Arithmétique, géométrie et indécidabilité

Laurent Moret-Bailly

IRMAR, Université de Rennes 1

Séminaire Réga, Paris, 15 mai 2013

Sommaire

Décidabilité existentielle (ou « diophantienne »)

Soient $A_0 \subset A$ deux anneaux.

On dit que A est (existentiellement) décidable relativement à A_0 (en abrégé Dec (A, A_0))
s'il existe un algorithme calculant la fonction suivante :

ENTRÉE :

une famille finie de polynômes $F_i \in A_0[X_1, \ldots, X_n] \quad (i = 1, \ldots, s)$

SORTIE :

$$\begin{cases} \text{VRAI} & \text{si le système } F_i(x_1, \ldots, x_n) = 0 \quad (i = 1, \ldots, s) \\ & \quad \text{a une solution dans } A^n, \\ \text{FAUX} & \text{sinon.} \end{cases}$$

(Dans la suite, on omettra parfois « existentiellement ».)

Le dixième problème de Hilbert

« Montrer que $\mathbb{Z}$ est existentiellement décidable »

« On donne une équation diophantienne à un nombre quelconque d'inconnues et à coefficients entiers rationnels : on demande de trouver une méthode par laquelle, au moyen d'un nombre fini d'opérations, on pourra distinguer si l'équation est résoluble en nombres entiers rationnels. »

(D. Hilbert, congrès international de Paris, 1900)

Le théorème de Matiyasevich

Un tel algorithme n'existe pas !

(Yu. Matiyasevich (1970), à la suite de travaux de M. Davis, H. Putnam et J. Robinson).

Julia Robinson et Yuri Matiyasevich (1971 ?)

Commentaires

Hilbert pensait probablement que $\mathbb{Z}$ était existentiellement décidable. Ceci aurait immédiatement entraîné la même propriété :

- pour $\mathbb{Q}$: $F(x_1, \ldots, x_n)$ a un zéro dans $\mathbb{Q}^n$ si et seulement si

$$\widetilde{F}(t, y_1, \ldots, y_n) := t^{\deg F} F(\frac{y_1}{t}, \ldots, \frac{y_n}{t})$$

  a un zéro $(t, \underline{y})$ dans $\mathbb{Z}^{n+1}$ avec $t > 0$, c'est-à-dire de la forme $1 + a^2 + b^2 + c^2 + d^2$ $(a, b, c, d \in \mathbb{Z})$;
- pour tout corps de nombres (utiliser une $\mathbb{Q}$-base) ;
- pour tout anneau A qui est un $\mathbb{Z}$-module libre de rang fini (utiliser une $\mathbb{Z}$-base), par exemple l'anneau des entiers d'un corps de nombres.

L'indécidabilité existentielle de $\mathbb{Q}$ et des corps de nombres est une question ouverte, ainsi que celle des anneaux d'entiers algébriques, à part certains cas particuliers (entiers des corps quadratiques).

Exemples :

A_0	A	**Décidabilité diophantienne**	
$\mathbb{Q}$	$\mathbb{C}$	oui	th. des zéros de Hilbert
$\mathbb{Q}$	$\mathbb{R}$	oui	Tarski (1951)
$\mathbb{Q}$	$\mathbb{Q}_p$	oui	Nerode (1963)
	$\mathbb{F}_p((t))$	?	
$\mathbb{Z}$	$\mathbb{Z}$	non	Matyasevich (1970)
$\mathbb{Q}$ (ou $\mathbb{Z}$)	$\mathbb{Q}$	?	
$\mathbb{Q}(t)$	$k(t)$ (k réel)	non	J. Denef (1978)
	$k(t)$ (k p-adique)	non	Kim et Roush (1995)
$\overline{\mathbb{Q}}(t)$	$\mathbb{C}(t)$	?	
	$\mathbb{C}(t_1, t_2)$	non	Kim et Roush (1992)

Parenthèse : indécidabilité au premier ordre

En dehors de cet exposé, « décidable » signifie en général « décidable au premier ordre ».
Dans le cas des anneaux :
A est décidable au premier ordre relativement à A_0 s'il existe un algorithme calculant la fonction suivante :

ENTRÉE :

une formule φ du langage des anneaux,
sans variable libre, avec constantes dans A_0

SORTIE :

$$\begin{cases} \text{VRAI} & \text{si } \varphi \text{ est vraie dans } A \\ \text{FAUX} & \text{sinon.} \end{cases}$$

Parenthèse : indécidabilité au premier ordre

Une « formule φ du langage des anneaux, sans variable libre, avec constantes dans A_0 » s'écrit avec :

- l'attirail logique habituel : variables, parenthèses, symboles logiques $\vee$, $\wedge$, $\neg$, $\to$, $\exists$, $\forall$;
- les opérations : $+$ et $\times$;
- les constantes : 0, 1, éléments de A_0.

Important : les variables parcourent A : « $\forall x$ » signifie toujours « $\forall x \in A$ » (interdiction de quantifier sur les parties de A, les polynômes,...).

On retrouve la décidabilité existentielle en interdisant $\forall$ et $\neg$.

Parenthèse : indécidabilité au premier ordre

Exemples : pour les formules du premier ordre,

- $\mathbb{Z}$ est indécidable (Gödel, 1931) ;
- $\mathbb{Q}$ est indécidable (J. Robinson, 1949) ;
- $\mathbb{R}$ est décidable (Tarski, 1951) ;
- $\mathbb{Q}_p$ est décidable (Eršov, 1965 ; Ax et Kochen, 1966) ;
- pour $\mathbb{C}(t)$, on ne sait pas.

Ensembles diophantiens : définition

Soient $A_0 \subset A$ deux anneaux.

Un sous-ensemble V de A^n est dit :

- A_0-algébrique élémentaire s'il est défini par un système (fini) d'équations polynômes à coefficients dans A_0 ;
- A_0-algébrique s'il est réunion finie d'ensembles algébriques élémentaires ;
- A_0-diophantien (ou *existentiellement définissable*) s'il est l'image d'un sous-ensemble A_0-algébrique de A^{m+n} par l'une des projections évidentes $A^{n+m} \to A^n$.

Remarques

- Si A est intègre, les ensembles algébriques sont algébriques élémentaires. Un ensemble diophantien est alors de la forme

$$V = \{\underline{x} \in A^n \mid \exists \underline{z} \in A^m,\ F_1(\underline{x}, \underline{z}) = \cdots = F_r(\underline{x}, \underline{z}) = 0\}$$

  pour $F_1, \ldots, F_r \in A_0[\underline{X}, \underline{Z}]$ convenables.

- La classe des ensembles diophantiens est stable par :
  - réunions et intersections finies ;
  - produits finis ;
  - images et images réciproques par des applications $A^m \to A^n$, polynomiales à coefficients dans A_0.

Exemples (avec $n = 1$) :

1. $\mathbb{R}_+$ est-il diophantien dans $\mathbb{R}$?

   Oui : c'est l'ensemble des carrés.
2. $\mathbb{N}$ est-il diophantien dans $\mathbb{Z}$?

   Oui : c'est l'ensemble des sommes de 4 carrés.
3. $\mathbb{Z} \smallsetminus \{0\}$ est-il diophantien dans $\mathbb{Z}$?

   Oui : $n \neq 0 \iff (\exists u)(\exists v)\ n^2 = (2u+1)(3v+1)$.
4. $\mathbb{Z}_p \smallsetminus \{0\}$ est-il diophantien dans $\mathbb{Z}_p$?

   Non : sur $\mathbb{Z}_p$, les ensembles diophantiens sont compacts.
5. $\mathbb{Z}$ est-il diophantien dans $\mathbb{R}$?

   Non : les ensembles diophantiens réels n'ont qu'un nombre fini de composantes connexes.
6. $\mathbb{Z}$ est-il diophantien dans $\mathbb{Q}$?

   On ne sait pas ! (non, d'après une conjecture de Mazur).

Un exemple instructif (et utilisé plus tard)

Proposition

Posons $K = \mathbb{R}(t)$, $\mathscr{O} := \mathbb{R}[t]_{(t)} \subset K$ (l'anneau local de l'origine dans $\mathbb{P}^1_{\mathbb{R}}$), $\mathscr{M} := \{f \in K \mid f(0) = 0\}$ (idéal maximal de $\mathscr{O}$).

1. *La relation $f \geq 0$ est diophantienne dans K.*
2. *$\mathbb{R}$ est diophantien dans K.*
3. *$\mathscr{M}$ et $\mathscr{O}$ sont diophantiens dans K.*

Démonstration :

(1) en effet on a dans $\mathbb{R}(t)$ (exercice)

$$f \geq 0 \iff f \text{ est somme de deux carrés.}$$

Un exemple instructif

Proposition

Posons $K = \mathbb{R}(t)$, $\mathscr{O} := \mathbb{R}[t]_{(t)} \subset K$ *(l'anneau local de l'origine dans* $\mathbb{P}^1_{\mathbb{R}}$*),* $\mathscr{M} := \{f \in K \mid f(0) = 0\}$ *(idéal maximal de* $\mathscr{O}$*).*

1. *La relation* $f \geq 0$ *est diophantienne dans* K*.*
2. $\mathbb{R}$ *est diophantien dans* K*.*
3. $\mathscr{M}$ *et* $\mathscr{O}$ *sont diophantiens dans* K*.*

(2) Si $g \in \mathbb{R}(t)$, alors :

$$g \text{ est constante } \iff (\exists h \in \mathbb{R}(t)) \left(g^2 = h^3 + 1\right) :$$

- si g est constante, prendre $h = \sqrt[3]{g^2 - 1}$;
- si $g^2 = h^3 + 1$, alors (h, g) est un $\mathbb{R}(t)$-point de la courbe elliptique réelle $E : y^2 = x^3 + 1$, donc une application rationnelle $\mathbb{P}^1_{\mathbb{R}} \cdots \to E$, nécessairement constante.

Un exemple instructif

Proposition

Posons $K = \mathbb{R}(t)$, $\mathscr{O} := \mathbb{R}[t]_{(t)} \subset K$ *(l'anneau local de l'origine dans* $\mathbb{P}^1_{\mathbb{R}}$*),* $\mathscr{M} := \{f \in K \mid f(0) = 0\}$ *(idéal maximal de* $\mathscr{O}$*).*

1. *La relation* $f \geq 0$ *est diophantienne dans* K*.*
2. $\mathbb{R}$ *est diophantien dans* K*.*
3. $\mathscr{M}$ *et* $\mathscr{O}$ *sont diophantiens dans* K*.*

Conséquence de (1) et (2) : la relation « f est minorée » (comme fonction sur $\mathbb{R}$) est diophantienne.
(3) Pour $f \in \mathbb{R}(t)$, on a l'équivalence (exercice) :

$$f(0) = 0 \iff f = 0, \text{ ou } \frac{1}{f^2} + \frac{1}{t} \text{ est minorée.}$$

Donc $\mathscr{M}$ est diophantien, et $\mathscr{O} = t^{-1}\mathscr{M}$ aussi. □

Ensembles diophantiens et décidabilité

Proposition

Soient $A_0 \subset A \subset B$ trois anneaux.

Hypothèses :

- $\mathrm{Dec}(B, A_0)$;
- *A est diophantien dans B (relativement à A_0).*

Alors on a $\mathrm{Dec}(A, A_0)$.

(Démonstration immédiate)

D'où l'intérêt des questions suivantes :

- si A est l'anneau des entiers d'un corps de nombres, est-ce que $\mathbb{Z}$ est diophantien dans A ? (Si oui, on a $\neg\,\mathrm{Dec}(A, \mathbb{Z})$).
- Est-ce que $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$? (Si oui, on a $\neg\,\mathrm{Dec}(\mathbb{Q}, \mathbb{Z})$).

La conjecture de Mazur

Conjecture (B. Mazur)

Soit V une variété quasi-projective sur $\mathbb{Q}$. Alors l'adhérence de $V(\mathbb{Q})$ dans $V(\mathbb{R})$ n'a qu'un nombre fini de composantes connexes.

Cette conjecture impliquerait que $\mathbb{Z}$ n'est pas diophantien dans $\mathbb{Q}$.

Variante : modèles diophantiens

Un modèle diophantien de $\mathbb{Z}$ sur A (relativement à $A_0 \subset A$) est une injection

$$\varphi : \mathbb{Z} \hookrightarrow A^n$$

avec les propriétés suivantes :

1. l'image D de φ est A_0-diophantienne dans A^n ;
2. la structure d'anneau sur D déduite de φ est diophantienne.

Proposition

S'il existe un tel modèle, A est existentiellement indécidable relativement à A_0.

Exemples

Corps de fractions rationnelles (J. Denef, H.K. Kim, F.W. Roush) : soient k un corps de caractéristique nulle, et $K = k(t)$. Alors il existe un modèle diophantien de $\mathbb{Z}$ sur K dans les cas suivants :

- k est réel (Denef) ;
- k est un sous-corps d'un corps p-adique, avec $p \neq 2$ (Kim-Roush) ;
- $k = \mathbb{C}(z)$ (Kim-Roush).

La méthode sera expliquée dans la suite.

Sous-anneaux de $\mathbb{Q}$ (Poonen, 2003) : il existe un ensemble S de nombres premiers, de densité 1, tel que $\mathbb{Z}$ ait un modèle diophantien sur $\mathbb{Z}[S^{-1}]$.

Théorème (Cornelissen-Zahidi, 1999)

L'existence d'un modèle diophantien de $\mathbb{Z}$ sur $\mathbb{Q}$ contredirait la conjecture de Mazur.

Une stratégie

Soit K un corps, dont on veut montrer l'indécidabilité existentielle. On construit un modèle diophantien de $\mathbb{Z}$ sur K comme suit :

1. on trouve une K-courbe elliptique E telle que $E(K) \cong \mathbb{Z}$ (comme groupe).
   Possible sur certains corps ; nous aurons plutôt un certain sous-groupe diophantien $\Delta \subset E(K)$, d'indice fini et $\cong \mathbb{Z}$.
2. Fixant un isomorphisme $E(K) \cong \mathbb{Z}$, on obtient une multiplication (saugrenue) sur $E(K)$.
3. On montre que cette multiplication est diophantienne.
   C'est l'étape difficile.
4. Comme l'addition l'est automatiquement, on a bien un modèle diophantien de $\mathbb{Z}$.

Dans toute la suite on prend

$$K = k(t)$$

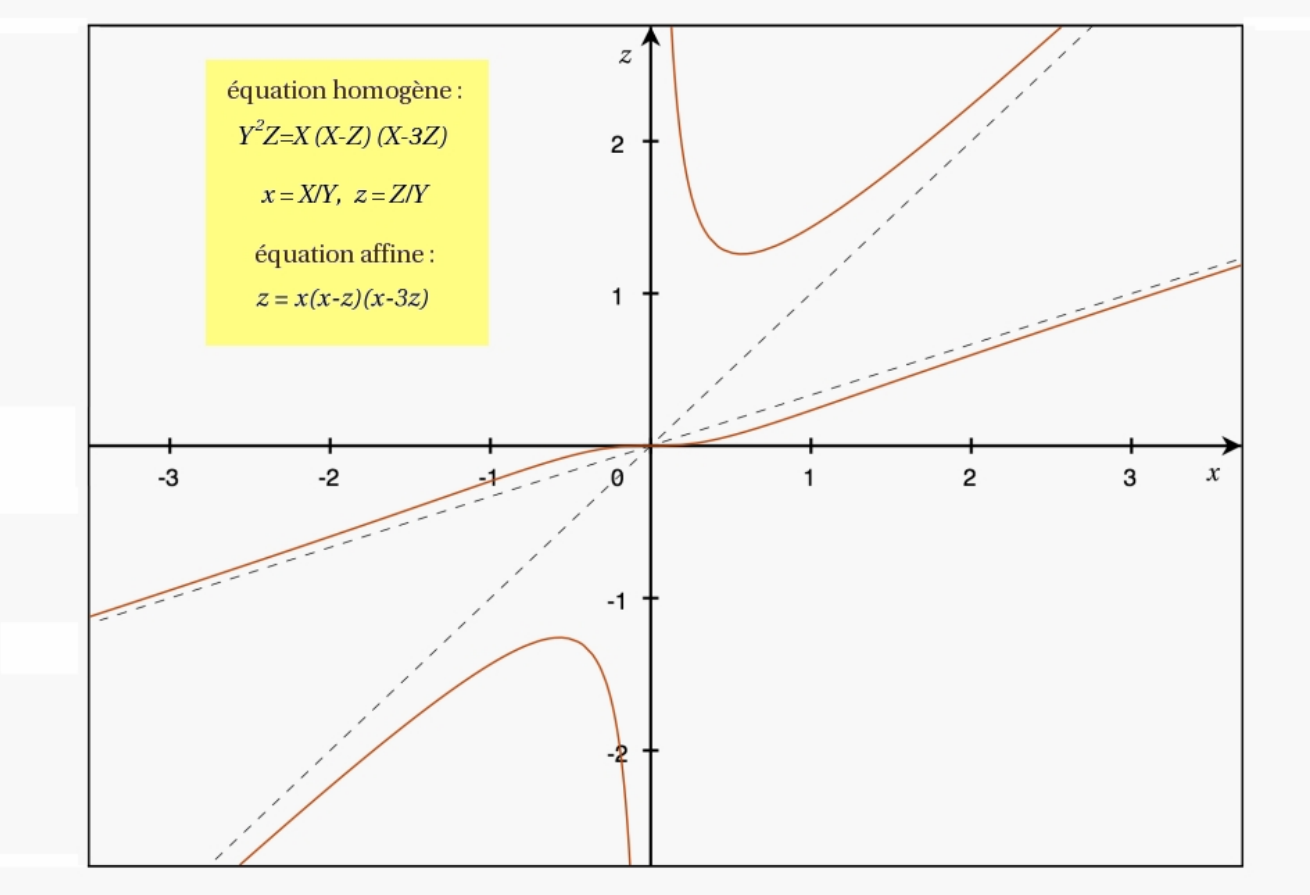
où k est un corps de caractéristique nulle.

On verra K comme le corps des fonctions de $\mathbb{P}^1_k$.

On fixe une courbe elliptique E, d'équation affine (centrée à l'origine de la courbe)

$$E : \qquad z = x^3 + a\,x^2\,z + b\,x\,z^2 + c\,z^3 =: F(x,z),$$

avec a, b, c dans $\mathbb{Q}$. On suppose E sans multiplication complexe (pour plus tard).



Torsion quadratique

Soit $\widetilde{K} = K(\sqrt{D})$ une extension quadratique de K. Elle correspond à un revêtement double

$$\pi : \Gamma \to \mathbb{P}^1_k$$

où Γ est la k-courbe projective lisse de corps de fonctions $\widetilde{K}$.

La tordue de E (ou plutôt de E_K) par $\widetilde{K}/K$ est la courbe elliptique $\mathscr{E}$ sur K d'équation affine

$$\mathscr{E} : \quad D z = F(x, z).$$

Noter que l'on peut voir $\mathscr{E}$:

- soit comme une courbe sur K (géométrie sur le corps K),
- soit comme une surface elliptique sur k (géométrie sur le corps k).

Propriétés de la tordue :

1. $\mathscr{E}$ a mauvaise réduction additive aux points de ramification de $\pi : \Gamma \to \mathbb{P}^1$;
2. on « connaît » le groupe de Mordell-Weil de $\mathscr{E}$, en termes de géométrie sur k :

$$\begin{aligned} \mathscr{E}(K) &\cong \mathrm{Mor}_k^{\mathrm{odd}}(\Gamma, E) \\ &= \{k\text{-morphismes } \Gamma \to E \\ &\quad \text{commutant aux involutions naturelles}\}. \end{aligned}$$

La tordue de Manin-Denef

$$E : \qquad z = x^3 + a\,x^2\,z + b\,x\,z^2 + c\,z^3 =: F(x,z),$$

On prend pour $\pi : \Gamma \to \mathbb{P}^1_k$ le revêtement double standard $E \to \mathbb{P}^1_k$, normalisé pour envoyer l'origine $(0,0)$ de E sur $0 \in \mathbb{P}^1(k)$; explicitement :

- π est la fonction rationnelle z/x sur E ;
- l'extension quadratique $\widetilde{K}$ est $K\left(\sqrt{\frac{F(1,t)}{t}}\right)$ (ici $\sqrt{\frac{F(1,t)}{t}}$ correspond à la fonction $\frac{1}{x}$) ;
- l'équation affine de $\mathscr{E}$ peut donc s'écrire

$$\mathscr{E} : \qquad z = \frac{t}{F(1,t)}\,F(x,z).$$

La tordue de Manin-Denef

$$\mathscr{E} : \qquad z = \frac{t}{F(1,t)}\,F(x,z)$$

On voit que $\mathscr{E}$ est définie sur $\mathbb{Q}(t)$, et l'on trouve immédiatement

$$\mathscr{E}(K) \cong \mathrm{End}_k(E) \times E[2](k) \cong \mathbb{Z} \times E[2](k)$$

pour E sans multiplication complexe (en particulier, le point $\gamma := (1,t)$ correspond à $(\mathrm{Id}_E, 0)$).

Le sous-groupe $\Delta := \mathbb{Z}\gamma$ de $\mathscr{E}(K)$ est égal à $2\mathscr{E}(K) \cup (\gamma + 2\mathscr{E}(K))$ et en particulier diophantien : ce sera notre modèle de $\mathbb{Z}$.

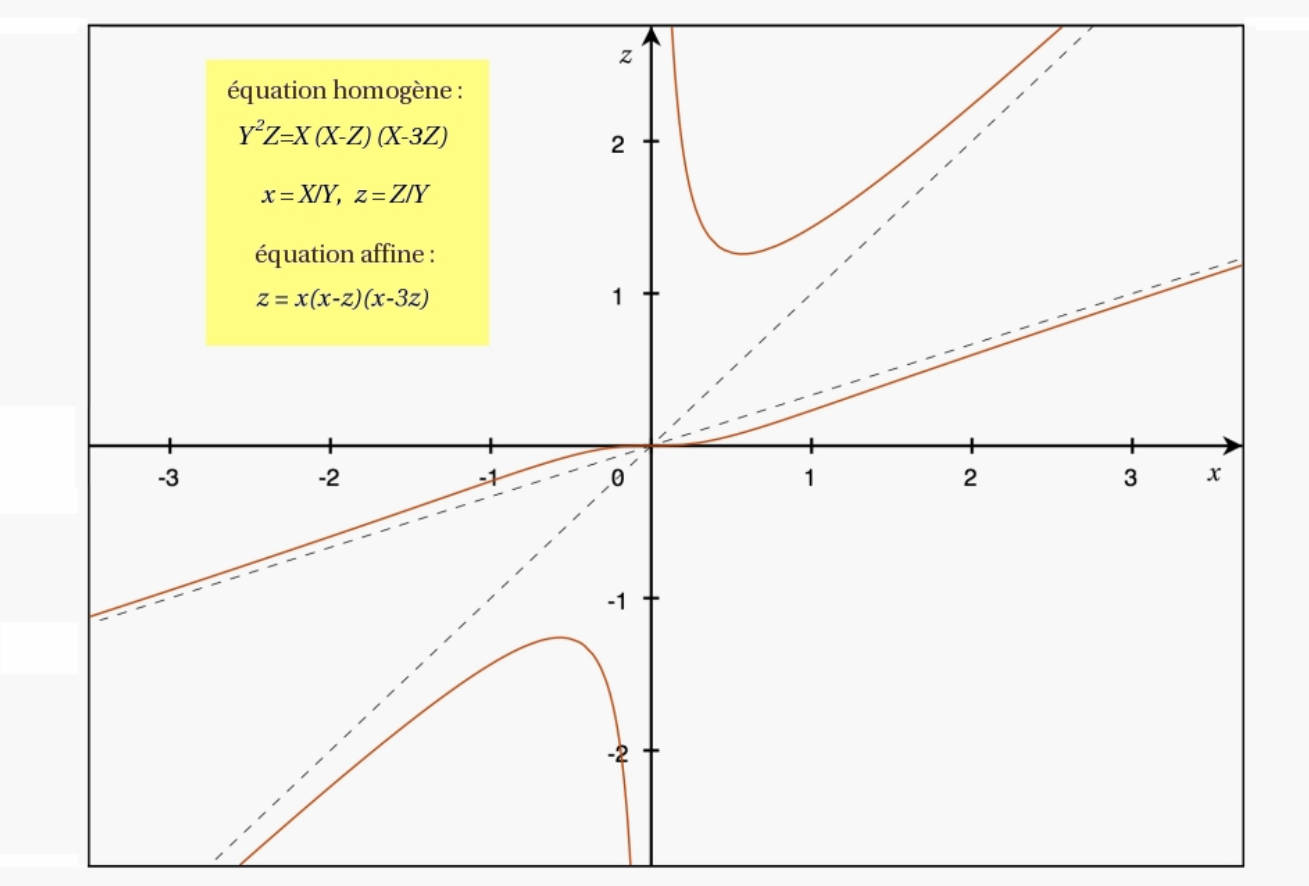
Quelques figures pour faire joli...

On prend $k = \mathbb{R}$, et

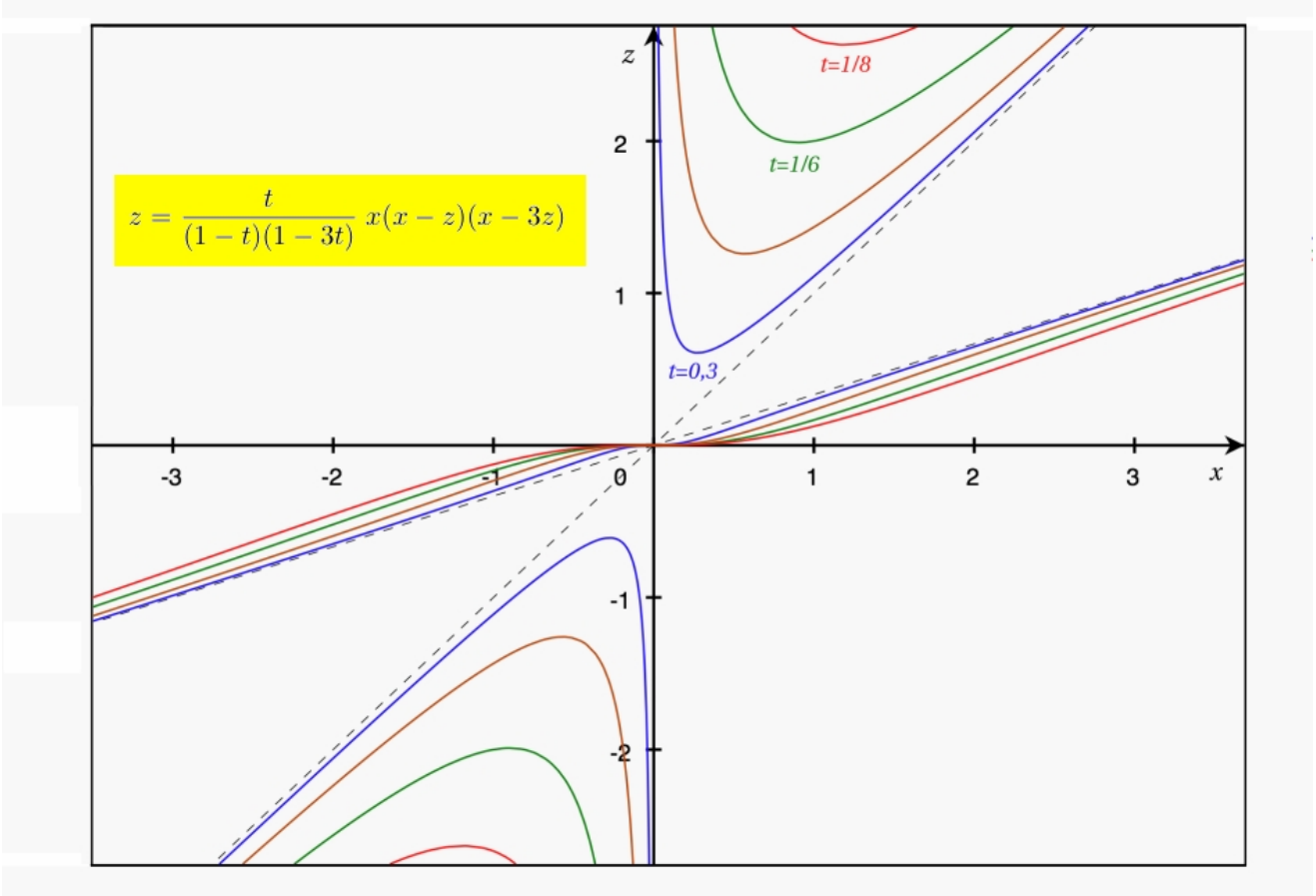
$$E : \quad z = x(x-z)(x-3z)$$

$$\mathscr{E}_t : \quad z = \frac{t}{(1-t)(1-3t)}\, x(x-z)(x-3z).$$

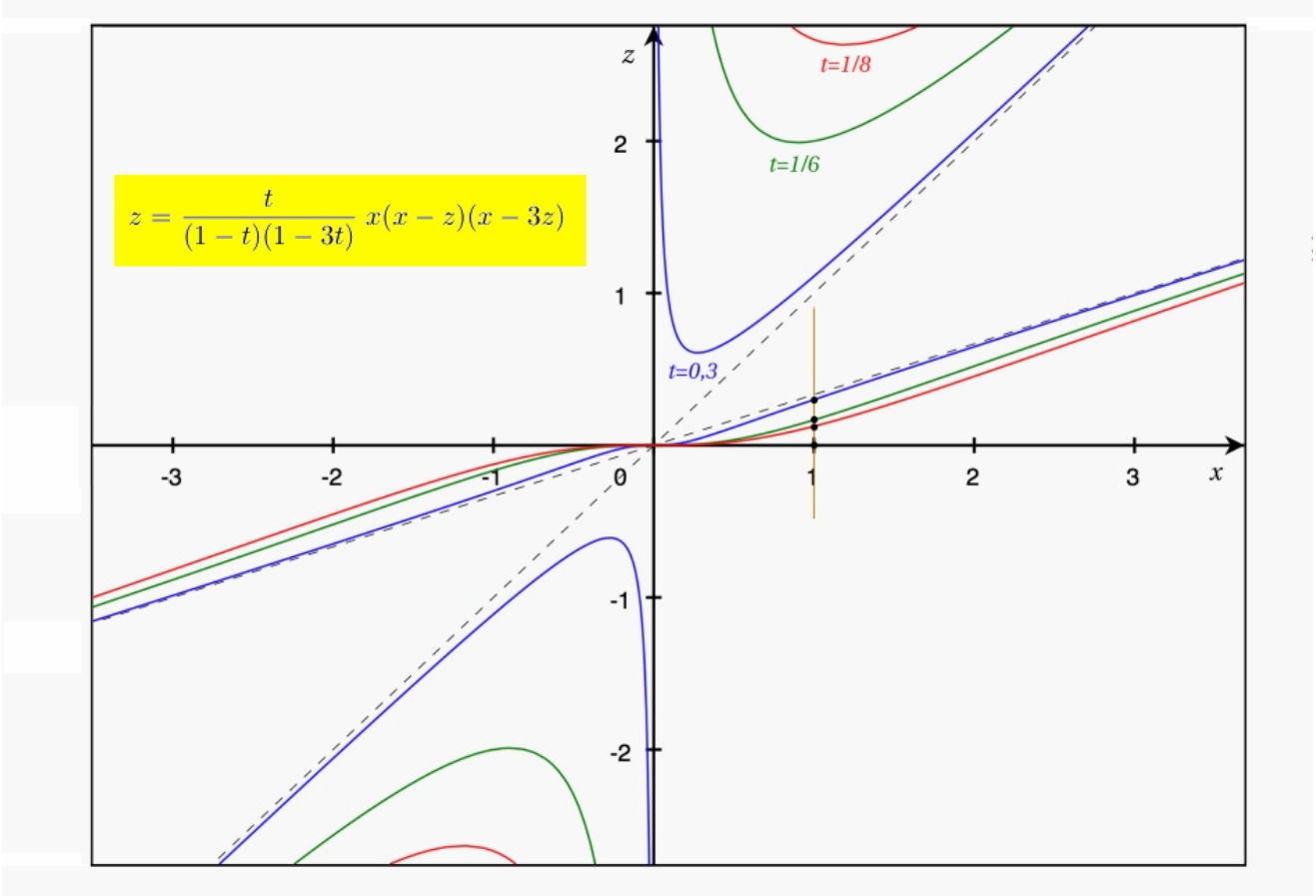
La courbe E



E et $\mathscr{E}_t$ pour trois valeurs de t



$\mathscr{E}_t$ et le point $\gamma = (1, t)$

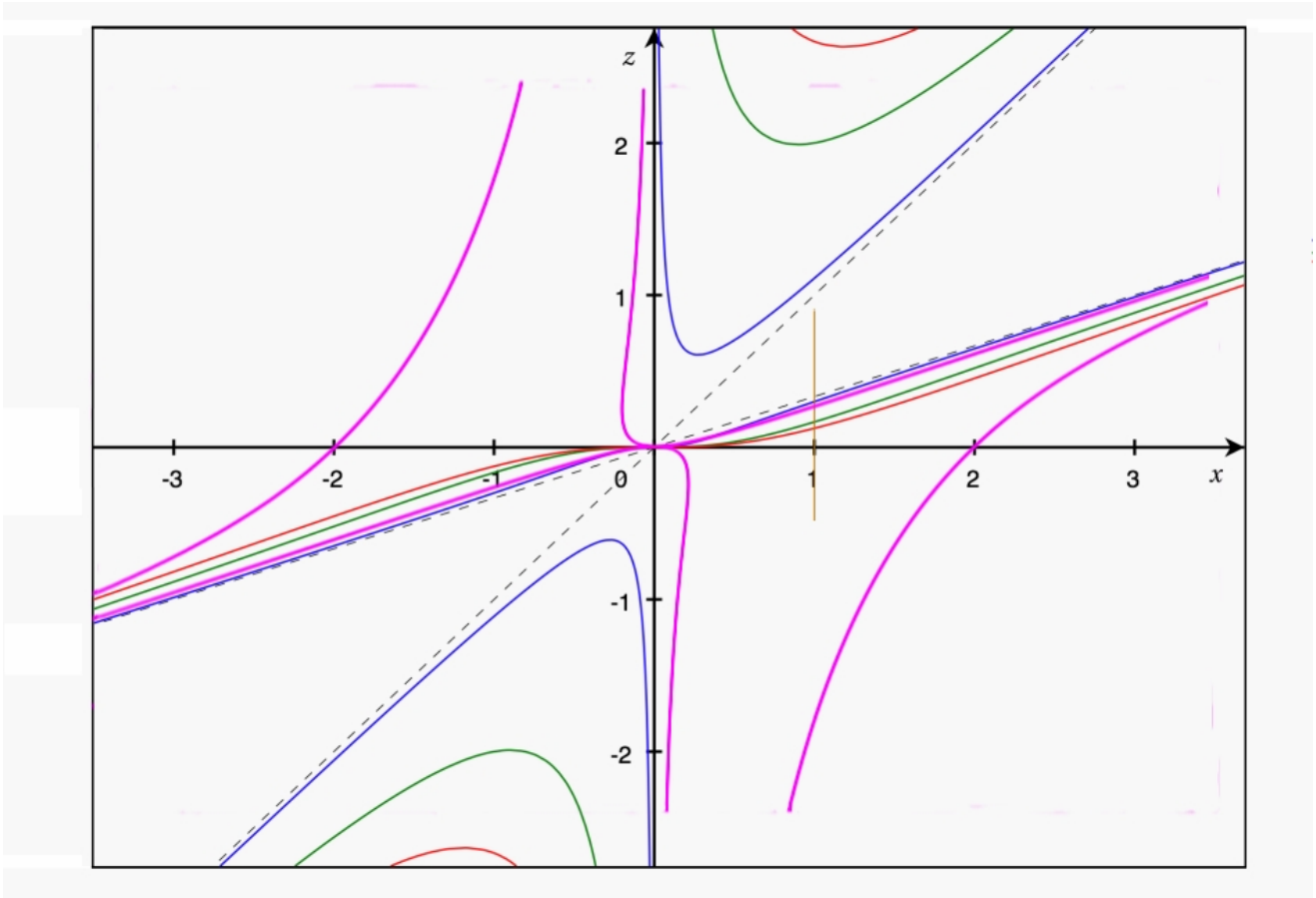


Dans la figure suivante, la courbe violette est le lieu de $2\gamma(t)$ (le double de $\gamma = (1, t)$ pour la loi de groupe de $\mathscr{E}$) :

$$2\gamma(t) \quad \begin{cases} x = -2\,\dfrac{(t-1)(3t-1)(3t^2-1)}{(3t^2-6t+1)(3t^2-2t+1)} \\ \\ z = -8\,t\,\dfrac{(t-1)^2\,(3t-1)^2}{(3t^2-1)(3t^2-6t+1)(3t^2-2t+1)} \end{cases}$$

Équation cartésienne :

$$\begin{aligned} x^6 - 8x^5z + 22x^4z^2 - 24x^3z^3 + 9x^2z^4 \\ -4x^4 + 24x^3z - 44x^2z^2 + 24xz^3 + 4z^2 \quad = \quad 0 \end{aligned}$$



Spécialisation

La courbe $\mathscr{E}$ a mauvaise réduction additive en $t = 0$

d'où un homomorphisme de spécialisation

$$\mathbb{Z} \cong \Delta \xrightarrow{\text{sp}} (k, +).$$

Avec les équations données, on a

$$\begin{aligned} \text{sp}(x(t), z(t)) &= x(0) \\ \text{sp}(n.\gamma) &= n \quad (n \in \mathbb{Z}) \end{aligned}$$

En particulier, on peut calculer la multiplication $*$ sur Δ comme suit :

étant donnés $A = a.\gamma = (x_A, z_A)$ et $B = b.\gamma = (x_B, z_B)$, le point $A * B = ab.\gamma$ est l'unique point $M = (x_M, z_M)$ vérifiant :

- $M \in \Delta$;
- $x_M(0) = x_A(0)\, x_B(0)$.

- $M \in \Delta$;
- $x_M(0) = x_A(0)\, x_B(0)$.

La première condition est bien diophantienne.

Si l'on note $\mathscr{M} \subset K$ l'idéal maximal de l'origine dans $\mathbb{P}^1_k$ (autrement dit, $\mathscr{M} = t\, k[t]_{(t)}$), la deuxième condition s'écrit

$$x_M - x_A\, x_B \in \mathscr{M}$$

qui est aussi diophantienne si $\mathscr{M}$ est diophantien dans K.

On a donc montré :

Théorème

Si $\mathscr{M}$ est diophantien dans $k(t)$, alors $k(t)$ est existentiellement indécidable.

Corollaire

$\mathbb{R}(t)$ est existentiellement indécidable.

Grâce au fait que $\mathbb{R}$ est diophantien dans $\mathbb{R}(t)$, on a même un peu mieux :

Théorème

$\mathbb{Z}$ est diophantien dans $\mathbb{R}(t)$ (relativement à $\mathbb{Q}(t)$).

Démonstration : si $f \in \mathbb{R}(t)$, alors

$$f \in \mathbb{Z} \iff \begin{cases} f \in \mathbb{R} \\ \exists M = (x, z) \in \Delta, \quad f(0) = x(0) \end{cases}$$

et la deuxième condition équivaut à $x - f \in \mathscr{M}$. □

En général il est difficile de prouver que $\mathscr{M}$ est diophantien dans $k(t)$.

On peut remplacer cette condition par une autre plus faible, et satisfaite si k est réel ou p-adique.

Jan Denef (2011)

Merci de

votre

attention !