Ueber die Composition der quadratischen Formen von beliebig vielen Variabeln.

Von

A. Hurwitz in Zürich,
correspondirendem Mitgliede der Gesellschaft.

Vorgelegt in der Sitzung am 9. Juli 1898.

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

$$(1)\qquad \varphi(x_1, x_2, \ldots x_n)\psi(y_1, y_2, \ldots y_n) = \chi(z_1, z_2, \ldots z_n)$$

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

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

betrachten. Hiernach ist die Frage, ob für quadratische Formen mit n Variabeln eine Compositionstheorie existirt, im Wesentlichen identisch mit der andern, ob man der Gleichung (2) durch geeignete bilineare Functionen $z_1, z_2, \ldots z_n$ der $2n$ unabhängigen Variabeln $x_1, x_2, \ldots x_n, y_1, y_2, \ldots y_n$ 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 Variabeln eine Compositionstheorie existirt. 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 [1]).

Zur Erleichterung der Darstellung bediene ich mich der wohl auf Cayley [2]) zurückzuführenden Rechnung mit linearen Transformationen. Bezeichnet

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

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 Verticalreihen hervorgeht. Die Aufgabe, der Gleichung (2) durch n bilineare Functionen

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

zu genügen, läßt sich nun offenbar auch so formuliren:

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

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

genügt.

---

1) Roberts und Cayley haben sich im 16ten und 17ten 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 Probiren beruhenden Betrachtungen besitzen indessen keine Beweiskraft, weil ihnen bezüglich der bilinearen Formen $z_1, z_2, \dots$ specielle Annahmen zu Grunde liegen, die durch nichts gerechtfertigt sind. Die ältere Litteratur uber 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. 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. A. Puchta, „Ueber einen Satz von Euler-Brioschi-Genocchi". Wiener Berichte. Bd. 96.

2) Cayley, A memoir on the theory of Matrices. Phil. Trans. vol. 148.

Ordnet man A nach den Variabeln $x_1, x_2, \ldots x_n$, so erhält man

$$(5) \qquad A = x_1 A_1 + x_2 A_2 + \cdots + x_n A_n,$$

wo $A_1, A_2, \ldots A_n$ Transformationen mit constanten Coefficienten bezeichnen, und die Gleichung (4) gewinnt die Gestalt:

$$(6) \qquad (x_1 A_1 + x_2 A_2 + \cdots + x_n A_n)(x_1 A_1' + x_2 A_2' + \cdots + x_n A_n') = \\ = (x_1^2 + x_2^2 + \cdots + x_n^2).$$

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

$$(7) \qquad B_1 = A_1 A_n', \; B_2 = A_2 A_n', \; \ldots \; B_{n-1} = A_{n-1} A_n'$$

ein und setzt dementsprechend

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

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

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

Entwickelt man hier die linke Seite, so ergiebt die Coefficientenvergleichung

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

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

$$(9) \qquad B_i^2 = -1, \qquad B_i B_k = -B_k B_i, \qquad B_i' = -B_i \quad (i \gtrless k)$$

Auf diese Weise ergeben sich also aus jeder Transformation A, welche der Bedingung (4) genügt, $n-1$ Transformationen $B_1, B_2, \ldots B_{n-1}$, welche die Gleichungen (9) befriedigen. Wenn umgekehrt $B_1, B_2, \ldots B_{n-1}$ 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 $B_1, B_2, \ldots B_{n-1}$ zu bestimmen, welche den Gleichungen (9) genügen. Wir unterziehen jetzt diese Gleichungen einer näheren Discussion, welche zeigen wird, daß ausschließlich in den Fällen $n = 2, 4, 8$, Systeme von $n-1$ Transformationen $B_1, B_2, \ldots B_{n-1}$ existiren können, für welche die Gleichungen (9) erfüllt sind. Betrachten wir zunächst die Gleichungen $B'_\iota = -B_\iota$. Dieselben besagen, daß die Transformationen B_ι schiefsymmetrisch sind. Daher sind die Gleichungen (9) unverträglich, wenn n ungerade ist. Denn in diesem Falle würde die Determinante von B_ι verschwinden müssen, was der Gleichung $B_\iota^2 = -1$ widerspricht.

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

$$(10)\quad 1,\quad B_{i_1},\quad B_{i_1}B_{i_2},\quad B_{i_1}B_{i_2}B_{i_3}, \ldots\ldots,\quad B_1 B_2 \ldots B_{n-1},$$

wobei die Indices bezüglich alle, den Ungleichungen

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

genügenden Werthsysteme zu erhalten haben. In Betreff dieser Transformationen (10) lehrt die Gleichung

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

daß die Transformation

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

symmetrisch oder schiefsymmetrisch ist, je nachdem $r \equiv 0, 3$ oder $r \equiv 1, 2 \pmod 4$ ist. Diese Thatsache gestattet nun weiter, die Frage zu entscheiden, ob zwischen den Transformationen (10) eine lineare Abhängigkeit bestehen kann. Bezeichnen wir allgemein mit $R, R_1, R_2, \ldots$ lineare Combinationen der Transformationen (10) mit nicht sämmtlich verschwindenden Coefficienten, 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 verschwindenden Coefficienten behaftet ist, möge an der Relation „betheiligt“ heißen. Sind ferner $R_1 = 0$, $R_2 = 0$ zwei Relationen, so will ich dieselben „einander fremd“ nennen, wenn es keine Transformation giebt, die gleichzeitig an beiden Relationen betheiligt ist. Endlich heiße eine Relation $R = 0$ „reducibel“, 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 $R = 0$ „irreducibel“.

Offenbar genügt es, die irreducibeln Relationen zu betrachten. Eine solche Relation bleibt irreducibel, wenn man sie mit einer der Transformationen (10) multiplicirt, und durch eine derartige Multiplication kann man erreichen, daß die Transformation 1 mit einem nicht verschwindenden Coefficienten in die Relation eingeht.

Ferner leuchtet ein, daß die Transformationen, welche an einer irreducibeln Relation betheiligt sind, entweder sämmtlich symmetrisch oder sämmtlich schiefsymmetrisch sind. Sei nun

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

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

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

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 sämmtliche Coefficienten $c_{i_1 i_2 i_3} = 0$ 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 sämmtliche Coefficienten $c_{i_1 i_2 i_3 i_4} = 0$. Indem man so weiter schließt, erkennt man, daß die Relation (11) nur die Form

$$(11') \qquad 1 = c \cdot B_1 B_2 \ldots B_{n-1}$$

besitzen kann, wobei überdies noch $n \equiv 0 \pmod{4}$ sein muß, weil andernfalls $B_1 B_2 \ldots B_{n-1}$ eine schiefsymmetrische Transformation sein würde. Quadrirt man die beiden Seiten der Relation (11′), so erkennt man, daß $c = \pm 1$ sein muß. Außer der Relation (11′) können keine andern irreducibeln Relationen existiren, als die, welche aus (11′) durch Multiplication mit den Transformationen (10) hervorgehen.

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

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

$$(12) \qquad B_1 B_2 \ldots B_{n-1} = \pm 1$$

durch Multiplication mit den Transformationen (10) hervorgehen und keine andern irreducibeln 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 möglicher Weise 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 Variabeln eine lineare Abhängigkeit, und es ergiebt sich für $n = 6$ der Werth von $\frac{n(n-1)}{2}+1 = 16$.

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

$$A_0 = \begin{vmatrix} x_1, & -x_2 \\ x_2, & x_1 \end{vmatrix},$$

$$A_0 = \begin{vmatrix} x_1, & -x_2, & -x_3, & -x_4 \\ x_2, & x_1, & -x_4, & x_3 \\ x_3, & x_4, & x_1, & -x_2 \\ x_4, & -x_3, & x_2, & x_1 \end{vmatrix},$$

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

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 constanten Coefficienten 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 Product von zwei quadratischen Formen von je n Variabeln $x_1, \dots x_n$, $y_1, \dots y_n$ darzustellen als quadratische Form von n bilinearen Functionen $z_1, z_2, \dots z_n$ jener Variabeln, so ist doch eine Darstellung jenes Produktes als quadratische Form von einer genügend groß gewählten Anzahl bilinearer Functionen der Variabeln $x_1, \dots x_n$, $y_1, \dots y_n$ immer möglich. Es fragt sich nun, welches der kleinste zulässige Werth dieser Anzahl ist. Transformirt man die quadratischen Formen auf Summen von Quadraten, so gewinnt die Frage folgende Gestalt:

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

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

durch geeignet gewählte bilineare Functionen $z_1, z_2, \dots z_m$ der Variabeln $x_1, \dots x_n, y_1, \dots y_n$ befriedigt werden kann?

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

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

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

Andererseits kann man in vorstehender Gleichung auch n und m als gegeben annehmen und nach dem größten zulässigen Werthe 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 Coordinaten eines Punktes mit $a_{ik}\,(i, k = 1, 2, \dots n)$ bezeichnet werden mögen, das Gebilde, welches durch die Gleichungen

$$\sum_{i=1}^{n} a_{i1}^2 = \sum_{i=1}^{n} a_{i2}^2 = \dots = \sum_{i=1}^{n} a_{in}^2,$$

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

definirt ist, so bezeichnet der Maximalwerth von p nichts anderes, als die höchste Dimension linearer Räume, die auf diesem Gebilde liegen. Uebrigens ergiebt eine Analyse, welche der oben dargelegten ganz ähnlich ist, daß dieser Maximalwerth von p im Falle eines ungeraden n gleich 1 ist und im Falle eines geraden n durch die Ungleichungen $2^{p-1} \leqq n^2$, resp. $2^{p-2} \leqq n^2$ eingeschränkt ist, je nachdem $n \equiv 2$ oder $n \equiv 0$ (mod. 4) ist. Es kann also, wenn n eine gerade Zahl ist, der Maximalwerth von p nicht über $\frac{2 \lg n}{\lg 2} + 1$ bez. $\frac{2 \lg n}{\lg 2} + 2$ liegen.

Zürich, den 25. Juni 1898.