Darstellungsanzahlen von quaternären quadratischen Stammformen mit quadratischer Diskriminante.

Autor(en): **Gross, H.**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **34 (1960)**

PDF erstellt am: **16.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-26632

Darstellungsanzahlen von quaternären quadratischen Stammformen mit quadratischer Diskriminante

von H. Gross, Zürich

Auf Grund einer neulich von G. Aeberli[1]) publizierten Arbeit über die Zusammenhänge zwischen quaternären quadratischen Formen mit quadratischer Diskriminante und Idealen in Quaternionenalgebren ergeben sich ziemlich direkt die Darstellungsanzahlen für die definiten und indefiniten quaternären Stammformen mit quadratischer Diskriminante. Viele quaternäre quadratische Formen quadratischer Diskriminante vom Typus $ax^2 + by^2 + cz^2 + dt^2$ sind von Liouville[2]) untersucht worden. Im Gegensatz zu den Unregelmäßigkeiten, die die Darstellungsanzahlen dieser Formen aufweisen, ergeben sich für die Darstellungsanzahlen von quaternären Stammformen quadratischer Diskriminante ganz einfache Ergebnisse. Durch den Zusammenhang mit der Idealtheorie wird auch die Sonderrolle der Diskriminantenteiler leicht verständlich.

Verteilt man alle ganzen $\mathfrak{o}$-Linksideale $\mathfrak{b}$ (bezüglich einer festen Maximalordnung $\mathfrak{o}$) mit der ganzrationalen Norm m in Klassen äquivalenter Ideale $A_1^{-1}, A_2^{-1}, \ldots, A_n^{-1}$, so gehört zu jeder linksinversen Idealklasse $A_1, A_2, \ldots, A_n$ eine Stammform $f_1, f_2, \ldots, f_n$ und zugehörige Linkshauptform $h_1, h_2, \ldots, h_n$. Liegen a_i Ideale $\mathfrak{b}$ in A_i^{-1} und ist e_i die Anzahl der Einsdarstellungen von h_i so stellt die Form f_i die ganzrationale Zahl m auf $e_i a_i$ Arten dar (Satz 4). Für die einzelnen a_i gibt es bis jetzt keine einfache Formel, wohl aber für ihre Summe, das heißt für die Gesamtzahl der ganzen $\mathfrak{o}$-Linksideale der Norm m (Satz 2). Diese Formel wurde mit einer andern Methode auch von M. Eichler in der Arbeit: Zur Zahlentheorie der Quaternionen-Algebren, J. reine angew. Math. 195 (1956) 127–151, Formeln (46) bis (48), hergeleitet. Ist die Klassenzahl der betrachteten Quaternionenalgebra 1, oder ist die darzustellende Zahl m relativ prim zur Diskriminante der Algebra, so erhält man einfache Formeln für die Anzahl der Darstellungen einer Zahl durch eine Stammform (vgl. III.3).

Die Abhandlung ist die gekrönte Lösung der Preisaufgabe «Hurwitz heeft aangetoond, dat de bekende formule voor het aantal representaties van n als $x^2 + y^2 + z^2 + t^2$ uit de ideaaltheorie der quaternionen kan worden afgeleid. Gevraagd wordt, het onderzoek tot andere quaternaire quadratische vormen,

---

[1]) G. Aeberli, Der Zusammenhang zwischen quaternären quadratischen Formen und Idealen in Quaternionenalgebren. Comment. Math. Helv. *33*, 1959, 212–239. Diese Arbeit ist im Folgenden als Aeberli zitiert.

[2]) Siehe etwa die Zusammenstellung in Dickson, History of the Theory of Numbers, vol. III, Washington, 1923, 227–229.

waarvan de discriminant een quadraat is, uit te breiden.», die die niederländische mathematische Gesellschaft «Een onvermoeide arbeid komt alles te boven» für das Jahr 1958 gestellt hatte.

I. Definitionen. Die Ergebnisse von AEBERLI

1. Quaternäre Formen

Im Folgenden werden immer nur *ganze* quaternäre Formen $f(x_i) = \sum_{i,k=1}^{4} a_{ik} x_i x_k$ betrachtet, das heißt, wir verlangen, daß die Zahlen a_{ii}, $2a_{ij}$, $i, j = 1, 2, 3, 4$ ganzrational sind. (Man nennt diese Formen auch ganze Formen zweiter Art; ganze Formen erster Art besitzen ganzrationale Koeffizienten a_{ij}, $i, j = 1, 2, 3, 4$.)

Als *Diskriminante* D der Form f definiert man

$$D = \left| \frac{\partial^2 f}{\partial x_i \partial x_k} \right| = 16 \mid a_{ik} \mid .$$

Die Form f heißt *primitiv*, falls die Zahlen $a_{11}, \ldots, a_{44}, 2a_{12}, \ldots, 2a_{34}$ teilerfremd sind. Erteilt man den Unbestimmten x_i ganzrationale Werte, $x_i = u_i$, die nicht alle Null sind, so heißt die Zahl $m = \sum_{i,k=1}^{4} a_{ik} u_i u_k$, durch die Form f dargestellt. Zwei Formen $f = \Sigma a_{ik} x_i x_k$, $g = \Sigma b_{ik} y_i y_k$ heißen *äquivalent*, falls sie durch eine unimodulare Transformation auseinander hervorgehen, mit andern Worten, wenn gilt $f = g$ für $x_i = \Sigma \alpha_i^k y_k$, mit α_i^k *ganzrational* und $\det(\alpha_i^k) = +1$. Um die Darstellungen einer Zahl durch Formen zu untersuchen, genügt es offenbar, aus den Klassen äquivalenter Formen je einen Repräsentanten auszuwählen.

2. Quaternionenalgebren

Für die Definitionen und Sätze dieses Paragraphen siehe die grundlegende Arbeit von H. BRANDT, Idealtheorie in Quaternionenalgebren, Math. Annalen 99 (1928) 4–9[3]).

Die vierdimensionalen rationalen Algebren sind die sogenannten Algebren der verallgemeinerten Quaternionen: Es sei $\mathfrak{A}$ ein vierdimensionaler Vektorraum über dem Körper der rationalen Zahlen mit den vier Basisvektoren u_1, u_2, u_3, u_4. Dabei sei u_1 das Einselement, also

$$u_1 u_j = u_j u_1 = u_j \qquad j = 1, 2, 3, 4$$

Weiter sei

$$u_2 u_3 = -u_3 u_2 = u_4$$

[3]) Diese Arbeit ist im Folgenden als BRANDT zitiert.

und $u_2^2 = -\alpha u_1$, $u_3^2 = -\beta u_1$ α, β rational. Aus diesen Gleichungen ergibt sich die ganze Multiplikationstafel, die wir in

$$u_i u_k = \Sigma c_{ik}^j u_j$$

zusammenfassen.

Es sei $\bar{q} = x_1 - x_2 u_2 - x_3 u_3 - x_4 u_4$ das zum Quaternion $q = x_1 + x_2 u_2 + x_3 u_3 + x_4 u_4$ konjugierte Quaternion. Ein Quaternion q heißt ganz, falls seine *Norm* $n(q)$:

$$n(q) = q\bar{q} = x_1^2 + \alpha x_2^2 + \beta x_3^2 + \alpha\beta x_4^2$$

und seine *Spur*

$$s(q) = q + \bar{q} = 2x_1$$

ganzrational sind.

BRANDT definiert als *Zwischennorm* zweier Quaternionen $p = \Sigma x_i u_i$, $q = \Sigma y_i u_i$ den Ausdruck $n(p, q) = p\bar{q} + q\bar{p} = n(q, p) = s(p\bar{q})$ und definiert weiter als Diskriminante der vier beliebigen Quaternionen $p_\nu = \Sigma x_{\nu\mu} u_\mu$ $\nu = 1, 2, 3, 4$ die Determinante:

$$\Delta(p_1, p_2, p_3, p_4) = |\, s(p_\nu \bar{p}_\mu)\,| = |\, n(p_\nu, p_\mu)\,| \tag{1}$$

Man findet durch Ausrechnen:

$$\Delta(p_1, p_2, p_3, p_4) = 16\alpha^2\beta^2\, |\, x_{\nu\mu}\,|^2 .$$

Bemerkung. Betrachtet man die *reguläre* Spur $S(p)$ eines Quaternions p: $S(p) = \Sigma_{\mu,\nu} c_{\mu\nu}^\mu x_\nu$ (siehe VAN DER WAERDEN, Algebra I, Berlin 1955, S. 145), das heißt die in beliebigen hyperkomplexen Systemen gültige Spurendefinition, und definiert man $\Delta'(p_1, p_2, p_3, p_4) = |\, S(p_\nu p_\mu)\,|$, so findet man durch Ausrechnen $\Delta' = -16\Delta$.

Sind vier neue Quaternionen p'_ν gegeben durch $p'_\nu = \Sigma \alpha_\nu^\mu p_\mu$, $\nu = 1, 2, 3, 4$, so gilt

$$\Delta(p'_1, p'_2, p'_3, p'_4) = |\, \alpha_\nu^\mu\,|^2 \Delta(p_1, p_2, p_3, p_4) . \tag{2}$$

Die Norm eines beliebigen Quaternions der Algebra wird durch eine *rationale* quadratische Form (die *Normenform* der Basis) gegeben:

$$G^{(u)}(x_i) = n(\Sigma x_i u_i) = \Sigma x_i x_j u_i \bar{u}_j = \tfrac{1}{2}\Sigma x_i x_j s(u_i \bar{u}_j) . \tag{3}$$

Aus (3) folgt, daß die Diskriminante dieser Form gleich der Diskriminante der Basis ist.

Eine Basis v_ν, $\nu = 1, 2, 3, 4$, heißt *Minimalbasis*, wenn ihre Multiplikationszahlen c_{ik}^j ganz sind und ihre Diskriminante möglichst klein ist.

Bemerkung. Aus der Ganzzahligkeit der Multiplikationszahlen c_{ik}^j folgt die Ganzzahligkeit der Normenform (3), also auch die Ganzzahligkeit der Diskriminante der Basis, woraus folgt, daß es wirklich Minimalbasen gibt.

BRANDT fand, daß die Diskriminante einer Minimalbasis eine *Quadratzahl* ist:

$$\Delta(v_1, v_2, v_3, v_4) = d^2 .$$

Man nimmt d mit positivem Vorzeichen, falls die Normenform $G^{(v)}$ definit ist, dagegen mit negativem Vorzeichen, falls die Normenform $G^{(v)}$ eine indefinite Form ist. Die in dieser Weise bestimmte ganze Zahl d heißt die *Grundzahl* der Algebra. Wegen (2) ist die Grundzahl eine Invariante der Algebra, das heißt von der speziellen Wahl der Minimalbasis unabhängig, da für zwei Minimalbasen v_ν, v'_μ, $v'_\mu = \Sigma \alpha^\nu_\mu v_\nu$, notwendigerweise $|\alpha^\nu_\mu| = \pm 1$ ist.

3. Ideale

Wir nannten ein Quaternion q einer Quaternionenalgebra ganz, wenn seine Spur und seine Norm ganzrational sind.

Definition. Eine Ordnung $\mathfrak{o}$ von $\mathfrak{A}$ ist ein Ring ganzer Quaternionen, der den Ring der ganzen rationalen Zahlen umfaßt und vier linear unabhängige Quaternionen von $\mathfrak{A}$ enthält. Die Ordnung $\mathfrak{o}$ heißt *maximal*, wenn es keine Ordnung gibt, die $\mathfrak{o}$ umfaßt, aber von $\mathfrak{o}$ verschieden ist (DEURING, Algebren, Ergebnisse der Mathematik IV_1 Berlin 1935, S. 69)[4]).

Wir definieren weiter:

Definition. Ein Modul $\mathfrak{a}$ der Algebra $\mathfrak{A}$ ist eine Teilmenge $\mathfrak{a}$ von Quaternionen der Algebra $\mathfrak{A}$ mit den Eigenschaften

(i) $\mathfrak{a}$ enthält vier linear unabhängige Quaternionen von $\mathfrak{A}$,
(ii) $\mathfrak{a}$ enthält mit zwei Quaternionen p, q auch deren Differenz $p - q$,
(iii) es gibt eine rationale Zahl r derart, daß $r\mathfrak{a}$ nur ganze Quaternionen enthält.

Man beweist: Ein Modul $\mathfrak{a}$ besitzt eine *Basis* (a_1, a_2, a_3, a_4), das heißt vier linear unabhängige Quaternionen a_1, a_2, a_3, a_4, derart, daß $\mathfrak{a}$ aus allen ganzrationalen Linearkombinationen $\Sigma x_i a_i$ besteht (BRANDT, S. 13). Es gilt weiter der

Satz. *Zu jedem Modul* $\mathfrak{a}$ *gibt es zwei eindeutig bestimmte Ordnungen* $\mathfrak{o}_l$, $\mathfrak{o}_r$ *mit* $\mathfrak{o}_l\mathfrak{a} = \mathfrak{a} = \mathfrak{a}\mathfrak{o}_r$ (DEURING, S. 71).

Wir schreiben dann für $\mathfrak{a}$ auch ${}_l\mathfrak{a}_r$, wo die Indices sinngemäß die zugehörigen Ordnungen angeben.

Definition. Ein Modul $\mathfrak{a}$ heißt *Ideal*, wenn die zugehörigen Ordnungen $\mathfrak{o}_l$, $\mathfrak{o}_r$ maximal sind. (Bei DEURING heißen diese Ideale «normale Ideale», vgl. DEURING, S. 72.)

Ist $\mathfrak{o}_l = \mathfrak{o}_r$, so heißen die Ideale ${}_l\mathfrak{a}_r$ gleichseitig. Man beweist, daß ein

[4]) Im Folgenden als DEURING zitiert.

Ideal ${}_i\mathfrak{a}_r$, falls es in einer seiner Ordnungen $\mathfrak{o}_l$, $\mathfrak{o}_r$ enthalten ist, in beiden Ordnungen $\mathfrak{o}_l$, $\mathfrak{o}_r$ enthalten ist. Man trifft daher folgende

Definition. Ein Ideal heißt ganz, wenn es in einer seiner Ordnungen enthalten ist (Deuring, S. 71).

Die Multiplikation zweier Ideale ${}_i\mathfrak{a}_r$, ${}_i\mathfrak{b}_j$ wird im Folgenden eingeschränkt, und zwar derart, daß den beiden Idealen nur dann ein Produkt $\mathfrak{a}\mathfrak{b}$ zugeordnet wird, wenn $\mathfrak{o}_r = \mathfrak{o}_i$ gilt. Man spricht dann der Deutlichkeit halber auch von *eigentlicher* Multiplikation der Ideale. Bei dieser eigentlichen Multiplikation gilt nämlich der folgende

Satz. *Sind* ${}_i\mathfrak{a}_r$ *und* ${}_i\mathfrak{b}_j$ *zwei Ideale, dann ist es genau dann unmöglich, in der Gleichung* $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$ *einen der Faktoren* $\mathfrak{a}, \mathfrak{b}$ *durch echte Teiler zu ersetzen, wenn die Rechtsordnung* $\mathfrak{o}_r$ *von* ${}_i\mathfrak{a}_r$ *gleich der Linksordnung* $\mathfrak{o}_i$ *von* ${}_i\mathfrak{b}_j$ *ist* (Deuring, S. 76).

In der Folge wird auch oft, ohne spezielle Erwähnung, von dem folgenden Satze Gebrauch gemacht:

Satz. *Das Ideal* ${}_i\mathfrak{a}_k$ *ist genau dann durch das Ideal* ${}_r\mathfrak{b}_s$ *teilbar, das heißt,* $\mathfrak{a} \subseteq \mathfrak{b}$, *wenn es eine Produktdarstellung* ${}_i\mathfrak{a}_k = {}_i\mathfrak{c}_r\, {}_r\mathfrak{b}_s\, {}_s\mathfrak{d}_k$ *mit ganzen* ${}_i\mathfrak{c}_r$, ${}_s\mathfrak{d}_k$ *gibt. Ist* $\mathfrak{o}_i = \mathfrak{o}_r$, *so gilt sogar* ${}_i\mathfrak{a}_k = {}_i\mathfrak{b}_s\, {}_s\mathfrak{d}_k$ *mit ganzem* ${}_s\mathfrak{d}_k$ (Deuring, S. 76).

4. Die Idealnorm

Vgl. dazu die übersichtliche Darstellung in der Arbeit von Aeberli, S. 225. Es sei $\mathfrak{o}$ eine Maximalordnung in $\mathfrak{A}$ und $\mathfrak{a}$ ein $\mathfrak{o}$-Linksideal; man habe die Basisdarstellungen $\mathfrak{a} = (a_1, a_2, a_3, a_4)$, $\mathfrak{o} = (u_1, u_2, u_3, u_4)$, $a_i = \Sigma \alpha_i^k u_k$. $\mathrm{Det}(\alpha_i^k)$ ist dann ein positives oder negatives rationales *Quadrat*. Bei geeigneter Wahl der Reihenfolge der Basiselemente ist $\det(\alpha_i^k) > 0$. Die positive, rationale Zahl $n(\mathfrak{a}) = {}_+\sqrt{|\alpha_i^k|}$ heißt dann die *Norm des Ideals* $\mathfrak{a}$. Man zeigt, daß die Idealnorm von der bei der Definition zugrunde gelegten Maximalordnung unabhängig ist. Es gelten weiter die folgenden Sätze:

Normenmultiplikationssatz. *Sind* ${}_i\mathfrak{a}_k$, ${}_k\mathfrak{b}_l$ *zwei Ideale, so gilt* $n(\mathfrak{a}\mathfrak{b}) = n(\mathfrak{a})n(\mathfrak{b})$ (Deuring, S. 80).

Satz. *Ein ganzes Ideal der Norm* 1 *ist eine Maximalordnung* (Aeberli, S. 225).

5. Normenformen

Ist $\mathfrak{a}$ ein Modul der Algebra $\mathfrak{A}$ mit der Basis (a_1, a_2, a_3, a_4), dann wird die Norm eines allgemeinen Quaternions q des Moduls, $q = \Sigma x_i a_i$, durch eine *rationale* quadratische Form gegeben: $F(x_i) = n(q) = n(\Sigma x_i a_i)$.

Wir setzen $F(x_i) = \lambda \cdot f_{\mathfrak{a}}^{(a)}(x_i)$, λ rational, wobei $f_{\mathfrak{a}}^{(a)}$ eine *ganzzahlige*, pri-

mitive quaternäre quadratische Form ist, die vom Modul $\mathfrak{a}$ und der darin gewählten Basis abhängig ist. Nun gilt der Satz, daß der Modul $\mathfrak{a}$ genau dann ein Ideal ist, wenn gilt $\lambda = n(\mathfrak{a})$ (AEBERLI, S. 225). Man hat also das für uns in der Folge wichtige

Ergebnis. *Ist* $\mathfrak{a}$ *ein Ideal,* $\mathfrak{a} = (a_1, a_2, a_3, a_4)$, *und ist* $q = \Sigma x_i a_i$ *das allgemeine Quaternion des Ideals* $\mathfrak{a}$, *dann gilt* $n(q) = n(\mathfrak{a}) f_{\mathfrak{a}}^{(a)}(x_i)$, *wo* $f_{\mathfrak{a}}^{(a)}$ *eine ganzzahlige, primitive quaternäre quadratische Form ist.*

Es seien $\mathfrak{a} = (a_1, a_2, a_3, a_4)$, $\mathfrak{b} = (b_1, b_2, b_3, b_4)$ zwei Moduln und es sei weiter $F(x_i) = n(\Sigma x_i a_i)$, $G(y_i) = n(\Sigma y_i b_i)$. Es gibt eine rationale Transformation $a_i = \Sigma \alpha_i^k b_k$ mit $\det(\alpha_i^k) \neq 0$. Ist q ein beliebiges Quaternion, so gibt es Darstellungen $q = \Sigma x_i a_i = \Sigma y_j b_j = \Sigma x_i \alpha_i^j b_j$, folglich ist $y_j = \Sigma \alpha_i^j x_i$. Geht also $\mathfrak{a}$ über in $\mathfrak{b}$ mit der Substitution (α_i^k), so geht die dem Modul $\mathfrak{b}$ zugeordnete Form G mittels der Substitution ${}^{\tau}(\alpha_i^k)$ über in die dem Modul $\mathfrak{a}$ zugeordnete Form F. Daraus ergibt sich, daß die Normenform eines Moduls der Quaternionenalgebra $\mathfrak{A}$ immer eine *quadratische Diskriminante* besitzt. Es sei nämlich (u_1, u_2, u_3, u_4) die im Paragraphen 2 betrachtete Basis der Algebra $\mathfrak{A}$ und $F(x_i) = n(\Sigma x_i u_i)$, also $F(x_i) = x_1^2 + \alpha x_2^2 + \beta x_3^2 + \alpha\beta x_4^2$. $F(x_i)$ hat dann die Diskriminante $16\alpha^2\beta^2$. Ist $g_{\mathfrak{a}}^{(a)}$ Normenform des Moduls $\mathfrak{a} = (a_1, a_2, a_3, a_4)$ und $G(y_i) = n(\Sigma y_i a_i)$, $a_i = \Sigma \alpha_i^k u_k$, so ist die Diskriminante der Form $G(y_i)$ gleich $16 \mid \alpha_i^k \mid^2 \alpha^2\beta^2$, also wieder quadratisch. Beim Übergang von $G(y_i)$ zur Normenform $g_{\mathfrak{a}}^{(a)}$, $G = \lambda g_{\mathfrak{a}}^{(a)}$, geht die Diskriminante von $G(y_i)$ über in die quadratische Diskriminante $\frac{16}{\lambda^4} \mid \alpha_i^k \mid^2 \alpha^2\beta^2$ von $g_{\mathfrak{a}}^{(a)}$.

6. Stammformen und Kernformen

Bei AEBERLI werden die *Stammformen* und die *Kernformen* folgendermaßen eingeführt (AEBERLI, S. 223):

Irgendeine ganzzahlige primitive Form $G(x_i)$ definiert eine Gesamtheit von Formen auf folgende Weise: Man übt auf die Formen $cG(x_i)$, wo c beliebig rational ist, alle rationalen Substitutionen mit von Null verschiedener Determinante aus. Jede entstehende Form schreiben wir als $kF(x_i)$, wo k größter Koeffiziententeiler, also $F(x_i)$ auch primitiv ganzzahlig ist. Die Formen $F(x_i), G(x_i), \ldots$ bilden eine sogenannte Sippe. Die Formen mit absolut kleinster Determinante einer Sippe heißen *Stammformen.*

Übt man auf $G(x_i)$ alle rationalen Substitutionen mit von Null verschiedener Determinante aus, so bilden die entstandenen Formen eine Gesamtheit, die man Familie nennt.

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

Es gilt dann der Satz: *Die Kernformen sind diejenigen ganzzahligen Formen,*

welche in der von ihnen erzeugten Familie die absolut kleinste Diskriminante besitzen (BRANDT, Speiser-Festschrift, Zürich 1945, S. 96).

AEBERLI bewies, daß für die Normenformen der Moduln, also insbesondere für die Normenformen der Ideale, die Begriffe Stammform und Kernform zusammenfallen, und es gilt der

Satz. *Ein Modul* $\mathfrak{a}$ *ist genau dann ein Ideal, wenn die zugehörige Normenform* $f_{\mathfrak{a}}^{(a)}$ *eine Stammform ist* (AEBERLI, S. 227).

Die Normenformen von Idealen sind also Stammformen mit quadratischer Diskriminante.

7. Äquivalenzklassen

Ist ${}_{l}\mathfrak{a}_{r}$ ein Ideal mit den Ordnungen $\mathfrak{o}_l$, $\mathfrak{o}_r$ und sind p, q zwei beliebige Quaternionen mit nicht verschwindender Norm, so ist der Modul $p\mathfrak{a}q$ wieder ein Ideal mit der Linksordnung $p\mathfrak{o}_l p^{-1}$ und der Rechtsordnung $q^{-1}\mathfrak{o}_r q$.

Auf Grund dieser Tatsache stellt man folgende Definition auf:

Definition. Zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ heißen *äquivalent*, wenn es zwei Quaternionen p, q gibt, derart, daß $n(pq) > 0$ und $\mathfrak{a} = p\mathfrak{b}q$ ist. Ist speziell $p = 1$ oder $q = 1$, so spricht man von rechtsseitiger bzw. linksseitiger Äquivalenz.

Im Folgenden wird unter Äquivalenz nur dann die schärfere einseitige Äquivalenz verstanden, wenn das ausdrücklich bemerkt wird. (Über die Forderung $n(pq) > 0$ siehe AEBERLI, S. 237.)

AEBERLI bewies den fundamentalen **Satz:** *Zwei Ideale sind genau dann äquivalent, wenn die zugehörigen Normenformen äquivalent sind* (AEBERLI, S. 233). Und weiter gilt auch der **Satz:** *Hat die Quaternionenalgebra* $\mathfrak{A}$ *Normenstammformen der Diskriminante* $D = d^2$, *dann sind alle Stammformen der Diskriminante* d^2 *Normenformen einer Idealklasse der Algebra* $\mathfrak{A}$ (AEBERLI, S. 236).

Man hat also eine 1 — 1 *deutige* Beziehung zwischen den Idealklassen der Algebra $\mathfrak{A}$ und den Klassen äquivalenter Stammformen der Diskriminante d^2.

AEBERLI bewies, daß dieser Isomorphismus sogar ein *Gruppoidisomorphismus* ist bei geeigneter Definition der Multiplikation (Komposition) der Ideal- und Formenklassen (AEBERLI, S. 237). (Vgl. den folgenden Paragraphen.) Dieses letzte Ergebnis werden wir allerdings im Folgenden nicht benötigen.

8. Gruppoide

Es sei G eine nichtleere Menge mit einer zweistelligen Operation, die jedem geordneten Paar (a, b) einer gewissen Teilmenge T von $G \times G$ eindeutig ein Element ab von G zuordnet. ab heißt dann das Produkt oder die Komposition von a mit b (in dieser Reihenfolge). Zu zwei Elementen a, b aus G braucht also nicht immer ein Produkt definiert zu sein.

G heißt *Gruppoid*, falls für die Produktoperation folgende Axiome erfüllt sind:

(i) Zu jedem a in G gibt es genau ein Paar Elemente e, f mit $ea = af = a$.
(ii) Ist $ea = a$ oder $ae = a$ für ein a, e in G, dann ist $ee = e$.
(iii) Zu a, b in G ist ab genau dann definiert, wenn es ein Element e in G gibt, mit $ae = a$ und $eb = b$.
(iv) Ist zu a, b, c in G auch ab und bc definiert, dann sind auch die Produkte $(ab)c$ und $a(bc)$ definiert, und es ist $(ab)c = a(bc)$.
(v) Ist $ea = a$, $af = a$ für a, e, f in G, so existiert ein Element b in G mit $ab = e$ und $ba = f$.
(vi) Ist $ee = e$ und $ff = f$ in G, dann existiert ein Element a in G mit $ea = a$ und $af = a$.

(Für die verschiedenen Axiomensysteme des Gruppoids siehe H. Brandt, Über die Axiome des Gruppoids, Vierteljschr. Naturforsch. Ges. Zürich 85 (1940), Beiblatt 32, 95–104. Das oben angegebene Axiomensystem findet sich in R. H. Bruck, A Survey of Binary Systems, Ergebnisse der Mathematik, neue Folge 20, Berlin 1958, 34.)

Es gilt nun der folgende Satz über die Ideale einer Quaternionenalgebra:

Satz. *Die Ideale einer Quaternionenalgebra bilden bei der eigentlichen Multiplikation ein Gruppoid mit den Maximalordnungen als Einheiten* (Deuring, S. 76).

Insbesondere gilt für das zu einem Ideal $\mathfrak{a}$ inverse Ideal $\mathfrak{a}^{-1} = \dfrac{\bar{\mathfrak{a}}}{n(\mathfrak{a})}$ wo $n(\mathfrak{a})$ die Norm von $\mathfrak{a}$ ist und $\bar{\mathfrak{a}}$ das zu $\mathfrak{a}$ konjugierte Ideal bedeutet. Wir betrachten jetzt die Klassen äquivalenter Ideale.

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

Daß diese Definition sinnvoll, das heißt nicht von den Repräsentanten der Klassen A, B abhängig ist, ergibt sich aus den Untersuchungen von Aeberli:

Es sei nämlich $AB = C$ definiert durch $\mathfrak{ab} = \mathfrak{c}$ $\mathfrak{a} \in A$, $\mathfrak{b} \in B$, $\mathfrak{c} \in C$. Ist nun $\mathfrak{a}' \sim \mathfrak{a}$, so existiert mindestens ein $\mathfrak{b}'$, $\mathfrak{b}' \sim \mathfrak{b}$ derart, daß $\mathfrak{a}' \cdot \mathfrak{b}'$ definiert ist, und für jedes solche $\mathfrak{b}'$ ist $\mathfrak{c} \sim \mathfrak{c}' = \mathfrak{a}' \cdot \mathfrak{b}'$.

Da die Ideale ein Gruppoid bilden, verifiziert man leicht die Gruppoidaxiome für die Idealklassen bei der oben definierten Komposition für Klassen. Da die Idealklassenzahl für rationale Algebren endlich ist (Deuring, S. 90), ergibt sich also der **Satz:** *Die Idealklassen der Algebra* $\mathfrak{A}$ *bilden ein endliches Gruppoid.*

II. Die Anzahl ganzer Ideale einer beliebigen Maximalordnung von vorgeschriebener Norm

Es sei $\mathfrak{o}$ eine beliebige, aber feste Maximalordnung der Algebra $\mathfrak{A}$. Im Folgenden soll die Anzahl aller ganzen $\mathfrak{o}$-Linksideale von vorgeschriebener Norm bestimmt werden. Dazu ist es notwendig, sich einen Überblick über die Zerlegung von Idealen in Primideale und unzerlegbare Ideale zu verschaffen. Wir beginnen mit einigen Definitionen.

Definition. Das gleichseitige $\mathfrak{o}$-Ideal $\mathfrak{p}$ heißt Primideal, wenn es kein durch $\mathfrak{p}$ teilbares Produkt von gleichseitigen $\mathfrak{o}$-Idealen, $\mathfrak{a}\cdot\mathfrak{b}$, gibt, dessen beide Faktoren $\mathfrak{a}$, $\mathfrak{b}$ nicht durch $\mathfrak{p}$ teilbar sind.

Definition. Ein ganzes Ideal heißt unzerlegbar, wenn es nicht als eigentliches Produkt von echten Teilern darstellbar ist.

Definition. Ein ganzes Ideal $\mathfrak{a}$ heißt primitiv, wenn es kein ganzrationales $n > 1$ gibt, derart, daß $\frac{1}{n} \cdot \mathfrak{a}$ ganz ist.

Es gelten dann die Sätze (BRANDT, S. 24):

A. Satz. *Es gibt kein ganzes und primitives Ideal mit zur Grundzahl d primer Norm, das rechts und links zu derselben Ordnung $\mathfrak{o}$ gehört, außer $\mathfrak{o}$ selbst.*

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

C. Satz. *Ein ganzes und primitives Ideal ist genau dann gleichseitig, wenn seine Norm ein Teiler t von d ist, und für jeden Teiler t gibt es zu jeder Maximalordnung gerade ein einziges derartiges Ideal.*

Wir beweisen dazu noch den folgenden

1. Hilfssatz. *Ein gleichseitiges ganzes Ideal $\mathfrak{a}$, dessen Norm verschiedene Primfaktoren enthält, ist nicht prim.*

Beweis. Es sei $n(\mathfrak{a}) = ab, (a, b) = 1$. Wir setzen $\mathfrak{a}' = (\mathfrak{a}, a), \mathfrak{b}' = (\mathfrak{a}, b)$. Dann gilt $\mathfrak{a}'\mathfrak{b}' = \mathfrak{a}$, $\mathfrak{a} \neq \mathfrak{a}'$, $\mathfrak{b}' \neq \mathfrak{a}$. Da nämlich allgemein $n(\mathfrak{a}) \in \mathfrak{a}$ gilt, ist sicher $\mathfrak{a}'\mathfrak{b}' \subseteq \mathfrak{a}$. Wegen $(a, b) = 1$ kann man aber jedes x aus $\mathfrak{a}$ in der Form $x = \lambda xa + \mu xb$ schreiben mit geeigneten ganzrationalen λ, μ. Also ist auch $\mathfrak{a} \subseteq \mathfrak{a}'\mathfrak{b}'$.

Auf Grund dieses Hilfssatzes sind die Normen von Primidealen Primzahlpotenzen. Insbesondere können wir also die Primideale einteilen in solche, deren Normen zur Diskriminante prim sind und in solche, deren Normen Potenzen von Diskriminantenprimteilern sind.

Aus Satz C ergibt sich, daß es zu jedem Primteiler t von d genau ein Prim-

ideal der Norm t gibt. Diese Primideale sind wegen des Normenmultiplikationssatzes natürlich zugleich unzerlegbare Ideale.

Aus Satz A ergibt sich, daß die Primideale mit zu d primer Norm durch die rationalen Primzahlen, die zu d prim sind, erschöpft werden, genauer, durch die von ihnen erzeugten Hauptideale.

Die Teiler der zweiseitigen $\mathfrak{o}$-Ideale (p), wo $(p, d) = 1$ ist, sind dann unzerlegbare einseitige $\mathfrak{o}$-Ideale der Norm p. Um diese zu finden, betrachten wir den Ring $\mathfrak{o}/\mathfrak{o}p$.

Der Ring $\mathfrak{o}/\mathfrak{o}p$ ist isomorph zum Ring $\bar{\mathfrak{o}}$ der p^4 zweizeiligen Matrizen, deren Elemente das Galoisfeld $GF(p)$ durchlaufen. Es gilt nämlich der **Satz.** *Jede Algebra, welche eine von Null verschiedene Diskriminante besitzt, ist halbeinfach und die direkte Summe einfacher Algebren.* (L. E. Dickson, Algebren und ihre Zahlentheorie, Zürich 1927, S. 110[5].) Der Ring $\mathfrak{o}/\mathfrak{o}p$ muß aber einfach sein, sonst wäre er eine Summe von Galoisfeldern, also kommutativ.

Das allgemeinste $\mathfrak{o}$-Linksideal in $\mathfrak{o}/\mathfrak{o}p$ besteht aus allen denjenigen Matrizen, deren Spalten S_1, S_2 einer beliebigen, aber festen Relation

$$r_1 S_1 + r_2 S_2 \equiv 0 (p) \qquad r_1, r_2 \text{ ganzrational} \tag{1}$$

genügen. Da es $p + 1$ derartige Relationen gibt, die unter sich unabhängig sind, besitzt das zweiseitige $\mathfrak{o}$-Ideal (p) $p + 1$ Linksteiler. Diese $p + 1$ $\mathfrak{o}$-Linksideale der Norm p sind nun alle *rechtsäquivalent* (vgl. Abschnitt I.7.). Sei nämlich $\mathfrak{p}$ das durch die Relation (1) definierte Ideal. Wir betrachten dann die Matrix $\begin{pmatrix} r_1 & s \\ r_2 & t \end{pmatrix}$, wo r_1, r_2 die Koeffizienten aus (1) sind; s, t seien so gewählt, daß $\det \begin{pmatrix} r_1 & s \\ r_2 & t \end{pmatrix} > 0$ ist. Ist jetzt $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ein beliebiges Element aus $\mathfrak{p}$, so folgt wegen (1):

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} r_1 & s \\ r_2 & t \end{pmatrix} = \begin{pmatrix} 0 & as + bt \\ 0 & cs + dt \end{pmatrix}$$

Das beliebige Ideal $\mathfrak{p}$ kann also durch Multiplikation mit einem geeigneten Element $\begin{pmatrix} r_1 & s \\ r_2 & t \end{pmatrix}$ aus $\bar{\mathfrak{o}}$ in das spezielle Ideal $\mathfrak{p}_0$ aller Matrizen $\begin{pmatrix} 0 & m \\ 0 & n \end{pmatrix}$ über geführt werden. Daraus ergibt sich unmittelbar die Behauptung. Wir erhalten also das in der Folge wichtige Ergebnis:

1. Satz. *In einer beliebigen Maximalordnung $\mathfrak{o}$ der Algebra $\mathfrak{A}$ gibt es zu jeder Primzahl p, wo p die Diskriminante nicht teilt, $p + 1$ ganze $\mathfrak{o}$-Linksideale $\mathfrak{p}$ der Norm p (Linksteiler des zugehörigen zweiseitigen $\mathfrak{o}$-Primideals (p)). Alle diese $p + 1$ unzerlegbaren Ideale $\mathfrak{p}$ sind rechtsäquivalent.*

Selbstverständlich kann man in diesem Satz die Ausdrücke Linksteiler, rechtsäquivalent durch die Ausdrücke Rechtsteiler, linksäquivalent ersetzen.

[5]) In der Folge als Dickson zitiert.

Es gelten die folgenden beiden Sätze über ganze Ideale einer beliebigen Maximalordnung.

D. Satz. *Jedes ganze Ideal* ${}_i\mathfrak{a}_k$ *ist Produkt von unzerlegbaren Idealen* (DEURING, S. 77).

E. Satz. *In der Darstellung eines Ideals* ${}_i\mathfrak{a}_k$ *als Produkt unzerlegbarer Ideale kann die Reihenfolge der Primideale, von denen die unzerlegbaren Faktoren Teiler sind, beliebig vorgeschrieben werden* (DEURING, S. 106).

Es sei jetzt $\mathfrak{a}$ ein primitives ganzes $\mathfrak{o}$-Linksideal mit der Norm $n(\mathfrak{a}) = p \cdot s$ wo p eine Primzahl ist (p und s brauchen nicht teilerfremd zu sein). Nach dem 1. Satz und den beiden Sätzen D und E gibt es Darstellungen:

$\mathfrak{a} = \mathfrak{p}\mathfrak{q}$ mit $n(\mathfrak{p}) = p$, $n(\mathfrak{q}) = s$, $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ wo $\bar{\mathfrak{p}}$ das zu $\mathfrak{p}$ konjugierte Ideal ist. Der größte gemeinsame Linksteiler von $\mathfrak{a}$ und (p) ist also ein Teiler von $\mathfrak{p}$. Wegen $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ wo $\mathfrak{p}$ und $\bar{\mathfrak{p}}$ unzerlegbare Ideale sind, ist der größte gemeinsame Linksteiler von $\mathfrak{a}$ und (p) genau $\mathfrak{p}$, da $\mathfrak{a}$ primitiv vorausgesetzt wurde. Wir erhalten daher den

2. Hilfssatz. *Es sei* $\mathfrak{a}$ *ein ganzes primitives* $\mathfrak{o}$*-Linksideal mit der Norm* $n(\mathfrak{a}) = ps$ *wobei* p *eine Primzahl ist. Der größte gemeinsame* $\mathfrak{o}$*-Linksteiler von* $\mathfrak{a}$ *und dem zweiseitigen* $\mathfrak{o}$*-Ideal* (p) *ist ein unzerlegbares* $\mathfrak{o}$*-Linksideal* $\mathfrak{p}$ *der Norm* p.

Wir beweisen weiter den folgenden

3. Hilfssatz. *Ist das ganze Ideal* $\mathfrak{a}$ *Produkt von primitiven unzerlegbaren Idealen:*

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r\mathfrak{q}_1 \dots \mathfrak{q}_s \dots, n(\mathfrak{p}_i) = p,\ n(\mathfrak{q}_i) = q, \dots \tag{2}$$

wobei kein Faktor konjugiert zum vorangehenden ist, dann ist das Ideal $\mathfrak{a}$ *auch primitiv.*

Beweis. Ist die Norm $n(\mathfrak{a})$ eine quadratfreie Zahl, so ist der Satz trivialerweise richtig, so daß wir also $r \geqslant 2$ annehmen können. Wir beweisen den Satz durch Induktion nach der Anzahl der Faktoren von $\mathfrak{a}$. Der Satz sei also richtig für ν Faktoren. (Für $\nu = 1$ ist die Behauptung richtig.) Es sei $\mathfrak{a}$ ein Ideal der Form (2) mit $\nu + 1$ unzerlegbaren Faktoren:

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{b}\,, \qquad \mathfrak{b} = \mathfrak{p}_2 \dots \mathfrak{p}_r\mathfrak{q}_1 \dots \tag{3}$$

$\mathfrak{b}$ ist primitiv nach Induktionsvoraussetzung. Gesetzt es sei jetzt

$$\mathfrak{a} = s\mathfrak{c} \quad s > 1, s \text{ ganzrational}, \quad \mathfrak{c} \text{ ganz}. \tag{4}$$

Aus (3) folgt

$$\bar{\mathfrak{p}}_1\mathfrak{a} = p \cdot \mathfrak{b}\,. \tag{5}$$

Aus (4) und (5) folgt $\bar{\mathfrak{p}}_1\mathfrak{c} \cdot s = p\mathfrak{b}$, also da p Primzahl und $\mathfrak{b}$ primitiv ist, folgt $s \mid p$, also $s = p$. Man hätte also die Darstellungen

$$\mathfrak{b} = \bar{\mathfrak{p}}_1 \mathfrak{c}\,, \quad \mathfrak{b} = \mathfrak{p}_2 \dots \mathfrak{p}_r \mathfrak{q}_1 \dots\,, \quad (p) = \bar{\mathfrak{p}}_1 \mathfrak{p}_1\,.$$

Nach dem 2. Hilfssatz ergibt sich $\mathfrak{p}_2 = \bar{\mathfrak{p}}_1$, womit wir einen Widerspruch zur Voraussetzung erhalten haben. Die Behauptung ist also auch richtig für $\nu + 1$ Faktoren.

Es gilt nun der folgende Zerlegungssatz für ganze und primitive Ideale:

4. Hilfssatz (*«Eindeutigkeitssatz»*). *Ist* $\mathfrak{a}$ *ein ganzes und primitives Ideal mit der Norm* $n(\mathfrak{a}) = \Pi p_i$ *(wobei die Primzahlen* p_i *nicht notwendigerweise voneinander verschieden sind) und ist in der Zerlegung* $n(\mathfrak{a}) = p_1 p_2 \dots p_r$ *die Reihenfolge der* p_i *fest, so gibt es gerade eine Darstellung von* $\mathfrak{a}$ *in unzerlegbare Faktoren* $\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r$ *derart, daß* $n(\mathfrak{p}_i) = p_i$ *gilt.*

Der Beweis ergibt sich direkt aus dem 2. Hilfssatz, indem man von $\mathfrak{a}$ den größten gemeinsamen Linksteiler von $\mathfrak{a}$ und (p_1) abspaltet und auf den verbleibenden Faktor Induktionsvoraussetzung anwendet. Für das Folgende vgl. auch M. Eichler, Zur Zahlentheorie der Quaternionen. J. reine angew. Math. 195 (1956) 127–151.

Auf Grund der vorangehenden Hilfssätze werden wir jetzt den folgenden Satz beweisen:

2. Satz. *Es sei* $n = t p_1^{\nu_1} p_2^{\nu_2} \dots p_r^{\nu_r}$ *wo die Primzahlen* p_i *zur Grundzahl* d *prim sind, während* t *nur Primteiler von* d *enthält. Ist* $\mathfrak{o}$ *eine beliebige Maximalordnung, so ist die Anzahl* $\psi(n)$ *der ganzen* $\mathfrak{o}$*-Linksideale der Norm* n *gleich*

$$\psi(n) = (p_1^{\nu_1} + p_1^{\nu_1 - 1} + \dots + p_1 + 1) \dots (p_r^{\nu_r} + p_r^{\nu_r - 1} + \dots + p_r + 1)$$

(«Summe der zu d *primen Teiler von* n*»).*

Beweis. Um zunächst alle primitiven $\mathfrak{o}$-Linksideale $\mathfrak{a}$ mit zu d primer Norm

$$n = n(\mathfrak{a}) = p^r q^s \dots u^l > 1 \qquad (n, d) = 1$$

zu bestimmen, hat man nach den beiden letzten Hilfssätzen alle Produkte

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r \mathfrak{q}_1 \dots \mathfrak{q}_s \dots \mathfrak{u}_1 \dots \mathfrak{u}_l$$

zu bilden, wobei die Faktoren unzerlegbar sind, der erste Faktor immer ein $\mathfrak{o}$-Linksideal und keiner der Faktoren zum vorangehenden konjugiert ist. Bezeichnet $Q(n)$ die gesuchte Anzahl, so gilt

$$Q(n) = (p+1)p^{r-1}(q+1)q^{s-1} \dots (u+1)u^{l-1} = n\left(1 + \frac{1}{p}\right)\left(1 + \frac{1}{q}\right) \dots \left(1 + \frac{1}{u}\right),$$

Suchen wir jetzt die Anzahl aller $\mathfrak{o}$-Linksideale mit zu d primer Norm n, also auch die nichtprimitiven, so gilt für ihre Anzahl $\psi(n)$

$$\psi(n) = \Sigma Q\left(\frac{n}{\delta^2}\right)$$

wobei sich die Summation über alle Quadratteiler $\delta^2 = p^{2r'} q^{2s'} \dots u^{2l'}$ $(2r' \leqslant r, 2s' \leqslant s, \dots 2l' \leqslant l)$ von n erstreckt. Wegen $Q(m_1 m_2) = Q(m_1)Q(m_2)$ gilt:

$$\psi(n) = \sum_{2r' \leqslant r} Q(p^{r-2r'}) \cdot \sum_{2s' \leqslant s} Q(q^{s-2s'}) \cdot \dots \cdot \sum_{2l' \leqslant l} Q(u^{l-2l'})$$

und

$$\sum Q(p^{r-2r'}) = p^r + p^{r-1} + \dots + p + 1$$

also

$$\psi(n) = (p^r + p^{r-1} + \dots + p + 1)(q^s + q^{s-1} + \dots + q + 1) \dots (u^l + u^{l-1} + \dots + u + 1).$$

Da es zu jedem Primteiler l der Grundzahl d und zu jeder Maximalordnung genau ein unzerlegbares Ideal der Norm l, nämlich ein Primideal gibt, so gibt es zu jedem t, das nur Diskriminantenprimteiler enthält und zu jeder Maximalordnung genau ein ganzes $\mathfrak{o}$-Linksideal $\mathfrak{a}$ mit $n(\mathfrak{a}) = t$; $\mathfrak{a}$ ist nach dem Gesagten sogar immer zweiseitig. Hierbei hat man nicht darauf zu achten, ob das Ideal $\mathfrak{a}$ primitiv ist oder nicht, da ja das Rechnen mit Primidealen kommutativ ist. Aus dem 4. Hilfssatz ergibt sich, daß man alle Ideale der Norm $t \cdot n$, wo $(n, d) = 1$ und t nur Diskriminantenprimteiler enthält, bekommt, indem man alle Idealprodukte $\mathfrak{a}\mathfrak{b}$ betrachtet mit $n(\mathfrak{a}) = t$, $n(\mathfrak{b}) = n$.

Damit ist die in unserem Satze aufgestellte Behauptung in voller Allgemeinheit bewiesen.

III. Darstellungszahlen für Normenformen

In dem folgenden Abschnitt sollen Sätze hergeleitet werden, die Auskunft geben über die Anzahl Möglichkeiten, eine beliebige, aber feste ganzrationale Zahl m durch eine vorgelegte ganze quaternäre quadratische Stammform mit quadratischer Diskriminante darzustellen. Diese quadratischen Formen können nach dem Vorangehenden als Normenformen von Idealen in einer geeigneten Quaternionenalgebra aufgefaßt werden. Wir beginnen daher mit

1. Darstellungszahlen für positive Normenformen

Es sei f die (positive) Normenform des Ideals $\mathfrak{a}$. Das Ideal $\mathfrak{a}$ habe die Linksordnung $\mathfrak{o}_l$, die Rechtsordnung $\mathfrak{o}_r$. A sei die durch das Ideal $\mathfrak{a}$ bestimmte Idealklasse, $A = \{p\mathfrak{a}q \mid n(pq) > 0\}$.

3. Satz. *Damit f eine ganzrationale Zahl m darstellt, ist notwendig und hinreichend, daß es in der zu A rechtsinversen Idealklasse A^{-1} ein ganzes $\mathfrak{o}_r$-Linksideal der Norm m gibt.*

Beweis. Es ist $n(q) = n(\mathfrak{a}) f(x_q)$ für $q \in \mathfrak{a}$. Es sei $f(\overset{\circ}{x}_i) = m$ also $n(\overset{\circ}{q}) = n(\mathfrak{a})m$; $\mathfrak{q} = \mathfrak{o}_l \overset{\circ}{q}$ ist dann ein Hauptideal mit den Ordnungen $\mathfrak{o}_l$, $\overset{\circ}{q}^{-1}\mathfrak{o}_l\overset{\circ}{q}$. Man hat also eine Darstellung $\mathfrak{q} = \mathfrak{a} \cdot \mathfrak{b}$, $\mathfrak{b}$ ganz, wo $\mathfrak{b}$ die Ordnungen $\mathfrak{o}_r$,

$\overset{\circ}{q}^{-1}\mathfrak{o}_l\overset{\circ}{q}$ besitzt. $\mathfrak{b}$ liegt in der zu A rechtsinversen Idealklasse A^{-1} und wegen des Normensatzes folgt:

$$n(\mathfrak{b}) = m\ .$$

Hat man umgekehrt ein $\mathfrak{o}_r$-Linksideal $\mathfrak{b}$ aus A^{-1} mit der Norm m, so hat man eine Gleichung $\mathfrak{q} = \mathfrak{a}_r\,{}_r\mathfrak{b}$, wobei $\mathfrak{q}$ ein Hauptideal ist, $\mathfrak{q} = (q)$. Aus dem Normensatz folgt $n(q) = n(\mathfrak{a})m$ und es ist $q \in \mathfrak{a}$, also $n(\mathfrak{a})f(q) = n(\mathfrak{a})m$, $f(q) = m$ q.e.d.

Es gibt offenbar soviele verschiedene Darstellungen von m durch f, als es in $\mathfrak{a}$ Quaternionen gibt mit der Norm $n(\mathfrak{a})m$. Betrachten wir für einen Moment nur solche p, $q \in \mathfrak{a}$ mit $n(p) = n(q) = n(\mathfrak{a})m$, die sich nicht bloß um eine Einheit ε aus $\mathfrak{o}_l$ als Linksfaktor unterscheiden: $p \neq \varepsilon q$, $\varepsilon \in \mathfrak{o}_l$, $n(\varepsilon) = 1$. Der Beweis des vorangehenden Satzes zeigt, daß jedem solchen p eineindeutig eines der ganzen $\mathfrak{o}_r$-Linksideale der Norm m aus der Idealklasse A^{-1} zugeordnet ist. Wir erhalten so den

4. Satz. *Es sei f positive Normenform des Ideals $\mathfrak{a}$ mit den Ordnungen $\mathfrak{o}_l$, $\mathfrak{o}_r$. A sei die durch $\mathfrak{a}$ bestimmte Idealklasse und A^{-1} die zu A rechtsinverse Idealklasse. Die Anzahl Darstellungen von m durch f ist dann gleich dem Produkt aus der Anzahl der Einheiten in $\mathfrak{o}_l$ mit der Anzahl der ganzen $\mathfrak{o}_r$-Linksideale der Norm m aus A^{-1}.*

Bemerkung. Diese $\mathfrak{o}_r$-Linksideale in A^{-1} sind alle *rechtsäquivalent*. Es seien nämlich $\mathfrak{c}$, $\mathfrak{d}$ zwei beliebige $\mathfrak{o}_r$-Linksideale aus A^{-1}. Dann ist $(q) = \mathfrak{a}_r\,{}_r\mathfrak{c}$, $(p) = \mathfrak{a}_r\,{}_r\mathfrak{d}$ und $(q) = \mathfrak{o}_l q$, $(p) = \mathfrak{o}_r p$, also $(q) = (p)p^{-1}q$ schließlich $\mathfrak{c} = \mathfrak{d}\cdot p^{-1}q$ mit $n(pq) > 0$, da $n(p) > 0$, $n(q) > 0$ in $\mathfrak{A}$.

Betrachtet man an Stelle der $\mathfrak{o}_r$-Linksideale in A^{-1} die entsprechenden konjugierten $\mathfrak{o}_r$-Rechtsideale in A, so erhält man auf Grund des letzten Satzes und der eben gemachten Bemerkung den

5. Satz. *Es sei f positive Normenform des Ideals $\mathfrak{a}$ mit den Ordnungen $\mathfrak{o}_l$, $\mathfrak{o}_r$. Die Anzahl der Darstellungen der Zahl m durch die Form f ist gleich der Anzahl der Einheiten in $\mathfrak{o}_l$, multipliziert mit der Anzahl der ganzen $\mathfrak{o}_r$-Rechtsideale der Norm m in der durch $\mathfrak{a}$ bestimmten Linksäquivalenzklasse.*

Es sei jetzt ${}_r\mathfrak{b}_s$ ein beliebiges ganzes $\mathfrak{o}_r$-Linksideal der Norm m, das nicht in A^{-1} liegt. Weiter sei $\mathfrak{m} = \mathfrak{o}_s m$, woraus man die Gleichung $\mathfrak{m} = {}_s\mathfrak{a}_r\,{}_r\mathfrak{b}_s$ für ein geeignetes ganzes ${}_s\mathfrak{a}_r$ erhält. Weiter ist $n({}_s\mathfrak{a}_r) = m \in {}_s\mathfrak{a}_r$. Zu ${}_s\mathfrak{a}_r$ gehört eine Normenform g, die zu f nicht äquivalent ist:

$$n(q_x) = n({}_s\mathfrak{a}_r)g(x_q) = mg(x_q) \quad \text{für} \quad q_x \in {}_s\mathfrak{a}_r\ .$$

Wegen $m \in {}_s\mathfrak{a}_r$ folgt $n(m) = m^2 = mg(x_m)$, $g(x_m) = m$. g stellt also m dar. Jetzt

kann man dieselben Überlegungen von vorhin anwenden, das heißt im 4. Satz f durch g und $\mathfrak{o}_l$ durch $\mathfrak{o}_s$ ersetzen, also:

6. Satz. *Man verteile alle ganzen $\mathfrak{o}_r$-Linksideale ${}_r\mathfrak{b}$ der Norm m in Klassen äquivalenter Ideale $A_1^{-1}, A_2^{-1}, \ldots, A_n^{-1}$. Zu jeder linksinversen Klasse $A_1, A_2, \ldots A_n$ gehört eine Form $f_1, f_2, \ldots f_n$ und zugehörige Linkshauptform $h_1, h_2, \ldots, h_n$. In A_i^{-1} mögen a_i Ideale ${}_r\mathfrak{b}$ liegen, e_i sei die Anzahl der Einsdarstellungen von h_i. Dann wird m durch die Gesamtheit der Formen $f_1, f_2, \ldots, f_n$ auf $\Sigma e_i a_i$ Arten dargestellt.*

2. Darstellungszahlen durch indefinite Normenformen

Ist die Normenform f des Ideals $\mathfrak{a}$ eine *indefinite* Form, so erhält man aus einer Darstellung von m durch f eine unendliche Serie von Darstellungen. Wählt man dann aus jeder solchen Serie von Darstellungen eine einzige aus (das heißt, daß man im vorangehenden Beweis alle zu einem Quaternion q in $\mathfrak{a}$ mit der Norm $n(\mathfrak{a})m$ linksassoziierten Quaternionen εq zu einem System zusammenfaßt und man an Stelle aller Quaternionen εq mit der Norm $n(\mathfrak{a})m$ nur diese Systeme von zueinander linksassoziierten Quaternionen εq auszählt), dann erhält man wegen des 2. Satzes in II und dem vorangehenden Beweis ohne Mühe das

Ergebnis. Die Anzahl der wesentlich verschiedenen Darstellungen einer Zahl m durch die Gesamtheit der indefiniten Formen $f_1, f_2, \ldots f_n$ ist gleich der Summe aller positiven, zu d primen Teiler von m.

Nun gibt es aber in einer indefiniten Quaternionenalgebra nur eine einzige Idealklasse (M. EICHLER, Neuere Ergebnisse der Theorie der einfachen Algebren, Jber. Deutsch. Math. Verein. 47 (1937) 209); man erhält also das folgende Theorem:

7. Satz. *Ist f eine indefinite Normenform, dann ist die Anzahl der wesentlich verschiedenen Darstellungen von m durch f gleich der Summe aller Teiler von m, die zu d prim sind.*

3. Beispiele

Der 4. Satz über Darstellungszahlen positiv definiter Normenformen läßt sich in drei verschiedenen Spezialfällen besonders einfach anwenden:

a) *wenn die darzustellende Zahl m nur Diskriminantenprimteiler enthält,*

b) *wenn die darzustellende Zahl m eine Primzahl ist, die zu d prim ist,*

c) *wenn die Idealklassenzahl der Algebra $\mathfrak{A}$ eins ist.*

a) Es sei f Normenform des Ideals $\mathfrak{a}$ mit der Linksordnung $\mathfrak{o}$. Enthält die darzustellende Zahl m nur Diskriminantenprimteiler, $m = \Pi t_i^{\nu_i}$, $t_i \mid d$, so gibt es nach dem 2. Satz in II genau ein $\mathfrak{o}$-Linksideal mit der Norm m. *Stellt also f die Zahl m dar, dann ist die Anzahl der verschiedenen Darstellungen von m durch f gleich der Anzahl der Einheiten in $\mathfrak{o}$.*

b) Ist die darzustellende Zahl hingegen eine Primzahl p mit $(p, d) = 1$, dann gibt es $p + 1$ ganze $\mathfrak{o}$-Linksideale der Norm p und alle diese Ideale sind äquivalent nach dem 1. Satz in II. Man erhält so das **Ergebnis:** *Ist f eine beliebige Normenform, die die Primzahl p mit $(p, d) = 1$ darstellt, dann beträgt die Anzahl der verschiedenen Darstellungen von p durch f das $(p + 1)$-fache der Anzahl Einheiten von $\mathfrak{o}$.*

c) Ist die Idealklassenzahl der Algebra $\mathfrak{A}$ gleich 1, so ist die (einzige) Normenform Normenform einer Maximalordnung $\mathfrak{o}$, stellt also nach dem 3. Satz *alle* ganzrationalen Zahlen m dar. Man hat also das **Ergebnis:** *Die Anzahl der Darstellungen einer beliebigen festen Zahl m durch die Form f ist gleich dem Produkt aus der Anzahl der Einheiten von $\mathfrak{o}$ mit der Summe aller zu d primen Teiler von m.*

Um zu diesem letzten Falle Beispiele zu haben, leiten wir drei spezielle Ergebnisse her, die man bei DICKSON dargestellt findet[6]).

A) Wir betrachten die sogenannte *Hurwitzsche Algebra* der gewöhnlichen Quaternionen. Diese Algebra wird erzeugt von den vier Elementen $1, i, j, ij$ mit der Multiplikationstafel: $i^2 = -1$, $j^2 = -1$, $ij + ji = 0$, $1i = i$, $1j = j$, $1 \cdot ij = ij$. Man hat also für die Norm eines Quaternions

$$q = x_1 + x_2 \cdot i + x_3 j + x_4 ij : n(q) = x_1^2 + x_2^2 + x_3^2 + x_4^2 .$$

In der Hurwitzschen Quaternionenalgebra hat man für zwei ganze Quaternionen einen euklidischen Divisionsalgorithmus (DICKSON, S. 163), also ist jedes Ideal Hauptideal, die Idealklassenzahl also gleich 1. Diese (einzige) Idealklasse kann repräsentiert werden durch die Maximalordnung (DICKSON, S. 157)[7]):

$$\mathfrak{o} = (1, i, j, \tfrac{1}{2}(1 + i + j + ij)) .$$

Für die zugehörige Normenform findet man sofort:

$$f = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_1 x_4 + x_2 x_4 + x_3 x_4$$

und für die Diskriminante von f gilt $D = d^2 = 2^2$.

---

[6]) Einige dieser Ergebnisse sind zuerst von HURWITZ gefunden worden. Wir verweisen des allgemeinen Zusammenhangs wegen auf die Darstellung von DICKSON.

[7]) Vgl. Fußnote 6.

Setzt man $f(x_i) = 1$, so erhält man vierundzwanzig Einheiten von $\mathfrak{o}$, nämlich ± 1, $\pm i$, $\pm j$, $\pm ij$, $\frac{1}{2}(\pm 1 \pm i \pm j \pm ij)$[7]) (DICKSON, S. 180). Wir erhalten also den **Satz:** *Die Anzahl Darstellungen einer beliebigen Zahl m durch die quadratische Form $f = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_4(x_1 + x_2 + x_3)$ beträgt 24mal die Summe aller ungeraden Teiler von m.* (Vgl. dazu Satz 17, DICKSON, S. 180.)

B) Betrachten wir die Algebra $\mathfrak{A} = (1, u, v, uv)$ mit der Multiplikationstafel:

$$u^2 = -1, \quad v^2 = -3, \quad uv + vu = 0, \quad 1u = u, \quad 1v = v, \quad 1 \cdot uv = uv,$$

so erhält man für die Norm eines Quaternions $q = x_1 + x_2 u + x_3 v + x_4 uv$ die Form $n(q) = x_1^2 + x_2^2 + 3x_3^2 + 3x_4^2$. In dieser Algebra ist aus demselben Grunde wie bei der Hurwitzschen Algebra die Idealklassenzahl gleich 1. Eine Maximalordnung ist gegeben durch $\mathfrak{o} = (1, u, \frac{1}{2}(u + v), \frac{1}{2}(1 + uv))$. Für die zugehörige Normenform findet man $f = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_1 x_4 + x_2 x_3$ und für ihre Diskriminante D, $D = d^2 = 3^2$. In $\mathfrak{o}$ gibt es zwölf Einheiten, nämlich ± 1, $\pm u$, $\pm \frac{1}{2}(u + v)$, $\pm \frac{1}{2}(1 + uv)$, $\pm \frac{1}{2}(v - u)$, $\pm \frac{1}{2}(uv - 1)$ (DICKSON, S. 170), so daß wir das folgende **Ergebnis** erhalten: *Die Anzahl der Darstellungen einer beliebigen ganzrationalen Zahl m durch die Form $x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_1 x_4 + x_2 x_3$ beträgt 12mal die Summe aller zu 3 primen Teiler von m.* (Vgl. dazu Satz 19, DICKSON, S. 181).

C) Betrachten wir zum Schluß noch eine *indefinite* Form. Wir gehen dazu aus von der Quaternionenalgebra, die aus der vorhergehenden entsteht, wenn man in der Multiplikationstafel die Zahl 3 durch die Zahl -3 ersetzt, also

$$u^2 = -1, \quad v^2 = 3, \quad uv + vu = 0.$$

Es ist dann also $n(x_1 + x_2 u + x_3 v + x_4 uv) = x_1^2 + x_2^2 - 3x_3^2 - 3x_4^2$. Genau wie in den vorangehenden Fällen ist in dieser Algebra jedes Ideal Hauptideal, also die Idealklassenzahl gleich 1. Eine Maximalordnung dieser Algebra ist gegeben durch (DICKSON, S. 160)

$$\mathfrak{o} = (1, u, v, \tfrac{1}{2}(1 + u + v + uv)).$$

Für die zugehörige Normenform erhält man die Form

$$f = x_1^2 + x_2^2 - 3x_3^2 - x_4^2 + x_1 x_4 + x_2 x_4 - 3x_3 x_4.$$

Ihre Diskriminante D beträgt $D = d^2 = 6^2$. Also hat man den **Satz:** *Die Anzahl der wesentlich verschiedenen Darstellungen einer beliebigen ganzrationalen Zahl m durch die Form $x_1^2 + x_2^2 - 3x_3^2 - x_4^2 + x_1 x_4 + x_2 x_4 - 3x_3 x_4$ ist gleich der Summe aller zu 6 primen Teiler der Zahl m.* (Vgl. dazu Satz 21, DICKSON, S. 181).

IV. Die Automorphismen positiver Normenformen

Aus den drei am Anfang von II genannten BRANDTschen Sätzen ergeben sich in ziemlich direkter Weise die *Automorphismenanzahlen* von *positiven* Normenformen. Es sei $\mathfrak{o}$ eine beliebige Maximalordnung der Algebra $\mathfrak{A}$. Wir betrachten die Gruppe $\mathfrak{H}_\mathfrak{o}$ aller zweiseitigen $\mathfrak{o}$-Hauptideale. Diese Gruppe $\mathfrak{H}_\mathfrak{o}$ besteht aus *endlich* vielen ganzen und primitiven Hauptidealen und ihren rationalen Multipla, denn die Norm jedes ganzen und primitiven zweiseitigen Ideals ist nach Satz A und Satz B ein Teiler t von d, und zu jedem solchen Teiler t gibt es genau ein ganzes und primitives zweiseitiges $\mathfrak{o}$-Ideal der Norm t. Die Gruppe $\mathfrak{H}_\mathfrak{o}$ ist also charakterisiert durch die Menge $H_\mathfrak{o}$ aller Teiler t von d, die Normen von $\mathfrak{o}$-Hauptidealen sind. Wir multiplizieren zwei Teiler t', t'' in $H_\mathfrak{o}$ und lassen dabei die im Produkt eventuell auftretenden quadratischen Faktoren weg. Bei dieser «neuen» Multiplikation wird $H_\mathfrak{o}$ zu einer endlichen Gruppe, deren Elemente gerade die Normen aller ganzen und primitiven $\mathfrak{o}$-Hauptideale sind (BRANDT, S. 24f.). Diese Behauptung ergibt sich aus Satz B.

Es sei nun f Normenform des Ideals $\mathfrak{a}$ mit den Ordnungen $\mathfrak{o}_l$, $\mathfrak{o}_r$. Weiter seien $H_{\mathfrak{o}_l}$, $H_{\mathfrak{o}_r}$ die Gruppen (im obigen Sinne) der Teiler t von d, die zu den Gruppen $\mathfrak{H}_{\mathfrak{o}_l}$, $\mathfrak{H}_{\mathfrak{o}_r}$ der zweiseitigen Hauptideale von $\mathfrak{o}_l$ bzw. $\mathfrak{o}_r$ gehören.

Ein Automorphismus von f wird geliefert durch eine Transformation

$$\mathfrak{a} = p\mathfrak{a}q^{-1}, \qquad \mathfrak{a}q = p\mathfrak{a} \tag{1}$$

wobei die Quaternionen p und q ganz und primitiv angenommen werden können. Aus (1) folgt

$$n(p) = n(q)\ . \tag{2}$$

Durch Vergleichen der Ordnungen folgt

$$\mathfrak{o}_l = p\mathfrak{o}_l p^{-1} \text{ oder } \mathfrak{o}_l p = p\mathfrak{o}_l \text{ und } \mathfrak{o}_r = q^{-1}\mathfrak{o}_r q \text{ oder } \mathfrak{o}_r q = q\mathfrak{o}_r\ ,$$

so daß also p und q in $\mathfrak{o}_l$ bzw. $\mathfrak{o}_r$ *gleichseitige* Hauptideale erzeugen. Die ganzrationale Zahl $t = n(p) = n(q)$ liegt also in $H_{\mathfrak{o}_l} \frown H_{\mathfrak{o}_r}$. Umgekehrt gehört natürlich zu einem solchen t ein Automorphismus von f.

Ist $\mathfrak{a} = (a_1, a_2, a_3, a_4)$ und $\mathfrak{a} = p\mathfrak{a}q^{-1}$, so ist pa_1q^{-1}, pa_2q^{-1}, pa_3q^{-1}, pa_4q^{-1} eine Basis von $p\mathfrak{a}q^{-1}$ (AEBERLI, S. 236):

$$\mathfrak{a} = p\mathfrak{a}q^{-1} = (pa_1q^{-1}, \ldots, pa_4q^{-1})\ . \tag{3}$$

Durch die Gleichung (3) wird genau dann der identische Automorphismus von f induziert, wenn $p = q = \pm 1$ gilt. Wird nämlich durch (3) der identische Automorphismus erzeugt, so gilt $pa_iq^{-1} = a_i$ $(i = 1, 2, 3, 4)$ oder $pxq^{-1} = x$ für alle x in $\mathfrak{a}$. In $\mathfrak{a}$ gibt es sicher eine rationale Zahl s, also ist $psq^{-1} = s$,

woraus $p = q$, also $pxp^{-1} = x$ für alle x in $\mathfrak{a}$ folgt. Da $\mathfrak{a}$ eine Basis der ganzen Algebra enthält, liegt p also im Zentrum der Algebra und ist somit rational. Das Quaternion p wurde aber ganz und primitiv angenommen, somit kann nur $p = \pm 1$ sein. Erzeugt die Transformation $\mathfrak{a} = p'\mathfrak{a}q'^{-1}$ denselben Automorphismus von f wie die Transformation (3), dann gilt $p'a_iq'^{-1} = pa_iq^{-1}$ für $i = 1, 2, 3, 4$ oder $(p^{-1}p')x(q^{-1}q')^{-1} = x$ für alle x in $\mathfrak{a}$, woraus $p^{-1}p' = q^{-1}q' = \pm 1$.

Gilt (1), so gilt auch $\mathfrak{a} = (ep)\mathfrak{a}(\varepsilon q)^{-1}$ für beliebige Einheiten e_1, ε, $e \epsilon \mathfrak{o}_l$, $\varepsilon \epsilon \mathfrak{o}_r$. Man hat also, wenn man gleichzeitigen Vorzeichenwechsel von e und ε berücksichtigt, das Ergebnis

8. Satz. *Ist f Normenform des Ideals $\mathfrak{a}$ mit den Ordnungen $\mathfrak{o}_l$, $\mathfrak{o}_r$, dann gibt es $\frac{1}{2}(e_l \cdot e_r \cdot k)$ Automorphismen der Form f. Dabei bedeuten e_l, e_r die Anzahl Einheiten in $\mathfrak{o}_l$ bzw. $\mathfrak{o}_r$; k bedeutet die Anzahl Elemente in $H_{\mathfrak{o}_l} \frown H_{\mathfrak{o}_r}$.*

Korollar. *Ist $\mathfrak{o}$ eine Maximalordnung, dann gibt es $\frac{1}{2}(e \cdot k)$ Automorphismen des Ringes $\mathfrak{o}$. Dabei bedeutet e die Anzahl der Einheiten von $\mathfrak{o}$ und k die Anzahl der Elemente in $H_{\mathfrak{o}}$.*

Beweis. In (1) sei $\mathfrak{a}$ eine Maximalordnung, etwa $\mathfrak{o} = p\mathfrak{o}q^{-1}$. Bei einem Ringautomorphismus geht die Eins in sich über: $1 = p1q^{-1}$, also erhalten wir statt (2) hier die schärfere Bedingung $p = q$. $\mathfrak{o}$ hat sich selbst als Links- und Rechtsordnung, so daß k tatsächlich die Anzahl Elemente in $H_{\mathfrak{o}}$ ist.

Beispiel. Als Anwendung des letzten Satzes betrachten wir nochmals die Hurwitzsche Algebra $\mathfrak{A}$ und in $\mathfrak{A}$ die Maximalordnung

$$\mathfrak{o} = (1, i, j, \tfrac{1}{2}(1 + i + j + ij)),$$

das heißt den größten Ring ganzer Quaternionen, der die Elemente i, j enthält (vgl. Abschnitt II.3). Der Ring $\mathfrak{o}$ besitzt 24 Einheiten, $e = 24$. $H_{\mathfrak{o}}$ enthält die beiden Zahlen 1 und 2, da $d = 2$ und in $\mathfrak{A}$ jedes Ideal Hauptideal ist. Die zugehörige Normenform $f = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_1x_4 + x_2x_4 + x_3x_4$ besitzt also $\frac{1}{2}(e^2k) = 24^2$ Automorphismen. Der Ring $\mathfrak{o}$ besitzt $\frac{1}{2}(ek) = 24$ Automorphismen. Dieses letzte Ergebnis ist von Hurwitz direkt hergeleitet worden (A. Hurwitz, Zahlentheorie der Quaternionen, Berlin 1919). In genau derselben Weise findet man natürlich, daß die Form (vgl. Abschnitt II.3): $x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_1x_4 + x_2x_3$ 12^2 Automorphismen besitzt.

V. Anhang: Die Ergebnisse von FATOU und HUMBERT über binäre hermitesche Formen

FATOU und HUMBERT haben Sätze über hermitesche Formen bewiesen, die sich im Falle einer einzigen Formenklasse bequem als Sätze über gewisse quaternäre quadratische Formen mit quadratischer Diskriminante aussprechen lassen.

Es sei $F(x,y) = ax\bar{x} + bx\bar{y} + \bar{b}\bar{x}y + cy\bar{y}$ eine binäre hermitesche Form, das heißt es ist $x = x_1 + ix_2$, $y = y_1 + iy_2$, $b = b_1 + ib_2$, $\bar{x} = x_1 - ix_2$, ...; $a, c, x_1, x_2, y_1, y_2, b_1, b_2$, ganzrational. Die Invariante $\Delta = b\bar{b} - ac$ heißt die Determinante der Form $F(x,y)$. Es gilt dann: Die Form $F(x,y)$ ist *definit*, falls $\Delta < 0$. Ist hingegen $\Delta > 0$, dann ist die Form $F(x,y)$ *indefinit* (CH. HERMITE, Oeuvres I, Paris, 1905, S. 240).

Zwei hermitesche Formen $F(x,y)$, $G(x',y')$ derselben Determinante heißen *äquivalent*, falls es eine Substitution

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \qquad ad - bc = 1 \tag{1}$$

gibt mit ganzen komplexen Zahlen a, b, c, d.

Eine hermitesche Form $F(x,y) = ax\bar{x} + bx\bar{y} + \bar{b}\bar{x}y + cy\bar{y}$ heißt *eigentlich primitiv*, falls $a, b, \bar{b}, c$ keinen gemeinsamen Faktor besitzen und a, c nicht gleichzeitig gerade sind.

Schreibt man

$$x = x_1 + ix_2\,, \qquad y = x_3 + ix_4 \tag{2}$$

so erhält man aus $F(x,y)$ eine quaternäre quadratische Form $f(x_i)$:

$$F(x,y) = \sum_1^4 a_{ik} x_i x_k = f(x_i) \qquad a_{ik} = a_{ki}$$

mit

$$a_{11} = a_{22} = a\,,\ a_{33} = a_{44} = c\,;\ a_{12} = a_{34} = 0\,,\ a_{13} = a_{24} = b_1\,,\ a_{14} = -a_{23} = b_2\,.$$

Man findet durch Ausrechnen

$$\Delta^2 = (b\bar{b} - ac)^2 = |a_{ik}| = \frac{1}{16}\left|\frac{\partial^2 f}{\partial x_i\,\partial x_k}\right|\,. \tag{3}$$

Selbstverständlich kann man aus der Form $F(x,y)$ auch alle quaternären quadratischen Formen $g(x_i)$ gewinnen, die sich von $f(x_i)$ nur durch Vertauschung der Indices unterscheiden. Man hat dazu einfach die Indices in (2) entsprechend zu vertauschen.

Aus (3) ergibt sich, daß die als quaternäre Form $f(x_i)$ aufgefaßte binäre

hermitesche Form $F(x, y)$ eine *quadratische* Diskriminante besitzt. Schreibt man die Transformation (1) als reelle Substitution:

$$x_i = \sum_1^4 \alpha_{ik} x_k \tag{4}$$

so findet man

$$|\alpha_{ik}| = (ad - bc)(\overline{ad} - \overline{bc}) . \tag{5}$$

Sind also zwei hermitesche Formen $F(x, y)$, $G(x', y')$ äquivalent im Sinne von (1), dann sind die zugehörigen quaternären Formen $f(x_i)$, $g(x_i')$ äquivalent mit der unimodularen Substitution (4).

FATOU betrachtete *positive, eigentlich primitive* binäre hermitesche Formen $F(x, y)$: $F(x, y) = ax\bar{x} + bx\bar{y} + \bar{b}\bar{x}y + cy\bar{y}$, $\Delta < 0$, $(a, 2b_1, 2b_2, c) = 1$ wo $b = b_1 + ib_2$. Sind $F, F', F'', \ldots$ die Repräsentanten der verschiedenen Äquivalenzklassen, so gilt (C. R. Acad. Sci., Paris, 142 (1906) S. 505–506 und 166 (1918), S. 582 (Korrekturen)):

$$\frac{1}{k}\Sigma F^{-1} + \frac{1}{k'}\Sigma F'^{-1} + \ldots = \Sigma\frac{1}{n^s}\Sigma\frac{1}{n^{s-1}} \qquad s > 2 \tag{6}$$

Die Summen linkerhand erstrecken sich über die ganzen komplexen Zahlenpaare (x, y), für die die entsprechende Form eine zu 2Δ prime Zahl darstellt, während die Summation rechterhand sich über alle zu 2Δ primen Zahlen n erstreckt; $k^{(\nu)}$ bedeutet die Anzahl Automorphismen von $F^{(\nu)}$.

Schreibt man für das Produkt rechts $\sum_n \frac{1}{n^s} \sum_n \frac{1}{n^{s-1}} = \sum_{n', n''} \frac{n'}{(n' n'')^s}$ und faßt die Glieder mit gleichem Nenner zusammen, so folgt $\sum_n \frac{1}{n^s} \sum_n \frac{1}{n^{s-1}} = \sum_n \frac{\psi(n)}{n^s}$, wo $\psi(n)$ gleich der Summe aller Teiler von n ist. Zählt man eine Darstellung einer Zahl m durch $F^{(\nu)}$ $\frac{1}{k^{(\nu)}}$-fach, so erhält man für die Anzahl $\lambda(m)$ der Darstellungen von m durch die Formen $F, F', F'', \ldots$ aus (6)

$$\sum_m \frac{\lambda(m)}{m^s} = \sum_n \frac{\psi(n)}{n^s} \qquad s > 2$$

und daraus

$$\lambda(m) = \psi(m) . \tag{7}$$

Im Falle $\Delta = -1$ hat man eine Formenklasse, die Automorphismenzahl ist 8 und als Repräsentant kann die Form $x\bar{x} + y\bar{y} = x_1^2 + x_2^2 + x_3^2 + x_4^2$ gewählt werden. Eine ungerade Zahl m kann somit auf genau $8\psi(m)$ verschiedene Weisen als Summe von vier Quadraten geschrieben werden. Die Form $x_1^2 + x_2^2 + x_3^2 + x_4^2$ ist, wie man aus dem Beispiel in Abschnitt III.3 ersieht, keine Stammform. Sie besitzt die Diskriminante $D = 4^2$ und ist

ganzzahlig in der Form $x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_4(x_1 + x_2 + x_3)$ mit der Diskriminante $D = 2^2$ enthalten. Diese Stammform läßt sich aber auch nicht als binäre hermitesche Form schreiben, so daß sich das formal gleich lautende Ergebnis von Fatou nicht mit dem unsrigen deckt.

HUMBERT hat für *indefinite* hermitesche Formen, $\Delta > 0$, eine zur Gleichung (6) analoge Gleichung hergeleitet (C. R. Acad. Sci., Paris, 166 (1918) S. 581–587): Geht man zu indefiniten Formen über, so erhält man aus einer Darstellung von m durch $F^{(\nu)}$ eine unendliche Serie von Darstellungen der Zahl m durch $F^{(\nu)}$. Um die bekannten transzendenten Methoden von DIRICHLET anwenden zu können, hat man aus jeder solchen unendlichen Serie von Darstellungen eine einzige Darstellung auszuzeichnen. Unter den Darstellungen einer (festen) Serie $m = F^{(\nu)}(x, y)$ gibt es genau eine Darstellung mit den Eigenschaften:

$$m = F^{(\nu)}(x_0, y_0)$$

(1) Der Punkt $z_0 = x_0/y_0$ liegt innerhalb oder auf dem Rand des zugehörigen Fundamentalbereiches $R^{(\nu)}$

(2) Der Realteil von y_0 ist nicht negativ.

HUMBERT läßt die Bedingung (2) fallen, zeichnet also die beiden Darstellungen $m = F^{(\nu)}(x_0, y_0) = F^{(\nu)}(-x_0, -y_0)$ aus und erhält die zu (6) analoge Gleichung:

$$\Sigma F^{-s} + \Sigma F'^{-s} + \Sigma F''^{-s} + \ldots = 2\Sigma\frac{1}{n^s}\Sigma\frac{1}{n^{s-1}} \qquad s > 2 \tag{8}$$

Die Summen links erstrecken sich über alle ganzen komplexen Zahlen x, y derart, daß (1) $F^{(\nu)}(x, y)$ positiv und zu 2Δ prim ist, (2) der Punkt $z = x/y$ innerhalb oder auf dem Rande von $R^{(\nu)}$ liegt. Die Summe rechts erstreckt sich über alle zu 2Δ primen ganzrationalen n.

Liegt der Punkt $z = x/y$ auf dem Rande von $R^{(\nu)}$, so zählt die entsprechende Darstellung $m = F^{(\nu)}(x, y)$ $\frac{1}{2}$-fach und entsprechen $1/\nu$-fach, falls der Punkt $z = x/y$ auf einer von ν äquivalenten Ecken von $R^{(\nu)}$ liegt. Bezeichnet $\lambda(m)$ die Summe der mit diesen Gewichten versehenen Darstellungsanzahlen von m durch die Formen $F, F', F'', \ldots$, so erhält man entsprechend zu (7)

$$\lambda(m) = 2\psi(m) \tag{9}$$

wenn $\psi(m)$ wieder die Summe aller Teiler von m bedeutet.

Auch dieses Ergebnis deckt sich dem Wortlaut nach mit dem unsrigen bis auf den Faktor 2. HUMBERT zeichnet aber in jeder unendlichen Serie von Darstellungen deren zwei aus, im Gegensatz zur Auszeichnung einer einzigen Darstellung bei uns.

Da die Sätze und Vergleiche über Darstellungsanzahlen besonders übersichtlich sind im Falle einer einzigen Äquivalenzklasse, führen wir noch einige Sätze von HUMBERT an, die angeben, wann dieser Fall eintritt:

Satz: *Die indefiniten, eigentlich primitiven hermiteschen Formen $F(x,y)$ gegebener Determinante Δ bilden in den beiden Fällen $\Delta \equiv 1(2)$, $\Delta \equiv 2(4)$ je eine einzige Äquivalenzklasse* (C. R. Acad. Sci., Paris, 166 (1918), S. 869–870).

Insbesondere bilden also die entsprechenden quaternären quadratischen Formen $f(x_i)$ in diesen beiden Fällen je eine einzige Idealklasse. Und weiter, falls man allgemeiner hermitesche Formen in einem Körper $i\sqrt{d}$ betrachtet, $F(x,y) = a x\bar{x} + b x\bar{y} + \bar{b}\bar{x}y + c y\bar{y}$, $b = b_1 + i\sqrt{d}\,b_2$, $x = x_1 + i\sqrt{d}\,x_2$, $\bar{x} = x_1 - i\sqrt{d}\,x_2, \ldots$, gilt der **Satz:** *Ist $d > 0$ und $d \equiv 1(4)$ oder $d \equiv 2(4)$, so gibt es zu $\Delta \equiv 1(2)$ und $\Delta \equiv 2(4)$ in beiden Fällen genau eine Äquivalenzklasse indefiniter, eigentlich primitiver hermitescher Formen im Körper $i\sqrt{d}$ mit der Determinante Δ, falls d und Δ keinen ungeraden Teiler gemeinsam haben (loc. cit.).*

Für hermitesche Formen in einem quadratischen Körper $i\sqrt{d}$ hat HUMBERT ebenfalls eine der Gleichung (8) entsprechende Gleichung hergeleitet:

Es seien die Ideale $I_1, I_2, \ldots I_h$ Repräsentanten der h Idealklassen des quadratischen Körpers $i\sqrt{d}$ und $F_1, F_2, \ldots F_H$ Repräsentanten der H Klassen eigentlich primitiver positiver hermitescher Formen. Es sei $\bar{I}$ das zum Ideal I konjugierte Ideal und u, v ganze Zahlen des Ideals I, dann ist $m = (I\bar{I})^{-1} F(u,v) = F\left(\frac{u}{I}, \frac{v}{I}\right)$ eine ganzrationale Zahl und man spricht von einer dem Ideal I angehörenden Darstellung von m durch F. Es gilt dann die Gleichung (C. R. Acad. Sci., Paris, 169 (1919), 360–365):

$$s > 2 \quad \sum_{l,c,X,Y} \frac{1}{k_l} F_l^{-s}\left(\frac{X}{I_c}, \frac{Y}{I_c}\right) = h \sum \frac{1}{n^s} \sum \frac{1}{n^{s-1}} \Pi_\omega \left\{1 + \left(\frac{-\Delta}{\omega}\right) \frac{1}{\omega^{s-1}}\right\} \tag{10}$$

$l = 1, 2, \ldots H$, H: Formenklassenzahl; $c = 1, 2, \ldots h$, h: Idealklassenzahl. Die Summation linkerhand erstreckt sich über alle l, c und alle Terme $\left(\frac{X}{I_c}, \frac{Y}{I_c}\right)$ mit der Eigenschaft: X, Y sind beliebige ganze Zahlen des Ideals I_c derart, daß der Wert $F_l\left(\frac{X}{I_c}, \frac{Y}{I_c}\right)$ zu 2Δ prim ist. k_l ist wieder die Automorphismenanzahl von F_l. Rechts ist über alle zu 2Δ primen ganzrationalen n zu summieren, während sich das Produkt Π_ω über alle ungeraden Primteiler ω von d erstreckt.

Für $d = 1$ erhält man aus (10) offensichtlich die Gleichung (6) von FATOU zurück. Aus (10) lassen sich völlig analog zum Vorangehenden Sätze über

Darstellungszahlen ableiten. Wegen dem Faktor $\Sigma n^{-s}\Sigma n^{-s+1}$ rechts ist die Darstellungsanzahl jedesmal ein Vielfaches der Summe aller Teiler der dargestellten Zahl.

LITERATUR

[1] G. Aeberli, *Der Zusammenhang zwischen quaternären quadratischen Formen und Idealen in Quaternionenringen.* Comment. Math. Helv. *33* (1959), 212–239.

[2] H. Brandt, *Idealtheorie in Quaternionenalgebren.* Math. Ann. *99* (1928), 1–29.

[3] L. E. Dickson, *Algebren und ihre Zahlentheorie* (darin enthalten als Kap. XIII: A. Speiser, Idealtheorie in rationalen Algebren), Zürich 1927.

[4] A. Hurwitz, *Zahlentheorie der Quaternionen.* Berlin 1919.

[5] Ch. Hermite, *Oeuvres I.* Paris 1905, 240.

[6] P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie.* Braunschweig, 1894.

[7] C. R. Acad. Sci. Paris, *142* (1906), 505–506.

[8] C. R. Acad. Sci. Paris, *166* (1918), 581–587.

[9] C. R. Acad. Sci. Paris, *169* (1919), 869–870.

[10] M. Eichler, *Quadratische Formen und orthogonale Gruppen.* Berlin 1952.

[11] M. Eichler, *Zur Zahlentheorie der Quaternionen-Algebren.* J. reine angew. Math. 195 (1956) 127–151.

(Eingegangen den 20. November 1959)