ARKIV FÖR MATEMATIK Band 6 nr 15

1.65 06 2 Communiqué le 14 avril 1965

Quelques résultats sur les diviseurs fixes de l'index des nombres entiers d'un corps algébrique

Par TRYGVE NAGELL

§ 1. Lemmes sur les formes binaires

1. *Résumé de quelques résultats antérieurs*

Il est bien connu que la condition nécessaire et suffisante pour que le polynôme $f(x)$ représente des nombres entiers pour toutes les valeurs entières de x, est que $f(x)$ soit de la forme

$$f(x) = A_0 + A_1\binom{x}{1} + A_2\binom{x}{2} + \ldots + A_n\binom{x}{n}, \tag{1}$$

où les coefficients $A_0, A_1, \ldots, A_n$ sont des nombres entiers.

On peut y ajouter la proposition suivante:

Si le polynôme $f(x)$ du n-ième degré représente des entiers pour $n+1$ valeurs entières consécutives de x, $f(x)$ est un nombre entier pour toute valeur entière de x.

Soit $f(x)$ un polynôme du type (1) à coefficients entiers $A_0, A_1, \ldots, A_n$. Si tous les nombres $f(x)$, pour x entier, sont divisibles par le nombre naturel δ nous dirons que δ est un *diviseur fixe* de $f(x)$. Alors, nous pouvons énoncer les résultats suivants:

La condition nécessaire et suffisante pour que le polynôme (1) *ait le diviseur fixe δ, est que tous les coefficients $A_0, A_1, \ldots, A_n$ soient divisibles par δ.*

Si un polynôme $f(x)$ du n-ième degré représente des nombres entiers divisibles par le nombre naturel δ pour $n+1$ valeurs entières consécutives de x, ce polynôme a le diviseur fixe δ.

J'ai publié les démonstrations de ces quatre propositions en 1918; voir Nagell [1][1], p. 53–62; comparez aussi Nagell [2], p. 120–122. Dans un autre travail j'ai établi des résultats analogues pour les polynômes de plusieurs variables; voir Nagell [3], p. 2–11. La notion de diviseur fixe peut évidemment être étendue au cas de plusieurs variables. Si δ est le diviseur fixe *maximal* d'un polynôme, tout autre diviseur fixe du polynôme divise δ. Soit $f(x)$ un polynôme *primitif* du n-ième degré en x; alors tout diviseur fixe de $f(x)$ divise le nombre $n!$.

Dans ce paragraphe « nombre entier » a partout la signification « nombre entier rationnel ». Dans la suite nous considérons seulement des polynômes à coefficients entiers rationnels.

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

2. *Lemmes sur les formes binaires*

Nous désignerons par le symbole $((a_0, a_1, a_2, \ldots, a_n))$ la forme binaire du n-ième degré

$$F(x,y) = a_0x^n + a_1x^{n-1}y + \ldots + a_ny^n, \tag{2}$$

où les coefficients a_i sont des entiers.

La proposition suivante est évidente :

Lemme 1. *Supposons que la forme* (2) *admet le diviseur fixe* δ. *Par la transformation linéaire*

$$x = eu + fv,\ y = gu + hv,$$

où e, f, g *et* h *sont des nombres entiers, tels que* $eh - fg \neq 0$, *la forme* $F(x,y)$ *sera transformée dans la forme binaire* $G(u,v)$. *Alors* $G(u,v)$ *admet aussi le diviseur fixe* δ. *Si la transformation est unimodulaire les deux formes ont les mêmes diviseurs fixes.*

Remarque. Il peut arriver que $G(u,v)$ admet un diviseur fixe $\delta_1 = k\delta$, où le nombre naturel k est >1. Il faut observer que $G(u,v)$ n'est pas nécessairement primitive lorsque $F(x,y)$ est primitive. Si $F(x,y)$ est primitive et si la transformation est unimodulaire, $G(u,v)$ est toujours primitive.

On vérifie aisément le résultat suivant :

Lemme 2. *Supposons que la forme* $F(x,y)$ *du n-ième degré représente le nombre entier* c *pour* $x = x_0$, $y = y_0$, *où* x_0 *et* y_0 *sont des entiers. Alors, celle-ci sera transformée par la transformation*

$$x = x_0u + fv, \quad y = y_0u + hv,$$

où f *et* h *sont des nombres entiers tels que* $x_0h - y_0f \neq 0$, *dans une forme* $G(u,v)$, *où le coefficient de* u^n *est égal à* c.

Dans un travail antérieur j'ai établi le résultat suivant :

Lemme 3. *Tout diviseur fixe d'une forme binaire primitive du n-ième degré divise le nombre* $(n-1)!$.

Si $n = 3$ *le diviseur fixe* (>1) *peut seulement avoir la valeur* 2. *Si* $n = 4$ *le diviseur fixe* (>1) *ne peut avoir que les valeur* 2, 3 *et* 6.

La condition nécessaire et suffisante pour que la forme cubique $((a, b, c, d))$ *primitive ait le diviseur fixe* 2, *est que* a *et* d *soient pairs, tandis que* b *et* c *soient impairs.*

Pour la démonstration voir Nagell [3], p. 2–11.

Supposons donnée la forme $((a_0, a_1, \ldots, a_n))$ du n-ième degré, irréductible dans le corps rationnel, et soit θ une racine de l'équation

$$a_0x^n + a_1x^{n-1} + \ldots + a_n = 0.$$

Alors, nous dirons que le corps $\mathbf{K}(\theta)$ est engendré par la forme $((a_0, a_1, \ldots, a_n))$. Nous dirons aussi que la forme est construite sur le corps $\mathbf{K}(\theta)$.

Soit $\mathbf{R}$ un anneau entier composé de nombres entiers appartenant à $\mathbf{K}(\theta)$. Nous dirons que $\mathbf{R}$ est du n-ième degré s'il contient des nombres générateurs de $\mathbf{K}(\theta)$. $\mathbf{R}$ sera dit *ordinaire* s'il contient le nombre 1. Par $\mathbf{R}(1, \alpha_1, \alpha_2, \ldots, \alpha_{n-1})$ nous désignerons un anneau ayant la base $1, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}$.

§ 2. Formes binaires et corps cubiques

3. *Le théorème de F. Levi*

Dans ce numéro nous supposons donné le corps cubique $\mathbf{K}(\theta)$. Forme signifiera une forme binaire cubique à coefficients entiers rationnels, construite sur le corps $\mathbf{K}(\theta)$; cette forme est irréductible dans le corps des nombres rationnels. Anneau signifiera un anneau entier ordinaire du troisième degré appartenant à $\mathbf{K}(\theta)$.

Entre les classes des formes binaires cubiques et les anneaux du troisième degré il existe une correspondence biunivoque qui a été découverte par F. Levi; voir Levi [4]. Pour formuler son résultat rappelons d'abord le fait (dû à Voronoï) qu'une base $1, \alpha, \beta$ de l'anneau cubique $\mathbf{R}(1, \alpha, \beta)$ peut être choisie de façon qu'on ait les relations

$$\alpha^3 - b\alpha^2 + ac\alpha - a^2 d = 0, \quad \beta^3 - c\beta^2 + bd\beta - ad^2 = 0, \quad \alpha\beta = ad,$$

où a, b, c et d sont des nombres entiers rationnels. Alors, le théorème de Levi peut être formulé ainsi qu'il suit :

Soient α, β, α_1 et β_1 des nombres entiers du troisième degré dans le corps cubique $\mathbf{K}(\theta)$, tels que

$$\alpha^3 - b\alpha^2 + ac\alpha - a^2 d = 0, \quad \alpha\beta = ad,$$

$$\alpha_1^3 - b_1\alpha_1^2 + a_1 c_1 \alpha_1 - a_1^2 d_1 = 0, \quad \alpha_1\beta_1 = a_1 d_1.$$

Alors, si les anneaux $\mathbf{R}(1, \alpha, \beta)$ et $\mathbf{R}(1, \alpha_1, \beta_1)$ sont identiques, les formes binaires cubiques

$$((a, b, c, d)) \quad \text{et} \quad ((a_1, b_1, c_1, d_1))$$

sont équivalentes; et inversement, l'équivalence des deux formes entraîne l'identité des anneaux. Les formes et les anneaux ont le même discriminant.

Le discriminant de la forme $((a, b, c, d))$ ainsi que celui de l'anneau $\mathbf{R}(1, \alpha, \beta)$ a pour expression

$$b^2c^2 + 18abcd - 4ac^3 - 4db^3 - 27a^2d^2. \tag{3}$$

L'anneau de tous les nombres entiers du corps $\mathbf{K}(\theta)$ s'appellera l'*anneau fondamental*. La classe des formes correspondant à cet anneau sera appelée la *classe fondamentale*.

Il faut observer que, dans le théorème de Levi, il peut arriver que les formes sont imprimitives.

Soit $\mathbf{R}(1, \alpha, \beta)$ l'anneau fondamental, où α et β satisfont aux relations

$$\alpha^3 - b\alpha^2 + ac\alpha - a^2 d = 0, \quad \alpha\beta = ad. \tag{4}$$

Si le plus grand commun diviseur des nombres a, b, c et d est égal à δ, il est évident que le nombre α/δ est entier. Or, si $\delta > 1$, cela est impossible vu qu'une relation

$$\alpha/\delta = x\alpha + y\beta + z$$

ne peut pas subsister pour x, y et z entiers rationnels. On a donc :

Lemme 4. *Les formes de la classe fondamentale sont primitives. Dans une base de l'anneau fondamental donné par* (4) *le plus grand commun diviseur des nombres a, b, c et d est égal à* 1.

4. *Le nombre 2 comme facteur commun de tous les indices*

Soit $\mathbf{K}(\theta)$ un corps du n-ième degré engendré par le nombre algébrique entier θ. Si D^* signifie le discriminant du corps l'index $I(\theta)$ de θ est le nombre $\sqrt{D(\theta)/D^*}$. Si le nombre premier p divise tous les indices $I(\theta)$, θ entier, du corps, nous disons, pour raccourcir, que p est un f. c. i. (=facteur commun de tous les indices) dans le corps. On sait que les nombres premiers de ce type ne paraissent que dans certaines catégories de corps.

Supposons maintenant que le corps $\mathbf{K}(\theta)$ est cubique. Alors, il est bien connu que le nombre 2 est le seul nombre premier qui peut être un f. c. i. L'exemple classique, qu'on trouve dans tous les exposés, a été donné par Dedekind. Il s'agit des corps définis par l'équation

$$x^3 - x^2 - 2x - 8 = 0;$$

dans ces corps le nombre 2 est un f. c. i. Voir p. ex. Bachmann [5], p. 280–283, Hensel [6], p. 271–274, Fricke [7], p. 108–110, Hasse [8], p. 328–337. Un autre exemple a été donné par Hensel [9], p. 147–150, qui a établi le théorème suivant :

Soit p un nombre premier $\equiv 1$ (mod 6), et soit $\mathbf{K}$ le corps cubique engendré par les trois périodes constituées de la somme de $\frac{1}{3}(p-1)$ termes dans le corps cyclotomique $\mathbf{K}(e^{2\pi i/p})$. Alors, la condition nécessaire et suffisante pour que le nombre 2 soit un f. c. i. dans $\mathbf{K}$ est qu'on ait $p = x^2 + 27y^2$, où x et y sont des nombres naturels.

D'après un résultat bien connu (voir p. ex. Nagell [10], théorème 4) cette condition peut être remplacée par la suivante : *Il faut et il suffit que le nombre 2 soit un reste cubique modulo p.* Ce théorème nous donne une infinité de corps cubiques cycliques dans lesquels le nombre 2 est un f. c. i.

Nous nous proposons de déterminer tous les corps cubiques jouissant de cette propriété. Grâce au théorème de Levi nous pouvons obtenir ce résultat par des raisonnements très simples.

Soit 1, α, β une base des entiers du corps cubique $\mathbf{K}$, telle qu'on ait

$$\alpha^3 - b\alpha^2 + ac\alpha - a^2d = 0,\ \beta^3 - c\beta^2 + bd\beta - ad^2 = 0,\ \alpha\beta = ad.$$

Alors, le discriminant du corps ainsi que celui de la forme $((a, b, c, d))$ a pour expression

$$D^* = b^2c^2 + 18abcd - 4ac^3 - 4db^3 - 27a^2d^2. \tag{5}$$

Le discriminant de tout autre représentant de la classe fondamentale a la même valeur.

Soit θ un nombre entier quelconque dans $\mathbf{K}$,

$$\theta = x\alpha - y\beta + z,$$

où x, y et z sont des entiers rationnels. Donc

$$\theta^2 = x_1\alpha + y_1\beta + z_1,$$

où $x_1 = bx^2 + dy^2 + 2xz$ et $y_1 = ax^2 + cy^2 - 2yz$. Il en résulte que

$$D(\theta) = (ax^3 + bx^2y + cxy^2 + dy^3)^2 D^*, \tag{6}$$

où la forme $((a, b, c, d))$ est un représentant de la classe fondamentale des formes. D'après le lemme 4 cette forme est *primitive*, et d'après le lemme 3 tout diviseur fixe de la forme est $\leqslant 2$. Il en résulte :

Si le nombre naturel $v>1$ divise tous les indices $I(\theta)$ dans le corps cubique on a $v=2$.

Si la forme $((a, b, c, d))$ a le diviseur fixe 2, il résulte de la formule (6) que tous les indices dans le corps sont des nombres pairs. D'après la dernière partie du lemme 3 il faut alors que les coefficients a et d soient pairs tandis que b et c soient impairs.

De tout cela il résulte :

Théorème 1. *Soit $((a, b, c, d))$ un représentant de la classe fondamentale des formes binaires cubiques construites sur le corps cubique* **K**. *La condition nécessaire et suffisante pour que le nombre premier 2 soit un f. c. i. dans* **K** *est que les nombres a et d soient pairs tandis que b et c soient impairs.*

Dans la démonstration nous n'avons pas fait usage de la décomposition de 2 en idéaux premiers. On peut, bien entendu, remplacer la classe fondamentale des formes par l'anneau fondamental. On voit d'ailleurs sans difficulté que la classe fondamentale des formes (l'anneau fondamental) peut être remplacée par une autre classe (anneau) ayant un discriminant impair.

Considérons maintenant toutes les formes $((a, b, c, d))$ pour $|a| \leqslant z$, $|b| \leqslant z$, $|c| \leqslant z$ et $|d| \leqslant z$, où les nombres a, b, c et d ne sont pas pairs tous les quatre à la fois. Le nombre de ces formes est de l'ordre de grandeur $15z^4$. En tenant compte du théorème 1 il semble naturel de proposer l'hypothèse suivante : Soit $A(x)$ le nombre de corps cubiques pour lesquels la valur absolue du discriminant est $\leqslant x$. Alors, parmi ces corps il y a approximativement $\frac{1}{15}A(x)$ corps dans lesquels le nombre 2 est un f. c. i.

Remarque. Soit donné le corps cubique **K** dans lequel le nombre 2 est un f. c. i. Alors, on sait, d'après la théorie générale de Hensel, que l'idéal (2) est le produit de trois idéaux premiers distincts; comparez le numéro 5. Nous allons montrer comment ce résultat peut être obtenu par un raisonnement très simple Soit 1, α, β une base des entiers de **K** donnée par les relations (4). Alors, on a évidemment

$$\alpha^2 - \alpha \equiv \alpha^2 - b\alpha \equiv -ac + a\frac{ad}{\alpha} \equiv 0 \pmod 2,$$

$$\beta^2 - \beta \equiv \beta^2 - c\beta \equiv -bd + d\frac{ad}{\beta} \equiv 0 \pmod 2,$$

vu que a et d sont pairs. Tout nombre entier γ du corps est de la forme

$$\gamma = x_0 + x_1\alpha + x_2\beta,$$

x_0, x_1 et x_2 étant des nombres entiers rationnels. Donc

$$\gamma^2 \equiv x_0^2 + x_1^2\alpha^2 + x_2^2\beta^2 \pmod 2,$$

et $$\gamma^2 - \gamma \equiv x_0^2 - x_0 + \alpha(x_1^2 - x_1) + x_1^2(\alpha^2 - \alpha) + \beta(x_2^2 - x_2) + x_2^2(\beta^2 - \beta) \pmod 2.$$

Par conséquent, pour tout nombre entier γ du corps on a

$$\gamma^2 \equiv \gamma \pmod 2.$$

Cela signifie que l'idéal (2) est le produit de trois idéaux premiers du premier degré. Ces idéaux sont distincts, vu que le discriminant du corps est impair.

Tous les idéaux qui divisent (2) se trouvent parmi les idéaux $(2,\alpha)$, $(2,\beta)$, $(2,1+\alpha)$, $(2,1+\beta)$, $(2,\alpha+\beta)$, $(2,1+\alpha+\beta)$, (1) et (2), où 1, α, β est une base des entiers du corps. Cela peut servir à déterminer la décomposition de (2) en idéaux premiers.

§ 3. Contributions à la théorie des nombres premiers f. c. i. dans un corps de degré supérieur à 3

5. *Généralités*

Soit $F(x_1, x_2, \ldots, x_r)$ une forme du m-ième degré des $r(\geqslant 2)$ variables $x_1, x_2, \ldots, x_r$, à coefficients entiers rationnels et primitive, et soit δ un diviseur fixe de la forme. Si $r=2$ nous savons, d'après le lemme 2, que δ est un diviseur de $(m-1)!$ Or, *cela est vrai même pour* $r \geqslant 3$. Pour le voir on aura seulement à mettre $x_3 = \ldots = x_r = 0$. Donc, il suffit de considérer les formes binaires quant aux diviseurs fixes.

Soit maintenant **K** un corps algébrique du n-ième degré dont une base des entiers est donnée par $1, \omega_1, \omega_2, \ldots, \omega_{n-1}$. Soit θ un nombre entier quelconque qui engendre le corps :

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

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

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

D^* étant le discriminant du corps. L'index $I(\theta)$ de θ est une forme primitive des $n-1$ variables $x_1, x_2, \ldots, x_{n-1}$ de degré $\frac{1}{2}n(n-1)$ à coefficients entiers rationnels.

Supposons maintenant que le nombre premier p est un f. c. i. (=facteur commun de tous les indices) dans le corps **K**. D'après ce que nous venons de dire sur les diviseurs fixes des formes de plusieurs variables, il faut alors que $p \leqslant \frac{1}{2}n(n-1)-1$. D'ailleurs nous allons voir qu'on a encore $p \leqslant n-1$ (théorème 2).

Hensel a donné le critère suivant pour que le nombre premier p soit un f. c. i. dans le corps **K**.

Soient $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ *les différents idéaux premiers qui divisent le nombre premier* p, *où* $\mathfrak{p}_k$ *a le degré* f_k. *Désignons par* $f_1^*, f_2^*, \ldots, f_s^*$ *les nombres parmi les degrés* f_k *qui sont différents entre eux, et soit* t_i *le nombre des degrés* f_k *qui ont la valeur* f_i^*. *Alors, on a* $t_1 + t_2 + \ldots + t_s = r$ *et*

$$f_1 + f_2 + \ldots + f_r = t_1 f_1^* + t_2 f_2^* + \ldots + t_s f_s^*.$$

De plus, désignons par $G_p(f)$ *le nombre*

$$\sum_d \mu(d) p^{f/d},$$

où la somme est étendue à tous les diviseurs positifs d de f.

Alors, pour que p soit un f. c. i. dans le corps **K**, *il faut et il suffit qu'une au moins des inégalités*

$$t_i f_i^* > G_p(f_i^*) \tag{7}$$

soit satisfaite.

Voir Hensel [6], p. 278–279 ou Bachmann [5], p. 276.

Une conséquence immédiate du théorème de Hensel est la proposition :

Lemme 5. *Si p est le produit de n idéaux premiers distincts, et si $p<n$, le nombre premier p est un f. c. i. dans le corps.*

Voir Hensel [6], p. 274.

A ce résultat nous ajoutons le

Théorème 2. *Tous les nombres premiers f. c. i. dans un corps de degré n sont $\leqslant n-1$.*

Démonstration. Avec les notations du théorème de Hensel nous avons

$$f_1 + f_2 + \ldots + f_r = t_1 f_1^* + t_2 f_2^* + \ldots + t_s f_s^*.$$

Donc, pour tous les $i = 1, 2, \ldots, s$,

$$t_i f_i^* \leqslant f_1 + f_2 + \ldots + f_r \leqslant n.$$

Si le nombre premier p est $\geqslant n$, on a évidemment

$$G_p(f_i^*) \geqslant p \geqslant n.$$

Il en résulte, pour toutes les valeurs de i,

$$t_i f_i^* \leqslant n \leqslant G_p(f_i^*).$$

Donc, d'après le théorème de Hensel, on conclut que p n'est jamais un f. c. i.

Nous ajoutons encore la proposition suivante :

Théorème 3. *Le nombre premier p n'est jamais un f. c. i. dans le corps, si l'idéal (p) est un idéal premier ou la puissance d'un idéal premier.*

Démonstration. Supposons que $(p) = \mathfrak{p}^m$ où $\mathfrak{p}$ est un idéal premier du degré n/m, m étant un diviseur de n. On a, dans ce cas, $r = s = 1$, $f_1^* = n/m$ et $t_1 = 1$. Maintenant, rappelons le fait que le nombre $G_p(h)$, h nombre naturel, est positif et divisible par h (voir p. ex. Bachmann [13], p. 372–375); donc $G_p(h) \geqslant h$. Il en résulte que

$$t_1 f_1^* = \frac{n}{m} \leqslant G_p\left(\frac{n}{m}\right) = G_p(f_1^*).$$

En vertu du théorème de Hensel on conclut alors que p n'est pas un f. c. i. dans le corps.

Il est facile de vérifier le résultat suivant :

Lemme 6. *Soient $c_1, c_2, \ldots, c_n (n \geqslant 2)$ des nombres entiers rationnels tels que le corps*

$$\mathbf{K} = \mathbf{K}(\sqrt{c_1}, \sqrt{c_2}, \ldots, \sqrt{c_n})$$

soit du degré 2^n.

1°) *Si l'on a* $c_1 \equiv c_2 \equiv \ldots \equiv c_n \equiv 1 \pmod 8$, *l'idéal* (2) *est égal au produit de* 2^n *idéaux premiers dans* **K**.

2°) *Si* p *est un nombre premier impair tel qu'on ait*

$$\left(\frac{c_1}{p}\right) = \left(\frac{c_2}{p}\right) = \ldots = \left(\frac{c_n}{p}\right) = +1,$$

l'idéal (p) *est égal au produit de* 2^n *idéaux premiers dans* **K**.

Pour la démonstration voir Värmon [18], p. 62–63.

En combinant ce résultat avec le lemme 5 on obtient le

Théorème 4. 1°) *Les conditions de la première partie du lemme* 6 *étant remplies, le nombre* 2 *est un f. c. i. dans le corps.*

2°) *Les conditions de la seconde partie du lemme* 6 *étant remplies, le nombre premier* p *est un f. c. i. dans le corps, pourvu que* $p < 2^n$.

On en conclut : Si p est un nombre premier $< 2^n, n \geqslant 2$, il existe une infinité de corps de degré 2^n dans lesquels p est un f. c. i.

6. *Les corps biquadratiques*

Considérons maintenant le cas où le corps **K** est du quatrième degré. Alors, d'après le théorème 2 il n'y a que les deux possibilités $p = 2$ et $p = 3$ pour un nombre premier f. c. i. A l'aide du théorème de Hensel il est facile d'établir les résultats suivants :

Théorème 5. *Pour que le nombre premier* 2 *soit un f. c. i. dans un corps biquadratique il faut et il suffit qu'on ait l'un des trois cas suivants :* 1°) *l'idéal* (2) *est le produit de quatre idéaux premiers différents entre eux;* 2°) *l'idéal* (2) *est le produit de quatre idéaux premiers, dont trois sont différents entre eux, tandis que deux coincident;* 3°) *l'idéal* (2) *est le produit de deux idéaux premiers différents entre eux, tous les deux du second degré.*

Théorème 6. *Pour que le nombre premier* 3 *soit un f. c. i. dans un corps biquadratique il faut et suffit que l'idéal* (3) *soit le produit de quatre idéaux premiers différents entre eux.*

Démonstration du théorème 5. Vu que $G_p(f_i^*) \geqslant f_i^*$, il suffit de considérer les cas où $t_i \geqslant 2$ et $r \geqslant 2$. En ayant égard au lemme 5 et au théorème 3, on peut se borner à examiner les cas où l'idéal (2) a l'une des décompositions suivantes en idéaux premiers $\mathfrak{p}_1$, $\mathfrak{p}_2$ et $\mathfrak{p}_3$ différents entre eux :

$\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{p}_1^2\mathfrak{p}_2^2$, $\mathfrak{p}_1^3\mathfrak{p}_2$, où $\mathfrak{p}_1$, $\mathfrak{p}_2$ et $\mathfrak{p}_3$ sont du premier degré.
$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, où $\mathfrak{p}_1$ est du second degré, tandis que $\mathfrak{p}_2$ et $\mathfrak{p}_3$ sont du premier degré.
$\mathfrak{p}_1\mathfrak{p}_2$, où $\mathfrak{p}_1$ est du troisième degré et $\mathfrak{p}_2$ du premier degré.
$\mathfrak{p}_1\mathfrak{p}_2$, où $\mathfrak{p}_1$ et $\mathfrak{p}_2$ sont tous les deux du second degré.
$\mathfrak{p}_1^2\mathfrak{p}_2$, où $\mathfrak{p}_1$ est du premier degré et $\mathfrak{p}_2$ du second degré.

Dans le premier cas on a $r = 3$, $s = 1$, $f_1^* = 1$ et $t_1 = 3$. Vu que $G_2(1) = 2$, le nombre 2 est un f. c. i.

Dans le deuxième cas on a $r = 2$, $s = 1$, $f_1^* = 1$ et $t_1 = 2$. Vu que $G_2(1) = 2$, le nombre 2 n'est pas un f. c. i.

Dans le troisième cas on a $r=2$, $s=1$, $f_1^*=1$ et $t_1=2$, et le nombre 2 n'est pas un f. c. i.

Dans le quatrième cas on a $r=3$, $s=2$, $f_1^*=2$, $t_1=1$, $f_2^*=1$, $t_2=2$. Donc, le nombre 2 n'est pas un f. c. i.

Dans le cinquième cas on a $r=2$, $s=2$, $f_1^*=3$, $t_1=1$, $f_2^*=1$, $t_2=1$. Donc, le nombre 2 n'est pas un f. c. i.

Dans le sixième cas on a $r=2$, $s=1$, $f_1^*=2$, $t_1=2$. Vu que $4=t_1f_1^*>G_2(2)=2$, on constate que le nombre 2 est un f. c. i.

Dans le septième cas on a $r=2$, $s=1$, $f_1^*=1$, $t_1=1$, $f_2^*=2$, $t=1$. Donc, le nombre 2 n'est pas un f. c. i.

Le théorème 5 se trouve ainsi démontré.

Démonstration du théorème 6. Il suffit d'examiner les mêmes sept possibilités que tout à l'heure pour le nombre 2.

Dans le premier cas on a $r=3$, $s=1$, $f_1^*=1$ et $t_1=3$. Vu que $G_3(1)=3$, le nombre 3 n'est pas un f. c. i.

Dans le deuxième cas on a $r=2$, $s=1$, $f_1^*=1$ et $t_1=2$. Donc, le nombre 3 n'est pas un f. c. i.

Dans les troisième, quatrième et cinquième cas on obtiendra d'une façon analogue que le nombre 3 n'est pas un f. c. i.

Dans le sixième cas on a $r=2$, $s=1$, $f_1^*=2$ et $t_1=2$. Vu que $4=t_1f_1^*<G_3(2)=6$ on voit que le nombre 3 n'est pas un f. c. i.

Dans le septième cas on a $r=2$, $s=1$, $f_1^*=1$, $t_1=1$, $f_2^*=2$, $t_2=1$. Il s'ensuit que le nombre 3 n'est pas un f. c. i.

Cela démontre le théorème 6.

Nous dirons que le nombre 2 est un f. c. i. de la première, deuxième ou troisième catégorie suivant qu'on a le premier, deuxième ou troisième cas dans le théorème 5.

Le théoréme 4 nous rend, pour $n=2$, des résultats sur les nombres 2 et 3 en qualité de f. c. i. dans des corps biquadratiques particuliers. Dans la suite de ce paragraphe nous allons construire des exemples dans des corps plus généraux. Il en résulte que toutes les trois catégories existent réellement.

7. *Corps biquadratiques dans lesquels le premier cas du théorème 5 est réalisé*

Considérons l'équation biquadratique

$$x^4+a_1x^3+a_2x^2+a_3x+a_4=0, \tag{8}$$

où les coefficients sont des nombres entiers rationnels satisfaisant aux congruences

$$a_1\equiv 2\,(\mathrm{mod}\ 32),\quad a_2\equiv -1\,(\mathrm{mod}\ 32),\quad a_3\equiv -2\,(\mathrm{mod}\ 32),\quad a_4\equiv 0\,(\mathrm{mod}\ 32). \tag{9}$$

Supposons que l'équation (8) est irréductible dans le domaine rationnel et désignons par θ une racine de celle-ci. Appliquant la formule qui donne le discriminant des équations biquadratiques, on trouvera que

$$D(\theta)\equiv 16\,(\mathrm{mod}\ 32). \tag{10}$$

Nous allons montrer que le nombre

$$\beta=\tfrac{1}{2}(\theta+\theta^2) \tag{11}$$

est un entier. De la relation

$$\theta^4 = -a_1\theta^3 - a_2\theta^2 - a_3\theta - a_4 \tag{8'}$$

nous obtenons de proche en proche les congruences

$$\sum\theta_i \equiv -2 \pmod{32}, \quad \sum\theta_i^2 \equiv 6 \pmod{32}, \quad \sum\theta_i^3 \equiv -8 \pmod{32},$$

$$\sum\theta_i^4 \equiv 18 \pmod{32}, \quad \sum\theta_i^5 \equiv 0 \pmod{32}, \quad \sum\theta_i^6 \equiv 2 \pmod{32},$$

où les sommes sont étendues à tous les nombres conjugués θ_i.

A l'aide de ces résultats nous trouvons que les sommes $\Sigma\beta_i$, $\Sigma\beta_i^2$ et $\Sigma\beta_i^3$, étendues à tous les nombres conjugués, sont des nombres entiers satisfaisant aux congruences suivantes :

$$\sum\beta_i \equiv 2 \pmod{16}, \quad \sum\beta_i^2 \equiv 2 \pmod{8}, \quad \sum\beta_i^3 \equiv 2 \pmod{4}.$$

En posant $$\prod(y-\beta_i) = y^4 + b_1y^3 + b_2y^2 + b_3y + b_4,$$

nous trouvons que les coefficients b_1, b_2, b_3 et b_4 sont des nombres entiers satisfaisant aux congruences suivantes

$$b_1 \equiv -2 \pmod{16}, \quad b_2 \equiv 1 \pmod{4}, \quad b_3 \equiv 0 \pmod{2},$$

$$b_4 = N(\beta) = \tfrac{1}{16}N(\theta)\,N(\theta+1) \equiv 0 \pmod{64}.$$

Le facteur 3 qui paraît dans le dénominateur dans le calcul de b_3 peut évidemment être négligé.

Alors, ayant égard à la congruence (10), on conclut que le discriminant des quatre nombres

$$1, \theta, \tfrac{1}{2}(\theta+\theta^2), \tfrac{1}{2}(\theta^2+\theta^3) \tag{12}$$

est un nombre impair. Il en résulte que *le discriminant D^* du corps $\mathbf{K}(\theta)$ est impair.* Tout nombre entier η du corps est donc de la forme

$$\eta = \frac{1}{m}(x_0 + x_1\theta + x_2\beta + x_3\beta\theta), \tag{13}$$

où m est un nombre naturel *impair*, et où x_0, x_1, x_2 et x_3 sont des nombres entiers rationnels. Nous allons montrer que, pour tout nombre entier η, la congruence suivante est satisfaite :

$$\eta^2 \equiv \eta \pmod{2}. \tag{14}$$

Cela signifie que l'idéal (2) est le produit de quatre idéaux premiers, qui sont distincts, vu que D^* est impair.

β étant entier on a $\theta^2 \equiv \theta \pmod{2}$. A l'aide de l'équation (8') nous obtenons $\beta^2 \equiv \beta \pmod{8}$. De plus on a

$$(\beta\theta)^2 - \beta\theta = \beta^2(\theta^2-\theta) + \theta(\beta^2-\beta) \equiv 0 \pmod{2}.$$

Si η est le nombre entier donné par (13) on obtient

$$\eta^2 \equiv x_0^2 + x_1^2\theta^2 + x_2^2\beta^2 + x_3^2(\beta\theta)^2 \pmod{2}.$$

Donc $$\eta^2-\eta\equiv x_0^2-x_0+\theta^2(x_1^2-x_1)+x_1(\theta^2-\theta)+\beta^2(x_2^2-x_2)$$
$$+x_2(\beta^2-\beta)+(\beta\theta)^2(x_3^2-x_3)+x_3((\beta\theta)^2-\beta\theta) \pmod 2.$$

Il en résulte que la congruence (14) est satisfaite pour tout nombre entier η.

Par conséquent, nous avons établi le

Théorème 7. *Soit θ une racine de l'équation irréductible* (8), *dont les coefficients satisfont aux congruences* (9). *Alors, dans le corps* $\mathbf{K}(\theta)$ *le nombre* 2 *est un f. c. i., et l'idéal* (2) *est le produit de quatre idéaux premiers distincts dans ce corps.*

On voit sans difficulté que les corps dans ce théorème ne sont pas en général des corps de Galois; comparez Nagell [14]. Dans le numéro suivant nous allons voir comment on peut résoudre complètement le problème dans un corps biquadratique de Galois qui n'est pas cyclique.

8. *Corps biquadratiques abéliens non cycliques*

Les corps biquadratiques abéliens non cycliques sont les corps engendrés par deux racines carrées, c'est-à-dire les corps du type

$$\mathbf{K}(\sqrt{\Delta},\sqrt{\Delta_1}), \tag{15}$$

où Δ et Δ_1 sont des nombres entiers rationnels, qui ne sont divisibles par aucun carré >1; $\Delta\Delta_1$ ne doit pas être un carré. Le corps (15) est contenu dans le corps cyclotomique engendré par le nombre $e^{2\pi i/N}$, où $N=|\Delta\Delta_1|/\delta$, $\delta=(\Delta,\Delta_1)$, si $\Delta\equiv\Delta_1\equiv 1 \pmod 4$, et où $N=4|\Delta\Delta_1|/\delta$, $\delta=(\Delta,\Delta_1)$, dans les autres cas; voir p. ex. Nagell [19], p. 164–165.

Pour que le nombre premier p divise le discriminant du corps (15) il faut et il suffit que p divise $\Delta\Delta_1$ ou $2\,\Delta\Delta_1$ selon que $\Delta\equiv\Delta_1\equiv 1 \pmod 4$ ou non.

Désignons par s_1 la substitution $\sqrt{\Delta}\to-\sqrt{\Delta}$, par s_2 la substitution $\sqrt{\Delta_1}\to-\sqrt{\Delta_1}$, et par s_1s_2 la substitution composée.

Le théorème 4 contient comme cas particulier des résultats sur les corps (15). Par exemple : Le nombre 3 est un f. c. i. dans (15) si $\Delta\equiv\Delta_1\equiv 1 \pmod 3$.

Nous pouvons préciser ce résultat en démontrant le

Théorème 8. *Pour que le nombre* 3 *soit un f. c. i. dans le corps* (15) *il faut et il suffit que* $\Delta\equiv\Delta_1\equiv 1 \pmod 3$.

En effet, si $\Delta\Delta_1$ est divisible par 3, le discriminant du corps est divisible par 3. Si $\Delta\equiv 1 \pmod 3$ et $\Delta_1\equiv -1 \pmod 3$, l'idéal (3) est le produit de deux idéaux premiers dans le sous-corps $\mathbf{K}(\sqrt{\Delta})$:

$$(3)=(3,\,1+\sqrt{\Delta})\,(3,\,1-\sqrt{\Delta}).$$

Dans le sous-corps $\mathbf{K}(\sqrt{\Delta_1})$ l'idéal (3) restera un idéal premier. Supposons qu'on aurait dans le corps (15) la décomposition de (3) en quatre ideaux premiers

$$(3)=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4,$$

de façon que $\mathfrak{p}_2 = s_1\mathfrak{p}_1$, $\mathfrak{p}_3 = s_2\mathfrak{p}_1$ et $\mathfrak{p}_4 = s_1 s_2 \mathfrak{p}_1$. Donc, les idéaux $\mathfrak{p}_1\mathfrak{p}_2$ et $\mathfrak{p}_3\mathfrak{p}_4$ seraient des idéaux dans le sous-corps $\mathbf{K}(\sqrt{\Delta_1})$, tous les deux différents de l'idéal unité. Or, cela est impossible. Par conséquent, dans le corps (15) l'idéal (3) est le produit de deux idéaux premiers.

Si $\Delta \equiv \Delta_1 \equiv -1 \pmod 3$, on a $\Delta\Delta_1 \equiv 1 \pmod 3$, et on retombe sur le cas précédent.

Du théorème 4 nous aurons le résultat : Le nombre 2 est un f. c. i. de la première catégorie si $\Delta \equiv \Delta_1 \equiv 1 \pmod 8$. Nous allons préciser ce résultat en démontrant le

Théorème 9. *Pour que le nombre 2 soit un f. c. i. de la première catégorie dans le corps* (15) *il faut et il suffit que* $\Delta \equiv \Delta_1 \equiv 1$ (*mod* 8).

Pour que le nombre 2 soit un f. c. i. de la troisième catégorie dans le corps (15) *il faut et il suffit que* $\Delta \equiv \Delta_1 \equiv 1$ (*mod* 4) *et que* Δ *et* Δ_1 *ne soient pas tous les deux* $\equiv 1$ (*mod* 8).

En effet, si Δ (ou Δ_1) n'est pas $\equiv 1 \pmod 4$, le discriminant du corps est divisible par 2. Si $\Delta \equiv 1 \pmod 8$ et $\Delta_1 \equiv 5 \pmod 8$, on montre de la même manière que plus haut que l'idéal (2) est le produit de deux idéaux premiers dans (15) :

$$(2) = (2, \tfrac{1}{2}(1+\sqrt{\Delta}))\,(2, \tfrac{1}{2}(1-\sqrt{\Delta})).$$

Si $\Delta \equiv \Delta_1 \equiv 5 \pmod 8$, on a $\Delta\Delta_1 \equiv 1 \pmod 8$, et on retombe sur le cas précédent.

Il est évident que la deuxième catégorie du théorème 5 ne peut pas se présenter dans un corps de Galois. En effet, dans un corps de Galois l'idéal (p) est une puissance si le nombre premier p divise le discriminant du corps.

Il résulte du théorème 8 que le nombre 3 est un f. c. i. dans approximativement $\frac{1}{4}$ des corps biquadratiques du type (15).

Du théorème 9 il résulte que le nombre 2 est un f. c. i. de la première catégorie dans approximativement $\frac{1}{10}$ des corps biquadratiques du type (15). De plus, on obtient que le nombre 2 est un f. c. i. de la troisième catégorie dans approximativement $\frac{1}{10}$ des corps biquadratiques du type (15).

9. *Corps biquadratiques dans lesquels le nombre 3 est un f. c. i.*

Considérons l'équation biquadratique

$$x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0, \tag{16}$$

où les coefficients sont des nombres entiers rationnels satisfaisant aux congruences

$$a_1 \equiv 2 \pmod{81}, \quad a_2 \equiv -1 \pmod{81}, \quad a_3 \equiv -2 \pmod{81}, \quad a_4 \equiv 0 \pmod{81}. \tag{17}$$

Supposons que l'équation (16) est irréductible dans le domaine rationnel et désignons par θ une racine de celle-ci. De la manière courante on trouvera que le discriminant de θ satisfiera à la congruence

$$D(\theta) \equiv 9 \pmod{27}. \tag{18}$$

Nous allons montrer que le nombre

$$\beta = \tfrac{1}{3}(\theta^3 - \theta) \tag{19}$$

est un entier. De la relation

$$\theta^4 = -a_1\theta^3 - a_2\theta^2 - a_3\theta - a_4 \tag{16'}$$

nous obtenons de proche en proche les congruences

$$\sum\theta_i\equiv -2 \pmod{81}, \quad \sum\theta_i^2\equiv 6 \pmod{81}, \quad \sum\theta_i^3\equiv -8 \pmod{81},$$

$$\sum\theta_i^4\equiv 18 \pmod{81}, \quad \sum\theta_i^5\equiv -32 \pmod{81}, \quad \sum\theta_i^6\equiv 66 \pmod{81},$$

$$\sum\theta_i^7 = 34 \pmod{81}, \quad \sum\theta_i^8\equiv 15 \pmod{81}, \quad \sum\theta_i^9\equiv -26 \pmod{81},$$

où les sommes sont étendues à tous les nombres conjugués θ_i.

A l'aide de ces résultats nous trouvons que les sommes $\Sigma\beta_i$, $\Sigma\beta_i^2$ et $\Sigma\beta_i^3$, étendues à tous les nombres conjugués, sont des nombres entiers satisfaisant aux congruences suivantes :

$$\sum\beta_i\equiv -2 \pmod{27}, \quad \sum\beta_i^2\equiv 4 \pmod{9}, \quad \sum\beta_i^3\equiv 1 \pmod{3}.$$

En posant

$$\Pi(y-\beta_i) = y^4+b_1y^3+b_2y^2+b_3y+b_4,$$

nous trouvons que les coefficients b_1, b_2, b_3 et b_4 sont des nombres entiers satisfaisant aux congruences suivantes

$$b_1\equiv 2 \pmod{27}, \quad b_2\equiv 0 \pmod{9},$$

$$b_4 = N(\beta) = \frac{1}{81}N(\theta)N(\theta+1)N(\theta-1)\equiv 0 \pmod{81}.$$

Alors, ayant égard à la congruence (18) on conclut que le discriminant des quatre nombres

$$1, \theta, \theta^2, \tfrac{1}{3}(\theta^3-\theta) \tag{20}$$

est un nombre entier non divisible par 3. Il en résulte que *le discriminant D^* du corps* $\mathbf{K}(\theta)$ *n'est pas divisible par* 3. Donc, tout nombre entier η du corps est de la forme

$$\eta = \frac{1}{m}(x_0+x_1\theta+x_2\theta^2+x_3\beta), \tag{21}$$

où m est un nombre naturel $\equiv \pm 1 \pmod 3$, et où x_0, x_1, x_2 et x_3 sont les nombres entiers rationnels. Nous allons montrer que, pour tout nombre entier η, la congruence suivante est satisfaite :

$$\eta^3\equiv\eta \pmod 3. \tag{22}$$

Cela signifie que l'idéal (3) est le produit de quatre idéaux premiers, qui sont distincts, vu que D^* n'est pas divisible par 3.

Puisque β est entier on a $\theta^3\equiv\theta \pmod 3$. On vérifie aisément que

$$9(\beta^2-\beta)\equiv -9\theta^3+9\theta \pmod{81},$$

d'où $\beta^2-\beta\equiv 0 \pmod 3$ et donc

$$\beta^3\equiv\beta^2\equiv\beta \pmod 3.$$

Si η est le nombre donné par (21) on obtient

$$m\eta^3\equiv x_0^3+x_1^3\theta^3+x_2^3\theta^6+x_3^3\beta^3 \pmod 3.$$

Donc,
$$m(\eta^3-\eta)\equiv x_0^3-x_0+\theta^3(x_1^3-x_1)+x_1(\theta^3-\theta)+\theta^6(x_2^3-x_2)$$
$$+x_2(\theta^6-\theta^2)+\beta^3(x_3^2-x_3)+x_3(\beta^3-\beta) \pmod 3.$$

Il en résulte que la congruence (22) est satisfaite par tout nombre entier η. Par conséquent, nous avons établi le

Théorème 10. *Soit θ une racine de l'équation irréductible* (16), *dont les coefficients satisfont aux congruences* (17). *Alors, dans le corps* $\mathbf{K}(\theta)$ *le nombre* 3 *est un f. c. i., et l'idéal* (3) *est le produit de quatre idéaux premiers distincts dans ce corps.*

On voit sans difficulté que les corps dans ce théorème ne sont pas en général des corps de Galois; comparez Nagell [14]. Dans le numéro précédent nous avons vu comment on peut résoudre complètement le problème concernant le nombre 3 dans un corps biquadratique de Galois qui n'est pas cyclique. Dans les numéros 11 et 12 nous allons considérer les corps biquadratiques cycliques.

10. *Les nombres 2 et 3 simultanément des f. c. i. dans un corps biquadratique*

Une conséquence immédiate des théorèmes 7 et 10 est donnée par le

Théorème 11. *Soit θ une racine de l'équation irréductible*

$$x^4+a_1x^3+a_2x^2+a_3x+a_4=0,$$

où les coefficients sont des entiers satisfaisant aux congruences

$$a_1\equiv 2 \pmod{2^5\cdot 3^4}, \quad a_2\equiv -1 \pmod{2^5\cdot 3^4},$$

$$a_3\equiv -2 \pmod{2^5\cdot 3^4}, \quad a_4\equiv 0 \pmod{2^5\cdot 3^4}.$$

Alors, dans le corps $\mathbf{K}(\theta)$ *les nombres* 2 *et* 3 *sont des f. c. i. Les idéaux* (2) *et* (3) *sont tous les deux des produits de quatre idéaux premiers distincts dans ce corps.*

En combinant les théorèmes 8 et 9 du numéro 8 on peut déterminer tous les corps biquadratiques abéliens non cycliques dans lesquels les nombres 2 et 3 sont en même temps des f. c. i.

11. *Sur une catégorie de corps biquadratiques cycliques*

Les corps biquadratiques cycliques sont les corps engendrés par les nombres de la forme

$$\sqrt{s(1+t^2+\sqrt{1+t^2})}.$$

où s et t sont des nombres rationnels; voir Nagell [14], p. 350–351. Il y en a deux types suivant que s est positif ou négatif. Dans le premier cas tous les corps conjugués sont réels (classe 9 dans mon travail précité). Dans le dernier cas tous les corps conjugués sont imaginaires (classe 6 dans mon travail précité; classe 5 dans mes travaux [15], p. 346, et [11], p. 483, et avec cette classification la classe 5 con-

tient et des corps non-galoisiens et des corps cycliques; dans le travail [11] il faut donc remplacer « **N** » par « **N** et **C** »).

Recapitulons quelques faits sur le corps biquadratique cyclique engendré par les quatre périodes η_0, η_1, η_2 et η_3 chacune constituée de la somme de $\frac{1}{4}(p-1)$ termes dans le corps cyclotomique $\mathbf{K}(e^{2\pi i/p})$, p étant un nombre premier $\equiv 1 \pmod 4$. Ces périodes sont données par les expressions suivantes, où ξ est une racine imaginaire de l'équation $x^p-1=0$, où $f=\frac{1}{4}(p-1)$ et où g est une racine primitive (positive) modulo p:

$$\left.\begin{aligned}\eta_0 &= \xi+\xi^{g^4}+\xi^{g^8}+\ldots+\xi^{g^{4(f-1)}},\\ \eta_1 &= \xi^g+\xi^{g^5}+\xi^{g^9}+\ldots+\xi^{g^{4(f-1)+1}},\\ \eta_2 &= \xi^{g^2}+\xi^{g^6}+\xi^{g^{10}}+\ldots+\xi^{g^{4(f-1)+2}},\\ \eta_3 &= \xi^{g^3}+\xi^{g^7}+\xi^{g^{11}}+\ldots+\xi^{g^{4(f-1)+3}}.\end{aligned}\right\} \tag{23}$$

Les nombres η_0, η_1, η_2 et η_3 constituent une base des entiers du corps $\mathbf{K}(\eta_0)$; voir Weber [17], p. 337–338. Le discriminant D^* de ce corps a la valeur p^3.

Supposons d'abord que $p\equiv 1 \pmod 8$. Alors, les nombres η_0, η_1, η_2 et η_3 sont les racines de l'équation

$$\left.\begin{aligned}x^4+x^3-\tfrac{3}{8}(p-1)x^2-\tfrac{1}{8}[p(a+1)+\tfrac{1}{2}(p-1)]x\\ +\tfrac{1}{64}[\tfrac{1}{4}(p-1)^2-p(a+1)^2]=0,\end{aligned}\right\} \tag{24}$$

où $p=a^2+b^2$, $a\equiv -1 \pmod 4$ et $b\equiv 0 \pmod 4$; pour la démonstration voir Bachmann [16]. Le discriminant de cette équation a la valeur

$$4p^3\left(\frac{b}{4}\right)^6.$$

Les racines sont données par les expressions

$$\tfrac{1}{4}(-1+\sqrt{p})\pm\tfrac{1}{2}\sqrt{\tfrac{1}{2}(p+a\sqrt{p})} \quad \text{et} \quad \tfrac{1}{4}(-1-\sqrt{p})\pm\tfrac{1}{2}\sqrt{\tfrac{1}{2}(p-a\sqrt{p})}.$$

Elles sont réelles toutes les quatre. Le corps est aussi engendré par le nombre

$$\sqrt{\tfrac{1}{2}(p+a\sqrt{p})}.$$

Supposons ensuite que $p\equiv 5 \pmod 8$. Alors, les nombres η_0, η_1, η_2 et η_3 sont les racines de l'équation

$$\left.\begin{aligned}x^4+x^3+\tfrac{1}{8}(p+3)x^2+\tfrac{1}{8}[p(a+1)-\tfrac{1}{2}(p-1)]x\\ +\tfrac{1}{64}[\tfrac{1}{4}(p-1)^2-p(a+1)^2]=0,\end{aligned}\right\} \tag{25}$$

où $p=a^2+b^2$, $a\equiv 1 \pmod 4$, $b\equiv 2 \pmod 4$; pour la démonstration voir Bachmann [16]. Le discriminant de cette équation a la valeur

$$p^3\left(\frac{b}{2}\right)^2\cdot\left(\frac{4p-b^2}{16}\right)^2.$$

Les racines sont données par les expressions

$$\tfrac{1}{4}(-1+\sqrt{p})\pm\tfrac{1}{2}\sqrt{\tfrac{1}{2}(-p-a\sqrt{p})} \quad \text{et} \quad \tfrac{1}{4}(-1-\sqrt{p})\pm\tfrac{1}{2}\sqrt{\tfrac{1}{2}(-p+a\sqrt{p})}.$$

Toutes les quatre sont imaginaires. Le corps est aussi engendré par le nombre

$$\sqrt{\tfrac{1}{2}(-p+a\sqrt{p})}.$$

12. *Exemples de f. c. i. dans les corps biquadratiques cycliques*

Soit donné le nombre premier $p\equiv 1 \pmod 4$. Alors, dans le corps quadratique $\mathbf{K}(\sqrt{p})$, l'idéal (2) est égal au produit de deux idéaux premiers distincts :

$$(2)=(2,\tfrac{1}{2}(1+\sqrt{p}))\,(2,\tfrac{1}{2}(1-\sqrt{p})). \tag{26}$$

Supposons d'abord que le nombre 2 appartient à l'exposant $\frac{1}{2}(p-1)$ modulo p. Alors, on sait que, dans le corps cyclotomique $\mathbf{K}(e^{2\pi i/p})$, l'idéal (2) est égal au produit de deux idéaux premiers distincts; voir p. ex. Hecke [20], § 30. On en conclut que, dans le corps biquadratique cyclique $\mathbf{K}(\eta_0)$ du numéro précédent, les deux facteurs dans l'équation (26) sont des idéaux premiers distincts, tous les deux du second degré. Cela entraîne que le nombre 2 est un reste quadratique modulo p; donc $p\equiv 1 \pmod 8$. Cependant, le nombre 2 ne doit pas être un reste biquadratique modulo p. Donc, il faut dans $p=a^2+b^2$, a impair, que $b\equiv 4 \pmod 8$. En effet, d'après un résultat de Gauss, le nombre 2 est un reste biquadratique si $b\equiv 0 \pmod 8$ et seulement dans ce cas. Par conséquent, nous avons le

Théorème 12. *Le nombre 2 est un f. c. i. de la troisième catégorie dans le corps biquadratique cyclique* $\mathbf{K}(\eta_0)$ *s'il appartient à l'exposant* $\frac{1}{2}(p-1)$ *modulo* p.

Exemple numérique : Si $p=17$ le nombre 2 appartient à l'exposant 8.

Supposons ensuite que le nombre 2 appartient à l'exposant $\frac{1}{4}(p-1)$ modulo p. Dans ce cas le nombre 2 est un reste biquadratique modulo p, et dans $p=a^2+b^2$, on a $b\equiv 0 \pmod 8$. Il existe évidemment une racine primitive $g(>0)$ modulo p telle qu'on ait $g^4\equiv 2 \pmod p$. Nous prenons cette valeur de g dans les expressions (23). Alors, nous aurons

$$\eta_0=\xi+\xi^2+\xi^4+\ldots+\xi^{2^{f-1}},$$

$$\eta_1=\xi^g+\xi^{2g}+\xi^{4g}+\ldots+\xi^{2^{f-1}g},$$

$$\eta_2=\xi^{g^2}+\xi^{2g^2}+\xi^{4g^2}+\ldots+\xi^{2^{f-1}g^2},$$

$$\eta_3=\xi^{g^3}+\xi^{2g^3}+\xi^{4g^3}+\ldots+\xi^{2^{f-1}g^3}.$$

Il en résulte

$$\eta_0^2\equiv\xi^2+\xi^4+\xi^8+\ldots+\xi^{2^f}\equiv\eta_0 \pmod 2$$

et d'une manière analogue,

$$\eta_1^2\equiv\eta_1,\quad \eta_2^2\equiv\eta_2,\quad \eta_3^2\equiv\eta_3 \pmod 2.$$

Tout nombre entier β du corps $\mathbf{K}(\eta_0)$ est de la forme

$$\beta = x_0\eta_0 + x_1\eta_1 + x_2\eta_2 + x_3\eta_3,$$

où x_0, x_1, x_2 et x_3 sont des nombres entiers rationnels. Comme dans des cas précédents, il en résulte

$$\beta^2 - \beta \equiv x_0(\eta_0^2 - \eta_0) + x_1(\eta_1^2 - \eta_1) + x_2(\eta_2^2 - \eta_2) + x_3(\eta_3^2 - \eta_3) \pmod 2,$$

donc

$$\beta^2 - \beta \equiv 0 \pmod 2.$$

Cela entraîne que l'idéal (2) est le produit de quatre idéaux premiers distincts du premier degré dans $\mathbf{K}(\eta_0)$. Il s'ensuit le

Théorème 13. *Le nombre 2 est un f. c. i. de la première catégorie dans le corps biquadratique cyclique* $\mathbf{K}(\eta_0)$ *s'il appartient à l'exposant* $\frac{1}{4}(p-1)$ *modulo p.*

Exemple numérique : Si $p = 281$, le nombre 2 appartient à l'exposant 70.
D'une manière analogue on démontre le

Théorème 14. *Soit p un nombre premier* $\equiv 1$ *(mod 12). Alors, le nombre 3 est un f. c. i. dans le corps biquadratique cyclique* $\mathbf{K}(\eta_0)$ *s'il appartient à l'exposant* $\frac{1}{4}(p-1)$ *modulo p.*

Exemples numériques : Si $p = 13$, le nombre 3 appartient à l'exposant 3. Si $p = 109$, le nombre 3 appartient à l'exposant 27.

13. *Corps dans lesquels le nombre 2 est un f. c. i. de la deuxième catégorie*

Nous finissons nos recherches sur les nombres f. c. i. dans les corps biquadratiques par le résultat suivant :

Théorème 15. *Soit* θ *une racine de l'équation* $x^4 - p = 0$, *où p est un nombre premier* $\equiv 1$ *(mod 8). Alors, le nombre 2 est un f. c. i. de la deuxième catégorie dans le corps* $\mathbf{K}(\theta)$.

Démonstration. On a $D(\theta) = -2^8p^3$, et on trouvera aisément que les quatre nombres

$$1, \theta, \alpha = \tfrac{1}{2}(1+\theta^2), \beta = \tfrac{1}{4}(1+\theta+\theta^2+\theta^3)$$

constituent une base des entiers de $\mathbf{K}(\theta)$. En effet, on a $\alpha = \frac{1}{2}(1+\sqrt{p})$, et le nombre $\beta = \frac{1}{4}\cdot(p-1)/(\theta-1)$ est racine de l'équation

$$y^4 - y^3 - 3ty^2 - 4t^2y - 2t^3 = 0,$$

où $t = \frac{1}{8}(p-1)$. Le discriminant du corps est donc $-4p^3$.
Finalement on vérifiera sans peine qu'on a

$$(2) = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3,$$

où les idéaux premiers sont donnés par les formules

$$\mathfrak{p}_1=(2,1+\theta,\alpha,\beta),\quad \mathfrak{p}_2=(2,1+\theta,1+\alpha,\beta),\quad \mathfrak{p}_3=(2,1+\theta,1+\alpha,1+\beta).$$

Il est évident que ces idéaux sont distincts.

§ 4. Sur une question concernant le discriminant des formes binaires

13. *Lemme sur les polynômes à coefficients entiers*

Nous avons besoin du résultat suivant :

Lemme 7. *Soit $f(x)$ un polynôme à coefficients entiers, et soit δ le diviseur fixe maximal de $f(x)$.*

Si a est un nombre entier tel que $f(a)\neq 0$, il existe une infinité de nombres entiers b tels que $f(a)/\delta$ et $f(b)/\delta$ soient premiers entre eux.

Démonstration. Il suffit évidemment de montrer l'existence d'un seul nombre b ayant la propriété en question.

Soit p un nombre premier tel que la congruence

$$f(x)\equiv 0 \pmod{\delta p}$$

ait une solution. Alors, il existe au moins un nombre entier x_p tel que $f(x_p)/\delta$ ne soit pas divisible par p. Désignons par P le produit de tous les nombres premiers qui divisent le nombre $f(a)$. Soit maintenant b un nombre qui satisfait à toutes les congruences

$$b\equiv x_p \pmod{\delta p},$$

où p parcourt tous les facteurs premiers de P. Alors, il est évident que le nombre $f(b)/\delta$ est premier à P. Cela démontre le lemme.

Pour une forme binaire à coefficients entiers on conclut : Si δ est le diviseur fixe maximal de la forme, celle-ci peut représenter deux nombres A et B tels qu'on ait $(A,B)=\delta$.

14. *La relation entre le discriminant d'une forme binaire et celui d'un corps correspondant*

Une conséquence immédiate du théorème de Levi est la proposition suivante :

Soit $((a, b, c, d))$ une forme binaire cubique irréductible, à coefficients entiers, construite sur le corps cubique **K**. *Alors, si D est le discriminant de la forme et si D^* est le discriminant du corps, on a la relation*

$$D=D^*h^2,$$

h étant un nombre naturel.

Il existe des formes dont le discriminant $=D^*$.

Il est bien connu qu'un résultat analogue existe pour les formes binaires quadratiques.

On peut se démander si ce résultat peut être étendu aux formes binaires d'un degré $\geqslant 4$. Nous allons établir le

Théorème 15. *Soit* $((a_0, a_1, \ldots, a_n))$ *une forme binaire du n-ième degré, irréductible, à coefficients entiers, construite sur le corps* **K** *du n-ième degré.*

Si le diviseur fixe maximal δ *de la forme est* $= 1$, *on a la relation*

$$D = D^* h^2,$$

où D^* *est le discriminant du corps* **K**, *et où* h *est un nombre naturel. Si* $\delta > 1$ *et* $(D^*, \delta) = 1$, *la même relation subsiste.*

Démonstration. Soit

$$F(x,y) = a_0 x^n + a_1 x^{n-1} y + \ldots + a_n y^n$$

la forme binaire. Les coefficients a_0 et a_n sont divisibles par le diviseur fixe maximal δ. Si nous posons $F = F(x, 1)$ nous aurons pour le discriminant

$$D(F(x,y)) = D(F).$$

Posons de plus

$$F_1(z) = a_0^{n-1} F\left(\frac{z}{a_0}, 1\right) = z^n + a_1 z^{n-1} + a_2 a_0 z^{n-2} + \ldots + a_0^{n-1} a_n.$$

Alors, d'après les règles du calcul avec les discriminants, on aura

$$D(F_1(z)) = a_0^{(2n-2)(n-1) - n(n-1)} D(F) = a_0^{(n-1)(n-2)} D(F).$$

Vu que les racines de $F_1(z) = 0$ sont des nombres algébriques entiers du n-ième degré, on aura

$$D(F_1(z)) = D^* h^2,$$

où h est un nombre naturel. Donc, en posant $m = (n-1)(n-2)$,

$$a_0^m D(F) = D^* h^2.$$

D'après le lemme 2, le nombre a_0 peut être remplacé par un nombre entier quelconque A représentable par la forme. D'après le lemme 7 il existe deux nombres entiers A et B représentables par la forme tels qu'on ait $(A, B) = \delta$. Donc

$$A^m D(F) = D^* C^2,$$

$$B^m D(F) = D^* C_1^2,$$

où C et C_1 sont des nombres naturels. Il s'ensuit que

$$\delta^m D(F) = D^* H^2,$$

où H est un nombre naturel. Le théorème 16 résulte immédiatement de cette relation.

Il est probable que le théorème est vrai pour toutes les valeurs de δ. Nous allons revenir sur cette question prochainement.

§ 5. Remarques sur un travail antérieur

Dans mon travail [10] je me suis proposé, entre autres, de déterminer la densité des nombres premiers pour lesquels les nombres 2, 3, 5 et 7 sont des restes cubiques.

Pour les nombres 2 et 3 j'ai montré que la densité est égal à 1/6. Pour les nombres 5 et 7 j'ai trouvé la densité 1/4 qui s'est montré d'être fausse, puisque j'ai opéré avec des formes quadratiques erronées. En effet, dans le cas du nombre 5 les formes doivent être

$$13u^2+25uv+25v^2 \quad \text{et} \quad u^2+uv+169v^2.$$

Vu que ces formes sont ambiguës on aura, par l'application du théorème de Landau, la valeur 1/6 pour la densité. Dans le cas du nombre 7 les formes doivent être

$$9u^2+49uv+49v^2 \quad \text{et} \quad u^2+uv+331v^2.$$

Comme ces formes sont ambiguës on obtient pour la densité la valeur 1/6. Il en résulte qu'il faut, dans les théorèmes 6 et 7, remplacer 1/4 par 1/6. Dans le théorème 8 il faut donc remplacer 1/4 par 1/3.

Cependant, la solution complète du problème a été donnée par Emma Lehmer. En effet, elle a montré, par une méthode plus effective que la mienne, que la densité des nombres premiers $p \equiv 1 \pmod 6$ pour lesquels un nombre premier donné est un reste cubique est toujours égale à 1/6; voir Lehmer [20]. Elle a de même montré que la densité correspondante pour les restes biquadratiques est toujours égale à 1/8.

Je profite de l'occasion pour corriger la démonstration du théorème 9 de mon travail [10]. Dans la forme (9), p. 217, le terme r^2v^2 est disparu. Celle-ci doit être

$$(a^2+27Q^2b^2)u^2+(2ar+54brQ^2)uv+r^2(1+27Q^2)v^2. \tag{9}$$

Sur la page 218 la démonstration doit continuer ainsi qu'il suit :

Pour le raisonnement il faut choisir le nombre a tel que cette forme soit primitive. Nous allons montrer que cela est possible. Désignons par δ le plus grand commun diviseur des coefficients de la forme. Alors, δ n'est pas divisible par le nombre premier r. En effet, le coefficient $a^2+27Q^2b^2$ n'est pas divisible par r, vu que le nombre $\alpha=a+3Qb\sqrt{-3}$ est un non-reste cubique modulo r. Les deux nombres $a-b$ et $1+27Q^2$ sont donc divisibles par δ, et on voit aisément que δ est leur plus grand commun diviseur. Supposons que $\delta>1$. Désignons par A le plus grand diviseur de $1+27Q^2$, tel que $(A,\delta)=1$. Nous savons que a est premier avec b et que a satisfait à une congruence $a \equiv h \pmod{Qbr}$. Remplaçons maintenant a par le nombre

$$a^*=a+QbrA.$$

Alors, il est évident que le nombre

$$a^*-b=a-b+QbrA$$

est premier avec $1+27Q^2$. On en conclut que a peut être choisi de manière que la forme (9) soit primitive.

Le reste de la démonstration sera la même que auparavant. Seulement, dans la première ligne de la page 218, il faut supprimer les mots : « Cette forme est primitive puisque $(a,3Qb)=1$. » Dans la neuvième ligne d'en bas de la même page il faut remplacer $(a,3Qb)$ par $(a-b,1+27Q^2)$.

INDEX BIBLIOGRAPHIQUE

1. NAGELL, T., Einige Sätze über die ganzen rationalen Funktionen. Nyt Tidsskrift f. Matem., Bd. 29, Köbenhavn 1918.
2. NAGELL, T., Über zahlentheoretische Polynome. Norsk matem. tidsskrift, Bd. 1, Kristiania 1919.
3. NAGELL, T., Introduction to Number Theory, New York 1951.
4. LEVI, F., Kubische Zahlkörper und binäre kubische Formenklassen. Berichte d. Sächsischen Ges. d. Wiss., Math. Phys. Klasse, Bd. 66, Leipzig 1914.
5. BACHMANN, P., Allgemeine Arithmetik der Zahlenkörper, Leipzig 1905.
6. HENSEL, K., Theorie der algebraischen Zahlen, Leipzig 1908.
7. FRICKE, R., Lehrbuch der Algebra, Bd. III, Braunschweig 1928.
8. HASSE, H., Zahlentheorie, Berlin 1949.
9. HENSEL, K., Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Diskriminantenteiler einer Gattung. Journ. f. Math. Bd. 113, 1894.
10. NAGELL, T., Sur quelques problèmes dans la théorie des restes quadratiques et cubiques. Arkiv för matematik, Bd. 3, nr. 16, Stockholm 1955.
11. 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.
12. NAGELL, T., Zur Arithmetik der Polynome, Abhandl. aus dem mathem. Seminar der Hamburg. Universität, Bd. I, 1922.
13. BACHMANN, P., Niedere Zahlentheorie, Bd. 1, Berlin 1902.
14. NAGELL, T., Sur quelques questions dans la théorie des corps biquadratiques. Arkiv för matematik, Bd. 4, nr. 26, Stockholm 1961.
15. NAGELL, T., Sur une propriété des unités d'un corps algébrique. Arkiv för matematik, Bd. 5, nr. 25, Stockholm 1964.
16. BACHMANN, P., Die Lehre von der Kreisteilung, Leipzig 1872.
17. WEBER, H., Kleines Lehrbuch der Algebra, Braunschweig 1912.
18. VÄRMON, J., Über Abelsche Körper, deren alle Gruppeninvarianten aus einer Primzahl l bestehen und über Abelsche Körper als Kreiskörper. Akademische Abhandlung. Lund 1925.
19. NAGELL, T., Contributions à la théorie des corps et des polynômes cyclotomiques. Arkiv för matematik, Bd. 5, nr. 10, Stockholm 1963.
20. LEHMER, E., Criteria for cubic and quartic residuacity. Mathematika, Vol. 5, London 1958.

Tryckt den 16 december 1965

Uppsala 1965. Almqvist & Wiksells Boktryckeri AB