ARKIV FÖR MATEMATIK Band 7 nr 19

1.67 05 4 Communique le 8 Mars 1967

Sur les discriminants des nombres algébriques

Par Trygve Nagell

§ 1. Quelques propriétés arithmétiques des formes décomposables

1. Dans ce travail les nombres algébriques sont toujours supposés entiers.

Supposons donné le corps algébrique **K** du n-ième degré, $n \geqslant 2$. Désignons par N la norme dans ce corps. Soient $\alpha_1, \alpha_2, \ldots, \alpha_n$ des nombres entiers dans **K** linéairement indépendants. Considérons l'équation du n-ième degré

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

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

2. Soient $\alpha_1, \alpha_2, \ldots, \alpha_m$ des nombres algébriques, linéairement indépendants tels que le corps $\mathbf{K}(\alpha_1, \alpha_2, \ldots, \alpha_m)$ soit du n-ième degré. Alors, le problème de résoudre l'équation du n-ième degré

$$N(x_1 \alpha_1 + x_2 \alpha_2 + \ldots + x_m \alpha_m) = A \tag{2}$$

en nombres entiers rationnels $x_1, x_2, \ldots, x_m$, est beaucoup plus difficile si $m < n$. Si $m = 2$ et $n \geqslant 3$ on sait que le nombre de solutions est fini (théorème d'Axel Thue). Si $m = 2$ et $n = 3$ ou $= 4$ on sait déterminer toutes les solutions dans des cas particuliers; voir p. ex. Skolem [1], p. 108–114, et Nagell [3], p. 186.

Une question naturelle se pose : Lesquelles sont les conditions pour que l'équation (2) admette un nombre infini de solutions lorsque $m < n$? S'il y a un sous-corps, qui n'est pas du second degré et imaginaire, il existe toujours des équations du type (2) admettant une infinité de solutions pour $m < n$. Nous allons en donner un exemple dans la Remarque 4 à la fin de ce mémoire.

Skolem a traité l'équation (2) dans le cas où **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 Chabauty [4] :

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

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

$$N(\alpha x + \beta y + \gamma z) = A, \tag{3}$$

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

Le rang r indique le nombre d'unités dans un système fondamental d'unités. La méthode de démonstration ne permet pas de décider sur la solubilité ni de déterminer toutes les solutions, sauf dans des cas d'exception.

3. Les résultats que nous venons de citer sont, à ce que je sache, les seuls connus jusqu'ici sur les équations du type (2). Il est d'ailleurs possible d'obtenir, par d'autres méthodes, des résultats sur certaines équations ternaires. Nous allons les publier prochainement. Pour le moment nous nous contentons d'établir le résultat particulier que voici :

Théorème 1. *Soit ξ une racine primitive p-ième de l'unité, p étant un nombre premier > 5. Alors, l'équation ternaire*

$$N(x + \xi y + \xi^2 z) = 1 \tag{4}$$

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

Vu que le corps $\mathbf{K}(\xi)$ n'est pas primitif, ce résultat n'est pas compris dans le théorème de Chabauty.

Démonstration. En profitant du Lemme 2 dans [2], p. 518, nous aurons de (4)

$$x + \xi y + \xi^2 z = \xi^h E,$$

où E est une unité réelle dans le corps $\mathbf{K}(\xi + \xi^{-1})$, et où h est un nombre entier rationnel qui n'est pas divisible par p. En passant de ξ à ξ^{-1} nous aurons

$$x + \xi^{-1} y + \xi^{-2} z = \xi^{-h} E.$$

Il en résulte que

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

Ici le nombre à droite est une unité dans $\mathbf{K}(\xi + \xi^{-1})$. Si N_1 signifie la norme dans ce corps, on en conclut que

$$N_1[y + z(\xi + \xi^{-1})] = \pm 1. \tag{5}$$

Vu que $p > 5$ le degré du nombre $\xi + \xi^{-1}$ est au moins égal à 3. Donc, d'après le théorème de Thue, l'équation (5) n'a qu'un nombre limité de solutions. Cela démontre le Théorème 1.

Il est évident comment on peut généraliser ce résultat.

Nous avons donné un aperçu sur certaines propriétés arithmétiques des formes décomposables, représentables comme la norme d'un nombre algébrique variable. Le but de ce travail est l'étude des discriminants de nombres algébriques. Pour la théorie des discriminants les formes décomposables joue un grand rôle.

§ 2. Sur les nombres algébriques entiers de discriminant donné

4. Nous comprenons par le discriminant du nombre algébrique entier α le discriminant dans le corps engendré par α.

Dans un mémoire antérieur nous avons, entre autres, commencé une étude sur les nombres algébriques de discriminant donné; voir Nagell [5], § 5. Du Théorème 16 de ce mémoire il résulte :

Théorème 2. *Désignons par $\mathbf{\Phi}$ le domaine consistant de tous les nombres entiers du second degré. Soit α un nombre de $\mathbf{\Phi}$ qui possède le discriminant D. Alors, tout nombre dans $\mathbf{\Phi}$ ayant le discriminant D est nécessairement de la forme $\pm\alpha+k$, où k est un nombre entier rationnel quelconque.*

Comparez aussi le Théorème 18 du mémoire [5].

On doit observer le fait suivant de la théorie des corps quadratiques. Pour que le nombre entier rationnel D soit le discriminant d'un nombre entier du second degré il faut et il suffit que D satisfasse aux conditions suivantes : 1°) D est ou $\equiv 1$ ou $\equiv 0 \pmod 4$; 2°) $\sqrt{D}$ est irrationnel.

Lorsque le degré du nombre algébrique est >2 la première de ces conditions est toujours nécessaire; la seconde n'est pas nécessaire.

5. Il y a aussi un résultat analogue pour les nombres du troisième degré. En effet, il résulte du Théorème 19 du même mémoire [5] :

Théorème 3. *Désignons par $\mathbf{\Phi}$ le domaine consistant de tous les nombres entiers du troisième degré. Soit D le discriminant d'un nombre de $\mathbf{\Phi}$. Alors il existe dans $\mathbf{\Phi}$ un nombre fini de nombres : $\alpha_1, \alpha_2, \dots, \alpha_m$, jouissant de la propriété suivante : Tout nombre dans $\mathbf{\Phi}$ ayant le discriminant D est de la forme $\pm\alpha_i+k$, $i=1, 2, \dots, m$, où k est un nombre entier rationnel quelconque.*

Lorsque le discriminant D est négatif, on peut souvent, par un nombre fini d'opérations, déterminer un système pareil de nombres $\alpha_1, \alpha_2, \dots, \alpha_m$. Il faut observer que les nombres α_i n'appartiennent pas nécessairement au même corps cubique.

Comparez aussi les Théorèmes 19 bis et 20 du même travail.

6. Considérons maintenant les nombres du n-ième degré. Soit $\mathbf{K}$ un corps algébrique de degré n. Soient $1, \omega_1, \omega_2, \dots, \omega_{n-1}$ une base des entiers de $\mathbf{K}$ et D^* le discriminant de ce corps. Si θ est un nombre entier quelconque qui engendre le corps, on a

$$\theta = x_0 + x_1\omega_1 + \dots + x_{n-1}\omega_{n-1},$$

où les x_i sont des entiers rationnels variables. Alors on a

$$D(\theta) = D(x_1\omega_1 + \dots + x_{n-1}\omega_{n-1}) = [F(x_1, x_2, \dots, x_{n-1})]^2 \cdot D^*,$$

où F est une forme primitive des $n-1$ variables $x_1, x_2, \dots, x_{n-1}$, de degré $\frac{1}{2}n(n-1)$ à coefficients entiers rationnels. F est le produit de formes linéaires dont les coefficients appartiennent au corps de Galois engendré par les n conjugués de θ. Si $\mathbf{K}$ est un corps primitif, F est irréductible dans le corps rationnel. Si $\mathbf{K}$ admet un sous corps irrationnel F est réductible.

Soit D le discriminant d'un nombre θ dans $\mathbf{K}$. Pour cela il faut que D soit de la forme A^2D^*, où A est un nombre naturel. Pour déterminer tous les nombres dans $\mathbf{K}$ ayant le discriminant D on aura à résoudre l'équation

$$F(x_1, x_2, \ldots, x_{n-1}) = \pm A \tag{6}$$

en nombres entiers rationnels $x_1, x_2, \ldots, x_{n-1}$. Si F est irréductible dans le corps rationnel et si $n \geqslant 4$, nos connaissances sur les équations de ce type sont extrèmement limitées. Même si F est réductible il est difficile de voir comment on puisse obtenir des résultats sur les solutions de (6), sauf dans des cas particuliers.

Dans les numéros suivants nous allons traiter le cas de $n=4$ avec des méthodes variées.

Remarque 1. Il est possible de reconnaître, par un nombre fini d'opérations, si un nombre entier donné D peut être le discriminant d'un nombre algébrique entier ou non. En effet, si nous posons $D = D^*h^2$, où h est un nombre naturel, nous pouvons déterminer, à l'aide des inégalités de Minkowski, tous les corps algébriques ayant le discriminant D^*. Dans tous ces corps on aura ensuite à déterminer tous les anneaux de discriminant D^*h^2. Comparez Nagell [5], § 3.

D'apres un résultat de L. Stickelberger le discriminant d'un nombre algébrique doit être ou $\equiv 1$ ou $\equiv 0$ (mod. 4); voir Stickelberger [9] et aussi Schur [10].

§ 3. Les discriminants dans les corps biquadratiques

7. Passons maintenant aux corps du quatrième degré. Supposons d'abord que le corps soit primitif et de rang 1. Dans ce cas nous pouvons appliquer le théorème de Chabauty, cité plus haut dans le numéro 2.

Alors nous aurons le résultat :

Théorème 4. *Désignons par Φ le domaine consistant de tous les nombres entiers du quatrième degré qui engendrent des corps primitifs du premier rang. Soit D le discriminant d'un nombre de Φ. Alors il existe dans Φ un nombre fini de nombres : $\alpha_1, \alpha_2, \ldots, \alpha_m$, jouissant de la propriété suivante : Tout nombre dans Φ ayant le discriminant D est de la forme $\pm\alpha_i + k$, $i = 1, 2, \ldots, m$, où k est un nombre entier rationnel quelconque.*

Cependant, la méthode de démonstration ne donne aucun moyen pour déterminer les nombres α_i.

8. Considérons ensuite le cas des corps biquadratiques qui admettent un sous-corps quadratique imaginaire. Nous allons établir le résultat suivant :

Théorème 5. *Désignons par Φ le domaine de tous les nombres entiers du quatrième degré qui engendrent des corps admettant au moins un sous-corps quadratique imaginaire. Soit D le discriminant d'un nombre de Φ. Alors il existe dans Φ un nombre fini de nombres : $\alpha_1, \alpha_2, \ldots, \alpha_m$, jouissant de la propriété suivante : Tout nombre dans Φ ayant le discriminant D est de la forme $\pm\alpha_i + k$, $i = 1, 2, \ldots, m$, où k est un nombre entier rationnel quelconque. Par un nombre fini d'opérations on peut déterminer un système pareil de nombres $\alpha_1, \alpha_2, \ldots, \alpha_m$.*

Il faut observer que les nombres α_i n'appartiennent pas nécessairement au même corps biquadratique. Les corps dont il s'agit sont du premier rang.

Démonstration. Soit θ un nombre du domaine $\mathbf{\Phi}$, et soit $\mathbf{U}$ un sous-corps quadratique imaginaire de $\mathbf{K}(\theta)$. Supposons que $\mathbf{U}$ est engendré par la racine $\sqrt{-\Delta}$, où Δ est un nombre naturel qui n'est divisible par aucun carré >1. Supposons que θ est racine de l'équation

$$x^4-px^3+qx^2-rx+s=0, \tag{7}$$

où les coefficients p, q, r et s sont des nombres entiers rationnels. Donc θ est racine d'une équation quadratique $x^2-ax+b=0$ irréductible dans $\mathbf{U}$, où a et b sont des nombres entiers dans $\mathbf{U}$. Soit θ'' l'autre racine de cette équation quadratique.

Supposons d'abord que $-\Delta$ n'est pas $\equiv 1 \pmod{4}$. Alors nous avons

$$\theta+\theta''=u+v\sqrt{-\Delta}, \quad \theta\theta''=u_1+v_1\sqrt{-\Delta}, \tag{8}$$

où u, v, u_1 et v_1 sont des entiers rationnels. Pour les coefficients de l'équation (7) on aura les relations

$$\left.\begin{aligned} p&=2u, \quad q=u^2+\Delta v^2+2u_1,\\ r&=2uu_1+2\Delta vv_1, \quad s=u_1^2+\Delta v_1^2. \end{aligned}\right\} \tag{9}$$

Pour le discriminant D de θ on obtiendra la formule

$$D=16\Delta^2 D_1 D_2, \tag{10}$$

$$D_1=(u^2-\Delta v^2-4u_1)^2+\Delta(2uv-4v_1)^2, \tag{11}$$

$$D_2=(uvv_1-v_1^2-u_1v^2)^2. \tag{12}$$

Dans le cas où $-\Delta$ est $\equiv 1 \pmod 4$ on aura seulement à remplacer, dans les formules (8)–(12), les nombres u, v, u_1 et v_1 par $\frac{1}{2}u$, $\frac{1}{2}v$, $\frac{1}{2}u_1$ et $\frac{1}{2}v_1$.

Pour la démonstration de toutes ces formules je renvoie à Nagell [2], § 3.

Lorsque D est donné, il résulte de (10) que les nombres (positifs) Δ, D_1 et D_2 sont limités. Il suffit de supposer que p a une des valeurs 0 ou 2; donc $u=0$ ou $=1$; comparez [2], p. 484–485. Si nous posons

$$u^2-\Delta v^2-4u_1=k, \tag{13}$$

$$2uv-4v_1=k_1, \tag{14}$$

$$uvv_1-v_1^2-u_1v^2=k_2, \tag{15}$$

les entiers k, k_1 et k_2 sont limités. En éliminant u_1 et v_1 on aura de l'équation (15) la relation

$$uv(2uv-k_1)+(2uv-k_1)^2-4v^2(u^2-\Delta v^2-k)=16k_2.$$

Il en résultera un nombre fini de valeurs pour v. Ensuite on aura de l'équation (13) un nombre fini de valeurs pour u_1; et enfin le nombre v_1 sera limité par l'équation (14).

Le raisonnement sera tout-à-fait analogue dans le das où $-\Delta \equiv 1 \pmod 4$.

Le Théorème 5 se trouve ainsi démontré. Nous n'avons pas compris les corps biquadratiques du premier rang qui possèdent un sous-corps quadratique réel et qui n'admettent aucun sous-corps imaginaire. Il s'agit des classes 5 et 6; pour la définition des classes voir [2], p. 483. Dans les sections suivantes nous allons résoudre le problème pour les corps de ces deux classes et également pour tous les corps biquadratiques imprimitifs des rangs $r=2$ et $r=3$.

9. *La constitution du discriminant lorsqu'il y a trois sous-corps quadratiques.* Lorsque le corps $\mathbf{K}(\theta)$ dans le n° 6 est biquadratique, la forme ternaire

$$\pm \sqrt{D(\theta)/D^*} = F(v, w, z)$$

est du sixième degré. Si $\mathbf{K}(\theta)$ est imprimitif cette forme est évidemment réductible dans le corps rationnel. Nous allons déterminer les formes diviseurs par une multiplication convenable des facteurs linéaires conjugués.

Supposons que $\mathbf{K}(\theta)$ admet trois sous-corps quadratiques, engendrés par les nombres $\sqrt{\Delta}$, $\sqrt{\Delta_1}$ et $\sqrt{\Delta_2}$, où Δ, Δ_1 et Δ_2 sont des nombres entiers rationnels qui ne sont divisibles par aucun carré >1. Il faut observer que $\Delta_2 = \Delta\Delta_1/d^2$, où d est le plus grand commun diviseur de Δ et Δ_1. On voit sans peine que dans ce cas le discriminant D^* du corps est un carré parfait. Alors il est évident que tout nombre entier θ du corps est de la forme

$$\theta = \tfrac{1}{4}(u + v\sqrt{\Delta} + w\sqrt{\Delta_1} + z\sqrt{\Delta_2}),$$

où u, v, w et z sont des nombres entiers rationnels variables. Les nombres conjugués sont

$$\theta' = \tfrac{1}{4}(u + v\sqrt{\Delta} - w\sqrt{\Delta_1} - z\sqrt{\Delta_2}),$$

$$\theta'' = \tfrac{1}{4}(u - v\sqrt{\Delta} - w\sqrt{\Delta_1} + z\sqrt{\Delta_2}),$$

$$\theta''' = \tfrac{1}{4}(u - v\sqrt{\Delta} + w\sqrt{\Delta_1} - z\sqrt{\Delta_2}).$$

Il en résulte

$$\begin{aligned}
2(\theta - \theta') &= w\sqrt{\Delta_1} + z\sqrt{\Delta_2},\\
2(\theta - \theta'') &= v\sqrt{\Delta} + w\sqrt{\Delta_1},\\
2(\theta - \theta''') &= v\sqrt{\Delta} + z\sqrt{\Delta_2},\\
2(\theta' - \theta'') &= v\sqrt{\Delta} - z\sqrt{\Delta_2},\\
2(\theta' - \theta''') &= v\sqrt{\Delta} - w\sqrt{\Delta_1},\\
2(\theta'' - \theta''') &= -w\sqrt{\Delta_1} + z\sqrt{\Delta_2}.
\end{aligned}$$

Pour la forme $64\sqrt{D(\theta)} = \pm\sqrt{D^*}\cdot F(v, w, z)$ on aura donc l'expression

$$(\Delta v^2 - \Delta_2 z^2)(\Delta v^2 - \Delta_1 w^2)(\Delta_1 w^2 - \Delta_2 z^2). \tag{16}$$

10. *La constitution du discriminant lorsqu'il y a un seul sous-corps quadratique.* Supposons que $\mathbf{K}(\theta)$ admet un seul sous-corps quadratique, engendré par le nombre $\sqrt{\Delta}$, où Δ est un nombre entier rationnel qui n'est divisible par aucun carré >1. Nous pouvons prendre pour nombre générateur la quantité

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

où a et b sont des entiers rationnels tels que $\frac{1}{2}(a+b\sqrt{\Delta})$ soit un entier algébrique; voir Nagell [7], p. 349 et p. 357. L'un des nombres conjugués est donc

$$\xi'=\sqrt{\tfrac{1}{2}(a-b\sqrt{\Delta})}.$$

On voit aisément que tout nombre entier θ du corps est de la forme

$$\theta=\frac{1}{s}(u+v\sqrt{\Delta}+w\xi+z\sqrt{\Delta}\,\xi),$$

où s est un certain nombre naturel fixe et où u, v, w et z sont des nombres entiers rationnels variables. Les nombres conjugués sont

$$\theta'=\frac{1}{s}(u-v\sqrt{\Delta}+w\xi'-z\sqrt{\Delta}\,\xi'),$$

$$\theta''=\frac{1}{s}(u+v\sqrt{\Delta}-w\xi-z\sqrt{\Delta}\,\xi),$$

$$\theta'''=\frac{1}{s}(u-v\sqrt{\Delta}-w\xi'+z\sqrt{\Delta}\,\xi').$$

Il en résulte

$$\begin{aligned}
s(\theta-\theta') &= 2v\sqrt{\Delta}+w(\xi-\xi')+z\sqrt{\Delta}(\xi+\xi'),\\
s(\theta-\theta'') &= 2w\xi+2z\sqrt{\Delta}\,\xi,\\
s(\theta-\theta''') &= 2v\sqrt{\Delta}+w(\xi+\xi')+z\sqrt{\Delta}(\xi-\xi'),\\
s(\theta'-\theta'') &= -2v\sqrt{\Delta}+w(\xi+\xi')+z\sqrt{\Delta}(\xi-\xi'),\\
s(\theta'-\theta''') &= 2w\xi'-2z\sqrt{\Delta}\,\xi',\\
s(\theta''-\theta''') &= 2v\sqrt{\Delta}-w(\xi-\xi')-z\sqrt{\Delta}(\xi+\xi').
\end{aligned}$$

En multipliant les six différences on obtient

$$\pm s^6\sqrt{D(\theta)}=2\sqrt{a^2-\Delta b^2}\,(w^2-\Delta z^2)\,f(v,w,z),$$

où $f(v, w, z)$ est une forme du quatrième degré en v, w et z :

$$f(v, w, z) = (4\Delta v^2 - aw^2 - 2\Delta bwz - \Delta az^2)^2 - (a^2 - \Delta b^2)(w^2 - \Delta z^2)^2. \tag{17}$$

11. *Le cas des corps biquadratiques qui admettent trois sous-corps quadratiques réels.* Lorsque le corps $\mathbf{K}(\theta)$ admet un sous-corps imaginaire nous avons montré que l'équation

$$F(v, w, z) = A \tag{18}$$

n'a qu'un nombre fini de solutions en nombres entiers rationnels v, w et z; voir les n^os^ 6 et 8. En outre, nous pouvons reconnaître si cette équation est résoluble, et les solutions éventuelles peuvent être déterminées par un nombre fini d'opérations.

Passons maintenant au cas dans lequel il n'y a pas de sous-corps imaginaires. Considérons d'abord les corps qui admettent trois sous-corps réels. Soit $\mathbf{K}(\theta)$ un tel corps, et supposons que les sous-corps soient engendrés par les nombres $\sqrt{\Delta}$, $\sqrt{\Delta_1}$ et $\sqrt{\Delta_2}$, où Δ, Δ_1 et Δ_2 sont des nombres naturels, qui ne sont divisibles par aucun carré >1; on a $\Delta_2 = \Delta\Delta_1/(\Delta, \Delta_1)^2$. Alors nous venons de voir, dans le numéro précédent, que l'expression $\pm\sqrt{D^*}\cdot F(v, w, z)$ prendra la forme (16). Donc, résoudre l'équation (18) dans ce cas-ci signifie de résoudre un nombre fini de systèmes d'équations

$$\Delta v^2 - \Delta_2 z^2 = a, \quad \Delta v^2 - \Delta_1 w^2 = b, \quad \Delta_1 w^2 - \Delta_2 z^2 = c,$$

où a, b et c sont des nombres entiers rationnels tels que $abc = \pm\sqrt{D^*}A$. Pour l'existence simultanée de ces trois équations il faut évidemment que $a = b + c$. Donc, le problème revient èràsoudre un nombre fini de systèmes

$$\Delta v^2 - \Delta_2 z^2 = a, \quad \Delta v^2 - \Delta_1 w^2 = b. \tag{19}$$

Nous allons montrer que tout système de ce type n'admet qu'un nombre fini de solutions. En effet, le système (19) entraîne la relation

$$(a\Delta - b\Delta)v^2 - a\Delta_1 w^2 + b\Delta_2 z^2 = 0, \tag{20}$$

où a est nécessairement $\neq b$. En appliquant le critère de Legendre nous pouvons reconnaître si cette équation est résoluble ou non; voir p. ex. Nagell [6], p. 219. Si l'équation est résoluble on peut, par des essais, trouver une solution propre $v = v_1$, $w = w_1$, $z = z_1$, avec $v_1 w_1 z_1 \neq 0$. Alors, il est bien connu que toutes les solutions propres de (20) sont données par les formules suivantes

$$\begin{aligned} \delta v &= -(a-b)\Delta v_1 X^2 + 2a\Delta_1 w_1 XY - a\Delta_1 v_1 Y^2, \\ \delta w &= (a-b)\Delta w_1 X^2 - 2(a-b)\Delta v_1 XY + a\Delta_1 w_1 Y^2, \\ \pm\delta z &= (a-b)\Delta z_1 X^2 - a\Delta_1 z_1 Y^2, \end{aligned}$$

où X et Y sont des nombres entiers rationnels, premiers entre eux, et où δ est le plus grand commun diviseur des trois termes à drotie; voir p. ex. [6], p. 225. En introduisant ces valeurs de v et z dans l'équation

$$\Delta v^2 - \Delta_2 z^2 = a$$

nous aurons la relation

$$\left.\begin{aligned} \Delta[(a-b)\Delta v_1 X^2 - 2a\Delta_1 w_1 XY + a\Delta_1 v_1 Y^2]^2 \\ -\Delta_2[(a-b)\Delta z_1 X^2 - a\Delta_1 z_1 Y^2]^2 = a\delta^2. \end{aligned}\right\} \tag{21}$$

On peut montrer que la forme à gauche dans (21) n'est pas décomposable en facteurs à coefficients rationnels; pour la démonstration de cette assertion voir la Remarque 2 qui suivra ci-dessous.

Donc, d'après le théorème de Thue l'équation (21) ne possède qu'un nombre limité de solutions en nombres entiers X et Y. Par conséquent, le nombre de solutions du système (19), pour des valeurs données de Δ, Δ_1, Δ_2, a et b, est aussi limité.

Remarque 2. Nous allons déterminer le genre de la courbe algébrique $F=0$ représentée par l'équation (21). Nous homogénéisons l'équation en remplaçant $a\delta^2$ par $a\delta^2 Z^4$. Alors on voit d'abord que les points doubles éventuels se trouvent sur la droite $Z=0$. En différentiant par rapport à X et à Y on aura :

$$\frac{\partial F}{\partial X} = 2\Delta[2(a-b)\Delta v_1 X - 2a\Delta_1 w_1 Y]\cdot H(X, Y) - 2\Delta_2[2(a-b)\Delta z_1 X]\cdot G(X, Y),$$

$$\frac{\partial F}{\partial Y} = 2\Delta[2a\Delta_1 v_1 Y - 2a\Delta_1 w_1 X]\cdot H(X, Y) + 2\Delta_2\cdot 2a\Delta_1 z_1 Y\cdot G(X, Y),$$

où

$$H(X, Y) = (a-b)\Delta v_1 X^2 - 2a\Delta_1 w_1 XY + a\Delta_1 v_1 Y^2,$$

$$G(X, Y) = (a-b)\Delta z_1 X^2 - a\Delta_1 z_1 Y^2.$$

Il en résulte

$$[2(a-b)\Delta v_1 X - 2a\Delta_1 w_1 Y]2a\Delta_1 z_1 Y = 2(a-b)\Delta z_1 X[2a\Delta_1 v_1 Y - 2a\Delta_1 w_1 X],$$

ce qui entraîne

$$a\Delta_1 Y^2 = (a-b)\Delta X^2.$$

En introduisant cette relation dans l'équation de la courbe et en posant $Z=0$, nous aurons la condition

$$\Delta[(a-b)\Delta v_1 a\Delta_1 - 2a\Delta_1 w_1 \sqrt{a(a-b)\Delta\Delta_1} + a\Delta_1 v_1 (a-b)\Delta]^2 = 0.$$

Donc, si $a(a-b)\Delta\Delta_1$ est un carré parfait la courbe possède les deux points doubles $(\sqrt{a\Delta_1}, \pm\sqrt{(a-b)\Delta}, 0)$. Si $a(a-b)\Delta\Delta_1$ n'est pas un carré parfait il n'y a pas de points doubles. Donc, le genre de la courbe est ou $=1$ ou $=3$. En effet, il n'y a pas de singularités supérieures, et la quartique n'est ni dégénérée ni unicursale.

12. *Le cas des corps biquadratiques qui admettent un seul sous-corps quadratique réel.* Considérons enfin le cas où il n'existe qu'un seul sous-corps irrationnel lequel est réel. Résoudre l'équation (6) revient d'après le numéro 10 au problème de résoudre un nombre fini de systèmes d'équations

$$w^2 - \Delta z^2 = h, \tag{22}$$

$$(4\Delta v^2 - aw^2 - 2\Delta bwz - \Delta az^2)^2 - (a^2 - \Delta b^2)(w^2 - \Delta z^2)^2 = h_1, \tag{23}$$

où h et h_1 sont des nombres entiers rationnels tels que $2\sqrt{a^2 - \Delta b^2}\, hh_1 = \pm s^6 \sqrt{D(\theta)}$.

Nous allons éliminer z de l'équation (23) à l'aide de (22), et nous procédons en étapes. Pour commencer nous aurons

$$2\Delta v^2 - aw^2 - b\Delta wz = \tfrac{1}{2}\left(\sqrt{h_1 + (a^2 - \Delta b^2)h^2} - ah\right) = h_3,$$

où h_3 est un entier rationnel limité, et finalement nous obtenons la relation

$$(2\Delta v^2 - aw^2 - h_3)^2 - b^2\Delta(w^4 - hw^2) = 0. \tag{24}$$

Cette équation représente une courbe algébrique du premier genre; pour la démonstration de cette assertion voir la Remarque 3 qui suivra ci-dessous.

Donc, d'après un résultat de Siegel la courbe n'admet qu'un nombre fini de points à coordonnées entières rationnelles v et w; voir Siegel [8]. Ainsi, le nombre de solutions du système (22)–(23), pour des valeurs données de Δ, a, b, h et h_1, est aussi limité.

Cependant, pour un type particulier de corps on peut arriver à ce résultat sans recourir au théorème de Siegel; il s'agit des corps des classes 5 et 6. En effet, lorsque le corps est du premier rang la quartique (24) est fermée. Dans ces corps les nombres $a+b\sqrt{\Delta}$, $a-b\sqrt{\Delta}$ et a sont négatifs, et par conséquent la forme

$$(2\Delta v^2 - aw^2)^2 - \Delta b^2 w^4 = [2\Delta v^2 - (a + b\sqrt{\Delta})w^2]\,[2\Delta v^2 - (a - b\sqrt{\Delta})\,w^2]$$

est définite; voir Nagell [7] les tableaux p. 351 et p. 352. Alors, dans ce cas on aura une méthode très simple pour déterminer les solutions entières v et w de l'équation (24).

La quartique possède des branches courant à l'infini dans les cas suivants : 1°) Les nombres $a+b\sqrt{\Delta}$ et $a-b\sqrt{\Delta}$ sont de signes opposés, ce qui entraîne $r=2$; 2°) les nombres $a+b\sqrt{\Delta}$ et $a-b\sqrt{\Delta}$ sont tous les deux positifs, ce qui entraîne $r=3$.

Remarque 3. Nous allons montrer que la courbe algébrique $C=0$ représentée par l'équation (24) est du premier genre. Nous introduisons dans (24) la variable homogénéisante u. En différentiant par rapport à v, w et u nous aurons

$$\frac{\partial C}{\partial v} = 8\Delta v(2\Delta v^2 - aw^2 - h_3u^2),$$

$$\frac{\partial C}{\partial w} = -4aw(2\Delta v^2 - aw^2 - h_3u^2) - \Delta b^2(4w^3 - 2hwu^2),$$

$$\frac{\partial C}{\partial u} = -2h_3u(2\Delta v^2 - aw^2 - h_3u^2) + 2b^2h\Delta w^2u.$$

Considérons les conditions nécessaires

$$\frac{\partial C}{\partial v} = \frac{\partial C}{\partial w} = \frac{\partial C}{\partial u} = 0.$$

Si $v \neq 0$ il faut qu'on ait

$$2\Delta v^2 - aw^2 - h_3 u^2 = 0,$$

$$\Delta b^2(4w^3 - 2hwu^2) = 2\Delta b^2 hw^2 u = 0.$$

Vu qu'on ne peut pas avoir à la fois $w=0$ et $u=0$, on obtient la possibilité

$$v = \pm\sqrt{h_3/2\Delta}, \quad w=0, \quad u=1.$$

On vérifiera que ces valeurs satisfieront à l'équation de la courbe. Nous avons ainsi trouvé deux points doubles.

Considérons ensuite le cas de $v=0$. Alors on aura

$$2aw(aw^2+h_3u^2) = \Delta b^2(2w^3 - hwu^2),$$

et

$$h_3 u(aw^2+h_3u^2) = -\Delta b^2 hw^2 u.$$

On ne peut pas avoir $u=0$ vu que $a^2 \neq \Delta b^2$. Donc nous pouvons poser $u=1$. Si $w=0$ on obtient $u=0$, ce qui est impossible. En divisant par w nous aurons de la première équation

$$w^2 = -\frac{\Delta b^2 h + 2ah_3}{2(a^2 - \Delta b^2)}.$$

En introduisant cette valeur de w^2 et $v=0$ dans l'équation (24) nous aurons

$$\tfrac{1}{4}(\Delta b^2 h + 2ah_3)^2 - \tfrac{1}{2}(\Delta b^2 h + 2ah_3)^2 + (a^2 - \Delta b^2)\, h_3^2 = 0.$$

Il en résulte

$$(\Delta b^2 h + 2ah_3)^2 = 4(a^2 - \Delta b^2)\, h_3^2.$$

Or, cela est impossible vu que le nombre $a^2 - \Delta b^2$ n'est pas un carré parfait; voir Nagell [7], les tableaux p. 351 et p. 352. Donc, la courbe (24) admet exactement 2 points doubles; elle est ainsi du premier genre. En effet, la quartique n'a pas de singularités supérieures, et elle n'est ni dégénérée ni unicursale.

13. En résumant les résultats obtenus dans les numéros 11 et 12 nous puovons formuler la proposition suivante :

Théorème 6. *Désignons par* $\mathbf{\Phi}$ *le domaine de tous les nombres entiers du quatrième degré qui engendrent des corps jouissant de la propriété suivante : il y a au moins un sous-corps quadratique réel, il n'y a aucun sous-corps imaginaire. Soit D le discriminant d'un nombre de* $\mathbf{\Phi}$. *Alors il existe dans* $\mathbf{\Phi}$ *un nombre fini de nombres* $\alpha_1, \alpha_2, \ldots, \alpha_m$, *tels qu'on ait : Tout nombre dans* $\mathbf{\Phi}$ *ayant le discriminant D est de la forme* $\pm\alpha_i + k$, $i=1, 2, \ldots, m$, *où k est un nombre entier rationnel quelconque.*

Il faut observer que les nombres α_i n'appartiennent pas nécessairement au même corps biquadratique. La méthode de démonstration ne donne pas de moyen pour déterminer les nombres α_i, sauf dans le cas des corps du premier rang, dans lesquels il existe toujours une méthode simple pour déterminer ces nombres ainsi que nous venons de le montrer.

Les résultats établis dans les Théorèmes 2–6 montrent que, pour les nombres de discriminant donné, la même loi existe dans un domaine embrassant les corps quadratiques, cubiques et biquadratiques, exception faite (pour le moment) des corps biquadratiques primitifs d'un rang >1.

Vraisemblablement cette loi est valable pour tous les corps algébriques.

§ 4. Le probléme dans quelques corps particuliers

14. *Le corps cyclotomique d'index* 5. La démonstration du Théorème 5 nous donne une méthode pour effectivement déterminer les nombres α_i dans un corps donné. Cela n'est pas le cas au sujet des Théorèmes 4 et 6. Dans le Théorème 5 tous les corps sont du premier rang. Dans le Théorème 6 le rang est >1, sauf dans les cas des corps des classes 5 et 6 où le rang est $=1$. Même pour ces corps nous venons d'exposer une méthode pour déterminer les α_i. Nous considérons ici seulement la classe 6, qui ne contient qu'un seul corps, à savoir le corps cyclotomique $\mathbf{K}(\xi)$ engendré par le nombre $\xi = e^{2\pi i/5}$. Le discriminant du corps est $D^* = D(\xi) = 125$. Comme base des entiers du corps nous pouvons prendre $1, \xi, \xi^2, \xi^{-1}$. Nous avons besoin des identités suivantes

$$\xi^{-1} = -\xi^2 - \xi - 1 - \xi^{-1}, \tag{25}$$

$$\frac{5}{1-\xi} = 3 + 2\xi + \xi^2 - \xi^{-1}, \tag{26}$$

$$\frac{1}{1+\xi} = -\xi - \xi^3. \tag{27}$$

Si θ est un nombre générateur du corps $K(\xi)$ on a $D(\theta) = 125A^2$, où A est un nombre naturel. Nous nous proposons de déterminer tous les nombres dans le corps dont le discriminant a la valeur minimum 125. Par une méthode tout-à-fait différente de celles appliquées jusqu'ici nous allons établir le résultat suivant :

Théorème 7. *La condition nécessaire et suffisante pour qu'un nombre θ dans $\mathbf{K}(\xi)$ ait le discriminant* 125, *est qu'il soit de l'une des formes suivantes :*

$$\pm\xi + k, \quad \pm\xi^2 + k, \quad \pm\xi^3 + k, \quad \pm\xi^4 + k,$$

$$\pm(\xi + \xi^2) + k, \quad \pm(\xi + \xi^3)) + k,$$

où k est un nombre entier rationnel quelconque.

Démonstration. Nous pouvons supposer que le nombre θ ayant le discriminant donné D soit de la forme

$$\theta = a\xi + b\xi^2 + c\xi^{-1},$$

où a, b et c sont des nombres entiers rationnels. En effet, θ et $\theta + k$ ont le même discriminant.

Si θ' désigne le nombre imaginairement conjugué à θ, on a

$$\theta' = a\xi^{-1} + b\xi^{-2} + c\xi.$$

Donc, a l'aide de (25),

$$\theta' = (c-b)\xi - b\xi^2 + (a-b)\xi^{-1} - b.$$

En échangeant ξ par ξ^2 on aura

$$\theta'' = -c\xi + (a-c)\xi^2 + (b-c)\xi^{-1} - c,$$

$$\theta''' = (-a+b)\xi + (-a+c)\xi^2 - a\xi^{-1} - a.$$

Pour les six différences on obtient

$$\theta - \theta' = (a+b-c)\xi + 2b\xi^2 + (b-a+c)\xi^{-1} + b,$$

$$\theta - \theta'' = (a+c)\xi + (b-a+c)\xi^2 + (2c-b)\xi^{-1} + c,$$

$$\theta - \theta''' = (2a-b)\xi + (a+b-c)\xi^2 + (a+c)\xi^{-1} + a,$$

$$\theta' - \theta'' = (2c-b)\xi + (c-a-b)\xi^2 + (a-2b+c)\xi^{-1} - b + c,$$

$$\theta' - \theta''' = (a+c-2b)\xi + (a-b-c)\xi^2 + (2a-b)\xi^{-1} + a - b,$$

$$\theta'' - \theta''' = (a-b-c)\xi + (2a-2c)\xi^2 + (a+b-c)\xi^{-1} + a - c.$$

Toutes les différences sont divisibles par $1-\xi$. On en aura

$$(\theta-\theta')\ (\theta''-\theta''') = -\sqrt{5}(a^2+c^2-b^2-2ac+ab-bc),$$

$$(\theta-\theta'')\ (\theta'-\theta''') = \tfrac{1}{2}\sqrt{5}(b^2-a^2-c^2+2ac+ab-bc) + \tfrac{1}{2}5(a^2+b^2+c^2-ab-bc).$$

Donc, on obtiendra pour le discriminant

$$D(\theta) = 125[G(a,b,c)]^2 \cdot [H(a,b,c)]^2,$$

où

$$G(a,b,c) = a^2-b^2+c^2-2ac+ab-bc, \tag{28}$$

$$4H(a,b,c) = (a^2-b^2+c^2-2ac-ab+bc)^2 - 5(a^2+b^2+c^2-ab+bc)^2. \tag{29}$$

Si le discriminant de θ est égal à 125, les nombres a, b et c doivent satisfaire aux équations

$$G(a,b,c) = \pm 1, \quad H(a,b,c) = \pm 1,$$

où les signes sont indépendants entre eux.

Lorsque $D(\theta) = 125$ on vérifie aisément qu'on aura la relation

$$\frac{\theta-\theta''}{1-\xi} = c - b + (a-b+c)\,\xi + c\xi^2 + (c-b)\,\xi^{-1} = \xi^h E, \tag{30}$$

où h a une des valeurs 0, ± 1, ± 2, et où E est une unité réelle.

Si $h=0$ le coefficient du terme purement imaginaire s'évanouit. Donc il faut que

$$(a-b+c)\sin\frac{2\pi}{5} + c\sin\frac{4\pi}{5} - (c-b)\sin\frac{2\pi}{5} = 0,$$

Il en résulte que $a=c=0$, et par conséquent $b=\pm 1$.

Si $h=1$ l'équation (30) peut s'écrire

$$a+b\xi+(b-c)\xi^2=E.$$

Il en résulte

$$b\sin\frac{2\pi}{5}+(b-c)\sin\frac{4\pi}{5}=0,$$

et par conséquent $b=c=0$ et $a=\pm 1$.

Si $h=-1$ l'équation (30) peut s'écrire

$$-b-b\xi+(a-b)\xi^2-c\xi^{-1}=E.$$

Il en résulte

$$-b\sin\frac{2\pi}{5}+(a-b)\sin\frac{4\pi}{5}+c\sin\frac{2\pi}{5}=0,$$

et par conséquent $c-b=a-b=0$. On en conclut que $a=b=c=\pm 1$.

Si $h=2$ l'équation (30) peut s'écrire

$$b+(b-c)\xi+a\xi^{-1}=E.$$

Par le même raisonnement on en aura $b=a+c$. Ainsi on peut éliminer b des équations $G(a, b, c)=\pm 1$ et $H(a, b, c)=\pm 1$. Alors on obtient $a^2-c^2-4ac=\pm 1$ et

$$(-a^2+c^2-4ac)^2-5(a^2+c^2)^2=\pm 4,$$

d'où

$$(2c^2-2a^2\pm 1)^2-5(a^2+c^2)=\pm 4.$$

Vu que cette équaiton peut s'écrire

$$-(a^2+c^2)^2-16a^2c^2\pm 4(c^2-a^2)=\pm 4-1,$$

on voit qu'elle est impossible si tous les deux nombres $|a|$ et $|c|$ sont $\geqslant 1$. Donc, les seules solutions sont $a=0$, $b=c=\pm 1$ et $c=0$, $a=b=\pm 1$.

Considérons enfin le cas de $h=-2$. Alors, l'équation (30) peut s'écrire

$$-a\xi-a\xi^2+(b-a)\xi^{-1}-a+b-c=E.$$

Il en résulte

$$b\sin\frac{2\pi}{5}+a\sin\frac{4\pi}{5}=0.$$

d'où $a=b=0$, $c=\pm 1$.

Le Théorème 7 se trouve ainsi démontré. La même méthode s'appliquera à détermines les nombres de discriminant $125A^2$, où $A>1$.

Correction au travail [5], p. 171 : Dans la ligne 4 il faut supprimer les mots : « Il en résulte que. » Encore, il faut remplacer les lignes 5–7 par le texte suivant : L'anneau $\mathbf{R}(\varepsilon^m\xi)$, où $\varepsilon=\frac{1}{2}(1+\sqrt{5})$ et $m\geqslant 2$, est différent de l'anneau fondamental; ainsi il existe une infinité d'anneaux qui contiennent des unités imaginaires. L'anneau

$\mathbf{R}(1, c\xi, c\xi^2, c\xi^{-1})$ où c est un nombre naturel >1 ne contient aucune unité imaginaire. En effet, soit

$$\varepsilon^m \xi^h = x + yc\xi + zc\xi^2 + wc\xi^{-1},$$

où $m>0$ et $h \neq 0 \pmod 5$. Si $h=1$ nous aurons

$$\varepsilon^m = yc - wc + (zc - wc)\xi - wc\xi^2 + (x - wc)\xi^{-1}.$$

Donc $zc - wc - x + wc = wc = 0$, ce qui est évidemment impossible. Si $h=-1$ nous obtenons

$$\varepsilon^m = wc - zc + (x - zc)\xi + (yc - zc)\xi^2 - zc\xi^{-1},$$

d'où $x - zc + zc = yc - zc = 0$, ce qui est impossible. Si $h=2$ il résulte que

$$\varepsilon^m = zc - x + (wc - x)\xi - x\xi^2 + (yc - x)\xi^{-1},$$

d'où $wc - x - (yc - x) = x = 0$, impossible. Si $h=-2$ nous aurons

$$\varepsilon^m = -yc + (wc - yc)\xi + (x - yc)\xi^2 + (zc - yc)\xi^{-1},$$

d'où $wc - yc - (zc - yc) = x - yc = 0$, impossible.

Donc, il existe une infinité d'anneaux dans lesquels toutes les unités sont réelles.

15. *Le corps cyclotomique d'index* 8. Dans le corps $\mathbf{K}(\xi)$ où $\xi = e^{\pi i/4}$ on a $D^* = D(\xi) = 256$. Comme base des entiers du corps nous puovons prendre $1, \xi, \xi^2, \xi^3$. Si θ est un nombre générateur du corps on a $D(\theta) = 256\, A^2$, où A est un nombre naturel. Nous allons établir le théorème suivant :

Théorème 8. *La condition nécessaire et suffisante pour qu'un nombre θ dans $\mathbf{K}(\xi)$ ait le discriminant* 256 *est qu'il soit de l'une des formes suivantes :*

$$\pm\xi + k, \quad \pm\xi^3 + k,$$

où k est un nombre entier rationnel quelconque.

Démonstration. Nous pouvons supposer que le nombre θ ayant le discriminant donné D soit de la forme

$$\theta = a\xi + b\xi^2 = c\xi^3,$$

où a, b et c sont des nombres entiers rationnels. Si θ' désigne le nombre imaginairement conjugué à θ, on a

$$\theta' = -a\xi^3 - b\xi^2 - c\xi.$$

En échangeant ξ par ξ^3 on aura

$$\theta'' = a\xi^3 - b\xi^2 + c\xi,$$

$$\theta''' = -a\xi + b\xi^2 - c\xi^3.$$

Pour les six différences on obtient

$$\begin{aligned}
\theta-\theta' &= (a+c)\xi+2b\xi^2+(a+c)\xi^3,\\
\theta-\theta'' &= (a-c)\xi+2b\xi^2+(c-a)\xi^3,\\
\theta-\theta''' &= 2a\xi+2c\xi^3,\\
\theta'-\theta'' &= -2c\xi-2a\xi^3,\\
\theta'-\theta''' &= (a-c)\xi-2b\xi^2+(c-a)\xi^3,\\
\theta''-\theta''' &= (a+c)\xi-2b\xi^2+(a+c)\xi^3.
\end{aligned}$$

Pour le discriminant on aura donc

$$D(\theta)=2^8[a^2+c^2]^2[2b^2-(a+c)^2]^2[2b^2+(a-c)^2]^2.$$

En posant $D(\theta)=2^8$ on obtient les solutions suivantes : $a=b=0$, $c=\pm 1$ et $b=c=0$, $a=\pm 1$; et le théorème se trouve démontré.

Il est évident que la même méthode s'appliquera pour déterminer tous les nombres θ dans le corps qui ont le discriminant 2^8A^2 lorsque $A>1$.

16. *Le corps cyclotomique d'index* 12. Dans le corps $\mathbf{K}(\xi)$ où $\xi=e^{\pi i/6}$ on a $D^*=D(\xi)=144$. Comme base des entiers du corps nous pouvons prendre $1, \xi, \xi^2, \xi^3$. Si θ est un nombre générateur du corps on a $D(\theta)=144\ A^2$, A nombre naturel. Nous allons établir le résultat suivant :

Théorème 9. *La condition nécessaire et suffisante pour qu'un nombre θ dans $\mathbf{K}(\xi)$ ait le discriminant* 144 *est qu'il soit de l'une des formes suivantes :*

$$\pm\xi+k,\quad \pm\xi^5+k,\quad \pm(\xi^2+\xi^3)+k,\quad \pm(\xi^2-\xi^3)+k,$$

où k est un nombre entier rationnel quelconque.

Démonstration. Nous pouvons supposer que le nombre θ ayant le discriminant donné D soit de la forme

$$\theta=a\xi+b\xi^2+c\xi^3,$$

a, b et c étant des nombres entiers rationnels.

Si θ' désigne le nombre imaginairement conjugué à θ, on a

$$\theta'=a\xi-b\xi^2+(-a-c)\xi^3+b.$$

En échangeant ξ par ξ^5 on aura

$$\theta''=-a\xi-b\xi^2+(a+c)\xi^3+b,$$

$$\theta'''=-a\xi+b\xi^2-c\xi^3.$$

Pour les six différences on obtient

$$\begin{aligned}
\theta-\theta' &= 2b\xi^2+(a+2c)\xi^3-b,\\
\theta-\theta'' &= 2a\xi+2b\xi^2-a\xi^3-b,\\
\theta''-\theta''' &= -2b\xi^2+(a+2c)\xi^3+b,\\
\theta'-\theta''' &= 2a\xi-2b\xi^2-a\xi^3+b,\\
\theta-\theta''' &= 2a\xi+2c\xi^3,\\
\theta'-\theta'' &= 2a\xi-2(a+c)\xi^3.
\end{aligned}$$

Pour le discriminant on aura donc

$$D(\theta)=144[a^2+b^2]^2[a^2+ac+c^2]^2[(a+2c)^2-3b^2]^2.$$

En posant $D(\theta)=144$ on obtient les solutions suivantes : $a=0$, $b=1$, $c=\pm1$; $a=0$ $b=-1$, $c=\pm1$; $a=\pm1$, $b=c=0$; $b=0$, $a=\pm1$, $c=\mp1$; et le théorème se trouve démontré.

La même méthode s'appliquera évidemment pour déterminer tous les nombres θ dans le corps qui ont le discriminant 144 A^2, lorsque $A>1$.

Remarque 4. Il est facile d'établir le résultat suivant :

Théorème 10. *Si $\xi=e^{\pi i/4}$ l'équation ternaire*

$$N(u+v\xi+w\xi^2)=1 \tag{31}$$

admet une infinité de solutions en nombres entiers rationnels u, v et w, lesquelles sont données par les relations $v^2-2u^2=\pm1$ et $w=u$; outre ces solutions on a seulement les possibilités suivantes : $u=\pm1$, $v=w=0$ et $u=v=0$, $w=\pm1$.

Démonstration. L'équation (31) entraîne que

$$u+v\xi+w\xi^2=\xi^h\cdot E, \tag{32}$$

où E est une unité réelle et où h a une des valeurs 0, $+1$, -1 ou 2. Si $h=0$ on obtient $v\sin\frac{1}{4}\pi+w=0$, donc $v=w=0$ et $u=\pm1$. Si $h=1$ on aura de (32) en divisant par ξ

$$u\xi^{-1}+v+w\xi=E,$$

d'où $u=w$ et $u\sqrt{2}+v=E$. Si $h=-1$ on obtient de (32) en multipliant par ξ

$$u\xi+vi-w\xi^{-1}=E,$$

d'où $u+w=v=0$, ce qui est évidemment impossible. Si $h=2$ on aura de (32) en divisant par ξ^2

$$u\xi^{-2}+v\xi^{-1}+w=E,$$

d'où $u=v=0$ et $w=\pm1$. Cela démontre le Théorème 10. L'effet dépend ici sur le fait qu'il y a un sous-corps quadratique réel.

Institut de mathématiques, Université, Uppsala

INDEX BIBLIOGRAPHIQUE

1. Skolem, Th., Diophantische Gleichungen, *Ergebnisse der Mathematik* t. 5, Berlin 1938.
2. Nagell, T., Sur les représentations de l'unité par les formes binaires biquadratiques du premier rang, *Arkiv för matematik* Bd. 5, nr. 33, Stockholm 1965.
3. Nagell, T., Zur algebraischen Zahlentheorie, *Math. Zeitschrift* Bd. 34, Berlin 1931.
4. Chabauty, C., Sur certaines équations diophantiques ternaires, *Comptes rendus Acad Sci.*, t. 202, Paris 1936, p. 2117–2119.
5. Nagell, T., Contributions à la théorie des modules et des anneaux algébriques, *Arkiv för matematik* Bd. 6, nr. 9, Stockholm 1965.
6. Nagell, T., Introduction to number theory, New York 1951.
7. Nagell, T., Sur quelques questions dans la théorie des corps biquadratiques, *Arkiv för matematik* Bd. 4, nr. 26, Stockholm 1961.
8. Siegel, C., Über einige Anwendungen diophantischer Approximationen, *Abhandl. Preuss. Akad. d. Wissensch.* Berlin, Jahrg. 1929, *Phys.-Math. Klasse*, Nr. 1.
9. Stickelberger, L., Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, *Verhandl. d. ersten intern. Math.-Kongresses*, Zürich 1897, S. 182–193.
10. Schur, I., Elementarer Beweis eines Satzes von L. Stickelberger, *Mathematische Zeitschrift* Bd. 29, Berlin 1929.

Tryckt den 4 oktober 1967

Uppsala 1967. Almqvist & Wiksells Boktryckeri AB