LE THÉORÈME DE MATIYASSÉVITCH ET RÉSULTATS CONNEXES

(M. Margenstern)

L'exposé est consacré aux travaux développés depuis une quinzaine d'années dans la recherche de la solution du dixième problème de Hilbert, à savoir l'existence éventuelle d'une méthode générale permettant de décider si une équation diophantienne admet ou non des solutions.

Les travaux de PUTNAM, DAVIS et J. ROBINSON ont abouti à une approche de la solution que MATIYASSÉVITCH a conduit à son terme en 1970. La réponse négative au dixième problème se fonde sur un résultat très important et tout à fait surprenant puisqu'il établit l'identité de deux notions qui appartiennent à des domaines mathématiques a priori fort éloignés : la logique mathématique et la théorie des nombres.

Cet exposé est en principe "self-contained". Il comprend trois parties. Dans la première relativement technique, on donne une démonstration (dûe pour l'essentiel à MATIYASSÉVITCH) du théorème principal sur l'équivalence entre les ensembles diophantiens et les ensembles récursivement énumérables.

Dans la seconde partie, on cherche à donner au lecteur, en s'appuyant sur des exemples célèbres, une idée de l'étendue du champ

des problèmes intéressants qui peuvent être réduits à la détermination de la solubilité ou de l'insolubilité d'une équation diophantienne. On indique également quelques unes des méthodes utilisées pour obtenir cette réduction.

Dans la troisième partie, on aborde l'étude du dixième problème de Hilbert sur d'autres ensembles de nombres que $\mathbb{N}$.

I. Le théorème principal.

Le but de cette première partie est de démontrer que tout ensemble récursivement énumérable est diophantien.

Le plan de la démonstration se décompose en deux étapes :

- tout d'abord on démontre que tout ensemble récursivement énumérable est exponentiellement diophantien,
- puis on démontre que tout ensemble exponentiellement diophantien est diophantien, en montrant que le graphe de l'exponentielle est diophantien.

Seule la seconde étape de la démonstration fait appel à des résultats assez fin d'arithmétique. Nous les indiquerons et les démontrerons à ce moment là.

Dans la suite de l'exposé, on appellera entiers positifs, les éléments de $\mathbb{N}^* = \mathbb{N}\setminus\{0\}$, les éléments de $\mathbb{N}$ étant appelés entiers naturels.

Donnons quelques définitions préliminaires :

Soit $\mathcal{S}$ une partie de $(\mathbb{N}^*)^k$. On dit que $\mathcal{S}$ est diophantienne si on peut trouver un entier n et un polynôme P dans $\mathbb{Z}[X_1,\ldots,X_k, Y_1,\ldots,Y_n]$ tels que :

$(a_1,\ldots,a_k) \in \mathcal{S} \iff \exists y_1,\ldots,y_n \in \mathbb{N}^* \quad P(a_1,\ldots,a_k, y_1,\ldots,y_n) = 0$.

Les symboles $a_1\ldots a_k$ sont appelés les paramètres de P et $y_1,\ldots,y_n$ les inconnues. Notons que la restriction des valeurs des inconnues aux entiers positifs est introduite pour la commodité des

calculs et de l'exposé et n'altère en rien la généralité. En effet : $P(x) = 0$ a des solutions dans $\mathbb{N}$ ssi $P(x_1^2 + x_2^2 + x_3^2 + x_4^2) = 0$ a des solutions dans $\mathbb{Z}$ (tout entier naturel est somme de quatre carrés), $P(x) = 0$ a des solutions dans $\mathbb{N}^*$ ssi $P(x+1) = 0$ a des solutions dans $\mathbb{N}$ et $P(x) = 0$ a des solutions dans $\mathbb{Z}$ ssi $P(x)P(0)P(-x) = 0$ a des solutions dans $\mathbb{N}^*$.

Enfin nous dirons qu'une relation sur des entiers positifs est diophantienne ssi son graphe est un ensemble diophantien.

Définissons les ensembles exponentiellement diophantiens :

On définit les <u>monômes exponentiels en</u> $X_1,\ldots,X_k$ de la façon suivante :

ce sont les expressions de la forme

$$ab^{\Theta}X_1^{\Xi_1}\ldots X_k^{\Xi_k}$$

où a,b sont des entiers naturels, Θ l'entier naturel 0 ou la variable X_i, Ξ_i un entier naturel ou une des variables $X_1,\ldots,X_k$. On convient de poser $X_i^0 = 1$ et de considérer que le produit des $X_i^{\Xi_i}$ entre eux est commutatif.

On appelle <u>polynôme exponentiel en</u> $X_1,\ldots,X_k$ (ou à k <u>variables</u>) toute somme finie de monômes exponentiels en $X_1,\ldots,X_k$.

Un ensemble $\mathcal{E}$ de $(\mathbb{N}^*)^k$ est dit <u>exponentiellement diophantien</u> s'il existe un entier n et un polynôme exponentiel P en $X_1,\ldots,X_k, Y_1,\ldots,Y_n$ tel que :

$$(a_1,\ldots,a_k) \in \mathcal{E} \Longleftrightarrow \exists y_1,\ldots,y_n \in \mathbb{N}^* \quad P(a_1,\ldots,a_k, y_1,\ldots,y_n) = 0 .$$

De même on dit qu'une relation est exponentiellement diophantienne ssi son graphe l'est.

1. <u>Représentation exponentiellement diophantienne des ensembles récursivement énumérables</u>.

La démonstration que nous exposons ici reprend la démonstration récente de Matiyassévitch dans [3]. Elle ne fait pratiquement pas

appel à l'arithmétique. En particulier, elle permet de court-circuiter les constructions complexes fondées sur le théorème chinois et sa représentation diophantienne.

Elle se fonde sur la simulation du fonctionnement d'une machine de Turing par un nombre fini de relations exponentiellement diophantiennes. Ce qui est suffisant puisqu'on sait que les fonctions récursives partielles sont exactement les fonctions définissables par une machine de Turing (cf. Par exemple [11]).

Diverses présentations équivalentes des machines de Turing existent dans la littérature. Pour des raisons techniques, nous prendrons la présentation suivante (cf. Matiyassévitch [3]), qui consiste en quelque sorte à décrire une machine de Turing par un semi-système de Thue.

1.1 Machines de Turing.

La machine est constituée d'une mémoire infinie représentée par une bande illimitée à droite divisée en cases. La case la plus à gauche dite première case est marquée par le signe * qui ne peut être effacé ni écrit dans une autre case. Chaque case en dehors de la première contient une des lettres de l'alphabet fini $A = \{a_o,\ldots,a_n\}$ (on suppose $a_i \neq *$). On conviendra d'appeler case vide tout case contenant a_o. Au départ, toutes les cases de la mémoire, sauf un nombre fini d'entre elles sont vides. La machine dispose d'un nombre fini d'états désignés par $E_o,\ldots,E_m$, E_1 étant l'état de départ et E_o l'état d'arrêt de la machine.

La machine transforme le mot écrit au départ sur la bande par étapes où elle n'effectue qu'une opération dans une seule case, appelée case vue, qui consiste à remplacer la lettre figurant dans la case vue par une autre. Puis la machine passe à une des cases adjacentes à la case vue. Elle effectue ces deux opérations selon des instructions en nombre fini que l'on peut représenter de la façon suivante :

$$E_i \; a \rightarrow b \; E_j \; U \qquad (1)$$

Où a et b désignent un des symboles $a_o,\ldots,a_n,*$, et U désigne une des deux lettres G,D (à gauche, à droite) avec la condition : si $a = *$ alors $b = *$ et $U = D$. $E_i \; a$ est appelé <u>couple d'entrée</u> et $b \; E_j \; U$, <u>triplet de sortie</u>.

En vue d'arithmétiser le fonctionnement de la machine de Turing considérée, on ne s'intéressera qu'aux <u>configurations</u> de la machine qui, par définition, représentent l'état de la bande après chaque pas du travail de la machine. Afin de faire apparaître la case vue et l'état de la machine au pas considéré, on introduit de nouvelles lettres pour représenter les états : $\vec{E}_o,\ldots,\vec{E}_m$, $\overleftarrow{E}_o,\ldots,\overleftarrow{E}_m$ (cf. [3]). Les configurations seront des mots de la forme :

$$* \; \Delta \; \vec{E}_i \; \Xi \qquad (2a)$$

$$* \; \Delta \; \overleftarrow{E}_i \; \Xi \qquad (2b)$$

où Δ et Ξ sont des mots dans A (éventuellement vides), étant entendu que les cases à droite de Ξ sont vides. Dans la configuration (2a), la case vue est celle qui contient la première lettre du mot Ξ (ou la première case vue à droite du mot Δ si le mot Ξ est vide) et dans (2b) la case vue est celle qui contient la dernière lettre du mot Δ (ou la première case si le mot Δ est vide), la machine se trouvant dans l'état E_i .

Le passage d'une configuration à la configuration suivante se présente comme le passage d'un mot à un autre dans un calcul formel par l'application d'une des règles de la forme :

$$\vec{E}_i \; a \rightarrow \overleftarrow{E}_j \; b \qquad (3a)$$

$$a \; \overleftarrow{E}_i \rightarrow \overleftarrow{E}_j \; b \qquad (3b)$$

$$\vec{E}_i \; a \rightarrow b \; \vec{E}_j \qquad (3c)$$

$$a \; \overleftarrow{E}_i \rightarrow b \; \vec{E}_j \qquad (3d)$$

où $a,b \neq *$ dans (3a), (3b), (3c) et, dans (3d), si $a = *$, alors

$b = *$. Les règles (3a) à (3d) découlent des instructions (1). Par exemple, l'instruction

$$E_i \; a \rightarrow b \; E_j \; D$$

donne naissance à deux règles :

$$\vec{E}_i \; a \rightarrow b \; \vec{E}_j$$
$$a \; \overleftarrow{E}_i \rightarrow b \; \vec{E}_j$$

suivant le sens du mouvement de la machine au pas précédent la case vue.

Le programme de la machine, constitué par la liste des instructions, peut être représenté par une liste de ℓ règles :

$$L_i M_i \rightarrow S_i T_i \qquad (4)$$

où $L_i , M_i , S_i , T_i \in \{a_o,\ldots,a_n , \vec{E}_o,\ldots,\vec{E}_m , \overleftarrow{E}_o,\ldots,\overleftarrow{E}_m , *\}$.

Considérons maintenant une machine de Turing $\mathbb{K}$ et un mot M . On dit que la machine converge en M s'il existe un entier s tel que l'état E_o apparaisse au $s^{\text{ième}}$ pas du travail de la machine pour la configuration initiale $* \overleftarrow{E}_1 M$. Il est clair que le travail de la machine $\mathbb{K}$ s'arrête au bout de s pas si et seulement si il existe des mots Z et W et une suite $K_o,\ldots,K_s$ de configurations telles que :

(i) Z ne contient que la lettre a_o ;

(ii) $K_o = * \overleftarrow{E}_1 M \; Z$, K_i s'obtient à partir de K_{i-1} par une des règles (4) pour $i = 1,\ldots,s$ et $K_s = W$;

(iii) W contient $\vec{E}_o$ ou $\overleftarrow{E}_o$.

Il est malcommode de représenter, arithmétiquement, une liste de mots de longueur arbitraire. Aussi peut-on remplacer la suite des configurations $K_1,\ldots,K_{s-1}$ par un seul mot : $L = K_1,\ldots,K_{s-1}$. On remarque que chacun des K_i commence par le signe $*$ qui n'est présenté qu'une fois dans une configuration, et les K_i ont la même longueur. Ceci permet de remplacer la condition (ii) par :

(ii*) LW s'obtient à partir de K_oL par la substitution simultanée de toutes les occurrences des mots de la forme L_iM_i par ceux de la forme S_iT_i . Cela se vérifie sans difficulté par le fait que cette opération transforme K_o en K_1 , K_1 en K_2 , etc... K_{s-1} en $K_s = W$.

Cela permet aussi de ne plus faire figurer l'entier s .

Il nous reste encore une étape avant de passer à l'arithmétisation : ramener la transformation des mots L_iM_i en S_iT_i à une transformation portant seulement sur des lettres. Pour cela, on remarque qu'il y a ℓ règles (4). Construisons 2ℓ lettres $B_1,\ldots,B_\ell$, $C_1,\ldots,C_\ell$. Soit P le mot obtenu à partir de K_oL par les règles :

$$L_iM_i \rightarrow B_iC_i \qquad (5a)$$

Alors LW s'obtient à partir de P par les règles

$$B_iC_i \rightarrow S_iT_i \qquad (5b)$$

Mais on peut considérer également que K_oL s'obtient à partir de P par les règles

$$B_iC_i \rightarrow L_iM_i \qquad (5c)$$

Remarquons qu'on peut décomposer les règles (5b) et (5c) en :

$$B_i \rightarrow S_i \quad C_i \rightarrow T_i \qquad (6a)$$

$$B_i \rightarrow L_i \quad C_i \rightarrow M_i \qquad (6b)$$

Car chaque occurence de B_i est suivie de C_i et chaque occurence de C_i précédée de B_i . Précisons cette relation : on dit que dans le mot N , la lettre d est <u>l'ombre</u> de la lettre c si chaque occurence de c est suivie de d et si chaque occurence de d est précédée de c . On note cette relation $Sh(N,c,d)$. Et donc P se déduit de K_oL par les règles (5a) ssi M_i est l'ombre de L_i dans P et K_oL se déduit alors de P par les règles (6b). On note le résultat de la substitution de c par d dans N par $Sub(N,c,d)$.

Alors (cf. [3]) la machine $\mathbb{K}$ converge en M si et seulement si il existe des mots Z, L, W et P dans l'alphabet $A_1 = A \cup \{\vec{E}_o,\ldots,\vec{E}_m, \overleftarrow{E}_o,\ldots,\overleftarrow{E}_m\} \cup \{B_1,\ldots,B_\ell, C_1,\ldots,C_\ell\} \cup \{*\}$ tels que

$$(I)\quad \begin{cases} \text{(i)} & Z \text{ ne contient que la lettre } a_o \\ \text{(ii)} & P \text{ ne contient aucune des lettres } \vec{E}_o,\ldots,\vec{E}_m,\overleftarrow{E}_o,\ldots,\overleftarrow{E}_m \\ \text{(iii)} & Sh(P,B_i,C_i) \quad i = 1,\ldots,\ell \\ \text{(iv)} & *\overleftarrow{E}_1 M Z L = Sub(..Sub(P,B_1,L_1),C_1,M_1),..B_\ell,L_\ell)C_\ell M_\ell) \\ \text{(v)} & LW = Sub(..Sub(Sub(P,B_1,S_1),C_1,T_1),..B_\ell,S_\ell)C_\ell T_\ell) \\ \text{(vi)} & W \text{ contient } \vec{E}_o \text{ ou } \overleftarrow{E}_o . \end{cases}$$

1.2 Arithmétisation.

Nous allons maintenant coder les mots dans l'alphabet A_1 par des entiers naturels et exprimer les relations I (i) à (vi) par des relations entre les codes des entiers correspondants. Il nous restera alors à établir que les relations entre les codes sont exponentiellement diophantiennes ainsi que la relation unaire "n est le code d'un mot dans A_1".

Considérons donc l'alphabet $A_1 = \{F_1,\ldots,F_k\}$. Suivant [3] on définit le code d'un mot R dans A_1 comme un k+1-uplet d'entiers naturels $<r_o,\ldots r_k>$ où r_o est la longueur du mot R ($r_o = 0$ si R est le mot vide) et les r_j ($j = 1,\ldots,k$) sont définis de la façon suivante : si le mot R est vide, $r_j = 0$, sinon, R s'écrit $Q_{r_o}\ldots Q_1$ et on pose :

$$\chi_{ij} = \begin{cases} 1 & \text{si } Q_i = F_j \\ 0 & \text{si } Q_i \neq F_j \end{cases}$$

et $r_j = \sum_{i=1}^{r_o} \chi_{ij}\, 2^{i-1}$, de sorte que si on écrit r_j en base 2, on obtient "la fonction caractéristique" des occurences de F_j dans le mot R.

Il est clair que l'on peut reconstruire le mot R à partir de son code de façon univoque.

On établit sans difficulté que si R et S sont des mots dans A_1 de codes respectifs $<r_o,r_1,\ldots r_k>$, $<s_o,s_1,\ldots,s_k>$, alors $R=S$ ssi $r_i = s_i$ pour $i = 0,\ldots,k$ et RS a pour code $<r_o+s_o\ ,\ r_1 2^{s_o} + s_1,\ldots,r_k 2^{s_o} + s_k>$. Si $<r_o,r_1,\ldots r_k>$ est le code du mot R, le code de $Sub(R,F_i,F_j)$, où $i \neq j$, est le $k+1$-uplet $<r'_o,r'_1,\ldots,r'_k>$ où $r'_o = r_o$, $r'_i = 0$, $r'_j = r_j + r_i$, $r'_h = r_h$ pour $h \neq i,j$ et on a $Sh(R,F_i,F_j)$ si et seulement si $r_j = 2r_i$. R ne contient que la lettre F_i si et seulement si $r_i = 2^{r_o}-1$ et R contient F_i ou F_j si et seulement si $r_i + r_j > 0$ et R ne contient pas les lettres $F_{i_1},\ldots,F_{i_h}$ ssi $r_{i_1}^2 + \ldots + r_{i_h}^2 = 0$. Il reste à exprimer que "le $k+1$-uplet $<r_o,r_1,\ldots,r_k>$ est le code d'un mot R dans A_1". Soient x et y deux entiers naturels, $\alpha_1,\ldots,\alpha_q$ et $\beta_1,\ldots,\beta_r$ respectivement les chiffres de la représentation binaire de ces entiers. On a donc : $x = \sum_{i=1}^{q} \alpha_i 2^{i-1}$ et $y = \sum_{i=1}^{r} \beta_i 2^{i-1}$. Il est clair qu'on a $\alpha_i, \beta_j \in \{0,1\}$ et qu'on peut supposer $r = q$ en ajoutant éventuellement un nombre convenable d'α_i ou de β_i nuls. On dira que x et y sont <u>compatibles</u> et on le notera $x\,C\,y$ si et seulement si $\alpha_i + \beta_i \in \{0,1\}$ pour $i = 1,\ldots,r$. C'est-à-dire les 1 dans l'écriture binaire de x et de y ne doivent pas se trouver aux mêmes places. Il est alors clair que $<r_o,r_1,\ldots r_k>$ est le code d'un mot R dans A_1 si et seulement si

$$\Big[\bigwedge_{1\leqslant i<j\leqslant k} r_i\,C\,r_j\Big] \;\&\; \big[r_1+\ldots+r_k = 2^{r_o}-1\big] \qquad (7)$$

Il est clair, d'après le codage utilisé que les relations associées aux relations I(i) (ii) sont exponentiellement diophantiennes. Il nous reste à démontrer que la relation (7) est également exponentiellement diophantienne.

Remarquons tout d'abord que si R_1 et R_2 sont des relations (exponentiellement) diophantiennes, exprimées par les polynômes

(exponentiels) P_1 et P_2 respectivement, alors $R_1 \& R_2$ est exprimée par le polynôme (exponentiel) $P_1^2 + P_2^2$. Donc il suffit de montrer que la relation $x\,C\,y$ est exponentiellement diophantienne. Pour cela, on va établir que :

$$x\,C\,y \Longleftrightarrow \binom{x+y}{x} \equiv 1 \pmod 2 \quad \text{(avec la convention } \binom{0}{0} = 1\text{)} \qquad (8)$$

et que $c = \binom{n}{k}$ est une relation exponentiellement diophantienne.

Le résultat s'en suivra, car : $n \equiv q \pmod m$ $m > 0$ et $n \geqslant q$ si il existe un entier positif u tel que $n-q = (u-1)m$.

Pour établir (8), nous procéderons comme suit :
soit $x = \sum_{i=1}^{s} \alpha_i 2^{i-1}$ $y = \sum_{i=1}^{s} \beta_i 2^{i-1}$ et $x+y = \sum_{i=1}^{s} \gamma_i 2^{i-1}$ où $\alpha_i, \beta_i, \gamma_i \in \{0,1\}$ et s choisi de telle sorte que $\gamma_s \neq 0$. Suivant [10], nous désignerons par $E(n)$ l'exposant de la plus grande puissance de 2 qui divise l'entier naturel n (avec $E(0) = +\infty$). On remarque que E est additive, c'est-à-dire que pour tous entiers naturels n et m, $E(nm) = E(n) + E(m)$. Alors, comme

$$(2^m)! = 2^m.(2^m-1).(2^m-2)\ldots 2^k.(2^k-1)(2^k-2)\ldots 4.3.2 .$$

$$\begin{aligned} \text{Donc } E((2^m)!) &= E(2^m.(2^m-2)\ldots 2^k.(2^k-2)\ldots 4.2) = \\ &= E(2.2^{m-1}.2.(2^{m-1}-1)\ldots 2.2^{k-1}.2.(2^{k-1}-1)\ldots 2.2.2.1) = \\ &= E((2^{m-1})!) + 2^{m-1} \end{aligned}$$

et donc, par sommation $E((2^m)!) = 2^m - 1$.

Par ailleurs, si $n = 2^m + n_1$ avec $n_1 < 2^m$, on a $E(n) = E(n_1)$ et donc, comme $n! = (2^m+n_1)(2^m+n_1-1)\ldots(2^m+n_1-n_1+1)(2^m)!$ on a :

$$E(n!) = E((2^m)!) + E(n_1.(n_1-1)\ldots 1) = E((2^m)!) + E(n_1!) .$$

Il en résulte que (cf. [10]) : $E(x!) = \sum_{i=1}^{s} \alpha_i (2^i - 1) = x - \sum_{i=1}^{s} \alpha_i$ et par conséquent, comme

$$E(\binom{x+y}{x}) = E((x+y)!) - E(x!) - E(y!)$$

on a (cf. [10]) : $E(\binom{x+y}{x}) = \sum_{i=1}^{s} (\alpha_i + \beta_i - \gamma_i)$.

En outre $\binom{x+y}{x} \equiv 1 \pmod 2$ équivaut à $E(\binom{x+y}{x}) = 0$. On démontre par récurrence sur s que $\sum_{i=1}^{s} (\alpha_i+\beta_i-\gamma_i) = 0$ si et seulement si $\alpha_i+\beta_i = \gamma_i$ pour $i = 1,\ldots,s$. Pour cela, on établit qu'il existe un plus petit indice i_o pour lequel $\alpha_{i_o}+\beta_{i_o}-\gamma_{i_o} = -1$ si et seulement si on trouve un plus petit indice j_o avec $j_o < i_o$ pour lequel $\alpha_{j_o}+\beta_{j_o}-\gamma_{j_o} = 2$ et qu'alors $\sum_{i=1}^{i_o} (\alpha_i+\beta_i-\gamma_i) \geqslant 1$. Or $\alpha_i+\beta_i = \gamma_i$ si et seulement si $\alpha_i+\beta_i \in \{0,1\}$ pour $i = 1,\ldots,s$, c'est-à-dire $x \mathrel{C} y$, ce qui établit (8).

Il reste à montrer que $c = \binom{n}{k}$ est une relation exponentiellement diophantienne. Pour cela, on remarque (cf. [3], [7]), que

$$\text{si } u > 2^n \text{ , alors } \binom{n}{k} = \text{Rés}\left(\left[\frac{(u+1)^n}{u^k}\right], u\right) \qquad (9)$$

où $[\frac{p}{q}]$ est la partie entière du rationnel $\frac{p}{q}$ et $\text{Rés}(a,b)$ désigne le reste de la division de a par b . En effet, comme $u > 2^n$ et que $2^n = \sum_{j=o}^{n} \binom{n}{j} > \binom{n}{k}$, on a que $\left[\frac{(u+1)^n}{u^k}\right] = \binom{n}{k} + u \sum_{j=k+1}^{n} \binom{n}{j} u^{j-1}$ puisque $\frac{1}{u^k} \sum_{j=o}^{k-1} \binom{n}{j} u^j \leqslant \frac{1}{u} \sum_{j=o}^{k-1} \binom{n}{j} \leqslant \frac{2^n}{u} < 1$. Mais alors, comme $\binom{n}{k} \leqslant 2^n < u$, on a bien (9). Or, $c = \text{Rés}(a,b)$ si et seulement si il existe des entiers positifs v et w tels que $a = bv+c$ et $b = c+w$.

Nous avons donc démontré que la relation (7) est exponentiellement diophantienne. C'est-à-dire qu'il existe un entier r et un polynôme exponentiel Π en $X_o, X_1, \ldots, X_k$, $Y_1, \ldots, Y_r$ tel que :

" $< r_o, r_1, \ldots, r_k >$ est le code d'un mot dans A_1 "

$\Longleftrightarrow \exists y_1 \ldots y_r \ \Pi(r_o, r_1, \ldots, r_k, y_1, \ldots, y_r) = 0$.

Par conséquent, "la machine $\mathbb{K}$ converge en M" est une relation exponentiellement diophantienne.

Or on sait que tout ensemble récursivement énumérable est le domaine de convergence d'une machine de Turing. La démonstration indiquée ci-dessus est effective en ce sens qu'elle construit les relations exponentiellement diophantiennes exprimant la convergence de la machine $\mathbb{K}$ en M d'une façon uniforme (par rapport à la machine $\mathbb{K}$ et au mot M). On peut donc énoncer le

Théorème 1 : La classe des ensembles récursivement énumérables est identique à celle des ensembles exponentiellement diophantiens. De plus il existe un algorithme transformant tout code d'un ensemble récursivement énumérable $\mathcal{E}$ en un polynôme exponentiel définissant un ensemble exponentiellement diophantien égal à $\mathcal{E}$.

2. Représentation diophantienne du graphe de l'exponentielle.

L'objet de ce paragraphe est de démontrer le

Théorème 2 [Matiyassévitch] : La relation $c = a^b$ est diophantienne.

Il résulte aussitôt de ce théorème et du théorème 2 qu'on a le

Théorème principal : La classe des ensembles récursivement énumérables est identique à celle des ensembles diophantiens. De plus il existe un algorithme transformant tout code d'un ensemble récursivement énumérable $\mathcal{E}$ en un polynôme définissant un ensemble diophantien égal à $\mathcal{E}$.

Démonstration : Il suffit de remarquer que l'algorithme de recherche des solutions de $P(a_1,\ldots,a_k, y_1,\ldots,y_n) = 0$ est descriptible par une machine de Turing : la procédure consistant à calculer les valeurs de $P(a_1,\ldots,a_k, y_1,\ldots,y_n)$ par récurrence sur $|y_1|+\ldots+|y_n|$ est parfaitement effective et montre que l'ensemble $\mathcal{E}$ défini par : $<a_1,\ldots,a_k> \in \mathcal{E} \Longleftrightarrow \exists y_1\ldots y_n\ P(a_1,\ldots,a_k, y_1,\ldots,y_n) = 0$ est récursivement énumérable, puisqu'il est le domaine de convergence d'une machine de Turing. ■

Passons à la démonstration du théorème 2. Nous suivrons à cet effet la démonstration exposée par Matiyassévitch et J. Robinson dans [6] qui se décompose en deux étapes : tout d'abord on établit le caractère diophantien d'une certaine suite de "taille exponentielle" c'est-à-dire qui croît aussi vite que l'exponentielle, puis on ramène le cas de l'exponentielle elle-même à celui de cette suite.

La suite utilisée dans [6] est la suite de Lucas, c'est-à-dire, la suite constituée par les solutions en y de l'équation de Pell $x^2-dy^2 = 1$ pour des valeurs de d positives et différentes d'un carré. Aussi commencerons nous par introduire quelques notations et à énoncer les résultats concernant les solutions en y de l'équation de Pell et leur relation avec l'exponentielle que nous utiliserons par la suite.

2.1 Résultats préliminaires.

Notons tout d'abord qu'une relation $\mathcal{R}$ sur $(\mathbb{N}^*)^k$ est diophantienne si et seulement si on peut trouver des entiers n et m et m polynômes $P_1,\ldots,P_m$ avec $P_i \in \mathbb{Z}(X_1,\ldots,X_k, Y_1,\ldots,Y_n)$ tels que

$$\mathcal{R}(a_1,\ldots,a_k) \Longleftrightarrow \text{le système } \begin{cases} P_1(a_1,\ldots,a_k, y_1,\ldots,y_n) = 0 \\ \cdots\cdots \\ P_m(a_1,\ldots,a_k, y_1,\ldots,y_n) = 0 \end{cases} \text{admet une solution}$$

Les équations de ce système sont dites diophantiennes.

En effet, $P_1 = 0 \,\&\ldots\&\, P_m = 0 \Longleftrightarrow P_1^2+\ldots+P_m^2 = 0$.

Ainsi nous représenterons l'exponentielle à l'aide d'un système d'équations diophantiennes pour établir le théorème 2.

Rappelons que $(n,m) = 1$ signifie que les entiers n et m sont premiers entre eux. Nous noterons $x = \square$ au lieu de $x = k^2$ avec $k > 0$ (on dira : x est un carré).

2.1.1 Résultats sur les solutions de l'équation de Pell.

Considérons l'équation de Pell $x^2-dy^2 = 1$. Si d est un carré, la seule solution est $x = 1$ et $y = 0$. Si $d = 0$ les solutions sont $x = 1$ et $y = 0,1,\ldots,n,\ldots$. Dans la suite, on considérera les équations de la forme

$$x^2 - (a^2-1)y^2 = 1 \qquad \text{où} \quad a > 1 \ . \tag{1}$$

Nous allons montrer que l'ensemble des solutions (x,y) de (1) avec $x,y > 0$ peut être ordonné en une suite strictement croissante suivant y .

Comme il est d'usage de le faire, on utilisera le langage de la théorie algébrique des nombres pour faciliter l'exposé.

On dira qu'une solution (x,y) de l'équation (1) est <u>positive</u> si et seulement si $x>0$ et $y>0$. A toute solution (α,β) de (1) on associe le nombre $\alpha+\beta\sqrt{a^2-1}$ qui est une unité de l'anneau $\mathbb{Z}[\sqrt{a^2-1}]$. Si $\xi=u+v\sqrt{a^2-1} \in \mathbb{Z}[\sqrt{a^2-1}]$, on lui associe son conjugué $\bar{\xi} = u-v\sqrt{a^2-1}$ et sa norme $N(\xi) = \xi\bar{\xi} = u^2-v^2(a^2-1)$. Les unités de $\mathbb{Z}[\sqrt{a^2-1}]$ sont les éléments de norme $+1$ ou -1. Les solutions de l'équation (1) sont exactement les unités de norme 1. La norme étant multiplicative et comme pour $\xi \neq 0$ $\xi^{-1} = \frac{\bar{\xi}}{N(\xi)}$, les unités de norme 1 constituent un sous-groupe du groupe U des unités de l'anneau.

Soit U_p l'ensemble des solutions positives de (1). On peut l'identifier à l'ensemble des unités de $\mathbb{Z}[\sqrt{a^2-1}]$ plus grandes strictement que 1 car :

pour $\alpha,\beta \in \mathbb{Z}$ $\quad \alpha+\beta\sqrt{a^2-1} \in U \Longrightarrow (\alpha+\beta\sqrt{a^2-1} > 1 \Longleftrightarrow \alpha$ et $\beta>0)$.

En effet : $\alpha^2 = 1+\beta^2(a^2-1) \Longrightarrow |\alpha| > |\beta|\sqrt{a^2-1}$. Comme $\alpha^2-\beta^2(a^2-1)=1$, un seul des quatre nombres $|\alpha|+|\beta|\sqrt{a^2-1}$, $|\alpha|-|\beta|\sqrt{a^2-1}$, $-|\alpha|+|\beta|\sqrt{a^2-1}$, $-|\alpha|-|\beta|\sqrt{a^2-1}$ est strictement plus grand que 1. C'est donc $|\alpha|+|\beta|\sqrt{a^2-1}$.

Montrons que U_p a un plus petit élément.

On remarque que $u-u^{-1}$ est une fonction strictement croissante de u pour $u>1$ et pour $u \in U_p$, avec $u = x+y\sqrt{a^2-1}$, $u^{-1} = x-y\sqrt{a^2-1}$ on a : $u-u^{-1} = 2y\sqrt{a^2-1}$. Donc pour $x,y,x',y' \in \mathbb{N}^*$ on a : $x+y\sqrt{a^2-1} \leqslant x'+y'\sqrt{a^2-1} \Longleftrightarrow y \leqslant y'$. Or $(a,1)$ est visiblement une solution positive de (1) et c'est la plus petite puisque $(x,y) \in U_p \Longrightarrow y \geqslant 1$. D'où :

<u>Proposition</u> 1 : L'ensemble des solutions positives de (1) a un plus petit élément $(a,1)$ (ou $a+\sqrt{a^2-1}$).

Cet élément est appelé unité fondamentale de l'anneau $\mathbb{Z}[\sqrt{a^2-1}]$ lorsqu'il n'y a pas d'unité de norme négative.

De la proposition 1 on tire la

Proposition 2. L'ensemble des solutions positives de (1) est constitué par les nombres $(x_a(n),y_a(n))$ définis par la relation

$$(a+\sqrt{a^2-1})^n = x_a(n) + y_a(n)\sqrt{a^2-1} \qquad n \geqslant 1 . \qquad (2)$$

On remarque que pour $n=0$ on trouve $x_a(0) = 1 \quad y_a(0) = 0$ qui est évidemment solution de (1).

Démonstration de la proposition 2 : Soit $u \in U_p$, et soit $\omega = a+\sqrt{a^2-1}$. Il existe un entier n unique, $n \geqslant 0$ tel que $\omega^n < u \leqslant \omega^{n+1}$. Alors $1 < u\omega^{-n} \leqslant \omega$. Donc $u\omega^{-n} \in U_p$ (première inégalité) et $u\omega^{-n} = \omega$ car ω est le plus petit élément de U_p. Donc $u = \omega^{n+1}$. ▲

On utilisera dans la suite les résultats suivants (cf. [6]).

Proposition 3. Soit $a > 0$. Pour tout entier positif m il existe une infinité de n tels que $m \mid y_a(n)$.

Démonstration : D'après (2) il vient que $y_a(2n) = 2x_a(n).y_a(n)$. Donc il suffit de trouver un n tel que $m \mid y_a(n)$.

Pour cela on utilisera, en l'appliquant à $d = (a^2-1)m^2$, le

Lemme : L'équation de Pell $x^2-dy^2 = 1$ où $d \in \mathbb{Z}$, d non carré, admet au moins une solution (x,y) positive.

Démonstration du lemme : On montre tout d'abord qu'il existe une infinité de $(x,y) \in \mathbb{N}^2$ avec $y \neq 0$ t.q. $|x^2-dy^2| < 1+2\sqrt{d}$.

Pour cela, N étant fixé, on pose $y = 0,1,2,\ldots,N$ successivement.

Pour chaque valeur de y, on définit un x unique tel que $y\sqrt{d} \leqslant x < 1+y\sqrt{d}$; comme d n'est pas un carré, $y\sqrt{d} = x$ n'est possible que pour $y = x = 0$. On a ainsi $N+1$ nombres dans $[0,1[$. La distance mutuelle de deux quelconques d'entre eux ne peut être supérieure ou égale à $\frac{1}{N}$, sinon les points extrêmes auraient une distance au moins égale à 1. Donc, par soustraction, on trouve x,y avec

$y>0$, tel que

$$(*) \qquad |x-y\sqrt{d}| < \frac{1}{N} .$$

On a donc $|x-y\sqrt{d}| < \frac{1}{y}$ a fortiori, car $y \leqslant N$. Soit $x-y\sqrt{d} = \frac{\delta}{y}$. On a $|\delta| < 1$ et $\delta \neq 0$ car d n'est pas un carré. Donc $x+y\sqrt{d} = \frac{\delta}{y} + 2y\sqrt{d}$ et donc $x^2-dy^2 = \frac{\delta^2}{y^2} + 2\delta\sqrt{d}$. Comme $|\delta| < 1$ et $y>0$, on a donc :

$$(**) \qquad |x^2-dy^2| < 1+2\sqrt{d} \quad , \quad y>0 .$$

Si on a déjà construit n nombres (x_i,y_i) vérifiant $(**)$, soit N tel que $\frac{1}{N} < |x_i - y_i\sqrt{d}|$, la construction indiquée au début nous donne un $n+1$-ème nombre en vertu de $(*)$.

Soient donc les solutions de $(**)$. D'après le lemme des tiroirs, il existe un entier k avec $|k| < 1+2\sqrt{d}$, telle que l'équation $x^2-dy^2 = k$ ait une infinité de solutions vérifiant $y>0$. Donc, d'après le lemme des tiroirs, il existe p et q tels que

$$(***) \qquad x^2-dy^2 = k \quad x \equiv q \pmod{k} \quad y \equiv p \pmod{k} \quad y \neq 0$$

ait une infinité de solutions. Soient (x,y) et (x',y') des solutions de $(***)$.

Alors : $x'y - xy' \equiv 0 \pmod{k}$ et $xx' - dyy' \equiv x'^2 - dy'^2 \equiv 0 \pmod{k}$.

Donc $(x'-y'\sqrt{d})(x+y\sqrt{d}) = k(\xi+\eta\sqrt{d})$ avec $\xi,\eta \in \mathbb{Z}$.

D'où il vient $\xi^2-d\eta^2 = 1$.

Si $\eta = 0$, $\xi = \pm 1$ d'où $(x'-y'\sqrt{d})(x+y\sqrt{d}) = \pm k$ et donc, en vertu de $(***)$, $x'-y'\sqrt{d} = \pm(x-y\sqrt{d})$ ce qui peut être exclus, puisqu'on a une infinité de solutions à $(***)$. Ce qui donne la solution cherchée. ▲

Proposition 4 : Pour $a>0$ on a $y_a(n) \geqslant n$ pour tout n .

C'est évident en vertu de (2).

Proposition 5 (règle de congruence 1) : Pour $a,b>0$, si $a \equiv b \pmod{m}$, alors, pour tout n , $x_a(n) \equiv x_b(n) \pmod{m}$ et $y_a(n) \equiv y_b(n) \pmod{m}$. En particulier (règle de congruence 2) pour tout n ,

$y_a(n) \equiv n \pmod{a-1}$.

Démonstration : Pour la première règle, on remarque que d'après (2), $x_a(n)$ et $y_a(n)$ sont des polynômes en a à coefficients entiers.

Pour la seconde règle, puisque $(a+\sqrt{a^2-1})^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}(\sqrt{a^2-1})^k$, $y_a(n)\sqrt{a^2-1}$ réunit toutes les puissances impaires de $\sqrt{a^2-1}$. Donc, modulo $a-1$, $y_a(n)$ est congru à la première puissance impaire, c'est-à-dire $y_a(n) \equiv \binom{n}{1} a^{n-1} \pmod{a-1}$. Comme $\binom{n}{1} = n$ et $a \equiv 1 \pmod{a-1}$ on en tire $+ y_a(n) \equiv n \pmod{a-1}$.

Proposition 6 (première réduction) : Pour $a > 0$, si $y_a(m)^2 | y_a(n)$, alors $y_a(m) | n$.

Démonstration : Si $y_a(m)^2 | y_a(n)$ on a donc, d'après (2) que $m \leqslant n$. On remarque en outre, que $y_a(m+k) = y_a(m)x_a(k) + y_a(k)x_a(m)$ donc

$$y_a(m+k) \equiv x_a(m)\, y_a(k) \ [\mathrm{mod}\ y_a(m)]$$

d'où, si $n = mq+r$ avec $0 \leqslant r < m$, on a, par récurrence,

$$y_a(n) \equiv x_a(m)^q y_a(r) \ [\mathrm{mod}\ y_a(m)] .$$

Donc, comme pour tout k $(x_a(k), y_a(k)) = 1$ $(x_a(k)^2 - (a^2-1)y_a^2(k) = 1$ et Bezout), on a $y_a(m)^2 | y_a(n)$ implique $y_a(m) | y_a(n)$. Or y_a est une fonction strictement croissante de n, donc $0 \leqslant r < m \Longrightarrow 0 \leqslant y_a(r) < y_a(m)$ d'où $y_a(r) = 0$ et donc $r = 0$. Donc $y_a(m)^2 | y_a(n) \Longrightarrow m | n$.

Par ailleurs, $y_a(km) = \frac{1}{2\sqrt{a^2-1}} [(x_a(m) + y_a(m)\sqrt{a^2-1})^k$

$$- (x_a(m) - y_a(m)\sqrt{a^2-1})^k] =$$

$$= \sum_{\substack{0 \leqslant j \leqslant k \\ j \text{ impair}}} \binom{k}{j} x_a(m)^{k-j}\, y_a(m)^j (a^2-1)^{\frac{j-1}{2}} .$$

D'où

$$y_a(km) \equiv k x_a(m)^{k-1} y_a(m) \pmod{y_a(m)^3}.$$

Comme $(y_a(m), x_a(m)) = 1$, $y_a(m)^2 | y_a(km) \Longrightarrow y_a(m) | k$ d'où le résultat.

▲

Proposition 7 (seconde réduction) : Pour $a>1$ et $n>0$, si $y_a(i) \equiv y_a(k) \pmod{x_a(n)}$, alors $k \equiv \pm i \pmod{2n}$.

Démonstration : A l'aide de (2), on démontre que les résidus modulo $x_a(n)$ de $y_a(m)$ ont une période égale à $4n$; on a en effet :

$$y_a(4n+\varepsilon m) \equiv -y_a(2n+\varepsilon m) \equiv \varepsilon y_a(m) \pmod{x_a(n)} \qquad \varepsilon = +1 \text{ ou } -1$$

Il reste à montrer que $y_a(m) \not\equiv \pm y_a(m')$ pour $m<m'\leqslant n$. Or si $a>2$, $4y_a(n)^2 < (a^2-1)y_a(n)^2 + 1 = x_a(n)^2$ c-à-d. $y_a(n) < \frac{1}{2}\, x_a(n)$ donc les résidus modulo $x_a(n)$ des $y_a(m)$ sont égaux à $y_a(m)$ pour $m\leqslant n$ et ils sont donc deux à deux distincts. Ces restes sont alors entièrement déterminés (par "symétrie" par rapport au point n) car pour $n\leqslant m\leqslant 2n$ on a :

$$y_a(m) = y_a(2n-(2n-m)) \equiv y_a(2n-m) \pmod{x_a(n)} \quad \text{et} \quad 0\leqslant 2n-m\leqslant n .$$

Il reste à examiner le cas $a=2$ pour achever la démonstration. Dans ce cas, en écrivant que $(2+\sqrt{3})^{n-1} = (2+\sqrt{3})^n(2+\sqrt{3})^{-1} = (2+\sqrt{3})^n(2-\sqrt{3})$ on a : $y_2(n-1) = 2y_2(n) - x_2(n) \geqslant 0$ et $x_2(n-1) = 2x_2(n) - 3y_2(n) = x_2(n) - y_2(n) - y_2(n-1) > 0$ on tire que $\frac{1}{2}x_2(n) \geqslant x_2(n) - y_2(n) > y_2(n-1)$ pour $n>0$. D'où la même conclusion. ■

2.1.2 Comparaison des solutions de l'équation de Pell et de l'exponentielle.

On va maintenant exprimer l'exponentielle en fonction des solutions de l'équation (1). Tout d'abord on établit la

Proposition 8 (majoration des solutions de (1)) : Pour $a>1$ on a, pour tout $n\geqslant 1$

$$(2a-1)^n \leqslant y_a(n+1) \leqslant (2a)^n \qquad (3)$$

Démonstration : On a que $y_a(n+1) = a y_a(n) + x_a(n)$.
Pour $n\geqslant 1$, on a que $(*)$ $x_a(n)^2 = 1 + y_a^2(n)(a^2-1) < 1+a^2\, y_a^2(n)$ donc $x_a(n) \leqslant a y_a(n)$. D'où, pour $n\geqslant 1$: $y_a(n+1) \leqslant 2a\, y_a(n)$.

D'où l'inégalité de droite, par récurrence. Pour l'inégalité de gauche on remarque que pour $a>1$, $x_a(n) \geqslant (a-1)y_a(n)$ (utiliser dans (*) que $a^2-1 \geqslant (a-1)^2$). D'où $y_a(n+1) \geqslant (2a-1)y_a(n)$ d'après (2) et par récurrence, l'inégalité de gauche. ■

Soit λ un nombre réel. On désigne par $<\lambda>$ l'unique entier tel que $|<\lambda> - \lambda| < \frac{1}{2}$, $<\lambda>$ n'étant pas défini pour les nombres de la forme $n+\frac{1}{2}$, $n \in \mathbb{Z}$. On a alors :

Proposition 9 : Soient y , x , n entiers naturels, $y,x>0$ tels que $y = x^n$. Alors si $\ell > 4n(y+1)$, $x^n = <\frac{y_{\ell x}(n+1)}{y_\ell(n+1)}>$.

Démonstration : Soit $\lambda_\ell = \frac{y_{\ell x}(n+1)}{y_\ell(n+1)}$. On remarque sans difficulté, grâce à (3) que $\lambda_\ell \to x^n$ si $\ell \to +\infty$. Soit maintenant $\ell > 4n(y+1)$. On a : $\lambda \leqslant \frac{(2\ell x)^n}{(2\ell-1)^n} = x^n(1-\frac{1}{2\ell})^{-n} \leqslant x^n(1-\frac{n}{2\ell})^{-1} \leqslant x^n(1+\frac{n}{\ell})$ en utilisant (3), et de même, $\lambda \geqslant \frac{(2\ell x-1)^n}{(2\ell)^n} = x^n(1-\frac{1}{2\ell x})^n \geqslant x^n(1-\frac{n}{2\ell x})$,

c'est-à-dire

$$-\frac{nx^{n-1}}{2\ell} \leqslant \lambda - x^n \leqslant \frac{nx^n}{\ell} .$$

Or $nx^n = ny < 2\ell$. Donc $\frac{nx^n}{\ell} < \frac{1}{2}$ d'où $|\lambda - x^n| < \frac{1}{2}$ et donc $<\lambda> = x^n$. ■

2.2 Représentation diophantienne des $y_a(b)$.

Dire qu'il existe a tel que $c = y_a(b)$ est diophantien. Nous allons montrer comment, sachant que $c = y_a(b)$ pour un certain a , calculer cet entier a en résolvant des équations diophantiennes.

Théorème 3 (Matiyassévitch - J. Robinson [6]) : Soient $a>1$, $b>0$, $c>0$. Alors $c = y_a(b)$ si et seulement si il existe des entiers naturels d,e,f,g,h,i,u,v tels que :

A1 $\quad dfi = \square$, $f \mid h-c$, $b \leqslant c$

A2 $\quad d = (a^2-1)c^2+1$

A3 $\quad e = 2(u+1)dc^2$

A4 $\quad f = (a^2-1)e^2+1$

A5 $g = a + f(f-a)$

A6 $h = b + 2vc$

A7 $i = (g^2-1)h^2+1$.

Démonstration (cf. [6]) : a,b,c étant donnés, avec $a>1$, $b,c>0$, supposons qu'il existe des entiers naturels d,e,f,g,h,i,u,v tels que l'on ait A1 - A7 .

1. $d,e,f,g,h,i \geqslant 1$.

En effet : $d \geqslant 1$ par A2 et, par A3, $e>1$ (car $c>0$) et $f \geqslant 1$ par A4. Comme $f \geqslant a$ d'après A4 ($e>0$ d'où $f \geqslant a^2-1+1 \geqslant a$) et $a>1$, donc $g \geqslant 1$ par A5. Comme $b>0$, $h \geqslant 1$ par A6. Comme $g \geqslant 1$ et $h \geqslant 1$, $i \geqslant 1$ par A7.

2. d,f,i sont premiers deux à deux.

En effet, par A4 et Bezout, $(e,f)=1$. Mais par A3, $d|e$, donc $(d,f)=1$. Par A4, $f \equiv 1 \pmod d$ ($d|e$). Donc $g \equiv 1 \pmod d$ donc, par A7, $i \equiv 1 \pmod d$ et donc, par Bezout, $(d,i)=1$. Par A1, $h \equiv c \pmod f$ et $g \equiv a \pmod f$, donc $i \equiv d \pmod f$ par A7 donc $\delta|i,f \Longrightarrow \delta|i,d$ et donc $\delta|1$ puisque $(d,i)=1$. D'où $(i,f)=1$.

3. Il existe p,q,r entiers positifs tels que $c = y_a(p)$, $e = y_a(q)$, $h = y_g(r)$.

En effet, de d,f,i premiers deux à deux et $dfi = \square$, on tire $d=\square$, $f=\square$, $i=\square$ c'est-à-dire, que $(\sqrt{d},c)$, $(\sqrt{f},e)$ et $(\sqrt{i},h)$ sont des solutions de l'équation (1) avec a pour les deux premiers et g pour le troisième couple. Comme, $c,f,h>0$ ce sont des solutions positives, d'où l'existence de p, q et r . On a d'ailleurs également $d = x_a(p)^2$, $f = x_a(q)^2$ et $i = x_g(r)^2$.

4. $b \equiv r \pmod{2c}$.

D'après la seconde règle de congruence, $h \equiv r \pmod{g-1}$. Or $2c|e$ par A3, donc $f \equiv 1 \pmod{2c}$ d'où $g \equiv 1 \pmod{2c}$. Donc $h \equiv r \pmod{2c}$. Par A6, $h \equiv b \pmod{2c}$. Donc $b \equiv r \pmod{2c}$.

5. $r \equiv \pm p \pmod{2c}$.

En effet, $g \equiv a \pmod{f}$ et donc, par la règle de congruence 1 , $h = y_g(r) \equiv y_a(r) \pmod{f}$. Or $c \equiv h \pmod{f}$ par A1, donc $y_a(r) \equiv y_a(p) \pmod{f}$. Or $f = x_a(q)^2$ donc, $y_a(r) \equiv y_a(p) \pmod{x_a(q)}$ et donc, par la seconde réduction $(*)$ $r \equiv \pm p \pmod{2q}$. Or par A3, $c^2 | e$, c-à-d. $y_a(p)^2 | y_a(q)$ et donc, par la première réduction $y_a(p) | q$, c-à-d. $c | q$ et donc, en vertu de $(*)$, $r \equiv \pm p \pmod{2c}$.

6. $b = p$ <u>et donc</u> $c = y_a(b)$.

En effet, par 4 et 5, $b \equiv \pm p \pmod{2c}$. Par A1, $b \leqslant c$ et $c = y_a(p) \Longrightarrow p \leqslant c$ (proposition 4). Donc $b = p$.

<u>Réciproquement</u>, supposons que $c = y_a(b)$ avec $a > 1$ et $b > 0$. Alors $c > 0$ (on a une solution positive) et $c \geqslant b$ par la proposition 4. Posons $d = x_a(b)^2$. On a alors A2. D'après la proposition 3, on peut trouver un entier positif q tel que $2dc^2 | y_a(q)$. Soit q un tel entier. Posons $e = y_a(q)$ et $f = x_a(q)^2$. Alors $2dc^2 | q \Longrightarrow$ il existe u entier naturel tel que $e = 2(u+1)dc^2$, d'où A3 et on a A4. Soit g défini par A5. On pose $h = y_g(b)$ et $i = x_g(b)^2$. Donc A7 est vérifié. Or $g \equiv a \pmod{f}$ par A5 $\Longrightarrow h = y_g(b) \equiv y_a(b) = c \pmod{f}$ (première règle de congruence). Donc $f | h-c$. Mais $h = y_g(b) \equiv b \pmod{g-1}$. Or, par A3, $e \equiv 0 \pmod{2c}$ d'où $f \equiv 1 \pmod{2c}$ d'où $g \equiv 1 \pmod{2c}$ par A4 et A5. Donc il existe $v \in \mathbb{N}$ tel que $h = b+2vc$ puisque $h = y_g(b) \Longrightarrow h \geqslant b$ (proposition 4). D'où le théorème. ■

2.3 <u>Représentation diophantienne de l'exponentielle</u>.

Le théorème 3 et la proposition 9 permettent déjà de démontrer le théorème 2. En effet, $y = x^n$ si et seulement si il existe des entiers positifs p, q, ℓ, r tels que

B1 $\quad p = y_r(n+1)$

B2 $\quad q = y_\ell(n+1)$

B3 $\quad \ell > 4n(y+1)$

B4 $\quad q^2 - 4(p-yq)^2 > 0 \quad$ (c-à-d. $(\frac{p}{q} - y)^2 < \frac{1}{4}$)

B5 $\quad r = \ell x$.

Ce système d'équations utilise deux fois le système A1-A7. Nous allons indiquer un système d'équations n'utilisant qu'une fois les suites de Lucas, ce qui permettra de réduire le nombre de variables dans le polynôme universel.

Théorème 4 (Matiyassévitch - J. Robinson (cf. [6]) : Soient $x,n > 0$. Alors $y = x^n$ si et seulement si il existe des entiers naturels a,b,c,j,k,u , tels que :

C1 $\quad c = y_a(b)$

C2 $\quad (k^2-1)j^2+1 = \square$

C3 $\quad j^2-4(c-yj)^2 > 0$, $y > 0$ et $c \geqslant b$

C4 $\quad k = 4n(y+1)+x+1$

C5 $\quad j = b+u(k-1)$

C6 $\quad a = kx$

C7 $\quad b = n+1$.

Démonstration : Supposons qu'il existe des entiers a,b,c,j,k,u tels que C1-C7 soient vérifiés.

1. $j = y_k(b+v(k-1))$ pour un $v \in \mathbb{N}$.

On remarque tout d'abord que $x,y > 0$ et $b > 1$ d'après C3 et C7. D'après C2, $j = y_k(p)$ pour un entier naturel p , et $j \geqslant p$ (proposition 4). Par la seconde règle de congruence, $y_k(p) \equiv p \pmod{k-1}$ c-à-d. $j \equiv p \pmod{k-1}$. Mais, par C5, $j \equiv b \pmod{k-1}$, donc $b \equiv p \pmod{k-1}$, c-à-d. $p = b+v(k-1)$ pour un $v \in \mathbb{Z}$. Par C4, $k > b+1$ $(b > 1)$ et comme $p \in \mathbb{N}$, $v \in \mathbb{N}$.

2. $v = 0$, c-à-d. $j = y_k(b)$.

En effet, supposons $v > 0$. Comme la fonction y_k est strictement croissante, $y_k(b+v(k-1)) \geqslant y_k(b+k-1)$ puisque $v \geqslant 1$. Donc :

$$\frac{y_{kx}(n+1)}{y_k(n+1+v(k-1))} \leqslant \frac{y_{kx}(n+1)}{y_k(n+1+k-1)} \leqslant \frac{(2kx)^n}{(2k-1)^{n+k-1}} \quad \text{d'après (3)}$$

$$= \frac{(2k)^n}{(4k(k-1)+1)^n} \cdot \frac{x^n}{(2k-1)^{k-2n-1}} = a_{x,n,k} \cdot$$

D'après C4, $2k-1 > x$ et $k-2n > n-1$, d'où $\frac{x^n}{(2k-1)^{k-2n-1}} < 1$. Comme $k > 2$ puisque $b > 1$ par C4, on a $4k < 4k(k-1)+1$ d'où $\frac{(2k)^n}{(4k(k-1)+1)^n} \leqslant \frac{2k}{4k(k-1)+1} < \frac{1}{2}$. Donc $a_{x,n,k} < \frac{1}{2}$. Donc par C4, comme $(\frac{c}{j} - y)^2 < \frac{1}{4}$ on a $y = 0$. Mais, par C4, $y > 0$. Il y a donc contradiction et $v = 0$, c-à-d. $j = y_k(b)$. Comme $k > 4n(y+1)$, on a, par C3 et la proposition 9 que $y = x^n$.

Réciproquement, soit $y = x^n$ avec $x, n > 0$. Alors $y > 1$. On définit k et a par C4 et C6, b par C7, c par C1. On pose $j = y_k(b)$. Alors C2 est vérifiée. Par la règle de congruence 2, $j = y_k(b) \equiv b \pmod{k-1}$ et $j \geqslant b$ par la proposition 4. Comme $k-1 > b$ d'après C4, il existe $u \in \mathbb{N}$ tel que $j = b+u(k-1)$ d'où C5. Enfin, comme $k > 4n(y+1)$, $(\frac{c}{j} - y)^2 < \frac{1}{4}$ d'après la proposition 9 et donc C3 est vérifiée. ■

Il est clair maintenant que le théorème 2 découle immédiatement des théorèmes 3 et 4.

II. Applications.

Tout d'abord, montrons que du théorème principal résulte la réponse négative au dixième problème de Hilbert :

Théorème 5 (Matiyassévitch) : Il n'existe pas d'algorithmes permettant de décider si une équation diophantienne a ou n'a pas de solutions.

Preuve (cf. [1] : Soit K un ensemble d'entiers récursivement énumérable et non récursif. Il existe donc, d'après le théorème principal, un entier n et un polynôme $P \in \mathbb{Z}[X,Y_1,\ldots,Y_n]$ tel que $a \in K \Longleftrightarrow \exists y_1,\ldots,y_n \; P(a,y_1,\ldots,y_n) = 0$. Si la réponse au dixième problème de Hilbert était positive, on aurait donc que K est récursif, ce qui n'est pas. Donc la réponse au dixième problème est négative. ■

Naturellement, il existe des problèmes qui ne se réduisent pas à la résolution d'une équation diophantienne. Cependant, le champ des problèmes qui peuvent se réduire à un problème diophantien est bien plus large que ce qu'on imagine. Et, suivant [1], nous reprendrons ici quelques exemples illustrant la complexité de ce problème, en même temps que nous indiquerons quelques directions de recherches partant des méthodes utilisées pour établir le théorème principal.

1. Universalité et réduction.

On sait qu'il existe des machines de Turing universelles c'-à-d. A étant un alphabet donné, ν un codage fixé dans A des machines de Turing, il existe une machine de Turing $\mathbb{K}$ telle que pour toute machine de Turing $\mathbb{M}$ dans A et tout mot P dans A on ait :

$$\mathbb{K}(\nu(\mathbb{M})P) \simeq \mathbb{M}(P)$$

(le signe $\simeq$ signifie que si $\mathbb{M}$ converge en P , $\mathbb{K}$ converge en

$\nu(\mathbb{M})P$ et réciproquement et qu'alors les résultats sont les mêmes). On déduit du théorème principal le :

Théorème 6 (théorème de l'équation universelle (cf. [1]) : Il existe un polynôme diophantien $U(a,n,x_1,\ldots,x_\nu) = 0$ tel que pour toute partie diophantienne D de $\mathbb{N}$ il existe un entier n tel que $a \in D \Longleftrightarrow \exists x_1,\ldots,x_\nu (U(a,n,x_1,\ldots,x_\nu) = 0)$.

Posons $D_k = \{a \in \mathbb{N} ; \exists x_1,\ldots,x_\nu (U(a,k,x_1,\ldots,x_\nu) = 0)\}$. On dira que D_k est l'ensemble diophantien de numéro k , et le codage ainsi réalisé est diophantien. On a ainsi une énumération diophantienne de toutes les parties diophantiennes de $\mathbb{N}$.

On passe aux ensembles diophantiens de $\mathbb{N}^k$ de la façon suivante : Soit $J(x,y) = \frac{1}{2}[(x+y)^2 + 3x + y]$, $J_1(x) = x$ et $J_{n+1}(x_1,\ldots,x_{n+1}) = J(J_n(x_1,\ldots,x_n),x_{n+1})$. Il en résulte que

$$U(J_m(a_1,\ldots,a_m),k,x_1,\ldots,x_\nu)$$

est un polynôme universel pour les parties diophantiennes de $\mathbb{N}^m$. On peut étendre ceci aux suites finies d'entiers en utilisant le code : $H(a_1,\ldots,a_m) = J_{m+1}(m,a_1,\ldots,a_m)$.

Si on considère maintenant D un ensemble diophantien de $\mathbb{N}^k$. Il est donné par un polynôme diophantien $P(a_1,\ldots,a_k, y_1,\ldots,y_n)$ à n inconnues. D'après les considérations précédentes, il existe un entier m tel que

$$\exists y_1,\ldots,y_n \; P(a_1,\ldots,a_k, y_1,\ldots,y_n) = 0 \Longleftrightarrow \exists x_1,\ldots,x_\nu$$
$$U(J_k(a_1,\ldots,a_k),m,x_1,\ldots,x_\nu) = 0$$

c'est-à-dire que D peut être défini par un polynôme diophantien à ν inconnues. Donc le nombre d'inconnues d'une équation diophantienne, a priori, arbitraire, peut-être ramené à une borne uniforme. On ne connaît pas actuellement la valeur exacte de cette borne. Le meilleur résultat publié actuellement est donné dans [6] par Matiyassévitch et J. Robinson :

Théorème 7 (Matiyassévitch - J. Robinson) : A toute équation diophantienne de ν inconnues et μ paramètres $P(a_1,\ldots,a_\mu, z_1,\ldots,z_\nu) = 0$ correspond une équation diophantienne à μ paramètres et 13 inconnues $Q(a_1,\ldots,a_\mu, x_1,\ldots,x_{13}) = 0$ ayant une solution pour les mêmes valeurs des paramètres.

En particulier, il existe un polynôme universel à 2 paramètres et 13 inconnues.

L'idée de la démonstration consiste en un codage particulier à deux paramètres des $z_1,\ldots,z_\nu$, qui peut-être réduit à la condition $\forall t\ R(t) > 0$ pour un certain polynôme R dépendant des a_i et des deux paramètres du codage. La condition $\forall t\ R(t) > 0$ peut s'exprimer à l'aide de coefficients binomiaux reliés de façon adéquate au polynôme R. On passe donc par la représentation "courte" de l'exponentielle exposée en I.2. Le lecteur intéressé trouvera la démonstration détaillée dans [6]. Depuis, le nombre d'inconnues a été réduit à 9 (cf. [4]).

Il est à noter que par une telle réduction du nombre des variables, le degré du polynôme Q est augmenté. Il est clair qu'inversement, on peut réduire le degré du polynôme à 4, en augmentant celui des variables par des équations du genre (suivant SKOLEM)

$$(*) \qquad \begin{aligned} u &= x+y \\ v &= xy \end{aligned}$$

L'équation initiale $P = 0$ peut se décomposer en $A = B$ où les coefficients de A et B sont positifs, puis, par applications successives de $(*)$, on aura un système de k équations $(**)$ $A_i = B_i$ équivalent à $P = 0$ où chacun des A_i, B_i est de degré au plus 2. Le système $(**)$ est équivalent à $\sum_{i=1}^{k} (A_i - B_i)^2 = 0$, d'où un polynôme de degré au plus 4. J.P. Jones (cf. [2]) a étudié les couples (δ,ν) pour lesquels il existe un polynôme universel de degré δ à ν inconnues. Ainsi les couples suivant (4,153), (6,129), (8,108), (10,107),

(20,86), (44,83), (1952,80) (cités dans [1]) répondent-ils à la question. En outre, il est clair que si $U(a,k,x_1,\ldots,x_{13})$ est universel, alors $U(J_m(a_1,\ldots,a_m),k,x_1,\ldots,x_{13})$, qui est universel pour les parties diophantiennes de $\mathbb{N}^m$, a un degré par rapport aux paramètres qui tend vers $+\infty$ si $m \to +\infty$. La question de savoir s'il existe (δ,ν) tel que pour tout m, il y a un polynôme universel pour les parties diophantiennes de $\mathbb{N}^m$ de ν inconnues et de degré total (paramètres et inconnues) δ, est ouverte.

On conviendra de désigner par $[\delta,\infty]$ l'ensemble des polynômes diophantiens de degré au plus δ à un nombre quelconque d'inconnues et par $[\infty,\nu]$ l'ensemble des polynômes diophantiens à ν inconnues et de degré quelconque. La réduction de Skolem, montre que pour la classe $[4,\infty]$, et les classes supérieures, le dixième problème de Hilbert est indécidable. SIEGEL a construit dans [9] un algorithme de décision du dixième problème pour la classe $[2,\infty]$. La décidabilité ou l'indécidabilité du problème pour la classe $[3,\infty]$ reste entièrement ouverte. Pour les classes $[\infty,\nu]$, la situation est moins précise. Le théorème de réduction à 9 inconnues établit l'indécidabilité du dixième problème pour la classe $[\infty,9]$. Par contre, on ne sait rien pour les classes $[\infty,\nu]$ avec $\nu \leqslant 8$ (sauf pour $\nu = 1$ qui est évidemment trivial). Même pour $\nu = 2$ le problème reste ouvert, le meilleur résultat connu, dû à BAKER and COATES (cité dans [1]) donnant une procédure de décision pour une sous-classe (assez large) d'équations à deux inconnues.

Par contre, si l'on considère les polynômes exponentiels diophantiens, on a l'indécidabilité pour la classe $[\infty,3]$, cf. [5].

2. Représentation de parties récursives ; les nombres premiers.

Il est clair que tout ensemble récursif est diophantien. En fait, D est récursif si et seulement si D et N\D sont récursivement énumérables, donc diophantiens d'après le théorème principal.

Ainsi, soit $\mathcal{P}$ l'ensemble des nombres premiers. $\mathcal{P}$ est évidemment récursif et donc diophantien. Il est intéressant de voir comment on peut représenter $\mathcal{P}$ et $\mathbb{N}\setminus\mathcal{P}$ par des équations diophantiennes.

Il est clair que

$$a \in \mathbb{N}\setminus\mathcal{P} \iff \exists y_1, y_2 \ ([a = (y_1+1)(y_2+1)]_v[a = 0]_v[a = 1])$$

(on rappelle que $y_1, y_2 \in \mathbb{N}^*$) c-à-d.

$$a \in \mathbb{N}\setminus\mathcal{P} \iff \exists y_1, y_2 \ (a(a-1)[a-(y_1+1)(y_2+1)] = 0) \ .$$

Par ailleurs, on a :

$$\alpha \in \mathcal{P} \iff \exists y_1, y_2 \ (\alpha = y_1+1 \ \& \ y_1!+1 = y_2\alpha)$$

$(y_1, y_2 \in \mathbb{N}^*)$, en vertu du théorème de Wilson. Nous allons nous contenter d'une représentation exponentiellement diophantienne de $\mathcal{P}$: à cet effet, on établit que

$$n! = \left[\frac{t^n}{\binom{t}{n}}\right] \qquad \text{pour} \quad t \geqslant 4n^{n+2} \ .$$

On a, en effet, $\dfrac{t^n}{\binom{t}{n}} = n!t^n \dfrac{(t-n)!}{t!} = n!t^{n-1} \dfrac{1}{(t-1)\ldots(t-n+1)}$

$$= n! \frac{t}{t-1}\ldots\frac{t}{t-n+1} = n!\left(1+\frac{1}{t-1}\right)\ldots\left(1+\frac{n-1}{t-n+1}\right) \ .$$

Donc :

$$n! \leqslant \frac{t^n}{\binom{t}{n}} = n!\left(1+\frac{1}{t-1}\right)\ldots\left(1+\frac{n-1}{t-n+1}\right) \ ,$$

d'où $\dfrac{t^n}{\binom{t}{n}} \to n!$ si $t \to +\infty$. Or $\left(1+\dfrac{1}{t-1}\right)\ldots\left(1+\dfrac{n-1}{t-n+1}\right) \leqslant \left(1+\dfrac{n}{t-n}\right)^n$.

Or $\log\left(1+\dfrac{n}{t-n}\right)^n \leqslant \dfrac{n^2}{t-n} \Longrightarrow \left(1+\dfrac{n}{t-n}\right)^n \leqslant e^{\frac{n^2}{t-n}}$. Pour $0 \leqslant \lambda \leqslant 1$ on a $e^{\lambda} \leqslant 1+e\lambda$ d'où pour $t > n^2+n$, on a :

$$n! \leqslant \frac{t^n}{\binom{t}{n}} \leqslant n!\left(1+\frac{en^2}{t-n}\right). \text{ Or, pour } \ t \geqslant 4n^{n+2} \ , \ \frac{n!en^2}{t-n} \leqslant \frac{3}{4n} \ .$$

Donc, comme on a déjà vu une représentation exponentiellement diophantienne de $\binom{t}{n}$, on peut en déduire une telle représentation de $n!$.

Si P est un polynôme définissant les nombres premiers c-à-d.

$$a \in \mathcal{P} \iff \exists y_1, \ldots, y_v \ P(a, y_1, \ldots, y_v) = 0$$

(il existe de tels polynômes avec $\nu = 9$), on peut à partir de là représenter $\mathcal{P}$ comme l'ensemble des valeurs positives d'un polynôme :

Soit $Q(a,y_1,\ldots,y_\nu) = (a+1)(1 - P^2(a,y_1,\ldots,y_\nu)) - 1$.

Soit p un nombre premier. Il existe $y_1,\ldots,y_\nu$ t.q. $P^2(p,y_1,\ldots,y_\nu) = 0$ et donc $Q(p,y_1,\ldots,y_\nu) = p > 0$. Soit maintenant $k = Q(a,y_1,\ldots,y_\nu)$ avec $y_1,\ldots,y_\nu \in D^*$ et $a \in \mathbb{N}$, et $k > 0$. Alors, nécessairement $P^2(a,y_1,\ldots,y_\nu) = 0$, et donc $k = a$ d'où a est premier. Donc $\mathcal{P} = \mathrm{Im}\, Q \cap \mathbb{N}$.

Cette propriété, comme on le constate par cette démonstration (due à Putnam) est plus générale et donc :

Proposition 10 : D est un ensemble diophantien si et seulement si D est l'ensemble des valeurs positives ou nulles d'un polynôme diophantien.

En effet : si D est diophantien, c'est ce que nous venons de voir et si $D = \mathrm{Im}\, Q \cap \mathbb{N}$, c-à-d. $n \in D \iff \exists x_1,\ldots,x_\nu (n = Q(x_1,\ldots,x_\nu))$, alors si $P(n,x_1,\ldots,x_\nu) = (n - Q(x_1,\ldots,x_\nu))^2$, on a bien $n \in D \iff \exists x_1,\ldots,x_\nu [P(n,x_1,\ldots,x_\nu) = 0]$.

3. Le quantificateur universel ; problèmes célèbres.

Naturellement, tous les ensembles diophantiens ne sont pas récursifs. Cela se déduit du théorème principal, mais aussi, directement, en traduisant la preuve classique en termes diophantiens. Soit, en effet $U(a,n,x_1,\ldots,x_\nu)$ un polynôme universel pour les parties diophantiennes de $\mathbb{N}$. Posons : D_k l'ensemble des a tels que $U(a,k,x_1,\ldots,x_\nu) = 0$ admet une solution au moins en $x_1,\ldots,x_\nu$. Posons

$$K = \{n \in \mathbb{N} ; n \in D_n\} .$$

K est évidemment diophantien. Par contre :

Proposition 11 : K n'est pas récursif.

En effet : supposons $\mathbb{N}\setminus K$ diophantien. On a donc $\mathbb{N}\setminus K = D_k$ pour un certain k. Si $k \notin K$, alors $k \in D_k$, par définition de K, et donc $k \in K$. Donc $k \in K$. Mais alors $k \in D_k$ par définition de K. D'où $k \notin K$ par définition de D_k. De cette contradiction, il résulte que $\mathbb{N}\setminus K$ n'est pas diophantien. ■

Nous avons vu précédemment que certaines propriétés peuvent être énoncées comme liées à l'existence de solutions d'une équation diophantienne. Nous allons voir comment certaines propriétés sont liées à la <u>non existence</u> de telles solutions.

Le plus évident de ces problèmes, est celui de Fermat :

$$x^n + y^n = z^n \quad \text{n'a pas de solutions pour} \quad n \geqslant 3 \qquad (4)$$

est évidemment, pour chaque n fixé, équivalent à la non existence de solutions d'une équation diophantienne. En fait, la <u>conjecture entière de Fermat</u> est équivalente à la non existence de solutions <u>d'une</u> équation diophantienne.

En effet, suivant [1], il existe un polynôme $E(a,b,c,x_1,\ldots,x_\nu)$ tel que $c = a^b \iff \exists x_1,\ldots,x_\nu (E(a,b,c,x_1,\ldots,x_\nu) = 0)$.
Donc, (4) admet une solution pour n fixé peut s'écrire :

$$\exists a,b,x,y,z,x_1,\ldots,x_\nu,y_1,\ldots,y_\nu,z_1,\ldots,z_\nu (E^2(x,n,a,x_1,\ldots,x_\nu) + E^2(y,n,b,y_1,\ldots,y_\nu) + E^2(z,n,a+b,z_1,\ldots,z_\nu) = 0)$$

et donc la conjecture de Fermat est vraie ssi l'équation

$$(n-2m-p)^2 + E^2(x,n,a,x_1,\ldots,x_\nu) + E^2(y,n,b,y_1,\ldots,y_\nu) + E^2(z,n,a+b,z_1,\ldots,z_\nu) = 0$$

n'a pas de solution en $a,b,m,n,p,x,y,z,x_1,\ldots,x_\nu,y_1,\ldots,y_\nu,z_1,\ldots,z_\nu$.

Ainsi, une réponse positive au 10è problème de Hilbert aurait fourni un moyen de lever la conjecture de Fermat.

En fait ce résultat est plus général. On a (cf. [1]) :

<u>Théorème</u> 8 : Soit P un prédicat récursif à une place. Alors il existe une équation diophantienne $Q(n,x_1,\ldots,x_k) = 0$ telle que

$\forall n\ P(n)$ si et seulement si l'équation $Q(n,x_1,\ldots,x_k) = 0$ n'admet pas de solution.

Preuve : Comme P est récursif il existe deux polynômes diophantiens $P(n,x_1,\ldots,x_k)$ et $Q(n,x_1,\ldots,x_k)$ tels que

$$P(n) \Longleftrightarrow \exists x_1,\ldots,x_k\ P(n,x_1,\ldots,x_k) = 0 \quad \text{et}$$
$$\neg P(n) \Longleftrightarrow \exists x_1,\ldots,x_k\ Q(n,x_1,\ldots,x_k) = 0\ .$$

Il est clair que $Q(n,x_1,\ldots,x_k) = 0$ admet une solution au moins si et seulement si $\exists n\ \neg P(n)$. ■

Remarque : La démonstration montre que le théorème 8 reste vrai en supposant seulement que P est le complémentaire d'un récursivement énumérable.

De nombreuses conjectures de théorie des nombres tombent dans le champ de ce théorème. Nous citerons simplement la conjecture de Goldbach. En effet, si $P(n)$ désigne $\exists p_1 p_2\ (p_1 \in \mathcal{P}\ \&\ p_2 \in \mathcal{P}\ \&\ p_1 + p_2 = 2(n+2))$. $P(n)$ est récursif, car on a nécessairement $p_1, p_2 \leqslant 2(n+1)$. Donc toute la conjecture de Goldbach se réduit à l'insolubilité d'une équation diophantienne.

Une autre conjecture fameuse, à l'intersection de la théorie des nombres et de l'analyse est l'hypothèse de Riemann.

On sait que la fonction ζ de Riemann est définie par

$$\zeta(s) = \sum_{n=1}^{+\infty} n^{-s}\ ,$$

série qui converge pour $\mathrm{Re}(s) > 1$. La fonction obtenue peut-être prolongée analytiquement au plan complexe privé du point 1. Les points $-2k$ $(k \in \mathbb{N})$, sont des zéros de ζ . Les autres zéros de ζ sont appelés non triviaux. On sait qu'ils se trouvent dans la bande $0 < \mathrm{Re}(s) < 1$, symétriquement par rapport à la droite $\mathrm{Re}\, s = \frac{1}{2}$. L'hypothèse de Riemann affirme que les zéros non triviaux de cette fonction sont sur la droite $\mathrm{Re}\, s = \frac{1}{2}$. Par symétrie, l'hypothèse

revient à affirmer que ζ n'a pas de zéros dans la bande $\frac{1}{2} < \mathrm{Re}(s) < 1$. Or cette bande est une réunion dénombrable de rectangles $\mathcal{R}_n$ de sommets, $(\frac{1}{2}+\frac{1}{n},n)$, $(1-\frac{1}{n},n)$, $(\frac{1}{2}+\frac{1}{n},-n)$, $(1-\frac{1}{n},-n)$. Si l'hypothèse de Riemann est vraie, alors $\int_{\mathcal{R}_n} \frac{\zeta'(s)}{\zeta(s)}\,ds = 0$ pour tout n , et réciproquement, car si $\int_{\mathcal{R}_n} \frac{\zeta'(s)}{\zeta(s)}\,ds = 0$ l'intégrale existe (donc il n'y a pas de zéro sur le bord du rectangle) et l'intégrale étant zéro, les résidus (positifs ou nuls) sont donc nuls (l'indice des points intérieurs au rectangle est toujours 1), ce qui signifie qu'il n'y a pas de zéros. En outre, en toute généralité, pour $\mathcal{R}$, un rectangle contenu dans le domaine de définition de ζ (et homotope à zéro dans ce domaine), on a $\frac{1}{2i\pi}\int_{\mathcal{R}} \frac{\zeta'(s)}{\zeta(s)}\,ds = 0,1,\ldots,n,\ldots,+\infty$. Donc $\int_{\mathcal{R}_n} \frac{\zeta'(s)}{\zeta(s)}\,ds = 0 \Longleftrightarrow \left|\int_{\mathcal{R}_n} \frac{\zeta'(s)}{\zeta(s)}\,ds\right| < \frac{1}{2}$. Posons $P(n) \Longleftrightarrow \left|\int_{\mathcal{R}_n} \frac{\zeta'(s)}{\zeta(s)}\,ds\right| < \frac{1}{2}$. L'hypothèse de Riemann s'énonce donc $\forall n\ P(n)$. Or $P(n)$ est décidable : il suffit de prendre une approximation convenable de $\frac{\zeta'(s)}{\zeta(s)}$ par une fonction rationnelle et prendre un rationnel assez proche de l'intégrale de la nouvelle fonction.

Donc, l'hypothèse de Riemann équivaut à l'insolubilité d'une équation diophantienne. (On trouvera une autre présentation de ce résultat dans [1]).

Enfin, signalons une application du théorème 8, concernant plus spécialement la logique.

Considérons une théorie formelle donnée par un certain alphabet et des règles de formations de certains mots (les formules), par un ensemble récursivement énumérable d'axiomes et un nombre fini de règles de déduction. Alors l'ensemble des théorèmes d'une théorie formelle est récursivement énumérable. En effet, on peut obtenir un algorithme énumérant les théorèmes et eux seuls en considérant une première étape où on ajoute un axiome à la liste des théorèmes, grâce à l'algorithme énumérant les axiomes, puis une seconde, où, dans la

liste des théorèmes déjà énumérés (y compris après la première étape) on prend toutes les occurences possibles des règles de déduction et on adjoint les résultats obtenus à la liste. On obtient ainsi des théorèmes et tous les théorèmes.

Considérons maintenant le problème de la cohérence d'une théorie formelle, c-à-d., la théorie est cohérente si et seulement si il n'y a pas de formule R telle que R et $\neg R$ soient déductibles dans la théorie. Il résulte de ce qui suit la

Proposition informelle : Le problème de la cohérence d'une théorie formelle est équivalent à celui de l'insolubilité d'une certaine équation diophantienne.

Preuve (informelle) : Considérons l'algorithme d'énumération des théorèmes indiqué ci-dessus. Appelons pas l'exécution consécutive de l'étape 1 et de l'étape 2. La propriété $P(n)$ définie par : "il n'y a pas de contradiction au pas n" est évidemment récursive. Or la cohérence de la théorie s'exprime par la formule $\forall n\ P(n)$. D'où la correspondance avec une équation diophantienne, en vertu du théorème 8.▲

Ainsi, comme un problème d'indépendance d'axiome se ramène à deux problèmes de cohérence (la théorie + A est cohérente et la théorie + $\neg$A est cohérente), on a, par exemple qu'à l'hypothèse du continu correspondent deux équations diophantiennes insolubles.

La propriété que l'existence d'un cardinal inaccessible implique la cohérence de ZF se traduit par l'existence d'une équation diophantienne dont l'insolubilité résulte de l'axiome du cardinal inaccessible alors qu'elle ne peut être démontrée dans ZF seul. De même, la cohérence de Peano se traduit par une équation diophantienne dont l'insolubilité ne peut se démontrer dans Peano, mais se déduit dans ZF.

Un autre corollaire de la proposition informelle, est qu'on peut donner une "teinture diophantienne" au théorème d'incomplétude de

Gödel, à savoir qu'à toute théorie formelle τ assez forte, on peut associer une équation diophantienne insoluble dont l'insolubilité n'est pas déductible dans τ . Voici une formulation plus précise, tirée de [1].

Théorème 9 : théorème d'incomplétude de Gödel. Soit $\mathcal{G}$ un système d'axiomes d'un langage contenant les symboles mathématiques $0,S,+,.,<$ et tel que :

(i) $\mathcal{G}$ est cohérent

(ii) $\mathcal{G}$ est énumérable

(iii) $\mathcal{G}$ est assez fort pour démontrer tout énoncé vrai de la forme

$$p+q = r$$

$$pq = r$$

$$p < q$$

où p.q.r figurent parmi $0,S0,SS0,\ldots$ et S est la fonction successeur.

Alors on peut construire une équation diophantienne $F(x_1,\ldots,x_\nu) = 0$ correspondant à $\mathcal{G}$ telle que $F(x_1,\ldots,x_\nu) = 0$ n'ait pas de solutions dans $\mathbb{N}^\nu$ mais telle qu'on ne puisse déduire $\neg\exists x_1,\ldots,x_\nu(F(x_1,\ldots,x_\nu) = 0)$ de $\mathcal{G}$.

Preuve : Soit $U(a,k,x_1,\ldots,x_\nu)$ énumérant les parties diophantiennes de $\mathbb{N}$. Soit alors $A = \{a ; [\neg\exists x_1,\ldots,x_\nu(U(a,a,x_1,\ldots,x_\nu) = 0)]$ est déductible de $\mathcal{G}\}$.

Alors A est évidemment récursivement énumérable (A est l'"ombre" de K dans la théorie associée à $\mathcal{G}$) (cf. p. 29), donc diophantien, par le théorème principal. Donc $A = D_k$ pour un certain k . Soit alors $F(x_1,\ldots,x_\nu) = U(k,k,x_1,\ldots,x_\nu)$ (k est une constante). Si l'insolubilité de F est déductible de $\mathcal{G}$, d'après la définition de A , $k \in D_k$ et, par définition de D_k , on a donc

$\exists x_1,\ldots,x_k(U(k,k,x_1,\ldots,x_\nu) = 0)$, ce qui est impossible puisque $\mathcal{Q}$ est cohérent. Donc l'insolubilité de F n'est pas déductible de $\mathcal{Q}$ et donc $k \notin D_k$. Mais, par définition de D_k , $k \notin D_k$ signifie l'insolubilité de F . ■

Toutes les conjectures, ne relèvent pas directement de cette traduction : par exemple la conjecture de l'infinité des nombres premiers jumeaux. Cette conjecture est de la forme $\forall n\ P(n)$ mais avec $P(n)$ non décidable car $P(n)$ s'écrit $\exists p_1,p_2\ [p_1,p_2 \in \mathcal{P}\ \&\ p_2=p_1+2\ \&\ p_1>n$ La non décidabilité (a priori) résulte de ce que le quantificateur existentiel n'est pas borné. En fait si on considère $P'(n) = \exists p_1,p_2\ [p_1,p_2 \in \mathcal{P}\ \&\ p_2 = p_1+2\ \&\ n+4 < p_1 \leqslant 2^{n+4}]$ alors $\forall n\ P'(n)$ équivaut à l'insolubilité d'une certaine équation diophantienne. Les arithméticiens qui sont prêts à admettre $\forall n\ P(n)$ sont également prêts à accepter $\forall n\ P'(n)$ qui est cependant plus forte.

On peut se demander quel intérêt présente une telle traduction des conjectures. Selon Matiyassévitch, J. Robinson et Davis [1] il réside dans l'étude des classes décidables d'équations diophantiennes. Ces auteurs pensent qu'il faut développer les recherches dans la construction de nouvelles classes décidables et vérifier ensuite, éventuellement à l'aide d'ordinateurs, que la "traduction" de telle ou telle conjecture, figure dans une des classes découvertes. On remarquera que pour l'instant, le problème des quatre couleurs, relevable d'une traduction diophantienne, a été résolu par des techniques de théorie des graphes. Cependant, comme les auteurs cités l'observent à juste titre dans [1] "la classe des ensembles diophantiens n'est étudiée que depuis 25 ans. Sa richesse a étonné les spécialistes et, peut être, son utilité le fera également".

III. Autres problèmes connexes.

Comme il a été précisé dans l'introduction, on considère ici le dixième problème de Hilbert en se plaçant sur un autre ensemble d'entiers que $\mathbb{N}$. On sait déjà (cf. début du I p. 1) que la recherche de solutions d'une équation diophantienne dans $\mathbb{Z}$ équivaut à la recherche des solutions dans $\mathbb{Z}$.

Considérons maintenant un anneau commutatif unitaire intègre $\mathcal{R}$ contenant $\mathbb{Z}$. Pour poser le dixième problème sur $\mathcal{R}$, il faut redéfinir le terme "diophantien". Or, ici, il y a deux notions possibles selon le sens qu'on donne au mot "entier" dans la définition des coefficients des polynômes figurant dans la caractérisation des ensembles diophantiens.

On dit que $\mathcal{S} \subset \mathcal{R}^k$ est un ensemble diophantien sur $\mathcal{R}$ (resp. diophantien pur sur $\mathcal{R}$) s'il existe un entier $n > 0$ et un polynôme $P \in \mathcal{R}[X_1,\ldots,X_k,Y_1,\ldots,Y_n]$ (resp. $P \in \mathbb{Z}[X_1,\ldots,X_k,Y_1,\ldots,Y_n]$) tel que :

$$(a_1,\ldots,a_k) \in \mathcal{S} \iff \exists y_1,\ldots,y_n \in \mathcal{R} \; P(a_1,\ldots,a_k,y_1,\ldots,y_n) = 0 \; .$$

On définit de la même façon les relations diophantiennes (pures), les polynômes diophantiens (purs) et les équations diophantiennes (pures).

Le dixième problème de Hilbert relatif à $\mathcal{R}$ (on dira "dixième problème sur $\mathcal{R}$") se scinde en deux, selon le sens donné au terme "diophantien" et s'énonce ainsi :

"Existe-t-il un algorithme permettant de décider si une équation diophantienne (pure) sur $\mathcal{R}$ a ou n'a pas de solutions ?"

Actuellement, le problème a été et est étudié dans les cas suivants :

(i) $\mathcal{R}$ est l'anneau des entiers d'une extension quadratique de $\mathbb{Q}$.

(ii) $\mathcal{R}$ est l'anneau des entiers d'une extension de $\mathbb{Q}$ de degré fini au moins égal à 3.

(iii) $\mathfrak{R}$ est l'anneau des entiers algébriques sur $\mathbb{Q}$.

(iv) $\mathfrak{R} = \mathbb{Q}$.

Seul le cas (i) a reçu récemment une solution, dans les deux sens du dixième problème, qui est négative (travaux de DENEF, cités dans [1]).

La démonstration de DENEF repose sur un analogue du Théorème Principal. Il faut naturellement préciser ce qu'est une relation sur $\mathfrak{R}$ récursivement énumérable. Dans les 4 cas considérés ci-dessus, $\mathfrak{R}$ est lui-même récursivement énumérable. Nous supposerons $\mathfrak{R}$ récursivement énumérable. Nous dirons donc qu'une relation k-aire $\mathcal{M}$ sur $\mathfrak{R}$ est récursivement énumérable si et seulement si, la relation définie par $\mathcal{M}$ sur les numéros des éléments de $\mathfrak{R}$ est récursivement énumérable. Dans le cas (i) DENEF démontre alors qu'une partie de $\mathfrak{R}^k$ est diophantienne sur $\mathfrak{R}$ si et seulement si elle est récursivement énumérable. En fait, il suffit de démontrer que $\mathbb{Z}$ est diophantien sur $\mathfrak{R}$ comme le prouve la

Proposition 12 : Soit F une extension de $\mathbb{Q}$ de degré fini et $\mathfrak{R}$ l'anneau des entiers de F (entiers algébriques de F sur $\mathbb{Q}$). Toute relation sur $\mathfrak{R}$ récursivement énumérable est diophantienne sur $\mathfrak{R}$ si et seulement si l'ensemble $\mathbb{Z}$ est diophantien sur $\mathfrak{R}$.

Démonstration : Soit $A \subset \mathfrak{R}^k$ une relation sur $\mathfrak{R}$ récursivement énumérable. Soit $\{\eta_1,\ldots,\eta_n\}$ une base de $\mathfrak{R}$ sur $\mathbb{Z}$, où n est le degré de F sur $\mathbb{Q}$ (on sait qu'une telle base existe toujours). Définissons la relation B sur $\mathbb{Z}$ où $B \subset \mathbb{Z}^{nk}$ par :
$B(a_1^{(1)},\ldots,a_n^{(1)},\ldots,a_1^{(k)},\ldots,a_n^{(k)})$ si et seulement si
$A(\sum_{i=1}^{n} a_i^{(1)}\eta_i,\ldots,\sum_{i=1}^{n} a_i^{(k)}\eta_i)$. Il est clair que B est une relation sur $\mathbb{Z}$ récursivement énumérable. Il existe donc un polynôme P à coefficients entiers (dans $\mathbb{Z}$) tel que :
$B(a_1^{(1)},\ldots,a_n^{(1)},\ldots,a_1^{(k)},\ldots,a_n^{(k)}) \Longleftrightarrow \exists y_1,\ldots,y_m \in \mathbb{Z}$
$P(a_1^{(1)},\ldots,a_n^{(1)},\ldots,a_1^{(k)},\ldots,a_n^{(k)},y_1,\ldots,y_m) = 0$. On a donc :

$A(x_1,\ldots,x_k) \Longleftrightarrow \exists a_1^{(1)},\ldots,a_n^{(1)},\ldots,a_1^{(k)},\ldots,a_n^{(k)},y_1,\ldots,y_m$

$[a_1^{(1)} \in \mathbb{Z} \,\&\ldots\&\, a_n^{(1)} \in \mathbb{Z} \,\&\, a_1^{(k)} \in \mathbb{Z} \,\&\ldots\&\, a_n^{(k)} \in \mathbb{Z} \,\&\, y_1 \in \mathbb{Z} \,\&\ldots\&\, y_m \in \mathbb{Z} \,\&$

$\&\; x_1 = \sum_{i=1}^{n} a_i^{(1)}\eta_i \,\&\ldots\&\, x_k = \sum_{i=1}^{n} a_i^{(k)}\eta_i \,\&$

$\&\; P(a_1^{(1)},\ldots,a_n^{(1)},\ldots,a_1^{(k)},\ldots,a_n^{(k)},y_1,\ldots,y_m)]$.

Par hypothèse, les relations de la forme $\alpha \in \mathbb{Z}$ sont diophantiennes sur $\mathfrak{R}$ et une conjonction de relations diophantiennes sur $\mathfrak{R}$ est diophantienne sur $\mathfrak{R}$.

En effet : F étant une extension de $\mathbb{Q}$ de degré fini, il existe un N tel que la racine primitive Nème de l'unité ne soit pas dans F (et donc pas dans $\mathfrak{R}$, car une telle racine est un entier algébrique sur $\mathbb{Z}$). Soit alors $\Phi_N(X,Y) \in \mathbb{Z}[X,Y]$ le polynôme homogène tel que $\Phi_N(X,1)$ soit le polynôme cyclotomique d'ordre N . On dira que $\Phi_N(X,Y)$ est le polynôme cyclotomique homogène d'ordre N . Alors il est clair que dans $\mathfrak{R}$ on a $\forall xy(\Phi_N(x,y) = 0 \Longleftrightarrow x = y = 0)$.

Il reste à montrer qu'une relation de la forme $\beta = 0$ où $\beta \in \mathfrak{R}$ est diophantienne sur $\mathfrak{R}$. Or il est clair que :

$\beta = 0 \Longleftrightarrow \beta \in \mathbb{Z} \,\&\, \exists u_1,\ldots,u_4,v_1,\ldots,v_4 \in \mathbb{Z}\; [\beta = u_1^2+\ldots+u_4^2 \,\&\, -\beta = v_1^2+\ldots+v_4^2]$

donc $\beta = 0$ est bien une relation diophantienne sur $\mathfrak{R}$. ■

Pour le résultat concernant les parties diophantiennes pures, il nous faut une caractérisation des relations diophantiennes pures. On suppose que $\mathfrak{R}$ est l'anneau des entiers d'une extension algébrique F de $\mathbb{Q}$. Soit G le groupe de Galois de F sur $\mathbb{Q}$ (c-à-d. le groupe des automorphismes de F sur $\mathbb{Q}$ ou, ce qui est la même chose, celui des automorphismes de $\mathfrak{R}$). On dit qu'une relation T sur $\mathfrak{R}$ est <u>invariante</u> si, pour tout $\sigma \in G$ on a : $T(x_1,\ldots,x_k) \Longrightarrow T(x_1^\sigma,\ldots,x_k^\sigma)$ où α^σ désigne $\sigma(\alpha)$. De même un élément α est invariant ssi $\alpha^\sigma = \alpha$ pour tout $\sigma \in G$. On a :

<u>Proposition</u> 13 : Soit $\mathfrak{R}$ l'anneau des entiers d'une extension de $\mathbb{Q}$ de degré fini. Une relation A sur $\mathfrak{R}$ est diophantienne pure

sur $\mathcal{R}$ si et seulement si elle est diophantienne sur $\mathcal{R}$ et invariante.

Démonstration : Si A est diophantienne pure, elle est a fortiori diophantienne (puisque $\mathbb{Z} \subset \mathcal{R}$) et il est trivial qu'elle est invariante.

Soit donc A une relation diophantienne sur $\mathcal{R}$ qui soit invariante. Soit P le polynôme diophantien (sur $\mathcal{R}$) définissant A :

$$A(a_1,\ldots,a_k) \Longleftrightarrow \exists y_1,\ldots,y_n \in \mathcal{R}\ P(a_1,\ldots,a_k,y_1,\ldots,y_n) = 0 .$$

Pour $\sigma \in G$, désignons par P^σ le polynôme obtenu à partir de P en y remplaçant les coefficients par leurs images selon σ. Le nombre des polynômes obtenus est en fait fini, car chaque coefficient α est algébrique sur $\mathbb{Q}$ et donc α^σ est racine du même polynôme minimal que α. Soient $\sigma_1,\ldots,\sigma_r$ une suite d'automorphismes donnant tous les P^σ (on peut supposer que $\sigma_1 = \mathrm{id}$). Soit

$$Q(x_1,\ldots,x_k,y_1,\ldots,y_n) = \prod_{i=1}^{r} P^{\sigma_i}(x_1,\ldots,x_k,y_1,\ldots,y_n). \qquad (*)$$

Alors $A(a_1,\ldots,a_k) \Longleftrightarrow \exists y_1,\ldots,y_n \in \mathcal{R}\ Q(a_1,\ldots,a_k,y_1,\ldots,y_n) = 0$.

En effet, si $A(a_1,\ldots,a_k)$, comme $P \mid Q$ on a $\exists y_1,\ldots,y_n \in \mathcal{R}$ $P(a_1,\ldots,a_k,y_1,\ldots,y_n)$ puisque A est diophantienne. Supposons $\exists y_1,\ldots,y_n \in \mathcal{R}\ Q(a_1,\ldots,a_k,y_1,\ldots,y_n) = 0$. Alors pour un certain j, $P^{\sigma_j}(a_1,\ldots,a_k,y_1,\ldots,y_n) = 0$ et donc si $\tau = \sigma_j^{-1}$, $P(a_1^\tau,\ldots,a_k^\tau,y_1^\tau,\ldots,y_n^\tau) = 0$. D'où $A(a_1^\tau,\ldots,a_k^\tau)$, avec $\tau \in G$. Comme A est invariante, on a $A(a_1,\ldots,a_k)$ puisque $a_i = (a_i^\tau)^{\sigma_i}$.

Il reste à montrer qu'on peut avoir une définition diophantienne pure de Q. Pour cela, il suffit d'avoir une telle définition pour les coefficients de Q. La démonstration donnée ici suit, à quelques détails près, celle d'un résultat voisin due à R.M. Robinson (cf. [8]). Soit α un coefficient de Q. On remarque, d'après (*) que $\alpha \in \mathcal{R}$ puisque les coefficients des P^{σ_i} sont dans $\mathcal{R}$ et que α est invariant car α est une fonction symétrique des coefficients des P^{σ_i}.

Comme F est une extension de $\mathbb{Q}$ de degré fini, il existe $\theta \in F$ tel que $F = \mathbb{Q}(\theta)$. On peut même supposer que $\theta \in \mathcal{R}$ (en multipliant θ par un entier naturel convenable). Soit U le polynôme irréductible de θ sur $\mathbb{Q}$. On peut prendre U unitaire et à coefficients dans $\mathbb{Z}$. On sait qu'il existe un entier naturel $k \neq 0$ tel que tout élément ε de $\mathcal{R}$ s'écrive : $\varepsilon = \sum_{m=0}^{\nu-1} k^{-1} \lambda_m \theta^m$ où $\lambda_m \in \mathbb{Z}$ et ν est le degré de F sur $\mathbb{Q}$ (cf. un cours d'algèbre). Donc, α étant fixé, il existe un polynôme V à coefficients dans $\mathbb{Z}$ tel que $\alpha = k^{-1}V(\theta)$, ou encore : $k\alpha = V(\theta)$. Soient $\theta_1, \ldots, \theta_q$ les racines de U dans F (elles sont alors dans $\mathcal{R}$ car U est unitaire et à coefficients dans $\mathbb{Z}$). Alors les automorphismes de F sont au nombre de q et entièrement déterminés par $\sigma_j(\theta) = \theta_j$ $(\theta_1 = \theta)$. Donc $k\alpha^{\sigma} = V(\theta^{\sigma})$ où σ est un des σ_j. Comme α est invariant, on a donc $k\alpha = V(\theta_j)$ pour $j = 1, \ldots, q$. Et donc :

$$x = \alpha \iff \exists y \, [U(y) = 0 \;\&\; kx = V(y)]$$

(avec, naturellement, $y \in \mathcal{R}$).

Comme nous l'avons vu dans la démonstration de la proposition 12, comme F est de degré fini sur $\mathbb{Q}$, $\exists y \, [U(y) = 0 \;\&\; kx = V(y)]$ s'écrit :

$$\exists y \, [\Phi_N(U(y), kx - V(y)) = 0]$$

où Φ_N est le polynôme cyclotomique homogène d'un certain ordre N. Et donc $x = \alpha$ est bien une condition diophantienne pure sur $\mathcal{R}$. ■

La démonstration de la proposition 12 montre qu'une relation sur $\mathcal{R}$ récursivement énumérable est diophantienne pure sur $\mathcal{R}$, si et seulement si $\mathbb{Z}$ est diophantien pur sur $\mathcal{R}$ (sous l'hypothèse que F est de degré fini sur $\mathbb{Q}$). Mais alors, d'après la proposition 13, comme $\mathbb{Z}$ est évidemment invariant, s'il est diophantien sur $\mathcal{R}$, il est diophantien pur sur $\mathcal{R}$.

Dans le cas (ii), aucune solution n'est apportée à l'heure actuelle, pas même pour des extensions cubiques. Comme on le voit d'après

les propositions 12 et 13, tout se résume à montrer que Z est diophantien (pur) sur $\mathfrak{R}$. Les auteurs de [1] conjecturent qu'il en est bien ainsi.

Dans le cas de (iii), on ne peut plus utiliser les propositions 12 et 13 dont les démonstrations que nous connaissons font intervenir l'hypothèse de dimension finie d'une façon essentielle. En outre, on peut trouver dans ce cas un ensemble récursivement énumérable et qui n'est pas diophantien sur $\mathfrak{R}$. Soit en effet E l'ensemble des entiers algébriques réels. On peut toujours calculer la partie imaginaire d'un entier algébrique et déterminer si elle est nulle ou non, car on peut se ramener en dimension finie où l'on se trouve alors dans un $\mathbb{Z}$-module (en fonction d'un élément primitif). Or dans ce cas, il est aisé de voir si un nombre est réel ou non (récursivement). Par contre, E n'est pas diophantien sur $\mathfrak{R}$. Supposons le contraire. Il existe un polynôme P tel que $a \in E \Longleftrightarrow \exists y_1,\ldots,y_n\ P(a,y_1,\ldots,y_n) = 0$. Les coefficients de P , $\alpha_1,\ldots,\alpha_k$ sont dans un sous-anneau $\mathfrak{R}' = \mathbb{Z}[\alpha_1,\ldots,\alpha_k]$ de $\mathfrak{R}$, qui est dans une extension de $\mathbb{Q}$ de degré fini. Donc il existe un automorphisme σ de $\mathfrak{R}$ qui laisse cette extension fixe, mais qui transforme un certain élément a de E en un entier algébrique non réel. Or $a \in E \Longrightarrow \exists y_1,\ldots,y_n\ P(a,y_1,\ldots,y_n) = 0$. D'où $P^\sigma(a^\sigma,y_1^\sigma\ldots y_n^\sigma) = 0$. Mais $P^\sigma = P$ par construction de σ . Et donc $a^\sigma \in E$. Or a^σ n'est pas réel. Donc E n'est pas diophantien sur $\mathfrak{R}$. A fortiori, il n'est pas diophantien pur sur $\mathfrak{R}$.

Ceci conduit les auteurs de [1] à penser que dans le cas (iii), la réponse au dixième problème de Hilbert pourrait être positive.

Dans le cas (iv) où $\mathfrak{R} = \mathbb{Q}$, on remarque d'abord que toute partie diophantienne sur $\mathbb{Q}$ est diophantienne pure sur $\mathbb{Q}$, puisque $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$. C'est pourquoi, pour simplifier le vocabulaire, nous parlerons de parties diophantiennes sur $\mathbb{Q}$.

Nous allons montrer que dans le cas $\mathcal{R} = \mathbb{Q}$, le dixième problème de Hilbert équivaut au problème de la décision de la résolubilité des équations diophantiennes homogènes. C'est-à-dire, que le problème se pose pour une sous-classe de la classe des équations diophantiennes. Nous montrerons ensuite, que, comme dans le cas (iii), on obtient une réponse négative du dixième problème relatif à $\mathbb{Q}$ si on établit le caractère diophantien sur $\mathbb{Q}$ de $\mathbb{Z}$.

Proposition 14 : Soit A une relation k-aire sur $\mathbb{Q}$. A est diophantienne sur $\mathbb{Q}$ si et seulement si il existe un entier n et un polynôme homogène $P \in \mathbb{Z}[X_1,\ldots,X_k,Y_1,\ldots,Y_k,Z_1,\ldots,Z_n]$ tel que

$A(a_1,\ldots,a_k) \iff \exists z_1 \in \mathbb{Z},\ldots,z_n \in \mathbb{Z}\ [P(p_1,\ldots,p_k,q_1,\ldots,q_k,z_1,\ldots,z_n) = 0]$

où $a_i = \frac{p_i}{q_i}$, $p_i \in \mathbb{Z}$, $q_i \in \mathbb{N}^*$.

Démonstration : Il suffit de la faire pour $k = 1$. La propriété est évidemment suffisante. Montrons qu'elle est nécessaire :

A étant diophantienne sur $\mathbb{Q}$, il existe un entier m et un polynôme $P_1 \in \mathbb{Z}\ [X,Y_1,\ldots,Y_m]$ tel que :

$$a \in A \iff \exists y_1 \in \mathbb{Q},\ldots,y_m \in \mathbb{Q}\ [P_1(a,y_1,\ldots,y_m) = 0] \ .$$

On observe que si $a = \frac{p}{q}$ avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ et $y_i = \frac{\alpha_i}{\beta_i}$, $\alpha_i \in \mathbb{Z}$ et $\beta_i \in \mathbb{N}^*$, on a : $P_1(a,y_1,\ldots,y_m) = 0 \iff q^d\beta_1^d,\ldots,\beta_m^d\ P_1(a,y_1,\ldots,y_m) = 0$, quelque soit l'entier naturel d . Prenons pour d le maximum du degré de a et de y_i dans P_1 . On a alors que $q^d\beta_1^d,\ldots,\beta_m^d\ P_1(\frac{p}{q},\frac{\alpha_1}{\beta_1},\ldots,\frac{\alpha_m}{\beta_m})$ est une expression polynomiale homogène en $p,q,\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_m$. C-à-d. il existe un polynôme homogène $P \in \mathbb{Z}\ [X,Y,Z_1,\ldots,Z_m,T_1,\ldots,T_m]$ tel que $\forall p\, q\, \alpha_1,\ldots,\alpha_m \beta_1,\ldots,\beta_m$ $(\beta_i \neq 0)$

$q^d\beta_1^d,\ldots,\beta_m^d P_1(\frac{p}{q},\frac{\alpha_1}{\beta_1},\ldots,\frac{\alpha_m}{\beta_m}) = P(p,q,\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_m)$. Donc

$a \in A \iff \exists \alpha_1,\ldots,\alpha_m \in \mathbb{Z}\ \beta_1,\ldots,\beta_m \in \mathbb{N}^*[P(p,q,\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_m) = 0]$.

Comme un entier naturel est somme de quatre carrés de $\mathbb{Z}$, la démonstration est achevée (puisqu'une somme de carré est homogène par

rapport à ses termes). ■

Proposition 15 : Les parties récursivement énumérables de $\mathbb{Q}$ sont les parties de $\mathbb{Q}$ diophantiennes sur $\mathbb{Q}$ ssi $\mathbb{Z}$ est diophantien sur $\mathbb{Q}$.

Démonstration : Elle est calquée sur la preuve de la proposition 12. En effet, si $A \subset \mathbb{Q}$ est récursivement énumérable, on peut construire une partie β de $\mathbb{Z}^2$ telle que :

$$B(p,q) \Longleftrightarrow q \in \mathbb{N}^* \ \& \ \frac{p}{q} \in A \ .$$

Il est clair que B est récursivement énumérable. Donc B est diophantienne au sens ordinaire. Il existe donc un entier n et un polynôme $P \in \mathbb{Z}[X_1,X_2,Y_1,\ldots,Y_n]$ tel que

$$B(p,q) \Longleftrightarrow \exists y_1,\ldots,y_n \in \mathbb{Z}\ [P(p,q,y_1,\ldots,y_n) = 0] \ .$$

Donc :

$$a \in A \Longleftrightarrow \exists p,q,y_1,\ldots,y_n \in \mathbb{Z}\ [q \in \mathbb{N}^* \ \& \ qa = p \ \& \ P(p,q,y_1,\ldots,y_n) = 0] \ .$$

Les relations $p \in \mathbb{Z}$, $q \in \mathbb{Z}$, $y_1 \in \mathbb{Z},\ldots,y_n \in \mathbb{Z}$ sont diophantiennes sur $\mathbb{Q}$ par hypothèses. L'expression $qa = p$ est diophantienne sur $\mathbb{Q}$ puisque $ax - y$ est un polynôme en a,x,y à coefficients dans $\mathbb{Z}$ et que $p \in \mathbb{Z}$, $q \in \mathbb{Z}$ sont diophantiennes sur $\mathbb{Q}$. La condition $q \in \mathbb{N}^*$ l'est aussi car $q \in \mathbb{N}^* \Longleftrightarrow \exists t\,u\,v\,w \in \mathbb{Z}\,[q = t^2+u^2+v^2+w^2+1]$. On utilise implicitement qu'une conjonction de relations diophantiennes sur $\mathbb{Q}$ est diophantienne sur $\mathbb{Q}$. Cela est clair, car sur $\mathbb{Q}$, $\alpha^2+\beta^2 = 0 \Longleftrightarrow \alpha = \beta = 0$. Ce qui achève la démonstration. ■

Il résulte donc des propositions 14 et 15 qu'on peut apporter une réponse négative au dixième problème de Hilbert sur $\mathbb{Q}$ si on trouve un entier n et un polynôme homogène $P \in \mathbb{Z}[X,Y,Z_1,\ldots,Z_n]$ tel que:

$$a|b \Longleftrightarrow \exists y_1,\ldots,y_n \in \mathbb{Z}\ [P(a,b,y_1,\ldots,y_n) = 0] \ .$$

Ce qui est un problème ouvert.

Bibliographie

[1] DAVIS, MATIYASSÉVITCH, J. ROBINSON. Proceedings of Symposia in Pure Mathematics. Vol. 28 (1976), pp. 323-378.

[2] J.P. JONES. Universal Diophantine Equation. The University of Calgary, Dept. Math. Research Paper, n° 274 (avril 75).

[3] MATIYASSÉVITCH. Une nouvelle démonstration du théorème de représentation exponentiellement diophantienne des prédicats récursivement énumérables. Zapiski naoutchnykh seminarov LOMI, t. 60 (1976), pp. 75-89 (en russe).

[4] MATIYASSÉVITCH. Les nombres premiers sont énumérés par un polynôme de 10 variables. Zapisky naoutchnykh seminarov LOMI, t. 68 (1977), pp. 62-82 (en russe).

[5] MATIYASSÉVITCH. "Indécidabilité algorithmique des équations exponentiellement diophantiennes à trois inconnues" in Recherches en théorie des algorithmes et en logique mathématique. Ed. Naouka. Moscou 1979, pp. 69-77 (en russe).

[6] MATIYASSÉVITCH, J. ROBINSON. Reduction of an arbitrary Diophantine equation to one in 13 unknowns. Acta Arithmetica 27, (1974) 521-553.

[7] J. ROBINSON. Existential representability in arithmetic. Trans. Amer. Math. Society, (1952) v. 72, pp. 437-449.

[8] R.M. ROBINSON. Arithmetical definability of field elements. J. Symbolic Logic 16, (1951) pp. 125-126.

[9] C.L. SIEGEL. Zur Theorie der quadratischen Formen. Nachr. Akad. Wiss. Göttingen Math. Phys. KI. II (1972) pp. 21-46.

[10] D. SINGMASTER. Notes on binomial coefficient. I. J. London Math. Soc. (1974) v. 8, n° 3, pp. 545-548.

[11] V.A. USPENSKY. Leçons sur les fonctions calculables. Hermann, Paris (1966) (trad.).

3, rue Mozart
l'Ermitage
91940 LES ULIS