Indécidabilité du 10^{eme} problème de Hilbert

Benjamin Hellouin

Matiassevitch 1 & 5.4

Définition 1. *Un ensemble $E \subset \mathbb{N}$ est dit* diophantien *si $\exists P \in \mathbb{Z}[X_0 \dots X_n], a \in E \Leftrightarrow P(a, x_1 \dots x_n) = 0$ admet une solution en $x_1 \dots x_n \in \mathbb{N}$.*

Théorème 1 (Matiiassevitch)**.** *Les ensembles diophantiens sont exactement les ensembles récursivement énumérables (à encodage standard près)*

On prouve que ce résultat implique l'indécidabilité du 10e problème de Hilbert :

Définition 2 (10e problème de Hilbert)**.**

Entrée *$P \in \mathbb{Z}[X_1 \dots X_n]$;*

Sortie *OUI si P admet une racine dans $\mathbb{Z}^n$, NON sinon.*

est récursivement énumérable, non décidable.

Ce problème est clairement récursivement énumérable. $\mathbb{Z}^n$ étant dénombrable, on peut trouver une énumération $\varphi : \mathbb{N} \to \mathbb{Z}^n$ et tester successivement si $P(\varphi(n) = 0, n = 1, 2 \dots$. Si P admet une racine, cet algorithme termine et renvoie le bon résultat.

On fournit une preuve négative en montrant que ces deux problèmes sont équivalents.

Preuve. ($\Leftarrow$) Soit $P \in \mathbb{Z}[X_0, X_1 \dots X_n]$. Puisque tout entier est décomposable en quatre carrés (Lagrange), toute solution positive de l'équation $P(a, x_1 \dots x_n) = 0$ donne au moins une solution relative du système

$$\begin{cases} P(a, x_1 \dots x_n) = 0 \\ x_1 = y_{1,1}^2 + y_{1,2}^2 + y_{1,3}^2 + y_{1,4}^2 \\ \vdots \\ x_n = y_{n,1}^2 + y_{n,2}^2 + y_{n,3}^2 + y_{n,4}^2 \end{cases}$$

Par conséquent, si on peut trouver une solution relative de ce système, on obtient une solution positive à l'équation précédente. Il reste à montrer que ce système peut se réduire à une seule équation. Il suffit de voir que l'équation

$$P(a, x_1 \dots x_n)^2 + (y_{1,1}^2 + y_{1,2}^2 + y_{1,3}^2 + y_{1,4}^2 - x_1)^2 + \dots + (y_{n,1}^2 + y_{n,2}^2 + y_{n,3}^2 + y_{n,4}^2 - x_n)^2$$

a exactement le même ensemble de solutions.

($\Rightarrow$) Soit $P \in \mathbb{Z}[X_1 \dots X_n]$.

Conclusion. On réduit le 10e problème de Hilbert au problème de décider de l'appartenance à un ensemble récursivement énumérable. Soit E un ensemble récursivement énumérable, i.e. diophantien, et P quelque chose. Ce dernier problème se réduit au 10e problème par le lemme 1.