Sur la démonstration de M. Hilbert du théorème de Waring.

Par

E. Stridsberg à Stockholm.

M. Hilbert a bien voulu m'inviter à rédiger pour les Math. Ann. la traduction de deux notes que j'ai publiées en suédois dans l'Arkiv för Matematik*) concernant la preuve célèbre donnée par lui du théorème de Waring. Je suis très flatté de cet appel de l'éminent géomètre, et je m'empresse de donner ici — avec quelques légères modifications — un résumé de mes deux articles précités.

Par regard aux méthodes introduites, à ce propos, par M. Hilbert, M. Poincaré a fait la remarque importante qui suit:

«Nous ne devons pas douter que ces considérations .... ne puissent un jour, quand on en aura bien compris le sens, être appliquées à des problèmes bien plus étendus que celui de Waring».**)

Dans ces circonstances une simplification telle que la présente pourra être d'une certaine utilité pour des recherches futures.

D'après la proposition de Waring, dont on doit à M. Hilbert la première démonstration générale***), *tout nombre entier positif peut être décomposé en une somme de N puissances n^{es} de nombres entiers $\geqq 0$, le nombre N ne dépendant que de l'exposant n.*

La preuve du théorème peut être dans une certaine mesure simplifiée par l'observation suivante de M. Hurwitz.

Soit $\sum_{1}^{N}\lambda\, \varrho_\lambda P_\lambda^\mu$ une somme de N puissances μ^{es} de nombres entiers arbitraires $P_\lambda \geqq 0$ multipliés par des nombres rationnels positifs ϱ_λ, N et ϱ_λ

*) Öfver Hilberts bevis för Warings sats. Not 1 och 2. Arkiv för Mat., Astr. Fys. 6. N-is 32. 39. Stockholm 1910, 1911.

**) Prix Bolyai, Rapport par Henri Poincaré. Acta Math. 35 (1911).

***) Hilbert, Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n^{ter} Potenzen. (Waringsches Problem.). Math. Ann. 67 (1909), S. 281.

ne dépendant que de μ. Pour abréger, je désignerai toujours, dans ce qui suit, par la notation simple $\sum(\mu)$ une somme $\sum_1^N{}^\lambda \varrho_\lambda P_\lambda^\mu$ de ce genre. Donc, la remarque de M. Hurwitz*) peut être énoncée ainsi:

Théorème 1. *Soit B une quantité réelle quelconque, et supposons, que tout nombre entier positif $H \geqq B$ puisse s'écrire sous la forme $H = \sum(\mu)$, alors le théorème de Waring sera vrai pour $n = \mu$.*

En effet, soit σ le plus petit commun multiple des dénominateurs des nombres ϱ_λ, on aura $\sigma H = \sum_1^N \sigma_\lambda P_\lambda^\mu$, où tous les σ_λ seront des entiers positifs.

Si donc X est un entier quelconque $\geqq \sigma B$, soit $X = \sigma H + \theta$ $(H \geqq B,\ 0 \leqq \theta < \sigma)$, nous aurons $X = \sum_1^N{}^\lambda \sigma_\lambda P_\lambda^\mu + \theta$, et, par conséquent, tout nombre entier X suffisamment grand peut être décomposé en une somme d'au plus $\left[\sum_1^N{}^\lambda \sigma_\lambda + \sigma - 1\right]$ puissances μ^{es} de nombre entiers positifs.

C. Q. F. D.

M. Hurwitz a en outre énoncé*) la proposition suivante très remarquable, mais dont il n'a pas réussi à prouver la vérité:

Théorème 2. *En désignant par $x_1, \cdots, x_r$ un nombre arbitraire de variables indépendantes, on pourra, pour tout nombre entier positif m, trouver une identité de la forme*

$$(1) \qquad (x_1^2 + \cdots + x_r^2)^m = \sum_1^M{}^\lambda \varrho_\lambda (a_{1.\lambda} x_1 + \cdots + a_{r.\lambda} x_r)^{2m},$$

M désignant un entier positif, ϱ_λ des nombres rationnels positifs et $a_{\nu.\lambda}$ des nombres rationnels $\gtreqless 0$, qui sont tous indépendants de $x_1, \cdots, x_r$. Pour préciser, on peut en outre, en supprimant dans la parenthèse le commun multiple des dénominateurs des $a_{\nu.\lambda}$, supposer que tous les $a_{\nu.\lambda}$ soient des nombres entiers.

M. Hilbert a le premier donné la preuve fort ingénieuse de cette supposition de M. Hurwitz.**) De la modification très élégante de cette preuve donnée plus tard par M. Hausdorff***), il résulte qu'elle peut être ramenée à une étude arithmétique élémentaire des coefficients de binôme.

En étudiant ces coefficients, on peut dans bien des cas se servir avec profit d'un symbole qui a été pour la première fois introduit par

---

*) Hurwitz, Über die Darstellung ganzer Zahlen als Summen von n^{ten} Potenzen ganzer Zahlen. Math. Ann. 65 (1908), S. 424.

**) Hilbert, loc. cit.

***) Hausdorff, Zur Hilbertschen Lösung des Waringschen Problems. Math. Ann. 67 (1909), S. 301.

M. Gordan*) et qui se prête bien à des généralisations. A ce sujet je renvoie à la note précitée de M. Gordan ou à un article que j'ai publié dans les Acta Mathematica 33, où le symbole de M. Gordan a été généralisé dans diverses directions. Dans la recherche présente je ferai usage de la modification suivante du symbole:

J'introduis un caractère h qui aura la signification symbolique suivante: $h^{2\mu}$ désignera $\frac{(2\mu)!}{\mu!}$ pour tous les entiers pairs $2\mu \geqq 0$, et $h^{2\mu+1}$ désignera *zéro* pour tous les entiers impairs $2\mu + 1 \geqq 1$. $h^\mu \cdot h^\nu$ signifiera toujours $h^{\mu+\nu}$ et non pas le produit de h^μ et h^ν. $(x+h)^\nu$ sera défini par la formule du binôme et, par conséquent, $f(x)$ désignant un polynôme quelconque, soit de degré m, $f(x+h)$ sera défini par le développement taylorien, savoir

$$\frac{(x+h)^\nu}{\nu!} = \sum_0^\nu{}_\mu \frac{x^\mu}{\mu!} \frac{h^{\nu-\mu}}{(\nu-\mu)!}, \quad f(x+h) = \sum_0^m{}_\mu \frac{h^\mu}{\mu!} f^\mu(x).$$

Pour exprimer le produit de h^μ et h^ν, il y a lieu d'introduire deux caractères h_1 et h_2 qui auront tous deux la signification symbolique développée ci-dessus pour h, de façon que $h_1{}^\mu = h_2{}^\mu = h^\mu$, $h_1{}^\mu \cdot h_1{}^\nu = h_1{}^{\mu+\nu}$, et ainsi de suite, tandis que $h_1{}^\mu \cdot h_2{}^\nu$ désignera naturellement le produit de $h_1{}^\mu$ et $h_2{}^\nu$.

En se servant de ces symboles et des propriétés élémentaires bien connues de la fonction eulérienne $\Gamma(x)$, on peut sous une forme simple énoncer et prouver quelques propriétés arithmétiques très intéressantes des coefficients de binôme parmi lesquelles je ne ferai usage ici que de la proposition suivante établie par M. Hausdorff dans son étude sur la preuve de M. Hilbert du théorème de Waring:

Lemme. *En désignant par $f(x)$ un polynôme rationnel quelconque, qui ne devient jamais négatif pour des valeurs réelles de l'argument, on aura toujours $f(x+h) > 0$ pour x réel**).*

---

*) Gordan, Transcendenz von e und π. Math. Ann. 43 (1893).

**) Il n'est pas sans intérêt de rappeler, à ce propos, que Hermite et M. Hurwitz ont établi un théorème tout à fait analogue à celui de M. Hausdorff mais où h est le symbole original de M. Gordan, à savoir $h^r = r!$. La preuve découle directement de la formule bien connue

$$f(x+h) = \int_0^\infty e^{-\alpha} f(x+\alpha)\, d\alpha.$$

(Voir Hurwitz. Über die Nullstellen der Besselschen Funktion. Math. Ann. 33 (1889), S. 259.) — Pour plus de détails je renvoie à mes deux notes précitées (Arkiv för mat.).

En effet, on aura, d'après les éléments de la théorie de la fonction $\Gamma(x)$,

$$h^{2\mu} = 4^\mu \frac{\Gamma\left(\mu+\frac{1}{2}\right)}{\Gamma\left(\frac{1}{2}\right)} = \frac{2}{\Gamma\left(\frac{1}{2}\right)} \int_0^\infty e^{-\frac{\alpha^2}{4}} \alpha^{2\mu} d\alpha = \frac{1}{\Gamma\left(\frac{1}{2}\right)} \int_{-\infty}^{+\infty} e^{-\frac{\alpha^2}{4}} \alpha^{2\mu} d\alpha,$$

$$h^{2\mu+1} = 0 = \frac{1}{\Gamma\left(\frac{1}{2}\right)} \int_{-\infty}^{+\infty} e^{-\frac{\alpha^2}{4}} \alpha^{2\mu+1} d\alpha,$$

et, par suite, on aura

$$f(x+h) = \frac{1}{\Gamma\left(\frac{1}{2}\right)} \int_{-\infty}^{+\infty} e^{-\frac{\alpha^2}{4}} f(x+\alpha)\, d\alpha.$$

Si donc $f(\alpha) \geqq 0$ pour $-\infty \leqq \alpha \leqq +\infty$, on aura évidemment $f(x+h) > 0$.

C. Q. F. D.

Maintenant, en profitant des idées de M. Hilbert, on peut aisément démontrer le théorème 2. On aura, en effet,

$$\begin{cases} (h_1 x_1 + \cdots + h_r x_r)^{2m} = \underline{|2m} \sum\limits_{\mu_1+\cdots+\mu_r=m} \dfrac{h_1^{2\mu_1} x_1^{2\mu_1}}{\underline{|2\mu_1}} \cdots \dfrac{h_r^{2\mu_r} x_r^{2\mu_r}}{\underline{|2\mu_r}} \\ \qquad = \underline{|2m} \sum\limits_{\mu_1+\cdots+\mu_r=m} \dfrac{x_1^{2\mu_1}}{\underline{|\mu_1}} \cdots \dfrac{x_r^{2\mu_r}}{\underline{|\mu_r}} = \dfrac{\underline{|2m}}{\underline{|m}} (x_1^2 + \cdots + x_r^2)^m, \\ (h_1 x_1 + \cdots + h_r x_r)^{2m+1} = 0, \end{cases}$$

ou, en d'autres termes,

$$(2) \qquad (h_1 x_1 + \cdots + h_r x_r)^m = h^m (x_1^2 + \cdots + x_r^2)^{\frac{m}{2}} \qquad (m = 0, 1, 2, \cdots).$$

Soient maintenant $\beta_1, \cdots, \beta_m$ des quantités réelles quelconques, toutes inégales, et dont le discriminant sera, par suite, $\neq 0$, et désignons par $\varrho_1, \cdots, \varrho_m$ m quantités réelles bien définies par les égalités

$$(3) \qquad \sum_1^m {}_\lambda\, \varrho_\lambda \beta_\lambda^{\,\nu} = h^\nu \qquad (\nu = 0, 1, \cdots, m-1).$$

D'après les équations (2) et (3) nous aurons

$$h^\mu (x_1^2 + \cdots + x_r^2)^{\frac{\mu}{2}} = (h_1 x_1 + \cdots + h_r x_r)^\mu = \sum_{\lambda_1, \cdots, \lambda_r = 1}^m \varrho_{\lambda_1} \cdot \varrho_{\lambda_2} \cdots \varrho_{\lambda_r} (\beta_{\lambda \cdot 1} x_1 + \cdots + \beta_{\lambda \cdot r} x_r)^\mu,$$

$$(\mu = 0, 1, \cdots, m-1).$$

Donc, il reste seulement à prouver qu'on peut toujours donner à $\beta_1, \cdots, \beta_m$ des valeurs rationnelles auxquelles correspondent des valeurs également rationnelles et *positives* de $\varrho_1, \cdots, \varrho_m$.

A cet effet, introduisons dans (2) $r = 2$, $x_1 = x + 1$, $x_2 = i$, nous aurons

$$(h_1 x + h_1 + h_2 i)^{2m} = h^{2m} x^m (x+2)^m,$$

$$(h_1 x + h_1 + h_2 i)^{2m+1} = 0.$$

En identifiant les coefficients de x^μ, nous aurons

$$(4') \qquad h_1^\mu (h_1 + h_2 i)^\nu = 0 \quad \text{pour} \quad \mu < \nu,$$

et, par suite, nous aurons, en désignant par $\varphi_{m-1}(x)$ un polynôme quelconque de degré $\leqq m-1$,

$$(4) \qquad \varphi_{m-1}(h_1) \cdot (h_1 + h_2 i)^m = 0.$$

Pour la fonction $H_m(x) = (x + h_2 i)^m$ nous aurons la formule de récurrence qui suit

$$(5) \qquad (x + h_2 i)^m = x(x + h_2 i)^{m-1} - 2(m-1)\,(x + h_2 i)^{m-2}.$$

Dès lors, les fonctions de Sturm correspondant à $H_m(x)$ seront $H_m, H_{m-1}, \cdots, H_1, H_0 = 1$, et $H_m(x)$ aura donc toujours m zéros réels différents (pour $m = 1, 2, 3, \cdots$).

Substituons donc d'abord pour $\beta_1, \cdots, \beta_m$ les racines de $H_m(x) = 0$.

Soit, de plus, $f_n(x)$ un polynôme quelconque de degré $n \leqq 2m - 1$, et désignons, si $n \geqq m$, par $f_{m-1}(x)$ le résidu de $f_m(x)$ (mod. $H_m(x)$), de sorte que

$$(6) \qquad f_n(x) = \varphi_{m-1}(x) \cdot H_m(x) + f_{m-1}(x),$$

nous aurons, d'après les égalités (4) et (6),

$$(7) \qquad \begin{cases} f_n(h_1) = f_{m-1}(h_1), \quad \text{et} \\ f_n(\beta_\lambda) = f_{m-1}(\beta_\lambda) \end{cases} \qquad \lambda = 1, 2, \cdots, m.$$

En vertu des égalités (3), nous aurons

$$\sum_1^m{}^\lambda \varrho_\lambda f_{m-1}(\beta_\lambda) = f_{m-1}(h_1).$$

Donc, on aura, d'après les équations (7),

$$(7') \qquad \sum_1^m{}^\lambda \varrho_\lambda f_n(\beta_\lambda) = f_n(h_1).$$

Introduisons dans l'identité (7') cette valeur particulière de $f_n(x)$:

$$f_n(x) = \left(\frac{H_m(x)}{x - \beta_\varkappa}\right)^2,$$

nous aurons

$$f_n(\beta_\lambda) = 0 \quad \text{pour} \quad \lambda \neq \pi \quad \text{et} \quad f_n(\beta_\pi) = (H'_m(\beta_\pi))^2 > 0,$$

d'où suit, d'apres (7'),

$$\varrho_\pi (H'_m(\beta_\pi))^2 = f_n(h_1) \qquad (\pi = 1, 2, \cdots, m).$$

Suivant le théorème de M. Hausdorff, nous aurons $f_n(h_1) > 0$, d'où l'on tire finalement $\varrho_\pi > 0$, pour $\pi = 1, 2, \cdots, m$.

Si, d'autre part, $\beta_1, \cdots, \beta_m$ sont des nombres rationnels suffisamment rapprochés des racines de $H_m(x) = 0$, les $\varrho_1, \cdots, \varrho_m$ correspondants seront évidemment toujours positifs, et, d'après les égalités (3), ils seront en outre rationnels.

C. Q. F. D.

De ce théorème, M. Hurwitz a encore tiré une conclusion bien intéressante, qui, avec une légère modification, faite par M. Hilbert, peut être exprimée ainsi:

Théorème 3. *En désignant par* m, x *et* θ *des entiers quelconques* $\geqq 0$, *on aura toujours*

$$(1') \qquad (x^2 + \theta)^m = \sum_1^M {}_\lambda\, \varrho_\lambda (\alpha_\lambda x + \beta_\lambda)^{2m} = \sum (2m),$$

M désignant un entier positif, ϱ_λ des nombres rationnels positifs, α_λ et β_λ des entiers $\gtreqless 0$, et M, ϱ_λ, α_λ ne dépendant que de m.

En effet, tout nombre entier $\theta \geqq 0$ peut être décomposé en une somme de quatre carrés, soit

$$\theta = x_1^2 + x_2^2 + x_3^2 + x_4^2, \qquad x_1, x_2, x_3, x_4 \geqq 0.$$

Donc, nous aurons, d'après le théorème 2,

$$(x^2 + \theta)^m = (x^2 + x_1^2 + \cdots + x_4^2)^m = \sum_1^M {}_\lambda\, \varrho_\lambda (\alpha_\lambda x + a_{1\lambda} x_1 + a_{2\lambda} x_2 + a_{3\lambda} x_3 + a_{4\lambda} x_4)^{2m}.$$

C. Q. F. D.

Corollaire de M. Hurwitz. *Si le théorème de Waring est valable pour $n = m$, il le sera aussi pour $n = 2m$.*

A l'aide de ces théorèmes préliminaires, on peut sans peine démontrer la proposition de Waring.

Nous aurons d'abord le lemme suivant:

Lemme. *Soit p un entier positif quelconque $\leq m$; en désignant par x un entier positif quelconque et par T un entier quelconque $\geqq x^2$, on peut toujours trouver une égalité de la forme*

$$(1'') \qquad \sum_0^{p-1} {}_\nu\, B_{\nu \cdot p}\, x^{2\nu} T^{m-\nu} + x^{2p} T^{m-p} = \sum (m),$$

où les $B_{\nu \cdot p}$ désignent certains entiers positifs qui ne dépendent que de m et p.

En effet, introduisons dans (1') $m+p$ au lieu de m et différentions $2p$ fois par rapport à x, nous aurons

$$\sum_0^p{}^{\nu} A_{\nu\,p}\, x^{2\nu}(x^2+\theta)^{m-\nu} = \sum_1^M{}^{\lambda} \varrho_\lambda \frac{\underline{|2(m+p)}}{\underline{|2m}}\, \alpha_\lambda^{2p}(\alpha_\lambda x+\beta_\lambda)^{2m} = \sum (2m),$$

où $A_{\nu\cdot p}$ désignent des entiers positifs qui ne dépendent que de m et p.

Or, faisons $x^2+\theta = A_{p\cdot p} T$ et introduisons

$$B_{\nu\cdot p} = A_{\nu\cdot p} A_{p\cdot p}^{p-\nu-1} \qquad (\nu = 0, 1, \cdots, p),$$

nous aurons

$$\sum_0^p{}^{\nu} B_{\nu\cdot p}\, x^{2\nu}\, T^{m-\nu} = \sum (m), \quad B_{p\cdot p} = 1.$$

C. Q. F. D.

Soit maintenant $m > 2$, et supposons que le théorème de Waring soit valable pour $n < m$. Donc, suivant le corrollaire de M. Hurwitz, ce théorème est aussi valable pour toutes les valeurs entières paires $n < 2m$.

Donc, en désignant par K_{m-p} un entier positif*) quelconque $< T$, on peut toujours trouver r nombres entiers $x_{1\cdot p}, x_{2\cdot p}, \cdots, x_{r\cdot p} \geqq 0$, qui remplissent la condition

$$(8) \qquad \sum_1^r{}^{i} x_{i\cdot p}^{2p} = K_{m-p} \qquad (p = 1, 2, \cdots, m-1),$$

r étant un nombre qui ne dépend que de m.

Introduisons dans l'équation (1'') $x = x_{1\cdot p}, x_{2\cdot p}, \cdots, x_{r\cdot p}$ respectivement, et ajoutons les égalités, il vient

$$(9') \qquad \sum_0^{p-1}{}^{\nu} T^{m-\nu} B_{\nu\cdot p} \cdot \sum_1^r{}^{i} x_{i\cdot p}^{2\nu} + K_{m-p} \cdot T^{m-p} = \sum (m).$$

Soit B le plus grand des nombres $B_{\nu\cdot p}$ ($\nu = 1, 2, \cdots, p$; $p = 1, 2, \cdots, m-1$), nous aurons $B_{\nu\cdot p} \cdot \sum_1^r{}^{i} x_{i\cdot p}^{2\nu} \leqq BK_{m-p} < BT$, pour $\nu = 1, 2, \cdots, p$, tandis que, pour $\nu = 0$, $B_{0\cdot p} r \leqq Br$. Par conséquent, l'expression (9') doit être $< (r+2)BT^m$. Ecrivons, en substituant $q = m-p$,

$$(9) \qquad J_{q+1} T^{q+1} + K_q T^q = \sum (m) < B(r+2)\, T^m \quad (q = 1, 2, \cdots, m-1).$$

Ajoutant les égalités (9), nous aurons

$$\sum_1^{m-1}{}^{q} (J_{q+1} T^{q+1} + K_q T^q) = \sum_1^m{}^{q} (J_q + K_q)\, T^q = \sum (m) < (m-1)\, B(r+2)\, T^m.$$

*) Par entier «positif» j'entends toujours un entier $\geqq 0$.

Par conséquent, en désignant par $K_0', K_1', \cdots, K_{m-1}'$ des entiers positifs quelconques $< T$, on peut toujours disposer des quantités $K_1, \cdots, K_m$ de manière qu'on aura d'abord

$$(10) \qquad JT^m + \sum_1^{m-1}{}^q K_q' T^q = \sum(m), \quad J \leqq (m-1)B(r+2),$$

et, de même, en substituant $T+1$ au lieu de T,

$$J(T+1)^m + K_0' \cdot (T+1) = \sum(m),$$

ou, en d'autres termes,

$$(11) \qquad JT^m + \sum_2^{m-1}{}^q \binom{m}{q} JT^q + (mJ + K_0')T + J + K_0' = \sum(m).$$

En ajoutant les équations (10) et (11), nous aurons une égalité de la forme

$$(12) \qquad LT^m + \sum_0^{m-1}{}^q L_q \cdot T^q = \sum(m),$$

où l'on peut toujours supposer — en attribuant aux nombres K_q' des valeurs convenablement choisies — que $L_0, \cdots, L_{m-1}$ soient des entiers quelconques compris dans l'intervalle $0 \sim T$, et où L ne dépend que de m.

Désignons maintenant par $T_0 - 1$ le plus grand des produits $\binom{m}{q} L$, par H un entier quelconque $\geqq LT_0^m$ et par T l'entier de Gauss:

$$T = \left[\sqrt[m]{\frac{H}{L}}\right] \geqq T_0,$$

nous aurons $LT^m \leqq H < L(T+1)^m$. Or, par hypothèse, nous aurons $T \geqq T_0 > \binom{m}{q} L$ $(q = 0, 1, \cdots, m)$, et par suite l'expression (12) renferme tous les entiers H compris dans l'intervalle $LT^m \leqq H \leqq L(T+1)^m$ $(T \geqq T_0)$, ce qui entraîne $H = \Sigma(m)$.

Donc, en vertu du théorème 1, la supposition de Waring est valable pour $n = m$.

Nous avons donc prouvé que si le théorème de Waring-Hilbert est vrai pour $n < m$, il le sera aussi pour $n = m$. Or le théorème étant valable, comme on le sait, pour $n = 1$ et pour $n = 2$, il le sera aussi pour toutes les valeurs entières positives de n.

C. Q. F. D.