Université de Montréal

Dixième problème de Hilbert pour des anneaux d'entiers algébriques

par

Annie Bacon

Département de mathématiques et de statistique
Faculté des arts et sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)
en mathématiques

juillet 1998

Université de Montréal

Faculté des études supérieures

Ce mémoire intitulé

Dixième problème de Hilbert pour des anneaux d'entiers algébriques

présenté par

Annie Bacon

a été évalué par un jury composé des personnes suivantes :

Khalid Benabdallah
(président-rapporteur)

Hidemitsu Sayeki
(directeur de recherche)

Leo Rosenberg
(membre du jury)

Mémoire accepté le :

98.09.28

SOMMAIRE

Nous avons choisi d'explorer un sujet presque centenaire se situant à l'intersection entre la théorie des nombres et la logique. Le dixième problème de Hilbert demandait à l'origine de trouver un algorithme permettant de savoir pour n'importe quelle équation diophantienne si elle avait des solutions. On appelle équation diophantienne l'équation $P(x_1, \ldots, x_n) = 0$ lorsque P est un polynôme à coefficients entiers où n est un nombre naturel et qu'on cherche $x_1, \ldots, x_n$ dans l'ensemble des entiers relatifs $\mathbb{Z}$.

Ce n'est qu'en 1970 que Yuri Matijasevič réussit à démontrer qu'un tel algorithme n'existait pas. Ce fut le dénouement de 70 ans de recherche, ainsi que le prélude à d'encore plus vastes découvertes. En effet, soit B un anneau ou un corps arbitraire, on étendit le problème à la recherche d'un algorithme pour des équations diophantiennes dans B, c'est-à-dire d'équations à coefficients dans B pour lesquelles on cherche des solutions dans B. En particulier, la question demeure irrésolue lorsque B est le corps des nombres rationnels $\mathbb{Q}$.

Dans ce mémoire, nous avons d'abord désiré faire prendre connaissance des récents développements et des possibilités de ce domaine de recherche à des non-spécialistes. À cette fin, nous avons retracé et expliqué les travaux les plus pertinents. Nous nous sommes spécialement interessés aux cas où B est l'anneau des entiers algébriques d'un corps puisque ce cheminement mème à un théorème très important de Shapiro et Shlapentokh **[17]** stipulant que $\mathbb{Z}$ est diophantien dans l'anneau des entiers algébriques de toute extension abélienne des rationnels.

Par la suite, nous avons entrepris de reconstituer les preuves de l'article *Diophantine sets over some rings of algebraic integers* de J. Denef et L. Lipshitz [7], dont la méthode nous semblait adaptable à de nouveaux corps algébriques. Ainsi, il était impératif de le maîtriser. De plus, nous souhaitions compléter cet article de manière à le rendre plus accessible, donc à lui redonner de l'impact.

Étant donné le théorème de Shapiro et Shlapentokh, nous avons finallement étudié des corps algébriques qui soient galois, mais non abéliens. De cette façon, nous allions au-delà des résultats connus. Notre but était d'énoncer des conditions suffisantes pour obtenir la conclusion de Matijasevič sur de nouveaux anneaux d'entiers de corps algébriques. Pour ce faire, nous nous sommes inspirés des idées de [7], ce qui nous a menés à deux propositions et cinq corollaires. La première proposition s'applique aux extensions de degré six des rationnels, tandis que la seconde est généralisée à des extensions finies contenant deux sous-corps propres dont un est de degré deux sur $\mathbb{Q}$. Nous avons conclu ce mémoire en soumettant en conjecture un exemple original d'extension galoisienne, mais non abélienne des rationnels pour laquelle la réponse au dixième problème de Hilbert étendu à son anneau des entiers algébriques soit négative.

REMERCIEMENTS

Je tiens à remercier mon directeur Monsieur Hidemitsu Sayeki de m'avoir donné l'intérêt pour la théorie des nombres et la logique à travers ses cours bien structurés ainsi que pour sa grande disponibilité et sa remarquable patience. De même, ma mère, mon amoureux, sa famille et mes amis ont aussi fait preuve de beaucoup de patience et m'ont moralement supportée dans les bons et moins bons moments. Je remercie tout particulièrement ma mère à qui je voudrais dédier ce mémoire. Je remercie aussi mes confréres Sébastien, Valérie et Jérôme qui m'ont à leur façon respective encouragée, inspirée par leur travail acharné et stimulée mathématiquement.

Table des matières

INTRODUCTION: MOTIVATION ET HISTORIQUE

La motivation première de ce travail est née d'un problème imaginé par un grand mathématicien allemand au tournant du siècle. En 1900, lors du Congrès international des mathématiciens à Paris, David Hilbert (1862-1943) avait en fait 23 problèmes à proposer à son auditoire. Il les jugeait comme étant de grand intérêt pour le prochain siècle. Le dixième problème de sa liste, qu'il choisit d'ailleurs de ne pas présenter par manque de temps, demandait de trouver un algorithme qui déterminerait si il y a des solutions dans $\mathbb{Z}$ pour une équation diophantienne arbitraire. Il est donc essentiel de connaître dès maintenant la signification des expressions équation diophantienne et ensemble diophantien.

Soit $P(x_1, \ldots, x_n)$ un polynôme à coefficients entiers alors $P(x_1, \ldots, x_n) = 0$ est une équation diophantienne lorsqu'on cherche $x_1, \ldots, x_n \in \mathbb{Z}$. Un ensemble S est dit diophantien (dans $\mathbb{Z}$) si la relation $x \in S$ est diophantienne, c'est-à-dire si il existe un polynôme $Q(x, y_1, \ldots, y_m)$ à coefficients entiers tel que $x \in S$ si et seulement si il existe $y_1, \ldots, y_m \in \mathbb{Z}$ tels que $Q(x, y_1, \ldots, y_m) = 0$.

Plusieurs années après le congrès de Paris, soit en 1931, le travail de Gödel lui permit de suggérer qu'un tel algorithme n'existe pas. Par contre, les recherches durent se poursuivre jusqu'en janvier 1970 avant que ce ne soit prouvé. Le mathématicien russe Yuri Matijasevič obtint ce résultat en réalisant l'étape finale d'un programme développé par Julia Robinson, Martin Davis, et Hilary Putnam. Il montra qu'il n'existe pas d'algorithme pouvant dire pour n'importe quelle équation diophantienne si elle possède ou non des solutions dans $\mathbb{N}$. En particulier,

il prouva en 1975 qu'il n'existe pas d'algorithme pour résoudre une équation diophantienne à 9 variables dont on cherche les solutions dans $\mathbb{N}$. Le lecteur interessé peut trouver la démonstration de Matijasevič dans [9].

Cette découverte lui donna la réponse au dixième problème d'Hilbert puisqu'il était connu que $\mathbb{N}$ est diophantien dans $\mathbb{Z}$. En effet, soit $t \in \mathbb{N}$, on sait qu'il existe $A, B, C, D \in \mathbb{Z}$ tels que $t = A^2 + B^2 + C^2 + D^2$ par le théorème de Lagrange. Donc soit $t \in \mathbb{Z}$, alors $t \in \mathbb{N}$ si et seulement si il existe $A, B, C, D \in \mathbb{Z}$ tels que $t-(A^2+B^2+C^2+D^2) = 0$. Ainsi, soit $P(x_1, \ldots, x_n)$ une équation diophantienne. On a que P possède une solution pour $(x_1, \ldots, x_n) \in \mathbb{N}^n$ si et seulement si $P(A_1^2 + B_1^2 + C_1^2 + D_1^2, \ldots, A_n^2 + B_n^2 + C_n^2 + D_n^2) = 0$ possède une solution dans $\mathbb{Z}^{4n}$. Donc si il existait un algorithme dévoilant si une équation diophantienne arbitraire possède ou non une solution dans $\mathbb{Z}$, nous aurions du même coup un algorithme dans $\mathbb{N}$.

Cette preuve attendue depuis longtemps raviva la recherche dans ce domaine. L'énoncé modifié du dixième problème de Hilbert fut adapté pour un anneau puis un corps arbitraire. Pour ce faire, on introduit la notion d'équation diophantienne dans B (c'est-à-dire avec coefficients dans B plutôt que dans $\mathbb{Z}$ et solutions dans B plutôt que dans $\mathbb{Z}$) et la notation abrégée H10B signifiant "existe-t-il un algorithme pour toute équation diophantienne dans B révélant si elle a des solutions dans B?". Cette dernière question illustre l'étendue de ce nouveau sujet de recherche. En particulier, l'étude de H10$\mathbb{Q}$, qui est un problème ouvert, est très intéressante. L'article de Dan Flath et Stan Wagon [8] et celui écrit en collaboration par Martin Davis, Yuri Matijasevič et Julia Robinson [4] pour ne citer que ceux-là, semblent indiquer que leurs auteurs sont de cet avis. Une des avenues possibles pour résoudre ce problème serait de trouver une définition diophantienne de $\mathbb{Z}$ dans $\mathbb{Q}$. En effet, une telle définition et le résultat de Matijasevič stipulant que la réponse à H10$\mathbb{Z}$ est négative pourraient être utilisés de la même façon qu'au paragraphe précédent pour démontrer que H10$\mathbb{Q}$ est non résoluble (réponse négative à H10$\mathbb{Q}$). Malheureusement, une définition si simple de $\mathbb{Z}$ dans

$\mathbb{Q}$ n'a pas encore été trouvée. Pourtant, c'est depuis 1948 que nous savons que $\mathbb{Z}$ est arithmétiquement définissable dans $\mathbb{Q}$ grâce à Julia Robinson **[14]**. En plus de ce résultat remarquable elle prouva une importante généralisation dans **[15]**. Elle montra d'abord que $\mathbb{Z}$ est arithmétiquement définissable dans tout anneau d'entiers algébriques $\mathcal{O}_L$ de corps algébrique L. Ensuite elle donna une définition arithmétique de $\mathcal{O}_L$ dans L. Ainsi, $\mathbb{Z}$ est arithmétiquement définissable dans tout corps algébrique L.

Avant de regarder la définition arithmétique de $\mathbb{Z}$ dans $\mathbb{Q}$ de **[14]**, voici quelques éclaircissements sur le caractère définissable des ensembles. Un ensemble $A \subset B$ est définissable dans B si il existe une formule S telle que pour $t \in B$, S(t) est vraie dans B si et seulement si $t \in A$. En outre, A est arithmétiquement définissable dans B si S est une formule n'empruntant rien à la théorie des ensembles. Ceci veut dire que S ne fait intervenir que la logique du premier ordre qui comprend des variables de B, des constantes de $\mathbb{Z}$, l'addition et la multiplication sur B, et un nombre fini de symboles logiques et mathématiques parmi $\sim$ (non),$\vee$,$\wedge$, $\Longrightarrow$,$\Longleftrightarrow$,$\exists$,$\forall$,=,<.

Prenons l'exemple suivant d'une définition qui n'est pas arithmétique. Soit B=$\mathbb{N} \cup \{0\}$ et A un ensemble tel que $A \subset B$. Considérons $S_1(t)$.

$$S_1(t) : \forall_A([2 \in A \wedge \forall_y(y \in A \leftrightarrow y + 2 \in A)] \rightarrow t \in A)$$

Puisque $S_1(t)$ est vraie dans B si et seulement si t est un entier pair non négatif, S_1 est une formule qui définit les entiers pairs non négatifs dans B. Par contre, elle contient un quantificateur universel qui agit sur un ensemble d'entiers $(\forall_A)$ et le symbole $\in$ qui dénote la relation d'appartenance. Donc si cette formule était la plus simple à définir les entiers pairs non négatifs dans $\mathbb{N} \cup \{0\}$, ils ne seraient pas arithmétiquement définissable dans B. Or ce n'est pas le cas puisque la prochaine définition des entiers pairs non négatifs dans B est arithmétique. Soit $t \in B$:

$$S_2(t) : \exists_y \; t = y + y.$$

Revenons maintenant à la définition arithmétique de $\mathbb{Z}$ dans $\mathbb{Q}$ de Julia Robinson. Soient $q,\ p \in \mathbb{Q}$ et $R(q,p,t)$ la formule ci-après:

$$\exists_{a,b,c\in\mathbb{Q}}\ (2 + qpt^2 = a^2 + qb^2 - pc^2). \tag{0.0.1}$$

En pensant à q et p comme étants fixés, $R(q,p,t)$ définit alors un sous-ensemble de $\mathbb{Q}$ décrit par les variations de la variable t. L'idée est de s'assurer qu'aucun nombre premier ne divise le dénominateur de t lorsque la condition 0.0.1 est vérifiée et que la fraction t est simplifiée au maximum (numérateur et dénominateur copremiers). Soit maintenant S(x), la formule suivante qui définit $\mathbb{Z}$ dans $\mathbb{Q}$:

$$\forall_{q,p\in\mathbb{Q}}([R(q,p,0) \wedge \forall_{t\in\mathbb{Q}}\{R(q,p,t) \Rightarrow R(q,p,t+1)\}] \Rightarrow R(q,p,x)).$$

Alors pour $x \in \mathbb{Q}$, $S(x)$ est vrai dans $\mathbb{Q}$ si et seulement si $x \in \mathbb{Z}$. Pour de plus amples détails nous suggérons de consulter [**14**] ou encore [**8**].

Heureusement, les recherches des dernières années ont été beaucoup plus fructueuses lorsqu'on abandonne $\mathbb{Q}$ au profit de divers autres corps ou anneaux. Parmi les cas particuliers on a abondamment étudié celui de $\mathcal{O}_L$, l'anneau des entiers algébriques d'un corps algébrique L. Il a été démontré que la réponse à H10$\mathcal{O}_L$ est négative pour plusieurs classes de corps algébriques L. Le problème de caractériser tous les corps algébriques ou anneaux B qui ont une réponse négative à H10B reste cependant ouvert.

Presque cent ans après le congrès de Paris, des recherches en rapport avec le dixième problème de Hilbert sont donc encore le sujet de beaucoup d'efforts. La perspicacité de cet homme ainsi que la diversité des conséquences des recherches dans ce domaine ont inspiré ce mémoire.

Pour ce travail, nous nous sommes proposés de trouver de nouveaux anneaux d'entiers algébriques tels que la réponse au dixième problème de Hilbert y soit négative. Nous adoptons une nouvelle terminologie; H10B est résoluble si il existe un algorithme révélant pour n'importe quelle équation diophantienne dans B si

elle a des solutions dans B. Notre premier chapitre trace un cheminement chronologique des principaux résultats obtenus sur les anneaux d'entiers algébriques. Pour chacun d'entre eux, nous présentons un résumé de preuve ou expliquons la méthodologie utilisée. Ce chapitre relate entre autres les étapes menant au résultat que $\mathbb{Z}$ est diophantien dans l'anneau des entiers algébriques de toute extension abélienne des rationnels. Nous nous sommes donc interrogés à propos des extensions non abéliennes des rationnels. Le chapitre deux explicite quant à lui, un article essentiel de J. Denef et L. Lipshitz [7]. La méthode utilisée par ces auteurs méritait des efforts de compréhension et de synthèse car elle nous a permis, après quelques ajustements, de formuler deux propositions et cinq corollaires. Les démonstrations de ces nouveaux résultats constituent d'ailleurs le noyau de notre dernier chapitre. De plus, nous y avons également inclus en conjecture une extension algébrique non abélienne des rationnels L qui satisferait notre troisième corollaire et donc tel que H10$\mathcal{O}_L$ serait non résoluble. Notre contribution s'inscrit ainsi dans le cadre de la conjecture de Denef et Lipshitz stipulant que la réponse à H10$\mathcal{O}_L$ est négative pour tout corps algébrique L.

Chapitre 1

REVUE DE LA LITTÉRATURE

Nous allons d'abord survoler pour vous les résultats intermédiaires et les différentes méthodes qui ont mené à pouvoir affirmer aujourd'hui que $\mathbb{Z}$ est diophantien dans l'anneau des entiers algébriques de toute extension abélienne des rationnels. Ensuite, nous vous guiderons à travers les développements plus récents.

À la base de toutes ces recherches réside la preuve de Matijasevič. Puisqu'il était impossible de trouver un algorithme pour savoir si une équation diophantienne arbitraire a des solutions dans $\mathbb{N}$ et donc dans $\mathbb{Z}$ par le théorème de Lagrange, qu'en était-il pour des anneaux ou des corps plus généraux?

Notre premier arrêt sera en 1975. À cette époque, J. Denef fait paraître un article intitulé *Hilbert's tenth problem for quadratic rings* [5]. Son travail porte alors sur les entiers algébriques des corps quadratiques. Ces corps sont de la forme $F = \mathbb{Q}(\sqrt{D})$ où D est un entier relatif ne contenant pas de facteur carré. Étant donné le résultat de Matijasevič, il suffira à Denef de montrer que la relation $x \in \mathbb{N}$ est diophantienne dans $\mathcal{O}_F$ pour obtenir le théorème suivant:

Théorème 1.0.1. *Soit $\mathcal{O}_F$ l'anneau des entiers algébriques du corps quadratique $F = \mathbb{Q}(\sqrt{D})$. Il n'existe pas d'algorithme pour decider si une équation diophantienne donnée a une solution dans $\mathcal{O}_F$ ou non. Donc $H10\mathcal{O}_F$ est non résoluble.*

L'idée maîtresse de la démonstration consiste à utiliser des équations de Pell dans la définition de $\mathbb{N}$ dans $\mathcal{O}_F$ et les suites $x_n(A) \in \mathbb{N}$, $y_n(A) \in \mathbb{N}$, $A > 1$, telles que $x_n(A) + \sqrt{A^2-1} \cdot y_n(A) = (A + \sqrt{A^2-1})^n$. Soit D'$\neq$D un autre entier relatif sans facteur carré. On voit que pour tout x, y dans $\mathcal{O}_F$, $x = 0$ et $y = 0$ si et seulement si $x^2 - D'y^2 = 0$. Étant donné que cette dernière équation est diophantienne, la définition cherchée peut être un système fini d'équations diophantiennes. Aussi, on sait par le théorème de Lagrange que tout nombre naturel est la somme de quatre carrés de nombre naturel. Ainsi, grâce à ce qui précède il suffit de montrer que:
Pour tout anneau $\mathcal{O}_F$ d'un corps quadratique $F = \mathbb{Q}(\sqrt{D})$, il existe Σ un système fini d'équations diophantiennes dont les inconnues sont $t, x, \ldots, s$ et telles que
(1) si Σ a une solution $< t, x, \ldots, s >$ dans $\mathcal{O}_F$ alors $t \in \mathbb{Z}$
et
(2) si $0 \neq k \in \mathbb{N}$ alors Σ a une solution $< t, x, \ldots, s >$ dans $\mathcal{O}_F$ avec $t = k^2$.

On trouve d'abord ce système d'équations dans la cas d'un corps quadratique réel $F = \mathbb{Q}(\sqrt{D})$, i.e. $D > 1$. Soit $< A, B >$ une des solutions dans $\mathbb{N}$ de $A^2 - DB^2 = 1$, où $B \neq 1$. Soit $E = A^2 - 1$. Alors le système suivant d'équations diophantiennes avec inconnues $t, x, y, u, v, z, w, h, q, r, s$ satisfait (1) et (2):

i. $x^2 - Ey^2 = 1$
ii. $u^2 - Ev^2 = 1$
iii. $v^2 - y^2t = zy^4$
iv. $t = w^2$
v. $y^2 - t = 1 + h^2 + q^2 + r^2 + s^2$.

Dans le cas d'un corps quadratique imaginaire, $F = \mathbb{Q}(\sqrt{D})$, avec $D \leq -1$, on pose $A = 2$ et $G = A^2 - 1 = 3$ si $D \neq -1$ et $D \neq -3$ ou bien $A = 4$ et

$G = A^2 - 1 = 15$ si $D = -1$ ou $D = -3$. Le système devient:

i. $x^2 - Gy^2 = 1$

ii. $u^2 - Gv^2 = 1$

iii. $v^2 - y^2t = zy^4$

iv. $ry + s(5h + 2) = 1$

v. $y = 2tw$.

Dans les deux cas, nous ne donnons pas ici la preuve de Denef que ces systèmes satisfont effectivement (1) et (2). Le lecteur peut plutôt se concentrer sur la preuve de la prochaine découverte puisque les corps quadratiques constituent des cas particuliers de ce qui suit.

À la suite de la précédente publication, J. Denef s'associe avec L. Lipshitz pour étendre l'idée des équations de Pell à un plus large éventail de corps algébriques. Ils vont même jusqu'à émettre la conjecture que H10$\mathcal{O}_L$ est non résoluble pour tout corps algébrique L. Leur article *Diophantine sets over some rings of algebraic integers* [**7**] paru en 1978 prouve la conjecture pour trois types de corps comme en témoigne leur théorème:

Théorème 1.0.2. *$\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$ si le corps algébrique L satisfait une des conditions suivantes:*

a): *$[L : \mathbb{Q}]=2$,*

b): *$[L : \mathbb{Q}]=4$, L n'est pas totallement réel et L contient un sous-corps K tel que $[K : \mathbb{Q}]=2$,*

c): *L n'est pas totallement réel et est de degré 2 sur un sous-corps K totallement réel pour lequel $\mathbb{Z}$ est diophantien dans $\mathcal{O}_K$.*

Les corps quadratiques tels qu'étudiés dans [**5**] sont tels que $[L : \mathbb{Q}]=2$ et donc sont traités par le présent théorème. Nous avons repris la preuve de messieurs Denef et Lipshitz au chapitre deux du présent ouvrage. Notre travail donne

beaucoup d'explications supplémentaires, de manière à ce que le résultat soit complet en lui-même. De plus, nous nous sommes proposés de rendre ces recherches accessibles à des lecteurs non initiés afin que plus de gens puissent l'apprécier.

En bref, les auteurs montrent que $\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$ car alors H10$\mathcal{O}_L$ est non résoluble. En effet, si $\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$ alors il existe un polynôme $P(k, x_1, \ldots, x_n)$ à coefficients dans $\mathcal{O}_L$ et $x_1, \ldots, x_n \in \mathcal{O}_L$ tels que pour $k \in \mathcal{O}_L$, $k \in \mathbb{Z}$ si et seulement si $P(k, x_1, \ldots, x_n) = 0$. Donc une équation diophantienne $R(y_1, \ldots, y_m) = 0$ a des solutions dans $\mathbb{Z}$ si et seulement si $R(y_1, \ldots, y_m) = 0$ a des solutions dans $\mathcal{O}_L$ et $P(y_i, x_{i1}, \ldots, x_{in}) = 0$, $i = 1, \ldots, m$. Alors un algorithme dans $\mathcal{O}_L$ en donnerait un dans $\mathbb{Z}$. On obtient alors une contradiction.

Un autre pas très important fut franchi par Denef. Dans son article *Diophantine sets over algebraic integer rings II* [6] , le chercheur dévoile en 1980 le théorème suivant:

Théorème 1.0.3. *Si K est un corps algébrique totallement réel, alors $\mathbb{Z}$ est diophantien dans $\mathcal{O}_K$.*

En combinant cette découverte avec celles de [7], on trouve comme corollaire que $\mathbb{Z}$ est diophantien dans $\mathcal{O}_K$ pour toute extension quadratique K d'un corps de nombres algébrique totallement réel. Cette fois par contre, Denef doit varier un peu sa méthodologie, bien qu'il continue à définir des suites $x_m(a)$, $y_m(a)$ comme suit: soit K un corps algébrique, $a \in \mathcal{O}_K$, $\delta(a) = \sqrt{a^2 - 1}$, $\varepsilon(a) = a + \delta(a)$. Si $\delta(a) \notin K$, alors $x_m(a)$, $y_m(a) \in \mathcal{O}_K$, $m \in \mathbb{N}$ et $x_m(a) + \delta(a)y_m(a) = (\varepsilon(a))^m$. Si K est un corps totallement réel et si $\sigma_1, \ldots, \sigma_n$ sont ses plongements dans $\mathbb{R}$, alors il prouve dans son troisième lemme que si $a \in \mathcal{O}_K$ est tel que:

$$\sigma_i(a) \geq 2^{2n} \text{ et } |\sigma_1(a)| \leq \frac{1}{2}, i = 2, \ldots, n \tag{1.0.2}$$

alors $\pm x_m(a), \pm y_m(a)$ sont exactement les solutions de $x^2 - (a^2 - 1)y^2 = 1$ dans $\mathcal{O}_K$. Ainsi, il utilise encore abondamment les équations de Pell, mais ces solutions

ne sont plus nécessairement entières. Il doit donc adapter une idée de Matijasevič dans **[13]** pour dériver m de $y_m(a)$ de façon diophantienne.

Voici donc un apperçu de la preuve de Denef. Soit K un corps algébrique totallement réel de degré n sur $\mathbb{Q}$, et $\sigma_1, \ldots, \sigma_n$ ses plongements dans $\mathbb{R}$. Supposons que $a \in \mathcal{O}_K$ et satisfait:

$$\sigma_i(a) \geq 2^{2n} \text{ et } |\sigma_1(a)| \leq \frac{1}{8},\ i = 2, \ldots, n. \tag{1.0.3}$$

On peut se convaincre qu'un tel a existe par le lemme de Minkowski (voir **[2]**). De plus, on définit $S \subset \mathcal{O}_K$ par

$\xi \in S \iff \xi \in \mathcal{O}_K \wedge \exists x, y, w, z, u, v, s, t, b \in \mathcal{O}_K$:

1. $x^2 - (a^2 - 1)y^2 = 1$
2. $w^2 - (a^2 - 1)z^2 = 1$
3. $u^2 - (a^2 - 1)v^2 = 1$
4. $s^2 - (a^2 - 1)t^2 = 1$
5. $\sigma_1(b) \geq 2^{2n}$
6. $|\sigma_i(b)| \leq \frac{1}{2}\ i = 2, \ldots, n$
7. $|\sigma_i(z)| \geq \frac{1}{2}\ i = 2, \ldots, n$
8. $|\sigma_i(u)| \geq \frac{1}{2}\ i = 2, \ldots, n$
9. $v \neq 0$
10. $z^2 | v$
11. $b \equiv 1 mod(z)$
12. $b \equiv a mod(u)$
13. $s \equiv x mod(u)$
14. $t \equiv \xi mod(z)$
15. $2^{n+1}\xi^n(\xi + 1)^n \ldots (\xi + n - 1)^n x^n (x + 1)^n \ldots (x + n - 1)^n | z$

Alors $\mathbb{N}_0 \subset S \subset \mathbb{Z}$.

En effet, supposons qu'il existe $x, y, \ldots, b \in \mathcal{O}_K$ satisfaisant 1-15 et on voudrait montrer que $\xi \in \mathbb{Z}$. Or, les conditions (1.0.3), 5 et 6 entraînent que a et b

satisfont (1.0.2). Donc par 1-4 et le lemme 3 de [6], il existe $k, h, m, j \in \mathbb{N}$ tels que

$$x = \pm x_k(a) \text{ et } y = \pm y_k(a)$$

$$w = \pm x_n(a) \text{ et } z = \pm y_n(a)$$

$$u = \pm x_m(a) \text{ et } v = \pm y_m(a)$$

$$s = \pm x_j(a) \text{ et } t = \pm y_j(a)$$

Donc 7-14 deviennent:

7'. $|\sigma_i(y_h(a))| \geq \frac{1}{2}, i = 2, \ldots, n$
8'. $|\sigma_i(x_m(a))| \geq \frac{1}{2}, i = 2, \ldots, n$
9'. $y_m(a) \neq 0$
10'. ${y_h}^2(a) | y_m(a)$
11'. $b \equiv 1 mod(y_h(a))$
12'. $b \equiv a mod(x_m(a))$
13'. $x_j(b) \equiv \pm x_k(a) mod(x_m(a))$
14'. $y_j(b) \equiv \pm \xi mod(y_h(a))$.

Conséquemment on a:

16. $j \equiv \pm \xi mod(y_h(a))$
17. $k \equiv \pm j mod(m)$
18. $k \equiv \pm \xi mod(z)$

Donc on obtient $\xi = \pm k \in \mathbb{Z}$ car $|N(k \pm \xi)| < |\mathrm{N}(\mathrm{z})|$.

Inversement, si $\xi \in \mathbb{N}_0$, on veut montrer qu'il existe $x, y, \ldots, b \in \mathcal{O}_K$ satisfaisant 1-15. On pose $k = \xi \in \mathbb{N}_0$, $x = x_k(a)$, $y = y_k(a)$. Alors, 1 est satisfait. Aussi, on peut montrer qu'il existe un $h \in \mathbb{N}_0$ tel que le côté gauche de 15 divise $y_n(a)$ et tel que $|\sigma_i(y_h(a))| \geq \frac{1}{2}$, pour $i = 2, \ldots, n$. On pose donc $w = x_h(a)$,

$z = y_h(a)$ et 2,7 et 15 sont satisfaits. De la même façon, il existe un $m \in \mathbb{N}_0$ tel que ${y_h}^2(a)|y_m(a)$ et $|\sigma_i(x_m(a))| \geq \frac{1}{2}$, pour $i = 2, \ldots, n$. Puis on pose $u = x_m(a)$ et $v = y_m(a)$. On obtient ainsi 3,8,9 et 10. Puisqu'il existe un $b \in \mathcal{O}_K$ satisfaisant 5,6,11 et 12, on pose $s = x_k(b)$ et $t = y_k(b)$ donc 4 est satisfait. Finallement, 12 implique 13 et 11 implique 14. Donc $\xi \in S$.

Ainsi, on a prouvé qu'un ensemble diophantien sur $\mathcal{O}_K$ est coincé entre $\mathbb{N}_0$ et $\mathbb{Z}$. Donc $\mathbb{Z}$ est aussi diophantien sur $\mathcal{O}_K$ car pour $t \in \mathcal{O}_K$, si T est la définition de S dans $\mathcal{O}_K$, on a :

$$t \in \mathbb{Z} \Longleftrightarrow [T(t) \vee T(-t)].$$

Donc la réponse de H10$\mathcal{O}_K$ est négative lorsque K est un corps algébrique totallement réel.

Grace à ce dernier gain de Denef, Harold N. Shapiro et Alexandra Shlapentokh ont développé le dernier volet leur permettant de conclure que le dixième problème de Hilbert pour l'anneau des entiers de toute extension abélienne des rationnels est non résoluble. C'est en 1989 que fut publié leur article *Diophantine relationships between algebraic number fields* [**17**]. Ils ont introduit une notation intéressante pour présenter leur importante découverte. Soit E une extension finie du corps algébrique K. On écrira Dioph(E/K) si $\mathcal{O}_K$ est diophantien dans $\mathcal{O}_E$. Voici maintenant l'énoncé si simple d'un théorème si utile:

Théorème 1.0.4. *Soient K,E,L des corps algébriques tels que $K \subset E \subset L$. Alors Dioph(L/K) $\Longleftrightarrow$ Dioph(E/K) et Dioph(L/E).*

Avant d'attaquer la démonstration du théorème nous allons citer le lemme 2.2 de [**17**] dont nous aurons grand besoin.

Lemme 1.0.1. *Soient K,E des corps algébriques tels que $K \subset E$ et Dioph(E/K). Alors il existe une définition diophantienne $f(t, x_1, \ldots, x_n)$ de $\mathcal{O}_K$ dans $\mathcal{O}_E$ avec coefficients dans $\mathcal{O}_K$.*

Preuve du théorème:

($\Longrightarrow$) Par le lemme précédent, Dioph(L/K) entraîne l'existence d'une définition diophantienne de $\mathcal{O}_K$ dans $\mathcal{O}_L$ avec coefficients dans $\mathcal{O}_K$, disons $f(t, x_1, \ldots, x_n)$. Soit $w_1, \ldots, w_m$ une base de L/E avec $w_i \in \mathcal{O}_L$. Puisque cette base n'est pas nécessairement intégrale pour L sur E, il existe une constante $c = c(L, E) \in \mathcal{O}_K$ telle que pour tout x_i dans $\mathcal{O}_L$, $x_i = \sum_{j=1}^{m} a_{ij}(w_j/c)$ avec $a_{ij} \in \mathcal{O}_E$. Alors pour $t \in \mathcal{O}_L$, on obtiendra que $t \in \mathcal{O}_K$ si et seulement si il existe $x_1, \ldots, x_n \in \mathcal{O}_L$ tels que:

$$f(t, \sum_{j=1}^{m} a_{1j}(w_j/c), \ldots, \sum_{j=1}^{m} a_{nj}(w_j/c)) = 0. \tag{1.0.4}$$

Si on écrit:

$$f(t, x_1, \ldots, x_n) = \sum_{i_0, \ldots, i_n} c_{i_0, \ldots, i_n} t^{i_0} x_1^{i_1} \ldots x_n^{i_n}, \; c_{i_0, \ldots, i_n} \in \mathcal{O}_K \tag{1.0.5}$$

alors 1.0.4 entraîne que

$$\sum_{i_0, \ldots, i_n} c_{i_0, \ldots, i_n} t^{i_0} [\sum_{j=1}^{m} a_{1j}(w_j/c)]^{i_1} \ldots [\sum_{j=1}^{m} a_{nj}(w_j/c)]^{i_n} = 0. \tag{1.0.6}$$

De plus, $w_1^{j_1} \ldots w_m^{j_m} \in L$ donc peut s'écrire

$$w_1^{j_1} \ldots w_m^{j_m} = \sum_{k=1}^{m} r_{j_1, \ldots, j_m, k}(w_k/c), \; r_{j_1, \ldots, j_m, k} \in \mathcal{O}_E. \tag{1.0.7}$$

Ainsi 1.0.6 est de la forme:

$$\sum_{k=1}^{m} g_k(t, a_{11}, \ldots, a_{1m}, \ldots, a_{n1}, \ldots, a_{nm}) w_k = 0. \tag{1.0.8}$$

On constate que les g_k sont des polynômes dont les coefficients sont de la forme b/c^e, $b \in \mathcal{O}_E$ et $e \in \mathbb{N}$ avec $e \leq 1 + i_{1_0} + \ldots + i_{n_0} = d$ où $i_{1_0} + \ldots + i_{n_0} = degf$. Pour cette raison,

$$h_k(t, a_{11}, \ldots, a_{nm}) = c^d g_k(t, a_{11}, \ldots, a_{nm}), \; k = 1, \ldots, m \tag{1.0.9}$$

sont des polynômes avec coefficients dans $\mathcal{O}_E$. Donc pour tout $t \in \mathcal{O}_L$, 1.0.8 et 1.0.9 impliquent que si $t \in \mathcal{O}_K$ alors les équations $h_k(t, a_{11}, \ldots, a_{nm}) = 0$ ont une solution pour $a_{ij} \in \mathcal{O}_E$ et $k = 1, \ldots, m$ (car les w_k sont linéairement indépendants sur E). Donc pour $t \in \mathcal{O}_E$, $t \in \mathcal{O}_K$ implique que les h_k à coefficients dans $\mathcal{O}_E$ ont une solution en $a_{ij} \in \mathcal{O}_E$.

Inversement, si pour un t donné dans $\mathcal{O}_E \subset \mathcal{O}_L$ les équations $h_k = 0$ ont une solution pour $a_{ij} \in \mathcal{O}_E$, les $x_i = \sum_{j=1}^{m} a_{ij}(w_j/c)$ et t sont des solutions de $f(t, x_1, \ldots, x_n) = 0$. Par contre, pour conclure que $t \in \mathcal{O}_K$ il faut vérifier que les x_i sont éléments de $\mathcal{O}_L$ afin de pouvoir utiliser Dioph(L/K). Pour ce faire, on ajoute des équations polynômiales satisfaites lorsque $t \in \mathcal{O}_K$.

Jusqu'à présent, on peut seulement affirmer que $x_i \in \mathcal{O}_{L/c}$. On choisira donc plutôt c=c(L) parmi les entiers. Pour voir que ceci est possible consultez [**10**]. Ainsi, l'idéal principal $c \cdot \mathcal{O}_E$ a un nombre fini de classes modulo c dans $\mathcal{O}_E$. On choisit un représentant par classe ce qui donne $\mu_1, \ldots, \mu_q \in \mathcal{O}_E$. Par conséquent, pour $a_{ij} \in \mathcal{O}_E$ on trouve

$$a_{ij} \equiv \mu(a_{ij}) \ mod(c \cdot \mathcal{O}_E) \tag{1.0.10}$$

avec $\mu(a_{ij})$ parmi $\mu_1, \ldots, \mu_q$. Alors le fait que $x_i = \sum_{j=1}^{m} a_{ij}(w_j/c)$ soit dans $\mathcal{O}_L$ est équivalent à

$$\sum_{j=1}^{m} a_{ij} w_j \equiv \sum_{j=1}^{m} \mu(a_{ij}) w_j \equiv 0 \ mod(c \cdot \mathcal{O}_L). \tag{1.0.11}$$

Mais l'ensemble des vecteurs $A = (\mu_{i_1}, \ldots, \mu_{i_m})$ tels que

$$\sum_{j=1}^{m} \mu_{i_j} w_j \equiv 0 \ mod(c \cdot \mathcal{O}_L) \tag{1.0.12}$$

est fini car le nombre de représentants est fini. Soit $A^{(p)} = (\alpha_{p1}, \ldots, \alpha_{pm})$, avec $p = 1, \ldots, \nu$ cet ensemble où chacun des α_{pj} est un des μ_i et donc un élément de

$\mathcal{O}_E$. Ainsi, pour tout $i = 1, \ldots, n$ il existe un p tel que pour tout $j = 1, \ldots, m$

$$a_{ij} - \alpha_{pj} - cz_{ij} = 0 \tag{1.0.13}$$

avec $z_{ij} \in \mathcal{O}_L$ comme nouvelles variables. On s'assure ainsi que $x_i \in \mathcal{O}_L$ si et seulement si il existe $z_{ij} \in \mathcal{O}_L$ satisfaisants 1.0.13. Avec l'ajout de cette équation, on a donc Dioph(E/K).

Montrons maintenant que Dioph(L/E). Soit $t \in \mathcal{O}_L$, par Dioph(L/K) on a $t \in \mathcal{O}_K$ si et seulement si il existe $x_i \in \mathcal{O}_L$ tel que $f(t, x_1, \ldots, x_n) = 0$. On suppose les coefficients de f dans $\mathcal{O}_K$ par le lemme 1.0.1. Si [E:K]=m et soient $w_j \in \mathcal{O}_E$, $j = 1, \ldots, m$ les éléments d'une base de E/K. De même que précédemment, il existe $0 \neq c = c(L) \in \mathbb{Z}$ tel que tout $t \in \mathcal{O}_E$ peut s'écrire

$$t = \sum_{j=1}^{m} a_j(w_j/c) \tag{1.0.14}$$

avec a_j dans $\mathcal{O}_K$. De plus il existe certains $x_{ij} \in \mathcal{O}_L$ tels que

$$a_j \in \mathcal{O}_K \Longleftrightarrow f(a_j, x_{1j}, \ldots, x_{nj}) = 0. \tag{1.0.15}$$

Donc pour $t \in \mathcal{O}_E$ on a 1.0.14, et 1.0.15 a des solutions $x_{1j}, \ldots, x_{nj} \in \mathcal{O}_L$ pour tout $j = 1, \ldots, m$. Pour $t \in \mathcal{O}_L$, si 1.0.15 a des solutions en $x_{ij} \in \mathcal{O}_L$ pour tout $j = 1, \ldots, m$ les a_j sont éléments de $\mathcal{O}_K$. Par 1.0.14 ceci implique que $t \in E$. Donc $t \in E \cap \mathcal{O}_L = \mathcal{O}_E$.

($\Longleftarrow$) Finallement, pour déduire Dioph(L/K) de Dioph(L/E) et Dioph(E/K), on pose $f(t, x_1, \ldots, x_n)$ comme définition diophantienne de $\mathcal{O}_E$ dans $\mathcal{O}_L$ et on pose $g(t, y_1, \ldots, y_q)$ comme définition diophantienne de $\mathcal{O}_K$ dans $\mathcal{O}_E$. On considère ensuite le système suivant:

$$f(t, x_1, \ldots, x_k) = 0 \tag{1.0.16}$$

$$\begin{cases} f(y_1, z_{11}, \ldots, z_{1k}) = 0 \\ \ldots \\ f(y_q, z_{q1}, \ldots, z_{qk}) = 0 \end{cases} \tag{1.0.17}$$

$$g(t, y_1, \ldots, y_q) = 0 \tag{1.0.18}$$

Si ce système a une solution dans $\mathcal{O}_L$ alors 1.0.16 implique que $t \in \mathcal{O}_E$ et 1.0.17 que $y_1, \ldots, y_q \in \mathcal{O}_E$. Par conséquent, 1.0.18 implique que $t \in \mathcal{O}_K$. Inversement, si $t \in \mathcal{O}_K$ il existe $y_1, \ldots, y_q \in \mathcal{O}_E$ tels que 1.0.18 est vraie. Puis pour tout y_j il existe $z_{ij} \in \mathcal{O}_L$ tels que l'équation correspondante de 1.0.17 est satisfaite. En conclusion, comme $t \in \mathcal{O}_E$ il y a une solution de 1.0.16 dans $\mathcal{O}_L$. □

La venue de ce dernier théorème fut un merveilleux avancement des connaissances. En effet, nous pouvons en déduire le corollaire:

Corollaire 1.0.1. *Si E est une extension abélienne des rationnels alors Dioph(E/$\mathbb{Q}$), c'est-à-dire $\mathbb{Z}$ est diophantien dans l'anneau des entiers algébriques de toute extension abélienne des rationnels.*

Preuve:

Comme nous l'avons vu dans ce chapitre, J. Denef et L. Lipschitz dans leurs articles [**7**] et [**6**] ont montré que $\mathbb{Z}$ est diophantien dans l'anneau des entiers algébriques de toute extension totallement réelle des rationnels, ainsi que dans leurs extensions de degré deux. Les corps cyclotomiques que nous noterons C sont des extensions de degré deux de corps totallement réels. Donc $\mathbb{Z}$ est diophantien dans l'anneau des entiers des corps cyclotomiques $\mathcal{O}_C$. En conséquence, on obtient Dioph(C/$\mathbb{Q}$). De plus, le théorème de Kronecker (voir [**10**]) implique que les extensions abéliennes des rationnels, disons Ab, sont des sous-corps de corps cyclotomiques. Donc $\mathbb{Q} \subseteq Ab \subseteq C$ et Dioph(C/$\mathbb{Q}$) implique Dioph(Ab/$\mathbb{Q}$) et Dioph(C/Ab). De la première de ces déductions on tire que $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$ est diophantien dans $\mathcal{O}_{Ab}$.

Nous concluons maintenant cette revue avec un dernier résultat très important lui aussi. Nous allons d'ailleurs l'utiliser abondamment au chapitre trois. Toujours en 1989, Alexandra Shlapentokh publie un nouvel article nommé *Extension of Hilbert's tenth problem to some algebraic number fields* [18]. Elle y obtient un théorème similaire à celui qu'avait trouvé Pheidas Thaneses en 1987. En voici l'énoncé:

Théorème 1.0.5. *Soit K un corps algébrique avec exactement une paire d'isomorphismes complexes conjugués. Alors $\mathbb{Z}$ est diophantien dans $\mathcal{O}_K$.*

Sa preuve est constitiée d'une succession de vingt et un lemmes. Nous allons tenter de vous la résumer! On suppose que K est de degré n sur $\mathbb{Q}$. Soit σ_1=id, et σ_2 le deuxième $\mathbb{Q}$-isomorphisme complexe de K. Alors $\sigma_3, \ldots, \sigma_n$ sont les $\mathbb{Q}$-isomorphismes réels de K. Soit ρ une racine de l'unité de degré plus petit ou égal à 2n. Voici la liste de quelques-uns des lemmes qui sont indispensables à la bonne compréhension de la suite. Par soucis de concision, nous allons par contre nous limiter à démontrer le corps de la preuve.

Lemme 1.0.2. *Il existe $a \in \mathcal{O}_K$ tel que $0 < \sigma_i(a) < 1$ pour $i = 3, \ldots, n$, et $|a| = |\sigma_2(a)| > 2^n$.*

Lemme 1.0.3. *Si $|\sigma_i(a)| < 1$ pour $3 \leq i \leq n$, alors $a^2 - 1$ n'est pas un carré dans K.*

Lemme 1.0.4. *Soient $a, b \in \mathcal{O}_K$ tel que a^2-1, b^2-1 ne sont pas des carrés dans K. On définit $x_m(a) \pm y_m(a)\delta(a) = (a \pm \delta(a))^m = (a \pm (a^2-1)^{\frac{1}{2}})^m = (\varepsilon(a))^m$. On définit $x_m(b)$ et $y_m(b)$ de façon similaire. Alors pour $m \in \mathbb{Z}$, $(x_m(a), y_m(a))$ sont des $\mathcal{O}_K$-solutions de l'équation de Pell $x^2 - (a^2-1)y^2 = 1$, de même que $(x_m(b), y_m(b))$ sont des $\mathcal{O}_K$-solutions de l'équation de Pell $x^2 - (b^2-1)y^2 = 1$. De plus, x_m, y_m ont les propriétés suivantes:*

i. $h/m \Rightarrow y_h(a)|y_m(a)$;

ii. $y_m \equiv m \ mod \ (a-1)$;

iii. si $a \equiv b \ mod\ c$ *alors* $x_k(a) \equiv x_k(b) \ mod\ c$, *et* $y_k(a) \equiv y_k(b) \ mod\ c$;

iv. si $v \in \mathcal{O}_K$, $v \neq 0$, *alors il existe* $m \in \mathbb{N}_o$ *tel que* $v | y_m(a)$.

Lemme 1.0.5. *On considère* $S = \{x + y\delta | x^2 - Dy^2 = 1, x, y \in \mathcal{O}_K\} \subseteq \mathcal{O}_K$ *avec* $D = a^2 - 1$, *et* $\delta = \delta(a)$. *Alors le rang de* S *est 1.*

Notation: chaque σ_i, $i = 1, \ldots, n$, est étendu en deux plongements distincts de $K(\delta)$. On note ces deux extensions par σ_{i1}, σ_{i2}. À partir de maintenant, $\sigma_{11}(\varepsilon(a))$ sera noté par ε et $\sigma_{12}(\varepsilon(a))$ par ε^{-1}. On choisit le signe de $a \pm \delta(a)$ dans le lemme 1.0.4 tel que $|\varepsilon| > 1$.

Lemme 1.0.6. *Si* $a \in \mathcal{O}_K$, $|\sigma_i(a)| \leq \frac{1}{2}$, $i = 3, \ldots, n$, *et* $|a| = |\sigma_2(a)| \geq 2^n$, $S = \{x + y\delta | x^2 - Dy^2 = 1, x, y \in \mathcal{O}_K\}$ *où* $D = a^2 - 1$, $\delta = D^{\frac{1}{2}}$. *Alors* ε *génère* S *à une racine de l'unité près.*

Lemme 1.0.7. *Il existe une constante C=C(K) telle que pour tout entier t non nul, il existe des multiples entiers positifs r et h de t tels que* $|\sigma_i(x_r(a))| \geq \frac{1}{2}$ *et* $|\sigma_i(y_h(a))| \geq C > 0$ *avec* $i = 3, \ldots, n$ *et* $(x_r(a), y_r(a)), (x_h(a), y_h(a))$ *solutions de l'équation de Pell comme en 1.0.4.*

Lemme 1.0.8. *Soit* $C_0 = max_{i=3,\ldots,n}\{\frac{1}{|\sigma_{i1}(\delta)|}\}$, *et soit e un entier positif tel que* $|\varepsilon^e| > 2(C_0/C)^{(n-2)/2} + 2$. *Supposons aussi que* $m, h \in \mathbb{N}$, $|\sigma_i(y_{eh})| \geq C$. *Alors*

i. $y_{eh} | y_{em} \Rightarrow h | m$,

ii. ${y_{eh}}^2 | y_{em} \Rightarrow ehy_{eh} | em$.

Lemme 1.0.9. *Supposons que* $b \in \mathcal{O}_K, k \in \mathbb{Z}$ *sont tels que*
$2^k \prod_{i=3}^{n} |\sigma_i(a)| \geq 1$ *et* $\prod_{i=3}^{n} |\sigma_i(b)| \leq 2^{-(k+3n-2)}$
où $0 \neq b \equiv 0 \ mod\ x_m^4 + a(1 - x_m^2)$. *Alors* $|b| > 2^n$.

Lemme 1.0.10. *Soit* $b = (x_m^2 + Dy_m^2)^{2s}(x_m^4 + a(1 - x_m^2))$. *Alors*

i. $b \equiv 1 \ mod\ y_m(a)$

ii. $b \equiv a \ mod\ x_m(a)$

iii. si $i = 3, \ldots, n$ *et s est suffisament grand dans* $\mathbb{Z}_0$ *on a* $|\sigma_i(b)| \leq 2^{(2-3n-k)/n-2}$.

Lemme 1.0.11. *Soient K un corps algébrique de degré n sur $\mathbb{Q}$ et $\sigma_1, \ldots, \sigma_n$ ses plongements dans $\mathbb{C}$. Soient $\xi,\ z \in \mathcal{O}_K$, $z \neq 0$. Si $2^{n+1}\xi^n(\xi+1)^n \cdots (\xi+n-1)^n | z$, alors pour tout $i = 1, \ldots, n$ $|\sigma_i(\xi)| < \frac{1}{2}|N_{K/\mathbb{Q}}(z)|^{1/n}$.*

Alors grâce à tous ces lemmes préliminaires nous pouvons maintenant aborder la démonstration du lemme principal:

Lemme 1.0.12. *Soient $a, C, C_0, \varepsilon(a), k, e$ définis comme dans les lemmes précédents. Soit $r \in \mathbb{N}$ tel que pour toute racine de l'unité ρ, $\rho^r = 1$. De plus, on choisit a de manière à ce que $\varepsilon(a)$ ne soit pas une racine de l'unité dans $K(a^2-1)^{1/2}$. Alors $er\mathbb{N}_0 \subseteq S \subseteq \mathbb{Z}$ où $S \subseteq \mathcal{O}_K$ est défini par:*
$\xi \in S \Longleftrightarrow \xi \in \mathcal{O}_K$ et $\exists x, x_1, y, y_1, w, w_1, z, z_1, u, u_1, v, v_1, s, s_1, t, t_1, b \in \mathcal{O}_K$ tels que;

$$x_1^2 - (a^2-1)y_1^2 = 1, \tag{1.0.19}$$

$$x - \delta(a)y = (x_1 - \delta(a)y_1)^{re}, \tag{1.0.20}$$

$$w_1^2 - (a^2-1)z_1^2 = 1, \tag{1.0.21}$$

$$w - \delta(a)z = (w_1 - \delta(a)z_1)^{re}, \tag{1.0.22}$$

$$u_1^2 - (a^2-1)v_1^2 = 1, \tag{1.0.23}$$

$$u - \delta(a)v = (u_1 - \delta(a)v_1)^{re}, \tag{1.0.24}$$

$$|\sigma_i(b)| < 2^{(2-3n-k)/n-2},\ i = 3, \ldots, n, \tag{1.0.25}$$

$$b \equiv 0\ mod\ (u^4 + a(1-u^2)), \tag{1.0.26}$$

$$s_1^2 - (b^2-1)t_1^2 = 1, \tag{1.0.27}$$

$$s - \delta(b)t = (s_1 - \delta(b)t_1)^{re}, \tag{1.0.28}$$

$$|\sigma_i(z)| \geq C, \tag{1.0.29}$$

$$|\sigma_i(u)| > \frac{1}{2}, \tag{1.0.30}$$

$$v \neq 0, \tag{1.0.31}$$

$$z^2|v, \tag{1.0.32}$$

$$b \equiv 1 \ mod \ z, \tag{1.0.33}$$

$$b \equiv a \ mod \ u, \tag{1.0.34}$$

$$s \equiv x \ mod \ u, \tag{1.0.35}$$

$$t \equiv \xi \ mod \ z, \tag{1.0.36}$$

$$2^n\xi^n(\xi+1)^n\cdots(\xi+n-1)^n x^n\cdots(x+n-1)^n|z, \tag{1.0.37}$$

$$\varepsilon(b) = b \pm \delta(b) \ \textit{n'est pas une racine de l'unité.} \tag{1.0.38}$$

Preuve du lemme principal:

I) supposons qu'il existe $x, \ldots, b$ satisfaisant les conditions énumérées ci-haut. Alors par le lemme 1.0.6 on peut écrire:
$x_1 - \delta(a)y_1 = \rho(\varepsilon(a))^{\pm k}$, donc $x - \delta(a)y = (\varepsilon(a))^{\pm erk}$ par 1.0.20.
En conséquence, $x = \pm x_{erk}(a)$ et $y = \pm y_{erk}(a)$. De même on a, $w = \pm x_{erh}(a)$, $u = \pm x_{erm}(a)$, $z = \pm y_{erh}(a)$ et $v = \pm y_{erm}(a)$.

On obtient par le lemme 1.0.9 que $|b| = |\sigma_2(b)| > 2^n$. Comme 1.0.27, 1.0.28 entraînent $|\sigma_i(b)| < \frac{1}{2}$ pour $i = 3, \ldots, n$, alors $b^2 - 1$ n'est pas un carré dans K par le lemme 1.0.3. Ensuite, le lemme 1.0.5 nous assure que pour $D(b) = b^2 - 1$, l'ensemble $S(b) = \{x + y\delta(b) | x^2 - D(b)y^2 = 1, x, y \in \mathcal{O}_K\}$ est de rang 1. On pose $\varepsilon(b) = b \pm \delta(b)$ et alors $\varepsilon(b)$ génère $S(b)$ à une unité près. Ainsi, on a

$s = \pm x_{erj}(b)$, $t = \pm y_{erj}(b)$. Par ce qui précède, on réécrit les équations 1.0.29 à 1.0.36:

$$|\sigma_i(y_{erh}(a))| \geq C, \tag{1.0.39}$$

$$|\sigma_i(x_{erm}(a))| > \frac{1}{2}, \tag{1.0.40}$$

$$y_{erm}(a) \neq 0, \tag{1.0.41}$$

$$y_{erh}(a)^2 | y_{erm}(a), \tag{1.0.42}$$

$$b \equiv 1 \ mod \ y_{erh}(a), \tag{1.0.43}$$

$$b \equiv a \ mod \ x_{erm}(a), \tag{1.0.44}$$

$$x_{erj}(b) \equiv \pm x_{erk}(a) \ mod \ x_{erm}(a), \tag{1.0.45}$$

$$y_{erj} \equiv \xi \ mod \ y_{erh}(a). \tag{1.0.46}$$

Par le lemme 1.0.4 $y_{erj}(b) \equiv erj \ mod \ (b-1)$, puis comme $y_{erh}(a) | b-1$ par 1.0.43 on trouve $y_{erj}(b) \equiv erj \ mod \ y_{erh}(a)$. Ceci entraîne par 1.0.46 que $erj \equiv \pm\xi \ mod \ y_{erh}(a)$. Par le lemme 1.0.4 toujours et 1.0.44 on trouve que $x_{erj}(b) \equiv x_{erj}(a) \ mod \ x_{erm}(a)$, donc $x_{erj}(a) \equiv x_{erk}(a) \ mod \ x_{erm}(a)$ par 1.0.45. On en tire que $erj \equiv \pm erk \ mod \ erm$ à l'aide du lemme 1.0.8 et de 1.0.40. De plus, du même lemme et 1.0.39, 1.0.42 on obtient que $y_{erh}(a) | erm$ donc que $erj \equiv \pm erk \ mod \ y_{erh}(a)$.

On a $\xi \equiv \pm erk \ mod \ y_{erh}(a)$ selon 1.0.38 donc

$$\xi \equiv \pm erk \ mod \ z. \tag{1.0.47}$$

Puisque $erk < |x_{erk}(a)|$, $erk < \frac{1}{2}|N_{K/\mathbb{Q}}(z)|^{1/n}$ par 1.0.37 et 1.0.11. En outre, $|\sigma_i(\xi)| < \frac{1}{2}|N_{K/\mathbb{Q}}(z)|^{1/n}$ pour tout $i = 1, \ldots, n$. Alors

$$\begin{aligned} |\sigma_i(erk \pm \xi)| &\leq erk + |\sigma_i(\xi)| \\ &< |N_{K/\mathbb{Q}}(z)|^{1/n} \\ \Rightarrow |N_{K/\mathbb{Q}}(erk \pm \xi)| &< |N_{K/\mathbb{Q}}(z)| \end{aligned}$$

$\Rightarrow erk = \pm\xi$ par 1.0.47

$\Rightarrow \xi \in \mathbb{Z}_0$.

II) Inversement, supposons que $\xi = erk$ pour un certain $k \in \mathbb{N}_0$. On pose $x_1 = x_k(a), y_1 = y_k(a), x = x_{erk}(a), y = y_{erk}(a)$. Ainsi 1.0.19 et 1.0.20 sont satisfaits. On utilise le lemme 1.0.4 pour trouver $l \in \mathbb{N}_0$ tel que le côté gauche de l'équation 1.0.37 divise $y_l(a)$. Par le lemme 1.0.8, on obtient g un multiple de erl tel que $|\sigma_i(y_g)| \geq C$, $i = 3, \ldots, n$. Soit erh=g. On pose par conséquent $w_1 = x_h(a), z_1 = y_h(a), w = x_{erh}(a), z = y_{erh}(a)$. Alors 1.0.21, 1.0.22, 1.0.29, et 1.0.37 sont satisfaits. On sait par le lemme 1.0.4 qu'il existe $g' \in \mathbb{N}_0$ tel que $y_{erh}(a)^2 | y_{g'}$. De plus 1.0.7 assure l'existence de f un multiple de erg tel que $|\sigma_i(x_f)| > \frac{1}{2}$, pour $i = 3, \ldots, n$. Soit f=erm. On remarque que $y_{g'}(a) | y_f(a)$. Donc, $y_{erh}(a)^2 | y_{erm}(a)$.

Les équations 1.0.23, 1.0.24, 1.0.30, 1.0.31, 1.0.32 sont satisfaites lorsqu'on pose $u_1 = x_m(a), v_1 = y_m(a), u = x_{erm}(a), v = y_{erm}(a)$. On considère maintenant $b = (x_{erm}(a)^2 + D(a)y_{erm}(a)^2)^{2s}(x_{erm}(a)^4 + a(1 - x_{erm}(a)^2))$. On a que $b \equiv 1 \ mod \ y_{erm}(a)$ et $b \equiv a \ mod \ x_{erm}(a)$ par 1.0.10, qui entraîne aussi qu'on puisse choisir un s assez grand tel que $|\sigma_i(b)| \leq 2^{(2-3n-k)/n-2}$, $i = 3, \ldots, n$. De plus, $y_{erh}(a) | b-1$ puisque $y_{erh}(a) | y_{erm}(a)$. Donc, a et b respectent 1.0.26, 1.0.27, 1.0.28, 1.0.33, 1.0.34. Finallement, en posant $s_1 = x_k(b), t_1 = y_k(b), s = x_{erk}(b)$, et $t = y_{erk}(b)$ on satisfait 1.0.25, puis 1.0.35 et 1.0.36 par le lemme 1.0.4.

La preuve du théorème 1.0.5 devient très simple lorsque le lemme principal est démontré. Voici d'ailleurs les quelques explications qui la composent.
Preuve du théorème:

On a trouvé un ensemble S coincé entre $er\mathbb{N}_0$ et $\mathbb{Z}$. Cet ensemble est diophantien dans $\mathcal{O}_K$ puisque toutes les conditions qui le définissent le sont. Aussi, si $\xi \in \mathbb{Z}_0$ alors $\pm\xi \in \mathbb{N}_0$ donc $\pm er\xi \in er\mathbb{N}_0 \subseteq S$. En conséquence, pour tout $\xi \in \mathcal{O}_K$, on a $\xi \in \mathbb{Z}_0 \Longleftrightarrow \pm er\xi \in S$ car si $er\xi \in S \subseteq \mathbb{Z}$ alors $\xi \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$ étant donné que $er \in \mathbb{N}$. Le cas de zéro peut être regardé préalablement. Donc la conclusion est que $\mathbb{Z}$ est diophantien dans $\mathcal{O}_K$. □

Dans tous les cas traités jusqu'à maintenant, des chercheurs de grand talent ont démontré le caractère non résoluble du dixième problème de Hilbert adapté à des anneaux d'entiers algébriques pour certaines classes de corps algébriques. Pour ce faire, nous avons montré qu'ils ont défini $\mathbb{Z}$ de façon diophantienne dans ces anneaux d'entiers algébriques.

D'un autre point de vue, Robert S. Rumely a découvert en 1985 par un travail sur les variétés affines qu'il existe un algorithme permettant de savoir quand un système d'équations diophantiennes a des solutions dans l'anneau de tous les entiers algébriques. On retrouve donc une preuve que la réponse au dixième problème de Hilbert est positive dans ce dernier anneau dans son article *Arithmetic over the ring of all algebraic integers* [**16**]. Or il est impossible de construire une définition diophantienne de $\mathbb{Z}$ dans l'anneau de tous les entiers algébriques réels (voir [**4**]).

Ces différents résultats soulèvent de nombreuses questions quant au type d'extension algébrique des rationnels L se situant à la limite entre H10$\mathcal{O}_L$ résoluble et H10$\mathcal{O}_L$ non résoluble. De plus, le caractère résoluble ou non du dixième problème de Hilbert pour des anneaux d'entiers algébriques en général ainsi que des corps algébriques eux-mêmes restent un problème ouvert.

Récemment, Alexandra Shlapentokh publiait l'article *Diophantine undecidability in some rings of algebraic numbers of totally real infinite extensions of*

$\mathbb{Q}$ [**19**]. Avec cet article, elle effectue une percée en obtenant des résultats significatifs sur les extensions algébriques infinies des rationnels. Nous citons ici son théorème 4.3 afin d'illustrer une partie de son travail.

Théorème 1.0.6. *Soit K_{inf} une extension totallement réelle infinie des rationnels. Soient K un sous-corps de degré fini de K_{inf} et S un ensemble de nombres premiers de K restant premiers dans K_{inf}. Alors $\mathbb{Z}$ a une définition diophantienne dans la clôture intégrale de $\mathcal{O}_{K,S}$ dans K_{inf}, où $\mathcal{O}_{K,S}$=$\{x \in K | ord_q x \geq 0, \forall q \notin S\}$.*

Dans cette revue, nous vous avons guidés à travers les plus récentes découvertes et nous allons maintenant tenter au chapitre trois d'obtenir la conjecture de Lipshitz et Denef pour des corps algébriques n'étant pas des extensions abéliennes des rationnels, mais ayant tout de même des propriétés pouvant s'en rapprocher. Cependant, avant d'entreprendre ce périple il importe d'abord de se familiariser avec la preuve de Lipshitz et Denef afin d'en comprendre et maîtriser toutes les subtilités. À cette fin, nous espérons que notre version présentée au prochain chapitre en facilitera la compréhension.

Chapitre 2

ENSEMBLES DIOPHANTIENS SUR DES ANNEAUX D'ENTIERS ALGÉBRIQUES

Ce chapitre est consacré à l'étude de l'article [7] de J.Denef et L.Lipshitz. Nous souhaitons à la fois en vulgariser le contenu et repérer les résultats intermédiaires réutilisables avec des anneaux d'entiers algébriques d'extensions non abéliennes des rationnels.

Soit B un anneau commutatif ($1 \in$ B) et soit $R(x_1, x_2, \ldots, x_n)$ une relation dans B. On dira que cette relation est diophantienne dans B si il existe un polynôme $P(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m)$ à coefficients dans B, tel que pour tout $x_1, x_2, \ldots, x_n \in B$:

$$R(x_1, x_2, \ldots, x_n) \Longleftrightarrow \exists y_1, y_2, \ldots, y_m \in B : P(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0.$$

De plus, un sous-ensemble S de B est diophantien dans B si la relation unaire $x \in$ S est diophantienne dans B. Nous reprenons ici l'exemple de l'article original. Soit W l'ensemble des entiers k pour lesquels il existe $x, y \in \mathbb{Z}$ tels que l'équation de Mordell $y^2 = x^3 + k$ soit vraie. Cet ensemble est diophantien dans $\mathbb{Z}$ puisque $k \in W \Longleftrightarrow \exists x, y \in Z : y^2 - x^3 - k = 0$.

Étant donné un anneau B, il serait souhaitable de caractériser toutes les relations qui sont diophantiennes dans B. Dans ce but, M. Davis, Y. Matijasevič, H. Putnam et J. Robinson ont prouvé qu'une relation R est diophantienne dans

$\mathbb{Z}$ si et seulement si R est récursivement énumérable. Ceci a permis de démontrer entre autres, que la réponse au 10^e problème d'Hilbert dans $\mathbb{Z}$ était négative. Aussi soient L un corps algébrique, et $\mathcal{O}_L$ son anneau des entiers algébriques. Soit B=L ou B=$\mathcal{O}_L$ et supposons que $\mathbb{Z}$ est diophantien dans B, nous allons montrer qu'une relation R est diophantienne dans B si et seulement si R est récursivement énumérable en utilisant leur résultat.

Notation: À partir de maintenant, nous utiliserons $L = B(\alpha_1, \ldots, \alpha_s)$ pour signifier que $\{\alpha_1, \ldots, \alpha_s\}$ est une base de L considéré comme un B module. De plus, $B[x_1, \ldots, x_n]$ désignera l'anneau des polynômes à coefficients dans B dont les variables sont $x_1, \ldots, x_n$.

($\Longrightarrow$)

i) $B = \mathcal{O}_L = \mathbb{Z}(\alpha_1, \alpha_2, \ldots, \alpha_l)$ où $L = \mathbb{Q}(\theta)$.

R une relation dans B est diophantienne dans B si et seulement si

$\exists P \in B[x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m]$ tel que $\forall x_1, x_2, \ldots, x_n \in B$,

$R(x_1, x_2, \ldots, x_n) \Longleftrightarrow \exists y_1, y_2, \ldots, y_m \in B$ tels que

$P(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0$.

Soient $x_1, x_2, \ldots, x_n \in \mathbb{Z} \subseteq B$. Alors,

$$
\begin{aligned}
R(x_1, \ldots, x_n) &\Longleftrightarrow \exists y_1, y_2, \ldots, y_m \in B \text{ tels que} \\
&\quad P(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0 \\
&\Longleftrightarrow \exists {y_1}^1, \ldots, {y_1}^l, \ldots, {y_m}^1, \ldots, {y_m}^l \in \mathbb{Z} \text{ tels que} \\
&\quad P(x_1, \ldots, x_n, {y_1}^1\alpha_1, + \ldots + {y_1}^l\alpha_l, \ldots, {y_m}^1\alpha_1 + \ldots + {y_m}^l\alpha_l) \\
&\quad = 0 \\
&\Longleftrightarrow \exists {y_j}^k \in \mathbb{Z}, 1 \leq k \leq l, 1 \leq j \leq m \text{ tels que, pour } 1 \leq i \leq n \\
&\quad P_1(x_i, {y_j}^k)\alpha_1 + \ldots + P_l(x_i, {y_j}^k)\alpha_l = 0, \\
&\quad \text{pour } P_1 \ldots, P_l \text{ des polynômes à coefficients entiers.}
\end{aligned}
$$

On a séparé tous les éléments de B, en particulier les coefficients, mais aussi les $\alpha_k^r, r \geq 2$ le cas échéant car ils restent éléments de B, donc s'expriment dans la base. Ainsi, les polynômes $P_1, \ldots, P_l$ ont des coefficients entiers. Donc,

$$\begin{aligned} R(x_1, \ldots, x_n) \Longleftrightarrow & \exists {y_j}^k \in \mathbb{Z}, 1 \leq k \leq l, 1 \leq j \leq m \text{ tels que }, \\ & P_1(x_i, {y_j}^k) = \ldots = P_l(x_i, {y_j}^k) = 0 \\ & \text{car } \alpha_1, \ldots, \alpha_l \text{ sont linéairement indépendants sur B} \\ \Longleftrightarrow & \exists {y_j}^k \in \mathbb{Z}, 1 \leq k \leq l, 1 \leq j \leq m, \\ & \left(P_1(x_i, {y_j}^k)^2 - aP_2(x_i, {y_j}^k)^2\right)^2 - \ldots\Big)^2 - aP_l(x_i, {y_j}^k)^2 = 0 \\ & \text{où } a \in I\!N, \text{ mais } \sqrt{a} \notin B. \end{aligned}$$

Nous savons que a existe car L est une extension finie de $\mathbb{Q}$ et $\{\sqrt{m} : m \in I\!N\}$ est infini donc ne peut pas être inclus dans B.
Ainsi R est diophantienne dans $\mathbb{Z}$ ce qui entraîne que R soit récursivement énumérable par le résultat de Davis, Matijasevič, Putnam et Robinson. □

ii) $B = L = \mathbb{Q}(\theta)$ dont une base sur $\mathbb{Q}$ est $\{1, \theta, \theta^2, \ldots, \theta^{l-1}\}$.
R est diophantienne dans B si et seulement si
$\exists P \in B[x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m]$ tel que $\forall x_1, x_2, \ldots, x_n \in B$,
$R(x_1, x_2, \ldots, x_n) \Longleftrightarrow \exists y_1, y_2, \ldots, y_m \in B$ tels que
$P(x_i, y_j) = 0$ où $i = 1, \ldots, n$ et $j = i, \ldots, m$. Soient $x_1, \ldots, x_n \in \mathbb{Z} \subseteq B$. Alors,

$$\begin{aligned} R(x_1, \ldots, x_n) \iff & \exists y_1, y_2, \ldots, y_m \in B \text{ tel que} \\ & P(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0 \\ \iff & \exists y_j^0, \ldots, y_j^{l-1} \in \mathbb{Q} \\ & P(x_i, y_1^0 + y_1^1\theta + \ldots + y_1^{l-1}\theta^{l-1}, \ldots, y_m^0 + \ldots + y_m^{l-1}\theta^{l-1}) = 0 \end{aligned}$$

$$\iff \exists a_j^k,\ b_j^k \in \mathbb{Z}\ , k = 0, 1, \ldots, l-1$$

$$P(x_i, \frac{a_1^0}{b_1^0} + \frac{a_1^1}{b_1^1}\theta + \ldots + \frac{a_1^{l-1}}{b_1^{l-1}}\theta^{l-1}, \ldots, \frac{a_m^0}{b_m^0} + \ldots + \frac{a_m^{l-1}}{b_m^{l-1}}\theta^{l-1}) = 0$$

$$\iff \exists a_j^k,\ b_j^k \in \mathbb{Z}$$

$$P_0(x_i, \frac{a_j^k}{b_j^k}) + P_1(x_i, \frac{a_j^k}{b_j^k})\theta + \ldots + P_{l-1}(x_i, \frac{a_j^k}{b_j^k})\theta^{l-1} = 0$$

$$\iff \exists a_j^k,\ b_j^k \in \mathbb{Z}$$

$$(P_0(x_i, \frac{a_j^k}{b_j^k})^2 - cP_1(x_i, \frac{a_j^k}{b_j^k})^{2\,2} - \ldots)^2 - cP_{l-1}(x_i, \frac{a_j^k}{b_j^k})^2 = 0$$

où c $\in \mathbb{N}$, mais $\sqrt{c} \notin$B

Donc R est diophantienne sur $\mathbb{Z}$

$\Rightarrow$ R est récursivement énumérable. □

($\Longleftarrow$)

i) $B = \mathcal{O}_L = \mathbb{Z}(\alpha_1, \alpha_2, \ldots, \alpha_l)$.

On a $\mathbb{Z}$ est diophantien dans B et on veut montrer que R est récursivement énumérable entraîne que R est diophantienne dans B. Soient $x_1, \ldots, x_n \in B$. On veut montrer qu'il existe un polynôme T à coefficients dans B tel que:

$$R(x_1, \ldots, x_n) \iff \exists v_1, \ldots, v_k \in B \text{ tels que } T(x_1, \ldots, x_n, v_1, \ldots, v_k) = 0.$$

Nous posons:

$$\psi : B \longrightarrow \mathbb{Z}^l$$

$$x_i = \sum_{j=1}^{l} a_{ij}\alpha_j \mapsto (a_{i1}, \ldots, a_{il})$$

pour $i = 1, \ldots, n$.

Soit S une relation sur $\mathbb{Z}^{nl}$ telle que

$$S(a_{11}, \ldots, a_{1l}, a_{21}, \ldots, a_{2l}, \ldots, a_{n1}, \ldots, a_{nl}) \iff R(x_1, \ldots, x_n).$$

Comme R est récursivement énumérable, alors $S \subseteq \mathbb{Z}^{nl}$ l'est aussi, ce qui implique d'aprés Matijasevič que S est diophantienne dans $\mathbb{Z}$.

$$\begin{aligned} &\Longrightarrow \quad \exists P \in \mathbb{Z}[x_1, \ldots, x_{nl+m}],\ \forall z_1, \ldots, z_{nl} \in \mathbb{Z}, S(z_1, \ldots, z_{nl}) \\ &\Longleftrightarrow \quad \exists y_1, \ldots, y_m \in \mathbb{Z}, P(z_1, \ldots, z_{nl}, y_1, \ldots, y_m) = 0. \end{aligned}$$

Donc, $R(x_1, \ldots, x_n) \Longleftrightarrow \exists a_{11}, \ldots, a_{1l}, a_{21}, \ldots, a_{n1}, \ldots, a_{nl} \in \mathbb{Z}$ et $y_1, \ldots, y_m \in \mathbb{Z}$ tels que $x_i = \sum_{j=1}^{l} a_{ij}\alpha_j$ et $P(a_{11}, \ldots, a_{nl}, y_1, \ldots, y_m) = 0$.

Mais, $\mathbb{Z}$ est diophantien dans B signifie qu'il existe $Q \in B[X]$ tel que

$$\forall x \in B,\ x \in \mathbb{Z} \Longleftrightarrow \exists s_1, \ldots, s_w \in B,\ Q(x, s_1, \ldots, s_w) = 0.$$

Donc,

$$R(x_1, \ldots, x_n) \Longleftrightarrow \exists a_{11}, \ldots, a_{nl}, y_1, \ldots, y_m \in B$$

et

$$s_{11}, \ldots, s_{1w}, \ldots, s_{(nl+m)1}, \ldots, s_{(nl+m)w} \in B$$

tels que

$$\begin{aligned} &((P(a_{11}, \ldots, a_{nl}, y_1, \ldots, y_m)^2 - cQ(a_{11}, s_{11}, \ldots, s_{1w})^2)^2 - \ldots \\ &-cQ(a_{nl}, s_{(nl)1}, \ldots, s_{(nl)w})^2)^2 - \ldots - c(x_1 - \sum_{j=1}^{l} a_{1j}\alpha_j)^2)^2 - \ldots \\ &-c(x_n - \sum_{j=1}^{l} a_{nj}\alpha_j)^2) = 0, \end{aligned}$$

où $c \in \mathbb{N}$, mais $\sqrt{c} \notin B$.

ii) $B = L = \mathbb{Q}(\alpha)$ dont une base sur $\mathbb{Q}$ est $\{1, \alpha, \ldots, \alpha^{l-1}\}$.
On a $\mathbb{Z}$ diophantien dans B et on veut montrer que si R est récursivement énumérable alors R est diophantienne dans B. Soit:

$$\begin{aligned} \psi : B &\longrightarrow \mathbb{Q}^l \\ \sum_{i=0}^{l-1} a_i\alpha^i &\mapsto (a_0, \ldots, a_{l-1}) \end{aligned}$$

Soient $x_1, \ldots, x_n \in B$. On a:

$$\begin{aligned} \psi(x_i) &= (x_{i0}, \ldots, x_{i(l-1)}) \\ &= (\frac{c_{i0}}{d_{i0}}, \ldots, \frac{c_{i(l-1)}}{d_{i(l-1)}}) \end{aligned}$$

où c_{ij}, $d_{ij} \in \mathbb{Z}$ et pour $i = 1, \ldots, n$, $j = 0, \ldots, (l-1)$.

On définit une relation S sur $\mathbb{Z}^{2nl}$ telle que S contient tous les 2nl-tuples dans $\mathbb{Z}$ qui sont les numérateurs et les dénominateurs d'une image par ψ d'un n-tuple de R. C'est -à-dire,

$$\text{si } R(x_1, \ldots, x_n)$$

et

$$\begin{aligned} \psi(x_1) &= (\frac{c_{10}}{d_{10}}, \ldots, \frac{c_{1(l-1)}}{d_{1(l-1)}}) \\ &= (\frac{\xi_0}{\rho_0}, \ldots, \frac{\xi_{l-1}}{\rho_{l-1}}) \text{ car la représentation n'est pas unique,} \end{aligned}$$

alors par exemple,
$(c_{i0}, \ldots, c_{i(l-1)}, d_{i0}, \ldots, d_{i(l-1)}) \in S$ et $(\xi_0, \ldots, \xi_{(l-1)}, c_{rs}, \rho_o, \ldots, \rho_{(l-1)}, d_{rs}) \in S$
où $i = 1, \ldots, n$; $r = 2, \ldots, n$ et $s = 0, \ldots, l-1$.

En résumé, pour chaque n-tuple de R on énumère tous les 2nl-tuples de $\mathbb{Z}$ pouvant le représenter. Comme R est récursivement énumérable alors $S \subseteq \mathbb{Z}^{2nl}$ l'est aussi car l'ensemble des façons d'écrire un nombre rationel comme un rapport de deux nombres entiers est dénombrable. Par le résultat de Matijasevič on peut donc affirmer que S est diophantienne dans $\mathbb{Z}$. D'où

$$\exists P \in \mathbb{Z}[X] \text{ tel que } \forall z_1, \ldots, z_{2nl} \in \mathbb{Z},\ S(z_1, \ldots, z_{2nl}) \Longleftrightarrow \exists y_1, \ldots, y_m \in \mathbb{Z},$$

$$P(z_1, \ldots, z_{2nl}, y_1, \ldots, y_m) = 0.$$

Donc,

$$R(x_1,\ldots,x_n) \Longleftrightarrow \exists c_{io},\ldots,c_{i(l-1)},d_{io},\ldots,d_{i(l-1)} \in \mathbb{Z}, \text{ et } y_1,\ldots,y_m \in \mathbb{Z}$$

$$\text{tels que } x_i = \sum_{j=0}^{l-1} \frac{c_{ij}}{d_{ij}}\alpha^j \text{ et } P(c_{ij},d_{ij},y_1,\ldots,y_m) = 0,\ i = 1,\ldots,n.$$

Mais $\mathbb{Z}$ est diophantien dans B implique qu'il existe un polynôme $Q \in B[X]$ tel que

$$\forall x \in B, x \in \mathbb{Z} \Longleftrightarrow \exists s_1,\ldots,s_w \in B,\ Q(x,s_1,\ldots,s_w) = 0.$$

Donc,

$$R(x_1,\ldots,x_n) \Longleftrightarrow \exists c_{io},\ldots,c_{i(l-1)},d_{io},\ldots,d_{i(l-1)},\ y_1,\ldots,y_m \in B$$

$$\text{et } \exists s_{11},\ldots,s_{(2nl+m)w} \in B, i = 1,\ldots,n \text{ tels que}$$

$((((P(c_{ij},d_{ij},y_1,\ldots,y_m)^2 - a\sum_{i,j} Q(c_{ij},s_{(ij)1},\ldots,s_{(ij)w})^2)^2 -$
$a\sum_{i,j} Q(d_{ij},s_{(ij)1},\ldots,s_{(ij)w}^2)^2 - a\sum_r Q(y_r,s_{(2nl+r)1},\ldots,s_{(2nl+r)w})^2)^2 -$
$a\sum_{i=1}^n (x_i - \sum_{j=o}^{l-1} a_{ij}\alpha^j)^2)^2 = 0$ où $a \in \mathbb{N}$, mais $\sqrt{a} \notin B$.
Finallement, on a R est diophantienne dans B. □

J. Denef et L. Lipshitz ont formulé la conjecture que $\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$ pour tout corps algébrique L. La preuve de cette affirmation serait un résultat d'une grande importance puisque si $\mathbb{Z}$ est diophantien dans un corps ou un anneau B, alors la réponse au 10^e problème de Hilbert adapté à B (H10B) est négative. Ceci veut dire qu'il n'y a pas d'algorithme permettant de savoir si une équation polynômiale avec coefficients dans B a une solution dans B. En effet, un algorithme pour H10B en donnerait un pour H10$\mathbb{Z}$ en utilisant le polynôme qui définit $\mathbb{Z}$ de manière diophantienne dans B. Ce serait une contradiction:

Si $\exists P \in B[X]$ tel que pour $x \in B$, on a $x \in \mathbb{Z} \Longleftrightarrow \exists y \in B,\ P(x,y) = 0$,

alors soit $Q(x_1, \ldots, x_n) = 0$ un polynôme à coefficients dans $\mathbb{Z}$. Comme $\mathbb{Z} \subseteq B$, on peut considérer $Q \in B[X]$ donc il possède une solution dans $\mathbb{Z}$ si et seulement si $Q(x_1, \ldots, x_n) = 0$, un polynôme à coefficients dans B, a une solution $x_1, \ldots, x_n$ dans B et $\exists y_1, \ldots, y_n \in B$ tels que $P(x_1, y_1) = 0, \ldots, P(x_n, y_n) = 0$. Donc l'algorithme s'applique.

J. Denef a prouvé que cette conjecture était vraie lorsque [L:$\mathbb{Q}$]=2 dans son article **[5]**. La méthode que Denef et Lipshitz ont utilisée dans l'article que nous présentons est une adaptation de celle de **[5]**, dans le but de trouver quelques nouveaux corps algébriques pour lesquels la conjecture est vraie. Ils ont trouvé deux nouvelles conditions suffisantes décrites avec celle de **[5]** dans le prochain théorème.

Sachez d'abord qu'un corps algébrique L est appelé totallement réel si tout plongement de L dans $\mathbb{C}$ envoie L dans $\mathbb{R}$.

Théorème 2.0.7. *$\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$ si le corps algébrique L satisfait une des conditions suivantes:*

a): *$[L : \mathbb{Q}]=2$,*

b): *$[L : \mathbb{Q}]=4$, L n'est pas totallement réel et L contient un sous-corps K tel que $[K : \mathbb{Q}]=2$,*

c): *L n'est pas totallement réel et est de degré 2 sur un sous-corps K totallement réel pour lequel $\mathbb{Z}$ est diophantien dans $\mathcal{O}_K$.*

De plus, 5 ans après la publication de ces résultats J.Denef fit paraître un nouvel article **[6]** dans lequel il prouvait que la conjecture est vraie pour tout corps algébrique totallement réel et donc (par c)) pour toute extension quadratique d'un corps algébrique totallement réel. Une ébauche de cette preuve est donnée au chapitre un.

Le théorème sera prouvé en utilisant le lemme principal, qui nécessite à son tour quelques lemmes et propriétés. Nous commençons par élaborer la démonstration de quatre propriétés des relations diophantiennes qui apparaissaient dans l'article original avec une suggestion pour chacune des preuves.

Proposition 2.0.1. *Soient K et L des corps algébriques tels que $K \subseteq L$*
a) Si R_1 et R_2 sont des relations diophantiennes sur $\mathcal{O}_L$ alors $R_1 \vee R_2$ et $R_1 \wedge R_2$ le sont aussi.
b) La relation $x \neq 0$ est diophantienne sur $\mathcal{O}_L$.
c) Si $\mathbb{Z}$ est diophantien sur $\mathcal{O}_K$ et si $\mathcal{O}_K$ est diophantien sur $\mathcal{O}_L$, alors $\mathbb{Z}$ est diophantien sur $\mathcal{O}_L$.
d) Si $\mathbb{Z}$ est diophantien sur $\mathcal{O}_L$ alors $\mathbb{Z}$ est diophantien sur $\mathcal{O}_K$.

Preuve:

a)

$(P_1 = 0) \vee (P_2 = 0) \Longleftrightarrow P_1 P_2 = 0$ donc $R_1 \vee R_2$ est diophantienne sur $\mathcal{O}_L$.
Soit $x^d + a_1 x^{d-1} + \ldots + a_d$ un polynôme sur $\mathbb{Z}$ n'ayant pas de racines dans L. Alors nous avons pour P_1 et P_2 dans $\mathcal{O}_L$:
$(P_1 = 0) \wedge (P_2 = 0) \Longleftrightarrow P_1^d + a_1 P_1^{d-1} P_2 + \ldots + a_d P_2^d = 0$ car:
$(\Longleftarrow)$ $\frac{P_1}{P_2} \in L$ puisque $P_1, P_2 \in \mathcal{O}_L$ et L est le corps de nombres de $\mathcal{O}_L$ et donc $(\frac{P_1}{P_2})^d + a_1 (\frac{P_1}{P_2})^{d-1} + \ldots + a_d = k \neq 0$.
$\Longrightarrow P_1^d + a_1 P_1^{d-1} P_2 + \ldots + a_d P_2^d = P_2^d k = 0 \Leftrightarrow P_2^d = 0$
$\Longrightarrow P_2 = 0$
$\Longrightarrow P_1^d = 0$
$\Longrightarrow P_1 = 0.$
$(\Longrightarrow)$: évident.

b) $x \neq 0 \Longleftrightarrow \exists u, v, y \in \mathcal{O}_L, xy = (2u-1)(3v-1)$
$(\Longleftarrow)$:Nous démontrons la contraposée. Si x=0 alors 0=xy=(2u-1)(3v-1) $\Rightarrow$ u=$\frac{1}{2}$ ou v=$\frac{1}{3} \notin \mathcal{O}_L$.

($\Longrightarrow$): Si x$\neq$0 alors $\exists s, t$ tels que $t \neq 0$ et x=$3^s t$ avec $3 \not| t$.
Par le théorème chinois de reste, il existe z tel que

$$\begin{aligned} z &\equiv 0 \ mod\ (t) \\ z &\equiv -1 \ mod\ (3) \text{ car } (3,t)=1 \end{aligned}$$

$\Longrightarrow \exists$ y,v $\in \mathcal{O}_L$ tels que $z = ty = 3v - 1$
$\Longrightarrow xy = 3^s ty = 3^s z = 3^s(3v-1)$ et 3^s est impair donc $\exists u \in \mathcal{O}_L$ tel que $3^s = 2u - 1$. Donc, si x$\neq$0 $\exists y, u, v \in \mathcal{O}_L$, xy=(2u-1)(3v-1).

c) On a pour $x \in \mathcal{O}_K$:

$$\exists P \in \mathcal{O}_K[X] \text{ tel que } x \in \mathbb{Z} \Leftrightarrow \exists y_1, \ldots, y_n \in \mathcal{O}_K \ P(x, y_1, \ldots, y_n) = 0, \quad (2.0.48)$$

et on a pour $x \in \mathcal{O}_L$:

$$\exists Q \in \mathcal{O}_L[X] \text{ tel que } x \in \mathcal{O}_K \Leftrightarrow \exists z_1, \ldots, z_m \in \mathcal{O}_L, \ Q(x, z_1, \ldots, z_m) = 0. \quad (2.0.49)$$

Donc soit $x \in \mathcal{O}_L$. On veut montrer qu'il existe un polynôme S à coefficients dans $\mathcal{O}_L$ tel que

$$x \in \mathbb{Z} \Leftrightarrow \exists v_1, \ldots, v_s \in \mathcal{O}_L \ S(x, v_1, \ldots, v_s) = 0. \quad (2.0.50)$$

Or, pour $x \in \mathcal{O}_L$ on a $x \in \mathbb{Z} \Leftrightarrow \exists z_1, \ldots, z_m, w_{11}, \ldots, w_{1m}, \ldots, w_{n1}, \ldots, w_{nm}$ et $y_1, \ldots, y_n \in \mathcal{O}_L$ tels que
$(Q(x, z_1, \ldots, z_m)^2 - aP(x, y_1, \ldots, y_n)^2)^2 - aQ(y_1, w_{11}, \ldots, w_{1m})^2)^2 - \ldots$
$- aQ(y_n, w_{n1}, \ldots, w_{nm})^2 = 0$, où $a \in \mathbb{N}$ mais $\sqrt{a} \notin \mathcal{O}_L$.
En effet, si $x \in \mathbb{Z}$ alors par 2.0.48 il existe $y_1, \ldots, y_n \in \mathcal{O}_K \subseteq \mathcal{O}_L$ tel que $P(x_{,1}, \ldots, y_n) = 0$. De plus, $\mathbb{Z} \subseteq \mathcal{O}_K$ donc par 2.0.49 il existe $z_1, \ldots, z_m \in \mathcal{O}_L$ tels que $Q(x, z_1, \ldots, z_m) = 0$ et il existe $w_{11}, \ldots, w_{1m}, \ldots, w_{n1}, \ldots, w_{nm} \in \mathcal{O}_L$ tels que $Q(y_1, w_{11}, \ldots, w_{1m}) = 0 = Q(y_n, w_{n1}, \ldots, w_{nm})$.

Inversement, si $Q(x, z_1, \ldots, z_m) = 0$, $Q(y_1, w_{11}, \ldots, w_{1m}) = 0$ et si $Q(y_n, w_{n1}, \ldots, w_{nm}) = 0$ alors $x, y_1, \ldots, y_n \in \mathcal{O}_K$. Donc la conjonction des $P(x, y_j) = 0$ avec $y_j \in \mathcal{O}_K$ entraîne que $x \in \mathbb{Z}$ par 2.0.48.

Donc il existe $S \in \mathcal{O}_L[x, y_1, \ldots, w_{11}, \ldots, w_{nm}, y_n, z_1, \ldots, z_m]$ tel que cherché en 2.0.50.

d) Remarquons d'abord que $\mathcal{O}_L = \mathcal{O}_K(\alpha_1, \ldots, \alpha_s)$. On a pour $x \in \mathcal{O}_L$ que $x \in \mathbb{Z} \Leftrightarrow \exists y \in \mathcal{O}_L$ tel que $P(x, y) = 0$ où $P \in \mathcal{O}_L[x, y]$. Ainsi, soit $x \in \mathcal{O}_K \subseteq \mathcal{O}_L$,

$$
\begin{aligned}
x \in \mathbb{Z} &\iff \exists y \in \mathcal{O}_L \text{ tel que } P(x, y) = 0 \\
&\iff \exists y_i \in \mathcal{O}_K \text{ tel que } P(x, y_1\alpha_1 + \ldots + y_s\alpha_s) = 0 \\
&\iff \exists y_i \in \mathcal{O}_K \text{ tel que } P_1(x, y_i)\alpha_1 + \ldots + P_s(x, y_i)\alpha_s = 0 \\
&\iff \exists y_i \in \mathcal{O}_K \text{ tel que } ((P_1(x, y_i)^2 + aP_2(x, y_i)^2)^2 + \ldots + aP_s(x, y_i)^2 = 0
\end{aligned}
$$

où $a \in \mathcal{O}_K$ mais $\sqrt{a} \notin \mathcal{O}_L$, P_i sont des polynômes à coefficients dans $\mathcal{O}_K$ et $i = 1, \ldots, s$. □

Lemme 2.0.13. *Soient K et L des corps algébriques tels que $K \subseteq L$, L est Galois sur K et $[L : \mathbb{Q}]$=n. Supposons $\xi \in \mathcal{O}_L$, $w \in \mathcal{O}_K$, $z \in \mathcal{O}_K$,*

$$w \equiv \xi \ mod \ (z) \tag{2.0.51}$$

et

$$2^{n+1}\xi^n(\xi + 1)^n \ldots (\xi + n - 1)^n | z. \tag{2.0.52}$$

Alors $\xi \in \mathcal{O}_K$.

Preuve:

Si $z = 0$, alors $w \equiv \xi \ mod \ (0) \Longrightarrow \exists k \in \mathcal{O}_L \ \ w - \xi = k \cdot 0 = 0 \Longrightarrow \xi = w \in \mathcal{O}_K$. Supposons donc que $z \neq 0$. Soit $j = 0, 1, \ldots, n - 1$. Par 2.0.52 , $2^{n+1}(\xi + j)^n | z$ donc $\exists s \in \mathcal{O}_L \ 2^{n+1}(\xi + j)^n s = z$

$\Longrightarrow N(2^{n+1}(\xi+j)^n s) = N(z)$ où N est $N_{L/\mathbb{Q}}$. Donc,

$$|N(2^{n+1})||N(\xi+j)^n||N(s)| = |N(z)| \tag{2.0.53}$$

$$\Longrightarrow |N(\xi+j)^n||N(s)| = \frac{|N(z)|}{|N(2^{n+1})| \neq 0}$$

$$\Longrightarrow |N(\xi+j)^n| \leq \frac{|N(z)|}{|N(2^{n+1})|} \text{ car } s \in \mathcal{O}_L \text{ donc } N(s) \in \mathbb{Z}$$

$$\Longrightarrow |N(\xi+j)^n| \leq |N(\frac{z}{2^{n+1}})|$$

$$\Longrightarrow |N(\xi+j)| \leq |N(\frac{z}{2^{n+1}})|^{\frac{1}{n}}.$$

Posons c=$|N(\frac{z}{2^{n+1}})|^{\frac{1}{n}}$. On a $c \geq 1$ car $|N(2^{n+1})| \leq |N(z)|$ par 2.0.53, puisque $N(\xi+j)^n$ est élément de $\mathbb{Z}$ étant donné que $(\xi+j)^n \in \mathcal{O}_L$. Soient $\sigma_1, \ldots, \sigma_n$ les n plongements de L vers $\mathbb{C}$. Nous avons $\prod_i |\sigma_i(\xi)+j| \leq c$ car par l'équation 2.0.52 on a $\exists w \in \mathcal{O}_L$ $(\xi+j)^n w = \frac{z}{2^{n+1}}$

$\Longrightarrow (\xi+j)w' = (\frac{z}{2^{n+1}})^{\frac{1}{n}}$

$\Longrightarrow \sigma_i[(\xi+j)w'] = \sigma_i[(\frac{z}{2^{n+1}})^{\frac{1}{n}}]$

$\Longrightarrow (\sigma_i(\xi)+j)\sigma_i(w') = (\frac{z}{2^{n+1}})^{\frac{1}{n}}$ car σ_i laissent K fixe puisque L est Galois sur K.

Donc $\sigma_i(\xi)+j \mid (\frac{z}{2^{n+1}})^{\frac{1}{n}}$ $\forall i = 1, \ldots, n$,

$\Longrightarrow \prod_{i=1}^{n}(\sigma_i(\xi)+j) \mid (\frac{z}{2^{n+1}})$

$\Longrightarrow N[\prod_{i=1}^{n}(\sigma_i(\xi)+j)] = N[\prod_{i=1}^{n}\sigma_i(\xi+j)] \leq |N(\frac{z}{2^{n+1}})|$.

Aussi $\prod_{i=1}^{n}\sigma_i(\xi+j) = N(\xi+j) \in \mathbb{Q}$

$\Longrightarrow N_{L/\mathbb{Q}}[\prod_{i=1}^{n}(\sigma_i(\xi+j))] = [\prod_{i=1}^{n}(\sigma_i(\xi+j))]^n$

$\Longrightarrow[\prod_{i=1}^{n}(\sigma_i(\xi+j))]^n \leq |N(\frac{z}{2^{n+1}})|$

$\Longrightarrow \prod_{i=1}^{n}(\sigma_i(\xi)+j) \leq |N(\frac{z}{2^{n+1}})|^{\frac{1}{n}}$ =c.

De plus, si $a_1,\ldots,a_n \in \mathbb{C}$, $c \in I\!R, c \geq 1$ et si $\prod_i |a_i+j| \leq c \ \forall j=0,\ldots,n-1$, alors $|a_i| < 2^n c \ \forall i=1,\ldots,n$.

En effet, nous pouvons distinguer deux cas:

a) $\exists j \ \forall i |a_i+j| \geq \frac{1}{2}$

Supposons $\exists k \in \{1,\ldots,n\}$ tel que $|a_k| \geq 2^n c$ alors

$\prod_i |a_i+j| = (\prod_{i\neq k}|a_i+j|)|a_k+j| \geq 2^n c \prod_{i\neq k}|a_i+j| \geq 2^n c \prod_{i\neq k}\frac{1}{2} = 2^n c \frac{1}{2^{n-1}} = 2c$

donc $2c \leq \prod_i |a_i+j| \leq c$

$\Longrightarrow 2 \leq 1$ car $c \geq 1$. Contradiction.

b)$\forall j \ \exists i \ |a_i+j| < \frac{1}{2} \Longrightarrow \forall i \ \exists j \ |a_i+j| < \frac{1}{2}$

car si $\forall j \ \exists i \ |a_i+j| = d(a_i,-j) < \frac{1}{2}$ alors $\nexists i_0 \ |a_{i_0}+j| < \frac{1}{2}$ et $|a_{i_0}+j'| < \frac{1}{2}$ avec $j \neq j'$ car sinon $d(-j,-j') = d(-j,a_{i_0}) + d(a_{i_0},-j') < \frac{1}{2}+\frac{1}{2} = 1$.

Contradicton car $d(-j,-j') = 1$. Donc, $\forall j \ \exists!\ i \ |a_i+j| < \frac{1}{2} \Longrightarrow \forall i \ \exists j \ |a_i+j| < \frac{1}{2}$ (car la cardinalité de l'ensemble $\{1,\ldots,n\}$ égale celle de $\{0,\ldots,n-1\}$).

Ainsi, si Re $a_i \geq 0$ alors $\exists j \ |a_i| \leq |a_i+j| < \frac{1}{2} < 2^n c$.

Sinon, Re $a_i < 0$ entraîne $\exists j \ |a_i| - |j| \leq |a_i+j| < \frac{1}{2}$

$\Longrightarrow |a_i| < \frac{1}{2} + j \leq \frac{1}{2} + n - 1 = \frac{2n-1}{2} < 2^n \leq 2^n c$.

En applicant ceci avec $a_i = \sigma_i(\xi)$ on trouve:

$$\begin{aligned} \forall i = 1,\ldots,n, |\sigma_i(\xi)| &< 2^n c \\ &= 2^n \Big(\frac{|N(z)|}{|N(2^{n+1})|}\Big)^{\frac{1}{n}} \\ &= 2^n \frac{|N(z)|^{\frac{1}{n}}}{((2^{n+1})^n)^{\frac{1}{n}}} \\ &= \frac{1}{2}|N(z)|^{\frac{1}{n}}. \end{aligned} \tag{2.0.54}$$

Soit τ un élément du groupe de Galois de L sur K. On tire de 2.0.51 que $\exists k \in \mathcal{O}_L,\ w-\xi = kz \in \mathcal{O}_L \Rightarrow \tau(w)-\tau(\xi) = \tau(w-\xi) = \tau(kz) \Rightarrow \tau(w)-\tau(\xi) = \tau(k)\tau(z) \Rightarrow \tau(w) \equiv \tau(\xi)\ mod\ \tau(z)$. Donc $w \equiv \tau(\xi)\ mod\ z$ car τ laisse K fixe, et puisque $w \equiv \xi\ mod\ z$ on a:

$$\xi \equiv \tau(\xi)\ mod\ z. \tag{2.0.55}$$

Par 2.0.54 et le fait que $\sigma_i\tau$ est un homomorphisme injectif de L vers $\mathbb{C}$ qui préserve K, on a $|\sigma_i\tau(\xi)| < \frac{1}{2}|N(z)|^{\frac{1}{n}}$. De plus,

$$\begin{aligned}|\sigma_i(\xi-\tau(\xi))| = |\sigma_i(\xi)-\sigma_i\tau(\xi))| &< |\sigma_i(\xi)| + |\sigma_i\tau(\xi)| \\ &< \frac{1}{2}|N(z)|^{\frac{1}{n}} + \frac{1}{2}|N(z)|^{\frac{1}{n}} = |N(z)|^{\frac{1}{n}}\end{aligned}$$

et donc

$$|N(\xi-\tau(\xi))| = \prod_{i=1}^{n}|\sigma_i(\xi-\tau(\xi))| < \prod_{i=1}^{n}|N(z)|^{\frac{1}{n}} = |N(z)|.$$

De cette dernière inégalité et 2.0.55, on conclue que $\xi = \tau(\xi)$ car sinon $\xi-\tau(\xi) = \gamma z \Rightarrow |N(\xi-\tau(\xi))| = |N(\gamma)||N(z)| \Rightarrow |N(z)| \leq |N(\xi-\tau(\xi))|$ car $\gamma \in \mathcal{O}_L \Rightarrow |N(\gamma)| \in \mathbb{Z}$. Ceci est une contradiction .

Étant donné que $\xi = \tau(\xi)\ \forall\tau \in Gal(L/K)$, on a $\xi \in \mathcal{O}_L \cap K = \mathcal{O}_K$. □

Lemme 2.0.14. *Soit L un corps algébrique, ε une unité dans $\mathcal{O}_L$ et $t \in \mathcal{O}_L$, $t \neq 0$. Alors $\exists m \in \mathbb{N}\backslash\{0\}$ tel que $t|\varepsilon^m - \varepsilon^{-m}$.*

Preuve:

Soit m l'ordre de groupe des unités de l'anneau fini $\mathcal{O}_L/(t)$, où (t) est l'idéal engendré par t. Alors $\varepsilon^m \equiv 1\ mod\ (t)$ et $\varepsilon^{-m} \equiv 1\ mod\ (t)$. Ceci entraîne que $t|\varepsilon^m - 1$ et $t|\varepsilon^{-m} - 1$ donc $t|[(\varepsilon^m-1)-(\varepsilon^{-m}-1)]$. □

Lemme 2.0.15. *Soit L un corps algébrique, ε une unité dans $\mathcal{O}_L$ et k un nombre naturel impair. Alors $\frac{\varepsilon^k-\varepsilon^{-k}}{\varepsilon-\varepsilon^{-1}} \equiv k\ mod\ (\varepsilon-\varepsilon^{-1})$.*

Preuve:

On a $\frac{\varepsilon^k-\varepsilon^{-k}}{\varepsilon-\varepsilon^{-1}} = \varepsilon^{k-1} + \varepsilon^{k-2}\varepsilon^{-1} + \ldots + (\varepsilon^{-1})^{k-1}$ car si on pose

$S = \varepsilon^{k-1} + \varepsilon^{k-3} + \varepsilon^{k-5} + \ldots + \varepsilon^{-k+1}$ alors $S\varepsilon = \varepsilon^{k} + \varepsilon^{k-2} + \ldots + \varepsilon^{-k+2}$
et $S\varepsilon^{-1} = \varepsilon^{k-2} + \varepsilon^{k-4} + \ldots + \varepsilon^{-k}$ ce qui donne $S(\varepsilon - \varepsilon^{-1}) = \varepsilon^{k} - \varepsilon^{-k}$.

De plus, $\varepsilon \equiv \varepsilon^{-1}\ mod\ (\varepsilon - \varepsilon^{-1})$. Ainsi, $\varepsilon^2 \equiv \varepsilon^{-2} \equiv \varepsilon\varepsilon^{-1} = 1\ mod\ (\varepsilon - \varepsilon^{-1})$ et donc $\frac{\varepsilon^k - \varepsilon^{-k}}{\varepsilon - \varepsilon^{-1}} \equiv \varepsilon^{k-1} + \varepsilon^{k-1} + \ldots + \varepsilon^{k-1} \equiv k\varepsilon^{k-1}\ mod\ (\varepsilon - \varepsilon^{-1})$. Puisque k est impair, k-1 est pair alors $\frac{\varepsilon^k - \varepsilon^{-k}}{\varepsilon - \varepsilon^{-1}} \equiv k\varepsilon^{2s} \equiv k(\varepsilon^2)^s \equiv k\ mod\ (\varepsilon - \varepsilon^{-1})$. □

Lemme 2.0.16 (Lemme principal). *Soient K et L des corps algébriques tels que $K \subseteq L$ et L est Galois sur K. Soit $d \in \mathcal{O}_L, d \neq 0$, et supposons que*

$$x^2 - dy^2 = 1 \tag{2.0.56}$$

possède une infinité de solutions dans $\mathcal{O}_L$. Supposons aussi qu'il existe $e \in \mathbb{N}\backslash\{0\}$ tel que

$$\frac{(x + y\sqrt{d})^e - (x - y\sqrt{d})^e}{2\sqrt{d}} \in K \tag{2.0.57}$$

$\forall x, y \in \mathcal{O}_L$ satisfaisant 2.0.56. Alors $\mathcal{O}_K$ est diophantien dans $\mathcal{O}_L$.

Preuve:

Posons n=[L:$\mathbb{Q}$] et considérons le sous-ensemble S de $\mathcal{O}_L$ défini par:
$\xi \in S \Longleftrightarrow \xi \in \mathcal{O}_L \wedge \exists x, y, u, v, w, z \in \mathcal{O}_L$:

$$x^2 - dy^2 = 1 \tag{2.0.58}$$

$$u^2 - dv^2 = 1 \tag{2.0.59}$$

$$z = \frac{(x + y\sqrt{d})^e - (x - y\sqrt{d})^e}{2\sqrt{d}} \tag{2.0.60}$$

$$z \neq 0 \tag{2.0.61}$$

$$zw = \frac{(u + v\sqrt{d})^e - (u - v\sqrt{d})^e}{2\sqrt{d}} \tag{2.0.62}$$

$$w \equiv (2\xi + 1) \; mod \; z \tag{2.0.63}$$

$$2^{n+1}(2\xi + 1)^n \ldots (2\xi + n)^n | z. \tag{2.0.64}$$

S est diophantien dans $\mathcal{O}_L$ car $\mathcal{O}_L$ l'est sur lui-même, la conjonction de relations diophantiennes est diophantienne (par la proposition 2.0.1), on peut remplacer 2.0.60 et 2.0.62 par des équations ne contenant pas $\sqrt{d}$, $z \neq 0$ est une relation diophantiennne par la proposition 2.0.1 , 2.0.63 peut être remplacée par $\exists k \in \mathcal{O}_L \; w-(2\xi+1) = kz$ et 2.0.64 par $\exists q \in \mathcal{O}_L \; 2^{n+1}(2\xi + 1)^n \ldots (2\xi + n)^n q = z$. Nous allons prouver en a) et b) que $\mathbb{N} \subseteq S \subseteq \mathcal{O}_K$. Ceci entraîne que $\mathcal{O}_K$ est diophantien dans $\mathcal{O}_L$. En effet, soit $\mathcal{O}_K = \mathbb{Z}(\alpha_1, \ldots, \alpha_s)$. On pose, $T(\xi, x, y, u, v, w, z)$ comme étant le polynôme définissant S dans $\mathcal{O}_L$, i.e. la conjonction des conditions 2.0.58 à 2.0.64 et aussi $\xi \in \mathcal{O}_L$.

Soit $\xi \in \mathcal{O}_L$, alors on a la définition suivante de $\mathcal{O}_K$ dans $\mathcal{O}_L$:

$\xi \in \mathcal{O}_K \Longleftrightarrow \forall i = 1, \ldots, s \; \exists a_i \in \mathcal{O}_L$ et $\exists x, y, u, v, w, z \in \mathcal{O}_L$

$\xi = a_1\alpha_1 + a_2\alpha_2 + \ldots + a_s\alpha_s \; (\alpha_i \in \mathcal{O}_K \subseteq \mathcal{O}_L)$ et

$[T(-a_i, x, y, u, v, w, z) \; \vee \; T(a_i, x, y, u, v, w, z)]$

Démonstration:

$(\Longleftarrow)$ $\xi \in \mathcal{O}_L$. $\exists a_i \in \mathcal{O}_L$ tels que $\xi = \sum_{i=1}^{s} a_i\alpha_i$ et $T(\pm a_i) \; \forall i = 1, \ldots, s$

$\Rightarrow \pm a_i \in S \subseteq \mathcal{O}_K$ et $\alpha_i \in \mathcal{O}_K \; \Rightarrow \; \xi = \sum_{i=1}^{s} a_i\alpha_i \in \mathcal{O}_K$.

$(\Longrightarrow)$ $\xi \in \mathcal{O}_K \; \Rightarrow \; \xi = \sum_{i=1}^{s} a_i\alpha_i$ avec $a_i \in \mathbb{Z} \subseteq \mathcal{O}_L$. Puisque $\mathbb{N} \subseteq S \subseteq \mathcal{O}_K$, $\pm a_i \in \mathbb{N} \subseteq S \; \forall i = 1, \ldots, s \; \Rightarrow \; T(\pm a_i) \; \forall i$.

Voici donc l'étape majeure et finale de la preuve:

a) Soit $\xi \in S$ alors $\exists x, y, u, v, w, z \in \mathcal{O}_L$ satisfaisant 2.0.58 à 2.0.64. De plus, de 2.0.57, 2.0.58 et 2.0.60 on tire que $z \in \mathcal{O}_L \cap K = \mathcal{O}_K$. De même, 2.0.57, 2.0.59 et 2.0.62 impliquent $zw \in \mathcal{O}_K = \mathcal{O}_L \cap K$. Puisque $z \neq 0$ par 2.0.61, on a qu'il existe $z^{-1} \in K$ donc $zw \in K \Rightarrow z^{-1}zw = w \in K$. On avait $w \in \mathcal{O}_L$ donc $w \in \mathcal{O}_K$. Par 2.0.63, 2.0.64 et le lemme 2.0.13, on conclut que

$2\xi+1 \in \mathcal{O}_K \Rightarrow 2\xi+1 \in K \Rightarrow \xi \in K$. Donc $\xi \in K \cap \mathcal{O}_L = \mathcal{O}_K$. Ainsi on a montré que $S \subseteq \mathcal{O}_K$.

b) Soit $\xi \in I\!N \subseteq \mathcal{O}_L$. Choisissons x_0 et y_0 dans $\mathcal{O}_L$ satisfaisant 2.0.56 et tels que $x_0 + y_0\sqrt{d}$ ne soit pas une racine de l'unité. Ceci est possible car le nombre de racines de l'unité est fini et par hypothèse 2.0.56 a une infinité de solutions dans $\mathcal{O}_L$. Posons $\varepsilon = x_0 + y_0\sqrt{d}$. On remarque que ε est une unité dans $\mathcal{O}_{L'}$ où $L' = L(\sqrt{d})$ avec $\varepsilon^{-1} = x_0 - y_0\sqrt{d}$ puisque $N_{L'/L}(\varepsilon) = (x_0+y_0\sqrt{d})(x_0-y_0\sqrt{d}) = 1$. Par le lemme 2.0.14, il existe $m \in I\!N\backslash\{0\}$ tel que

$$2^{n+1}(2\xi+1)^n \ldots (2\xi+n)^n 2\sqrt{d} | \varepsilon^m - \varepsilon^{-m} \tag{2.0.65}$$

car $\xi \in I\!N \subseteq \mathcal{O}_L \Longrightarrow 2^{n+1}(2\xi+1)^n \ldots (2\xi+n)^n 2\sqrt{d} \in \mathcal{O}_{L'}$ et
$2^{n+1}(2\xi+1)^n \ldots (2\xi+n)^n | z$ et $z \neq 0$ donc $2^{n+1}(2\xi+1)^n \ldots (2\xi+n)^n 2\sqrt{d} \neq 0$.
Soit (x,y) la seule solution de $x + y\sqrt{d} = \varepsilon^m, x - y\sqrt{d} = \varepsilon^{-m}$. Montrons ceci par induction sur m:
Pour m=1 on a: $\varepsilon^1 = x_0 + y_0\sqrt{d}$ et $\varepsilon^{-1} = x_0 - y_0\sqrt{d}$.
Supposons vrai pour m-1, c'est-à-dire $\varepsilon^{m-1} = a + b\sqrt{d} \Longrightarrow \varepsilon^{-(m-1)} = a - b\sqrt{d}$.
Alors $\varepsilon^m = \varepsilon^{m-1}\varepsilon = (a + b\sqrt{d})(x_0 + y_0\sqrt{d}) = (ax_0 + dby_0) + (ay_0 + bx_0)\sqrt{d}$ et
$\varepsilon^{-m} = \varepsilon^{-(m-1)}\varepsilon^{-1} = (a - b\sqrt{d})(x_0 - y_0\sqrt{d}) = (ax_0 + dby_0) - (ay + bx_0)\sqrt{d}$.
Sachant que x_0, y_0 et d sont éléments de $\mathcal{O}_L$ nous utilisons la démonstration précédente pour établir que x, y sont aussi éléments de $\mathcal{O}_L$. Lorsque $m = 1$, on a $x = x_0$ et $y = y_0$. L'hypothèse d'induction étant que $a, b \in \mathcal{O}_L$, on obtient le résultat pour $ax_0 + dby_0$ et $ay_0 + bx_0$. Donc, $x^2 - dy^2 = \varepsilon^{-m}\varepsilon^{-m} = 1$ et 2.0.58 est satisfaite.

Posons $z = \dfrac{\varepsilon^{me} - \varepsilon^{-me}}{2\sqrt{d}}$. En applicant la formule du binôme de Newton, on constate que $2\sqrt{d}|\varepsilon^{me} - \varepsilon^{-me} = (x + y\sqrt{d})^e - (x - y\sqrt{d})^e$ donc $z \in \mathcal{O}_{L'}$. Si $\sqrt{d} \in L$ alors $L' = L$ donc $z \in \mathcal{O}_L$. Sinon l'automorphisme $\tau : L' \to L'$ tel que $\tau(\sqrt{d}) = -\sqrt{d}$ laisse z fixe ce qui entraîne que $z \in L \cap \mathcal{O}_{L'} = \mathcal{O}_L$ et donc z satisfait 2.0.60. En outre, 2.0.61 est satisfait puisque $z = 0 \Longleftrightarrow \varepsilon^{me} = \varepsilon^{-me} \Longleftrightarrow \varepsilon^{2me} = 1 \Longleftrightarrow \varepsilon$ est une racine de l'unité. Or ce n'est pas le cas. On a aussi 2.0.65 implique 2.0.64.

Soient $u, v \in \mathcal{O}_L$ donnés par $u + v\sqrt{d} = \varepsilon^{m(2\xi+1)}, u - v\sqrt{d} = \varepsilon^{-m(2\xi+1)}$ alors 2.0.59 est satisfaite. Posons $w = \dfrac{\varepsilon^{me(2\xi+1)} - \varepsilon^{-me(2\xi+1)}}{\varepsilon^{me} - \varepsilon^{-me}}$ pour obtenir 2.0.62. Le lemme 2.0.15 implique 2.0.63 puisque ε^{me} est une unité de $\mathcal{O}_{L'}$ et $2\xi+1$ un nombre naturel impair, puis on a $w = \dfrac{\varepsilon^{me(2\xi+1)} - \varepsilon^{-me(2\xi+1)}}{\varepsilon^{me} - \varepsilon^{-me}} \equiv 2\xi + 1 \ mod\ (\varepsilon^{me} - \varepsilon^{-me})$,

$\Longrightarrow \exists k \in \mathcal{O}_{L'}\ w - (2\xi + 1) = k(\varepsilon^{me} - \varepsilon^{-me}) = k2\sqrt{d}z$

$\Longrightarrow w \equiv (2\xi + 1)\ mod\ z$. Comme $\tau(w) = w$ on a que w est élément de L et par ce qui précède, $\exists s\ \in \mathcal{O}_{L'}$, tel que $w = sz + (2\xi + 1)$. Donc $w \in L \cap \mathcal{O}_{L'} = \mathcal{O}_L$. D'où $\xi \in S$. Donc $\mathbb{N} \subseteq S$ ce qui complète la preuve du lemme principal.

Soit L un corps algébrique. Le groupe des unités de $\mathcal{O}_L$ sera noté $\mathcal{U}_L$. Ce groupe est engendré par un ensemble fini et on note le nombre de ses générateurs par $rk\ \mathcal{U}_L$.

Lemme 2.0.17. *Soit L un corps algébrique, $d \in \mathcal{O}_L$, $L' = L(\sqrt{d})$ et supposons que $L' \neq L$. On pose $V_L = \{x + y\sqrt{d} : x, y \in \mathcal{O}_L \wedge x^2 - dy^2 = 1\}$. Alors $V_L < \mathcal{U}_{L'}$ (sous-groupe) et $rk\ V_L = rk\ \mathcal{U}_{L'} - rk\ \mathcal{U}_L$.*

Preuve:

Nous montrons d'abord que V_L est un sous-groupe de $\mathcal{U}_{L'}$. Puisque $d \in \mathcal{O}_L$ on a

$\exists a_0, \ldots, a_{n-1} \in \mathbb{Z},\ d^n + a_{n-1}d^{n-1} + \ldots + a_1 d + a_0 = 0$

$\Longrightarrow (\sqrt{d})^{2n} + a_{n-1}(\sqrt{d})^{2(n-1)} + \ldots + a_1(\sqrt{d})^2 + a_0 = 0$

$\Longrightarrow \sqrt{d} \in \mathcal{O}$ car il est racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$

$\Longrightarrow \sqrt{d} \in \mathcal{O} \cap L' = \mathcal{O}_{L'}$ donc $x + y\sqrt{d} \in \mathcal{O}_{L'}$ car $x, y \in \mathcal{O}_L$.

De plus, $1 = x^2 - dy^2 = (x+y\sqrt{d})(x-y\sqrt{d}) = N_{L'/L}(x+y\sqrt{d})$ et $N_{L'/\mathbb{Q}}(x+y\sqrt{d}) = N_{L/\mathbb{Q}}(N_{L'/L}(x + y\sqrt{d})) = N_{L/\mathbb{Q}}(1) = 1^l = 1$ où $l = [L : \mathbb{Q}]$. Donc on a bien $V_L \subseteq \mathcal{U}_{L'}$. Reste à montrer que V_L est un sous-groupe. Soient $x_0 + y_0\sqrt{d} \in V_L$ et $x_1 + y_1\sqrt{d} \in V_L$ alors $(x_0 + y_0\sqrt{d})(x_1 + y_1\sqrt{d}) = x_0x_1 + dy_0y_1 + (x_0y_1 + y_0x_1)\sqrt{d}$ alors $x_0x_1 + dy_0y_1$ et $x_0y_1 + y_0x_1$ sont éléments de $\mathcal{O}_L$ car d, x_0, x_1, y_0, y_1 le sont et $(x_0x_1 + dy_0y_1)^2 - d(x_0y_1 + y_0x_1)^2 = 1$. Nous montrons finallement que $V_L \neq \emptyset$. En effet, $x = 1$ et $y = 0$ sont éléments de $\mathcal{O}_L$ et $1 + 0\sqrt{d} \in V_L$ car $1^2 - d \cdot 0^2 = 1$.

Deuxièmement il faut montrer que $rk\ V_L = rk\ \mathcal{U}_{L'} - rk\ \mathcal{U}_L$.

$$\text{Considérons } \varphi : \mathcal{U}_{L'} \to \mathcal{U}_L$$
$$x \mapsto N_{L'/L}(x)$$

Nous montrons que φ est un homomorphisme:

i. φ est bien défini car soit $x \in \mathcal{U}_{L'}$ alors $\varphi(x) = N_{L'/L}(x)$ et donc on a $N_{L/\mathbb{Q}}(\varphi(x)) = N_{L/\mathbb{Q}}(N_{L'/L}(x)) = N_{L'/\mathbb{Q}}(x) = \pm 1$ par définition de $x \in \mathcal{U}_{L'}$. Ainsi si $\varphi(x) \in \mathcal{O}_L$ on aura $\varphi(x) \in \mathcal{U}_L$. Mais justement, $\varphi(x) = N_{L'/L}(x)$ qui est élément de $\mathcal{O} \cap L = \mathcal{O}_L$ parce que $x \in \mathcal{O}_{L'}$.

ii. $\varphi(xy) = N(xy) = N(x)N(y) = \varphi(x)\varphi(y)$.

On note respectivement le noyau et l'image de φ par ker et Im. On remarque que V_L est un sous-groupe de ker car si $x+y\sqrt{d} \in V_L$, on a $\varphi(x+y\sqrt{d}) = x^2 - dy^2 = 1$ et 1 est l'élément neutre de $(\mathcal{U}_L, \cdot)$. Donc $V_L \subseteq$ ker et on a déjà montré que V_L est un groupe. Il serait possible qu'il existe $\varepsilon \in$ker tel que $\varepsilon = x + y\sqrt{d}$, $x, y \in L$ mais $x, y \notin \mathcal{O}_L$. Par contre, si $\varepsilon \in$ ker $\subseteq \mathcal{U}_{L'}$ et comme $0 \neq 2\sqrt{d} \in \mathcal{O}_{L'}$ par le lemme 2.0.14 on trouve:

$$\exists m \in \mathbb{N}\ 2\sqrt{d} | \varepsilon^m - \varepsilon^{-m} \text{ dans } \mathcal{O}_{L'}. \tag{2.0.66}$$

Posons $\varepsilon^m = x + y\sqrt{d}, x, y \in L$. Alors $(\varepsilon^m)^{-1} = \varepsilon^{-m} = x - y\sqrt{d}$ car $x^2 - dy^2 = (x+y\sqrt{d})(x-y\sqrt{d}) = 1 \Rightarrow (x+y\sqrt{d})^{-1} = x - y\sqrt{d}$. D'où $2y\sqrt{d} = \varepsilon^m - \varepsilon^{-m}$. Par 2.0.66, $y \in \mathcal{O}_{L'} \cap L = \mathcal{O}_L$ et $x = \varepsilon^m - y\sqrt{d} \in \mathcal{O}_{L'} \cap L = \mathcal{O}_L$. Donc V_L est d'indice fini dans ker c'est-à-dire, [ker:V_L] $= k_1$ fini et de même [Im:$\mathcal{U}_L$] $= k_2$ fini. Ainsi, $\exists a_1, \ldots, a_{k_1-1} \in$ ker tel que ker$=V_L + a_1V_L + \ldots + a_{k_1-1}V_L$ et $\exists b_1, \ldots, b_{k_2-1} \in$ Im tel que Im$=\mathcal{U}_L + b_1\mathcal{U}_L + \ldots + b_{k_2-1}\mathcal{U}_L$. D'où le nombre de générateurs de ker est le même que celui de V_L puisque ceux-ci (les générateurs de V_L) engendrent V_L et a_iV_L, donc $V_L + a_1V_L + \ldots + a_{K_1-1}V_L$=ker. On obtient ainsi aussi le résultat pour Im. En conclusion par ce qui précède et le fait que $rk\ \mathcal{U}_{L'} = rk\ ker + rk\ Im$ on trouve que, $rk\ V_L = rk\ ker = rk\ \mathcal{U}_{L'} - rk\ Im = rk\ \mathcal{U}_{L'} - rk\ \mathcal{U}_L$.

Grâce à ces lemmes et la proposition 2.0.1, nous pouvons maintenant obtenir le résultat principal.

Preuve du théorème:

Pour chacun des cas a),b) et c), nous devons trouver une équation $x^2-dy^2=1$ satisfaisant les hypothèses du lemme principal. D'abord, nous allons expliquer un fait largement utilisé dans ce qui suit. Soit $U=\mathbb{Q}(\theta)$ un corps algébrique de degré n sur $\mathbb{Q}$. U possède exactement n isomorphismes distincts de U dans $\mathbb{C}$. En effet, $[U:\mathbb{Q}]$=n signifie qu'il existe un polynôme irréductible sur $\mathbb{Q}$ noté $p_{\theta/\mathbb{Q}}(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ tel que $a_i\in\mathbb{Q}, i=0,\ldots,n-1$ et $p_{\theta/\mathbb{Q}}(\theta)=0$. Soient $\theta_1,\ldots,\theta_n$ les n racines complexes de ce polynôme. Alors les n isomorphismes sont:

$$U=\mathbb{Q}(\theta)\to\mathbb{C}$$
$$\sigma_j(\sum_{i=0}^{n-1}b_i\theta^i)\mapsto\sum_{i=0}^{n-1}b_i(\theta_j)^i \text{ où } j=1,\ldots,n,\ b_i\in\mathbb{Q}.$$

cas c):

Soient $\sigma_1,\ldots,\sigma_h$ les plongements de K dans $\mathbb{R}$ qui ne se prolongent pas en plongements de L dans $\mathbb{R}$, et $\sigma_{h+1},\ldots,\sigma_k$ ceux qui se prolongent à L. Nous montrons que h ≥ 1. Comme $[L:K]=2$ et $[K:\mathbb{Q}]=k$ alors $[L:\mathbb{Q}]=2k$ donc L possède $2k$ isomorphismes distincts de L dans $\mathbb{C}$. Posons L=K($\sqrt{m}$), $m\in\mathbb{Z}$ sans facteur carré. Or, pour $x\in L$, on a $x=k_1+k_2\sqrt{m}$, $k_1,k_2\in K$ car L est de degré 2 sur K. On peut donc prolonger ainsi les isomorphismes de K:

$$x\mapsto\begin{cases}\sigma_1(k_1)+\sigma_1(k_2)\sqrt{m}\mapsto\begin{cases}\sigma_1(k_1)+\sigma_1(k_2)\sqrt{m}\\ \sigma_1(k_1)-\sigma_1(k_2)\sqrt{m}\end{cases}\\ \vdots\\ \sigma_k(k_1)+\sigma_k(k_2)\sqrt{m}\mapsto\begin{cases}\sigma_k(k_1)+\sigma_k(k_2)\sqrt{m}\\ \sigma_k(k_1)-\sigma_k(k_2)\sqrt{m}.\end{cases}\end{cases}$$

Si h égalait zéro, on aurait que les k plongements de K se prolongent en plongements réels de L , donc $\sigma_i(k_1) + \sigma_i(k_2)\sqrt{m} \in \mathbb{R}(\sqrt{m}) \subseteq \mathbb{R}\ \forall i = 1, \ldots, k$. Dans ce cas, on a alors que les $2k$ isomorphismes distincts de L dans $\mathbb{C}$ sont aussi réels car leur image est incluse dans $\mathbb{R}(\sqrt{m}) \subseteq \mathbb{R}$. On obtient une contradiction car L n'est pas totallement réel.

On choisit $d \in \mathcal{O}_k$ tel que $\sqrt{d} \notin L$ et

$$\sigma_i(d) > 0\ \forall i = 1, \ldots, h$$

$$\sigma_i(d) < 0\ \forall i = h+1, \ldots, k.$$

Ceci est possible étant donné que $\{(\sigma_1(d), \ldots, \sigma_k(d)) \in \mathbb{R}^k : d \in \mathcal{O}_k\}$ est un treillis complet dans $\mathbb{R}^k$. Nous expliquons ici les grandes lignes de la méthode utilisée pour représenter les nombres algébriques d'un corps algébrique K de degré k comme des points dans l'espace à k dimensions, formant dans notre cas un treillis complet. Cette méthode est analogue à la représentation planaire des nombres complexes. Pour tout isomorphisme complexe de K, on définit $\overline{\sigma}$ tel que $\overline{\sigma}(x) = \overline{\sigma(x)}$, où $\bar{}$ dénote le conjugué complexe. On dit que σ et $\overline{\sigma}$ sont des isomorphismes complexes conjugués. Ainsi, l'ensemble des isomorphismes complexes de K est de cardinalité paire et K a $n_K = s + 2t = k$ comme nombre d'isomorphismes. De chaque paire d'isomorphismes complexes, on en choisit un, ce qui donne $\{\sigma_{s+1}, \ldots, \sigma_{s+t}\}$. On exprimera d'ailleurs dorénavant $\{\sigma_1, \ldots, \sigma_k\} = \{\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \overline{\sigma_{s+1}} \ldots, \sigma_{s+t}, \overline{\sigma_{s+t}}\}$.

On notera $\mathcal{L}^{s,t} = \{(x_1, \ldots, x_s; x_{s+1}, \ldots, x_{s+t})\}$ l'anneau commutatif avec $+, \cdot$ et la multiplication scalaire définies composantes par composantes. Une base de $\mathcal{L}^{s,t}$ sur $\mathbb{R}$ est:

$$\left.\begin{array}{l} (1, \ldots, 0; 0, \ldots, 0) \\ \ldots \\ (0, \ldots, 1; 0, \ldots, 0) \end{array}\right\} s$$

$$\left.\begin{array}{l}(0,\ldots,0;1,\ldots,0)\\(0,\ldots,0;i,\ldots,0)\\\ldots\\(0,\ldots,0;0,\ldots,1)\\(0,\ldots,0;0,\ldots,i).\end{array}\right\} 2t$$

On définit pour $x = (x_1, \ldots, x_{s+t}) \in \mathcal{L}^{s,t}$ la norme de x par la formule suivante, $N(x) = x_1 \cdot \ldots \cdot x_s \cdot |x_{s+1}|^2 \cdot \ldots \cdot |x_{s+t}|^2$, qui est le déterminant de la matrice de la transformation linéaire $x' \mapsto xx'$ avec $x' \in \mathcal{L}^{s,t}$. Pour chaque $\alpha \in K$, on pose $x(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha); \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha)) \in \mathcal{L}^{s,t}$. On voit que cette construction est telle que :

$$\alpha \neq \beta \Longrightarrow x(\alpha) \neq x(\beta)$$

$$x(\alpha + \beta) = x(\alpha) + x(\beta)$$

$$x(\alpha\beta) = x(\alpha)x(\beta)$$

$$x(a\alpha) = ax(\alpha)$$

$$N(x(\alpha)) = N(\alpha).$$

En outre, si $\alpha_1, \ldots, \alpha_k$ est une base de $K/\mathbb{Q}$ alors $x(\alpha_1), \ldots, x(\alpha_k)$ sont linéairement indépendants sur $\mathbb{R}$. Soit M un module dans K tel que M contient k éléments linéairement indépendants sur $\mathbb{Q}$. Soit $\alpha_1, \ldots, \alpha_k$ une base de M. On obtient des propriétés précédentes que si $\alpha = a_1\alpha_1 + \ldots + a_k\alpha_k \in$ M $(a_i \in \mathbb{Z})$, alors $x(\alpha) = a_1x(\alpha_1) + \ldots + a_kx(\alpha_k)$. Ainsi les éléments de M sont représentés par l'ensemble de toutes les combinaisons linéaires entières $(a_i \in \mathbb{Z})$ des k vecteurs $x(\alpha_1), \ldots, x(\alpha_k)$ linéairement indépendants sur $\mathcal{L}^{s,t}$. Pour plus de renseignements sur ce sujet, voir **[2]**.

Posons $K' = K(\sqrt{d})$ et $L' = L(\sqrt{d})$. Le théorème de Dirichlet-Minkowski sur les unités stipule que si le nombre d'isomorphismes de V dans $\mathbb{C}$ est $n_v = s + 2t$ pour un corps algébrique V, alors $r = rk\ \mathcal{U}_V = s + t - 1$ où s est le nombre d'isomorphismes réels et 2t celui d'isomorphismes complexes. On utilise ce théorème

pour montrer que:

$rk\ \mathcal{U}_K = k-1$ car K est totallement réel,

$rk\ \mathcal{U}_L = 2k-h-1$ car $n_L = 2k = 2(k-h)+2h$ avec $s = 2(k-h)$ et $2t = 2h$,

$rk\ \mathcal{U}_{K'} = h+k-1$ car $n_{K'} = 2k = 2h+2(k-h)$ avec $s = 2h$ et $2t = 2(k-h)$,

$rk\ \mathcal{U}_{L'} = 0+2k-1$ car $n_{L'} = 4k = 0+2(2k)$ avec $s = 0$ et $2t = 2(2k)$.

$$\text{On pose } V_K = \{x+y\sqrt{d} : x,y \in \mathcal{O}_K \text{ satisfont } 2.0.56\}$$

$$V_L = \{x+y\sqrt{d} : x,y \in \mathcal{O}_L \text{ satisfont } 2.0.56\}.$$

Par le lemme 2.0.17 on trouve:

$$\begin{aligned} rk\ V_K &= rk\ \mathcal{U}_{K'} - rk\ \mathcal{U}_K \\ &= k+h-1-(k-1) \\ &= h \end{aligned}$$

$$\begin{aligned} \text{et } rk\ V_L &= rk\ \mathcal{U}_{L'} - rk\ \mathcal{U}_L \\ &= 2k-1-(2k-h-1) \\ &= h. \end{aligned}$$

Puisque $h \geq 1$, 2.0.56 a une infinité de solutions. On a $V_K \leq V_L$ (sous-module) et V_K et V_L ont le même nombre de générateurs donc V_K est d'indice fini dans V_L par le rappel suivant: soient M un module libre de rang n avec base $\{u_1,\ldots,u_n\}$ et $(0) \neq N \leq M$ (sous-module). Il existe $m \leq n$ et $c_1,\ldots,c_m \in \mathbb{N}$ tels qu'une base de N soit $\{c_1u_1,\ldots,c_mu_m\}$. Ceci entraîne lorsque le rang de M égal le rang de N que m=n et donc $c_1u_1,\ldots,c_nu_n$ sont indépendants, i.e. $c_i \neq 0, i = 1,\ldots,n$. Alors $[M:N] = c_1 \times \ldots \times c_n < \infty$.

Posons e=$[V_L : V_K]$. Alors pour tout $x,y, \in \mathcal{O}_L$ satisfaisant 2.0.56 on a que $(x+y\sqrt{d})^e$ est élément de $V_K \subseteq K'$ et donc le membre de gauche de l'équation 2.0.57 du lemme principal est un élément de K' (un corps). Aussi comme $\sqrt{d}$

n'est pas dans K et que

$$\frac{(x+y\sqrt{d})^e-(x-y\sqrt{d})^e}{2\sqrt{d}} \tag{2.0.67}$$

est invariant sous τ, 2.0.67 est élément de K. Par le lemme principal, on obtient que $\mathcal{O}_K$ est diophantien dans $\mathcal{O}_L$ et comme $\mathbb{Z}$ est diophantien dans $\mathcal{O}_K$ par hypothèse du théorème au point c) et que L est Galois sur K car $[L:K]=2$, la proposition 2.0.1 c) donne le résultat voulu, c'est-à-dire $\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$.

cas a):

Si L est un corps imaginaire, on applique c) avec $K=\mathbb{Q}$ car alors $L=\mathbb{Q}(\sqrt{\theta})$ où $\theta<0$ et donc L n'est pas totallement réel (en fait, il est totallement imaginaire) et est de degré 2 sur $K=\mathbb{Q}$ qui lui est totallement réel. Aussi, $\mathbb{Z}$ est diophantien dans $\mathbb{Z}=\mathcal{O}_{\mathbb{Q}}$.

Sinon, soit $d\in\mathbb{N}_0$ tel que $L=\mathbb{Q}(\sqrt{d})$, $\sqrt{d}\notin\mathbb{Q}$. Alors $x^2-dy^2=1$ a une infinité de solutions dans $\mathbb{Z}\subseteq\mathcal{O}_L$ qui sont:

$$\{(\pm x,\pm y): x+y\sqrt{d}=(x_0+y_0\sqrt{d})^m, m\in\mathbb{N}\}$$

où (x_0,y_0) est la plus petite solution dont la somme de ses deux termes est plus grande que 1.

Pour $x,y\in\mathcal{O}_L$ satisfaisant $x^2-dy^2=1$ on a que $\dfrac{(x+y\sqrt{d})^e-(x-y\sqrt{d})^e}{2\sqrt{d}}$ est élément de L car $x,y,\sqrt{d}\in\mathcal{O}_L$ et L est un corps. Nous voulons montrer que τ laisse ce quotient fixe et par conséquent, qu'il est élément de $\mathbb{Q}$ puisque $\sqrt{d}\notin\mathbb{Q}$. Il faut faire attention ici car $\sqrt{d}\in L$ donc on ne peut pas affirmer sans autre vérification que $\tau(x)=x$ si $x\in\mathcal{O}_L$. Par contre, nous avons que

$$(x+y\sqrt{d})(x-y\sqrt{d})=x^2-dy^2=1$$

ce qui entraîne que

$$(x+y\sqrt{d})^{-1}=(x-y\sqrt{d})\in\mathcal{O}_L$$

et donc $x + y\sqrt{d} \in \mathcal{U}_L$ alors

$$N(x + y\sqrt{d}) \in \mathcal{U}_{\mathbb{Q}} = \{\pm 1\} \text{ car ce sont les unités de } \mathcal{O}_{\mathbb{Q}} = \mathbb{Z}.$$

Ainsi,

$$N(x + y\sqrt{d}) = (x + y\sqrt{d})\tau(x + y\sqrt{d}) = \pm 1$$

$$\Longrightarrow \tau(x + y\sqrt{d}) = \pm(x + y\sqrt{d})^{-1} = \pm(x - y\sqrt{d}).$$

D'où nous avons montré que $\dfrac{(x + y\sqrt{d})^e - (x - y\sqrt{d})^e}{2\sqrt{d}}$ est invariant sous τ lorsque e=2. Maintenant, il est possible d'appliquer le lemme principal avec $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt{d})$ étant donné que $\mathbb{Q}(\sqrt{d})$ est Galois sur $\mathbb{Q}$. On obtient de cette façon que $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ est diophantien dans $\mathcal{O}_L$.

cas b):

Si K est réel, on trouve le résultat voulu en combinant les cas a) et c). Supposons par conséquent que K est imaginaire, $K = \mathbb{Q}(\sqrt{\theta})$ avec $\theta < 0$. Alors $\mathcal{U}_K$ est fini. Soit e l'ordre de ce groupe. On choisit sans perte de généralité $d \in \mathcal{O}_K$ tel que $L = K(\sqrt{d})$ et $\sqrt{d} \notin K$. Alors pour $V_K = \{x+y\sqrt{d} : x, y \in \mathcal{O}_K \wedge x^2 - dy^2 = 1\}$ on sait par le lemme 2.0.17 que

$$rk\ V_K = rk\ \mathcal{U}_L - rk\ \mathcal{U}_K$$
$$\geq 1.$$

La dernière inégalité vient du fait que $n_L = 4$ et L n'est pas totallement réel alors $t = 1$ ou $t = 2$ et $n_K = 0 + 2 \cdot 1$, ce qui donne $rk\ \mathcal{U}_K = 0 + 1 - 1 = 0$ et $rk\ \mathcal{U}_L = 2 + 1 - 1 = 2$ ou $rk\ \mathcal{U}_L = 0 + 2 - 1 = 1$. On en conclut que $x^2 - dy^2 = 1$ a une infinité de solutions dans $\mathcal{O}_K \subseteq \mathcal{O}_L$. Pour tous ces $x, y \in \mathcal{O}_L$ qui satisfont $x^2 - dy^2 = 1$ on peut affirmer que:

$$N_{L/K}(x + y\sqrt{d}) \in \mathcal{U}_K$$

donc

$$(x + y\sqrt{d})^e \tau (x + y\sqrt{d})^e = 1$$

impliquant que

$$\tau(x + y\sqrt{d})^e = (x + y\sqrt{d})^{-e} = (x - y\sqrt{d})^e.$$

Il en découle que le côté gauche de l'équation 2.0.57 du lemme principal est invariant sous τ, ce qui en fait un élément de K. Conséquemment, on peut appliquer le lemme principal pour obtenir $\mathcal{O}_K$ est diophantien dans $\mathcal{O}_L$. Le cas a) nous donne $\mathbb{Z}$ est diophantien dans $\mathcal{O}_K$ et la proposition 2.0.1 c) lie le tout.

Chapitre 3

RECHERCHE DE NOUVELLES EXTENSIONS L NON ABÉLIENNES DE $\mathbb{Q}$ TELLES QUE H10$\mathcal{O}_L$ SOIT NON RÉSOLUBLE

Nous voulons maintenant retravailler l'idée de la preuve de l'article *Diophantine sets over some rings of algebraic integers* de J. Denef et L. Lipshitz (voir chapitre 2) afin de l'appliquer à une extension algébrique non abélienne de $\mathbb{Q}$. Pour ce faire, nous avons d'abord choisi un corps L de degré 6 qui soit Galois sur $\mathbb{Q}$, mais non abélien. Ainsi, le groupe de Galois de ce corps sera S_3. On suppose que L contient un sous-corps K de degré 3 et un sous-corps quadratique k.

Étant donné que L est Galois sur $\mathbb{Q}$, on peut utiliser sans problème la proposition 2.0.1 et les lemmes 2.0.13 à 2.0.15. Nos efforts seront donc concentrés dans la recherche de conditions suffisantes pour appliquer le lemme principal (2.0.16). En effet, puisque $[K : \mathbb{Q}]=3$, K possède exactement 2 isomorphismes complexes donc par le résultat de Alexandra Shlapentokh dans [**18**], $\mathbb{Z}$ est diophantien dans $\mathcal{O}_K$. De même, $[k : \mathbb{Q}]=2$ entraîne que $\mathbb{Z}$ est diophantien dans l'anneau des entiers algébriques de k. Alors en satisfaisant les hypothèses du lemme principal pour K ou respectivement pour k on obtiendrait la conclusion que $\mathcal{O}_K$ est diophantien dans $\mathcal{O}_L$ ou respectivement que $\mathcal{O}_k$ est diophantien dans $\mathcal{O}_L$. En conséquence, il serait possible d'appliquer le troisième point de la proposition 2.0.1 et de conclure

que $\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$. Le lemme 2.0.17 quant à lui ne nous sera d'aucune utilité. En effet, dans les deux cas précédents sa conclusion ne nous permet pas d'appliquer l'argument prouvant que V_K ou V_k est d'indice fini dans V_L. Démontrons ceci:

a)V_K n'est pas d'indice fini dans V_L.

Il existe un s $\in \mathbb{Z}$ tel que $L = K(\sqrt{s})$. Donc tout élément l de L peut être exprimé comme l=a+b$\sqrt{s}$, a,b $\in K$. Soit 0$\neq$d$\in \mathcal{O}_L$ tel que $L' = L(\sqrt{d})$ et $K' = K(\sqrt{d})$. Soit H un corps algébrique de degré n_H. Nous rappellons que la signature de H est $n_H = s + 2t$ où s est le nombre d'isomorphismes réels de H et 2t le nombre d'isomorphismes complexes de H. Trouvons alors la signature de chacun des corps K,K',L,L' :

$n_K = 1 + 2 \cdot 1$

$$n_L = \begin{cases} 2 + 2 \cdot 2 \text{ si s>0} \\ 0 + 2 \cdot 3 \text{ si s<0} \end{cases}$$

$$n_{K'} = \begin{cases} 2 + 2 \cdot 2 \text{ si d>0} \\ 0 + 2 \cdot 3 \text{ si d<0} \end{cases}$$

et finallement,

$$n_{L'} = \begin{cases} 4 + 2 \cdot 4 \text{ si s,d>0} \\ 0 + 2 \cdot 6 \text{ si s<0 ou d<0 .} \end{cases}$$

Ensuite on utilise le théorème de Dirichlet-Minkowski (voir [2], chapitre 2, section 4) qui nous assure que pour le corps H mentionné plus haut, le nombre de générateurs du groupe des unités de $\mathcal{O}_H$ est $rkU_H = s + t - 1$. Donc dans les cas qui nous intéressent on constate ce qui suit:

$rkU_K = 1 + 1 - 1 = 1$

$$rkU_L = \begin{cases} 2 + 2 - 1 = 3 \text{ si s>0} \\ 0 + 3 - 1 = 2 \text{ si s<0} \end{cases}$$

$$rkU_{K'} = \begin{cases} 2 + 2 - 1 = 3 \text{ si d>0} \\ 0 + 3 - 1 = 2 \text{ si d<0} \end{cases}$$

$$rkU_{L'} = \begin{cases} 4+4-1=7 \text{ si s,d}>0 \\ 0+6-1=5 \text{ si s}<0 \text{ ou d}<0\ . \end{cases}$$

Posons

$$V_K = \{x + y\sqrt{d} : x, y \in \mathcal{O}_K \text{ et } x^2 - dy^2 = 1\}$$

$$V_L = \{x + y\sqrt{d} : x, y \in \mathcal{O}_L \text{ et } x^2 - dy^2 = 1\}.$$

Par le lemme 2.0.17, on obtient comme résultat que

$$rkV_K = \begin{cases} 1 \text{ si d}<0 \text{ ou} \\ 2 \text{ sinon} \end{cases}$$

et

$$rkV_L = \begin{cases} 4 \text{ si s,d}>0 \text{ ou} \\ 3 \text{ sinon.} \end{cases}$$

En conséquence, $rkV_L \neq rkV_K$ et donc $[V_K : V_L]$ est infini.

Remarque: on a supposé que $\sqrt{d} \notin L$ car sinon $L' = L$ et alors on dérogerait aux hypothèses du lemme 2.0.17.

b)V_k n'est pas d'indice fini dans V_L.

Il existe un t $\in \mathbb{Z}$ tel que $k = \mathbb{Q}(\sqrt{t})$ et soit $K = \mathbb{Q}(\theta_0)$. Donc tout élément l de L peut être exprimé comme l=(a+b$\sqrt{t}$)+(c+d$\sqrt{t}$)θ+(e+f$\sqrt{t}$)θ^2, avec a,b,... ,f $\in \mathbb{Q}$. Soit 0$\neq$d$\in \mathcal{O}_L$ tel que $L' = L(\sqrt{d})$ et $k' = k(\sqrt{d})$. La remarque du cas précédent s'applique, donc on choisit $\sqrt{d} \notin L$. Nous pouvons trouver les signatures suivantes en supposant premièrement que t>0:

$n_k = 2 + 0$

$n_L = 2 + 2 \cdot 2$

$$n_{k'} = \begin{cases} 4+0 \text{ si d}>0 \\ 0+2\cdot 2 \text{ si d}<0 \end{cases}$$

et

$$n_{L'} = \begin{cases} 4+2\cdot 4 \text{ si d}>0 \\ 0+2\cdot 6 \text{ si d}<0\ . \end{cases}$$

Nous utilisons encore le théorème de Dirichlet-Minkowski:

$rkU_k = 2+0-1 = 1$

$rkU_L = 2+2-1 = 3$

$$rkU_{k'} = \begin{cases} 4+0-1 = 3 \text{ si d>0} \\ 2+0-1 = 1 \text{ si d<0} \end{cases}$$

et

$$rkU_{L'} = \begin{cases} 4+4-1 = 7 \text{ si d>0} \\ 0+6-1 = 5 \text{ si d<0 .} \end{cases}$$

Ainsi le lemme 2.0.17 nous donnerait,

$$rkV_k = \begin{cases} 0 \text{ si d<0 ou} \\ 2 \text{ sinon} \end{cases}$$

et $rkV_L = \begin{cases} 2 \text{ si d<0 ou} \\ 4 \text{ sinon.} \end{cases}$

Donc, $rkV_L \neq rkV_k$ et donc $[V_k : V_L]$ est infini.

Sinon, t<0 et alors tous les isomorphismes sont complexes. Ainsi,

$n_k = 0+2\cdot 1$ et $n_{k'} = 0+2\cdot 2$,

$n_L = 0+2\cdot 3$ et $n_{L'} = 0+2\cdot 6$.

Donc par le théorème de Dirichlet-Minkowski:

$rkU_k = 0$ et $rkU_{k'} = 1$,

$rkU_L = 2$ et $rkU_{L'} = 5$.

Cela nous donne $rkV_k = 1$ et rkV_L=3. Finallement la même conclusion s'impose; $[V_k : V_L]$ est infini.

Nous venons de voir que nous devrons trouver de nouvelles astuces pour satisfaire les hypothèses du lemme principal puisque V_K et V_k ne sont pas d'indice fini dans V_L contrairement aux cas traités dans [**7**]. Il nous faut donc prouver l'existence d'un élément $0 \neq d \in \mathcal{O}_L$ tel que l'équation $x^2 - dy^2 = 1$ ait une infinité de solutions dans $\mathcal{O}_L$ et l'existence d'un $e \in I\!N\backslash\{0\}$ tels que

$$\frac{(x+y\sqrt{d})^e - (x-y\sqrt{d})^e}{2\sqrt{d}} \in H$$

$\forall x, y \in \mathcal{O}_L$ satisfaisant $x^2 - dy^2 = 1$ où H est un des corps K ou k.

Notation: Nous notons Gal(M/N) le groupe de Galois de M sur N.

Proposition 3.0.2. *Soit L un corps algébrique de degré six avec un sous-corps cubique K et un sous-corps quadratique k=$\mathbb{Q}(\sqrt{t})$. Alors les conditions suivantes sont suffisantes pour appliquer le lemme principal 2.0.16 et donc obtenir une réponse négative à H10$\mathcal{O}_L$.*

i. L est une extension galoisienne de $\mathbb{Q}$ avec Gal$(L/\mathbb{Q})$=S_3,
ii. $x^2 - \sqrt{t}y^2 = 1$ a une infinité de solutions dans $\mathcal{O}_L$
iii. $\sqrt[4]{t} \notin L$.

Preuve:

Nous montrons d'abord que les hypothèses du lemme 2.0.16 sont respectées. Premièrement, L est Galois sur $\mathbb{Q}$ par i) donc L est Galois sur K. On pose $0 \neq d = \sqrt{t}$. On a bien que $d \in \mathcal{O}_L$ car $t \in \mathbb{Z} \subseteq \mathcal{O}_L$ et $\sqrt{t} \in L$ ce qui entraine $\sqrt{t} \in \mathcal{O}_L$. Aussi, $x^2 - \sqrt{t}y^2 = 1$ a une infinité de solutions dans $\mathcal{O}_L$ par ii). Posons $e = 1 \in \mathbb{N}_0$. Alors $\forall x, y \in L$ $(x \pm y\sqrt[4]{t})^e = (x \pm y\sqrt[4]{t})$ est élément de $L(\sqrt{d}) = L(\sqrt[4]{t})$. Or $L(\sqrt[4]{t}) = K(\sqrt{t})(\sqrt[4]{t}) = K(\sqrt[4]{t})$. Donc $\forall x, y \in L$ $(x \pm y\sqrt[4]{t}) \in K(\sqrt[4]{t})$, et conséquemment $\dfrac{(x + y\sqrt[4]{t}) - (x - y\sqrt[4]{t})}{2\sqrt[4]{t}} \in K(\sqrt[4]{t})$.

Définissons τ un K-automorphisme de $L(\sqrt[4]{t})$ tel que $\tau : \sqrt[4]{t} \mapsto -\sqrt[4]{t}$. Puisque $\sqrt[4]{t} \notin L$ et

$$\tau\left(\frac{(x + y\sqrt[4]{t}) - (x - y\sqrt[4]{t})}{2\sqrt[4]{t}}\right) = \frac{(x + y\sqrt[4]{t}) - (x - y\sqrt[4]{t})}{2\sqrt[4]{t}}$$

on peut maintenant affirmer que $\forall x, y \in L$

$$\frac{(x + y\sqrt[4]{t}) - (x - y\sqrt[4]{t})}{2\sqrt[4]{t}} \in K.$$

Par le lemme 2.0.16 on a donc que $\mathcal{O}_K$ est diophantien dans $\mathcal{O}_L$. En outre, $\mathbb{Z}$ est diophantien dans $\mathcal{O}_K$ car $[K : \mathbb{Q}]$=3 donc K a exactement deux isomorphismes complexes. Alors $\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$ par la proposition 2.0.1.

En conclusion nous ne pouvons pas affirmer que H10$\mathcal{O}_L$ est non résoluble mais c'est encore possible selon notre proposition. De plus, ce cas n'avait jamais été traité car L est de degré deux sur K, mais K est un corps qui n'est pas totallement réel. De plus, L n'est pas abélien étant donné que son groupe de galois est S_3 un groupe non abélien.

De façon plus générale, nous considérons maintenant les extensions galoisiennes et non abéliennes L des rationnels, avec $[L : \mathbb{Q}]$=m où m est un nombre naturel plus grand que cinq et L possède un sous-corps quadratique propre k. Alors les hypothèses des lemmes 2.0.13, 2.0.14, 2.0.15 sont respectées. Celles de la proposition 2.0.1 aussi. Nous faisons maintenant la preuve que l'argument de l'indice fini ne peut pas être utilisé avec k.

V_k n'est pas d'indice fini dans V_L:
On sait qu'il existe un z $\in \mathbb{Z}$ tel que $k = \mathbb{Q}(\sqrt{z})$. Supposons premièrement que z>0 et comme précédemment que $L' = L(\sqrt{d})$, $K' = K(\sqrt{d})$ avec $\sqrt{d} \notin L$, alors

$n_k = 2 + 0$

$$n_{k'} = \begin{cases} 4 + 0 \text{ si d>0} \\ 0 + 2 \cdot 2 \text{ si d<0} \end{cases}$$

$n_L = s + 2 \cdot t$

et

$$n_{L'} = \begin{cases} 2s + 2 \cdot (2t) \text{ si d>0} \\ 0 + 2 \cdot (s + 2t) \text{ si d<0} \end{cases}$$

ce qui entraîne par le théorème de Dirichlet-Minkowski

$rkU_k = 2 + 0 - 1 = 1$

$rkU_{k'} = 4 + 0 - 1 = 3$ si d>0 ou bien $rkU_{k'} = 2 + 0 - 1 = 1$ si d<0

$rkU_L = s + t - 1$ et

$rkU_{L'} = 2s + 2t - 1$ si d>0 ou $rkU_{L'} = 0 + s + 2t - 1$ si d<0 .

Donc,

$$rkV_k = \begin{cases} 0 \text{ si d<0 ou} \\ 2 \text{ sinon} \end{cases}$$

et

$$rkV_L = \begin{cases} t \text{ si d<0 ou} \\ s+t \text{ sinon.} \end{cases}$$

En conséquence, $rkV_L = rkV_k$ si et seulement si $\begin{cases} d<0 \text{ et } t=0 \text{ ou} \\ d>0 \text{ et } s+t=2. \end{cases}$

Dans le cas où $s+t=2$ et $d>0$ on obtient $\begin{cases} s=2, t=0 \Rightarrow m=2, \\ s=1, t=1 \Rightarrow m=3, \\ s=0, t=2 \Rightarrow m=4. \end{cases}$

Puisqu'on s'intéresse à $m \geq 6$, on rejette toutes ces conditions. Autrement, $t=0$ implique que $rkV_L = t = 0$ donc on n'a pas que $x^2 - dy^2 = 1$ a une infinité de solutions dans $\mathcal{O}_L$ alors on exclut ce cas.

Puis, on suppose encore que $\sqrt{d} \notin L$, mais cette fois que z<0. Alors on a

$n_k = 0 + 2 \cdot 1$

$n_{k'} = 0 + 2 \cdot 2$

$n_L = s + 2 \cdot t$ et finallement,

$$n_{L'} = \begin{cases} 2s + 2 \cdot 2t \text{ si } d>0 \\ 0 + 2 \cdot (s+2t) \text{ si } d>0. \end{cases}$$

Conséquemment on trouve

$rkU_k = 0$

$rkU_{k'} = 1$

$rkU_L = s + t - 1$

$rkU_{L'} = 2s + 2t - 1$ si $d>0$ ou bien $rkU_{L'} = s + 2t - 1$ sinon

ce qui donne $rkV_L = \begin{cases} t \text{ si d<0 ou} \\ s+t \text{ sinon} \end{cases}$

et $rkV_k = 1$.

Ainsi on voit que $rkV_L = rkV_k$ si et seulement si $\begin{cases} d<0 \text{ et } t=1 \text{ ou} \\ d>0 \text{ et } s+t=1. \end{cases}$

Si $t=1$ alors L a exactement deux isomorphismes complexes. Donc $\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$ par le résultat de Alexandra Shlapentokh énoncé dans [**18**]. Nous sommes par conséquent en présence d'un cas déjà traité.

Si s+t=1 alors $\begin{cases} s=1,t=0 \Rightarrow m=1, \\ s=0,t=1 \Rightarrow m=2, \end{cases}$
ces conditions mènent à une contradiction car $m \geq 6$.

On peut supposer sans perte de généralités que $k=\mathbb{Q}(\sqrt{z})$ et que $L=K(\sqrt{z})$ pour un certain $z \in \mathbb{Z}$ et K un sous-corps de L. On prouve aussi que:

V_K n'est pas d'indice fini dans V_L:

$n_K = s+2\cdot t$

$n_{K'} = \begin{cases} 2s+2\cdot 2t \text{ si d>0} \\ 0+2\cdot(s+2t) \text{ si d<0} \end{cases}$

$n_L = \begin{cases} 2s+2\cdot 2t \text{ si z>0} \\ 0+2\cdot(s+2t) \text{ sinon} \end{cases}$

et finallement, si $\sqrt{d} \notin L$ (pour satisfaire les hypothèses du lemme 2.0.17)

$n_{L'} = \begin{cases} 4s+2\cdot 4t \text{ si z,d>0} \\ 0+2\cdot(2s+4t) \text{ si z<0 ou d<0.} \end{cases}$

On trouve par le théorème de Dirichlet-Minkowski:

$rkU_K = s+t-1$

$rkU_{K'} = \begin{cases} 2s+2t-1 \text{ si d>0} \\ s+2t-1 \text{ sid<0} \end{cases}$

$rkU_L = \begin{cases} 2s+2t-1 \text{ si z>0} \\ s+2t-1 \text{ sinon} \end{cases}$

$rkU_{L'} = \begin{cases} 4s+4t-1 \text{ si z,d>0} \\ 2s+4t-1 \text{ si z<0 ou d<0.} \end{cases}$

On obtiendrait par le lemme 2.0.17 le résultat suivant:

$rkV_K = \begin{cases} s+t \text{ si d>0 ou} \\ t \text{ sinon} \end{cases}$

et

$$rkV_L = \begin{cases} 2s + 2t \text{ si z,d>0 ou} \\ s + 2t \text{ si z<0 ou d <0.} \end{cases}$$

Donc $rkV_L = rkV_K$ si et seulement si $\begin{cases} d < 0 \text{ et } t = s + 2t \text{ ou} \\ d > 0 \text{ et } s + t = 2s + 2t. \end{cases}$

Nous sommes en présence de contradictions puisque s et t sont des entiers positifs ou nuls, mais au moins un des deux est non nul car $m > 5$.

Ainsi encore une fois on délaisse le lemme 2.0.17 et on doit se résoudre à contourner l'argument des indices finis. Pour ce faire, on se restreint à des corps plus simples (item iv) et on trouve la proposition suivante:

Proposition 3.0.3. *Soit L un corps algébrique avec un sous-corps K et un sous-corps quadratique $k = \mathbb{Q}(\sqrt{z})$ tels que:*

i. $L = K(\sqrt{z})$,

ii. $L/\mathbb{Q}$ *soit galoisien mais non abélien,*

iii. $x^2 - \sqrt{z}y^2 = 1$ *ait une infinité de solutions dans* $\mathcal{O}_L$,

iv. $\sqrt[4]{z} \notin L$ *et*

v. $\mathbb{Z}$ *diophantien dans* $\mathcal{O}_K$

alors $\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$ et par conséquent, la réponse au dixième problème de Hilbert pour l'anneau des entiers algébriques de L est négative.

Preuve:

Pour utiliser le lemme principal (2.0.16), on cherche $d \in \mathcal{O}_L$ et $e \in \mathbb{N}\backslash\{0\} = \mathbb{N}_0$ tels que $x^2 - dy^2 = 1$ ait une infinité de solutions dans $\mathcal{O}_L$ et que $\forall x, y \in \mathcal{O}_L$ satisfaisant $x^2 - dy^2 = 1$;

$$\frac{(x + y\sqrt{d})^e - (x - y\sqrt{d})^e}{2\sqrt{d}} \in H$$

où H est un sous-corps de L. De plus, L doit être Galois sur H. Posons H=K. Par ii) L est Galois sur $\mathbb{Q}$ donc L est Galois sur K. On pose maintenant $0 \neq d = \sqrt{z}$. On a $d \in \mathcal{O}_L$ car $z \in \mathbb{Z} \subseteq \mathcal{O}_L$ et $\sqrt{z} \in L$ ce qui entraine $\sqrt{z} \in \mathcal{O}_L$. Aussi, $x^2 - \sqrt{z}y^2 = 1$ a une infinité de solutions dans $\mathcal{O}_L$ par iii). Posons $e = 1 \in \mathbb{N}_0$.

Alors $\forall x, y \in L\ (x \pm y\sqrt[4]{z})^e = (x \pm y\sqrt[4]{z})$ est élément de $L(\sqrt{d}) = L(\sqrt[4]{z})$. Or on constate que $L(\sqrt[4]{z}) = K(\sqrt{z})(\sqrt[4]{z}) = K(\sqrt[4]{z})$. Donc $\forall x, y \in L\ (x \pm y\sqrt[4]{z}) \in K(\sqrt[4]{z})$ et par conséquent $\dfrac{(x + y\sqrt[4]{z}) - (x - y\sqrt[4]{z})}{2\sqrt[4]{z}} \in K(\sqrt[4]{z})$. Mais comme

$$\tau\Big(\frac{(x + y\sqrt[4]{z}) - (x - y\sqrt[4]{z})}{2\sqrt[4]{z}}\Big) = \frac{(x + y\sqrt[4]{z}) - (x - y\sqrt[4]{z})}{2\sqrt[4]{z}}$$

où τ est le K-automorphisme de $L(\sqrt[4]{z})$ tel que $\tau : \sqrt[4]{z} \mapsto -\sqrt[4]{z}$, on trouve $\forall x, y \in L$ que $\dfrac{(x + y\sqrt[4]{z}) - (x - y\sqrt[4]{z})}{2\sqrt[4]{z}} \in K$ car $\sqrt[4]{z} \notin L$.

Cela étant le résultat voulu, $\mathcal{O}_K$ est diophantien dans $\mathcal{O}_L$ par le lemme principal 2.0.16. Puis, comme $\mathbb{Z}$ est diophantien dans $\mathcal{O}_K$ par hypothèse, on a bien que $\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$ par la proposition 2.0.1.

Finallement ce cas n'avait jamais été traité car L est de degré arbitraire sur $\mathbb{Q}$ et K n'est pas nécessairement totallement réel. De plus, L n'est pas abélien. On peut maintenant remplacer les conditions iii et iv de manière à ce qu'elles soient plus générales:

Corollaire 3.0.2. *Soit L un corps algébrique avec un sous-corps K et un sous-corps quadratique $k = \mathbb{Q}(\sqrt{z})$ et supposons que $\exists s \in \mathbb{N}_o$ tels que:*

i. $L = K(\sqrt{z})$,

ii. $L/\mathbb{Q}$ *soit galoisien mais non abélien,*

iii. $x^2 - \sqrt[s]{z}y^2 = 1$ *ait une infinité de solutions dans* $\mathcal{O}_L$,

iv. $\sqrt[2s]{z} \notin L$ *mais* $\sqrt[s]{z} \in L$

v. $\mathbb{Z}$ *diophantien dans* $\mathcal{O}_K$

alors $\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$ et par conséquent, la réponse au dixième problème de Hilbert pour l'anneau des entiers algébriques de L est négative.

Preuve:

Par ii) L est Galois sur $\mathbb{Q}$ donc sur K. On pose $0 \neq d = \sqrt[s]{z}$. On a $d \in \mathcal{O}_L$ car $z \in \mathbb{Z} \subseteq \mathcal{O}_L$ et $\sqrt[s]{z} \in L$ par iv) ce qui entraine $\sqrt[s]{z} \in \mathcal{O}_L$. Aussi, $x^2 - \sqrt[s]{z}y^2 = 1$ a une infinité de solutions dans $\mathcal{O}_L$ par iii). Posons $e = 1 \in \mathbb{N}_0$. Alors il est clair que $\forall x, y \in L,\ (x \pm y\sqrt[2s]{z})^e = (x \pm y\sqrt[2s]{z})$ est élément de $L(\sqrt{d}) = L(\sqrt[2s]{z})$.

Or $L(\sqrt[2^s]{z}) = K(\sqrt{z})(\sqrt[2^s]{z}) = K(\sqrt[2^s]{z})$. Donc $(x \pm y\sqrt[2^s]{z}) \in K(\sqrt[2^s]{z})$ et par conséquent $\forall x, y \in L$ on a $\dfrac{(x + y\sqrt[2^s]{z}) - (x - y\sqrt[2^s]{z})}{2\sqrt[2^s]{z}} \in K(\sqrt[2^s]{z})$. Mais comme

$$\tau\Big(\frac{(x + y\sqrt[2^s]{z}) - (x - y\sqrt[2^s]{z})}{2\sqrt[2^s]{z}}\Big) = \frac{(x + y\sqrt[2^s]{z}) - (x - y\sqrt[2^s]{z})}{2\sqrt[2^s]{z}}$$

où $\tau : \sqrt[2^s]{z} \mapsto -\sqrt[2^s]{z}$, on trouve $\forall x, y \in L$ que $\dfrac{(x + y\sqrt[2^s]{z}) - (x - y\sqrt[2^s]{z})}{2\sqrt[2^s]{z}} \in K$ car $\sqrt[2^s]{z} \notin L$.

Par le lemme principal 2.0.16 on a donc que $\mathcal{O}_K$ est diophantien dans $\mathcal{O}_L$ et comme $\mathbb{Z}$ est diophantien dans $\mathcal{O}_K$ par v), alors $\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$.

Grâce aux connaissances acquises au chapitre un, nous pouvons formuler d'autres corollaires. Nous savons que $\mathbb{Z}$ est diophantien dans l'anneau des entiers algébriques de quelques classes d'extensions algébriques des rationnels. Nous allons donc utiliser ces résultats dans ce qui suit.

Corollaire 3.0.3. *Soit L un corps algébrique avec un sous-corps K et un sous-corps quadratique $k = \mathbb{Q}(\sqrt{z})$ et supposons que $\exists s \in \mathbb{N}_o$ tels que:*

i. $L = K(\sqrt{z})$,

ii. $L/\mathbb{Q}$ *soit galoisien mais non abélien,*

iii. $x^2 - \sqrt[s]{z}y^2 = 1$ *ait une infinité de solutions dans* $\mathcal{O}_L$,

iv. $\sqrt[2^s]{z} \notin L$ *mais* $\sqrt[s]{z} \in L$ *et*

v. K possède exactement deux isomorphismes complexes

alors $\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$ et par conséquent, la réponse au dixième problème de Hilbert pour l'anneau des entiers algébriques de L est négative,

ou bien

Corollaire 3.0.4. *Soit L un corps algébrique avec un sous-corps K et un sous-corps quadratique $k = \mathbb{Q}(\sqrt{z})$ et supposons que $\exists s \in \mathbb{N}_o$ tels que:*

i. $L = K(\sqrt{z})$,

ii. $L/\mathbb{Q}$ *soit galoisien mais non abélien,*

iii. $x^2 - \sqrt[s]{z}y^2 = 1$ *ait une infinité de solutions dans* $\mathcal{O}_L$,

iv. $\sqrt[2s]{z} \notin L$ *mais* $\sqrt[s]{z} \in L$ *et*

v. $[K: \mathbb{Q}]=4$, K *n'est pas totallement réel et* K *possède un sous-corps quadratique*

alors $\mathbb{Z}$ *est diophantien dans* $\mathcal{O}_L$ *et par conséquent, la réponse au dixième problème de Hilbert pour l'anneau des entiers algébriques de* L *est négative,*

ou bien

Corollaire 3.0.5. *Soit* L *un corps algébrique avec un sous-corps* K *et un sous-corps quadratique* $k = \mathbb{Q}(\sqrt{z})$ *et supposons que* $\exists s \in \mathbb{N}_o$ *tels que:*

i. $L = K(\sqrt{z})$,

ii. $L/\mathbb{Q}$ *soit galoisien mais non abélien,*

iii. $x^2 - \sqrt[s]{z}y^2 = 1$ *ait une infinité de solutions dans* $\mathcal{O}_L$,

iv. $\sqrt[2s]{z} \notin L$ *mais* $\sqrt[s]{z} \in L$ *et*

v. K *soit abélien*

alors $\mathbb{Z}$ *est diophantien dans* $\mathcal{O}_L$ *et par conséquent, la réponse au dixième problème de Hilbert pour l'anneau des entiers algébriques de* L *est négative.*

ou bien

Corollaire 3.0.6. *Soit* L *un corps algébrique avec un sous-corps* K, *un sous-corps quadratique imaginaire* $k = \mathbb{Q}(\sqrt{z})$ $(z<0)$ *et un sous-corps totallement réel* K' *puis supposons que* $\exists s \in \mathbb{N}_o$ *tels que:*

i. $L = K(\sqrt{z})$,

ii. $L/\mathbb{Q}$ *soit galoisien mais non abélien,*

iii. $x^2 - \sqrt[s]{z}y^2 = 1$ *ait une infinité de solutions dans* $\mathcal{O}_L$,

iv. $\sqrt[2s]{z} \notin L$ *mais* $\sqrt[s]{z} \in L$ *et*

v. $K = K'(\sqrt{v})$ *où* $v < 0$,

alors $\mathbb{Z}$ *est diophantien dans* $\mathcal{O}_L$ *et par conséquent, la réponse au dixième problème de Hilbert pour l'anneau des entiers algébriques de* L *est négative.*

D'après les résultats connus antérieurement (voir chapitre un), K pourrait appartenir à d'autres classes d'extensions telles que $\mathbb{Z}$ soit diophantien dans $\mathcal{O}_K$. Par contre, nous ne les avons pas retenues parce qu'elles mènent à des cas déjà traités. En effet, si K est totallement réelle alors L est de degré deux sur une extension totallement réelle, donc on rejette ce cas. De même, si K n'est pas totallement réelle et est de degré deux sur une extension totallement réelle alors, $K = K'(\sqrt{v})$ pour un certain $v<0$ et K' totallement réelle, donc $L = K'(\sqrt{v})(\sqrt{z}) = K'(\sqrt{z})(\sqrt{v})$ qui est un corps non totallement réel, mais de degré deux sur un corps totallement réel soit $K'(\sqrt{z})$ lorsque z>0. Dans un autre ordre d'idées, nous ne supposerons pas que $[\mathrm{K}:\mathbb{Q}] = 2$ car nous souhaitons que $[\mathrm{L}:\mathbb{Q}] \geq 6$.

Enfin, nous soumettons la conjecture qu'il existe une extension algébrique non abélienne des rationnels répondant aux critères du corollaire 3.0.4 avec s=4 et donc telle que son anneau des entiers algébriques soit non résoluble. En effet, nous allons démontrer que l'extension $L = \mathbb{Q}(\alpha, i)$ où $\alpha = \sqrt[4]{2}$ et $i^2 = -1$ respecte les conditions i),ii),iv) et v) du corollaire 3.0.4. Il suffirait donc de prouver qu'elle remplit aussi la condition iii) pour obtenir une démonstration complète, ce que nous croyons possible.

Dans un premier temps, nous allons démontrer que $L = K(\sqrt{z})$ où $z = 2$ et $K = \mathbb{Q}(\alpha(1+i)) = \mathbb{Q}(\alpha + i\alpha)$.

a) $\mathbb{Q}(\sqrt{2},\ \alpha(1+i)) \subseteq \mathbb{Q}(\alpha, i)$.

Étant donné que $\sqrt{2} = \alpha^2 \in \mathbb{Q}(\alpha, i)$ et clairement, α et $1+i$ sont éléments de $\mathbb{Q}(\alpha, i)$ donc $\alpha(1+i)$ aussi.

b) $\mathbb{Q}(\alpha, i) \subseteq \mathbb{Q}(\sqrt{2},\ \alpha(1+i))$.

On trouve $2\sqrt{2}i = \alpha^2(1+i)^2 \in \mathbb{Q}(\sqrt{2},\ \alpha(1+i))$. Donc $i \in \mathbb{Q}(\sqrt{2},\ \alpha(1+i))$ puisque $(2\sqrt{2})^{-1} \in \mathbb{Q}(\sqrt{2},\ \alpha(1+i))$. Ainsi, $1+i \in \mathbb{Q}(\sqrt{2},\ \alpha(1+i))$. Il reste à prouver que $\alpha \in \mathbb{Q}(\sqrt{2},\ \alpha(1+i))$, mais $\alpha(1+i)$ est triviallement élément de $\mathbb{Q}(\sqrt{2},\ \alpha(1+i))$ et $(1+i)^{-1}$ aussi. Donc $\alpha \in \mathbb{Q}(\sqrt{2},\ \alpha(1+i))$.

Ensuite nous avons bien que $\mathbb{Z}$ est diophantien dans $\mathcal{O}_K$ puisque $\mathbb{Q}(i\sqrt{2}) \subseteq \mathbb{Q}(\alpha + i\alpha) = K$ et $[K:\ \mathbb{Q}] = 4$. En effet, $2\sqrt{2}i = (\alpha + i\alpha)^2$ et 4 est le plus

petit $s \in \mathbb{N}_0$ tel que $(\alpha + i\alpha)^s \in \mathbb{Q}$. De plus, K n'est pas totallement réel car $(\alpha + i\alpha) \notin \mathbb{R}$, donc par le résultat de Denef et Lipshitz H10$\mathcal{O}_K$ est non résoluble.

En outre, $\sqrt[4]{2} = \alpha \in L$, mais $\sqrt[8]{2} \notin L$ car sinon nous aurions $a, b \in \mathbb{Q}$ tels que $\sqrt[8]{2} + 0i = a\sqrt[4]{2} + bi$ mais alors $b = 0$ puisque $\sqrt[8]{2}$ est un nombre réel. Donc $\frac{\sqrt[8]{2}}{\sqrt[4]{2}} = \frac{1}{\sqrt[8]{2}} = a \in \mathbb{Q}$. Contradiction.

Finallement, notons $\sigma_{u,v}$, $u = 1, 2, 3, 4$, $v = 1, 2$ les huit automorphismes de $L = \mathbb{Q}(\alpha, i)$ où $\sigma_{u,1}(i) = i$, $\sigma_{u,2}(i) = -i$ et $\sigma_{1,v}(\alpha) = \alpha$, $\sigma_{2,v}(\alpha) = -\alpha$, puis $\sigma_{3,v}(\alpha) = i\alpha$, $\sigma_{4,v}(\alpha) = -i\alpha$. L est donc une extension galoisienne mais non abélienne des rationnels car $\sigma_{1,2}\sigma_{3,1}(\alpha) = \sigma_{1,2}(i\alpha) = -i\alpha \neq \sigma_{3,1}\sigma_{1,2}(\alpha) = \sigma_{3,1}(\alpha) = i\alpha$.

Étant donné ce qui précède, nous ne pouvons pas conclure que H10$\mathcal{O}_{\mathbb{Q}(\sqrt[4]{2},i)}$ est non résoluble. Cependant, nous croyons fortement qu'il est possible de démontrer la troisième condition du corollaire 3.0.4 et donc que $\mathbb{Q}(\sqrt[4]{2}, i)$ est en effet une extension non résoluble de $\mathbb{Q}$.

En résumé, nous avons établi une proposition et 5 corollaires permettant de reconnaître de nouveaux anneaux d'entiers algébriques comme étant non résolubles. De plus, nous avons utilisé un de ces corollaires afin d'émettre la conjecture qu'il existe une extension algébrique non abélienne des rationnels telle que la réponse au dixième problème de Hilbert pour son anneau d'entiers algébriques soit négative. Cette extension est $\mathbb{Q}(\sqrt[4]{2}, i)$.

Nous pouvons affirmer en conclusion que nous avons fait un petit pas dans la direction de Jan Denef et Leonard Lipshitz. En effet, non seulement avons nous suivi leurs traces tant qu'au type de preuves utilisées, mais aussi nous obtenons des résultats qui se situent dans le cadre de leur conjecture: *pour tout corps algébrique L, $\mathbb{Z}$ est diophantien dans $\mathcal{O}_L$.*

BIBLIOGRAPHIE

[1] JULIO R. BASTIDA, Field extensions and Galois theory, *Encyclopedia of mathematics and its applications*, Addison-Wesley (1984)

[2] Z.I. BOREVICH ET I.R. SHAFAREVICH, Number theory, *Pure and applied Mathematics.*, **20** Academic press inc., New York, (1966)

[3] M. DAVIS, Hilbert's tenth problem is unsolvable, *American Mathematical Monthly*, **80**, pp.233-269 (1973)

[4] M. DAVIS, YU. MATIJASEVIČ, J. ROBINSON, Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution,, *Proceedings of Symposia in Pure Mathematics*, **28**, pp. (1976)

[5] J.DENEF, Hilbert's tenth problem for quadratic rings, *Proc. Amer. Math. Soc.*, **48**, pp. 214-220 (1975)

[6] J.DENEF, Diophantine sets over algebraic integer rings II, *Transactions of the American Mathematical Society.*, **257**,numéro 1, pp. (1980)

[7] J.DENEF, L. LIPSHITZ, Diophantine sets over some rings of algebraic integers, *J. London Mathematical Society.*, **2**,numéro 18, pp.385-391 (1978)

[8] DAN FLATH, STAN WAGON , How to pick out the integers in the rationals: an application of number theory to logic, *American Mathematical Monthly*, **98**, pp.812-823 (1991)

[9] J. P. JONES, Universal diophantine equation, *the Journal Of Symbolic Logic*, **47, no. 3**, pp.549-571 (1982)

[10] S. LANG, Algebraic number theory, *Addison Wesley Publ. Co.*, (1970)

[11] J. MARTINET, J.J. PAYAN, Sur les extensions cubiques non-Galoisiennes des rationnels et leur clôture Galoisienne, *Journal Für die Reine und Angewandte Mathematik*, **228**, pp.15-37 (1967)

[12] J. MARTINET, J.J. PAYAN, Sur les bases d'entiers des extensions galoisiennes et non abéliennes de degré 6 des rationnels, *Journal Für die Reine und Angewandte Mathematik*, **229-231**, pp.29-33 (1968)

[13] YU. MATIJASEVIČ, Enumerable sets are diophantine, *Soviet Mathematics Doklady*, **11**, pp.354-357 (1970)

[14] J. ROBINSON, Definability and decision problems in arithmetic, *The Journal of Symbolic Logic*, **14, no. 2**, pp.98-114 (1949)

[15] J. ROBINSON, Diophantine decision problems, *MAA Studies in Mathematics*, **6**, pp.76-116 (1969)

[16] ROBERT S. RUMELY, Arithmetic over the ring of all algebraic integers, *Journal Für die Reine und Angewandte Mathematik*, **368**, pp.127-133 (1986)

[17] H. N. SHAPIRO, A. SHLAPENTOKH, Diophantine relationships between algebraic number fields, *Communications on Pure and Applied Mathematics*, **XLII**, pp.1113-1122 (1989)

[18] A. SHLAPENTOKH, Extension of Hilbert's tenth problem to some algebraic number fields, *Communications on Pure and Applied Mathematics*, **XLII**, pp.939-962 (1989)

[19] A. SHLAPENTOKH, Diophantine undecidability in some rings of algebraic numbers of totally real infinite extensions of $\mathbb{Q}$, *Annals of pure and applied logic*, **68**, pp.299-325 (1994)

[20] I.N.STEWART, D.O. TALL, Algebraic number theory, *Chapman and Hall*, (1979)