Werk

Titel: Mathematische Annalen
Jahr: 1928
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN235181684_0099
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235181684_0099

LOG Id: LOG_0004
LOG Titel: Idealtheorie in Quaternionenalgebren
LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN235181684
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235181684
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=235181684

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Idealtheorie in Quaternionenalgebren.

Von

H. Brandt in Aachen.

Einleitung.

1. Meine Untersuchungen über die Komposition der quaternären quadratischen Formen[1]) haben mich zu einer allgemeinen Idealtheorie der *rationalen Dedekindschen Algebren*[2]) geführt, die, wie schon die ersten grundlegenden Sätze zeigen, an Schönheit der Idealtheorie algebraischer Zahlkörper kaum nachsteht. An Stelle des hier geltenden Satzes: „Alle Ideale bilden in bezug auf die Multiplikation eine unendliche Gruppe und lassen sich auf Grund einer Äquivalenzdefinition in Klassen einteilen, welche eine endliche Gruppe bilden" tritt einfach ein allgemeiner, diesen als Spezialfall enthaltender Satz, der sich mit Hilfe des von mir durch Verallgemeinerung des Gruppenbegriffes gewonnenen Gruppoidbegriffes[3]) sehr einfach formulieren läßt und so lautet: *„Alle Ideale bilden in bezug auf die Multiplikation ein unendliches Gruppoid und lassen sich auf Grund einer Äquivalenzdefinition in Klassen einteilen, die ein endliches Gruppoid bilden."*

[1]) Hier kommen namentlich die folgenden Arbeiten in Betracht:

I. Zur Komposition der quaternären quadratischen Formen (Dissertation, Straßburg 1912), Journal für reine und angewandte Mathematik **143** (1913), S. 106.

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

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

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

[2]) Dedekindsche Algebra = Algebra ohne Radikal, in Anlehnung an die Frobeniussche Bezeichnung Dedekindsche Gruppe. Vgl. Frobenius, Theorie der hyperkomplexen Größen, Sitzungsberichte der Berliner Akademie 1903, S. 509.

[3]) Über eine Verallgemeinerung des Gruppenbegriffes, Math. Annalen **96** (1926), S. 360.

Wir geben hier den Beweis dieses Satzes für diejenigen aus Quaternionen gebildeten Algebren, welche der Kompositionstheorie der ganzzahligen quaternären quadratischen Formen in ähnlicher Weise entsprechen wie die algebraischen Zahlkörper einer Kompositionstheorie der zerlegbaren Formen mit ganzzahligen Koeffizienten[4]). (Der allgemeine Beweis folgt in Kürze.)

2. Schon Hurwitz hat die einfachste derartige Algebra zahlentheoretisch behandelt[5]), doch findet sich bei ihm noch nicht die geringste Andeutung für diesen Satz. Unsere Betrachtungen stehen daher auch mit den seinigen kaum in Zusammenhang. Sie sind in ihrem Gegenstand viel umfassender und verfolgen auch ganz andere Ziele. Das soll hier kurz an dem Hurwitzschen Beispiel dargelegt werden.

Die Hurwitzsche Algebra besteht aus allen Hamiltonschen Quaternionen mit rationalen Komponenten. Hurwitz bestimmt für diese Algebra einen größten Integritätsbereich, ohne nach den andern möglichen größten Integritätsbereichen zu fragen[6]). Sind $\iota_0 = 1, \iota_1, \iota_2, \iota_3$ die Hamiltonschen Basiseinheiten der Quaternionen, so ist der Hurwitzsche Integritätsbereich durch die Basis $\frac{1}{2}(1 + \iota_1 + \iota_2 + \iota_3), \iota_1, \iota_2, \iota_3$ festgelegt.

Unterwirft man aber $\iota_1, \iota_2, \iota_3$ einer rationalen eigentlichen ternären orthogonalen Transformation, so kann man aus den transformierten Basiseinheiten $\iota_1', \iota_2', \iota_3'$ in derselben Weise einen Integritätsbereich konstruieren. Man sieht auch leicht, daß man auf diese Weise alle möglichen größten Integritätsbereiche der Algebra erhält. Scheinbar ist es nun unnötig, diese neuen Integritätsbereiche, die offenbar in unendlicher Anzahl vorhanden sind, neben dem Hurwitzschen Bereich in Betracht zu ziehen, weil die Produktrelationen zwischen den neuen Basiseinheiten vollständig mit den Produktrelationen zwischen den alten übereinstimmen. Deshalb können alle möglichen größten Integritätsbereiche einander isomorph zugeordnet werden, und es ist daher völlig gleichgültig, welchen von diesen Bereichen man betrachtet, sobald man nur einen für sich allein nimmt.

3. Man wird aber in ganz natürlicher Weise dazu geführt, diese Integritätsbereiche, die auch als Einheitsideale aufgefaßt werden können,

[4]) Über die Resultate dieser Arbeit habe ich bereits am 30. August 1926 in Freiburg (Schweiz) auf der Tagung der Schweizer Mathematischen Gesellschaft vorgetragen. Vgl. Verhandlungen der Schweizerischen Naturforschenden Gesellschaft 1926, II. Teil, S. 155, oder L'Enseignement Mathématique 25 (1926), S. 290.

[5]) A. Hurwitz, Zahlentheorie der Quaternionen, Nachrichten der Gesellschaft der Wissenschaften Göttingen 1896 und Vorlesungen über die Zahlentheorie der Quaternionen. Berlin 1919.

[6]) Vgl. auch L. E. Dickson, Algebras and their Arithmetics, Chicago 1923, S. 148, oder zweite Auflage in deutscher Sprache, herausgegeben von A. Speiser, Algebren und ihre Zahlentheorie, Zürich 1927, S. 157.

sämtlich gleichzeitig nebeneinander zu betrachten. Das zeigen die folgenden Erörterungen, denen wir der kürzeren und klareren Ausdrucksweise wegen noch einige Bezeichnungen vorausschicken.

Ist $\mathfrak{e}$ einer von diesen Integritätsbereichen und werden alle Quaternionen aus $\mathfrak{e}$ durch $\varepsilon, \varepsilon_1, \ldots$ bezeichnet, so nennen wir ein System $\mathfrak{a}$ von Quaternionen $\alpha, \alpha_1, \ldots$ der Algebra ein *Rechtsideal* von $\mathfrak{e}$ und ein System $\mathfrak{b}$ von Quaternionen $\beta, \beta_1, \ldots$ der Algebra ein *Linksideal von* $\mathfrak{e}$, wenn $\mathfrak{a}$ mit $\alpha, \alpha_1, \ldots$ auch $\alpha\varepsilon, \alpha_1\varepsilon_1, \alpha\varepsilon + \alpha_1\varepsilon_1, \ldots$ und $\mathfrak{b}$ mit $\beta, \beta_1, \ldots$ auch $\varepsilon\beta, \varepsilon_1\beta_1, \varepsilon\beta + \varepsilon_1\beta_1, \ldots$ enthält [7]). Wir schreiben dann $\mathfrak{a}\,\mathfrak{e} = \mathfrak{a}$ und $\mathfrak{e}\,\mathfrak{b} = \mathfrak{b}$ und bezeichnen $\mathfrak{e}$ als *rechtes Einheitsideal von* $\mathfrak{a}$ und als *linkes Einheitsideal von* $\mathfrak{b}$. Die Gesamtheit der Quaternionen $\alpha\beta, \alpha_1\beta_1, \alpha\beta + \alpha_1\beta_1, \ldots$, wo also die Quaternionen des Rechtsideals $\mathfrak{a}$ den ersten und die Quaternionen des Linksideals $\mathfrak{b}$ den zweiten Faktor bilden, werde durch $\mathfrak{a}\,\mathfrak{b}$ bezeichnet und *Idealprodukt von* $\mathfrak{e}$ genannt. Wegen $\mathfrak{a} = \mathfrak{a}\,\mathfrak{e}$ und $\mathfrak{b} = \mathfrak{e}\,\mathfrak{b}$ ist jedes Rechtsideal von $\mathfrak{e}$ und jedes Linksideal von $\mathfrak{e}$ gleichzeitig auch Idealprodukt von $\mathfrak{e}$.

4. Dann gelten folgende Sätze, deren Beweis wir hier übergehen (vgl. dazu Kap. IV): Jedes Rechtsideal $\mathfrak{a}$ von $\mathfrak{e}$ ist gleichzeitig auch Linksideal für einen im allgemeinen von $\mathfrak{e}$ verschiedenen Integritätsbereich $\mathfrak{e}'$, so daß $\mathfrak{e}'\,\mathfrak{a} = \mathfrak{a}$, und jedes Linksideal $\mathfrak{b}$ von $\mathfrak{e}$ ist gleichzeitig auch Rechtsideal für einen im allgemeinen von $\mathfrak{e}, \mathfrak{e}'$ verschiedenen Integritätsbereich $\mathfrak{e}''$, so daß $\mathfrak{b}\,\mathfrak{e}'' = \mathfrak{b}$. Jedes Idealprodukt $\mathfrak{a}\,\mathfrak{b}$ von $\mathfrak{e}$ ist gleichzeitig auch für jeden andern Integritätsbereich ein Idealprodukt und dabei gerade für einen selbst ein Rechtsideal und gerade für einen selbst ein Linksideal.

Die Menge der Rechtsideale für alle Integritätsbereiche, die Menge der Linksideale für alle Integritätsbereiche und die Menge der Idealprodukte für einen bestimmten Integritätsbereich sind daher miteinander identisch.

5. Da es danach nur eine Frage der Auffassung ist, ob ein System von Quaternionen als Rechtsideal oder als Linksideal oder als Idealprodukt angesehen wird, so scheint es angemessen, von Idealen schlechthin zu sprechen. Die Multiplikation der Ideale zeigt dann ganz gruppenähnliche Eigenschaften, ist aber an die einschränkende Bedingung geknüpft: Für zwei Ideale $\mathfrak{a}, \mathfrak{b}$ existiert das Produkt $\mathfrak{a}\,\mathfrak{b}$ dann und nur dann, wenn das rechte Einheitsideal von $\mathfrak{a}$ zugleich linkes Einheitsideal von $\mathfrak{b}$ ist. Den präzisen Ausdruck für die Gesetzmäßigkeit in der multiplikativen Verknüpfung der Ideale gibt der Satz: Die Ideale bilden in bezug auf die Multiplikation ein unendliches Gruppoid.

---

[7]) In derselben Weise werden die Rechts- und Linksideale auch von Herrn Speiser definiert [Allgemeine Zahlentheorie, Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich 71 (1926) = [6]) zweite Auflage, Kap. XIII], während bei Hurwitz die Bezeichnungen vertauscht sind.

6. Wir beschränken uns bei den folgenden Betrachtungen nicht auf die Hurwitzsche Algebra, sondern fassen alle (in unendlicher Anzahl vorhandenen) Quaternionenalgebren ins Auge, welche dadurch charakterisiert werden können, daß sie ein *rationales Zentrum*[8]) besitzen. Auch hier gelten genau entsprechende Sätze (Kap. IV).

Die Untersuchung wird gekrönt durch das Ergebnis, daß man nach dem Vorbild der Idealtheorie in algebraischen Zahlkörpern eine Äquivalenzdefinition für unsere Ideale aufstellen kann, wodurch die sämtlichen Ideale sich auf Klassen verteilen, deren Anzahl sich als endlich erweist. Aus der Multiplikation der Ideale entsteht dann eine Komposition dieser Idealklassen. Dadurch werden diese in gesetzmäßiger Weise miteinander verknüpft und bilden dabei wiederum ein Gruppoid (Kap. V).

I. Grundbegriffe.

7. Wir bezeichnen gewöhnliche Größen (Zahlen) durch kleine lateinische Buchstaben. Da im folgenden algebraische Zahlen keine Verwendung finden, dürfen ganze rationale Zahlen kurz *ganze Zahlen* genannt werden. Quaternionen bezeichnen wir durch kleine griechische Buchstaben in der Form

$$\xi = x_0 + x_1 \iota_1 + x_2 \iota_2 + x_3 \iota_3 .$$

Dabei sind $\iota_0 = 1, \iota_1, \iota_2, \iota_3$ die bekannten *Hamiltonschen Basiseinheiten* und x_0, x_1, x_2, x_3 die *Komponenten des Quaternions* ξ.

Eine Komponente Null wird nicht hingeschrieben, die Quaternionen $\xi = x_0$, deren drei letzte Komponenten verschwinden, werden nicht von den Zahlen x_0 unterschieden.

8. Das Quaternion

$$\bar{\xi} = x_0 - x_1 \iota_1 - x_2 \iota_2 - x_3 \iota_3$$

wird nach Hurwitz *konjugiert* zu ξ genannt[5]). Offenbar ist auch ξ konjugiert zu $\bar{\xi}$.

Die Ausdrücke

$$\xi + \bar{\xi} = 2x_0 = s(\xi),$$
$$\xi\bar{\xi} = x_0^2 + x_1^2 + x_2^2 + x_3^2 = E((x)) = n(\xi)$$

werden als *Spur* und *Norm von* ξ bezeichnet. Das Quaternion ξ genügt der Gleichung

$$\xi^2 - s(\xi)\cdot\xi + n(\xi) = 0 .$$

Wenn $n(\xi) \neq 0$, so wird das Quaternion $\frac{\bar{\xi}}{n(\xi)}$ durch ξ^{-1} bezeichnet und *reziprok zu* ξ genannt. Offenbar ist ξ reziprok zu ξ^{-1}.

[8]) Siehe etwa [6]), erste Auflage, S. 31.

Wenn $\xi \neq 0$, aber $n(\xi) = 0$, so heißt ξ *Nullteiler*. Die Nullteiler ξ sind durch die Existenz nicht verschwindender Quaternionen η und ζ charakterisiert, für welche $\eta\xi = \xi\zeta = 0$. Dabei sind η, ζ natürlich selbst Nullteiler.

9. Ist neben $\xi = x_0 + x_1\iota_1 + x_2\iota_2 + x_3\iota_3$ ein zweites Quaternion $\eta = y_0 + y_1\iota_1 + y_2\iota_2 + y_3\iota_3$ gegeben, so wird der Ausdruck

$$\xi\bar{\eta} + \eta\bar{\xi} = \bar{\xi}\eta + \bar{\eta}\xi = 2(x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3) = n(\xi, \eta)$$

als *Zwischennorm von ξ und η* bezeichnet. Man findet

$$n(\xi, \eta) = s(\xi\bar{\eta}) = s(\bar{\xi}\eta), \qquad n(\xi, \xi) = 2n(\xi),$$
$$n(\xi, \xi\eta) = n(\xi, \eta\xi) = n(\xi)\, s(\eta).$$

Sind $\xi_\nu = \sum_k \iota_k x_{k\nu}$ [9]) irgend vier Quaternionen, so wird die aus den Zwischennormen gebildete Determinante

$$|n(\xi_i, \xi_k)| = 16\,|x_{ik}|^2 = \Delta(\xi_0, \xi_1, \xi_2, \xi_3)$$

Diskriminante der vier Quaternionen ξ_ν genannt. Δ ist dann und nur dann von Null verschieden, wenn die ξ_ν linear unabhängig sind.

10. Die Multiplikationsgleichungen

$$\iota_1^2 = -1, \quad \iota_2\iota_3 = -\iota_3\iota_2 = \iota_1 \quad \text{usw.}$$

fassen wir in der Formel

$$\iota_\mu\iota_\nu = \sum_k \iota_k v_{k\mu\nu}$$

zusammen. Die Komponenten z_ν des Produktes

$$\xi\eta = \zeta$$

erhält man also durch die Gleichungen

$$z_\nu = \sum_{ik} v_{\nu ik} x_i y_k.$$

Für sie wird identisch

$$n(\xi)\, n(\eta) = n(\zeta) \quad \text{oder} \quad E((x))\, E((y)) = E((z)).$$

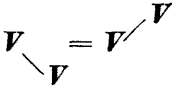
11. Das *assoziative Gesetz* der Quaternionenmultiplikation drückt sich durch die Formeln

$$\sum_i v_{\varkappa\lambda i} v_{i\mu\nu} = \sum_i v_{\varkappa i\nu} v_{i\lambda\mu}$$

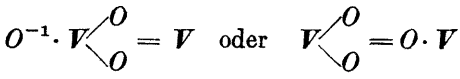
---

[9]) Σ bedeutet eine Summation über die Indizes 0, 1, 2, 3. Summationsindizes werden durch i, j, k, feste Indizes durch $\varkappa, \lambda, \mu, \nu$ bezeichnet.

aus, für die wir auch in einer leicht verständlichen, schon mehrfach benutzten Matrizensymbolik[10])



schreiben. Bedeutet O eine eigentliche orthogonale Substitution mit der ersten Spalte $1, 0, 0, 0$, sonst aber ganz beliebigen Koeffizienten, so geht die bilineare Substitution V in sich selbst über, wenn die x_ν, y_ν, z_ν gleichzeitig durch O transformiert werden, was wir durch die Formeln



zum Ausdruck bringen[11]).

12. Ein Quaternion wird *ganz* genannt, wenn seine Spur und seine Norm ganze Zahlen sind. Zwei ganze Quaternionen heißen *konkordant*, wenn ihre Zwischennorm ganz ist.

Wenn α und β ganze Quaternionen bezeichnen, so ist jedes der Quaternionen

$$\alpha + \beta,\ \alpha - \beta,\ \alpha\beta$$

dann und nur dann ganz, wenn α und $\bar{\beta}$ konkordant sind. Es ist nämlich

$$s(\alpha \pm \beta) = s(\alpha) \pm s(\beta), \qquad n(\alpha \pm \beta) = n(\alpha) + n(\beta) \pm n(\alpha, \beta),$$
$$s(\alpha\beta) = s(\alpha)\, s(\beta) - n(\alpha, \beta), \qquad n(\alpha\beta) = n(\alpha)\, n(\beta),$$

woraus die Behauptung folgt.

Weiter gilt: Wenn α und β ganze und konkordante Quaternionen bezeichnen, so sind alle Quaternionen, die aus den Quaternionen α, β oder auch aus $1, \alpha, \beta$ durch beliebig oft wiederholte Additionen, Subtraktionen und Multiplikationen hergeleitet werden können, ganz und konkordant mit α und β.

13. Ein System von unendlich vielen Quaternionen, in dem Addition, Subtraktion und Multiplikation unbeschränkt und die Division, soweit sie möglich ist, ausgeführt werden können, wird eine *Quaternionenalgebra* genannt. Enthält die Algebra keine Nullteiler, so heißt sie *Divisionsalgebra*[12]).

---

[10]) III, S. 168.

[11]) Die Richtigkeit der Behauptung ergibt sich leicht direkt durch Ausrechnen daraus, daß die zu O adjungierte Substitution O selbst ist. Vgl. auch IV, S. 192.

[12]) Hurwitz sagt Quaternionenkörper, ich habe selbst diesen Ausdruck in dem unter [4]) genannten Vortrag gebraucht; doch scheint es mir jetzt zweckmäßiger, den Ausdruck Körper auf Divisionsalgebren mit kommutativer Multiplikation zu beschränken.

Wir betrachten im folgenden solche Quaternionenalgebren $\mathfrak{Q}$, die nur Quaternionen mit rationalen Normen und Spuren, jedoch vier linear unabhängige Quaternionen enthalten.

Offenbar sind in einer Algebra $\mathfrak{Q}$ wegen

$$n(\alpha, \beta) = s(\alpha)\, s(\beta) - s(\alpha\beta)$$

auch alle Zwischennormen rational.

14. *Sind $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ irgend vier linear unabhängige Quaternionen aus $\mathfrak{Q}$ und ist α ein beliebiges Quaternion, für welches die Zwischennormen $n(\alpha, \alpha_\nu)$ rational sind, so liegt auch α in $\mathfrak{Q}$.*

Wegen der linearen Unabhängigkeit der α_ν gibt es jedenfalls eindeutig bestimmte Zahlen k_ν, so daß

$$\alpha = k_0\alpha_0 + k_1\alpha_1 + k_2\alpha_2 + k_3\alpha_3.$$

Hier sind aber die k_ν rational; denn sie ergeben sich durch Auflösen der vier linearen Gleichungen

$$n(\alpha_0, \alpha_\nu)k_0 + n(\alpha_1, \alpha_\nu)k_1 + n(\alpha_2, \alpha_\nu)k_2 + n(\alpha_3, \alpha_\nu)k_3 = n(\alpha, \alpha_\nu),$$

deren Koeffizienten rational sind und deren Determinante

$$|n(\alpha_i, \alpha_k)| = \Delta(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$$

nicht verschwindet.

Nimmt man α rational an, so zeigt sich, daß in $\mathfrak{Q}$ alle rationalen Zahlen (im besonderen also auch die Zahl 1) vorkommen.

15. Nach dem Vorhergehenden bilden irgend vier linear unabhängige Quaternionen α_ν aus $\mathfrak{Q}$ eine *Basis*, d. h. $\mathfrak{Q}$ enthält alle und nur die Quaternionen von der Form

$$\xi = x_0\alpha_0 + x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3,$$

wo die x_ν rational sind. Die Quaternionen α_ν heißen *Basiselemente*, die x_ν *Koordinaten von ξ in bezug auf die Basis*.

Bildet man die Norm von ξ, wobei die x_ν als Variable angesehen werden, so erhält man eine quadratische Form, die wir die *Normenform der Basis* nennen. Die Diskriminante dieser Form ist zugleich die Diskriminante der vier Basiselemente und heißt deshalb auch *Diskriminante der Basis*[13]).

Die Koordinaten der Produkte der Basiselemente heißen die *Multiplikationszahlen der Basis*. Sie sind im allgemeinen gebrochen. Doch läßt sich eine Basis so wählen, daß sie ganz werden, z. B. dadurch, daß

[13]) Die allgemeine von Dedekind stammende Definition der Diskriminante liefert den -16-fachen Wert von unserer Diskriminante. Siehe etwa Speiser a. a. O. [7]), S. 20.

man die Basiselemente mit dem Generalnenner der Multiplikationszahlen multipliziert.

II. Minimalbasen.

16. *Eine Basis heißt Minimalbasis, wenn ihre Multiplikationszahlen ganz sind und ihre Diskriminante möglichst klein ist.*

Da aus der Ganzzahligkeit der Multiplikationszahlen, wie sich unten zeigen wird, auch die Ganzzahligkeit der Diskriminante folgt (20), so ist klar, daß es unter den Basen mit ganzen Multiplikationszahlen Minimalbasen geben muß.

Offenbar erhält man durch ganzzahlige unimodulare Transformation aus einer Minimalbasis ω_ν wieder eine Minimalbasis. Da jede Algebra $\mathfrak{Q}$ alle rationalen Zahlen enthält (14), läßt sich die neue Basis ω'_ν so wählen, daß $\omega'_0 = r$ eine positive rationale Zahl wird. Wegen der Ganzzahligkeit der Multiplikationszahlen der ω'_ν muß r ganz sein, wegen der Minimalbedingung für die Diskriminante kann dann r aber nur den Wert 1 haben.

Eine Minimalbasis ω_ν, bei der $\omega_0 = 1$ ist, wird *reduziert* genannt.

17. Für eine beliebige Minimalbasis ω_ν setzen wir

$$\omega_\nu = \sum_k \iota_k t_{k\nu},$$

$$\omega = \omega(x) = x_0\omega_0 + x_1\omega_1 + x_2\omega_2 + x_3\omega_3,$$

und bezeichnen die Normenform durch

$$n(\omega) = \sum_j \sum_{ik} t_{ji} t_{jk} x_i x_k = \frac{1}{2} \sum_{ik} g_{ik} x_i x_k = G((x)).$$

Die Koordinaten der Zahl 1, die nach dem vorigen ganze teilerfremde Zahlen sind, bezeichnen wir durch e_ν, so daß

$$1 = e_0\omega_0 + e_1\omega_1 + e_2\omega_2 + e_3\omega_3.$$

Für die Spur von ω gilt dann

$$s(\omega) = n(1, \omega) = \sum_{ik} g_{ik} e_i x_k.$$

18. Die Multiplikationszahlen seien $w_{\lambda\mu\nu}$, so daß

$$\omega_\mu \omega_\nu = \sum_i \omega_i w_{i\mu\nu}.$$

Die drei aus den $w_{\lambda\mu\nu}$ gebildeten Matrizen aus Linearformen bezeichnen wir durch

$$\| \sum_j w_{ijk} x_j \| = \Omega(x), \qquad \| \sum_j w_{ikj} y_j \| = \Omega'(y), \qquad \| \sum w_{jik} z_j \| = \Omega''(z).$$

Durch die Substitution $T = \| t_{ik} \|$, wobei die $t_{\mu\nu}$ die eben eingeführten

Größen sind, stellt sich die bilineare Matrix W bei Benutzung der in 11 eingeführten Symbolik durch die Formel

$$W = T^{-1} \cdot V \begin{matrix} T \\ \diagdown \\ T \end{matrix}$$

dar.

19. Deshalb wird vermöge der bilinearen Substitution

$$z_\nu = \sum_{ik} w_{\nu ik} x_i y_k$$

identisch

$$G((x))\,G((y)) = G((z))$$

und

$$\left|\frac{\partial z_i}{\partial y_k}\right| = |\Omega(x)| = [G((x))]^2,$$

$$\left|\frac{\partial z_i}{\partial x_k}\right| = |\Omega'(y)| = [G((y))]^2,$$

$$|\Omega''(z)| = -[\mathfrak{G}((z))]^2,$$

wobei $\mathfrak{G}$ eine Form bezeichnet, die wir früher die *Reziproke von G* genannt haben[14]). Schreibt man

$$\mathfrak{G}((z)) = \frac{1}{2}\sum_{ik} \mathfrak{g}_{ik} z_i z_k$$

und

$$|g_{ik}| = |\mathfrak{g}_{ik}| = d^2,$$

so ist

$$\mathfrak{g}_{\mu\nu} = \frac{1}{d}\frac{\partial |g_{ik}|}{\partial g_{\mu\nu}}.$$

20. Weil die $w_{\lambda\mu\nu}$ ganz sind, müssen die Koeffizienten von G und $\mathfrak{G}$ ganz sein. Demnach ist auch d ganz. Wir wollen d mit positivem oder negativem Vorzeichen nehmen, je nachdem die Normenform eine definite oder indefinite Form ist[15]). Im ersten Fall kann dann G nur positiv sein, im zweiten Fall nur den Trägheitsindex 2 haben[16]). Die in dieser Weise bestimmte ganze Zahl d ist wegen der Definition der Minimalbasis unabhängig von der Auswahl der Minimalbasis. Sie wird die *Grundzahl der Algebra* genannt.

Die Diskriminante einer Minimalbasis, die wir auch *Diskriminante der Algebra* nennen und durch Δ bezeichnen, ist das Quadrat der Grundzahl.

Die Grundzahl kann nicht jeden beliebigen Wert haben, wie weiter unten näher angegeben wird (25).

Da die Normenform einer Minimalbasis die Zahl 1 darstellt, ist sie nach früherer Terminologie eine *Hauptform*, welche eine Komposition mit sich selbst zu sich selbst gestattet[17]).

---

[14]) I, S. 110 oder II, S. 302.

[15]) Vgl. II, S. 302. [16]) I, S. 118. [17]) I, S. 122 und II, S. 309.

21. Wenn $\omega_0 = 1$, die Minimalbasis also reduziert ist, hat die Normenform den ersten Koeffizienten $\frac{1}{2} g_{00} = 1$. Dann wird

$$s(\omega) = 2x_0 + g_{01} x_1 + g_{02} x_2 + g_{03} x_3,$$

deshalb sind die Koordinaten $\bar{x}_\nu$ von $\bar{\omega}$

$$\bar{x}_0 = x_0 + g_{01} x_1 + g_{02} x_2 + g_{03} x_3, \quad \bar{x}_1 = -x_1, \quad \bar{x}_2 = -x_2, \quad \bar{x}_3 = -x_3.$$

Sie werden also aus den Koordinaten x_ν von ω durch die Transformation

$$E_* = \begin{Vmatrix} 1 & g_{01} & g_{02} & g_{03} \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{Vmatrix}$$

erhalten. Wird

$$E_0 = \begin{Vmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{Vmatrix}$$

gesetzt, so wird

$$E_* = T^{-1} \cdot E_0 \cdot T,$$

wobei $T = \| t_{ik} \|$ die frühere Bedeutung hat (17), aber für eine reduzierte Basis die erste Spalte 1, 0, 0, 0 besitzt.

22. Im Fall der reduzierten Basis sind die Multiplikationszahlen merkwürdigerweise durch die Koeffizienten der Normenform und ihrer Reziproken schon vollständig bestimmt. Man findet nämlich nach Ausführung der Transformation unter 18 die von den $t_{\mu\nu}$ ganz unabhängigen, schon früher an anderer Stelle[18]) angegebenen Formeln

$$z_0 = x_0 y_0 - \frac{1}{2} \sum_{ik}{}' g_{ik} x_i y_k \pm \frac{1}{2} \sum_i{}' g_{0i} s_i,$$

$$z_\tau = \frac{1}{2} \sum_i g_{0i} (x_\tau y_i + x_i y_\tau) \pm \frac{1}{2} \sum_i{}' g_{\tau i} s_i \qquad (\tau = 1, 2, 3).$$

Dabei ist zur Abkürzung gesetzt

$$x_2 y_3 - x_3 y_2 = s_1, \quad x_3 y_1 - x_1 y_3 = s_2, \quad x_1 y_2 - x_2 y_1 = s_3,$$

und Σ' bezeichnet eine Summation über die Indizes 1, 2, 3. Hier gelten entweder die oberen oder die unteren Zeichen, und die Zeichen vertauschen sich, wenn die drei Variablenreihen x_ν, y_ν, z_ν gleichzeitig durch die Substitution E_* transformiert werden.

[18]) II, S. 308 oder 309.

Die Koeffizienten dieser bilinearen Substitution sind, wie früher gezeigt wurde, stets ganzzahlig, sobald $G = \frac{1}{2}\sum_{ik} g_{ik} x_i x_k$ eine Form mit einer ganzzahligen Reziproken $\mathfrak{G} = \frac{1}{2}\sum_{ik} \mathfrak{g}_{ik} x_i x_k$ und mit dem ersten Koeffizienten $\frac{1}{2} g_{00} = 1$ bezeichnet[19]).

23. Die Formen, welche als Normenformen einer beliebigen Basis auftreten können, sind dadurch ausgezeichnet, daß sie sich rational ineinander transformieren lassen und eine rationale Reziproke, also quadratische Diskriminante besitzen. Dabei kann auch jede Form, welche rational in eine von diesen Formen transformiert werden kann, selbst als Normenform auftreten.

Es muß daher unter den möglichen Normenformen auch Stammformen, d. h. solche Formen geben, welche nicht unter einer ganzzahligen Form mit kleinerer Diskriminante enthalten sind. Wie eine einfache Diskussion zeigt, sind solche Formen von zweiter Art[20]) und besitzen eine ganzzahlige Reziproke. Außerdem gehören sie einem bestimmten Geschlecht an, das wir *Stammgeschlecht* nennen können, da es nur Stammformen enthält. Entsteht aus einer Stammform durch rationale unimodulare Transformation eine ganzzahlige Form, so ist diese auch Stammform.

Hieraus ergeben sich in Verbindung mit der am Schlusse der vorigen Nummer gemachten Bemerkung die folgenden Sätze:

Eine Basis ist dann und nur dann eine Minimalbasis, wenn die Normenform eine Stammform ist und die Koordinaten der Zahl 1 *ganz sind.*

Aus einer Minimalbasis erhält man alle Minimalbasen, wenn man alle rationalen Transformationen der Determinante ± 1 *ausübt, bei denen die Normenform und die Koordinaten der Zahl* 1 *wieder ganzzahlig werden.*

24. Eine Gesamtheit von ganzen Quaternionen, die mit α, β auch $\alpha + \beta$, $\alpha - \beta$ und $\alpha\beta$ enthält, wird *Integritätsbereich* genannt.

Ein Integritätsbereich heißt *größter oder maximaler Integritätsbereich*, wenn er nicht durch Aufnahme weiterer Quaternionen vergrößert werden kann, d. h. mit andern Worten (12), wenn jedes ganze Quaternion, das mit allen Quaternionen des Bereiches konkordant ist, schon in dem Bereich enthalten ist.

Dann gilt der Satz:

Eine Basis ist dann und nur dann eine Minimalbasis, wenn alle Quaternionen mit ganzen Koordinaten einen größten Integritätsbereich bilden.

---

[19]) II, S. 303.

[20]) D. h. sie sind halb genommene uneigentlich primitive Formen.

Hat eine Basis nämlich diese Eigenschaft, so sind die Multiplikationszahlen ganz. Außerdem sind die Koordinaten der Zahl 1 ganz und die Normenform ist eine Stammform; denn sonst könnte man den Integritätsbereich noch vergrößern. Es liegt also eine Minimalbasis vor.

Umgekehrt ist klar, daß alle Quaternionen, die in bezug auf eine Minimalbasis ganze Koordinaten haben, einen Integritätsbereich bilden. Gäbe es nun ein ganzes mit den Basiselementen konkordantes Quaternion, dessen Koordinaten den Generalnenner r hätten, so könnte man die Basis transformieren durch eine ganzzahlige unimodulare Substitution $\| u_{ik} \|$, für welche die Elemente der ersten Spalte diesen Koordinaten proportional wären. Dann würden aber bei der Normenform G' der neuen Basis die Koeffizienten g'_{00} durch r^2 und $g'_{01}, g'_{02}, g'_{03}$ durch r teilbar werden, was für eine Stammform unmöglich ist.

25. Diskutiert man die möglichen Fälle, für welche eine quaternäre quadratische Form eine quadratische Diskriminante haben und zugleich Stammform sein kann, so ergibt sich, daß die Grundzahl d jeden positiven oder negativen quadratfreien Wert, in dem für $d > 0$ eine ungerade und für $d < 0$ eine gerade Anzahl Primfaktoren aufgehen, jedoch keinen andern Wert haben kann.

Der Fall $d = 2$ entspricht der Hurwitzschen Algebra (siehe Einleitung). Der Fall $d = -1$ (Primzahlanzahl Null) nimmt eine Ausnahmestellung ein, er umfaßt diejenigen Algebren, welche Nullteiler enthalten. Alle andern Algebren sind Divisionsalgebren. Das ergibt sich daraus, daß jede quaternäre quadratische Form mit quadratischer Diskriminante, welche die Null darstellt, unter der Form $x_0 x_3 - x_1 x_2$ enthalten ist.

26. Es fragt sich noch, wie die verschiedenen Algebren, welche dieselbe Grundzahl haben, miteinander zusammenhängen. Da es nur ein Stammgeschlecht der Diskriminante d^2 gibt und Formen eines Geschlechts sich rational ineinander transformieren lassen, können in zwei verschiedenen Algebren der Grundzahl d zwei Minimalbasen so angenommen werden, daß zunächst die Normenformen und wegen der in 22 gemachten Bemerkungen auch die Multiplikationszahlen dieselben sind. Dadurch sind aber beide Algebren isomorph aufeinander bezogen.

Es läßt sich leicht zeigen, daß es zu derselben Grundzahl d unendlich viele Algebren gibt, und ihre Menge ist nicht einmal abzählbar. Die Substitution T der Nummer 18 kann nämlich nach 11, ohne daß W sich ändert, durch $O\,T$ ersetzt werden, wo O eine ganz beliebige eigentliche orthogonale Substitution mit der ersten Spalte $1, 0, 0, 0$ bezeichnet. Offenbar kann man aber in die Koeffizienten von O noch ganz beliebige Irrationalitäten aufnehmen.

Faßt man alle die unendlich vielen Algebren zu derselben Grundzahl als verschiedene Darstellungen einer einzigen abstrakten Algebra auf, so bestimmt jede Grundzahl eine einzige Algebra.

III. Moduln.

27. Zum näheren Studium der Eigenschaften unserer Algebren werde jetzt in einer Algebra $\mathfrak{Q}$ eine Minimalbasis ω_ν mit den Multiplikationszahlen $w_{\lambda\mu\nu}$ beliebig aber fest ausgewählt und als *Grundbasis* bezeichnet, die Normenform heiße *Grundform*. Zur bequemeren Formulierung der Sätze darf ohne Einschränkung der Allgemeinheit die Basis als *reduziert*, somit $\omega_0 = 1$ angenommen werden.

Ein System von Quaternionen aus $\mathfrak{Q}$, die entweder sämtlich ganz sind oder doch nach Multiplikation mit einer festen Zahl sämtlich ganz werden, wird *Modul* genannt, wenn das System vier linear unabhängige Quaternionen enthält und mit α, β auch $\alpha + \beta$ und $\alpha - \beta$ darin vorkommen.

Ein Modul heißt *ganzer Modul*, wenn er nur ganze Quaternionen enthält.

28. *Jeder Modul besitzt eine Basis.*

Zum Beweise genügt es, nur die ganzen Moduln ins Auge zu fassen, weil die andern darauf zurückgeführt werden können. In einem ganzen Modul $\mathfrak{a}$ sind aber auch die Zwischennormen und somit die Diskriminanten für vier linear unabhängige Quaternionen ganz (12). Wählt man nun aus $\mathfrak{a}$ vier linear unabhängige Quaternionen α_ν aus, für welche die Diskriminante einen Minimalwert annimmt, so enthält $\mathfrak{a}$ alle aber auch nur die Quaternionen, welche linear mit ganzen Koeffizienten durch die α_ν darstellbar sind. Andernfalls könnte man nämlich, wie man leicht erkennt, vier Quaternionen mit noch kleinerer Diskriminante finden.

29. Ist $\mathfrak{a}$ ein beliebiger Modul und bilden die Quaternionen

$$\alpha_\nu = \sum_i \omega_i a_{i\nu}$$

eine Basis, so wird die Matrix $A = \| a_{ik} \|$ *Basismatrix des Moduls* genannt. Die Reihenfolge der Basiselemente werde immer so gewählt, daß die Determinante dieser Matrix, welche wir auch *Determinante des Moduls* nennen und durch $|a_{ik}| = |\mathfrak{a}|$ bezeichnen, positiv wird.

Die Norm der Linearform

$$\alpha(x) = x_0\alpha_0 + x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3$$

ist eine quaternäre quadratische Form mit im allgemeinen gebrochenen Koeffizienten. Sie kann aber stets in der Gestalt

$$n(\alpha(x)) = a\,F((x))$$

geschrieben werden, wo F eine ganzzahlige primitive Form bezeichnet und a positiv ist. Wir nennen dann den Koeffizienten a die *Norm des Moduls* und schreiben $a = n(\mathfrak{a})$. Die Form F aber werde die zu der Basis gehörige *Normenform des Moduls* genannt.

30. Offenbar sind Norm und Determinante eines Moduls gänzlich unabhängig sowohl von der Basis des Moduls wie von der Grundbasis der Algebra, dagegen ist für die Normenform nur die Klasse bestimmt. (Würde man für die Determinante eines Moduls auch negative Werte zulassen, so würden die Normenformen zwei im allgemeinen verschiedenen Klassen angehören.)

Weil die Grundform G durch die lineare Substitution A in aF übergeht und G Stammform ist, so gilt immer

$$a^2 \leqq |\mathfrak{a}|, \quad \text{d. h. in Worten:}$$

Für jeden Modul ist das Quadrat der Norm kleiner oder höchstens so groß wie die Determinante.

31. Ersetzt man alle Quaternionen des Moduls $\mathfrak{a}$ durch die konjugierten Quaternionen, so erhält man wieder einen Modul (21), den wir durch $\bar{\mathfrak{a}}$ bezeichnen und den *konjugierten Modul* nennen.

Bilden die Quaternionen α_ν eine Basis von $\mathfrak{a}$, so ist klar, daß durch die konjugierten Quaternionen $\bar{\alpha}_\nu$ jedes Quaternion von $\bar{\mathfrak{a}}$ linear mit ganzzahligen Koeffizienten dargestellt werden kann. Die $\bar{\alpha}_\nu$ liefern daher eine Basis, wenn sie (wegen der Forderung der positiven Determinante) noch durch eine beliebige ganzzahlige Substitution mit der Determinante -1 z. B. durch E_0 transformiert werden. Daher gilt:

Aus der Basismatrix A von $\mathfrak{a}$ erhält man durch die Formel

$$\bar{A} = E_* A E_0$$

eine Basismatrix von $\bar{\mathfrak{a}}$.

32. Wenn man alle Quaternionen des Moduls $\mathfrak{a}$ links mit ϱ und rechts mit σ multipliziert, wobei ϱ, σ irgend zwei Quaternionen aus $\mathfrak{Q}$ mit positivem Normenprodukt bezeichnen, so erhält man wieder einen Modul, den wir durch $\mathfrak{a}' = \varrho\,\mathfrak{a}\,\sigma$ bezeichnen. Wenn die Quaternionen α_ν eine Basis von $\mathfrak{a}$ bilden, so bilden die Quaternionen $\alpha'_\nu = \varrho\,\alpha_\nu\,\sigma$ offenbar eine Basis von $\mathfrak{a}'$. Werden die Koordinaten von ϱ durch r_ν und von σ durch s_ν bezeichnet, so ergibt eine einfache Rechnung für die Basismatrix dieser Basis von $\mathfrak{a}'$

$$A' = \Omega(r)\,\Omega'(s)\,A.$$

Deshalb ist

$$n(\mathfrak{a}') = n(\varrho)\,n(\sigma)\,n(\mathfrak{a}), \qquad |\mathfrak{a}'| = [n(\varrho)]^2\,[n(\sigma)]^2\,|\mathfrak{a}|,$$

und die Normenformen der Moduln $\mathfrak{a}$, $\mathfrak{a}'$ gehören derselben Formenklasse an.

33. Sind zwei Moduln $\mathfrak{a}$ und $\mathfrak{b}$ gegeben und durchläuft α alle Quaternionen von $\mathfrak{a}$, β alle Quaternionen von $\mathfrak{b}$, so bilden die Produkte $\alpha\beta$ und ihre Summen wieder einen Modul, den wir durch

$$\mathfrak{c} = \mathfrak{a} \times \mathfrak{b}$$

bezeichnen und das *Produkt der Moduln* $\mathfrak{a}$ *und* $\mathfrak{b}$ nennen. Werden nämlich die $\alpha\beta$ und ihre Summen durch γ bezeichnet, so ist klar, daß unter den γ vier linear unabhängige Quaternionen und mit γ_1, γ_2 auch $\gamma_1 + \gamma_2$ und $\gamma_1 - \gamma_2$ vorkommen, die γ bilden daher einen Modul, wenn wir noch zeigen können, daß sie nach Multiplikation mit einer festen ganzen Zahl sämtlich ganz werden. Ein solcher Multiplikator wird aber erhalten, wenn man den Generalnenner der Koeffizienten einer Basismatrix von $\mathfrak{a}$ mit dem Generalnenner der Koeffizienten einer Basismatrix von $\mathfrak{b}$ multipliziert. Sind nämlich die Basismatrizen von $\mathfrak{a}$ und $\mathfrak{b}$ ganzzahlig, so sind alle Quaternionen der beiden Moduln $\mathfrak{a}$, $\mathfrak{b}$ ganz und untereinander konkordant, daher sind auch alle γ ganz (12).

Für die Multiplikation der Moduln gilt das assoziative, aber nicht das kommutative Gesetz.

Das folgt aus den Multiplikationsgesetzen der Quaternionen.

34. Sind A, B Basismatrizen der Moduln $\mathfrak{a}, \mathfrak{b}$, so genügt jede Basismatrix C des Produktes $\mathfrak{c} = \mathfrak{a} \times \mathfrak{b}$ den Bedingungen:

Die bilineare Substitution

$$C^{-1} \cdot W \left\langle \begin{matrix} A \\ B \end{matrix} \right. = M$$

ist ganzzahlig, und die Determinanten der rechteckigen Matrix

$$\| m_{\lambda\mu\nu} \| \qquad (\lambda = 0, 1, 2, 3; \ \mu\nu = 00, 01, \ldots, 33)$$

haben keinen gemeinsamen Teiler.

Sind umgekehrt für eine Matrix C mit nicht verschwindender positiver Determinante diese beiden Bedingungen erfüllt, so ist C Basismatrix des Produktes $\mathfrak{c} = \mathfrak{a} \times \mathfrak{b}$.

35. Werden die Normen von $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ durch a, b, c und die durch A, B, C bestimmten Normenformen durch F_a, F_b, F_c bezeichnet, so transformiert die bilineare Substitution M die Form cF_c in das Produkt $aF_a \cdot bF_b$, d. h. F_c ganzzahlig in $\frac{ab}{c} F_a F_b$.

Hier ist $\frac{ab}{c}$ ganz.

Erteilt man nämlich den Variablen von F_a und F_b ganzzahlige Werte, so müssen wegen der Ganzzahligkeit von M die Variablen von F_c und somit auch der Wert von F_c ganzzahlig ausfallen. Da aber F_a und F_b

primitive Formen sind, so können ihre Werte zu jeder vorgegebenen Zahl prim gemacht werden, also auch zu dem etwaigen Nenner von $\frac{ab}{c}$. Dann könnte aber F_c nicht ganzzahlig sein.

Demnach gilt der Satz:

Das Produkt der Normen zweier Moduln ist stets durch die Norm ihres Produktes teilbar, d. h. $n(\mathfrak{a})\,n(\mathfrak{b})$ *ist teilbar durch* $n(\mathfrak{a} \times \mathfrak{b})$.[21])

36. Bildet man endlich die beiden Determinanten

$$|\sum_j m_{ijk}\, x_j|, \qquad |\sum_j m_{ikj}\, y_j|,$$

so haben diese wegen der Matrizengleichung aus 34 die Werte

$$a^2 \frac{|\mathfrak{b}|}{|\mathfrak{c}|} F_a^2, \qquad b^2 \frac{|\mathfrak{a}|}{|\mathfrak{c}|} F_b^2.$$

Also gilt:

Wenn $\mathfrak{a} \times \mathfrak{b} = \mathfrak{c}$, *so sind* $a^2|\mathfrak{b}|$ *und* $b^2|\mathfrak{a}|$ *beide durch* $|\mathfrak{c}|$ *teilbar.*

IV. Ideale.

37. Wir stellen jetzt folgende Definition auf:

Ein Modul wird Ideal genannt, wenn seine Determinante das Quadrat seiner Norm ist[22]).

Da jedes Ideal ein Modul ist, können die Begriffe der Basis, der Determinante, der Norm, der Normenform ohne weiteres auf Ideale übertragen werden.

Der zu einem Ideal $\mathfrak{a}$ konjugierte Modul $\bar{\mathfrak{a}}$ ist offenbar auch ein Ideal und heißt *konjugiertes Ideal.* Dividiert man die sämtlichen Quaternionen des konjugierten Ideals $\bar{\mathfrak{a}}$ durch die Norm a, so entsteht ein Ideal $\frac{1}{a}\bar{\mathfrak{a}} = \mathfrak{a}^{-1}$ mit der Norm $\frac{1}{a}$, welches *reziprok zu* $\mathfrak{a}$ heißen soll. Offenbar ist $\mathfrak{a}$ zu $\mathfrak{a}^{-1}$ reziprok.

Ein Ideal heißt *ganz*, wenn es nur aus ganzen Quaternionen besteht; ein ganzes Ideal $\mathfrak{a}$ heißt *primitiv*, wenn es keine ganze Zahl $t > 1$ gibt, so daß $\frac{1}{t}\mathfrak{a}$ ganz ist.

---

[21]) Dabei heißt eine rationale Zahl a durch eine rationale Zahl b teilbar, wenn der Quotient $\frac{a}{b}$ eine ganze Zahl ist.

[22]) Diese Definition mag vielleicht auf den ersten Blick befremden, doch werden sich bald weitere charakteristische Eigenschaften unserer Ideale ergeben, die einen Zusammenhang mit den üblichen Definitionen eines Ideals in einem algebraischen Zahlkörper herstellen. (Übrigens wird auch in einem algebraischen Zahlkörper ein Modul durch eine ähnliche Forderung, nämlich die Gleichheit von Determinante und Norm als Ideal charakterisiert.)

Die sämtlichen Quaternionen, die in bezug auf die Grundbasis ganze Koordinaten haben, bilden ein Ideal von der Norm 1, das wir *Grundideal* nennen und durch $\mathfrak{o}$ bezeichnen.

38. Ist $\mathfrak{a}$ ein beliebiges Ideal mit der Norm a, bilden die Quaternionen $\alpha_\nu = \sum_i \omega_i a_{i\nu}$ eine Basis von $\mathfrak{a}$ und ist F die zugehörige Normenform, so ist nach einer früheren Terminologie die Basismatrix A *eine zur Grundform* G *gehörige, die Form* F *erzeugende Substitution* mit der Norm a.[23]) Diese Erzeugende ist zudem eigentlich, weil $|\mathfrak{a}| > 0$. Umgekehrt ist auch jede eigentliche Erzeugende zur Grundform G Basismatrix eines Ideals. Der einzige Unterschied gegen früher besteht darin, daß wir jetzt auch gebrochene Werte für die Koeffizienten der Matrix A zulassen, während wir uns früher auf ganzzahlige Werte beschränken konnten.

Wegen der Bedeutung der *Erzeugenden von positivem und negativem Charakter* vgl. man weiter unten Nr. 55.

39. *In jedem Ideal* $\mathfrak{a}$ *gibt es Quaternionen* α, *für welche der Quotient* $n(\alpha)/n(\mathfrak{a})$ *unter einer festen, nur von der Grundzahl* d *der Algebra abhängigen Schranke liegt.*

Stellt man nämlich die Quaternionen des Ideals $\mathfrak{a}$ durch eine Basis dar, so zeigt sich, daß dieser Quotient eine durch die Normenform F von $\mathfrak{a}$ darstellbare Zahl ist. Bekanntlich stellt aber eine quadratische Form Zahlen unterhalb einer endlichen Schranke dar, für welche man den Wert $2|\sqrt{d}|$ nehmen kann, wo d die Grundzahl der Algebra bezeichnet.

Da eine primitive quadratische Form stets Zahlen darstellt, die zu einer beliebig vorgegebenen Zahl prim sind, so gilt weiter:

In jedem Ideal $\mathfrak{a}$ *gibt es Quaternionen* α, *für welche der Quotient* $n(\alpha)/n(\mathfrak{a})$ *zu einer beliebig vorgegebenen Zahl prim ist.*

40. *Ein Ideal von der Norm* 1, *das die Zahl* 1 *enthält, wird Einheitsideal genannt.*

Ein Einheitsideal $\mathfrak{e}$ enthält nur ganze Quaternionen; denn wenn ε in $\mathfrak{e}$ liegt, so sind $n(\varepsilon)$ und $s(\varepsilon) = n(1, \varepsilon)$ ganz (29). Deshalb ist auch $\bar{\varepsilon} = s(\varepsilon) - \varepsilon$ in $\mathfrak{e}$ enthalten. Ein Einheitsideal ist also dem konjugierten und, weil die Norm gleich 1 ist, auch dem reziproken Ideal gleich.

Jede Basis eines Einheitsideals ist zugleich Minimalbasis der Algebra, und umgekehrt ist jede Minimalbasis zugleich Basis eines Einheitsideals (weshalb man den Begriff der reduzierten Basis (16) auf die Einheitsideale anwenden kann); im besonderen ist also das Grundideal $\mathfrak{o}$ ein Einheitsideal.

---

[23]) IV, S. 180.

Die Einheitsideale sind daher mit den größten Integritätsbereichen der Algebra identisch.

41. Wir betrachten im besonderen diejenigen Einheitsideale, deren Normenformen der Grundform äquivalent sind. Für ein solches Ideal $\mathfrak{e}$ kann man eine reduzierte Basis so auswählen, daß die Normenform der Grundform gleich wird. Die Basismatrix U ist dann eine eigentliche automorphe Substitution der Grundform mit der ersten Spalte $1, 0, 0, 0$.

Aus der bekannten Eulerschen Darstellung der ternären orthogonalen Substitutionen[24]) folgt dann für U die Darstellung

$$U = \Omega(r)^{-1}\,\Omega'(r).$$

(Diese Formel geht nämlich in die Eulersche über, wenn $\boldsymbol{W} = \boldsymbol{V}$ (10, 11), und folgt aus dieser durch lineare Transformation (18).)

Schreibt man sie in der Gestalt $\Omega(r)\,U = \Omega'(r)$, so erkennt man, daß die r_ν als Auflösung linearer homogener Gleichungen mit rationalen Koeffizienten selbst rational, daher auch ganz angenommen werden können. Umgekehrt ist klar, daß jedes U von dieser Form mit ganzen r_ν Basismatrix eines Einheitsideals ist. Also gilt:

Die Formel

$$U = \Omega(r)^{-1}\,\Omega'(r),$$

wobei die r_ν ganz sind, liefert als Basismatrix alle und nur die Einheitsideale, deren Normenformen der Grundform äquivalent sind.

Wählt man die r_ν im besonderen so, daß $G((r)) = m$ eine zu $2d$ prime Zahl ist, so hat U den Generalnenner m.[25]) Da m unendlich viele verschiedene Werte haben kann und verschiedenen Werten von m natürlich auch verschiedene Einheitsideale entsprechen, so gilt weiter:

Es gibt unendlich viele verschiedene Einheitsideale.

42. *Sind $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale, für welche das Modulprodukt $\mathfrak{c} = \mathfrak{a} \times \mathfrak{b}$ der Bedingung $n(\mathfrak{c}) = n(\mathfrak{a})\,n(\mathfrak{b})$ genügt, so ist $\mathfrak{c}$ ebenfalls ein Ideal.*

Daß die Annahmen dieses Satzes möglich sind, ergibt sich schon aus früheren Betrachtungen über die Komponierbarkeit der quaternären quadratischen Formen[26]).

Zum Beweise beachte man, daß wegen 30 die Determinante des Moduls $\mathfrak{c} = \mathfrak{a} \times \mathfrak{b}$ der Bedingung

$$|\mathfrak{c}| \geqq [n(\mathfrak{c})]^2$$

---

[24]) L. Euler, Opera omnia, I. Serie, 6, S. 309.

[25]) IV, S. 186 ff.

[26]) IV, S. 195.

und wegen 36 der Bedingung

$$|\mathfrak{c}| \leqq [n(\mathfrak{a})\, n(\mathfrak{b})]^2$$

genügt, woraus wegen $n(\mathfrak{a})\, n(\mathfrak{b}) = n(\mathfrak{c})$

$$|\mathfrak{c}| = [n(\mathfrak{c})]^2$$

folgt, d. h. der Modul $\mathfrak{c}$ ist ein Ideal.

Wir definieren daher:

Wenn für zwei Ideale $\mathfrak{a}, \mathfrak{b}$ *das Modulprodukt* $\mathfrak{c} = \mathfrak{a} \times \mathfrak{b}$ *der Bedingung* $n(\mathfrak{c}) = n(\mathfrak{a})\, n(\mathfrak{b})$ *genügt, so daß* $\mathfrak{c}$ *wieder ein Ideal ist, so schreiben wir* $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ *und nennen* $\mathfrak{c}$ *Idealprodukt oder, wenn keine Verwechslung mit dem allgemeinen Modulprodukt möglich ist, kurz Produkt aus* $\mathfrak{a}$ *und* $\mathfrak{b}$.

43. Für die Multiplikation der Ideale gilt das *assoziative Gesetz* in folgendem Sinne:

Wenn für eine Anzahl in fester Reihenfolge gegebene Ideale für eine bestimmte Art der Klammersetzung ein Idealprodukt existiert, so existiert dasselbe Idealprodukt auch für jede andere Art der Klammersetzung, sobald nur die Reihenfolge erhalten bleibt.

Das folgt aus der Gültigkeit des assoziativen Gesetzes für die Modulmultiplikation. Wendet man dies Gesetz auf Ideale an und ergibt sich bei einer Anordnung der Klammern, daß die sämtlichen auftretenden Modulprodukte Idealprodukte sind, so muß das auch für jede andere Anordnung der Klammern der Fall sein, weil sonst das Endprodukt nicht der Idealbedingung genügen könnte.

Demnach können die Klammern bei Idealprodukten ganz entbehrt werden [27]).

44. Gilt für die Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ die Produktgleichung

$$\mathfrak{a}\mathfrak{b} = \mathfrak{c}$$

und sind A, B, C Basismatrizen dieser Ideale, so ist die bilineare Substitution

$$C^{-1} \cdot W \left\langle \begin{matrix} A \\ B \end{matrix} \right. = M$$

wie bei der Modulmultiplikation ganzzahlig. Sie vermittelt gleichzeitig die Komposition der Normenformen. Hält man zwei der drei Matrizen A, B, C fest, so kann, wenn M ganzzahlig und $|A|\,|B| = |C|$ bleiben soll, die dritte immer nur durch rechts äquivalente ersetzt werden, d. h. durch AU, BU, CU, wo U eine ganzzahlige Matrix der Determinante 1 bezeichnet.

[27]) Vgl. hierzu Brandt, Über das assoziative Gesetz bei der Komposition der quaternären quadratischen Formen, Math. Annalen **96** (1926), S. 353.

Das folgt daraus, daß die Determinanten der drei rechteckigen Matrizen mit den Elementen $m_{\lambda\mu\nu}$, $m_{\nu\lambda\mu}$, $m_{\mu\nu\lambda}$ $(\lambda = 0, 1, 2, 3;\ \mu\nu = 00, 01, \ldots, 33)$ wegen der Primitivität der Normenformen von $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ keinen gemeinsamen Teiler haben können.

Das besagt für die Ideale:

Wenn das Produkt $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$ *existiert, so ist jedes der drei Ideale* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ *durch die beiden andern eindeutig bestimmt.*

45. Weil ein Einheitsideal $\mathfrak{e}$ ein Integritätsbereich ist, so gilt $\mathfrak{e}\mathfrak{e} = \mathfrak{e}$. *Zwei verschiedene Einheitsideale können aber nicht multipliziert werden.* Existierte nämlich für zwei verschiedene Einheitsideale $\mathfrak{e}_1, \mathfrak{e}_2$ das Idealprodukt $\mathfrak{e}_1\mathfrak{e}_2 = \mathfrak{e}_3$, so müßte $\mathfrak{e}_3$ Einheitsideal und somit auch größter Integritätsbereich sein. Weil die Zahl 1 in $\mathfrak{e}_2$ und $\mathfrak{e}_1$ vorkommt, sind in $\mathfrak{e}_3$ wegen $\mathfrak{e}_1\mathfrak{e}_2 = \mathfrak{e}_3$ alle Quaternionen aus $\mathfrak{e}_1$ und alle Quaternionen aus $\mathfrak{e}_2$ enthalten. Das ist aber unmöglich, weil $\mathfrak{e}_1$ und $\mathfrak{e}_2$ selbst schon größte Integritätsbereiche sind.

46. *Für jedes Ideal* $\mathfrak{a}$ *gibt es zwei eindeutig bestimmte Einheitsideale* $\mathfrak{e}_1$ *und* $\mathfrak{e}_2$, *so daß* $\mathfrak{e}_1\mathfrak{a} = \mathfrak{a}$ *und* $\mathfrak{a}\mathfrak{e}_2 = \mathfrak{a}$. *Wir nennen* $\mathfrak{e}_1$ *das links zugehörige oder linke und* $\mathfrak{e}_2$ *das rechts zugehörige oder rechte Einheitsideal von* $\mathfrak{a}$ *und* $\mathfrak{a}$ *Linksideal von* $\mathfrak{e}_1$ *und Rechtsideal von* $\mathfrak{e}_2$.

Ist nämlich A eine Basismatrix und F die zugehörige Normenform, so gibt es nach meinen früheren Ergebnissen[28]) zu F links und rechts zugehörige Hauptformen H_1 und H_2, welche die Kompositionen $H_1 F = F$ und $F H_2 = F$ gestatten. Zugleich müssen zwei diese Kompositionen vermittelnde bilineare Substitutionen von der Form

$$A^{-1} \cdot W \begin{matrix} \nearrow E_1 \\ \searrow A \end{matrix} \quad \text{und} \quad A^{-1} \cdot W \begin{matrix} \nearrow A \\ \searrow E_2 \end{matrix}$$

existieren, wobei E_1 und E_2 unimodulare Substitutionen bezeichnen, welche die Grundform G bzw. in H_1 und H_2 transformieren[29]).

Daraus folgt aber die Behauptung[30]).

Ist das Ideal $\mathfrak{a}$ im besonderen ganz, so sind alle seine Quaternionen sowohl in dem linken wie in dem rechten Einheitsideal von $\mathfrak{a}$ enthalten (12, 40).

47. Aus den früheren Betrachtungen über koordinierte bilineare Sub-

---

[28]) II, S. 308 ff.

[29]) III, S. 171.

[30]) Die links und rechts zugehörigen Einheitsideale können in Anlehnung an den Dedekindschen Begriff der Ordnung eines Moduls auch als Links- und Rechtsordnung von $\mathfrak{a}$ aufgefaßt und hergeleitet werden.

stitutionen[31]) ergibt sich, daß mit den eben angegebenen bilinearen Substitutionen auch diese

$$\tilde{A}^{-1} \cdot W \begin{matrix} \tilde{A} \\ E_1 \end{matrix}, \quad \tilde{A}^{-1} \cdot W \begin{matrix} E_2 \\ \tilde{A} \end{matrix}, \quad E_1^{-1} \cdot W \begin{matrix} A \\ \tilde{A} \end{matrix}, \quad E_2^{-1} \cdot W \begin{matrix} \tilde{A} \\ A \end{matrix}$$

ganzzahlig sind. Dabei ist

$$\tilde{A} = \frac{1}{a} E_* A E_0$$

Basismatrix des reziproken Ideals. Das besagt für die Ideale

$$\mathfrak{a}^{-1} \mathfrak{e}_1 = \mathfrak{a}^{-1}, \quad \mathfrak{e}_2 \mathfrak{a}^{-1} = \mathfrak{a}^{-1}, \quad \mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{e}_1, \quad \mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{e}_2.$$

48. *Zwei Ideale* $\mathfrak{a}$ *und* $\mathfrak{b}$ *lassen sich in dieser Reihenfolge dann und nur dann multiplizieren, wenn das rechte Einheitsideal von* $\mathfrak{a}$ *zugleich linkes Einheitsideal von* $\mathfrak{b}$ *ist.*

Wenn nämlich $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$ und $\mathfrak{e}$ das rechte Einheitsideal von $\mathfrak{a}$ ist, so gilt $\mathfrak{c} = (\mathfrak{a}\mathfrak{e})\mathfrak{b} = \mathfrak{a}(\mathfrak{e}\mathfrak{b}) = \mathfrak{a}\mathfrak{b}$, also $\mathfrak{e}\mathfrak{b} = \mathfrak{b}$ (43, 44).

Und wenn $\mathfrak{a}\mathfrak{e} = \mathfrak{a}$ und $\mathfrak{e}\mathfrak{b} = \mathfrak{b}$, also auch $\mathfrak{b}\mathfrak{b}^{-1} = \mathfrak{e}$, so existiert $\mathfrak{a}(\mathfrak{b}\mathfrak{b}^{-1})$, also auch $\mathfrak{a}\mathfrak{b}$ (47, 43).

Daraus folgt: Wenn zwei Ideale $\mathfrak{a}$, $\mathfrak{a}'$ das rechte oder zwei Ideale $\mathfrak{b}$, $\mathfrak{b}'$ das linke Einheitsideal gemeinsam haben, so gibt es Ideale $\mathfrak{p}$, $\mathfrak{q}$, so daß $\mathfrak{a}' = \mathfrak{p}\mathfrak{a}$, $\mathfrak{b}' = \mathfrak{b}\mathfrak{q}$.

49. *Sind* $\mathfrak{e}_1$ *und* $\mathfrak{e}_2$ *irgend zwei Einheitsideale, so gibt es stets Ideale* $\mathfrak{a}$, *die Linksideale für* $\mathfrak{e}_1$ *und Rechtsideale für* $\mathfrak{e}_2$ *sind.*

Zum Beweise bilde man das Modulprodukt $\mathfrak{e}_1 \times \mathfrak{e}_2 = \mathfrak{a}$. Dann bestehen die Modulgleichungen

$$\mathfrak{e}_1 \times \mathfrak{a} = \mathfrak{a}, \quad \mathfrak{a} \times \mathfrak{e}_2 = \mathfrak{a},$$

welche nach 36 erkennen lassen, daß $\mathfrak{a}$ ein Ideal ist[32]). Deshalb kann man auch schreiben

$$\mathfrak{e}_1 \mathfrak{a} = \mathfrak{a} \quad \text{und} \quad \mathfrak{a}\mathfrak{e}_2 = \mathfrak{a}.$$

Als wichtige Folgerung ergibt sich:

Ist $\mathfrak{c}$ *ein beliebiges Ideal und* $\mathfrak{e}$ *ein beliebiges Einheitsideal, so gibt es ein Rechtsideal* $\mathfrak{a}$ *von* $\mathfrak{e}$ *und ein Linksideal* $\mathfrak{b}$ *von* $\mathfrak{e}$, *so daß* $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ *ist.*

50. Die Sätze dieses Kapitels zeigen, daß *die Ideale von* $\mathfrak{Q}$ *in bezug auf die Multiplikation ein unendliches Gruppoid bilden*[3]).

---

[31]) I, S. 111, oder Bilineare Transformation quadratischer Formen, Math. Zeitschr. **20** (1924), S. 153.

[32]) Sind $\mathfrak{e}_1$ und $\mathfrak{e}_2$ Einheitsideale, so wird also ein beliebiger Modul $\mathfrak{a}$ durch jede dieser beiden Modulgleichungen als Ideal charakterisiert (vgl. 3).

Die Einheitselemente sind die Einheitsideale, die inversen Elemente sind die reziproken Ideale. Die links bzw. rechts einander zugehörigen Elemente sind die Ideale, welche das linke bzw. das rechte Einheitsideal gemeinsam haben. Doppelt zugehörig sind also diejenigen Ideale, welche sowohl das linke wie das rechte Einheitsideal gemeinsam haben.

Die einem Einheitsideal $\mathfrak{e}$ doppelt zugehörigen Ideale sind die zweiseitigen Ideale des Integritätsbereichs $\mathfrak{e}$, d. h. diejenigen Ideale, die sowohl Rechts- wie Linksideale von $\mathfrak{e}$ sind. Weil dazu alle Ideale $r\,\mathfrak{e}$ gehören, wo r eine beliebige rationale Zahl ist, so ist die Anzahl dieser Ideale, d. h. die Ordnung des Gruppoids unendlich. Daß auch der Rang, d. h. die Anzahl der Einheitselemente unendlich ist, wurde bereits gezeigt (41).

V. Idealklassen.

51. *Wenn* $\mathfrak{a}$ *ein beliebiges Ideal bezeichnet und* ϱ, σ *irgendwelche Quaternionen aus* $\mathfrak{Q}$ *mit nicht verschwindenden Normen sind, so ist der Modul* $\mathfrak{a}' = \varrho\,\mathfrak{a}\,\sigma$ *ebenfalls ein Ideal.*

Ist $\mathfrak{e}_1$ *das linke und* $\mathfrak{e}_2$ *das rechte Einheitsideal von* $\mathfrak{a}$, *so ist* $\mathfrak{e}_1' = \varrho\,\mathfrak{e}_1\,\varrho^{-1}$ *das linke. und* $\mathfrak{e}_2' = \sigma^{-1}\,\mathfrak{e}_2\,\sigma$ *das rechte Einheitsideal von* $\mathfrak{a}'$.

Die erste Behauptung ergibt sich nach unserer Idealdefinition (37) aus 32. Daraus folgt auch, daß $\mathfrak{e}_1'$, $\mathfrak{e}_2'$ Einheitsideale sind. $\mathfrak{e}_1'$, $\mathfrak{e}_2'$ genügen aber den Gleichungen $\mathfrak{e}_1'\,\mathfrak{a}' = \mathfrak{a}'$ und $\mathfrak{a}'\,\mathfrak{e}_2' = \mathfrak{a}'$, woraus sich die Richtigkeit der letzten Behauptung ergibt.

52. Auf Grund dieses Satzes stellen wir folgende Definitionen auf:

Zwei Ideale $\mathfrak{a}$ *und* $\mathfrak{a}'$ *heißen äquivalent, wenn es zwei Quaternionen* ϱ, σ *gibt, so daß* $n(\varrho\,\sigma) \neq 0$ *und* $\mathfrak{a}' = \varrho\,\mathfrak{a}\,\sigma$. *Alle äquivalenten Ideale bilden eine Idealklasse.*

Ist im besonderen $\sigma = 1$ *bzw.* $\varrho = 1$, *so wird die Äquivalenz als rechtsseitige bzw. linksseitige Äquivalenz bezeichnet. Alle rechts bzw. links äquivalenten Ideale bilden eine Rechts- bzw. Linksidealklasse.*

Offenbar haben rechts äquivalente Ideale dasselbe rechte und links äquivalente Ideale dasselbe linke Einheitsideal. Vgl. 59.

(Für Einheitsideale besagt die Äquivalenz dasselbe wie die Möglichkeit der isomorphen Zuordnung der von ihnen gebildeten Integritätsbereiche.)

53. *In jeder Rechts- und in jeder Linksidealklasse gibt es ganze Ideale, deren Norm unter einer endlichen Schranke liegt.*

Ist $\mathfrak{a}$ ein beliebiges Ideal mit der Norm a, und $\mathfrak{e}_1$ das linke, $\mathfrak{e}_2$ das rechte Einheitsideal von $\mathfrak{a}$, so wähle man aus dem reziproken Ideal $\mathfrak{a}^{-1}$ nach 39 ein Quaternion ϱ so aus, daß

$$0 < n(\varrho) \leqq \frac{1}{a} 2 \left| \sqrt{d} \right|.$$

Bildet man dann die beiden Ideale $\mathfrak{a}_1 = \mathfrak{a}\varrho$ und $\mathfrak{a}_2 = \varrho\mathfrak{a}$, von denen $\mathfrak{a}_1$ der Linksidealklasse von $\mathfrak{a}$ und $\mathfrak{a}_2$ der Rechtsidealklasse von $\mathfrak{a}$ angehört, so ist wegen $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{e}_1$ und $\mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{e}_2$ $\mathfrak{a}_1$ in $\mathfrak{e}_1$ und $\mathfrak{a}_2$ in $\mathfrak{e}_2$ enthalten, beide Ideale bestehen also aus lauter ganzen Quaternionen. Man findet aber

$$n(\mathfrak{a}_1) \leqq 2\,|\sqrt{d}\,|, \qquad n(\mathfrak{a}_2) \leqq 2\,|\sqrt{d}\,|.$$

54. *Für jedes Einheitsideal hat die Anzahl der Rechts- und Linksidealklassen, in die die rechts bzw. links äquivalenten Ideale zerfallen, denselben endlichen von der ausgewählten Einheitsklasse unabhängigen Wert h, der als Klassenzahl der Algebra bezeichnet wird.*

Wählt man als Einheitsideal zunächst das Grundideal $\mathfrak{o}$ aus, so kann man die Rechtsideale von $\mathfrak{o}$ auf Rechtsidealklassen verteilen und jede Klasse nach dem vorigen Satze durch ein ganzes Ideal, dessen Norm kleiner als $2\,|\sqrt{d}\,|$ ist, repräsentieren.

Die Basismatrizen dieser Ideale sind nach der am Schlusse von 46 gemachten Bemerkung ganzzahlig. Weil zwei Basismatrizen A und AU, wo U eine ganzzahlige Matrix mit der Determinante $+1$ bezeichnet, dasselbe Ideal liefern, so ist die Anzahl der repräsentierenden Ideale gewiß kleiner als die Anzahl der Klassen von Substitutionen mit einer positiven Determinante $< 4\,|d|$, also endlich.

Wird die Anzahl der Rechtsidealklassen von $\mathfrak{o}$ durch h bezeichnet, so ist klar, daß die Anzahl der Linksidealklassen von $\mathfrak{o}$ ebenso groß ist. Durchläuft nämlich $\mathfrak{a}$ alle Ideale der Rechtsidealklassen von $\mathfrak{o}$, so durchläuft entsprechend $\bar{\mathfrak{a}}$ alle Ideale der Linksidealklassen von $\mathfrak{o}$.

Endlich ist die Anzahl auch von der ausgewählten Einheitsklasse ganz unabhängig. Ist nämlich $\mathfrak{e}$ irgendein Einheitsideal, so kann man ein Ideal $\mathfrak{p}$ finden, das $\mathfrak{o}$ als linkes und $\mathfrak{e}$ als rechtes Einheitsideal hat (49). Durchläuft dann $\mathfrak{a}$ alle Rechtsideale von $\mathfrak{o}$, so durchläuft $\mathfrak{a}' = \mathfrak{a}\mathfrak{p}$ alle Rechtsideale von $\mathfrak{e}$. Zwei Ideale $\mathfrak{a}'$ sind aber dann und nur dann rechts äquivalent, wenn die entsprechenden Ideale $\mathfrak{a}$ rechts äquivalent sind.

55. *Für das Grundideal $\mathfrak{o}$ sind die Basismatrizen der ganzen und primitiven Rechts- und Linksideale mit zu d primer Norm mit den erzeugenden Substitutionen von positivem bzw. negativem Charakter*[33]) *identisch.*

Es genügt zu zeigen, daß die Rechtsideale mit den genannten Eigenschaften vollständig den Erzeugenden von positivem Charakter entsprechen, weil der zweite Teil der Behauptung genau entsprechend folgt. Das ergibt sich aber aus dem Satz:

---

[33]) IV, S. 180.

Von den ganzzahligen primitiven erzeugenden Substitutionen A mit der zu d primen Norm a liefern alle und nur diejenigen eine ganzzahlige bilineare Substitution

$$A^{-1} \cdot W^{A} = M,$$

welche die Elementarteiler $1, 1, a, a$ und positiven Charakter haben.

Der erste Teil dieses Satzes ergibt sich aus früheren Betrachtungen[34]). (Diese erfordern, wenn d ungrade und a grade, nur eine kleine Ergänzung.) Für den zweiten Teil beachte man, daß mit M nach 47 auch die bilinearen Substitutionen

$$W^{\tilde{A}}_{A} = N$$

ganz ausfallen[35]). Deshalb gestattet A die Parameterdarstellung

$$A = \| \sum_j n_{ijk} p_j \|,$$

welche, wie früher gezeigt, nur solche ganzzahligen primitiven Substitutionen A mit einer zu d primen Determinante a^2 liefern kann, welche die Elementarteiler $1, 1, a, a$ und positiven Charakter haben[36]).

56. *Es gibt kein ganzes und primitives Ideal mit zu d primer Norm, das rechts und links zu demselben Einheitsideal* e *gehört außer* e *selbst.*

Würde man nämlich eine Basis von e als Grundbasis annehmen, so würde nach dem vorigen Satz die Basismatrix eines solchen Ideals eine erzeugende Substitution sein, die sowohl positiven wie negativen Charakter hat, was unmöglich ist.

Untersucht man bei Stammformen die ganzen und primitiven erzeugenden Substitutionen, deren Norm nur Primteiler von d enthält, so ergeben sich die Sätze:

Die Norm eines ganzen und primitiven Ideals kann einen Diskriminantenteiler stets nur einfach, nicht im Quadrat enthalten.

Ein ganzes und primitives Ideal ist dann und nur dann gleichseitig, d. h. gehört links und rechts zu demselben Einheitsideal, wenn seine Norm ein Teiler t von d ist, und für jeden Teiler t gibt es zu jedem Einheitsideal e *gerade ein einziges derartiges Ideal.*

57. Aus diesen Sätzen ergeben sich wichtige Folgerungen für die aus gleichseitigen Idealen gebildeten Gruppen. Dabei soll eine solche Gruppe mit einem Ideal i auch alle rationalen Multipla ri enthalten.

---

[34]) IV, S. 192.

[35]) Die sämtlichen A, welche dasselbe M liefern, ergeben auch dasselbe N und umgekehrt.

[36]) IV, S. 187.

Eine derartige Gruppe $\mathfrak{h}$ wird dann vollständig charakterisiert durch die darin enthaltenen ganzen und primitiven gleichseitigen Ideale oder nach 56 auch durch die Normen dieser Ideale, d. h. durch ein System von Teilern t von d. Diese Teiler bilden dann selbst eine multiplikative Gruppe, wenn man die bei der Multiplikation etwa auftretenden quadratischen Faktoren jedesmal entfernt. Die Anzahl dieser Teiler und somit auch die der ganzen und primitiven in $\mathfrak{h}$ enthaltenen Ideale ist somit eine Potenz von 2.

Daraus schließt man, daß auch der Index der Gruppe $\mathfrak{h}$ in der Gruppe $\mathfrak{g}$ aller zu demselben Einheitsideal $\mathfrak{e}$ gehörigen gleichseitigen Ideale eine Potenz von 2 sein muß.

58. Ist umgekehrt ein System (t) von Teilern t von d so beschaffen, daß es in dem eben genannten Sinne eine multiplikative Gruppe bildet, so werden dadurch für irgend zwei Einheitsideale $\mathfrak{e}_1$ und $\mathfrak{e}_2$ in eindeutiger Weise Gruppen $\mathfrak{h}_1$ und $\mathfrak{h}_2$ von gleichseitigen Idealen bestimmt.

Diese Gruppen sind isomorph aufeinander bezogen, wenn man die demselben Teiler t von d entspringenden, bzw. in $\mathfrak{h}_1$ und $\mathfrak{h}_2$ liegenden ganzen Ideale $\mathfrak{i}_1$ und $\mathfrak{i}_2$ und ihre entsprechenden rationalen Multiplika $r\,\mathfrak{i}_1$ und $r\,\mathfrak{i}_2$ einander zuordnet.

Ist $\mathfrak{a}$ ein beliebiges Ideal, das links zu $\mathfrak{e}_1$ und rechts zu $\mathfrak{e}_2$ gehört, und sind $\mathfrak{j}_1$ und $\mathfrak{j}_2$ irgend zwei einander in dieser Weise entsprechende Ideale aus den Gruppen $\mathfrak{h}_1$ und $\mathfrak{h}_2$, so gilt stets $\mathfrak{j}_1\mathfrak{a} = \mathfrak{a}\mathfrak{j}_2$.

59. Hält man $\mathfrak{a}$ fest und läßt $\mathfrak{j}_1$ die Gruppe $\mathfrak{h}_1$ oder $\mathfrak{j}_2$ die Gruppe $\mathfrak{h}_2$ durchlaufen, so werde die Gesamtheit der Ideale $\mathfrak{j}_1\mathfrak{a} = \mathfrak{a}\mathfrak{j}_2$ durch $(\mathfrak{a})$ bezeichnet und die *durch das Teilersystem* (t) *bestimmte Schar* von $\mathfrak{a}$ genannt.

Sind $\mathfrak{a}, \mathfrak{b}$ Ideale, für welche das Produkt $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$ existiert, und durchläuft $\mathfrak{a}$ die Schar $(\mathfrak{a})$, $\mathfrak{b}$ die Schar $(\mathfrak{b})$, so durchläuft auch $\mathfrak{c}$ die Schar $(\mathfrak{c})$, die wir daher durch $(\mathfrak{a})(\mathfrak{b}) = (\mathfrak{c})$ bezeichnen und das *Produkt der Scharen* $(\mathfrak{a})$ und $(\mathfrak{b})$ nennen können.

Aus diesem Satz ergibt sich, daß auch die Scharen ebenso wie die Ideale *durch die Multiplikation zu einem Gruppoid verknüpft* sind. Die Ordnung dieses Gruppoids ist aber endlich, nämlich gleich dem Quotienten der Anzahl aller Teiler von d durch die Anzahl der in dem System (t) enthaltenen Teiler oder gleich dem Index der für irgendein Einheitsideal $\mathfrak{e}$ gebildeten Gruppe $\mathfrak{h}$ in $\mathfrak{g}$ (57).

60. Die sämtlichen ganzen Quaternionen μ, für welche $n(\mu) \neq 0$ und der größte gemeinsame Teiler $(n(\mu), d)$ dem Teilersystem (t) angehört, bilden zusammen mit den rationalen Multipla $r\mu$ eine multiplikative Gruppe, welche wir die *zu dem Teilersystem* (t) *gehörige Multiplikatorengruppe* nennen wollen.

Ist $\mathfrak{a}$ ein beliebiges Ideal, das links zu dem Einheitsideal $\mathfrak{e}_1$ und rechts zu dem Einheitsideal $\mathfrak{e}_2$ gehört, sind ferner τ_1 und τ_2 zwei Quaternionen der Multiplikatorengruppe, die den Bedingungen $\tau_1 \mathfrak{e}_1 = \mathfrak{e}_1 \tau_1$, $\tau_2 \mathfrak{e}_2 = \mathfrak{e}_2 \tau_2$ genügen, so ist das Ideal $\tau_1 \mathfrak{a} \tau_2$ in der durch das Teilersystem (t) bestimmten Schar $(\mathfrak{a})$ enthalten (58).

Sind ϱ, σ irgend zwei Quaternionen der Multiplikatorengruppe und durchläuft das Ideal $\mathfrak{a}$ die ganze Schar $(\mathfrak{a})$, so durchläuft das Ideal $\mathfrak{b} = \varrho \mathfrak{a} \sigma$ ebenfalls die Schar $(\mathfrak{b})$, die wir daher durch $(\mathfrak{b}) = \varrho (\mathfrak{a}) \sigma$ bezeichnen und der Schar $(\mathfrak{a})$ *in bezug auf das Teilersystem* (t) *äquivalent* nennen können.

Alle äquivalenten Scharen werden zu einer *Scharenklasse* zusammengefaßt, und die in einer Scharenklasse enthaltenen Ideale heißen *in bezug auf das Teilersystem* (t) *äquivalent* und bilden eine *Idealklasse in bezug auf das Teilersystem* (t).

61. Wir nennen eine solche Ideal- oder Scharenklasse $\mathfrak{K}_1$ *komponierbar* mit einer Klasse $\mathfrak{K}_2$, wenn es in $\mathfrak{K}_1$ Scharen $(\mathfrak{a})$ und in $\mathfrak{K}_2$ Scharen $(\mathfrak{b})$ gibt, für welche das Produkt $(\mathfrak{a})(\mathfrak{b}) = (\mathfrak{c})$ existiert. Bildet man auf alle möglichen Weisen solche Produkte, so ergeben die Scharen $(\mathfrak{c})$ wieder eine Scharenklasse $\mathfrak{K}_3$, die wir *komponiert aus* $\mathfrak{K}_1$ *und* $\mathfrak{K}_2$ nennen.

Bezeichnet man nämlich durch $\mathfrak{e}$ das rechts zu $\mathfrak{a}$ und links zu $\mathfrak{b}$ gehörige Einheitsideal, so kann die Schar $\varrho (\mathfrak{a}) \varrho_1$ nur mit der Schar $\sigma_1 (\mathfrak{b}) \sigma$ multipliziert werden, wenn $\varrho_1 \sigma_1 = \tau$ der Bedingung $\tau \mathfrak{e} = \mathfrak{e} \tau$ genügt (48). Daher ist nach dem zweiten Satz des vorigen Paragraphen $(\mathfrak{a}) \tau = (\mathfrak{a})$ oder $\tau (\mathfrak{b}) = (\mathfrak{b})$ und somit $\varrho (\mathfrak{a}) \tau (\mathfrak{b}) \sigma = \varrho (\mathfrak{a}) (\mathfrak{b}) \sigma = \varrho (\mathfrak{c}) \sigma$.

Deshalb bilden die *Idealklassen in bezug auf das Teilersystem* (t) *wieder ein Gruppoid.* Dies Gruppoid kann aufgefaßt werden als Faktorgruppoid[37]) aus dem Gruppoid aller Ideale und dem Gruppoid der Ideale einer *Einheitsklasse*, d. h. einer Klasse $\varrho (\mathfrak{e}) \sigma$, wo $\mathfrak{e}$ ein beliebiges Einheitsideal bezeichnet. Statt der Ideale kann man auch die Scharen als die Elemente der beiden Gruppoide ansehen, ohne daß das Faktorgruppoid sich ändert.

Der Rang des Gruppoids der Klassen ist endlich, nämlich gewiß kleiner als das Produkt $h 2^e$, wo h dieselbe Bedeutung hat wie in 54 und e die Anzahl der Primteiler von d bezeichnet.

62. Wenn das Teilersystem (t) nur aus der Zahl 1 besteht, erhält man den engsten Klassenbegriff. Stellt man nun für das Gruppoid $\mathfrak{G}$ dieser Klassen eine Kompositionstafel her, so kann man daran auch die Kompositionsgesetze für die Idealklassen in bezug auf ein beliebiges Teilersystem (t) veranschaulichen.

---

[37]) Vgl. F. K. Schmidt, Bemerkungen zum Brandtschen Gruppoid. Sitzungsberichte der Heidelberger Akademie 1927, 8. Abh., S. 94.

Man erhält nämlich die Idealklassen in bezug auf das Teilersystem (t), wenn man die Elemente dieses Gruppoids in geeigneter Weise zu Komplexen zusammenfaßt. Ein Komplex $\mathfrak{k}$, der ein Einheitselement E des Gruppoids $\mathfrak{G}$ enthält, ist eine Gruppe, und das gesuchte Klassengruppoid kann als Faktorgruppoid $\mathfrak{G}/\mathfrak{k}$ aufgefaßt werden. Zugleich kann man durch geeignete Anordnung der Zeilen und Spalten der Tafel von $\mathfrak{G}$ erreichen, daß die Komplexe sich auf quadratische Bezirke verteilen, die zugleich die Felder einer Kompositionstafel für das gesuchte Klassengruppoid darstellen[3]).

63. Aber auch die Idealklassen im früheren Sinne (52) können aus den Elementen des Gruppoids $\mathfrak{G}$ aufgebaut werden.

Durchläuft nämlich t_s alle Teiler von d, so kann man stets ganze Quaternionen μ_s in der Algebra $\mathfrak{Q}$ finden, für welche der größte gemeinsame Teiler, den die Norm von μ_s mit d gemeinsam hat, gerade t_s ist. Ist dann $\mathfrak{A}$ eine beliebige Idealklasse, in der sich das Element A befindet, so enthält $\mathfrak{A}$ alle und nur die Elemente $\mu_s A \mu_{s'}$. Diese Elemente sind aber nicht sämtlich verschieden voneinander.

Um die Anzahl der verschiedenen Elemente zu bestimmen, verstehen wir unter dem *Index eines Ideals* $\mathfrak{a}$ die Anzahl der ganzen und primitiven, in der Form $\nu_1 \mathfrak{a} = \mathfrak{a} \nu_2$ darstellbaren Ideale. Ähnliche Betrachtungen wie in 57 zeigen, daß der Index endlich und eine Potenz von 2 ist.

Der Index hat für alle Ideale derselben Idealklasse für ein beliebiges Teilersystem und auch für alle Ideale einer Idealklasse schlechthin stets denselben Wert.

Wird die Anzahl der Primfaktoren von d mit e bezeichnet, so daß es 2^e Teiler von d gibt, so finden sich in der Idealklasse $\mathfrak{A}$ vom Index 2^i gerade 2^{e-i} verschiedene Elemente.

64. Ist $\mathfrak{A} = \mathfrak{E}$ speziell eine Einheitsklasse, d. h. eine solche, die ein Einheitsideal $\mathfrak{e}$ oder auch ein Einheitselement E des Gruppoids $\mathfrak{G}$ enthält, so bilden die 2^{2e-i} Elemente von $\mathfrak{E}$ selbst ein Gruppoid vom Range 2^{e-i} und von der Ordnung 2^i, das ein Teilgruppoid von $\mathfrak{G}$ ist.

Wir wollen nun die Kompositionstafel für $\mathfrak{G}$ so anordnen, daß in quadratischen Bezirken von 2^{2e} Feldern entlang der von links oben nach rechts unten verlaufenden Diagonale gerade diese Teilgruppoide der Einheitsklassen $\mathfrak{E}$ erscheinen, wobei die Einheitselemente von $\mathfrak{G}$ zweckmäßig auf der Diagonale selbst stehen. Ist E eins von ihnen, so besteht die Zeile des Bezirkes von E aus den Elementen $\mu_s E$ und die Spalte aus den Elementen $E \mu_s$.

Durch diese Anordnung ist nun zugleich eine Einteilung der ganzen Tafel in horizontale und vertikale Streifen von der Breite 2^e und damit auch eine Einteilung in quadratische Bezirke von 2^{2e} Feldern gegeben.

Ist A ein Element eines solchen Bezirkes und trifft die Spalte von A die Diagonale im Feld E_1, die Zeile im Feld E_2, so enthält der Bezirk wegen der Grundeigenschaft der Tafel [3]) alle und auch nur die Elemente

$$\mu_s E_1 \cdot A \cdot E_2 \mu_{s'} = \mu_s A \mu_{s'},$$

umfaßt also gerade eine Idealklasse $\mathfrak{A}$.

65. Wenn dasselbe Element A außerhalb des betrachteten Bezirkes noch an einer anderen Stelle der Tafel vorkommt, so enthält der neue Bezirk wieder die ganze Klasse $\mathfrak{A}$ und keine anderen Elemente. Betrachtet man nun einen von diesen Bezirken, welche die Idealklasse $\mathfrak{A}$ enthalten und die beiden Streifen von der Breite 2^e, welche sich in diesem Bezirk kreuzen, so möge die Idealklasse, welche sich in dem Diagonalfeld des vertikalen Streifens befindet, durch $\mathfrak{E}_1$ und die Idealklasse, welche sich in dem Diagonalfeld des horizontalen Streifens befindet, durch $\mathfrak{E}_2$ bezeichnet werden. Wir nennen $\mathfrak{E}_1$ *die links* und $\mathfrak{E}_2$ *die rechts zu* $\mathfrak{A}$ *gehörige Einheitsklasse.*

Sind dann die Indizes der drei Klassen $\mathfrak{A}$, $\mathfrak{E}_1$, $\mathfrak{E}_2$ bzw. 2^i, 2^{i_1}, 2^{i_2}, wobei, wie man leicht zeigt, i höchstens so groß ist wie die kleinere der beiden Zahlen i_1 und i_2, so enthalten diese Klassen 2^{2e-i}, 2^{2e-i_1}, 2^{2e-i_2} verschiedene Elemente. In einem Streifen der Kompositionstafel eines Gruppoids kommt aber jedes Element und somit auch jeder Komplex von Elementen gleich oft vor. Der Komplex $\mathfrak{E}_1$ kommt in seinem Bezirk 2^{i_1}-mal und in dem vertikalen Streifen sonst nicht vor, ebenso kommt der Komplex $\mathfrak{E}_2$ in seinem Bezirk 2^{i_2}-mal und in dem horizontalen Streifen sonst nicht vor.

Da nun der Komplex $\mathfrak{A}$ in jedem Bezirk, wo er auftritt, 2^i-mal vorkommt und ein Bezirk aus dem Komplex $\mathfrak{A}$ entweder alle oder keine Elemente enthält, so muß der vertikale Streifen 2^{i_1-i} und der horizontale Streifen 2^{i_2-i} Bezirke enthalten, in denen sich jedesmal die Klasse $\mathfrak{A}$ befindet.

66. Die Einteilung in Bezirke kann zugleich als Kompositionstafel für die Idealklassen in dem früheren Sinn angesehen werden. Für den Gebrauch der Tafel muß man nur die für ein Gruppoid [3]) oder auch für die Formenklassen [38]) gegebene Regel anwenden. Die bei der Komposition der Klassen i. a. auftretenden Mehrdeutigkeiten werden durch die Tafel gerade vollständig zum Ausdruck gebracht.

Alle Klassen $\mathfrak{A}$, für die die Indizes 2^i, 2^{i_1}, 2^{i_2} denselben Wert haben, schließen sich zu einem oder auch zu mehreren Gruppoiden zusammen.

---

[38]) Verhandlungen der Schweizerischen Naturforschenden Gesellschaft 1924, II. Teil, S. 102.

Alle Klassen, die derselben Einheitsklasse links und rechts zugehören, bilden eine Idealklasse in bezug auf das System aller Teiler von d, haben daher denselben Index (63) und bilden eine Gruppe.

Die Idealklassen entsprechen vollständig den von den Normenformen gebildeten Formenklassen, wenn $d > 0$ und wenn $d < 0$ bei denjenigen Algebren $\mathfrak{Q}$, bei denen es ganze Quaternionen der Norm -1 gibt. Ist das nicht der Fall, so besteht ein Unterschied, der sich aber beheben läßt, wenn man den Äquivalenzbegriff verengt.

67. Ist $\mathfrak{a}$ ein beliebiges Ideal der Klasse $\mathfrak{A}$, $\mathfrak{e}_1$ das linke und $\mathfrak{e}_2$ das rechte Einheitsideal von $\mathfrak{a}$, so betrachten wir die für die Einheitsideale $\mathfrak{e}_1$ und $\mathfrak{e}_2$ gebildeten Rechts- und Linksideale und deren Klassen und fragen, wieviel von ihnen auf die Klasse $\mathfrak{A}$ entfallen. Man findet für $\mathfrak{e}_1$ 2^{i_1-i} und für $\mathfrak{e}_2$ 2^{i_2-i} Klassen, also dieselben Anzahlen[39]), welche angeben, wie oft die Klasse $\mathfrak{A}$ in den Spalten und Zeilen der Kompositionstafel vorkommt (66).

Daraus ergibt sich, daß die *Anzahl der Zeilen und Spalten in der Kompositionstafel gleich der früheren Klassenzahl h* ist (54).

Wendet man zur Bestimmung von h die bekannten transzendenten Methoden von Dirichlet an, so ergibt sich für $d > 3$ die Formel

$$h_1 + \frac{1}{2} h_2 + \frac{1}{3} h_3 = \frac{1}{12} \varphi(d),$$

wobei $h_1 + h_2 + h_3 = h$ und φ die Eulersche Funktion bezeichnet[40]).

---

[39]) Siehe auch III, S. 172 Fußnote.

[40]) Die §§ 57–67 haben bei der Korrektur im Dezember 1927 eine vollständige Umarbeitung erfahren wegen eines irrtümlichen Diskriminantensatzes in der früheren Darstellung, der mich veranlaßt hatte, meine bereits vor mehreren Jahren auf dem Begriff der Relativkomposition beruhenden Untersuchungen über die Kompositionstafeln der Formenklassen (vgl. meine Vorträge in Nauheim 1920 uud Luzern 1924) bei maximalen Ordnungen (Stammformen) für entbehrlich zu halten. Diese Untersuchungen erscheinen hier in den §§ 63–67 in ganz neuer Form, so daß zugleich ihre Verallgemeinerung auf beliebige Dedekindsche Algebren ersichtlich ist. Die §§ 57–62 sind auch inhaltlich neu und aus dem Gedanken entstanden, den Faktorgruppoidbegriff in allgemeinerer Auffassung für die Klassenbildung zu benutzen.

Den Hinweis auf das Versehen verdanke ich Herrn Artin, der übrigens in seiner im März 1927 erschienenen, mir aber erst nach Abschluß der Fahnenkorrektur bekannt gewordenen, daher oben nicht berücksichtigten Arbeit „Zur Arithmetik hyperkomplexer Größen", Hamburger Abhandlungen 1927, S. 282 einen wesentlichen Teil des in der Einleitung genannten allgemeinen Satzes vom Gruppoid der Ideale bewiesen hat.

(Eingegangen am 11. 1. 1927.)