Werk

Titel: Mathematische Annalen
Ort: Berlin
Jahr: 1930
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN235181684_0102
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235181684_0102

LOG Id: LOG_0044
LOG Titel: Idealtheoretisehe Deutung der Darstellbarkeit beliebiger natürlicher Zahlen durch quadratische Formen
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

Idealtheoretische Deutung der Darstellbarkeit beliebiger natürlicher Zahlen durch quadratische Formen[1]).

Von

Werner Weber in Göttingen.

Das Problem der Darstellbarkeit natürlicher Zahlen durch quadratische Formen mit ganzen rationalen Koeffizienten und von gegebener Klasse[2]) ist bisher nur auf dem Umweg über die Idealtheorie eines quadratischen Zahlkörpers mit Erfolg anzugreifen. Zum klassischen Bestande dieser Theorie gehört eine bei R. Dedekind[3]) und H. Weber[4]) vorkommende typische Relation, deren Bedeutung sich kurz durch das Schlagwort „darstellbar sein heißt Idealnorm sein" charakterisieren läßt[5]). Allen bisherigen Ergebnissen war nun gemeinsam, daß sie sich notwendigerweise auf den besonderen Fall beschränkten, in welchem die dargestellte Zahl bzw. die gegebene Idealnorm zu einem gewissen Bestandteil der Formendiskriminante, nämlich zu dem nach Abspaltung des Diskriminantenstammes Δ verbleibenden Faktor k^2 (k eine natürliche Zahl) teilerfremd ist. Im allgemeinen Fall versagt das Verfahren.

---

[1]) Die vorliegende Abhandlung ist bis auf geringfügige Änderungen ein Abdruck der von mir im April 1929 bei der mathematisch-naturwissenschaftlichen Fakultät der Universität Göttingen zur Erlangung der Doktorwürde eingereichten Dissertation. Ich habe Fräulein E. Noether für viele Ratschläge dabei zu danken.

[2]) Verzichtet man auf die Klassenbedingung, so wird das Problem arithmetisch wesentlich einfacher und ist als völlig gelöst zu betrachten. Man vergleiche etwa Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, 4. Aufl. (1894), §§ 53—66 und § 91.

[3]) Es handelt sich um § 182 aus dem XI. Supplement des in Fußnote [2]) genannten Buches von Dirichlet und Dedekind. Das hier allein in Frage kommende XI. Supplement wird im folgenden unter „Dedekind" kurz mit „a. a. O." zitiert.

[4]) H. Weber, Lehrbuch der Algebra, 2. Aufl., **3** (1908), §§ 90—101. Im folgenden unter „H. Weber" mit „a. a. O." zitiert.

[5]) Man vergleiche auch Hecke, Theorie der algebraischen Zahlen (1923), Kap. VII, § 53; Fricke, Lehrbuch der Algebra **3** (1928), 2. Abschn., 3. Kap., § 6; Landau, Vorlesungen über Zahlentheorie **3** (1927), XI. Teil, Kap. 3, §§ 2, 3.

Zur Bewältigung dieses Falles kam aus der ganzen Literatur nur eine einzige, bei Dedekind[6]) auftretende Gleichung in Frage, die keine Teilerfremdheitsvoraussetzung enthält, aber andrerseits nicht von Idealen, sondern von beliebigen Moduln aus ganzen oder gebrochenen Zahlen des quadratischen Körpers handelt. Dedekind gewinnt für diese Moduln eine passende Normdefinition und erreicht damit eine scheinbar vollständige Analogie. Es zeigt sich nun freilich sofort, daß dieser Modulbegriff zu allgemein ist, um ein wirklich umkehrbar eindeutiges Verfahren zu liefern. Auch erscheint es recht unbequem, Moduln mit gebrochenen Elementen aufnehmen zu müssen; und überdies weiß man über die allgemeinsten Moduln, selbst aus ganzen Körperzahlen, noch recht wenig. Der Zweck der nachstehenden Arbeit ist es, den Modulbegriff hierbei auf das geeignete Maß einzuschränken. Es wird sich nämlich ergeben, daß man vollständig mit Moduln aus ganzen Elementen, und zwar speziell mit Idealen in den verschiedenen Ordnungen des quadratischen Körpers auskommt. Mehr noch: Die Ideale in einer Ordnung $\mathfrak{n}$ braucht man nicht sämtlich; sondern unter ihnen erscheinen diejenigen Ideale $\mathfrak{c}$ ausgezeichnet, die in keiner umfassenderen Ordnung mehr Ideal sind, d. h. die in einem von Dedekind präzisierten Sinne „der Gleichung $\mathfrak{c}^0 = \mathfrak{n}$ genügen“ oder „die Ordnung $\mathfrak{n}$ haben“. In der Hauptordnung ist diese einschränkende Bedingung natürlich von selbst erfüllt. Geht man aber in eine weniger umfassende Ordnung $\mathfrak{n}$ hinein, so spaltet sich diese Kategorie von Moduln aus ganzen Elementen sofort in zwei verschiedene auf: Moduln $\mathfrak{m}$ mit $\mathfrak{m}^0 = \mathfrak{n}$, die aber nicht notwendig Untermengen von $\mathfrak{n}$ sind, und Ideale $\mathfrak{m}$ in $\mathfrak{n}$, deren Ordnung $\mathfrak{m}^0$ eine echte oder unechte Obermenge von $\mathfrak{n}$ ist[7]). Der Durchschnitt dieser beiden Kategorien erscheint bereits algebraisch ausgezeichnet und ist bisher meines Wissens in der Literatur noch nirgends berücksichtigt worden.

Unter Benutzung dieses Begriffes wird sich zeigen, daß für die Darstellungen von Zahlen durch Formen der Diskriminante $k^2 \Delta$ lediglich die Ideale in derjenigen Ordnung $\mathfrak{n}$ des quadratischen Zahlkörpers von der Diskriminante Δ nötig sind, die den Führer k hat, unter diesen Idealen aber, wie gesagt, nur diejenigen, die zugleich von der Ordnung $\mathfrak{n}$ sind. Beschränkt man sich auf Formen einer gegebenen Klasse K, so gehört dazu eine gewisse Modulklasse M, in der die zugeordneten Ideale zu suchen sind. Wird endlich auch noch die darzustellende natürliche Zahl m vorgeschrieben, so kommen nur Ideale von der Norm m in Betracht. Jedem der so ausge-

---

[6]) A. a. O., § 187, (14).

[7]) Im „teilerfremden“ Falle vereinfacht sich der Zusammenhang insofern, als dann die zweite Kategorie in der ersten steckt. Vgl. Satz 24.

siebten Ideale entsprechen nun, wie sich weiter zeigt, wirklich Darstellungen von m, und zwar vermittels eines genau angebbaren und rechnerisch brauchbaren Algorithmus. Dabei erscheinen bei gegebenem Ideal alle Formen aus K für die Darstellung gleichberechtigt. Aber auch innerhalb einer einzelnen Form können im allgemeinen dem gegebenen Ideal mehrere Darstellungen entsprechen. Es ist eine weitere Aufgabe, die in § 4 behandelt werden wird, die zu demselben Ideal gehörigen Darstellungen, sei es durch dieselbe oder durch verschiedene Formen, zusammenzufassen und ihre Verwandtschaft zahlentheoretisch zu fixieren. Bei festgehaltener Form werden sich diese Darstellungen ein-eindeutig den in der Ordnung $\mathfrak{n}$ gelegenen Einheiten von positiver Norm zuordnen. — Verallgemeinerungen sind dann dadurch möglich, daß man auch das Ideal variiert. Hierfür gibt § 6 ein naheliegendes Beispiel: Gefragt wird nach der Gesamtheit der Darstellungen, deren zugeordnete Ideale bis auf Einheitsfaktoren mit einem gegebenen Ideal übereinstimmen. Die Anzahl dieser Darstellungen läßt sich abermals mit Hilfe von Einheiten kennzeichnen, jedoch nicht in so einfacher Weise wie im bisherigen Fall.

Nach dieser Deutung der Darstellbarkeit ist es dann eine Aufgabe besonderer Art, die für eine allgemeine Ordnung gewonnenen Ergebnisse auf die Hauptordnung zu übertragen. Dieses Problem fällt aus dem Rahmen der vorliegenden Arbeit heraus; doch sollen hierüber in § 7 wenigstens einige erste Sätze bewiesen werden. Es wird sich dabei eine ausgezeichnete Stellung der von Grell[8]) so genannten „Erweiterungsideale“ ergeben. Zugleich lassen sich unter Benutzung dieses Begriffes die klassischen Sätze über die Darstellung zu k teilerfremder Zahlen ohne Mühe einordnen.

§ 1.

Vorbemerkungen.

Eine primitive binäre quadratische Form mit ganzen rationalen Koeffizienten a, b, c, positivem Anfangskoeffizienten a und nichtquadratischer Diskriminante wird im folgenden kurz quadratische Form, noch kürzer Form genannt und, wenn es auf die Benennung der Variablen nicht ankommt, mit $\{a, b, c\}$ bezeichnet. Die Begriffe der Darstellbarkeit bzw. eigentlichen Darstellbarkeit einer Zahl durch eine Form sind bekannt, ebenso die einfachsten Eigenschaften der Formenklassen. Der letztere Begriff soll wiederum in eingeschränkter Bedeutung gebraucht werden: Eine Formenklasse bezeichnet im folgenden bei positiver Diskriminante jede beliebige, bei negativer Diskriminante dagegen nur jede positiv-definite Klasse. Geht

[8]) H. Grell, Beziehungen zwischen den Idealen verschiedener Ringe. Math. Annalen 97 (1927), S. 490—523.

die Form $ax^2 + bxy + cy^2$ durch die ganzzahlige lineare Variablentransformation von der Determinante 1

$$(1) \qquad \begin{cases} x = \alpha x' + \beta y', \\ y = \gamma x' + \delta y' \end{cases}$$

in die Form $a'x'^2 + b'x'y' + c'y'^2$ über, so soll von zwei zugehörigen Darstellungen

$$m = ax^2 + bxy + cy^2,$$
$$m = a'x'^2 + b'x'y' + c'y'^2$$

gesagt werden, daß sie durch die vollständige lineare Substitution (1) auseinander hervorgehen. Eine vollständige lineare Substitution einer Darstellung bezieht sich also auf Variablenwerte und Formen und ändert die dargestellte Zahl nicht.

Ist Δ eine von 1 verschiedene Stammdiskriminante[9]), so bedeutet künftig der „Körper Δ" den quadratischen Zahlkörper mit der Diskriminante Δ, hierin ein Modul eine additive Gruppe beliebiger ganzer oder gebrochener Körperzahlen. Ein Modul heißt ganz, wenn er nur ganze Zahlen enthält. Eine Modulbasis wird durch eckige Klammern ausgedrückt. Ist $\mathfrak{m}$ ein Modul mit endlicher Basis, so sei unter der Ordnung $\mathfrak{m}^0$ von $\mathfrak{m}$ der Ring derjenigen (eo ipso ganzen) Zahlen α des Körpers verstanden, für die der Modul $\alpha\mathfrak{m}$ eine Untermenge von $\mathfrak{m}$ ist. Die einfachsten Sätze über Ordnungen im quadratischen Körper können bei Dedekind[10]) nachgelesen werden; hier finde nur die Tatsache Platz, daß jede Ordnung $\mathfrak{n}$ eine Basisdarstellung von der Gestalt

$$\mathfrak{n} = [1, k\Theta]$$

zuläßt, worin Θ die ganze Zahl $\frac{\Delta + \sqrt{\Delta}}{2}$ und k eine durch $\mathfrak{n}$ eindeutig bestimmte natürliche Zahl, der „Führer" der Ordnung $\mathfrak{n}$, ist.

Der Modul aller Zahlen α, für die $\alpha\mathfrak{m}$ Untermenge von $\mathfrak{m}^0$ ist, wird mit $\mathfrak{m}^{-1}$ bezeichnet.

Für die späteren Untersuchungen ist der Begriff der Norm $N(\mathfrak{m})$ eines Moduls $\mathfrak{m}$ von zweigliedriger Basis besonders wichtig. In Übereinstimmung mit Dedekind[11]) soll hierunter der absolute Betrag der Determinante einer Linearsubstitution mit rationalen Koeffizienten verstanden werden, die eine Basis von $\mathfrak{m}^0$ in eine Basis von $\mathfrak{m}$ überführt.

---

[9]) Eine Diskriminante heißt Stammdiskriminante, wenn sie keinen quadratischen Teiler außer 1 hat, nach dessen Abspaltung eine Diskriminante übrigbleibt. Jede Diskriminante läßt sich eindeutig als Produkt einer Quadratzahl mit einer Stammdiskriminante darstellen.

[10]) A. a. O., S. 642.

[11]) A. a. O., S. 643.

Dedekind zeigt[12]), daß sich jede unverkürzbare zweigliedrige Modulbasis auf die Gestalt

$$[m, m\omega]$$

bringen läßt, worin m eine positive rationale Zahl ist. Ist $\mathfrak{m}$ der zugehörige Modul und bedeutet

$$ax^2 - bx + c = 0$$

die irreduzible quadratische Gleichung mit teilerfremden ganzen rationalen Koeffizienten und positivem Koeffizienten des höchsten Gliedes, der die Zahl ω genügt, so hat die Norm von $\mathfrak{m}$ den Wert

$$N(\mathfrak{m}) = \frac{m^2}{a}. \tag{2}$$

Zugleich ist

$$\mathfrak{m}^0 = [1, a\omega].$$

Bedeutet $\overline{\mathfrak{m}}$ denjenigen Modul, dessen Elemente konjugiert zu denen von $\mathfrak{m}$ sind, so gilt

$$\mathfrak{m}\overline{\mathfrak{m}} = N(\mathfrak{m})\,\mathfrak{m}^0. \tag{3}$$

Für zwei Moduln $\mathfrak{a}$, $\mathfrak{b}$ mit zweigliedriger Basis gilt immer die Gleichung

$$N(\mathfrak{a})\,N(\mathfrak{b}) = N(\mathfrak{a}\mathfrak{b}).$$

Die Einteilung der Moduln in Klassen und deren Zuordnung zu den Formenklassen wird im folgenden von Dedekind (a. a. O., S. 655f.) übernommen und besteht darin, daß man der Form $\{a, b, c\}$ von der Diskriminante $D = k^2\Delta$ die Klasse des Moduls

$$\left[1, \frac{b+\sqrt{D}}{2a}\right]$$ [13]),

d. h. die Gesamtheit der von diesem Modul nur durch Zahlfaktoren positiver Norm unterschiedenen Moduln zuordnet. Jeder Modul dieser Klasse hat die Ordnung $\left[1, \frac{b+\sqrt{D}}{2}\right]$ vom Führer k.

Endlich wird alsbald auch der Begriff des Ideals in einer Ordnung herangezogen werden, der als hinlänglich bekannt gelten kann[14]).

---

[12]) Für das Folgende vgl. Dedekind, a. a. O., S. 640–645.

[13]) $\sqrt{D}$ soll hier und im folgenden, wie üblich, den positiven bzw. positiv-imaginären Wert der Quadratwurzel bedeuten.

[14]) Die von Dedekind in der Arbeit „Über die Anzahl der Idealklassen in den verschiedenen Ordnungen eines endlichen Körpers“ (Festschrift zur Säkularfeier des Geburtstages von Carl Friedrich Gauß, 1877), § 4 gegebene Definition umfaßt nach heutigen Begriffen nur einen Spezialfall. Vgl. Fußnote [22]). — Wohl aber findet sich der Idealbegriff in dem auch heute üblichen Sinne in der 3. Auflage des Buches von Dirichlet und Dedekind (1879), § 172, S. 522. (In der 4. Auflage ist dieser Paragraph fortgefallen, und nur die Fußnote *) auf S. 554 deutet noch auf den allgemeineren Idealbegriff hin.)

An Bezeichnungen ist noch zu merken: Ist α eine Zahl des Körpers, so bedeutet $\bar{\alpha}$ die zu α konjugierte Zahl, $N(\alpha)$ die Norm von α. Derjenige Modul, dessen Elemente konjugiert zu denen des Moduls $\mathfrak{m}$ sind, heiße $\bar{\mathfrak{m}}$. Der Buchstabe $\mathfrak{o}$ bezeichnet stets die Hauptordnung. Mit (a, b) wird der größte gemeinsame Teiler der ganzen rationalen Zahlen a und b bezeichnet; $a|b$ bedeutet „a ist Teiler von b“; $\leqq$ bedeutet Untermenge, $<$ echte Untermenge, $\geqq$ Obermenge, $>$ echte Obermenge, $\in$ das Enthaltensein, $\mathfrak{a} \wedge \mathfrak{b}$ den Durchschnitt der Moduln $\mathfrak{a}$ und $\mathfrak{b}$.

§ 2.

Der $\mathfrak{m}$-Algorithmus.

Satz 1. *Die natürliche Zahl m ist dann und nur dann durch die Formenklasse K darstellbar, wenn es in der zugeordneten Idealklasse von der Ordnung $\mathfrak{n}$ ein Ideal in $\mathfrak{n}$ mit der Norm m gibt.*

Beweis. Es sei $\{a, b, c\}$ eine Form aus der Klasse K von der Diskriminante $D = k^2 \Delta$; x und y seien ganze rationale Zahlen und

$$m = ax^2 + bxy + cy^2. \tag{4}$$

Unter den Wurzeln

$$\frac{1}{a}\,\frac{b \pm \sqrt{D}}{2}$$

der Gleichung $au^2 - bu + c = 0$ sei diejenige, in welcher die Quadratwurzel das positive Vorzeichen hat, mit ω bezeichnet. In der K zugeordneten Modulklasse M, deren Ordnung $\mathfrak{n}$ den Führer k hat, liegt dann nach Definition der Modul $[1, \omega]$ und demnach auch der Modul

$$\mathfrak{c} = a(x + y\bar{\omega})[1, \omega];$$

denn die Norm des Zahlfaktors $a(x + y\bar{\omega})$ hat den Wert

$$a(x + y\bar{\omega})\,a(x + y\omega) = a(ax^2 + bxy + cy^2) = am,$$

ist also positiv. Da $a\omega$, $a\bar{\omega}$ und $a\omega\bar{\omega}$ in $\mathfrak{n}$ liegen, so ist $\mathfrak{c}$ Untermenge von $\mathfrak{n}$ (also insbesondere ein ganzer Modul). Weil aber $\mathfrak{c}$ die Ordnung $\mathfrak{n}$ hat, ist es sogar Ideal in $\mathfrak{n}$. Zugleich ist

$$N(\mathfrak{c}) = am\,N([1, \omega]),$$

nach (2) hierin

$$N([1, \omega]) = \frac{1}{a},$$

also

$$N(\mathfrak{c}) = m\ ^{15}).$$

---

[15]) Meine ursprüngliche Methode, zu diesem Ideal $\mathfrak{c}$ zu gelangen, war etwas umständlicher. Die hier gegebene Fassung verdanke ich einer Bemerkung von Fräulein E. Noether. Ähnliches gilt für den folgenden Rückweg von $\mathfrak{c}$ zur Darstellung.

Umgekehrt sei $\mathfrak{x}$ ein Ideal in $\mathfrak{n}$ von der Norm m, das zur Modulklasse M gehört. Wird zu irgendeiner Form $\{a, b, c\}$ aus K in der obigen Weise der in M gelegene Modul $[1, \omega]$ konstruiert, so liegt im Körper eine Zahl μ von positiver Norm, für die

$$\mu\mathfrak{x} = m[1, \omega]$$

ist. Nach (3) ist

$$\mu m\mathfrak{n} = \mu\mathfrak{x}\bar{\mathfrak{x}};$$

da mit $\mathfrak{x}$ auch $\bar{\mathfrak{x}}$ Untermenge von $\mathfrak{n}$ ist und $\mu\mathfrak{x}$ die Ordnung $\mathfrak{n}$ hat, so kommt

$$\mu m\mathfrak{n} \leqq \mu\mathfrak{x} = m[1, \omega],$$

wegen $1 \in \mathfrak{n}$ also

$$\mu \in [1, \omega].$$

Es gibt demnach zwei ganze rationale Zahlen x und y mit

$$\mu = x + y\omega.$$

Wegen $N(\mu) > 0$ ist nun

$$N(\mu)N(\mathfrak{x}) = N(m)N([1, \omega]),$$

$$N(\mu) = \frac{m^2}{ma} = \frac{m}{a},$$

$$m\bar{\mu}[1, \omega] = \mu\bar{\mu}\mathfrak{x} = N(\mu)\mathfrak{x} = \frac{m}{a}\mathfrak{x},$$

$$\mathfrak{x} = a\bar{\mu}[1, \omega],$$

$$m = N(\mathfrak{x}) = a^2\bar{\mu}\mu N([1, \omega]) = a(x + y\bar{\omega})(x + y\omega) = ax^2 + bxy + cy^2.$$

Das im ersten Teil des Beweises zur Konstruktion des Ideals $\mathfrak{c}$ in $\mathfrak{n}$ angewandte Verfahren ist offenbar bei gegebener Darstellung (4) völlig eindeutig. Es wird auch im weiteren Verlaufe dieser Arbeit eine Rolle spielen und verdient deshalb einen besonderen Namen. Der Modul $[1, \omega]$ wird künftig mit $\mathfrak{m}$, die Zahl $x + y\omega$ mit μ bezeichnet. Die zentrale Stellung des Moduls rechtfertigt die

Definition 1. *Die obige Konstruktion der Zahl ω, des Moduls $\mathfrak{m}$, der Zahl μ und des Ideals $\mathfrak{c}$ sei als der auf die Darstellung* (4) *angewandte $\mathfrak{m}$-Algorithmus bezeichnet. — Das Ideal $\mathfrak{c}$ heißt kurz das der Darstellung* (4) *zugeordnete Ideal.*

Die tiefere Bedeutung[16]) des Ideals $\mathfrak{c}$ erkennt man, wenn man $\mathfrak{c}$ in der allgemeinen Gestalt

$$\mathfrak{c} = (\varrho x + \sigma y)[1, \omega]$$

ansetzt, wo x und y die Variablenwerte der Ausgangsdarstellung bedeuten und ϱ und σ noch freibleibende Körperzahlen sind. Verlangt man, daß

[16]) Diese Überlegung rührt inhaltlich von Fräulein E. Noether her.

die Norm von $\mathfrak{c}$ in dieser Bezeichnungsweise formal gleich der gegebenen quadratischen Form in x und y wird, so ergibt sich:

$$\frac{1}{a}(\varrho x + \sigma y)(\bar{\varrho} x + \bar{\sigma} y) = ax^2 + bxy + cy^2$$
$$= a(x + \omega y)(x + \bar{\omega} y),$$

also bei passender Einheit ε

$$\varrho x + \sigma y = \varepsilon a(x + \omega y) \quad \text{oder} \quad \varrho x + \sigma y = \varepsilon a(x + \bar{\omega} y).$$

Damit $\mathfrak{c}$ Untermenge von $\mathfrak{n}$ ist, genügt es, den zweiten dieser Fälle zu betrachten und $\varepsilon = 1$ zu setzen, womit $\mathfrak{c}$ in der Tat in das oben konstruierte Ideal übergeht.

Der vorige Beweis liefert — da $\{a, b, c\}$ willkürlich in der Klasse K angenommen war — noch den

Satz 2. *Ist $\mathfrak{c}$ ein Ideal in $\mathfrak{n}$, das in der Klasse M liegt und die Norm m hat, so gibt es in jeder Form aus der M zugeordneten Formenklasse mindestens eine Darstellung von m, deren zugeordnetes Ideal $\mathfrak{c}$ ist.*

§ 3.

Der Teiler einer Darstellung.

In Analogie zu einem für den teilerfremden Fall gültigen Satz von H. Weber (a. a. O., § 97, Satz 8) kann man auch im allgemeinen Falle fragen, inwieweit sich die im größten gemeinsamen Teiler der darstellenden Variablenwerte aufgehenden Primfaktoren in den natürlichen Zahlteilern des zugeordneten Ideals wiederfinden und umgekehrt. Hierbei wird sich im folgenden eine ausgezeichnete Stellung der Primteiler des Führers ergeben.

Satz 3. *Es sei t eine von Null verschiedene ganze rationale Zahl. Dann haben die darstellenden Variablenwerte x und y in*

$$m = ax^2 + bxy + cy^2 \tag{4}$$

dann und nur dann den gemeinsamen Teiler t, wenn das zugeordnete Ideal $\mathfrak{c}$ durch t teilbar und überdies der Modul $\frac{\mathfrak{c}}{t}$ wieder Ideal in $\mathfrak{n}$ ist. Zugleich ist dann der Darstellung

$$\frac{m}{t^2} = a\left(\frac{x}{t}\right)^2 + b\frac{x}{t}\frac{y}{t} + c\left(\frac{y}{t}\right)^2 \tag{5}$$

das Ideal $\frac{\mathfrak{c}}{t}$ zugeordnet.

Beweis. 1. Es sei $t|x$, $t|y$. Die Buchstaben ω, $\mathfrak{m}$, μ mögen die Bedeutung aus dem auf (4) angewandten $\mathfrak{m}$-Algorithmus haben. Wendet man diesen auf die Darstellung (5) an, so bleiben ω und $\mathfrak{m}$ erhalten; μ wird ersetzt durch

$$\mu' = \frac{x}{t} + \frac{y}{t}\omega = \frac{\mu}{t}$$

und daher $\mathfrak{c}$ durch

$$\mathfrak{c}' = a\overline{\mu'}\mathfrak{m} = \frac{1}{t}a\bar{\mu}\mathfrak{m} = \frac{1}{t}\mathfrak{c},$$

so daß $\frac{\mathfrak{c}}{t}$ wieder Ideal in $\mathfrak{n}$ ist.

2. Umgekehrt sei $\mathfrak{c}' = \frac{\mathfrak{c}}{t}$ Ideal in $\mathfrak{n}$. Die Zwischenglieder des auf die Darstellung (4) angewandten $\mathfrak{m}$-Algorithmus seien ω, $\mathfrak{m}$, μ. Dann ist

$$\mathfrak{c}'\overline{\mathfrak{m}} \leqq \overline{\mathfrak{m}}, \tag{6}$$

da $\overline{\mathfrak{m}}$ die Ordnung $\mathfrak{n}$ hat und $\mathfrak{c}'$ in $\mathfrak{n}$ liegt. Die linke Seite hat aber wegen (3) den Wert

$$\left(\frac{x}{t} + \frac{y}{t}\bar{\omega}\right) a\mathfrak{m}\overline{\mathfrak{m}} = \left(\frac{x}{t} + \frac{y}{t}\bar{\omega}\right) aN(\mathfrak{m})\mathfrak{n}$$
$$= \left(\frac{x}{t} + \frac{y}{t}\bar{\omega}\right)\mathfrak{n}.$$

Da $\mathfrak{n}$ die Zahl 1 enthält, folgt also mit Rücksicht auf (6)

$$\frac{x}{t} + \frac{y}{t}\bar{\omega} \leqq \overline{\mathfrak{m}} = [1, \bar{\omega}],$$

so daß $\frac{x}{t}$ und $\frac{y}{t}$ ganz sein müssen.

Definition 2. *Das Ideal* $\mathfrak{c}$ *in der Ordnung* $\mathfrak{n}$ *habe einen ganzen rationalen Zahlteiler* t *von der Beschaffenheit, daß der Modul* $\frac{\mathfrak{c}}{t}$ *noch Ideal in* $\mathfrak{n}$ *ist. Dann heißt* t *ein (in bezug auf die Ordnung* $\mathfrak{n}$*) hebbarer ganzer rationaler Zahlteiler von* $\mathfrak{c}$.

Definition 3. *Der größte gemeinsame Teiler der Variablenwerte* x, y *in einer Darstellung*

$$m = ax^2 + bxy + cy^2$$

heiße der Teiler dieser Darstellung.

Aus Satz 3 ergibt sich dann sofort der

Satz 4. *Unter den hebbaren ganzen rationalen Zahlteilern jedes Moduls* $\mathfrak{c}$, *der Ideal in seiner Ordnung* $\mathfrak{c}^0$ *ist, gibt es* (natürlich) *einen größten; in diesem gehen alle übrigen auf. Er ist gleich dem Teiler jeder Darstellung, deren zugeordnetes Ideal* $\mathfrak{c}$ *ist.*

Satz 5. $\mathfrak{c}$ *sei Ideal in seiner Ordnung* $\mathfrak{c}^0 = \mathfrak{n}$ *mit dem Führer* k. *Dann ist jeder zu* k *teilerfremde ganze rationale Zahlteiler von* $\mathfrak{c}$ *hebbar (in bezug auf* $\mathfrak{n}$).

Beweis. Die ganze rationale Zahl t sei zu k teilerfremd und gehe in $\mathfrak{c}$ auf. Da der Modul $\frac{\mathfrak{c}}{t}$ die Ordnung $\mathfrak{n}$ hat, so genügt es, zu zeigen, daß er Untermenge von $\mathfrak{n}$ ist. Da $\mathfrak{c}$ diese Eigenschaft hat, so gibt es zu

jeder Zahl α aus $\mathfrak{c}$ eine ganze rationale Zahl r so, daß

$$\alpha \equiv r \pmod{k}$$

ist. Wegen der Teilerfremdheit von k und t ist ferner die Kongruenz

$$st \equiv 1 \pmod{k}$$

durch ein ganzes rationales s lösbar. Setzt man $\alpha = t\alpha'$, so ist α' ganz, ferner

$$\alpha' \equiv st\alpha' \equiv s\alpha \equiv sr \pmod{k};$$

die Zahl α' ist also mod k kongruent einer ganzen rationalen Zahl und gehört mithin zu $\mathfrak{n}$. Damit ist die Behauptung bewiesen.

Hieraus folgen ohne weiteres die Sätze:

Satz 6. *Die Menge der zu k teilerfremden gemeinsamen Teiler der Variablenwerte einer Darstellung durch eine Form von der Diskriminante $k^2\Delta$ ist identisch mit der Menge der zu k teilerfremden ganzen rationalen Zahlteiler des zugeordneten Ideals in $\mathfrak{n}$.*

Satz 7. *Der Modul $\mathfrak{c}$ sei Ideal in seiner Ordnung $\mathfrak{c}^0 = \mathfrak{n}$ vom Führer k. Unter den zu k teilerfremden ganzen rationalen Zahlteilern von $\mathfrak{c}$ gibt es dann* (natürlich) *eine größte Zahl; in dieser gehen alle übrigen auf. Sie ist gleich dem größten zu k teilerfremden gemeinsamen Teiler der Variablenwerte jeder Darstellung, deren zugeordnetes Ideal $\mathfrak{c}$ ist.*

Satz 8. *Ist der Teiler einer Darstellung durch eine Form von der Diskriminante $k^2\Delta$ Potenzteiler*[17]) *von k, so ist jeder ganze rationale Zahlteiler des zugeordneten Ideals Potenzteiler von k.*

§ 4.

Assoziierte Darstellungen derselben Zahl.

Anschließend an das Ergebnis von § 2 erhebt sich sofort die Frage nach einer ein-eindeutigen Zuordnung. Zunächst ist aber klar, daß hierbei nur dann eine Hoffnung auf Eindeutigkeit bestehen kann, wenn man sich auf eine bestimmte Form aus der Klasse K beschränkt. Denn dasselbe Ideal $\mathfrak{c}$ ist nach Satz 2 mindestens einer Darstellung von m durch jede Form aus K zugeordnet. Es wird sich jedoch bald zeigen, daß auch eine Darstellung von m durch eine gegebene Form keineswegs durch Angabe ihres $\mathfrak{c}$ bestimmt ist.

Definition 4. *Zwei Darstellungen einer und derselben natürlichen Zahl durch zwei beliebige* (eventuell verschiedene) *Formen einer und derselben Klasse heißen assoziiert, wenn ihnen dasselbe Ideal zugeordnet ist.*

[17]) Eine Zahl a heißt Potenzteiler einer Zahl b, wenn sie in einer hinreichend hohen Potenz von b aufgeht, d. h. wenn alle verschiedenen Primfaktoren von a auch in b enthalten sind.

Eine formentheoretische Deutung erlangt dieser Begriff durch den

Satz 9. *Zwei Darstellungen einer und derselben natürlichen Zahl m durch Formen der Klasse K sind dann und nur dann assoziiert, wenn sie durch eine vollständige lineare Substitution von der Determinante* 1 *auseinander hervorgehen.*

Beweis. Die Variablensubstitution

$$(1) \qquad \begin{cases} x = \alpha x' + \beta y', \\ y = \gamma x' + \delta y' \end{cases}$$

mit $\alpha\delta - \beta\gamma = 1$ möge die Form $ax^2 + bxy + cy^2$ in die Form $a'x'^2 + b'x'y' + c'y'^2$ überführen. Auf ein spezielles Wertepaar x, y mit

$$(4) \qquad m = ax^2 + bxy + cy^2$$

angewandt, ergibt die Substitution (1) ein Wertepaar x', y' mit

$$(7) \qquad m = a'x'^2 + b'x'y' + c'y'^2.$$

In (4) und (7) hat man die allgemeine Gestalt zweier Darstellungen, die durch eine vollständige unimodulare Substitution ineinander übergehen. Der $\mathfrak{m}$-Algorithmus erzeuge nun aus den Darstellungen (4) und (7) die Zahlen ω und ω', die Moduln $\mathfrak{m}$ und $\mathfrak{m}'$, die Zahlen μ und μ' und die Ideale $\mathfrak{c}$ und $\mathfrak{c}'$; es ist zu zeigen, daß $\mathfrak{c} = \mathfrak{c}'$ ist. Zwischen den Werten ω und ω' besteht die Beziehung

$$\omega' = \frac{\beta + \delta\omega}{\alpha + \gamma\omega}.$$

Sind also X und Y ganze rationale Zahlen und ist

$$X = \alpha X' + \beta Y',$$
$$Y = \gamma X' + \delta Y',$$

so folgt identisch

$$X' + Y'\omega' = X' + Y'\frac{\beta + \delta\omega}{\alpha + \gamma\omega},$$

$$(8) \qquad (\alpha + \gamma\omega)(X' + Y'\omega') = (\alpha X' + \beta Y') + (\gamma X' + \delta Y')\omega = X + Y\omega.$$

Da nun X', Y' mit X, Y alle Paare ganzer rationaler Zahlen darstellt, so besagt (8) dasselbe wie die Modulgleichung

$$(9) \qquad (\alpha + \gamma\omega)\mathfrak{m}' = \mathfrak{m}.$$

Setzt man speziell $X = x$, $Y = y$, so ergibt sich aus (8) weiter

$$(\alpha + \gamma\omega)\mu' = \mu,$$

demnach durch Übergang zum Konjugierten

$$(10) \qquad (\alpha + \gamma\bar{\omega})\bar{\mu'} = \bar{\mu}.$$

Durch Multiplikation folgt aus (9) und (10)

$$\bar{\mu}\mathfrak{m} = (\alpha + \gamma\omega)(\alpha + \gamma\bar{\omega})\,\bar{\mu}'\mathfrak{m}' = \left(\alpha^2 + \frac{b}{a}\alpha\gamma + \frac{c}{a}\gamma^2\right)\bar{\mu}'\mathfrak{m}',$$

also (wegen $a' = a\alpha^2 + b\alpha\gamma + c\gamma^2$)

$$\bar{\mu}\mathfrak{m} = \frac{a'}{a}\,\bar{\mu}'\mathfrak{m}',$$

$$a\bar{\mu}\mathfrak{m} = a'\bar{\mu}'\mathfrak{m}',$$

$$\mathfrak{c} = \mathfrak{c}'.$$

Beim Beweis der Umkehrung ist das Merkwürdige, daß die Behauptung auf Grund des ersten Teils fast trivial wird, wenn sie erst einmal für Darstellungen durch eine und dieselbe Form gezeigt ist. Ist sie nämlich für diesen Fall nachgewiesen, so schließt man im allgemeinen Falle folgendermaßen: Ist

(4) $$m = ax^2 + bxy + cy^2,$$

(7) $$m = a'x'^2 + b'x'y' + c'y'^2$$

und wird die Form $aX^2 + bXY + cY^2$ durch die Substitution

$$\begin{cases} X = \alpha X' + \beta Y', \\ Y = \gamma X' + \delta Y' \end{cases} \qquad (\alpha\delta - \beta\gamma = 1)$$

in die Form $a'X'^2 + b'X'Y' + c'Y'^2$ übergeführt (eine solche Substitution gibt es immer, wenn die beiden Formen zur selben Klasse gehören), so sei etwa

$$x = \alpha x'' + \beta y'',$$

$$y = \gamma x'' + \delta y''$$

gesetzt. Es ist dann

(11) $$m = a'x''^2 + b'x''y'' + c'y''^2.$$

Ist nun den Darstellungen (4) und (7) dasselbe Ideal $\mathfrak{c}$ zugeordnet, so entspricht $\mathfrak{c}$ nach dem schon bewiesenen Teil des Satzes auch der Darstellung (11), da (11) aus (4) durch eine vollständige lineare Substitution hervorgeht. Nach dem für eine und dieselbe Form als bewiesen angenommenen Satze geht also die Darstellung (7) aus der Darstellung (11) durch eine vollständige lineare Substitution hervor. Ist deren Matrix etwa $\begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix}$, so führt die vollständige Substitution mit der Matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix}$ die Darstellung (4) in die Darstellung (7) über. Die Produktmatrix ist aber natürlich wieder ganzzahlig und von der Determinante 1.

Der Beweis braucht also nur noch für den Fall erbracht zu werden, daß zwei Darstellungen durch dieselbe Form $\{a, b, c\}$:

$$m = a x_1^2 + b x_1 y_1 + c y_1^2, \tag{12}$$

$$m = a x_2^2 + b x_2 y_2 + c y_2^2, \tag{13}$$

dasselbe Ideal $\mathfrak{c}$ zugeordnet ist. Der $\mathfrak{m}$-Algorithmus läßt aus den beiden Darstellungen dieselbe Zahl ω und denselben Modul $\mathfrak{m}$, sodann zwei Zahlen μ_1 und μ_2 entspringen. Dann wird

$$\mu_1 = x_1 + y_1 \omega,$$

$$\mu_2 = x_2 + y_2 \omega,$$

$$\mathfrak{c} = a \overline{\mu_1}\, \mathfrak{m} = a \overline{\mu_2}\, \mathfrak{m}. \tag{14}$$

Multiplikation von (14) mit der Hauptordnung $\mathfrak{o}$ ergibt

$$a \overline{\mu_1}\, \mathfrak{m}\, \mathfrak{o} = a \overline{\mu_2}\, \mathfrak{m}\, \mathfrak{o},$$

$$a \mu_1 \overline{\mathfrak{m}}\, \mathfrak{o} = a \mu_2 \overline{\mathfrak{m}}\, \mathfrak{o}.$$

Da $a \overline{\mathfrak{m}}\, \mathfrak{o}$ Ideal in $\mathfrak{o}$ ist, so muß es also in $\mathfrak{o}$ eine Einheit ε geben, für die

$$\mu_1 = \varepsilon \mu_2$$

ist. Wegen $N(\mu_1) = N(\mu_2)\left(= \frac{m}{a}\right)$ muß

$$N(\varepsilon) = +1$$

sein. Es folgt

$$\bar{\varepsilon}\,[1, \omega] = \bar{\varepsilon}\, \mathfrak{m} = \frac{\bar{\varepsilon}\, \mathfrak{c}}{a \overline{\mu_1}} = \frac{\mathfrak{c}}{a \overline{\mu_2}} = \mathfrak{m} = [1, \omega],$$

und demnach gibt es vier ganze rationale Zahlen $\alpha, \beta, \gamma, \delta$ mit $\alpha\delta - \beta\gamma = \pm 1$ so, daß

$$\begin{cases} \bar{\varepsilon} = \alpha + \beta \omega, \\ \bar{\varepsilon}\, \omega = \gamma + \delta \omega \end{cases} \tag{15}$$

ist. Setzt man

$$\begin{cases} x = \alpha x' + \gamma y', \\ y = \beta x' + \delta y', \end{cases} \tag{16}$$

so wird identisch

$$\begin{aligned} a x^2 + b x y + c y^2 &= a (x + y\omega)(x + y\overline{\omega}) \\ &= a ((\alpha + \beta\omega) x' + (\gamma + \delta\omega) y')((\alpha + \beta\overline{\omega}) x' + (\gamma + \delta\overline{\omega}) y') \\ &= a \bar{\varepsilon} (x' + y'\omega)\, \varepsilon (x' + y'\overline{\omega}) \\ &= a (x' + y'\omega)(x' + y'\overline{\omega}), \end{aligned}$$

$$a x^2 + b x y + c y^2 = a x'^2 + b x' y' + c y'^2. \tag{17}$$

Da die Substitution (16) also die Form $\{a, b, c\}$ in sich überführt, muß ihre Determinante $\alpha\delta - \beta\gamma$ nach einem bekannten Satze den Wert $+1$ haben; dies folgt übrigens auch aus

$$1 = N(\varepsilon) = \varepsilon\bar{\varepsilon} = (\alpha + \beta\bar{\omega})\frac{\gamma + \delta\omega}{\omega},$$

$$\omega = \alpha\gamma + \alpha\delta\omega + \beta\gamma\bar{\omega} + \beta\delta\omega\bar{\omega}$$

$$= \alpha\gamma + (\alpha\delta - \beta\gamma)\omega + \beta\gamma\frac{b}{a} + \beta\delta\frac{c}{a}.$$

Andrerseits liefert das Einsetzen der speziellen Werte x_1, y_1 für x', y' in (16) wegen

$$x_2 + y_2\omega = \mu_2 = \frac{1}{\varepsilon}\mu_1 = \bar{\varepsilon}\mu_1 = \bar{\varepsilon}(x_1 + y_1\omega)$$

$$= (\alpha + \beta\omega)x_1 + (\gamma + \delta\omega)y_1$$

$$= (\alpha x_1 + \gamma y_1) + (\beta x_1 + \delta y_1)\omega$$

die Werte x_2, y_2. Mit Rücksicht auf (17) ergibt sich also, daß die Darstellung (12) aus der Darstellung (13) durch die vollständige lineare Substitution (16) hervorgeht, die die Form $\{a, b, c\}$ in sich überführt. Damit ist der Satz bewiesen.

Nebenbei läßt die zweite Hälfte dieses Beweises den folgenden Satz vermuten, der sich auch sofort bestätigen läßt:

Satz 10. *Ist $\{a, b, c\}$ eine Form von der Diskriminante $k^2\Delta$, so lassen sich die in $\mathfrak{n}$ enthaltenen Einheiten von positiver Norm ein-eindeutig denjenigen Linearsubstitutionen zuordnen, welche die Form $\{a, b, c\}$ in sich überführen.*

Beweis. Irgendeiner Darstellung (4) durch die Form $\{a, b, c\}$ möge der $\mathfrak{m}$-Algorithmus die Zahl ω und den Modul $\mathfrak{m} = [1, \omega]$ zuweisen. Für jede Einheit ε aus $\mathfrak{n}$ mit $N(\varepsilon) = 1$ ist, da $\mathfrak{m}$ die Ordnung $\mathfrak{n}$ hat und auch $\bar{\varepsilon}$ in $\mathfrak{n}$ liegt,

$$\bar{\varepsilon}\,\mathfrak{m} \subseteqq \mathfrak{m},$$

andrerseits

$$\frac{1}{\bar{\varepsilon}}\mathfrak{m} = \varepsilon\,\mathfrak{m} \subseteqq \mathfrak{m},$$

$$\mathfrak{m} \subseteqq \bar{\varepsilon}\,\mathfrak{m},$$

also

$$\bar{\varepsilon}\,\mathfrak{m} = \mathfrak{m}.$$

Wiederum bestehen also zwei Gleichungen von der Gestalt (15), so daß die zugehörige Substitution (16) die Form $\{a, b, c\}$ in sich überführt. Der Einheit ε ordne man diese Substitution zu. Natürlich entsprechen verschiedenen Einheiten verschiedene Substitutionen. Andrerseits läßt sich jede Substitution von der Gestalt (16), welche die Form in sich überführt, auf die genannte Art aus einer in $\mathfrak{n}$ gelegenen Einheit ε von der Norm 1

erzeugen. Unter Zugrundelegung zweier beliebiger Darstellungen von der Gestalt (12) und (13), wobei (12) durch die vollständige Substitution (16) aus (13) hervorgeht, ergibt sich nämlich genau wie im zweiten Teil des Beweises von Satz 9 und unter Benutzung dieses Satzes die Existenz einer Einheit ε von positiver Norm mit $\bar{\varepsilon}\mathfrak{m} = \mathfrak{m}$, die definiert ist durch

$$x_1 + y_1\omega = \varepsilon(x_2 + y_2\omega).$$

Wegen $\bar{\varepsilon} \in \mathfrak{m}^0 = \mathfrak{n}$ liegt ε in $\mathfrak{n}$. Aus

$$x_2 = \alpha x_1 + \gamma y_1,$$
$$y_2 = \beta x_1 + \delta y_1$$

folgt

$$\bar{\varepsilon}(x_1 + y_1\omega) = (\alpha x_1 + \gamma y_1) + (\beta x_1 + \delta y_1)\omega = x_1(\alpha + \beta\omega) + y_1(\gamma + \delta\omega);$$

wegen der unschwer zu verifizierenden Gleichung $\gamma + \delta\omega = \omega(\alpha + \beta\omega)$ ist also

$$\bar{\varepsilon}(x_1 + y_1\omega) = (x_1 + y_1\omega)(\alpha + \beta\omega),$$
$$\bar{\varepsilon} = \alpha + \beta\omega,$$
$$\bar{\varepsilon}\omega = \gamma + \delta\omega,$$

so daß die Gleichungen (15) erfüllt sind. Damit ist der Satz völlig bewiesen.

Aus Satz 9 und 10 folgt noch:

Satz 11. *Diejenigen Darstellungen der natürlichen Zahl m durch die feste Form $\{a, b, c\}$ aus der Klasse K, denen das feste Ideal $\mathfrak{c}$ in $\mathfrak{n}$ aus der K zugeordneten Modulklasse zugeordnet ist, dessen Norm m ist, entsprechen ein-eindeutig denjenigen linearen Substitutionen von der Determinante* 1, *welche die Form $\{a, b, c\}$ in sich überführen. Ihre „Anzahl“* (worunter gegebenenfalls auch die „Zahl“ ∞ zu verstehen ist) *hängt also nur von der Diskriminante der Form ab,* im übrigen weder von der Form selbst noch von ihrer Klasse noch von der darzustellenden Zahl noch von dem Ideal $\mathfrak{c}$. *Sie ist überdies gleich der „Anzahl“ der in $\mathfrak{n}$ gelegenen Einheiten von der Norm* $+1$.

Der Anschluß des Assoziiertheitsbegriffes an den gleichlautenden alten arithmetischen Begriff kann nun in folgender Weise hergestellt werden:

Satz 12. *Die ganzzahlige Substitution*

$$\begin{cases} X = \alpha X' + \beta Y', \\ Y = \gamma X' + \delta Y' \end{cases}$$

habe die Determinante 1 *und führe die Form $aX^2 + bXY + cY^2$ in die Form $mX'^2 + rX'Y' + sY'^2$ über, so daß also insbesondere*

(18) $$m = a\alpha^2 + b\alpha\gamma + c\gamma^2$$

ist. Aus der letzteren Darstellung von m mögen durch den $\mathfrak{m}$-Algorithmus der Modul $\mathfrak{m}$ und die Zahl μ entstehen, aus der Darstellung

$$m = m \cdot 1^2 + r \cdot 1 \cdot 0 + s \cdot 0^2 \tag{19}$$

durch denselben Algorithmus der Modul $\mathfrak{r}$. Dann ist

$$\mu \mathfrak{r} = \mathfrak{m}.$$

Beweis. Sind ω und Ω durch den auf (18) bzw. (19) angewandten $\mathfrak{m}$-Algorithmus definiert, so ist

$$\mathfrak{m} = [1, \omega],$$
$$\mu = \alpha + \gamma\omega,$$
$$\Omega = \frac{\beta + \delta\omega}{\alpha + \gamma\omega},$$

daher

$$\mathfrak{r} = [1, \Omega] = \frac{1}{\alpha + \gamma\omega}[\alpha + \gamma\omega,\ \beta + \delta\omega] = \frac{1}{\mu}[\alpha + \gamma\omega,\ \beta + \delta\omega].$$

Da eine zweigliedrige Modulbasis stets ohne Änderung des Moduls einer ganzzahligen Linearsubstitution von der Determinante 1 unterworfen werden kann, so wird

$$\mathfrak{r} = \frac{1}{\mu}[1, \omega],$$
$$\mu \mathfrak{r} = \mathfrak{m}.$$

Satz 13. *Zwei eigentliche Darstellungen einer und derselben Zahl m durch eine und dieselbe Form $\{a, b, c\}$:*

$$\begin{cases} m = ax_1^2 + bx_1y_1 + cy_1^2, \\ m = ax_2^2 + bx_2y_2 + cy_2^2, \end{cases} \tag{20}$$

sind dann und nur dann assoziiert, wenn unter den unendlich vielen Paaren ganzzahliger Linearsubstitutionen von der Determinante 1 und der Gestalt

$$\begin{cases} X = x_1X' + \beta_1Y', \\ Y = y_1X' + \delta_1Y', \end{cases} \tag{21}$$

$$\begin{cases} X = x_2X' + \beta_2Y', \\ Y = y_2X' + \delta_2Y' \ ^{18}) \end{cases} \tag{22}$$

mindestens eins (und daher jedes) *die Eigenschaft hat, daß die durch diese Substitutionen aus der Form $aX^2 + bXY + cY^2$ hervorgehenden*

---

[18]) Daß es solche Substitutionen gibt, und zwar in unendlicher Anzahl, folgt aus der Teilerfremdheit der darstellenden Variablenwerte in (20).

Formen von der Gestalt $mX'^2+r_1X'Y'+s_1Y'^2$ *und* $mX'^2+r_2X'Y'+s_2Y'^2$ *einander „parallel" sind, d. h. der Bedingung*

$$r_1 \equiv r_2 \pmod{2m} \tag{23}$$

genügen.

Beweis. 1. Die Darstellungen (20) seien assoziiert. Zwei unimodulare Substitutionen von der Gestalt (21) bzw. (22) mögen die Form $aX^2+bXY+cY^2$ in die Formen $mX'^2+r_1X'Y'+s_1Y'^2$ und $mX'^2+r_2X'Y'+s_2Y'^2$ überführen. Der $\mathfrak{m}$-Algorithmus ordnet den Darstellungen (20) einen gemeinsamen Modul $\mathfrak{m}$ und zwei Zahlen μ_1 und μ_2 von der Norm $\frac{m}{a}$, den Darstellungen

$$\begin{cases} m = m\cdot 1^2 + r_1\cdot 1\cdot 0 + s_1\cdot 0^2, \\ m = m\cdot 1^2 + r_2\cdot 1\cdot 0 + s_2\cdot 0^2 \end{cases} \tag{24}$$

zwei Zahlen Ω_1 und Ω_2 und zwei Moduln $\mathfrak{r}_1$ und $\mathfrak{r}_2$ zu. Nach Voraussetzung ist

$$\begin{cases} a\overline{\mu}_1\,\mathfrak{m} = a\overline{\mu}_2\,\mathfrak{m}, \\ \overline{\mu}_1\,\mathfrak{m} = \overline{\mu}_2\,\mathfrak{m}, \\ \frac{m}{a\mu_1}\,\mathfrak{m} = \frac{m}{a\mu_2}\,\mathfrak{m}, \\ \frac{\mathfrak{m}}{\mu_1} = \frac{\mathfrak{m}}{\mu_2}, \end{cases} \tag{25}$$

nach Satz 12 also

$$\begin{gathered} \mathfrak{r}_1 = \mathfrak{r}_2, \\ [1, \Omega_1] = [1, \Omega_2], \\ \Omega_1 \in [1, \Omega_2]. \end{gathered}$$

Es gibt also zwei ganze rationale Zahlen p und q so, daß

$$\Omega_1 = p + q\,\Omega_2$$

ist. Dies besagt:

$$\frac{1}{m}\,\frac{r_1+\sqrt{D}}{2} = p + q\,\frac{1}{m}\,\frac{r_2+\sqrt{D}}{2},$$

also

$$\begin{aligned} &r_1 = 2mp + qr_2, \qquad 1 = q, \\ &r_1 - r_2 = 2mp, \\ &r_1 \equiv r_2 \pmod{2m}. \end{aligned}$$

2. Umgekehrt sei für die Darstellungen (20) bei geeigneter Wahl der Substitutionen (21) und (22) die Bedingung (23) erfüllt. Durch den $\mathfrak{m}$-Algorithmus mögen aus den Darstellungen (24) die Zahlen Ω_1 und Ω_2

sowie die Moduln $\mathfrak{r}_1$ und $\mathfrak{r}_2$ hervorgehen. Dann ist

$$\Omega_1 = \frac{1}{m}\,\frac{r_1+\sqrt{D}}{2},$$

$$\Omega_2 = \frac{1}{m}\,\frac{r_2+\sqrt{D}}{2}.$$

Wegen (23) ist also

$$\Omega_1 - \Omega_2 = \frac{r_1-r_2}{2m}$$

eine ganze Zahl; demnach besteht die Modulgleichung

$$[1, \Omega_1] = [1, \Omega_2],$$

$$\mathfrak{r}_1 = \mathfrak{r}_2.$$

Unter Benutzung von Satz 12 folgen hieraus in genau umgekehrter Reihenfolge die Relationen (25) und somit die Gleichheit der den Darstellungen (20) zugeordneten Ideale. Die Darstellungen sind also assoziiert.

Legt man in Satz 9 im Spezialfall eigentlicher Darstellungen durch eine und dieselbe Form die alte, als gleichberechtigt erwiesene arithmetische Definition des Assoziiertseins zugrunde, so bedarf der Satz des obigen Beweises nicht, sondern ist auch zahlentheoretisch leicht einzusehen. Die im Sinne des Beweises zu Satz 13 konstruierten Darstellungen (24) entsprechen sich nämlich vermittelst der vollständigen Substitution $\begin{pmatrix} 1 & \frac{r_2-r_1}{2m} \\ 0 & 1 \end{pmatrix}$ bzw. ihrer Inversen, entsprechen aber andrerseits den gegebenen Darstellungen (20) vermittelst der vollständigen Substitutionen (21) und (22).

Aus Satz 4 folgt noch der

Satz 14. *Assoziierte Darstellungen einer und derselben Zahl haben denselben Teiler.*

§ 5.

Assoziierte Darstellungen verschiedener Zahlen.

Alles Bisherige bezog sich auf Darstellungen einer und derselben Zahl. Wünschenswert erscheint es nun, auch gewisse Darstellungen verschiedener Zahlen unter Umständen zu einer engeren Klasse vereinigen zu können, die sich durch ein und dasselbe in geeigneter Weise zugeordnete Ideal kennzeichnen läßt. Das Ideal $\mathfrak{c}$ ist hierzu unbrauchbar, da es die dargestellte Zahl m als seine Norm eindeutig bestimmt. Dagegen hilft eine andere Normierung einen Schritt weiter. Es sei nämlich d der Teiler einer

Darstellung, c das zugeordnete Ideal, und man bilde den Modul

$$\mathfrak{z} = \frac{\mathfrak{c}}{d},$$

der nach Satz 3 wieder Ideal in $\mathfrak{n}$ ist[19]). Es gilt nun der

Satz 15. *Zwei Darstellungen einer und derselben natürlichen Zahl m durch beliebige Formen derselben Diskriminante D sind dann und nur dann assoziiert, wenn ihnen dasselbe Ideal $\mathfrak{z}$ entspricht.* Oder: *Wenn D und m gegeben sind, so besagt Gleichheit der* c *dasselbe wie Gleichheit der* $\mathfrak{z}$.

Beweis. Es seien d_1 und d_2 die Teiler zweier Darstellungen von m, ferner $\mathfrak{c}_1$ und $\mathfrak{c}_2$ die zugeordneten Ideale, $\mathfrak{z}_1 = \frac{\mathfrak{c}_1}{d_1}$, $\mathfrak{z}_2 = \frac{\mathfrak{c}_2}{d_2}$. Sind zunächst die Darstellungen als assoziiert vorausgesetzt, so folgt aus Definition 4 und Satz 14 sofort $\mathfrak{z}_1 = \mathfrak{z}_2$. Ist umgekehrt $\mathfrak{z}_1 = \mathfrak{z}_2$ vorausgesetzt, so ergibt sich hieraus durch Übergang zur Norm

$$\frac{m}{d_1^2} = \frac{m}{d_2^2},$$

$$d_1 = d_2,$$

$$\mathfrak{c}_1 = d_1 \mathfrak{z}_1 = d_2 \mathfrak{z}_2 = \mathfrak{c}_2;$$

die Darstellungen sind also assoziiert.

Dieser Satz rechtfertigt die folgende erweiterte

Definition 5. *Zwei Darstellungen beliebiger natürlicher Zahlen durch beliebige Formen derselben Diskriminante heißen assoziiert, wenn ihnen dasselbe Ideal $\mathfrak{z}$ entspricht.*

Der arithmetische Übergang zu eigentlichen Darstellungen kann nun folgendermaßen vollzogen werden:

Satz 16. *Haben in der Darstellung*

$$m = ax^2 + bxy + cy^2 \tag{4}$$

die Variablenwerte x und y den gemeinsamen Teiler t, so entspricht der Darstellung

$$\frac{m}{t^2} = a\left(\frac{x}{t}\right)^2 + b\,\frac{x}{t}\,\frac{y}{t} + c\left(\frac{y}{t}\right)^2 \tag{5}$$

dasselbe Ideal $\mathfrak{z}$ wie der Darstellung (4).

---

[19]) Ursprünglich arbeitete ich hier mit dem komplizierteren Modul $\frac{d}{N(\mathfrak{c})}\mathfrak{c}$, der im Falle einer eigentlichen Darstellung mit dem Modul $\mathfrak{r}$ aus Satz 12 übereinstimmt. Die Einführung des Ideals $\mathfrak{z}$ schlug mir Fräulein E. Noether vor.

Beweis. Der Darstellung (4) sei das Ideal $\mathfrak{c}$, der Darstellung (5) also nach Satz 3 das Ideal $\frac{\mathfrak{c}}{t}$ zugeordnet. Bedeutet d den Teiler von (4), so ist

$$\frac{\frac{\mathfrak{c}}{t}}{\frac{d}{t}} = \frac{\mathfrak{c}}{d},$$

und das ist die Behauptung.

Satz 17. *Zwei Darstellungen beliebiger natürlicher Zahlen:*

$$(26) \qquad \begin{cases} m_1 = a_1 x_1^2 + b_1 x_1 y_1 + c_1 y_1^2, \\ m_2 = a_2 x_2^2 + b_2 x_2 y_2 + c_2 y_2^2, \end{cases}$$

von den Teilern d_1 und d_2 sind dann und nur dann assoziiert, wenn die eigentlichen Darstellungen

$$(27) \qquad \begin{cases} \frac{m_1}{d_1^2} = a_1 x_1'^2 + b_1 x_1' y_1' + c_1 y_1'^2, \\ \frac{m_2}{d_2^2} = a_2 x_2'^2 + b_2 x_2' y_2' + c_2 y_2'^2 \end{cases}$$

mit

$$x_1' = \frac{x_1}{d_1}, \quad y_1' = \frac{y_1}{d_1},$$

$$x_2' = \frac{x_2}{d_2}, \quad y_2' = \frac{y_2}{d_2}$$

assoziiert sind. Zugleich ist dann $\frac{m_1}{d_1^2} = \frac{m_2}{d_2^2}$.

Beweis. Der erste Teil des Satzes folgt nach Definition 5 sofort aus Satz 16. Die Gleichung $\frac{m_1}{d_1^2} = \frac{m_2}{d_2^2}$ ergibt sich dann aus der Gleichheit der $\mathfrak{s}$ durch Übergang zur Norm.

§ 6.

Vereinigte Darstellungen.

Nächst den assoziierten Darstellungen derselben Zahl, deren zugehörige Ideale $\mathfrak{c}$ miteinander übereinstimmen, beanspruchen diejenigen Scharen von Darstellungen ein erhöhtes Interesse, deren zugehörige $\mathfrak{c}$ sich nur durch Einheitsfaktoren unterscheiden.

Definition 6. *Zwei Darstellungen einer und derselben natürlichen Zahl heißen vereinigt, wenn die zugeordneten Ideale in der Ordnung $\mathfrak{n}$ sich nur durch einen Einheitsfaktor unterscheiden.*

Es gilt also:

Satz 18. *Assoziierte Darstellungen einer und derselben natürlichen Zahl sind stets vereinigt.*

Satz 19. *Stehen zwei Ideale* $\mathfrak{c}_1$ *und* $\mathfrak{c}_2$ *in* $\mathfrak{n}$, *deren Ordnung genau* $\mathfrak{n}$ *ist*[20]), *zueinander in der Beziehung*

$$\mathfrak{c}_1 = \varepsilon \mathfrak{c}_2,$$

wo ε *eine Körpereinheit ist, so ist dann und nur dann* $\mathfrak{c}_1 = \mathfrak{c}_2$, *wenn* ε *in* $\mathfrak{n}$ *liegt.*

Beweis. 1. Es sei $\mathfrak{c}_1 = \mathfrak{c}_2$. Dann folgt $\mathfrak{c}_1 = \varepsilon \mathfrak{c}_1$, nach Definition der Ordnung eines Moduls also $\varepsilon \in \mathfrak{c}_1^0$, $\varepsilon \in \mathfrak{n}$.

2. Es sei $\varepsilon \in \mathfrak{n}$. Da $\mathfrak{c}_2$ Ideal in $\mathfrak{n}$ ist, so wird $\varepsilon \mathfrak{c}_2 \leqq \mathfrak{c}_2$, $\mathfrak{c}_1 \leqq \mathfrak{c}_2$. Da nun ε die Norm ± 1 hat, so ist

$$\bar{\varepsilon} \mathfrak{c}_1 = \bar{\varepsilon} \varepsilon \mathfrak{c}_2 = \mathfrak{c}_2. \tag{28}$$

Mit ε liegt aber auch $\bar{\varepsilon}$ in der Ordnung $\mathfrak{n}$. Aus (28) folgt also ebenso $\mathfrak{c}_2 \leqq \mathfrak{c}_1$, also $\mathfrak{c}_1 = \mathfrak{c}_2$.

Die hiernach zu vermutende ein-eindeutige Zuordnung der in $\mathfrak{n}$ enthaltenen Einheiten zu den Elementen einer Schar assoziierter Darstellungen einer festen natürlichen Zahl durch eine feste Form besteht nach Satz 11 nur dann, wenn es in $\mathfrak{n}$ keine Einheiten negativer Norm gibt.

Satz 20. *Ist* $\mathfrak{c}$ *Ideal in* $\mathfrak{n}$ *von der Ordnung* $\mathfrak{n}$, *ferner* ε *eine Einheit, so ist* $\varepsilon \mathfrak{c}$ *dann und nur dann Ideal in* $\mathfrak{n}$, *wenn* ε *in* $\mathfrak{c}^{-1}$ *liegt.*

Beweis. 1. $\varepsilon \mathfrak{c}$ sei Ideal in $\mathfrak{n}$. Dann ist $\varepsilon \mathfrak{c} \leqq \mathfrak{n} = \mathfrak{c}^0$, nach Definition von $\mathfrak{c}^{-1}$ (§ 1) also $\varepsilon \in \mathfrak{c}^{-1}$.

2. Die Einheit ε liege in $\mathfrak{c}^{-1}$. Dann ist $\varepsilon \mathfrak{c} \leqq \mathfrak{c}^0 = \mathfrak{n}$, und da $\varepsilon \mathfrak{c}$ die Ordnung $\mathfrak{n}$ hat, so ist es sogar Ideal in $\mathfrak{n}$.

Satz 21. *Ist* $\mathfrak{c}$ *Ideal in* $\mathfrak{n}$ *von der Ordnung* $\mathfrak{n}$, *so ist die Anzahl*[21]) *derjenigen Ideale in* $\mathfrak{n}$, *die sich von* $\mathfrak{c}$ *nur durch Einheitsfaktoren unterscheiden, gleich dem Index der multiplikativen Gruppe* $\mathfrak{E}'$ *der in* $\mathfrak{n}$ *enthaltenen Einheiten in der Obergruppe* $\mathfrak{E}$ *der in* $\mathfrak{c}^{-1}$ *enthaltenen Einheiten.*

(Man beachte, daß wegen $\mathfrak{c}\mathfrak{n} = \mathfrak{c} \leqq \mathfrak{n}$ stets $\mathfrak{c}^{-1} \geqq \mathfrak{n}$ ist.)

Beweis. Nach Satz 20 sind die in Rede stehenden Ideale genau die Moduln von der Gestalt $\varepsilon \mathfrak{c}$, wo ε eine Einheit aus $\mathfrak{c}^{-1}$, d. h. Element von $\mathfrak{E}$

---

[20]) Zwischen Idealen in der Ordnung $\mathfrak{n}$ und Idealen (oder Moduln) von der Ordnung $\mathfrak{n}$ muß scharf geschieden werden. Vgl. die Einleitung.

[21]) Darunter ist, wie bei Satz 11, gegebenenfalls auch die „Zahl" ∞ zu verstehen.

ist. Sind ε_1 und ε_2 Elemente von $\mathfrak{E}$, so ist dann und nur dann $\varepsilon_1 \mathfrak{c} = \varepsilon_2 \mathfrak{c}$, wenn $\mathfrak{c} = \frac{\varepsilon_2}{\varepsilon_1} \mathfrak{c}$ ist, d. h. nach Satz 19: wenn $\frac{\varepsilon_2}{\varepsilon_1}$ in $\mathfrak{E}'$ liegt oder wenn ε_1 und ε_2 zur selben Restklasse von $\mathfrak{E}$ nach $\mathfrak{E}'$ gehören. Daraus folgt die Behauptung.

Aus der in § 5 gegebenen Definition des Ideals $\mathfrak{s}$ folgt nun sofort der

Satz 22. *Zwei Darstellungen einer und derselben natürlichen Zahl m vom selben Teiler d sind dann und nur dann vereinigt, wenn die ihnen zugeordneten Ideale $\mathfrak{s}$ sich nur durch einen Einheitsfaktor unterscheiden.* Oder: *Bei gegebenem D, m und d stimmen dann und nur dann die $\mathfrak{c}$ bis auf einen Einheitsfaktor überein, wenn die $\mathfrak{s}$ es tun.*

Dieser Satz rechtfertigt die gegenüber Definition 6 zum Teil erweiterte, zum Teil dahinter zurückbleibende

Definition 7. *Haben zwei Darstellungen natürlicher Zahlen m_1 und m_2 die Teiler d_1 bzw. d_2 und ist*

$$\frac{m_1}{d_1^2} = \frac{m_2}{d_2^2}, \tag{29}$$

so heißen die Darstellungen vereinigt, wenn die zugehörigen Ideale $\mathfrak{s}$ sich nur durch einen Einheitsfaktor unterscheiden.

In den Fällen nämlich, auf die sowohl Definition 6 wie auch Definition 7 paßt, ist $m_1 = m_2$, nach (29) also $d_1 = d_2$; Satz 22 lehrt also die Äquivalenz der beiden Definitionen.

Satz 23. *Assoziierte Darstellungen beliebiger natürlicher Zahlen m_1, m_2 sind stets vereinigt.*

Beweis. Sind d_1 und d_2 die Teiler der Darstellungen, so gilt nach Satz 17 die Gleichung (29); die Darstellungen fallen also unter Definition 7. Aus Definition 5 folgt also die Behauptung.

Da für den Schlußsatz dieses Paragraphen eine Hilfsbetrachtung über „Ideale in verschiedenen Ringen“ (Satz 25) nötig ist und diese Methode in § 7 nochmals zur Geltung kommt, so ist es zweckmäßig, an dieser Stelle die beiden folgenden Hilfssätze einzufügen, deren erster nur in § 7 benutzt wird.

Satz 24. *Ist $\mathfrak{a}$ ein zu k teilerfremdes Ideal in $\mathfrak{o}$, ferner*

$$\mathfrak{x} = \mathfrak{a} \wedge \mathfrak{n},$$

so ist $\mathfrak{x}$ Ideal in $\mathfrak{n}$, genügt der Gleichung

$$\mathfrak{x}\mathfrak{o} = \mathfrak{a}$$

und hat die Ordnung $\mathfrak{n}$.

Beweis. Hinsichtlich der beiden ersten Behauptungen kann auf § 5 der in Fußnote [14]) genannten Arbeit von Dedekind verwiesen werden [22]). Zu zeigen ist also nur noch $\mathfrak{x}^0 = \mathfrak{n}$. Es sei $\mathfrak{x}^0 = \mathfrak{n}_1$ gesetzt; da $\mathfrak{x}$ Ideal in $\mathfrak{n}$ ist, so ist $\mathfrak{n}_1 \geqq \mathfrak{n}$. Bezeichnet man die zu k teilerfremde Zahl $N(\mathfrak{x}) = N(\alpha)$ mit m, so ist nach (3)

$$m\mathfrak{n}_1 = \mathfrak{x}\bar{\mathfrak{x}};$$

da $\mathfrak{x}$ Ideal in $\mathfrak{n}$, $\bar{\mathfrak{x}}$ Untermenge von $\mathfrak{n}$ ist, so folgt

$$m\mathfrak{n}_1 \subseteqq \mathfrak{x},$$
$$m \in \mathfrak{x}.$$

Jedes Element α von $\mathfrak{n}_1$ genügt demnach der Bedingung

$$\alpha m \in \mathfrak{x} \subseteqq \mathfrak{n}.$$

In

$$\alpha = \frac{\alpha m}{m}$$

sind also Zähler und Nenner des Bruches Zahlen aus der Ordnung $\mathfrak{n}$, der Nenner überdies zu k teilerfremd; da nun α ganz ist, so muß es sogar in $\mathfrak{n}$ liegen [23]). Somit ist $\mathfrak{n}_1 \subseteqq \mathfrak{n}$, also $\mathfrak{n}_1 = \mathfrak{n}$.

Satz 25. *Jedes Ideal* $\mathfrak{c}$ *in* $\mathfrak{n}$ *von der Ordnung* $\mathfrak{n}$, *dessen Norm* m *zu* k *teilerfremd ist, genügt der Gleichung*

$$\mathfrak{c} = \mathfrak{c}\mathfrak{o} \cap \mathfrak{n}.$$

Beweis. Nach (3) ist

$$m\mathfrak{n} = \mathfrak{c}\bar{\mathfrak{c}} \subseteqq \mathfrak{c};$$

wegen $(m, k) = 1$ ist

$$m\mathfrak{n} + k\mathfrak{o} \geqq m\mathfrak{n} + k\mathfrak{n} = \mathfrak{n},$$

also um so mehr

$$\mathfrak{c} + k\mathfrak{o} \geqq \mathfrak{n},$$
$$\mathfrak{c} + k\mathfrak{o} = \mathfrak{n},$$

und § 5 der mehrfach zitierten Arbeit von Dedekind liefert die Behauptung.

Satz 26. *Zwei Darstellungen natürlicher Zahlen* m_1, m_2 *durch Formen der Diskriminante* $k^2\Delta$ *mögen die Teiler* d_1 *bzw.* d_2 *haben. Es sei*

$$\frac{m_1}{d_1^2} = \frac{m_2}{d_2^2},$$

---

[22]) Dedekinds Begriff des „Ideals in der Ordnung $\mathfrak{n}$" ist dort freilich ein anderer als der heute gebräuchliche: Außer den gewöhnlichen Idealeigenschaften verlangt Dedekind von einem solchen Ideal $\mathfrak{x}$ noch das Bestehen der Gleichung $\mathfrak{x} + k\mathfrak{o} = \mathfrak{n}$. Aber jedes Ideal im dortigen Sinne ist auch Ideal in dem oben zugrunde gelegten Sinne, und das genügt für den vorliegenden Zweck. — Man findet das Ergebnis auch bei Grell, a. a. O., S. 516.

[23]) Vgl. den Beweis zu Satz 5.

und der gemeinsame Wert dieser beiden Brüche sei zu k teilerfremd. Sind dann die Darstellungen vereinigt, so sind sie sogar assoziiert.

Beweis. Zunächst sei $m_1 = m_2$, $d_1 = d_2 = 1$. Dann ist also $m_1 (= m_2)$ zu k teilerfremd. Sind $\mathfrak{c}_1$ und $\mathfrak{c}_2$ die den Darstellungen zugeordneten Ideale, so gibt es nach Definition 6 eine Einheit ε so, daß

$$\mathfrak{c}_1 = \varepsilon \mathfrak{c}_2$$

ist. Es folgt

$$\mathfrak{c}_1 \mathfrak{o} = \varepsilon \mathfrak{c}_2 \mathfrak{o} = \mathfrak{c}_2 \mathfrak{o},$$

also nach Satz 25

$$\mathfrak{c}_1 = \mathfrak{c}_1 \mathfrak{o} \cap \mathfrak{n} = \mathfrak{c}_2 \mathfrak{o} \cap \mathfrak{n} = \mathfrak{c}_2;$$

die Darstellungen sind also assoziiert.

Im allgemeinen Fall seien etwa die Darstellungen (26) vorgelegt. Entsprechen ihnen die Ideale $\mathfrak{s}_1$ und $\mathfrak{s}_2$, den zugehörigen Darstellungen (27) die Ideale $\mathfrak{s}_1'$ und $\mathfrak{s}_2'$, so ist nach Satz 16

$$\mathfrak{s}_1' = \mathfrak{s}_1,$$
$$\mathfrak{s}_2' = \mathfrak{s}_2;$$

nach Definition 7 sind also auch die Darstellungen (27) vereinigt, also, da sie dem schon erledigten Fall angehören, sogar assoziiert. Nach Satz 17 sind dann auch die Darstellungen (26) assoziiert.

Im Falle $\Delta < -4$ sind übrigens vereinigte Darstellungen stets assoziiert; das erkennt man direkt aus Definition 6 bzw. 7, da es in diesem Fall außer ± 1 keine Einheiten gibt.

§ 7.

Bedeutung der Erweiterungsideale in der Hauptordnung.

In der in Fußnote [8]) genannten Arbeit von Grell findet sich der Begriff des „Erweiterungsideals" präzisiert. Für den hier vorliegenden Fall des Systems der beiden Ringe $\mathfrak{n}$ und $\mathfrak{o}$ sei aus der genannten Arbeit die folgende Definition entnommen:

Definition 8. *Ein Ideal $\mathfrak{x}$ im Ring $\mathfrak{o}$ heißt Erweiterungsideal (in bezug auf $\mathfrak{n}$), wenn es sich in der Gestalt $\mathfrak{y}\mathfrak{o}$ darstellen läßt, wo $\mathfrak{y}$ Ideal in $\mathfrak{n}$ ist.*

Satz 27. *Ist die natürliche Zahl m durch die Formenklasse K darstellbar, M die K zugeordnete Modulklasse, O die Klasse des Moduls $\mathfrak{o}$, so gibt es in der Klasse MO ein Erweiterungsideal (in $\mathfrak{o}$) von der Norm m.*

Beweis. Zu einer Darstellung von m durch eine Form aus K werde im Sinne des $\mathfrak{m}$-Algorithmus das Ideal $\mathfrak{c}$ in M von der Norm m konstruiert. Das Ideal $\mathfrak{c}\mathfrak{o}$ in $\mathfrak{o}$ liegt dann in der Klasse MO, hat die Norm m und ist Erweiterungsideal.

Dieser Satz ist aber nicht allgemein umkehrbar. Aus der Existenz eines Erweiterungsideals $\mathfrak{x}$ von der Norm m in MO kann nämlich nicht rückwärts auf die Existenz eines Ideals $\mathfrak{y}$ in $\mathfrak{n}$ von der Norm m geschlossen werden, das in M liegt. Um ein solches Ideal zu konstruieren, ist man versucht, es noch der Bedingung $\mathfrak{y}\mathfrak{o} = \mathfrak{x}$ zu unterwerfen, die erfüllbar scheint, weil $\mathfrak{x}$ Erweiterungsideal ist. Die Forderung, daß $\mathfrak{y}$ speziell der Klasse M angehört, ist dabei jedoch zu stark[24]); ein Ideal $\mathfrak{y}$ in $\mathfrak{n}$ mit $\mathfrak{y}\mathfrak{o} = \mathfrak{x}$ braucht nicht einmal die Ordnung $\mathfrak{n}$ zu haben[25]).

Dieser Übelstand läßt sich nun aber in gewissem Grade reparieren. Im allgemeinen gibt es nämlich, wie Grell[26]) im einzelnen ausführt, zu einem gegebenen Erweiterungsideal $\mathfrak{x}$ mehrere Ideale $\mathfrak{y}$ in $\mathfrak{n}$ mit $\mathfrak{y}\mathfrak{o} = \mathfrak{x}$. Für ihre Gesamtheit werde von Grell die folgende Bezeichnung übernommen:

Definition 9. *Die Gesamtheit aller Ideale $\mathfrak{y}$ in $\mathfrak{n}$, für die $\mathfrak{y}\mathfrak{o}$ gleich dem festen Erweiterungsideal $\mathfrak{x}$ in $\mathfrak{o}$ ist, heißt die zu $\mathfrak{x}$ gehörige Erweiterungsklasse*[27]) *(in der Ordnung $\mathfrak{n}$).*

Offenbar muß die Ordnung jedes Ideals der Erweiterungsklasse die Ordnung $\mathfrak{n}$ umfassen. Es gilt nun aber der

Satz 28. *Ist $\mathfrak{y}$ Ideal in $\mathfrak{n}$ und von einer Ordnung $\mathfrak{n}_1 \supset \mathfrak{n}$, so gibt es in der zu $\mathfrak{y}\mathfrak{o}$ gehörigen Erweiterungsklasse ein Ideal $\mathfrak{z}$, welches echtes Vielfaches von $\mathfrak{y}$ ist und genau die Ordnung $\mathfrak{n}$ hat.*

Beweis. Wegen $\mathfrak{n}\mathfrak{n}_1 = \mathfrak{n}_1$ gibt es nach Dedekinds Theorie der Moduln[28]) einen Modul $\mathfrak{z}$ von der Ordnung $\mathfrak{n}$, der die Gleichung

$$\mathfrak{z}\mathfrak{n}_1 = \mathfrak{y}$$

löst. Für dieses $\mathfrak{z}$ wird zunächst

$$\mathfrak{z} \subseteq \mathfrak{z}\mathfrak{n}_1 = \mathfrak{y},$$

wegen $\mathfrak{z}^0 \neq \mathfrak{y}^0$ aber sogar

$$\mathfrak{z} \subset \mathfrak{y}.$$

Hieraus folgt überdies $\mathfrak{z} \subset \mathfrak{n}$; wegen $\mathfrak{z}^0 = \mathfrak{n}$ ist also $\mathfrak{z}$ Ideal in $\mathfrak{n}$. Endlich ist

$$\mathfrak{z}\mathfrak{o} = \mathfrak{z}\mathfrak{n}_1\mathfrak{o} = \mathfrak{y}\mathfrak{o};$$

$\mathfrak{z}$ liegt also in der zu $\mathfrak{y}\mathfrak{o}$ gehörigen Erweiterungsklasse aus $\mathfrak{n}$.

---

[24]) Sie ließe sich natürlich erfüllen, wenn $\mathfrak{y}$ nur Modul zu sein brauchte; aber $\mathfrak{y}$ soll Ideal in $\mathfrak{n}$ sein.

[25]) Ein einfaches Beispiel hierfür bietet schon der Führer $\mathfrak{y} = k\mathfrak{o}$. — Ist dagegen $N(\mathfrak{x})$ zu k teilerfremd angenommen, so muß allerdings, wie sich zeigen läßt, $\mathfrak{y}^0 = \mathfrak{n}$ sein.

[26]) A. a. O., S. 507.

[27]) Natürlich hat dieser Begriff nichts mit Idealklassen im gewöhnlichen Sinne zu tun.

[28]) A. a. O., S. 650ff.

Hierin steckt unter anderem der

Satz 29. *In jeder Erweiterungsklasse aus* $\mathfrak{n}$ *gibt es mindestens ein Ideal, dessen Ordnung genau* $\mathfrak{n}$ *ist.*

Man greife nämlich irgendein Ideal $\mathfrak{y}$ aus der Erweiterungsklasse heraus. Hat $\mathfrak{y}$ schon die Ordnung $\mathfrak{n}$, so ist man fertig; andernfalls liefert der vorige Satz die Behauptung.

Mit diesen Hilfsmitteln gelingt nun eine teilweise Umkehrung des Satzes 27 in folgender Weise:

Satz 30. *Gibt es in der Idealklasse* A *in der Hauptordnung ein Erweiterungsideal* $\mathfrak{x}$ *von der Norm* m *und sind* $M_1, M_2, \ldots, M_r$ *diejenigen Modulklassen von der Ordnung* $\mathfrak{n}$, *die durch Multiplikation mit der Klasse* O *des Moduls* $\mathfrak{o}$ *die Klasse* AO *liefern,* $K_1, K_2, \ldots, K_r$ *die zugehörigen Formenklassen, so ist* m *durch mindestens eine der Klassen* K_i *darstellbar.*

Beweis. Nach Satz 29 gibt es in der zu $\mathfrak{x}$ gehörigen Erweiterungsklasse in $\mathfrak{n}$ mindestens ein Ideal $\mathfrak{y}$, das genau die Ordnung $\mathfrak{n}$ hat, also in einer Modulklasse von der Ordnung $\mathfrak{n}$ liegt. Wegen $\mathfrak{y}\mathfrak{o} = \mathfrak{x}$ muß dies überdies eine der Klassen $M_1, M_2, \ldots, M_r$ sein. Da $\mathfrak{y}$ ebenfalls die Norm m hat, so liefert Satz 1 die Behauptung.

Aus Satz 24 folgt sofort der

Satz 31. *Jedes zum Führer* k *von* $\mathfrak{n}$ *teilerfremde Ideal in* $\mathfrak{o}$ *ist Erweiterungsideal.*

Definition 10. *Unter einer Erweiterungsprimzahl (in bezug auf die Diskriminante* $D = k^2\Delta$*) sei eine natürliche Primzahl* p *verstanden, die so beschaffen ist, daß jedes in* p *aufgehende Primideal des Körpers* Δ *Erweiterungsideal in bezug auf die Ordnung vom Führer* k *ist.*

Jede nicht in k aufgehende Primzahl ist Erweiterungsprimzahl; das ergibt sich aus Satz 31 unmittelbar. Aber es gibt auch Diskriminanten D, deren Erweiterungsprimzahlen teilweise in dem zugehörigen k aufgehen. Das zeigt folgender Satz:

Satz 32. *Ist die Primzahl* p *ein Teiler von* k, *aber nicht von* Δ, *und zugleich quadratischer Nichtrest nach* Δ, *d. h. im Körper* Δ *unzerlegbar, so ist das Primideal* $\mathfrak{p} = p\mathfrak{o}$ *Erweiterungsideal in bezug auf die Ordnung* $\mathfrak{n}$ *vom Führer* k.

Beweis. Es ist

$$\mathfrak{p} = (p\mathfrak{n})\mathfrak{o},$$

und $p\mathfrak{n}$ ist Ideal in $\mathfrak{n}$.

Definition 11. *Das Produkt aller in* k *aufgehenden Erweiterungsprimzahlen (mehrfache mehrfach gezählt) heiße der größte Erweiterungsteiler von* k.

Der größte Erweiterungsteiler von k hängt außer von k noch von Δ ab. Satz 32 zeigt, daß er im allgemeinen von 1 verschieden ist.

Definition 12. *Eine Zahl m heißt zu k erweiterungsprim (in bezug auf die Stammdiskriminante Δ), wenn (m, k) Potenzteiler*[17]) *des größten Erweiterungsteilers von k ist.*

Satz 33. *Ist die natürliche Zahl m erweiterungsprim zu k, gibt es in der Idealklasse A aus der Hauptordnung ein Ideal $\mathfrak{x}$ von der Norm m und sind die Formenklassen $K_1, K_2, \ldots, K_r$ denjenigen Modulklassen von der Ordnung $\mathfrak{n}$ zugeordnet, die durch Multiplikation mit der Klasse O des Moduls $\mathfrak{o}$ die Klasse AO liefern, so ist m durch mindestens eine der Klassen K_i darstellbar.*

Beweis. Man zerlege $\mathfrak{x}$ in Primideale:

$$\mathfrak{x} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_s .$$

Ist etwa p_i die durch $\mathfrak{p}_i$ teilbare natürliche Primzahl, so folgt

$$p_i | N(\mathfrak{x}),$$
$$p_i | m.$$

Entweder ist also p_i zu k teilerfremd, oder es ist $p_i | (m, k)$; im ersten Fall folgt aus Satz 31, im zweiten aus Definition 12 und 11, daß p_i Erweiterungsprimzahl und daher $\mathfrak{p}_i$ Erweiterungsideal ist. Offenbar gilt letzteres dann auch für das Produkt $\mathfrak{x}$ der $\mathfrak{p}_i$. Satz 30 ergibt also die Behauptung.

Auf Grund dieses Prinzips der Idealerweiterung ordnen sich schließlich auch die klassischen Ergebnisse über die Darstellung der zum Führer teilerfremden natürlichen Zahlen ein. Nach Satz 1 waren für die Darstellbarkeit der natürlichen Zahl m maßgebend die Ideale $\mathfrak{c}$ in $\mathfrak{n}$, soweit sie die Ordnung $\mathfrak{n}$ und die Norm m haben. Ist nun m teilerfremd zu k, so sind diese Ideale gemäß Satz 24 und 25 ein-eindeutig den sämtlichen zu k teilerfremden Idealen $\mathfrak{a}$ in der Hauptordnung zugeordnet vermöge der Beziehung

$$\mathfrak{c}\mathfrak{o} = \mathfrak{a} \tag{30}$$

oder der Beziehung

$$\mathfrak{c} = \mathfrak{a} \cap \mathfrak{n}.$$

Im Anschluß hieran übertragen sich die Ergebnisse auf die Ideale der Hauptordnung, indessen erst dann, wenn auch die Klasseneinteilung übertragen ist. Eine Zuordnung der Modulklassen von der Ordnung $\mathfrak{n}$ zu den Idealklassen in der Hauptordnung ist wegen der im allgemeinen verschiedenen Anzahl nicht möglich. Wohl aber leisten die von H. Weber[29]) aus-

[29]) A. a. O., § 99.

führlich betrachteten und dort als „Idealklassen nach der Ordnung $\mathfrak{n}$" bezeichneten Klassen das Gewünschte. Eine solche Klasse ist definiert als die Gesamtheit aller derjenigen Ideale $\mathfrak{b}$ in der Hauptordnung, die zu einem festen zu k teilerfremden Ideal $\mathfrak{a}$ in der Beziehung

$$\mathfrak{b} = \frac{\eta_1}{\eta_2}\,\mathfrak{a}$$

stehen, wo η_1 und η_2 ganze zu k teilerfremde Zahlen in der Ordnung $\mathfrak{n}$ sind und $\frac{\eta_1}{\eta_2}$ positive Norm hat[30]). Zu einer Darstellung einer zu k teilerfremden natürlichen Zahl m konstruiere man nun im Sinne des $\mathfrak{m}$-Algorithmus das Ideal $\mathfrak{c}$, welches ehemals die der Klasse K der darstellenden Form zugeordnete Modulklasse M lieferte. Das Ideal

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

in der Hauptordnung ist zu k teilerfremd und hat die Norm m. Diejenige Idealklasse M' „nach der Ordnung $\mathfrak{n}$", die das Ideal $\mathfrak{a}$ enthält, kann man nun im Anschluß an H. Weber[31]) der gegebenen Darstellung von m zuordnen. Aus dem erwähnten durch (30) vermittelten ein-eindeutigen Entsprechen folgt aber unschwer, daß die Zuordnung $M \longrightarrow M'$ eine ein-eindeutige Zuordnung der Modulklassen von der Ordnung $\mathfrak{n}$ zu den Idealklassen (in $\mathfrak{o}$) nach der Ordnung $\mathfrak{n}$ bedeutet. Die in Betracht kommenden Ideale in zwei einander zugeordneten Klassen stehen paarweise in der Beziehung (30). Daraus ersieht man sofort: Eine zu k teilerfremde natürliche Zahl m ist dann und nur dann durch die Formenklasse K darstellbar, wenn es in der zugehörigen Klasse M' ein Ideal in $\mathfrak{o}$ von der Norm m gibt. Die klassische Deutung der Darstellbarkeit erscheint damit als ein nachträglicher Übergang zur Hauptordnung und ist, wie man sieht, streng an den teilerfremden Fall gebunden.

---

[30]) Im vorliegenden Spezialfall des quadratischen Körpers kann diese Klasseneinteilung auch charakterisiert werden als eine solche, die durch „Komplexion" aus der bekannten, in der Klassenkörpertheorie üblichen Einteilung in „Strahlklassen" entsteht. Zu diesen Begriffen vgl. H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil I: Klassenkörpertheorie (Jahresbericht der Deutschen Mathematiker-Vereinigung **35** (1926), S. 1—55, dort S. 5f. und 41). — Ein entsprechender Satz für Körper höheren Grades besteht nicht.

[31]) Dieser nimmt allerdings (a. a. O., § 99) die Klasse des Ideals $\bar{\mathfrak{a}}$.

(Eingegangen am 26. 6. 1929.)