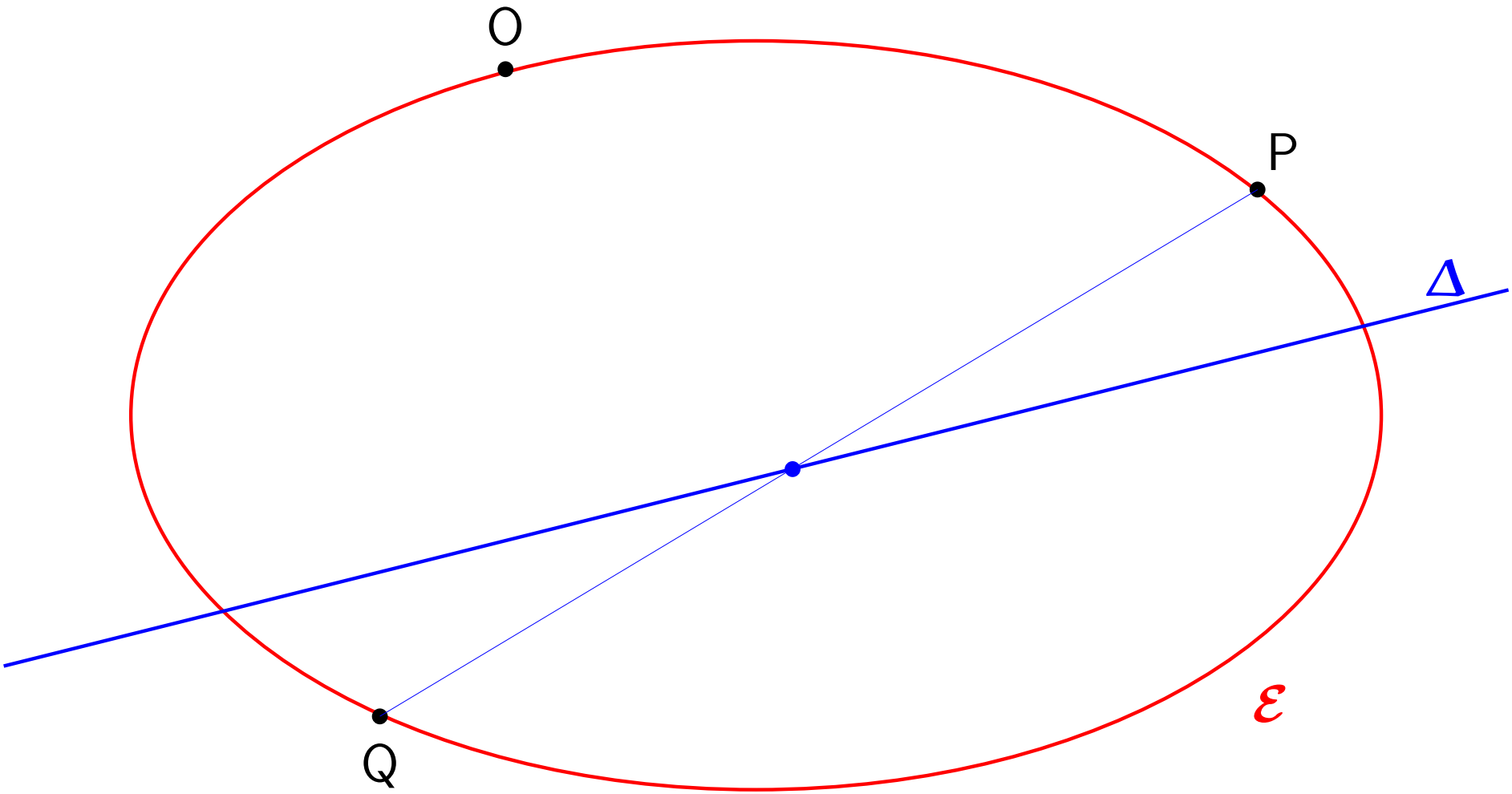
Théorème de Pascal

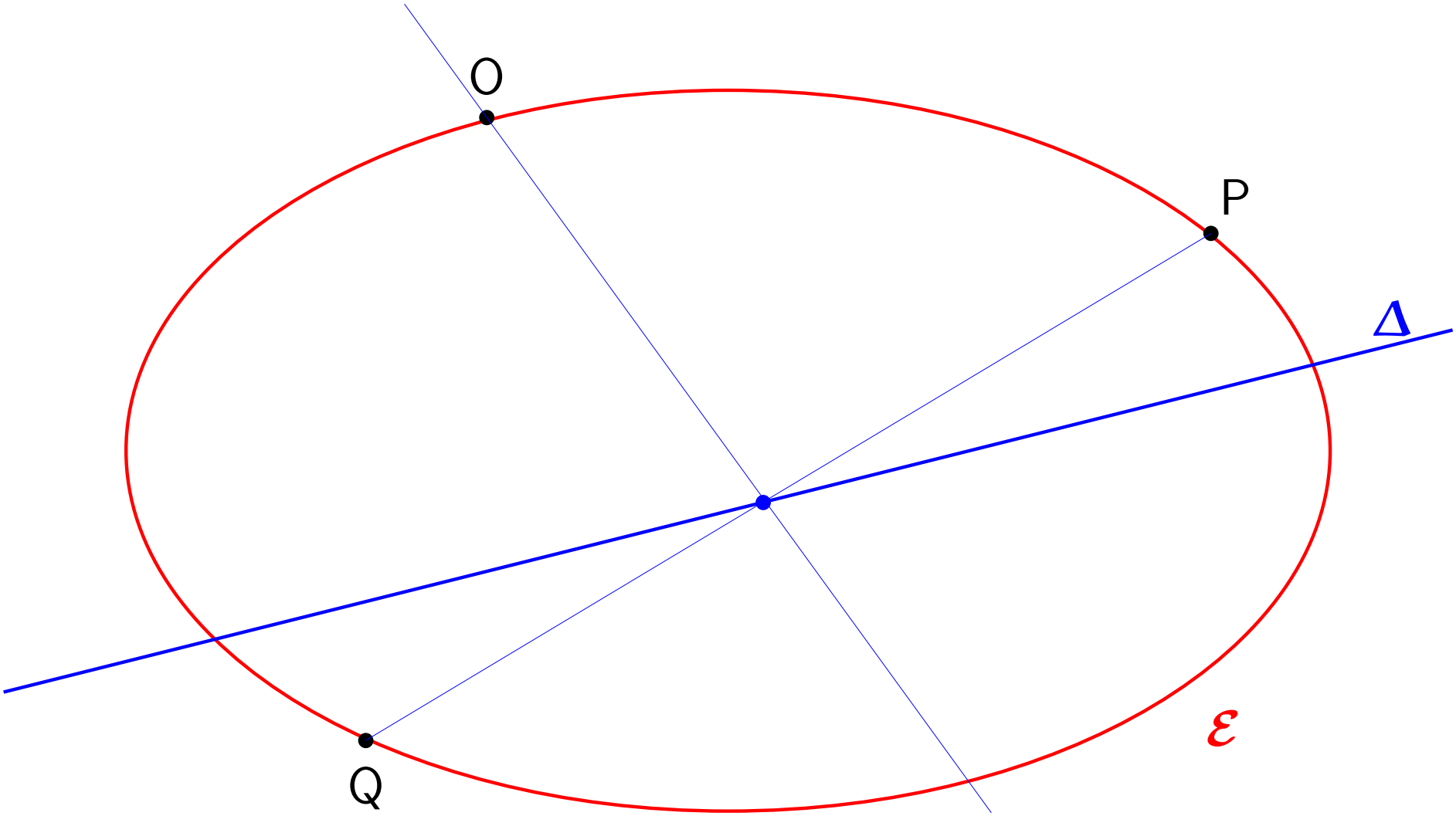


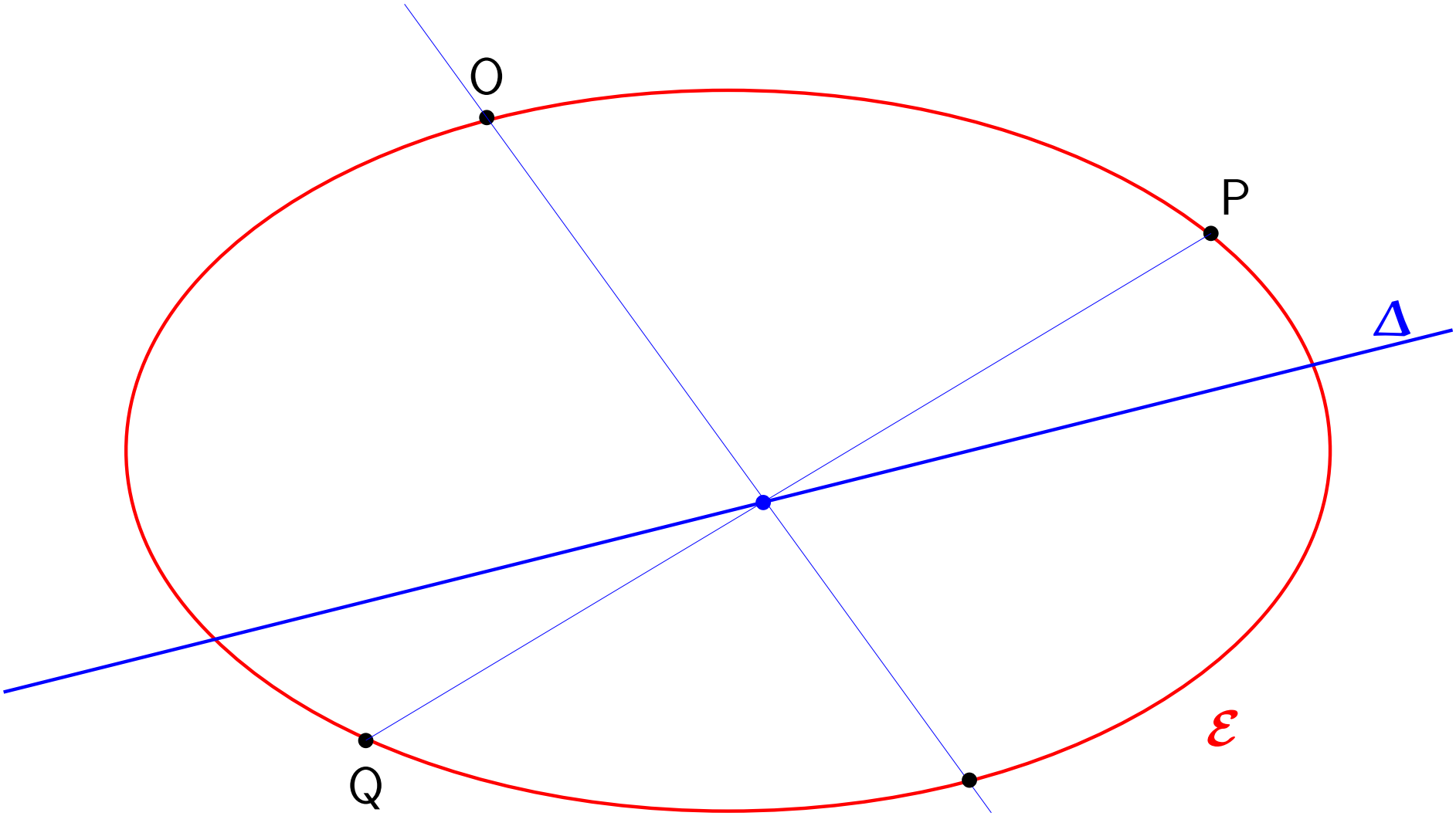

O
Δ
ε

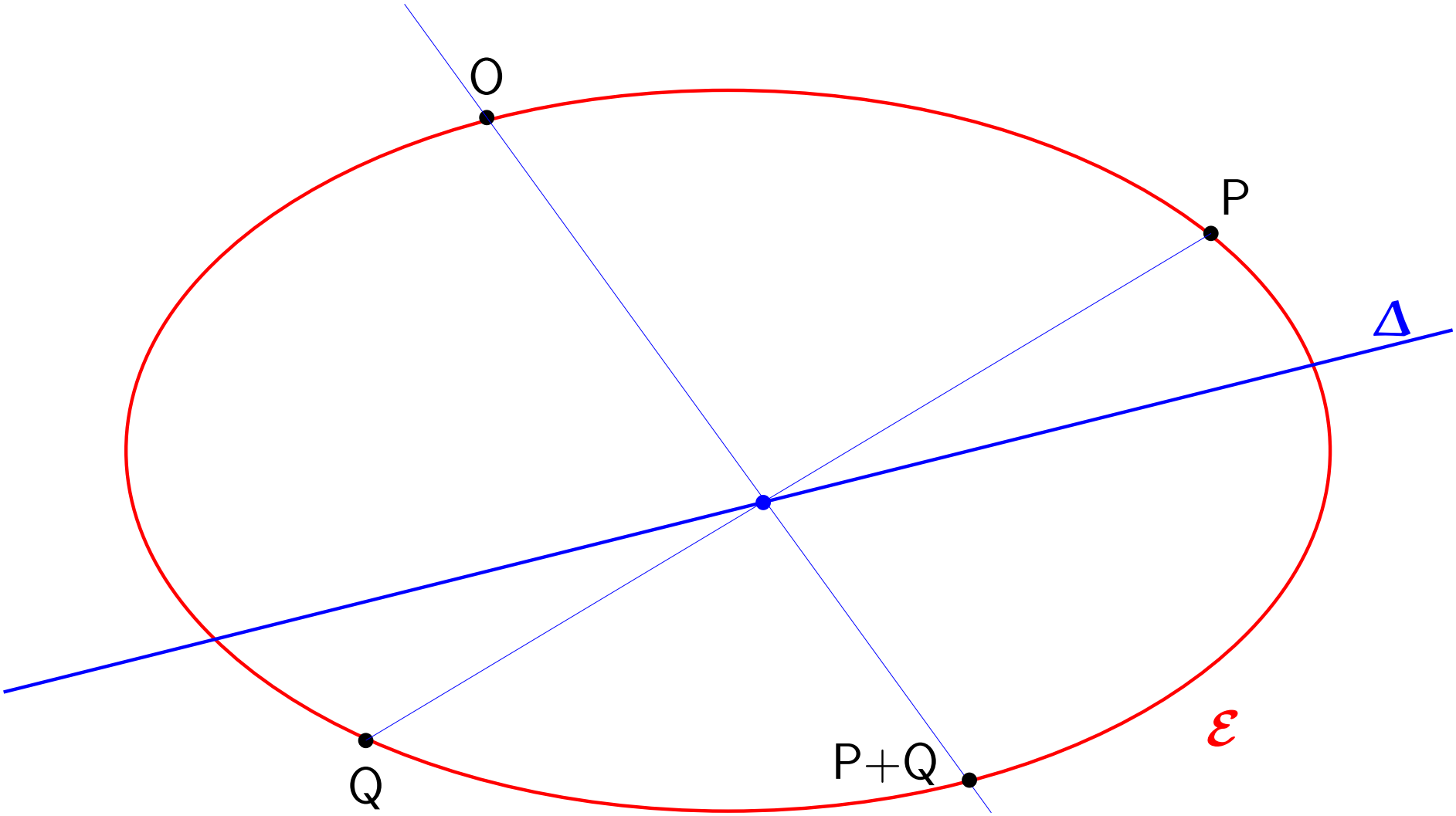

O
P
Δ
ε
Q

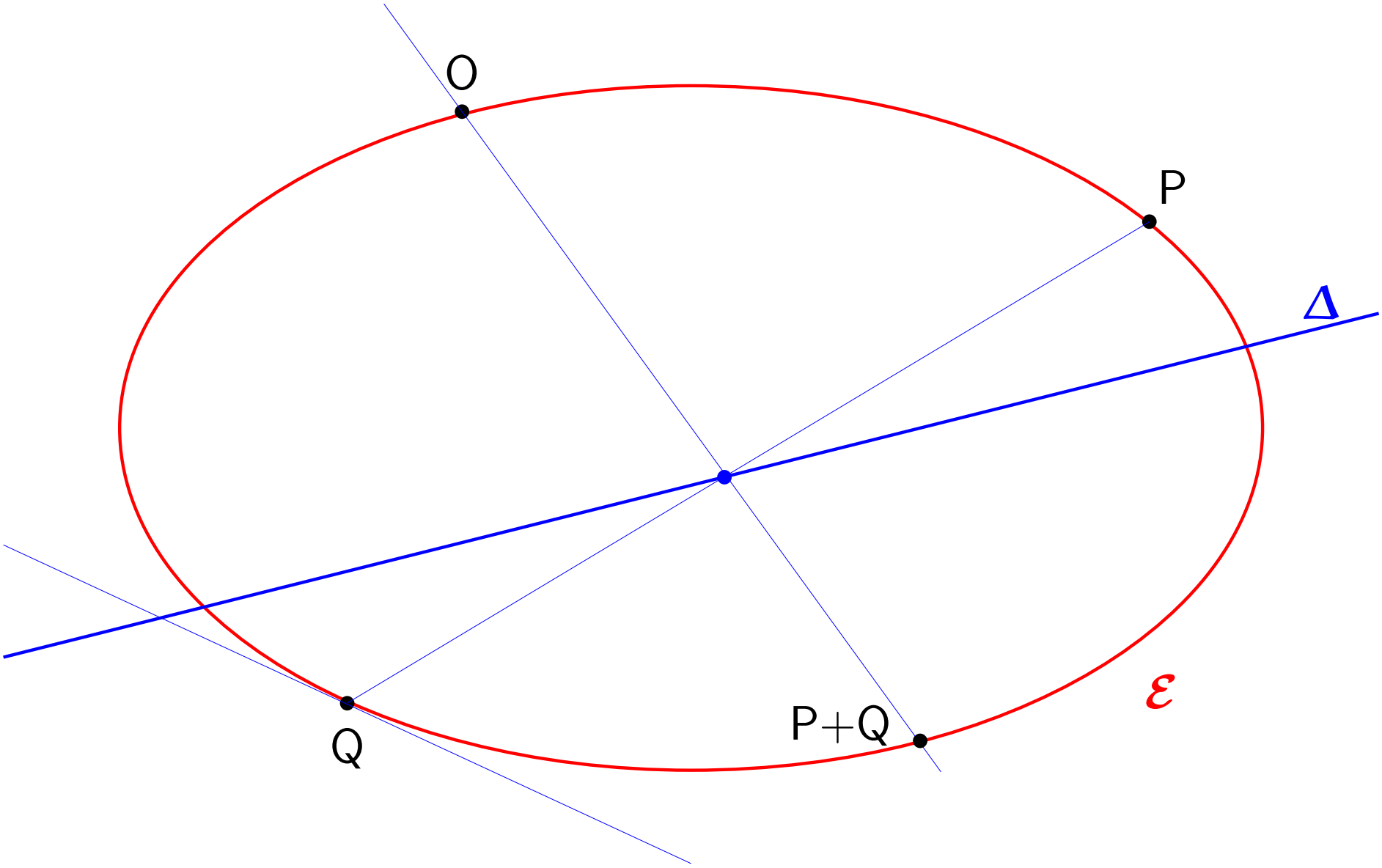

O
P
Δ
ε
Q

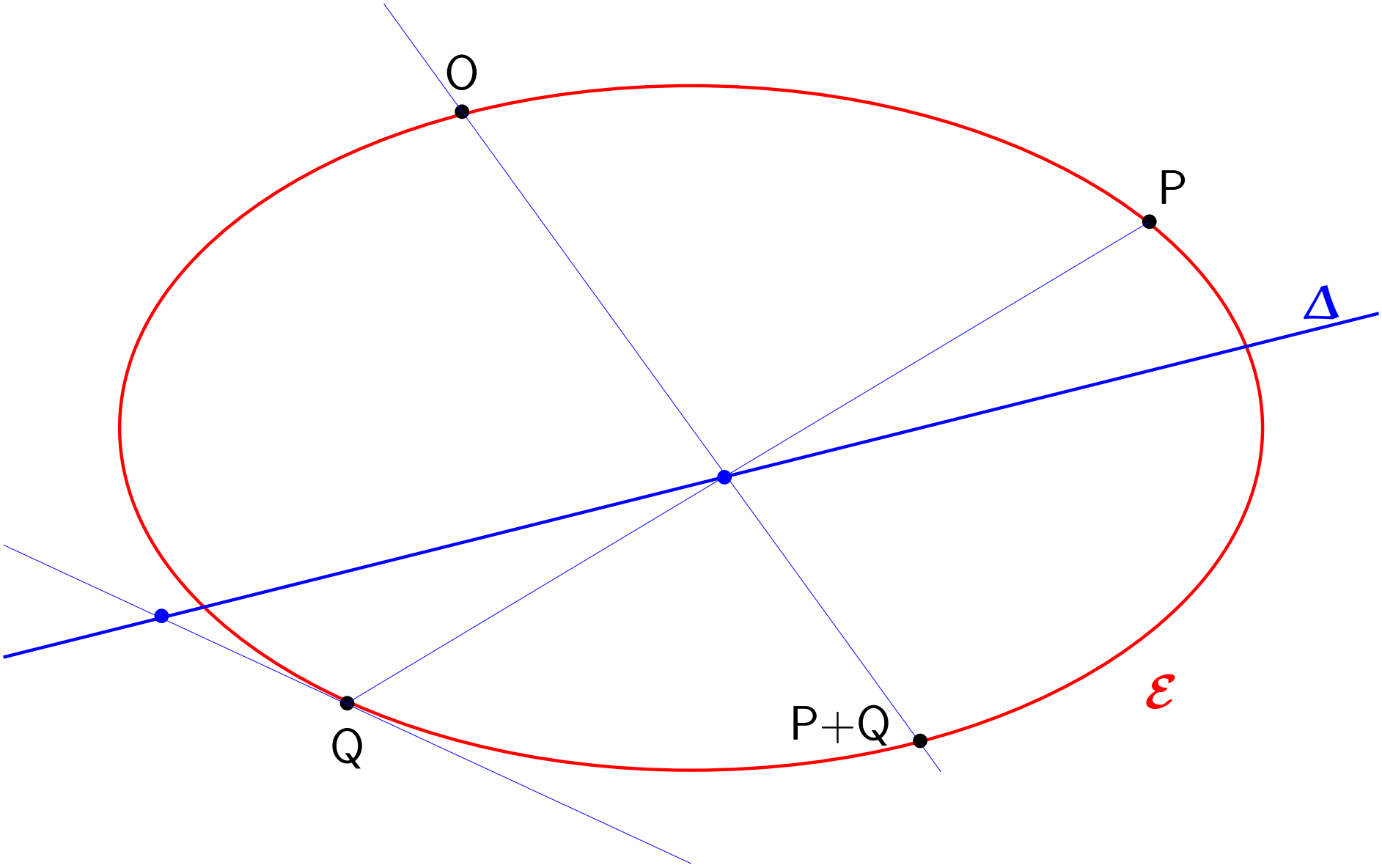

O
P
Δ
ε
Q

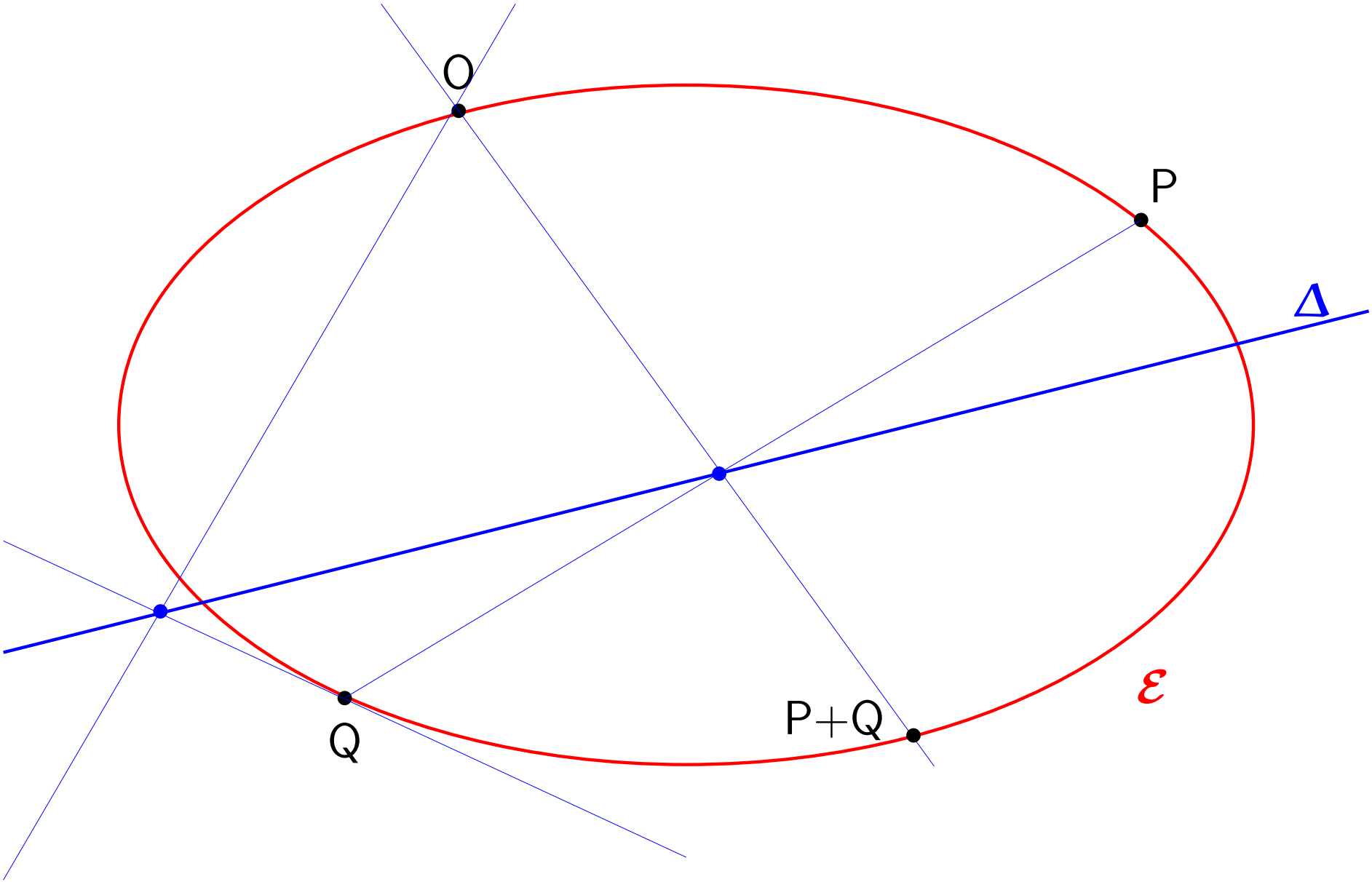

O
P
Δ
ε
Q

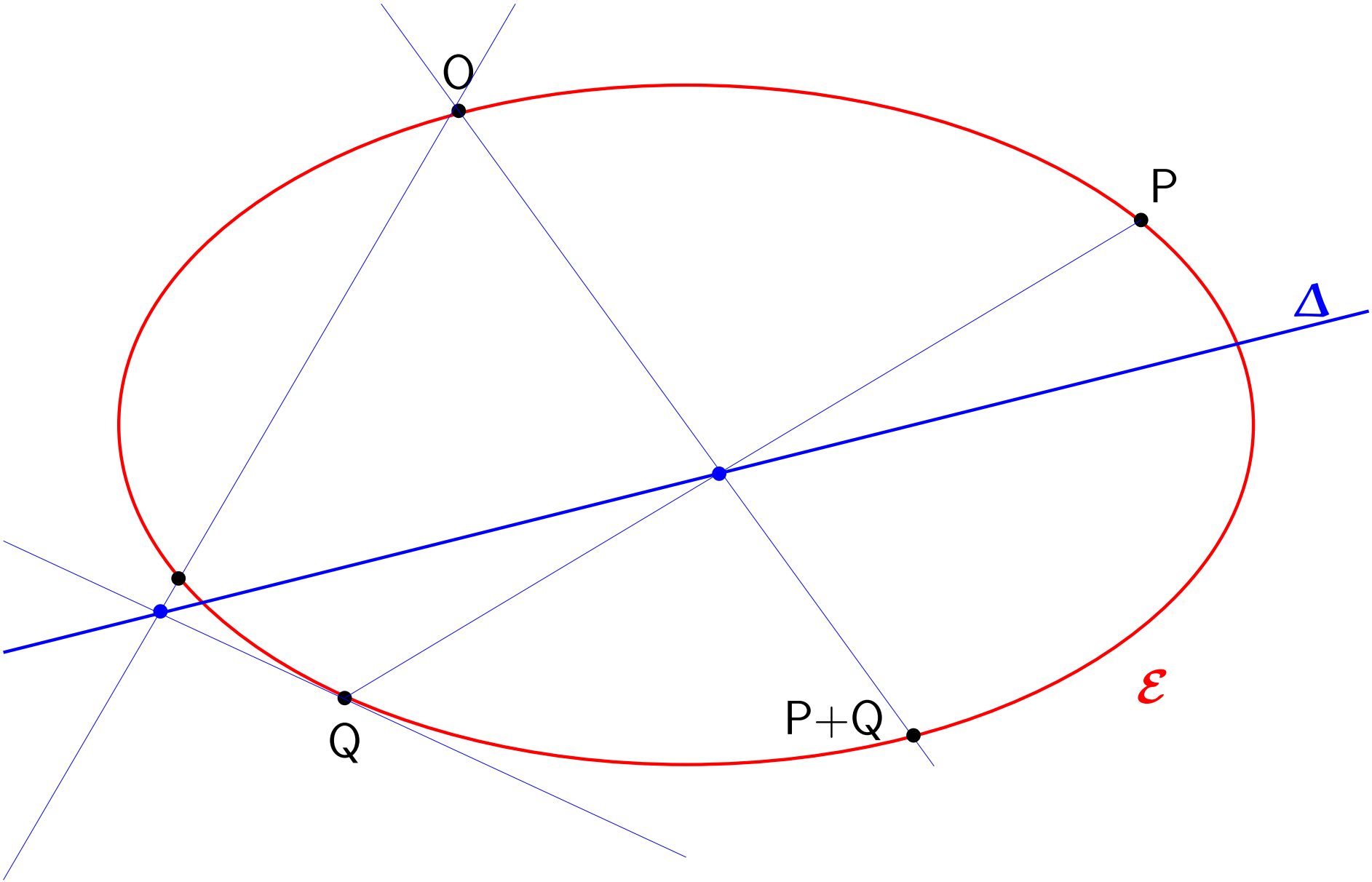

O
P
Δ
Q
ε

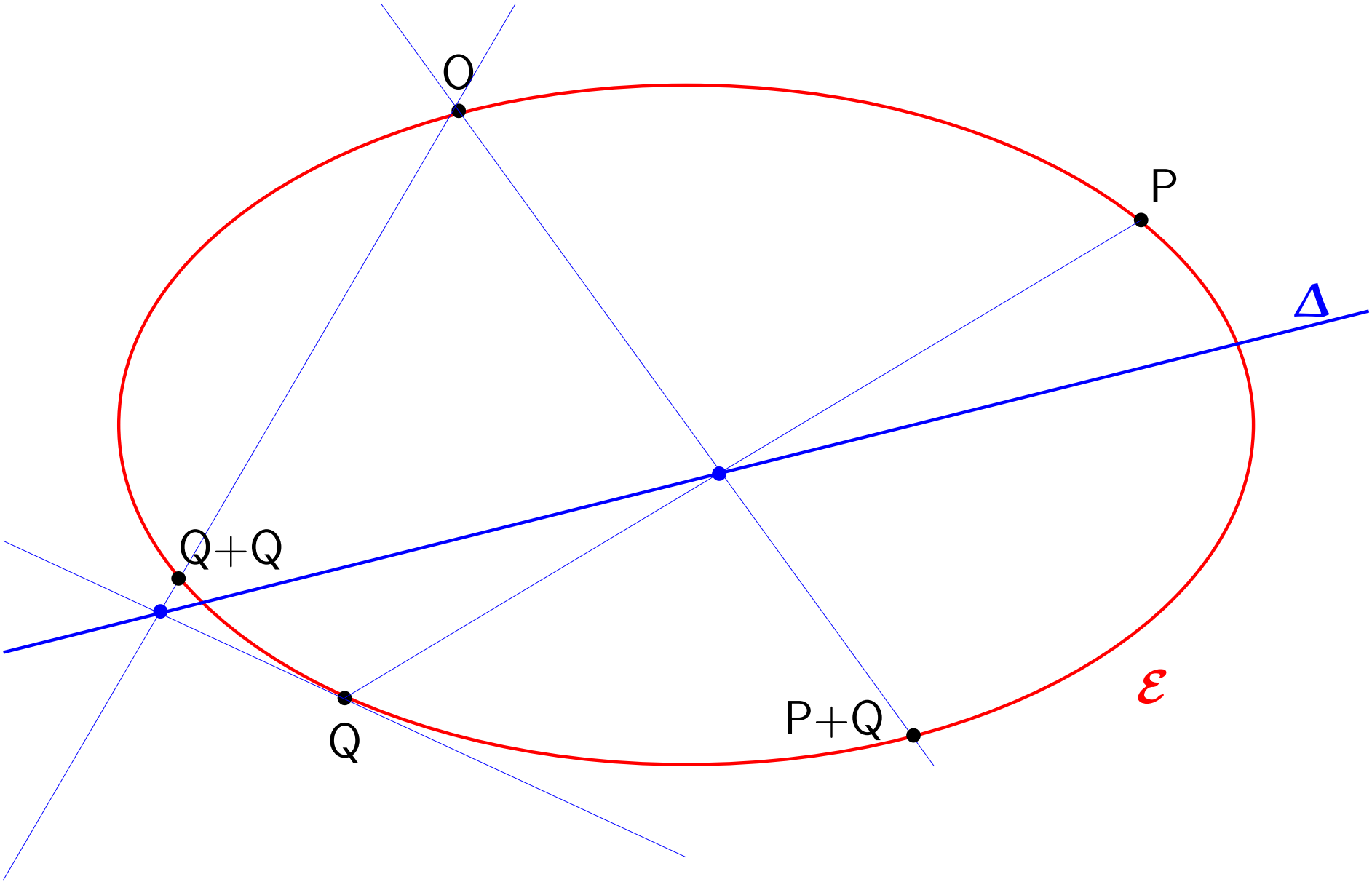

O
P
Δ
ε
Q
P+Q


O
P
Δ
ε
P+Q
Q


O
P
Δ
ε
P+Q
Q


O
P
Δ
ε
P+Q
Q


O
P
Δ
ε
P+Q
Q


O
P
Δ
Q+Q
Q
P+Q
ε

Théorème

$\mathcal{E} \setminus \Delta$, muni de la loi $+$, est un groupe (commutatif) ! L'élément neutre est O.

Théorème

$\mathcal{E} \setminus \Delta$, muni de la loi $+$, est un groupe (commutatif) ! L'élément neutre est O.

Preuve -

Théorème

$\mathcal{E} \setminus \Delta$, muni de la loi $+$, est un groupe (commutatif) ! L'élément neutre est O.

Preuve -

- Élément neutre : en effet, $O + P = P$ (voir dessin)

Théorème

$\mathcal{E} \setminus \Delta$, muni de la loi $+$, est un groupe (commutatif) ! L'élément neutre est O.

Preuve -

- Élément neutre : en effet, $O + P = P$ (voir dessin)
- Symétrique : voir dessin

Théorème

$\mathcal{E} \setminus \Delta$, muni de la loi $+$, est un groupe (commutatif) ! L'élément neutre est O.

Preuve -

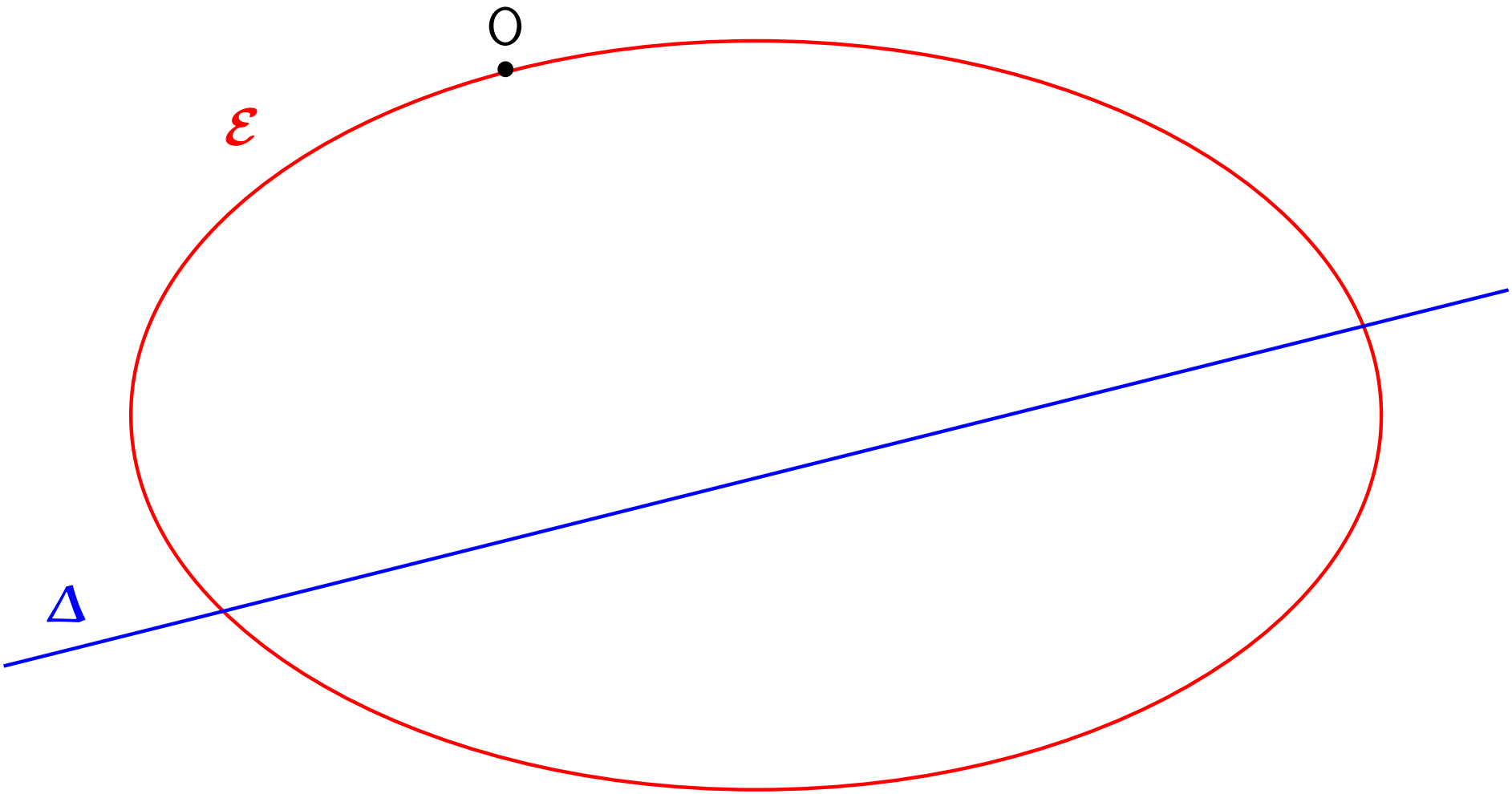
- Élément neutre : en effet, $O + P = P$ (voir dessin)
- Symétrique : voir dessin
- Commutativité : trivial

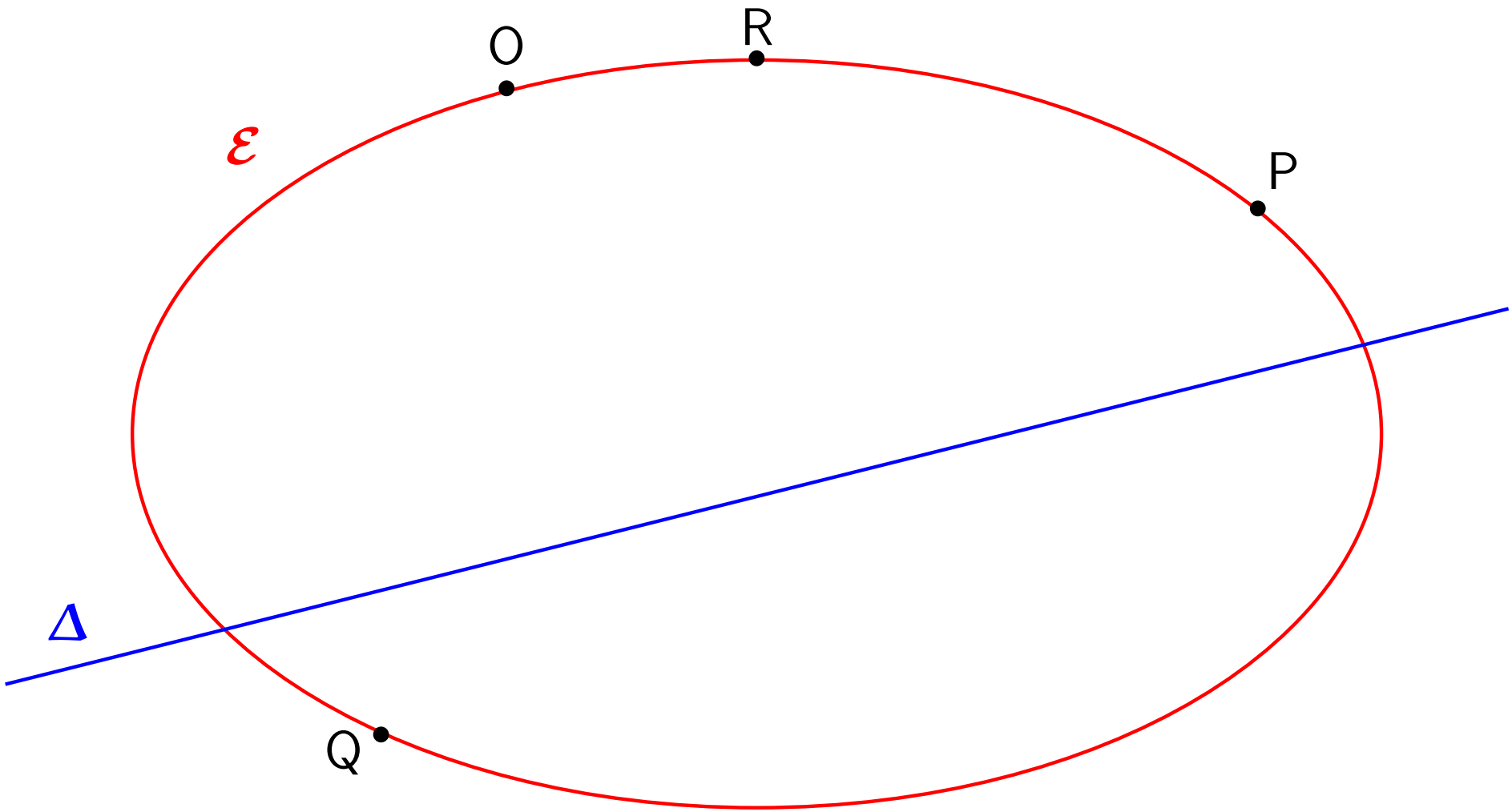
Théorème

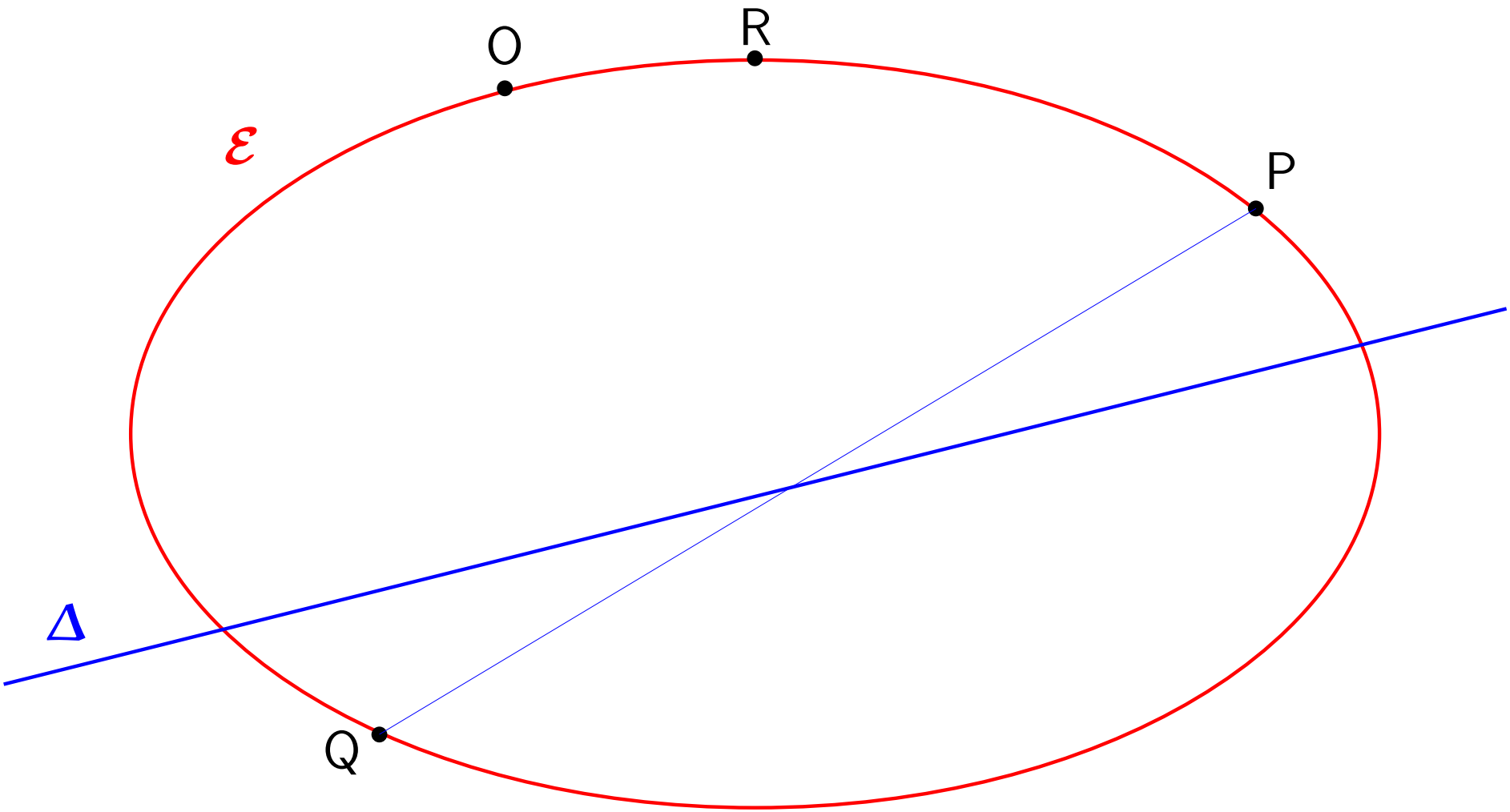
$\mathcal{E} \setminus \Delta$, muni de la loi $+$, est un groupe (commutatif) ! L'élément neutre est O.

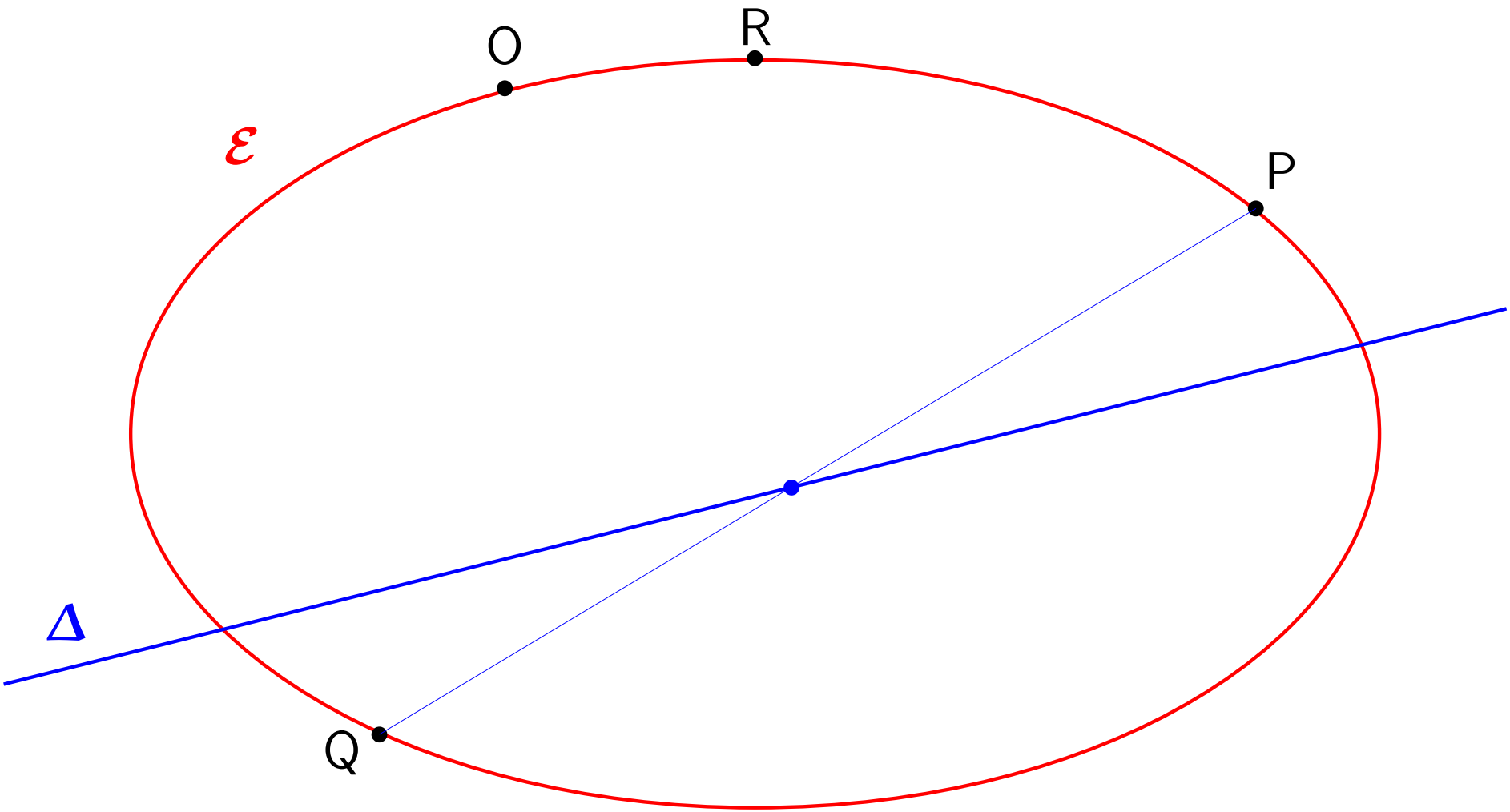
Preuve -

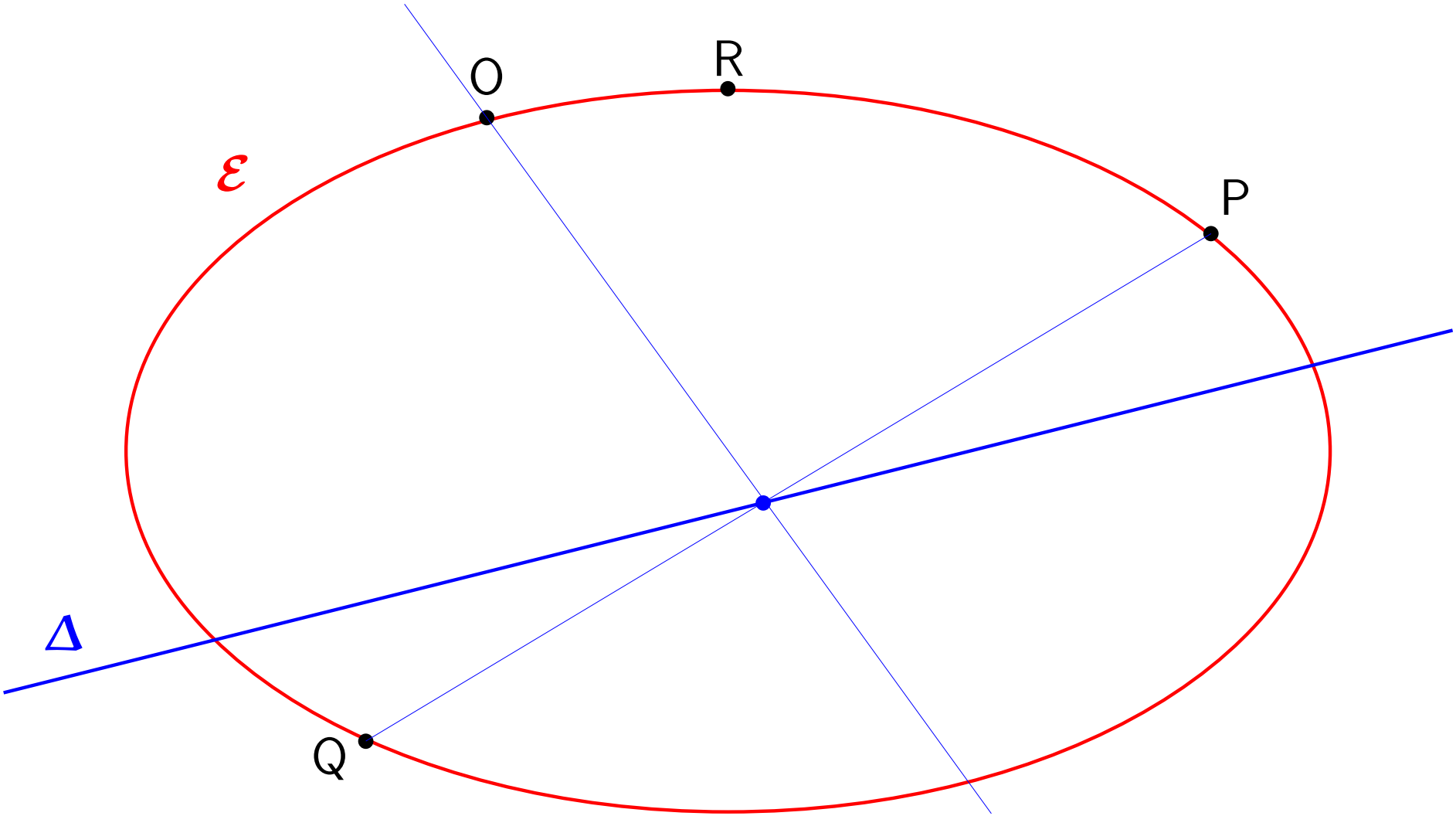
- Élément neutre : en effet, $O + P = P$ (voir dessin)
- Symétrique : voir dessin
- Commutativité : trivial
- Associativité : $(P + Q) + R = P + (Q + R)$ (théorème de Pascal)

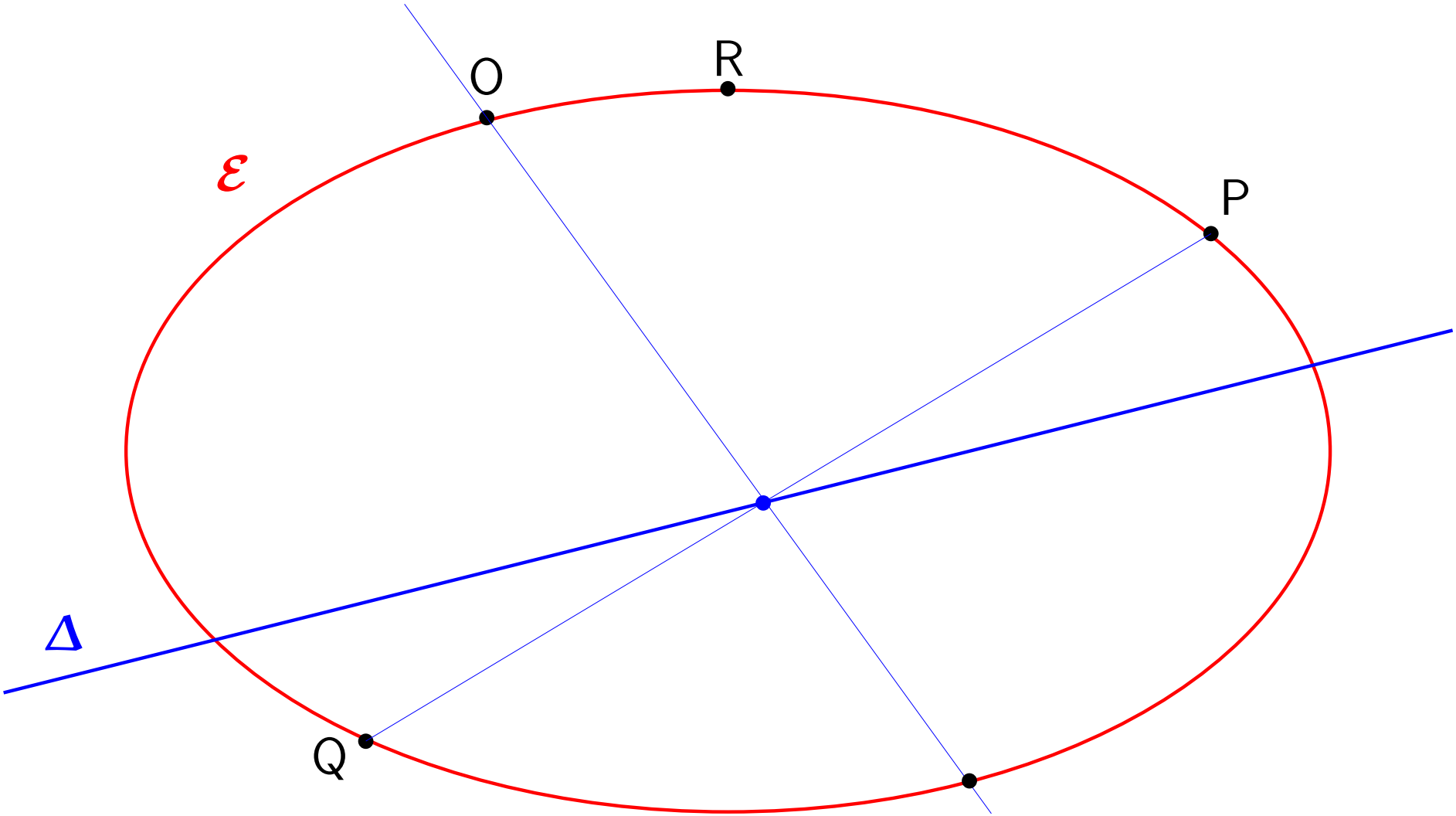

O
$\mathcal{E}$
Δ

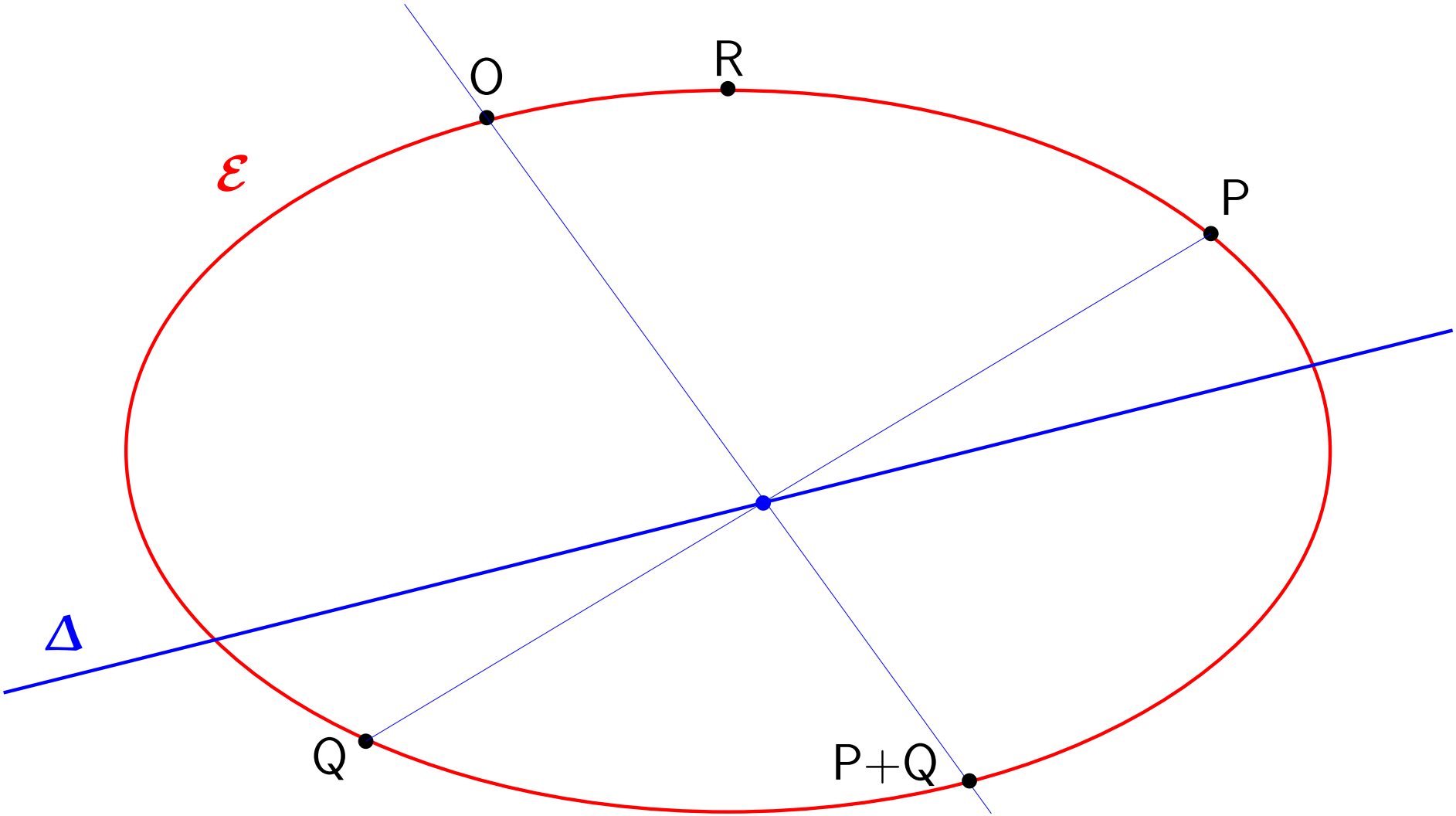

O
R
P
Q
$\mathcal{E}$
Δ

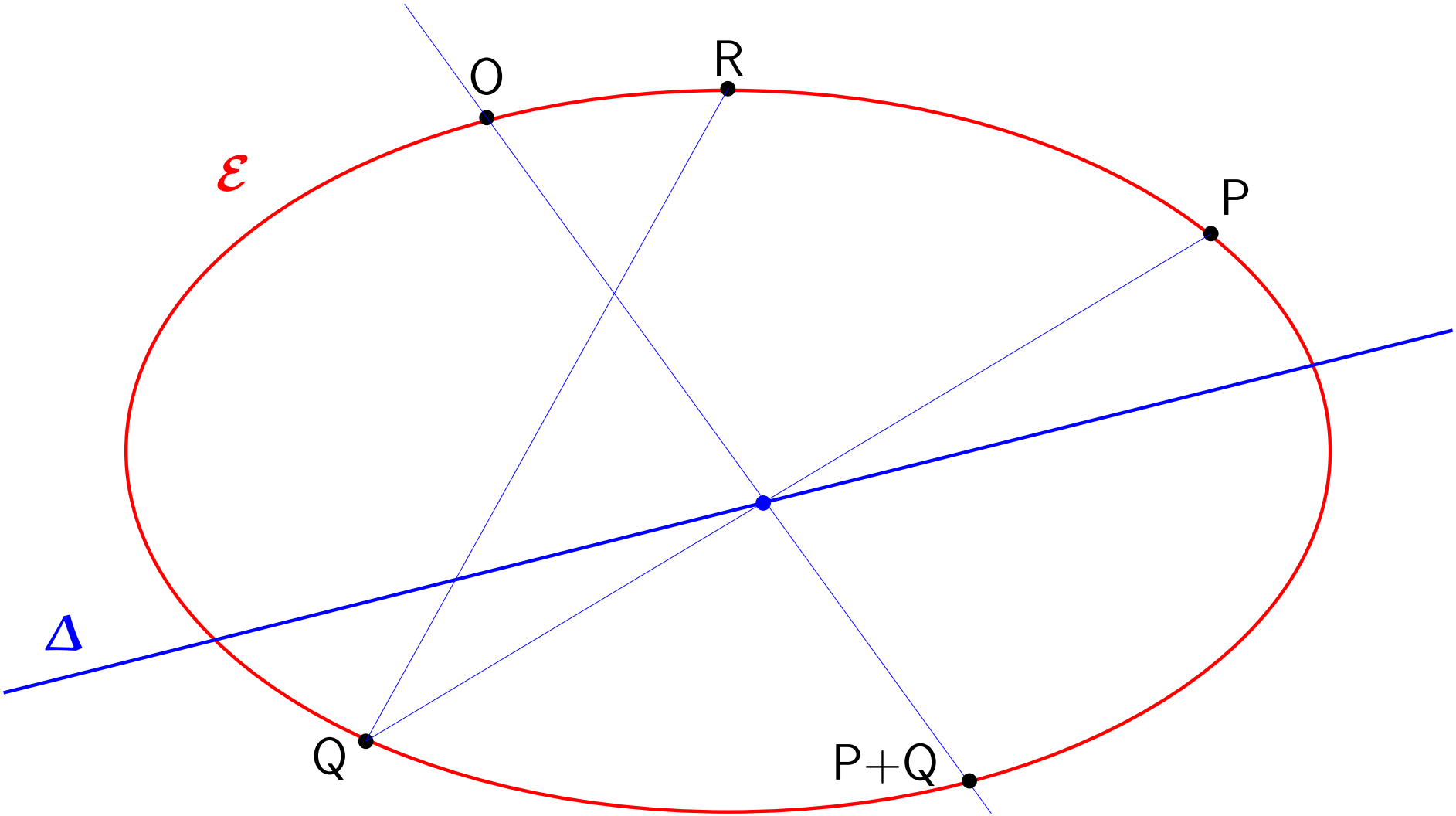

O
R
P
Q
$\mathcal{E}$
Δ

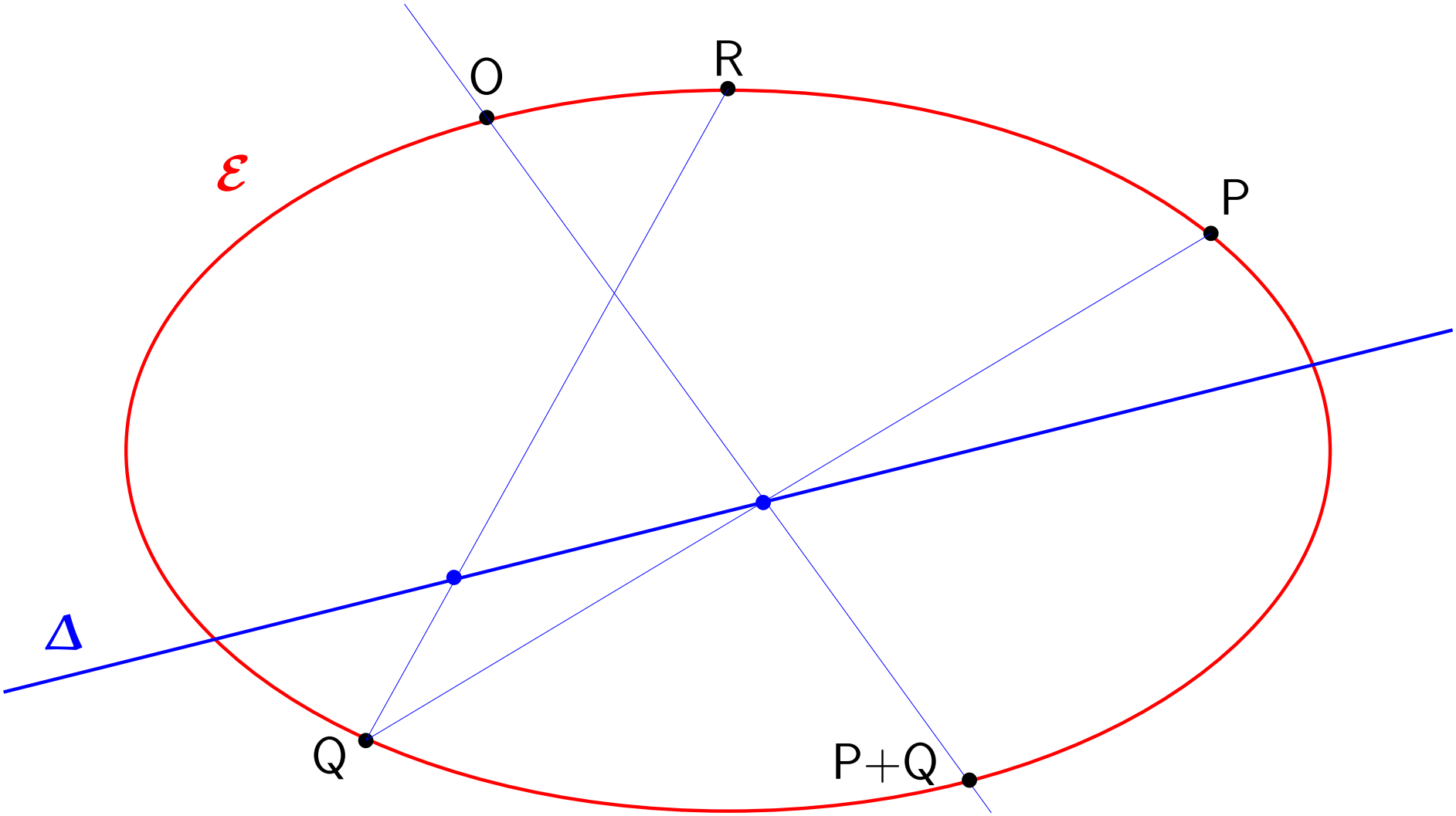

O
R
P
Q
ε
Δ

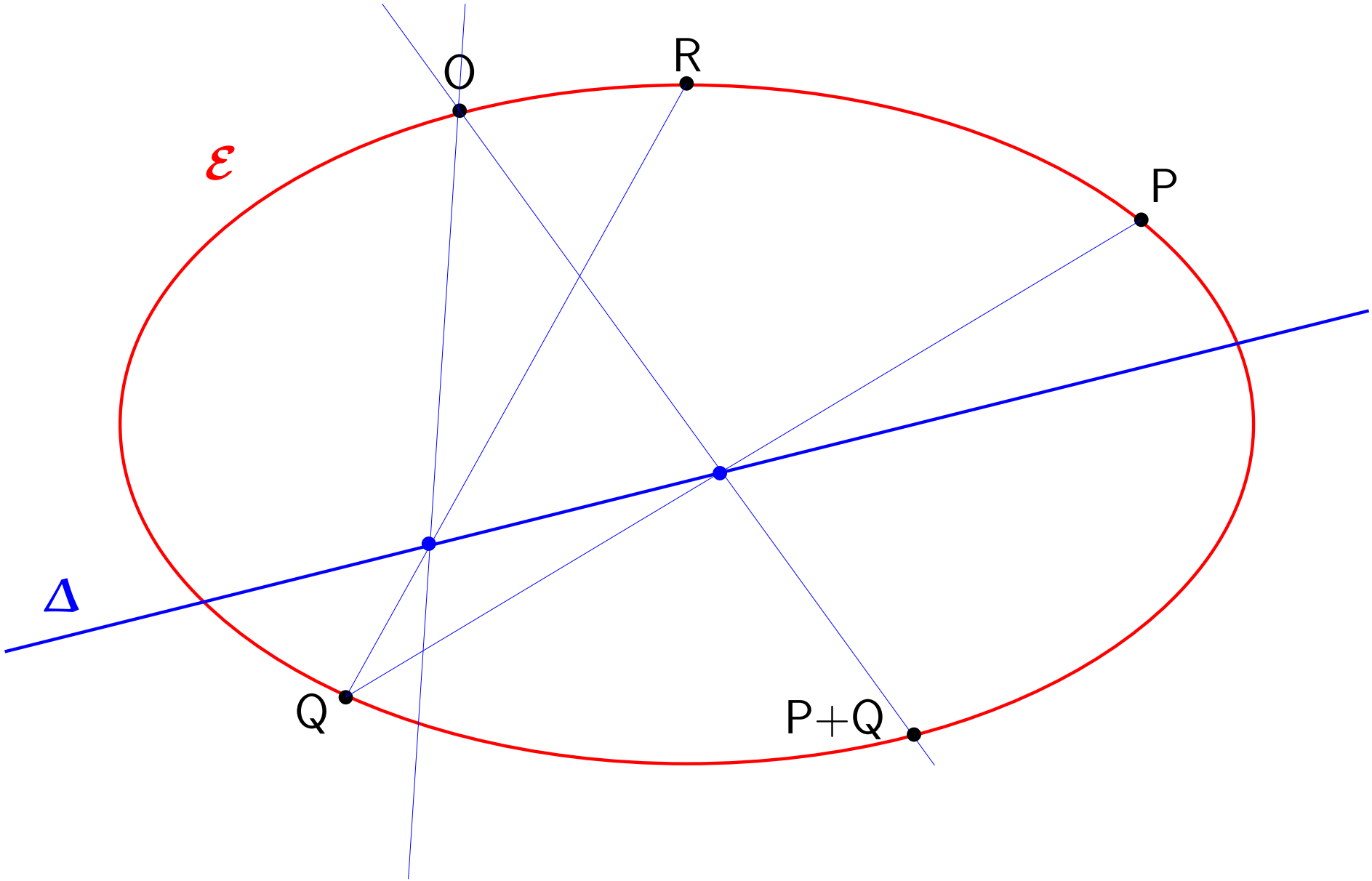

O
R
P
Q
ε
Δ

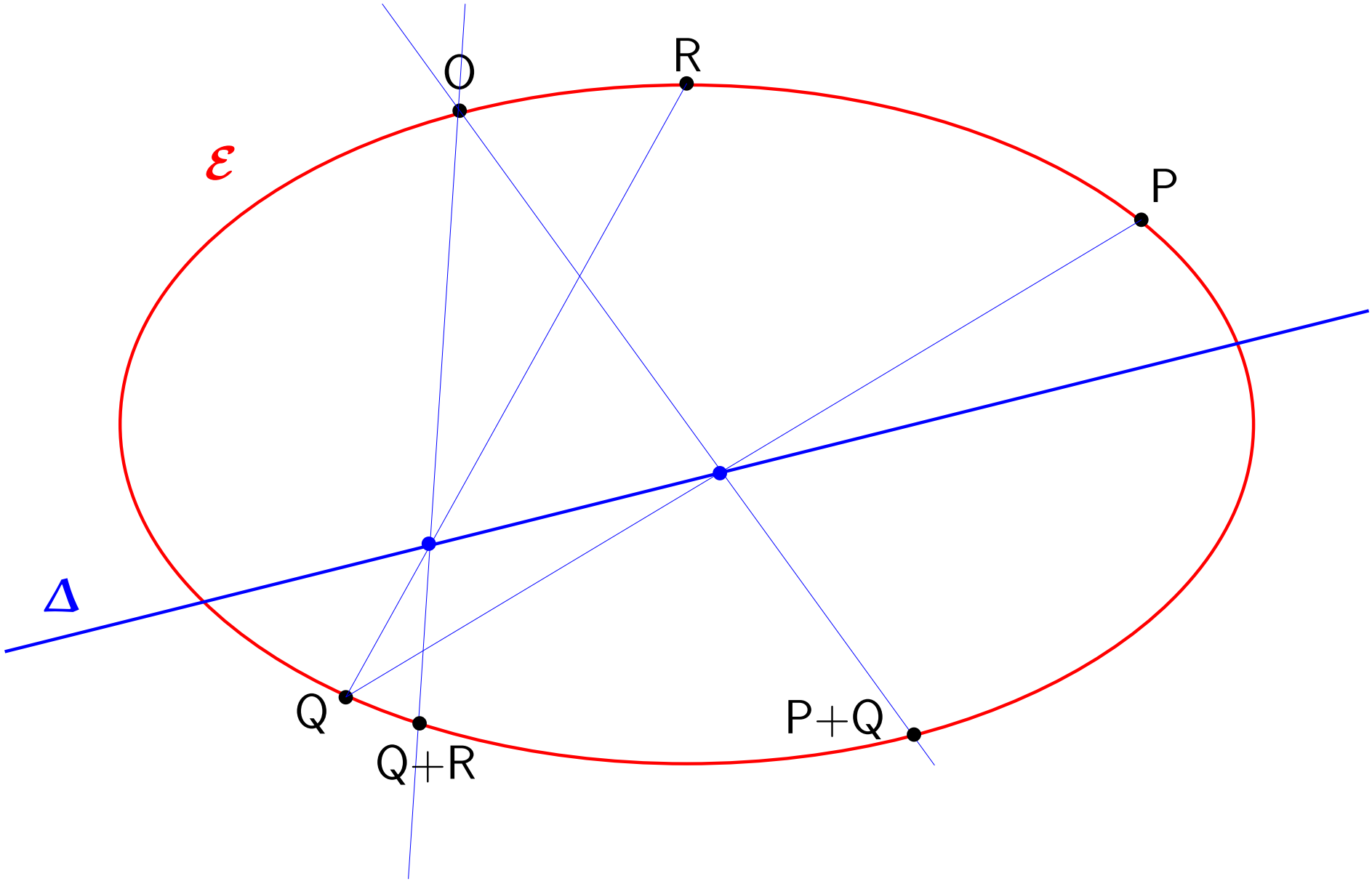

O
R
P
Q
ε
Δ

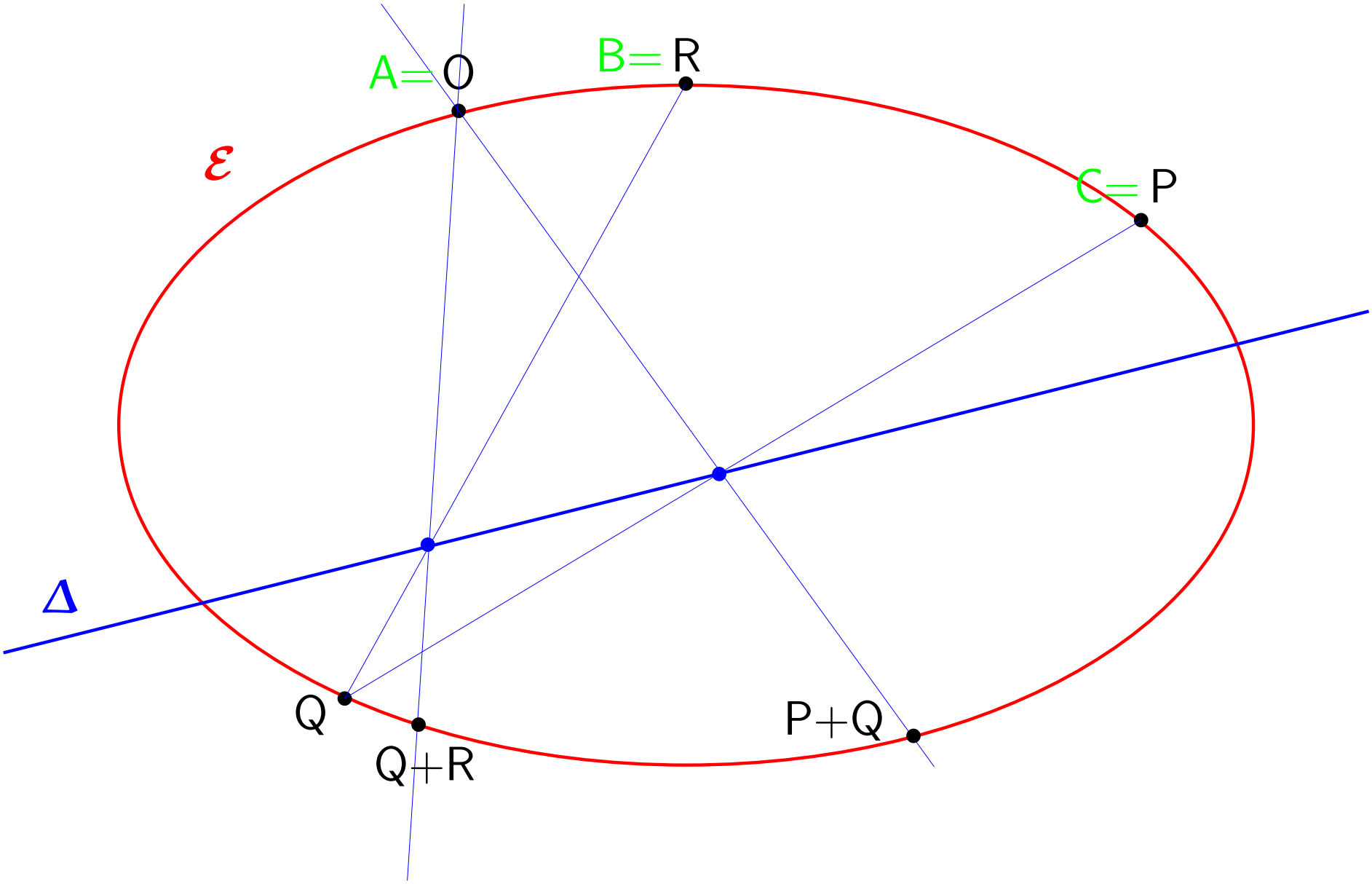

O
R
P
$\mathcal{E}$
Δ
Q
P+Q

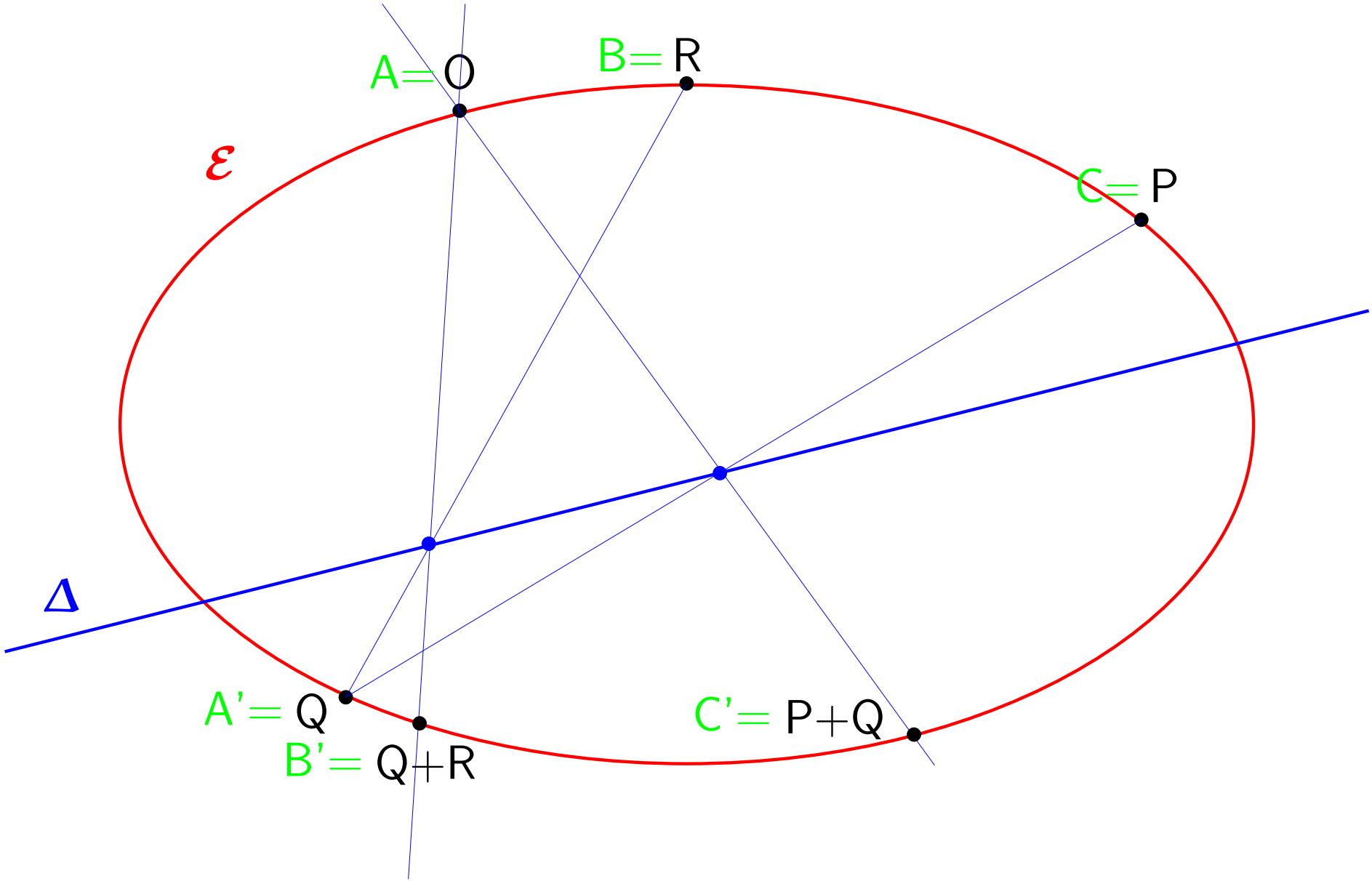

O
R
P
$\mathcal{E}$
Δ
Q
P+Q

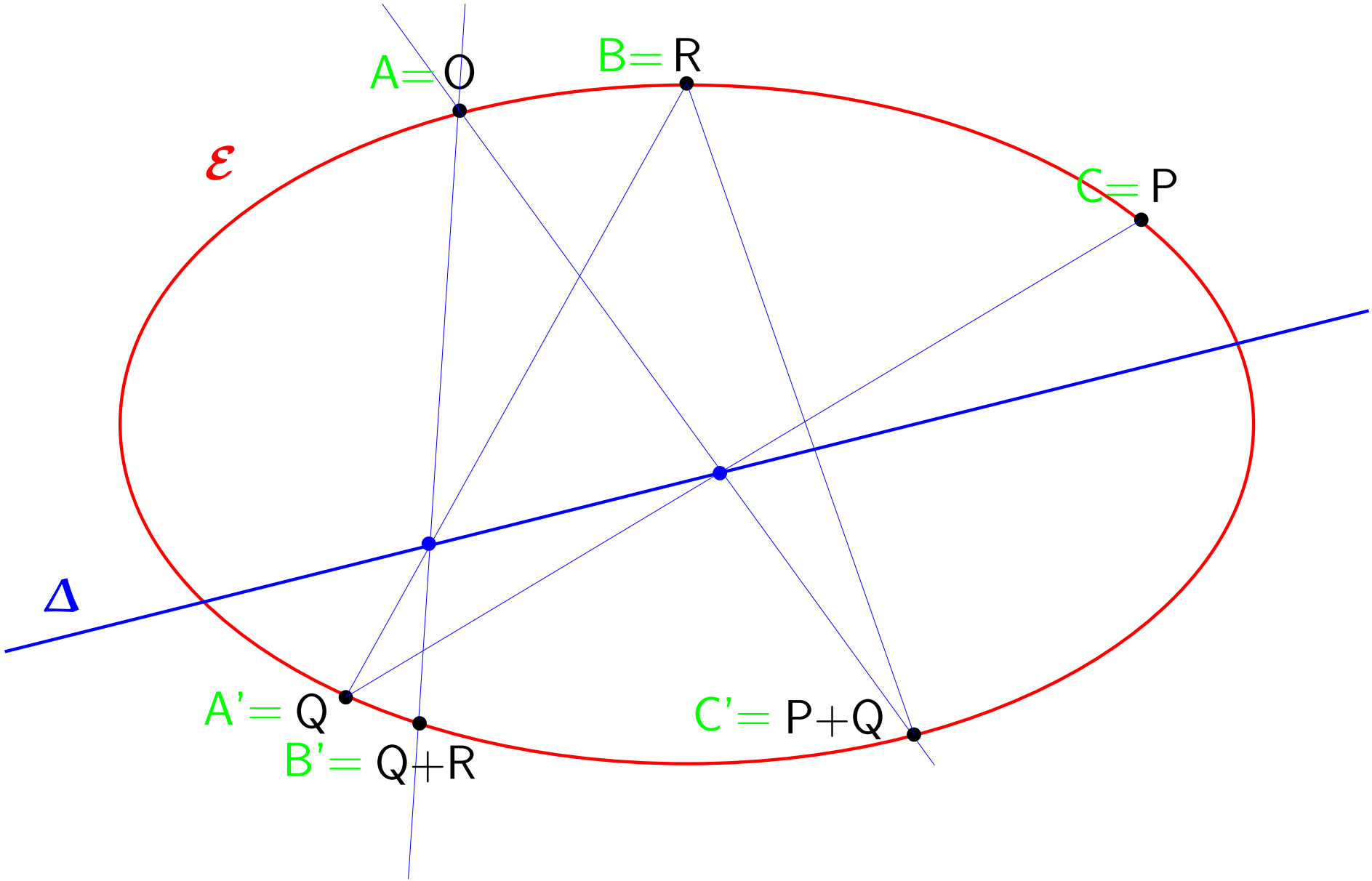

O
R
P
ε
Δ
Q
P+Q

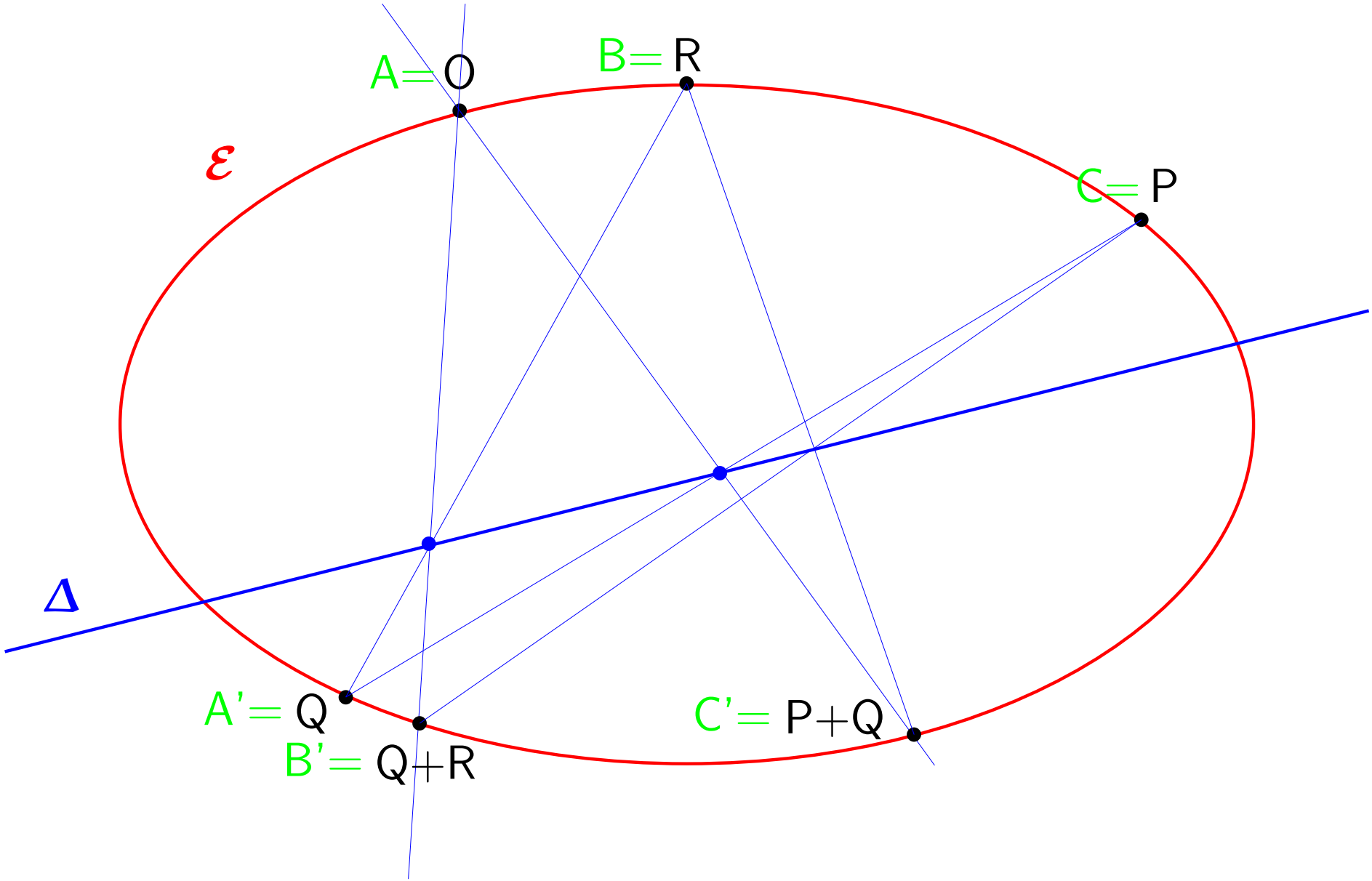

O
R
P
ε
Δ
Q
P+Q

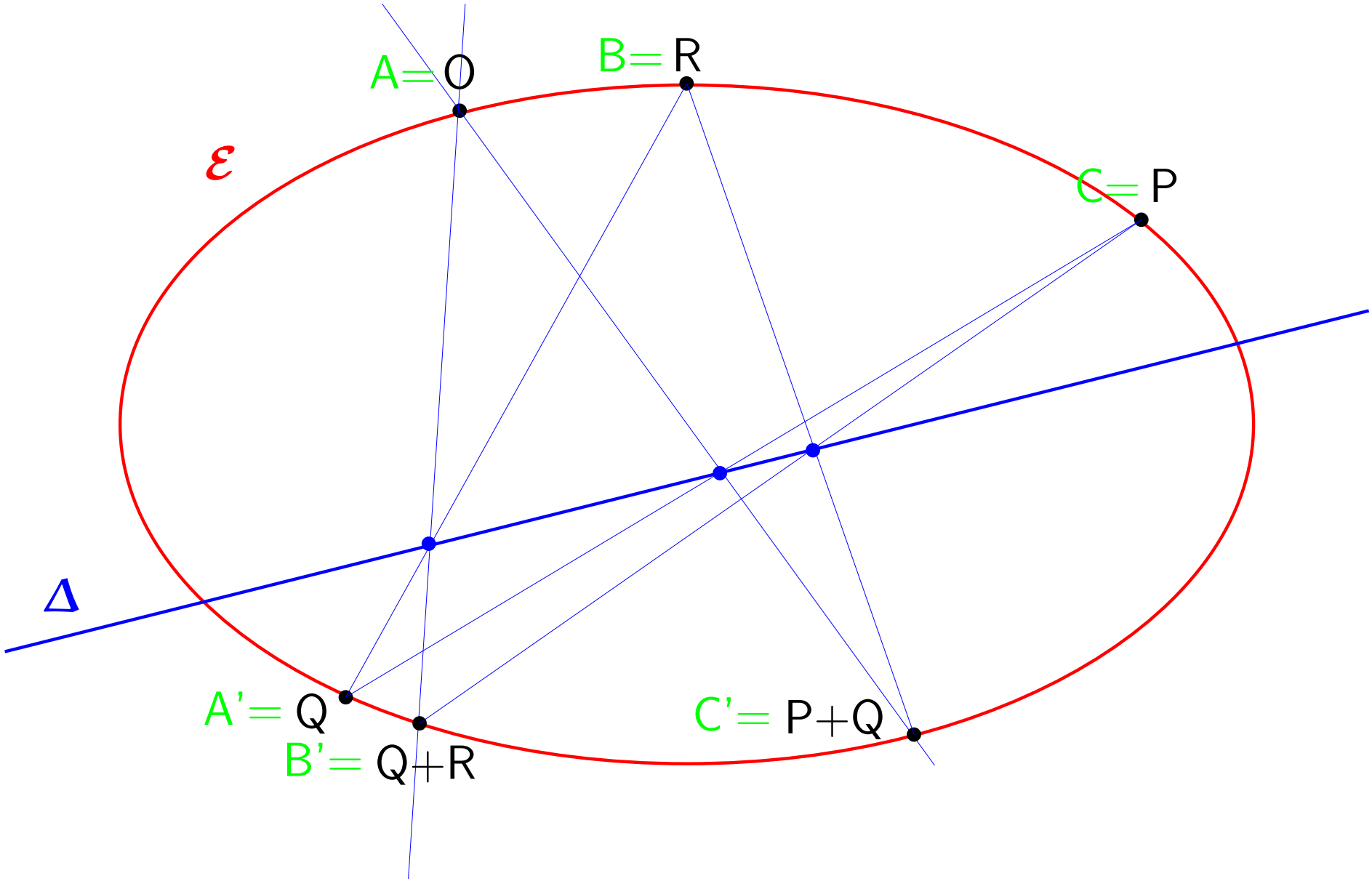

O
R
P
$\mathcal{E}$
Δ
Q
Q+R
P+Q

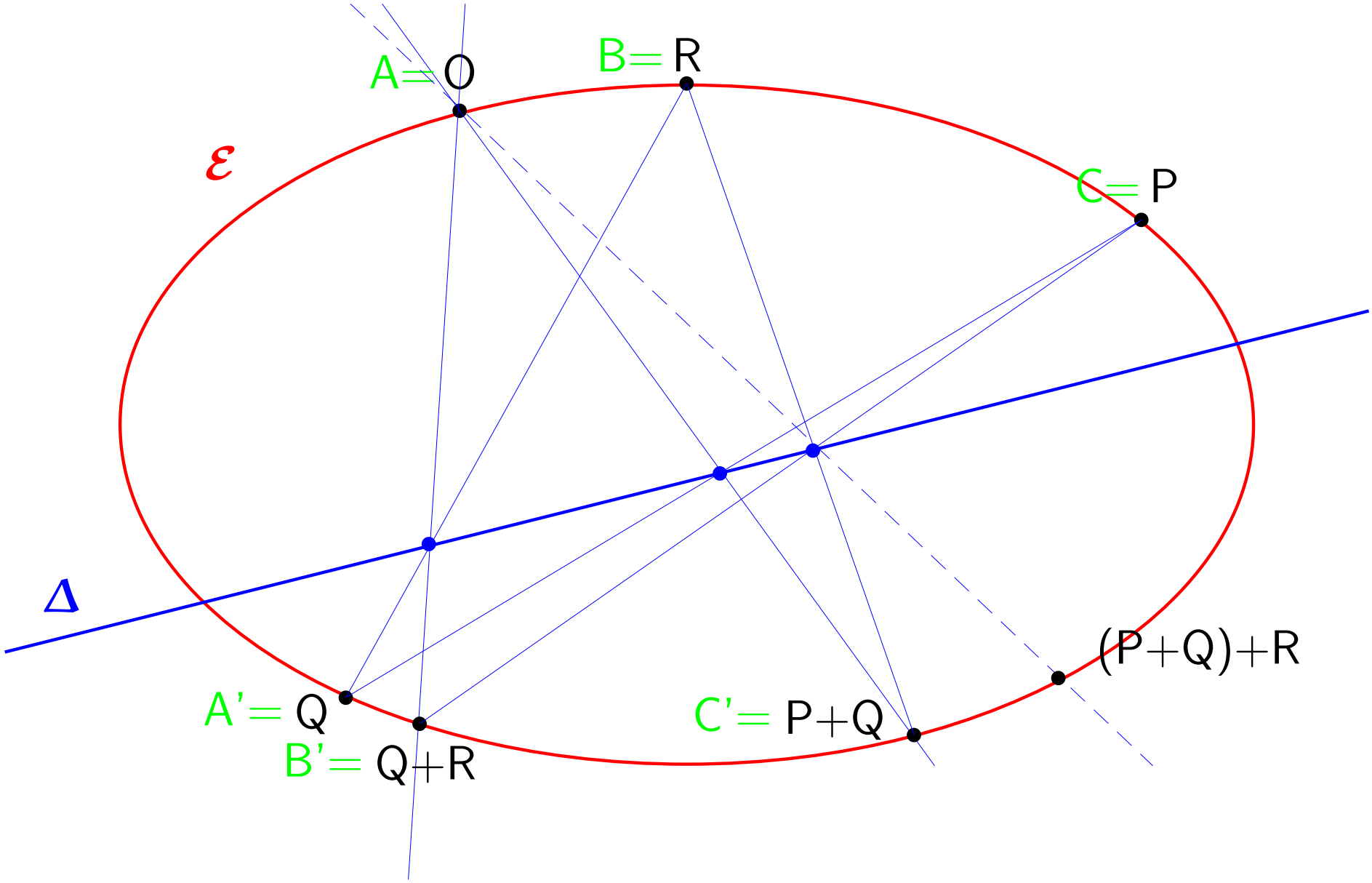

A = O
B = R
C = P
$\mathcal{E}$
Δ
Q
Q+R
P+Q

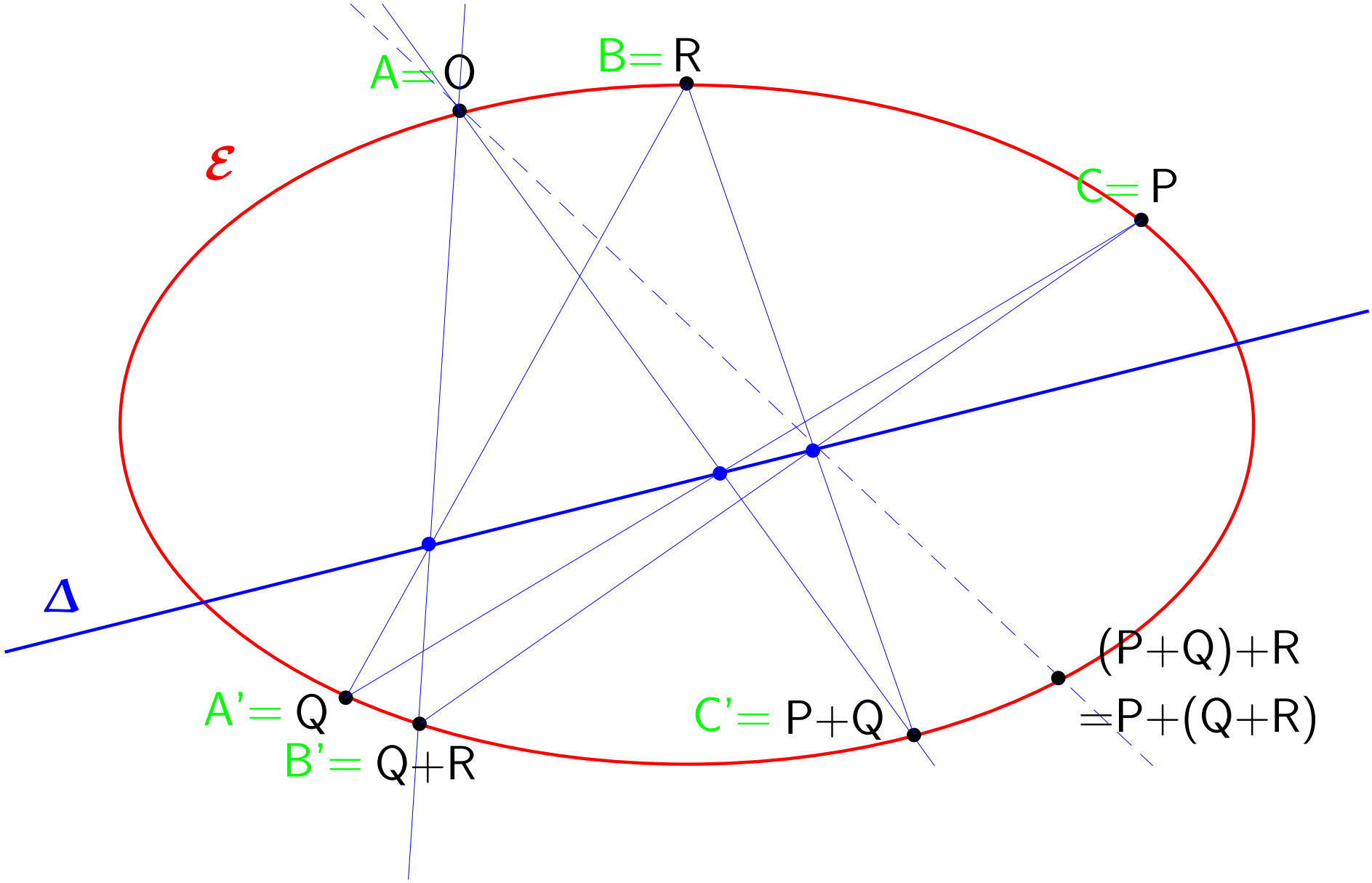

A = O
B = R
C = P
ε
Δ
A' = Q
B' = Q+R
C' = P+Q


A = O
B = R
C = P
ε
Δ
A' = Q
B' = Q+R
C' = P+Q


A = O
B = R
C = P
$\mathcal{E}$
Δ
A' = Q
B' = Q+R
C' = P+Q


A = O
B = R
C = P
ε
Δ
A' = Q
B' = Q+R
C' = P+Q


A= O
B= R
C= P
ε
Δ
(P+Q)+R
A'= Q
B'= Q+R
C'= P+Q


A= O
B= R
C= P
ε
Δ
A'= Q
B'= Q+R
C'= P+Q
(P+Q)+R
=P+(Q+R)

Théorème. $\mathcal{E} \setminus \Delta$, *muni de la loi* $+$, *est un groupe* **commutatif** *! L'élément neutre est* O.

Pour montrer ce résultat, on a utilisé la réunion $\mathcal{E} \cup \Delta$ de la courbe et de la droite :

Théorème. $\mathcal{E} \setminus \Delta$, *muni de la loi* $+$, *est un groupe* **commutatif** *! L'élément neutre est* O.

Pour montrer ce résultat, on a utilisé la réunion $\mathcal{E} \cup \Delta$ de la courbe et de la droite :

$$\mathcal{E} = \{(x, y) \in \mathbb{R}^2 \mid P_2(x, y) = 0\}$$

$$\Delta = \{(x, y) \in \mathbb{R}^2 \mid P_1(x, y) = 0\}$$

où P_i est un polynôme de degré total i.

Théorème. $\mathcal{E} \setminus \Delta$, *muni de la loi* $+$, *est un groupe* **commutatif** *! L'élément neutre est* O.

Pour montrer ce résultat, on a utilisé la réunion $\mathcal{E} \cup \Delta$ de la courbe et de la droite :

$$\mathcal{E} = \{(x, y) \in \mathbb{R}^2 \mid P_2(x, y) = 0\}$$

$$\Delta = \{(x, y) \in \mathbb{R}^2 \mid P_1(x, y) = 0\}$$

où P_i est un polynôme de degré total i. Donc

$$\mathcal{E} \cup \Delta = \{(x, y) \in \mathbb{R}^2 \mid P_1(x, y)P_2(x, y) = 0\}.$$

C'est une **cubique** !

Théorème. $\mathcal{E} \setminus \Delta$, *muni de la loi* $+$, *est un groupe* **commutatif** *! L'élément neutre est* O.

Pour montrer ce résultat, on a utilisé la réunion $\mathcal{E} \cup \Delta$ de la courbe et de la droite :

$$\mathcal{E} = \{(x, y) \in \mathbb{R}^2 \mid P_2(x, y) = 0\}$$

$$\Delta = \{(x, y) \in \mathbb{R}^2 \mid P_1(x, y) = 0\}$$

où P_i est un polynôme de degré total i. Donc

$$\mathcal{E} \cup \Delta = \{(x, y) \in \mathbb{R}^2 \mid P_1(x, y)P_2(x, y) = 0\}.$$

C'est une **cubique** ! On a aussi utilisé son point à l'infini...

- Soit $\mathcal{C}$ une cubique **irréductible non dégénérée**.

- Soit $\mathcal{C}$ une cubique **irréductible non dégénérée**. Rajoutons-lui les points à l'infini,

- Soit $\mathcal{C}$ une cubique **irréductible non dégénérée**. Rajoutons-lui les points à l'infini, enlevons-lui les points singuliers.

- Soit $\mathcal{C}$ une cubique **irréductible non dégénérée**. Rajoutons-lui les points à l'infini, enlevons-lui les points singuliers. On obtient $\overline{\mathcal{C}}$. Fixons $O \in \overline{\mathcal{C}}$.

- Soit $\mathcal{C}$ une cubique **irréductible non dégénérée**. Rajoutons-lui les points à l'infini, enlevons-lui les points singuliers. On obtient $\overline{\mathcal{C}}$. Fixons $O \in \overline{\mathcal{C}}$.
- Si P, $Q \in \overline{\mathcal{C}}$, soit X le troisième point d'intersection de $(PQ) \cap \overline{\mathcal{C}}$.

- Soit $\mathcal{C}$ une cubique **irréductible non dégénérée**. Rajoutons-lui les points à l'infini, enlevons-lui les points singuliers. On obtient $\overline{\mathcal{C}}$. Fixons $O \in \overline{\mathcal{C}}$.
- Si P, $Q \in \overline{\mathcal{C}}$, soit X le troisième point d'intersection de $(PQ) \cap \overline{\mathcal{C}}$. On note $P + Q$ le troisième point d'intersection de $(OX) \cap \overline{\mathcal{C}}$.

- Soit $\mathcal{C}$ une cubique **irréductible non dégénérée**. Rajoutons-lui les points à l'infini, enlevons-lui les points singuliers. On obtient $\overline{\mathcal{C}}$. Fixons $O \in \overline{\mathcal{C}}$.
- Si P, $Q \in \overline{\mathcal{C}}$, soit X le troisième point d'intersection de $(PQ) \cap \overline{\mathcal{C}}$. On note $P + Q$ le troisième point d'intersection de $(OX) \cap \overline{\mathcal{C}}$.

Théorème. $(\overline{\mathcal{C}}, +)$ *est un groupe* **commutatif**. *L'élément neutre est* O.

Courbes elliptiques :

Courbes elliptiques :

- Dorénavant,

$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 \mid y^2 = F(x)\}$$

où $F(x) = x^3 + ax + b$, a, $b \in \mathbb{R}$.

Courbes elliptiques :

- Dorénavant,
$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 \mid y^2 = F(x)\}$$
où $F(x) = x^3 + ax + b$, a, $b \in \mathbb{R}$.
- On a donc $y = \pm\sqrt{F(x)}$ et,

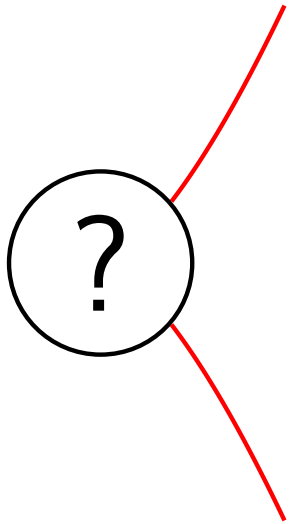
Courbes elliptiques :

- Dorénavant,

$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 \mid y^2 = F(x)\}$$

où $F(x) = x^3 + ax + b$, a, $b \in \mathbb{R}$.

- On a donc $y = \pm\sqrt{F(x)}$ et, lorsque $x \to +\infty$, on a $y \sim \pm x^{3/2}$.



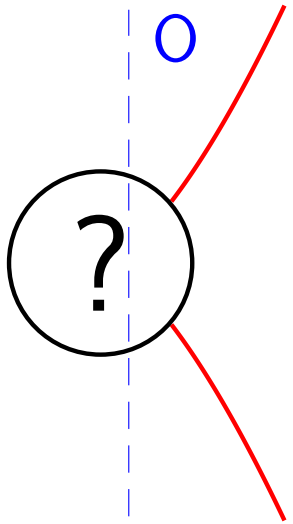
Courbes elliptiques :

- Dorénavant,

$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 \mid y^2 = F(x)\}$$

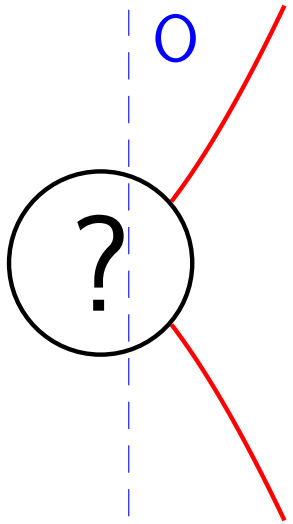
où $F(x) = x^3 + ax + b$, a, $b \in \mathbb{R}$.

- On a donc $y = \pm\sqrt{F(x)}$ et, lorsque $x \longrightarrow +\infty$, on a $y \sim \pm x^{3/2}$.



Courbes elliptiques :

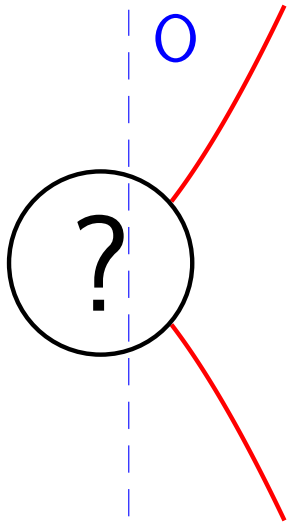
- Dorénavant,
$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 \mid y^2 = F(x)\}$$
où $F(x) = x^3 + ax + b$, a, $b \in \mathbb{R}$.
- On a donc $y = \pm\sqrt{F(x)}$ et, lorsque $x \to +\infty$, on a $y \sim \pm x^{3/2}$.



- $\overline{\mathcal{C}} = \mathcal{C} \cup \{O\}$.

Courbes elliptiques :

- Dorénavant,
$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 \mid y^2 = F(x)\}$$
où $F(x) = x^3 + ax + b$, a, $b \in \mathbb{R}$.
- On a donc $y = \pm\sqrt{F(x)}$ et, lorsque $x \to +\infty$, on a $y \sim \pm x^{3/2}$.

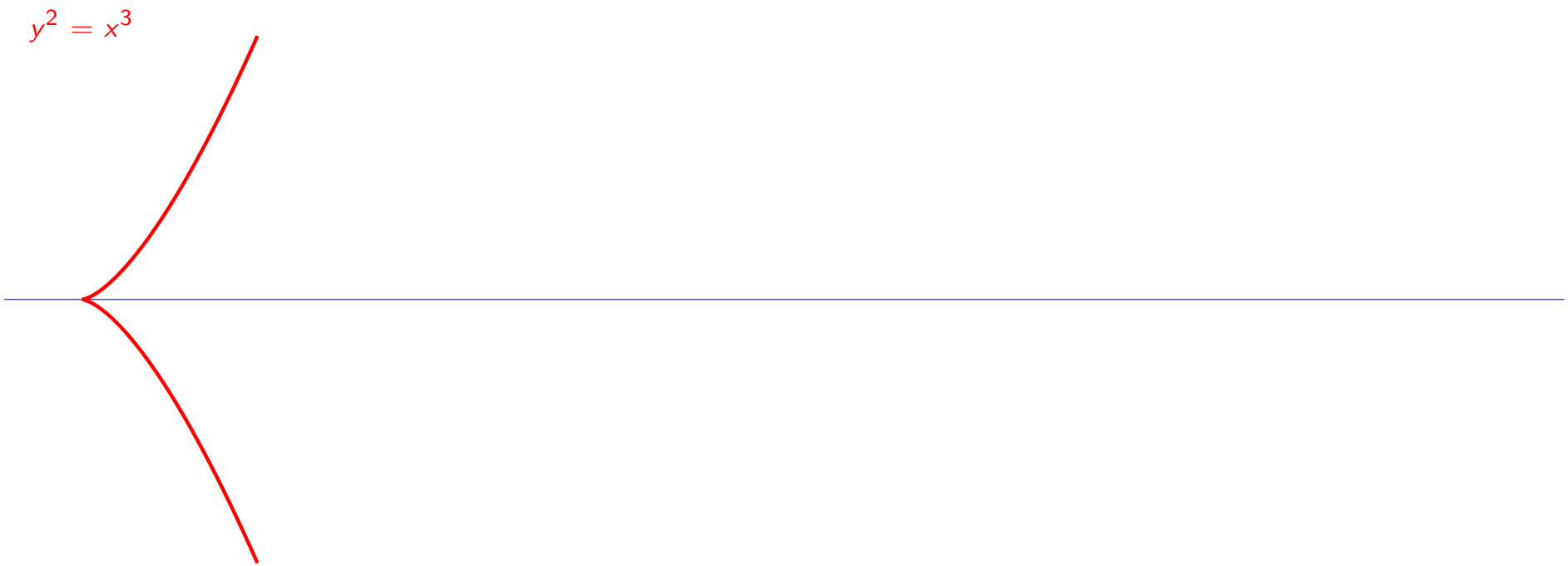


- $\overline{\mathcal{C}} = \mathcal{C} \cup \{O\}$.

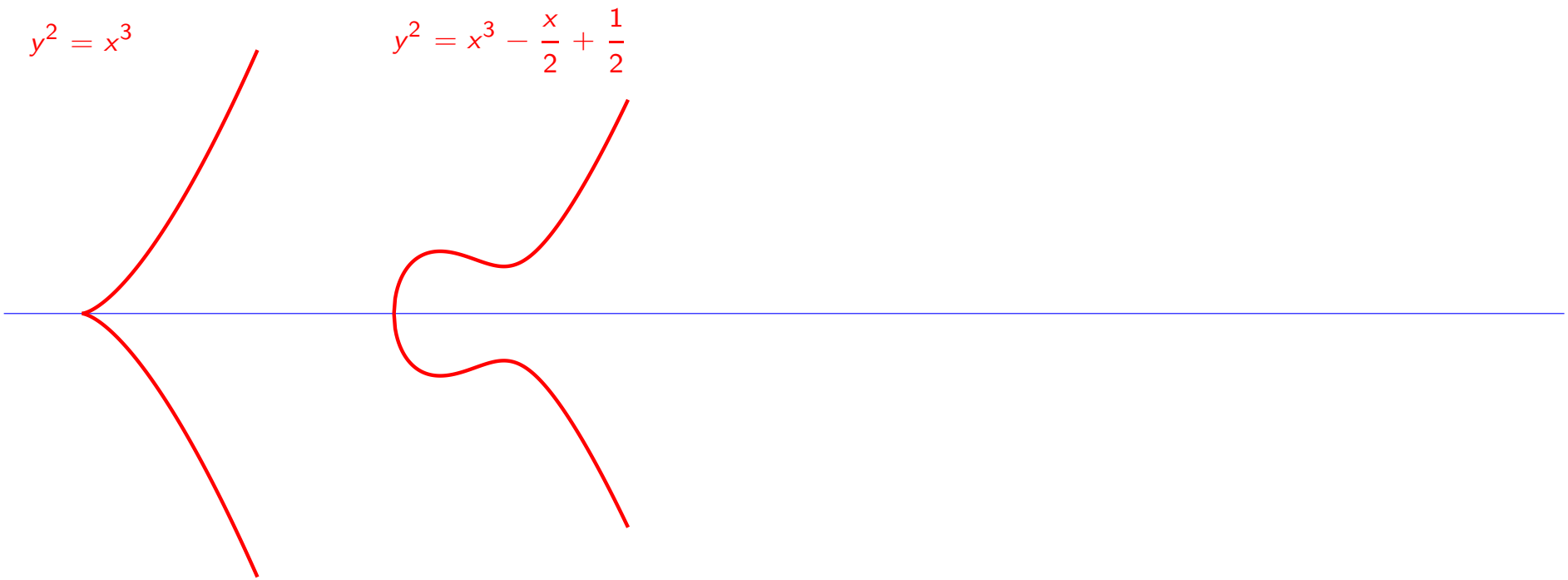
Remarque - à transformation projective près, toute cubique est de cette forme...

À quoi ressemble $\overline{\mathcal{C}}$?

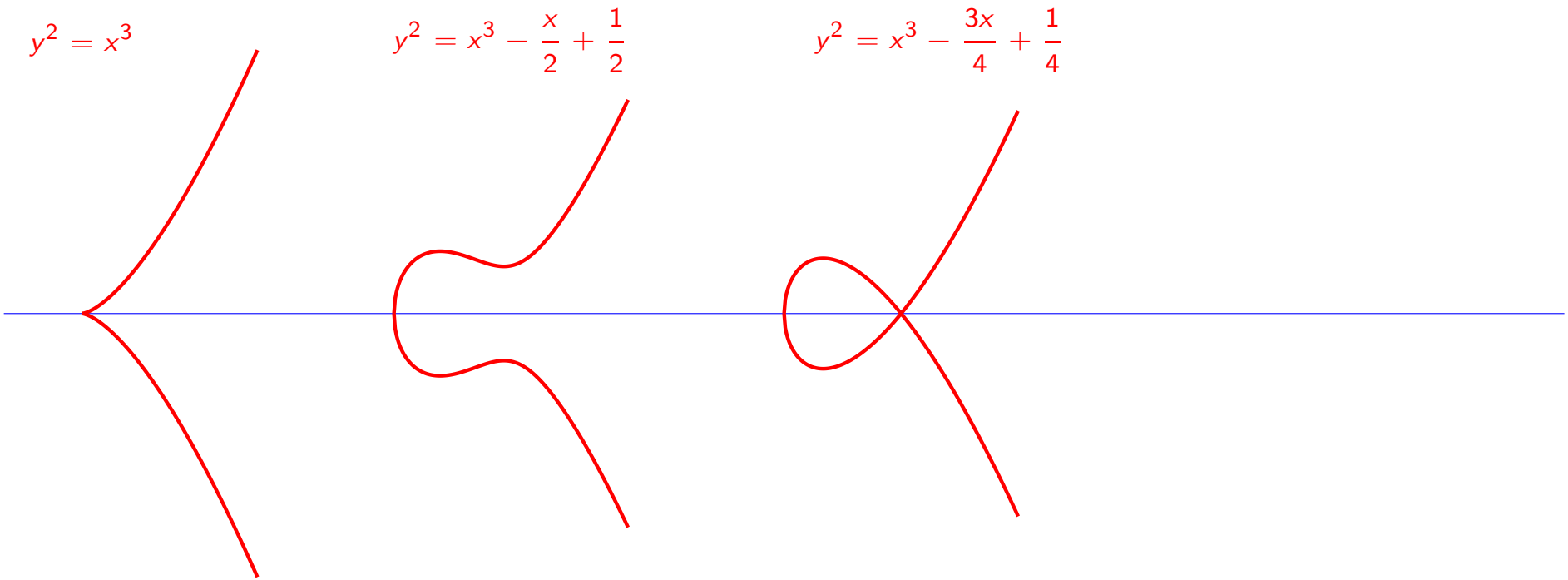
À quoi ressemble $\overline{\mathcal{C}}$?



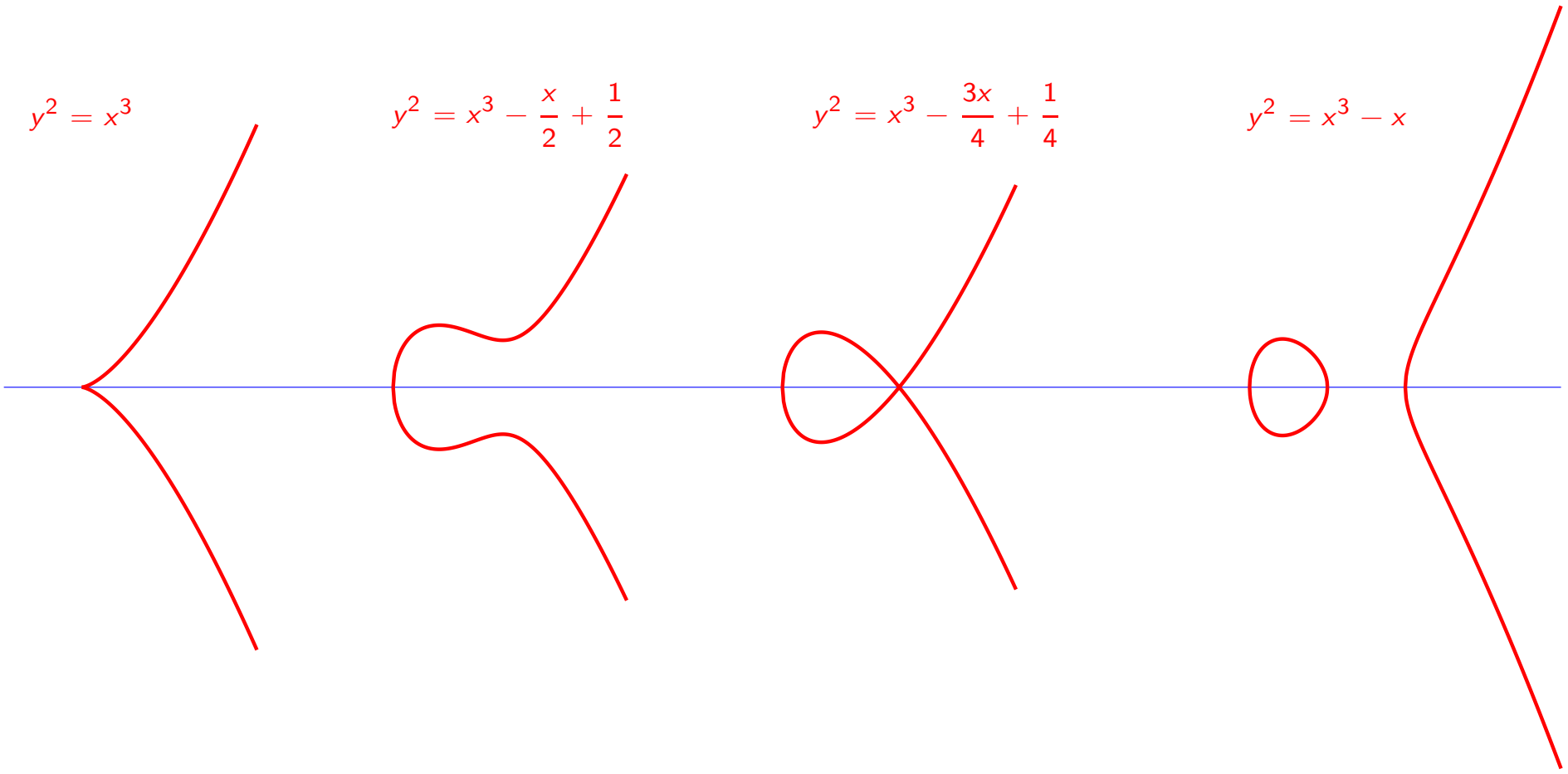
À quoi ressemble $\overline{\mathcal{C}}$?



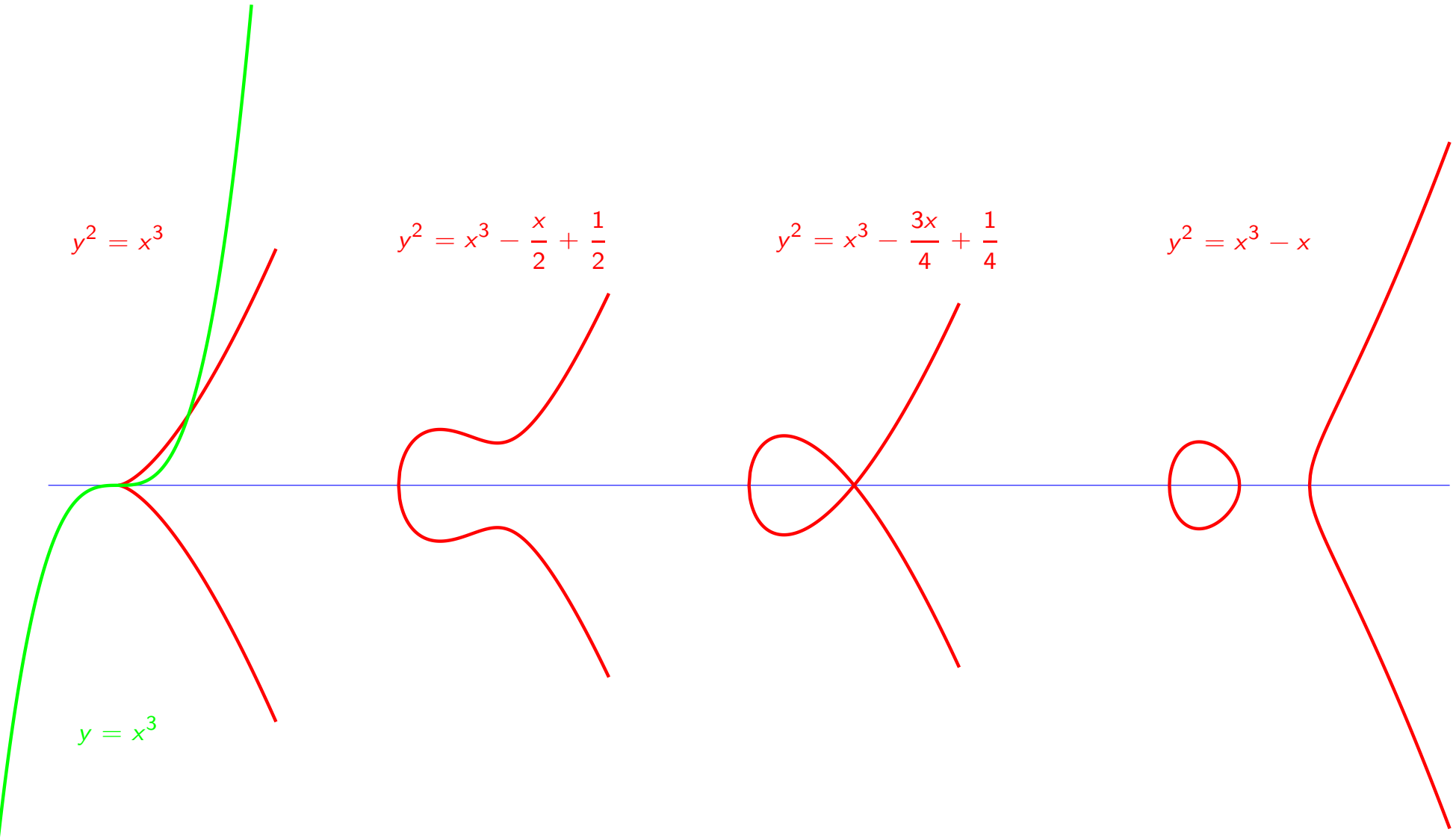
À quoi ressemble $\overline{\mathcal{C}}$?



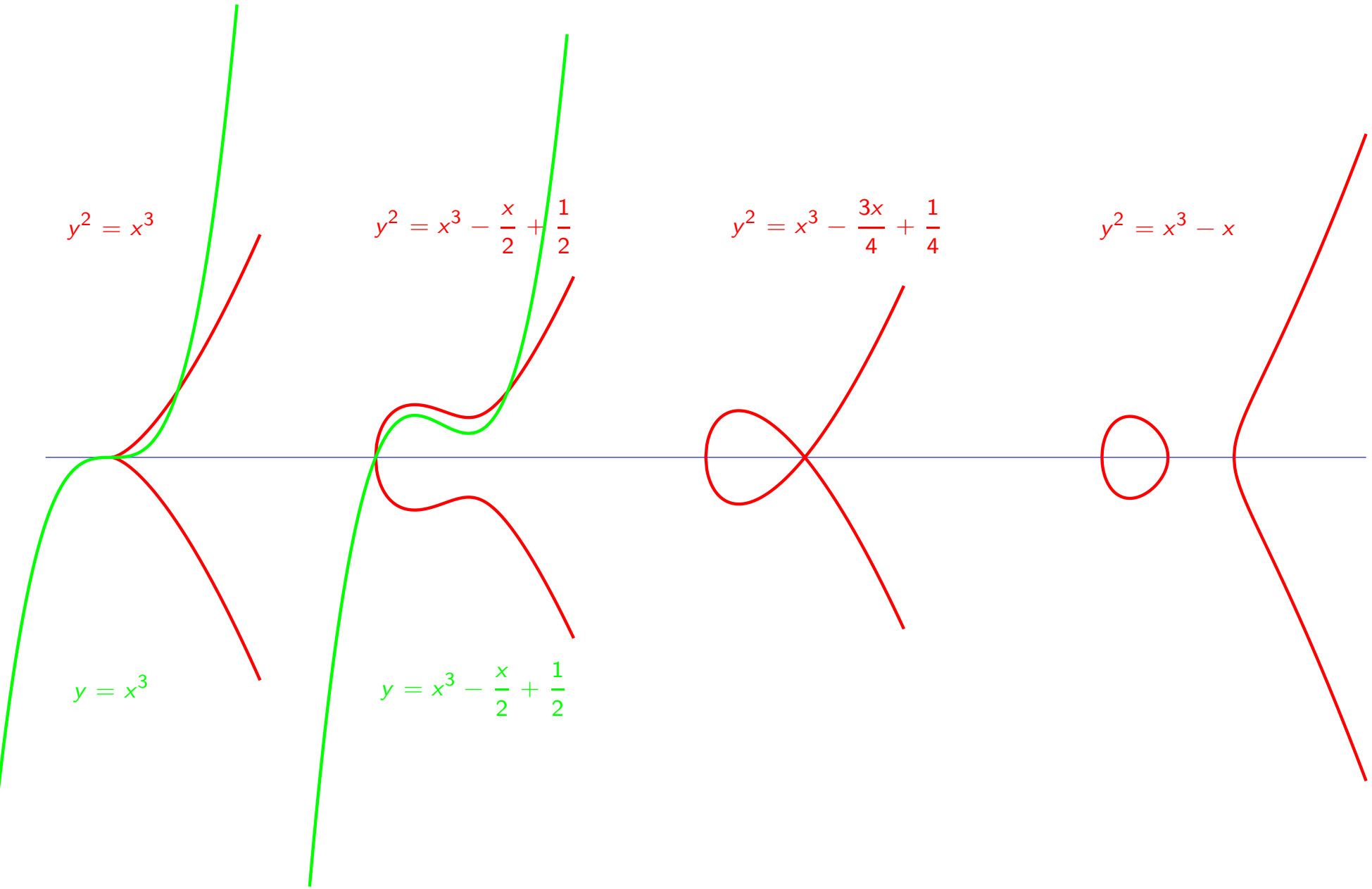
À quoi ressemble $\overline{\mathcal{C}}$?



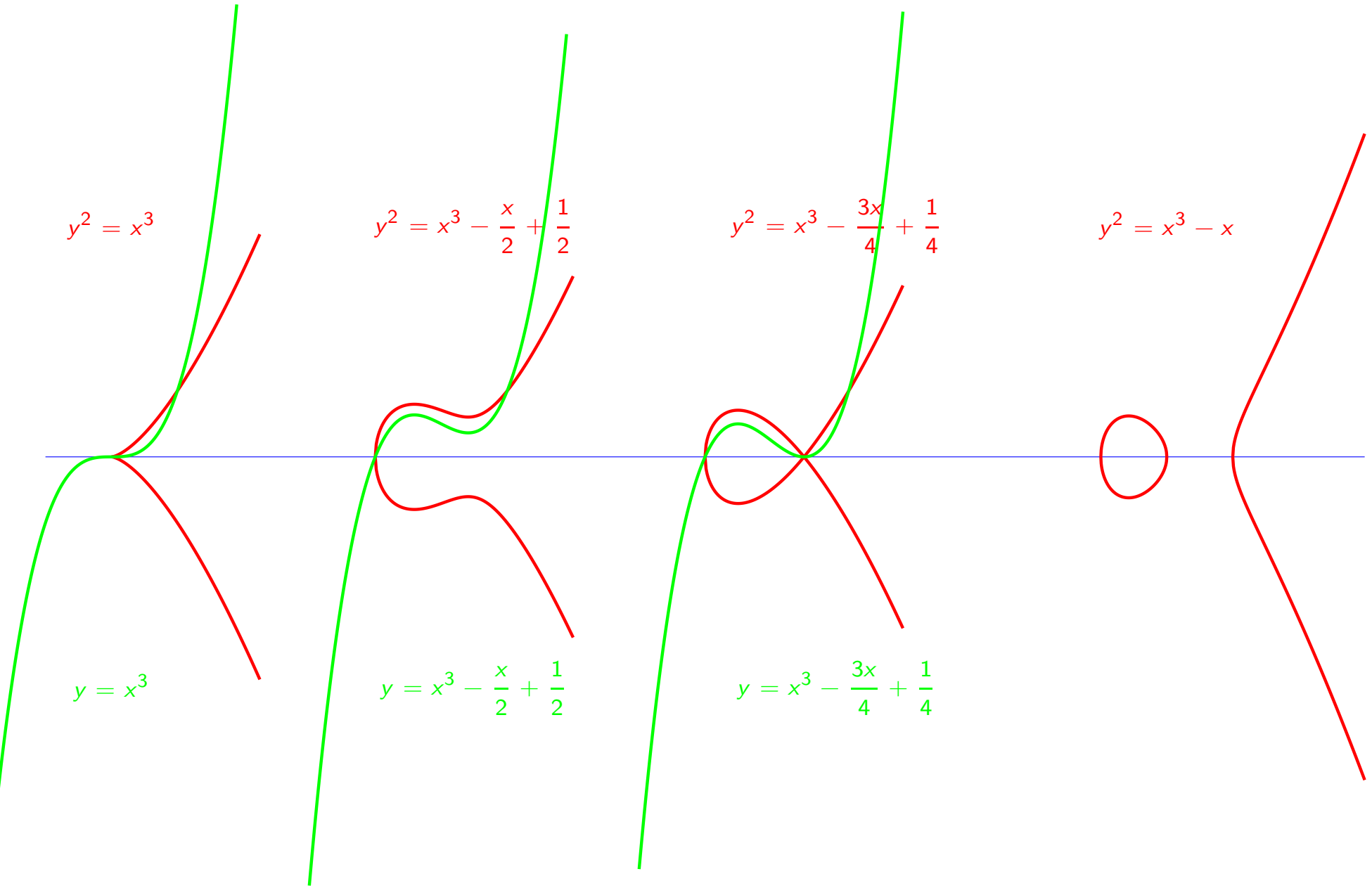
À quoi ressemble $\overline{\mathcal{C}}$?



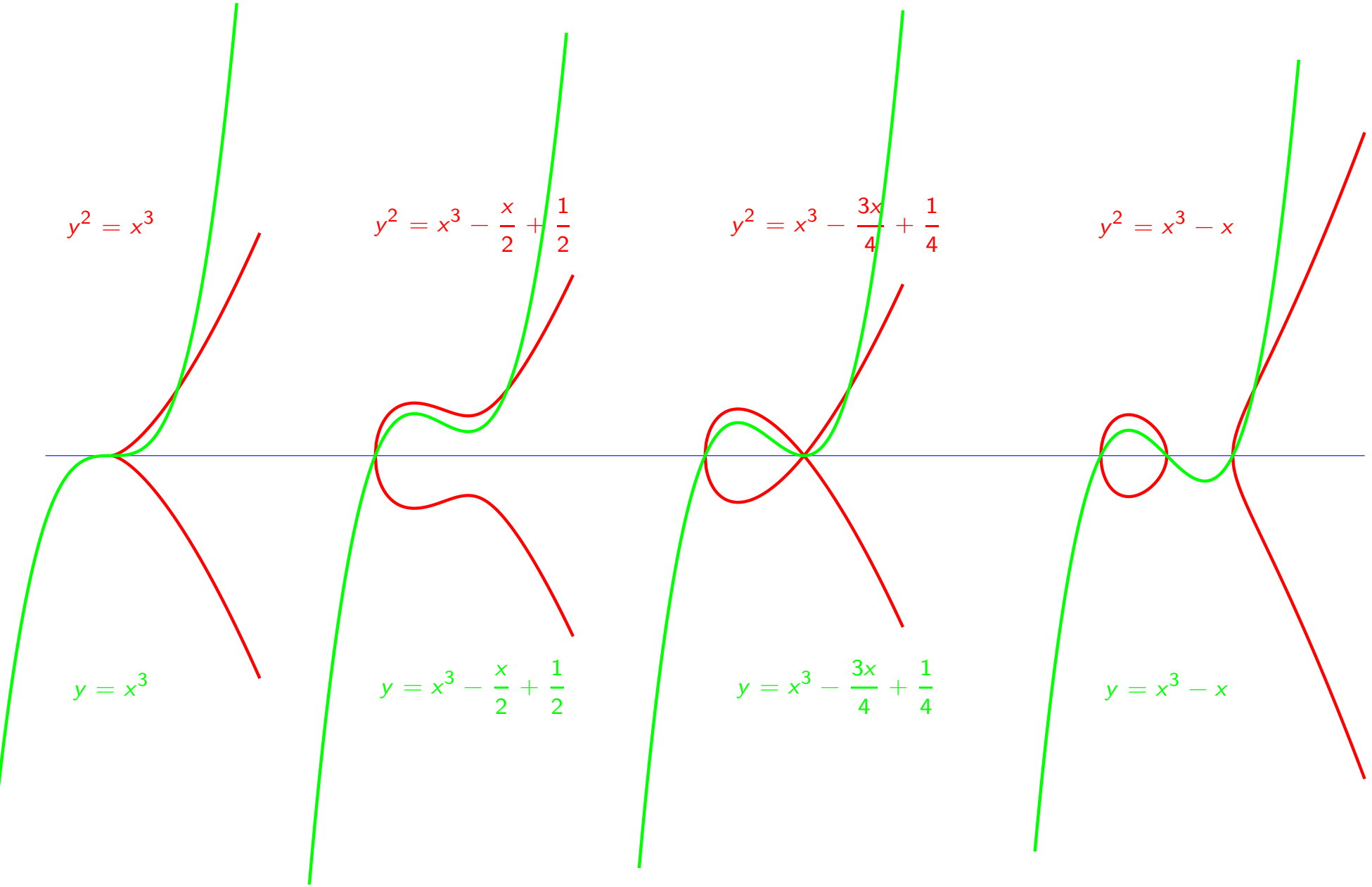
À quoi ressemble $\overline{\mathcal{C}}$?



À quoi ressemble $\overline{\mathcal{C}}$?



À quoi ressemble $\overline{\mathcal{C}}$?



Lissité :

- $\overline{\mathcal{C}}$ est lisse (i.e. n'a pas de points singuliers)

Lissité :

- $\overline{\mathcal{C}}$ est lisse (i.e. n'a pas de points singuliers)

$\Longleftrightarrow$ $F(x)$ n'a pas de racine double (ou triple...)

Lissité :

- $\overline{\mathcal{C}}$ est lisse (i.e. n'a pas de points singuliers)

$\iff$ $F(x)$ n'a pas de racine double (ou triple...)

$\iff$ $4a^3 + 27b^2 \neq 0$.

Lissité :

- $\overline{\mathcal{C}}$ est lisse (i.e. n'a pas de points singuliers)

$\Longleftrightarrow$ $F(x)$ n'a pas de racine double (ou triple...)

$\Longleftrightarrow$ $4a^3 + 27b^2 \neq 0$.

- Dorénavant, on suppose que $4a^3 + 27b^2 \neq 0$

Lissité :

- $\overline{\mathcal{C}}$ est lisse (i.e. n'a pas de points singuliers)

$\iff$ $F(x)$ n'a pas de racine double (ou triple...)

$\iff$ $4a^3 + 27b^2 \neq 0$.

- Dorénavant, on suppose que $4a^3 + 27b^2 \neq 0$
- $\overline{\mathcal{C}}$ est donc une courbe elliptique.

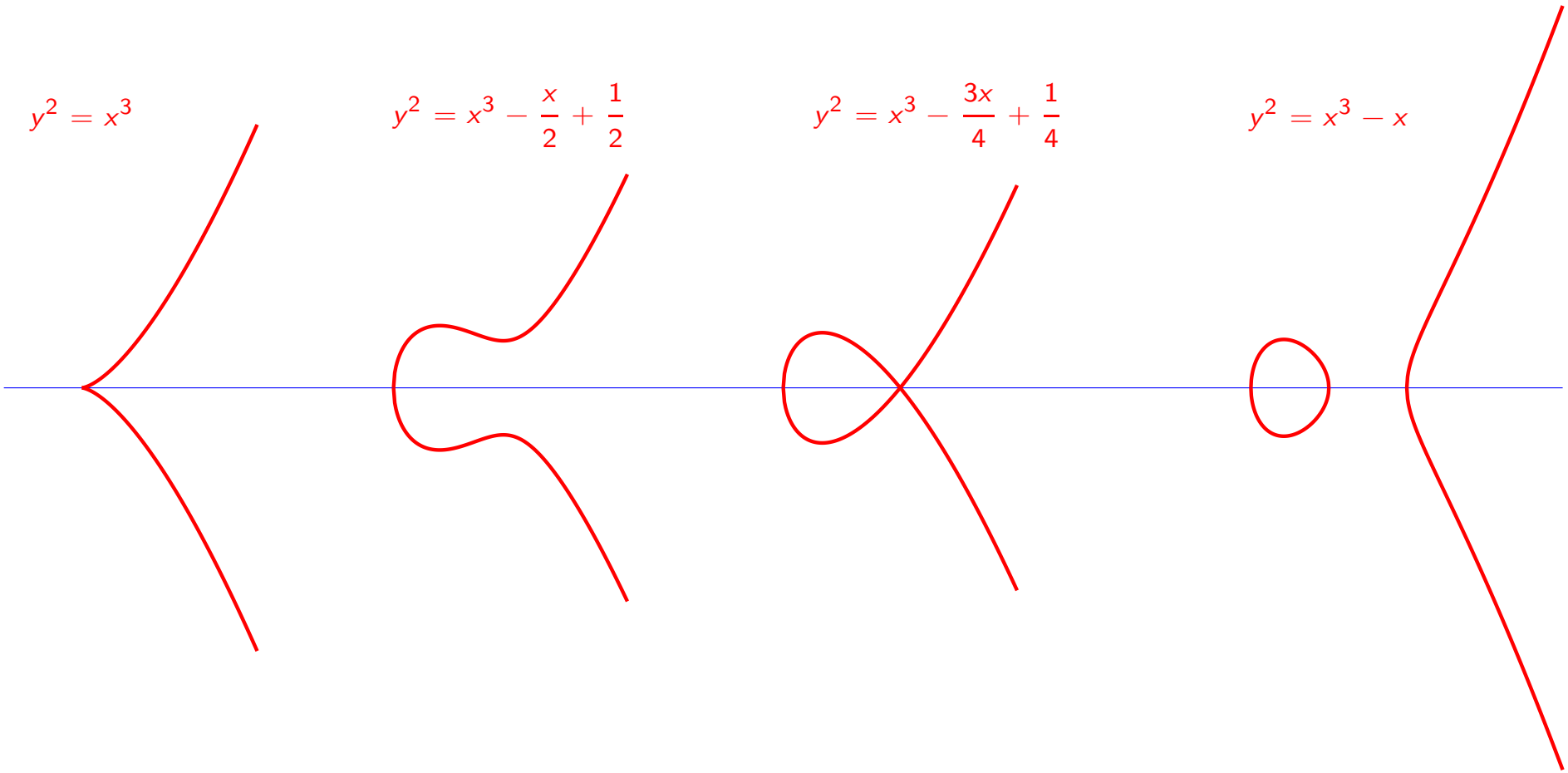
Lissité :

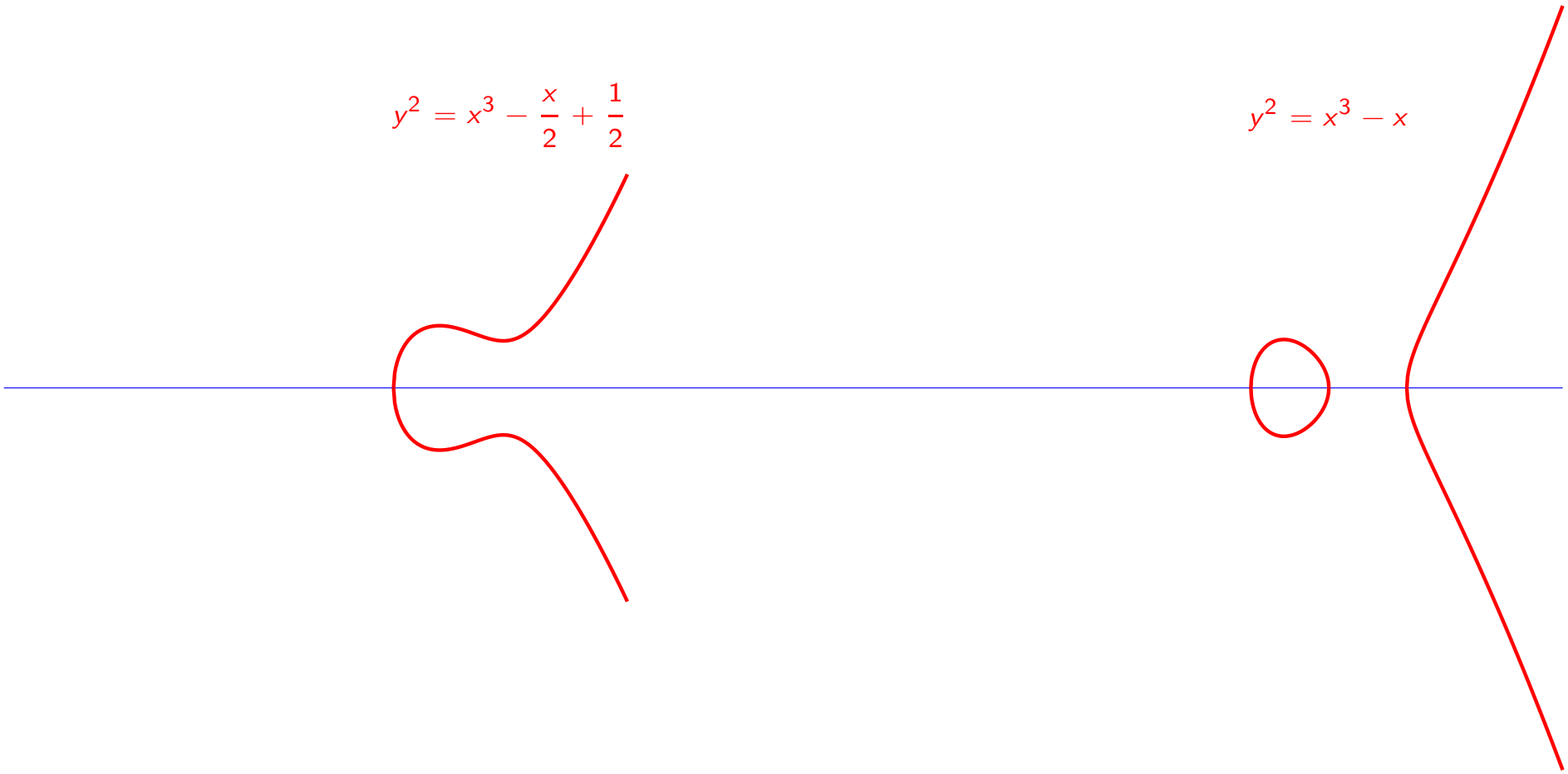
- $\overline{\mathcal{C}}$ est lisse (i.e. n'a pas de points singuliers)

$\Longleftrightarrow$ $F(x)$ n'a pas de racine double (ou triple...)

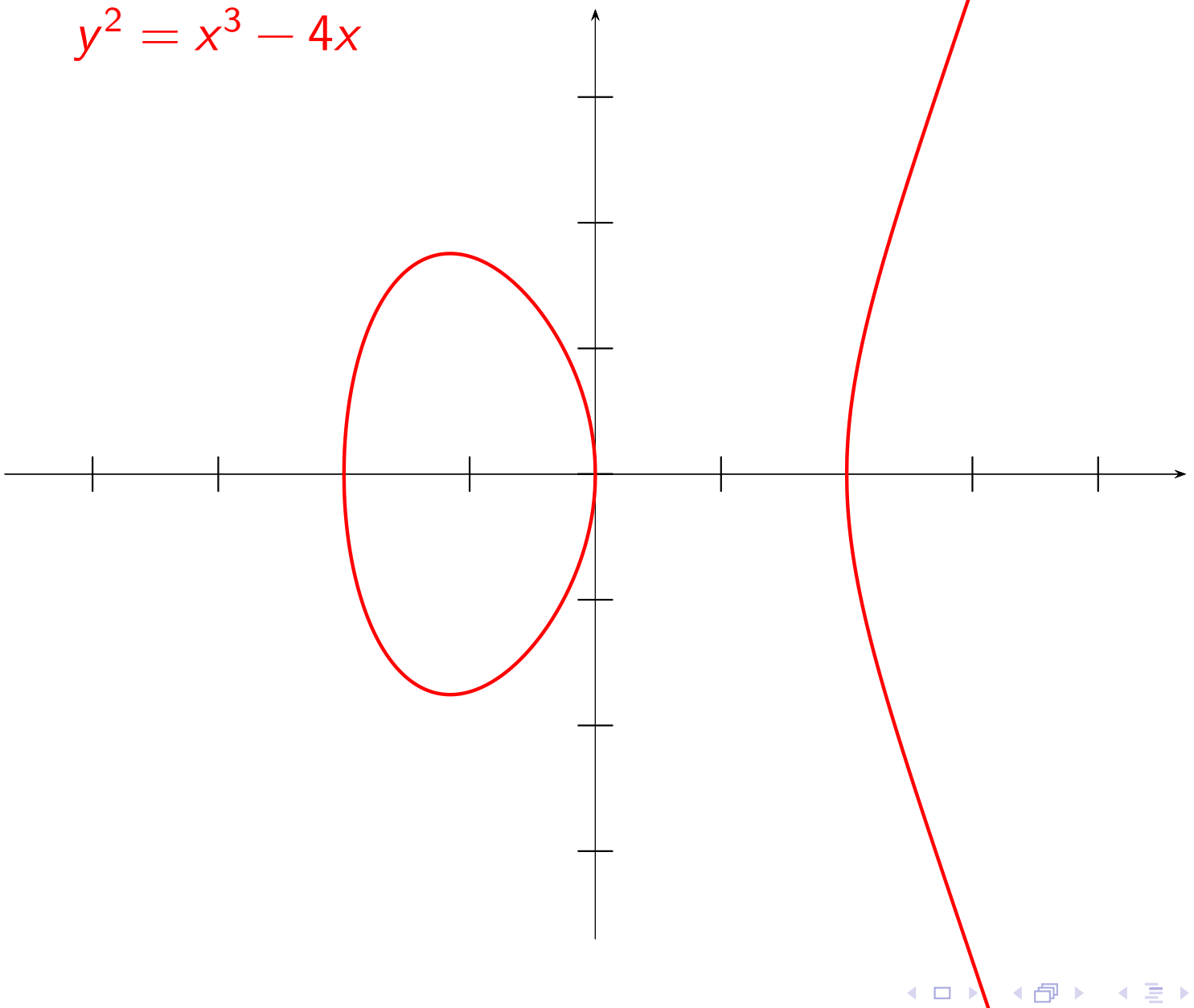
$\Longleftrightarrow$ $4a^3 + 27b^2 \neq 0$.

- Dorénavant, on suppose que $4a^3 + 27b^2 \neq 0$
- $\overline{\mathcal{C}}$ est donc une courbe elliptique.
- On la munit de la structure de groupe $+$ telle que le point à l'infini O est l'élément neutre.

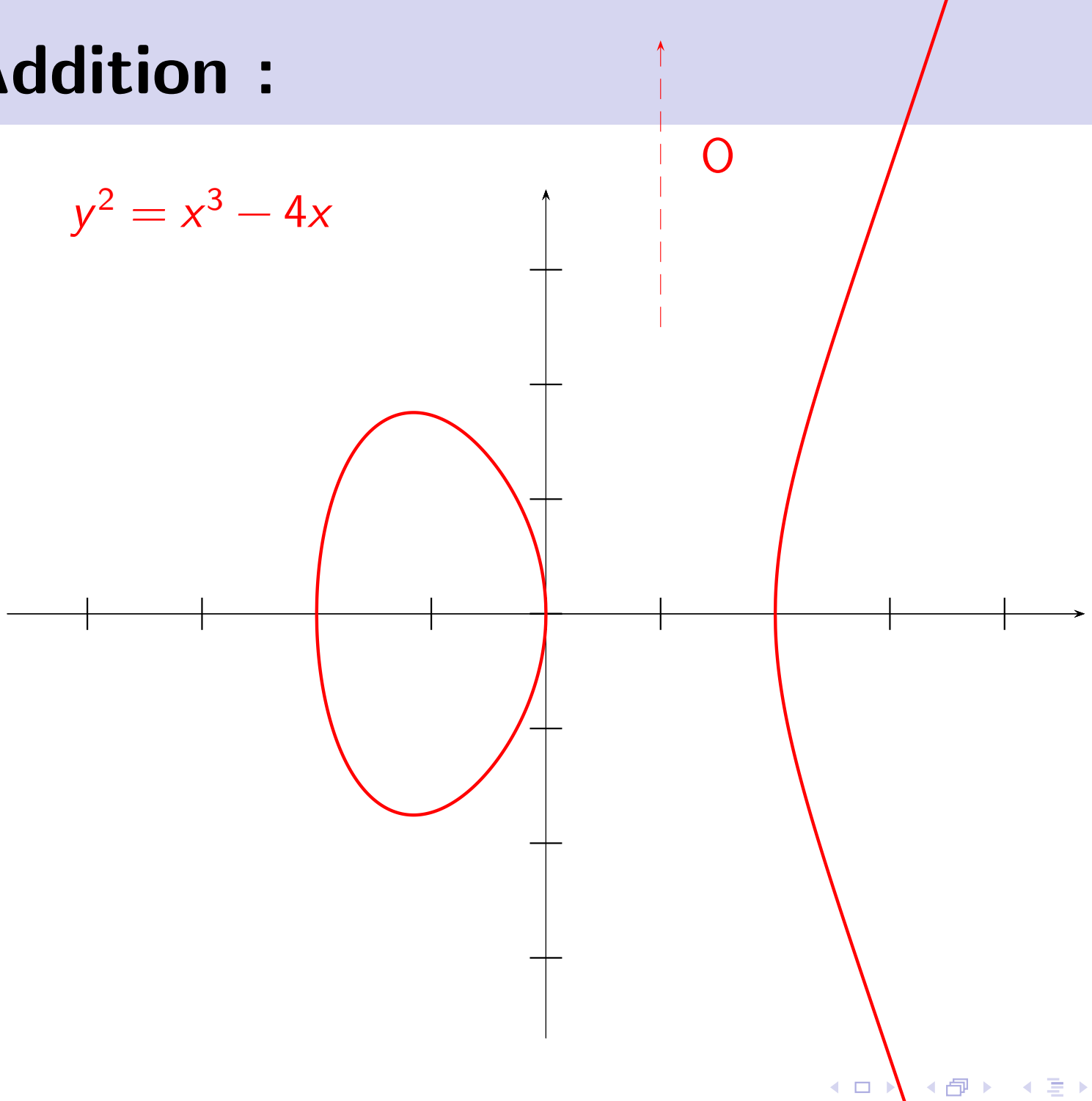

$y^2 = x^3$
$y^2 = x^3 - \frac{x}{2} + \frac{1}{2}$
$y^2 = x^3 - \frac{3x}{4} + \frac{1}{4}$
$y^2 = x^3 - x$


$y^2 = x^3 - \frac{x}{2} + \frac{1}{2}$
$y^2 = x^3 - x$

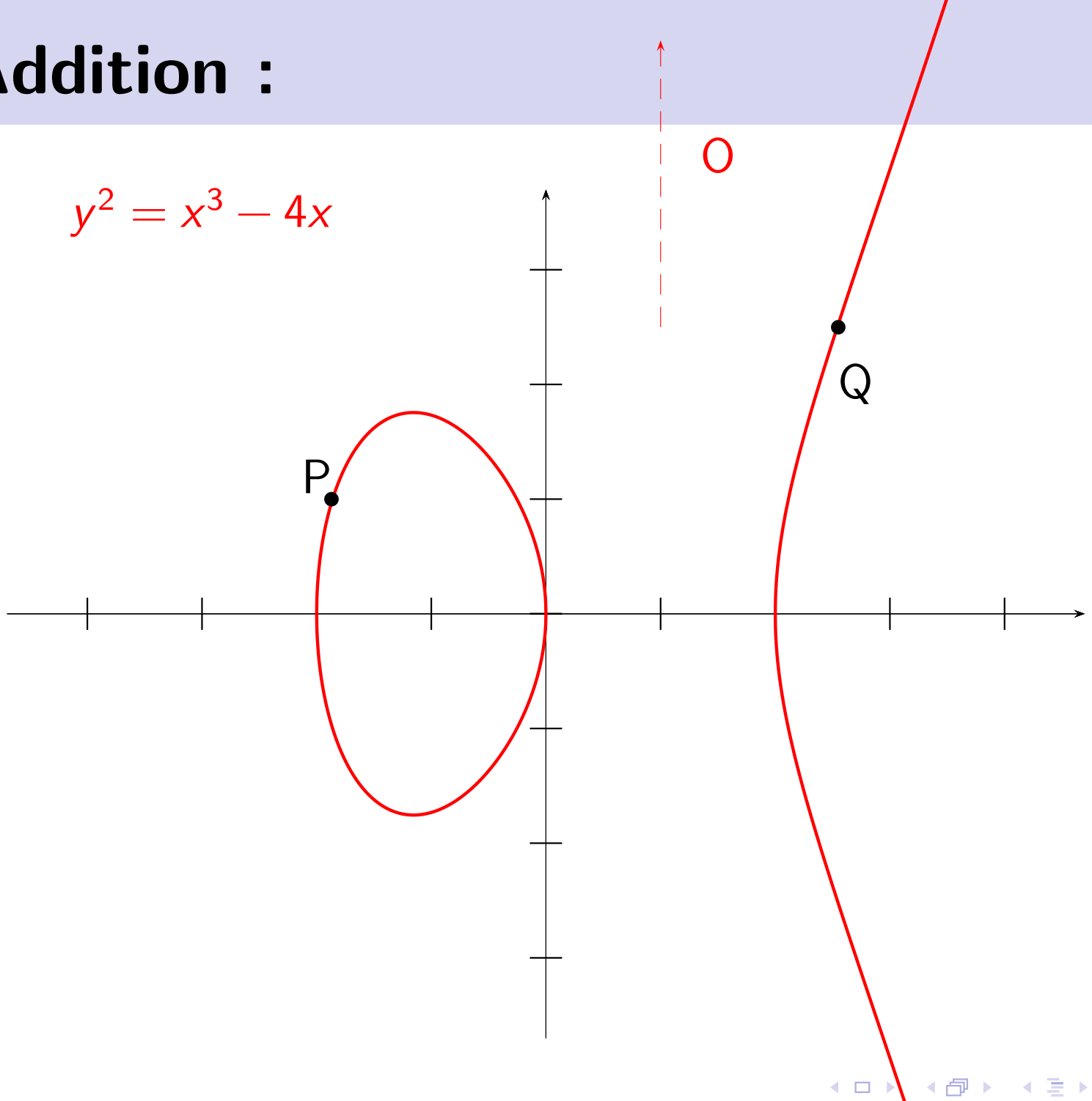
Addition :



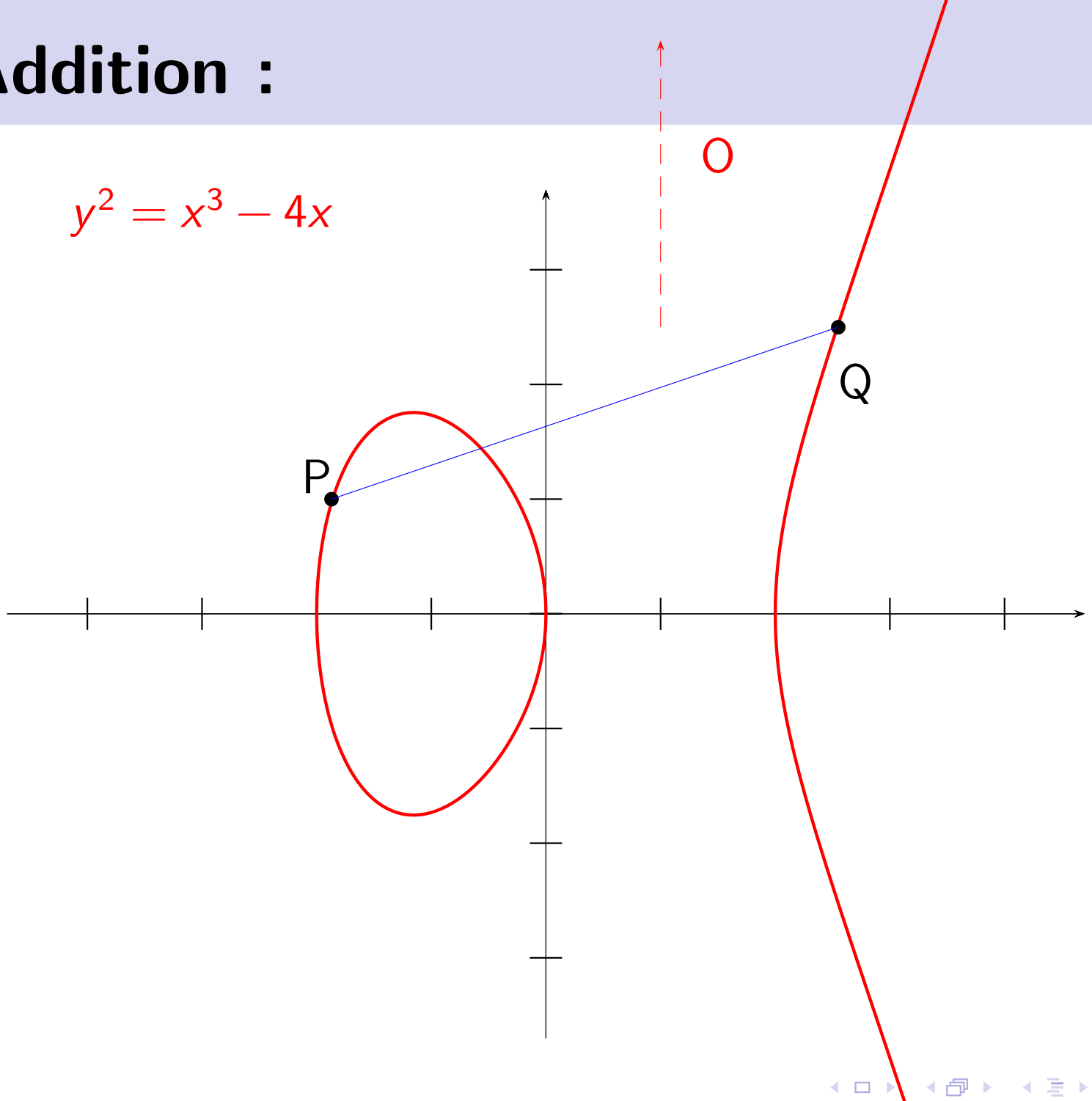
Addition :



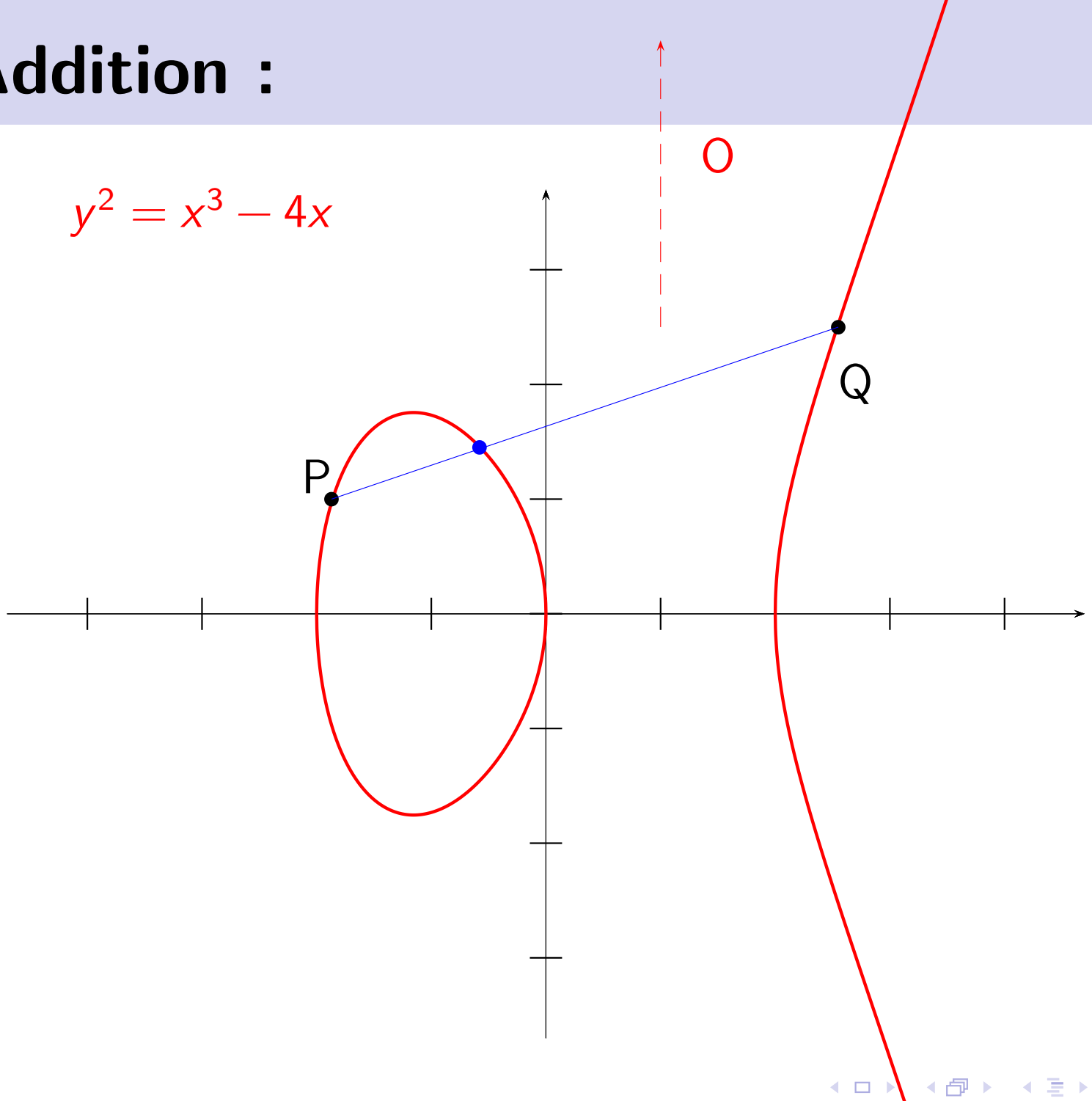
Addition :



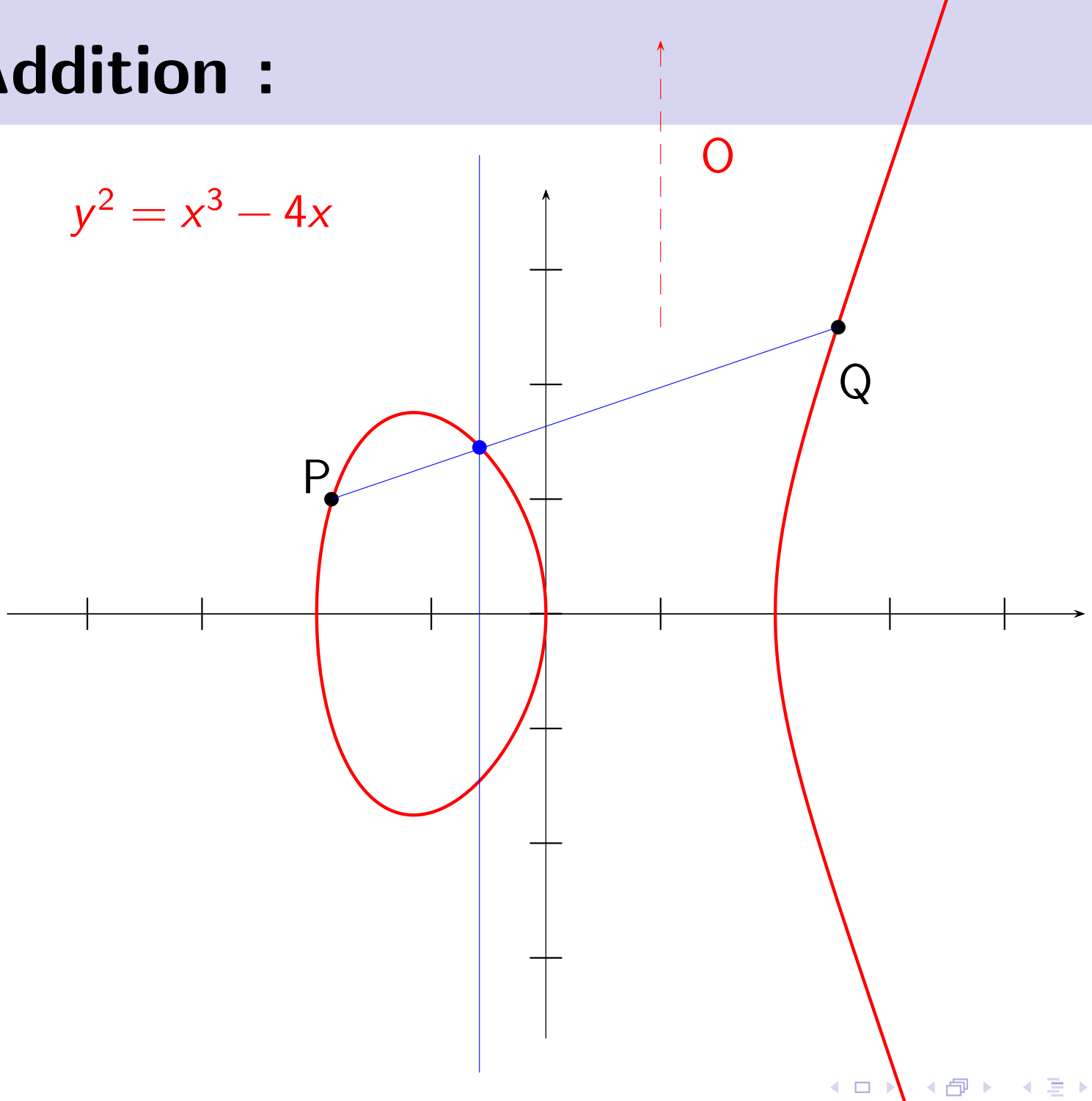
Addition :



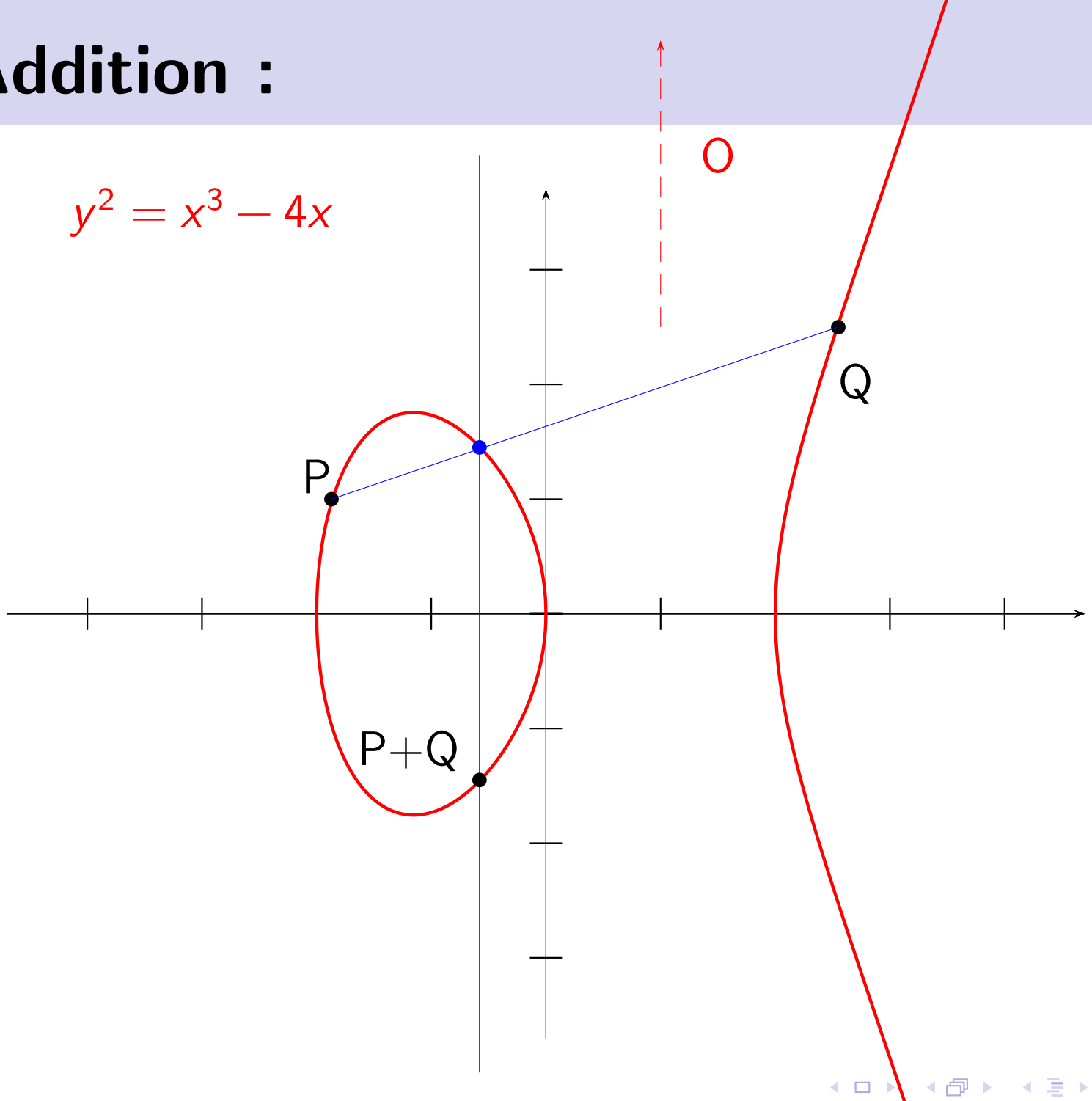
Addition :



Addition :



Addition :



Formule :

Formule :

Si $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$, alors

Formule :

Si $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$, alors

$$P+Q = \Big(\underbrace{-x_P - x_Q + \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2}_{x_{P+Q}},$$

Formule :

Si $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$, alors

$$P+Q = \Big(\underbrace{-x_P - x_Q + \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2}_{x_{P+Q}}, \frac{y_Q(x_P - x_{P+Q}) + y_P(x_{P+Q} - x_Q)}{x_Q - x_P} \Big)$$

Formule :

Si $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$, alors

$$P+Q = \Big(\underbrace{-x_P - x_Q + \Big(\frac{y_Q - y_P}{x_Q - x_P}\Big)^2}_{x_{P+Q}}, \frac{y_Q(x_P - x_{P+Q}) + y_P(x_{P+Q} - x_Q)}{x_Q - x_P} \Big)$$

$$P + P = 2P = \Big(\underbrace{-2x_P + \Big(\frac{3x_P^2 + a}{2y_P}\Big)^2}_{x_{2P}},$$

Formule :

Si $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$, alors

$$P+Q = \Big(\underbrace{-x_P - x_Q + \Big(\frac{y_Q - y_P}{x_Q - x_P}\Big)^2}_{x_{P+Q}}, \frac{y_Q(x_P - x_{P+Q}) + y_P(x_{P+Q} - x_Q)}{x_Q - x_P} \Big)$$

$$P + P = 2P = \Big(\underbrace{-2x_P + \Big(\frac{3x_P^2 + a}{2y_P}\Big)^2}_{x_{2P}}, -y_P - \frac{(x_{2P} - x_P)(3x_P^2 + a)}{2y_P} \Big)$$

Formule :

Si $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$, alors

$$P+Q = \Big(\underbrace{-x_P - x_Q + \Big(\frac{y_Q - y_P}{x_Q - x_P}\Big)^2}_{x_{P+Q}}, \frac{y_Q(x_P - x_{P+Q}) + y_P(x_{P+Q} - x_Q)}{x_Q - x_P} \Big)$$

$$P + P = 2P = \Big(\underbrace{-2x_P + \Big(\frac{3x_P^2 + a}{2y_P}\Big)^2}_{x_{2P}}, -y_P - \frac{(x_{2P} - x_P)(3x_P^2 + a)}{2y_P} \Big)$$

Conséquences : On peut travailler sur n'importe quel corps (par exemple, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$,

Formule :

Si $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$, alors

$$P+Q = \Big(\underbrace{-x_P - x_Q + \Big(\frac{y_Q - y_P}{x_Q - x_P}\Big)^2}_{x_{P+Q}}, \frac{y_Q(x_P - x_{P+Q}) + y_P(x_{P+Q} - x_Q)}{x_Q - x_P} \Big)$$

$$P + P = 2P = \Big(\underbrace{-2x_P + \Big(\frac{3x_P^2 + a}{2y_P}\Big)^2}_{x_{2P}}, -y_P - \frac{(x_{2P} - x_P)(3x_P^2 + a)}{2y_P} \Big)$$

Conséquences : On peut travailler sur n'importe quel corps (par exemple, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$...)

Formule :

Si $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$, alors

$$P+Q = \Big(\underbrace{-x_P - x_Q + \Big(\frac{y_Q - y_P}{x_Q - x_P}\Big)^2}_{x_{P+Q}}, \frac{y_Q(x_P - x_{P+Q}) + y_P(x_{P+Q} - x_Q)}{x_Q - x_P} \Big)$$

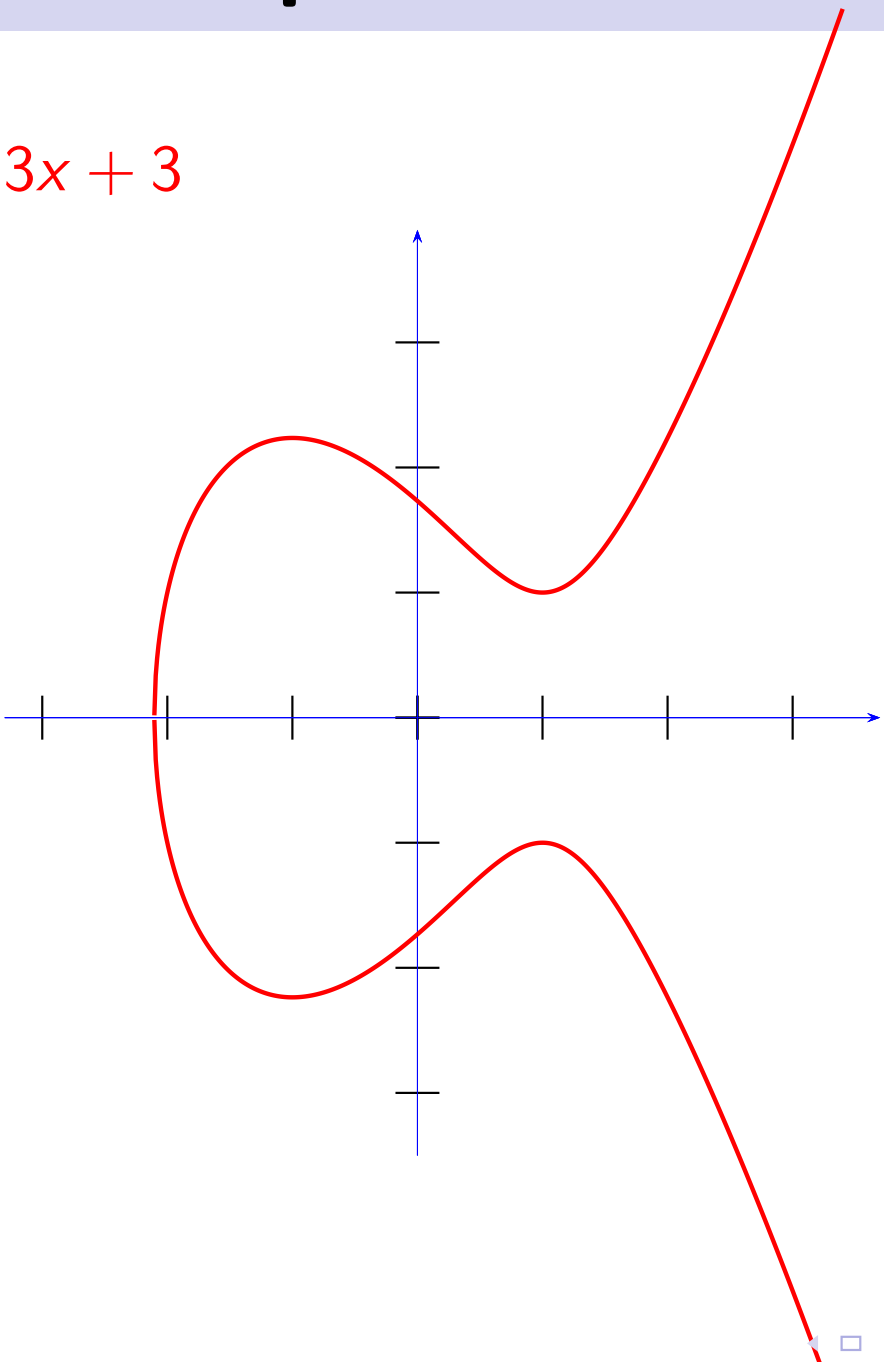
$$P + P = 2P = \Big(\underbrace{-2x_P + \Big(\frac{3x_P^2 + a}{2y_P}\Big)^2}_{x_{2P}}, -y_P - \frac{(x_{2P} - x_P)(3x_P^2 + a)}{2y_P} \Big)$$

Conséquences : On peut travailler sur n'importe quel corps (par exemple, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$...). Il suffit de prendre a et b dans ce corps.

Multiples d'un point :

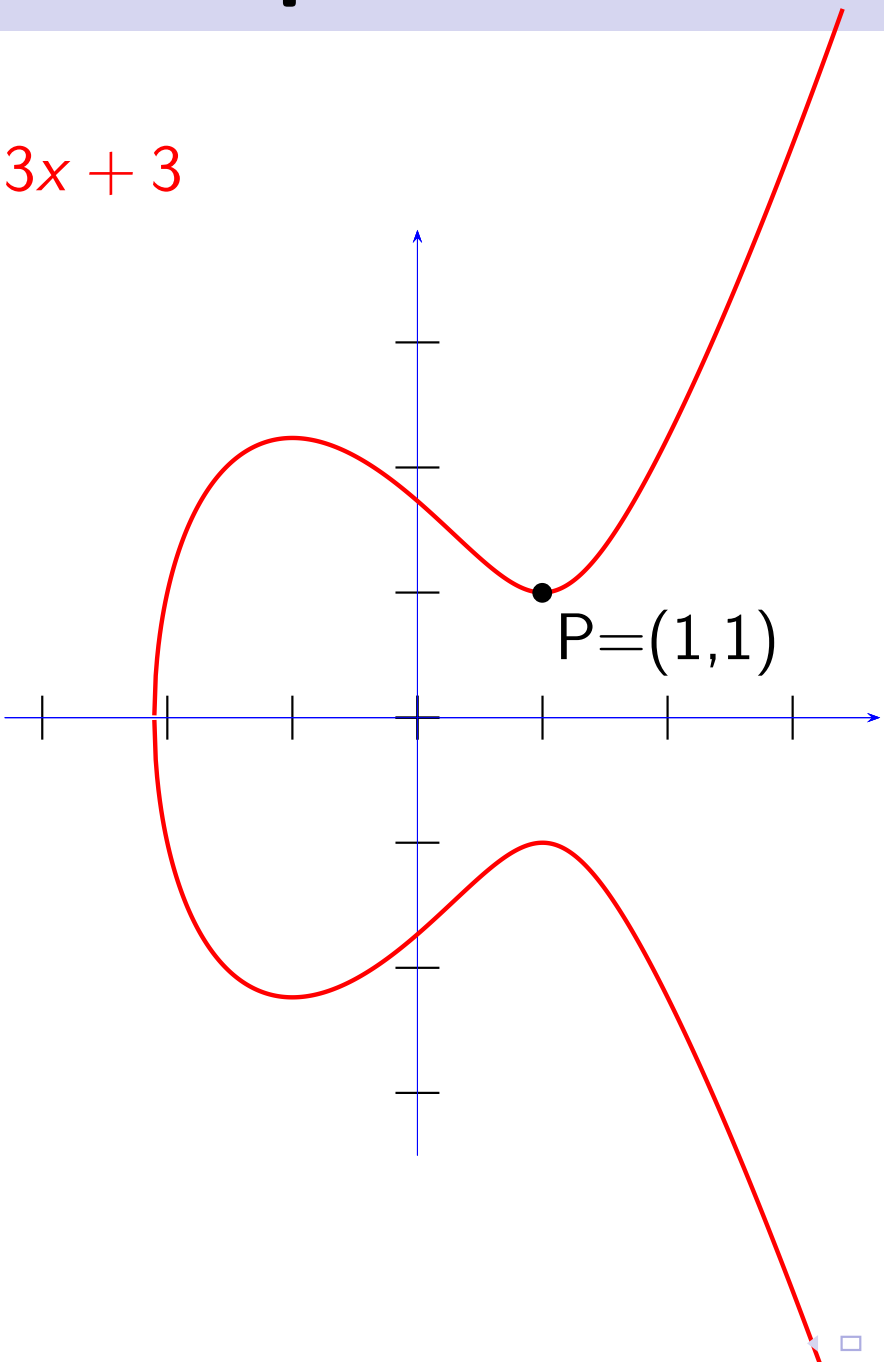
Multiples d'un point :

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



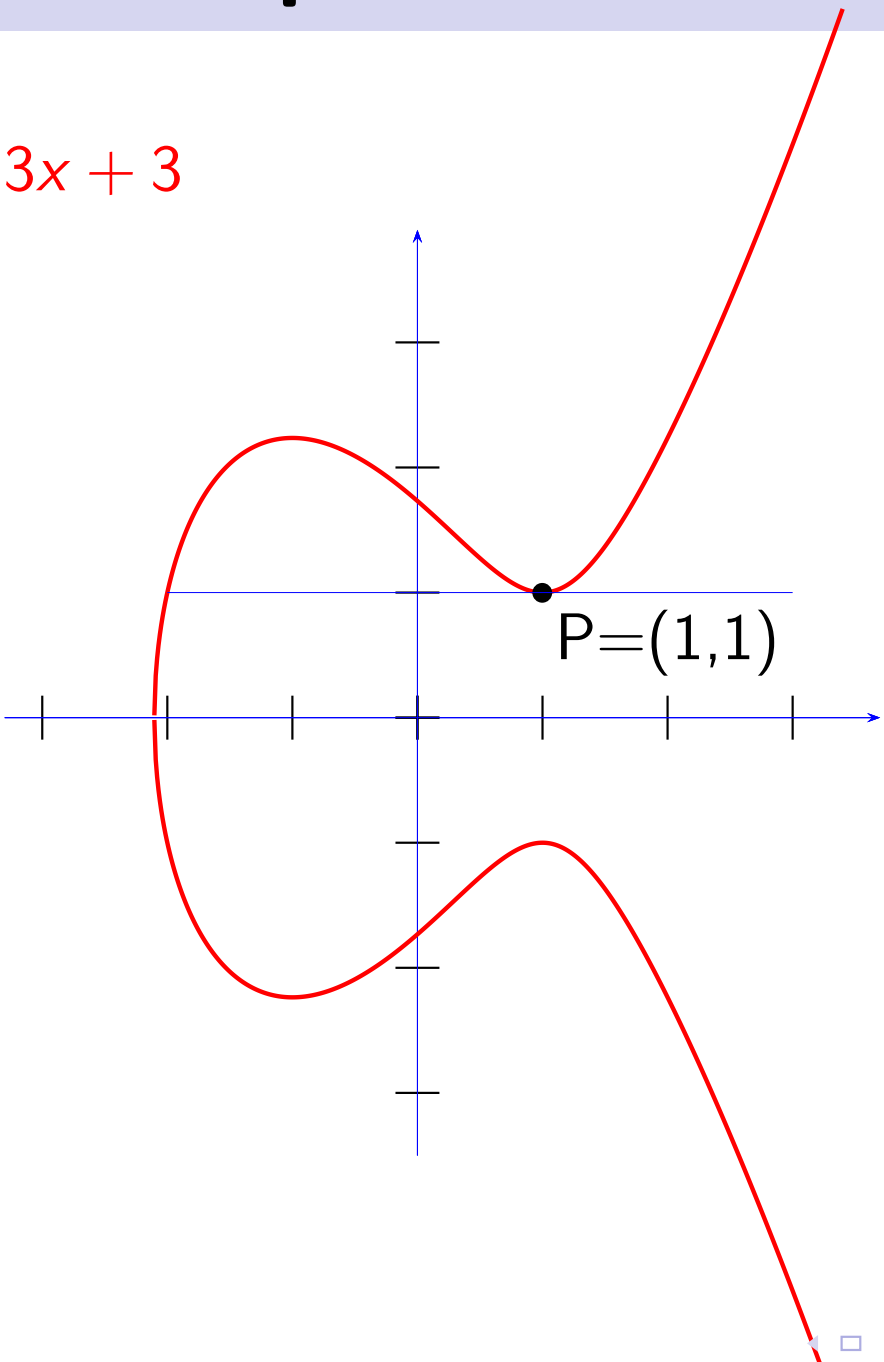
Multiples d'un point :

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



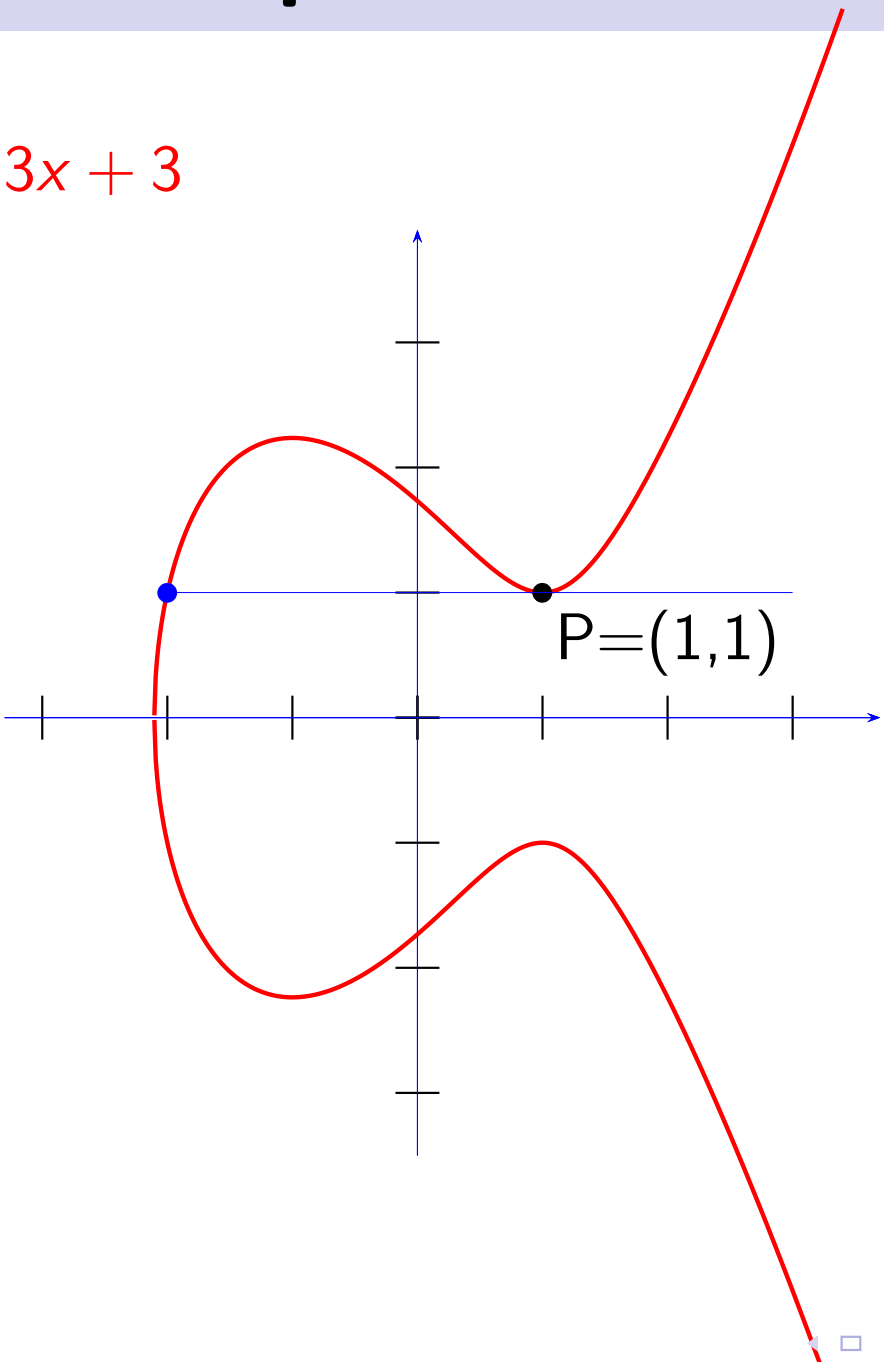
Multiples d'un point :

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



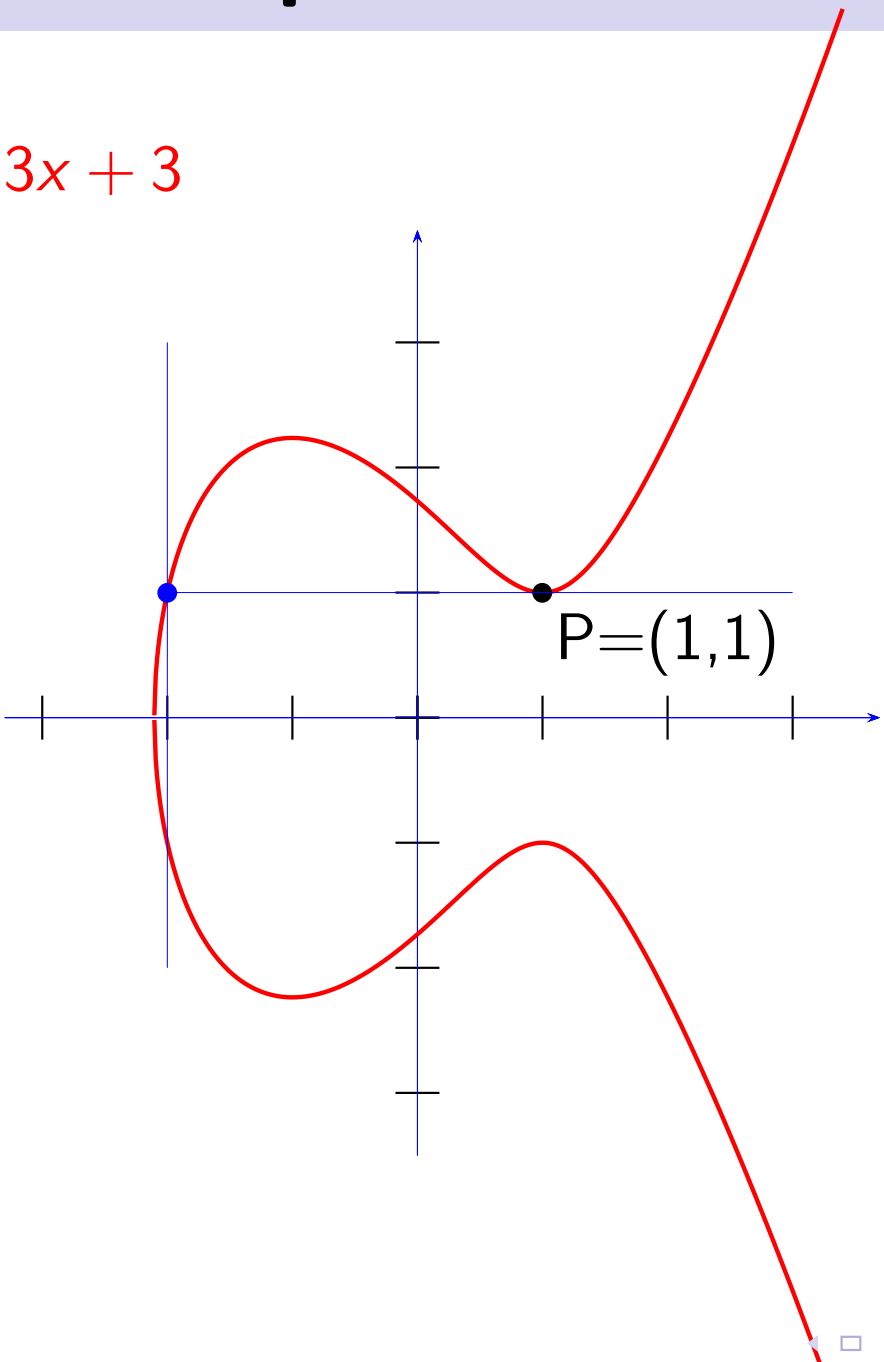
Multiples d'un point :

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



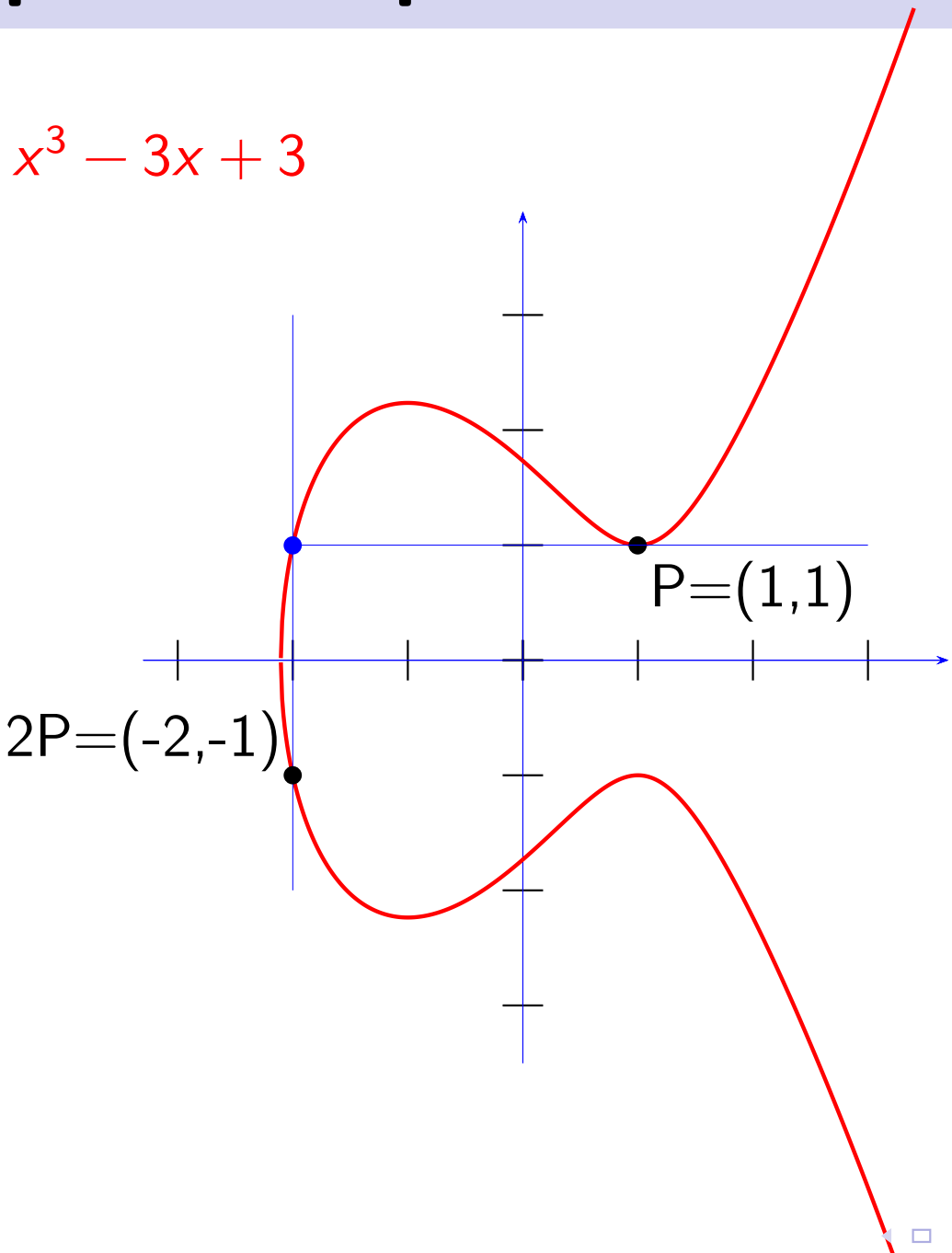
Multiples d'un point :

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



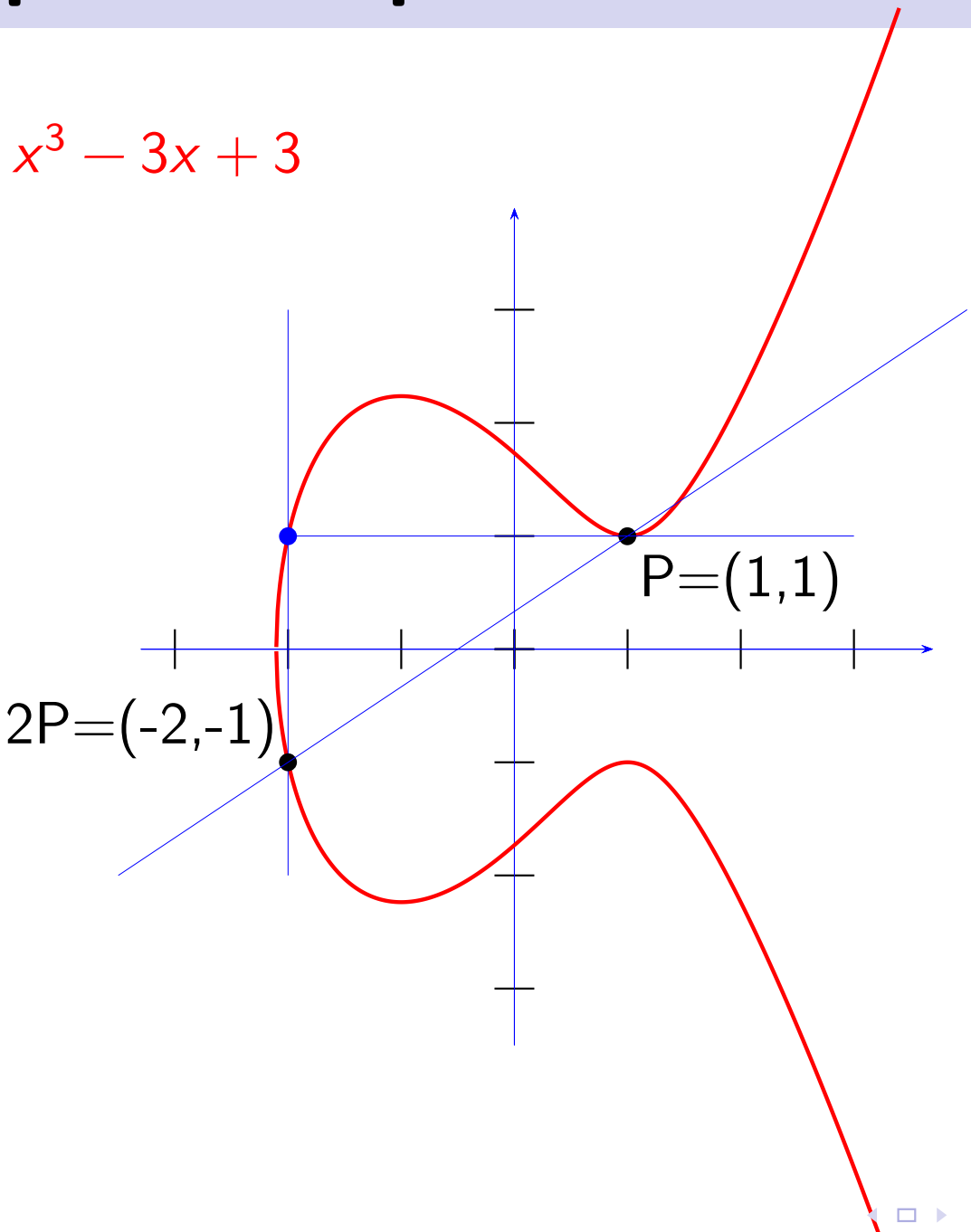
Multiples d'un point :

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



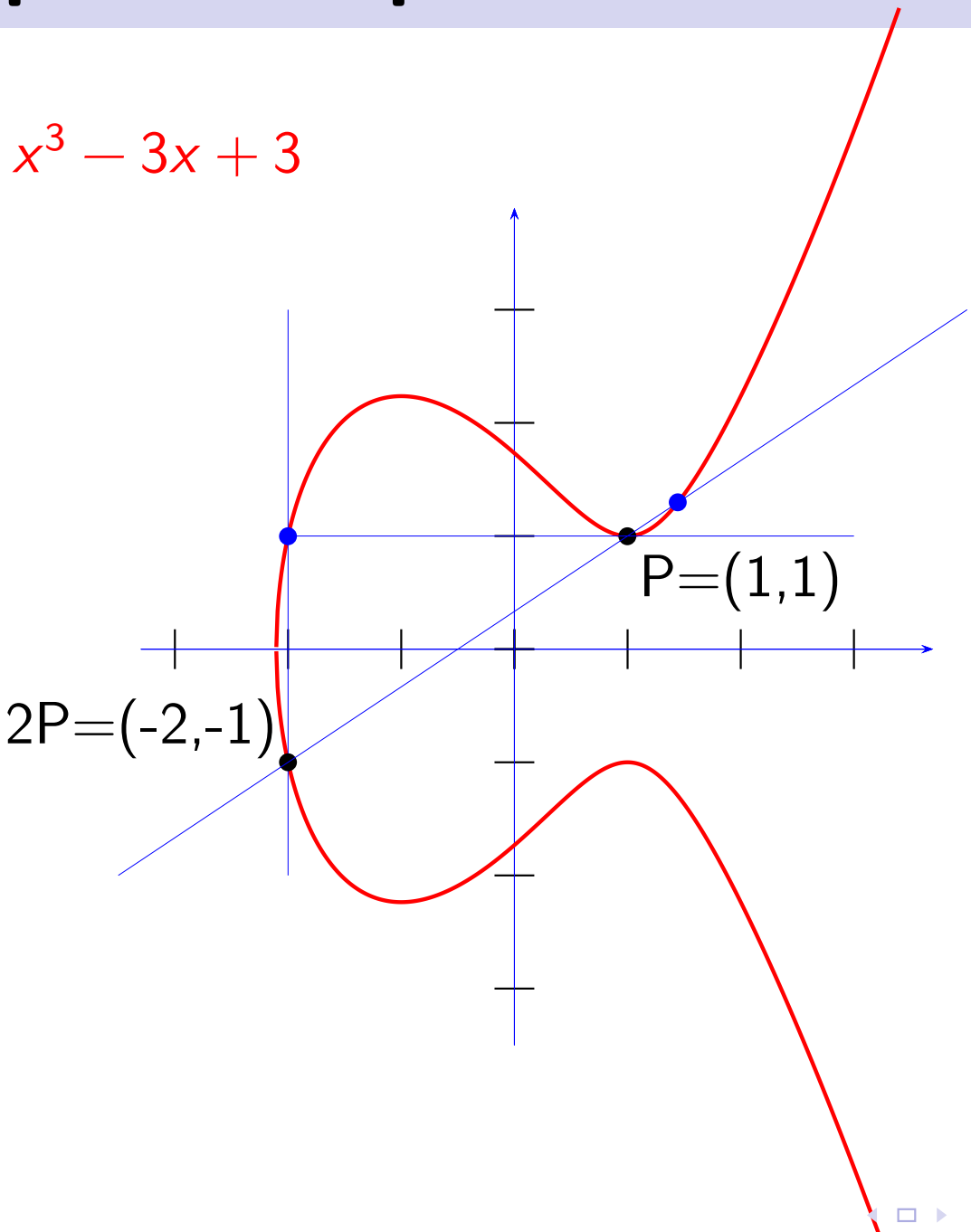
Multiples d'un point :

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



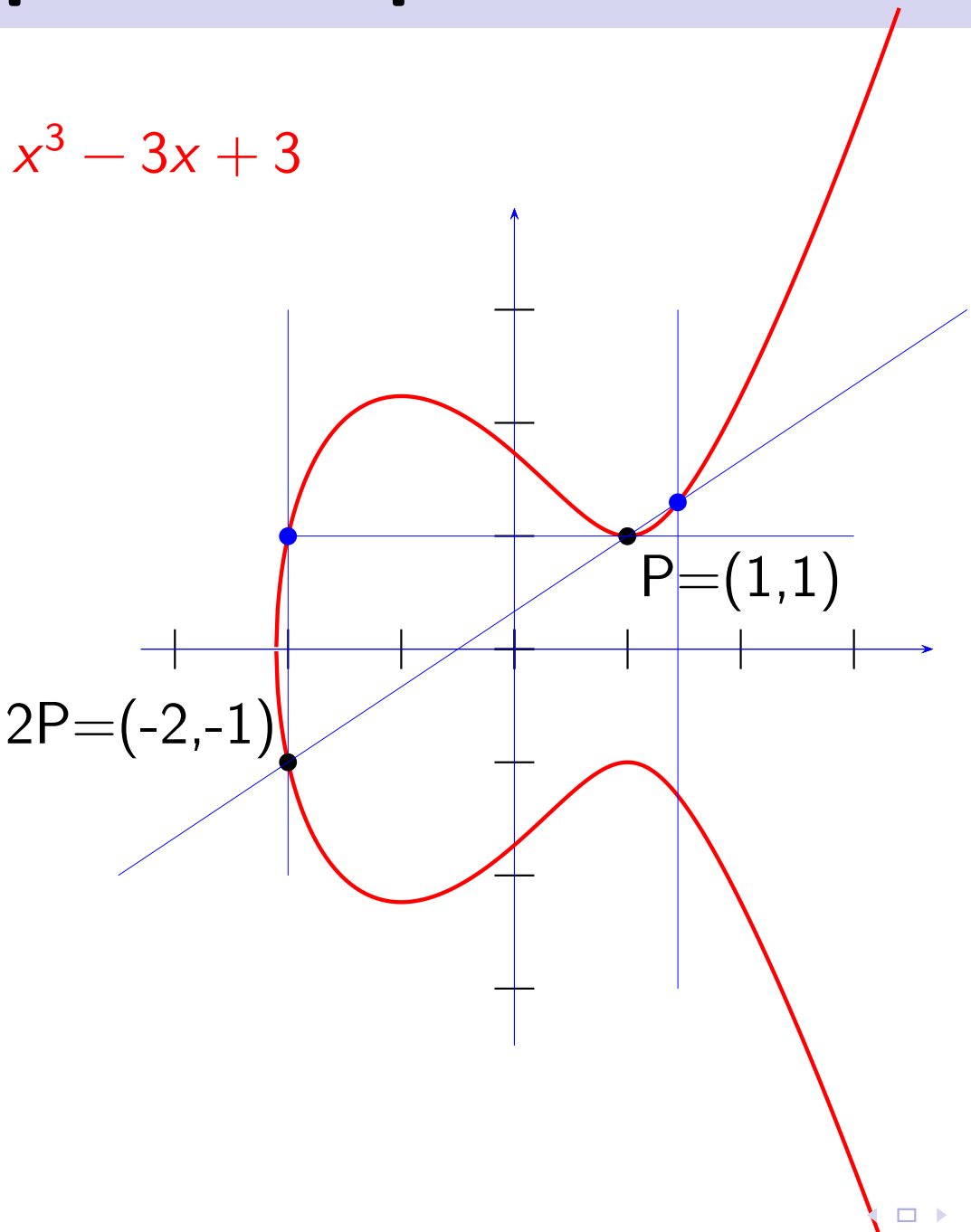
Multiples d'un point :

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



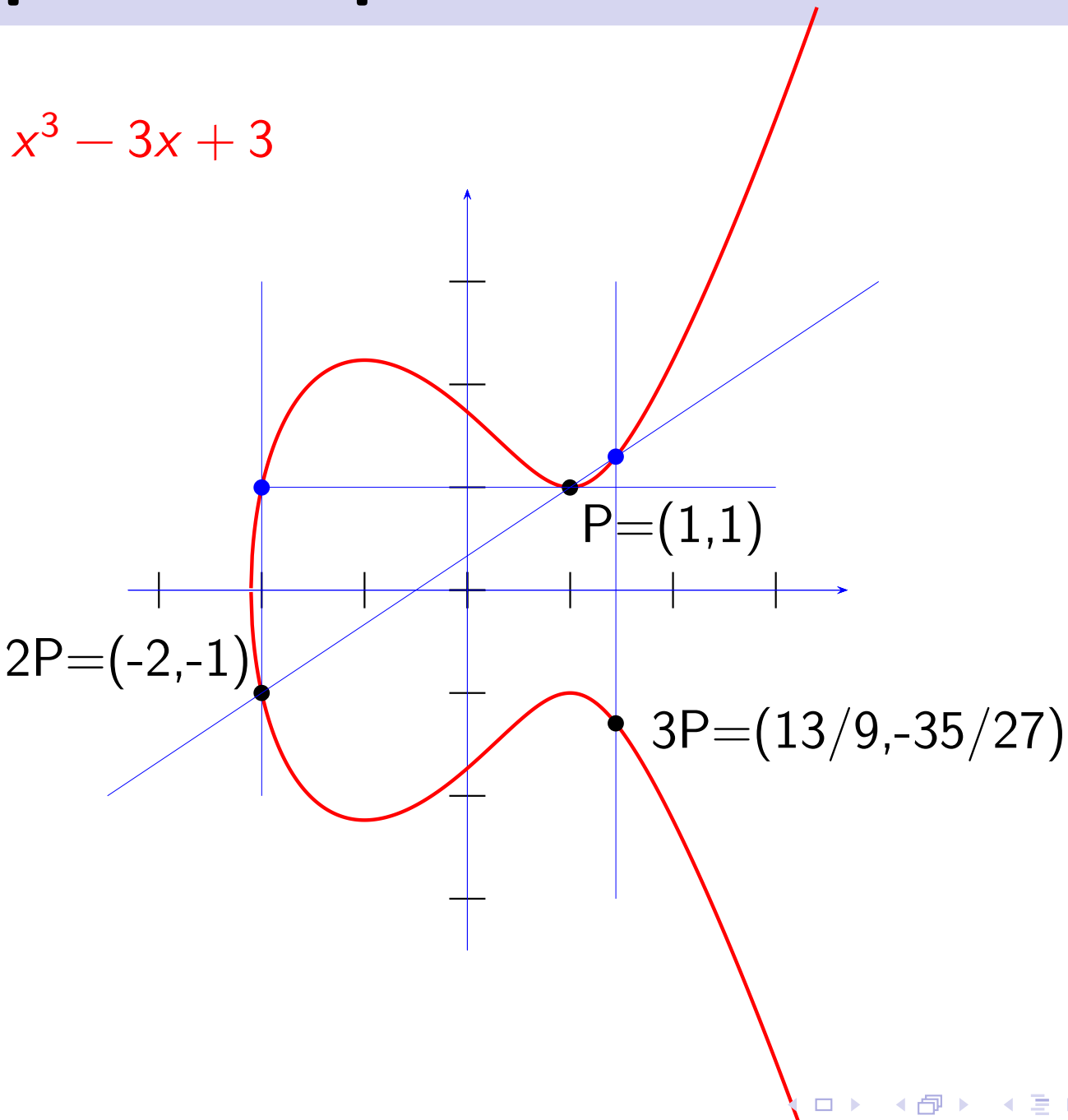
Multiples d'un point :

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



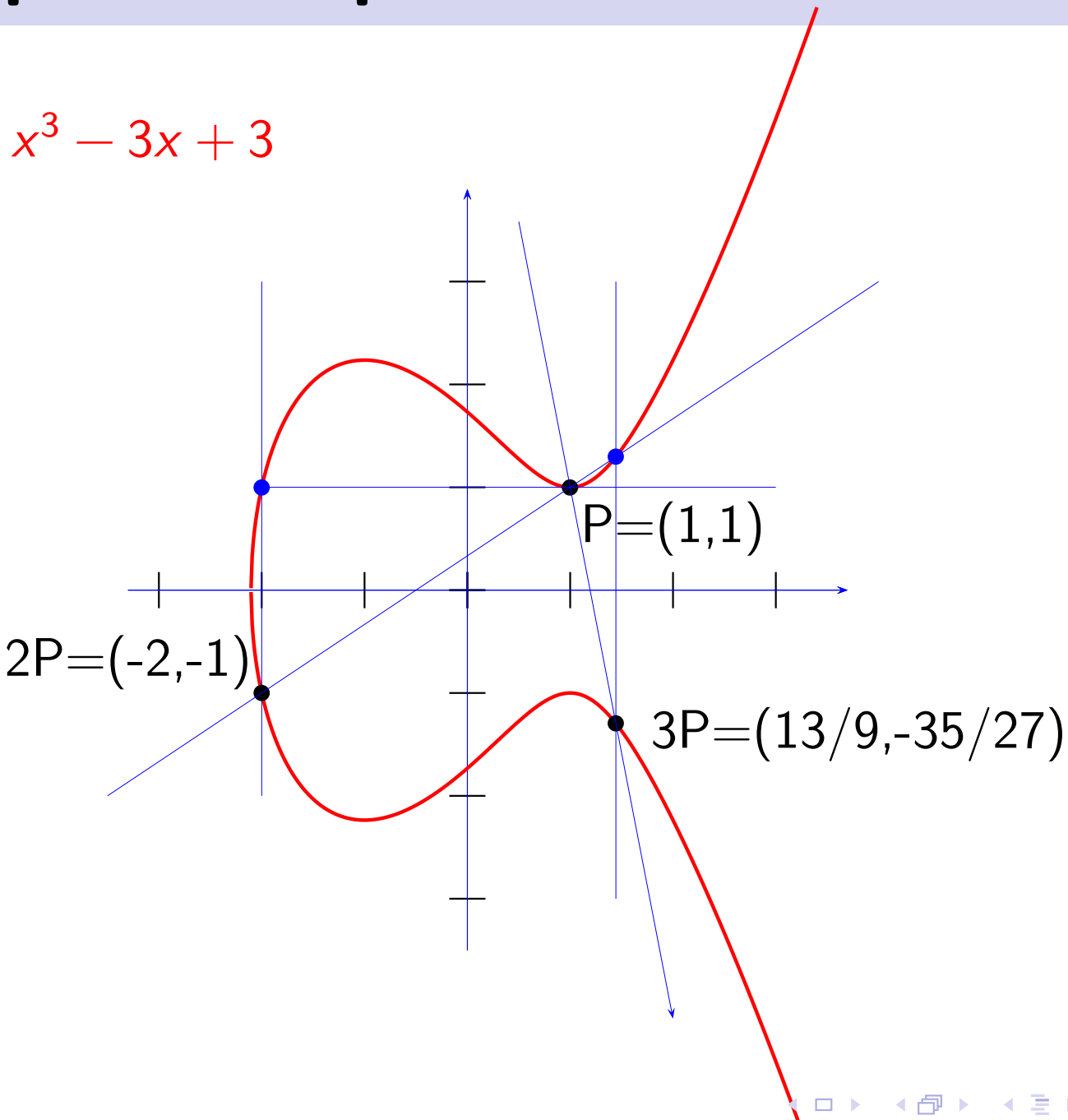
Multiples d'un point :

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



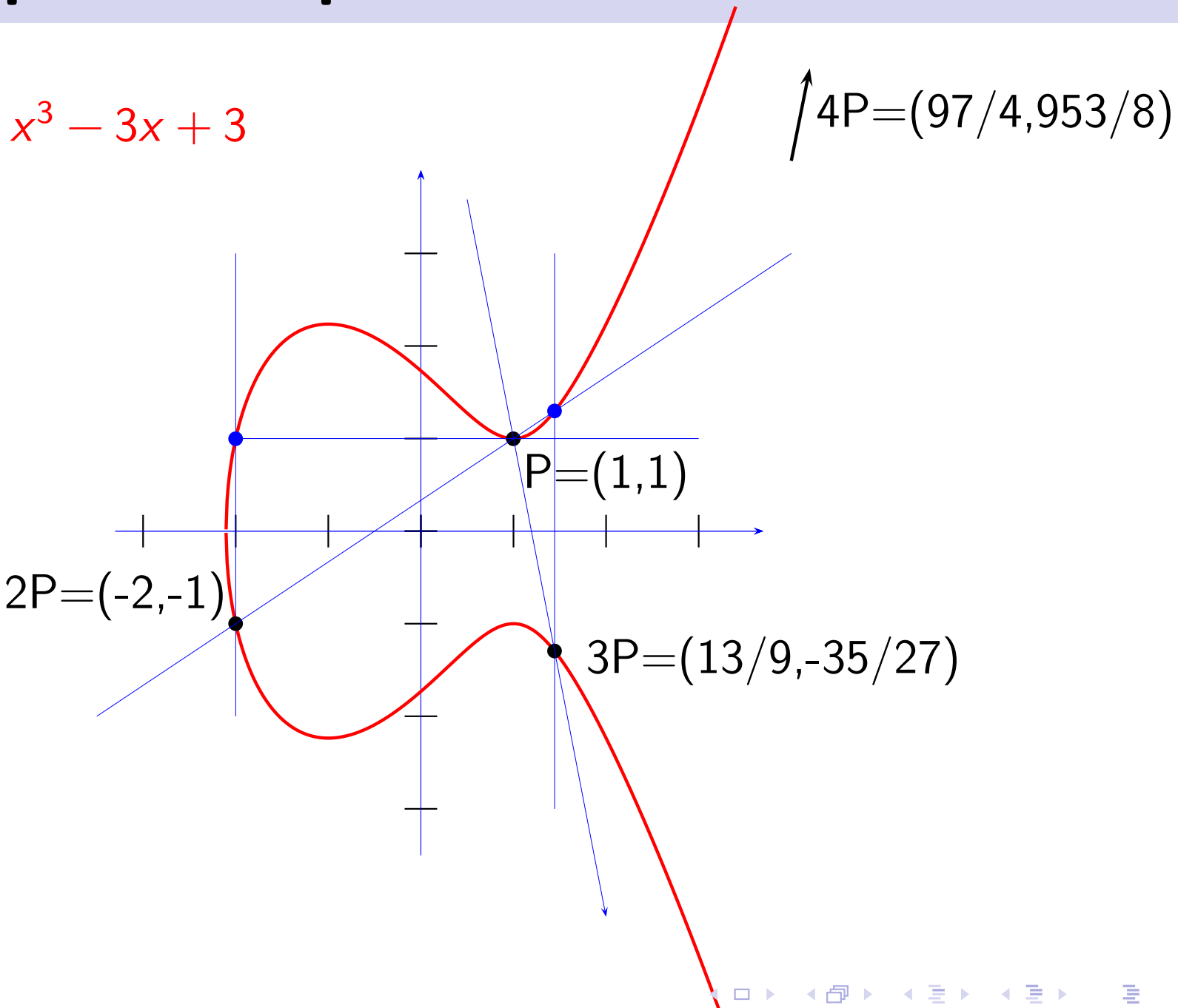
Multiples d'un point :

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



Multiples d'un point :

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



Torsion :

Torsion :

Définition. Un point P est dit de torsion s'il existe un entier naturel non nul m tel que $mP = O$.

Torsion :

Définition. Un point P est dit de torsion s'il existe un entier naturel non nul m tel que $mP = O$.

- $2P = O \iff$ la tangente à $\overline{\mathcal{C}}$ en P est verticale

Torsion :

Définition. Un point P est dit de torsion s'il existe un entier naturel non nul m tel que $mP = O$.

- $2P = O \iff$ la tangente à $\overline{\mathcal{C}}$ en P est verticale
- $3P = O \iff P$ est un point d'inflexion...

Corps des nombres complexes

Corps des nombres complexes

- Soit (λ_1, λ_2) une $\mathbb{R}$-base de $\mathbb{C}$

Corps des nombres complexes

- Soit (λ_1, λ_2) une $\mathbb{R}$-base de $\mathbb{C}$
- Soit $\Lambda = \{m\lambda_1 + n\lambda_2 \mid (m, n) \in \mathbb{Z}^2\}$

Corps des nombres complexes

- Soit (λ_1, λ_2) une $\mathbb{R}$-base de $\mathbb{C}$
- Soit $\Lambda = \{m\lambda_1 + n\lambda_2 \mid (m, n) \in \mathbb{Z}^2\}$
- On pose

$$\wp_\Lambda(z) = \wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Corps des nombres complexes

- Soit (λ_1, λ_2) une $\mathbb{R}$-base de $\mathbb{C}$
- Soit $\Lambda = \{m\lambda_1 + n\lambda_2 \mid (m, n) \in \mathbb{Z}^2\}$
- On pose

$$\wp_\Lambda(z) = \wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right).$$

$$g_2(\Lambda) = g_2 = \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^4} \quad \text{et} \quad g_3(\Lambda) = g_3 = \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^6}$$

Corps des nombres complexes

- Soit (λ_1, λ_2) une $\mathbb{R}$-base de $\mathbb{C}$
- Soit $\Lambda = \{m\lambda_1 + n\lambda_2 \mid (m,n) \in \mathbb{Z}^2\}$
- On pose

$$\wp_\Lambda(z) = \wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right).$$

$$g_2(\Lambda) = g_2 = \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^4} \quad \text{et} \quad g_3(\Lambda) = g_3 = \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^6}$$

- $\wp_\Lambda : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ est appelée la fonction elliptique de Weierstraß (associée à Λ)

Corps des nombres complexes

- Soit (λ_1, λ_2) une $\mathbb{R}$-base de $\mathbb{C}$
- Soit $\Lambda = \{m\lambda_1 + n\lambda_2 \mid (m,n) \in \mathbb{Z}^2\}$
- On pose

$$\wp_\Lambda(z) = \wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right).$$

$$g_2(\Lambda) = g_2 = \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^4} \quad \text{et} \quad g_3(\Lambda) = g_3 = \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^6}$$

- $\wp_\Lambda : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ est appelée la fonction elliptique de Weierstraß (associée à Λ)
- $\wp_\Lambda(z+\lambda) = \wp_\Lambda(z)$ si $z \in \mathbb{C}$ et $\lambda \in \Lambda$.

Corps des nombres complexes (suite)

Corps des nombres complexes (suite)

Théorème

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

Corps des nombres complexes (suite)

Théorème

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

Corollaire

Soit $\overline{\mathcal{C}} = \{(x, y) \in \mathbb{C}^2 \mid y^2 = 4x^3 - g_2x - g_3\} \cup \{O\}$. Alors

$$\begin{array}{rccc} \wp : & \mathbb{C}/\Lambda & \longrightarrow & \overline{\mathcal{C}} \\ & z & \longmapsto & (\wp(z), \wp'(z)) \end{array}$$

est un isomorphisme de groupes

Corps des nombres complexes (suite)

Théorème

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

Corollaire

Soit $\overline{\mathcal{C}} = \{(x, y) \in \mathbb{C}^2 \mid y^2 = 4x^3 - g_2x - g_3\} \cup \{O\}$. Alors

$$\begin{array}{rccc} \wp : & \mathbb{C}/\Lambda & \longrightarrow & \overline{\mathcal{C}} \\ & z & \longmapsto & (\wp(z), \wp'(z)) \end{array}$$

est un isomorphisme de groupes (algébriques).

Corps des nombres complexes (curiosité)

Corps des nombres complexes (curiosité)

$$g_2(\mathbb{Z}+\mathbb{Z}\tau) = \frac{4\pi^4}{3}\left(1 - 240\sum_{n=1}^{\infty}\sigma_3(n)e^{2in\pi\tau}\right)$$

Corps des nombres complexes (curiosité)

$$g_2(\mathbb{Z}+\mathbb{Z}\tau) = \frac{4\pi^4}{3}\left(1 - 240\sum_{n=1}^{\infty}\sigma_3(n)e^{2in\pi\tau}\right)$$

$$g_3(\mathbb{Z}+\mathbb{Z}\tau) = \frac{8\pi^6}{27}\left(1 + 504\sum_{n=1}^{\infty}\sigma_5(n)e^{2in\pi\tau}\right)$$

Corps des nombres complexes (curiosité)

$$g_2(\mathbb{Z}+\mathbb{Z}\tau) = \frac{4\pi^4}{3}\left(1 - 240\sum_{n=1}^{\infty}\sigma_3(n)e^{2in\pi\tau}\right)$$

$$g_3(\mathbb{Z}+\mathbb{Z}\tau) = \frac{8\pi^6}{27}\left(1 + 504\sum_{n=1}^{\infty}\sigma_5(n)e^{2in\pi\tau}\right)$$

où $$\sigma_k(n) = \sum_{d \mid n} d^k$$

Corps des nombres rationnels

Corps des nombres rationnels

On suppose ici a, $b \in \mathbb{Q}$.

Corps des nombres rationnels

On suppose ici a, $b \in \mathbb{Q}$.

Alors $\overline{\mathcal{C}} = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + ax + b\} \cup \{O\}$ est un sous-groupe de $\overline{\mathcal{C}}(\mathbb{R})$.

Corps des nombres rationnels

On suppose ici $a,\ b \in \mathbb{Q}$.

Alors $\overline{\mathcal{C}} = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + ax + b\} \cup \{O\}$ est un sous-groupe de $\overline{\mathcal{C}}(\mathbb{R})$.

Théorème (Mordell, 1922)

Il existe $P_1, \ldots, P_n$ tels que $\overline{\mathcal{C}} = \langle P_1, P_2, \ldots, P_n \rangle$.

Définition

On note $\mathrm{rang}(\overline{\mathcal{C}})$ le plus grand entier r tel qu'il existe $P_1, \ldots, P_r \in \overline{\mathcal{C}}$ qui soient $\mathbb{Z}$-linéairement indépendants.

Corps des nombres rationnels

On suppose ici a, $b \in \mathbb{Q}$.

Alors $\overline{\mathcal{C}} = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + ax + b\} \cup \{O\}$ est un sous-groupe de $\overline{\mathcal{C}}(\mathbb{R})$.

Théorème (Mordell, 1922)

Il existe $P_1, \ldots, P_n$ tels que $\overline{\mathcal{C}} = \langle P_1, P_2, \ldots, P_n \rangle$.

Définition

On note $\mathrm{rang}(\overline{\mathcal{C}})$ le plus grand entier r tel qu'il existe $P_1, \ldots, P_r \in \overline{\mathcal{C}}$ qui soient $\mathbb{Z}$-linéairement indépendants. Le nombre $\mathrm{rang}(\overline{\mathcal{C}})$ est appelé le rang de $\overline{\mathcal{C}}$.

Conjecture

Il existe des courbes elliptiques de rang aussi grand que l'on veut.

Conjecture

Il existe des courbes elliptiques de rang aussi grand que l'on veut.

Record du monde (Elkies, 2006) : rang $\geqslant 28$

Conjecture

Il existe des courbes elliptiques de rang aussi grand que l'on veut.

Record du monde (Elkies, 2006) : rang $\geqslant 28$

$$y^2 + xy + y = x^3 - x^2$$

$$-20067762415575526585033208209338542750930230312178956502\ x$$

$$+3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

Conjecture

Il existe des courbes elliptiques de rang aussi grand que l'on veut.

Record du monde (Elkies, 2006) : rang $\geqslant 28$

$$y^2 + xy + y = x^3 - x^2$$

$$-2006776241557552658503320820933854275093023031217895650 2\, x$$
$$+3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

$$\begin{aligned}
P_1 &= (-212415009125438107329213746 3, \\
&\quad 259854492051899599030515511070780628911531) \\
P_2 &= (233450986603470175688475453 7, \\
&\quad 188720041954944691808683165528036279315 31) \\
&\ldots \\
P_{28} &= (223086828977357602377867873 7, \\
&\quad 285587600305974856633870206007686400285 31)
\end{aligned}$$

Conjecture

Le rang moyen d'une courbe elliptique est $1/2$,

Conjecture

Le rang moyen d'une courbe elliptique est $1/2$*, avec probabilité* $1/2$ *pour le rang* 0 *et probabilité* $1/2$ *pour le rang* 1*.*

Conjecture

Le rang moyen d'une courbe elliptique est $1/2$*, avec probabilité* $1/2$ *pour le rang* 0 *et probabilité* $1/2$ *pour le rang* 1*.*

Théorème (Bhargava-Shankar, 2013)

Le rang moyen d'une courbe elliptique est $\leqslant 0,885$*.*

Corps finis

Corps finis

a, $b \in \mathbb{Z}/p\mathbb{Z}$, p nombre premier

Corps finis

a, $b \in \mathbb{Z}/p\mathbb{Z}$, p nombre premier

$$\overline{\mathcal{C}}(\mathbb{Z}/p\mathbb{Z}) = \{(x, y) \in \mathbb{Z}/p\mathbb{Z} \mid y^2 = x^3 + ax + b\} \cup \{O\}.$$

Corps finis

a, $b \in \mathbb{Z}/p\mathbb{Z}$, p nombre premier

$$\overline{\mathcal{C}}(\mathbb{Z}/p\mathbb{Z}) = \{(x, y) \in \mathbb{Z}/p\mathbb{Z} \mid y^2 = x^3 + ax + b\} \cup \{O\}.$$

On pose $N_p = |\overline{\mathcal{C}}(\mathbb{Z}/p\mathbb{Z})|$.

Théorème (Hasse, 1936)

$$|N_p - (p+1)| \leqslant 2\sqrt{p}.$$

Corps finis

a, $b \in \mathbb{Z}/p\mathbb{Z}$, p nombre premier

$$\overline{\mathcal{C}}(\mathbb{Z}/p\mathbb{Z}) = \{(x, y) \in \mathbb{Z}/p\mathbb{Z} \mid y^2 = x^3 + ax + b\} \cup \{O\}.$$

On pose $N_p = |\overline{\mathcal{C}}(\mathbb{Z}/p\mathbb{Z})|$.

Théorème (Hasse, 1936)

$$|N_p - (p+1)| \leqslant 2\sqrt{p}.$$

Exemple : $y^2 = x^3 - 3x + 3$

p	2	3	5	7	11	13	$\cdots$	129	$\cdots$	1361
$N_p - p - 1$	-1	-1	0	-3	3	1	$\cdots$	-13	$\cdots$	55

Corps finis (suite)

Corps finis (suite)

On prends ici a, $b \in \mathbb{Z}$ et on note

$$\overline{\mathcal{C}}(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + ax + b\}$$

et $$\overline{\mathcal{C}}(\mathbb{Z}/p\mathbb{Z}) = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid y^2 = x^3 + ax + b\}.$$

Corps finis (suite)

On prends ici a, $b \in \mathbb{Z}$ et on note

$$\overline{\mathcal{C}}(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + ax + b\}$$

et $$\overline{\mathcal{C}}(\mathbb{Z}/p\mathbb{Z}) = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid y^2 = x^3 + ax + b\}.$$

Conjecture de Birch et Swinnerton-Dyer

Il existe une constante c ne dépendant que de $\overline{\mathcal{C}}$ telle que

$$\prod_{p \leqslant x} \frac{N_p}{p} \underset{x \to +\infty}{\sim} c\mathrm{Log}(x)^{?} \quad .$$

Corps finis (suite)

On prends ici a, $b \in \mathbb{Z}$ et on note

$$\overline{\mathcal{C}}(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + ax + b\}$$

et $$\overline{\mathcal{C}}(\mathbb{Z}/p\mathbb{Z}) = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid y^2 = x^3 + ax + b\}.$$

Conjecture de Birch et Swinnerton-Dyer

Il existe une constante c ne dépendant que de $\overline{\mathcal{C}}$ telle que

$$\prod_{p \leqslant x} \frac{N_p}{p} \underset{x \to +\infty}{\sim} c\mathrm{Log}(x)^{\mathrm{rang}(\overline{\mathcal{C}}(\mathbb{Q}))}.$$

Corps finis (suite)

On prends ici a, $b \in \mathbb{Z}$ et on note

$$\overline{\mathcal{C}}(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + ax + b\}$$

et $$\overline{\mathcal{C}}(\mathbb{Z}/p\mathbb{Z}) = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid y^2 = x^3 + ax + b\}.$$

Conjecture de Birch et Swinnerton-Dyer

Il existe une constante c ne dépendant que de $\overline{\mathcal{C}}$ telle que

$$\prod_{p \leqslant x} \frac{N_p}{p} \underset{x \to +\infty}{\sim} c\mathrm{Log}(x)^{\mathrm{rang}(\overline{\mathcal{C}}(\mathbb{Q}))}.$$

Théorème (Bhargava-Skinner-Zhang, 2014)

Au moins 66% des courbes elliptiques vérifient la conjecture de Birch et Swinnerton-Dyer

Corps finis (suite)

On prends ici a, $b \in \mathbb{Z}$ et on note

$$\overline{\mathcal{C}}(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + ax + b\}$$

et $$\overline{\mathcal{C}}(\mathbb{Z}/p\mathbb{Z}) = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid y^2 = x^3 + ax + b\}.$$

Conjecture de Birch et Swinnerton-Dyer

Il existe une constante c ne dépendant que de $\overline{\mathcal{C}}$ telle que

$$\prod_{p \leqslant x} \frac{N_p}{p} \underset{x \to +\infty}{\sim} c\mathrm{Log}(x)^{\mathrm{rang}(\overline{\mathcal{C}}(\mathbb{Q}))}.$$

Théorème (Bhargava-Skinner-Zhang, 2014)

Au moins 66% des courbes elliptiques vérifient la conjecture de Birch et Swinnerton-Dyer (!).

Avec les courbes elliptiques, on peut faire :

Avec les courbes elliptiques, on peut faire :

- de l'algèbre (théorie des groupes)

Avec les courbes elliptiques, on peut faire :

- de l'algèbre (théorie des groupes)
- de l'analyse réelle (*intégrales elliptiques*)

Avec les courbes elliptiques, on peut faire :

- de l'algèbre (théorie des groupes)
- de l'analyse réelle (*intégrales elliptiques*)
- de l'analyse complexe (fonction de Weierstraß)

Avec les courbes elliptiques, on peut faire :

- de l'algèbre (théorie des groupes)
- de l'analyse réelle (*intégrales elliptiques*)
- de l'analyse complexe (fonction de Weierstraß)
- de la théorie des nombres (Birch et Swinnerton-Dyer)

Avec les courbes elliptiques, on peut faire :

- de l'algèbre (théorie des groupes)
- de l'analyse réelle (*intégrales elliptiques*)
- de l'analyse complexe (fonction de Weierstraß)
- de la théorie des nombres (Birch et Swinnerton-Dyer)
- de la cryptographie

Avec les courbes elliptiques, on peut faire :

- de l'algèbre (théorie des groupes)
- de l'analyse réelle (*intégrales elliptiques*)
- de l'analyse complexe (fonction de Weierstraß)
- de la théorie des nombres (Birch et Swinnerton-Dyer)
- de la cryptographie
- la démonstration du théorème de Fermat (Wiles, Taylor-Wiles) :

Avec les courbes elliptiques, on peut faire :

- de l'algèbre (théorie des groupes)
- de l'analyse réelle (*intégrales elliptiques*)
- de l'analyse complexe (fonction de Weierstraß)
- de la théorie des nombres (Birch et Swinnerton-Dyer)
- de la cryptographie
- la démonstration du théorème de Fermat (Wiles, Taylor-Wiles) : si $a^p + b^p = c^p$ avec p premier $\geqslant 3$ et $abc \neq 0$, alors la courbe elliptique définie par l'équation

$$y^2 = x(x + a^p)(x - b^p)$$

Avec les courbes elliptiques, on peut faire :

- de l'algèbre (théorie des groupes)
- de l'analyse réelle (*intégrales elliptiques*)
- de l'analyse complexe (fonction de Weierstraß)
- de la théorie des nombres (Birch et Swinnerton-Dyer)
- de la cryptographie
- la démonstration du théorème de Fermat (Wiles, Taylor-Wiles) : si $a^p + b^p = c^p$ avec p premier $\geqslant 3$ et $abc \neq 0$, alors la courbe elliptique définie par l'équation

$$y^2 = x(x + a^p)(x - b^p)$$

est trop bizarre pour exister (courbe de Hellegouarch).

Avec les courbes elliptiques, on peut faire :

- de l'algèbre (théorie des groupes)
- de l'analyse réelle (*intégrales elliptiques*)
- de l'analyse complexe (fonction de Weierstraß)
- de la théorie des nombres (Birch et Swinnerton-Dyer)
- de la cryptographie
- la démonstration du théorème de Fermat (Wiles, Taylor-Wiles) : si $a^p + b^p = c^p$ avec p premier $\geqslant 3$ et $abc \neq 0$, alors la courbe elliptique définie par l'équation

$$y^2 = x(x + a^p)(x - b^p)$$

  est trop bizarre pour exister (courbe de Hellegouarch).

- de la géométrie...

Avec les courbes elliptiques, on peut faire :

- de l'algèbre (théorie des groupes)
- de l'analyse réelle (*intégrales elliptiques*)
- de l'analyse complexe (fonction de Weierstraß)
- de la théorie des nombres (Birch et Swinnerton-Dyer)
- de la cryptographie
- la démonstration du théorème de Fermat (Wiles, Taylor-Wiles) : si $a^p + b^p = c^p$ avec p premier $\geqslant 3$ et $abc \neq 0$, alors la courbe elliptique définie par l'équation

$$y^2 = x(x + a^p)(x - b^p)$$

  est trop bizarre pour exister (courbe de Hellegouarch).
- de la géométrie...