BULLETIN DE LA S. M. F.

WEILL

Sur la décomposition d'un nombre en quatre carrés

Bulletin de la S. M. F., tome 13 (1885), p. 28-34

<http://www.numdam.org/item?id=BSMF_1885__13__28_0>

Sur la décomposition d'un nombre en quatre carrés;

par M. Weill.

(Séance du 20 décembre 1884.)

Un nombre étant mis sous la forme d'une somme de quatre carrés, il existe des relations simples entre le nombre des décompositions de l'entier considéré et celui des décompositions de certains multiples de cet entier en une somme de quatre carrés.

Le nombre N étant mis sous la forme $x^2+y^2+z^2+t^2$, nous chercherons à mettre pN sous la forme d'une somme de carrés de quatre nombres, dont chacun soit une fonction linéaire et homogène, à coefficients entiers, de x, y, z, t. Pour commencer par un cas particulièrement simple, considérons les deux identités

$$\begin{aligned}4\mathrm{N} &= 4(x^2+y^2+z^2+t^2)\\ &= (x+y+z+t)^2+(x+y-z-t)^2+(x-y-z+t)^2+(x-y+z-t)^2,\end{aligned}$$

$$4\mathrm{N} = (x+y+z-t)^2+(x+y-z+t)^2+(x-y+z+t)^2+(x-y-z-t)^2.$$

Ces deux décompositions de 4N sont les seules qui répondent aux conditions imposées; car chacune des fonctions linéaires contient nécessairement les quatre lettres x, y, z et t avec les coefficients $+1$ ou (-1), et l'on voit facilement comment ces coefficients doivent être distribués pour que les rectangles des variables disparaissent dans la somme. Dès lors, à une décomposition de N en quatre carrés, correspondront deux décompositions de 4N en quatre carrés; mais il faut chercher si, inversement, toute décomposition de 4N en quatre carrés peut être représentée par l'une ou l'autre des identités considérées. Nous considérerons le cas où, N étant impair, on se propose de décomposer 4N en une somme de quatre carrés tous impairs. Désignons par (A) un nombre entier impair, et dont le signe est choisi de manière qu'il soit un multiple de 4, plus 1, ce qui est toujours possible. Je dis qu'il existe des entiers x, y, z et t vérifiant les équations

$$\begin{aligned}x+y+z+t &= (\mathrm{A}),\\ x+y-z-t &= (\mathrm{B}),\\ x-y-z+t &= (\mathrm{C}),\\ x-y+z-t &= (\mathrm{D}),\\ x^2+y^2+z^2+t^2 &= \mathrm{N}.\end{aligned}$$

En effet, de ces équations on tire

$$\begin{aligned} 4x &= (A)+(B)+(C)+(D),\\ 4y &= (A)+(B)-(C)-(D),\\ 4z &= (A)+(D)-(B)-(C),\\ 4t &= (A)+(C)-(B)-(D); \end{aligned}$$

et les valeurs de x, y, z, t sont entières.

Les nombres de x, y, z, t étant déterminés, les nombres E, F, G, H, qui vérifient les égalités

$$\begin{aligned} E^2+F^2+G^2+H^2 &= 4N,\\ x+y+z-t &= E,\\ x+y-z+t &= F,\\ x-y+z+t &= G,\\ x-y-z-t &= H \end{aligned}$$

sont tous impairs; ils sont donnés, en effet, par les relations

$$\begin{aligned} 2E &= (A)+(B)+(D)-(C),\\ 2F &= (A)+(B)+(C)-(D),\\ 2G &= (A)+(C)+(D)-(B),\\ 2H &= (B)+(C)+(D)-(A). \end{aligned}$$

Il en résulte qu'un système de valeurs x, y, z, t donne, pour $4N$, deux systèmes de nombres, tous impairs, A, B, C, D et E, F, G, H. D'ailleurs, à deux systèmes de nombres x, y, z, t et x', y', z', t' *différents,* ne peuvent correspondre, *en grandeur et en signe,* les mêmes valeurs de (A), (B), (C), (D); car le système d'équations

$$\begin{aligned} x+y+z+t &= x'+y'+z'+t',\\ x+y-z-t &= x'+y'-z'-t',\\ x-y-z+t &= x'-y'-z'+t',\\ x-y+z-t &= x'-y'+z'-t' \end{aligned}$$

n'admet, comme solutions, que $x=x', y=y', z=z', t=t'$.

D'autre part, si l'on change les signes des quatre nombres (A), (B), (C), (D), les valeurs de x, y, z, t changent de signe sans changer de grandeur; si l'on change les signes de une ou trois des quantités (A), (B), (C), (D), les valeurs de $x, y, \ldots$ ne sont plus entières, comme le montrent les expressions de $4x, 4y, \ldots$. Reste à examiner le cas où l'on change le signe de deux des quan-

tités (A), (B), (C), (D); supposons que ces changements de signe, *qui ne changent pas la forme de décomposition de* 4N, engendrent deux systèmes différents de nombres x, y, z, t et x', y', z', t', on aurait, par exemple, les équations

$$\begin{aligned} x+y+z+t &= \quad x'+y'+z'+t', \\ x+y-z-t &= -(x'+y'-z'-t'), \\ x-y-z+t &= -(x'-y'-z'+t'), \\ x-y+z-t &= \quad x'-y'+z'-t'; \end{aligned}$$

ces équations donnent

$$\begin{aligned} x &= z', \\ z &= x', \\ y &= t', \\ t &= y'; \end{aligned}$$

donc les systèmes des nombres x, y, z, t et x', y', z', t' ne donnent pas, pour

$$\mathrm{N} = x^2 + y^2 + z^2 + t^2,$$

deux décompositions distinctes. De tout ce qui précède, il résulte que, si le nombre impair N a été décomposé en quatre carrés, le nombre 4N admettra deux décompositions correspondantes en une somme de quatre carrés tous impairs, et que, inversement, toute décomposition de 4N en une somme de quatre carrés tous impairs pourra être obtenue par cette correspondance. On peut donc énoncer le théorème suivant :

Théorème. — N *étant un entier impair, le nombre des décompositions de* 4N *en une somme de quatre carrés tous impairs est double du nombre des décompositions de* N *en quatre carrés.*

Ce théorème est dû à Jacobi, qui l'a déduit de l'identité

$$k^2 + k'^2 = 1,$$

dans la théorie des fonctions elliptiques.

La démonstration exposée plus haut donne la raison de ce théorème et le moyen de former les décompositions de 4N connaissant celles de N, et inversement.

Pour donner une autre application de la même méthode, consi-

dérons l'identité

$$3(x^2+y^2+z^2+t^2) = (x+y+z)^2+(x-y+t)^2 + (y+t-z)^2+(z+t-x)^2;$$

de cette identité, on en déduit trois autres, en faisant une permutation circulaire sur x, y, z et t.

Donc, si l'entier N a été mis sous la forme d'une somme de quatre carrés, l'entier 3N sera mis, de quatre manières différentes, sous la forme d'une somme de quatre carrés. Inversement, soit N un nombre non multiple de 3, l'entier 3N étant mis sous la forme

$$3N = A^2+B^2+C^2+D^2;$$

on aura nécessairement pour l'un des quatre nombres, soit A, un multiple de 3, les trois autres étant des multiples de 3, plus ou moins 1.

En désignant par (B) le nombre B affecté d'un signe convenable, on aura donc

$$\left.\begin{array}{l}(A)\equiv 0\\(B)\equiv 1\\(C)\equiv 1\\(D)\equiv 1\end{array}\right\}\pmod 3.$$

Ceci posé, les trois équations

$$\begin{aligned}x+y+z&=(A),\\x-y+t&=(B),\\y+t-z&=(C),\\z+t-x&=(D)\end{aligned}$$

donnent

$$\begin{aligned}3t&=(B)+(C)+(D),\\3x&=(A)+(B)-(D),\\3y&=(A)+(C)-(B),\\3z&=(A)+(D)-(C),\end{aligned}$$

et les valeurs de x, y, z, t sont entières

On voit que, N étant un entier quelconque multiple de 3, ou non-multiple de 3, le nombre 3N admet quatre fois autant de décompositions en quatre carrés quelconques que le nombre N, si l'on ne tient pas compte des signes; et en effet, habituellement, on considère comme distinctes des décompositions qui ne dif-

fèrent que par le signe d'un des nombres A, B, C, D, d'où l'énoncé que j'ai donné dans les *Comptes rendus de l'Académie des Sciences* (17 novembre 1884). Mais, si l'on tient compte des signes, le résultat est différent, comme on va le voir, et n'est simple que lorsque N n'est pas multiple de 3. Notre analyse prouve que, le signe des trois nombres B, C, D ayant été choisi, on ne peut changer le signe de l'un ou de deux de ces nombres, mais celui des trois à la fois, ce qui revient à changer le signe de A; car, en changeant le signe de B, par exemple, ou les signes de B et C, les nombres x, y, z, t ne sont plus tous des entiers. Donc, 3N ayant été mis sous la forme

$$3N = A^2 + B^2 + C^2 + D^2,$$

il y aura deux systèmes de nombres $x, y, z, t, x', y', z', t'$ *dont les signes et les valeurs seront entièrement déterminés,* correspondant à deux décompositions de N; on aura

$$\begin{aligned}
3t &= (B) + (C) + (D),\\
3x &= (A) + (B) - (D),\\
3y &= (A) + (C) - (B),\\
3z &= (A) + (D) - (C);
\end{aligned}$$

$$\begin{aligned}
3t' &= 3t,\\
3x' &= -(A) + (B) - (D),\\
3y' &= -(A) + (C) - (B),\\
3z' &= =(A) + (D) - (C).
\end{aligned}$$

Les relations entre les deux systèmes sont

$$\begin{aligned}
t' &= t,\\
3x' &= x - 2y - 2z,\\
3y' &= y - 2x - 2z,\\
3z' &= z - 2z - 2y
\end{aligned}$$

ou bien

$$\begin{aligned}
x + y + z &= -(x' + y' + z')\\
x - y + t &= x' - y' + t',\\
y + t - z &= y' + t' - z',\\
z + t - x &= z' + t' - x'.
\end{aligned}$$

Ces deux systèmes sont distincts en général. En effet, supposons

$x' = x$, on en déduit

$$z' = z, \quad y' = y,$$

et, par suite,

$$x + y + z = (A) = o,$$

ce qui est impossible, si l'on suppose 3N décomposé en quatre carrés et non en un nombre moindre de carrés.

D'autre part, en supposant $x' = -x$, on en déduit

$$y + z = 2x,$$

d'où

$$(B) = (D),$$

ce qui est impossible, si 3N a été décomposé en quatre carrés distincts. En supposant $x' = y$, on en déduit

$$y' = 2y - x,$$
$$z' = x - z - y.$$

Pour que les deux systèmes ne soient pas distincts, il faut alors

$$y' = 2y - x = \pm x \quad \text{ou} \quad y' = 2y - x = \pm z;$$

aucune de ces solutions ne convient, si l'on suppose N décomposé en quatre carrés distincts, dont aucun n'est nul. Enfin, si l'on suppose $x' = -y$, on en déduit

$$x + y = 2z,$$

ce qui est impossible, car on aurait alors

$$(D) = (C).$$

De tout ce qui précède résulte le théorème suivant :

THÉORÈME. — N *étant un entier non multiple de* 3, *si les deux nombres* N *et* 3N *n'admettent l'un et l'autre que des décompositions en quatre carrés positifs, non nuls, et distincts, le nombre des décompositions de* 3N *est double du nombre des décompositions de* N.

Ce théorème renferme le cas général qui se présente; car, si N est, par exemple, décomposable en trois carrés, cela constitue un cas exceptionnel. La démonstration du théorème prouve que, à une décomposition d'un nombre quelconque N en quatre carrés,

$x^2 + y^2 + z^2 + t^2$, correspondent les quatre décompositions de ce même nombre, données par les formules

$$t' = t, \quad x' = \frac{x - 2y - 2z}{3}; \quad y' = \frac{y - 2x - 2z}{3}, \quad z' = \frac{z - 2x - 2y}{3},$$

et par celles que l'on en déduit par permutation circulaire; mais ces nouvelles solutions n'en engendrent pas d'autres.

(*A suivre.*)