ARKIV FÖR MATEMATIK Band 8 nr 14

1.69 02 2 Communiqué le 22 Janvier 1969

Quelques problèmes relatifs aux unités algébriques

Par TRYGVE NAGELL

§ 1. Introduction

1. Mes recherches sur certains sujets de la théorie des nombres algébriques m'ont conduit à la question de résoudre l'équation

$$1+E+E_1=0 \tag{1}$$

en unités E et E_1 d'un corps algébrique donné $\mathbf{K}$. Ainsi, dans un travail sur la représentation des nombres entiers par une forme binaire cubique, j'ai eu besoin de déterminer les solutions de l'équation (1) dans un corps cubique à discriminant négatif; voir Nagell [1][1], Hilfssatz IV. De plus, le problème de déterminer les points exceptionnels d'une certaine catégorie de courbes cubiques appartenant à un corps algébrique $\mathbf{K}$ exige qu'on détermine les solutions de l'équation (1) dans $\mathbf{K}$; voir Nagell [2], p. 346–355 et [3], p. 176–179. J'ai continué mes recherches sur l'équation (1) dans les travaux [4] et [5]. Dans ces cinq travaux (dont le premier fut publié en 1928) j'ai résolu le problème complètement dans le cas d'un corps algébrique d'un rang $\leqslant 1$; il s'agit alors des corps quadratiques, des corps cubiques à discriminent négatif et des corps biquadratiques du premier rang, caracterisés par la propriété que tous les corps conjugués sont imaginaires. J'ai montré que le nombre de solutions de (1) dans un corps donné est limité dans ces cas, et j'en ai déterminé toutes les solutions.

En fait, le nombre de solutions de (1) est limité dans un corps algébrique quelconque, ainsi qu'il a été montré par S. Chowla en 1961; voir [6]. Sans connaître la démonstration de Chowla j'ai établi le même résultat en 1964; voir [4], Théorème 8. Les deux démonstrations, qui dépendent d'un théorème de Siegel, sont identiques. Cependant, la nature de cette démonstration est telle qu'elle ne donne aucun moyen pour déterminer les solutions. Dans mon travail [4] j'ai montré que le Théorème 8 n'est qu'un cas particulier d'un théorème beaucoup plus général; voir le Théorème 9 dans le travail en question. Du Théorème 9 il résulte, entre autres, que la somme de deux unités dans un corps algébrique donné ne peut avoir la même valeur que dans un nombre fini de cas.

2. Désignons par m le nombre de solutions de (1) dans un corps donné $\mathbf{K}$ sans compter la permutation de E et E_1. Supposons qu'on ait la solution

$$1+E+E_1=0. \tag{1}$$

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

Alors on a aussi les deux solutions

$$1+E_1E^{-1}+E^{-1}=0 \quad \text{et} \quad 1+EE_1^{-1}+E_1^{-1}=0. \tag{1a}$$

Les trois solutions sont dfférentes entre elles sauf dans le cas où E et E_1 sont les racines de l'équation $x^2+x+1=0$. On en conclut:

Le nombre m de solutions de (1) *est divisible par* 3 *quand le corps* **K** *ne contient pas le nombre* $\sqrt{-3}$. *Quand* **K** *contient le nombre* $\sqrt{-3}$, *on a* $m\equiv 1 \pmod 3$.

On voit aisément que $m\geqslant 3$ lorsque le corps **K** contient le nombre $\sqrt{5}$; comparez le Théorème 1.

Soient **K'** un corps conjugué à **K** et E' et E_1' des unités conjuguées à E et à E_1. Alors la relation (1) entraîne aussi la relation conjuguée

$$1+E'+E_1'=0 \tag{1b}$$

et encore les deux relations

$$1+E_1'(E')^{-1}+(E')^{-1}=0 \quad \text{et} \quad 1+E'E_1^{-1}+E_1^{-1}=0. \tag{1c}$$

Supposons maintenant que les deux corps **K** et **K'** soient identiques. Alors, si la relation (1b) n'est identique à aucune des trois relations (1) et (1a) nous obtenons de cette manière un nouveau triplet de solutions de (1) dans **K**. Si, au contraire, la relation (1b) est identique à une des relations (1) et (1a), le triplet (1b)+(1c) est identique au triplet (1)+(1a).

Si **K** est un corps de Galois de degré n, il peut arriver que la relation (1) donnera naissance à n triplets, y compris le triplet (1)+(1a).

Nous dirons qu'un corps algébrique est du rang r, lorsque le groupe multiplicatif des unités possède le rang r; alors on ne prend pas en considération les racines de l'unité. On a $r=0$ seulement pour les corps quadratiques imaginaires.

§ 2. Le nombre de solutions de l'équation (1) dans un corps d'un rang <2

3. Comme plus haut m signifie le nombre de solutions de l'équation (1), sans compter la permutation de E et E_1. D'après les mémoires [1]–[5] nous avons les résultats suivants sur le nombre m dans les corps de rang $\leqslant 1$. Commençons avec les corps quadratiques.

Théorème 1. *Dans l'ensemble des corps quadratiques toutes les solutions de l'équation* (1) *sont données par les relations suivantes :*

$$1+\varrho+\varrho^2=0 \text{ dans le corps } \mathbf{K}(\sqrt{-3}), \text{ et donc } m=1;$$

$$1+\varepsilon-\varepsilon^2=0, \quad 1-\varepsilon+\varepsilon^{-1}=0, \quad 1-\varepsilon^{-1}-\varepsilon^{-2}=0$$

$$\text{dans le corps } \mathbf{K}(\sqrt{5}), \text{ et donc } m=3.$$

Dans tous les autres corps quadratiques on a $m=0$.

On doit observer que la relation (1) admet des solutions seulement dans les deux corps pour lesquels la valeur absolue du discriminant a son minimum; les minima sont 3 et 5.

4. Passons ensuite aux corps cubiques. On a le

Théorème 2. *Dans l'ensemble des corps cubiques à discriminant négatif toutes les solutions de l'équation* (1) *sont données par les relations suivantes :*

$$1-\xi^2-\xi^3=0, \quad 1-\xi-\xi^5=0, \quad 1+\xi^{-1}-\xi^{-3}=0,$$

$$1+\xi-\xi^{-2}=0, \quad 1+\xi^4-\xi^{-1}=0, \quad 1+\xi^{-4}-\xi^{-5}=0,$$

et donc $m=6$ *dans* $\mathbf{K}(\xi)$;

$$1-\eta-\eta^3=0, \quad 1+\eta^{-2}-\eta^{-3}=0, \quad 1+\eta^2-\eta^{-1}=0,$$

et donc $m=3$ *dans* $\mathbf{K}(\eta)$.

Le discriminant du corps $\mathbf{K}(\xi)$ *est* $=-23$, *et celui du corps* $\mathbf{K}(\eta)$ *est* $=-31$. *Dans tous les autres corps cubiques du premier rang on a* $m=0$.

Même ici on observe que la relation (1) admet des solutions seulement dans les (six) corps pour lesquels la valeur absolue du discriminant a son minimum. Les minima sont ici 23 et 31.

5. Passons ensuite aux corps biquadratiques. On a le

Théorème 3. *Soit* $\mathbf{K}$ *un corps biquadratique du premier rang.*

Dans les corps appartenant aux classes 1, 2, 3, 5, 7, 8, 9, 10 *et* 13 *on a* $m=0$, *sauf dans les cas suivants :* 1°) *Si le corps contient le nombre* $\sqrt{5}$, *on a* $m=3$; 2°) *si le discriminant du corps est* $=229$, *on a* $m=3$; *les quatre corps appartiennent dans ce cas à la classe* 1; 3°) *si le discriminant du corps est* $=272$, *on a* $m=3$; *les quatre corps appartiennent dans ce cas à la classe* 3.

Dans les corps des classes 4, 11 *et* 12 *on a* $m=1$, *sauf dans les cas suivants :* 1°) *Dans le corps* $\mathbf{K}(\sqrt{-3}, \sqrt{5})$ *on a* $m=4$; *le corps appartient dans ce cas à la classe* 11; 2°) *si le discriminant du corps est* $=189$, *on a* $m=4$; *les deux corps appartiennent dans ce cas à la classe* 4; 3°) *si le discriminant du corps est* $=117$, *on a* $m=10$; *les deux corps appartiennent dans ce cas à la classe* 4.

Dans la classe 14, *qui contient seulement le corps* $\mathbf{K}(e^{\pi i/6})$, *on a* $m=7$. *Dans la classe* 6, *qui contient seulement le corps* $\mathbf{K}(e^{2\pi i/5})$, *on a* $m=9$.

Donc, les seules valeurs possibles de m *sont* 0, 1, 3, 4, 7, 9 *et* 10.

Il y a évidemment une infinité de corps dans lesquels on a $m=0$, 1, 3 *ou* 4. *On a* $m=7$ *seulement pour le corps engendré par une racine de l'équation* $x^4-x^2+1=0$. *On a* $m=9$ *seulement pour le corps engendré par une racine de l'équation* $x^4+x^3+x^2+x+1=0$. *On a* $m=10$ *seulement pour les deux corps engendrés par les racines de l'équation* $x^4-x^3-x^2+x+1=0$.

Pour la définition des classes des corps biquadratiques je renvoie aux travaux [4], [7] et [8].

Il est intéressant d'observer que les valeurs maximales de m, à savoir 7, 9 et 10, sont obtenues pour les corps biquadratiques du premier rang qui possèdent les discriminants les plus petits. En effet, à $m=7$ correspond le discriminant 144, à $m=9$ correspond le discriminant 125, et à $m=10$ correspond le discriminant 117.

§ 3. L'équation (1) dans les corps cubiques de discriminant positif

6. Soit ε une unité $\neq \pm 1$ dans le corps cubique $\mathbf{K}$ de discriminant positif. Alors le rang de $\mathbf{K}$ est $=2$. Supposons que ε soit racine de l'équation

$$x^3 - px^2 + qx \mp 1 = 0 \tag{2}$$

à coefficients entiers rationnels p et q. Le discriminant de ε est alors

$$D(\varepsilon) = p^2q^2 - 4q^3 \mp 4p^3 - 27 \pm 18pq. \tag{3}$$

Supposons maintenant que $\varepsilon - 1$ soit aussi une unité. Si la norme de $\varepsilon - 1$ est égale à -1 nous aurons la condition

$$1 - p + q \mp 1 = +1.$$

Il en résulte les deux possibilités $q = p + 1$ et $q = p - 1$.

Si la norme de $\varepsilon - 1$ est égale à $+1$ nous aurons la condition

$$1 - p + q \mp 1 = -1,$$

et par suite les deux possibilités $q = p - 1$ et $q = p - 3$.

En prenant $q = p + 1$ et le signe supérieur dans (2) et (3) nous obtenons

$$D(\varepsilon) = p^4 - 6p^3 + 7p^2 + 6p - 31$$

et pour $p = 1 + z$

$$D(\varepsilon) = z^4 - 2z^3 - 5z^2 + 6z - 23. \tag{4}$$

En prenant $q = p - 1$ et le signe inférieur dans (2) et (3) nous obtenons

$$D(\varepsilon) = p^4 - 2p^3 - 5p^2 + 6p - 23.$$

En prenant $q = p - 1$ et le signe supérieur dans (2) et (3) nous obtenons

$$D(\varepsilon) = p^4 - 10p^3 + 31p^2 - 30p - 23,$$

d'où résulte pour $p = z + 2$

$$D(\varepsilon) = z^4 - 2z^3 - 5z^2 + 6z - 23.$$

En prenant finalement $q = p - 3$ et le signe inférieur dans (2) et (3) nous obtenons

$$D(\varepsilon) = p^4 - 6p^3 + 27p^2 - 54p + 81. \tag{5}$$

Ici le polynome en p est un carré parfait; et l'on aura

$$D(\varepsilon) = (p^2 - 3p + 9)^2. \tag{6}$$

Donc, dans ce cas, le corps cubique est cyclique.

Nous nous sommes déjà servis de la même méthode dans le cas d'un discriminant négatif; voir [1], Hilfssatz IV. Ici nous traitions le cas d'un discriminant positif; et dans ce qui suivra il faut distinguer entre les corps cycliques et les corps non-cycliques.

§ 4. Les corps cubiques non-cycliques de discriminant positif

7. On vérifie aisément que le polynome

$$z^4-2z^3-5z^2+6z-23, \tag{7}$$

représentant dans trois cas le discriminant $D(\varepsilon)$ dans le § 3, est irréductible, et qu'il peut s'écrire

$$(z^2-z-3)^2-32.$$

Il en résulte que le discriminant $D(\varepsilon)$ est égal à un produit de nombres premiers $\equiv \pm 1 \pmod 8$, et qu'on a $D(\varepsilon)\equiv 1 \pmod 8$. Si D^* est le discriminant du corps $\mathbf{K}$ on a $D(\varepsilon)=D^*y^2$, où y est un entier rationnel. Donc, tout diviseur premier de D^* est $\equiv \pm 1 \pmod 8$ et l'on a $D^*\equiv 1 \pmod 8$.

Considérons maintenant l'équation diophantienne

$$D(\varepsilon)=(z^2-z-3+4\sqrt{2})\,(z^2-z-3-4\sqrt{2})=D^*y^2. \tag{8}$$

Dans le corps quadratique engendré par $\sqrt{2}$ le nombre de classes d'idéaux est $=1$, et les deux facteurs

$$z^2-z-3+4\sqrt{2} \quad \text{et} \quad z^2-z-3-4\sqrt{2}$$

sont évidemment premiers entre eux. Alors on obtient de (8)

$$z^2-z-3\pm 4\sqrt{2}=(a+b\sqrt{2})\,(u+v\sqrt{2})^2,$$

où u et v sont des entiers rationnels, tels que $\pm y=u^2-2v^2$, et où a et b sont des entiers rationnels tels que $a^2-2b^2=D^*$; il est possible de choisir a et b de façon qu'on ait

$$0<a<\sqrt{2D^*} \quad \text{et} \quad 0<|b|<\tfrac{1}{2}\sqrt{2D^*};$$

comparez Nagell [9], Theorem 108.

Par conséquent, on aura le système suivant

$$\left.\begin{aligned} z^2-z-3&=a(u^2+2v^2)+4buv,\\ \pm 4&=b(u^2+2v^2)+2auv. \end{aligned}\right\} \tag{9}$$

Vu que y et D^* sont impairs, u et a le sont aussi; donc b est pair. D'après ce que nous venons de dire sur l'équation (1) nous savons que ce système ne possède qu'un nombre fini de solutions en nombres entiers rationnels z, u et v. On connaît un grand nombre de cas dans lesquels on peut effectivement déterminer toutes les solutions de ce système. Nous allons revenir sur cette question prochainement.

8. Il résulte de ce qui précède dans ce paragraphe le

Théorème 4. *Soit donné le corps cubique* $\mathbf{K}$ *non-cyclique de discriminant positif. Si* ε *et* $\varepsilon+1$ *sont simultanément des unités dans* $\mathbf{K}$, *le discriminant* $D(\varepsilon)$ *de* ε *est égal à un produit de nombres premiers* $\equiv \pm 1$ *(mod* 8*), et le discriminant du corps a la même propriété.*

Nous allons y ajouter le

Théorème 5. *Il y a une infinité de corps cubiques non-cycliques de discriminant positif dans lesquels il existe des unités de différence* 1.

Démonstration. Nous avons besoin du lemme suivant (pour la démonstration voir [10] Lemme 3) :

Lemme 1. Soit $f(x)$ un polynome à coefficients entiers rationnels qui ne possède aucun zéro multiple. Si p est un nombre premier tel que la congruence $f(x) \equiv 0 \pmod{p}$ soit résoluble, et si p ne divise pas le discriminant de $f(x)$, on peut trouver un nombre entier rationnel x_0 tel que $f(x_0)$ soit divisible par p et non par p^2.

Supposons qu'il y ait seulement les m corps cubiques non-cycliques de discriminant positif

$$\mathbf{K}_1, \mathbf{K}_2, \ldots, \mathbf{K}_m \tag{10}$$

dans lesquels il existe des unités de différence 1. Désignons par

$$D_1^*, D_2^*, \ldots, D_m^* \tag{11}$$

les discriminants de ces corps. Soit maintenant p un nombre premier jouissant des propriétés suivantes : 1°) p ne divise aucun des discriminants (11). 2°) p ne divise pas le discriminant du polynome

$$f(z) = z^4 - 2z^3 - 5z^2 + 6z - 23.$$

3°) La congruence $f(z) \equiv 0 \pmod{p}$ est résoluble.

Alors, d'après le Lemme 1 nous pouvons choisir l'entier rationnel z_0 tel que $f(z_0)$ soit divisible par p et non par p^2. De plus, nous choisissons z_0 suffisamment grand pour que $f(z_0)$ soit positif. Alors $f(z_0)$ est le discriminant d'une équation

$$x^3 - z_0 x^2 + (z_0 - 1)x + 1 = 0,$$

qui engendre un corps cubique K_{m+1} de discriminant positif. Il résulte de ce qui précède que le discriminant de K_{m+1} est divisible par p et non par p^2. Ce corps est donc non-cyclique et différent des corps (10). D'après le § 3 il existe des unités de différence 1 dans ce corps. Le Théorème 5 se trouve ainsi démontré.

9. Un supplément au Théorème 5 est le

Théorème 6. *Il y a une infinité de corps cubiques non-cycliques de discriminant positif dans lesquels il n'existe aucune couple d'unités de différence* 1.

Démonstration. D'après le Théorème 4 il suffit de montrer qu'il existe une infinité de ce type de corps cubiques possédant un discriminant qui est divisible par un nombre premier $\equiv 5 \pmod{8}$.

Considérons un corps engendré par l'équation

$$x^3 - rx + 1 = 0, \tag{12}$$

où r est un entier rationnel $\geqslant 3$. Nous formons le discriminant D de l'équation et considérons la congruence

$$D = 4r^3 - 27 \equiv 0 \pmod{q}.$$

Il est bien connu que cette congruence est résoluble pour tous les nombres premiers q qui sont $\equiv 5 \pmod 6$. Nous supposons de plus que $q \equiv 5 \pmod{24}$. D'après le lemme 1 nous pouvons choisir r tel que $4r^3 - 27$ soit divisible par q et non par q^2. Alors le discriminant des corps engendrés par l'équation (12) est divisible par q. En variant le nombre premier q on achève la démonstration du Théorème **6**.

§ 5. Les corps cubiques cycliques

10. Supposons maintenant que le corps cubique **K** soit cyclique. Dans ce cas le discriminant D^* du corps est égal à un carré parfait C^2. D'après l'expression (4) nous aurons d'abord à résoudre l'équation diophantienne

$$z^4 - 2z^3 - 5z^2 + 6z - 23 = D^* w^2 = (Cw)^2 = y^2 \tag{13}$$

en nombres entiers rationnels y et z.

Cette équation est un cas particulier d'un type d'équations pour lesquelles C. Runge a montré comment on peut déterminer toutes les solutions; voir [11] et aussi Nagell [12]. On trouve aisément que l'équation (13) n'admet que les solutions $z = -3$ et $= 4$ avec $y = 7$, $C = 7$ et $w = 1$. Les unités ε qu'on obtiendra pour ces valeurs de z sont les racines des équations suivantes

$$\left.\begin{array}{ll} x^3 + 2x^2 - x - 1 = 0, & x^3 + x^2 - 2x - 1 = 0. \\ x^3 + 3x^2 - 4x + 1 = 0, & x^3 - 4x^2 + 3x + 1 = 0, \\ x^3 - 5x^2 + 6x - 1 = 0, & x^3 - 6x^2 + 5x - 1 = 0. \end{array}\right\} \tag{14}$$

Toutes ces 18 unités ε, ayant la propriété que $\varepsilon - 1$ est aussi une unité, appartiennent au corps cubique engendré par le nombre $2 \cos (2\pi/7)$ et possèdent le discriminant 49.

Il nous reste à examiner le cas où ε est racine de l'équation

$$x^3 - px^2 + (p-3)x + 1 = 0. \tag{15}$$

Soient $D^* = C^2$ le discriminant du corps **K** et

$$D(\varepsilon) = (p^2 - 3p + 9)^2 = D^* y^2 \tag{16}$$

le discriminant de ε; C et y sont supposés positifs. En remplaçant p par z nous aurons la relation

$$z^2 - 3z + 9 = Cy. \tag{17}$$

Il en résulte que Cy est le produit de nombres premiers $\equiv 1 \pmod 6$ ou bien égal à un tel produit multiplié par 9 ou par 27.

Soit $1, \omega_1, \omega_2$ une base des entiers dans le corps **K** et posons

$$\varepsilon = u + v\omega_1 + w\omega_2,$$

u, v et w étant des entiers rationnels. Alors nous aurons de (15), après avoir remplacé p par z,

$$z = L(u, v, w), \tag{18}$$

où L signifie une forme linéaire en u, v et w à coefficients entiers rationnels. De plus

$$z-3=Q(u, v, w), \tag{19}$$

où Q signifie une forme quadratique en u, v et w à coefficients entiers rationnels. On aura encore

$$-1=F(u, v, w), \tag{20}$$

où F est une forme cubique en u, v et w à coefficients entiers rationnels. En éliminant z et u entre les équations (18), (19) et (20) on aura une relation

$$G(v, w)=0, \tag{21}$$

où G est un polynome en v et w du sixième degré à coefficients entiers rationnels. Le problème est donc réduit à résoudre l'équation (21) en nombres entiers rationnels v et w.

11. Nous allons établir le résultat suivant analogue au Théorème 5.

Théorème 7. *Il y a une infinité de corps cubiques cycliques dans lesquels il existe des unités de différence* 1.

Démonstration. Supposons qu'il y ait seulement les m corps cubiques cycliques

$$\mathbf{K}_1, \mathbf{K}_2, \ldots, \mathbf{K}_m \tag{22}$$

dans lesquels il existe des unités de différence 1. Désignons par

$$D_1^*, D_2^*, \ldots, D_m^* \tag{23}$$

les discriminants de ces corps. Nous considérons seulement les corps dont les discriminants ne sont pas divisibles par 3. Posons maintenant

$$H=D_1^* D_2^* \ldots D_m^*,$$

et désignons par K_{m+1} le corps engendré par une racine ε de l'équation

$$x^3-Hx^2+(H-3)x+1=0.$$

Alors le discriminant de ε a la valeur

$$(H^2-3H+9)^2.$$

Ce nombre est premier à chacun des nombres (23). Il en résulte que le discriminant de $\mathbf{K}_{m+1}$ est premier à chacun des nombres (23). Donc $\mathbf{K}_{m+1}$ est différent des corps (22), et le Théorème 7 se trouve démontré.

12. Il est même possible d'établir le résultat suivant analogue au Théorème 6 :

Théorème 8. *Il y a une infinité de corps cubiques cycliques dans lesquels il n'existe aucune couple d'unités de différence* 1.

Démonstration. Soit p un nombre premier $\equiv 1 \pmod 6$ et $\geqslant 13$. Soit de plus

$$4p=A^2+27B^2,$$

où A et B sont des nombres entiers rationnels, $A \equiv 1 \pmod 3$. Considérons le corps cubique cyclique engendré par les trois périodes η_0, η_1 et η_2 chacune constituée de la somme de $\frac{1}{3}(p-1)$ termes dans le corps cyclotomique $\mathbf{K}(e^{2\pi i/p})$. Les nombres η_0, η_1 et η_2 sont les racines de l'équation cubique

$$x^3 + x^2 - \tfrac{1}{3}(p-1)\,x - \tfrac{1}{27}(Ap + 3p - 1) = 0;$$

ils constituent une base des entiers du corps $\mathbf{K}(\eta_0)$. Le discriminant de ce corps a la valeur p^2, et le discriminant de η_0 a la valeur p^2B^2. Pour la démonstration de ces résultats voir Bachmann [14] et aussi Weber [15], p. 337–338.

L'anneau $\mathbf{R}(1, \eta_0, \eta_0^2)$ a le discriminant p^2B^2. Si α est un nombre de cet anneau on a

$$D(\alpha) = p^2B^2h^2,$$

où h est un nombre naturel. Soit E une unité $\neq \pm 1$ de l'anneau, et supposons que $E-1$ soit une autre unité. Alors, d'après le numéro 10 il faut qu'on ait

$$D(E) = (z^2 - 3z + 9)^2 = p^2B^2h_1^2,$$

où z et h_1 sont des nombres entiers rationnels différents de zéro. Or, cette relation est impossible si B est divisible par un nombre premier $\equiv -1 \pmod 3$. Choisissons par exemple le nombre premier $p = \frac{1}{4}(A^2 + 27B^2)$ tel que A et B soient pairs. D'après un résultat de Weber la forme quadratique $x^2 + 27y^2$ représente une infinité de nombres premiers; comparez Weber [16] et aussi Landau [17]. Donc, par ce choix de p, le Théorème 8 se trouve établi. Plus précisément nous avons démontré le

Théorème 8 bis. *Soit p un nombre premier $\equiv 1 \pmod 6$ et >7, tel que le nombre 2 soit un reste cubique modulo p. De plus, soit $\mathbf{K}$ un sous-corps cubique du corps cyclotomique $\mathbf{K}(e^{2\pi i/p})$. Alors, il n'existe dans $\mathbf{K}$ aucune couple d'unités de différence* 1.

En effet, la condition nécessaire et suffisante pour que le nombre 2 soit un reste cubique modulo p est qu'on ait $p = x^2 + 27y^2$, où x et y sont des nombres naturels. Voir Nagell [18], Théorème 4, p. 213, et aussi Nagell [19], p. 272.

On aura évidemment un résultat analogue en choisissant le nombre premier $p = \frac{1}{4}(A^2 + 27B^2)$ tel que B soit divisible par un nombre premier $\equiv -1 \pmod 6$.

§ 6. Sur une extension des problèmes

13. On peut aisément montrer qu'il existe une infinité de corps du degré donné n dans lesquels l'équation (1) possède des solutions. En effet, considérons l'équation

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + 1 = 0, \tag{24}$$

où les coefficients entiers rationnels sont choisis tels que l'équation soit irréductible et tels qu'on ait la relation

$$a_1 + a_2 + \ldots + a_{n-1} = -1.$$

Alors, si ε est une racine de (24), les deux nombres ε et $\varepsilon - 1$ sont des unités. Il est bien connu qu'il existe une infinité d'équations irréductibles du type (24) pour une valeur donnée de n.

Plus généralement nous pouvons noter le résultat suivant :

Théorème 9. *Soient $a_1, a_2, \ldots, a_n$ des nombres entiers rationnels, différents entre eux. Si ξ est une racine de l'équation du degré $n \geqslant 5$*

$$(x-a_1)(x-a_2)\ldots(x-a_n)\pm 1 = 0 \tag{25}$$

les n nombres $\xi - a_1, \xi - a_2, \ldots, \xi - a_n$ sont tous des unités du n-ième degré.

En effet, d'après un théorème de I. Schur le polynome (25) est irréductible; comparez G. Pólya [13], Bd. 2, probl. 121, 122, p. 136 et p. 346.

On peut appliquer ce résultat pour établir le

Théorème 10. *Soit* **K** *un corps algébrique du n-ième degré engendré par une racine ξ de l'équation*

$$x(x+1)(x+2)\ldots(x+n-1)\pm 1 = 0. \tag{26}$$

Alors, pour $n \geqslant 5$, l'équation (1) *possède au moins $3(n-1)$ solutions dans* **K**.

En effet, nous avons les relations entre unités

$$\left.\begin{aligned} &(\xi+k)+(-\xi-k+1)=1,\\ &\frac{1}{\xi+k}+\frac{\xi+k-1}{\xi+k}=1,\\ &\frac{\xi+k}{\xi+k-1}+\frac{-1}{\xi+k-1}=1, \end{aligned}\right\} \tag{27}$$

pour $k = 1, 2, \ldots, n-1$. Donc, il est évident que le nombre m de solutions est $\geqslant 3(n-1)$.

On en conclut que le nombre m peut surpasser toute limite donnée d'avance pour des corps de degré suffisamment grand.

Il est d'ailleurs possible d'améliorer le résultat du Théorème **10** de la manière suivante.

Outre les relations (27) nous avons aussi les trois relations entre unités :

$$\left.\begin{aligned} &(\xi+h)^2+[-(\xi+h-1)(\xi+h+1)]=1,\\ &\frac{1}{(\xi+h)^2}+\frac{(\xi+h-1)(\xi+h+1)}{(\xi+h)^2}=1,\\ &\frac{-1}{(\xi+h-1)(\xi+h+1)}+\frac{(\xi+h)^2}{(\xi+h-1)(\xi+h+1)}=1, \end{aligned}\right\} \tag{28}$$

pour $h = 1, 2, \ldots, n-2$. Vu que $n \geqslant 5$ il est évident que les solutions données par (27) et (28) sont distinctes. Il en résulte le

Théorème 10 bis. *Dans un corps* **K** *engendré par l'équation* (26), *où $n \geqslant 5$, on a*

$$m \geqslant 3(n-1)+3(n-2) = 3(2n-3).$$

En employant la même méthode aux corps engendrés par l'équation

$$x(x+1)(x+2)\ldots(x+n-2)(x+a)\mp 1 = 0,$$

où $n \geqslant 6$ et où a est un nombre entier rationnel $\geqslant n-1$ ou <0, on obtiendra pour le maximum du nombre m la borne inférieure $3(2n-5)$. Par conséquent :

Il y a une infinité de corps du n-ième degré tels que $m \geqslant 3(2n-5)$.

En effet, il est possible de varier le nombre a de manière que les corps obtenus soient différents entre eux.

14. Si l'on prend dans (26) $n=3$, on vérifie sans peine que cette équation est irréductible pour tous les deux signes et que le discriminant des corps est dans tous les deux cas $=-23$. Pour cette valeur du discriminant le problème est complètement résolu dans le Théorème 2; on a $m=6$.

Posons ensuite dans (26) $n=4$. Pur le signe inférieur l'équation est réductible $=(x^2+3x+1)^2$. Pour le signe supérieur nous aurons, en posant $x=z-1$, l'équation

$$z(z^2-1)(z+2)=1, \tag{29}$$

qui est irréductible. Le rang des corps est $=2$. Il y a un sous-corps engendré par $\sqrt{2}$. Donc les corps conjugués sont identiques deux à deux; comparez pour ces faits Nagell [20]. Soit ξ une racine de (29). Lesquelles sont alors les relations entre unités qui sont possibles dans le corps $\mathbf{K}(\xi)$? Nous avons d'abord trois triplets du type (27), pour $k=1$, 2 et 3. Nous avons ensuite deux triplets du type (28), pour $h=1$ et 2. Cependant, ces derniers deux triplets coincident vu que les deux relations

$$1=\frac{-1}{\xi(\xi+2)}+\frac{(\xi+1)^2}{\xi(\xi+2)} \quad \text{et} \quad \xi^2+(1-\xi^2)=1$$

sont les mêmes; en effet, on a

$$1-\xi^2=\frac{-1}{\xi(\xi+2)}.$$

Jusqu'ici nous avons donc obtenu $m \geqslant 9+3=12$.

Soit maintenant $\mathbf{K}'$ le corps conjugué à $\mathbf{K}$ et identique à $\mathbf{K}$. Alors en passant des 12 relations en $\mathbf{K}$ aux 12 relations conjuguées en $\mathbf{K}'$ nous aurons 24 relations entre unités. Si ξ' est le conjugué à ξ dans K' on trouvera aisément que $\xi'=-1-\xi$. Il en résulte que les relations conjuguées sont identiques aux relations originaires. Par conséquent, nous avons obtenu le résultat :

Pour les corps biquadratiques du second rang le maximum du nombre m est $\geqslant 12$.

Nous finissons avec l'exemple suivant d'un corps biquadratique du troisième rang engendré par l'équation

$$x^4-5x^2+3=0,$$

dont toutes les racines sont réelles. Si ξ est une racine de cette équation les nombres $\xi-1$, $\xi-2$, $\xi+1$ et $\xi+2$ sont des unités. Par les méthodes développées dans ce qui précède nous aurons seulement $m \geqslant 6$. Donc :

Pour les corps biquadratiques non-abéliens du troisième rang le maximum du nombre m est $\geqslant 6$.

Nous avons déjà vu que le maximum de m est $=10$ pour les corps biquadratiques du premier rang.

15. Nous finissons avec quelques remarques sur le corps cubique cyclique engendré par le nombre $2\cos(2\pi/7)$. Ce corps a le discriminant 49, ce qui est la plus petite

valeur possible pour les corps cubiques cycliques. Considérons de nouveau les équations (14). Désignons par E le nombre $2\cos(2\pi/7)$. Alors on vérifie sans peine les résultats suivants. Les racines de l'équation $x^3+x^2-2x-1=0$ sont

$$E,\ -1-E^{-1},\ -(1+E)^{-1}. \tag{30}$$

Les racines de l'équation $x^3+3x^2-4x+1=0$ sont

$$E(2E+1)^{-1},\ (E+1)(E+2)^{-1},\ (1-E)^{-1}. \tag{31}$$

Les racines de l'équation $x^3-5x^2+6x-1=0$ sont

$$1-E^{-1},\ E^2=(2E+1)(E+1)^{-1},\ E+2. \tag{32}$$

Les racines des trois autres équations dans (14) sont évidemment les inverses des nombres (30), (31) et (32). Nous en obtenons les neuf solutions suivantes de l'équation (1) :

$$E+(1-E)=1,\ E^{-1}+(1-E^{-1})=1,\ E+2+(-E-1)=1,$$

$$(1-E)^{-1}+E(E-1)^{-1}=1,\ (-1-E^{-1})+(2+E^{-1})=1,$$

$$-(1+E)^{-1}+(E+2)(E+1)^{-1}=1,\ (E+1)(E+2)^{-1}+(E+2)^{-1}=1,$$

$$E(2E+1)^{-1}+(1+E)(2E+1)^{-1}=1,\ -E(E+1)^{-1}+(2E+1)(E+1)^{-1}=1.$$

Vu que tous les nombres dans la sequence

$$E-1,\ E,\ E+1,\ E+2$$

sont des unités il faut aussi examiner si les relations (27) donnent des solutions ultérieures de l'équation (1). En effet, on aura alors les trois solutions suivantes :

$$E+1+(-E)=1,\ -E^{-1}+(1+E^{-1})=1,\ (1+E)^{-1}+E(1+E)^{-1}=1,$$

et pas d'autres. Il faut ensuite examiner si l'on obtient des solutions ultérieures de (1) à l'aide des relations (28). En vertu des égalités

$$E^2=(2E+1)(E+1)^{-1} \quad \text{et} \quad (E+1)^2=E(E-1)^{-1}$$

il est évident que cela n'est pas le cas. Il résulte de tout cela : *Le maximum du nombre m pour les corps cubiques cycliques est* $\geqslant 12$. Il est vraisemblable que le maximum soit >12.

16. Il reste encore un grand nombre de problèmes à résoudre à propos du nombre m. Mentionnons par exemple les questions suivantes : Les nombres naturels n et r étant donnés, existe-t-il une infinité de corps de degré n et de rang r pour lesquels le nombre $m=0$ ou pour lesquels $m>0$? Nous avons résolu ce problème pour $n=2$ et $n=3$ et pour $n=4$ lorsque $r=1$. Nous n'avons pas encore la réponse pour $n=4$ lorsque $r>1$, et non plus pour $n\geqslant 5$.

Il se présente aussi le problème suivant : Trouver une limite supérieure, en fonction de n, pour le nombre m de solutions de l'équation (1) valable pour tout corps algébrique du n-ième degré. Il reste à résoudre ce problème pour $n=4$ lorsque $r>1$ et pour $n\geqslant 5$.

Il est facile d'indiquer des solutions de l'équation (1) dans les corps cyclotomiques. Désignons par ξ une racine n-ième primitive de l'unité. Alors, si n n'est pas de la forme p^α, p nombre premier, il est bien connu que le nombre $1-\xi$ est une unité.

Il est évident que ce fait donnera au moins $\frac{3}{2}\varphi(n)$ solutions de l'équation (1), sauf pour $n=6$. De plus, si n n'est pas de la forme $2p^{\alpha}$, p nombre premier, le nombre $1+\xi$ est une unité. Ce cas fournira aussi au moins $\frac{3}{2}\varphi(n)$ solutions, sauf pour $n=3$. On aura outre cela un nombre de solutions dans les sous-corps. Nous allons revenir sur ces problèmes.

INDEX BIBLIOGRAPHIQUE

1. NAGELL, T., Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante, Mathematische Zeitschrift, Bd. 28, Berlin 1928.
2. NAGELL, T., Les points exceptionnels rationnels sur certaines cubiques du premier genre, Acta Arithmetica, 5 (1959), Warszawa.
3. NAGELL, T., Les points exceptionnels sur les cubiques $ax^3+by^3+cz^3=0$, Acta Scientiarum Mathematicarum, XXI (1960), Szeged.
4. NAGELL, T., Sur une propriété des unités d'un corps algébrique, Arkiv för matematik, Bd. 5, nr. 25, Stockholm 1964.
5. NAGELL, T., Sur les unités dans les corps biquadratiques primitifs du premier rang, Arkiv för matematik, Bd. 7, nr. 27, Stockholm 1968.
6. CHOWLA, S., Proof of a conjecture of Julia Robinson, Det kongelige norske videnskabers selskabs forhandlinger, Bd. 34, Nr. 20, Trondheim 1961.
7. 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.
8. NAGELL, T., Remarques sur les formes à plusieurs variables décomposables en facteurs linéaires, Arkiv för matematik, Bd. 7, nr. 23, Stockholm 1967.
9. NAGELL, T., Introduction to number theory, New York 1950.
10. NAGELL, T., Sur la résolubilité des équations diophantiennes cubiques à deux inconnues dans un domaine relativement algébrique, Nova Acta Regiæ Soc. Scient. Ups., Ser. IV, Vol. 13, Nr. 3, Uppsala 1942.
11. RUNGE, C., Über ganzzahlige Lösungen von Gleichungen mit zwei Veränderlichen, Journ. für Mathematik, Bd. 100, Berlin 1887.
12. NAGELL, T., Vollständige Lösung der unbestimmten Gleichung $z^4+az^3+bz^2+cz+d=y^2$, Zahlentheoretische Notizen VIII, Norsk matem. forening skrifter, Ser. I, Nr. 17, Oslo 1927.
13. PÓLYA, G., Aufgaben und Lehrsätze, Bd. 2, Berlin 1928.
14. BACHMANN, P., Die Lehre von der Kreistheilung, Leipzig 1872.
15. WEBER, H., Kleines Lehrbuch der Algebra, Braunschweig 1912.
16. WEBER, H., Beweis des Satzes dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist, Mathem. Annalen, Bd. 20, 1882.
17. LANDAU, E., Über die Verteilung der Primideale in den Idealklassen eines algebraischen Zahlkörpers, Mathem. Annalen, Bd. 63, 1907.
18. NAGELL, T., Sur quelques problèmes dans la théorie des restes quadratiques et cubiques, Arkiv för matematik, Bd. 3, nr. 16, Stockholm 1955.
19. NAGELL, T., Quelques résultats sur les diviseurs fixes de l'index des nombres entiers d'un corps algébrique, Arkiv för matematik, Bd. 6, nr. 15, Stockholm 1965.
20. NAGELL, T., Sur quelques questions dans la théorie des corps biquadratiques, Arkiv för matematik, Bd. 4, nr. 26, Stockholm 1961.

Errata au travail [*19*]:

Page 276, lignes 2 et 5, a jouter le mot *différents* après le mot premiers.
Page 280, dans les lignes 14 et 16, à partir d'en bas, remplacer $\frac{1}{10}$ par $\frac{1}{12}$.
Page 284, ligne 6, remplacer mod 4 par mod 8.
Page 284. La ligne 14 doit être remplacée par : Le nombre 2 est évidemment un reste quadratique modulo p.
Page 286, ligne 5, lire 14 au lieu de 13; ligne 13, à partir d'en bas, lire 15 au lieu de 14.
Page 287, ligne 1, lire 16 au lieu de 15.

Tryckt den 17 december 1969

Uppsala 1969. Almqvist & Wiksells Boktryckeri AB