Courbes elliptiques et indécidabilité des corps de fonctions

Laurent Moret-Bailly

IRMAR, Université de Rennes 1

Référence : prépublication IRMAR 04-42 (accepté pour publication à Crelle)

Décidabilité et dixième problème de Hilbert

Définition :

Soient $A_0 \subset A$ deux anneaux.

On dit que A est existentiellement décidable relativement à A_0 si :

il existe un algorithme qui, étant donné un système fini d'équations polynomiales

$$F_i(x_1, \ldots, x_n) = 0 \quad (i = 1, \ldots, r)$$

à coefficients dans A_0, dit si le système a une solution $(x_1, \ldots, x_n)$ dans A^n.

(On pourra omettre « existentiellement » et oublier de préciser A_0.)

Dixième problème de Hilbert

Il peut se formuler ainsi :

« $\mathbb{Z}$ est-il existentiellement décidable ? »

La réponse est non (Matijasevich, 1970, à la suite de nombreux travaux de Davis, Putnam et Robinson).

Quelques exemples :

Anneau A	**Sous-anneau A_0**	**Décidabilité**	
$\mathbb{C}$	$\mathbb{Q}$	oui	théorème des zéros
$\mathbb{Z}$	$\mathbb{Z}$	non	Matijasevich (1970)
$\mathbb{Q}$	$\mathbb{Q}$ (ou $\mathbb{Z}$)	?	
$k(t)$ (k réel)	$\mathbb{Q}(t)$	non	Denef (1978)
$\mathbb{C}(t_1, t_2)$		non	Kim et Roush (1992)
$k(t)$ (k p-adique, $p \neq 2$)		non	Kim et Roush (1995)
$\mathbb{C}(t)$		?	

But de l'exposé :

généraliser les résultats de Denef et de Kim-Roush aux corps de fonctions K sur k, pour k réel ou p-adique.

Théorème :

Soit K une extension de type fini et transcendante d'un corps k. On suppose :

- soit que K est réel ;
- soit que k est un sous-corps d'une extension finie de $\mathbb{Q}_p$, pour p premier impair.

Alors K est existentiellement indécidable.

Théorème :

Soit K une extension de type fini et transcendante d'un corps k. On suppose :

- soit que K est réel ;
- soit que k est un sous-corps d'une extension finie de $\mathbb{Q}_p$, pour p premier impair.

Alors K est existentiellement indécidable.

(Dans cet exposé, on se limitera au cas où $\deg \operatorname{tr}(K/k) = 1$.)

Ensembles diophantiens

Définition :

Soient $K_0 \subset K$ deux corps.
Soit V un K_0-schéma (de type fini).
Soit $X \subset V(K)$.

Ensembles diophantiens

Définition :

Soient $K_0 \subset K$ deux corps.
Soit V un K_0-schéma (de type fini).
Soit $X \subset V(K)$.

Alors X est dit (K_0, K)-diophantien (ou encore existentiellement définissable) si :
il existe un K_0-schéma de type fini W et un K_0-morphisme $\phi : W \to V$ tel que $X = \phi(W(K))$.

Exemples :

$\mathbb{R}_+$ est diophantien dans $\mathbb{R}$;

$\mathbb{Q}_+$ est diophantien dans $\mathbb{Q}$;

$\mathbb{Z}$ n'est pas diophantien dans $\mathbb{R}$;

on ne sait pas si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$.

Exemples :

$\mathbb{R}_+$ est diophantien dans $\mathbb{R}$;

(c'est l'ensemble des carrés)

$\mathbb{Q}_+$ est diophantien dans $\mathbb{Q}$;

$\mathbb{Z}$ n'est pas diophantien dans $\mathbb{R}$;

on ne sait pas si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$.

Exemples :

$\mathbb{R}_+$ est diophantien dans $\mathbb{R}$;

(c'est l'ensemble des carrés)

$\mathbb{Q}_+$ est diophantien dans $\mathbb{Q}$;

(c'est l'ensemble des sommes de 4 carrés)

$\mathbb{Z}$ n'est pas diophantien dans $\mathbb{R}$;

on ne sait pas si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$.

Exemples :

$\mathbb{R}_+$ est diophantien dans $\mathbb{R}$;

(c'est l'ensemble des carrés)

$\mathbb{Q}_+$ est diophantien dans $\mathbb{Q}$;

(c'est l'ensemble des sommes de 4 carrés)

$\mathbb{Z}$ n'est pas diophantien dans $\mathbb{R}$;

(les ensembles diophantiens sont les réunions finies d'intervalles)

on ne sait pas si $\mathbb{Z}$ est diophantien dans $\mathbb{Q}$.

Structures diophantiennes :

Si X et X' sont des ensembles (K_0, K)-diophantiens, on peut évidemment parler :

- de relations binaires diophantiennes $R \subset X \times X'$,
- d'applications diophantiennes $f : X \to X'$,
- de lois de composition diophantiennes sur X.

En particulier, on a une notion naturelle
d'anneau (K_0, K)-diophantien.

Une conséquence facile du théorème de Matijasevich (et la clé de la plupart des preuves d'indécidabilité diophantienne) :

Proposition :

Soient $K_0 \subset K$ deux corps. On suppose que :

il existe un anneau (K_0, K)-diophantien $\mathscr{Z}$, isomorphe à $\mathbb{Z}$ comme anneau.

Alors K est existentiellement indécidable relativement à K_0.

Méthode des courbes elliptiques :

Pour montrer que K est indécidable, trouver :

– une courbe elliptique $\mathscr{E}$ sur K_0,
– un entier $d > 0$ (ici, $d = 2$),
– un isomorphisme de groupes $d\mathscr{E}(K) \cong \mathbb{Z}$

de telle sorte que la multiplication sur $d\mathscr{E}(K)$ soit diophantienne.

Courbes elliptiques tordues

On part des données suivantes :

- S : un schéma où 2 est inversible ;
- $E \to S$: une S-courbe elliptique ;
- $\pi : \widetilde{S} \to S$: un morphisme fini localement libre de degré 2 (d'où une S-involution naturelle sur $\widetilde{S}$).

Courbes elliptiques tordues

On part des données suivantes :

- S : un schéma où 2 est inversible ;
- $E \to S$: une S-courbe elliptique ;
- $\pi : \widetilde{S} \to S$: un morphisme fini localement libre de degré 2 (d'où une S-involution naturelle sur $\widetilde{S}$).

On définit un S-schéma en groupes $E^\pi \to S$, la *tordue de E par π*, par la propriété universelle suivante : pour tout S-schéma T, on a

$$E^\pi(T) = E(T \times_S \widetilde{S})^{\mathrm{odd}}$$

où $^{\mathrm{odd}}$ signifie « commutant aux involutions ».

Propriétés de la tordue :

– si π est étale, E^π est une S-courbe elliptique ;
– si $\widetilde{S} = S[\varepsilon]/(\varepsilon^2)$, alors E^π est le fibré tangent de E, restreint à $E[2]$;

Propriétés de la tordue :

– si π est étale, E^π est une S-courbe elliptique ;
– si $\widetilde{S} = S[\varepsilon]/(\varepsilon^2)$, alors E^π est le fibré tangent de E, restreint à $E[2]$;

– si $\pi : \widetilde{C} \to C$ est un revêtement de courbes projectives lisses sur un corps k, et si E est constante (i.e. définie sur k), alors

$$E^\pi(k(C)) = \mathrm{Mor}_k^{\mathrm{odd}}(\widetilde{C}, E)$$

(les k-morphismes $\widetilde{C} \to E$ commutant aux involutions).

La courbe « auto-tordue » de Denef

On prend $C = \mathbb{P}^1_k$, i.e. $K = k(t)$, et on prend pour π le revêtement double standard $E \longrightarrow \mathbb{P}^1_k$. La fibre générique de E^π est une $k(t)$-courbe elliptique $\mathscr{E}$ vérifiant

$$\mathscr{E}(k(t)) \cong \mathrm{Mor}_k^{\mathrm{odd}}(E, E) = \mathrm{End}_k(E) \times E[2](k).$$

La courbe « auto-tordue » de Denef

On prend $C = \mathbb{P}^1_k$, i.e. $K = k(t)$, et on prend pour π le revêtement double standard $E \longrightarrow \mathbb{P}^1_k$. La fibre générique de E^π est une $k(t)$-courbe elliptique $\mathscr{E}$ vérifiant

$$\mathscr{E}(k(t)) \;\cong \mathrm{Mor}_k^{\mathrm{odd}}(E,E) = \mathrm{End}_k(E) \times E[2](k).$$

En particulier, si E est sans multiplication complexe, alors

$$2\,\mathscr{E}(k(t)) \;\cong 2\,\mathrm{End}_k(E) \;\cong \mathbb{Z}.$$

Que peut-on dire de la multiplication sur $2\,\mathscr{E}(k(t))$?

Comme $\mathscr{E} \to \operatorname{Spec}(k(t))$ a réduction additive à l'infini, on obtient un homomorphisme de spécialisation

$$\mathbb{Z} \cong 2\,\mathscr{E}(k(t)) \xrightarrow{\text{sp}} \mathscr{E}_\infty(k) \cong (k, +).$$

Ce morphisme est non nul, donc (puisque $\operatorname{car} k = 0$) on peut supposer que c'est l'inclusion naturelle $\mathbb{Z} \to k$. En particulier il respecte la multiplication.

Pour conclure que $K = k(t)$ est indécidable, il suffit de montrer que

$$\mathrm{sp} : \mathscr{E}(k(t)) \longrightarrow \mathscr{E}_\infty(k)$$

a de bonnes propriétés diophantiennes.

En termes de coordonnées, cette application est essentiellement la réduction modulo l'idéal maximal du point ∞.

On obtient de cette façon :

Théorème :

Soit $\mathscr{O} \subset k(t)$ l'anneau local du point ∞ dans $\mathbb{P}^1_k$.

Si $\mathscr{O}$[1] est diophantien dans $k(t)$, alors la multiplication dans

$$2\,\mathscr{E}(k(t)) \;\cong \mathbb{Z}$$

est diophantienne, et en particulier $k(t)$ est existentiellement indécidable.

[1] ou son idéal maximal

Théorème :

Soit $\mathscr{O} \subset k(t)$ l'anneau local du point ∞ dans $\mathbb{P}^1_k$.

Si $\mathscr{O}$[1] est diophantien dans $k(t)$, alors la multiplication dans

$$2\,\mathscr{E}(k(t)) \;\cong \mathbb{Z}$$

est diophantienne, et en particulier $k(t)$ est existentiellement indécidable.

Il est en général difficile de prouver que $\mathscr{O}$ est diophantien dans $k(t)$ (mais c'est vrai par exemple si $k = \mathbb{R}$, par une astuce de « sommes de carrés »).

En pratique on remplace cette condition par une autre plus faible, qui est satisfaite si k est réel.

[1] ou son idéal maximal

On en déduit le théorème de Denef (k réel, $K = k(t)$).

Une variante plus compliquée donne le théorème de Kim-Roush (k p-adique, $K = k(t)$).

Généralisation à une courbe quelconque :

- k : corps de caractéristique nulle
- C : courbe projective, lisse, géométriquement connexe sur k
- $K := k(C)$ (corps des fonctions de C)
- E : courbe elliptique sur k, sans multiplication complexe.

But : étendre l'argument de Denef à K.

On utilise encore l'« auto-tordue » $\mathscr{E}$ de E sur $k(t)$. Pour en faire une courbe sur K, on doit faire de K une extension de $k(t)$.

On prend donc un k-morphisme

$$f : C \to \mathbb{P}^1_k$$

avec de bonnes propriétés (étale en 0 et ∞, ramification simple, etc.)

Via f, K devient une extension finie de $k(t)$, notée K_f. On en déduit une injection

$$j_f : \mathscr{E}(k(t)) \hookrightarrow \mathscr{E}(K_f).$$

Question :

Peut-on choisir f de telle sorte que

$$j_f : \mathscr{E}(k(t)) \hookrightarrow \mathscr{E}(K_f)$$

soit un isomorphisme ?

Question :

Peut-on choisir f de telle sorte que

$$j_f : \mathscr{E}(k(t)) \hookrightarrow \mathscr{E}(K_f)$$

soit un isomorphisme ?

Si oui, la courbe elliptique $\mathscr{E}_{K_f}$
- est de rang 1 ;
- a réduction additive aux pôles de f.

On peut alors reprendre les arguments de Denef et de Kim-Roush pour l'indécidabilité de K.

La condition en question peut être réalisée en

remplaçant le morphisme $f : C \to \mathbb{P}^1_k$ d'origine

par λf, pour $\lambda \in k^*$ convenable :

Théorème :

Soit Λ l'ensemble des $\lambda \in k^*$ tels que

$$j_{\lambda f} : \mathscr{E}(k(t)) \hookrightarrow \mathscr{E}(K_{\lambda f})$$

soit un isomorphisme.

Alors Λ est infini. Plus précisément :

- $\Lambda \cap \mathbb{Q}$ est infini ;
- si k est de type fini sur $\mathbb{Q}$, alors Λ contient un sous-ensemble hilbertien de k.

Esquisse de démonstration :

Pour chaque $\lambda \in k^*$, on a une courbe X_λ définie comme le produit fibré

$$\begin{array}{ccc} X_\lambda & \xrightarrow{\varphi_\lambda} & E \\ \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} \\ C & \xrightarrow{\lambda f} & \mathbb{P}^1_k \end{array}$$

(X_λ est donc un revêtement double de C, dépendant de λ).

On a un isomorphisme canonique

$$\mathscr{E}(K_{\lambda f}) \cong \mathrm{Mor}_k^{\mathrm{odd}}(X_\lambda, E).$$

Le problème devient donc :

Trouver « beaucoup » de $\lambda \in k$ tels que tout morphisme impair $X_\lambda \to E$ se factorise en

$$X_\lambda \xrightarrow{\varphi_\lambda} E \xrightarrow{v} E$$

pour un certain v.

Remarque : c'est un problème géométrique sur k (et plus sur K).

Traduction en termes de jacobiennes :

la définition de X_λ donne un morphisme de variétés abéliennes

$$i_\lambda : \quad \mathrm{Jac}\,(C) \times E \longrightarrow J_\lambda := \mathrm{Jac}\,(X_\lambda)$$

et il suffit de

trouver « beaucoup » de $\lambda \in k$ tels que tout morphisme $E \to J_\lambda$ de variétés abéliennes se factorise par i_λ.

Les X_λ sont les fibres d'un « pinceau de courbes »

$$C \times E \cdots \to \mathbb{P}^1_k$$

et J_λ est la fibre en λ d'un schéma abélien $J \to U$, où U est un ouvert de $\mathbb{P}^1_k$. Il s'agit de voir comment le groupe $\mathrm{Hom}_k(E, J_\lambda)$ varie avec λ.

Les X_λ sont les fibres d'un « pinceau de courbes »

$$C \times E \cdots \to \mathbb{P}^1_k$$

et J_λ est la fibre en λ d'un schéma abélien $J \to U$, où U est un ouvert de $\mathbb{P}^1_k$. Il s'agit de voir comment le groupe $\mathrm{Hom}_k(E, J_\lambda)$ varie avec λ.

Pour simplifier, on suppose désormais que

k est de type fini sur $\mathbb{Q}$.

Théorème (R. Noot) :

Soit k une extension de type fini de $\mathbb{Q}$.

Soient A, B deux schémas abéliens sur $U \subset \mathbb{P}^1_k$ (ouvert dense de point générique η).

Alors l'homomorphisme naturel de spécialisation

$$\mathrm{sp}_\lambda : \mathrm{Hom}_\eta(A_\eta, B_\eta) \longrightarrow \mathrm{Hom}_k(A_\lambda, B_\lambda)$$

est un isomorphisme pour tout λ dans un sous-ensemble hilbertien de $U(k)$.

Ceci entraîne notre théorème :

on prend $A = E_U$ (courbe elliptique constante sur U), $B = J$ (la famille des jacobiennes des X_λ). On obtient :

pour « beaucoup » de λ, le groupe $\mathrm{Hom}_k(E, J_\lambda)$ est égal au groupe « générique » $\mathrm{Hom}_\eta(E_\eta, J_\eta)$.

Ceci entraîne notre théorème :

on prend $A = E_U$ (courbe elliptique constante sur U), $B = J$ (la famille des jacobiennes des X_λ). On obtient :

pour « beaucoup » de λ, le groupe $\mathrm{Hom}_k(E, J_\lambda)$ est égal au groupe « générique » $\mathrm{Hom}_\eta(E_\eta, J_\eta)$.

Or ce groupe générique n'est autre que $\mathrm{Hom}_k(E, \mathrm{Jac}\,(C) \times E)$ (le point est que $\mathrm{Jac}\,(C) \times E$ est la « partie fixe » du schéma abélien $J \to U$).

Le théorème de Noot utilise :

– la conjecture de Tate pour les variétés abéliennes sur k et η (démontrée par Faltings),
– un « théorème d'irréductibilité de Hilbert pour les extensions infinies » dû à Serre.