Journée de rentrée

Emiliano AMBROSI

IRMA

25/09/2020

Domaine de recherche

Géométrie arithmétique

Qu'est-ce que fait le géomètre arithmétique ?

Domaine de recherche

Géométrie arithmétique

Qu'est-ce que fait le géomètre arithmétique ?

- Il ne connait pas très bien l'arithmétique

Domaine de recherche

Géométrie arithmétique

Qu'est-ce que fait le géomètre arithmétique ?

- Il ne connait pas très bien l'arithmétique
- Il ne connait pas très bien la géométrie

Domaine de recherche

Géométrie arithmétique

Qu'est-ce que fait le géomètre arithmétique ?

- Il ne connait pas très bien l'arithmétique
- Il ne connait pas très bien la géométrie
- Mais il est content de ça!

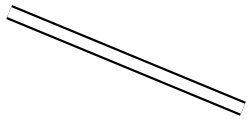
Domaine de recherche

Arithmétique

Géométrie

Domaine de recherche

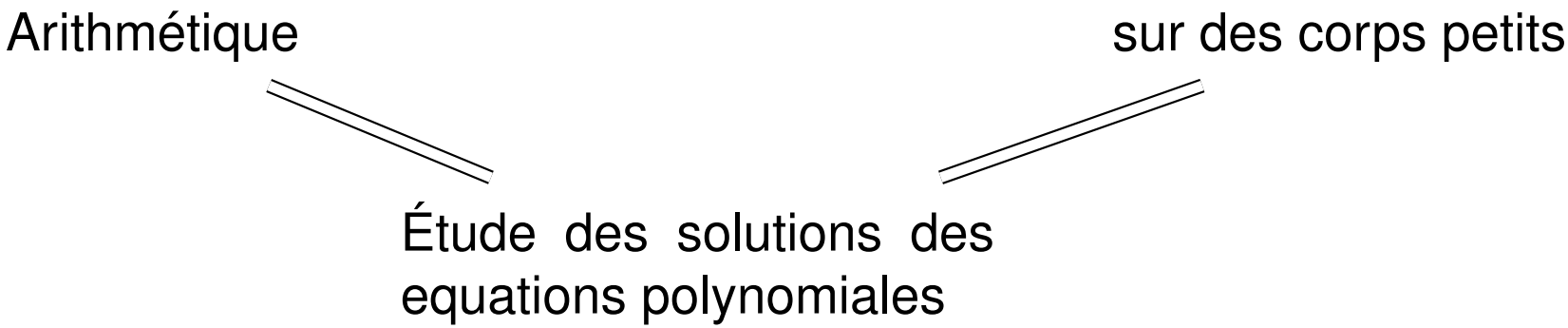
Arithmétique



Étude des solutions des equations polynomiales

Géométrie

Domaine de recherche



Domaine de recherche

$$\{(x, y) \in \mathbb{Q}^2 : x^n + y^n = 1\}$$

Arithmétique

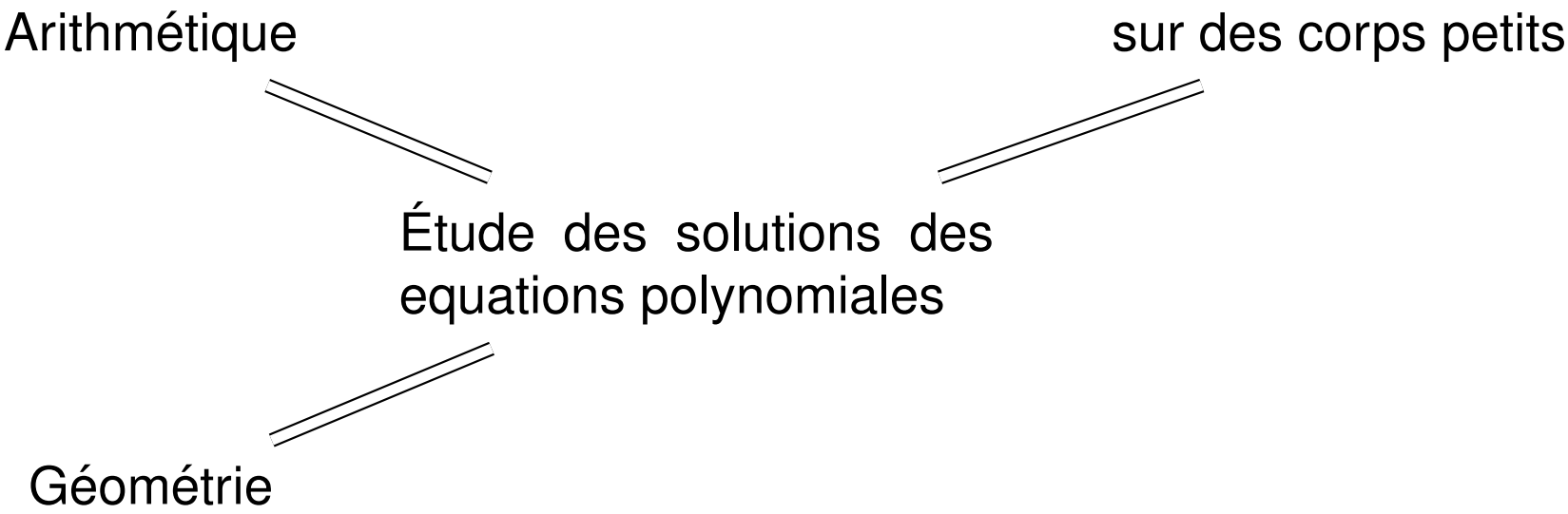
sur des corps petits

Étude des solutions des equations polynomiales

Géométrie

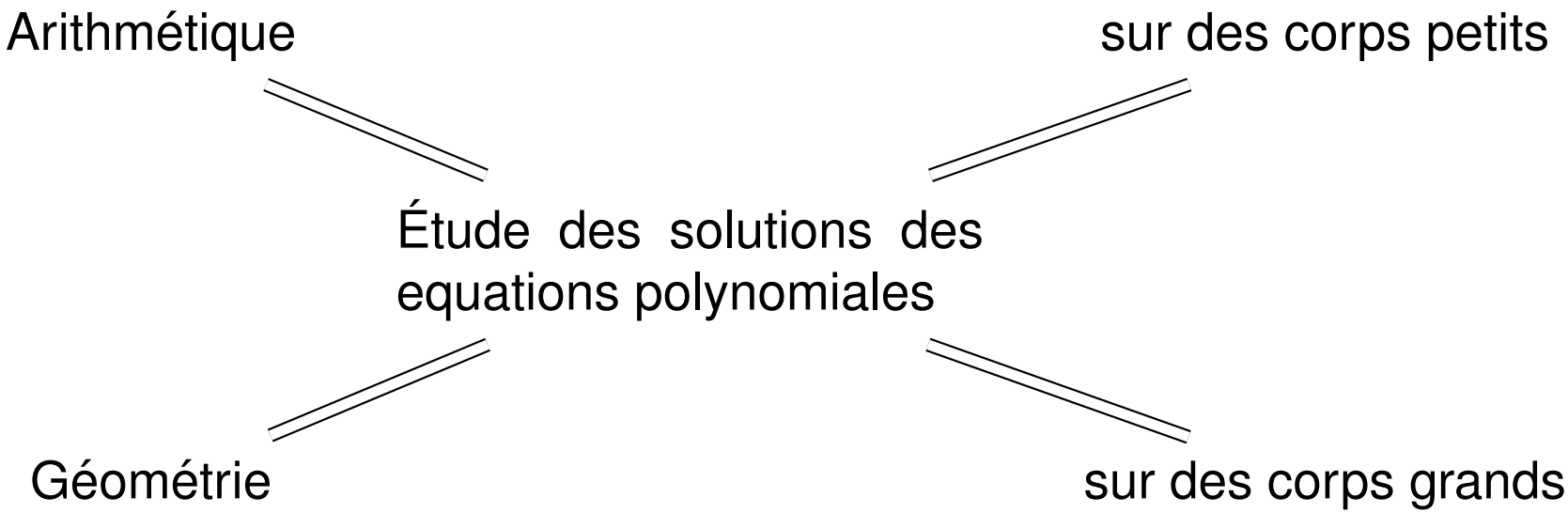
Domaine de recherche

$$\{(x, y) \in \mathbb{Q}^2 : x^n + y^n = 1\}$$



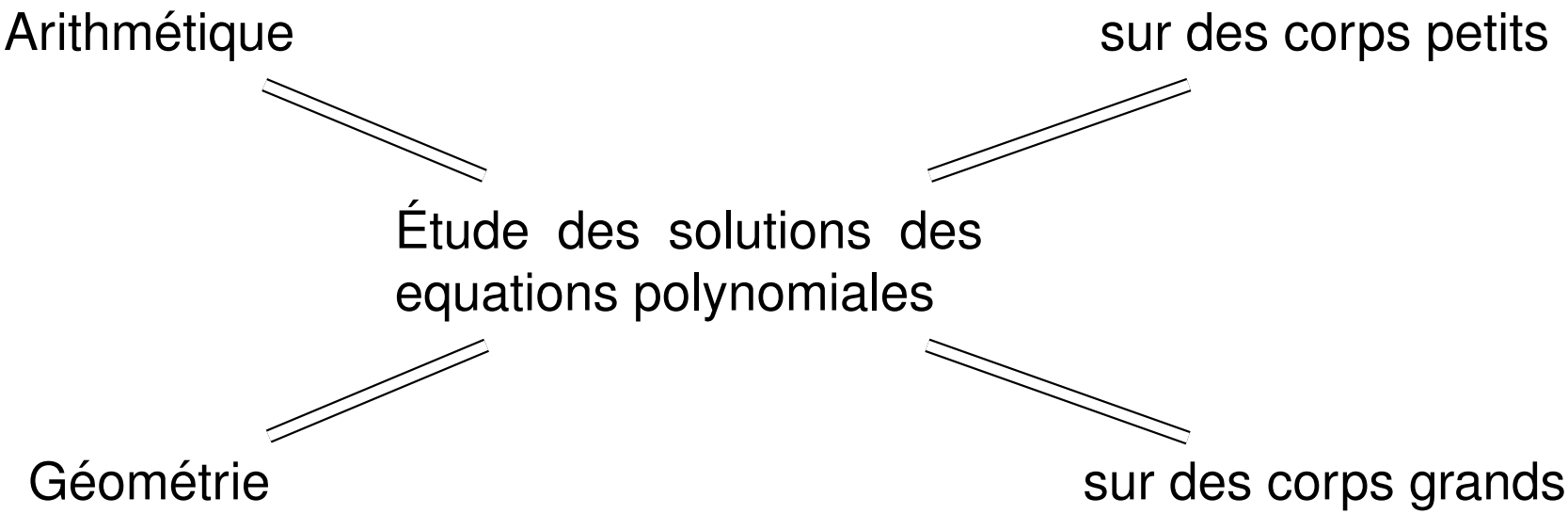
Domaine de recherche

$$\{(x, y) \in \mathbb{Q}^2 : x^n + y^n = 1\}$$



Domaine de recherche

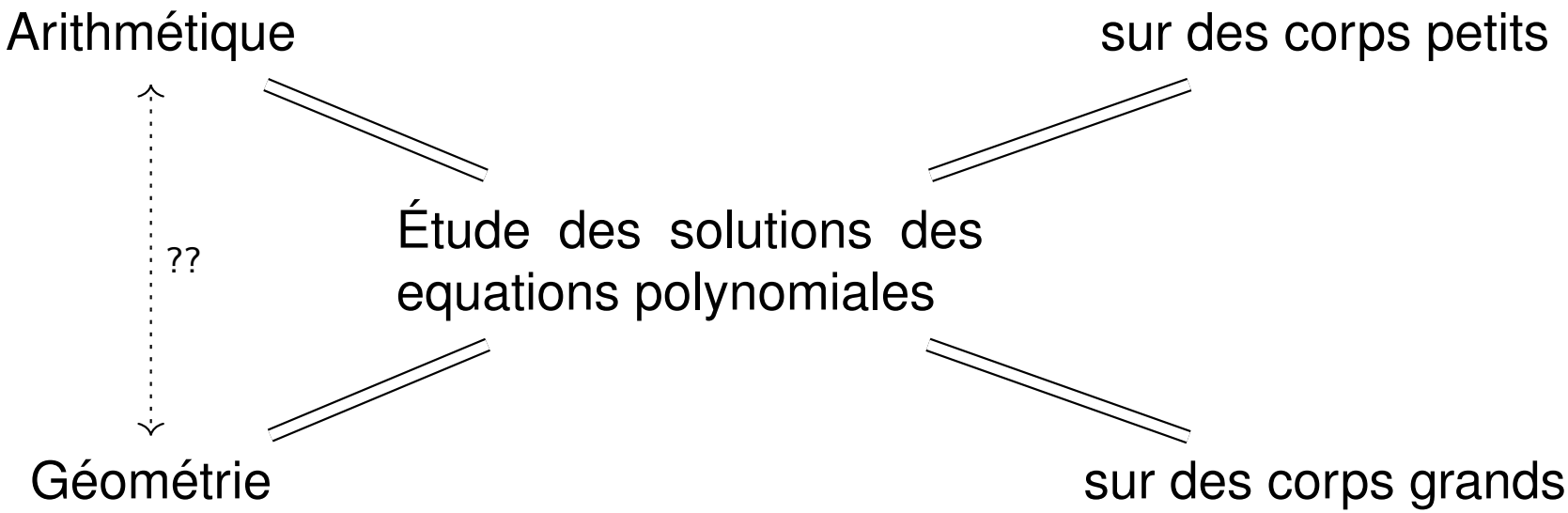
$$\{(x, y) \in \mathbb{Q}^2 : x^n + y^n = 1\}$$



$$\{(x, y) \in \mathbb{C}^2 : x^n + y^n = 1\}$$

Domaine de recherche

$$\{(x, y) \in \mathbb{Q}^2 : x^n + y^n = 1\}$$



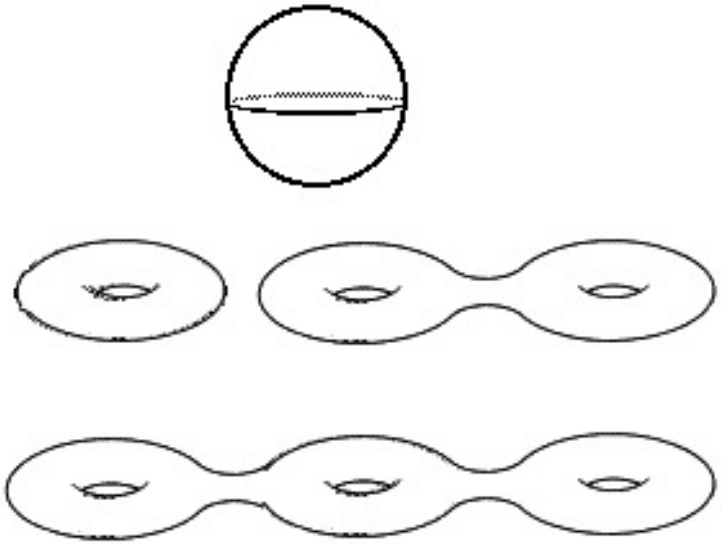
$$\{(x, y) \in \mathbb{C}^2 : x^n + y^n = 1\}$$

$x^n + y^n = 1$

$$X(\mathbb{C}) := \{(x, y) \in \mathbb{C}^2 : x^n + y^n = 1\}$$

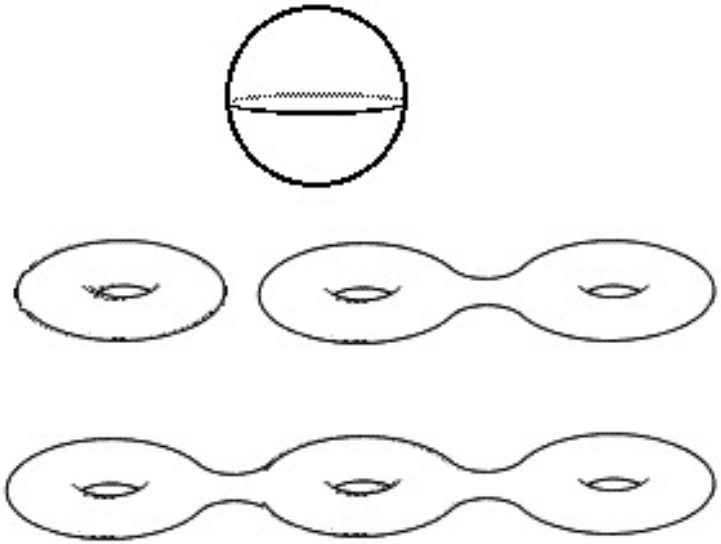
$x^n + y^n = 1$

$$X(\mathbb{C}) := \{(x, y) \in \mathbb{C}^2 : x^n + y^n = 1\}$$



$x^n + y^n = 1$

$$X(\mathbb{C}) := \{(x, y) \in \mathbb{C}^2 : x^n + y^n = 1\}$$

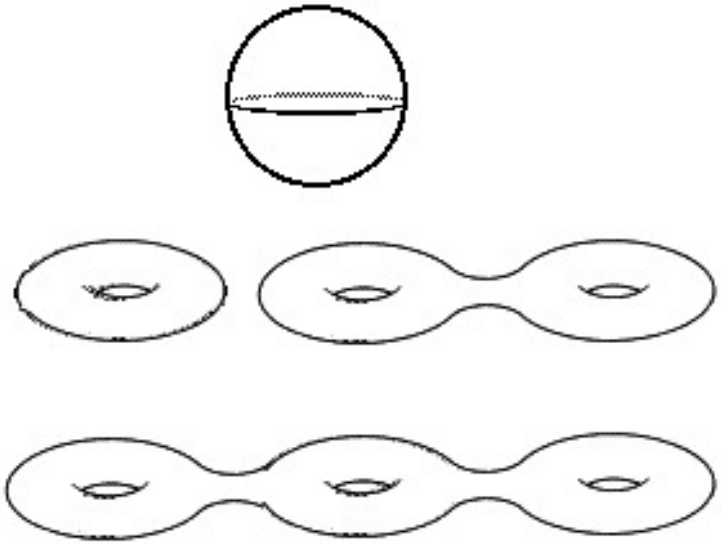


Sur les nombres complexes

- Si $n = 1$ ou 2, $X(\mathbb{C}) \simeq S^2$

$x^n + y^n = 1$

$$X(\mathbb{C}) := \{(x, y) \in \mathbb{C}^2 : x^n + y^n = 1\}$$

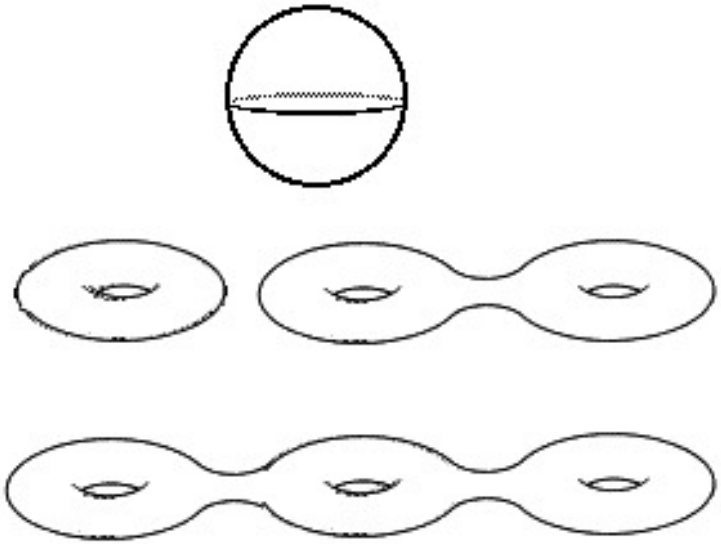


Sur les nombres complexes

- Si $n = 1$ ou 2, $X(\mathbb{C}) \simeq S^2$
- Si $n = 3$, $X(\mathbb{C}) \simeq S^1 \times S^1 \simeq \mathbb{T}$

$x^n + y^n = 1$

$$X(\mathbb{C}) := \{(x, y) \in \mathbb{C}^2 : x^n + y^n = 1\}$$



Sur les nombres complexes

- Si $n = 1$ ou 2, $X(\mathbb{C}) \simeq S^2$
- Si $n = 3$, $X(\mathbb{C}) \simeq S^1 \times S^1 \simeq \mathbb{T}$
- Si $n \geq 4$, $X(\mathbb{C}) \simeq \underbrace{\mathbb{T}\#\mathbb{T}\#\mathbb{T}\ldots\#\mathbb{T}}_{(n-1)(n-2)/2 \text{ fois}}$

Sur les nombres rationnelles

$$X(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : x^n + y^n = 1\}$$

Sur les nombres rationnelles

$$X(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : x^n + y^n = 1\}$$

- Si $n = 1$ ou 2, $X(\mathbb{Q})$ est infini (Triplet pythagoricien, VI siècle av. J.-C.)

Sur les nombres rationnelles

$$X(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : x^n + y^n = 1\}$$

- Si $n = 1$ ou 2, $X(\mathbb{Q})$ est infini (Triplet pythagoricien, VI siècle av. J.-C.)
- Si $n = 3$ ou 4, $X(\mathbb{Q})$ est fini (Fermat, XVII siècle)

Sur les nombres rationnelles

$$X(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : x^n + y^n = 1\}$$

- Si $n = 1$ ou 2, $X(\mathbb{Q})$ est infini (Triplet pythagoricien, VI siècle av. J.-C.)
- Si $n = 3$ ou 4, $X(\mathbb{Q})$ est fini (Fermat, XVII siècle)
- Si $3 \leq n \leq 100$ est fini (Kummer, 1857)

Sur les nombres rationnelles

$$X(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : x^n + y^n = 1\}$$

- Si $n = 1$ ou 2, $X(\mathbb{Q})$ est infini (Triplet pythagoricien, VI siècle av. J.-C.)
- Si $n = 3$ ou 4, $X(\mathbb{Q})$ est fini (Fermat, XVII siècle)
- Si $3 \leq n \leq 100$ est fini (Kummer, 1857)
- Si $n \geq 3$, $X(\mathbb{Q})$ est fini (Faltings '84)

Sur les nombres rationnelles

$$X(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : x^n + y^n = 1\}$$

- Si $n = 1$ ou 2, $X(\mathbb{Q})$ est infini (Triplet pythagoricien, VI siècle av. J.-C.)
- Si $n = 3$ ou 4, $X(\mathbb{Q})$ est fini (Fermat, XVII siècle)
- Si $3 \leq n \leq 100$ est fini (Kummer, 1857)
- Si $n \geq 3$, $X(\mathbb{Q})$ est fini (Faltings '84)
- Calcul exact des solutions (Wiles '94)

Conjecture de Mordell

- $F(x, y) \in \mathbb{Q}[x, y]$

Conjecture de Mordell

- $F(x, y) \in \mathbb{Q}[x, y]$
- $X(\mathbb{Q})$:= solutions de $F(x, y) = 0$ sur $\mathbb{Q}$

Conjecture de Mordell

- $F(x, y) \in \mathbb{Q}[x, y]$
- $X(\mathbb{Q})$:= solutions de $F(x, y) = 0$ sur $\mathbb{Q}$
- $X(\mathbb{C})$:= solutions de $F(x, y) = 0$ sur $\mathbb{C}$

Conjecture de Mordell

- $F(x, y) \in \mathbb{Q}[x, y]$
- $X(\mathbb{Q})$:= solutions de $F(x, y) = 0$ sur $\mathbb{Q}$
- $X(\mathbb{C})$:= solutions de $F(x, y) = 0$ sur $\mathbb{C}$

Théorème (Faltings '84)

Si $X(\mathbb{C}) \simeq \underbrace{\mathbb{T}\#\mathbb{T}\#\mathbb{T}\ldots\#\mathbb{T}}_{\text{n fois}}$ avec $n \geq 2 \Rightarrow X(\mathbb{Q})$ fini

Courbes elliptiques

- $X(\mathbb{C}) \simeq \mathbb{T} \Leftrightarrow F(x,y) = y^2 - axy + by - x^3 - cx^2 + dx + e$

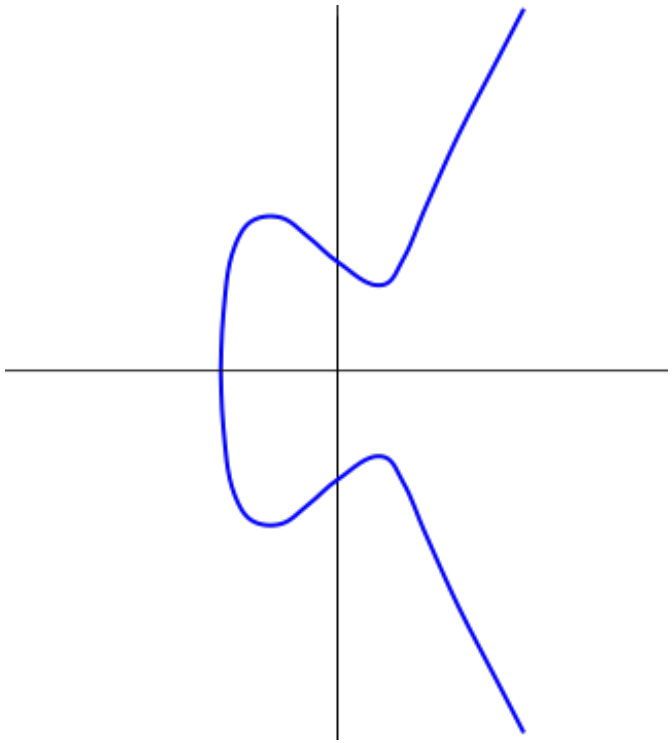
Courbes elliptiques

- $X(\mathbb{C}) \simeq \mathbb{T} \Leftrightarrow F(x,y) = y^2 - axy + by - x^3 - cx^2 + dx + e$
- $X(\mathbb{Q})$ et $X(\mathbb{C})$ sont des groupes abéliens

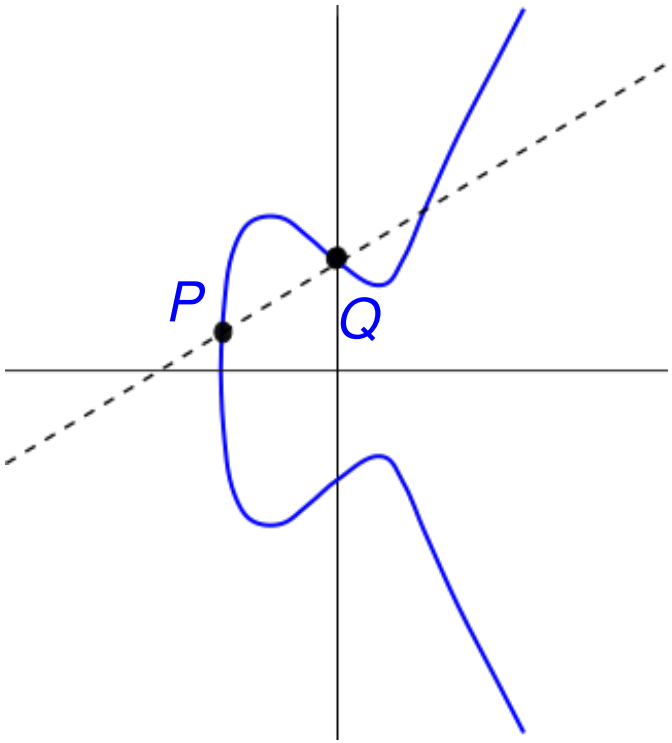
Courbes elliptiques

- $X(\mathbb{C}) \simeq \mathbb{T} \Leftrightarrow F(x,y) = y^2 - axy + by - x^3 - cx^2 + dx + e$
- $X(\mathbb{Q})$ et $X(\mathbb{C})$ sont des groupes abéliens
- $X(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ avec $\Lambda \simeq \mathbb{Z}^2$ réseau dans $\mathbb{C}$

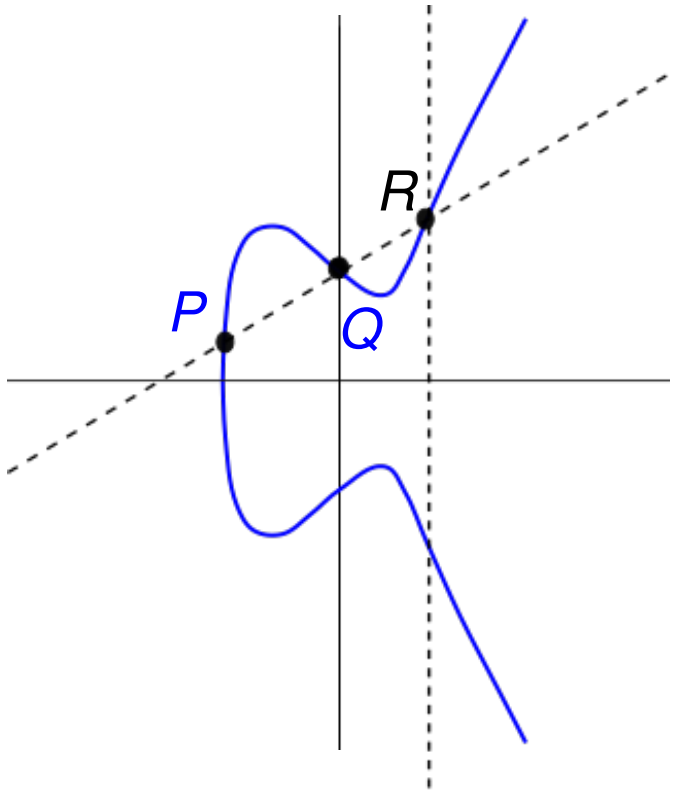
Courbes elliptiques



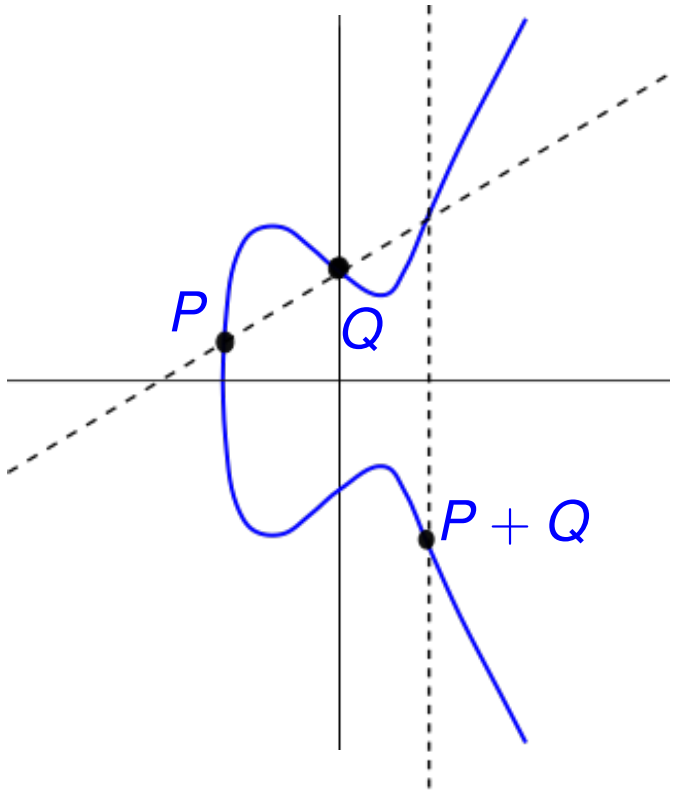
Courbes elliptiques



Courbes elliptiques



Courbes elliptiques



Variétés abéliennes

Définition

Variété abélienne A := solutions des équations algébriques munies d'une loi de groupe abélien

Variétés abéliennes

Définition

Variété abélienne A := solutions des équations algébriques munies d'une loi de groupe abélien

- $A(\mathbb{Q})$ et $A(\mathbb{C})$ sont des groupes abéliens

Variétés abéliennes

Définition

Variété abélienne A := solutions des équations algébriques munies d'une loi de groupe abélien

- $A(\mathbb{Q})$ et $A(\mathbb{C})$ sont des groupes abéliens
- $A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$ avec $\Lambda \simeq \mathbb{Z}^{2g}$ réseau dans $\mathbb{C}^g$

Variétés abéliennes

Définition

Variété abélienne A := solutions des équations algébriques munies d'une loi de groupe abélien

- $A(\mathbb{Q})$ et $A(\mathbb{C})$ sont des groupes abéliens
- $A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$ avec $\Lambda \simeq \mathbb{Z}^{2g}$ réseau dans $\mathbb{C}^g$
- $A(\mathbb{Q})$ peut être infini

Variétés abéliennes

Définition

Variété abélienne A := solutions des équations algébriques munies d'une loi de groupe abélien

- $A(\mathbb{Q})$ et $A(\mathbb{C})$ sont des groupes abéliens
- $A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$ avec $\Lambda \simeq \mathbb{Z}^{2g}$ réseau dans $\mathbb{C}^g$
- $A(\mathbb{Q})$ peut être infini

Théorème (Mordell-Weil '29)

$A(\mathbb{Q})$ est un groupe abélien de type fini

Corps bizarres

- $\mathbb{F}_p(T) :=$ corps des fractions des polynômes à coefficients dans le corps fini $\mathbb{F}_p$ avec p éléments

Corps bizarres

- $\mathbb{F}_p(T) :=$ corps des fractions des polynômes à coefficients dans le corps fini $\mathbb{F}_p$ avec p éléments
- Exemple: $\frac{T^p-4}{2T+2}$

Corps bizarres

- $\mathbb{F}_p(T) :=$ corps des fractions des polynômes à coefficients dans le corps fini $\mathbb{F}_p$ avec p éléments
- Exemple: $\frac{T^p-4}{2T+2}$
- Pathologie: $\frac{\partial T^p}{\partial T} = pT^{p-1} = 0$

Corps bizarres

- $\mathbb{F}_p(T) :=$ corps des fractions des polynômes à coefficients dans le corps fini $\mathbb{F}_p$ avec p éléments
- Exemple: $\frac{T^p-4}{2T+2}$
- Pathologie: $\frac{\partial T^p}{\partial T} = pT^{p-1} = 0$
- A variété abélienne sur $\mathbb{F}_p(T)$

Corps bizarres

- $\mathbb{F}_p(T) :=$ corps des fractions des polynômes à coefficients dans le corps fini $\mathbb{F}_p$ avec p éléments
- Exemple: $\frac{T^p-4}{2T+2}$
- Pathologie: $\frac{\partial T^p}{\partial T} = pT^{p-1} = 0$
- A variété abélienne sur $\mathbb{F}_p(T)$

Théorème (Lang-Néron '59)

$A(\mathbb{F}_p(T))$ est un groupe abélien de type fini

Corps encore plus bizarres

- Fr: $\mathbb{F}_p(T) \to \mathbb{F}_p(T)$ morphisme de Frobenius: $\mathrm{Fr}(a) := a^p$

Corps encore plus bizarres

- Fr: $\mathbb{F}_p(T) \to \mathbb{F}_p(T)$ morphisme de Frobenius: $\mathrm{Fr}(a) := a^p$
- $(a+b)^p = a^p + b^p$ (petit théorème de Fermat)

Corps encore plus bizarres

- Fr: $\mathbb{F}_p(T) \to \mathbb{F}_p(T)$ morphisme de Frobenius: $\mathrm{Fr}(a) := a^p$
- $(a+b)^p = a^p + b^p$ (petit théorème de Fermat)
- Fr: $\mathbb{F}_p(T) \to \mathbb{F}_p(T)$ est un morphisme de corps (donc injectif)

Corps encore plus bizarres

- Fr: $\mathbb{F}_p(T) \to \mathbb{F}_p(T)$ morphisme de Frobenius: $\mathrm{Fr}(a) := a^p$
- $(a+b)^p = a^p + b^p$ (petit théorème de Fermat)
- Fr: $\mathbb{F}_p(T) \to \mathbb{F}_p(T)$ est un morphisme de corps (donc injectif)
- Mais Fr: $\mathbb{F}_p(T) \to \mathbb{F}_p(T)$ n'est pas surjectif ($\sqrt[p]{T} \notin \mathbb{F}_p(T)$)

Corps encore plus bizarres

- Fr: $\mathbb{F}_p(T) \to \mathbb{F}_p(T)$ morphisme de Frobenius: $\mathrm{Fr}(a) := a^p$
- $(a+b)^p = a^p + b^p$ (petit théorème de Fermat)
- Fr: $\mathbb{F}_p(T) \to \mathbb{F}_p(T)$ est un morphisme de corps (donc injectif)
- Mais Fr: $\mathbb{F}_p(T) \to \mathbb{F}_p(T)$ n'est pas surjectif ($\sqrt[p]{T} \notin \mathbb{F}_p(T)$)
- Clôture parfaite: $\mathbb{F}_p(T)^{\mathrm{perf}} := \mathbb{F}_p(T, \sqrt[p]{T}, \sqrt[p^2]{T}, \dots)$

Corps encore plus bizarres

- Fr: $\mathbb{F}_p(T) \to \mathbb{F}_p(T)$ morphisme de Frobenius: $\mathrm{Fr}(a) := a^p$
- $(a+b)^p = a^p + b^p$ (petit théorème de Fermat)
- Fr: $\mathbb{F}_p(T) \to \mathbb{F}_p(T)$ est un morphisme de corps (donc injectif)
- Mais Fr: $\mathbb{F}_p(T) \to \mathbb{F}_p(T)$ n'est pas surjectif ($\sqrt[p]{T} \notin \mathbb{F}_p(T)$)
- Clôture parfaite: $\mathbb{F}_p(T)^{\mathrm{perf}} := \mathbb{F}_p(T, \sqrt[p]{T}, \sqrt[p^2]{T}, \dots)$

Théorème (A.)

Si toutes les symétries de A sont triviales alors $A(\mathbb{F}_p(T)^{\mathrm{perf}})$ est un groupe abélien de type fini