

Über das assoziative Gesetz bei der Komposition der quaternären quadratischen Formen.

Von

H. Brandt in Aachen.

1.

Wenn bei einem endlichen oder unendlichen System von Elementen A, B, C, \dots eine Verknüpfung (Komposition) existiert, welche jedem geordneten Paar von Elementen A, B eindeutig ein drittes Element $P = AB$ zuordnet, so sprechen wir von der Gültigkeit des *assoziativen Gesetzes*, wenn folgende Bedingung erfüllt ist: Sind A, B, C drei beliebige Elemente des Systems und entsteht durch Komposition von A mit B das Element $AB = P$ und durch Komposition von B mit C das Element $BC = Q$, so ergibt die Komposition von P mit C und A mit Q beidemale dasselbe Element, d. h. es ist $PC = AQ$ oder $(AB)C = A(BC)$. Hieraus folgt dann in bekannter Weise, daß Kompositionen aus beliebig vielen Elementen A, B, \dots, K allein durch die Reihenfolge schon eindeutig bestimmt sind, so daß keine Klammern gesetzt zu werden brauchen.

Ist das System so beschaffen, daß zwar bei jedem geordneten Paar von Elementen A, B eine Komposition möglich ist, das komponierte Element $AB = P$ aber in einzelnen Fällen oder auch immer mehrdeutig bestimmt ist, so wird man ebenfalls von der Gültigkeit des assoziativen Gesetzes sprechen können, wenn für jedes Tripel von Elementen A, B, C die Gesamtheit der Elemente $X = (AB)C$ mit der Gesamtheit der Elemente $Y = A(BC)$ identisch ist.

Wie steht es aber, wenn die Komposition nicht immer möglich ist, wenn vielmehr bei jedem vorgelegten Elementenpaar A, B zuerst entschieden werden muß, ob A mit B komponiert werden kann oder nicht? Hat es auch dann noch Sinn, von einem assoziativen Gesetz zu sprechen? Tatsächlich ist das möglich. Berücksichtigt man nämlich bei jedem zu komponierenden Paar von Elementen auch die Möglichkeit der Nichtkomponier-

barkeit, so wird man zu folgenden Forderungen geführt, die in unserm Falle als Ausdruck des assoziativen Gesetzes zu gelten haben:

Aus der Existenz von AB und BC folgt die von $(AB)C$ und $A(BC)$. Aus der Existenz von AB und $(AB)C$ folgt die von BC und $A(BC)$. Aus der Existenz von BC und $A(BC)$ folgt die von AB und $(AB)C$. Dabei ist in allen drei Fällen $(AB)C = A(BC)$.

Auch wenn ein System diesen Forderungen genügt, kann man von Kompositionen aus beliebig vielen Elementen A, B, \dots, K sprechen. Eine solche Komposition ist, wenn sie existiert, allein durch die Reihenfolge der Elemente bestimmt, so daß keine Klammern gesetzt zu werden brauchen. Für die Existenz aber ist erforderlich und auch ausreichend, daß an jeder Trennungsstelle zweier aufeinander folgenden Elemente $\dots F, G \dots$ ein Aggregat unmittelbar vorhergehender Elemente mit einem Aggregat unmittelbar nachfolgender Elemente, z. B. das vorhergehende Element F mit dem nachfolgenden Element G komponiert werden kann.

Nur in dieser Weise kann bei der Komposition der quaternären quadratischen Formen oder Formenklassen eine Gültigkeit des assoziativen Gesetzes in Frage kommen. Daß dies Gesetz in diesem Sinne aber auch tatsächlich gilt, das nachzuweisen ist der Zweck der folgenden Zeilen¹⁾.

2.

Die Komposition der quaternären quadratischen Formen der gleichen Diskriminante führt auf Systeme von endlich vielen Formenklassen, A, B, C, \dots , die zwar alle durch die Komposition eng miteinander verknüpft sind, aber doch nicht beliebig untereinander komponiert werden können. Wir bestimmen ein solches System von Klassen in der folgenden Weise. Wir wählen eine der für die Komposition in Betracht kommenden Klassen primitiver Formen, also primitiver K -Formen²⁾ beliebig aus. Dann fügen wir zu dieser Klasse A alle primitiven Klassen B der gleichen Diskriminante hinzu, mit denen A rechts oder links komponiert werden kann, für die also die Kompositionen AB oder BA existieren. Jede der

¹⁾ Vgl. hierzu die früheren Arbeiten:

I. Über ein Problem von A. Hurwitz, quaternäre quadratische Formen betreffend. Math. Ann. 88 (1923), S. 211.

II. Der Kompositionsbegriff bei den quaternären quadratischen Formen. Math. Ann. 91 (1924), S. 300.

III. Die Hauptklassen in der Kompositionstheorie der quaternären quadratischen Formen. Math. Ann. 94 (1925), S. 166.

IV. Über die Komponierbarkeit quaternärer quadratischer Formen. Math. Ann. 94 (1925), S. 179.

²⁾ II, S. 302.

hinzugefügten Klassen B behandeln wir wieder ebenso wie die Ausgangsklasse A . In dieser Weise fahren wir fort und ergänzen das System für jede bereits aufgeführte Klasse durch alle damit rechts oder links komponierbaren Klassen, soweit diese Klassen nicht bereits aufgeführt sind. Das Verfahren muß einmal zu einem Abschluß kommen, da es nur endlich viele Klassen der gleichen Diskriminante gibt. Wir haben dann ein in sich abgeschlossenes und zugleich möglichst kleines System von Klassen erhalten, das mit jeder Klasse, die darin aufgeführt ist, auch alle Klassen umfaßt, mit denen diese Klasse rechts oder links komponiert werden kann. Offenbar ist dies System durch eine beliebige seiner Klassen schon vollständig bestimmt.

Dies System ist nun tatsächlich von der oben erörterten Art. Daß die Komposition der Klassen nicht immer eindeutig ist, könnte leicht durch Beispiele belegt werden³⁾. Daß in dem System aber im allgemeinen (sobald nämlich mehr als eine Hauptklasse darin vorkommt) nicht zwei beliebige Klassen komponiert werden können, wurde früher gezeigt. Für die Komponierbarkeit der Klasse A mit der Klasse B ist nämlich notwendig⁴⁾ und hinreichend⁵⁾, daß die rechts zugehörige Hauptklasse von A mit der links zugehörigen von B übereinstimmt.

Der Nachweis, daß in diesem System von Klassen das assoziative Gesetz in dem obigen Sinne gültig ist, wird nun in zwei Schritten erledigt. Zuerst wird gezeigt, daß die drei genannten Existenzforderungen erfüllt sind. Dann folgt der Nachweis, daß die Kompositionen $(AB)C$ und $A(BC)$, wo sie existieren, zu demselben Ergebnis führen.

3.

Der erste Teil des Beweises ergibt sich unter Benutzung früherer Ergebnisse sehr einfach. Zum Beweise bezeichnen wir durch A, B, C, \dots wie oben die Klassen unseres Systems, setzen aber nicht voraus, daß verschiedene Symbole auch verschiedene Klassen bezeichnen. Ist dann A mit B komponierbar und $AB = P$, so haben B und P dieselbe rechts zugehörige Hauptklasse⁴⁾. Je nachdem nun, ob diese Hauptklasse der Klasse C links zugehört oder nicht, sind die beiden Kompositionen BC und PC gleichzeitig möglich⁵⁾ oder gleichzeitig nicht möglich⁴⁾. Ist ebenso B mit C komponierbar und $BC = Q$, so haben B und Q dieselbe links zugehörige Hauptklasse⁴⁾. Je nachdem nun, ob diese Hauptklasse der Klasse A rechts zugehört oder nicht, sind die beiden Kompositionen AB und AQ gleich-

³⁾ II, S. 314.

⁴⁾ IV, S. 194.

⁵⁾ IV, S. 196.

zeitig möglich⁵⁾ oder gleichzeitig nicht möglich⁴⁾. Daraus ergeben sich aber die obigen drei Existenzforderungen.

Es ist also nur noch zu zeigen, daß überall da, wo die Kompositionen $(AB)C$ und $A(BC)$ einen Sinn haben, die Gleichheit $(AB)C = A(BC)$ stattfindet. Zu dem Zwecke wählen wir aus den Klassen A, B, C, \dots in beliebiger Weise je eine bestimmte die Klasse repräsentierende Form aus und bezeichnen diese Formen wie ihre Klassen ebenfalls der Einfachheit halber durch A, B, C, \dots .

Sind nun A, B, C, D, D', L, K solche nicht notwendig sämtlich verschiedene Formen, für welche aber die Kompositionen $AB = L$, $LC = D$ und $BC = K$, $AK = D'$ möglich sind, so gibt es bilineare Substitutionen M, N, M', N' mit den für die Komposition erforderlichen Eigenschaften⁶⁾, welche der Reihe nach diese Kompositionen vermitteln. Übt man nun in N auf die Variablen von L die bilineare Substitution M aus, so entsteht eine trilineare Substitution \mathfrak{N} , die nach einer früher benutzten Symbolik⁷⁾ durch

$$\mathfrak{N} = N \begin{array}{l} / \\ M \end{array}$$

zu bezeichnen ist und die Komposition $(AB)C = D$ vermittelt. Übt man ebenso in N' auf die Variablen von K die bilineare Substitution M' aus, so entsteht eine trilineare Substitution

$$\mathfrak{N}' = N' \begin{array}{l} \backslash \\ M' \end{array},$$

welche die Komposition $A(BC) = D'$ vermittelt.

Der hier erforderliche Nachweis, daß die Gesamtheit der Formen D mit der Gesamtheit der Formen D' identisch ist, wird nun sogleich erbracht sein, wenn wir, was im folgenden geschehen wird, sogar zeigen können:

Jede trilineare Substitution, welche bei Zusammenfassung zweier in der einen Weise nacheinander ausgeführter Kompositionen entsteht, kann gleichzeitig auch durch Zusammenfassung zweier in der andern Weise nacheinander ausgeführter Kompositionen hergeleitet werden. Symbolisch geschrieben heißt das: Die eine der beiden Formeln

$$\mathfrak{N} = N \begin{array}{l} / \\ M \end{array} \qquad \mathfrak{N} = N' \begin{array}{l} \backslash \\ M' \end{array}$$

⁶⁾ II, S. 304.

⁷⁾ III, S. 168.

zieht die andere nach sich. Die Kompositionen $(AB)C = D$ und $A(BC) = D$ bedingen sich also gegenseitig und können beide durch dieselbe trilineare Substitution vermittelt werden.

4.

Um nun diese Behauptungen zu beweisen, bezeichnen wir wie früher⁷⁾ durch V_0 die bilineare Substitution der Quaternionenmultiplikation $z_0 = x_0 y_0 - x_1 y_1 - x_2 y_2 - x_3 y_3$, $z_1 = x_0 y_1 + x_1 y_0 + x_2 y_3 - x_3 y_2$ usw. und durch $A, B, \Gamma, \Delta, \Lambda, K$ lineare Substitutionen, welche die Form E , d. h. eine Summe von vier Quadraten bzw. in A, B, C, D, L, K transformieren. Sind nun M, N bilineare Substitutionen, welche die Kompositionen $AB = L$, $LC = D$ vermitteln, so kann man nach früherem⁸⁾ $A, B, \Gamma, \Delta, \Lambda$ mit gleicher (positiver bzw. negativer) Determinante so bestimmen, daß die Formeln

$$M = \Lambda^{-1} \cdot V_0 \begin{matrix} \swarrow A \\ \searrow B \end{matrix}, \quad N = \Delta^{-1} \cdot V_0 \begin{matrix} \swarrow \Lambda \\ \searrow \Gamma \end{matrix}$$

erfüllt sind. Setzt man dann

$$M' = K^{-1} \cdot V_0 \begin{matrix} \swarrow B \\ \searrow \Gamma \end{matrix}, \quad N' = \Delta^{-1} \cdot V_0 \begin{matrix} \swarrow A \\ \searrow K \end{matrix},$$

wobei über die Substitution K noch Näheres festgesetzt werden soll, so ist wegen der aus der Assoziativität der Quaternionenmultiplikation fließenden Beziehung⁹⁾

$$V_0 \begin{matrix} \swarrow V_0 \\ \searrow V_0 \end{matrix} = V_0 \begin{matrix} \swarrow V_0 \\ \searrow V_0 \end{matrix},$$

wie man durch Einsetzen der vorigen Formeln findet, jedenfalls

$$N \begin{matrix} \swarrow M \\ \searrow M' \end{matrix} = N' \begin{matrix} \swarrow M \\ \searrow M' \end{matrix}.$$

Nun kann aber K so gewählt werden, daß N' und M' wirklich auch Kompositionen vermitteln. Die Möglichkeit der ganzzahligen Bestimmung von N' und M' folgt zunächst aus diesem allgemeinen Hilfssatz:

Wenn eine bilineare Schar ganzzahliger Matrizen als Produkt nicht singulärer linearer Scharen darstellbar ist, können diese auch ganzzahlig gewählt werden.

⁸⁾ I, S. 214.

(Wird nämlich die bilineare Schar durch $\sum_{ik} T^{(ik)} x_i y_k$ bezeichnet und ist diese in der Form $\sum_i T^{(i)} x_i \cdot \sum_k T'^{(k)} y_k$ darstellbar, wobei die Determinanten $|\sum_i T^{(i)} x_i|$, $|\sum_k T'^{(k)} y_k|$ nicht identisch verschwinden, so schließt man aus der Ganzzahligkeit der $T^{(ik)}$ leicht, daß sich eine nicht singuläre Matrix R so bestimmen läßt, daß die sämtlichen Matrizen $T^{(i)} R$ und $R^{-1} T'^{(k)}$ ganzzahlig ausfallen.)

Ist die Substitution K diesem Hilfssatz entsprechend bestimmt und hat man dabei noch das Vorzeichen der offenbar reellen Determinante von K ebenso gewählt wie das der Determinanten der Substitutionen A, B usw., so möge die Form, in welche E durch K transformiert wird, durch K bezeichnet werden. Dann werden durch die bilinearen Substitutionen M' und N' die Identitäten $BC = K$ und $AK = D$ vermittelt. Dabei handelt es sich aber um Kompositionen; denn M' und N' haben wegen des gleichen Vorzeichens der Determinanten von A, B, \dots, K positive Signatur und Art, und A, B, C, D, K sind primitive Formen der gleichen Diskriminante. Das ist nur noch von K zu zeigen. K ist zunächst ganzzahlig, da N' es ist. K hat aber auch dieselbe Diskriminante wie die übrigen Formen, weil wegen der Identität $BC = K$ die Diskriminante höchstens so groß sein kann und wegen der Identität $AK = D$ mindestens so groß sein muß wie die der übrigen Formen, endlich ist K primitiv, weil K durch M' in das Produkt der primitiven Formen B, C transformiert wird.

Damit ist aus der Komposition $(AB)C = D$ die andere $A(BC) = D$ hergeleitet. Da man in ganz entsprechender Weise auch aus der zweiten Komposition die erste findet, ist damit die Gültigkeit des assoziativen Gesetzes nachgewiesen.

5.

Dies Gesetz gestattet, die Definition des Kompositionsbegriffes, die ursprünglich nur für zwei Formen gegeben wurde⁶⁾, auf drei und mehr Formen auszudehnen.

Die trilinearen Substitutionen, die bei Kompositionen von der Gestalt $(AB)C$ oder $A(BC)$ auftreten, unterscheiden sich nach dem vorigen nicht. Sie können durch gleichzeitige lineare Transformation ihrer vier Variablenreihen durch Substitutionen mit gleichen Determinanten in diejenige trilineare Substitution übergeführt werden, welche bei der Multiplikation dreier Quaternionen die Komponenten des Produktes durch die Komponenten der Faktoren ausdrückt. Umgekehrt läßt aber der vorige Beweis erkennen, daß jede ganzzahlige trilineare Substitution, welche bei

vier primitiven Formen gleicher Diskriminante A, B, C, D eine Identität $ABC = D$ vermittelt, sobald ihr nur jene Eigenschaft zukommt, so in doppelter Weise in bilineare Substitutionen gespalten werden kann, daß die Kompositionen $(AB)C = D$ und $A(BC) = D$ hervorgehen. Wir werden daher kurz sagen, eine solche trilineare Substitution vermittelt die Komposition $ABC = D$.

Es ist leicht, diese Betrachtungen auf beliebig viele Formen auszuweiten. Trennt man dabei noch den Fall der positiv-definiten K -Formen von dem Fall der indefiniten K -Formen, so wird man zu der folgenden allgemeinen Definitionen des Kompositionsbegriffes geführt.

Wenn durch eine ganzzahlige n -fach lineare Substitution

$$x_v = \sum_{i_1 i_2 \dots i_n} m_{v i_1 i_2 \dots i_n} x_{i_1}^{(1)} x_{i_2}^{(2)} \dots x_{i_n}^{(n)}$$

eine Form $A((x))$ in das Produkt der Formen $A_1((x)), A_2((x)), \dots, A_n((x))$ transformiert wird, wobei A, A_1, A_2, \dots, A_n primitive Formen der gleichen Diskriminante bedeuten, so liegt eine Komposition vor, wenn die n -fach lineare Substitution so beschaffen ist, daß sie sich durch reelle lineare Transformation ihrer $n + 1$ Variablenreihen durch Substitutionen mit gleichen positiven Determinanten auf die Form

$$X = X^{(1)} X^{(2)} \dots X^{(n)}$$

bringen läßt, wobei X im Fall positiv-definiten Formen die Matrix

$$X = \begin{vmatrix} x_0 + i x_1 & x_2 + i x_3 \\ -x_2 + i x_3 & x_0 - i x_1 \end{vmatrix}$$

und im Fall indefiniten Formen die Matrix

$$X = \begin{vmatrix} x_0 & x_2 \\ x_1 & x_3 \end{vmatrix}$$

bedeutet, während die übrigen Matrizen $X^{(1)}, X^{(2)}, \dots, X^{(n)}$ entsprechende Bedeutung haben.

(Eingegangen am 7. 11. 1925.)