Séminaire Dubreil.
Algèbre et théorie
des nombres

Bartel L. van der Waerden

Arithmétique des formes quadratiques quaternaires

Séminaire Dubreil. Algèbre et théorie des nombres, tome 16, n° 2 (1962-1963), exp. n° 17, p. 1-10

<http://www.numdam.org/item?id=SD_1962-1963__16_2_A6_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
16e année, 1962/63, n° 17

21 mars 1963

ARITHMÉTIQUE DES FORMES QUADRATIQUES QUATERNAIRES

par Bartel L. VAN DER WAERDEN

En utilisant la théorie des fonctions θ, C. G. JACOBI a établi (cf. [6]) que le nombre N des représentations d'un entier naturel m sous forme d'une somme de quatre carrés :

$$m = x^2 + y^2 + z^2 + t^2 \tag{1}$$

est égale à huit fois la somme des diviseurs de m, si m est impair, et à vingt quatre fois la somme des diviseurs de m, si m est pair. Donc, si la décomposition de m en facteurs premiers naturels est :

$$m = 2^a \prod_p p^b$$

où p décrit l'ensemble des diviseurs premiers impairs de m, on a :

$$N = 8 \prod_p (p^b + \ldots + p + 1) \quad \text{si} \quad a = 0$$

$$N = 24 \prod_p (p^b + \ldots + p + 1) \quad \text{si} \quad a \neq 0 .$$

A. HURWITZ, [5], a donné une démonstration algébrique de ce résultat ; cette démonstration, qui repose sur l'arithmétique des quaternions, est analogue à celle qui avait été utilisée par GAUSS [3], dans l'étude de la décomposition d'un entier naturel m sous forme d'une somme de deux carrés :

$$m = x^2 + y^2 .$$

Pour obtenir une telle représentation de m, il suffit de représenter m comme produit de deux entiers de Gauss conjugués :

$$m = (x + yi)(x - yi) .$$

On utilise la propriété de factorisation unique vérifiée par l'anneau des entiers de Gauss, pour factoriser m, d'abord en facteurs premiers naturels et, ensuite, si cela est possible, pour factoriser chacun des facteurs premiers naturels de m en facteurs complexes conjugués.

On détermine alors aisément le nombre des représentations de m sous forme d'une somme de deux carrés.

Pour traiter la forme (1), A. HURWITZ considère l'algèbre des quaternions. On désigne par $(1, i, j, k)$ la base canonique de cette algèbre. Un quaternion

$$q = xi + yj + zk + t1$$

est dit entier si x, y, z et t sont des entiers naturels ou bien si chacun des nombres x, y, z et t est de la forme $n + \frac{1}{2}$, où n est un entier. Dans le cas où x, y, z et t sont entiers, nous dirons que le quaternion q est entier au sens strict. On désignera par $\bar{q}$ le quaternion conjugué de q.

La norme d'un quaternion q étant définie par la relation :

$$n(q) = q\bar{q} = x^2 + y^2 + z^2 + t^2,$$

le problème de la représentation d'un entier naturel m sous la forme (1) est équivalent au problème suivant : étant donné un nombre naturel m, quel est le nombre de quaternions entiers au sens strict dont la norme est égale à m ?

Il est plus simple de répondre à la question précédente si l'on y remplace "entiers au sens strict" par "entiers".

Remarquant que l'anneau des quaternions entiers (au sens large) vérifie la propriété de factorisation unique, A. HURWITZ démontre le théorème suivant :

THÉORÈME. - Le nombre des quaternions entiers, dont la norme est égale à

$$m = 2^a \prod_p p^b$$

est

$$24 \prod_p (p^b + p^{b-1} + \ldots + p + 1) .$$

Si m est pair, tous les quaternions entiers, dont la norme est égale à m, sont entiers au sens strict. Si m est impair, la famille des quaternions entiers au sens strict de norme m ne constitue que le tiers de la famille des quaternions entiers, de norme m. On retrouve, ainsi, le résultat de Jacobi.

Un quaternion entier q pouvant s'écrire :

$$q = xi + yj + zk + t\,\frac{i + j + k + 1}{2}$$

où x, y, z et t sont des entiers, sa norme $n(q)$ prend la forme :

$$x^2 + y^2 + z^2 + (x + y + z)\,t + t^2 . \tag{2}$$

Il en résulte le théorème suivant, dû à A. HURWITZ :

THÉORÈME. - Le nombre des représentations d'un nombre entier naturel

$$m = 2^a \prod_p p^b$$

sous la forme (3) est

$$24 \prod_p (p^b + p^{b-1} + \dots + p + 1) .$$

Soit

$$f(x_i) = \sum_{i,k=1}^{4} a_{ik}\, x_i\, x_k$$

une forme quaternaire entière, c'est-à-dire que les nombres a_{ii} , $2a_{ij}$, i et $j = 1 , 2 , 3 , 4$, sont entiers rationnels et que $a_{ik} = a_{ki}$. On appelle discriminant de la forme f le déterminant :

$$D = \left| \frac{\partial^2 f}{\partial x_i\, \partial x_k} \right| .$$

Par suite, le discriminant de la forme (1) est égal à 16 ; celui de la forme (2), à 4.

La forme

$$f(x_i) = \sum_{i,k=1}^{4} a_{ik}\, x_i\, x_k$$

est dite primitive si les nombres $a_{11} , \dots , a_{44} , 2a_{12} , \dots , 2a_{34}$ sont premiers dans leur ensemble.

Deux formes

$$f = \sum_{i,k=1}^{4} a_{ik}\, x_i\, x_k \quad \text{et} \quad g = \sum_{i,k=1}^{4} b_{ik}\, y_i\, y_k$$

sont dites équivalentes si elles se correspondent par une transformation linéaire unimodulaire, c'est-à-dire si $f = g$ pour $x_i = \sum \alpha_i^k\, y_k$ où les nombres α_i^k sont entiers rationnels tel que $\det(\alpha_i^k) = + 1$.

La substitution $t = 2t'$ transforme la forme (2) en une forme équivalente à la forme (1). Donc la forme (1) s'obtient à partir d'une forme dont le discriminant est plus petit que le sien. Par contre, il n'en est pas ainsi de la forme (3). Nous dirons, pour cette raison, que la forme (3) est une forme non dérivée (Stammform).

Les formes non dérivées correspondent, dans la théorie géométrique des formes quadratiques, développée par J. DIEUDONNÉ, E. WITT et M. EICHLER (Voir par exemple [2]) aux réseaux maximaux (maximalen Gritter). Dans cette théorie, la forme (1)

correspond à un réseau cubique ; la forme (3) , à un réseau cubique centré.

En vue de généraliser la théorie de A. HURWITZ, H. BRANDT a, le premier, introduit la notion d'algèbre de quaternions généralisés ; on désigne sous ce nom une algèbre $\mathfrak{A}$ sur un anneau commutatif A ayant un élément unité (on prendra pour A le corps des nombres rationnels) ayant une base de quatre éléments, dont le premier est élément-unité de $\mathfrak{A}$, qu'on identifie à l'élément-unité 1 de A , et dont les trois autres u_1 , u_2 , u_3 se multiplient suivant la table :

$$\begin{cases} u_1^2 = \alpha \qquad u_2^2 = \beta \qquad u_3^2 = -\alpha\beta \\ u_1 u_2 = -u_2 u_1 = u_3 \\ u_1 u_3 = -u_3 u_1 = \alpha u_2 \\ u_2 u_3 = -u_3 u_2 = -\beta u_1 \end{cases}$$

α et β étant des nombres rationnels.

Pour tout quaternion $q = t + xu_1 + yu_2 + zu_3$, on désigne par $\bar{q}$ le quaternion $t - xu_1 - yu_2 - zu_3$ qu'on appelle le quaternion conjugué de q . Le produit $q\bar{q}$ est appelé la norme du quaternion q , et est noté $n(q)$. On a :

$$n(q) = t^2 - \alpha x^2 - \beta y^2 + \alpha\beta z^2 .$$

On appelle trace du quaternion q , le nombre rationnel $s(q) = q + \bar{q} = 2t$.

Un quaternion (généralisé) q est dit entier si sa norme et sa trace sont des entiers rationnels.

Dans une algèbre de quaternions généralisés, H. BRANDT [1] a développé une théorie des modules, des anneaux et des idéaux. Un module α de l'algèbre $\mathfrak{A}$ est l'ensemble des combinaisons linéaires à coefficients entiers de quatre quaternions α_1 , α_2 , α_3 et α_4 linéairement indépendants. Un anneau (Ordnung) est un module fermé pour le multiplication et qui contient l'élément-unité de $\mathfrak{A}$. Les éléments d'un anneau sont des quaternions entiers.

Les anneaux maximaux (maximale Ordnungen) sont d'une importance primordiale dans la théorie de H. BRANDT.

Chaque module α détermine deux anneaux :

$$D_g = \{q \; ; \; q \in \mathfrak{A} \; ; \; q\alpha \subseteq \alpha\}$$

$$D_d = \{q \; ; \; q \in \mathfrak{A} \; ; \; \alpha q \subseteq \alpha\}$$

désignés respectivement sous le nom d'anneau à gauche et d'anneau à droite associés à α .

Si D_d et D_g sont des anneaux maximaux, alors α est appelé idéal de $\mathfrak{A}$.

Les idéaux correspondent donc aux idéaux fractionnaires de la théorie classique des corps de nombres algébriques.

Si α et c sont deux idéaux tels que l'anneau à droite associé à α coïncide avec l'anneau à gauche associé à c, H. BRANDT définit le produit $\alpha.c$. Respectivement, à cette opération, l'ensemble des idéaux de $\mathfrak{A}$ est un groupoïde.

A chaque module $\mathfrak{A} = (\alpha_1 , \alpha_2 , \alpha_3 , \alpha_4)$ correspond une classe de formes dont un représentant est :

$$F(x_i) = n\left(\sum_{i=1}^{4} x_i \alpha_i\right) .$$

Soit $n(\alpha)$ le p. g. c. d. des coefficients de F. On a :

$$F(x_i) = n(\alpha).F_\alpha(x_i)$$

où $F_\alpha(x_i)$ est une forme entière primitive, appelée la forme de normes (Normenform) du module α.

On démontre que la forme F_α est une forme non dérivée si et seulement si α est un idéal.

Puisque $F(x_i)$ se déduit de la forme $t^2 - \alpha x^2 - \beta y^2 + \alpha\beta z^2$ par transformation linéaire rationnelle et que le discriminant de cette dernière forme est un carré, à savoir $(4\alpha\beta)^2$, on en déduit que le discriminant de F_α est un carré.

La méthode des quaternions ne s'applique qu'aux formes à discriminant carré. Pour de telles formes, H. BRANDT a défini une loi de composition, analogue à celle des formes binaires, précédemment définie par GAUSS.

Définition. - Si, par une substitution

$$z_q = \sum_{r,s=1}^{4} m_{qrs} X_r Y_s \qquad (q = 1 , 2 , 3 , 4)$$

une forme $C(z_i)$ est transformée en un produit de deux formes $A(x_i).B(y_i)$ on dit que C s'obtient par composition de A et de B.

Respectivement à cette loi de composition l'ensemble des classes de formes à discriminant carré donné, $D = \delta^2$, est un groupoïde.

D'autre part deux idéaux α et c de l'algèbre $\mathfrak{A}$ sont dits équivalents s'il existe deux quaternions ρ et σ tels que $n(\rho\sigma) > 0$ et que $c = \rho\alpha\sigma$.

L'ensemble des classes d'idéaux de $\mathfrak{A}$ est un groupoïde fini.

G. AEBERLI a démontré le théorème suivant :

THÉORÈME. - Le groupoïde des classes d'idéaux d'une algèbre de quaternions est isomorphe au groupoïde des classes de formes de normes non dérivées qui ont toutes le même discriminant $D = \delta^2$.

En utilisant les travaux de G. AEBERLI, et en appliquant la méthode de A. HURWITZ, H. GROSS [4] a trouvé le nombre des représentations d'un nombre entier donné m par une forme quadratique positive f à discriminant carré.

Soit f la forme de normes d'un idéal α de l'algèbre $\mathfrak{A}$. Soient $\mathfrak{D}_g$ et $\mathfrak{D}_d$ l'anneau à gauche et l'anneau à droite associés à α. Soit $\mathfrak{C}$ la classe de l'idéal α. On a :

THÉORÈME. - Le nombre des représentations de m par la forme f est égal au produit du nombre des unités de l'anneau $\mathfrak{D}_g$ par le nombre des idéaux à gauche de l'anneau $\mathfrak{D}_d$ dont la norme est égale à m et qui appartiennent à la classe $\mathfrak{C}^{-1}$.

Lorsqu'il n'y a qu'une classe d'idéaux (par exemple, dans le cas envisagé par A. HURWITZ) le nombre des idéaux à gauche de l'anneau $\mathfrak{D}_d$, ayant m pour norme et appartenant à la classe $\mathfrak{C}^{-1}$ est égal au nombre des idéaux de norme m dans un anneau maximal quelconque ; ce nombre est égal à :

$$\psi_D = \prod_p (p^b + \ldots + p + 1)$$

où p décrit l'ensemble des facteurs premiers de m qui ne sont pas diviseurs du discriminant D de f.

Comme l'anneau de Hurwitz possède vingt quatre unités, on retrouve la formule :

$$N = 24\ \psi_4(m) .$$

Appliquons, par exemple, le théorème de Gross, à la forme :

$$f = x^2 + xy + y^2 + z^2 + zt + t^2 \tag{3}$$

dont le discriminant est égal à 9. L'anneau correspondant possède douze unités. Par suite le nombre des représentations de m par la forme (3) est

$$N = 12\ \psi_q(m) .$$

Il y a trois ans, j'ai proposé à Oscar WEBER [7] de déterminer, par la méthode de réduction des formes quadratiques, les classes de formes positives dont le discriminant n'est pas un carré et est aussi petit que possible. Je lui ai demandé

également si l'on observe des propriétés régulières dans l'ensemble des nombres de représentations des entiers par de telles formes.

O. WEBER a démontré que le plus petit discriminant, non carré, est $D = 5$. A ce discriminant ne correspond qu'une classe de formes qui est représentée par la forme :

$$f = x^2 + y^2 + z^2 + t^2 + xy + yz + zt \ . \tag{4}$$

D'autre part, il a trouvé empiriquement la formule suivante. Soit

$$m = 5^a \Pi p^b \Pi q^c \quad \text{où} \quad \left(\frac{p}{5}\right) = 1 \quad \text{et} \quad \left(\frac{q}{5}\right) = -1 \ ,$$

[On représente par le symbole de Jacobi $\left(\frac{p}{5}\right)$ le reste quadratique de p modulo 5.] Soit

$$S'(m) = \Pi(p^b + p^{b-1}) \ \Pi(q^c - q^{c-1}) \ .$$

Alors, si m n'est pas divisible par 5, le nombre de représentations primitives de m est :

$$N' = 20 \, S'(m) \qquad \text{si} \quad \left(\frac{m}{5}\right) = 1 \ ,$$

$$N' = 30 \, S'(m) \qquad \text{si} \quad \left(\frac{m}{5}\right) = -1 \ ;$$

si m est divisible par 5 :

$$N' = 24.5^a \, S'(m) \qquad \text{si} \quad \frac{m}{5} \equiv 0 \ , \ 1 \ \text{ou} \ 4 \pmod 5$$

$$N' = 26.5^a \, S'(m) \qquad \text{si} \quad \frac{m}{5} \equiv 2 \ \text{ou} \ 3 \pmod 5 \ .$$

Cette formule explicite dépassa mes espérances les plus hardies.

De la formule de O. WEBER, on déduit aisément le nombre total N des représentations de $m = 5^a m'$ par la forme (4). Soit

$$S_5(m') = \sum_{dd'=m'} d.\left(\frac{d'}{5}\right)$$

où $\left(\frac{5}{d'}\right)$ est le symbole de Jacobi. On a :

$$N = 5\{5^{a+1} - \left(\frac{m'}{5}\right)\}.S_5(m') \ .$$

En utilisant les fonctions θ, et en étendant la méthode de Jacobi, J. CHAPELON avait donné le nombre des représentations d'un entier m par la forme :

$$x^2 + y^2 + z^2 + 5t^2 \ . \tag{5}$$

Or, si f désigne la forme (4), on remarque que $8f$ peut s'écrire :

$$8f = X^2 + Y^2 + Z^2 + 5T^2 .$$

On déduit ainsi la formule de O. WEBER de celle trouvée par J. CHAPELON.

O. WEBER a aussi trouvé qu'il ne correspond, au discriminant $D = 13$, qu'une classe de formes qui est représentée par la forme :

$$f = x^2 + y^2 + z^2 + xy + yz + zt + 2t^2 . \tag{6}$$

On remarque que l'on a

$$8f = X^2 + Y^2 + Z^2 + 13T^2 .$$

Le nombre N de représentations de

$$m = 13^a m' = 13^a \Pi p^b \Pi q^c ; \quad \left(\frac{p}{13}\right) = 1 \ \left(\frac{q}{13}\right) = -1$$

par la forme (6) est :

$$N = \{13^{a+1} - \left(\frac{m'}{13}\right)\} S_{13}(m')$$

où

$$S_{13}(m') = \sum_{\substack{d \mid m' \\ dd' = m'}} d . \left(\frac{d'}{13}\right) .$$

Cette formule, trouvée empiriquement par O. WEBER, n'a pas encore été démontrée.

Pour la forme

$$x^2 + y^2 + z^2 + 2t^2 . \tag{7}$$

J. LIOUVILLE a donné une formule générale que T. PEPIN a démontrée par une méthode directe.

Pour la forme

$$x^2 + y^2 + z^2 + 3t^2 \tag{8}$$

J. LIOUVILLE a aussi donné une formule sans démonstration. E. BENZ a démontré ces deux dernières formules au moyen des fonctions θ. Pour la forme (8), la démonstration, très difficile, a nécessité des idées nouvelles.

Dans le cas (7), on écrit :

$$m = 2^a m' = 2^a \Pi p^b \Pi q^c , \quad \left(\frac{p}{2}\right) = 1 \text{ et } \left(\frac{q}{2}\right) = -1$$

et on introduit la somme :

$$S_2(m') = \sum_{\substack{d \mid m \\ dd' = m}} d . \left(\frac{d'}{2}\right) .$$

Le nombre de représentations de m par la forme (7) est :

$$N = 2\{2^{a+1} - (\tfrac{m'}{2})\}\, S_2(m') .$$

Dans le cas (8), on écrit $m = 2^a 3^b m'$, et le nombre de représentations de m est

$$N = \{3^{b+1} - (-1)^{a+b+(m'-1)/2}.(\tfrac{m'}{3})\}\{2^{a+1} + (-1)^{a+b+(m'-1)/2}.(\tfrac{m'}{2})\} - S_3(m')$$

où $S_3(m') = \sum_{\substack{d|m \\ dd'=m'}} d.(\tfrac{d'}{3})$.

Il n'existe qu'une seule classe de formes dont le discriminant est $D = 8$. Elle est représentée par la forme :

$$x^2 + y^2 + z^2 + t^2 + xy + yz \quad . \tag{9}$$

O. WEBER a démontré que le nombre de représentations de m par (9) est égal au nombre de représentations de $2m$ par la forme (7).

FUCHS a obtenu quelques formules très générales, par une méthode élémentaire due à M. EICHLER.

GERMANN a dressé une table de classes de formes positives à coefficients entiers dont le discriminant est inférieur à 64.

AMREIN a commencé des recherches sur les genres des formes quaternaires.

On peut aussi mettre les résultats de H. GROSS, O. WEBER, E. BENZ et FUCHS en relation avec la "formule analytique de mesure" (Analytische Massformel) de Siegel.

Il existe donc dans ce domaine tout un programme de recherches futures.

BIBLIOGRAPHIE

[1] BRANDT (H.). - Idealtheorie in Quaternionenalgebren, Math. Annalen, t. 99, 1928, p. 1-29.

[2] EICHLER (M.). - Quadratische formen und orthogonale Gruppen. - Berlin, Springer-Verlag, 1952 (Grundlehren der mathematischen Wissenschaften..., 63).

[3] GAUSS (C. F.). - Werke, Band 2 ; p. 159-164. - Göttingen, Königliche, Gesellschaft der Wiseenschaften, 1863.

[4] GROSS (H.). - Darstellungsanzahlen von quaternären quadratischen Stammformen mit quadratischer Discriminante, Comment. Math. Helvet., t. 34, 1960, p. 198-221.

[5] HURWITZ (A.). - Zahlentheorie der Quaternionen. - Berlin, 1919.

[6] JACOBI (C. G.). - Note sur la décomposition d'un nombre donné en quatre carrés, J. für die reine und angew. Math., t. 3, 1828, p. 191 ; Gesammelte Werke, Band 1 ; p. 247. - Berlin, G. Reimer, 1881.

[7] WEBER (O.). - Über die Reduktion und die Darstellungen positiver quaternärer quadratischer Formen (Thèse, 1962).