Über die Komposition der quadratischen Formen von beliebig vielen Variablen[1].

(Nachrichten von der k. Gesellschaft der Wissenschaften zu Göttingen,
Mathematisch-physikalische Klasse, 1898, S. 309–316.)

Im Gebiete der quadratischen Formen von n Variablen wird eine Kompositionstheorie stattfinden, wenn für irgend drei quadratische Formen φ, ψ, χ von nicht verschwindender Determinante die Gleichung

$$\varphi(x_1,\, x_2, \dots x_n)\psi(y_1,\, y_2, \dots y_n) = \chi(z_1,\, z_2, \dots z_n) \tag{1}$$

dadurch befriedigt werden kann, dass man die Variablen $z_1,\, z_2, \dots z_n$ durch geeignet gewählte bilineare Funktionen der Variablen $x_1,\, x_2, \dots x_n$ und $y_1,\, y_2, \dots y_n$ ersetzt. Da eine quadratische Form durch lineare Transformation der Variablen in eine Summe von Quadraten übergeführt werden kann, so darf man, ohne die Allgemeinheit zu beeinträchtigen, an Stelle, der Gleichung (1) die folgende:

$$(x_1^2 + x_2^2 + \cdots + x_n^2)(y_1^2 + y_2^2 + \cdots + y_n^2) = z_1^2 + z_2^2 + \cdots + z_n^2 \tag{2}$$

betrachten. Hiernach ist die Frage, ob für quadratische Formen mit n Variablen eine Kompositionstheorie existiert, im wesentlichen identisch mit der andern, ob man der Gleichung (2) durch geeignete bilineare Funktionen $z_1,\, z_2, \dots z_n$ der $2n$ unabhängigen Variablen $x_1,\, x_2, \dots x_n,\, y_1,\, y_2, \dots y_n$ genügen kann. In den folgenden Zeilen will ich zeigen, dass dieses nur in den Fällen $n = 2,\, 4,\, 8$ möglich ist, dass also nur für binäre Formen, für quaternäre Formen und für Formen mit 8 Variablen eine Kompositionstheorie existiert. Durch diesen Nachweis wird dann insbesondere auch die alte Streitfrage, ob sich die bekannten Produktformeln für Summen von 2, 4 und 8 Quadraten auf Summen von mehr als 8 Quadraten ausdehnen lassen, endgültig, und zwar in verneinendem Sinne entschieden[2].

Zur Erleichterung der Darstellung bediene ich mich der wohl auf Cayley[3] zurückzuführenden Rechnung mit linearen Transformationen. Bezeichnet

$$A = \begin{Bmatrix} a_{11}, & a_{12}, & \dots & a_{1n} \\ a_{21}, & a_{22}, & \dots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1}, & a_{n2}, & \dots & a_{nn} \end{Bmatrix} \tag{3}$$

oder kürzer $A = (a_{\alpha\beta})$ eine solche Transformation, so möge unter A' diejenige Transformation verstanden werden, welche aus A durch Vertauschung der Horizontal- mit den Vertikalreihen hervorgeht. Die Aufgabe, der Gleichung (2) durch n bilineare Funktionen

$$z_\alpha = a_{\alpha 1}y_1 + a_{\alpha 2}y_2 + \cdots + a_{\alpha n}y_n \qquad (\alpha = 1,\, 2, \dots n)$$

[1]Hurwitz, Mathematische Werke, Bd. II (Algebra), LXXXII, S. 565–571.

[2]Roberts und Cayley haben sich im 16. und 17. Bande des Quarterly Journal mit dem Nachweis beschäftigt, dass ein Produkt von zwei Summen von je 16 Quadraten nicht als Summe von 16 Quadraten darstellbar sei. Ihre äusserst mühsamen, auf Probieren beruhenden Betrachtungen besitzen indessen keine Beweiskraft, weil ihnen bezüglich der bilinearen Formen $z_1,\, z_2, \dots$ spezielle Annahmen zugrunde liegen, die durch nichts gerechtfertigt sind. Die ältere Literatur über den Gegenstand findet sich in der Arbeit von Roberts erwähnt.
Man vergleiche auch: Brioschi, Sur l'analogie entre une classe de déterminants d'ordre pair, Crelles Journal, Bd. 52 (1856), S. 133–141 [Opere mathematiche, vol. 5, p. 511–520]. — F. Studnicka, Neuer Beweis des Satzes, dass das Produkt der Summe von acht Quadratzahlen mit der Summe von acht Quadratzahlen sich als Summe von acht Quadratzahlen darstellen lasse, Prager Berichte, 1883, S. 475–481. — A. Puchta, Über einen Satz von Euler-Brioschi-Genocchi, Wiener Berichte, Bd. 96 (1888), S. 110–133.

[3]Cayley, A memoir on the theory of Matrices, Phil. Trans., vol. 148 (1858), p. 17–38.

zu genügen, lässt sich nun offenbar auch so formulieren:

Man soll die Elemente $a_{\alpha\beta}$ der Transformation A als lineare homogene Funktionen der Variablen $x_1,\ x_2, \dots x_n$ so bestimmen, dass die Transformation A der Gleichung

$$AA' = (x_1^2 + x_2^2 + \cdots + x_n^2) \tag{4}$$

genügt.

Ordnet man A nach den Variablen $x_1,\ x_2, \dots x_n$, so erhält man

$$A = x_1 A_1 + x_2 A_2 + \cdots + x_n A_n, \tag{5}$$

wo $A_1,\ A_2, \dots A_n$ Transformationen mit konstanten Koeffizienten bezeichnen, und die Gleichung (4) gewinnt die Gestalt:

$$\begin{gathered}(x_1 A_1 + x_2 A_2 + \cdots + x_n A_n)(x_1 A_1' + x_2 A_2' + \cdots + x_n A_n') \\ = (x_1^2 + x_2^2 + \cdots + x_n^2).\end{gathered} \tag{6}$$

Der Vergleich der Glieder mit x_n^2 zeigt, dass $A_n A_n' = 1$ sein muss. Führt man daher die Transformationen

$$B_1 = A_1 A_n',\ B_2 = A_2 A_n', \dots\ B_{n-1} = A_{n-1} A_n' \tag{7}$$

ein und setzt dementsprechend

$$A_i = B_i A_n, \qquad A_i' = A_n' B_i', \qquad (i = 1,\ 2, \dots n-1)$$

so geht die Gleichung (6) in die folgende über:

$$\begin{gathered}(x_1 B_1 + x_2 B_2 + \cdots + x_{n-1} B_{n-1} + x_n)(x_1 B_1' + x_2 B_2' + \cdots + x_{n-1} B_{n-1}' + x_n) \\ = (x_1^2 + x_2^2 + \cdots + x_n^2).\end{gathered} \tag{8}$$

Entwickelt man hier die linke Seite, so ergibt die Koeffizientenvergleichung

$$B_i B_i' = 1, \qquad B_i' = -B_i, \qquad B_i B_k' = -B_k B_i', \qquad (i \lesseqgtr k)$$

und die letzteren Gleichungen können offenbar auch durch die folgenden ersetzt werden:

$$B_i^2 = -1, \qquad B_i B_k = -B_k B_i, \qquad B_i' = -B_i. \qquad (i \gtreqless k) \tag{9}$$

Auf diese Weise ergeben sich also aus jeder Transformation A, welche der Bedingung (4) genügt, $n-1$ Transformationen $B_1,\ B_2, \dots B_{n-1}$, welche die Gleichungen (9) befriedigen. Wenn umgekehrt $B_1,\ B_2, \dots B_{n-1}$ den Gleichungen (9) genügen, wenn ferner A_n eine beliebig gewählte orthogonale Transformation bezeichnet, so wird die Transformation

$$A = x_1 B_1 A_n + x_2 B_2 A_n + \cdots + x_{n-1} B_{n-1} A_n + x_n A_n$$

die Gleichung (4) befriedigen.

Hiernach brauchen wir uns nur noch mit der Aufgabe zu beschäftigen, alle Systeme von $n-1$ Transformationen $B_1,\ B_2, \dots B_{n-1}$ zu bestimmen, welche den Gleichungen (9) genügen. Wir unterziehen jetzt diese Gleichungen einer näheren Diskussion, welche zeigen wird, dass ausschliesslich in den Fällen $n = 2,\ 4,\ 8$, Systeme von $n-1$ Transformationen $B_1,\ B_2, \dots B_{n-1}$ existieren können, für welche die Gleichungen (9) erfüllt sind. Betrachten wir zunächst die Gleichungen $B_i' = -B_i$.

Dieselben besagen, dass die Transformationen B_i schiefsymmetrisch sind. Daher sind die Gleichungen (9) unverträglich, wenn n ungerade ist. Denn in diesem Falle würde die Determinante von B_i verschwinden müssen, was der Gleichung $B_i^2 = -1$ widerspricht.

Bei der weiteren Diskussion dürfen wir hiernach voraussetzen, dass n gerade ist. Vermöge der Gleichungen (9) ist jede ganze Funktion von $B_1,\ B_2, \dots B_{n-1}$ linear darstellbar durch die 2^{n-1} Transformationen

$$1, \quad B_{i_1}, \quad B_{i_1}B_{i_2}, \quad B_{i_1}B_{i_2}B_{i_3}, \dots, \quad B_1 B_2 \dots B_{n-1}, \tag{10}$$

wobei die Indices bzw. alle, den Ungleichungen

$$0 < i_1 < n, \quad 0 < i_1 < i_2 < n, \quad 0 < i_1 < i_2 < i_3 < n, \dots$$

genügenden, Wertsysteme zu erhalt haben. In betreff dieser Transformationen (10) lehrt die Gleichung

$$\begin{aligned}(B_{i_1}B_{i_2} \cdots B_{i_r})' = B'_{i_r} \cdots B'_{i_2} B'_{i_1} &= (-1)^r B_{i_r} \cdots B_{i_2} B_{i_1} \\ &= (-1)^{r+(r-1)+(r-2)+\cdots+1} B_{i_1} B_{i_2} \cdots B_{i_r},\end{aligned}$$

dass die Transformation

$$B_{i_1}B_{i_2} \cdots B_{i_r}$$

symmetrisch oder schiefsymmetrisch ist, je nachdem $r \equiv 0, 3$ oder $r \equiv 1, 2 \pmod 4$ ist. Diese Tatsache gestattet nun weiter, die Frage zu entscheiden, ob zwischen den Transformationen (10) eine lineare Abhängigkeit bestehen kann. Bezeichnen wir allgemein mit $R,\ R_1,\ R_2, \dots$ lineare Kombinationen der Transformationen (10) mit nicht sämtlich verschwindenden Koeffizienten, so wird $R = 0$ die allgemeine Gestalt einer linearen Relation zwischen den Transformationen (10) vorstellen. Jede der Transformationen (10), welche in einer solchen Relation mit einem nicht vershwindenden Koeffizienten behaftet ist, möge an der Relation „beteiligt" heissen. Sind ferner $R_1 = 0,\ R_2 = 0$ zwei Relationen, so will ich dieselben „einander fremd" nennen, wenn es keine Transformation gibt, die gleichzeitig an beiden Relationen beteiligt ist. Endlich heisse eine Relation $R = 0$ „reduzibel", wenn ihre linke Seite in die Form $R = R_1 + R_2$ gesetzt werden kann, derart, dass $R_1 = 0,\ R_2 = 0$ zwei einander fremde Relationen vorstellen. Im entgegengesetzten Falle heisse $R = 0$ „irreduzibel".

Offenbar genügt es, die irreduzibeln Relationen zu betrachten. Eine solche Relation bleibt irreduzibel, wenn man sie mit einer der Transformationen (10) multipliziert, und durch eine derartige Multiplikation kann man erreichen, dass die Transformation 1 mit einem nicht verschwindenden Koeffizienten in die Relation eingeht.

Ferner leuchtet ein, dass die Transformationen, welche an einer irreduzibeln Relation beteiligt sind, entweder sämtlich symmetrisch oder sämtlich schiefsymmetrisch sind. Sei nun

$$1 = \sum c_{i_1 i_2 i_3} B_{i_1} B_{i_2} B_{i_3} + \sum c_{i_1 i_2 i_3 i_4} B_{i_1} B_{i_2} B_{i_3} B_{i_4} + \cdots \tag{11}$$

eine irreduzible Relation. Durch Multiplikation mit B_i, wo i irgend einen der Indices $1,\ 2, \dots n-1$ bezeichnet, geht dieselbe über in:

$$B_i = \sum c_{i_1 i_2 i_3} B_{i_1} B_{i_2} B_{i_3} B_i + \sum c_{i_1 i_2 i_3 i_4} B_{i_1} B_{i_2} B_{i_3} B_{i_4} B_i + \cdots .$$

Hier dürfen nun rechter Hand nur schiefsymmetrische Transformationen auftreten. Es muss daher $c_{i_1 i_2 i_3} = 0$ sein, wenn der Index i sich nicht unter den Indices $i_1,\ i_2,\ i_3$ befindet. Da aber der Index i willkürlich wählbar ist, so müssen sämtliche Koeffizienten $c_{i_1 i_2 i_3} = 0$ sein. Ebenso folgt, dass $c_{i_1 i_2 i_3 i_4} = 0$ ist, wenn der Index i unter den Indices $i_1,\ i_2,\ i_3,\ i_4$ vorkommt; folglich sind sämtliche

Koeffizienten $c_{i_1 i_2 i_3 i_4} = 0$. Indem man so weiter schliesst, erkennt man, dass die Relation (11) nur die Form

$$1 = c \cdot B_1 B_2 \dots B_{n-1} \tag{11'}$$

besitzen kann, wobei überdies noch $n \equiv 0 \pmod{4}$ sein muss, weil andernfalls $B_1 B_2 \dots B_{n-1}$ eine schiefsymmetrische Transformation sein würde. Quadriert man die beiden Seiten der Relation (11′), so erkennt man, dass $c = \pm 1$ sein muss. Ausser der Relation (11′) können keine andern irreduzibeln Relationen existieren, als die, welche aus (11′) durch Multiplikation mit den Transformationen (10) hervorgehen.

Fassen wir die vorstehenden Überlegungen zusammen, so können wir sagen:

Befriedigen die $n-1$ Transformationen $B_1, B_2, \dots B_{n-1}$ die Gleichungen (9), so ist notwendig n eine gerade Zahl. Die 2^{n-1} Transformationen (10) sind ferner linear unabhängig, wenn $n \equiv 2 \pmod{4}$. Sie sind dagegen im Falle $n \equiv 0 \pmod{4}$ entweder linear unabhängig, ober aber es bestehen zwischen ihnen die Relationen, welche aus

$$B_1 B_2 \cdots B_{n-1} = \pm 1 \tag{12}$$

durch Multiplikation mit den Transformationen (10) hervorgehen und keine andern irreduzibeln Relationen. Die ersten 2^{n-2} der Transformationen (10) sind also unter allen Umständen linear unabhängig.

Hieraus folgt nun, dass die Lösbarkeit der Gleichungen (9) die Ungleichung

$$2^{n-2} \leqq n^2 \tag{13}$$

nach sich zieht, da zwischen mehr als n^2 Transformationen stets eine lineare Abhängigkeit besteht. Die Ungleichung (13) ist aber von $n = 10$ ab nicht mehr erfüllt. Es bleiben also nur die Fälle $n = 2, 4, 6, 8$, in welchen möglicherweise die Gleichungen (9) eine Auflösung zulassen. Der Fall $n = 6$ lässt sich ohne weiteres ausscheiden. In diesem Falle würden nämlich die $2^5 = 32$ Transformationen (10) linear unabhängig sein müssen. Unter diesen Transformationen finden sich $5+10+1 = 16$ schiefsymmetrische. Allgemein besteht aber zwischen $\frac{n(n-1)}{2}+1$ schiefsymmetrischen Transformationen bei n Variablen eine lineare Abhängigkeit, und es ergibt sich für $n = 6$ der Wert von $\frac{n(n-1)}{2} + 1 = 16$.

In den Fällen $n = 2, 4, 8$ ergibt eine leichte, wenn auch etwas umständliche Diskussion die wirkliche Auflösbarkeit der Gleichungen (9) und also die Existenz von Transformationen A, welche der Bedingung (4) genügen. Das Resultat dieser Diskussion lautet folgendermassen: Man verstehe unter A_0 in den Fällen $n = 2, 4, 8$ bzw. die Transformation

$$A_0 = \left\{ \begin{array}{rr} x_1, & -x_2 \\ x_2, & x_1 \end{array} \right\},$$

$$A_0 = \left\{ \begin{array}{rrrr} x_1, & -x_2, & -x_3, & -x_4 \\ x_2, & x_1, & -x_4, & x_3 \\ x_3, & x_4, & x_1, & -x_2 \\ x_4, & -x_3, & x_2, & x_1 \end{array} \right\},$$

$$A_0 = \left\{ \begin{array}{rrrrrrrr} x_1, & -x_2, & -x_3, & -x_4, & -x_5, & -x_6, & -x_7, & -x_8 \\ x_2, & x_1, & -x_4, & x_3, & -x_6, & x_5, & -x_8, & x_7 \\ x_3, & x_4, & x_1, & -x_2, & -x_7, & x_8, & x_5, & -x_6 \\ x_4, & -x_3, & x_2, & x_1, & x_8, & x_7, & -x_6, & -x_5 \\ x_5, & x_6, & x_7, & -x_8, & x_1, & -x_2, & -x_3, & x_4 \\ x_6, & -x_5, & -x_8, & -x_7, & x_2, & x_1, & x_4, & x_3 \\ x_7, & x_8, & -x_5, & x_6, & x_3, & -x_4, & x_1, & -x_2 \\ x_8, & -x_7, & x_6, & x_5, & -x_4, & -x_3, & x_2, & x_1 \end{array} \right\}.$$

Dann ist die allgemeinste Transformation A, welche der Bedingung (4) genügt, die folgende:

$$A = PA_0Q,$$

wobei P und Q willkürlich zu wählende orthogonale Transformationen mit konstanten Koeffizienten bezeichnen.

An die vorstehende Untersuchung knüpfen sich einige Fragen, auf die ich noch kurz hinweisen möchte. Wenn es auch, abgesehen von den Fällen $n = 2, 4, 8$, unmöglich ist, das Produkt von zwei quadratischen Formen von je n Variablen $x_1, \dots x_n$, $y_1, \dots y_n$ darzustellen als quadratische Form von n bilinearen Funktionen $z_1, z_2, \dots z_n$ jener Variablen, so ist doch eine Darstellung jenes Punktes als quadratische Form von einer genügend gross gewählten Anzahl bilinearer Funktionen der Variablen $x_1, \dots x_n$, $y_1, \dots y_n$ immer möglich. Es fragt sich nun, welches der kleinste zulässige Wert dieser Anzahl ist. Transformiert man die quadratischen Formen auf Summen von Quadraten, so gewinnt die Frage folgende Gestalt:

Welches ist der kleinste Wert von m, für welchen die Gleichung

$$(x_1^2 + x_2^2 + \dots + x_n^2)(y_1^2 + y_2^2 + \dots + y_n^2) = z_1^2 + z_2^2 + \dots + z_m^2 \tag{14}$$

durch geeignet gewählte bilineare Funktionen $z_1, z_2, \dots z_m$ der Variablen $x_1, \dots x_n$, $y_1, \dots y_n$ befriedigt werde kann?

Diese Frage lässt sich noch dadurch verallgemeinern, dass man an die Stelle der Gleichung (14) die folgende:

$$(x_1^2 + x_2^2 + \dots + x_p^2)(y_1^2 + y_2^2 + \dots + y_n^2) = z_1^2 + z_2^2 + \dots + z_m^2 \tag{15}$$

setzt, wobei p und n gegebene Zahlen bezeichnen und wiederum der Minimalwert von m in Frage steht.

Andererseits kann man in vorstehender Gleichung auch n und m als gegeben annehmen und nach dem grössten zulässigen Werte von p fragen. Diese Fragestellung gestattet in dem Falle $n = m$ eine andere Einkleidung. Betrachtet man nämlich im Raume von n^2 Dimensionen, in welchem die n^2 Koordinaten eines Punktes mit a_{ik} $(i, k = 1, 2, \dots n)$ bezeichnet werden mögen, das Gebilde, welches durch die Gleichungen

$$\sum_{i=1}^{n} a_{i1}^2 = \sum_{i=1}^{n} a_{i2}^2 = \dots = \sum_{i=1}^{n} a_{in}^2, \ \sum_{i=1}^{n} a_{ih}a_{ik} = 0 \quad (h, k = 1, 2, \dots n;\ h \gtrless k)$$

definiert ist, so bezeichnet der Maximalwert von p nichts anderes, als die höchste Dimension linearer Räume, die auf diesem Gebilde liegen. Übrigens ergibt eine Analyse, welche der oben dargelegten ganz ähnlich ist, dass dieser Maximalwert von p im Falle eines ungeraden n gleich 1 ist und im Falle eines geraden n durch die Ungleichungen $2^{p-1} \leqq n^2$, bzw. $2^{p-2} \leqq n^2$ eingeschränkt ist, je nachdem $n \equiv 2$ oder $n \equiv 0 \pmod{4}$ ist. Es kann also, wenn n eine gerade Zahl ist, der Maximalwert von p nicht über $\frac{2 \lg n}{\lg 2} + 1$ bzw. $\frac{2 \lg n}{\lg 2} + 2$ liegen.

Zürich, den 25. Juni 1898.