**Zeitschrift:** Commentarii Mathematici Helvetici

**Herausgeber:** Schweizerische Mathematische Gesellschaft

**Band:** 33 (1959)

**Artikel:** Der Zusammenhang zwischen quaternären quadratischen Formen und Idealen in Quaternionenringen.

**Autor:** Aeberli, G.

**DOI:** https://doi.org/10.5169/seals-26019

# Der Zusammenhang zwischen quarternären quadratischen Formen und Idealen in Quarternionenringen

von G. Aeberli (Zürich)

## Übersicht

Im 1. Paragraphen fasse ich die Resultate über die Zuordnung der Idealklassen eines quadratischen Körpers zu ihren Normenformklassen zusammen. In den Paragraphen 2 bis 8 folgt ein Überblick über die Brandtsche Kompositionstheorie quaternärer quadratischer Formen, die als wichtigstes Beweismittel verwendet werden wird. Ab Paragraph 9 befassen wir uns mit dem Hauptsatz über die Zuordnung der Idealklassen eines Quaternionenringes zu deren Normenformklassen, dessen Beweis in dieser Arbeit gegeben wird.

Die Abhandlung ist eine Überarbeitung der preisgekrönten Lösung der Preisaufgabe «Men weet dat er een correspondentie bestaat tussen klassen van binaire kwadratische vormen en idealklassen in kwadratische getallenlichamen. Gevraagd wordt een dergelijke relatie tussen kwaternaire kwadratische vormen en idealen in kwaternionenringen te ontwikkelen» die die niederländische mathematische Gesellschaft «Een onvermoeide arbeid komt alles te boven» für das Jahr 1957 gestellt hatte.

## 1. Die Zuordnung der Idealklassen in quadratischen Körpern zu den zugehörigen Normenformklassen

Im quadratischen Körper $k$ der Diskriminante $d$ betrachten wir ein Ideal $\mathfrak{a}$ in Basisdarstellung, $\mathfrak{a} = (\alpha_1, \alpha_2)$. Jedes Element $\alpha$ aus $\mathfrak{a}$ ist in der Form $\alpha = x_1\alpha_1 + x_2\alpha_2$ mit ganzrationalen $x_\nu$ darstellbar. Die Norm von $\alpha$, in Zeichen $n(\alpha)$, schreibt sich dann

$$n(\alpha) = n(\mathfrak{a})F_{\mathfrak{a}}^{(\alpha)}((x)), \qquad n(\mathfrak{a}) > 0$$

wo $F_{\mathfrak{a}}^{(\alpha)}((x))$ eine ganzzahlige, primitive, binäre quadratische Form der Diskriminante $d$ ist, ([9], S. 213) und wo $n(\mathfrak{a})$ die Norm von $\mathfrak{a}$ bedeutet. Aus dem Einheitsideal $\mathfrak{o} = (1)$ des Körpers $k$ wählen wir eine feste Basis $(\omega_1, \omega_2)$. Die Reihenfolge der Basiselemente in $(\alpha_1, \alpha_2)$ setzen wir dann so fest, daß die Determinante $|a_{ik}|$ ihrer Basismatrix $(a_{ik})$, definiert durch

$$\alpha_i = \sum_{k=1}^{2} a_{ik}\omega_k$$

positiv wird. Bezeichnen wir die im Ausdruck für $n(\alpha)$ vorkommende Form $F_{\mathfrak{a}}^{(\alpha)}$ mit Normenform, so sehen wir, daß zu jeder Basisdarstellung $(\alpha_1, \alpha_2)$ von $\mathfrak{a}$ eine bestimmte Normenform gehört. Indessen ist die Klasse aller dieser Normenformen dieselbe; sie heißt die Normenformklasse des Ideals $\mathfrak{a}$ (vgl. Nr. 12). Wir nennen zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ klassengleich, wenn eine Beziehung $\mathfrak{b} = \eta\mathfrak{a}$ mit $\eta \in k$, $n(\eta) > 0$ besteht. Man sieht dann, daß die Normenformklasse eines jeden Ideals der selben Klasse die gleiche ist (vgl. dazu die formal fast gleichen Entwicklungen im Falle der Quaternionenringe, Nr. 20 und 21).

Die Idealklassen des Körpers $k$ bilden eine endliche Gruppe. Es seien $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ solche Idealklassen, und $\mathfrak{a} = (\alpha_1, \alpha_2)$, $\mathfrak{b} = (\beta_1, \beta_2)$, $\mathfrak{c} = (\gamma_1, \gamma_2)$ Ideale, die sie repräsentieren. Gilt dann $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$, so hat man für jedes $\alpha = \sum\limits_{i=1}^{2} x_i\alpha_i$, $\beta = \sum\limits_{j=1}^{2} y_j\beta_j$, eine Gleichung $\alpha\beta = \gamma$, oder $\sum\limits_{i=1}^{2} x_i\alpha_i \sum\limits_{j=1}^{2} y_j\beta_j = \sum\limits_{k=1}^{2} z_k\gamma_k$, wo $z_k$ geeignete, eindeutig bestimmte, ganze Zahlen sind. Hieraus folgt für die Normenformen die Beziehung

$$n(\mathfrak{a})F_{\mathfrak{a}}^{(\alpha)}((x))n(\mathfrak{b})F_{\mathfrak{b}}^{(\beta)}((y)) = n(\mathfrak{c})F_{\mathfrak{c}}^{(\gamma)}((z));$$

wegen $n(\mathfrak{a})n(\mathfrak{b}) = n(\mathfrak{c})$ folgert man $F_{\mathfrak{a}}^{(\alpha)}((x))F_{\mathfrak{b}}^{(\beta)}((y)) = F_{\mathfrak{c}}^{(\gamma)}((z))$. Einer Multiplikation $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$ der Ideale entspricht somit die Komposition $F_{\mathfrak{a}}^{(\alpha)}((x))F_{\mathfrak{b}}^{(\beta)}((y)) = F_{\mathfrak{c}}^{(\gamma)}((z))$ der Normenformen. Ebenso gehört zur Multiplikation $\mathfrak{A}\mathfrak{B} = \mathfrak{C}$ der Idealklassen die Komposition der zugehörigen Normenformklassen $F_{\mathfrak{A}}F_{\mathfrak{B}} = F_{\mathfrak{C}}$, wenn $F_{\mathfrak{A}}$ die Normenformklasse von $\mathfrak{A}$ bedeutet, usw. (vgl. Nr. 22). Die primitiven, binären, quadratischen Formenklassen der Diskriminante $d$ bilden bei der Komposition eine abelsche Gruppe. Die Einheit dieser Gruppe ist die Hauptklasse, das heißt die Klasse, deren Formen 1 ganzzahlig darstellen (siehe [8], Seite 129–143, Kompositionstheorie der binären quadratischen Formen). *Jede* Formenklasse der Diskriminante $d$ ist Normenformklasse einer Idealklasse. Man nehme nämlich irgendeine Form der vorgegebenen Formenklasse, dann ist es möglich, aus den Koeffizienten der Form eine Basis eines Ideals anzugeben, für das diese Form Normenform ist ([9], Seite 214). Die Abbildung $\mathfrak{A} \to F_{\mathfrak{A}}$ ist eine homomorphe Abbildung der Idealklassengruppe *auf* die Gruppe der Normenformklassen, welche auch *alle* primitiven Formenklassen der Diskriminante $d$ enthält. Dieser Homomorphismus ist aber sogar ein Isomorphismus, weil dem Einselement der Formenklassengruppe genau die Eins der Idealklassengruppe entspricht. Diese Behauptung ist richtig, weil jedes Ideal, dessen Normenformklasse die Hauptklasse ist, selbst ein Hauptideal ist, das heißt der Hauptklasse (=Einselement der Idealklassengruppe) angehört.

Sei etwa $\mathfrak{d} = (\delta_1, \delta_2)$ ein solches Ideal, $n\sum\limits_{i=1}^{2} x_i\delta_i = n(\mathfrak{d})F_{\mathfrak{d}}^{(\delta)}((x))$, wo also

$F_{\mathfrak{d}}^{(\delta)}$ Hauptform ist. Dann existieren ganze rationale Zahlen $\xi_1$, $\xi_2$, so daß $F_{\mathfrak{d}}^{(\delta)}((\xi)) = 1$ gilt; betrachten wir dann das Element $\lambda$, definiert durch $\lambda = \sum_{i=1}^{2} \xi_i \delta_i$, dann ist $n(\lambda) = n(\mathfrak{d})$. $\mathfrak{d}$ muß gleich dem Hauptideal $(\lambda)$ sein. Wegen $\lambda \in \mathfrak{d}$ ist sicher $(\lambda) \subseteqq \mathfrak{d}$. Ist $(\lambda) = \mathfrak{d}$, so sind wir fertig. Ist $(\lambda) \subset \mathfrak{d}$, so gibt es ein *ganzes* Ideal $\mathfrak{l}$ mit $(\lambda) = \mathfrak{l}\mathfrak{d}$ (siehe [9], Seite 115), für die Normen folgt $n(\lambda) = n(\mathfrak{l})n(\mathfrak{d})$, was wegen $n(\lambda) = n(\mathfrak{d})$ die Beziehung $n(\mathfrak{l}) = 1$ ergibt. Da das Einheitsideal das einzige ganze Ideal der Norm 1 ist, so ist $\mathfrak{l} = (1)$, somit $(\lambda) = \mathfrak{d}$, was im Widerspruch zur gemachten Annahme $(\lambda) \subset \mathfrak{d}$ steht. Es ist somit $(\lambda) = \mathfrak{d}$; $\mathfrak{d}$ ist tatsächlich ein Hauptideal, wie behauptet.

Wir fassen das Ergebnis zusammen in dem

**Satz:** *Die Gruppe der Idealklassen des quadratischen Körpers k der Diskriminante d ist isomorph der Gruppe der Normenformklassen, welche alle primitiven Formenklassen der Diskriminante d umfaßt.*

## 2. Zur Transformation einer quadratischen Form in das Produkt zweier anderer

Wir betrachten irgendeine quadratische Form in $n$ Variablen mit komplexen Koeffizienten $c_{ik}$

$$C((z)) = \sum_{i,k=1}^{n} c_{ik} z_i z_k, \qquad c_{ik} = c_{ki}.$$

Bei Ausübung einer bilinearen Substitution

$$z_\nu = \sum_{r,s=1}^{n} m_{\nu rs} x_r y_s$$

geht $C((z))$ über in eine homogene Form 4. Grades in den $x_r$, $y_s$. Tritt dann der Fall ein, daß diese Form sich als Produkt zweier quadratischer Formen in $n$ Variablen schreiben läßt,

$$\sum_{i,k=1}^{n} c_{ik} z_i z_k = \sum_{i,k=1}^{n} a_{ik} x_i x_k \sum_{i,k=1}^{n} b_{ik} y_i y_k \quad \text{oder} \quad C((z)) = A((x)) B((y)),$$

so sagt man, daß $C$ in das Produkt $AB$ transformiert worden sei.

Im Jahre 1898 hat HURWITZ gefunden, daß solche Transformationen nur in den Fällen von 2, 4 und 8 Variablen möglich seien (siehe Göttinger Nachrichten 1898, Komposition quadratischer Formen in beliebig vielen Variablen). Den binären Fall hat GAUSS zuerst untersucht und dabei seine Kompositionstheorie dieser Formen entwickelt (Disquisitiones arithmeticae Art. 235).

Mit den Untersuchungen über die *quaternären* Formen hat HEINRICH BRANDT (1888–1954) im Jahre 1913 in seiner Dissertation begonnen ([7], Seite

106–127). Ebenso wie man das bei der Kompositionstheorie der binären, quadratischen Formen tut, beschränkt sich BRANDT auf die Betrachtung von Formen, die sämtlich dieselbe Diskriminante haben. Unter *Diskriminante* der Form $C((z))$ verstehen wir die Determinante $\left|\frac{\partial^2 C((z))}{\partial z_i \partial z_k}\right|$. Oft verwendet man auch den Begriff der *Determinante* einer Form $C((z))$, worunter man die Determinante $|c_{ik}|$ zu verstehen hat. Die Diskriminante einer quaternären ist offenbar das 16-fache der Determinante.

Für *reelle* Formen findet BRANDT: Alle und nur die Formen mit *positiver* Determinante lassen sich durch eine reelle Bilinearsubstitution in das Produkt zweier anderer transformieren.

Für die Möglichkeit einer Transformation bei rationalen Formen ist notwendig und hinreichend, daß ihre Determinante ein *rationales Quadrat* sei. Um die Bedingungen auch für *ganzzahlige* quaternäre Formen anzugeben, definieren wir: Unter der *reziproken Form* der Form $C((z))$ verstehen wir die Form

$\mathfrak{C}((z)) = \sum_{i,k=0}^{3} \mathfrak{c}_{ik} z_i z_k$, wo $\mathfrak{c}_{ik} = \frac{1}{\sqrt{D}} \frac{\partial |c_{ik}|}{\partial c_{ik}}$, $D =$ Determinante von $C((z))$;

der Größe $\sqrt{D}$ ist ein bestimmtes, festes Vorzeichen zu geben. Mit Hilfe gewisser Determinanteneigenschaften stellt man fest, daß auch umgekehrt $C((z))$ die Reziproke von $\mathfrak{C}((z))$ ist. Dann gilt: Eine primitive, ganzzahlige Form läßt sich genau dann in das Produkt zweier ebensolcher Formen mit einer ganzzahligen Bilinearsubstitution transformieren, wenn ihre Determinante $D$ eine Quadratzahl ist: $D = d^2$, und wenn ihre Reziproke auch ganzzahlig ist ([7], Seite 122).

### 3. Auszeichnung gewisser Bilinearsubstitutionen

Fortan wollen wir uns auf ganzzahlige Formen beschränken. Ausnahmen von dieser Annahme werden stets besonders vermerkt.

Während BRANDT 1913 seine Ergebnisse nur für ganzzahlige primitive Formen 1. Art formuliert hat, das heißt für solche $A((x)) = \sum_{i,k=0}^{3} a_{ik} x_i x_k$ wo alle $a_{ik}$ ganze Zahlen sind, hat er seine Resultate später auch auf solche ganzzahlige primitive Formen ausgedehnt, in denen wenigstens ein $a_{ik}$, $i \neq k$, die Hälfte einer ungeraden Zahl ist. $A((x))$ schreibt sich dann in der Form $A((x)) = \frac{1}{2} \sum_{i,k=0}^{3} (2a_{ik}) x_i x_k$, wo dann im Sinne von BRANDT $\frac{1}{2} \sum_{i,k=0}^{3} (2a_{ik}) x_i x_k$ eine primitive Form 2. Art ist.

Als fruchtbar hat sich BRANDTS Gedanke erwiesen, den Bilinearsubstitutionen, die eine Transformation vermitteln, die beiden folgenden Bedingungen aufzuerlegen:

1. Die Bilinearsubstitution sei von *positiver Signatur.*
2. Die Bilinearsubstitution sei von *positiver Art* (siehe unten).

Bilinearsubstitutionen, die diesen beiden Bedingungen genügen, vermitteln eine Transformation, die *BRANDT Komposition* nennt, die Theorie heißt dann *Kompositionstheorie* der quaternären quadratischen Formen.

## 4. Die Signatur einer bilinearen Substitution

Es sei $A((x))B((y))=C((z))$ mittels der Bilinearsubstitution $z_\nu=\sum_{i,k=0}^{3} m_{\nu ik}x_i y_k$. Denkt man sich den $x_i$ feste Werte zugeschrieben, so erhalten wir in den $y_k$ die lineare Substitution $z_\nu=\sum_{i,k=0}^{3}(m_{\nu ik}x_i)y_k$. Sie transformiert $C((z))$ in das Produkt $A((x))B((y))$, wo $A((x))$ jetzt einen festen Wert besitzt. Für die Determinanten ergibt sich dann die Beziehung $|c_{ik}||\sum_{i=0}^{3} m_{\nu ik}x_i|^2=|b_{ik}|A^4((x))$. Da für die Determinanten gleiche Werte vorausgesetzt wurden, ist $|c_{ik}|=|b_{ik}|$, also $|\sum_{i=0}^{3} m_{\nu ik}x_i|=\pm A^2((x))$. Ähnlich ist $|\sum_{k=0}^{3} m_{\nu ik}y_k|=\pm B^2((y))$. Hingegen wird $|\sum_{\nu=0}^{3} m_{\nu ik}z_\nu|=\pm \mathfrak{C}^2((z))$ ([7], Seite 110 unten).

Die Determinanten dieser Linearformensysteme, wie sie heißen, sind somit bis auf das Vorzeichen die Quadrate der quadratischen Formen $A$, $B$ bzw. $\mathfrak{C}$. Diese Vorzeichen sind nicht ganz beliebig. Setzen wir mit den positiven oder negativen Einheiten $\varepsilon_\nu$

$$|\sum_{\nu=0}^{3} m_{\nu ik}z_\nu|=\varepsilon_1\mathfrak{C}^2((z)),\ |\sum_{i=0}^{3} m_{\nu ik}x_i|=\varepsilon_2 A^2((x)),\ |\sum_{k=0}^{3} m_{\nu ik}y_k|=\varepsilon_3 B^2((y))$$

so ergibt sich

$$\varepsilon_1\varepsilon_2\varepsilon_3=-1 \qquad ([7], \text{Seite } 117)\,.$$

Es gibt somit nur die vier Fälle für die Reihenfolge von $\varepsilon_1$, $\varepsilon_2$, $\varepsilon_3$:

$$-\underbrace{++},\quad +\underbrace{+-},\quad +\underbrace{-+},\quad -\underbrace{--}\,.$$

Von jedem dieser Tripel nimmt man zur Kennzeichnung die beiden letzten Zeichen. Der Reihe nach hat dann die bilineare Substitution positive, positiv-negative, negativ-positive, negative Signatur.

Für die Kompositionstheorie haben wir positive Signatur, somit ist stets

$$|\sum_{\nu=0}^{3} m_{\nu ik}z_\nu|=-\mathfrak{C}^2((z)),\ |\sum_{i=0}^{3} m_{\nu ik}x_i|=+A^2((x)),\ |\sum_{k=0}^{3} m_{\nu ik}y_k|=+B^2((y))$$

für die Komposition $A((x))B((y))=C((z))$ mittels $z_\nu=\sum_{i,k=0}^{3} m_{\nu ik}x_i y_k$.

## 5. Weshalb positive Signatur?

Sei insbesondere $A((x))$ eine Hauptform, die also $+1$ darstellt, und denken wir uns, daß etwa $A((\xi)) = +1$ sei. Dann gilt für Komposition $|\sum_{i=0}^{3} m_{\nu i k}\xi_i| = +1$, was besagt, daß $\sum_{i=0}^{3}(m_{\nu i k}\xi_i)$ die Matrix einer unimodularen linearen Substitution ist. Daher gehören $B((y))$ und $C((z))$ derselben Klasse an. Wird also eine Form $G$ mit einer Hauptform $H$ zu der Form $K$ komponiert, $GH = K$, so gehören $G$ und $K$ zur selben Klasse.

## 6. Die Art einer Bilinearsubstitution

Im Jahre 1923 hat Brandt entdeckt, daß einer bilinearen Substitution außer den schon genannten $\varepsilon_1, \varepsilon_2, \varepsilon_3$ noch ein anderes, charakterisierendes Vorzeichen $\varepsilon$ zukommt ([4], Seite 211). Die Bilinearsubstitutionen zerfallen, bei gleicher Signatur, noch in zwei Kategorien, wir nennen sie *Arten*. Diese Einteilung beruht, kurz beschrieben, auf dem Folgenden: Ist eine Bilinearsubstitution $M$ gefunden, die die Transformation $A((x))B((y)) = C(z)$ bewirkt, dann existieren gleichzeitig noch zwei andere bilineare Substitutionen $S'$ und $R''$, welche die Transformationen $A = BC$ und $B = CA$ erzeugen. Zwischen den Linearformenmatrizen der Bilinearsubstitution $M$, das sind $\|\sum_{i=0}^{3} m_{\nu i k}x_i\|$, $\|\sum_{k=0}^{3} m_{\nu i k}y_k\|$, $\|\sum_{\nu=0}^{3} m_{\nu i k}z_\nu\|$, und den Linearformenmatrizen der Bilinearsubstitutionen $R''$ und $S'$ bestehen gewisse Beziehungen ([6] Seite 225, V). Brandt ([5], Seite 154) nennt diese Matrizen

$$\sum_{j=0}^{3} m_{jik}z_j = \pi(z), \quad \sum_{j=0}^{3} m_{kji}x_j = \mathfrak{p}(x), \quad \sum_{j=0}^{3} m_{ikj}y_j = p(y)\,.$$

Es gilt weiter

$$\begin{aligned} A((x)) &= B((y))C((z)) && \text{mittels der Bilinearsubstitution } S' \\ x_i &= \sum_{j,k=0}^{3} s_{kij}y_j z_k && \text{und} \\ B((y)) &= C((z))A((x)) && \text{mittels der Bilinearsubstitution } R'' \\ y_i &= \sum_{j,k=0}^{3} r_{jki}z_i x_k\,, && \text{sowie} \\ C((z)) &= \mathfrak{A}((x))\mathfrak{B}((y)) && \text{mittels einer Bilinearsubstitution } Q \\ z_i &= \sum_{j,k=0}^{3} q_{ijk}x_j y_k && \text{([5], Seite 155–157).} \end{aligned}$$

Mit Brandt schreiben wir die Matrizen

$$\sum_{j=0}^{3} q_{jik}z_j = \varkappa(z)\,, \quad \sum_{j=0}^{3} q_{kji}x_j = \mathfrak{q}(x)\,, \quad \sum_{j=0}^{3} q_{ikj}y_j = q(y)$$

$$\sum_{j=0}^{3} s_{jik} z_j = \sigma(z)\,, \quad \sum_{j=0}^{3} s_{kji} x_j = \mathfrak{s}(x)\,, \quad \sum_{j=0}^{3} s_{ikj} y_j = s(y)$$

$$\sum_{j=0}^{3} r_{jik} z_j = \varrho(z)\,, \quad \sum_{j=0}^{3} r_{kji} x_j = \mathfrak{r}(x)\,, \quad \sum_{j=0}^{3} r_{ikj} y_j = r(y)$$

und

$$\Xi = \sum_{i=0}^{3} x_i \xi_i\,, \quad H = \sum_{i=0}^{3} y_i \eta_i\,; \quad Z = \sum_{i=0}^{3} z_i \zeta_i\,.$$

Bezeichnet $t$ eine vierzeilige quadratische alternierende Matrix $(t_{ik})$ mit der Transponierten $\dot{t}$, so daß $t + \dot{t} = 0$, so heißt nach Brandt das Aggregat

$$t_{01} t_{23} + t_{02} t_{31} + t_{03} t_{12} = \{t\}$$

die *Halbdeterminante* der alternierenden Matrix $t$.

Es ist, wie leicht zu prüfen, $|t| = \{t\}^2$. Bedeuten schließlich noch $a$, $b$, $c$ die Matrizen der Formen $A$, $B$, $C$ und $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ die Matrizen der Formen $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, so haben wir für die alternierenden Matrizen $\varrho(z)\dot{\pi}(\zeta) - Za$ usw. ([6], Seite 225) folgendes Gleichungssystem:

$$\begin{aligned}
\{\varrho(z)\dot{\pi}(\zeta) - Za\} &= \{\sigma(z)\dot{\varkappa}(\zeta) - Z\mathfrak{a}\} &&= \varepsilon\varepsilon_1 [C((z))\mathfrak{C}((\zeta)) - dZ^2] \\
\{\mathfrak{p}(x)\dot{\mathfrak{s}}(\xi) - \Xi b\} &= \{\mathfrak{r}(x)\dot{\mathfrak{q}}(\xi) - \Xi\mathfrak{b}\} &&= \varepsilon\varepsilon_2 [A((x))\mathfrak{A}((\xi)) - d\Xi^2] \\
\{s(y)\dot{\mathfrak{r}}(\eta) - Hc\} &= \{p(y)\dot{q}(\eta) - H\mathfrak{c}\} &&= \varepsilon\varepsilon_3 [B((y))\mathfrak{B}((\eta)) - dH^2] \\
\{\dot{\sigma}(z)\pi(\zeta) - Zb\} &= \{\dot{\varrho}(z)\varkappa(\zeta) - Z\mathfrak{b}\} &&= -\varepsilon\varepsilon_2 [C((z))\mathfrak{C}((\zeta)) - dZ^2] \\
\{\dot{\mathfrak{r}}(x)\mathfrak{s}(\xi) - \Xi c\} &= \dot{\mathfrak{p}}\{(x)\mathfrak{q}(\xi) - \Xi\mathfrak{c}\} &&= -\varepsilon\varepsilon_3 [A((x))\mathfrak{A}((\xi)) - d\Xi^2] \\
\{\dot{p}(y)r(\eta) - Ha\} &= \{\dot{s}(z)q(\zeta) - H\mathfrak{a}\} &&= -\varepsilon\varepsilon_1 [B((y))\mathfrak{B}((\eta)) - dH^2]
\end{aligned}$$

([6], Gleichungen VII, Seite 226), wo $d$ die gemeinsame Determinante der vorkommenden quadratischen Formen ist und zwischen den geschweiften Klammern die Halbdeterminanten stehen. Dieses Gleichungssystem ergibt sich aus demjenigen von [6], Seite 226 durch zyklische Vertauschung, da wir die Komposition $C = AB$ annehmen, während Brandt dort $A = BC$ zugrundegelegt hat.

**Satz.** ([6], Seite 226.) *Übt man auf die Variabeln einer Bilinearsubstitution die linearen reellen Substitutionen $t$, $u$, $v$ mit gleichen Determinantenquadraten aus, ist also*

$$|t| = \iota_1 \delta\,, \quad |u| = \iota_2 \delta\,, \quad |v| = \iota_3 \delta\,, \quad (\delta < 0)$$

*wo $\iota_1$, $\iota_2$, $\iota_3$ positive oder negative Einheiten sind, dann gilt für die neuen Größen* $\bar{\varepsilon}_1$, $\bar{\varepsilon}_2$, $\bar{\varepsilon}_3$, $\bar{\varepsilon}$ (für Formen mit *beliebig komplexen* Koeffizienten) $\bar{\varepsilon}_1 = \varepsilon_1 \iota_2 \iota_3$, $\bar{\varepsilon}_2 = \varepsilon_2 \iota_3 \iota_1$, $\bar{\varepsilon}_3 = \varepsilon_3 \iota_1 \iota_2$, $\bar{\varepsilon} = \varepsilon \iota_1 \iota_2 \iota_3$.

### 7. Die Komposition der Formenklassen

Der Kompositionsbegriff kann sofort auf die Formenklassen ausgedehnt werden. Vermittelt nämlich $M$, das ist $z_\nu = \sum_{i,k=0}^{3} m_{\nu ik} x_i y_k$, die Komposition

$A((x))B((y)) = C((z))$, geht weiter $A((x))$ über in $A'((\xi))$ durch die lineare Transformation $x_i = \sum_{\lambda=0}^{3} u_{i\lambda}\xi_\lambda$, $B((y))$ in $B'((\eta))$ durch $y_k = \sum_{\mu=0}^{3} v_{k\mu}\eta_\mu$, $C((z))$ in $C'((\zeta))$ durch $z_\nu = \sum_{\varrho=0}^{3} w_{\nu\varrho}\zeta_\varrho$, $U$, $V$, $W$ als ganzzahlige unimodulare Substitutionen angenommen, dann wird die Transformation $A'((\xi))B'((\eta)) = C'((\zeta))$ durch die bilineare Substitution $M' = W^{-1} - M\genfrac{}{}{0pt}{}{U}{V}$ vermittelt, da ja $\zeta_\varrho = \sum_{\nu=0}^{3} w_{\varrho\nu}^{-1} z_\nu = \sum_{\nu,i,k,\lambda,\mu=0}^{3} w_{\varrho\nu}^{-1} m_{\nu ik} u_{i\lambda} v_{k\mu} \xi_\lambda \eta_\mu$ ist.

Hier läßt sich der Satz des vorhergehenden Paragraphen anwenden, indem wir $\delta = 1$, $\iota_1 = \iota_2 = \iota_3 = 1$ setzen. Es wird $\bar{\varepsilon}_1 = \varepsilon_1$, $\bar{\varepsilon}_2 = \varepsilon_2$, $\bar{\varepsilon}_3 = \varepsilon_3$, $\bar{\varepsilon} = \varepsilon$. Bei unimodular ganzzahligen Transformationen der Variabeln ändern sich somit weder Art noch Signatur einer Bilinearsubstitution, so daß mit $M$ auch $M'$ positive Art und Signatur besitzt. Es hat somit einen Sinn, von der Komposition der Formenklassen zu sprechen.

## 8. Zwei Theoreme der Kompositionstheorie

**1. Satz.** *Jede komponierbare Formenklasse $A$ besitzt eine eindeutig bestimmte Linkshauptklasse $H$ und Rechtshauptklasse $H'$ mit $HA = A$ und $AH' = A$* ([1], Seite 313).

**2. Satz.** *Die Formenklassen $F$ und $G$ sind in dieser Reihenfolge genau dann komponierbar, wenn die Rechtshauptklasse von $F$ gleich der Linkshauptklasse von $G$ ist* ([2], Seiten 194–196).

Der zweite Satz zeigt, daß die Komposition keineswegs immer zwei quaternären Formenklassen $A$ und $B$ in dieser Reihenfolge genommen eine Produktklasse zuordnet. Der erste Satz besagt, daß jede Klasse eine Links- und eine Rechtseinheit besitzt, die im allgemeinen voneinander verschieden sind. Der Bereich der quaternären Formenklassen ist also im allgemeinen gegenüber der Komposition *keine Gruppe*, im Unterschied zu den binären primitiven Formenklassen.

## 9. Idealklassen und Normenformklassen in Quaternionenringen

Ebenso wie in den quadratischen Körpern (siehe Paragraph 2) läßt sich auch in den Quaternionenringen (Definition siehe Paragraph 10) eine Idealtheorie aufbauen. Auch hier entspricht jeder Idealklasse die zugehörige Normenformklasse; der Multiplikation der Idealklassen geht die Komposition der Normenformklassen parallel. Die Idealklassen und ebenso die Normenformklassen bilden gegenüber der Multiplikation bzw. der Komposition ein sogenanntes *Grup-*

*poid*, welches insofern eine Verallgemeinerung des Gruppenbegriffs ist, als jedes Gruppoid mit nur einer Einheit eine Gruppe ist. Das Ziel dieser Arbeit ist zu zeigen, daß für die Zuordnung der Idealklassen zu den Normenformklassen in Quaternionenringen ein Satz gilt, dessen Wortlaut genau dem Satz am Ende des Paragraphen 1 über die Zuordnung der Idealklassen in quadratischen Körpern zu ihren Normenformklassen entspricht, wenn dort das Wort Gruppe durch das Wort Gruppoid ersetzt wird.

## 10. Die Quaternionenringe (= Quaternionenalgebren)

Die rationalen Algebren der Dimension 4 sind die sogenannten Algebren der verallgemeinerten Quaternionen. Sie sind darstellbar durch vier Basisgrößen $u_0 = 1$, $u_1$, $u_2$, $u_3$, zwischen denen folgende Beziehungen bestehen: $u_1^2 = \alpha$, $u_2^2 = \beta$, $u_3^2 = -\alpha\beta$, $\alpha, \beta$ rational, $u_1 u_2 = -u_2 u_1 = u_3$, $u_1 u_3 = -u_3 u_1 = \alpha u_2$, $u_2 u_3 = -u_3 u_2 = -\beta u_1$;

$$1 \cdot u_r = u_r \cdot 1 = u_r \quad (r = 1, 2, 3) \qquad ([8], \text{Seite } 44).$$

Ist $q = \sum_{i=0}^{3} x_i u_i$ ein Element der Algebra, so heißt

$$q\bar{q} = n(q) \text{ die Norm von } q\,,$$

wobei $\bar{q} = x_0 - x_1 u_1 - x_2 u_2 - x_3 u_3$ das konjugierte Element von $q$ heißt. Unter $s(q)$, der Spur von $q$, verstehen wir

$$s(q) = q + \bar{q} = 2x_0\,.$$

Spur und Norm jedes $q$ sind rational. Es ist nämlich

$$n(q) = n\Big(\sum_{i=0}^{3} x_i u_i\Big) = x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2\,.$$

Ein Quaternion mit ganzer Norm und Spur heißt *ganz*.

## 11. Moduln und zugeordnete Formen

Bezeichnen wir die betrachtete Algebra mit $\mathfrak{A}$, so heißt jede Teilmenge $\mathfrak{a}$ von $\mathfrak{A}$, die mit den Elementen $\alpha$ und $\beta$ auch $\alpha - \beta$ enthält und die außerdem 4 rational linear unabhängige Quaternionen umfaßt, ein *Modul*. Sei $\alpha_0$, $\alpha_1$, $\alpha_2$, $\alpha_3$ eine Basis des Moduls $\mathfrak{a}$. Diesem Modul ordnen wir eine rationale quaternäre quadratische Form zu, nämlich die Norm seines allgemeinen Elements

$$n\Big(\sum_{i=0}^{3} x_i \alpha_i\Big) = F((x)).$$

Sei $\mathfrak{b}$ ein anderer Modul mit der Basisdarstellung $\mathfrak{b} = (\beta_0, \beta_1, \beta_2, \beta_3)$ und der zugeordneten Form $G((y)) = n(\sum_{\nu=0}^{3} y_\nu \beta_\nu)$. Es ist dann $\alpha_i = \sum_{\nu=0}^{3} T_{i\nu}\beta_\nu$ ($T_{i\nu}$ rational, det $T_{i\nu} \neq 0$), wofür wir kürzer setzen $\alpha = T\beta$. $q$ ist gleichzeitig darstellbar als

$$q = \sum_{i=0}^{3} x_i \alpha_i = \sum_{\nu=0}^{3} y_\nu \beta_\nu = \sum_{i,\nu=0}^{3} x_i T_{i\nu} \beta_\nu .$$

Es ist somit $y_\nu = \sum_{i=0}^{3} T_{i\nu} x_i = \sum_{i=0}^{3} T'_{\nu i} x_i$ ($T'$ = Transponierte von $T$) diejenige lineare Transformation, die $G((y))$ in $F((x))$ überführt.

**Zusammenfassend:** Geht $\mathfrak{a}$ über in $\mathfrak{b}$ mittels $\alpha = T\beta$, so geht die dem Modul $\mathfrak{b}$ zugeordnete Form $G((y))$ über in die dem $\mathfrak{a}$ zugeordnete Form $F((x))$ mittels $y = T'x$, oder $\mathfrak{a} \to \mathfrak{b}$ mittels $\alpha = T\beta$, $G((y)) \to F((x))$ mittels $y = T'x$.

## 12. Norm und Normenform eines Moduls $\mathfrak{a} = (\alpha_0, \ldots, \alpha_3)$

Wir schreiben wieder $F((x)) = n(\sum \alpha_i x_i)$ und setzen

$$F((x)) = n(\mathfrak{a}) F_{\mathfrak{a}}^{(\alpha)}((x)) \quad \text{mit} \quad \underline{n(\mathfrak{a}) > 0},$$

wobei $F_{\mathfrak{a}}^{(\alpha)}((x))$ ganzzahlig und primitiv ist, das heißt in $F_{\mathfrak{a}}^{(\alpha)}((x)) = \sum f_{ik} x_i x_k$ sind $f_{00}, \ldots, f_{33}, 2f_{01}, \ldots, 2f_{23}$ ganz und teilerfremd.

$n(\mathfrak{a})$ heißt *Norm*, $F_{\mathfrak{a}}^{(\alpha)}((x))$ *Normenform des Moduls* $\mathfrak{a}$.

Zu verschiedenen Basen können verschiedene Normenformen gehören. Jedoch ist die *Klasse* der Normenformen eindeutig bestimmt. Ist nämlich $(\beta_0, \beta_1, \beta_2, \beta_3)$ eine andere Basis von $\mathfrak{a}$, die aus $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ durch ganzzahlige unimodulare Transformation hervorgeht,

$$\beta = T\alpha, \ \det T = +1, \quad \text{dann geht}$$

$$n(\mathfrak{a}) F_{\mathfrak{a}}^{(\alpha)}((x)) \ \text{über in} \ n(\mathfrak{a}) F_{\mathfrak{a}}^{(\beta)}((y)) \ \text{mittels}$$

$x = T'y$, somit gehören $F_{\mathfrak{a}}^{(\alpha)}((x))$ und $F_{\mathfrak{a}}^{(\beta)}((y))$ zur selben Klasse. Es ist ersichtlich, daß man über die Reihenfolge der Basiselemente noch eine Annahme treffen muß, die verhindert, daß die Übergangsdeterminante der linearen Transformation einer Basis in die andere den Wert $-1$ hat. In diesem letzteren Fall ist dann auch det $T' = -1$, so daß die transformierte Form im allgemeinen nicht in der selben Klasse liegt (siehe Paragraph 18).

## 13. Ordnungen und Ideale

**Definition.** Eine Ordnung ist ein Ring ganzer Quaternionen von $\mathfrak{A}$, der die ganzen rationalen Zahlen sowie 4 linear unabhängige Quaternionen umfaßt.

Zu jedem Modul $\mathfrak{a}_{ik}$ gibt es zwei eindeutig bestimmte Ordnungen $\mathfrak{o}_i$ und $\mathfrak{o}_k$ mit $\mathfrak{o}_i \mathfrak{a}_{ik} = \mathfrak{a}_{ik}$ und $\mathfrak{a}_{ik}\mathfrak{o}_k = \mathfrak{a}_{ik}$ ([11], Seite 75).

**Definition.** Ein Modul heißt Ideal, wenn seine beiden Ordnungen Maximalordnungen sind (das heißt in keiner andern Ordnung enthalten sind), wenn also gilt $\mathfrak{a}_{ik}\mathfrak{o}_k = \mathfrak{o}_i \mathfrak{a}_{ik} = \mathfrak{a}_{ik}$; $\mathfrak{o}_i$, $\mathfrak{o}_k$ maximal. Enthält das Ideal $\mathfrak{a}_{ik}$ nur ganze Quaternionen, dann nennt man $\mathfrak{a}_{ik}$ ein ganzes Ideal.

Wir schränken nun die Multiplikation der Ideale insofern ein, als wir zwei Idealen $\mathfrak{a}_{ik}$ und $\mathfrak{b}_{lj}$ nur dann ein Produkt zuordnen, die Faktoren in dieser Reihenfolge genommen, wenn $\mathfrak{o}_k = \mathfrak{o}_l$ ist. Durch diese Maßnahme erreicht man, daß die Teilung eindeutig ist, das heißt, daß in der Gleichung $\mathfrak{a}\mathfrak{x} = \mathfrak{b}$ das $\mathfrak{x}$ eindeutig bestimmt ist. Die so eingeschränkte Multiplikation heißt *eigentliche* Multiplikation. Es gilt nämlich ([11], Seite 75) der folgende

**Satz.** *Sind $\mathfrak{a}_{ik}$ und $\mathfrak{b}_{lj}$ beides Ideale, so ist es dann und nur dann unmöglich, in der Gleichung $\mathfrak{a}_{ik}\mathfrak{b}_{lj} = \mathfrak{c}_{ij}$ eines der Ideale $\mathfrak{a}_{ik}$ und $\mathfrak{b}_{lj}$ durch echte Teiler zu ersetzen, wenn die Rechtsordnung von $\mathfrak{a}_{ik}$ gleich der Linksordnung von $\mathfrak{b}_{lj}$ ist, das heißt wenn $\mathfrak{o}_k = \mathfrak{o}_l$.*

**Satz.** ([11], Seite 76, Satz 14.) *Die Ideale einer Quaternionenalgebra bilden bei der eigentlichen Multiplikation ein Gruppoid mit den Maximalordnungen als Einheiten.*

### 14. Die Gruppoidaxiome (s. Brandt, Math. Ann. 96)

Sei $\{A, B, C, \ldots\}$ eine Menge von Elementen. Für diese sei eine Verknüpfung definiert, die gewissen Elementen $A$ und $B$ in dieser Reihenfolge ein Produktelement $C$ zuordnet, für gewisse andere Elemente aber kein Produkt definiert. Existiert $AB$, so heißt $A$ mit $B$ in dieser Reihenfolge komponierbar (das heißt natürlich nicht, daß dann auch $BA$ existiert). Eine solche Menge von Elementen heißt *Gruppoid*, wenn die folgenden vier Axiome erfüllt sind:

**Axiom I.** Wenn zwischen drei Elementen $A$, $B$, $C$ eine Beziehung $AB = C$ besteht, so ist jedes der drei Elemente $A$, $B$, $C$ durch die beiden andern bestimmt.

**Axiom II.** Wenn $AB$ und $BC$ existieren, so existieren auch $(AB)C$ und $A(BC)$, wenn $AB$ und $(AB)C$ existieren, so auch $BC$ und $A(BC)$, wenn schließlich $BC$ und $A(BC)$ existieren, so auch $AB$ und $(AB)C$, und jedesmal ist $(AB)C = A(BC)$, so daß Klammern überflüssig sind und dafür $ABC$ gesetzt werden kann.

**Axiom III.** Für irgendein Element $A$ existieren stets die folgenden eindeutig bestimmten Elemente: Die Rechtseinheit $E$, die Linkseinheit $E'$ und das inverse Element $\bar{A}$ derart, daß gilt

$$AE = A\,, \qquad E'A = A\,, \qquad \bar{A}A = E\,.$$

Hieraus lassen sich noch die folgenden Gleichungen beweisen:

$$A\bar{A} = E', \qquad E\bar{A} = \bar{A}, \qquad \bar{A}E' = \bar{A}, \qquad EE = E, \qquad E'E' = E'\,.$$

**Axiom IV.** Für zwei beliebig vorgegebene Einheiten $E$ und $E'$ existieren immer Elemente $A$ so daß $AE = A$ und $E'A = A$.

Aus den Axiomen leiten wir noch den folgenden wichtigen Satz her:

**Satz.** *Zwei Elemente $A$ und $B$ sind in dieser Reihenfolge dann und nur dann komponierbar, wenn die Rechtseinheit von $A$ gleich der Linkseinheit von $B$ ist, also $A = AE$, $EB = B$.*

**Beweis.** Aus Axiom II folgt, daß wenn in der Reihe $A_1, A_2, \ldots, A_n$ stets $A_i$ mit $A_{i+1}$ komponierbar ist $(i = 1, \ldots, n-1)$, das Produkt $A_1A_2\ldots A_n$ existiert. Sei nun etwa $E_1$ Einheit, ebenso $E_2$, $E_1 \neq E_2$, so kann $E_1E_2$ nicht existieren, da $E_1E_2 = E_1 = E_2$ sein müßte, was einen Widerspruch ergibt. Existiert jetzt $AB$, so ist $AB = AE_1E_2B$, wo $E_1$ Rechtseins von $A$, $E_2$ Linkseins von $B$ bedeutet. Ist $E_1 \neq E_2$, so hat $E_1E_2$ keinen Sinn; somit muß $E_1 = E_2$ sein. Ist umgekehrt $AE = A$, $EB = B$, so existiert $AB = AEEB$, weil in der Reihe $A, E, E, B$ die aufeinanderfolgenden Produkte $AE, EE, EB$ existieren.

## 15. Stamm- und Kernformen

a) Irgendeine ganzzahlige primitive Form $G((x))$ definiert eine Gesamtheit von Formen auf folgende Weise: Man übt auf die Formen $cG((x))$, wo $c$ beliebig rational ist, alle regulären rationalen Substitutionen, das heißt alle rationalen Substitutionen mit Determinante $\neq 0$, aus. Jede entstehende Form schreiben wir als $kF((x))$, wo $k$ größter Koeffiziententeiler, also $F((x))$ auch ganzzahlig primitiv ist. Die Formen $F((x)), G((x)), \ldots$ bilden eine sogenannte *Sippe*; sie sind nicht immer rational ineinander transformierbar, wohl aber stets nach Multiplikation mit einer Rationalzahl. Die Formen mit absolut kleinster Diskriminante einer Sippe heißen *Stammformen.*

b) Üben wir auf $G((x))$ alle rationalen regulären linearen Substitutionen aus, ohne Multiplikation mit rationalen Faktoren, so bilden die entstandenen Formen eine Gesamtheit, die man *Familie* nennt.

**Definition.** *Kernformen* sind solche ganzzahlige primitive Formen, die nicht ganzzahlig in einer ganzzahligen Form kleinerer Diskriminante enthalten sind.

**Satz** (BRANDT, SPEISER-Festschrift, Zürich 1945, S. 96): *Die Kernformen sind diejenigen ganzzahligen Formen, welche in der von ihnen erzeugten Familie die absolut kleinste Determinante besitzen.*

Von HASSE (J. reine angew. Math. *153*, Satz 24, Seite 37) stammt der folgende

**Satz.** *Eine rationale quadratische Form ist genau dann jedem positiven rationalen Multiplum ihrer selbst rational äquivalent, wenn n in* $F = \sum_{i,k=1}^{n} a_{ik} x_i x_k$ *gerade und* $d = (-1)^{\frac{n}{2}} D$ *ein Quadrat ist* $(D = |a_{ik}|)$, *und genau dann jedem rationalen Vielfachen ihrer selbst äquivalent, wenn außerdem der Trägheitsindex* $J = \frac{n}{2}$ *ist.*

Die Normenformen der Moduln in Quaternionenalgebren erfüllen die Bedingungen des HASSEschen Satzes. Da $n = 4$ ist, so muß nur $D$, die Determinante, ein Quadrat sein. Liegt der Algebra das Basissystem $1, u_1, u_2, u_3$ zugrunde (Paragraph 12), dann ist, wie dort ausgeführt, die dem Modul $(1, u_1, u_2, u_3)$ zugeordnete Form $x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2$, ihre Determinante ist $\alpha^2\beta^2$, also ein rationales Quadrat. Ist dann $(\lambda_0, \ldots, \lambda_3) = \mathfrak{l}$ ein beliebiger Modul der Algebra, so geht $(\lambda_0, \ldots, \lambda_3)$ mittels rationaler Transformation über in $(u_0 = 1, \ldots, u_3)$, gleichzeitig aber geht $x_0^2 - \alpha x_1^2 - \ldots$ über in $n(\sum_{i=0}^{3} \lambda_i y_i) = n(\mathfrak{l}) F_{\mathfrak{l}}((y))$ mittels der transponierten Transformation (Paragraph 11), die Determinante von $n(\sum_{i=0}^{3} \lambda_i y_i)$ ist gleich der Determinante $\alpha^2\beta^2$ multipliziert mit dem Quadrat der Substitutionsdeterminante, also wieder ein Quadrat; das Herausziehen des Koeffiziententeilers $n(\mathfrak{l})$ bedeutet Division der Formendeterminante durch $n(\mathfrak{l})^4$, was nichts an der Tatsache ändert, daß die Determinante von $F_{\mathfrak{l}}((y))$ ein Quadrat ist. Somit sind die positiv-definiten Normenformen in ihre positiven Multipla rational überführbar. Indefinite Normenformen ergeben sich dann, wenn im vorigen nicht beide, $\alpha$ und $\beta$, negativ sind. Dann ist aber der Trägheitsindex, das ist die Anzahl der negativen Quadrate, stets gleich $J = 2 = \frac{4}{2}$, somit ist eine solche Normenform *jedem* rationalen Multiplum ihrer selbst äquivalent. Das heißt aber, daß für Normenformen die Begriffe Familie und Sippe zusammenfallen, und daß somit hier Stamm- wie Kernformen *dasselbe* sind. Somit reduziert sich der Nachweis, daß eine Form Stammform ist, darauf, zu zeigen, daß diese Form nicht ganzzahlig in einer andern ganzzahligen Form enthalten sei.

## 16. Die Idealnormen

DEURING [11] definiert den Idealbegriff wie oben unter 13 und stellt die Norm eines Ideals wie folgt dar: Sei $\mathfrak{o}_i$ Maximalordnung in $\mathfrak{A}$ und $\mathfrak{a}_{ik}$ ein Linksideal von $\mathfrak{o}_i$, also $\mathfrak{o}_i\mathfrak{a}_{ik} = \mathfrak{a}_{ik}$. Seien $\mathfrak{o}_i = (\omega_0, \ldots, \omega_3)$, $\mathfrak{a}_{ik} = (\alpha_0, \ldots, \alpha_3)$. Ist nun $\alpha_i = \sum_{k=0}^{3} A_{ik}\omega_k$, oder kurz $\alpha = A\omega$, so ist $\det A = |A_{ik}|$ ein positives oder negatives rationales Quadrat. $|A_{ik}|$ ist *positiv* bei geeigneter Reihenfolge der $\alpha_i$. Dann heißt

$$n(\mathfrak{a}_{ik}) = +\sqrt{|A_{ik}|}$$

die Norm des Ideals $\mathfrak{a}_{ik}$ ([11], Seiten 81–83).

BRANDT schreibt für den Modul $\mathfrak{a} = (\alpha_0, \ldots, \alpha_3)$ ebenfalls $\alpha = A\omega$. Die Reihenfolge der $\alpha_i$ wählt er so, daß $\det A = |A| > 0$. Sodann setzt er, wie im Paragraphen 12 ausgeführt, $n(\sum_{i=0}^{3} x_i\alpha_i) = n(\mathfrak{a})F_{\mathfrak{a}}((x))$ mit $n(\mathfrak{a}) > 0$. Nun zeichnet BRANDT diejenigen Moduln, für die $\underline{n(\mathfrak{a})^2 = |A|}$ gilt, besonders aus, indem er sie Ideale nennt. BRANDT zeigt ([3], Seiten 20/21), daß für diese Ideale $\mathfrak{a}$ genau je eine Links- und Rechtsmaximalordnung $\mathfrak{e}_1$ und $\mathfrak{e}_2$ mit $\mathfrak{e}_1\mathfrak{a} = \mathfrak{a}\mathfrak{e}_2 = \mathfrak{a}$ existieren. Also ist jedes Ideal im Sinne von BRANDT auch ein Ideal im Sinne von DEURING und umgekehrt. Ferner folgt, daß die bei BRANDT und DEURING gegebenen Idealnormdefinitionen äquivalent sind.

**Satz** von der Normenmultiplizität:
*Aus der Idealgleichung* $\mathfrak{c}_{il} = \mathfrak{a}_{ik}\mathfrak{b}_{kl}$ *folgt die Normengleichung* $n(\mathfrak{c}_{il}) = n(\mathfrak{a}_{ik})n(\mathfrak{b}_{kl})$ ([11], Satz 3, Seite 80).

**Satz.** *Ein ganzes Ideal der Norm* 1 *ist stets eine Maximalordnung.*

Beweis: Ist $(\omega_0, \ldots, \omega_3)$ die Linksmaximalordnung von $\mathfrak{a}$, so sind in der Transformationsgleichung $\alpha_i = \sum_{k=0}^{3} A_{ik}\omega_k$ die $A_{ik}$ ganzrational mit $|A_{ik}| = n(\mathfrak{a})^2 = 1$, so daß $\mathfrak{a}$ mit $\mathfrak{o}$ identisch ist. Hier sind die $A_{ik}$ deshalb ganzzahlig, weil ein ganzes Ideal stets in seinen Maximalordnungen (linker wie rechter) enthalten ist. Dies letztere ist eine Konsequenz des 1. Hilfssatzes im Paragraphen 26, es folgt nämlich aus $\mathfrak{a}_{ik} = \mathfrak{o}_i\mathfrak{o}_i\mathfrak{a}_{ik}$ die Beziehung $\mathfrak{a}_{ik} \subseteqq \mathfrak{o}_i$, weil $\mathfrak{a}_{ik}$ und $\mathfrak{o}_i$ ganz sind.

## 17. Satz: Die Normenform einer Maximalordnung $\mathfrak{o}$ ist eine Stammform $F((x))$

**Beweis.** Sei $\mathfrak{o} = (\omega_0, \ldots, \omega_3)$; da $n(\mathfrak{o}) = 1$, so ist $n(\sum\omega_i x_i) = F((x))$. Um nachzuweisen, daß $F((x))$ Stammform ist, müssen wir nach Paragraph 15 Schluß nur nachweisen, daß $F((x))$ Kernform ist, das heißt nicht ganzzahlig in einer ganzen Form kleinerer Diskriminante enthalten ist. Wäre, im Widerspruch zur Aussage des Satzes, $F((x))$ enthalten in der Form $G((y))$, so daß also $G((y)) \to F((x))$ mittels $y = Tx$, wo $T$ ganzzahlig ist, mit der Determinante $|T| > 1$, dann geht $(\omega_0, \ldots, \omega_3)$ über in den Modul $\mathfrak{l} = (\lambda_0, \ldots, \lambda_3)$ mittels $\omega = T'\lambda$. $\mathfrak{l}$ ist ein *ganzer* Modul, denn Normen und Spuren der Elemente von $\mathfrak{l}$ sind ganz rational.

Ist nämlich $\lambda = \sum_{i=0}^{3} \lambda_i y_i$ beliebig in $\mathfrak{l}$, so ist $n(\lambda) = G((y))$, also ganz; damit ist die Ganzheit der Normen aller Elemente von $\mathfrak{l}$ erkannt. Mit $\lambda \in \mathfrak{l}$ ist auch $\lambda + 1 \in \mathfrak{l}$. Denn wegen $\det T' > 1$ und weil $T'$ ganzzahlig ist, ist $\mathfrak{o}$ echter Untermodul von $\mathfrak{l}$, also mit $1 \in \mathfrak{o}$ auch $1 \in \mathfrak{l}$. Es ist

$$\underset{\text{ganz}}{n(\lambda + 1)} = (\lambda + 1)(\bar{\lambda} + 1) = \lambda\bar{\lambda} + 1 + (\lambda + \bar{\lambda}) = \underset{\text{ganz}}{n(\lambda)} + 1 + s(\lambda)$$

somit haben die $\lambda$ auch ganze Spuren.

Für Quaternionenalgebren hat Eichler in seiner Dissertation (J. reine angew. Math. 174, Seite 132) folgenden Satz bewiesen:

**Satz.** *Jeder ganze Modul ist in einer Maximalordnung enthalten.*

Sei somit $\mathfrak{l}$ in der Maximalordnung $\mathfrak{m}$ enthalten. Dann ist auch $\mathfrak{o} \subset \mathfrak{l} \subseteqq \mathfrak{m}$, also $\mathfrak{o} \subset \mathfrak{m}$; das ist aber nicht möglich, weil $\mathfrak{o}$ selbst Maximalordnung ist. Somit muß $F((x))$ Stammform sein, da die gegenteilige Annahme auf einen Widerspruch führt.

## 18. Die Unabhängigkeit der Idealnorm von der zugrundegelegten Maximalordnung

Sind $\mathfrak{o}_1$ und $\mathfrak{o}_2$ zwei Maximalordnungen in $\mathfrak{A}$, so geht $\mathfrak{o}_1$ in $\mathfrak{o}_2$ über mittels einer rationalen Substitution. Mit der Transponierten geht dann die Normenform $G_2((y))$ von $\mathfrak{o}_2$ in diejenige von $\mathfrak{o}_1$, nämlich $G_1((x))$, über. Da beides Stammformen sind und sie in der selben Sippe liegen, so haben sie die gleiche Diskriminante, nämlich die absolut kleinste der ganzen Sippenformen. Somit ist der Wert der Substitutionsdeterminante $= +1$, bei geeigneter Reihenfolge der Basiselemente von $\mathfrak{o}_1$ und $\mathfrak{o}_2$. Daraus folgern wir, daß es genügt, bei der Bestimmung der Idealnorm eine beliebige Maximalordnung zugrundezulegen, es braucht weder die Links- noch die Rechtsordnung von $\mathfrak{a}$ zu sein. Ist nämlich $\mathfrak{o}$ die beliebige Maximalordnung, $\mathfrak{o} = (\omega_0, \ldots, \omega_3)$, und ist $\mathfrak{o}' = (\nu_0, \ldots, \nu_3)$ die Linksordnung von $\mathfrak{a}$, so sei vorerst an dieser Stelle folgende *Bedingung* betreffs der *Reihenfolge der Basiselemente* sämtlicher Moduln in $\mathfrak{A}$ festgesetzt (siehe Paragraph 12 Schluß). Ist $\mathfrak{a}$ ein Modul, $\mathfrak{a} = (\alpha_0, \ldots, \alpha_3)$ in Basisdarstellung, so soll in der Transformationsgleichung

$$\alpha_i = \sum_{k=0}^{3} A_{ik}\,\omega_k \quad \text{oder} \quad \alpha = A\,\omega$$

$|A_{ik}| > 0$ sein, das heißt die Determinante der *Basismatrix* $A_{ik}$ soll *positiv* sein. Sei jetzt $\mathfrak{a}$ ein Ideal mit $\alpha = A\nu$, $\nu = E\omega$, dann ist $\alpha = AE\omega$, $\det(AE) = \det A \det E = \det A$, was heißt, daß die im Paragraphen 16 gemachte Voraussetzung, daß für die Bestimmung der Norm eines Ideals eine seiner Ordnungen zugrundegelegt werde, fallengelassen werden kann.

## 19. Die Ideale sind vor den gewöhnlichen Moduln dadurch ausgezeichnet, daß ihre Normenformen Stammformen sind

Wir können die Ideale auch so definieren: Ein Modul ist genau dann ein Ideal, wenn seine Normenform eine Stammform ist.

**Beweis.** Der Modul $\mathfrak{a} = (\alpha_0, \ldots, \alpha_3)$ mit der Normenform $G((y))$ gehe aus der Maximalordnung $\mathfrak{o} = (\omega_0, \ldots, \omega_3)$, deren Normenform $F((x))$ gemäß Paragraph 17 Stammform ist, durch die Substitution $\alpha = A'\omega$ hervor. Dann geht $F((x)) \to n(\mathfrak{a})G((y))$ mittels $x = Ay$. Faßt man $F$ und $G$ als Matrizen der durch sie bezeichneten Formen auf, so ist also

$n(\mathfrak{a})G((y)) = n(\mathfrak{a})y'Gy = y'A'FAy$, das gibt für die Determinanten
$n(\mathfrak{a})^4\,|G| = |A|^2\,|F|$.

Ist $n(\mathfrak{a})^4 = |A|^2$, was genau für die Ideale der Fall ist (siehe Nr. 16), so ist $|G| = |F|$, also hat auch $G((y))$ Minimaldiskriminante (die Diskriminante ist das 16fache der Determinante). Somit sind in der Tat gerade die den Idealen zugehörigen Normenformen Stammformen.

## 20. Die Idealklassen der Quaternionenringe

Zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ heißen äquivalent, $\mathfrak{a} \sim \mathfrak{b}$, wenn zwischen ihnen eine Beziehung mit Quaternionen $\varrho$ und $\sigma$ besteht, so daß

$$\mathfrak{b} = \varrho\mathfrak{a}\sigma \quad \text{ist mit} \quad \underline{n(\varrho\sigma) > 0}\,.$$

Diese Beziehung ist tatsächlich eine Äquivalenzrelation, denn es gilt die Transivität:

$$\begin{array}{llllll} \text{Aus} & \mathfrak{a} \sim \mathfrak{b}\,, & \text{also} & \mathfrak{a} = \mu\mathfrak{b}\nu\,, & n(\mu\nu) > 0 & \text{und} \\ & \mathfrak{b} \sim \mathfrak{c}\,, & \text{also} & \mathfrak{b} = \lambda\mathfrak{c}\tau\,, & n(\lambda\tau) > 0\,, & \text{folgt} \end{array}$$

$\mathfrak{a} = \mu\lambda\mathfrak{c}\tau\nu$ mit $n(\mu\lambda\tau\nu) > 0$, also $\mathfrak{a} \sim \mathfrak{c}$. Die Symmetrieeigenschaft ist erfüllt, denn aus $\mathfrak{b} = \varrho\mathfrak{a}\sigma$ folgt $\mathfrak{a} = \varrho^{-1}\mathfrak{b}\sigma^{-1}$ mit $n(\varrho^{-1}\sigma^{-1}) > 0$, das heißt aus $\mathfrak{a} \sim \mathfrak{b}$ folgt auch $\mathfrak{b} \sim \mathfrak{a}$.

Die zu einem Ideal äquivalenten Ideale fassen wir zu einer *Idealklasse* zusammen. Wir wollen nun für diese Idealklassen eine Art Multiplikation, die wir *Komposition der Idealklassen* nennen wollen, definieren, und alsdann prüfen, ob die Definition sinnvoll ist.

Die Idealklasse $\mathfrak{A}$ heiße mit der Klasse $\mathfrak{B}$ in dieser Reihenfolge komponierbar, wenn Ideale $\mathfrak{a} \in \mathfrak{A}$, $\mathfrak{b} \in \mathfrak{B}$ existieren, für die das Produkt $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$ existiert. Dann heißt $\mathfrak{C}$, die Klasse von $\mathfrak{c}$, die Produktklasse oder die komponierte Klasse von $\mathfrak{A}$ und $\mathfrak{B}$, $\mathfrak{A}\mathfrak{B} = \mathfrak{C}$.

Ist nun $\mathfrak{a}' \sim \mathfrak{a}$, sei etwa $\mathfrak{a}' = \varrho\mathfrak{a}\sigma$, $n(\varrho\sigma) > 0$, dann soll man auch ein Ideal $\mathfrak{b}' \sim \mathfrak{b}$ finden können, so daß $\mathfrak{a}'\mathfrak{b}' = \mathfrak{c}'$ existiert und $\mathfrak{c}'$ soll alsdann äquivalent zu $\mathfrak{c}$ sein, $\mathfrak{c}' \sim \mathfrak{c}$. Dazu setzen wir $\mathfrak{b}' = \sigma^{-1}\mathfrak{b}\tau$. Das Element $\tau$ werde so gewählt, daß $\operatorname{sign}(n(\tau)) = \operatorname{sign}(n(\varrho))$ ist, dann ergibt sich

$$\mathfrak{a}'\mathfrak{b}' = \varrho\mathfrak{a}\sigma\sigma^{-1}\mathfrak{b}\tau = \varrho\mathfrak{a}\mathfrak{b}\tau = \varrho\mathfrak{c}\tau = \mathfrak{c}'; \qquad \mathfrak{c} \sim \mathfrak{c}'.$$

Ist weiter $\mathfrak{a}' \sim \mathfrak{a}$, $\mathfrak{b}' \sim \mathfrak{b}$, und existiert $\mathfrak{a}'\mathfrak{b}' = \mathfrak{c}'$, dann muß $\mathfrak{c} \sim \mathfrak{c}'$ sein, wenn die gegebene Kompositionsvorschrift einen Sinn haben soll. Diese Frage ist nicht so einfach zu beantworten, sie steht nämlich in einer Beziehung zu einem Kernproblem des in dieser Arbeit zu beweisenden Hauptsatzes (Paragraph 26). Im nächsten Paragraphen wird gezeigt, daß zu äquivalenten Idealen die selbe Normenformklasse gehört. Später (Paragraphen 22–25) sehen wir, daß der Multiplikation der Ideale parallel die Komposition der Normenformklassen geht. Sind dann $A$, $B$ und $C$ die Normenformklassen der Ideale $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, dann haben wir zusammen mit den Multiplikationsgleichungen der Ideale

$$\mathfrak{a}\mathfrak{b} = \mathfrak{c} \quad , \qquad \mathfrak{a}'\mathfrak{b}' = \mathfrak{c}'$$

die Kompositionsgleichungen der zugehörigen Normenformklassen

$$AB = C\,, \qquad AB = C$$

Wie wir sehen, besitzen die Ideale $\mathfrak{c}$ und $\mathfrak{c}'$ äquivalente Normenformen. Kann man daraus schließen, daß dann auch die Ideale selbst äquivalent sind? Daß dem so ist, zeigt der Satz des Paragraphen 26.

Da die Ideale ein Gruppoid bilden, so kann man die Axiome des Paragraphen 14 prüfen und feststellen, daß auch die Idealklassen selber ein Gruppoid bilden. Die Einheiten dieses Gruppoids sind die von den Maximalordnungen (auch Einheitsideale genannt) erzeugten Klassen mit Idealen der Form $\varrho\mathfrak{o}\sigma$, wobei $n(\varrho\sigma) > 0$.

Weil die Idealklassenzahl rationaler Algebren endlich ist ([11], Seite 90, Satz 1), so ist das Idealklassengruppoid endlich.

## 21. Äquivalente Ideale besitzen äquivalente Normenformen

Sei $\mathfrak{a} = (\alpha_0, \ldots, \alpha_3)$; für $\mathfrak{b} \sim \mathfrak{a}$, etwa $\mathfrak{b} = \varrho \mathfrak{a} \sigma$ mit $n(\varrho\sigma) > 0$ können wir die Basisdarstellung $(\varrho\alpha_0\sigma, \ldots, \varrho\alpha_3\sigma)$ wählen. Ist dann

$$n(\sum_{i=0}^{3} \alpha_i x_i) = n(\mathfrak{a}) F_{\mathfrak{a}}((x)), \quad \text{so wird}$$

$$n(\sum_{i=0}^{3} \varrho\alpha_i x_i \sigma) = n(\varrho(\sum_{i=0}^{3} \alpha_i x_i)\sigma) = n(\varrho) n(\sigma) n(\mathfrak{a}) F_{\mathfrak{a}}((x)) .$$

Die Abbildung der Idealklassen auf die Normenformklassen ist also eindeutig. Daß sie sogar *umkehrbar eindeutig* ist, werden wir im Paragraphen 26 sehen.

## 22. Der Multiplikation der Ideale entspricht eine Transformation ihrer Normenformen

In den Paragraphen 23, 24 wird gezeigt daß, zufolge der Annahme in Nr. 18, wonach die Determinanten der Basismatrizen *positiv* seien, diese Transformationen sogar Kompositionen sind (siehe Nr. 3, Ende), wenn noch ein kleiner *Zusatz* gemacht wird (siehe Nr. 23, Ende).

Ist für die Ideale $\mathfrak{a} = (\alpha_0, \ldots, \alpha_3)$, $\mathfrak{b} = (\beta_0, \ldots)$, $\mathfrak{c} = (\gamma_0, \ldots)$ die Gleichung $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$ erfüllt, so gilt für je drei entsprechende Elemente

$$\alpha = \sum_{i=0}^{3} \alpha_i x_i ; \qquad \beta = \sum_{k=0}^{3} y_k \beta_k ; \qquad \gamma = \sum_{l=0}^{3} z_l \gamma_l$$

mit ganzrationalen $x_i$, $y_k$, $z_l$ eine Gleichung

$$\sum_{i=0}^{3} \alpha_i x_i \sum_{k=0}^{3} \beta_k y_k = \sum_{l=0}^{3} z_l \gamma_l .$$

Aus dieser Gleichung erhält man, mit $F_{\mathfrak{a}}((x))$, $F_{\mathfrak{b}}((y))$, $F_{\mathfrak{c}}((z))$ bzw. die Normenformen von $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ bezeichnend, durch Normenbildung

$$n(\mathfrak{a}) n(\mathfrak{b}) F_{\mathfrak{a}}((x)) F_{\mathfrak{b}}((y)) = n(\mathfrak{c}) F_{\mathfrak{c}}((z))$$

woraus wegen $n(\mathfrak{a}) n(\mathfrak{b}) = n(\mathfrak{c})$ folgt $F_{\mathfrak{a}}((x)) F_{\mathfrak{b}}((y)) = F_{\mathfrak{c}}((z))$. Welche Formen in diese Transformation eingehen, hängt offensichtlich von der Basisdarstellung der drei multiplizierten Ideale ab. Wir wollen zeigen, wie sich alle die diese Transformationen vermittelnden Bilinearsubstitutionen aus einer einzigen durch lineare Transformation ihrer Variabeln ableiten lassen. Dazu legen wir jetzt allen Untersuchungen die beliebige, aber feste Maximalordnung $\mathfrak{o} = (\omega_0, \ldots, \omega_3)$ von Nr. 18 zugrunde, die wir das *Grundideal* nennen. Die

Determinanten der auf diese Basis bezogenen Basismatrizen sollen $> 0$ sein. Ist $\omega_i \omega_k = \sum_{s=0}^{3} w_{sik} \omega_s$, wo die $w_{sik}$ *Multiplikationszahlen* der Basis $(\omega)$ heißen, und gilt weiter für die Basismatrizen $A, B, C$ $\alpha_i = \sum_{\sigma=0}^{3} A_{\sigma i} \omega_\sigma$; $\beta_k = \sum_{\tau=0}^{3} B_{\tau k} \omega_\tau$; $\gamma_l = \sum_{\kappa=0}^{3} C_{\kappa l} \omega_\kappa$, so wird

$$\sum_{i=0}^{3} x_i \alpha_i \sum_{k=0}^{3} y_k \beta_k = \sum_{i,k=0}^{3} x_i y_k \alpha_i \beta_k = \sum_{ik\sigma\tau\kappa} x_i y_k A_{\sigma i} B_{\tau k} w_{\kappa\sigma\tau} \omega_\kappa = \sum_{\kappa,l=0}^{3} z_l C_{\kappa l} \omega_\kappa ,$$

somit wegen der linearen Unabhängigkeit der $\omega_\nu$

$$\sum_{\sigma i\tau k} A_{\sigma i} B_{\tau k} w_{\kappa\sigma\tau} x_i y_k = \sum_{l=0}^{3} z_l C_{\kappa l} .$$

Auflösung nach $z$ gibt $z_\nu = \sum_{\kappa\sigma\tau i k} C_{\nu\kappa}^{-1} w_{\kappa\sigma\tau} A_{\sigma i} B_{\tau k} x_i y_k$; setzen wir noch $m_{\nu ik} = \sum_{\kappa\sigma\tau} C_{\nu\kappa}^{-1} w_{\kappa\sigma\tau} A_{\sigma i} B_{\tau k}$, so erhalten wir für die Bilinearsubstitution $M$ $z_\nu = \sum_{i,k=0}^{3} m_{\nu ik} x_i y_k$. In BRANDTscher Symbolik schreibt sich

$$M = C^{-1} - W \begin{matrix} \nearrow A \\ \searrow B \end{matrix} .$$

Wenn man $A = B = C = E$ (identische Substitution) setzt, so erkennt man, daß $W = (w_{sik})$ diejenige bilineare Substitution ist, welche die Transformation $GG = G$ der Normenform $G$ des Grundideals $\mathfrak{o}$ vermittelt. Transformieren wir jetzt die Variabeln $x, y, z$ ganzzahlig unimodular (Determinante $+1$), $x_i = \sum_{\alpha=0}^{3} U_{i\alpha} \xi_\alpha$; $y_k = \sum_{\beta=0}^{3} V_{k\beta} \eta_\beta$; $z_\nu = \sum_{\gamma=0}^{3} Z_{\nu\gamma} \zeta_\gamma$, so bedeutet dies den Übergang zu anderen Basen der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$; für die Normenformen bewirkt dies den Übergang zu den äquivalenten Formen $F'_\mathfrak{a}((\xi))$, $F'_\mathfrak{b}((\eta))$, $F'_\mathfrak{c}((\zeta))$. Man hat alsdann $F'_\mathfrak{a}((\xi)) F'_\mathfrak{b}((\eta)) = F'_\mathfrak{c}((\zeta))$ mittels

$$\mathfrak{M}_{\varrho\alpha\beta} = \sum_{\nu\kappa\sigma\tau i k} Z_{\varrho\nu}^{-1} C_{\nu\kappa}^{-1} w_{\kappa\sigma\tau} A_{\sigma i} U_{i\alpha} B_{\tau k} V_{k\beta} .$$

Symbolisch schreibt sich diese Bilinearsubstitution $\mathfrak{M}$ als

$$\mathfrak{M} = Z^{-1} C^{-1} - W \begin{matrix} \nearrow AU \\ \searrow BV \end{matrix} .$$

Der Multiplikation der Ideale entspricht somit die Transformation der zugehörigen Normenform*klassen*.

### 23. Die bilineare Substitution $W$ vermittelt die Komposition $GG = G$ (nicht bloß Transformation) der Normenform $G$ des Grundideals $\mathfrak{o}$

Der Gleichung $\mathfrak{o}\mathfrak{o} = \mathfrak{o}$ entspricht die Elementemultiplikation

$$\sum_{i=0}^{3} x_i \omega_i \sum_{k=0}^{3} y_k \omega_k = \sum_{l=0}^{3} z_l \omega_l,$$

daraus wird durch Normenbildung $G((x))G((y)) = G((z))$. Ist wieder $\omega_i \omega_k = \sum_{l=0}^{3} w_{lik} \omega_l$, so wird $\sum_{i=0}^{3} \omega_i x_i \sum_{k=0}^{3} y_k \omega_k = \sum_{i,k,l=0}^{3} x_i y_k w_{lik} \omega_l = \sum_{l=0}^{3} z_l \omega_l$, woraus $z_l = \sum_{i,k=0}^{3} w_{lik} x_i y_k$, das heißt, wie schon erwähnt, daß $W$ die Transformation $GG = G$ vermittelt. Die bilineare Substitution hat aber positive Signatur und Art (Nr. 3, Ende), letzteres, wenn man die Reihenfolge der Basiselemente des Grundideals selber geeignet wählt.

*Positive Signatur*: Da $1 \in \mathfrak{o}$, so gibt es eine Darstellung $1 = \sum_{k=0}^{3} \eta_k \omega_k$ mit ganzrationalen $\eta_k$, somit gilt $\sum_{i=0}^{3} x_i \omega_i \sum_{k=0}^{3} \eta_k \omega_k = \sum_{i=0}^{3} x_i \omega_i = \sum_{l=0}^{3} z_l \omega_l$, hierbei ist $z_l = \sum_{i,k=0}^{3} w_{lik} x_i \eta_k = \sum_{i,k=0}^{3} (w_{lik} \eta_k) x_i$. Da die $\omega_i$ linear unabhängig sind, ist $x_l = z_l$, also $\sum_{k=0}^{3} w_{lik} \eta_k = \delta_{li}$, somit $\left| \sum_{k=0}^{3} w_{lik} \eta_k \right| = | \delta_{li} | = +1$. Da aber die Determinante $\left| \sum_{k=0}^{3} w_{lik} y_k \right|$ für alle reellen Werte ihrer Variabeln entweder stets positiv oder stets negativ ist (siehe Nr. 4), und weil hier für das spezielle Quadrupel $\eta_k$ das Plus-Zeichen nachgewiesen wurde, so gilt

$$\left| \sum_{k=0}^{3} w_{lik} y_k \right| = + G^2((y)),$$

was zu zeigen war. Ebenso gilt

$$\left| \sum_{i=0}^{3} w_{lik} x_i \right| = + G^2((x)).$$

*Positive Art.* $W$ hat, wie gezeigt, positive Signatur. Sollte $W$ *negative* Art haben, dann gehe man von der Basis $(\omega_0, \ldots, \omega_3)$ des Grundideals zu einer andern, $(\omega_0', \ldots, \omega_3')$, mittels einer uneigentlichen ganzzahligen unimodularen Substitution (Determinante $-1$) über, etwa durch Vertauschung zweier Basiselemente. Ist etwa $\omega' = A'\omega$, $A$ ganzzahlig, $\det A = -1$, so geht $G((x))$ mittels $x = Au$ über in die Normenform $G'((u))$ der Basis $(\omega')$, die Transformation $G'G' = G'$ wird durch $W' = A^{-1} - W \begin{smallmatrix} \diagup A \\ \diagdown A \end{smallmatrix}$ vermittelt.

Der Satz der Nr. 6 lehrt aber, wenn man $\delta = 1$, $\iota_1 = \iota_2 = \iota_3 = -1$ setzt, daß bei dieser linearen Transformation die Art ändert, während die Signatur unverändert, also positiv, bleibt. Somit können wir bei geeigneter Wahl der Basiselemente des Grundideals stets erreichen, daß die Bilinearsubstitution *W Komposition* vermittelt. Diese Annahme wollen wir in der Folge immer als erfüllt ansehen; es ist dies der zu Beginn der Nr. 22 erwähnte Zusatz.

## 24. Alle Bilinearsubstitutionen $C^{-1} - W\genfrac{}{}{0pt}{}{\diagup A}{\diagdown B} = M$ vermitteln ebenfalls Komposition

Wie wir in Nr. 22 dargelegt, vermittelt $M = C^{-1} - W\genfrac{}{}{0pt}{}{\diagup A}{\diagdown B}$ die Transformation $F_{\mathfrak{a}}((x))F_{\mathfrak{b}}((y)) = F_{\mathfrak{c}}((z))$. $M$ geht aus $W$ durch die linearen Substitutionen $A$, $B$, $C$ hervor. Da ihre Determinantenquadrate nicht unbedingt gleich sind, so läßt sich der Satz von Nr. 6 nicht unmittelbar anwenden. Beachten wir (Nr. 19, Ende), daß $|A| = n(\mathfrak{a})^2$ ist, dann ist $A/+\sqrt{n(\mathfrak{a})}$ eine lineare Substitution der Determinante $+1$. Ebenso $B/+\sqrt{n(\mathfrak{b})}$ und

$$C/+\sqrt{n(\mathfrak{c})} = (\sqrt{n(\mathfrak{c})}C^{-1})^{-1}.$$

Die reelle Bilinearsubstitution $M'$ mit $M' = \sqrt{n(\mathfrak{c})}C^{-1} - W\genfrac{}{}{0pt}{}{\diagup A/\sqrt{n(\mathfrak{a})}}{\diagdown B/\sqrt{n(\mathfrak{b})}}$ vermittelt die Transformation $\frac{1}{n(\mathfrak{a})}F_{\mathfrak{a}}\frac{1}{n(\mathfrak{b})}F_{\mathfrak{b}} = \frac{1}{n(\mathfrak{c})}F_{\mathfrak{c}}$ oder wegen der Normenrelation $F_{\mathfrak{a}}F_{\mathfrak{b}} = F_{\mathfrak{c}}$. Der Satz in Nr. 6, angewendet auf $M'$, lehrt uns, daß $M'$ positive Signatur und Art hat. Es ist dies eine Konsequenz der Forderung in Nr. 18, daß die Determinanten der Basismatrizen positiv seien. Da $M = \frac{1}{\sqrt{n(\mathfrak{c})}} - M'\genfrac{}{}{0pt}{}{\diagup \sqrt{n(\mathfrak{a})}}{\diagdown \sqrt{n(\mathfrak{b})}}$ ist, das heißt aus $M'$ durch $x_i' = \sqrt{n(\mathfrak{a})}x_i$, $y_i' = \sqrt{n(\mathfrak{b})}y_i$, $z_i' = \sqrt{n(\mathfrak{c})}z_i$ hervorgeht, so ändert sich dadurch die Signatur nicht; denn, für $s$ eine beliebige Konstante gesetzt, gilt

$$|\sum_{i=0}^{3} m_{ikl} s x_i| = s^4 |\sum_{i=0}^{3} m_{ikl} x_i|,$$

während $A((sx))^2 = s^4 A((x))^2$ wird. Ebensowenig aber ändert sich die *Art*, denn ähnlich multipliziert sich jede Seite des Gleichungssystems ([6], Seite 225 unten), das die für die Art charakteristische Einheit $\varepsilon$ definiert, mit $s^4$, durch Wegkürzen erhält man die alte Gleichung wieder (vgl. auch Nr. 6). Somit haben tatsächlich alle in der Überschrift dieser Nummer erwähnten Bilinearsubstitutionen *positive Art* und *Signatur*, und vermitteln demzufolge die *Komposition* der Normenformen der Ideale.

## 25. Die Abbildung $\mathfrak{A} \to F_{\mathfrak{A}}$ ist ein Homomorphismus

Wir haben gesehen, daß die Idealmultiplikation $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$ von der Komposition $F_{\mathfrak{a}}F_{\mathfrak{b}} = F_{\mathfrak{c}}$ der Normenformen begleitet wird. Da nach Nr. 7 der Kompositionsbegriff von den Formen sofort auf die Formenklassen ausgedehnt werden kann, so entspricht der Komposition der Ideale die Komposition der zugehörigen Normenformklassen, und die Abbildung der Ideale auf die Formenklassen ist ein Homomorphismus, genauer Gruppoidhomomorphismus. Ferner haben äquivalente Ideale äquivalente Normenformen, also entspricht jeder Idealklasse $\mathfrak{A}$ eindeutig eine Formenklasse. In der nächsten Nummer werden wir zeigen, daß diese Abbildung der Idealklassen eineindeutig ist, das heißt daß zwei Ideale, denen dieselbe Formenklasse zugeordnet ist, äquivalent sind. Daraus folgt dann, wie in Paragraph 20 näher ausgeführt wurde, daß die Komposition der Idealklassen einen Sinn hat und daß die Idealklassen ein Gruppoid bilden. Dieses Gruppoid ist dann eineindeutig und homomorph, also isomorph auf das Gruppoid der Formenklassen abgebildet.

## 26. Zu äquivalenten Normenformen gehören äquivalente Ideale

**Satz.** *Aus* $F_{\mathfrak{a}}((x)) \sim F_{\mathfrak{b}}((y))$ *folgt* $\mathfrak{a} \sim \mathfrak{b}$.
Wir benötigen vier Hilfssätze.

**Hilfssatz 1.** Das Ideal $\mathfrak{a}_{ik}$ ist genau dann durch das Ideal $\mathfrak{b}_{jl}$ teilbar, das heißt gilt $\mathfrak{a}_{ik} \subseteqq \mathfrak{b}_{jl}$, wenn es eine eigentliche Produktdarstellung $\mathfrak{a}_{ik} = \mathfrak{c}_{ij}\mathfrak{b}_{jl}\mathfrak{f}_{lk}$ mit *ganzen* $\mathfrak{c}_{ij}$, $\mathfrak{f}_{lk}$ gibt. Ist $\mathfrak{o}_i = \mathfrak{o}_j$, so gilt sogar $\mathfrak{a}_{ik} = \mathfrak{b}_{il}\mathfrak{f}_{lk}$ mit ganzem $\mathfrak{f}_{lk}$. ([11], Seite 76, Satz 16.)

**Hilfssatz 2.** Ist die Normenform $F$ des Ideals $\mathfrak{a} = (\alpha_0, \ldots)$ mit $n(\sum_{i=0}^{3}\alpha_i x_i) = n(\mathfrak{a})F((x))$ eine Hauptform, dann ist $\mathfrak{a}$ Hauptideal.

**Beweis.** Da $F$ Hauptform ist, stellt $F$ die Eins ganzzahlig dar, sei etwa $F(\xi_0, \ldots \xi_3) = 1$. Dann ist $n(\alpha) = n(\sum_{i=0}^{3}\xi_i\alpha_i) = n(\mathfrak{a})F((\xi)) = n(\mathfrak{a})$, also $\underline{n(\alpha) = n(\mathfrak{a}) > 0}$, $\alpha = \sum_{i=0}^{3}\xi_i\alpha_i$ gesetzt.

Ist $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$, wo $\mathfrak{o}$ die Linksordnung von $\mathfrak{a}$ ist, so gilt die Beziehung $\mathfrak{o}\alpha \subseteqq \mathfrak{a}$. Ist $\mathfrak{o}\alpha = \mathfrak{a}$, so ist $\mathfrak{a}$ schon Hauptideal, nichts ist zu beweisen. Ist hingegen $\mathfrak{a}$ echter Teiler, also $\mathfrak{o}\alpha \subset \mathfrak{a}$, so ist nach Hilfssatz 1 $\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{b}$, wo $\mathfrak{b}$ ganzes Ideal. $\mathfrak{b}$ kann nicht die Rechtsordnung von $\mathfrak{a}$ sein, weil sonst $\mathfrak{a}\mathfrak{b} = \mathfrak{a}$, also ist $n(\mathfrak{b}) > 1$. Aus $\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{b}$ folgt $n(\alpha) = n(\mathfrak{a})n(\mathfrak{b})$, somit $n(\alpha) > n(\mathfrak{a})$, gegen Annahme. Somit ist $\mathfrak{o}\alpha = \mathfrak{a}$.

**Hilfssatz 3.** Sind $\mathfrak{o}_i$ und $\mathfrak{o}_k$ zwei Maximalordnungen mit den Hauptnormenformen $H_i((x))$ und $H_k((y))$, und gilt $H_i \sim H_k$, so ist $\mathfrak{o}_i \sim \mathfrak{o}_k$.

Um diesen Hilfssatz zu beweisen, verwenden wir einen Hilfssatz von Brandt.

**Hilfssatz 4.** Im Falle der *reduzierten* Basis (das heißt 1 ist Basiselement) sind die Multiplikationszahlen eindeutig bestimmt ([3], Seite 10, § 22). Dies ist so zu verstehen: Ist $(1, \ldots, \alpha_3)$ eine reduzierte Basis einer Maximalordnung, mit der Normenform $G((x))$, und ist $(1, \ldots, \beta_3)$ eine beliebige andere reduzierte Basis mit *derselben* Normenform $G$, dann sind die Multiplikationszahlen beider Basen dieselben (die Anordnung der Basiselemente stillschweigend so verstanden, daß die Determinante der Basismatrix bezüglich des Grundideals $> 0$ ist), das heißt, es gilt

$$\alpha_i \alpha_k = \sum_{j=0}^{3} r_{jik} \alpha_j \quad \text{und} \quad \beta_i \beta_k = \sum_{j=0}^{3} r_{jik} \beta_j \,.$$

Der ausführliche Beweis findet sich in [2], Seite 191. Es zeigt sich, daß es für die Normenform einer reduzierten Basis nur genau eine Bilinearsubstitution positiver Art und Signatur gibt, welche die Komposition $GG = G$ vermittelt. Gemäß Nr. 22 sind die Koeffizienten dieser Bilinearsubstitution identisch mit den Multiplikationszahlen $r_{jik}$ der zugehörigen Basis. Auch *sie* sind also *eindeutig bestimmt.*

Betrachten wir jetzt in $\mathfrak{o}_i$ die beliebige reduzierte Basis $(1, \alpha_1, \alpha_2, \alpha_3)$ und sei dann $n(\sum_{i=0}^{3} \alpha_i x_i) = G((x))$. Dann gilt $G(1, 0, 0, 0) = n(1) = 1$. In $\mathfrak{o}_k$ gibt es jedenfalls eine Basis $(\gamma_0, \ldots, \gamma_3)$ mit der Normenform $G((x))$, da ja $H_i \sim G \sim H_k$. Wegen $n(\gamma_0) = G(1, 0, 0, 0) = 1$ ist $\gamma_0$ eine Einheit, weil $\gamma_0^{-1} = \dfrac{\bar{\gamma}_0}{n(\gamma_0)}$ ebenfalls in $\mathfrak{o}_k$ liegt. Dann ist aber $(1, \gamma_0^{-1}\gamma_1, \ldots, \gamma_0^{-1}\gamma_3)$ eine *reduzierte* Basis. Nennen wir diese Basiselemente $(1, \beta_1, \ldots, \beta_3)$, in vorgeschriebener Reihenfolge gesetzt. Nach Hilfssatz 4 haben die Basen $(\alpha)$ und $(\beta)$ dieselben Multiplikationszahlen $a_{sik}$, es gelten somit die Gleichungen

$$\alpha_i \alpha_k = \sum_{s=0}^{3} a_{sik} \alpha_s \quad \text{und} \quad \beta_i \beta_k = \sum_{s=0}^{3} a_{sik} \beta_s \,.$$

Jetzt bilden wir $\mathfrak{o}_i$ auf $\mathfrak{o}_k$ isomorph ab durch die Zuordnung $\underline{\alpha_i \to \beta_i}$, wobei die rationalen Zahlen fest bleiben. Dann hat man weiter

$$\alpha = \sum_{j=0}^{3} x_j \alpha_j \to \sum_{j=0}^{3} x_j \beta_j = \beta; \text{ sei } \alpha' \text{ ein weiteres Element in } \mathfrak{o}_i$$

$$\alpha' = \sum_j x'_j \alpha_j \to \sum_j x'_j \beta_j = \beta'$$

$$\alpha + \alpha' = \sum_j (x_j + x'_j) \alpha_j \to \sum_j (x_j + x'_j) \beta_j = \beta + \beta'$$

$$\alpha\alpha' = \sum_j x_j\alpha_j \sum_l x'_l\alpha_l = \sum_{s,j,l=0}^{3} a_{sjl}x_j x'_l\alpha_s \to$$
$$\sum_{s,j,l=0}^{3} a_{sjl}x_j x'_l\beta_s = \sum_{j,l=0}^{3} \beta_j\beta_l x_j x'_l = \sum_j x_j\beta_j \sum_l x'_l\beta_l = \beta\beta'$$
$$k\alpha = \sum_{j=0}^{3}(k x_j)\alpha_j \to \sum_{j=0}^{3}(k x_j)\beta_j = k\sum_{j=0}^{3} x_j\beta_j = k\beta \quad (k \text{ rational}).$$

Der Isomorphismus $\mathfrak{o}_i \approx \mathfrak{o}_k$ läßt sich zu einem solchen der ganzen Quaternionenalgebra fortsetzen, indem man die $x_j$ den rationalen Zahlkörper durchlaufen läßt. Jetzt wenden wir den 1. Hauptsatz der Schiefkörpertheorie an.

**Satz** (VAN DER WAERDEN, Algebra II, 3. Auflage, Seite 202): *Sind $\Sigma_1$ und $\Sigma_2$ zwei zueinander isomorphe, einfache Teilsysteme des normalen einfachen hyperkomplexen Systems $K_r$, so wird jeder Isomorphismus zwischen $\Sigma_1$ und $\Sigma_2$, der die Elemente des Grundkörpers fest läßt, durch einen innern Automorphismus vermittelt. Insbesondere gilt der Satz für $\Sigma_1 = \Sigma_2 = K_r$.*

Somit bedeutet $\alpha_j \to \beta_j$ eine Gleichung $\alpha_j = \varrho\beta_j\varrho^{-1}$

$$\mathfrak{o}_i = \varrho\mathfrak{o}_k\varrho^{-1}, \qquad (n(\varrho) \neq 0),$$

welche Gleichung aber die im Hilfssatz 3 behauptete Äquivalenz $\mathfrak{o}_i \sim \mathfrak{o}_k$ offenbar macht.

**Bemerkung.** Die Quaternionenringe sind einfache Algebren. Denn die nullteilerfreien rationalen Quaternionenalgebren sind Divisionsalgebren, das heißt Schiefkörper (siehe [8], Seite 47), welche ja nur die beiden trivialen Ideale haben. Die Quaternionenalgebra *mit* Nullteilern ist die vollständige Matrixalgebra der Matrizen $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ im rationalen Körper, also ebenfalls einfach.

Beim Beweis des Satzes am Anfang dieser Nummer können wir $\mathfrak{a}$ und $\mathfrak{b}$ durch beliebige zu ihnen äquivalente Ideale ersetzen. Sei jetzt mit den Linksordnungen

$$\begin{array}{lcl} \mathfrak{o}_1\mathfrak{a} = \mathfrak{a} & \text{und} & \mathfrak{o}'_1\mathfrak{b} = \mathfrak{b} \\ HA = A & & HA = A, \end{array}$$

darunter steht die entsprechende Komposition der Normenformklassen; die Hauptklasse $H$ ist in beiden Gleichungen dieselbe, weil in der Kompositionstheorie die linke Hauptklasse eindeutig bestimmt ist (Nr. 8, Satz 1). Daher sind nach Hilfssatz 1 $\mathfrak{o}_1$ und $\mathfrak{o}'_1$ äquivalent, und der Beweis dieses Hilfssatzes lehrt, daß mit einem gewissen $\varrho$ gesetzt werden kann $\mathfrak{o}_1 = \varrho\mathfrak{o}'_1\varrho^{-1}$. Genau gleich erhält man aus $\mathfrak{a}\mathfrak{o}_2 = \mathfrak{a}$, $\mathfrak{b}\mathfrak{o}'_2 = \mathfrak{b}$ die Beziehung $\mathfrak{o}_2 = \sigma\mathfrak{o}'_2\sigma^{-1}$ mit einem gewissen $\sigma$.

Wir verwenden die Tatsache, daß bei beliebig vorgegebenen, ganzen oder gebrochenen Idealen (oder allgemeiner bei beliebigen Moduln) $\mathfrak{c}$ und $\mathfrak{d}$ das

Ideal $\mathfrak{c}$ mit einer ganzen rationalen Zahl $s$ multipliziert werden kann, so daß die Beziehung gilt $s\mathfrak{c} \subseteqq \mathfrak{d}$.

Ist nämlich $\mathfrak{c} = (\gamma_0, \ldots, \gamma_3)$, $\mathfrak{d} = (\delta_0, \ldots, \delta_3)$, so wird $\gamma_\nu = \sum_{k=0}^{3} d_{\nu k}\delta_k$, $d_{\nu k}$ rational. Ist $s$ der Generalnenner der $d_{\nu k}$, so wird $s\gamma_\nu = \sum_{k=0}^{3} (sd_{\nu k})\delta_k$ mit $sd_{\nu k}$ ganz rational, woraus die Behauptung folgt.

Ist nun in der weiter oben erwähnten Beziehung $\mathfrak{o}_1 = \varrho\mathfrak{o}_1'\varrho^{-1}$ etwa $n(\varrho) > 0$, dann betrachten wir statt $\mathfrak{b}$ das äquivalente Ideal $\varrho\mathfrak{b}$. Es hat die Linksmaximalordnung $\varrho\mathfrak{o}_1'\varrho^{-1} = \mathfrak{o}_1$; denn $\varrho\mathfrak{o}_1'\varrho^{-1}\varrho\mathfrak{b} = \varrho\mathfrak{b}$. Sei mit einem ganzrationalen $s$ die Beziehung $s\mathfrak{a} \subseteqq \varrho\mathfrak{b}$ erfüllt. Da $s\mathfrak{a}$ und $\varrho\mathfrak{b}$ dieselbe Linksordnung $\mathfrak{o}_1$ besitzen, so existiert nach Hilfssatz 1 dieser Nummer ein *ganzes* Ideal $\mathfrak{m}$, so daß $s\mathfrak{a} = \varrho\mathfrak{b}\mathfrak{m}$, woraus für die Normenformklassen die Beziehung $A = AH'$ folgt, dies weil die Normenform von $s\mathfrak{a}$ eine Form $A'((x))$ der zu $\mathfrak{a}$ gehörigen Formenklasse $A$ ist, ebenso $A''((x))$, die Normenform von $\varrho\mathfrak{b}$, die nach Voraussetzung derselben Klasse $A$ angehört. Ist noch $H'((x))$ die Normenform von $\mathfrak{m}$, so hat man die der Idealgleichung entsprechende Formenkomposition $A'((z)) = A''((x))H'((y))$, oder bei Übergang zu den Klassen die Klassenkomposition $A = AH'$, wo $H'$ die eindeutig bestimmte Rechtshauptklasse von $A$ ist. $\mathfrak{m}$ ist somit ein Ideal, dessen Normenform Hauptform ist. Hilfssatz 2 lehrt daher, daß $\mathfrak{m}$ ein Hauptideal ist, der Beweis dieses Hilfssatzes zeigt, daß $\mathfrak{m}$ in der Form $\mathfrak{m} = \mathfrak{o}_2'\tau$ mit $n(\tau) > 0$ geschrieben werden kann. Somit wird $s\mathfrak{a} = \varrho\mathfrak{b}\tau$, $n(\varrho\tau) > 0$, $\mathfrak{a}$ selber wird $\mathfrak{a} = \frac{\varrho}{s}\mathfrak{b}\tau$, also $\underline{\mathfrak{a} \sim \mathfrak{b}}$. Ist (statt $n(\varrho) > 0$) $n(\sigma) > 0$, so folgt ebenso $\mathfrak{a} \sim \mathfrak{b}$.

Ist sowohl $n(\varrho) < 0$ als auch $n(\sigma) < 0$, dann nehmen wir das Ideal $\mathfrak{b}' = \varrho\mathfrak{b}\sigma^{-1} \sim \mathfrak{b}$, da $n(\varrho\sigma^{-1}) > 0$. Dann hat $\mathfrak{b}'$ dieselben Links- und Rechtsordnungen $\mathfrak{o}_1 = \varrho\mathfrak{o}_1'\varrho^{-1}$ und $\mathfrak{o}_2 = \sigma\mathfrak{o}_2'\sigma^{-1}$ wie $\mathfrak{a}$. Ist wieder $s\mathfrak{a} \subseteqq \mathfrak{b}'$ mit einem ganzrationalen $s$, so existiert $\mathfrak{n}$ ganz mit $s\mathfrak{a} = \mathfrak{n}\mathfrak{b}'$ (nach Hilfssatz 1). Ähnlich wie vorhin erhalten wir für die Normenformklassen die Komposition $A = HA$, wo die Normenformklasse von $\mathfrak{n}$ die eindeutig bestimmte Linkshauptklasse von $A$ sein muß. $\mathfrak{n}$ ist somit wie vorher ein Hauptideal, darstellbar als $\mathfrak{n} = \mu\mathfrak{o}_1$, $n(\mu) > 0$. Es ist also $s\mathfrak{a} = \mu\mathfrak{b}'$, und $\underline{\mathfrak{a} \sim \mathfrak{b}' \sim \mathfrak{b}}$. Somit gehören tatsächlich zu äquivalenten Normenformen äquivalente Ideale.

## 27. Hat die Algebra $\mathfrak{A}$ Normenstammformen der Diskriminante $D = d^2$, dann sind alle Stammformen der Diskriminante $d^2$ Normenformen einer Idealklasse der Quaternionenalgebra

Die Stammformen mit einer gegebenen quadratischen Diskriminante bilden ein einziges Geschlecht ([3], Seiten 11/12), sie sind also rational ineinander transformierbar. Sei $G((x))$ Normenstammform des Ideals $\mathfrak{a} = (\alpha_0, \ldots)$ in $\mathfrak{A}$, also $n(\sum_{i=0}^{3} x_i \alpha_i) = n(\mathfrak{a}) G((x))$. Geht dann $G((x))$ über in die beliebige Stammform $F((y))$ der Diskriminante $d^2$ mittels der rationalen Transformation $x = Ty$, $|T| = \pm 1$, so geht nach Nr. 11 der durch $\beta = T'\alpha$ definierte Modul $\mathfrak{b} = (\beta_0, \ldots)$ über in $(\alpha_0, \ldots)$. Der Modul $\mathfrak{b}$ ist ein Ideal, weil seine Normenform Stammform ist (siehe Nr. 19). Somit ist $n(\sum_{i=0}^{3} y_i \beta_i) = n(\mathfrak{b}) F((y))$, und $F((y))$ ist Normenform des Ideals $\mathfrak{b}$.

## 28. Der Hauptsatz der Zuordnung

*Sowohl die Idealklassen einer Quaternionenalgebra, als auch die Stammformenklassen der gleichen Diskriminante $D = d^2$ bilden je ein endliches Gruppoid. Diese beiden Gruppoide lassen sich gruppoidisomorph aufeinander beziehen.*

## 29. Über die Notwendigkeit, bei der Äquivalenzdefinition der Ideale die Forderung $n(\varrho\sigma) > 0$ zu stellen

Sei jetzt für die Ideale $\mathfrak{a}$ und $\mathfrak{b}$ die Relation $\mathfrak{b} = \varrho \mathfrak{a} \sigma$ mit $n(\varrho\sigma) < 0$ gültig. Ist $\mathfrak{a} = (\alpha_0, \ldots)$, so gilt $n(\sum_{i=0}^{3} x_i \alpha_i) = n(\mathfrak{a}) F_{\mathfrak{a}}((x))$, also $\mathfrak{a} \leftrightarrow F_{\mathfrak{a}}((x))$. Dem Ideal $\mathfrak{b}$ ist aber $-F_{\mathfrak{a}}((x))$ als Normenform zugeordnet, denn $\mathfrak{b}$ ist gleich $(\varrho\alpha_0\sigma, \ldots, \varrho\alpha_3\sigma)$, deshalb wird

$$n(\sum_{i=0}^{3} \varrho\alpha_i\sigma) = n(\varrho\sigma) n(\mathfrak{a}) F_{\mathfrak{a}}((x)) = |n(\varrho\sigma)|\, n(\mathfrak{a}) \,(-F_{\mathfrak{a}}((x)))\,,$$

somit $\mathfrak{b} = \varrho\mathfrak{a}\sigma \leftrightarrow -F_{\mathfrak{a}}((x))$.

**Bemerkung.** Daß hier $(\varrho\alpha_0\sigma, \ldots)$ als Basis von $\varrho\mathfrak{a}\sigma$ angenommen wurde, ist legitim. Wir sehen nämlich, daß ihre Basismatrix positive Determinante hat. Zu zeigen ist bloß, daß, wenn $(\alpha_0, \ldots)$ eine Basis ist, auch $(\varrho\alpha_0, \varrho\alpha_1, \ldots)$ positive Determinante besitzt. Nach Voraussetzung ist in $\alpha_j = \sum_{k=0}^{3} A_{jk}\omega_k$ die Determinante $|A_{jk}|$ positiv, unter $(\omega)$ die Basis des Grundideals verstanden. Sei $\varrho = \sum_{i=0}^{3} r_i \omega_i$, $\varrho\omega_k = \sum_{i,l=0}^{3} r_i w_{lik} \omega_l$, so ist $\varrho\alpha_j = \sum_{k=0}^{3} A_{jk} \varrho\omega_k = \sum_{i,k,l=0}^{3} A_{jk} r_i w_{lik} \omega_l$; daraus erhält man die Determinante der Basismatrix von $(\varrho\alpha_0, \ldots)$ zu $|A_{jk}|\,|\sum_{i=0}^{3} w_{lik} r_i| = |A_{jk}|\, G^2((r)) \underline{> 0}$, wo $G$ die Normenform des Grundideals ist (siehe Nr. 23). Ebenso ist die Determinante der Basismatrix von

$(\alpha_0 \varrho, \ldots, \alpha_3 \varrho)$ positiv. Offenbar ist dies eine Folge der Forderung, daß die Bilinearsubstitutionen positive Signatur haben sollen.

Das Ideal $\mathfrak{b}$ ist dann und nur dann trotzdem äquivalent $\mathfrak{a}$, obwohl nur eine Relation $\mathfrak{b} = \varrho \mathfrak{a} \sigma$ mit $n(\varrho \sigma) < 0$ vorliegt, wenn gilt $F_{\mathfrak{a}}((x)) \sim - F_{\mathfrak{a}}((x))$, dies besagt ja gerade der Isomorphiehauptsatz. Dann, wenn diese Beziehung $F_{\mathfrak{a}} \sim - F_{\mathfrak{a}}$ stattfindet, können wir zeigen, daß auch für jede beliebige Normenstammform $G$ dieser Algebra gilt $G \sim - G$.

Sei $(G)$ die Klasse der Form $G$. Wir zeigen zunächst für alle Hauptklassen, daß sie ihrer «negativen» Klasse äquivalent sind. Ist $(H)$ die linke Hauptklasse von $F_{\mathfrak{a}}$, dann gilt $(H)(F_{\mathfrak{a}}) = (F_{\mathfrak{a}})$. Wenn $L, M, N$ quaternäre Formen sind, und eine Komposition $LM = N$ existiert, so existieren auch die Kompositionen $-LM = -N$ und $L(-M) = -N$, denn dieselbe Bilinearsubstitution, die die erste Komposition vermittelt, bewirkt auch die beiden andern Transformationen, deren Bilinearsubstitution also ebenfalls positive Art und Signatur haben. Diese Ausführungen gelten auch für die Komposition der Klassen. – Deshalb gilt ebenfalls $(-H)(F_{\mathfrak{a}}) = (-F_{\mathfrak{a}})$; ist, wie vorausgesetzt, $(F_{\mathfrak{a}}) = (-F_{\mathfrak{a}})$, so hat man $(-H)(F_{\mathfrak{a}}) = (F_{\mathfrak{a}})$, somit wegen der Eindeutigkeit der linken Hauptklasse $(-H) = (H)$. Ist $(H')$ eine beliebige andere Hauptklasse, so existiert eine Klasse $(L)$ mit $(H)$ als Links-, $(H')$ als Rechtshauptklasse. (Dies ist eine Gruppoideigenschaft, siehe Axiom IV, Nr. 14.)

Dann ist $(H)(L) = (L)$, $(L)(H') = (L)$. Da $(-H)(L) = (-L)$ und $(-H) = (H)$, so ist $(H)(L) = \underline{(-L) = (L)}$, und somit $(L)(-H') = (-L) = (L)$, das heißt $(H') = (-H')$, die unterstrichene Relation zeigt, daß überhaupt alle Normenformklassen der Algebra ihrer «negativen» äquivalent sind, nachdem dies für die Hauptklassen bewiesen worden ist.

Nennen wir Algebren mit indefiniten Normenformen indefinite Quaternionenalgebren, dann kann man sagen, daß in gewissen indefiniten Algebren die Normenformen ihrem Negativen äquivalent sind. Wenn wir die Maximalordnungen solcher Algebren betrachten, dann ist wie immer deren Normenform eine Hauptform. Da $(-H) = (H)$, so stellt eine solche Hauptform $-1$ ganzzahlig dar, was bedeutet, daß es in diesen Algebren Einheiten der Norm $-1$ gibt. Und zwar gibt es dann solche in allen Maximalordnungen. Umgekehrt, gibt es in der Algebra eine Einheit der Norm $-1$, und betrachten wir eine Maximalordnung, der diese Einheit angehört, dann ist deren Normenform eine Hauptform, welche $-1$ darstellt, somit ist $(H) = (-H)$ (siehe Nr. 5) für diese Form, welche Beziehung also für alle Normenformen gilt, wie oben gezeigt.

Bezeichnen wir zwei Ideale $\mathfrak{a}$ und $\varrho \mathfrak{a} \sigma$ äquivalent, wenn $n(\varrho \sigma) \neq 0$, dann erhalten wir eine Klasseneinteilung mit $h_0$ Klassen. Fordern wir schärfer, wie wir das auch getan haben, $n(\varrho \sigma) > 0$, dann erhalten wir die Klassenzahl $h$.

Bei Anwendung der schärferen Definition mit $n(\varrho\sigma) > 0$ gehören zwei Ideale $\mathfrak{a}$ und $\lambda\mathfrak{a}\mu$ noch zu zwei verschiedenen Klassen, wenn $n(\lambda\mu) < 0$ und die indefinite Algebra keine Einheiten der Norm $-1$ enthält. In diesem Fall ist $h = 2h_0$. Enthält die indefinite Algebra aber Einheiten der Norm $-1$, oder handelt es sich um eine definite Algebra (mit positiven Normenformen), so ist stets $h = h_0$.

Würde man die schärfere Forderung $n(\varrho\sigma) > 0$ nicht stellen, dann verlöre der Isomorphiesatz bei den indefiniten Quaternionenalgebren ohne Einheiten der Norm $-1$ seine Gültigkeit, weil hier die Abbildung der Idealklassen auf die Normenformklassen nicht mehr eindeutig wäre.

## LITERATUR

### Zeitschriften

[1] H. Brandt, *Der Kompositionsbegriff bei den quaternären quadratischen Formen*, Math. Ann. *91*, 1924, S. 300–315.

[2] H. Brandt, *Die Hauptklassen in der Kompositionstheorie der quaternären quadratischen Formen*, Math. Ann. *94*, 1925, S. 166–175.
*Über die Komponierbarkeit der quaternären quadratischen Formen*, S. 179–197.

[3] H. Brandt, *Idealtheorie in Quaternionenalgebren*, Math. Ann. *99*, 1928, S. 1–29.

[4] H. Brandt, *Über ein Problem von A. Hurwitz, quaternäre quadratische Formen betreffend*, Math. Ann. *88*, 1923, S. 211–214.

[5] H. Brandt, *Bilineare Transformation quadratischer Formen*, Math. Z. *17*, 1923, S. 153–160.

[6] H. Brandt, *Bilineare Transformation quadratischer Formen*, Math. Z. *20*, 1924, S. 223–230.

[7] H. Brandt, *Zur Komposition der quaternären, quadratischen Formen*, Journal f. reine u. angewandte Math. *143*, 1913, S. 106–129.

### Bücher

[8] L. E. Dickson, *Algebren und ihre Zahlentheorie*, Zürich 1927.

[9] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, 2. Aufl., Leipzig 1954.

[10] L. E. Dickson, *Einführung in die Zahlentheorie*, Berlin 1931, übersetzt durch Bodewig.

[11] M. Deuring, *Algebren, Ergebnisse der Mathematik $IV_1$*, Berlin 1935.

(Eingegangen den 30. August 1958)