1.67 07 2 Communiqué le 26 Avril 1967

Remarques sur les formes à plusieurs variables décomposables en facteurs linéaires

Par Trygve Nagell

§ 1. Introduction

1. Définitions. Soient **K** un corps algébrique de degré n, $\mathbf{K}^{(1)}=\mathbf{K}$, $\mathbf{K}^{(2)}$, ..., $\mathbf{K}^{(n)}$ les corps conjugués de **K** par rapport au corps des rationnels. Soient r_1 le nombre des $\mathbf{K}^{(i)}$ réels et $2r_2$ celui des $\mathbf{K}^{(i)}$ imaginaires. Alors, le nombre $r=r_1+r_2-1$ est le rang du corps **K** c'est-à-dire le rang du groupe abélien multiplicatif des unités de **K**.

Si α est un nombre dans **K** nous désignons par $N(\alpha)$ la norme de α dans **K**. Les nombres algébriques sont toujours supposés entiers. Soient $\alpha_1, \alpha_2, ..., \alpha_n$ des nombres dans **K** linéairement indépendants. Nous considérons dans ce travail seulement des formes du type

$$N(x_1\alpha_1+x_2\alpha_2+\ldots+x_m\alpha_m),$$

où $m\leqslant n$, et où les nombres $\alpha_1, \alpha_2, ..., \alpha_m$ satisfont à la condition que le corps composé $\mathbf{K}(\alpha_2\alpha_1^{-1}, \alpha_3\alpha_1^{-1}, ..., \alpha_m\alpha_1^{-1})$ soit égal à **K**. La forme est de degré n. Alors, nous dirons que la forme a le rang r. La forme est évidemment irréductible dans le corps rationnel. Nous supposons que $n\geqslant 3$.

2. Représentations. Considérons l'équation à m inconnues du n-ième degré

$$N(x_1\alpha_1+x_2\alpha_2+\ldots+x_m\alpha_m)=A, \tag{1}$$

où A est un nombre entier rationnel. Supposons d'abord que $m=n$. Dans ce cas le problème de résoudre l'équation (1) en nombres entiers rationnels $x_1, x_2, ..., x_n$ revient à déterminer les nombres de la norme donnée A dans le module $\mathbf{M}(\alpha_1, \alpha_2, ..., \alpha_n)$. Il existe des méthodes pour reconnaître si l'équation (1) est résoluble ou non pour une valeur donnée de A lorsque les nombres α_i sont donnés. Si l'équation est résoluble il y a une infinité de solutions, lesquelles peuvent être caractérisées complètement à l'aide de la théorie des unités. Voir p. ex. Skolem [1][1], p. 57–62; comparez aussi Nagell [2].

Il y a, même pour $m=n$, des équations du type (1) qui ne possèdent aucune solution. En effet, on peut établir le résultat suivant :

Théorème 1. *Soient $\alpha_1, \alpha_2, ..., \alpha_n$ des nombres dans* **K** *linéairement indépendants. Alors, il existe un nombre infini de nombres premiers p, tels que l'équation*

[1] Les numéros figurant entre crochets renvoient à la bibliographie placée à la fin de ce mémoire.

$$N(x_1\alpha_1+x_2\alpha_2+\ldots+x_n\alpha_n)=p \tag{2}$$

n'admette aucune solution en nombres entiers rationnels $x_1, x_2, \ldots, x_n$.

Démonstration. Si l'équation (2) est résoluble, le nombre premier p est divisible par l'idéal premier $(x_1\alpha_1+x_2\alpha_2+\ldots+x_n\alpha_n)$ du premier degré dans $\mathbf{K}$. Or, il résulte des lois de densité de Frobenius–Tchebotareff qu'il y a, dans tout corps algébrique, une infinité de nombres premiers, de densité positive, qui ne sont divisibles par aucun idéal premier du premier degré. Voir Hasse [3], §§ 23–24.

3. Les recherches sur l'équation diophantienne (1) présentent déjà pour $m=2$ et $n>2$ des difficultés qu'on n'a pu surmonter jusqu'ici. D'après le célèbre théorème d'Axel Thue on sait que le nombre de solutions est limité dans ce cas; il est même possible de déterminer une limite supérieure du nombre de solutions en fonction des coefficients; mais cette limite est, dans le cas général, sans intérêt à cause de la grandeur des valeurs qu'elle fournit. Il manque surtout un critère pour reconnaître si l'équation est résoluble ou non. De plus, il manque une méthode pour effectivement déterminer toutes les solutions en cas de solubilité. Il est évident que la méthode de Thue et ses successeurs, basée sur l'approximation de nombres algébriques par des nombres rationnels ou algébriques, ne suffit pas pour obtenir la solution complète du problème. Des nouvelles méthodes plus effectives sont nécessaires pour y arriver.

Le problème de résoudre l'équation (1) est essentiellement un problème concernant les propriétés des unités dans le corps algébrique en question. C'est en prenant cette idée pour point de départ qu'on a réussi, pour quelques équations binaires, de résoudre complètement le problème indépendamment des résultats de Thue. Ainsi, on a réussi pour certaines équations cubiques binaires lorsque le discriminant est négatif; voir Skolem [1], p. 108–112. Lorsque le corps est biquadratique et $r=1$ la résolution complète du problème binaire est possible dans tous les cas; voir Nagell [4]. Lorsque le corps est biquadratique et $r=2$ on peut résoudre complètement certains types d'équations binaires; voir Skolem [1], p. 112–114. On a aussi réussi lorsque le corps est cyclotomique d'un type particulier; voir Nagell [4], § 6.

Grâce à l'application de la théorie des nombres p-adiques combinée avec la méthode des unités, Skolem a obtenu des résultats remarquables même sur quelques équations ternaires; voir Skolem [1], p. 114–120. Cependant, la méthode p-adique ne donne pas toutes les solutions, sauf dans certains cas particuliers.

Ce travail-ci est une étude préliminaire sur les propriétés de l'équation diophantienne (1) pour $m\geqslant 3$ et $n\geqslant 4$ avec la condition $m\leqslant n-1$. Nous avons là un domaine de recherche très vaste, dans lequel les difficultés surpassent de beaucoup celles des cas $m=2$ et $m=n$, et les efforts n'ont pas été couronnés de beaucoup de succès. Après avoir présenté les résultats obtenus dans des travaux antérieurs, nous allons y ajouter quelques nouveaux résultats relatifs à certains corps imprimitifs. Ce sont des exemples choisis pour illustrer certaines possibilités. Pour les démonstrations nous utilisons la méthode des unités, modifiée selon le caractère du corps, et souvent combinée avec application du théorème de Thue.

Remarque. Lorsque les nombres entiers rationnels $x_1, x_2, \ldots, x_m$ satisfont à l'équation (1) nous dirons, pour abréger, que le nombre

$$x_1\alpha_1+x_2\alpha_2+\ldots+x_m\alpha_m$$

est une solution de cette équation.

§ 2. Équations admettant un nombre fini de solutions pour $m < n$

4. Théorèmes de Siegel et de Chabauty. Le problème de résoudre l'équation (1) lorsque $m \leqslant n-1$ présente des grandes difficultés. La question principale est évidemment de pouvoir décider si l'équation admet une infinité de solutions ou seulement un nombre fini. Si $m=2$ et $n \geqslant 3$ on sait que le nombre de solutions est limité (théorème d'Axel Thue). Si $m=2$ et $n=3$ ou $n=4$ on sait même déterminer toutes les solutions dans des cas particuliers; voir p. ex. Skolem [1], p. 108–114, et Nagell [4], p. 186. Cependant, dans la suite nous laissons de côté les formes binaires; ainsi nous supposons que $m \geqslant 3$.

On connaît deux résultats généraux dans lesquels le nombre de solutions de l'équation (1) est fini. Le résultat le plus général est dû à C. Siegel qui a établi le théorème suivant :

Soit ξ un nombre algébrique entier de degré n. Désignons par $F(x_1, x_2, \ldots, x_{h+1})$ la forme décomposable

$$N(x_1 + x_2\xi + \ldots + x_{h+1}\xi^h),$$

où h est un nombre naturel tel que

$$n > h^2\left(\frac{n}{s+1} + s\right)$$

pour $s = \frac{1}{2}(\sqrt{4n+1} - 1)$. Cela posé, l'équation

$$F(x_1, x_2, \ldots, x_{h+1}) = A,$$

où A est un nombre entier rationnel donné, n'a qu'un nombre limité de solutions $x_1, x_2, \ldots, x_{h+1}$ en nombres entiers rationnels.

Si $n < 57$ on a $h=1$; si $57 \leqslant n < 307$ on a $h=1$ ou $h=2$; si $n \geqslant 307$ on peut prendre $h=3$. En général, la plus petite valeur de n pour laquelle $n > h^2(n/(s+1)+s)$ est $n = 4h^4 - 2h^2 + 1$.

Siegel a obtenu ce résultat en utilisant ses résultats sur l'approximation des nombres algébriques par d'autres nombres algébriques; voir Siegel [5], Satz 4. Cependant, la démonstration ne donne aucun algorithme pour déterminer les solutions éventuelles.

Skolem a traité l'équation (1) dans le cas où $\mathbf{K}$ est du cinquième degré et du second rang pour $m=3$. A l'aide de sa méthode p-adique il a montré qu'alors le nombre de solutions est limité; voir Skolem [1], p. 118.

Ce résultat est compris dans le théorème plus général de C. Chabauty [6]:

Soient α, β, γ trois nombres entiers, linéairement indépendants, du corps primitif $\mathbf{K}$ du n-ième degré et du rang $r \leqslant n-3$. Alors, l'équation ternaire

$$N(\alpha x + \beta x + \gamma z) = A,$$

où A est un entier rationnel, n'admet qu'un nombre fini de solutions en nombres entiers rationnels x, y, z.

Pour établir ce résultat Chabauty se sert de la méthode p-adique et de certains résultats de Skolem et de Siegel. La méthode de démonstration ne permet pas de décider sur la solubilité ni de déterminer toutes les solutions, sauf dans des cas d'exception. La condition $r \leqslant n-3$ est équivalente à l'inégalité $r_2 \geqslant 2$.

5. Un exemple cyclotomique. Les théorèmes de Siegel, Skolem et Chabauty sont, à ce que je sache, les seuls résultats connus jusqu'ici sur les équations du type (1) pour $3 \leqslant m \leqslant n-1$. Dans un travail qui vient de paraître (Nagell [7]) j'ai montré comment on peut obtenir d'autres résultats par des méthodes plus simples. En effet, j'ai établi le théorème suivant :

Soit ξ une racine primitive p-ième de l'unité, p étant un nombre premier >5. Alors l'équation ternaire

$$N(x+\xi y+\xi^2 z)=1$$

n'admet qu'un nombre fini de solutions en nombres entiers rationnels x, y, z.

Ce résultat n'est pas compris dans le théorème de Chabauty, vu que le corps $\mathbf{K}(\xi)$ n'est pas primitif. En effet, celui-ci contient le nombre $\sqrt{p}$ ou $\sqrt{-p}$ suivant que p est $\equiv 1$ ou $\equiv -1$ (mod 4). Le corps $\mathbf{K}(\sqrt{p})$, respectivement $\mathbf{K}(\sqrt{-p})$, est le seul sous-corps quadratique dans $\mathbf{K}(\xi)$; voir Nagell [13], théorème 1.

Dans ce numéro nous désignons par ξ le nombre $e^{2\pi i/p}$, où p est un nombre premier >5. $\mathbf{K}$ signifie le corps $\mathbf{K}(\xi)$ et $\mathbf{K}_1$ le sous-corps $\mathbf{K}(\xi+\xi^{-1})$ de degré $\nu=\frac{1}{2}(p-1)$. N signifie la norme dans $\mathbf{K}$ et N_1 la norme dans $\mathbf{K}_1$. En substituant ξ par ξ^{-1} le nombre α sera transformé en α'.

Il est possible d'obtenir la généralisation suivante du théorème que nous venons de citer :

Théorème 2. *Si m est un nombre entier rationnel, tel que $m(m-1)$ ne soit pas divisible par p, l'équation ternaire*

$$N(x+\xi y+\xi^m z)=1$$

n'admet qu'un nombre fini de solutions en nombres entiers rationnels x, y, z.

Démonstration. Nous avons besoin des deux lemmes suivants :

Lemme 1. *Si le nombre premier p est $\equiv 1$ (mod 4) on a*

$$\tfrac{1}{2}(\sqrt{p}-1)=\sum_{0<r<\frac{1}{2}p}(\xi^r+\xi^{-r}),$$

où la somme est étendue à tous les restes quadratiques modulo p dans l'intervalle $0-\frac{1}{2}p$.

Lemme 2. *Supposons que le nombre premier p est >5 et $\equiv 1$ (mod 4) et que $m(m-1)$ n'est pas divisible par p. Alors le nombre entier*

$$\alpha=\frac{\xi^m-\xi^{-m}}{\xi-\xi^{-1}}.$$

n'appartient pas au corps $\mathbf{K}(\sqrt{p})$.

Pour la démonstration du lemme 1 voir par exemple Nagell [12], Theorem 99. Pour établir le lemme 2 on aura à montrer que la relation

$$\alpha = A + \tfrac{1}{2}B(\sqrt{p}-1),$$

A et B entiers rationnels, est impossible. Si cette relation a lieu on obtient d'après le lemme 1 l'identité

$$\frac{\xi^m - \xi^{-m}}{\xi - \xi^{-1}} = A + B\sum_r (\xi^r + \xi^{-r}).$$

Il est évident qu'on peut supposer $1 < m \leqslant \tfrac{1}{2}(p-1)$. Posons $\nu = \tfrac{1}{2}(p-1)$ et multiplions cette identité par ξ^ν. Nous obtenons alors

$$\xi^{\nu+m-1} + \xi^{\nu+m-3} + \xi^{\nu+m-5} + \ldots = A\xi^\nu + B\sum_r (\xi^{\nu+r} + \xi^{\nu-r}).$$

L'exposant à gauche $\nu+m-1$ est $\leqslant p-2$. Si $\tfrac{1}{2}(p-1)$ est un reste quadratique nous avons à droite le terme $B\xi^{p-1} = -B(\xi^{p-2} + \xi^{p-3} + \ldots)$. Alors il faut que $\nu+m-1$ soit $= p-2$. Cela entraîne que $B = -1$. Donc, le dernier terme (pour $\nu - r = 0$) à droite serait -1, ce qui est impossible.

Désignons par r^* le plus grand reste quadratique $< \tfrac{1}{2}p$ modulo p. Alors, il faut que $r^* \leqslant \tfrac{1}{2}(p-3)$. On aura donc $\nu+m-1 = \nu + r^*$ avec $B = 1$. Si m est impair il faut que $A = 1$. Si m est pair il faut que $A = 0$. Le nombre de termes à gauche est toujours $= m$. Le nombre de termes à droite est $= 1 + \tfrac{1}{2}(p-1)$ si $A = 1$; or, cela est impossible vu que $m \leqslant \tfrac{1}{2}(p-1)$. Il faut donc que $A = 0$ et $m = \tfrac{1}{2}(p-1)$. Par conséquent, la somme à gauche deviendra, après une division avec ξ^ν,

$$\xi + \xi^{-1} + \xi^3 + \xi^{-3} + \ldots + \xi^{\nu-1} + \xi^{-\nu+1}.$$

Il en résulterait que tous les restes quadratiques dans l'intervalle $0 - \tfrac{1}{2}p$ seraient impairs. Cela est impossible, vu que le nombre 4 est un reste et que $p > 5$. Donc, le lemme 2 se trouve démontré.

En profitant d'un résultat de Hilbert (voir [10], p. 335) nous obtenons de l'équation ternaire, la relation

$$x + \xi y + \xi^m z = \xi^h E,$$

où E est une unité (réelle) dans le corps $\mathbf{K}_1$.

En substituant ξ par ξ^{-1} nous aurons

$$x + \xi^{-1} y + \xi^{-m} z = \xi^{-h} E,$$

d'où par soustraction

$$y(\xi - \xi^{-1}) + z(\xi^m - \xi^{-m}) = (\xi^h - \xi^{-h})\, E.$$

Ici les nombres

$$\alpha = \frac{\xi^m - \xi^{-m}}{\xi - \xi^{-1}} \quad \text{et} \quad \frac{\xi^h - \xi^{-h}}{\xi - \xi^{-1}}$$

sont des unités (réelles) dans $\mathbf{K}_1$. Au lieu de l'équation ternaire on aura donc l'équation binaire

$$N_1(y+\alpha z) = \pm 1,$$

où N_1 signifie la norme dans $\mathbf{K}_1$. D'après le lemme 2 le nombre α ne peut être du second degré; vu que $m(m-1)$ n'est divisible par p, α est irrationnel. Donc, on peut appliquer le résultat de Thue, et le théorème 2 se trouve démontré.

Il est évident que la même méthode s'appliquera à l'équation plus générale

$$N(x+\beta y+\gamma z) = 1, \tag{T}$$

où β et γ sont des nombres entiers, générateurs du corps $\mathbf{K}$. Nous supposons qu'il n'y a aucune relation entre les nombres β et γ de la forme

$$\tau\beta-\gamma = \lambda. \tag{R}$$

où λ est un nombre dans $\mathbf{K}_1$ et où τ est un nombre dans $\mathbf{K}(\sqrt{p})$ si $p \equiv 1 \pmod 4$ et un nombre rationnel si $p \equiv -1 \pmod 4$.

On conclut de l'équation (T) que

$$x+\beta y+\gamma z = \xi^h E$$

et, en substituant ξ par ξ^{-1},

$$x+\beta' y+\gamma' z = \xi^{-h} E,$$

E étant une unité réelle dans $\mathbf{K}_1$. Par soustraction on obtient ensuite

$$(\beta-\beta')y+(\gamma-\gamma')z = (\xi^h-\xi^{-h})E.$$

Ici les nombres

$$\theta = \frac{\beta-\beta'}{\xi-\xi^{-1}}, \quad \theta_1 = \frac{\gamma-\gamma'}{\xi-\xi^{-1}}, \quad \frac{\xi^h-\xi^{-h}}{\xi-\xi^{-1}}$$

sont des entiers dans $\mathbf{K}_1$; le troisième nombre est une unité. Au lieu de l'équation ternaire (T) on aura donc l'équation binaire

$$N_1(\theta y+\theta_1 z) = \pm 1, \tag{S}$$

où N_1 signifie la norme dans $\mathbf{K}_1$. A cause de la restriction imposée aux nombres β et γ on voit aisément que le nombre $\vartheta = \theta_1\theta^{-1}$ n'est jamais rationnel et qu'il n'appartient pas au corps $\mathbf{K}(\sqrt{p})$ lorsque $p \equiv 1 \pmod 4$. En effet, vu que ϑ est réel, il résulte de

$$\vartheta(\beta-\beta') = \gamma-\gamma'$$

qu'on a une relation

$$\vartheta\beta-\gamma = \vartheta\beta'-\gamma' = \lambda,$$

où λ, étant réel, appartient à $\mathbf{K}_1$. Par conséquent, vu que $p>5$ et que la relation (R) n'est pas satisfaite le nombre $\theta_1\theta^{-1}$ est d'un degré $\geqslant 3$; donc le théorème de Thue s'applique.

Inversement, si la relation (R), ainsi que les conditions y appartenant, sont satisfaites, on obtient en substituant ξ par ξ^{-1}

$$\tau\beta' - \gamma' = \lambda,$$

d'où par soustraction

$$\tau(\beta - \beta') = \gamma - \gamma'.$$

Il en résulte $\tau = \theta_1 \theta^{-1}$ et l'équation (S) deviendra

$$N_1(\theta y + \theta\tau z) = \pm 1.$$

Supposons ensuite que τ est rationnel, $\tau = m_1/m$, où m et m_1 sont des entiers rationnels premiers entre eux. Donc $\eta = \theta/m = \theta_1/m_1$ est un nombre entier dans $\mathbf{K}_1$; et l'équation (S) peut s'écrire

$$N_1(\eta) \cdot (my + m_1 z)^\nu = \pm 1.$$

Donc, pour qu'il ait une infinité de solutions il faut et il suffit que $\eta = \theta/m$ soit une unité dans $\mathbf{K}_1$.

Lorsque τ est un nombre irrationnel dans $\mathbf{K}(\sqrt{p})$, $p \equiv 1 \pmod 4$, on obtiendra un résultat analogue, mais plus compliqué.

Il résulte des raisonnements précédents que nous avons établi le

Théorème 3. *Soient β et γ des nombres entiers, générateurs du corps $\mathbf{K}(\xi)$ jouissant de la propriété suivante : Il n'existe aucune relation de la forme (R), où λ est un nombre dans $\mathbf{K}_1(\xi + \xi^{-1})$, et où τ est un nombre rationnel ou un nombre irrationnel dans $\mathbf{K}(\sqrt{p})$ si $p \equiv 1$ (mod 4).*

Cela étant, l'équation ternaire (T) n'a qu'un nombre fini de solutions en nombres entiers rationnels x, y et z.

Si la relation (R) est satisfaite il peut exister une infinité de solutions pourvu que certaines autres conditions soient remplies.

Prenons par exemple $\beta = \xi$ et $\tau = c + \sqrt{p}$, où c est un nombre entier rationnel. Soient de plus λ un entier quelconque dans $\mathbf{K}_1$ et $\gamma = (c + \sqrt{p})\xi - \lambda$. Alors nous obtenons $\theta = 1$ et $\theta_1 = c + \sqrt{p}$. L'équation (S) aura donc la forme

$$N_1(y + cz + z\sqrt{p}) = [(y + cz)^2 - pz^2]^{\frac{1}{2}\nu} = \pm 1.$$

Par conséquent il y a une infinité de solutions dans ce cas.

§ 3. Equations admettant une infinité de solutions pour $m < n$

6. Le rôle des sous-corps. Dans mon travail que je viens de citer dans le numéro précédant (voir Nagell [7]) j'ai résolu complètement l'équation ternaire

$$N(x + \xi y + \xi^2 z) = 1, \tag{3}$$

ou $\xi = e^{\pi i/4}$. En effet, j'ai établi le résultat suivant :

L'équation (3) *admet une infinité de solutions en nombres entiers rationnels x, y et z, lesquelles sont données par les relations $y^2 - 2x^2 = \pm 1$ et $z = x$; outre ces solutions on a seulement les possibilités suivantes : $x = \pm 1$, $y = z = 0$* et *$x = y = 0$, $z = \pm 1$.*

Cet exemple montre que la possibilité d'un nombre infini de solutions peut être realisée même pour $m<n$. Dans ce cas-ci cela dépend de l'existence du sous-corps quadratique $\mathbf{K}(\sqrt{2})$. Dans le cas général il est facile de voir comment l'existence d'un sous-corps (irrationnel) donne la possibilité de construire des équations à m inconnues possédant une infinité de solutions lorsque $m<n$. Pour plus de simplicité nous prendrons dans la suite toujours $A=1$ dans les équations.

Soient $\mathbf{K}$ un corps algébrique de degré n qui possède le sous-corps $\mathbf{U}$ de degré $\nu \geqslant 2$; si $\nu=2$, $\mathbf{U}$ doit être réel. Soit encore $1, \alpha_2, \alpha_3, ..., \alpha_\nu$ une base d'un anneau entier ordinaire $\mathbf{R}$ dans $\mathbf{U}$. Nous supposons que $m \geqslant \nu+1$.

Considérons maintenant l'équation

$$N(x_1\xi_1+x_2\xi_2+...+x_m\xi_m)=1, \tag{4}$$

où $\xi_1, \xi_2, ..., \xi_m$ sont des nombres linéairement indépendants dans le corps $\mathbf{K}$, tels qu'on ait $\mathbf{K}(\xi_2\xi_1^{-1}, \xi_3\xi_1^{-1}, ..., \xi_m\xi_1^{-1})=\mathbf{K}$. Si nous posons $\xi_1=1, \xi_2=\alpha_2, ..., \xi_\nu=\alpha_\nu$, il est évident que l'équation (4) admet une infinité de solutions. En effet, si l'on choisit d'abord $x_{\nu+1}=x_{\nu+2}=...=x_m=0$, on peut choisir les autres x_i de manière que le nombre $x_1+x_2\alpha_2+...+x_\nu\alpha_\nu$ soit une unité dans l'anneau $\mathbf{R}$. Nous avons donc le

Théorème 4. *A chaque sous-corps de degré ν et de rang positif il existe des équations du type (4) admettant une infinité de solutions, pourvu que $\nu+1 \leqslant m$.*

7. Il reste le problème de trouver les conditions nécessaires et suffisantes pour que l'équation (4) ait une infinité de solutions provenant d'un anneau donné d'un sous-corps donné du corps initial $\mathbf{K}$.

Encore, lesquelles sont les conditions pour que cette équation puisse être réduite à une équation de la forme

$$(a_1x_1+a_2x_2+...+a_hx_h)^\nu=\pm 1, \tag{Q}$$

où $a_1, a_2, ..., a_h$ sont des nombres entiers rationnels, et où ν est un diviseur de n? Dans le numéro 5 nous avons montré l'existence de cette possibilité.

Il se présente la question suivante: Si une équation du type (4) possède une infinité de solutions, est-ce que celles-ci, à part d'un nombre fini de solutions, sont toujours données par les unités d'un anneau d'un sous-corps du corps $\mathbf{K}$? ou eventuellement par les solutions d'une équation de la forme (Q)? La réponse à cette question est sans doute affirmative.

Mes recherches numériques m'ont conduit à proposer l'hypothèse suivante : L'équation (4), où $m \leqslant n-1$, n'admet qu'un nombre fini de solutions si le corps $\mathbf{K}$ est primitif.

Dans la suite nous allons étudier quelques cas particuliers.

§ 4. Corps biquadratiques et formes ternaires

8. Classification des corps biquadratiques. Dans un travail antérieur j'ai donné une classification des corps biquadratiques; voir Nagell [8], p. 351–361. Ensuite, pour des recherches sur les corps biquadratiques du premier rang, il fallait une classification plus détaillée de ces corps-là; voir Nagell [9], p. 345–346, et [4], p. 482–483. Pour plus de clarté nous allons présenter ici une classification détaillée de tous les corps biquadratiques comprenant même ceux du rang 2 et du rang 3. La classification des corps du premier rang est la même qu'auparavant, abstraction faite d'une division de la classe 5 en deux sous-classes. On trouvera l'explication de la classification détaillée des corps du rang 2 et du rang 3 dans le travail [8], p. 351–376.

Supposons que le corps biquadratique **K** admet un sous-corps quadratique engendré par la racine carrée $\sqrt{\Delta}$, où Δ est un nombre entier rationnel qui n'est divisible par aucun carré >1. Alors j'ai établi le résultat suivant (voir [8], théorème 2) :

Il existe un nombre entier générateur du corps **K** *de la forme*

$$\theta = \sqrt{\tfrac{1}{2}(a+b\sqrt{\Delta})}, \tag{5}$$

où a et b sont des entiers rationnels.

Soit U un sous-corps quadratique réel de **K**. Alors, nous désignons par ε l'unité fondamentale de U; et celle-ci sera choisie >1. L'unité fondamentale d'un corps **K** du premier rang sera désignée par η; et il est évident que celle-ci peut être choisie de façon qu'on ait $|\eta|>1$. Pour indiquer le type des corps nous employons les raccourcissements suivants : ϱ signifie le nombre des corps conjugués réels. μ signifie le nombre des sous-corps quadratiques réels. ν signifie le nombre des sous-corps quadratiques imaginaires. **N** signifie que le corps n'est pas un corps de Galois. **A** signifie que le corps est abélien, non-cyclique. **C** signifie que le corps est cyclique. $\mathbf{R}(x^m=1)$ signifie que les racines de l'unité du corps sont les racines de l'équation $x^m-1=0$. **S** signifie que le corps ne contient pas le nombre $\sqrt{3}$. $N(\alpha)$ signifie la norme de α dans **K**. Dans les corps du premier rang on a $\varrho=0$.

Les corps du *premier rang* se répartissent en quinze classes caractérisées de la façon suivante :

Classe 1 : $\mu=\nu=0$. $\mathbf{R}(x^2=1)$. **N**. Corps primitifs.
Classe 2 : $\mu=0$; $\nu=1$. $\mathbf{R}(x^2=1)$. **N**.
Classe 3 : $\mu=0$; $\nu=1$. $\mathbf{R}(x^4=1)$. **N**.
Classe 4 : $\mu=0$; $\nu=1$. $\mathbf{R}(x^6=1)$. **N**.
Classe 5a : $\mu=1$; $\nu=0$. $\mathbf{R}(x^2=1)$. **N**. $\eta=\varepsilon$.
Classe 5b : $\mu=1$; $\nu=0$. $\mathbf{R}(x^2=1)$. **C**. $\eta=\varepsilon$.
Classe 6 : $\mu=1$; $\nu=0$. $\mathbf{R}(x^{10}=1)$. **C**. La classe ne contient qu'un seul corps, savoir le corps engendré par le nombre $e^{2\pi i/5}$. $\eta=\varepsilon$.
Classe 7 : $\mu=1$; $\nu=2$. $\mathbf{R}(x^2=1)$. **A**. $\eta=\varepsilon$.
Classe 8 : $\mu=1$; $\nu=2$. $\mathbf{R}(x^2=1)$. **A**. $\eta=\sqrt{-\varepsilon}$. $\varepsilon\geqslant 2+\sqrt{3}$. $N(\varepsilon)>0$.
Classe 9 : $\mu=1$; $\nu=2$. $\mathbf{R}(x^4=1)$. **A**. $\eta=\varepsilon$. **S**.
Classe 10 : $\mu=1$; $\nu=2$. $\mathbf{R}(x^4=1)$. **A**. $\eta=\sqrt{\varepsilon i}=\tfrac{1}{2}\alpha(1+i)$, où α est un nombre du sous-corps $\mathbf{K}(\varepsilon)$. $\varepsilon\geqslant 5+2\sqrt{6}$. $N(\varepsilon)>0$. **S**.
Classe 11 : $\mu=1$; $\nu=2$. $\mathbf{R}(x^6=1)$. **A**. $\eta=\varepsilon$. **S**.
Classe 12 : $\mu=1$; $\nu=2$. $\mathbf{R}(x^6=1)$. **A**. $\eta=\sqrt{-\varepsilon}$. $\varepsilon\geqslant 4+\sqrt{15}$. $N(\varepsilon)>0$. **S**.
Classe 13 : $\mu=1$; $\nu=2$. $\mathbf{R}(x^8=1)$. **A**. $\eta=\varepsilon=1+\sqrt{2}$. La classe ne contient qu'un seul corps, savoir le corps engendré par le nombre $e^{\pi i/4}$.
Classe 14 : $\mu=1$; $\nu=2$. $\mathbf{R}(x^{12}=1)$. **A**. $\eta=\sqrt{\varepsilon i}=\tfrac{1}{2}(1+\sqrt{3})(1+i)$. La classe ne contient qu'un seul corps, savoir le corps engendré par le nombre $e^{\pi i/6}$.

Il faut observer le fait suivant : Dans les corps appartenant aux classes 7, 8, 9, 10, 11, 12, 13 et 14 le nombre $a^2-\Delta b^2$ est le carré d'un nombre naturel; il n'en est pas ainsi dans les autres classes; dans les classes 5b et 6 le nombre $\Delta(a^2-\Delta b^2)$ est un carré parfait. Ici a, b et Δ sont les nombres dans la formule (5). Comparez le tableau à la page 352 dans [8], où la classe 10 corresponde aux classes 7–14 dans ce mêmoire-ci. Les corps des classes 1, 2, 3, 4, 5a, 5b et 6 correspondent aux corps des classes 1, 4, 5 et 6 dans [8].

Passons ensuite aux corps du *second rang*. Ces corps correspondent aux corps des deux classes 2 et 7 dans [8]. Il n'y a aucun corps de Galois parmi ces corps. On a $\nu=0$; donc il n'y a pas de racines de l'unité $\neq \pm 1$. Nous considérons seulement les corps conjuguées réels. Par ξ, η nous désignons une base des unités. Les corps en question se répartissent en quatre classes.

Classe 15 : $\mu=0$. Corps primitifs.
Classe 16 : $\mu=1$. $\xi=\varepsilon, \eta=E$.
Classe 17 : $\mu=1$. $\xi=\sqrt{\varepsilon}, \eta=E$.
Classe 18 : $\mu=1$. $\xi=\varepsilon, \eta=\sqrt{E\varepsilon}$.

Ici ε signifie l'unité fondamentale du sous-corps quadratique, $\varepsilon>1$. Soit θ le nombre réel générateur du corps défini par (5). E signifie une unité dans $\mathbf{K}(\theta)$ jouissant des propriétés suivantes : E est du quatrième degré. On a $E>1$ et $EE'=+1$, où E' s'obtient de E en substituant θ par $-\theta$. E n'est pas de la forme α^m, où α appartient à $\mathbf{K}(\theta)$ et où $m\geqslant 2$. Le nombre $a^2-\Delta b^2$ est négatif.

Considérons finalement les corps du *troisième rang*. Ces corps correspondent aux corps des classes 3, 8, 9 et 11 dans [8]. Nous les divisions en quatre classes.

Classe 19 : $\mu=\nu=0$. Corps primitifs.**N**.
Classe 20 : $\mu=1, \nu=0$.**N**.
Classe 21 : $\mu=1, \nu=0$. **C**.
Classe 22 : $\mu=3, \nu=0$. **A**.

Le nombre $a^2-\Delta b^2$ est positif, et dans la classe 22 celui-ci est un carré parfait; dans la classe 21 le nombre $\Delta(a^2-\Delta b^2)$ est un carré parfait.

Pour la démonstration de tous ces résultats je renvoie à mon travail [8].

Dans un corps $\mathbf{K}(\theta)$, où θ est défini par (5) tout nombre entier ξ est évidemment de la forme

$$\xi=\frac{1}{s}[x_1+x_2\sqrt{\Delta}+x_3\theta+x_4\theta\sqrt{\Delta}],$$

où s est un nombre naturel fixe qui dépend du corps, et où x_1, x_2, x_3 et x_4 sont des nombres entiers rationnels.

9. Équations ternaires. Cas où $\mu>0$. Supposons qu'il y a dans le corps biquadratique $\mathbf{K}$ un sous-corps quadratique reél engendré par le nombre $\sqrt{\Delta}$. Alors, nous savons d'après le numéro 6 qu'il existe des équations ternaires, construites sur le corps, admettant un nombre infini de solutions. Comme exemple on peut prendre l'équation ternaire

$$N(x+y\sqrt{\Delta}+z\theta)=1,$$

où θ est un nombre entier, générateur du corps $\mathbf{K}$. En y posant $z=0$ on aura l'équation

$$(x^2-\Delta y^2)^2=1.$$

De l'autre côté on peut construire des équations ternaires qui ne possèdent aucune solution. En effet, soit

$$\theta=\sqrt{\tfrac{1}{2}(a+b\sqrt{\Delta})}$$

un nombre entier, générateur de $\mathbf{K}$, et considérons l'équation ternaire

$$N(qx+\sqrt{\Delta}y+2q\theta z)=1,$$

où q est un nombre premier $\equiv 1 \pmod 4$, qui ne divise pas ab et pour lequel Δ est un non-reste quadratique. Cela étant, l'équation ternaire est impossible modulo q. Car, celle-ci peut s'écrire sous la forme

$$(q^2x^2+\Delta y^2-2q^2az^2)^2-\Delta(2qxy-2q^2bz^2)^2=1.$$

Il en résulte $\Delta^2y^4\equiv 1 \pmod q$. Or, les nombres $\pm\Delta$ sont des non-restes quadratiques modulo q.

10. Équations ternaires. Cas où $\mu=0$. Ce cas est réalisé dans tous les corps des classes 1, 2, 3, 4, 15 et 19 et seulement dans ces corps. Les corps des classes 1, 15 et 19 sont primitifs. Les corps de la classe 1 ont le rang 1, et par conséquent on peut appliquer le théorème de Chabauty du numéro 4. Il en résulte que, pour les corps de la classe 1, toute équation ternaire n'admet qu'un nombre fini de solutions. Nous allons compléter ce résultat en établissant le

Théorème 5. *Soit* $\mathbf{K}$ *un corps appartenant à l'une des classes 1, 2, 3, ou 4. Soient* $\gamma_1, \gamma_2, \gamma_3$ *trois nombres entiers dans* $\mathbf{K}$ *linéairement indépendants. Alors, l'équation ternaire*

$$N(\gamma_1x_1+\gamma_2x_2+\gamma_3x_3)=A, \tag{6}$$

où A est un nombre entier rationnel, n'admet qu'un nombre fini de solutions.

Démonstration. Nous avons besoin du lemme suivant dû à Chabauty [6] :

Soit $\mathbf{K}$ *un corps algébrique de degré n, et soit $\omega_1, \omega_2, \ldots, \omega_n$ une base des entiers de* $\mathbf{K}$. *Désignons par (N) la variété algébrique définie par la relation*

$$N(x_1\omega_1+x_2\omega_2+\ldots+x_n\omega_n)=1.$$

Alors, la condition nécessaire et suffisante pour qu'il existe une courbe algébrique, à coefficients rationnels, contenant une infinité de points entiers de (N) est que $\mathbf{K}$ *contienne un sous-corps quadratique réel.*

C'est à l'aide de ce lemme que Chabauty a démontré son théorème cité dans le numéro 4.

Le théorème 4 étant déjà établi pour la classe 1, il suffit de considérer le cas où $\mathbf{K}$ possède un sous-corps quadratique imaginaire engendré par $\sqrt{\Delta}$, $\Delta<0$. Il suffit évidemment de démontrer le théorème pour l'équation

$$N(x+\alpha y+\beta z)=1, \tag{7}$$

où les entiers 1, α, β sont linéairement indépendants. Lorsque θ est défini par (5) nous avons

$$\alpha=c+c_1\sqrt{\Delta}+c_2\theta+c_3\theta\sqrt{\Delta},$$

$$\beta=d+d_1\sqrt{\Delta}+d_2\theta+d_3\theta\sqrt{\Delta},$$

où c, c_1, c_2, c_3, d, d_1, d_2 et d_3 sont des nombres rationnels qu'on peut rendre entiers en les multipliant par un nombre naturel fixe s. Posons

$$\xi=x+\alpha y+\beta z$$

et désignons par ξ' le nombre conjugué qu'on obtient de ξ en substituant θ par $-\theta$. Posons ensuite

$$X=x+yc+zd, \quad Y_1=yc_1+zd_1,$$

$$Y_2=yc_2+zd_2, \quad Y_3=yc_3+zd_3.$$

Alors, on obtient pour le produit $\xi\xi'$ l'expression

$$(X+Y_1\sqrt{\Delta})^2-\theta^2(Y_2+Y_3\sqrt{\Delta})^2.$$

En vertu de (7) ce nombre est une unité dans le sous-corps $\mathbf{K}(\sqrt{\Delta})$. Cette unité est $=\pm 1$ si Δ est différent de -1 et de -3. Lorsque $\Delta=-1$ on a les quatre possibilités ± 1 et $\pm i$. Lorsque $\Delta=-3$ on a les six possibilités ± 1, $\pm\varrho$ et $\pm\varrho^2$, où $\varrho^2+\varrho+1=0$.

Si l'unité a la valeur ± 1 nous obtenons le système suivant

$$X^2+\Delta Y_1^2-a(Y_2^2+\Delta Y_3^2)-2b\Delta Y_2Y_3=\pm 1, \tag{8}$$

$$2XY_1-2aY_2Y_3-bY_2^2-b\Delta Y_3^2=0. \tag{9}$$

En éliminant X entre ces deux équations on aura une relation entre y et z seulement

$$F(y,z)=0, \tag{10}$$

où F est un polynome en y et z à coefficients rationnels et du quatrième degré. Tous les points entiers de cette courbe algébrique se trouvent sur la surface

$$N(x_1\omega_1+x_2\omega_2+x_3\omega_3+x_4\omega_4)=1,$$

où $\omega_1, \omega_2, \omega_3, \omega_4$ désigne une base des entiers de $\mathbf{K}$. Par conséquent, le lemme de Chabauty s'applique, et il en résulte que la courbe (10) n'admet qu'un nombre fini de points entiers.

Lorsque $\Delta=-1$ on aura encore à traiter la possibilité $\xi\xi'=\pm i$. Dans ce cas il faut seulement remplacer ± 1 par 0 dans l'équation (8) et 0 par ± 1 dans l'équation (9).

Lorsque $\Delta=-3$ on aura encore à traiter les possibilités $\xi\xi'=\pm\varrho$ et $=\pm\varrho^2$. Dans ces cas il faut seulement remplacer les termes à droite dans les équations (8) et (9) par $\pm\frac{1}{2}$.

Il est évident que la démonstration dans ces cas sera tout-à-fait analogue, et le théorème se trouve ainsi démontré dans tous les cas.

Dans un prochain travail nous allons montrer comment ce résultat peut être généralisé.

§ 5. Corps cyclotomiques et formes quaternaires

11. Résultats antérieurs dans les cas binaires et ternaires. Les corps cyclotomiques $\mathbf{K}(\xi)$ ont beaucoup de propriétés qui facilitent les raisonnements et les calculs dans leurs domaines. Pour cette raison il est souvent favorable de choisir de tels corps pour objet d'étude.

Dans des travaux antérieurs nous avons établi quelques théorèmes sur les formes binaires construites sur un type de corps cyclotomiques; voir Nagell [4], § 6. Nous avons, entre autres, démontré le théorème suivant :

Soient $n=p^\alpha$, où p est un nombre premier impair, et ξ une racine primitive n-ième de l'unité. De plus, soit θ un nombre entier, générateur du corps $\mathbf{K}(\xi)$, et considérons la forme binaire de degré $\varphi(n)$

$$G(x, y) = N(x-\theta y),$$

où N signifie la norme dans $\mathbf{K}(\xi)$. Désignons par M le nombre de solutions de l'équation

$$G(x, y) = 1 \tag{11}$$

en nombres entiers rationnels x et y. Alors, M est au plus égal à 6. Pour qu'on ait $M \geqslant 4$ il faut et il suffit que $G(x, y)$ soit équivalente à une forme $N(x-\eta y)$, où η est une unité de degré $\varphi(n)$ dans $\mathbf{K}(\xi)$. Le cas $M=6$ est possible pour un nombre fini de classes de formes, p. ex. pour la classe représentée par

$$F_n(x, y) = N(x-\xi y).$$

Si $G(x, y)$ n'est pas équivalente à une forme du type $N(x-\eta y)$ on a $M=2$. Pour les solutions y de (11) il n'y a que les trois possibilités $y=0$, $+1$ et -1. On peut toujours déterminer toutes les solutions de (11) lorsque θ est donné.

Vu que le polynome $G(x, y)$ est définite il est trivial que le nombre de solutions de (11) est fini. Cependant, il n'est pas trivial que l'équation ternaire

$$N(x+\xi y+\xi^m z) = 1$$

n'admet qu'un nombre limité de solutions lorsque $p>5$ et $1<m<p$. Nous venons d'établir ce résultat dans le numéro *5*.

12. Cas quaternaire. Nous allons ajouter aux résultats précédents la proposition suivante :

Théorème 6. *Soit ξ une racine primitive p-ième de l'unité où p est un nombre premier $\geqslant 7$. Alors l'équation quaternaire*

$$N(x_1\xi+x_2\xi^2+x_3\xi^3+x_4\xi^4)=1 \tag{12}$$

n'admet qu'un nombre fini de solutions en nombres entiers rationnels x_1, x_2, x_3, x_4.

Démonstration. Il est bien connu que toute unité dans $\mathbf{K}(\xi)$ est égale au produit d'une unité réelle par une puissance de ξ; voir Hilbert [10], p. 335. Par conséquent, il résulte de l'équation (12) qu'on a

$$x_1\xi+x_2\xi^2+x_3\xi^3+x_4\xi^4=\xi^h E, \tag{13}$$

où E est une unité réelle, et où h doit parcourir toutes les classes de restes modulo p; nous choisissons pour h les valeurs suivantes :

$$h=0, 1, 2, \ldots, \tfrac{1}{2}(p-1), \ -1, \ -2, \ldots, \ -\tfrac{1}{2}(p-1).$$

L'équation (13) peut s'écrire

$$x_1\xi^{1-h}+x_2\xi^{2-h}+x_3\xi^{3-h}+x_4\xi^{4-h}=E,$$

d'où, en substituant ξ par ξ^{-1},

$$x_1\xi^{h-1}+x_2\xi^{h-2}+x_3\xi^{h-3}+x_4\xi^{h-4}=E.$$

Donc par soustraction

$$x_1(\xi^{h-1}-\xi^{1-h})+x_2(\xi^{h-2}-\xi^{2-h})+x_3(\xi^{h-3}-\xi^{3-h})+x_4(\xi^{h-4}-\xi^{4-h})=0. \tag{14}$$

Il faut distinguer un certain nombre de cas selon la valeur de h.

Cas I : $h=0$.
Dans ce cas nous aurons de (14)

$$x_1(\xi-\xi^{-1})+x_2(\xi^2-\xi^{-2})+x_3(\xi^3-\xi^{-3})+x_4(\xi^4-\xi^{-4})=0,$$

d'où, en multipliant par ξ^4,

$$x_1(\xi^5-\xi^3)+x_2(\xi^6-\xi^2)+x_3(\xi^7-\xi)+x_4(\xi^8-1)=0.$$

Il est évident que cette relation entraîne $x_1=x_2=x_3=x_4=0$, pourvu que $p>7$. Pour $p=7$ on aura $x_1=x_2=0$ et $x_3=x_4=\pm 1$.

Cas II : $h=1$.
Dans ce cas nous obtenons de (14), en multipliant par ξ^3, la relation

$$x_2(\xi^4-\xi^2)+x_3(\xi^5-\xi)+x_4(\xi^6-1)=0.$$

Cette relation entraîne évidemment $x_2=x_3=x_4=0$, $x_1=\pm 1$.

Cas III : $h=2$.
Dans ce cas nous aurons de (14) après avoir multiplié avec ξ^2 :

$$(x_1-x_3)(\xi^3-\xi)-x_4(\xi^4-1)=0.$$

Il faut donc qu'on ait $x_1 = x_3$ et $x_4 = 0$. Alors, l'équation (12) peut s'écrire

$$N(x_2 + x_1(\xi + \xi^{-1})) = 1,$$

où le nombre $\xi + \xi^{-1}$ est de degré $\frac{1}{2}(p-1)$. D'après le théorème de Thue le nombre de solutions est fini :

Cas IV : $h = 3$.
Si nous multiplions l'équation (14) par ξ^2 nous obtenons

$$x_1(\xi^4 - 1) + (x_2 - x_4)(\xi^3 - \xi) = 0.$$

Cette relation entraîne que $x_1 = 0$ et $x_2 = x_4$. Alors, l'équation (12) peut s'écrire

$$N(x_3 + x_2(\xi + \xi^{-1})) = 1.$$

Ainsi, d'après le théorème de Thue le nombre de solutions est fini.

Cas V : $h = 4$.
Dans ce cas il résulte de l'équation (14) après la multiplication avec ξ^3 :

$$x_1(\xi^6 - 1) + x_2(\xi^5 - \xi) + x_3(\xi^4 - \xi^2) = 0.$$

Cette relation entraîne $x_1 = x_2 = x_3 = 0$ et $x_4 = \pm 1$.

Cas VI : $5 \leqslant h \leqslant \frac{1}{2}(p-1)$.
En multipliant l'équation (14) par ξ^{h-1} nous aurons

$$x_1(\xi^{2h-2} - 1) + x_2(\xi^{2h-3} - \xi) + x_3(\xi^{2h-4} - \xi^2) + x_4(\xi^{2h-5} - \xi^3) = 0.$$

Vu que $2h - 2 \leqslant p - 3$ et que $2h - 5 \geqslant 5$ on en conclut $x_1 = x_2 = x_3 = x_4 = 0$.
Passons maintenant aux valeurs négatives de h.

Cas VII : $1 \leqslant -h \leqslant \frac{1}{2}(p-11)$.
En multipliant l'équation (14) par ξ^{4-h} nous aurons

$$x_4(1 - \xi^{8-2h}) + x_3(\xi - \xi^{7-2h}) + x_2(\xi^2 - \xi^{6-2h}) + x_1(\xi^3 - \xi^{5-2h}) = 0.$$

Vu que $8 - 2h \leqslant p - 3$ on en conclut $x_1 = x_2 = x_3 = x_4 = 0$.
Il reste encore à examiner les valeurs suivantes de h :

$$-\tfrac{1}{2}(p-9),\ -\tfrac{1}{2}(p-7),\ -\tfrac{1}{2}(p-5),\ -\tfrac{1}{2}(p-3),\ -\tfrac{1}{2}(p-1).$$

Cas VIII : $h = -\frac{1}{2}(p-9)$.
Pour raccourcir nous posons $\nu = \frac{1}{2}(p-1)$. En multipliant l'équation (14) par ξ^ν nous aurons :

$$x_4(1 - \xi^{p-1}) + x_3(\xi - \xi^{p-2}) + x_2(\xi^2 - \xi^{p-3}) + x_1(\xi^3 - \xi^{p-4}) = 0.$$

Vu que $\xi^{p-1} = -\xi^{p-2} - \dots - \xi - 1$ il vient

$$x_4(2+\xi+\xi^2+\dots+\xi^{p-3}+\xi^{p-2})+x_3(\xi-\xi^{p-2})+x_2(\xi^2-\xi^{p-3})+x_1(\xi^3-\xi^{p-4})=0.$$

Il en résulte évidemment $x_4=0$ et ensuite $x_1=x_2=x_3=0$.

Cas IX : $h=-\frac{1}{2}(p-7)$.

En multipliant l'équation (14) par ξ^ν nous aurons

$$x_1(\xi^2-\xi^{p-3})+x_2(\xi-\xi^{p-2})+x_3(1-\xi^{p-1})+x_4(\xi^{p-1}-1)=0.$$

Comme dans le cas précédent nous obtenons :

$$x_1(\xi^2-\xi^{p-3})+x_2(\xi-\xi^{p-2})+(x_3-x_4)(2+\xi+\xi^2+\dots+\xi^{p-3}+\xi^{p-2})=0.$$

On en conclut d'abord $x_3=x_4$, et ensuite $x_1=x_2=0$, donc $x_3=x_4=\pm 1$.

Cas X : $h=-\frac{1}{2}(p-5)$.

Par la même méthode que dans les cas précédents nous aurons

$$x_1(\xi-\xi^{p-2})+x_2(1-\xi^{p-1})+x_3(\xi^{p-1}-1)+x_4(\xi^{p-2}-\xi)=0,$$

d'où
$$(x_4-x_1)(\xi^{p-2}-\xi)+(x_3-x_2)(\xi^{p-1}-1)=0.$$

Il en résulte $x_1=x_4$ et $x_2=x_3$; et l'équation (12) peut s'écrire

$$N(x_2-x_1+x_1(\xi+\xi^{-1}))=1.$$

D'après le théorème de Thue le nombre de solutions est fini.

Cas XI : $h=-\frac{1}{2}(p-3)$.

Dans ce cas-ci nous aurons d'une façon analogue :

$$x_1(1-\xi^{p-1})+x_2(\xi^{p-1}-1)+x_3(\xi^{p-2}-\xi)+x_4(\xi^{p-3}-\xi^2)=0$$

et ensuite

$$(x_1-x_2)(2+\xi+\xi^2+\dots+\xi^{p-2})+x_3(\xi^{p-2}-\xi)+x_4(\xi^{p-3}-\xi^2)=0.$$

Il en résulte $x_1=x_2$ et en conséquence $x_3=x_4=0$, ce qui entraîne $x_1=x_2=\pm 1$.

Cas XII : $h=-\frac{1}{2}(p-1)$.

Par la même méthode nous aurons

$$x_1(\xi^{p-1}-1)+x_2(\xi^{p-2}-\xi)+x_3(\xi^{p-3}-\xi^2)+x_4(\xi^{p-4}-\xi^3)=0.$$

En y remplaçant ξ^{p-1} par $-1-\xi-\xi^2-\dots-\xi^{p-2}$ on voit qu'il faut que $x_1=0$. Il en résulte que $x_2=x_3=x_4=0$, si $p>7$. Pour $p=7$ on aura $x_1=x_2=x_3=0$ et $x_4=\pm 1$.

Par conséquent, le théorème 6 se trouve démontré dans tous les cas.

Il est évident que l'équation plus générale

$$N(x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3 + x_4\alpha_4) = A,$$

où α_1, α_2, α_3 et α_4 sont des entiers dans $\mathbf{K}(\xi)$ tels que $\mathbf{K}(\alpha_2\alpha_1^{-1}, \alpha_3\alpha_1^{-1}, \alpha_4\alpha_1^{-1}) = \mathbf{K}(\xi)$, peut être traitée avec la même méthode. Pourtant, nous y renonçons vu que cela entraînerait un travail trop étendu.

INDEX BIBLIOGRAPHIQUE

1. Skolem, Th., Diophantische Gleichungen, *Ergebnisse der Mathematik*, Bd. 5, Berlin 1938.
2. Nagell, T., Zur algebraischen Zahlentheorie, *Mathem. Zeitschrift*, Bd. 34, Berlin 1931.
3. Hasse, H., Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II: Reziprozitätsgesetze, *Jahresber. d. Deutschen Mathem. Vereinigung*, Bd. 36, Berlin 1930.
4. Nagell, T., Sur les représentations de l'unité par les formes biquadratiques du premier rang, *Arkiv för matematik*, Bd. 5, nr. 33, Stockholm 1965.
5. Siegel, C., Approximation algebraischer Zahlen, *Mathem. Zeitschrift*, Bd. 10, Berlin 1921.
6. Chabauty, C., Sur certaines équations diophantiques ternaires, *Comptes rendus Acad. Sci.*, t. 202, Paris 1936, p. 2117–2119.
7. Nagell, T., Sur les discriminants des nombres algébriques, *Arkiv för matematik*, Bd. 7, nr. 19, Stockholm 1967.
8. Nagell, T., Sur quelques questions dans la théorie des corps biquadratiques, *Arkiv för matematik*, Bd. 4, nr. 26, Stockholm 1961.
9. Nagell, T., Sur une propriété des unités d'un corps algébrique, *Arkiv för matematik*, Bd. 5, nr. 25, Stockholm 1964.
10. Hilbert, D., Die Theorie der algebraischen Zahlkörper, *Jahresber. d. Deutschen Math. Vereinigung*, Bd. 4, Berlin 1898.
11. Fricke, R., *Lehrbuch der Algebra*, Bd. 3, Braunschweig 1928.
12. Nagell, T., *Introduction to number theory*, New York 1951.
13. Nagell, T., Contributions à la théorie des corps et des polynomes cyclotomiques, *Arkiv för matematik*, Bd. 5, nr. 10, Stockholm 1963.

Tryckt den 29 december 1967

Uppsala 1967. Almqvist & Wiksells Boktryckeri AB