Courbes elliptiques et indécidabilité

Laurent Moret-Bailly

IRMAR, Université de Rennes 1
Membre du réseau européen *Arithmetic Algebraic Geometry*

24 mars 2006 / Université Louis Pasteur

Sommaire

Le dixième problème de Hilbert

« 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).

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).

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 ?)


Yuri Matiyasevich et Martin Davis (2005)

(*Photos : A. Shlapentokh)*

Qu'en pense Hilbert ?

« 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. »

Qu'en pense Hilbert ?

Il modifie sa question :

« 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. »

Qu'en pense Hilbert ?

Il modifie sa question :

« 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. »

Qu'en pense Hilbert ?

Il modifie sa question :

« 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 rationnels. »

Qu'en pense Hilbert ?

Il modifie sa question :

« 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 rationnels. »

Cette question est encore ouverte.

Décidabilité existentielle (ou « diophantienne »)

Soient $A_0 \subset A$ deux anneaux.

On dit que A est (existentiellement) décidable relativement à 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 :

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

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

Décidabilité existentielle (ou « diophantienne »)

Soient $A_0 \subset A$ deux anneaux.

On dit que A est (existentiellement) décidable relativement à 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 :

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

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

Décidabilité existentielle (ou « diophantienne »)

Soient $A_0 \subset A$ deux anneaux.

On dit que A est (existentiellement) décidable relativement à 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 ».)

Décidabilité existentielle (ou « diophantienne »)

Soient $A_0 \subset A$ deux anneaux.

On dit que A est (existentiellement) décidable relativement à 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 ».)

Exemples :

A_0	A	**Décidabilité diophantienne**	
$\mathbb{Q}$	$\mathbb{C}$	oui	th. des zéros de Hilbert
$\mathbb{Z}$	$\mathbb{Z}$	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)

Exemples :

A_0	A	**Décidabilité diophantienne**	
$\mathbb{Q}$	$\mathbb{C}$	oui	th. des zéros de Hilbert
$\mathbb{Z}$	$\mathbb{Z}$	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)

Exemples :

A_0	A	**Décidabilité diophantienne**	
$\mathbb{Q}$	$\mathbb{C}$	oui	th. des zéros de Hilbert
$\mathbb{Z}$	$\mathbb{Z}$	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)

Exemples :

A_0	A	**Décidabilité diophantienne**	
$\mathbb{Q}$	$\mathbb{C}$	oui	th. des zéros de Hilbert
$\mathbb{Z}$	$\mathbb{Z}$	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)

Exemples :

A_0	A	**Décidabilité diophantienne**	
$\mathbb{Q}$	$\mathbb{C}$	oui	th. des zéros de Hilbert
$\mathbb{Z}$	$\mathbb{Z}$	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)

Exemples :

A_0	A	**Décidabilité diophantienne**	
$\mathbb{Q}$	$\mathbb{C}$	oui	th. des zéros de Hilbert
$\mathbb{Z}$	$\mathbb{Z}$	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)

Exemples :

A_0	A	**Décidabilité diophantienne**	
$\mathbb{Q}$	$\mathbb{C}$	oui	th. des zéros de Hilbert
$\mathbb{Z}$	$\mathbb{Z}$	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)

Exemples :

A_0	A	**Décidabilité diophantienne**	
$\mathbb{Q}$	$\mathbb{C}$	oui	th. des zéros de Hilbert
$\mathbb{Z}$	$\mathbb{Z}$	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)

Ensembles diophantiens : définition

Soient $K_0 \subset K$ deux corps.

On rappelle qu'un sous-ensemble V de K^n est dit K_0-algébrique s'il est défini par des équations polynômes à coefficients dans K_0.

Un sous-ensemble V de K^n est dit K_0-diophantien (ou *existentiellement définissable*) s'il est l'image d'un sous-ensemble K_0-algébrique de K^{m+n} par l'une des projections évidentes $K^{n+m} \longrightarrow K^n$.

Un ensemble diophantien est donc de la forme

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

pour $F_1, \ldots, F_r \in K_0[\underline{X}, \underline{Z}]$ convenables.

Ensembles diophantiens : définition

Soient $K_0 \subset K$ deux corps.

On rappelle qu'un sous-ensemble V de K^n est dit K_0-algébrique s'il est défini par des équations polynômes à coefficients dans K_0.

Un sous-ensemble V de K^n est dit K_0-diophantien (ou *existentiellement définissable*) s'il est l'image d'un sous-ensemble K_0-algébrique de K^{m+n} par l'une des projections évidentes $K^{n+m} \to K^n$.

Un ensemble diophantien est donc de la forme

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

pour $F_1, \ldots, F_r \in K_0[\underline{X}, \underline{Z}]$ convenables.

Ensembles diophantiens : définition

Soient $K_0 \subset K$ deux corps.

On rappelle qu'un sous-ensemble V de K^n est dit K_0-algébrique s'il est défini par des équations polynômes à coefficients dans K_0.

Un sous-ensemble V de K^n est dit K_0-diophantien (ou *existentiellement définissable*) s'il est l'image d'un sous-ensemble K_0-algébrique de K^{m+n} par l'une des projections évidentes $K^{n+m} \to K^n$.

Un ensemble diophantien est donc de la forme

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

pour $F_1, \ldots, F_r \in K_0[\underline{X}, \underline{Z}]$ convenables.

Ensembles diophantiens : définition

Soient $K_0 \subset K$ deux corps.

On rappelle qu'un sous-ensemble V de K^n est dit K_0-algébrique s'il est défini par des équations polynômes à coefficients dans K_0.

Un sous-ensemble V de K^n est dit K_0-diophantien (ou *existentiellement définissable*) s'il est l'image d'un sous-ensemble K_0-algébrique de K^{m+n} par l'une des projections évidentes $K^{n+m} \to K^n$.

Un ensemble diophantien est donc de la forme

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

pour $F_1, \ldots, F_r \in K_0[\underline{X}, \underline{Z}]$ convenables.

Exemples (avec $n = 1$) :

1. $\mathbb{R}_+$ est diophantien dans $\mathbb{R}$ (c'est l'ensemble des carrés),
2. $\mathbb{Q}_+$ est diophantien dans $\mathbb{Q}$
3. $\mathbb{Z}$ n'est pas diophantien dans $\mathbb{R}$
4. $\mathbb{R}$ n'est pas diophantien dans $\mathbb{C}$,
5. on ne sait pas si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$.

Exemples (avec $n = 1$) :

1. $\mathbb{R}_+$ est diophantien dans $\mathbb{R}$ (c'est l'ensemble des carrés),
2. $\mathbb{Q}_+$ est diophantien dans $\mathbb{Q}$
3. $\mathbb{Z}$ n'est pas diophantien dans $\mathbb{R}$
4. $\mathbb{R}$ n'est pas diophantien dans $\mathbb{C}$,
5. on ne sait pas si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$.

Exemples (avec $n = 1$) :

1. $\mathbb{R}_+$ est diophantien dans $\mathbb{R}$ (c'est l'ensemble des carrés),
2. $\mathbb{Q}_+$ est diophantien dans $\mathbb{Q}$ (c'est l'ensemble des sommes de 4 carrés),
3. $\mathbb{Z}$ n'est pas diophantien dans $\mathbb{R}$
4. $\mathbb{R}$ n'est pas diophantien dans $\mathbb{C}$,
5. on ne sait pas si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$.

Exemples (avec $n = 1$) :

1. $\mathbb{R}_+$ est diophantien dans $\mathbb{R}$ (c'est l'ensemble des carrés),
2. $\mathbb{Q}_+$ est diophantien dans $\mathbb{Q}$ (c'est l'ensemble des sommes de 4 carrés),
3. $\mathbb{Z}$ n'est pas diophantien dans $\mathbb{R}$

4. $\mathbb{R}$ n'est pas diophantien dans $\mathbb{C}$,
5. on ne sait pas si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$.

Exemples (avec $n = 1$) :

1. $\mathbb{R}_+$ est diophantien dans $\mathbb{R}$ (c'est l'ensemble des carrés),
2. $\mathbb{Q}_+$ est diophantien dans $\mathbb{Q}$ (c'est l'ensemble des sommes de 4 carrés),
3. $\mathbb{Z}$ n'est pas diophantien dans $\mathbb{R}$ (il a une infinité de composantes connexes),
4. $\mathbb{R}$ n'est pas diophantien dans $\mathbb{C}$,
5. on ne sait pas si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$.

Exemples (avec $n = 1$) :

1. $\mathbb{R}_+$ est diophantien dans $\mathbb{R}$ (c'est l'ensemble des carrés),
2. $\mathbb{Q}_+$ est diophantien dans $\mathbb{Q}$ (c'est l'ensemble des sommes de 4 carrés),
3. $\mathbb{Z}$ n'est pas diophantien dans $\mathbb{R}$ (il a une infinité de composantes connexes),
4. $\mathbb{R}$ n'est pas diophantien dans $\mathbb{C}$,
5. on ne sait pas si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$.

Exemples (avec $n = 1$) :

1. $\mathbb{R}_+$ est diophantien dans $\mathbb{R}$ (c'est l'ensemble des carrés),
2. $\mathbb{Q}_+$ est diophantien dans $\mathbb{Q}$ (c'est l'ensemble des sommes de 4 carrés),
3. $\mathbb{Z}$ n'est pas diophantien dans $\mathbb{R}$ (il a une infinité de composantes connexes),
4. $\mathbb{R}$ n'est pas diophantien dans $\mathbb{C}$,
5. on ne sait pas si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$.

Exemples (avec $n = 1$) :

1. $\mathbb{R}_+$ est diophantien dans $\mathbb{R}$ (c'est l'ensemble des carrés),
2. $\mathbb{Q}_+$ est diophantien dans $\mathbb{Q}$ (c'est l'ensemble des sommes de 4 carrés),
3. $\mathbb{Z}$ n'est pas diophantien dans $\mathbb{R}$ (il a une infinité de composantes connexes),
4. $\mathbb{R}$ n'est pas diophantien dans $\mathbb{C}$,
5. on ne sait pas si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$.

On aimerait bien le savoir car :

Un critère d'indécidabilité

Proposition

Si K est décidable et si $A \subset K$ est un sous-anneau diophantien de K, alors A est décidable.

(Démonstration immédiate).

Conséquence : si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$, alors $\mathbb{Q}$ est existentiellement indécidable.

Un critère d'indécidabilité

Proposition

Si K est décidable et si $A \subset K$ est un sous-anneau diophantien de K, alors A est décidable.

(Démonstration immédiate).

Conséquence : si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$, alors $\mathbb{Q}$ est existentiellement indécidable.

Un critère d'indécidabilité

Proposition

Si K est décidable et si $A \subset K$ est un sous-anneau diophantien de K, alors A est décidable.

(Démonstration immédiate).

Conséquence : si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$, alors $\mathbb{Q}$ est existentiellement indécidable.

Mais une conjecture de Mazur impliquerait que $\mathbb{Z}$ n'est pas diophantien dans $\mathbb{Q}$...

On prend désormais

$$K = \mathbb{R}(t)$$

et l'on se propose de montrer :

Théorème (J. Denef)

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

En conséquence, $\mathbb{R}(t)$ est existentiellement indécidable relativement à $\mathbb{Q}(t)$.

On prend désormais

$$K = \mathbb{R}(t)$$

et l'on se propose de montrer :

Théorème (J. Denef)

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

En conséquence, $\mathbb{R}(t)$ est existentiellement indécidable relativement à $\mathbb{Q}(t)$.

Les constantes sont définissables :

Proposition

$\mathbb{R}$ est diophantien dans $\mathbb{R}(t)$.

Démonstration : si $g \in \mathbb{R}(t)$, alors g est constante si et seulement si

il existe $f \in \mathbb{R}(t)$ telle que $g^2 = f^3 + 1$.

Le « seulement si » est trivial (prendre $f = \sqrt[3]{g^2 - 1}$).

Réciproquement, remarquer que la courbe plane d'équation $y^2 = x^3 + 1$ est de genre 1 et n'a donc pas de paramétrisation rationnelle.

Les constantes sont définissables :

Proposition

$\mathbb{R}$ *est diophantien dans* $\mathbb{R}(t)$.

Démonstration : si $g \in \mathbb{R}(t)$, alors g est constante si et seulement si

il existe $f \in \mathbb{R}(t)$ telle que $g^2 = f^3 + 1$.

Le « seulement si » est trivial (prendre $f = \sqrt[3]{g^2 - 1}$).

Réciproquement, remarquer que la courbe plane d'équation $y^2 = x^3 + 1$ est de genre 1 et n'a donc pas de paramétrisation rationnelle.

Les constantes sont définissables :

Proposition

$\mathbb{R}$ *est diophantien dans* $\mathbb{R}(t)$.

Démonstration : si $g \in \mathbb{R}(t)$, alors g est constante si et seulement si

il existe $f \in \mathbb{R}(t)$ telle que $g^2 = f^3 + 1$.

Le « seulement si » est trivial (prendre $f = \sqrt[3]{g^2 - 1}$).

Réciproquement, remarquer que la courbe plane d'équation $y^2 = x^3 + 1$ est de genre 1 et n'a donc pas de paramétrisation rationnelle.

Les constantes sont définissables :

Proposition

$\mathbb{R}$ est diophantien dans $\mathbb{R}(t)$.

Démonstration : si $g \in \mathbb{R}(t)$, alors g est constante si et seulement si

il existe $f \in \mathbb{R}(t)$ telle que $g^2 = f^3 + 1$.

Le « seulement si » est trivial (prendre $f = \sqrt[3]{g^2 - 1}$).

Réciproquement, remarquer que la courbe plane d'équation $y^2 = x^3 + 1$ est de genre 1 et n'a donc pas de paramétrisation rationnelle.

Les fonctions positives sont définissables :

Proposition

L'ensemble des $g \in \mathbb{R}(t)$ qui sont ≥ 0 sur $\mathbb{R}$ est diophantien dans $\mathbb{R}(t)$.

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

$$g \geq 0 \text{ sur } \mathbb{R} \iff g \text{ est somme de deux carrés dans } \mathbb{R}(t).$$

Les fonctions positives sont définissables :

Proposition

L'ensemble des $g \in \mathbb{R}(t)$ qui sont ≥ 0 sur $\mathbb{R}$ est diophantien dans $\mathbb{R}(t)$.

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

$$g \geq 0 \text{ sur } \mathbb{R} \Longleftrightarrow g \text{ est somme de deux carrés dans } \mathbb{R}(t).$$

Les fonctions nulles en 0 sont définissables :

Proposition

L'ensemble des $g \in \mathbb{R}(t)$ telles que $g(0) = 0$ est diophantien dans $\mathbb{R}(t)$.

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

$$g(0) = 0$$

$$\Updownarrow$$

$$\frac{1}{g^2} + \frac{1}{t} \text{ est minorée sur } \mathbb{R}$$

$$\Updownarrow$$

$$\exists c \in \mathbb{R}, \quad \frac{1}{g^2} + \frac{1}{t} + c \geq 0 \text{ (sur } \mathbb{R}).$$

Les fonctions nulles en 0 sont définissables :

Proposition

L'ensemble des $g \in \mathbb{R}(t)$ telles que $g(0) = 0$ est diophantien dans $\mathbb{R}(t)$.

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

$$g(0) = 0$$

$$\Updownarrow$$

$$\frac{1}{g^2} + \frac{1}{t} \text{ est minorée sur } \mathbb{R}$$

$$\Updownarrow$$

$$\exists c \in \mathbb{R}, \quad \frac{1}{g^2} + \frac{1}{t} + c \geq 0 \text{ (sur } \mathbb{R}).$$

Les fonctions nulles en 0 sont définissables :

Proposition

L'ensemble des $g \in \mathbb{R}(t)$ telles que $g(0) = 0$ est diophantien dans $\mathbb{R}(t)$.

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

$$g(0) = 0$$

$$\Updownarrow$$

$$\frac{1}{g^2} + \frac{1}{t} \text{ est minorée sur } \mathbb{R}$$

$$\Updownarrow$$

$$\exists c \in \mathbb{R}, \quad \frac{1}{g^2} + \frac{1}{t} + c \geq 0 \text{ (sur } \mathbb{R}).$$

La « spécialisation en 0 » est diophantienne :

Proposition

Si $D \subset \mathbb{R}(t)$ est diophantien, alors

$$D(0) := \{f(0)\}_{f \in D}$$

est diophantien dans $\mathbb{R}(t)$.

Démonstration : si $g \in \mathbb{R}(t)$, alors $g \in D(0)$ si et seulement si

- $g \in \mathbb{R}$;
- il existe $f \in D$ tel que $(f - g)(0) = 0$.

La « spécialisation en 0 » est diophantienne :

Proposition

Si $D \subset \mathbb{R}(t)$ est diophantien, alors

$$D(0) := \{f(0)\}_{f \in D}$$

est diophantien dans $\mathbb{R}(t)$.

Démonstration : si $g \in \mathbb{R}(t)$, alors $g \in D(0)$ si et seulement si

- $g \in \mathbb{R}$;
- il existe $f \in D$ tel que $(f - g)(0) = 0$.

En résumé :

Pour montrer que $\mathbb{Z}$ est diophantien dans $\mathbb{R}(t)$:

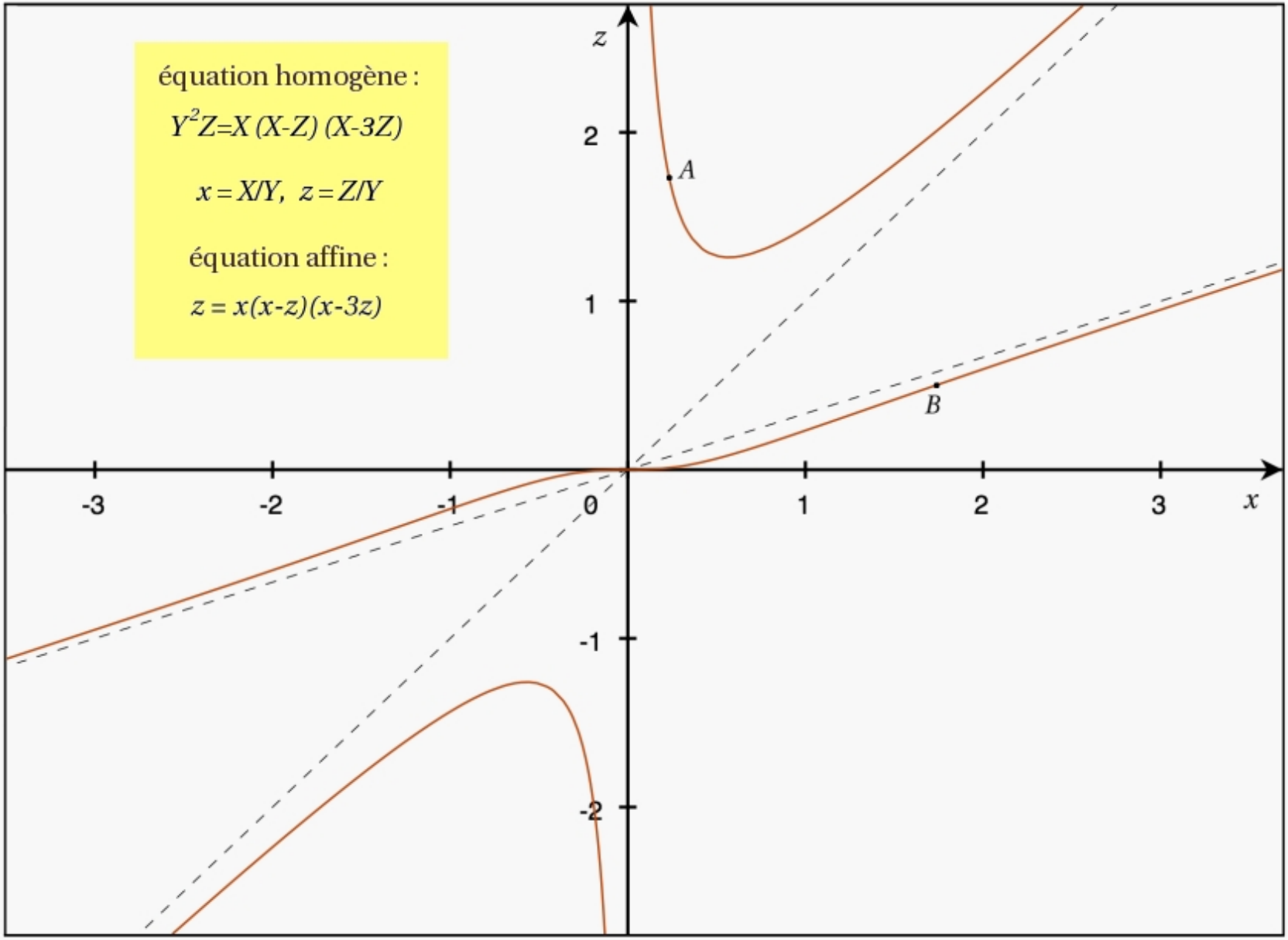
trouver $D \subset \mathbb{R}(t)$ diophantien tel que $D(0) = \mathbb{Z}$.

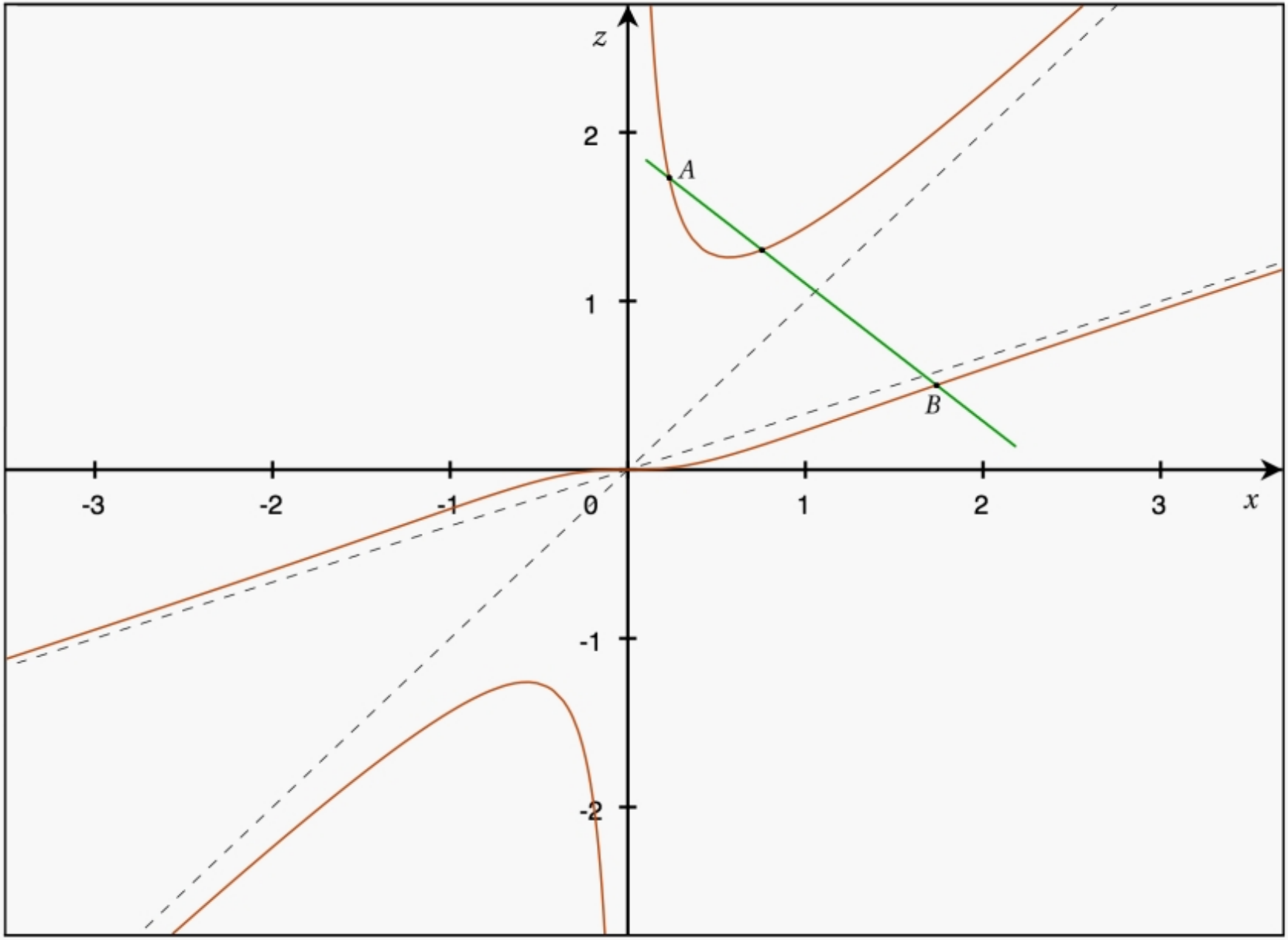
Utilisation des courbes elliptiques

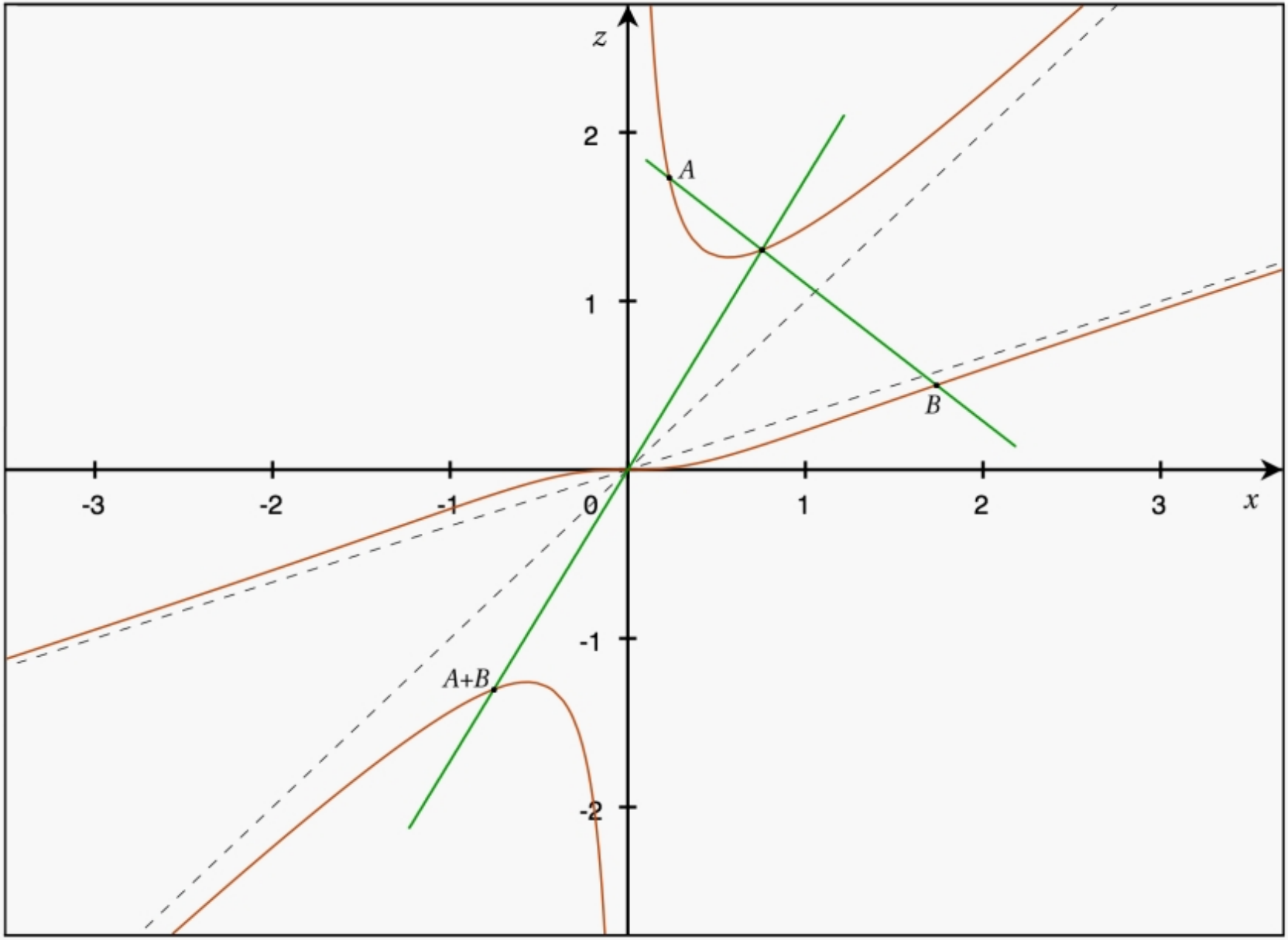
Une cubique plane (projective) non singulière

$$E : \qquad Y^2 Z = X^3 + aX^2 Z + bX Z^2 + cZ^3 =: F(X, Z)$$

($F \in K_0[X, Z]$, à discriminant non nul) admet une structure de groupe naturelle, donnée par des formules polynomiales.


équation homogène :
$Y^2Z=X(X-Z)(X-3Z)$
$x=X/Y,\ z=Z/Y$
équation affine :
$z=x(x-z)(x-3z)$
z
x
A
B
-3
-2
-1
0
1
2
3
2
1
-1
-2


z
2
1
-1
-2
A
B
-3
-2
-1
0
1
2
3
x


z
2
1
-1
-2
-3
-2
-1
0
1
2
3
x
A
B
A+B

La courbe « tordue » de Manin-Denef sur $\mathbb{R}(t)$

On part d'une courbe elliptique, d'équation affine

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

avec a, b, c dans $\mathbb{Q}$.

On définit la « tordue de Manin-Denef » de E comme la courbe E_t sur $\mathbb{R}(t)$ définie par

$$\begin{aligned} E_t : \qquad z &= \frac{t}{F(1,t)}\,F(x,z) \\ &= \frac{t}{1+a\,t+b\,t^2+c\,t^3}\,(x^3 + a\,x^2\,z + b\,x\,z^2 + c\,z^3). \end{aligned}$$

La courbe « tordue » de Manin-Denef sur $\mathbb{R}(t)$

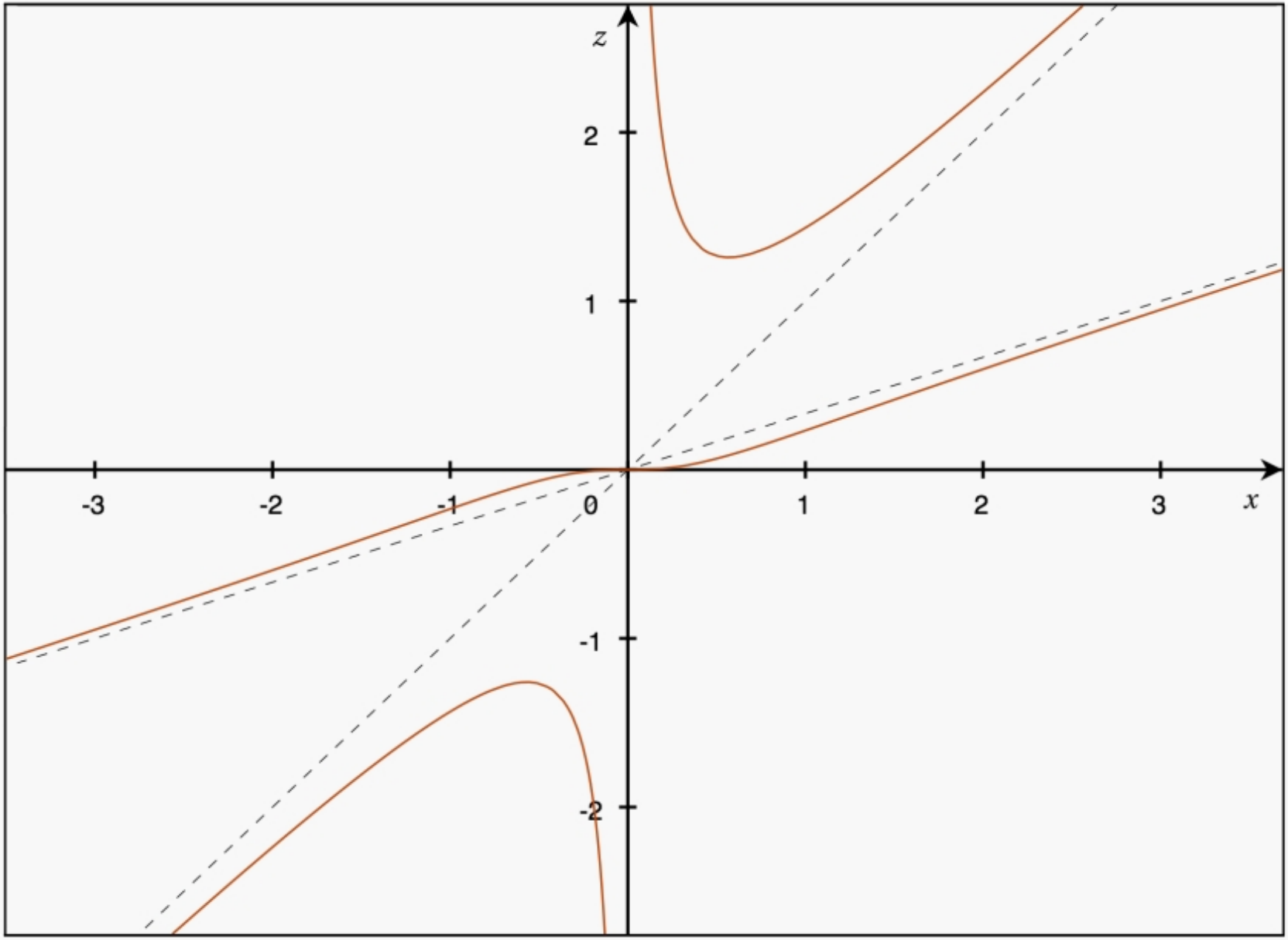
On part d'une courbe elliptique, d'équation affine

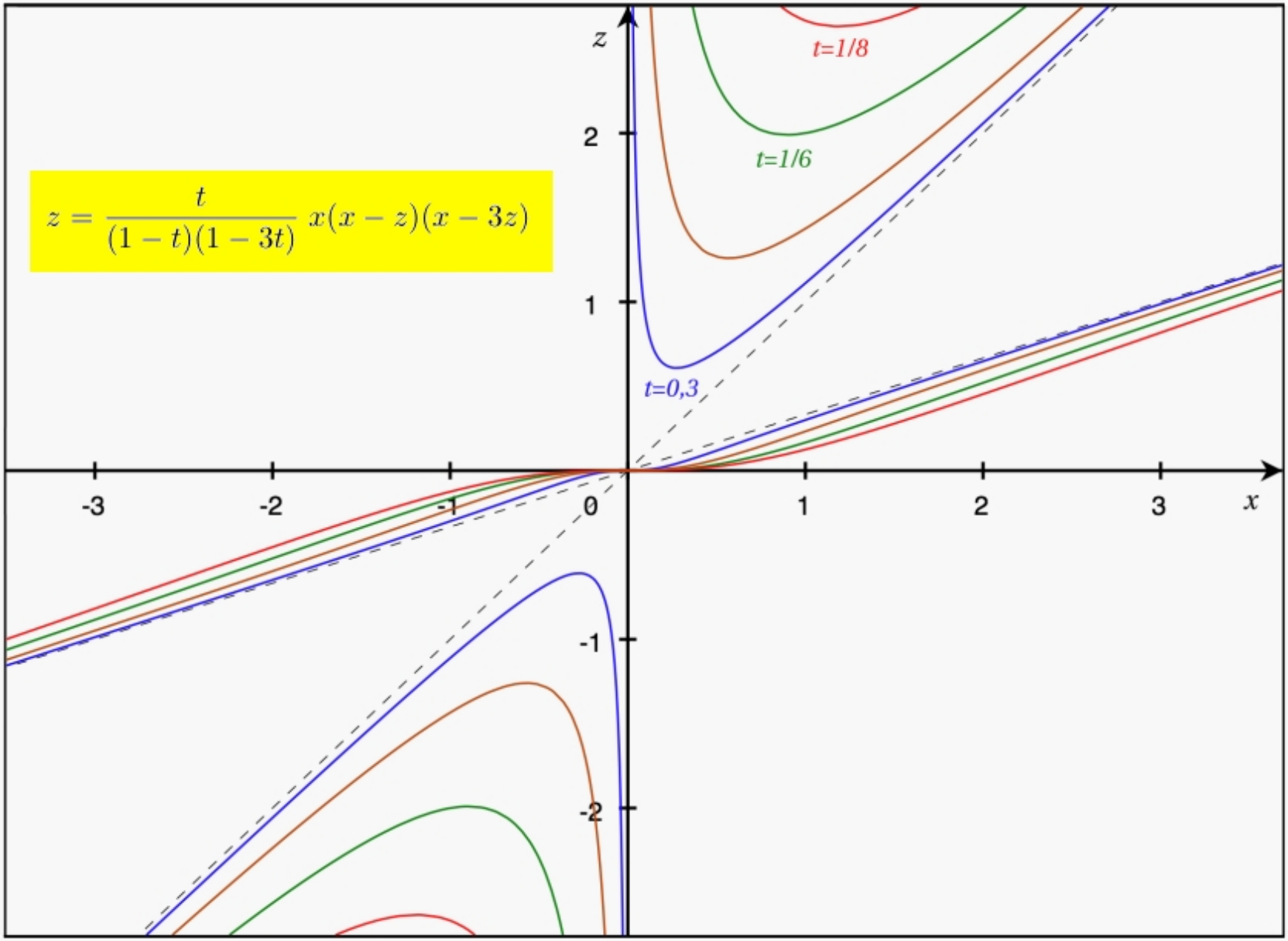
$$E : \qquad z = x^3 + a\,x^2\,z + b\,x\,z^2 + c\,z^3 =: F(x,z)$$

avec a, b, c dans $\mathbb{Q}$.

On définit la « tordue de Manin-Denef » de E comme la courbe E_t sur $\mathbb{R}(t)$ définie par

$$\begin{aligned} E_t : \qquad z &= \frac{t}{F(1,t)}\,F(x,z) \\ &= \frac{t}{1+a\,t+b\,t^2+c\,t^3}\,(x^3 + a\,x^2\,z + b\,x\,z^2 + c\,z^3). \end{aligned}$$

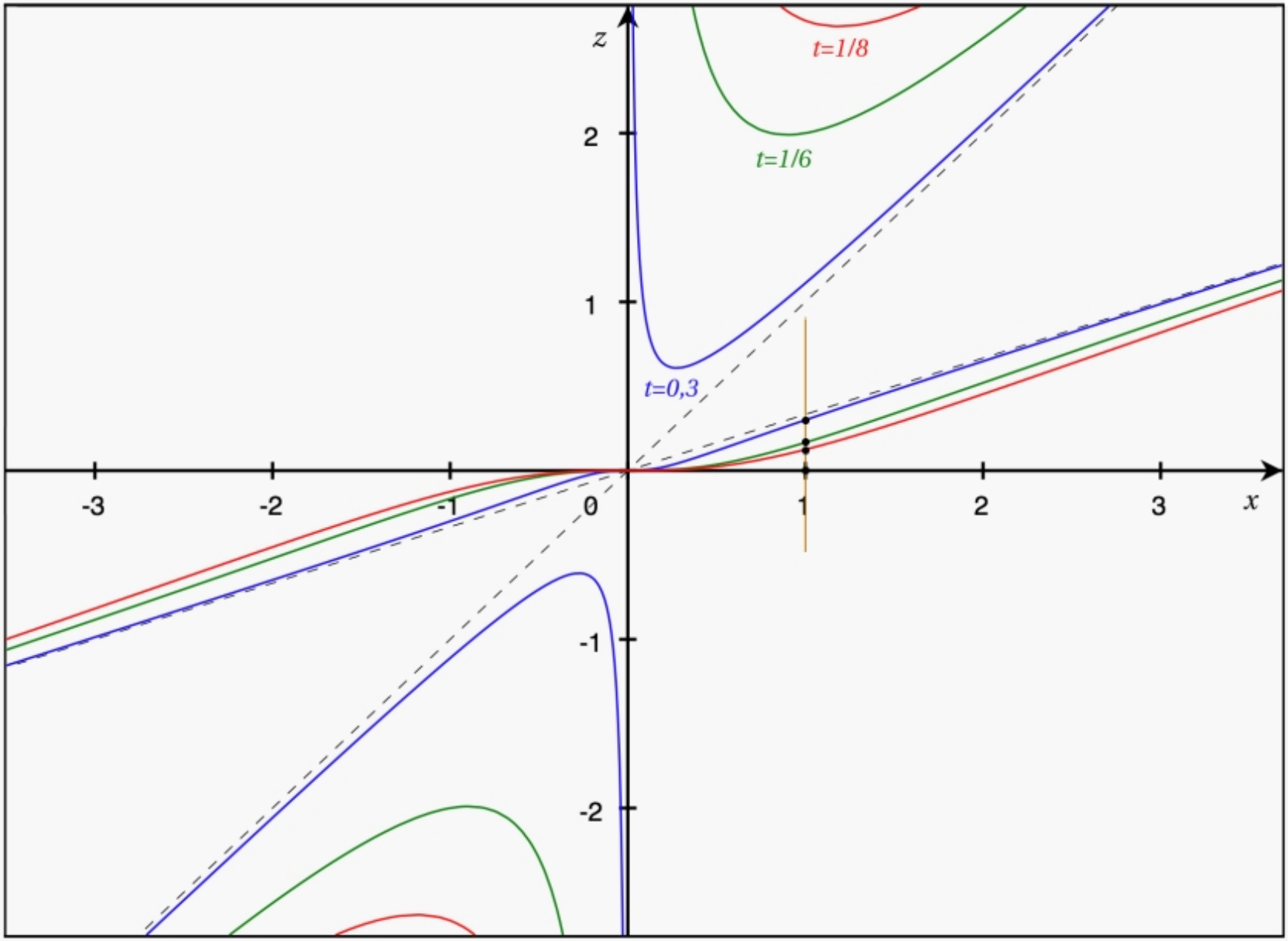

z
2
1
-1
-2
-3
-2
-1
0
1
2
3
x


$z = \frac{t}{(1-t)(1-3t)}\, x(x-z)(x-3z)$
z
x
t=1/8
t=1/6
t=0,3
-3
-2
-1
0
1
2
3
2
1
-1
-2

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

a un point évident donné par

$$\gamma = \gamma(t) = (1,t) \in E_t(\mathbb{R}(t)).$$


z
x
t=1/8
t=1/6
t=0,3
-3
-2
-1
0
1
2
3
2
1
-1
-2

On peut montrer que $E_t(\mathbb{R}(t))$ est « presque » engendré par γ, plus précisément

$$\begin{aligned} E_t(\mathbb{R}(t)) &\cong \mathbb{Z}\gamma \times (\mathbb{Z}/2\mathbb{Z})^r \\ &\cong \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^r \end{aligned}$$

avec $r \in \{1, 2\}$, pourvu que E soit convenablement choisie (i.e. sans multiplication complexe).

Conséquence :

$\Delta := \mathbb{Z}\gamma \subset \mathbb{R}(t)^2$ est diophantien

(relativement à $\mathbb{Q}(t)$).

On peut montrer que $E_t(\mathbb{R}(t))$ est « presque » engendré par γ, plus précisément

$$\begin{aligned} E_t(\mathbb{R}(t)) &\cong \mathbb{Z}\gamma \times (\mathbb{Z}/2\mathbb{Z})^r \\ &\cong \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^r \end{aligned}$$

avec $r \in \{1, 2\}$, pourvu que E soit convenablement choisie (i.e. sans multiplication complexe).

Conséquence :

$\Delta := \mathbb{Z}\gamma \subset \mathbb{R}(t)^2$ est diophantien

(relativement à $\mathbb{Q}(t)$).

Posons

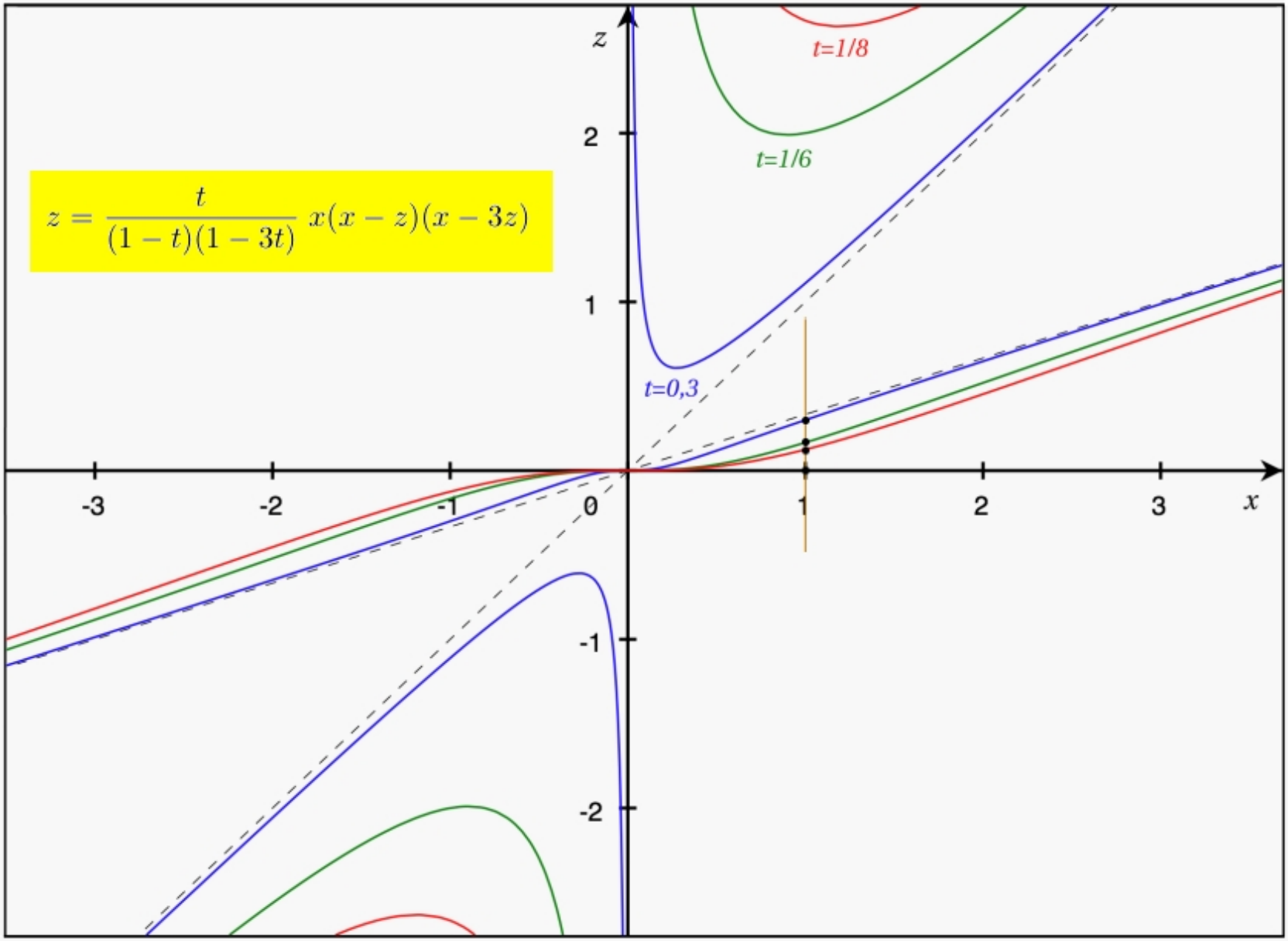
$$D := \{\text{abscisses des éléments de } \Delta\} \subset \mathbb{R}(t).$$

Alors D est diophantien, et on va montrer que $D(0) = \mathbb{Z}$.

$$E_t : \qquad z = t\,\frac{x^3 + a\,x^2\,z + b\,x\,z^2 + c\,z^3}{1 + a\,t + b\,t^2 + c\,t^3}.$$

On peut voir E_t comme une famille de courbes sur $\mathbb{R}$, paramétrée par t.

Pour presque tout $\tau \in \mathbb{R}$, on obtient une courbe elliptique E_τ sur $\mathbb{R}$.


$z = \frac{t}{(1-t)(1-3t)}\, x(x-z)(x-3z)$
t=1/8
t=1/6
t=0,3
z
x
2
1
-1
-2
-3
-2
-1
0
1
2
3

Que se passe-t-il pour $\tau = 0$?

- E_0 est la droite $z = 0$ (que l'on peut identifier à $\mathbb{R}$);
- $\gamma(t) = (1, t)$ se spécialise en $(1, 0)$;
- la loi de groupe sur E_t se spécialise en l'addition dans $\mathbb{R}$;
- par suite, pour n dans $\mathbb{Z}$, le point $n\gamma \in E_t(\mathbb{R}(t))$ se spécialise en $(n, 0)$!

Que se passe-t-il pour $\tau = 0$?

- E_0 est la droite $z = 0$ (que l'on peut identifier à $\mathbb{R}$);
- $\gamma(t) = (1, t)$ se spécialise en $(1, 0)$;
- la loi de groupe sur E_t se spécialise en l'addition dans $\mathbb{R}$;
- par suite, pour n dans $\mathbb{Z}$, le point $n\gamma \in E_t(\mathbb{R}(t))$ se spécialise en $(n, 0)$!

Que se passe-t-il pour $\tau = 0$?

- E_0 est la droite $z = 0$ (que l'on peut identifier à $\mathbb{R}$);
- $\gamma(t) = (1, t)$ se spécialise en $(1, 0)$;
- la loi de groupe sur E_t se spécialise en l'addition dans $\mathbb{R}$;
- par suite, pour n dans $\mathbb{Z}$, le point $n\gamma \in E_t(\mathbb{R}(t))$ se spécialise en $(n, 0)$!

On a donc bien $D(0) = \mathbb{Z}$, comme annoncé

Que se passe-t-il pour $\tau = 0$?

- E_0 est la droite $z = 0$ (que l'on peut identifier à $\mathbb{R}$);
- $\gamma(t) = (1, t)$ se spécialise en $(1, 0)$;
- la loi de groupe sur E_t se spécialise en l'addition dans $\mathbb{R}$;
- par suite, pour n dans $\mathbb{Z}$, le point $n\gamma \in E_t(\mathbb{R}(t))$ se spécialise en $(n, 0)$!

On a donc bien $D(0) = \mathbb{Z}$, comme annoncé

donc $\mathbb{Z}$ est diophantien dans $\mathbb{R}(t)$

Que se passe-t-il pour $\tau = 0$?

- E_0 est la droite $z = 0$ (que l'on peut identifier à $\mathbb{R}$);
- $\gamma(t) = (1, t)$ se spécialise en $(1, 0)$;
- la loi de groupe sur E_t se spécialise en l'addition dans $\mathbb{R}$;
- par suite, pour n dans $\mathbb{Z}$, le point $n\gamma \in E_t(\mathbb{R}(t))$ se spécialise en $(n, 0)$!

On a donc bien $D(0) = \mathbb{Z}$, comme annoncé
donc $\mathbb{Z}$ est diophantien dans $\mathbb{R}(t)$
donc $\mathbb{R}(t)$ est existentiellement indécidable.

Dans la figure suivante, la courbe violette est le lieu de $2\gamma(t)$ (le double de γ pour la loi de groupe de E_t) :

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

Équation cartésienne :

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


z
2
1
-1
-2
-3
-2
-1
0
1
2
3
x