Zur Hilbertschen Lösung des Waringschen Problems.

Von

F. Hausdorff in Leipzig.

Herr Hilbert hat seinen Beweis der Waringschen Vermutung auf die Existenz einer in den Variablen $x_1, x_2, \cdots, x_r$ identisch gültigen Formel

$$(1) \qquad (x_1^2 + x_2^2 + \cdots + x_r^2)^m = \sum_h \varrho_h (a_{1h} x_1 + a_{2h} x_2 + \cdots + a_{rh} x_r)^{2m}$$

gestützt, in der die Koeffizienten a_{ih} der Linearformen ganze Zahlen, die ϱ_h *positive* rationale Zahlen sind. Für die niedrigsten Werte des Exponenten m und der Variablenzahl r ist eine solche Identität schon von anderen Autoren aufgestellt und dazu verwendet worden, die Waringsche Hypothese von m auf $2m$ zu übertragen. Bei der außerordentlich vergrößerten Tragweite, die der Formel (1) nach der Hilbertschen Entdeckung nunmehr zukommt, ist es wohl nicht ohne Interesse, einen zweiten Beweis dieser Formel mitzuteilen, der sich mit dem von Herrn Hilbert selbst gegebenen an prinzipieller Wichtigkeit zwar nicht messen kann, aber zur tatsächlichen Auffindung der passenden Koeffizienten ϱ_h, a_{ih} geeigneter sein dürfte.

I. Die Formel

$$(2) \qquad e^{-x^2} f_m(x) = \left(-\frac{1}{2}\right)^m \frac{d^m e^{-x^2}}{dx^m}$$

definiert $f_m(x)$ als Polynom m^{ten} Grades, für das man die Rekursionsformel

$$(3) \qquad f_{m+1}(x) = x f_m(x) - \frac{1}{2} f_m'(x)$$

und den expliziten Ausdruck

$$(4) \quad f_m(x) = x^m - \binom{m}{2} \cdot \frac{1}{2} x^{m-2} + \binom{m}{4} \cdot \frac{1}{2} \cdot \frac{3}{2} x^{m-4} - \binom{m}{6} \cdot \frac{1}{2} \cdot \frac{3}{2} \cdot \frac{5}{2} x^{m-6} + \cdots$$

$$= \frac{1}{\sqrt{\pi}} \int_{-\infty}^{+\infty} e^{-\alpha^2} (x + i\alpha)^m \, d\alpha$$

findet. Durch partielle Integration folgt aus (2) die Formel

$$\int_{-\infty}^{+\infty} e^{-x^2} f_m(x)\, g_{m-1}(x)\, dx = 0 \tag{5}$$

für ein beliebiges Polynom $g_{m-1}(x)$ vom Grade $m-1$, die übrigens mit der Orthogonalitätsbeziehung

$$\int_{-\infty}^{+\infty} e^{-x^2} f_m(x) f_n(x)\, dx = 0 \qquad (m \neq n)$$

gleichbedeutend ist.

Die Gleichung $f_m(x) = 0$ hat m verschiedene reelle Wurzeln. In der Tat ist diese Behauptung für $m = 1$ richtig und gestattet den Schluß von m auf $m+1$. Denn wenn $f_m(x) = 0$ die m reellen Wurzeln $\beta_1 < \beta_2 < \cdots < \beta_m$ hat, so hat $f_m'(\beta_h)$ das Zeichen $(-1)^{m-h}$ und nach (3) hat $f_{m+1}(\beta_h) = -\frac{1}{2} f_m'(\beta_h)$ das Zeichen $(-1)^{m+1-h}$. Insbesondere hat $f_{m+1}(\beta_m)$ das negative Zeichen und $f_{m+1}(\beta_1)$ das Zeichen $(-1)^m$, während $f_{m+1}(+\infty)$ positiv ist und $f_{m+1}(-\infty)$ das Zeichen $(-1)^{m+1}$ hat. Aus alledem geht hervor, daß die Gleichung $f_{m+1}(x) = 0$ $m+1$ reelle Wurzeln $\gamma_0\, \gamma_1 \cdots \gamma_m$ hat ($\gamma_0 < \beta_1 < \gamma_1 < \beta_2 < \cdots < \gamma_{m-1} < \beta_m < \gamma_m$). Damit ist die ausgesprochene Behauptung bewiesen.

II. Es besteht für jede natürliche Zahl m eine Identität in den Variabeln x, y von der Form

$$\frac{1}{\sqrt{\pi}} \int_{-\infty}^{+\infty} e^{-\alpha^2} (y + \alpha x)^{m-1} d\alpha = \sum_{1}^{m} {}_h\, \varrho_h (y + \beta_h x)^{m-1}, \tag{6}$$

worin die β_h reelle verschiedene, die ϱ_h reelle positive Zahlen sind.

Beweis. Denkt man sich die β_h zunächst irgendwie als reelle verschiedene Zahlen gewählt, so gibt die Forderung (6) zur Bestimmung der ϱ_h die m linearen Gleichungen mit nicht verschwindender Determinante

$$\sum \varrho_h = l_0, \quad \sum \varrho_h \beta_h = l_1, \quad \sum \varrho_h \beta_h^2 = l_2, \cdots, \sum \varrho_h \beta_h^{m-1} = l_{m-1}, \tag{7}$$

wobei

$$l_n = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{+\infty} e^{-\alpha^2} \alpha^n\, d\alpha,$$

insbesondere

$$l_0 = 1, \quad l_2 = \frac{1}{2}, \quad l_4 = \frac{1}{2} \cdot \frac{3}{2}, \quad l_6 = \frac{1}{2} \cdot \frac{3}{2} \cdot \frac{5}{2}, \cdots,$$

$$l_1 = l_3 = l_5 = l_7 = \cdots = 0.$$

Aus (7) folgt, daß für ein beliebiges Polynom $\varphi(x)$ vom Grade $m-1$

$$(8)\qquad \sum \varrho_h \varphi(\beta_h) = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{+\infty} e^{-\alpha^2} \varphi(\alpha)\, d\alpha.$$

Es sind nun aber die β_h so zu wählen, daß die ϱ_h positiv ausfallen. Wir nehmen zu diesem Zweck für die β_h die Wurzeln der Gleichung $f_m(x) = 0$. In diesem Falle behaupten wir, daß neben (8) die weitergehende Relation

$$(9)\qquad \sum \varrho_h \Phi(\beta_h) = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{+\infty} e^{-\alpha^2} \Phi(\alpha)\, d\alpha$$

besteht, in der $\Phi(x)$ ein beliebiges Polynom des Grades $2m-1$ ist. In der Tat erhalten wir durch Division mit $f_m(\alpha)$

$$\Phi(\alpha) = f_m(\alpha) \cdot g_{m-1}(\alpha) + \varphi(\alpha),$$

wo $g_{m-1}(\alpha)$, $\varphi(\alpha)$ vom Grade $m-1$ (höchstens) sind. Dann ist einerseits

$$\Phi(\beta_h) = \varphi(\beta_h),$$

andererseits nach (5)

$$\int_{-\infty}^{+\infty} e^{-\alpha^2} \Phi(\alpha)\, d\alpha = \int_{-\infty}^{+\infty} e^{-\alpha^2} \varphi(\alpha)\, d\alpha,$$

so daß (9) unmittelbar aus (8) folgt.

Setzen wir jetzt insbesondere

$$\begin{aligned}\Phi(\alpha) &= [(\alpha-\beta_1)\cdots(\alpha-\beta_{h-1})(\alpha-\beta_{h+1})\cdots(\alpha-\beta_m)]^2\\ &= [f_m(\alpha) : (\alpha-\beta_h)]^2,\end{aligned}$$

so folgt aus (9)

$$\varrho_h f_m'(\beta_h)^2 = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{+\infty} e^{-\alpha^2} \left(\frac{f_m(\alpha)}{\alpha-\beta_h}\right)^2 d\alpha,$$

also sind die ϱ_h wirklich positiv.

Die so spezialisierten Werte ϱ_h, β_h erfüllen, wie aus (9) folgt, außer (6) die weitergehende Identität

$$\frac{1}{\sqrt{\pi}} \int_{-\infty}^{+\infty} e^{-\alpha^2} (y+\alpha x)^{2m-1}\, d\alpha = \sum_1^m{}_h\, \varrho_h (y+\beta_h x)^{2m-1},$$

sie „kanonisieren" die hier linkerhand stehende binäre Form, worauf wir indessen für unsere Absicht keinen Wert zu legen haben.

III. Die Identität (6) läßt sich auch mit rationalen Werten der β_h und rationalen positiven Werten der ϱ_h erfüllen.

Denn die durch die Gleichungen (7) definierten Werte ϱ_h sind an jeder Stelle, wo die Determinante $|1, \beta_h, \beta_h^2, \cdots, \beta_h^{m-1}|$ nicht verschwindet, stetige Funktionen von $\beta_1, \beta_2, \cdots, \beta_m$. Wenn man also für die β_h jetzt rationale Werte wählt, die den Wurzeln der Gleichung $f_m(x) = 0$ hinlänglich benachbart sind, so bleiben die ϱ_h positiv und werden selbst rational, da die rechten Seiten l_n der Gleichungen (7) rational sind.

Wir können also sagen: für jede natürliche Zahl n besteht eine Identität

$$\frac{1}{\sqrt{\pi}} \int_{-\infty}^{+\infty} e^{-\alpha^2} (y + \alpha x)^n \, d\alpha = \sum_h \varrho_h (y + \beta_h x)^n \tag{10}$$

mit rationalen β_h, rationalen positiven ϱ_h und einer Gliederzahl rechterhand, die jedenfalls nicht größer als $n + 1$ gewählt zu werden braucht.

IV. Schreibt man in (10) α_1, x_1 für α, x, verwandelt y in $y + \alpha_2 x_2$, multipliziert mit $e^{-\alpha_2^2} : \sqrt{\pi}$ und integriert nach α_2 zwischen $\pm\infty$, so kommt

$$\left(\frac{1}{\sqrt{\pi}}\right)^2 \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} e^{-\alpha_1^2 - \alpha_2^2} (y + \alpha_1 x_1 + \alpha_2 x_2)^n \, d\alpha_1 \, d\alpha_2 = \sum_{hk} \varrho_h \varrho_k (y + \beta_h x_1 + \beta_k x_2)^n.$$

Verwandelt man hierin wieder y in $y + \alpha_3 x_3$, multipliziert mit $e^{-\alpha_3^2} : \sqrt{\pi}$ und integriert nach α_3, so ergibt sich

$$\begin{aligned}\left(\frac{1}{\sqrt{\pi}}\right)^3 \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} & e^{-\alpha_1^2 - \alpha_2^2 - \alpha_3^2} (y + \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3)^n \, d\alpha_1 \, d\alpha_2 \, d\alpha_3 \\ & = \sum_{hkl} \varrho_h \varrho_k \varrho_l (y + \beta_h x_1 + \beta_k x_2 + \beta_l x_3)^n.\end{aligned}$$

So fortfahrend erhält man für jedes r die Identität

$$\begin{aligned}\left(\frac{1}{\sqrt{\pi}}\right)^r \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} & e^{-\alpha_1^2 - \alpha_2^2 - \cdots - \alpha_r^2} (y + \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_r x_r)^n \, d\alpha_1 \, d\alpha_2 \cdots d\alpha_r \\ & = \sum_{h_1 h_2 \cdots h_r} \varrho_{h_1} \varrho_{h_2} \cdots \varrho_{h_r} (y + \beta_{h_1} x_1 + \beta_{h_2} x_2 + \cdots + \beta_{h_r} x_r)^n \\ & = \sum_k \sigma_k (y + \beta_{1k} x_1 + \beta_{2k} x_2 + \cdots + \beta_{rk} x_r)^n\end{aligned} \tag{11}$$

mit rationalen β_{ik} und positiven rationalen σ_k.

V. Aus der bekannten Formel

$$\frac{1}{\sqrt{\pi}} \int_{-\infty}^{+\infty} e^{-\alpha^2 + 2\alpha x} \, d\alpha = e^{x^2}$$

folgt

$$\left(\frac{1}{\sqrt{\pi}}\right)^r \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} e^{-\alpha_1^2 - \cdots - \alpha_r^2 + 2(\alpha_1 x_1 + \cdots + \alpha_r x_r)} \, d\alpha_1 \cdots d\alpha_r = e^{x_1^2 + \cdots + x_r^2}$$

und daraus

$$\left(\frac{1}{\sqrt{\pi}}\right)^r \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} e^{-\alpha_1^2 - \cdots - \alpha_r^2} (\alpha_1 x_1 + \cdots + \alpha_r x_r)^{2m} \, d\alpha_1 \cdots d\alpha_r$$
$$= \frac{(2m)!}{4^m m!} (x_1^2 + x_2^2 + \cdots + x_r^2)^m.$$

Setzt man also in (11), für gerades $n = 2m$, $y = 0$, so folgt eine Identität

$$(x_1^2 + x_2^2 + \cdots + x_r^2)^m = \sum_k \tau_k (\beta_{1k} x_1 + \beta_{2k} x_2 + \cdots + \beta_{rk} x_r)^{2m} \tag{12}$$

mit rationalen β_{ik} und rationalen positiven τ_k. Indem man die $2m^{\text{te}}$ Potenz des Generalnenners von $\beta_{1k} \beta_{2k} \cdots \beta_{rk}$ mit τ_k vereinigt, erhält man eine Identität (1) mit ganzzahligen a_{ih} und positiven rationalen ϱ_h. Q. E. D.

Die Formeln (11), (12) können, nachdem einmal eine passende Identität (10) gefunden ist, fast ohne Rechnung unmittelbar hingeschrieben werden. Die Gliederanzahl der Schlußformel (12) verkleinert sich, wenn man die β_h in (10) paarweise entgegengesetzt gleich wählt, und läßt sich auf Grund der Relationen zwischen linear abhängigen Formen in der von Herrn Hilbert angegebenen Weise noch weiter reduzieren.