Mémoire

Encadrant : Silvain Rideau-Kikuchi

Thaïs Godet Arthur Molina-Mounier

Table des matières

La question posée par le 10^{e} problème de Hilbert est la suivante : étant donné un polynôme à coefficients entiers, existe-t-il un algorithme permettant de trouver toutes ses solutions entières, ou de déterminer s'il n'en y a pas ? La première partie de ce mémoire, qui s'appuie sur l'article de 1973 de Davis sur le sujet [Dav73], est dédiée à la preuve de la réponde négative qui a été apportée à ce problème. La seconde partie est employée à démontrer que $\mathbb{Z}$ est définissable dans $\mathbb{Q}$ à l'aide de quantificateurs universels, en s'inspirant notamment des travaux de Daans [Daa23]. Ce résultat est un produit des questionnements soulevés par la réponse négative au 10^{e} problème de Hilbert, parmi lesquels figure la question, encore ouverte, du caractère diophantien de $\mathbb{Z}$ dans $\mathbb{Q}$. L'un des enjeux est en effet l'existence d'un algorithme permettant de décider de l'existence de solutions aux équations polynomiales dans $\mathbb{Q}$, ce qui inscrit les travaux portant sur les moyens de définir $\mathbb{Z}$ dans $\mathbb{Q}$ dans la continuité du 10^{e} problème de Hilbert.

I 10^{e} problème de Hilbert

Si la résolution d'équations polynomiales est généralement assez bien comprise, de nombreux problèmes d'une grande complexité apparaissent en n'en étudiant que les solutions entières. Par exemple, l'équation de Pell

$$x^2 - dy^2 = 0$$

ou encore la célèbre l'équation du dernier théorème de Fermat

$$x^p + y^p = z^p \ .$$

Le travail combiné de Davis, Putnam, Robison et Matiyasevich a permis de répondre négativement au 10^{e}problème de Hilbert (Théorème A). Nous nous intéresserons ici à la preuve du théorème apportée par Davis [Dav73].

1 Ensembles diophantiens

Définition 1.1. Une **équation diophantienne** est une équation polynomiale à coefficients entiers à laquelle on cherche des solutions entières.

Définition 1.2. Un ensemble S de n-uplets d'entiers strictement positifs est un **ensemble diophantien** s'il est de la forme

$$S = \{(x_1, \dots, x_n) : \exists (y_1, \dots, y_m), P(x_1, \dots, x_n, y_1, \dots, y_m) = 0\}$$

où P est un polynôme à coefficients entiers, $n, m \in \mathbb{N}$ et $y_1, \dots, y_m$ sont des entiers strictement positifs.

Remarque 1.2.1. Les entiers quantifiés ont été pris strictement positifs alors que le 10^{e} problème de Hilbert mentionne l'existence de solutions entières à une équation diophantienne. Ce choix n'est pas plus contraignant que celui des entiers relatifs, car le théorème des quatres carrés de Lagrange donne une définition diophantienne de $\mathbb{N}^*$ dans $\mathbb{Z}$, à savoir :

$$\mathbb{N}^* = \{n \in \mathbb{Z} : \exists (p, q, r, s) \in \mathbb{Z}^4, n = p^2 + q^2 + r^2 + s^2 + 1\}$$

Sauf mention contraire, toutes les quantités quantifiées ou introduites dans des ensembles seront désormais des entiers strictement positifs.

Exemple 1.2.2. Quelques exemples simples d'ensembles diophantiens :

- Les nombres pairs : n est pair $\iff \exists k, n = 2k$
- Les nombres non premiers : n est composé $\iff \exists (a, b), n = (a + 1)(b + 1)$
- L'ensemble $\{3, 5, 7\} = \{x : (x - 3)(x - 5)(x - 7) = 0\}$
- La relation d'ordre : $x < y \iff \exists k, x + k = y$ et $x \leq y \iff x < y + 1$.
- La congruence à r modulo k : $n \equiv r[k] \iff \exists q, n = (q - 1)k + r$

Définition 1.3. Une **fonction diophantienne** est une fonction $f : (\mathbb{N}^*)^n \to \mathbb{N}^*$ dont le graphe est un ensemble diophantien, i.e pour laquelle $\{(x_1, \dots, x_n, y) : y = f(x_1, \dots, x_n)\}$ est un ensemble diophantien.

2 Prédicats diophantiens

Les exemples cités jusqu'ici sont très simples, voire simplistes. On va s'intéresser aux opérations que l'on peut effectuer sur les ensembles diophantiens, et plus particulièrement sur les formules qui les définissent.

Définition 2.1. On appelle **prédicat diophantien** une formule logique qui définit un ensemble diophantien, sous la forme "$\exists(y_1, \ldots, y_m), P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$" où P est un polynôme à coefficients entiers.

Proposition 2.2. *L'ensemble des prédicats diophantiens est stable par :*

(i) Disjonction logique ("ou" inclusif)

(ii) Conjonction logique ("et")

Démonstration. On peut toujours faire ressortir tous les quantificateurs existentiels jusqu'au plus haut niveau, quitte à renommer des variables pour éviter tout conflit. Cela fait, on remarque les points suivants.

(i) Si $P \in \mathbb{Z}[X_1, \ldots, X_n]$ et $Q \in \mathbb{Z}[X_1, \ldots, X_m]$, alors

$$[P(x_1, \ldots, x_n) = 0 \ \vee \ Q(x_1, \ldots, x_m) = 0] \iff P(x_1, \ldots, x_n)Q(x_1, \ldots, x_m) = 0 \ ,$$

et le polynôme de droite est bien un polynôme en $\max(n, m)$ variables.

(ii) Avec les mêmes objets que précédemment,

$$[P(x_1, \ldots, x_n) = 0 \ \wedge \ Q(x_1, \ldots, x_m) = 0] \iff P^2(x_1, \ldots, x_n) + Q^2(x_1, \ldots, x_m) = 0 \ .$$

Cela conclut la preuve. □

Exemple 2.2.1. Ces opérations permettent d'affirmer que des ensembles et des fonctions plus complexes sont diophantiennes :

- L'opérateur modulo définit $x\%y$ comme l'unique entier $0 \leq z < y$ tel que $x \equiv z \ [y]$. Son graphe est alors égal à

$$\{(x, y, z) : \exists k, z < y \ \wedge \ x = (k-1)y + z\} \ .$$

- L'ensemble des progressions arithmétiques à 3 éléments s'écrit

$$\{(x, y, z), \exists k, y = x + k - 1 \ \wedge \ z = x + 2(k-1)\} \ .$$

3 Fonctions diophantiennes utiles

Théorème 3.1. *Il existe une fonction diophantienne bijective $P(x, y)$ qui associe à chaque couple d'entiers strictement positifs un unique entier strictement positif. De plus, il existe une fonction L telle que $L(P(x, y)) = x$ et une fonction R telle que $R(P(x, y)) = y$, toutes deux diophantiennes.*

Démonstration. On définit $T : n \mapsto \frac{n(n+1)}{2}$. T est croissante, donc il existe, pour tout entier strictement positif z, un unique entier naturel n tel que $T(n) < z \leq T(n+1)$. Par conséquent, il existe un unique entier naturel n et un unique entier strictement positif y tels que

$$z = T(n) + y, \text{ avec } y \leq n + 1 \ ,$$

ce qui revient à dire qu'il existe un unique couple d'entiers strictement positifs (x, y) tel que

$$z = T(x + y - 2) + y \ .$$

On note $P(x, y) = z$, $L(z) = x$ et $R(z) = y$. Ces fonctions sont diophantiennes car

$$\begin{aligned} z = P(x,y) &\iff 2z = (x+y-2)(x+y-1) + 2y \\ x = L(z) &\iff \exists y, [2z = (x+y-2)(x+y-1) + 2y] \\ y = R(z) &\iff \exists x, [2z = (x+y-2)(x+y-1) + 2y] \ . \end{aligned}$$

Ceci conclut la preuve. □

Théorème 3.2. *Il existe une fonction diophantienne $S(i, u)$ telle que :*

- $S(i, u) \leq u$
- *Pour tous $a_1, \ldots, a_n$, il existe u tel que $S(i, u) = a_i$ pour tout $i \in \{1, \ldots, n\}$*

Démonstration. On définit S par $S(i, u) = \alpha$, où α est le reste de la division euclidienne de $L(u)$ par $1 + iR(u)$. À présent, on constate que

$$S(i,u) = v \iff \exists (x,y), u = P(x,y) \ \wedge \ v \equiv x \, [1 + iy] \ \wedge \ v \leq 1 + iy \ .$$

$S(i, u)$ est ainsi diophantienne. De plus, $S(i, u) \leq L(u) \leq u$. Enfin, pour $a_1, \ldots, a_n$ donnés, on choisit $y > a_i$ pour tout $i \in \{1, \ldots, n\}$ tel que $i \mid y$ pour tout $i \in \{1, \ldots, n\}$. Les $1 + iy$ sont alors premiers entre eux. En effet, si $d \mid 1 + ky$ et $d \mid 1 + k'y$ avec $k > k'$, alors $d \mid k - k'$. Dans ce cas, $d \leq n$, et $d \mid y$, donc $d \mid 1$, de sorte que $d = 1$. On peut donc appliquer le théorème des restes chinois pour trouver x tel que $x \equiv a_i \, [1 + iy]$ pour tout $i \in 1, \ldots, n$. On prend $u = P(x, y)$ et on obtient le résultat désiré, puisque $a_i < y = R(u) < 1 + iR(u)$, de sorte que $a_i = S(i, u)$. □

4 Théorie de la récursivité

Définition 4.1. Une fonction est dite **récursive** s'il s'agit de

- la fonction constante égale à 1
- la fonction successeur $s : x \mapsto x + 1$
- une projection $U_n^m : (x_1, \ldots, x_m) \mapsto x_n$

ou si elle s'obtient à partir de fonctions récursives par les opérations suivantes :

(i) La composition : on obtient par composition, avec $g_1, \ldots, g_m$ des fonctions à n arguments et f une fonction à m arguments, la fonction

$$h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) \ .$$

(ii) La minimisation : on obtient par minimisation, avec f et g telles qu'il existe y satisfaisant l'égalité

$$f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y) \ ,$$

une fonction

$$h(x_1, \ldots, x_n) = \min_y [f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y)] \ .$$

(iii) La récurrence : on obtient par récurrence, pour des fonctions $f(x_1, \ldots, x_n)$ et $g(x_1, \ldots, x_{n+2})$ données, une fonction

$$h(x_1, \ldots, x_n, y)$$

telle que

$$h(x_1, \ldots, x_n, 1) = f(x_1, \ldots, x_n)$$

et

$$h(x_1, \ldots, x_n, y+1) = g(y, h(x_1, \ldots, x_n, y), x_1, \ldots, x_n) \ .$$

Les fonctions récursives sont une formalisation de l'idée intuitive de calculabilité, et l'on considère qu'il existe un algorithme permettant de calculer une fonction si et seulement si cette fonction est récursive.

Définition 4.2. Un ensemble est dit **récursif** si sa fonction caractéristique est récursive.

Remarque 4.2.1. S'il existe un algorithme permettant de déterminer si une équation diophantienne admet des solutions, alors la fonction caractéristique de tout ensemble diophantien est récursive.

Définition 4.3. Un ensemble est dit **récursivement énumérable** s'il existe une fonction récursive dont il est l'image.

Cette définition est une formalisation de l'idée intuitive d'un ensemble récursivement énumérable, qui est celle d'un ensemble dont un algorithme est capable d'énumérer (pas nécessairement en un temps fini) les membres.

Théorème 4.4. *Il existe des ensembles rédursivement énumérables qui ne sont pas récursifs.*

Ce théorème bien connu de la théorie de la récursivité est, entre autre, une conséquence du problème de l'arrêt, dont on sait qu'il est indécidable : il n'existe pas d'algorithme permettant de déterminer en un temps fini si un programme informatique donné s'arrêtera. Cependant, il est possible de produire, sur un temps infini, une liste des programmes qui s'arrêtent, tout simplement en exécutant chaque programme et en plaçant dès qu'ils s'arrêtent (quand ils s'arrêtent) les programmes dans cette liste. L'ensemble des programmes qui s'arrêtent est donc récursivement énumérable, mais il n'est pas récursif. Un autre ensemble récursivement énumérable et non récursif sera construit dans la quatrième section de cette partie. Le théorème mentionné ci-dessus est fourni dès cette section car il permet de comprendre la démarche mise en place dans la réponse au 10^{e} problème de Hilbert.

Remarque 4.4.1. Si tout ensemble récursivement énumérable est diophantien, alors les ensembles diophantiens ne peuvent être tous récursifs, ce qui apporte une réponse négative au 10^{e} problème de Hilbert.

Nous allons en fait prouver ici que les fonctions diophantiennes sont exactement les fonctions récursives. Nous savons déjà que cela suffit pour répondre au problème, comme le montre la proposition suivante.

Proposition 4.5. *Si toute fonction récursive est diophantienne, alors tout ensemble récursivement énumérable est diophantien.*

Démonstration. Soit f diophantienne. Par définition, $\{(x_1, \ldots, x_n, y) : y = f(x_1, \ldots, x_n)\}$ est un ensemble diophantien, i.e. $f(x_1, \ldots, x_n) = y \Leftrightarrow \exists (y_1, \ldots, y_m), P(y, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$

pour un certain polynôme P. Ainsi,

$$\{y : \exists (x_1, \ldots, x_n), y = f(x_1, \ldots, x_n)\}$$
$$=$$
$$\{y : \exists (x_1, \ldots, x_n, y_1, \ldots, y_m), P(y, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0\}.$$

On voit donc que si une fonction est diophantienne, alors son image est un ensemble diophantien. Supposons à présent que toute fonction récursive est diophantienne. Alors les images de fonctions récursives, soit les ensembles récursivement énumérables, sont des ensembles diophantiens. □

5 Fonction exponentielle et quantificateurs bornés

On appelle fonction exponentielle la fonction

$$f : \begin{cases} (\mathbb{N}^*)^2 & \to \mathbb{N}^* \\ (n,k) & \mapsto n^k \end{cases}.$$

Celle-ci joue un rôle crucial dans la preuve que les fonctions diophantiennes sont exactement les fonctions récursives. En effet, cette preuve demande de pouvoir utiliser des quantificateurs universels bornés pour définir des ensembles diophantiens, i.e. que

$$S = \{(y, x_1, \ldots, x_n) : \forall z_{\leq y} \exists (y_1, \ldots, y_m), P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0\}$$

soit diophantien. Ceci se prouve en utilisant le fait que la fonction

$$h : (a, b, x) \mapsto \prod_{k=1}^{x} (a + bk)$$

est diophantienne, et ce dernier point est une conséquence du caractère diophantien de la fonction exponentielle.

Théorème 5.1. *La fonction exponentielle est diophantienne.*

Par souci de concision, nous admettons ici ce théorème, démontré par Davis [Dav73] à partir de vingt-quatre lemmes élémentaires utilisant l'équation de Pell :

$$\begin{cases} x^2 - dy^2 = 1 & x, y \geq 0 \\ d = a^2 - 1 & a > 1 \end{cases}.$$

Théorème 5.2. *Les fonctions*

(i) $f : (n,k) \mapsto \binom{n}{k}$

(ii) $g : n \mapsto n!$

(iii) $h : (a, b, x) \mapsto \prod_{k=1}^{x} (a + bk)$

sont diophantiennes.

Démonstration.

(i) Soient $0 < k \leq n$ et $u > 2^n$. Alors

$$\begin{aligned}\sum_{i=0}^{k-1} \binom{n}{i} u^{i-k} &< u^{-1} \sum_{i=0}^{k-1} \binom{n}{i} \\ &\leq u^{-1} \sum_{i=0}^{n} \binom{n}{i} \\ &= u^{-1} 2^n \\ &< 1\end{aligned}$$

donc

$$\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor = \left\lfloor \sum_{i=0}^{n} \binom{n}{i} u^{i-k} \right\rfloor = \sum_{i=k}^{n} \binom{n}{i} u^{i-k}$$

On remarque que pour $i > k$, chaque terme est divisible par u, d'où $\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor \equiv \binom{n}{k} \, [u]$. Par conséquent

$$z = \binom{n}{k} \iff \exists (u, v), u > 2^n \wedge v = \left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor \wedge v \equiv z \, [u] \wedge z < u \ ,$$

ce qui est bien diophantien car l'exponentielle est diophantienne et

$$v = \left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor \iff u^k v \leq (u+1)^n < u^k (v+1) \ .$$

(ii) Supposons $r > (2n)^{n+1}$. Alors d'une part

$$\begin{aligned}\frac{r^n}{\binom{r}{n}} &= \frac{r^n n!}{r(r-1)\cdots(r-n+1)} \\ &= n! \frac{1}{\left(1 - \frac{1}{r}\right) \cdots \left(1 - \frac{n-1}{r}\right)} \\ &< n! \frac{1}{\left(1 - \frac{n}{r}\right)^n} \ .\end{aligned}$$

D'autre part la deuxième égalité permet d'affirmer $r^n / \binom{r}{n} \geq n!$.
De plus, puisque $\frac{n}{r} < \frac{1}{2}$,

$$\begin{aligned}\frac{1}{1 - \frac{n}{r}} &= 1 + \frac{n}{r} + \left(\frac{n}{r}\right)^2 + \dots \\ &< 1 + \frac{n}{r} \left(1 + \frac{1}{2} + \frac{1}{4} + \dots\right) \\ &= 1 + \frac{2n}{r}\end{aligned}$$

et

$$\begin{aligned}\left(1 + \frac{2n}{r}\right)^n = \sum_{i=0}^{n} \binom{n}{i} \left(\frac{2n}{r}\right)^i &< 1 + \frac{2x}{r} \sum_{i=0}^{n} \binom{n}{i} \\ &< 1 + \frac{2n}{r} 2^n \ ,\end{aligned}$$

donc

$$\begin{aligned}\frac{r^n}{\binom{r}{n}} &< n! + n!\frac{2n}{r}2^n \\ &< n! + \frac{2^{n+1}n^{n+1}}{r} \\ &< n! + 1 \ ,\end{aligned}$$

d'où $n! = \left\lfloor r^n / \binom{r}{n} \right\rfloor$, et on conclut comme avant.

(iii) Supposons qu'on ait q et M tels que $bq \equiv a\,[M]$. Alors

$$\begin{aligned}b^y y! \binom{q+y}{y} &= b^y (q+y)(q+y-1)\cdots(q+1) \\ &= (bq+yb)(bq+(y-1)b)\cdots(bq+b) \\ &\equiv (a+yb)(a+(y-1)b)\cdots(a+b)\,[M] \\ &\equiv \prod_{k=1}^{y}(a+kb)\,[M] \ .\end{aligned}$$

On prend $M = b(a+by)^y + 1$. Puisque M et b sont premiers entre eux, on peut trouver q comme ci-dessus et $M > \prod_{k=1}^{y}(a+kb)$, ce qui permet de conclure. □

Théorème 5.3. *Tout ensemble de la forme*

$$S = \{(y, x_1, \ldots, x_n) : \forall z_{\leq y} \exists (y_1, \ldots, y_m), P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0\}$$

est diophantien.

Démonstration. Remarquons d'abord que

$$\begin{gathered}\forall z_{\leq y} \exists (y_1, \ldots, y_m), P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0 \\ \Longleftrightarrow \\ \exists u \forall z_{\leq y} \exists (y_1, \ldots, y_m)_{\leq u}, P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0 \ .\end{gathered}$$

L'implication $\boxed{\Leftarrow}$ est triviale. De plus, si

$$\forall z_{\leq y} \exists (y_1, \ldots, y_m), P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0 \ ,$$

alors pour tout $z \leq y$, en choisissant $y_1^{(z)}, \ldots, y_m^{(z)}$ satisfaisant l'égalité et en posant $u = \max\{y_i^{(z)}, 1 \leq i \leq m, 1 \leq z \leq y\}$, on obtient le membre de gauche et on a donc l'autre sens.

Soit maintenant $Q(y, u, x_1, \ldots, x_n)$ un polynôme tel que

(i) $Q(y, u, x_1, \ldots, x_n) > u$

(ii) $Q(y, u, x_1, \ldots, x_n) > y$

(iii) $[k \leq y \wedge y_1, \ldots, y_m \leq u] \Rightarrow |P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m)| \leq Q(y, u, x_1, \ldots, x_n)$.

Alors

$$\forall k_{\leq y} \exists (y_1, \ldots, y_m)_{\leq u}, P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$$
$$\iff$$
$$\exists (c, t, a_1, \ldots, a_m), \left[\begin{array}{l} 1 + ct = \prod_{k=1}^{x} (1 + kt) \\ \wedge\, t = Q(y, u, x_1, \ldots, x_n)! \\ \wedge\, 1 + ct \mid \prod_{j=1}^{u} (a_1 - j) \;\wedge\; \ldots \;\wedge\; 1 + ct \mid \prod_{j=1}^{u} (a_m - j) \\ \wedge\, P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0\, [1 + ct] \end{array} \right].$$

Prouvons $\boxed{\Leftarrow}$. Pour tout $k \in \{1, \ldots, y\}$, soit p_k un facteur premier de $1 + kt$, et $y_i^{(k)}$ le reste de la division euclidienne de a_i par p_k. On remarque que p_k divise $1 + kt$, qui divise $1 + ct$, qui divise $\prod_{j=1}^{u} (a_i - j)$ pour tout $i \in \{1, \ldots, m\}$. Ainsi, en fixant i, p_k divise $\prod_{j=1}^{u} (a_i - j)$. p_k étant premier, il existe j tel que $p_k \mid a_i - j$. Par conséquent, $j \equiv a_i \equiv y_i^{(k)}\, [p_k]$. De plus, $p_k \mid 1 + kt = 1 + kQ(y, u, x_1, \ldots, x_n)!$, donc p_k ne peut diviser $Q(y, u, x_1, \ldots, x_n)!$, par conséquent $p_k > Q(y, u, x_1, \ldots, x_n) > u$ par (i). Or $j \leq u$ donc $j < p_k$, et $y_i^{(k)}$ étant le reste de la division euclidienne de a_i par p_k, $y_i^{(k)} < p_k$. Grâce à la congruence établie ci-dessus, on peut conclure que $y_i^{(k)} = j$, et donc que $1 \leq y_i^{(k)} \leq u$.

Enfin, $1 + ct \equiv 0 \equiv 1 + kt\, [p_k]$ donc $k + ckt \equiv 0 \equiv c + ckt\, [p_k]$ et ainsi $k \equiv c\, [p_k]$. On sait déjà que $y_i^{(k)} \equiv a_i\, [p_k]$. Par conséquent,

$$P(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)}) \equiv P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0\, [p_k]\ .$$

Comme par (iii)

$$|P(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)})| \leq Q(y, u, x_1, \ldots, x_n) < p_k\ ,$$

on a $P(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)}) = 0$.

Prouvons à présent $\boxed{\Rightarrow}$. Commençons par poser $t := Q(y, u, x_1, \ldots, x_n)!$. Comme

$$\prod_{k=1}^{x} (1 + kt) \equiv 1\, [t]\ ,$$

il existe c tel que $1 + ct = \prod_{k=1}^{x} (1 + kt)$.

On choisit également pour chaque k des $y_1^{(k)}, \ldots y_m^{(k)} \leq u$ satisfaisant l'égalité

$$P(y, k, x_1, \ldots, x_n, y_1^k, \ldots, y_m^{(k)}) = 0\ .$$

Il s'agit maintenant de montrer que les $1+kt$ sont premiers entre eux. Supposons que p divise $1+kt$ et $1+lt$, avec $k>l$. Alors $p \mid (k-l)t$, or si $p \mid t$, $p \mid 1$ puisqu'il divise $1+kt$. Ainsi, $p \mid k-l$, donc $p < y$. Comme, par (ii), $Q(y,u,x_1,\dots,x_n) > y$, $p \mid Q(y,u,x_1,\dots,x_n)! = t$, et l'on obtient une contradiction. Les $1+kt$ sont donc premiers entre eux, et on peut appliquer le théorème des restes chinois pour trouver $a_1,\dots,a_m$ tels que

$$\forall i \in \{1,\dots,m\}, \forall k \in \{1,\dots,y\}, a_i \equiv y_i^{(k)}\ [1+kt]\ .$$

Comme $1+kt \equiv 0 \equiv 1+ct\ [1+kt]$ on a $k \equiv c\ [1+kt]$. Ainsi,

$$P(y,c,x_1,\dots,x_n,a_1,\dots,a_m) \equiv P(y,k,x_1,\dots,x_n,y_1^{(k)},\dots,y_m^{(k)}) = 0\ [1+kt]$$

pour tout $k \in \{1,\dots,y\}$. Puisque les $1+kt$ sont premiers entre eux, on obtient

$$P(y,c,x_1,\dots,x_n,a_1,\dots,a_m) \equiv 0\ [1+ct]\ .$$

De plus, $1+kt \mid a_i - y_i^{(k)}$, et on sait que $1 \leq y_i^{(k)} \leq u$, de sorte que $1+kt \mid \prod_{j=1}^{u}(a_i-j)$, et donc que $1+ct \mid \prod_{j=1}^{u}(a_i-j)$ puisque les $1+kt$ sont premiers entre eux.

On a ainsi prouvé l'équivalence obtenue sous les conditions (i), (ii) et (iii). Or il est toujours possible de construire un polynôme Q satisfaisant ces trois conditions. On écrit $P(y,k,x_1,\dots,x_n,y_1,\dots,y_m)$ sous la forme $\sum_{l=1}^{N} \alpha_l$ avec $\alpha_l = Cy^a k^b x_1^{\gamma_1}\dots x_n^{\gamma_n} y_1^{\delta_1}\dots y_m^{\delta_m}$ et C un entier. On pose alors

$$\beta_l = |C| y^{a+b} x_1^{\gamma_1}\dots x_n^{\gamma_n} u^{\delta_1+\dots+\delta_m}$$

et $Q(y,u,x_1,\dots,x_n) = u + y + \sum_{l=1}^{N} \beta_l$ convient.

Tout ensemble de la forme de l'ensemble S est donc diophantien. □

Remarque 5.3.1. Tout ensemble de la forme

$$R = \{(y,x_1,\dots,x_n) : \exists z_{\leq y} \exists (y_1,\dots,y_m), P(y,z,x_1,\dots,x_n,y_1,\dots,y_m) = 0\}$$

est diophantien, puisque

$$\begin{gathered}\exists z_{\leq y} \exists (y_1,\dots,y_m), P(y,z,x_1,\dots,x_n,y_1,\dots,y_m) = 0 \\ \Longleftrightarrow \\ \exists z, y_1,\dots,y_m, z \leq y \ \wedge\ P(y,z_1,x_1,\dots,x_n,y_1,\dots,y_m) = 0\ .\end{gathered}$$

6 Fonctions diophantiennes, fonctions récursives et conclusion

Proposition 6.1. *Les fonctions polynomiales à coefficients entiers positifs sont récursives.*

Démonstration. On note $U_n^m : (x_1,\dots x_m) \mapsto x_n$ et $s : x \mapsto x+1$

- L'addition est récursive, car $x+y = h_1(x,y)$ avec $h_1(n,1) = s(n)$, $h_1(n,k+1) = g_1(k,h_1(n,k),n)$ et $g_1(z_1,z_2,z_3) = s(z_2) = s(U_2^3(z_1,z_2,z_3))$. On définit ici h_1 par récurrence et g_1 par composition.

- La multiplication est récursive, car $x \cdot y = h_2(x, y)$ avec $h_2(n, 1) = n = U_1^2(n, 1)$ et $h_2(n, k+1) = g_2(k, h_2(n, k), n)$ avec $g_2(z_1, z_2, z_3) = z_2 + z_3 = U_2^3(z_1, z_2, z_3) + U_3^3(z_1, z_2, z_3)$. On définit ici h_2 par récurrence et g_2 est récursive par le point précédent.
- Les fonctions constantes sont récursives, car la fonction $c_1 : x \mapsto 1$ est une fonction de base et que, pour toute constante k, $c_{k+1} : x \mapsto k + 1 = c_k(x) + c_1(x)$.

Toute fonction polynomiale peut s'écrire comme une succession d'additions et de multiplications de variables et de constantes $c_k(U_1^n(x_1, \ldots, x_n))$, ce qui nous donne le résultat désiré. □

Nous admettons la proposition suivante par souci de concision.

Proposition 6.2. *La fonction $S(i, u)$ définie en 3.2 est récursive.*

Théorème 6.3. *Une fonction est diophantienne si et seulement si elle est récursive.*

Démonstration. Montrons dans un premier temps que toute fonction diophantienne est récursive.

Soit f une fonction diophantienne.

$$y = f(x_1, \ldots, x_n) \Leftrightarrow \exists (y_1, \ldots, y_m), P(x_1, \ldots, x_n, y, y_1, \ldots, y_m) = 0$$

pour un certain polynôme P à coefficients entiers, et donc

$$y = f(x_1, \ldots, x_n) \Leftrightarrow \exists (y_1, \ldots, y_m), P_1(x_1, \ldots, x_n, y, y_1, \ldots, y_m) = P_2(x_1, \ldots, x_n, y, y_1, \ldots, y_m)$$

avec P_1 et P_2 à coefficients positifs. Ainsi,

$$f(x_1, \ldots, x_n) = S\left(1, \min_u \begin{bmatrix} P_1(x_1, \ldots, x_n, S(1,u), S(2,u), \ldots, S(m+1,u)) \\ = \\ P_2(x_1, \ldots, x_n, S(1,u), S(2,u), \ldots, S(m+1,u)) \end{bmatrix}\right).$$

f est donc récursive.

Montrons à présent que toute fonction récursive est diophantienne. Cela revient à prouver que l'ensemble des fonctions diophantiennes est clos par composition, minimisation et récurrence, puisque les fonctions de base sont évidemment diophantiennes.

- Soit $h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$ une fonction obtenue par composition à partir de fonctions diophantiennes $f, g_1, \ldots, g_m$. Alors

$$y = h(x_1, \ldots, x_n) \iff \exists (t_1, \ldots, t_m),\ t_1 = g_1(x_1, \ldots, x_n) \wedge \ldots \wedge t_m = g_m(x_1, \ldots, x_n) \wedge y = f(t_1, \ldots, t_m)\ .$$

  h est donc diophantienne.

- Soit $h(x_1, \ldots, x_n) = \min_y [f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y)]$ une fonction obtenue par minimisation à partir de fonctions diophantiennes f et g. Alors

$$y = h(x_1, \ldots, x_n) \iff \exists z, [z = f(x_1, \ldots, x_n, y) \wedge z = g(x_1, \ldots, x_n, y)] \wedge [\forall t_{\leq y}, [(t = y) \vee [\exists (u, v), u = f(x_1, \ldots, x_n, t) \wedge v = g(x_1, \ldots, x_n, t) \wedge (u < v \vee v < u)]]]\ .$$

  h est donc diophantienne.

- Soit $h(x_1, \ldots, x_n, z)$ telle que

$$\begin{aligned} h(x_1, \ldots, x_n, 1) &= f(x_1, \ldots, x_n) \\ h(x_1, \ldots, x_n, z+1) &= g(z, h(x_1, \ldots, x_n, z), x_1, \ldots, x_n) \end{aligned}$$

obtenue par récurrence à partir de fonctions diophantiennes f et g. Alors

$$\begin{gathered} y = h(x_1, \ldots, x_n, z) \\ \Longleftrightarrow \\ \exists u, \exists v, \begin{bmatrix} v = S(1,u) \\ \wedge\, v = f(x_1, \ldots, x_n) \\ \wedge\, \forall t_{\leq z}[(t = z) \vee \exists w, (w = S(t+1,u) \wedge w = g(t, S(t,u), x_1, \ldots, x_n))] \\ \wedge\, y = S(z,u) \end{bmatrix} . \end{gathered}$$

h est donc diophantienne.

□

Il est désormais possible de construire un ensemble diophantien non récursif, comme annoncé en deuxième partie. On construit dans ce but une énumération explicite des ensembles diophantiens. Pour cela, il suffit de posséder une énumération des polynômes à coefficients entiers positifs.

On remarque que tout polynôme de cette sorte peut être obtenu à partir de la constante 1 et des variables $x_0, x_1, x_2 ...$ par additions et multiplications successives. On définit :

$$\begin{cases} P_1 & = 1 \\ P_{3n-1} & = x_{n-1} \\ P_{3n} & = P_{L(n)} + P_{R(n)} \\ P_{3n+1} & = P_{L(n)} P_{R(n)} \end{cases}$$

Les P_k constituent une énumération des polynômes à coefficients positifs.

Remarquons que pour tout entier n, P_n ne peut pas contenir plus de $n+1$ variables, puisque $L(n) \leq n$ et $R(n) \leq n$. On définit alors

$$D_n = \left\{ x : \exists (x_1, \ldots, x_n), [P_{L(n)}(x, x_1, \ldots, x_n) = P_{R(n)}(x, x_1, \ldots, x_n)] \right\} .$$

Les D_n constituent une énumération des ensembles diophantiens.

Proposition 6.4. *$\{(n,x) : x \in D_n\}$ est diophantien.*

Démonstration. On prouve que

$$\begin{gathered} x \in D_n \\ \Longleftrightarrow \\ \exists u, \begin{bmatrix} S(1,u) = 1 \\ \wedge\, S(2,u) = x \\ \wedge\, \forall k_{\leq n}[S(3k,u) = S(L(k),u) + S(R(k),u)] \\ \wedge\, \forall k_{\leq n}[S(3k+1,u) = S(L(k),u) S(R(k),u)] \\ \wedge\, S(L(n),u) = S(R(n),u) \end{bmatrix} . \end{gathered}$$

Soient x et n tels que $x \in D_n$. Alors, il existe $t_1, \ldots, t_n$ tels que $P_{L(n)}(x, t_1, \ldots, t_n) = Q_{R(n)}(x, t_1, \ldots, t_n)$. On choisit u tel que $S(i, u) = P_i(x, t_1, \ldots, t_n)$ pour tout $i \in 1, \ldots, 3n+2$, de sorte que le membre de gauche de l'équivalence est vérifié. Pour le sens inverse, on pose $t_{i-1} := S(3i-1)$ pour tout $i \in 2, \ldots, n+1$, et l'on obtient que $P_{L(n)}(x, t_1, \ldots, t_n) = Q_{R(n)}(x, t_1, \ldots, t_n)$, et donc que $x \in D_n$. □

Proposition 6.5. *$V := \{n : n \notin D_n\}$ n'est pas diophantien.*

Démonstration. Si V est diophantien, alors il existe n tel que $V = D_n$. Dans ce cas, $n \in V \Leftrightarrow n \in D_n$, mais $n \in V \Leftrightarrow n \notin D_n$, et l'on aboutit à une contradiction. □

Proposition 6.6. *Soit* $g : (n, x) \mapsto \begin{cases} 1 & \text{si } x \notin D_n \\ 2 & \text{sinon} \end{cases}$.
Alors g n'est pas récursive.

Démonstration. Si g était récursive, elle serait diophantienne, et alors V serait diophantien. En effet, on aurait pour un certain polynôme P :

$$g(n, x) = y \Leftrightarrow \exists (y_1, \ldots, y_m), P(n, x, y, y_1, \ldots, y_m) = 0 \ .$$

Ainsi, $V = \{x : \exists (y_1, \ldots, y_m), P(n, x, 1, y_1, \ldots, y_m) = 0\}$. □

Theorème A. *Il n'existe pas d'algorithme permettant de décider, pour n'importe quelle équation diophantienne, si celle-ci possède ou non des solutions.*

Démonstration. Dans le cas contraire, g serait récursive, car par 6.4, $x \in D_n$ si et seulement si, pour un certain polynôme P, $P(n, x, y_1, \ldots, y_m) = 0$ possède des solutions. □

II Définition universelle de $\mathbb{Z}$ dans $\mathbb{Q}$

Après avoir étudié les ensembles diophantiens dans $\mathbb{Z}$, le prolongement naturel est de voir ce qu'il se passe dans d'autres ensembles, notamment $\mathbb{Q}$. Dans cette partie, l'enjeu est d'arriver au résultat suivant :

Theorème B. *Il existe $P \in \mathbb{Z}[X, Y_1, \dots, Y_{16}]$ tel que*

$$\mathbb{Z} = \{x \in \mathbb{Q} : \forall (y_1, \dots, y_{16}) \in \mathbb{Q}^{16}, P(x, y_1, \dots, y_{16}) = 0\} \ .$$

Cela revient à dire que $\mathbb{Q}\backslash\mathbb{Z}$ est diophantien dans $\mathbb{Q}$, en n'employant pas plus de 16 quantificateurs existentiels. Nous reprenons pour cela les méthodes présentées par Daans [Daa23]. À cet effet, nous présentons d'abord des résultats en logique et en théorie algébrique des nombres auxquels la preuve fait appel.

1 Définissabilité par quantificateurs

La *signature* d'une structure algébrique est la donnée des constantes et opérations de base qui la caractérisent. La signature des anneaux $\mathcal{L}_{\text{ann}}$ est donnée par deux constantes 0 et 1, ainsi que les opérations binaires $+$, $-$, $\cdot$. La signature des corps $\mathcal{L}_{\text{corps}}$ comporte en plus une opération unaire $\cdot^{-1}$, en prenant la convention $0^{-1} = 0$. Pour un corps ou un anneau donné, on identifie naturellement les données de la signature avec celles de l'objet en question. Pour $\mathcal{L}$ une signature et $C \subseteq K$, on note $\mathcal{L}(C)$ la signature à laquelle on a adjoint tous les éléments de C en tant que constantes. Un $\mathcal{L}$-terme est une expression construite inductivement à partir de variables libres (distinctes des constantes), des constantes et des opérations de $\mathcal{L}$.

Une $\mathcal{L}$-formule sans quantificateurs est une formule logique ϕ construite inductivement à partir de $\mathcal{L}$-termes, de l'égalité, ainsi que de la conjonction, disjonction et négation logique. Si X est libre dans ϕ une $\mathcal{L}$-formule et t un $\mathcal{L}$-terme, on note $\phi(X|t)$ la formule obtenue en remplaçant les instances de X par t. Si K est une $\mathcal{L}$-structure, ϕ une $\mathcal{L}(K)$-formule et $x_1, \dots, x_n$ sont des variables libres dans ϕ, on pourra noter $\phi = \phi(x_1, \dots, x_n)$. Si $a_1, \dots, a_n \in K$ une $\mathcal{L}$-structure, on notera $\phi(a_1, \dots, a_n) = \phi(x_1|a_1, \dots, x_n|a_n)$. On appelera "$\mathcal{L}$-formule existentielle à m quantificateurs", notée $\exists_m$-$\mathcal{L}$-formule, une $\mathcal{L}$-formule sans quantificateurs précédée de m quantificateurs existentiels portant sur des variables libres dans la formule originelle. On appellera "$\exists_m$-formule" une $\exists_m$-$\mathcal{L}_{\text{corps}}(K)$-formule et "formule m-diophantienne" une $\exists_m$-$\mathcal{L}_{\text{ann}}(K)$-formule *sans négation logique*. On notera $K \models \phi$ si ϕ est vraie dans K.

Théorème 1.1. *Soit $\phi(x_1, \dots, x_n)$ une $\mathcal{L}_{corps}$-formule sans quantificateurs. Alors il existe une $\mathcal{L}_{ann}$-formule sans quantificateurs $\psi(x_1, \dots, x_n)$ telle que pour tout corps K vu naturellement comme une $\mathcal{L}_{corps}$-structure, on ait :*

$$\forall (a_1, \dots, a_n) \in K^n, K \models \phi(a_1, \dots, a_n) \iff K \models \psi(a_1, \dots, a_n) \ .$$

Observation 1.1.1. Ce théorème permet de faire abstraction de la différence entre une $\mathcal{L}_{\text{ann}}$-formule et une $\mathcal{L}_{\text{corps}}$-formule du point de vue logique.

Intuition. Le théorème énonce qu'on peut passer d'une expression dans les corps à une expression dans les anneaux en "annulant les dénominateurs". Par exemple, la formule $ab^{-1} = 1$ est équivalente à la formule $a = b \wedge b \neq 0$. La preuve retranscrit cette idée de manière formelle.

Démonstration. Soit $n \in \mathbb{N}$ et $t(x_1, \dots, x_n), s(x_1, \dots, x_n)$ deux $\mathcal{L}_{\text{ann}}(K)$-termes. Par induction structurelle, on peut trouver deux polynômes $f, g \in \mathbb{Z}[X_1, \dots, X_n]$ qui coincident avec l'évaluation du terme respectif (qu'on peut aussi définir inductivement) en chaque point de K^n. Soit $d \in \mathbb{N}$ et $f_0, \dots, f_d \in \mathbb{Z}[X_2, \dots, X_n]$ tels que $f = \sum_{i=0}^{d} X_1^i f_i(X_2, \dots, X_n)$. Posons $h = \sum_{i=0}^{d} X_1^{d-i} f_i(X_2, \dots, X_n)$.

On peut alors vérifier l'équivalence de la formule $t(x_1|x_1^{-1}) = s$ avec

$$\begin{aligned}&(x_1 \neq 0 \ \wedge \ h(x_1, \dots, x_n) = x_1^d g(x_1, \dots, x_n))\\ \vee\ &(x_1 = 0 \ \wedge \ f(0, x_2, \dots, x_n) = g(0, x_2, \dots, x_n))\end{aligned}$$

Si $\phi(x_1, \dots, x_n)$ est une $\mathcal{L}_{\text{corps}}(K)$-égalité sans quantificateurs, elle est équivalente à une égalité où tout a été distribué. Si besoin, on pourra introduire de nouvelles variables libres de façon à ce que tous les inverses soient appliqués à des variables, puis effectuer la substitution à la fin ; histoire de ne pas tomber dans une boucle, il faudrait s'occuper de ces nouvelles variables avant les anciennes variables desquelles elles dépendent. Si jamais les nouvelles variables contiennent elles-mêmes des inverses, il suffit d'itérer le processus total, ce qui terminera par finitude de la formule de base.

Dans le cadre d'anneaux commutatifs (il le seront ici), s'il y a des termes où une variable est multipliée par son inverse, on peut éliminer ces facteurs en faisant une disjonction de cas similaire à celle ci-dessus. On a alors une égalité équivalente qui peut bien s'écrire sous la forme $t(x_1|x_1^{-1}) = s$. On conclut par induction structurelle. □

Lemme 1.2. *Si K est un corps non algébriquement clos, pour tout $n > 1$ il existe $F_n \in K[X_1, \dots, X_n]$ tel que*

$$F_n(x_1, \dots, x_n) = 0 \iff x_1 = \cdots = x_n = 0$$

.

Démonstration. Comme K n'est pas algébriquement clos, il existe $P \in K[X]$ irréductible de degré $d \geq 2$. Alors le polynôme homogénéisé $P^*(X, Y) = Y^d P(\frac{X}{Y})$ n'a aucune racine non triviale. La suite de polynômes définie par $F_2 = P^*$ et $F_{n+1}(X_1, \dots, X_{n+1}) = P^*(F_n(X_1, \dots, X_n), X_{n+1})$ convient alors. □

Lemme 1.3. *Soit K un corps non algébriquement clos. Alors les formules diophantiennes dans K sont équivalentes aux prédicats diophantiens sur K au sens de I.2.1 et de plus, si φ, ψ sont respectivement des formules $\exists_m$- et $\exists_n$-K-diophantiennes, alors :*

(i) $\varphi \vee \psi$ est équivalente à une $\exists_{\max(m,n)}$-formule.

(ii) $\varphi \wedge \psi$ est équivalente à une $\exists_{m+n}$-formule.

Démonstration. Pour l'équivalence des deux notions, comme dans les deux cas les quantificateurs existentiels sont tout au début, il suffit de vérifier, par induction structurelle, que le résultat est conservé par disjonction et conjonction. La disjonction est donnée par multiplication, à l'instar de la preuve de 2.2 (ii), et la conjonction est donnée par 1.2.

Concernant le nombre de quantificateurs, dans le cas de la disjonction on peut confondre les variables des deux termes autant que possible avant la multiplication, et dans le cas de la conjonction il suffit de rendre distinctes les variables de chaque terme. □

Théorème 1.4. *Soient K un corps non algébriquement clos et $m, n > 0$. Si un ensemble $D \subseteq K^n$ est $\exists_m$-K-définissable (i.e définissable par une $\exists_m$-K-formule), il est $m+1$-diophantien, i.e il existe $P \in K[X_1, \dots, X_n, Y_1, \dots, Y_{m+1}]$ tel que*

$$D = \{x \in K^n : \exists y \in K^{m+1}, P(x, y) = 0\} \ .$$

Démonstration. Soit D défini par la $\exists_m$-formule φ. Par 1.1, on a ψ une formule m-diophantienne équivalente. Par distributivité, on peut la mettre sous *forme normale disjonctive*

$$\psi = \exists_m \bigvee_i \psi_i \ ,$$

où les ψ_i ne contiennent que des conjonctions d'égalités et éventuellement de non-égalités. En remarquant que

$$x_1 \neq 0 \ \wedge \ \cdots \ \wedge \ x_n \neq 0 \iff \exists y, x_1 \cdots x_n y = 1 \ ,$$

on peut retirer ces négations. Les $\mathcal{L}_{\text{ann}}$-formules sont équivalentes à des égalités de polynômes avec zéro, donc en confondant l'éventuelle nouvelle variable introduite dans chaque membre membre, on peut faire ressortir au plus un quantificateur existentiel au début, et donc définir D avec un seul quantificateur existentiel en plus. On conclut avec 1.3. □

Théorème 1.5. *Soit R un sous-anneau de $\mathbb{Q}$ intégralement clos (i.e toute racine d'un polynôme unitaire à coefficients dans R est lui-même dans R). Alors*

$$x \in R^\times \iff [x \neq 0 \ \wedge \ x + x^{-1} \in R] \ .$$

En particulier, si R est $\exists_m$-définissable, $R^\times$ aussi.

Démonstration. Le sens direct est évident. Supposons $x \neq 0$ et $x + x^{-1} = y \in R$. Alors x est racine du polynôme $X^2 - yX + 1 \in R[X]$, donc $x \in R$ par hypothèse, et $x^{-1} = y - x \in R$ donc $x \in R^\times$. □

2 Corps valués

Définition 2.1. Pour K un corps, une **valuation** sur K est une fonction surjective $v : K \to \mathbb{Z} \cup \{\infty\}$ satisfaisant :

(i) $\forall x \in K,\ v(x) = \infty \iff x = 0$.

(ii) $\forall x, y \in K,\ v(xy) = v(x) + v(y)$. *(morphisme sur K^*)*

(iii) $\forall x, y \in K,\ v(x + y) \geq \min(v(x), v(y))$. *(inégalité ultramétrique)*

On dit alors que (K, v) est un **corps valué**. On dit qu'une valuation v est *dyadique* si $v(2) > 0$. On notera $\mathcal{V}_K$ l'ensemble des valuations sur K.

Exemple 2.1.1. Pour p un nombre premier fixé, la *valuation p-adique* v_p est définie sur $\mathbb{Q}$ par : si $x \in \mathbb{Q}^*$, on peut écrire $x = p^n \frac{a}{b}$ de manière unique avec a et b premiers avec p. Alors $v_p(x) = n$.

Proposition 2.2 (Propriétés arithmétiques des valuations)**.** *Soit v une valuation sur K.*

- $v(\pm 1) = 0$.
- $\forall x \in K^*, v(x^{-1}) = -v(x)$.
- $\forall x \in K, v(x) = v(-x)$.
- *Si $x, y \in K$ et $v(x) \neq v(y)$, alors $v(x + y) = \min(v(x), v(y))$.*

Démonstration. On a $v(1) = v(1^2) = 2v(1)$ d'où $v(1) = 0$. Si $x \in K^*$, alors $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$. De plus, $2v(-1) = v\big((-1)^2\big) = v(1) = 0$ d'où $v(-1) = 0$. On en déduit que pour $x \in K$, $v(-x) = v(-1) + v(x) = v(x)$.

Soient $x, y \in K$ avec par exemple $v(x) < v(y)$. Si on avait $v(x + y) > v(x)$, on aurait $v(x) = v(x + y - y) \geq \min(v(x + y), v(-y)) > v(x)$, une absurdité. □

Définition 2.3. Pour (K, v) un corps valué, v induit une norme $|\cdot|_v$ sur K, définie par

$$\forall x \in K, |x|_v = c^{-v(x)}$$

avec $c > 1$ quelconque. Le complété de K par rapport à la topologie résultante (qui ne dépend pas du choix de c) est noté K_v. On définit en outre les objets suivants :

- *Anneau de valuation de v :* $\mathcal{O}_v = \{x \in K, v(x) \geq 0\}$.
- *Idéal maximal de valuation :* $\mathfrak{m}_v = \{x \in K, v(x) > 0\}$.
- *Corps résiduel de v :* $\overline{K_v} = \mathcal{O}_v/\mathfrak{m}_v$. Pour $x \in \mathcal{O}_v$, on notera $\bar{x}$ sa classe d'équivalence modulo $\mathfrak{m}_v$.

Observation 2.3.1. Le groupe $\mathcal{O}_v^\times$ des éléments inversibles de $\mathcal{O}_v$ est précisément l'ensemble des éléments de valuation nulle. On peut alors le lire à travers $\overline{K_v}$: $a \in \mathcal{O}_v^\times \iff \bar{a} \neq \bar{0}$.

Remarque 2.3.2. Le fait que $\mathcal{O}_v$ soit un anneau et $\mathfrak{m}_v$ un idéal maximal se déduisent de la définition des valuations. Quant au fait que $\overline{K_v}$ soit un corps, c'est un résultat classique d'algèbre.

La norme induite par une valuation telle qu'on l'a définie est appellée une norme "ultramétrique", en raison de la version plus forte de l'égalité triangulaire qu'elle satisfait. La topologie des espaces ultramétriques (i.e ceux munis d'une telle norme) a beaucoup de propriétés assez pathologiques :

- Tout point à l'intérieur d'une boule en est un centre.
- Si deux boules ne sont pas disjointes, l'une est contenue dans l'autre.
- Toutes les boules sont ouvertes et fermées à la fois. En particulier, K et K_v sont totalement déconnectés pour cette topologie.
- Les fibres d'une valuation $\{x \in K : v(x) = k\}$ sont ouvertes et fermées.

Exemple 2.3.3. Pour p premier, la complétion $\mathbb{Q}_{v_p}$ est notée $\mathbb{Q}_p$ et constitue le corps des nombres p-adiques. On note également $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ l'ensemble des entiers p-adiques, i.e l'ensemble des nombres p-adiques de valuation positive. Toujours dans le cas p-adique, on a $\mathfrak{m}_{v_p} = p\mathcal{O}_{v_p}$ d'où $\overline{\mathbb{Q}_{v_p}} \simeq \mathbb{Z}/p\mathbb{Z}$.

Théorème 2.4 (Ostrowski)**.** *Les seules valuations sur $\mathbb{Q}$ sont les valuations p-adiques v_p, avec p décrivant les nombres premiers.*

Voici maintenant plusieurs théorèmes d'approximation importants et très utiles pour travailler sur les corps de nombres valués.

Théorème 2.5 (Lemme de Hensel)**.** *Soit (K, v) un corps valué complet. Soit $f \in \mathcal{O}_v[X]$ et $a_0 \in \mathcal{O}_v$ tel que $v(f(a_0)) > 2v(f'(a_0))$. Alors il existe $a \in \mathcal{O}_v$ tel que $f(a) = 0$ et $v(a_0 - a) > v(f'(a_0))$.*

Corollaire 2.5.1. *Pour $f = \sum_{i=0}^{d} c_i X^i \in \mathcal{O}_v[X]$ de polynôme résiduel $\bar{f} = \sum_{i=0}^{d} \bar{c}_i X^i \in \mathfrak{m}_v[X]$, si $\bar{f}$ possède un zéro simple dans $\mathfrak{m}_v$, i.e $\bar{a}_0 \in \mathfrak{m}_v$ tel que $\bar{f}(\bar{a}_0) = 0$ et $\bar{f}'(\bar{a}_0) \neq 0$, alors f a un zéro $a \in \mathcal{O}_v$ tel que $\bar{a} = \bar{a}_0$.*

On se réfèrera à [EP05], 1.3.1 et 1.3.2 pour une preuve.

Intuition. D'après la définition de la norme, un grande valuation désigne un élément petit. L'intuition graphique (qui n'est qu'une grossière heuristique) du lemme de Hensel est que si la valeur de f en un point a est petite comparée à sa dérivée, alors f s'annule en un voisinage de ce point, au moins aussi proche de a que l'intersection de la tangente en a avec l'axe des abscisses.

Ceci contraste avec le cas réel, où un polynôme peut être arbitrairement proche de 0 avec une dérivée arbitrairement grande sans pour autant s'annuler quelque part. En d'autres termes, le théorème permet de déduire un véritable zéro d'un zéro approché.

Dans le cas p-adique, le corps résiduel est $\mathbb{Z}/p\mathbb{Z}$, donc la recherche de solutions à des équations polynomiales dans $\mathbb{Z}_p$ revient à une recherche dans $\mathbb{Z}/p\mathbb{Z}$, bien plus simple.

Exemple 2.5.2. Pour la valuation 5-adique, considérons $f = X^2 + 1 \in \mathcal{O}[X]$. On a $\bar{f}(\bar{2}) = \bar{0}$ et $\bar{f}'(\bar{2}) = \bar{4} \neq \bar{0}$, donc il existe $x \in \mathbb{Z}_5$ tel que $x^2 = -1$.

Théorème 2.6 (Théorème d'approximation faible)**.** *Soient $v_1, \dots, v_n$ des valuations distinctes sur K un corps, $a_1, \dots, a_n \in K$ et $\gamma_1, \dots, \gamma_n \in \mathbb{Z}$. Alors il existe $b \in K$ tel que*

$$\forall 1 \leq i \leq n, v_i(a_i - b) > \gamma_i \ .$$

De manière équivalente, si on note K_i le corps valué (K, v_i), alors la diagonale $\Delta = \{(x, \dots, x) : x \in K\}$ est dense dans $\prod_{i=1}^{n} K_i$.

Nous allons maintenant prouver le théorème.

Lemme 2.7. *Soient v, v' deux valuations distinctes sur K. Alors il existe $x \in K$ tel que $v(x) > 0$ et $v'(x) \leq 0$.*

Démonstration. Par contraposée, supposons que $\forall x \in K, v(x) > 0 \iff v'(x) > 0$. On en déduit que $v(x) \neq 0 \iff v'(x) \neq 0$ par un passage à l'inverse. Soient donc $a, b \in K$ de valuation non nulle pour v et v'. On a alors

$$\begin{aligned}
&\forall n, m \in \mathbb{Z}^*, (v(a^n b^m) \geq 0 \iff v'(a^n b^m) \geq 0) \\
\iff &\forall n, m \in \mathbb{Z}^*, (nv(a) + mv(b) \geq 0 \iff nv'(a) + mv(b) \geq 0) \\
\iff &\forall n, m \in \mathbb{Z}^*, \left(\frac{v(a)}{v(b)} \geq -\frac{m}{n} \iff \frac{v'(a)}{v'(b)} \geq -\frac{m}{n}\right) \\
\iff &\frac{v(a)}{v(b)} = \frac{v'(a)}{v'(b)} \\
\iff &\frac{v(a)}{v'(a)} = \frac{v(b)}{v'(b)}
\end{aligned}$$

Comme a, b sont quelconques, on a que $v = cv'$ pour $c \in \mathbb{Q}$. v est à valeurs entières donc $c \in \mathbb{Z}$. v est surjective donc $c = \pm 1$. v est une valuation donc $c = 1$, i.e $v = v'$. □

Démonstration (de 2.6). Montrons par récurrence sur n qu'il existe $a \in K$ tel que $v_1(a) < 0$ et $v_k(a) > 0$ pour $2 \leq k \leq n$.

- Supposons $n = 2$. Par 2.7 soit $x \in K$ tel que $v_1(x) > 0$ et $v_2(x) \leq 0$, et symétriquement $y \in K$ tel que $v_1(y) \leq 0$ et $v_2(y) > 0$. Alors $a = \frac{y}{x}$ convient.
- Supposons $n > 2$. Soit donc $a \in K$ tel que $v_1(a) < 0$ et $v_k(a) > 0$ pour $2 \leq k \leq n-1$. Soit de plus $b \in K$ tel que $v_n(b) > 0$ et $v_1(b) < 0$. Plusieurs cas :
  - Si $v_n(a) > 0$, alors a convient.
  - Si $v_n(a) = 0$, alors $a^r b$ convient pour un r assez grand.
  - Si $v_n(a) < 0$, alors $\frac{1}{1+a^{-r}} b$ convient pour r assez grand.

Par symétrie, on obtient $c_1, \dots, c_n \in K$ tels que pour tout $1 \leq i \leq n$, $v_i(c_i) < 0$ et $v_j(c_i) > 0$ pour $j \neq i$. Alors, $\delta_{i,r} = \frac{1}{1+c_i^{-r}}$ est tel que $v_i(\delta_{i,r} - 1) \underset{r \to \infty}{\to} \infty$ et pour $j \neq i$, $v_j(\delta_{i,r}) \underset{r \to \infty}{\to} \infty$. En d'autres termes, ce terme converge vers 1 pour $|\cdot|_{v_i}$ et vers 0 pour les autres $|\cdot|_{v_j}$.

Par conséquent, pour r suffisamment grand, $b = \sum_{i=1}^{n} \delta_{i,r} a_i$ convient. □

3 Algèbres de quaternions

La preuve du théorème B fait beaucoup appel à la théorie des algèbres de quaternions. Les outils utilisés ici reposent sur des résultats très avancés, certains dont nous sommes obligés d'omettre la preuve.

Définition 3.1. Un **corps de nombres** est une extension finie de $\mathbb{Q}$.

Définition 3.2. Une **algèbre de quaternions** sur K un corps est une K-algèbre de dimension 4, qui est également *centrale* (son centre est K) et *simple* (elle ne possède pas d'idéaux bilatères non triviaux). On dit qu'elle est **scindée** si elle est isomorphe à $\mathcal{M}_2(K)$.

Remarque 3.2.1. C'est un résultat non trivial qu'une algèbre de quaternions est scindée si et seulement si elle contient des diviseurs de zéro. Voir [Che10], Proposition 1.2.

Définition 3.3 (Extension de scalaires, non-réalité)**.** Soit Q une algèbre de quaternions sur K et $f : K \to L$ un morphisme de corps. Alors f induit une structure de K-espace vectoriel sur L via $k \cdot \ell = f(k)\ell$. On peut donc définir **l'extension de scalaires** de Q à L par $Q \otimes_K L$, qui est également une algèbre de quaternions. Si $Q \otimes_K L$ est scindée, on dit que Q *est scindée sur* f.

On dit que Q est **non-réelle** si Q est scindée sur tout morphisme de K dans $\mathbb{R}$. Par définition, Q est également non-réelle si aucun tel morphisme n'existe.

Dans le cas particulier où L/K est une extension de corps, l'inclusion est le choix canonique du morphisme f. Si cette extension est scindée, on dira alors que Q *est scindée sur* L et que L est un corps de scission de Q, sans faire référence au morphisme. Si Q est une algèbre de quaternions sur K, on pose

$$\Delta Q = \{v \in \mathcal{V}_K : Q \text{ n'est pas scindée sur } K_v\}$$

où $\mathcal{V}_K$ est l'ensemble des valuations sur K et K_v est défini dans 2.3.

Exemple 3.3.1. Si $K = \mathbb{Q}(\sqrt{2})$, alors la K-algèbre engendrée par $u^2 = -1$, $v^2 = 1 - \sqrt{2}$ et $uv = -vu$ est une algèbre de quaternions. Elle n'est pas scindée en tant qu'algèbre de quaternions sur l'extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, donc elle n'est pas non-réelle. Cependant, elle est scindée sur le morphisme de corps $K \to \mathbb{R}$ qui envoie $\sqrt{2}$ sur $-\sqrt{2}$, car on a alors

$$\left(\sqrt{1+\sqrt{2}}\right)^2 = v^2 = 1+\sqrt{2} \implies \underbrace{\left(\sqrt{1+\sqrt{2}}+v\right)}_{\neq 0}\underbrace{\left(\sqrt{1+\sqrt{2}}-v\right)}_{\neq 0} = 0$$

dans l'extension de scalaires.

4 Résultats admis

Proposition 4.1 ([Daa21], 6.7)**.** *Soit K un corps de nombres, $S \subseteq \mathcal{V}_K$ fini. Alors il existe $S' \supseteq S$ tel que $|S'|$ est impair et $\pi \in K^*$ tel que $S' = \{v \in \mathcal{V}_K : v(\pi)$ est impair$\}$.*

Remarque 4.1.1. Ce résultat est très simple quand $K = \mathbb{Q}$. Par le théorème d'Ostrowski, un ensemble fini de valuations $S = \{v_1, \dots, v_n\}$ sur $\mathbb{Q}$ est l'ensemble des valuations correspondant à un ensemble fini de nombres premiers $p_1, \dots, p_n$, et alors on a $S = \{v \in \mathcal{V}_\mathbb{Q} : v(p_1 \cdots p_n)$ est impair$\}$.

Proposition 4.2 (Paramétrisation des algèbres de quaternions, cf. [Alb39], IX.10)**.** *Si $a, b \in K$ sont tels que $(1+4a)b \neq 0$, la K-algèbre $[a,b)_K$ engendrée par $1, u, v$ avec $u^2 - u = a$, $v^2 = b$ et $uv + vu = v$ est une algèbre de quaternions. De plus, toute algèbre de quaternions sur K est de cette forme.*

Remarque 4.2.1. Une autre paramétrisation un peu plus simple et courante est donnée par les $(a,b)_K$ avec $a,b \neq 0$, engendrée par $u^2 = a$, $v^2 = b$ et $uv = -vu$.

Le résultat suivant montre que même si toutes les algèbres de quaternions ne sont pas scindées, on peut toujours y définir certains objets matriciels.

Proposition 4.3 (Trace et norme réduite, cf. [Sch85], §5, 5.8)**.** *Pour tout algèbre de quaternions Q sur K, il existe une extension de corps L/K sur laquelle Q est scindée. Via un isomorphisme avec l'anneau des matrices sur L, on peut alors remonter le déterminant et la trace à Q. Remarquablement, ces fonctions ne dépendent ni de l'isomorphisme choisi, ni de l'extension L. On appelle alors ces fonctions* ***norme réduite*** $\mathrm{Nrd} : Q \to K$ *et* ***trace réduite*** $\mathrm{Trd} : Q \to K$*, respectivement.*

Si $Q = [a,b)_K$ et $x = x_1 + x_2 u + x_3 v + x_4 uv \in Q$, alors on a les formules

$$\mathrm{Trd}(x) = 2x_1 + x_2$$
$$\mathrm{Nrd}(x) = x_1^2 + x_1 x_2 - a x_2^2 - b(x_3^2 + x_3 x_4 - a x_4^2)$$

.

Proposition 4.4 ([Vig80], II, 1.3 et 1.9)**.** *Soit Q une K-algèbre de quaternions non scindée, et L/K une extension quadratique. Alors Q est scindée sur L, et il existe un morphisme de L dans Q égal à l'identité sur K. De plus, si $\alpha \in Q \setminus K$, c'est la racine d'un polynôme de degré 2 (cf. 5.1), donc Q est scindée sur l'extension quadratique $K(\alpha)/K$.*

Théorème 4.5 (théorème d'Albert-Brauer-Hasse-Noether et réciprocité de Hilbert, cf. [Vig80], III.3, 3.1)**.** *Soit K un corps de nombres et Q une K-algèbre de quaternions non réelle. Alors ΔQ est fini, $|\Delta Q|$ est pair, et de plus $\Delta Q = \varnothing$ si et seulement si Q est scindé. Réciproquement, si $S \subseteq \mathcal{V}_K$ est de cardinal pair, il existe (à K-isomorphisme près) une unique algèbre de quaternions non-réelle Q telle que $\Delta Q = S$.*

Le théorème suivant donne une définition remarquablement simple d'une intersection d'anneaux de valuations via des propriétés d'une algèbre de quaternions. C'est ce résultat qui justifie en partie le recours à cette théorie qui est a priori assez éloignée de la problématique initiale.

Théorème 4.6 ([Dit18], 2.9)**.** *Pour Q une algèbre de quaternions non-réelle sur K, soit $S(Q) = \{\mathrm{Trd}(\alpha) : \alpha \in Q \setminus K, \mathrm{Nrd}(\alpha) = 1\}$. Alors*

$$\bigcap_{v \in \Delta Q} \mathcal{O}_v = \{x + y : x, y \in S(Q)\} \ .$$

5 $\exists_m$-définissabilité d'intersections finies d'anneaux de valuation

Dans cette partie nous prouvons plusieurs résultats de définissabilité concernant les intersections finies d'anneaux de valuation. Le théorème suivant est l'un des plus importants de ceux utilisant la théorie des algèbres de quaternions. Il permet de traduire le concept algébrique de scission d'une algèbre de quaternions de façon arithmétique, qui plus est avec seulement 3 quantificateurs existentiels. Pour K un corps et $a \in K$, on notera $K_{(a)}$ le corps de rupture de $X^2 - X - a$ sur K.

Théorème 5.1. *Soit K un corps, $a, b \in K$ tels que $(1+4a)b \neq 0$ et $Q = [a,b)_K$. Soient également $c, d \in K$. Alors on a l'équivalence entre :*

(i) Q *est scindé sur le corps de rupture de* $X^2 - cX + d$ *dans* K.

(ii) Il existe $\alpha \in Q \setminus K$ *tel que* $\mathrm{Trd}(\alpha) = c$ *et* $\mathrm{Nrd}(\alpha) = d$.

(iii) Il existe $x, y, z \in K$ *avec* $2x - c$, y *et* z *non tous nuls tels que*

$$x^2 + x(c-2x) - a(c-2x)^2 - b(y^2 + yz - az^2) = d \ .$$

Démonstration. L'équivalence entre (ii) et (iii) provient de l'identité classique des matrices 2x2, qui caractérise de manière univoque la trace et la norme pour les matrices non scalaires :

$$\forall M \in \mathcal{M}_2(K), M^2 - \mathrm{Tr}(M)M + \det(M) = 0 \ ,$$

qui se traduit naturellement dans Q via la norme réduite et la trace réduite :

$$\forall \alpha \in Q, \alpha^2 - \mathrm{Trd}(\alpha)\alpha + \mathrm{Nrd}(\alpha) = 0 \ . \tag{1}$$

Les formules de 4.3 montrent que (iii) revient à dire que le quaternion $x+(c-2x)u+yv+zuv \notin K$, qui a pour trace réduite c, a pour norme réduite d, i.e (ii).

Si Q est déjà scindé, (i) est vrai et on peut facilement trouver une matrice 2x2 avec une trace et un déterminant donné, d'où (ii). Sinon, si (ii) est vrai pour $\alpha \in Q \setminus K$, alors par (1), $K(\alpha)$ est le corps de rupture de $X^2 - cX + d$. D'après 4.4, on obtient que Q est scindé sur $K(\alpha)$, i.e (i). Si (i) est vrai, 4.4 donne également l'existence d'un morphisme du corps de rupture de $X^2 - cX + d$ dans Q, d'où l'existence d'une solution de $\alpha^2 - c\alpha + d = 0$ dans $Q \setminus K$, donc (ii) est vrai. □

Lemme 5.2. *Soit* K *un corps de nombres. Soit* $S \subseteq \mathcal{V}_K$ *fini, et* Q *une algèbre de quaternions non-réelle sur* K *telle que* $S \subseteq \Delta Q$. *Soient* $\pi, a \in K^*$ *tels que pour tout* $v \in \Delta Q$, $v(\pi) = 1$, $v(a) = v(1+4a) = 0$ *et tel que* $X^2 - X - a$ *a une racine dans* K_v *si et seulement si* $v \in S$. *Alors*

$$\bigcap_{v \in S} \mathcal{O}_v = \{0\} \cup \left\{x \in K : Q \text{ est scindée sur } K_{(a-(\pi x^2)^{-1})}\right\} \ . \tag{2}$$

Démonstration. Le cas où Q est déjà scindée est trivial, on supposera donc que ce n'est pas le cas par la suite. Soit $x \in K^*$ et $L = K_{(a-(\pi x^2)^{-1})}$. Comme Q est non-réelle, par 4.5 Q est scindée sur L si et seulement si Q est scindée sur L_w pour tout $w \in \mathcal{V}_L$. Si $w \in \mathcal{V}_L$, on note $v \in \mathcal{V}_K$ la restriction de w à K. Les résultats du début de [Neu99] §8 donnent $L_w = (K_v)_{(a-(\pi x^2)^{-1})}$. On en conclut que Q est scindée sur L si et seulement si elle est scindée sur tout les $(K_v)_{(a-(\pi x^2)^{-1})}$ pour $v \in \Delta Q$. Enfin, par 4.4, ceci revient à dire que $(K_v)_{(a-(\pi x^2)^{-1})}/K_v$ est quadratique car Q n'est pas scindée, i.e $X^2 - X - \left(a - (\pi x^2)^{-1}\right)$ est irréductible sur K_v. On veut donc :

$$x \in \bigcap_{v \in S} \mathcal{O}_v \iff \forall v \in \Delta Q, X^2 - X - \left(a - (\pi x^2)^{-1}\right) \text{ est irréductible sur } K_v \ .$$

Soit $v \in \Delta Q$. Supposons $x \in \mathcal{O}_v$ (en particulier vrai si $v \in S$) et qu'on ait $\alpha^2 - \alpha - \left(a - (\pi x^2)^{-1}\right) = 0$ avec $\alpha \in K_v$. Comme $v\left(a - (\pi x^2)^{-1}\right) < 0$, on devrait avoir $v(\alpha) < 0$. Mais alors

$$2v(\alpha) = v(\alpha^2 - \alpha - a) = v\left((\pi x^2)^{-1}\right) = -1 - 2v(x)$$

ce qui est absurde.

Si $x \notin \mathcal{O}_v$, $X^2 - X - \left(a - (\pi x^2)^{-1}\right) \equiv X^2 - X - a \bmod \mathfrak{m}_v$ donc par le lemme de Hensel, $X^2 - X - \left(a - (\pi x^2)^{-1}\right)$ possède une racine dans K_v si et seulement si $X^2 - X - a$ en a une, ce qui arrive si et seulement si $v \in S$. En particulier, si $v \notin S$, alors le polynôme est irréductible.

On a montré que pour $v \in S$, $x \in \mathcal{O}_v$ si et seulement si $X^2 - X - \left(a - (\pi x^2)^{-1}\right)$ est irréductible, et que c'est toujours vrai si $v \in \Delta Q \setminus S$, ce qui prouve le résultat. □

Théorème 5.3. *Pour K un corps de nombres et $S \subseteq \mathcal{V}_K$ fini, l'ensemble $\bigcap_{v\in S} \mathcal{O}_v$ est $\exists_3$-définissable.*

Démonstration. D'après 4.5, il est possible de trouver Q une algèbre de quaternions non-réelle sur K telle que $S \subseteq \Delta Q$. Vérifions alors qu'il est effectivement possible de choisir $\pi, a \in K^*$ comme dans l'énoncé. Pour π, c'est une conséquence directe du théorème d'approximation faible (2.6). Pour tout $v \in \Delta Q$, $U_v = \{x \in K : v(x) = 1\}$ est ouvert (cf. 2.3.2), donc $\prod_{v\in\Delta Q} U_v$ est un ouvert de $\prod_{v\in\Delta Q} (K, v)$. Par 2.6, ce produit contient un élément de la diagonale, i.e $\pi \in K$ tel que $\forall v \in \Delta Q, v(\pi) = 1$.

Pour a, il suffit de montrer que ces deux propriétés sont ouvertes (restent vraies dans un certain voisinage d'un élément qui les vérifie) et non vides. On obtient alors le résultat par intersection et produit fini, puis 2.6. La première est ouverte pour la même raison que précédemment. Dans $\overline{K_v}$, elle s'écrit $(\bar{a} \neq \bar{0} \wedge \bar{1} + 4\bar{a} \neq \bar{0})$. Si $\left|\overline{K_v}\right| = 2$, le corps est de caractéristique 2, et $\bar{a} = \bar{1}$ convient. Si $\left|\overline{K_v}\right| > 2$ il est possible de trouver $\bar{a}$ différent de $\bar{0}$ et $\overline{-1/4}$, donc la propriété est non vide. La seconde est ouverte, car pour $a \in K$, $\{x \in K : \bar{x} = \bar{a}\} = a + \{y \in K : v(y) > 0\}$ qui est ouvert, et on voit facilement qu'il est d'intersection non vide avec la propriété précédente.

Les conditions de 5.2 s'appliquent, donc d'après (2), le théorème est vrai si et seulement si le second membre de l'égalité admet une $\exists_3$-définition, ce qui est clair d'après 5.1. □

Nous avons donc une $\exists_3$-définition de toute intersection finie d'anneaux de valuations. Cependant, d'après 4.2 et 4.5, on peut paramétrer tous ceux de cardinalité paire par $\Delta[a, b)_K$. Mais la $\exists_3$-définition précédente ne fait pas apparaître explicitement a, b : nous allons donc essayer d'arriver à une définition de ce genre d'ensembles, uniforme en a et b, i.e dans laquelle a, b sont des paramètres explicites.

Théorème 5.4. *Soit K un corps de nombres. Il existe $\varphi(x, a, b)$ une $\exists_7$-formule telle que pour tous $a, b \in K$ tels que $(1 + 4a)b \neq 0$ et $[a, b)_K$ non-réelle,*

$$\bigcap_{v\in\Delta[a,b)_K} \mathcal{O}_v = \{x \in K : K \models \varphi(x, a, b)\} .$$

Démonstration. D'après équivalence de (i) et (ii) dans 5.1, l'ensemble $\{(x, a, b) : (1 + 4a)b \neq 0 \wedge x \in S([a, b)_K)\}$ est $\exists_3$-définissable.

D'après 4.6,

$$x \in \bigcap_{v\in\Delta[a,b)_K} \iff \exists y \in K, y \in S([a, b)_K) \wedge x - y \in S([a, b)_K) .$$

En appliquant 1.3 (iii), la conjonction est $\exists_6$-définissable, d'où la conclusion du théorème. □

6 Anneaux d'entiers

On a démontré la définissabilité d'intersections *finies* d'anneaux de valuations, mais le résultat qu'on veut montrer porte sur les anneaux d'entiers

$$\mathcal{O}_K = \bigcap_{v\in\mathcal{V}_K} \mathcal{O}_v ,$$

qui sont donc définis par intersection infinie. Pour arriver à définir existentiellement ces intersections, on va passer par les unions d'idéaux maximaux de valuations $\mathfrak{m}_v$. Grâce à quelques

résultats techniques et calculatoires, on peut relier ces unions infinies aux intersections finies étudiées précédemment. Mais comme le lemme suivant le démontre, ce passage se fait au prix d'une négation qui renverse tous les quantificateurs, d'où la définition par quantificateurs *universels* à laquelle nous arrivons.

Lemme 6.1. *Si K un corps et $V \subseteq \mathcal{V}_K$, alors $\bigcap_{v\in V} \mathcal{O}_v$ est $\forall_n$-définissable si et seulement si $\bigcup_{v\in V} \mathfrak{m}_v$ est $\exists_n$-définissable.*

Démonstration. Il suffit de remarquer que

$$\bigcap_{v\in V} \mathcal{O}_v = \left(K \setminus \left(\bigcup_{v\in V} \mathfrak{m}_v\right)^{-1}\right) \cup \{0\} \ .$$

□

Lemme 6.2. *Soit K un corps de nombres, $S \subseteq \mathcal{V}_K$ non vide et fini et $u \in \bigcap_{v\in S} \mathcal{O}_v^\times$. L'ensemble*

$$\Phi_u^S = \left\{(a,b) \in K^2 : \forall v \in S, v(a-u) > 0 \ \wedge \ v(b) = 0\right\}$$

est $\exists_6$-définissable dans K^2.

Démonstration. Par 2.6, on a $\pi \in K^*$ tel que $v(\pi) = 1$ pour tout $v \in S$. Alors par 1.5,

$$\begin{aligned}(a,b) \in \Phi_u^S &\iff \forall v \in S,\ v(b) = 0 \ \wedge \ v\left(\frac{a-u}{\pi}\right) \geq 0 \\ &\iff \forall v \in S,\ b \in \mathcal{O}_v^\times \ \wedge \ \frac{a-u}{\pi} \in \mathcal{O}_v \\ &\iff b + \frac{1}{b}, \frac{a-u}{\pi} \in \bigcap_{v\in S} \mathcal{O}_v \ .\end{aligned}$$

On conclut par 5.3. □

Le lemme calculatoire suivant établit l'existence d'une fraction rationnelle satisfaisant certaines propriétés intéressantes vis-à-vis des anneaux de valuation. La proposition qui suit, non moins technique et calculatoire, l'utilise pour définir une union presque infinie d'idéaux maximaux de valuation en utilisant une intersection finie d'anneaux de valuations, résultat annoncé plus tôt.

Lemme 6.3 ([Daa23], 5.3)**.** *Soit (K,v) un corps de nombres valué. Alors la fraction rationnelle $f(X,Y) = \frac{16X^4}{1+4X^2} - \left(\frac{(Y-1)^2}{Y}\right)^2 \in K(X,Y)$ est telle que, pour tous $a,b \in K$ avec $(1+4a^2)b \neq 0$, on a :*

(i) Si $1+4a^2, b \in \mathcal{O}_v^\times$ alors $f(a,b) \in \mathcal{O}_v$.

(ii) Si $v(1+4a^2) = 0$ et $v(b) \neq 0$ alors $v(f(a,b)) = -2|v(b)|$.

(iii) Si le lemme de Hensel 2.5 est vrai dans (K,v), que v est non dyadique, que $X^2 - X - a^2$ est irréductible et que $f(a,b) \in \mathcal{O}_v$, alors $1+4a^2, b \in \mathcal{O}_v^\times$.

Proposition 6.4 ([Daa23], 5.5). *Soit K un corps de nombres. Soit $\pi \in K^*$ tel que $S = \{v \in \mathcal{V}_K : v(c) \text{ est impair}\}$ soit de cardinalité impaire. Soit $u \in K^*$ tel que pour tout $v \in S$, $v(u) = 0$ et $X^2 - X - u^2$ est irréductible sur $\overline{K_v}$. On suppose que S contient toutes les valuations dyadiques, et on prend la fonction rationnelle f donnée par 6.3. Alors pour $x \in K$:*

$$x \in \bigcup_{v \in \mathcal{V}_K \setminus S} \mathfrak{m}_v \iff \exists (a,b) \in \Phi_u^S, \frac{a^2x^2 f(a,b)}{1 - x - a^2x^2} \in \bigcap_{v \in \Delta[a^2, b\pi)_K} \mathcal{O}_v \ .$$

Remarque 6.4.1. Nous omettons la majeure partie de la preuve calculatoire et quelque peu sybilline de ce résultat pour se concentrer sur les idées principales. Dans l'implication $\boxed{\Rightarrow}$, si $x \in \mathfrak{m}_w$, on trouve $(a,b) \in \Phi_u^S$ tels que $\Delta[a^2, b\pi)_K = S \cup \{w\}$. Les propriétés de Ψ_u^S différencient w des autres valuations de S et les propriétés de f permettent de conclure. Pour $\boxed{\Leftarrow}$, on peut montre que $S \subseteq \Delta[a^2, b\pi)_K$, et par parité (cf. 4.5), il existe $w \in \Delta[a^2, b\pi)_K \setminus S$. Là encore, les propriétés de Φ_u^S et f différencient w des autres valuations et permettent de montrer $x \in \mathfrak{m}_w$.

Théorème 6.5. *Soit K un corps de nombres, $S \subseteq \mathcal{V}_K$ fini. Alors $\bigcap_{v \in \mathcal{V}_K \setminus S} \mathcal{O}_v$ est $\forall_{15}$-définissable dans K.*

Démonstration. Par 6.1, il faut et il suffit de montrer que $\bigcup_{v \in \mathcal{V}_K \setminus S} \mathfrak{m}_v$ est $\exists_{15}$-définissable. Remarquons que si $S \subseteq S'$,

$$\bigcup_{v \in \mathcal{V}_K \setminus S} \mathfrak{m}_v = \bigcup_{v \in S' \setminus S} \mathfrak{m}_v \cup \bigcup_{v \in \mathcal{V}_K \setminus S'} \mathfrak{m}_v$$

Or si $v \in \mathcal{V}_K$ et $\pi \in K$ tel que $v(\pi) = 1$, alors $x \in \mathfrak{m}_v \iff x/\pi \in \mathcal{O}_v$, ce qui est $\exists_3$-définissable par 5.3. L'union finie $\bigcup_{v \in S' \setminus S} \mathfrak{m}_v$ l'est donc aussi par 1.3 (ii). Par ce même résultat, montrer le théorème pour $\bigcup_{v \in \mathcal{V}_K \setminus S'} \mathfrak{m}_v$ suffit, donc sans perte de généralité on peut prendre S fini aussi grand que nécessaire.

Si $\mathrm{char}(K) \neq 2$, on ajoute à S toutes les valuations dyadiques (en nombre fini), et par 4.1 on peut l'élargir jusqu'à avoir $|S|$ impair et $S = \{v : v(\pi) \text{ impair}\}$ pour un $\pi \in K^*$. Par approximation faible (2.6) et lemme de Hensel (2.5), on peut trouver $u \in \bigcap_{v \in S} \mathcal{O}_v^\times$ tel que $X^2 - X - u^2$ est irréductible sur chaque $\overline{K_v}$. Par 6.4, il existe $g \in K(X,Y)$ tel que pour tout $x \in K$,

$$x \in \bigcup_{v \in \mathcal{V}_K \setminus S} \mathfrak{m}_v \iff \exists (a,b) \in \Phi_u^S, \frac{a^2x^2 g(a,b)}{1 - x - a^2x^2} \in \bigcap_{v \in \Delta[a^2, b\pi)_K} \mathcal{O}_v \ .$$

Or Φ_u^S est $\exists_6$-définissable par 6.2 et $\bigcap_{v \in \Delta[a^2, b\pi)_K} \mathcal{O}_v$ est uniformément $\exists_7$-définissable par , donc par 1.3, on peut définir $\bigcup_{v \in \mathcal{V}_K \setminus S} \mathfrak{m}_v$ en 2+6+7=15 quantificateurs existentiels. □

Corollaire 6.5.1. *$\mathbb{Z}$ est 16-diophantien dans $\mathbb{Q}$.*

Démonstration. Il suffit pour cela de remarquer que, par le théorème d'Ostrowski,

$$\mathbb{Z} = \bigcap_{p \text{ premier}} \mathcal{O}_{v_p} \ .$$

Le résultat suit alors du théorème précédent appliqué à $S = \varnothing$, puis de 1.4. □

Proposition 6.6 (cf. [Daa23], 6.1)**.** *Soit $m \in \mathbb{N}$. Si $\mathbb{Z}$ est $\forall_m$-$\mathcal{L}_{ann}$-définissable dans $\mathbb{Q}$, alors tout sous-ensemble récursivement énumérable de $\mathbb{Z}$ est $\exists_9\forall_m$-$\mathcal{L}_{ann}$-définissable dans $\mathbb{Q}$.*

Corollaire 6.6.1. *La théorie $\exists_9\forall_{16}$-$\mathcal{L}_{ann}$ de Q est indécidable.*

Démonstration. On choisit un sous-ensemble non récursif de $\mathbb{N}$ (par exemple : I.6.5). Par 6.6, cet ensemble est $\exists_9\forall_m$-$\mathcal{L}_{\text{ann}}$-définissable dans $\mathbb{Q}$. La théorie $\exists_9\forall_{16}$-$\mathcal{L}_{\text{ann}}$ de Q ne peut donc pas être décidable. □

Références

[Alb39] A.A. Albert. *Structure of Algebras*. American Mathematical Society colloquium publications vol. 24. American Mathematical Society, 1939. ISBN : 9780821810248. URL : https://books.google.fr/books?id=1G0HcOcoJ1cC.

[Che10] Gaëtan Chenevier. *Definite quaternion algebras and their modular forms*. Notes de cours. Accessed : 2023-06-03. 2010. URL : http://gaetan.chenevier.perso.math.cnrs.fr/coursIHP/chenevier_lecture6.pdf.

[Daa21] Nicolas Daans. "Universally defining finitely generated subrings of global fields". In : *Documenta Mathematica* 26 (2021), p. 1851-1869. DOI : 10.4171/dm/858. URL : https://doi.org/10.4171%2Fdm%2F858.

[Daa23] Nicolas Daans. *Universally defining $\mathbb{Z}$ in $\mathbb{Q}$ with 10 quantifiers*. 2023. arXiv : 2301.02107 [math.NT].

[Dav73] Martin Davis. "Hilbert's Tenth Problem is Unsolvable". In : *The American Mathematical Monthly* 80.3 (1973), p. 233-269. DOI : 10.1080/00029890.1973.11993265.

[Dit18] Philip Dittmann. "Irreducibility of polynomials over global fields is diophantine". In : *Compositio Mathematica* 154.4 (mars 2018), p. 761-772. DOI : 10.1112/s0010437x17007977. URL : https://doi.org/10.1112%2Fs0010437x17007977.

[EP05] Antonio J. Engler et Alexander Prestel. *Valued Fields*. Springer-Verlag, 2005. DOI : 10.1007/3-540-30035-x. URL : https://doi.org/10.1007%2F3-540-30035-x.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Springer Berlin Heidelberg, 1999. DOI : 10.1007/978-3-662-03983-0. URL : https://doi.org/10.1007%2F978-3-662-03983-0.

[Sch85] Winfried Scharlau. *Quadratic and Hermitian Forms*. Springer Berlin Heidelberg, 1985. DOI : 10.1007/978-3-642-69971-9. URL : https://doi.org/10.1007%2F978-3-642-69971-9.

[Vig80] Marie-France Vignéras. *Arithmétique des Algèbres de Quaternions*. Springer Berlin Heidelberg, 1980. DOI : 10.1007/bfb0091027. URL : https://doi.org/10.1007%2Fbfb0091027.