Sitzungsberichte

der

mathematisch-naturwissenschaftlichen Abteilung

der

Bayerischen Akademie der Wissenschaften zu München

Jahrgang 1943

München 1944
Verlag der Bayerischen Akademie der Wissenschaften
In Kommission bei der C. H. Beck'schen Verlagsbuchhandlung

Druck der C. H. Beck'schen Buchdruckerei in Nördlingen

Über gewisse Anzahlformeln in der Theorie der quadratischen Formen

Von Martin Eichler in Darmstadt

Eingesandt von Herrn E. Hecke für die Sitzung vom 9. Dezember 1942

Einleitung

1. In den letzten Jahren hat Herr Hecke im Zusammenhang mit seinen Untersuchungen in der Theorie der elliptischen Modulfunktionen merkwürdige multiplikative Beziehungen zwischen den Darstellungsanzahlen von Zahlen durch quadratische Formen beliebiger gerader Variablenzahl gefunden, welche bisher erst in wenigen Spezialfällen von der Arithmetik der Formen her bewiesen werden konnten.[1] Diese Beziehungen sind um so auffallender, wenn man einerseits bedenkt, daß sie in diesen Fällen, wo die Formen die Normen aus quadratischen assoziativen Algebren darstellen, mit Eigenschaften von Idealen aus diesen Algebren äquivalent sind,[2] und wenn man andererseits weiß, daß die quadratischen Formen sonst in einer ähnlichen Beziehung zu assoziativen Algebren nicht stehen.

Man wird den zahlentheoretischen Grundlagen der Heckeschen Formeln auf die Spur kommen, wenn man gewisse Eigenschaften

---

[1] Eine übersichtliche Skizze seiner Ergebnisse hat Herr Hecke auf dem internationalen Mathematikerkongreß 1936 in Oslo gegeben: E. Hecke, Neuere Fortschritte in der Theorie der elliptischen Modulfunktionen, Comptes rendus du congrès international des Mathématiciens, Oslo 1936. Soweit sich die Sätze auf Darstellungsanzahlen von quadratischen Formen speziell, nicht auf Koeffizienten allgemeinerer Modulformen beziehen, sind sie in mehreren Abhandlungen zerstreut. Hiervon sind besonders zu nennen: Über Modulfunktionen und Dirichletsche Reihen mit Eulerscher Produktentwicklung I u. II. Math. Ann. **114** (1937), S. 1–28, 316–351. Über die Darstellung der Determinante einer positiven quadratischen Form durch die Form. Fueterfestschrift: Vierteljahrsschrift Naturf. Ges. Zürich 1940, S. 64–70. Analytische Arithmetik der positiven quadratischen Formen. Kgl. Danske Vidensk. Selsk.; Math.-Phys. Medd. XVII, 12, S. 1–134 (1940).

[2] H. Brandt, Idealtheorie in Quaternionenalgebren. Math. Ann. **99** (1928), S. 1–29. Siehe auch: Über die Komponierbarkeit der quaternären quadratischen Formen. Math. Ann. **94** (1925), S. 179–197.

der Ideale von Algebren herausschält, die sich in einer Weise in die Sprache der Formentheorie übersetzen lassen, daß weder in unmittelbarer noch in mittelbarer Weise, etwa auf dem Wege über die Kompositionstheorie, das Zugrundeliegen von Algebren in Erscheinung tritt. Eigenschaften, für die eine solche Abstraktion möglich ist, beruhen in der wechselseitigen Beziehung der Ideale zu Transformationen von Formen in das Vielfache anderer Formen.[1]

Diese Transformationen, die ich Transformatoren nennen möchte, bilden den Gegenstand dieser Zeilen. Die Transformatoren lassen sich hintereinander ausführen oder kürzer: multiplizieren, und sie gehorchen bezüglich der Multiplikation und der stets möglichen Primzerlegung denselben Gesetzen wie die Ideale einfacher Algebren. Dies ist auch nicht verwunderlich, denn in den Fällen, wo die betreffenden Formen die Normen aus Algebren darstellen, lassen sich die Transformatoren geradezu mit den Idealen dieser Algebren gleichsetzen. Herr Brandt hat sie schon längst als ein wichtiges Hilfsmittel bei der Begründung der Idealtheorie benutzt;[2] die vorliegenden Untersuchungen sind also gar nicht neuartig.

Die Theorie der Transformatoren wird hier bis zur Herleitung eines Formelsystems (Gl. (20)–(25)) verfolgt, in dem die Anzahlen der Transformatoren mit gegebener „Norm" und die Darstellungsanzahlen von natürlichen Zahlen durch quadratische Formen verknüpft auftreten, und welches in Gl. (27) und (28) dasselbe auszusagen scheint wie Herrn Heckes Relationen. Zwar werden diese Anzahlformeln noch unter der Annahme gewisser vereinfachender Voraussetzungen bewiesen, doch dürften sie trotzdem einen allgemeinen Begriff von den Gesetzmäßigkeiten vermitteln, die hier herrschen. Ich hoffe, bei späterer Gelegenheit eine vollständigere Behandlung des angeschnittenen Themas liefern zu können.

---

[1] Die Möglichkeit der hier durchgeführten Betrachtungen ist nicht auf die quadratischen Formen beschränkt. Selbstverständlich beanspruchen aber die quadratischen Formen schon aus historischen Gründen das meiste Interesse.

[2] So z. B. vielfach in Vorlesungen in Halle. Besonders s. Idealtheorie in Quaternionenalgebren, a. a. O. S. 1.

§ 1. Die Transformatoren

2. Den Betrachtungen liegen quadratische Formen gerader Variablenzahl

$$(1)\quad f(x_1, \ldots, x_{2n}) = \frac{1}{2}\sum_{i,k=1}^{2n} f_{ik}x_i x_k \qquad (f_{ik} = f_{ki}, f_{ii} \equiv 0 \bmod 2)$$

mit ganzen rationalen Koeffizienten und der Diskriminante

$$D = (-1)^n |f_{ik}|$$

zugrunde. Es ist praktisch, durchweg Matrizenschreibweise zu verwenden. Dazu werde folgendes verabredet: Matrizen werden mit deutschen Buchstaben bezeichnet, und zwar mit großen Buchstaben nur die quadratischen Matrizen. Falls es notwendig ist, sollen obere Indizes in Klammern die Anzahl der auftretenden Zeilen und Spalten angeben, so soll z. B. $\mathfrak{t}^{(2n,m)}$ eine Matrix aus $2n$-Zeilen und m-Spalten sein und $\mathfrak{T}^{(n)}$ eine n-reihige quadratische Matrix. Gelegentlich auftretende obere Indizes ohne Klammern werden stets eine andere Bedeutung haben, die aus dem Zusammenhang ersichtlich sein wird. Die Nullmatrix von n-Zeilen und m-Spalten schreibe ich $\mathfrak{N}^{(n,m)}$, die n-reihige Einheitsmatrix $\mathfrak{E}^{(n)}$. Der Spiegelungsprozeß wird üblicherweise durch einen Punkt angedeutet. Die Buchstaben $\mathfrak{F}$, $\mathfrak{F}_1$, ..., $\mathfrak{G}$ seien speziell für symmetrische Matrizen mit geraden Diagonalengliedern reserviert. Mit dem Spaltenvektor $\mathfrak{x}$, der die Komponenten $x_1, \ldots, x_{2n}$ hat, schreibt sich (1) so:

$$2f(x_1, \ldots, x_{2n}) = \dot{\mathfrak{x}}\mathfrak{F}\mathfrak{x}.$$

Da keine Mißverständnisse zu befürchten sind, darf abkürzend von der quadratischen Form $\mathfrak{F}$ gesprochen werden.

Sämtliche hier betrachteten Formen sollen untereinander in der Beziehung stehen, daß sie die gleiche Diskriminante haben und ineinander durch umkehrbare lineare Substitutionen mit rationalen Koeffizienten unter gleichzeitiger Abspaltung rationaler Faktoren überführbar sind.[1] Da hier nicht von den verschiedenen Einteilungsmöglichkeiten der Formen in größere oder

[1] Sie gehören in der Terminologie von Herrn Brandt zu einer Formensippe. H. Brandt: Zur Zahlentheorie der quadratischen Formen, Jahresbericht Deutsche Math.-Verein. **47** (1937), S. 149–159.

kleinere Gesamtheiten die Rede ist, sondern nur von einer jeweils bestimmten Gesamtheit, will ich kurz von dem Formensystem sprechen, das den Betrachtungen zugrunde liegt. Sämtliche h Klassen des Systems denke ich mir dabei durch je eine Form $\mathfrak{F}_1, \ldots, \mathfrak{F}_h$ vertreten.

3. Eine $2n$-reihige quadratische ganzzahlige Matrix $\mathfrak{T}_{ik}$ soll ein Transformator des Formensystems heißen, wenn es ein $\mathfrak{F}_i$ und ein $\mathfrak{F}_k$ im System so gibt, daß

$$\dot{\mathfrak{T}}_{ik}\,\mathfrak{F}_i\,\mathfrak{T}_{ik} = t\cdot\mathfrak{F}_k$$

mit einer ganzen rationalen Zahl t ist; $\mathfrak{T}_{ik}$ gehört links zu $\mathfrak{F}_k$ und rechts zu $\mathfrak{F}_i$. Die Zahl t ist die Norm des Transformators und wird $N(\mathfrak{T}_{ik})$ geschrieben; es gilt

$$N(\mathfrak{T}_{ik})^n = \pm\,|\,\mathfrak{T}_{ik}\,|.$$

Ist $\mathfrak{T}_{ik}$ unimodular, d. h. ist auch die inverse Matrix $\mathfrak{T}_{ik}^{-1}$ ganzzahlig, so ist $i = k$, und $\mathfrak{T}_{ik}$ ist ein Automorphismus (im weiteren Sinne) von $\mathfrak{F}_i$, oder eine Einheit. Die Normen der Einheiten sind ± 1.

Ist $\mathfrak{T}_i = \mathfrak{T}_i^{(2n)}$ eine ganzzahlige Matrix der Determinante t^n, für welche die Form $\dot{\mathfrak{T}}_i\,\mathfrak{F}_i\,\mathfrak{T}_i$ durch t teilbar ist, so enthält die Klasse der zu $\mathfrak{T}_i$ rechtsseitig assoziierten Matrizen, d. h. die Gesamtheit der $\mathfrak{T}_i\,\mathfrak{U}^{(2n)}$ mit unimodularem $\mathfrak{U}^{(2n)}$, mindestens einen Transformator $\mathfrak{T}_{ik}$. Die Gesamtheit aller dieser $\mathfrak{T}_i\,\mathfrak{U}^{(2n)}$ soll kurz eine rechts zu $\mathfrak{F}_i$ gehörige Transformatorenklasse heißen. Bezeichnet $\mathrm{I}^{(2n)}$ den Ring aller ganzzahligen $2n$-reihigen Matrizen, so ist die Transformatorenklasse, zu der ein Transformator $\mathfrak{T}_{ik}$ gehört, bereits durch das Ideal

$$\mathrm{T}_{ik} = \mathfrak{T}_{ik}\,\mathrm{I}^{(2n)}$$

eindeutig festgelegt.

Sind $\mathfrak{T}_{ij}$ und $\mathfrak{T}_{jk}$ zwei Transformatoren, und gehört $\mathfrak{T}_{ij}$ links zu der gleichen Form, zu welcher $\mathfrak{T}_{jk}$ rechts gehört, so ist auch das Matrizenprodukt $\mathfrak{T}_{ik} = \mathfrak{T}_{ij}\cdot\mathfrak{T}_{jk}$ ein Transformator. Läßt man „gebrochene" Transformatoren zu, was ich hier allerdings nicht vorhabe, so gilt:

Die ganzen und gebrochenen Transformatoren eines Formensystems bilden ein Gruppoid.

§ 2. Die primären Transformatoren

4. Ein ganzer Transformator soll ein Primtransformator heißen, wenn er sich nicht als Produkt zweier ganzer Transformatoren schreiben läßt, die beide keine Einheiten sind. Normen von Primtransformatoren sind stets Potenzen von Primzahlen, wie aus dem Folgenden hervorgeht. Allgemein möge ein Transformator, dessen Norm eine Primzahlpotenz ist, primär heißen.

Es sei $\mathfrak{T}_{ik}$ irgendein ganzer Transformator und p^h die höchste in seiner Norm aufgehende Potenz einer Primzahl p. Dann transformieren alle Matrizen aus dem Ideal

$$\mathfrak{T}_i = \mathfrak{T}_{ik}\, \mathfrak{I}^{(2n)} + p^h\, \mathfrak{I}^{(2n)}$$

die Form $\mathfrak{F}_i$ in das p^h-fache von Formen mit i. a. größeren Diskriminanten als D. Nun ist $\mathfrak{T}_i$ bekanntlich ein Hauptideal: $\mathfrak{T}_i = \mathfrak{T}_i\, \mathfrak{I}^{(2n)}$, dabei gibt es also eine ganzzahlige Matrix $\mathfrak{S}$ mit $\mathfrak{T}_i\, \mathfrak{S} = \mathfrak{T}_{ik}$. $\mathfrak{T}_i$ transformiert die Form $\mathfrak{F}_i$ in das p^h-fache einer Form der gleichen Diskriminante D, die schließlich mittels einer unimodularen Matrix $\mathfrak{U}$ in eine der Formen $\mathfrak{F}_1, \ldots, \mathfrak{F}_h$, etwa in $\mathfrak{F}_j$, übergeführt werden kann. Jetzt ist $\mathfrak{T}_i\, \mathfrak{U} = \mathfrak{T}_{ij}$ ein rechts zu $\mathfrak{F}_i$ gehöriger Transformator der Norm p^h, und zwar ein „Linksteiler" von $\mathfrak{T}_{ik}$. Der durchgeführten Konstruktion nach ist $\mathfrak{T}_{ij}$ offenbar durch $\mathfrak{T}_{ik}$ und seine Norm p^h bis auf rechtsseitige Einheiten $\mathfrak{T}_{jj}$ eindeutig bestimmt. Es gilt demnach:

Jeder ganze Transformator läßt sich als Produkt primärer Transformatoren schreiben. Die einzelnen Faktoren sind nach Vorgabe ihrer Normen bis auf Einheiten eindeutig festgelegt.

Entsprechendes gilt allgemeiner bei Zerlegung eines Transformators in ein Produkt von Transformatoren mit relativ primen Normen.

§ 3. Die Primtransformatoren

5. Die weitere Zerlegung der primären Transformatoren in Primtransformatoren soll unter der Voraussetzung durchgeführt werden, daß das zugrunde liegende Formensystem aus Stamm-

formen[1] besteht. Es ergeben sich dann besonders durchsichtige Verhältnisse. Ohne diese Voraussetzung wird die Theorie ähnlich schwerfällig, wie man es von der allgemeinen Dedekindschen Idealtheorie nicht maximaler Ordnungen weiß.

In völliger Analogie zu der Theorie des quadratischen Zahlkörpers gilt der Satz:

Die Norm eines Primtransformators ist entweder eine Primzahl p oder p^2, und zwar tritt der zweite Fall dann und nur dann ein, wenn

$$\left(\frac{D}{p}\right) = -1 \tag{2}$$

ist.

Die Behauptung des Satzes zerfällt in zwei Teile. Ich erledige als erstes den leichteren Teil, indem ich zeige: gibt es einen Transformator der Norm p, so ist (2) falsch. Es sei $\mathfrak{T}$ ein Transformator der Norm p, der rechts zu der Form $\mathfrak{F}$ gehört, dann ist also

$$\dot{\mathfrak{T}}\mathfrak{F}\mathfrak{T} \equiv 0 \bmod p; \tag{3}$$

diese Kongruenz ist im Falle $p = 2$ so zu verstehen, daß die durch 2 dividierte linke Seite eine symmetrische Matrix mit geraden Diagonalengliedern ist.

Es gilt nun mit zwei unimodularen Matrizen $\mathfrak{U}^{(2n)}$ und $\mathfrak{V}^{(2n)}$ und einer Diagonalmatrix $\mathfrak{D}$

$$\mathfrak{V}^{(2n)}\mathfrak{T}\mathfrak{U}^{(2n)} = \mathfrak{D} = \begin{pmatrix} p^{\alpha_1} & & & \\ & \cdot & & \\ & & \cdot & \\ & & & p^{\alpha_{2n}} \end{pmatrix}, \tag{4}$$

wobei $p^{\alpha_1}, \ldots, p^{\alpha_{2n}}$ die Elementarteilerquotienten von $\mathfrak{T}$ sind, also der Ungleichung

$$\alpha_1 \leqq \cdots \leqq \alpha_{2n} \tag{5}$$

[1] Unter einer Stammform versteht man nach H. Brandt (vgl. Anm. 1 S. 3) eine ganzzahlige Form $\mathfrak{F}$, die nicht rational in eine Form $a\,\mathfrak{F}'$ transformierbar ist, wobei a eine rationale Zahl und $\mathfrak{F}'$ eine ganzzahlige Form von kleinerer Determinante als $\mathfrak{F}$ ist.

genügen. Ersetzt man die allenfalls auftretenden α_ν, die größer als 1 sind, durch 1, so bleibt die Kongruenz (3) richtig, der so abgeänderte Transformator transformiert dann aber $\mathfrak{F}$ in das p-fache einer Form von kleinerer Diskriminante, was der vorausgesetzten Stammformeneigenschaft widerspricht. Da andererseits das Produkt sämtlicher p^{α_ν} gleich der n-ten Potenz der Norm, also gleich p^n sein muß, sind die Elementarteiler von $\mathfrak{T}$ zur Hälfte 1 und zur anderen Hälfte p.

Nun folgt aus (3) und (4)

$$\dot{\mathfrak{B}}^{-1}\,\mathfrak{F}\,\mathfrak{B}^{-1} \equiv \begin{pmatrix} \mathfrak{N}^{(n)} & \mathfrak{W}^{(n)} \\ \dot{\mathfrak{W}}^{(n)} & \mathfrak{X}^{(n)} \end{pmatrix} \bmod p, \tag{6}$$

und hieraus durch Determinantenbildung

$$D = |\mathfrak{W}|^2 \bmod p,$$

im Widerspruch zu (2).

Die Schlußweise bleibt auch dann noch gültig, wenn die Norm eine Potenz von p und der Rang von $\mathfrak{T}$ mod p gleich n ist. Hierauf wird weiter unten zurückgegriffen.

6. Als zweites ist umgekehrt zu zeigen, daß ein Transformator der Norm $p^\alpha > p$ stets einen echten Teiler haben muß, wenn (2) nicht zutrifft, und daß für $p^\alpha > p^2$ unter allen Umständen ein echter Teiler von $\mathfrak{T}$ existiert. Ich führe die folgenden Betrachtungen zunächst für $p > 2$ durch und gebe in Nr. 8 die Modifikationen an, die für $p = 2$ zu machen sind. Zunächst behandle ich den Spezialfall, daß $\mathfrak{T} = p\,\mathfrak{E}^{(2n)}$ ist, und zeige: ist (2) falsch, so läßt sich $\mathfrak{T}$ echt zerlegen. Es ist erlaubt, $\mathfrak{F}$ bei diesem Nachweis durch eine p-adisch ganz äquivalente Form zu ersetzen. Als solche ist unter den angenommenen Voraussetzungen eine der folgenden Formen möglich:

$$\begin{pmatrix} & \mathfrak{E}^{(n)} \\ \mathfrak{E}^{(n)} & \end{pmatrix}, \quad \begin{pmatrix} & & \mathfrak{E}^{(n-1)} \\ \mathfrak{E}^{(n-1)} & & \\ & a_1 & \\ & & a_2 p \end{pmatrix}, \quad \begin{pmatrix} & & \mathfrak{E}^{(n-2)} & \\ \mathfrak{E}^{(n-2)} & & & \\ & a_1 & & \\ & & a_2 & \\ & & & a_3 p \\ & & & & a_4 p \end{pmatrix} \tag{7}$$

(die nicht besetzten Stellen sind durch Nullen zu füllen) mit $a_1 \not\equiv 0 \bmod p$, ..., $a_4 \not\equiv 0 \bmod p$, je nach dem, ob D keinmal,

einmal oder zweimal durch p teilbar ist. Andere Fälle treten bei Stammformen und ungeradem p nicht auf. In den drei Fällen hat jeweils die Matrix

$$(8) \qquad \begin{pmatrix} \mathfrak{E}^{(n)} & \\ & p\,\mathfrak{E}^{(n)} \end{pmatrix}, \begin{pmatrix} \mathfrak{E}^{(n-1)} & & \\ & p\,\mathfrak{E}^{(n-1)} & \\ & & p \\ & & & 1 \end{pmatrix}, \begin{pmatrix} \mathfrak{E}^{(n-2)} & & & \\ & p\,\mathfrak{E}^{(n-2)} & & \\ & & p & \\ & & & p \\ & & & & 1 \\ & & & & & 1 \end{pmatrix}$$

die Eigenschaft, $\mathfrak{F}$ in das p-fache einer Form gleicher Diskriminante zu transformieren, und erzeugt daher eine Transformatorenklasse der Norm p; jeder Transformator dieser Klasse ist ein echter Teiler von $\mathfrak{T} = p\,\mathfrak{E}^{(2n)}$.

7. Jetzt sei $\mathfrak{T}$ irgendein Transformator von $\mathfrak{F}$ der Norm $p^\alpha > p$. Nimmt man $\mathfrak{F}$ nach Nr. 5 mit $\mathfrak{V}^{(2n)}$ transformiert an, so hat $\mathfrak{T}$ die in (4) angegebene Diagonalform $\mathfrak{D}$. Für die Exponenten der Elementarteiler von $\mathfrak{T}$ gilt neben der Ungleichung (5) die Gleichung

$$(9) \qquad \alpha_1 + \ldots + \alpha_{2n} = n\alpha.$$

Nach der Schlußweise von Nr. 5 ist keine der Zahlen $\alpha_i > \alpha$.

Ist $0 < \alpha_1 < \alpha_{2n}$ oder $1 < \alpha_1 = \alpha_{2n}$, so ist der Transformator $p\,\mathfrak{E}^{(2n)}$ ein echter Teiler von $\mathfrak{T}$. Ist ferner $\alpha_1 = \alpha_{2n} = 1$, so ist $\mathfrak{T} = p\,\mathfrak{E}^{(2n)}$ und auf Grund des in Nr. 6 Bewiesenen echt zerlegbar, wenn (2) falsch ist, nach Nr. 5 dagegen nicht zerlegbar, wenn (2) gilt, in Übereinstimmung mit der Behauptung.

Es bleibt mithin der Fall $\alpha_1 = 0$ zu diskutieren übrig. Jetzt sei

$$0 = \alpha_1 = \ldots = \alpha_\nu < \alpha_{\nu+1} \leqq \alpha_{2n-\mu} < \alpha_{2n-\mu+1} = \ldots = \alpha_{2n}.$$

Ich zeige zunächst, daß $\mu = \nu$ und $\alpha_{2n} = \alpha$ ist. Dazu betrachte ich die Teilmatrix $\mathfrak{f}^{(\nu,2n)}$ von $\mathfrak{F}$, die aus den ersten ν Zeilen von $\mathfrak{F}$ besteht. Wegen

$$(10) \qquad \dot{\mathfrak{T}}\,\mathfrak{F}\,\mathfrak{T} = \mathfrak{D}\,\mathfrak{F}\,\mathfrak{D} \equiv 0 \bmod p^\alpha$$

sind die Zahlen in der i-ten Spalte von $\mathfrak{f}^{(\nu,2n)}$ durch $p^{\alpha-\alpha_i}$ teilbar; insbesondere sind die Zahlen der ν ersten Spalten von $\mathfrak{f}^{(\nu,2n)}$ durch p^α, also auch durch p^2 teilbar. Wäre nun $\alpha_{2n} < \alpha$ oder $\alpha_{2n} = \alpha$ und $\mu < \nu$, so wäre der Rang von $\mathfrak{f}^{(\nu,2n)}$ mod p kleiner als ν, es gäbe demnach ein unimodulares $\mathfrak{M}^{(\nu)}$ so, daß die erste

Zeile von $\dot{\mathfrak{M}}^{(\nu)}$ $\mathfrak{f}^{(\nu, 2n)}$ durch p teilbar ist. Ergänzt man $\mathfrak{M}^{(\nu)}$ folgendermaßen zu einer $2n$-reihigen Matrix:

$$\mathfrak{M}^{(2n)} = \begin{pmatrix} \mathfrak{M}^{(\nu)} & \\ & \mathfrak{E}^{(2n-\nu)} \end{pmatrix},$$

so ist $\mathfrak{F}' = \dot{\mathfrak{M}}^{(2n)}\, \mathfrak{F}\, \mathfrak{M}^{(2n)}$ eine Matrix, deren erste Zeile und Spalte durch p, und deren Glied mit dem Indexpaar 11 sogar durch p^2 teilbar ist. Dann wäre aber $\mathfrak{F}'$ und damit auch $\mathfrak{F}$ keine Stammform, im Widerspruch zur Voraussetzung. Mithin ist $\alpha_{2n} = \alpha$ und $\mu \geqq \nu$. Der ebenfalls ganze Transformator $\overline{\mathfrak{T}} = p^{\alpha}\, \mathfrak{T}^{-1}$ gehört rechts zu der Form, zu der $\mathfrak{T}$ links gehört, und links zu der Form, zu der $\mathfrak{T}$ rechts gehört; ferner vertauschen μ und ν bei $\overline{\mathfrak{T}}$ ihre Rollen. Sonst bleibt alles ungeändert. Man kann dann also ebenso schließen, daß auch nicht $\mu > \nu$ sein kann.

Jetzt teile man $\mathfrak{F}$ folgendermaßen in 9 Teilmatrizen auf:

$$(11) \qquad \mathfrak{F} = \begin{pmatrix} \mathfrak{M}_{11}^{(\nu)} & \mathfrak{m}_{12}^{(\nu, 2(n-\nu))} & \mathfrak{M}_{13}^{(\nu)} \\ \dot{\mathfrak{m}}_{12} & \mathfrak{M}_{22}^{(2(n-\nu))} & \mathfrak{m}_{23}^{(2(n-\nu),\ \nu)} \\ \dot{\mathfrak{M}}_{13} & \dot{\mathfrak{m}}_{23} & \mathfrak{M}_{33}^{(\nu)} \end{pmatrix}.$$

Wegen (10) ist hierbei

$$(12) \qquad \mathfrak{M}_{11}^{(\nu)} \equiv 0 \bmod p^2,\ \mathfrak{m}_{12}^{(\nu, 2(n-\nu))} \equiv 0 \bmod p,$$

und $\mathfrak{M}_{13}^{(\nu)}$ hat eine durch p nicht teilbare Determinante, wie aus den letzten Überlegungen hervorgeht.

Ich unterscheide nunmehr drei Fälle:

Ist erstens $\nu = n$, so ist wegen $p^{\alpha} > p$

$$\begin{pmatrix} \mathfrak{E}^{(n)} & \\ & p\, \mathfrak{E}^{(n)} \end{pmatrix}$$

ein echter Teiler von $\mathfrak{T}$, welcher $\mathfrak{F}$ in das p-fache einer Form gleicher Diskriminante transformiert und deshalb einen Transformator liefert.

Ist zweitens $\nu < n$, und sind $\alpha_{\nu+1}, \ldots, \alpha_{2n-\nu}$ nicht sämtlich 1, so ist

$$(13) \qquad \begin{pmatrix} \mathfrak{E}^{(\nu)} & & \\ & p\, \mathfrak{E}^{2(n-\nu)} & \\ & & p^2\, \mathfrak{E}^{(\nu)} \end{pmatrix}$$

ein echter Teiler von $\mathfrak{T}$, der $\mathfrak{F}$ in das p^2-fache einer Form gleicher Diskriminante transformiert und deshalb einen Transformator liefert.

Als dritte Möglichkeit bleibt wegen (9) und $\alpha_i \leqq \alpha$ (s. oben) noch übrig, daß $\mathfrak{T}$ die Gestalt (13) hat. Es ist jetzt $\alpha = 2$, und $\mathfrak{T}$ ist nach Nr. 5, falls (2) gilt, nicht weiter zerlegbar, wie behauptet wird. Es sei nun (2) nicht erfüllt. Dann darf man $\mathfrak{M}_{22}^{(2(n-\nu))}$ in (11) auf Hauptachsen transformiert denken, was wegen $p > 2$ mittels einer p-adisch ganzen Substitutionsmatrix möglich ist. Höchstens zwei der dabei auftretenden Diagonalelemente können durch p teilbar sein, denn sonst würde die Diskriminante von $\mathfrak{F}$ durch eine höhere als die zweite Potenz von p teilbar sein, was aber bei Stammformen unmöglich ist. Benutzt man die aus (11), (12) und $|\mathfrak{M}_{13}^{(\nu)}| \not\equiv 0 \bmod p$ folgende Tatsache, daß die Diskriminante von $\mathfrak{M}_{22}^{(2(n-\nu))} \bmod p$ das gleiche quadratische Restverhalten zeigt wie die Diskriminante D von $\mathfrak{F}$, so kann man $\mathfrak{M}_{22}^{(2(n-\nu))}$ weiter p-adisch ganz in eine der Gestalten (7) (mit $n-1$ statt n) nach dem Modul p bringen, und dann wird eine der Substitutionen $\mathfrak{T}^{(2(n-\nu))}$ der Gestalt (8) die Form $\mathfrak{M}_{22}^{(2(n-\nu))}$ und

$$\mathfrak{T}' = \begin{pmatrix} \mathfrak{E}^{(\nu)} & & \\ & \mathfrak{T}^{(2(n-\nu))} & \\ & & p\,\mathfrak{E}^{(\nu)} \end{pmatrix}$$

die Form $\mathfrak{F}$ in das p-fache einer Form gleicher Diskriminante transformieren. $\mathfrak{T}'$ ist ein echter Teiler von $\mathfrak{T}$. Hiermit ist der behauptete Satz endlich in vollem Umfange bewiesen.

8. Daß der Beweis auch im Falle $p = 2$ durchführbar bleibt, verdanke ich einem freundlichen Hinweise von Herrn Brandt. Wie er bewiesen hat,[1] kann man auch jetzt jede Stammform p-adisch ganz auf eine zu (7) entsprechende Gestalt bringen. Die dort auftretenden Restformen

$$\begin{pmatrix} a_1 & \\ & a_2 p \end{pmatrix}, \begin{pmatrix} a_1 & & \\ & a_2 & \\ & & a_3 p \end{pmatrix}, \begin{pmatrix} & a_4 p \\ a_4 p & \end{pmatrix}$$

sind jetzt nur durch allgemeinere binäre oder quaternäre 2-adische Stammformen zu ersetzen, welche Normenformen von quadrati-

[1] Vgl. Anm. 1 S. 3.

schen Zahlkörpern oder von Quaternionenalgebren sind. Man kennt nun deren Transformatoren der Norm 2 und kann mit deren Hilfe die zu (8) entsprechenden Transformatoren von $\mathfrak{F}$ der Norm 2 bilden.

Die Übertragung der Nr. 7 macht ebenfalls keine Schwierigkeiten, wenn man die Kongruenz (10) so versteht, daß die durch 2^α geteilte linke Seite eine symmetrische Matrix mit geraden Diagonalengliedern ist. Dies hat man auch in den aus (10) gezogenen Folgerungen zu beachten. Die zum Schluß notwendige Transformation von $\mathfrak{M}_{22}^{(2(n-\nu))}$ auf die Normalform (7) läßt sich wieder unter Berufung auf den Brandtschen Satz bewerkstelligen, wobei man vorher wie oben die Folgerung ziehen muß, daß $\mathfrak{M}_{22}^{(2(n-\nu))}$ einer Stammform mod 2 kongruent ist.

9. Aus dem Satz von Nr. 5 geht unmittelbar hervor:

Eine Primzahl, nach welcher D ein quadratischer Nichtrest ist, kann die Norm eines Transformators nur in gerader Vielfachheit teilen.

§ 4. Die normalen Transformatoren

10. In den Fällen $n = 1$ und $n = 2$ bei kompositionsfähigen Formen sind die entwickelten Sätze mit Sätzen aus der elementaren Idealtheorie der quadratischen Zahlkörper oder der Quaternionenalgebren äquivalent. Die Transformatoren liefern Substitutionen der Basis der (bzw. einer) maximalen Ordnung H in die Basis von Idealen Θ. Es ist nun zu beachten, daß im Falle von Quaternionenalgebren die so erhaltenen Ideale Θ nicht immer Links- oder Rechtsideale für H sind, sondern i. a. für eine andere maximale Ordnung. Diejenigen Transformatoren, die Ideale Θ mit H als Links- oder Rechtsordnung erzeugen, haben ein Elementarteilersystem der Form a, a, ab, ab. Deshalb betrachte ich auch bei allgemeiner Variablenzahl $2n$ solche Transformatoren besonders, deren Elementarteilersystem einen ähnlich einfachen Bau hat. Auf diese Weise wird erreicht, daß die Primzerlegung primärer Transformatoren im wesentlichen eindeutig wird, wie man es von der Primzerlegung primärer Quaternionenideale weiß; für allgemeine Transformatoren trifft dies

nicht zu. Indessen stellt sich jetzt ein neuer Übelstand ein, der sich bisher nicht bewältigen ließ: die Transformatoren, die diesen engeren Bedingungen genügen, bilden i. a. nicht mehr ein Gruppoid.

Ein ganzer Transformator soll primitiv heißen, wenn er nicht durch einen „ganzrationalen" Transformator $t\,\mathfrak{E}^{(2n)}$ teilbar ist, wobei t eine ganze rationale Zahl ist. Jeder ganze oder gebrochene Transformator $\mathfrak{T}$ läßt sich in der Form $\mathfrak{T} = t \cdot \mathfrak{T}^*$ schreiben, wobei t eine geeignete rationale Zahl, der rationale Teiler, und $\mathfrak{T}^*$ primitiv, der primitive Anteil, von $\mathfrak{T}$ ist.

Ein Transformator $\mathfrak{T}$ heiße normal, wenn sein primitiver Anteil $\mathfrak{T}^*$ modulo N ($\mathfrak{T}^*$) den Rang n hat; das Elementarteilersystem von $\mathfrak{T}^*$ besteht dann n-mal aus 1 und n-mal aus N ($\mathfrak{T}^*$).

Primtransformatoren von Primzahlnorm p sind nach Nr. 5 stets normal. Dagegen geht aus Nr. 5 und 7 hervor, daß Primtransformatoren von Primzahlquadratnorm p^2 nur dann normal sind, wenn sie gleich $p\,\mathfrak{E}^{(2n)}$ sind. Es gilt der wichtige Satz:

Es gibt im wesentlichen nur eine Primzerlegung eines primären primitiven Transformators. Genauer: ist $\mathfrak{T}_{ik}$ ein solcher Transformator und

$$\mathfrak{T}_{ik} = \mathfrak{T}_{ij_1}\,\mathfrak{T}_{j_1 j_2} \dots \mathfrak{T}_{j_\alpha k}$$

eine Primzerlegung, so entstehen alle übrigen Primzerlegungen aus dieser durch Einschieben von Einheitenprodukten $\mathfrak{T}_{j_\nu j_\nu}\,\mathfrak{T}_{j_\nu j_\nu}^{-1}$. Der Beweis ergibt sich unmittelbar, wenn man $\mathfrak{T}_{ik}$ mit zwei unimodularen Matrizen $\mathfrak{U}$ und $\mathfrak{V}$ in der Form

$$\mathfrak{T}_{ik} = \mathfrak{U}\begin{pmatrix}\mathfrak{E}^{(n)} & \\ & p^\alpha\,\mathfrak{E}^{(n)}\end{pmatrix}\mathfrak{V} = \mathfrak{U}\begin{pmatrix}\mathfrak{E}^{(n)} & \\ & p\,\mathfrak{E}^{(n)}\end{pmatrix}\dots\begin{pmatrix}\mathfrak{E}^{(n)} & \\ & p\,\mathfrak{E}^{(n)}\end{pmatrix}\mathfrak{V}$$

schreibt. Der linke Faktor $\mathfrak{T}_{ij_1}$ von $\mathfrak{T}_{ik}$ ergibt sich bis auf einen unimodularen Rechtsfaktor eindeutig aus der Matrizenidealgleichung

$$\mathfrak{T}_{ij_1}\,\mathfrak{I}^{(2n)} = \mathfrak{T}_{ik}\,\mathfrak{I}^{(2n)} + p\,\mathfrak{I}^{(2n)}.$$

Im Gegensatz hierzu sind nicht primitive Transformatoren stets mehrdeutig zerlegbar, ausgenommen, wenn ihr rationaler Teiler nur rationale Zerlegungen zuläßt.

Jedem Transformator $\mathfrak{T}_{ik}$ kann man einen konjungierten Transformator

$$\overline{\mathfrak{T}}_{ik} = N(\mathfrak{T}_{ik})\,\mathfrak{T}_{ik}^{-1}$$

zuordnen. Er ist normal, ganz, und primitiv, je nachdem $\mathfrak{T}_{ik}$ es ist. $\overline{\mathfrak{T}}_{ik}$ gehört links zu der Form, zu der $\mathfrak{T}_{ik}$ rechts gehört, und rechts zu der Form, zu der $\mathfrak{T}_{ik}$ links gehört. Es gilt schließlich $\overline{\overline{\mathfrak{T}}}_{ik} = \mathfrak{T}_{ik}$. Den Transformator $p\,\mathfrak{E}^{(2n)}$, wo p eine Primzahl ist, nach der D kein quadratischer Nichtrest ist, kann man stets auf verschiedene Arten in ein Produkt $\mathfrak{T}_{ik}\,\overline{\mathfrak{T}}_{ik}$ zerlegen.

11. Die Zusammenfassung von normalen Transformatoren zu Gruppoiden bereitet Schwierigkeiten, wie man sich an Hand des nachstehenden Beispiels überzeugen möge. Alle hier betrachteten Transformatoren gehören links und rechts zu

$$\mathfrak{F} = \begin{pmatrix} \mathfrak{N}^{(3)} & \mathfrak{E}^{(3)} \\ \mathfrak{E}^{(3)} & \mathfrak{N}^{(3)} \end{pmatrix}.$$

Von den drei normalen Transformatoren

$$\mathfrak{T}^1 = \begin{pmatrix} \mathfrak{E}_1^{(3)} & p\,\mathfrak{E}^{(3)} \\ \mathfrak{E}^{(3)} & \mathfrak{N}^{(3)} \end{pmatrix}, \mathfrak{T}^2 = \begin{pmatrix} p\,\mathfrak{E}^{(3)} & \mathfrak{N}^{(3)} \\ \mathfrak{N}^{(3)} & \mathfrak{E}^{(3)} \end{pmatrix}, \mathfrak{T}^3 = \begin{pmatrix} \mathfrak{E}_3^{(3)} & p\,\mathfrak{E}^{(3)} \\ \mathfrak{E}^{(3)} & \mathfrak{N}^{(3)} \end{pmatrix},$$

wobei

$$\mathfrak{E}_1^{(3)} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \mathfrak{E}_3^{(3)} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$

bedeute, ergeben die Produkte $\mathfrak{T}^1\mathfrak{T}^2$, $\mathfrak{T}^2\mathfrak{T}^3$, $\mathfrak{T}^2\mathfrak{T}^2$ wieder normale Transformatoren, dagegen nicht die Produkte $\mathfrak{T}^1\mathfrak{T}^1$, $\mathfrak{T}^1\mathfrak{T}^3$.

§ 5. Die Anzahlmatrizen

12. Der weitere Ausbau der Theorie ist, ebenso wie die Zahlentheorie der Algebren, erst dann möglich, wenn die Einheiten hinreichend weit untersucht sind. Es herrschen nun besonders übersichtliche Verhältnisse, wenn es überhaupt nur endlich viele Einheiten gibt. Dieser Fall liegt hier bei definiten Formen vor. Von jetzt ab werden nur noch definite Formen den Betrachtungen zugrunde liegen.

Die indefiniten Formen beanspruchen übrigens von dem hier verfolgten Gesichtspunkt aus gar nicht das gleiche Interesse, da

für $n > 1$ die Klassenzahl h gleich der Geschlechterzahl, bei Stammformen also gleich 1 ist.

Die Anzahl $\mu_{ik}(t)$ der Transformatoren der Norm t, die links zu $\mathfrak{F}_k$ und rechts zu $\mathfrak{F}_i$ gehören, ist bei definiten Formensystemen endlich. Es gilt auf Grund der umkehrbar eindeutigen Beziehung zwischen konjugierten Transformatoren

$$\mu_{ik}(t) = \mu_{ki}(t). \tag{14}$$

Der Hauptgegenstand dieser Arbeit sind die Anzahlmatrizen

$$\mathfrak{M}(t) = (\mu_{ik}(t))$$

und die reduzierten Anzahlmatrizen

$$\mathfrak{R}(t) = \mathfrak{M}(t)\,\mathfrak{M}(1)^{-1},$$

Sind t und t' teilerfremde Zahlen, so gilt

$$\mathfrak{R}(t)\cdot\mathfrak{R}(t') = \mathfrak{R}(t\cdot t') = \mathfrak{R}(t')\cdot\mathfrak{R}(t). \tag{15}$$

Zum Beweise bemerke ich zuerst, daß $\mathfrak{M}(1)$ eine Diagonalmatrix ist, deren j-tes Diagonalenglied die Anzahl der Einheiten von $\mathfrak{F}_j$ angibt. Nun betrachte ich für ein festes Indexpaar ik sämtliche Transformatoren $\mathfrak{T}_{ik}$ der Norm $t\cdot t'$ und ihre Zerlegungen

$$\mathfrak{T}_{ik} = \mathfrak{T}_{ij}\,\mathfrak{T}_{jk} \tag{16}$$

in einen vorderen Faktor der Norm t und einen hinteren Faktor der Norm t'. Wie aus § 2 hervorgeht, liegt die Zerlegung (16) bis auf eingeschobene Einheitenfaktoren $\mathfrak{T}_{jj}\mathfrak{T}_{jj}^{-1}$ eindeutig fest. Es ist mithin

$$\mu_{ik}(t\cdot t') = \sum_{j=1}^{h} \frac{\mu_{ij}(t)\cdot\mu_{jk}(t')}{\mu_{jj}(1)},$$

was nach Division mit $\mu_{kk}(1)$ unmittelbar die behauptete Gleichung (15) liefert.

13. Die ganzen Zahlen

$$\rho_{ik}(t) = \frac{\mu_{ik}(t)}{\mu_{kk}(t)}$$

geben die Anzahlen der Transformatorenklassen der Norm t wieder, die rechts zu der Form $\mathfrak{F}_i$ und links zu beliebigen mit $\mathfrak{F}_k$ äquivalenten Formen gehören. Die Zahlen

$$\rho(t) = \sum_{k=1}^{h} \rho_{ik}(t) \tag{17}$$

sind die Anzahlen der Transformatorenklassen der Norm t überhaupt, die rechts zu $\mathfrak{F}_i$ gehören. Sie sind ersichtlich Invarianten der Klasse von $\mathfrak{F}_i$ nach dem Modul t. Da aber infolge der Stammformeneigenschaft alle $\mathfrak{F}_i$ bei $n > 1$ ganzzahlig p-adisch äquivalent sind, sind die Zahlen (17) sogar Invarianten des Formensystems und insbesondere auch von der Klasse von $\mathfrak{F}_i$ unabhängig. Für $n = 1$ versagt diese Schlußweise zwar, doch kann man auch jetzt die Invarianz von (17) leicht nachweisen. Durch Bildung der Zeilensummen in der Matrizengleichung (15) erhält man für teilerfremde t und t'

$$\rho(t) \cdot \rho(t') = \rho(t \cdot t') = \rho(t') \cdot \rho(t). \tag{18}$$

14. In § 6 wird der folgende Hilfssatz gebraucht:

Jeder kommutative durch Matrizen $\mathfrak{R}(t)$ erzeugte Ring ist halbeinfach, sämtliche in ihm enthaltenen Matrizen lassen sich simultan auf Diagonalform transformieren.

Bezeichnet $\mathfrak{D}$ eine Diagonalmatrix, die der Gleichung

$$\mathfrak{D}^2 = \mathfrak{M}(1)$$

genügt, so ist

$$\mathfrak{D}^{-1}\,\mathfrak{R}(t)\,\mathfrak{D} = \mathfrak{D}^{-1}\,\mathfrak{M}(t)\,\mathfrak{D}^{-1}.$$

Diese Matrizen sind nach (14) symmetrisch und lassen sich daher orthogonal auf Diagonalform transformieren, und zwar zwei oder mehr vertauschbare Matrizen gleichzeitig, und damit gleich der ganze durch sie erzeugte Ring. Infolgedessen kann dieser Ring keine nilpotenten Elemente enthalten.

Alle Schlußweisen und Ergebnisse dieses Paragraphen bleiben unverändert gültig, wenn man die betreffenden Anzahlen nur auf normale Transformatoren und sogar auf primitive bezieht. Von jetzt ab werde ich die nicht normalen Transformatoren von den Betrachtungen ausschließen. Um keine neuen Bezeichnungen einführen zu müssen, setze ich fest, daß sämtliche hier eingeführten Anzahlen sich ausschließlich auf normale Transformatoren beziehen sollen.

§ 6. Die Transformatoren und die Darstellung von Zahlen

15. Im Folgenden entwickele ich einen Zusammenhang zwischen den Anzahlen von Darstellungen von Zahlen durch die Formen des zugrunde liegenden Systems und den Anzahlen von Transformatoren gegebener Norm. Neben der bereits erwähnten Beschränkung auf normale Transformatoren will ich hier außerdem nur solche Zahlen t betrachten, deren sämtliche Primteiler p der Gleichung

$$\left(\frac{D}{p}\right) = 1$$

genügen. Derselben Einschränkung sollen schließlich die Normen der betrachteten Transformatoren unterworfen sein. Diese Einschränkungen sind wahrscheinlich bei dem Beweis der behaupteten Sätze zum großen Teil entbehrlich, sie sind es sicher, wenn man die Sätze entsprechend abändert. Indessen erlauben sie Vereinfachungen in der Schlußweise.

Es bezeichne $\delta_i(t)$ die Anzahl der ganzzahligen Darstellungen der Zahl t durch die Form $\mathfrak{F}_i$, d. h. die Anzahl der verschiedenen ganzzahligen einspaltigen Matrizen $\mathfrak{t}_i$, die der Gleichung

$$\dot{\mathfrak{t}}_i \, \mathfrak{F}_i \, \mathfrak{t}_i = 2t$$

genügen. Die Anzahl der primitiven Darstellungen von t sei $\delta_i^*(t)$. Jede Darstellung $\mathfrak{t}_i$ läßt sich mit einer primitiven $\mathfrak{t}_i^*$ eindeutig in der Form $\mathfrak{t}_i = t_i \cdot \mathfrak{t}_i^*$ schreiben, wobei t_i der rationale Teiler der Darstellung heißen möge. Die $\delta_i(t)$ und $\delta_i^*(t)$ fasse ich zu Spaltenvektoren, den Darstellungsanzahlvektoren $\mathfrak{d}(t)$ und $\mathfrak{d}^*(t)$ zusammen.

Eine Darstellung $\mathfrak{t}_i$ (einer Zahl $t \cdot t'$) soll durch einen Transformator $\mathfrak{T}_{ik}$ (der Norm t) teilbar heißen, wenn es einen Vektor $\mathfrak{s}$ so gibt, daß

$$\mathfrak{t}_i = \mathfrak{T}_{ik} \, \mathfrak{s}$$

ist. Dabei ist stets $N(\mathfrak{T}_{ik})$ ein Teiler der durch $\mathfrak{t}_i$ dargestellten Zahl. Die Gesetze der Teilbarkeit von Darstellungen durch Transformatoren gründen sich auf folgenden

Hilfssatz: Jede primitive Darstellung der Zahl $t \cdot t'$ ist durch mindestens einen primitiven normalen Transformator der Norm t

teilbar. Die Anzahl der normalen primitiven Transformatorenklassen der Norm t, welche eine solche Darstellung teilen, ist eine Invariante $\nu_1(t)$ des Formensystems nach dem Modul t.

Wird der Hilfssatz als richtig angenommen, so ergibt sich aus § 2 sofort der folgende Zusatz:

$$\nu_1(t) = \nu_1(t_1)\,\nu_1(t_2) \quad \text{für } t = t_1 t_2 \text{ und } (t_1, t_2) = 1. \qquad (19)$$

Dieser Hilfssatz ist als Spezialfall in einem allgemeineren von § 7 enthalten, so daß sich ein Beweis an dieser Stelle erübrigt. Aus ihm sollen nun zwei Folgerungen gezogen werden.

16. Zuerst seien die Zahlen t und t' teilerfremd. Ich denke mir die normalen primitiven Transformatorenklassen der Norm t nach den Indizes der Formenklassen geordnet, zu denen sie rechts und links gehören, und durch je einen Vertreter $\mathfrak{T}^1_{ik}, \mathfrak{T}^2_{ik}, \ldots$ dargestellt. Es seien ferner $\mathfrak{t}^1_k, \mathfrak{t}^2_k, \ldots$ alle primitiven Darstellungen der Zahl t' durch die Form $\mathfrak{F}_k$. Dann sind die Vektoren $\mathfrak{T}^\alpha_{ik}\,\mathfrak{t}^\beta_k$ Darstellungen der Zahl $t \cdot t'$ durch die Form $\mathfrak{F}_i$, und zwar sind es primitive Darstellungen, da die $\mathfrak{t}_k$ und $\mathfrak{T}_{ik}$ primitiv sind und $(t, t') = 1$ ist. Ein rationaler Primteiler p von $\mathfrak{T}_{ik}\,\mathfrak{t}_k$ müßte nämlich in t aufgehen. Da man ohne Beschränkung der Allgemeinheit

$$\mathfrak{T}_{ik} = \begin{pmatrix} \mathfrak{E}^{(n)} & \\ & t\,\mathfrak{E}^{(n)} \end{pmatrix}$$

annehmen darf, müßte p in den n ersten Komponenten von $\mathfrak{t}_k$ aufgehen. Dann wäre aber $\mathfrak{t}_k$ durch den Primtransformator

$$\mathfrak{T}_{kl} = \begin{pmatrix} p\,\mathfrak{E}^{(n)} & \\ & \mathfrak{E}^{(n)} \end{pmatrix}$$

teilbar, der zu dem (eindeutig bestimmten) Rechtsprimteiler von $\mathfrak{T}_{ik}$ konjugiert ist, und demnach wäre t' durch p teilbar, im Widerspruch zu $(t, t') = 1$.

Nach dem Hilfssatz erhält man auf diese Weise alle primitiven Darstellungen von $t \cdot t'$, und zwar jede genau $\nu_1(t)$ mal. Es ist daher

$$\nu_1(t)\,\mathfrak{d}^*(t \cdot t') = \mathfrak{R}^*(t)\,\mathfrak{d}^*(t'),$$

wenn der Stern an $\mathfrak{R}^*(t)$ bedeutet, daß es sich um die reduzierte Anzahlmatrix für primitive Transformatoren handelt. Zählt man

nun auch noch die imprimitiven Darstellungen von t' und die imprimitiven Transformatoren der Norm t nach ihrem rationalen Teiler geordnet auf, so erhält man die Formel

$$\mathfrak{d}(t \cdot t') = \mathfrak{S}(t)\,\mathfrak{d}(t') \tag{20}$$

mit

$$\mathfrak{S}(t) = \sum_{s^2 \mid t} \frac{1}{\nu_1\left(\frac{t}{s^2}\right)} \mathfrak{R}^*\left(\frac{t}{s^2}\right).$$

Es gilt aber auch

$$\mathfrak{d}(t \cdot t') = \mathfrak{S}(t')\,\mathfrak{d}(t) \tag{21}$$

und

$$\mathfrak{d}(t \cdot t') = \mathfrak{S}(t \cdot t')\,\mathfrak{d}(1). \tag{22}$$

Ferner erfüllen die $\mathfrak{S}(t)$ auf Grund ihrer Definition und wegen (19) bei teilerfremden t und t' die zu (15) analoge Gleichung

$$\mathfrak{S}(t) \cdot \mathfrak{S}(t') = \mathfrak{S}(t \cdot t') = \mathfrak{S}(t') \cdot \mathfrak{S}(t). \tag{23}$$

17. Mit der Abkürzung

$$\mathfrak{S}(t) = (\sigma_{ik}(t))$$

ergibt der Vergleich von (20) und (21)

$$\sum_{k=1}^{h} \sigma_{ik}(t)\,\delta_k(t') = \sum_{k=1}^{h} \sigma_{ik}(t')\,\delta_k(t) \tag{24}$$

Diese Gleichungen fasse man nach einem Gedanken von Herrn Hecke bei festgehaltenen Werten für i und t und bei beliebig teilerfremd zu t variierendem t' als unendlich viele Bestimmungsgleichungen für die h Unbekannten $\sigma_{i1}(t), \ldots, \sigma_{ih}(t)$ auf. Ist ihre Auflösung eindeutig möglich, so ergeben sich die $\sigma_{ik}(t)$ als lineare Ausdrücke in den $\delta_i(t)$, man kann sie dann in der Form

$$\mathfrak{S}(t) = \mathfrak{S}_1\,\delta_1(t) + \ldots + \mathfrak{S}_h\,\delta_h(t)$$

mit h von t nicht mehr abhängigen Matrizen $\mathfrak{S}_i$ schreiben. Im allgemeinen darf aber eine eindeutige Auflösbarkeit nicht er-

wartet werden. Zwischen den Darstellungsanzahlen $\delta_i(t')$ wird es nämlich gewisse lineare Abhängigkeiten mit von t' unabhängigen Koeffizienten geben. Ich denke mir nun die Formen $\mathfrak{F}_i$ derart numeriert, daß $\mathfrak{F}_1, \ldots, \mathfrak{F}_{h'}$ ein maximales Teilsystem von der Art darstellt, daß zwischen den Anzahlen $\delta_1(t'), \ldots, \delta_{h'}(t')$ keine lineare Abhängigkeit mit von t' unabhängigen Koeffizienten mehr besteht, und daß sämtliche $\delta_i(t')$ durch diese als Linearformen mit konstanten Koeffizienten darstellbar sind.

Man kann jetzt zunächst die Matrix $\mathfrak{S}(t)$ als Lösung von (24) in der Form

$$\mathfrak{S}(t) = \mathfrak{S}_0(t) + \mathfrak{S}_1 \delta_1(t) + \ldots + \mathfrak{S}_{h'} \delta_{h'}(t) \tag{25}$$

ansetzen, wobei die $\mathfrak{S}_i$ wiederum konstante Matrizen sind und $\mathfrak{S}_0(t)$ den Gleichungen

$$\mathfrak{S}_0(t)\,\mathfrak{d}(t') = 0 \tag{26}$$

für alle zu t teilerfremden t' genügen, d. h. dem zu (24) gehörigen homogenen Gleichungssystem. Die $\mathfrak{S}_i$ sind nun noch nicht eindeutig bestimmt; sie werden es aber, wenn man folgendem Gedankengang folgt: Man lasse t und t' je ein System Σ und Σ' von Zahlen durchlaufen, wobei jedes t aus Σ zu jedem t' aus Σ' teilerfremd ist. Das System Σ soll über dies noch die Eigenschaft haben, daß die $\mathfrak{S}(t)$ für alle t aus Σ einen kommutativen Ring P_Σ erzeugen; diese Forderung ist z. B. dann erfüllt, wenn alle t untereinander teilerfremd sind. Nun liegt $\mathfrak{S}_0(t)$ stets in einer linearen Schar von Matrizen, die durch (26) definiert ist. Mit einer Basis $\mathfrak{S}_{01}, \ldots, \mathfrak{S}_{0g}$ dieser Schar schreibt sich $\mathfrak{S}_0(t)$ folgendermaßen:

$$\mathfrak{S}_0(t) = \mathfrak{S}_{01}\alpha_1(t) + \ldots + \mathfrak{S}_{0g}\alpha_g(t),$$

wobei man voraussetzen darf, daß zwischen den von t abhängigen Zahlen $\alpha_i(t)$ keine lineare Beziehung mit von t unabhängigen Konstanten besteht. Setzt man dies in (25) ein und eliminiert schließlich noch diejenigen eventuell existierenden linearen Verbindungen der $\alpha_i(t)$, die sich durch die $\delta_i(t)$ mit konstanten Koeffizienten darstellen lassen, so darf man sogar die $\alpha_i(t)$ und $\delta_i(t)$ als linear unabhängig ansehen.

Nun erzeugen auch schon die $\mathfrak{S}_{0i}$ und $\mathfrak{S}_k$ den Ring P_ν. Die $\mathfrak{S}_{0i}$ erzeugen zufolge (26) in ihm ein Ideal. Da P_ν aber nach Nr. 13 halbeinfach ist, ist dieses Ideal ein direkter Summand. Der komplementäre direkte Summand werde mit Z_ν bezeichnet, die Komponenten von $\mathfrak{S}(t)$ und $\mathfrak{S}_i$ in Z_ν mit $\mathfrak{Z}(t)$ und $\mathfrak{Z}_i$.

Die gewonnenen Ergebnisse lassen sich folgendermaßen zusammenfassen:

Die Matrizen $\mathfrak{S}(t)$ und damit die $\mathfrak{N}(t)$ erzeugen einen halbeinfachen Ring P; die in Nr. 12 definierten Zahlen $\rho(t)$ liefern eine Darstellung ersten Grades von P.

Durchläuft t ein System Σ von Zahlen von der Art, daß es mindestens ein zu allen t teilerfremdes t' gibt, und daß die $\mathfrak{S}(t)$ einen kommutativen Unterring P_ν von P erzeugen, so enthält P_ν einen direkten Summanden Z_ν, der durch Matrizen

$$\mathfrak{Z}(t) = \mathfrak{Z}_1 \delta_1(t) + \ldots + \mathfrak{Z}_{h'} \delta_{h'}(t)$$

erzeugt wird; dabei hängen die $\mathfrak{Z}_k$ von t nicht ab. Diese Matrizen erfüllen bei teilerfremden t und t_1 aus Σ die Gleichung

$$\mathfrak{Z}(t) \cdot \mathfrak{Z}(t_1) = \mathfrak{Z}(t \cdot t_1) = \mathfrak{Z}(t_1) \cdot \mathfrak{Z}(t). \tag{27}$$

Die Formel (27) ist besonders deshalb bemerkenswert, weil sie die Berechnung der $\delta_i(t \cdot t_1)$ aus den $\delta_i(t)$ und den $\delta_i(t_1)$ ermöglicht. Auf die Bedeutung einer solchen Formel für die analytische Zahlentheorie hat Herr Hecke hingewiesen. Es besteht wohl kein Zweifel, daß die hier bewiesenen Formeln mit den von ihm auf analytischem Wege gefundenen in engstem Zusammenhang stehen und vielleicht sogar identisch sind.

18. Die zweite Folgerung, die aus dem Hilfssatz gezogen werden soll, knüpft an die Frage nach der Verallgemeinerbarkeit von (20) für nicht teilerfremde t und t' an. Es sei t gleich einer Primzahl p und $t' = p^\alpha$. Nach dem Hilfssatz bekommt man alle primitiven Darstellungen $\mathfrak{t}_i$ von $p^{\alpha+1}$ mittels der primitiven Darstellungen $\mathfrak{t}_k$ von p^α und den (von selbst primitiven) Transformatoren $\mathfrak{T}_{ik}$ der Norm p in der Form $\mathfrak{T}_{ik}\,\mathfrak{t}_k$, wenn k von 1 bis h

läuft; jedes primitive $\mathfrak{t}_i$ bekommt man so $\nu_1(p)$ mal. Jetzt sind aber nicht alle so gewonnenen $\mathfrak{t}_i$ primitiv, wie im Falle $(t, t') = 1$.

Die Frage nach der möglichen Anzahl der Fälle, in denen $\mathfrak{T}_{ik}\,\mathfrak{t}_k$ nicht primitiv ist, darf man wie üblich nach geeigneter unimodularer Transformation von $\mathfrak{F}_i$ und $\mathfrak{F}_n$ angreifen. Dann beschränkt es nicht die Allgemeinheit,

$$\mathfrak{T}_{ik} = \begin{pmatrix} \mathfrak{E}^{(n)} & \\ & p\,\mathfrak{E}^{(n)} \end{pmatrix}$$

anzunehmen. Ist jetzt $\mathfrak{T}_{ik}\,\mathfrak{t}_k$ imprimitiv, ohne daß $\mathfrak{t}_k$ es ist, so muß

$$\mathfrak{t}_k = \mathfrak{T}_{ik}\,\mathfrak{t}_i'$$

sein (vgl. die Schlußweise von Nr. 16), wobei $\mathfrak{t}_i'$ eine primitive Darstellung von $p^{\alpha-1}$ durch $\mathfrak{F}_i$ ist.

Die Abzählung dieser möglichen Fälle liefert die Formel

$$\sum_{k=1}^{h}{}' \varrho_{ik}(p)\,\delta_k^*(p^\alpha) = \nu_1(p)\,\delta_i^*(p^{\alpha+1})$$
$$+ \sum_{k=1}^{h}{}' \varrho_{ik}(p)\,(\delta_i^*(p^{\alpha-1}) - \delta_k^*(p^{\alpha-2}) + \delta_i^*(p^{\alpha-3}) - + \ldots),$$

welche sich folgendermaßen schreiben läßt:

$$\mathfrak{S}(p)\,(\mathfrak{d}^*(p^\alpha) + \mathfrak{d}^*(p^{\alpha-2}) + \ldots) = \mathfrak{d}^*(p^{\alpha+1})$$
$$+ \frac{\varrho(p)}{\nu_1(p)}\,(\mathfrak{d}^*(p^{\alpha-1}) + \mathfrak{d}^*(p^{\alpha-3}) + \ldots)$$

oder

$$(28)\qquad \mathfrak{S}(p)\,\mathfrak{d}(p^\alpha) = \mathfrak{d}(p^{\alpha+1}) + \left(\frac{\varrho(p)}{\nu_1(p)} - 1\right)\mathfrak{d}(p^{\alpha-1}).$$

Man könnte hiernach das Bestehen der Gleichung dieser Art

$$\mathfrak{Z}(p)\,\mathfrak{Z}(p^\alpha) = \mathfrak{Z}(p^{\alpha+1}) + \left(\frac{\varrho(p)}{\nu_1(p)} - 1\right)\mathfrak{Z}(p^{\alpha-1})$$

vermuten; dies trifft indessen im allgemeinen nicht zu, wie Herr Hecke gezeigt hat.

§ 7. Die Transformatoren und die Darstellung von Formen von kleinerer Variablenzahl

19. Die Betrachtungen des vorausgegangenen Paragraphen sind einer direkten Verallgemeinerung fähig; dabei ergeben sich keine neuen Gedanken, so daß ich mich kurz fassen kann. An Stelle nach den Darstellungen einer Zahl t durch die Formen $\mathfrak{F}_i$ frage man nach den Darstellungen von $t \cdot \mathfrak{G}$, wobei $\mathfrak{G}$ eine Form von $m \leqq n$ Variablen ist, d. h. nach den ganzzahligen Matrizen $\mathfrak{t}_i = \mathfrak{t}_i^{(2n,m)}$, welche die Gleichung

$$\mathfrak{t}_i \, \mathfrak{F}_i \, \mathfrak{t}_i = t \cdot \mathfrak{G}$$

befriedigen. Die Matrix $\mathfrak{t}_i$ heißt eine Darstellung von $\mathfrak{G}$ von der Norm t; $\mathfrak{t}_i$ soll primitiv genannt werden, wenn die Koeffizienten von $\mathfrak{t}_i$ keinen von 1 verschiedenen Teiler besitzen. Wie oben kann man die Begriffe „rationaler Teiler" und „primitiver Anteil" definieren. Eine Darstellung heiße normal, wenn der Rang des primitiven Anteils $\mathfrak{t}_i^*$ von $\mathfrak{t}_i$ nach dem Modul der Norm von $\mathfrak{t}_i^*$ gleich m ist. Schließlich kann man die Teilbarkeit erklären: $\mathfrak{t}_i$ heiße durch einen Transformator $\mathfrak{T}_{ik}$ teilbar, wenn es eine Matrix $\mathfrak{s}$ so gibt, daß

$$\mathfrak{t}_i = \mathfrak{T}_{ik} \, \mathfrak{s}$$

ist.

Die Anzahl der normalen Darstellungen von $\mathfrak{G}$ der Norm t durch $\mathfrak{F}_i$ sei $\gamma_i(t)$. Ist e die Anzahl der Einheiten von $\mathfrak{G}$, so ist $\gamma_i(t) \frac{1}{e}$ die Anzahl der Klassen von rechtsassoziierten Darstellungen einer zu $\mathfrak{G}$ äquivalenten Form. Der Gegenstand der folgenden Untersuchungen sind die Darstellungsanzahlvektoren $\mathfrak{g}(t)$, die aus den Komponenten $\gamma_i(t) \frac{1}{e}$ gebildet werden. Als Grundlage hierzu dient der

Hilfssatz: Jede primitive normale Darstellung der Norm $t \cdot t'$ von $\mathfrak{G}$ ist durch mindestens einen primitiven normalen Transformator der Norm t teilbar. Die Anzahl der sie teilenden verschiedenen primitiven normalen Transformatorenklassen der

Norm t ist eine Invariante $\nu_{\mathfrak{G}}(t)$ des Formensystems nach dem Modul t.

Es genügt offenbar, den Beweis für den p-adischen Zahlkörper als Grundkörper zu führen. Unter der Annahme, daß D mod p ein quadratischer Rest ist, kann $\mathfrak{F}_i$ auf die Gestalt

$$\mathfrak{F}_i = \begin{pmatrix} \mathfrak{N}^{(n)} & \mathfrak{E}^{(n)} \\ \mathfrak{E}^{(n)} & \mathfrak{N}^{(n)} \end{pmatrix} \tag{29}$$

gebracht werden. Auf $\mathfrak{F}_i$ kann man nun beliebige Einheitstransformatoren $\mathfrak{T}_{ii}$ ausüben und auf $\mathfrak{G}$ sogar beliebige unimodulare Substitutionen $\mathfrak{U}^{(m)}$, wobei $\mathfrak{t}_i$ in

$$\mathfrak{T}_{ii}\, \mathfrak{t}_i\, \mathfrak{U}^{(m)}$$

übergeht, ohne daß sich dadurch die Anzahl der primitiven normalen Transformatorenklassen ändert, die $\mathfrak{t}_i$ teilen. Durch Benutzung von folgenden Typen von Einheitstransformatoren: 1. Vertauschung der ν-ten und der $(n+\nu)$-ten Variablen ($\nu = 1, 2, \ldots, n$), 2.

$$\mathfrak{T}_{ii} = \begin{pmatrix} \mathfrak{B} & \\ & \dot{\mathfrak{B}}^{-1} \end{pmatrix},$$

wobei $\mathfrak{B}$ eine unimodulare n-reihige Matrix ist, und von geeigneten $\mathfrak{U}^{(m)}$ kann man zunächst $\mathfrak{t}_i$ nach dem Modul t in die Form

$$\begin{pmatrix} \mathfrak{E}^{(m)} \\ \mathfrak{N}^{(n-m,\, m)} \\ \mathfrak{w}^{(n,\, m)} \end{pmatrix}$$

bringen. Infolge (29) ist

$$\mathfrak{w}^{(n,\, m)} = \begin{pmatrix} \mathfrak{S}^{(m)} \\ \mathfrak{x}^{(n-m,\, m)} \end{pmatrix},$$

wobei $\mathfrak{S}^{(m)}$ mod t schiefsymmetrisch ist. Jetzt kann man durch Anwendung von Einheitstransformatoren der Gestalt

$$\mathfrak{T}_{ii} = \begin{pmatrix} \mathfrak{E}^{(n)} & \mathfrak{N}^{(n)} \\ \mathfrak{S}_1^{(n)} & \mathfrak{E}^{(n)} \end{pmatrix}$$

mit schiefsymmetrischem $\mathfrak{S}_1^{(n)}$ schließlich $\mathfrak{t}_i$ in die Endform

$$\mathfrak{t}_i = \begin{pmatrix} \mathfrak{E}^{(m)} \\ \mathfrak{N}^{(2n-m,\, m)} \end{pmatrix} \bmod t$$

bringen. Aus dieser Darstellung folgen die Behauptungen: $\mathfrak{t}_i$ ist durch

$$\mathfrak{T}_{ik} = \begin{pmatrix} \mathfrak{E}^{(n)} & \\ & t\mathfrak{E}^{(n)} \end{pmatrix}$$

teilbar, und die Anzahl der $\mathfrak{t}_i$ teilenden primitiven normalen Transformatorenklassen der Norm t ist deshalb eine Invariante des Formensystems mod t, weil sämtliche primitiven normalen Darstellungen $\mathfrak{t}_i$ nach dem Modul t äquivalent sind.

20. Jetzt kann man alle Schlüsse der Nrn. 16 und 17 fast unverändert durchführen. Ich notiere nur das Endergebnis: Entsprechend $\mathfrak{S}(t)$ und $\mathfrak{Z}(t)$ gibt es Matrizen $\mathfrak{S}_{\mathfrak{G}}(t)$ und $\mathfrak{Z}_{\mathfrak{G}}(t)$, die mit $\mathfrak{g}(t)$ an Stelle von $\mathfrak{d}(t)$ die Gleichungen (20)–(27) erfüllen. Die Schlußweise von Nr. 18 ist dagegen nicht übertragbar, da aus einem normalen Transformator $\mathfrak{T}_{ik}$ und einer normalen Darstellung $\mathfrak{t}_k$ unter Umständen eine nicht normale Darstellung $\mathfrak{T}_{ik}\,\mathfrak{t}_k$ entstehen kann. Interessant wäre es, zu wissen, in welcher Beziehung die $\mathfrak{S}_{\mathfrak{G}}(t)$ und $\mathfrak{Z}_{\mathfrak{G}}(t)$ mit verschiedenen $\mathfrak{G}$ stehen. Abschließend bemerke ich, daß die gemachte Annahme $m \leqq n$ entbehrlich ist; nur muß man für größeres m den Begriff der normalen Darstellung etwas abändern. Für $m = 2n$ sind übrigens die Darstellungen mit den Transformatoren identisch.