Grundzüge einer Zahlentheorie der quadratischen Formen im rationalen Zahlenkörper. II.

Autor(en): **Eichler, Martin**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **21 (1948)**

PDF erstellt am: **11.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-18593

Grundzüge einer Zahlentheorie der quadratischen Formen im rationalen Zahlkörper II.

Von MARTIN EICHLER, Göttingen

III. Die Darstellung von Zahlen durch Systeme definiter Formen

§ 10. Die Beziehungen zwischen Idealen und Vektoren

1. In den beiden folgenden Paragraphen werden die Formen des vorliegenden Systems grundsätzlich als definit angenommen. Sie besitzen dann endlich viele Einheiten, die Anzahl der Einheiten von $\mathfrak{F}_i$ sei e_i. Es gibt ferner endlich viele ganze primitive halbnormale Transformatoren $\mathfrak{T}_{ik}$ gegebener Norm t, welche links zu $\mathfrak{F}_i$ und rechts zu $\mathfrak{F}_k$ gehören. Ihre Anzahl werde mit $\pi_{ik}(t)$ bezeichnet. Hierbei werde verabredet, daß in dieser Anzahl nur dann halbnormale Transformatoren mitgezählt werden sollen, wenn es keine normalen dieser Norm gibt, und zwar genauer: für jede in t aufgehende Primzahl p sei der mittlere Elementarteiler möglichst wenig oft durch p teilbar. Also für gerade Variablenzahl und $\left(\frac{D}{p}\right) = 1$ seien genau $\frac{n}{2}$ Elementarteiler durch p^α teilbar, für gerade Variablenzahl und $\left(\frac{D}{p}\right) = -1$ seien 2 Elementarteiler genau durch p^α und je $\frac{n-2}{2}$ durch p^0 und $p^{2\alpha}$ teilbar, und für ungerade Variablenzahl sei ein Elementarteiler durch p^α und je $\frac{n-1}{2}$ durch p^0 und $p^{2\alpha}$ teilbar.

Da mit $\mathfrak{T}_{ik}$ auch $N(\mathfrak{T}_{ik})\mathfrak{T}_{ik}^{-1}$ ein ganzer primitiver halbnormaler Transformator der bezeichneten Art ist, welcher rechts zu $\mathfrak{F}_i$ und links zu $\mathfrak{F}_k$ gehört, und da diese Beziehung umkehrbar eindeutig ist, gilt

$$\pi_{ik}(t) = \pi_{ki}(t) \ . \tag{106}$$

Die Anzahl der ganzen primitiven halbnormalen Linksideale für $\mathfrak{F}_i$, deren rechts zugehörige Form $\mathfrak{F}_k$ ist, werde mit $\varrho_{ik}(t)$ bezeichnet, wobei für ihre Abzählung dasselbe gilt wie für $\pi_{ik}(t)$. Es ist offenbar

$$\varrho_{ik}(t) = \pi_{ik}(t)\frac{1}{e_k} \ . \tag{107}$$

Die Matrizen

$$\mathfrak{R}(t) = (\varrho_{ik}(t))$$

haben eine wichtige multiplikative Eigenschaft:

$$\mathfrak{R}(t_1)\,\mathfrak{R}(t_2) = \mathfrak{R}(t_1 t_2) \qquad \text{für} \quad (t_1, t_2) = 1 \ . \tag{108}$$

Diese Formel drückt die Eindeutigkeit der Zerlegung ganzer Transformatoren in primäre aus und läßt sich sehr einfach beweisen: es sei $\mathfrak{T}_{ik}(t_1 t_2)$[21]) ein Transformator, wie er in das Abzählung vorkommen darf. Er läßt sich als ein Produkt

$$\mathfrak{T}_{ik}(t_1 t_2) = \mathfrak{T}_{ij}(t_1)\,\mathfrak{T}_{jk}(t_2) \tag{109}$$

schreiben. Diese Zerlegung ist nach § 6, Nr. 1 durch t_1, t_2 bis auf Einheiten eindeutig bestimmt, da ja $(t_1, t_2) = 1$ sein sollte. Umgekehrt hat ein Produkt (109) aus zwei Faktoren dieser Art auch wieder die Eigenschaft, die für die Aufzählung oben verlangt wurden, und zwar ebenfalls wegen der Teilerfremdheit von t_1 und t_2. Mithin ist die Anzahl der $\mathfrak{T}_{ik}(t_1 t_2)$ in (109)

$$\pi_{ik}(t_1 t_2) = \sum_j \frac{\pi_{ij}(t_1)\,\pi_{jk}(t_2)}{e_j}$$

was nach (107) mit der Behauptung identisch ist.

Hilfssatz 10. Jeder kommutative durch Matrizen $\mathfrak{R}(t)$ erzeugte Ring P ist halbeinfach.

Beweis. Setzt man

$$\mathfrak{M} = \begin{pmatrix} \sqrt{e_1} & & \\ & \ddots & \\ & & \sqrt{e_h} \end{pmatrix} ,$$

so ist nach (107)

$$\mathfrak{M}^{-1}\,\mathfrak{R}(t)\,\mathfrak{M} = \left(\frac{\pi_{ik}(t)}{\sqrt{e_i\,e_k}}\right) ,$$

das ist nach (106) eine symmetrische Matrix. Ein kommutativer durch Matrizen $\mathfrak{R}(t)$ erzeugter Ring P läßt sich also durch symmetrische Matrizen darstellen, und da kommutierbare symmetrische Matrizen simultan auf Diagonalform transformierbar sind, gestattet P auch eine Darstellung durch Diagonalematrizen, womit die Behauptung zum Ausdruck kommt.

---

[21]) Sofern es praktisch erscheint, setze ich im folgenden bei Transformatoren, Idealen und Vektoren die Norm in Klammern hinzu: $[\mathfrak{T}_{ik}(N)$, $(\mathfrak{T}_{ik}(N)]$, $\mathfrak{t}_i(N)$.

2. Es bezeichne $\mathfrak{e}$ die einzeilige Matrix mit den Elementen $\frac{1}{e_1}, \ldots, \frac{1}{e_h}$, dann gilt

$$\mathfrak{e}\,\mathfrak{R}(t) = \varrho(t)\,\mathfrak{e}\ , \tag{110}$$

wo

$$\varrho(t) = \sum_{k=1}^{h} \varrho_{ik}(t) \tag{111}$$

die von i nicht mehr abhängige Anzahl der ganzen primitiven halbnormalen Linksideale in dem oben genannten Sinne für eine der Formen $\mathfrak{F}_i$ ist. Daß die Anzahl (111) von i nicht mehr abhängt, folgt schon daraus, daß sie nur von dem Verhalten von $\mathfrak{F}_i$ mod t abhängt; für zu $2D$ teilerfremde Primzahlen p, nach denen D ein quadratischer Rest ist, wurde sie in § 8, Nr. 6, Gleichung (77) berechnet. Die Formel (110) folgt nun leicht aus (106) und (107). Nach (108), (110) ist

$$\varrho(t_1)\,\varrho(t_2) = \varrho(t_1 t_2) \qquad \text{für} \quad (t_1, t_2) = 1\ . \tag{112}$$

Die Formel (110) gestattet eine Verallgemeinerung: die verschiedenen Geschlechter des vorliegenden Formensystems mögen von 1 bis g durchnumeriert werden, für das j-te Geschlecht sei $\mathfrak{e}_j$ die einzeilige Matrix mit den Elementen $\frac{1}{e_1}$ bzw. 0, je nachdem $\mathfrak{F}_i$ zu diesem Geschlecht gehört oder nicht. Alle Transformatoren derselben Norm gehören jeweils zum gleichen Geschlecht; wenn also $\mathfrak{F}_i$ sämtliche Klassen des j-ten Geschlechts durchläuft, so gehört $t \cdot \mathfrak{F}_i$ einem durch j und t wohlbestimmten Geschlecht an, es sei das k-te. Jetzt gilt

$$\mathfrak{e}_j\,\mathfrak{R}(t) = \varrho(t)\,\mathfrak{e}_k\ . \tag{113}$$

3. Die Anzahl der Darstellungen einer Zahl t durch die Form $\mathfrak{F}_i$, d. h. die Anzahl der Vektoren $\mathfrak{t}_i$ der Norm t in dem Gitter $\mathfrak{J}_i$ sei $\delta_i(t)$, die Anzahl der primitiven Vektoren $\mathfrak{t}_i$ der Norm t in $\mathfrak{J}_i$ sei $\delta_i^*(t)$. Diese Anzahlen mögen zu einspaltigen Matrizen $\mathfrak{d}(t)$ und $\mathfrak{d}^*(t)$ vereinigt werden; sie stehen mit den $\mathfrak{R}(t)$ in Beziehung.

Es seien zunächst t_1 und t_2 teilerfremde ganze Zahlen, und in t_1 mögen nur solche Primzahlen p aufgehen, für welche

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

ist; die Variablenzahl sei gerade. Dann gilt

$$\mathfrak{R}(t_1)\,\mathfrak{d}^*(t_2) = \nu(t_1)\,\mathfrak{d}^*(t_1 t_2)\ . \tag{114}$$

Zum Beweise betrachte man die Gleichung

$$\mathfrak{T}_{ik}(t_1)\, \mathfrak{t}_k(t_2) = \mathfrak{t}_i(t_1 t_2) \quad ^{21}) \ , \tag{115}$$

wo $\mathfrak{T}_{ik}(t_1)$ sämtliche ganzen primitiven normalen Transformatoren der Norm t_1 durchlaufen möge, die links zu $\mathfrak{F}_i$ und rechts zu $\mathfrak{F}_k$ gehören, und $\mathfrak{t}_k(t_2)$ sämtliche ganzen primitiven Vektoren der Norm t_2 aus dem Gitter $\mathfrak{J}_k$, der Index k durchlaufe dabei die ganze Reihe von 1 bis h. Auf diese Weise entstehen ganze Vektoren $\mathfrak{t}_i(t_1 t_2)$ des Gitters $\mathfrak{J}_i$, ihre Norm ist $t_1 t_2$. Diese Vektoren sind primitiv, wäre nämlich $\mathfrak{t}_i(t_1 t_2)$ durch eine Primzahl p teilbar, so müßte offenbar p in $|\, \mathfrak{T}_{ik}(t_1)\,|$, d. h. in t_1 aufgehen. Durch geeigneten Basiswechsel kann man erreichen (vgl. § 8), daß $\mathfrak{F}_i \equiv \mathfrak{F}_k \equiv \mathfrak{F}_0^{(n)} \mod p$ und

$$\mathfrak{T}_{ik}(t_1) \equiv \begin{pmatrix} \mathfrak{E}^{\left(\frac{n}{2}\right)} & \\ & \mathfrak{O}^{\left(\frac{n}{2}\right)} \end{pmatrix} \mod p$$

ist. Wenn nun $\mathfrak{t}_i(t_1 t_2)$ durch p teilbar wäre, so müßten die $\frac{n}{2}$ ersten Koeffizienten von $\mathfrak{t}_k(t_2)$ durch p teilbar sein; dann wäre aber $N(\mathfrak{t}_k(t_2)) = t_2$ durch p teilbar, im Gegensatz zu der gemachten Voraussetzung.

Jeder ganzzahlige primitive Vektor $\mathfrak{t}_i(t_1 t_2)$ läßt sich in der Form (115) schreiben, und zwar auf $\nu(t_1)$ wesentlich verschiedene Weisen, nämlich nach § 8, Nr. 5 gibt es $\nu(t_1)$ Ideale $(\mathfrak{T}_{ik}(t_1)]$, welche $\mathfrak{t}_i(t_1 t_2)$ teilen, womit (114) bewiesen ist.

Setzt man

$$\mathfrak{S}(t) = \sum_{s^2/t} \frac{1}{\nu(t s^{-2})}\, \mathfrak{R}(t s^{-2}) \ , \tag{116}$$

und summiert in (114) über sämtliche quadratischen Teiler, so ist wegen

$$\sum_{s^2/t} \mathfrak{d}^*(t s^{-2}) = \mathfrak{d}(t) : \tag{117}$$

$$\mathfrak{S}(t_1)\, \mathfrak{d}(t_2) = \mathfrak{d}(t_1 t_2) \qquad \text{für } (t_1, t_2) = 1 \ . \tag{118}$$

4. Diese Formel ist nun nach verschiedenen Richtungen hin zu verallgemeinern; zunächst sei weiterhin t_1 zu D prim und als Norm eines ganzen primitiven normalen Transformators möglich, jedoch dürfen t_1 und t_2 einen gemeinsamen Teiler besitzen. Um (118) auf diesen Fall zu übertragen, genügt es wegen (108),

$$t_1 = p^\alpha, \quad t_2 = p^\beta t, \quad (t, p) = 1 \ , \quad \alpha > 0, \quad \beta > 0$$

anzunehmen. Ohne Beschränkung der Allgemeinheit darf ferner vorausgesetzt werden, daß sämtliche Formen $\mathfrak{F}_i$ der Form $\mathfrak{F}_0^{(2m)}$ mod $p^{\alpha+\beta}$ kongruent sind. Alle ganzen primitiven normalen Linksideale $(\mathfrak{T}_{ik}(p^\alpha)]$ haben dann die Gestalt $(\mathfrak{U}\,\mathfrak{P}_0^\alpha]$, vgl. § 5, Nrn. 3, 4.

Es sei $\mathfrak{T}_{ik}(p^\alpha)\,\mathfrak{t}_k(p^\beta t)$ durch p teilbar, dann setze man

$$\mathfrak{T}_{ik}(p^\alpha) = \mathfrak{U}\,\mathfrak{P}_0^\alpha\,\mathfrak{V} \tag{119}$$

mit zwei unimodularen Matrizen $\mathfrak{U}, \mathfrak{V}$. Es ist also $\mathfrak{U}\,\mathfrak{P}_0^\alpha\,\mathfrak{V}\,\mathfrak{t}_k(p^\beta t)$ durch p teilbar, folglich ist es auch

$$\mathfrak{P}_0\,\mathfrak{V}\,\mathfrak{t}_k(p^\beta t) = p\,\mathfrak{V}'\,\mathfrak{t}_j(p^{\beta-1} t)\ ,$$

wo $\mathfrak{V}'$ eine unimodulare Matrix bedeutet, welche $p^{1-\alpha}\,\mathfrak{P}_0^{\alpha-1}\,\mathfrak{U}\,\mathfrak{F}_i\,\mathfrak{U}\,\mathfrak{P}_0^{\alpha-1}$ in eine der Formen $\mathfrak{F}_1, \ldots, \mathfrak{F}_h$ transformiert, etwa in $\mathfrak{F}_j$. Man erhält somit

$$\begin{aligned}\mathfrak{T}_{ik}(p^\alpha)\,\mathfrak{t}_k(p^\beta t) &= \mathfrak{U}\,\mathfrak{P}_0^\alpha\,\mathfrak{V}\,\mathfrak{t}_k(p^\beta t) = p\,\mathfrak{U}\,\mathfrak{P}_0^{\alpha-1}\,\mathfrak{V}'\,\mathfrak{t}_j(p^{\beta-1} t) = \\ &= p\,\mathfrak{T}_{ij}(p^{\alpha-1})\,\mathfrak{t}_j(p^{\beta-1} t)\ .\end{aligned} \tag{120}$$

Das Ideal $(\mathfrak{T}_{ij}(p^{\alpha-1})]$ ist eindeutig festgelegt als der einzige Linksteiler von $(\mathfrak{T}_{ik}(p^\alpha)]$ dieser Norm. Ist umgekehrt ein Vektor $\mathfrak{t}_j(p^{\beta-1} t)$ gegeben, so kann man $p\,\mathfrak{T}_{ij}(p^{\alpha-1})\,\mathfrak{t}_j(p^{\beta-1} t)$ in der Form (120) immer darstellen.

Zur Übertragung von (114) auf den vorliegenden Fall gehe man wieder von (115) aus, wobei $\mathfrak{t}_k(p^\alpha t)$ nicht auf primitive Vektoren beschränkt sei. Durch die Produkte (115) werden zwar auch jetzt noch sämtliche primitiven Vektoren $\mathfrak{t}_i(p^{\alpha+\beta} t)$ und jeder von ihnen $\nu(p^\alpha)$-mal geliefert, jedoch treten auch noch imprimitive Vektoren auf, deren Vielfachheit man aus (120) leicht erkennen kann: es durchlaufe $\mathfrak{U}$ ein System von Einheiten von $\mathfrak{F}_0^{(2m)}$ mod p^α derart, daß $(\mathfrak{U}\,\mathfrak{P}_0^\alpha]$ sämtliche $\varrho(p^\alpha)$ ganzen primitiven normalen Linksideale der Norm p^α durchläuft. Dann durchläuft auch $(\mathfrak{U}\,\mathfrak{P}_0^{\alpha-1}]$ sämtliche ganzen normalen primitiven Linksideale der Norm $p^{\alpha-1}$, und zwar jedes offenbar gleich oft, also $\dfrac{\varrho(p^\alpha)}{\varrho(p^{\alpha-1})}$-mal, wobei im Falle $\alpha = 1$ $\varrho(1) = 1$ zu nehmen ist. Folglich liefert die Abzählung sämtlicher Produkte (115)

$$\mathfrak{R}(p^\alpha)\,\mathfrak{d}(p^\beta t) = \nu(p^\alpha)\,\mathfrak{d}^*(p^{\alpha+\beta} t) + \frac{\varrho(p^\alpha)}{\varrho(p^{\alpha-1})}\,\mathfrak{R}(p^{\alpha-1})\,\mathfrak{d}(p^{\beta-1} t)$$

oder (wenn man $\nu(1) = 1$ nimmt)

$$\frac{1}{\nu(p^\alpha)}\,\mathfrak{R}(p^\alpha)\,\mathfrak{d}(p^\beta t) = \mathfrak{d}^*(p^{\alpha+\beta} t) + \frac{\varrho(p^\alpha)}{\nu(p^\alpha)}\,\frac{\nu(p^{\alpha-1})}{\varrho(p^{\alpha-1})}\,\frac{1}{\nu(p^{\alpha-1})}\,\mathfrak{R}(p^{\alpha-1})\,\mathfrak{d}(p^{\beta-1} t)\,,$$

das ist nach (76):

$$\frac{1}{\nu(p^\alpha)}\,\mathfrak{R}(p^\alpha)\,\mathfrak{d}(p^\beta t) = \mathfrak{d}^*(p^{\alpha+\beta} t) + (p^{m-1}+\varepsilon)\frac{1}{\nu(p^{\alpha-1})}\,\mathfrak{R}(p^{\alpha-1})\,\mathfrak{d}(p^{\beta-1} t)$$

$$\text{mit}\quad \varepsilon = \begin{cases} 0 \text{ für } \alpha > 1\,, \\ 1 \text{ für } \alpha = 1\,. \end{cases}$$

Man nehme diese Gleichung auch noch mit $\alpha - 2$, $\alpha - 4, \ldots$ an Stelle von α, die letzte der so entstehenden Gleichungen ist dann

$$\frac{1}{\nu(p)}\,\mathfrak{R}(p)\,\mathfrak{d}(p^\beta t) = \mathfrak{d}^*(p^{1+\beta} t) + (p^{m-1}+1)\,\mathfrak{d}(p^{\beta-1} t) \quad \text{für } \alpha \equiv 1 \bmod 2\,,$$

$$\frac{1}{\nu(p^2)}\,\mathfrak{R}(p^2)\,\mathfrak{d}(p^\beta t) =$$

$$= \mathfrak{d}^*(p^{2+\beta} t) + p^{m-1}\frac{1}{\nu(p)}\,\mathfrak{R}(p)\,\mathfrak{d}(p^{\beta-1} t) \quad \text{für } \alpha \equiv 0 \bmod 2\,;$$

im letzteren Falle füge man noch

$$\mathfrak{d}(p^\beta t) = \mathfrak{d}^*(p^\beta t) + \mathfrak{d}(p^{\beta-2} t)$$

an. Addiert man alle diese Gleichungen, so erhält man nach (116)

$$\mathfrak{S}(p^\alpha)\,\mathfrak{d}(p^\beta t) = \mathfrak{d}(p^{\alpha+\beta} t) + p^{m-1}\,\mathfrak{S}(p^{\alpha-1})\,\mathfrak{d}(p^{\beta-1} t)\,,$$

woraus sich unmittelbar

$$\mathfrak{S}(p^\alpha)\,\mathfrak{d}(p^\beta t) = \sum_{\sigma=0}^{\text{Min }(\alpha,\beta)} p^{(m-1)\sigma}\,\mathfrak{d}(p^{\alpha+\beta-2\sigma} t)$$

ergibt oder allgemeiner:

$$\mathfrak{S}(t_1)\,\mathfrak{d}(t_2) = \sum_{s\,/\,(t_1,t_2)} s^{m-1}\,\mathfrak{d}(t_1 t_2 s^{-2})\,; \tag{121}$$

es sei nochmals daran erinnert, daß in t_1 nur solche Primzahlen aufgehen dürfen, nach denen D ein quadratischer Rest ist, und die Variablenzahl ist gerade: $n = 2m$.

Ganz ähnlich wie die Matrizen $\mathfrak{S}(t)$ verhalten sich die folgenden Matrizen:

$$\begin{cases} \mathfrak{X}(1) = \mathfrak{E}^{(h)}\,, \\ \mathfrak{X}(p) = \mathfrak{S}(p)\,, \\ \mathfrak{X}(p^\alpha) = \mathfrak{X}(p^{\alpha-1})\,\mathfrak{S}(p) - p^{m-1}\,\mathfrak{X}(p^{\alpha-2})\,; \end{cases} \tag{122}$$

man bestätigt leicht durch vollständige Induktion bezüglich α unter Benutzung von (121), daß

$$\mathfrak{X}(p^\alpha)\,\mathfrak{d}(p^\beta t) = \sum_{\sigma=0}^{\mathrm{Min}\,(\alpha,\beta)} p^{\sigma(m-1)}\,\mathfrak{d}(p^{\alpha+\beta-2\sigma} t) \tag{123}$$

gilt.

5. Es soll nun (118) und (123) auf den Fall

$$t_1 = p^2\ , \quad t_2 = p^\beta t\ , \quad (t,p) = 1 \quad \text{und} \quad \left(\frac{D}{p}\right) = -1$$

bei gerader Variablenzahl übertragen werden. Man betrachte dazu die Produkte $\mathfrak{T}_{ik}(p^2)\,\mathfrak{t}_k(p^\beta t)$ bei festgehaltenem Index i, die $\mathfrak{T}_{ik}(p^2)$ seien ganz, primitiv und halbnormal, die $\mathfrak{t}_k(p^\beta t)$ ganzzahlig, primitiv oder imprimitiv. In dieser Gesamtheit kommen zunächst die primitiven $\mathfrak{t}_i(p^{2+\beta} t)$ vor, jeder dieser Vektoren (p^2)-mal. Dann treten wiederum imprimitive Vektoren auf, und zwar sowohl für $\beta = 0$ wie für $\beta > 0$; zu deren Abzählung ist eine kleine Vorbereitung notwendig.

Es sei $\lambda_{ik}(p^2; N)$ die Anzahl der ganzen primitiven und halbnormalen $\mathfrak{T}_{ik}(p^2)$, welche mit einem festen primitiven $\mathfrak{t}_i(N)$ in der Beziehung

$$\mathfrak{T}_{ik}(p^2)\,\mathfrak{t}_k(N) = p\,\mathfrak{t}_i(N) \tag{124}$$

stehen ($\mathfrak{t}_k(N)$ sei ganzzahlig). Man führe die Matrizen

$$\mathfrak{L}(p^2; N) = (\lambda_{ik}(p^2; N))$$

ein. Die einfache Abzählungsformel (101) aus § 9, Nr. 4 gilt offenbar auch für die Anzahlen $\lambda_{ik}(p; N)$, $\varrho_{ik}(p^2)$ an Stelle von $\lambda(p^2; N)$, $\varrho(p^2, r)$, also

$$\mathfrak{L}(p^2; N) = \frac{\varkappa(p^2; N)}{\delta(p; N)}\,\mathfrak{R}(p^2)\ , \tag{125}$$

wo $\varkappa(p^2; N)$, $\delta(p; N)$ aus (103) und (104) zu entnehmen sind. Die einzelnen Zeilensummen von $\mathfrak{L}(p^2; N)$ ergeben für alle Zeilen dasselbe Resultat $\lambda(p^2; N)$.

Nach dieser Vorbereitung kann man nun leicht zeigen:

$$\begin{aligned}\mathfrak{R}(p^2)\,\mathfrak{d}(p^\beta t) = {} & \nu(p^2, r)\,\mathfrak{d}^*(p^{2+\beta} t) + \mathfrak{L}(p^2; p^\beta t)\,\mathfrak{d}(p^\beta t) \\ & + \left(\varrho(p^2, r)\,\mathfrak{E}^{(h)} - \mathfrak{L}(p^2; p^\beta t)\right)\mathfrak{d}(p^{\beta-2} t)\ ,\end{aligned} \tag{126}$$

wo der letzte Term im Falle $\beta < 2$ zu streichen ist. Zum Beweis von (126) braucht man nur noch die Terme

$$\mathfrak{L}(p^2; p^\beta t)\,(\mathfrak{d}(p^\beta t) - \mathfrak{d}(p^{\beta-2} t)) = \mathfrak{L}(p^2; p^\beta t)\,\mathfrak{d}^*(p^\beta t)\,,\ \varrho(p^2, r)\,\mathfrak{d}(p^{\beta-2} t)$$

zu erklären. Der erstere gibt sämtliche Produkte (124) mit $N = p^\beta t$ und primitivem $\mathfrak{t}_i(p^\beta t)$ wieder, deren Anzahl ist bei gegebenem $\mathfrak{t}_i(p^\beta t)$ nach der getroffenen Definition gleich $\lambda_{ik}(p^2; p^\beta t)$. Endlich soll $\varrho(p^2, r)\,\mathfrak{d}(p^{\beta-2} t)$ die Anzahl der Produkte

$$\mathfrak{T}_{ik}(p^2)\,\mathfrak{t}_k(p^\beta t) = p^2\,\mathfrak{t}_i(p^{\beta-2} t) \tag{127}$$

sein. In der Tat tritt jedes $p^2\,\mathfrak{t}_i(p^{\beta-2} t)$ in dieser Gesamtheit auf, und zwar so oft, wie es ganze primitive halbnormale Rechtsideale $[\mathfrak{T}_{ki}(p^2))$ gibt, d. h. $\varrho(p^2, r)$-mal. Man setze nämlich für ein solches Rechtsideal

$$\mathfrak{t}_k(p^\beta t) = \mathfrak{T}_{ki}(p^2)\,\mathfrak{t}_i(p^{\beta-2} t)\ ,$$

dann gilt (127) mit

$$\mathfrak{T}_{ik}(p^2) = p^2\,\mathfrak{T}_{ki}(p^2)^{-1}\ .$$

Damit ist (126) bewiesen.

Setzt man

$$\left.\begin{aligned}
\mathfrak{X}(p^2) &= \frac{1}{\nu(p^2, r)}\,(\mathfrak{R}(p^2) - \mathfrak{L}(p^2; 1)) + \mathfrak{E}^{(h)}\ ,\\
\mathfrak{X}(p^{2\alpha}) &= \left[\frac{1}{\nu(p^2, r)}\,(\mathfrak{R}(p^2) - \mathfrak{L}(p^2; 0)) + \mathfrak{E}^{(h)}\right]\mathfrak{X}(p^{2\alpha-2}) -\\
&\quad - \left[\frac{\varrho(p^2, r)}{\nu(p^2, r)}\,\mathfrak{E}^{(h)} - \frac{1}{\nu(p^2, r)}\,\mathfrak{L}(p^2; 0)\right]\mathfrak{X}(p^{2\alpha-4})\ ,
\end{aligned}\right\} \tag{128}$$

so gilt

$$\left\{\begin{aligned}
\mathfrak{X}(p^{2\alpha})\,\mathfrak{d}(t) &= \mathfrak{d}(p^{2\alpha} t)\\
\mathfrak{X}(p^{2\alpha})\,\mathfrak{d}(p\,t) &= \mathfrak{d}(p^{2\alpha+1} t)
\end{aligned}\right\} \tag{129}$$

(für $(t, p) = 1$; bei ungerader Variablenzahl muß t eine Quadratzahl sein), wie man mit Hilfe von (126) und (128) durch vollständige Induktion bezüglich α ganz leicht bestätigt.

Als das Hauptergebnis dieses Paragraphen formuliere ich den

Satz 9. Aus den in Nr. 1 definierten Matrizen $\mathfrak{R}(t)$ werden für zu D teilerfremde Primzahlpotenzen $t = p^\alpha$ bzw. $p^{2\alpha}$, und zwar je nachdem ob p oder erst p^2 Idealnorm ist, durch (116), (122) bzw. (128), (125), (103), (104)[22]) und allgemein für zu D teilerfremde Zahlen, die als Idealnormen auftreten können, durch

[22]) Sofern Primideale 2. Grades in Betracht kommen, setze ich die Variablenzahl größer als 2 voraus. Sonst würde es keine ganzen primitiven halbnormalen Primtransformatoren geben und die Resultate würden trivial. In den Beweisen wurde für diesen Fall ferner $p > 2$ angenommen; die Übertragung auf $p = 2$ dürfte nicht schwierig sein.

$$\mathfrak{X}(p_1^{\alpha_1} p_2^{\alpha_2} \ldots) = \mathfrak{X}(p_1^{\alpha_1})\, \mathfrak{X}(p_2^{\alpha_2}) \ldots \tag{130}$$

Matrizen $\mathfrak{X}(t)$ gebildet. Mit ihnen gilt

$$\mathfrak{X}(t_1)\mathfrak{X}(t_2) = \mathfrak{X}(t_1 t_2)\ , \quad \mathfrak{X}(t_1)\mathfrak{d}(t_2) = \mathfrak{d}(t_1 t_2) \quad \text{für} \quad (t_1, t_2) = 1\ ;$$

sie erzeugen einen kommutativen halbeinfachen Ring Ξ.

Die Kommutativität folgt aus den Definitionsgleichungen und (108), die Halbeinfachheit aus Hilfssatz 10.

§ 11. Der Satz von Hecke und das Darstellungsmaß

1. Es seien $\mathfrak{X}(t_1)$ und $\mathfrak{X}(t_2)$ zwei Matrizen aus dem in Satz 9 erwähnten Ring Ξ. Dann gilt

$$\mathfrak{X}(t_1)\mathfrak{d}(t_2) = \mathfrak{X}(t_1)\mathfrak{X}(t_2)\mathfrak{d}(1) = \mathfrak{X}(t_2)\mathfrak{X}(t_1)\mathfrak{d}(1) = \mathfrak{X}(t_2)\mathfrak{d}(t_1)\ .$$

Diese Gleichung lautet ausgeschrieben, unter ξ_{ik} die Elemente von $\mathfrak{X}$ verstanden:

$$\sum_{k=1}^{h} \xi_{ik}(t_1)\,\delta_k(t_2) = \sum_{k=1}^{h} \xi_{ik}(t_2)\,\delta_k(t_1)\ . \tag{131}$$

Wenn t_2 sämtliche zu D teilerfremden Idealnormen durchläuft, so mögen die $\mathfrak{d}(t_2)$ einen Raum der Dimension f aufspannen. Man kann dieses auch so ausdrücken: unter den Anzahlen $\delta_i(t_2)$ seien f linear unabhängig, etwa $\delta_1(t_2), \ldots, \delta_f(t_2)$, die übrigen $\delta_i(t_2)$ lassen sich aus ihnen linear kombinieren, wobei die Koeffizienten von t_2 nicht abhängen. Man bringe (131) nun für so viele Werte t_j von t_2 zum Ansatz, daß der Rang der Matrix $(\delta_k(t_j))$ gleich f ist. Es entsteht (für jedes i) ein lineares Gleichungssystem für die Unbekannten $\xi_{ik}(t_1)$, dessen rechte Seite linear und homogen in den $\delta_k(t_1)$ ist. Die Auflösung wird also folgende Gestalt haben:

$$\mathfrak{X}(t_1) = \mathfrak{X}_1 \delta_1(t_1) + \cdots + \mathfrak{X}_f \delta_f(t_1) + \mathfrak{Y}(t_1)\ , \tag{132}$$

wo $\mathfrak{X}_1, \ldots, \mathfrak{X}_f$ konstante Matrizen sind und $\mathfrak{Y}(t_1)$ dem zu (131) gehörigen homogenen Gleichungssystem

$$\mathfrak{Y}(t_1)\mathfrak{d}(t_2) = \mathfrak{o}^{(h,1)} \tag{133}$$

genügt. Sämtliche Lösungen $\mathfrak{Y}$ von (133) bilden offenbar ein Ideal Y in Ξ, und dieses ist ein direkter Summand, da Ξ halbeinfach ist. Der komplementäre direkte Summand heiße Z, man darf annehmen, daß in (132) die Matrix

$$\mathfrak{Z}(t_1) = \mathfrak{X}_1\,\delta_1(t_1) + \cdots + \mathfrak{X}_f\,\delta_f(t_1) \tag{134}$$

in Z enthalten ist.

Der Rang von Z ist höchstens f. Andererseits ist wegen (133)

$$\mathfrak{Z}(t_1)\,\mathfrak{d}(t_2) = \mathfrak{d}(t_1 t_2) \quad \text{für} \quad (t_1, t_2) = 1\ . \tag{135}$$

Nun spannen die Vektoren $\mathfrak{d}(t) = \mathfrak{Z}(t)\,\mathfrak{d}(1)$ einen Raum der Dimension f auf, daraus folgt, daß Z den Rang f hat.

Satz 10. *t_1 und t_2 mögen beliebige zu D teilerfremde Idealnormen sein. Es gebe unter den Anzahlen $\delta_i(t_1)$ genau f linear unabhängige, d. h. zwischen $f+1$ dieser Anzahlen bestehe stets eine Gleichung $\alpha_1\,\delta_1(t_1) + \cdots + \alpha_{f+1}\,\delta_{f+1}(t_1) = 0$ mit von t_1 unabhängigen Konstanten α_r.*

Es gibt f linear unabhängige Matrizen $\mathfrak{X}_1, \ldots, \mathfrak{X}_f$ von der Art, daß die Matrizen (134) die Gleichungen

$$\mathfrak{Z}(t_1)\,\mathfrak{Z}(t_2) = \mathfrak{Z}(t_1 t_2) \quad \textit{für} \quad (t_1, t_2) = 1\ , \tag{136}$$

und im Primzahlpotenzfalle

$$\mathfrak{Z}(p^\alpha) = \mathfrak{Z}(p^{\alpha-1})\,\mathfrak{Z}(p) - p^{m-1}\,\mathfrak{Z}(p^{\alpha-2}) \tag{137}$$

bei gerader Variablenzahl und $\left(\frac{D}{p}\right) = 1$,

$$\mathfrak{Z}(p^{2\alpha}) = \mathfrak{Z}(p^{2(\alpha-1)})\left[\frac{p^m}{p^m - \left(\frac{D}{p}\right)^n}\,\mathfrak{Z}(p^2) - \frac{\left(\frac{D}{p}\right)}{p^m - \left(\frac{D}{p}\right)^n}\,\mathfrak{E}\right] + \tag{138}$$

$$+\,\mathfrak{Z}(p^{2(\alpha-2)})\left[\frac{p^{1-r}}{p^m - \left(\frac{D}{p}\right)^n}\,\mathfrak{Z}(p^2) - \left(p^{m-1}(p^{m+r-1}+1) + \frac{p^{1-r}}{p^m - \left(\frac{D}{p}\right)^n}\right)\mathfrak{E}\right]$$

bei gerader Variablenzahl $(r=2)$ *und* $\left(\frac{D}{p}\right) = -1$, *sowie bei ungerader Variablenzahl* $(r=1)$ *erfüllen*[22]).

Es ist nur noch (137) und (138) zu beweisen. (137) ergibt sich aus (122), wenn man dort $\mathfrak{X}(p^\alpha)$ durch $\mathfrak{X}(p)$ ausdrückt und dann die Komponente $\mathfrak{Z}(p^\alpha)$ von $\mathfrak{X}(p^\alpha)$ in Z nimmt. Ebenso folgt (138) aus (128), wobei man (125), (103), (104) benutzen muß.

Die Bedeutung des Satzes 10 ist die, daß man nur die Zahlen $\delta_i(p)$ für $\left(\frac{D}{p}\right) = 1$ und $\delta_i(p^2)$ für $\left(\frac{D}{p}\right) = -1$ zu kennen braucht, um die $\delta_i(t)$ für eine beliebige zu D teilerfremde Idealnorm t ausrechnen zu können. Allgemeine Zusammenhänge dieser Art bei geradem n wurden von Hecke[4]) gefunden, darunter die Formel (137), die hiermit auf einem neuen Wege bewiesen wurde. Für die Primzahlen p mit $\left(\frac{D}{p}\right) = -1$ ist mir der Anschluß an die Ergebnisse von Hecke bisher noch nicht gelungen.

2. Multipliziert man (122), (128), (130) und

$$\mathfrak{X}(t)\,\mathfrak{d}(1) = \mathfrak{d}(t)$$

von links mit einer der Matrizen $\mathfrak{e}$ oder $\mathfrak{e}_i$ (vgl. § 10, Nr. 2), so kommt man nach leichter Rechnung zu folgendem Formelsystem:

$$\mathfrak{e}_i\,\mathfrak{X}(t) = x(t)\,\mathfrak{e}_k$$

mit

$$x(p^\alpha) = \frac{p^{(\alpha+1)(m-1)} - 1}{p^{m-1} - 1} \qquad \text{für } n \equiv 0 \bmod 2\ ,\ \left(\frac{D}{p}\right) = 1\ , \tag{139}$$

$$x(p^{2\alpha}) = \frac{p^{(2\alpha+1)m} - 1}{p^m + 1} \qquad \text{für } n \equiv 0 \bmod 2\ ,\ \left(\frac{D}{p}\right) = -1\ ^{22})\ , \tag{140}$$

$$x(p^{2\alpha}) = 1 + p^{m-1}\left(p^m - \left(\frac{D}{p}\right)\right)\frac{p^{\alpha(2m-1)} - 1}{p^{2m-1} - 1} \quad \text{für } n \equiv 1 \bmod 2\ ^{22})\ , \tag{141}$$

$$x(p_1^{\alpha_1}\,p_2^{\alpha_2}\cdots) = x(p_1^{\alpha_1})\,x(p_2^{\alpha_2})\ldots\ , \tag{142}$$

$$\mathfrak{e}_i\,\mathfrak{d}(t) = x(t)\,\mathfrak{e}_k\,\mathfrak{d}(1)\ . \tag{143}$$

Hier ist $\mathfrak{e}_i\,\mathfrak{d}(t)$ das *Darstellungsmaß* für die Zahl t durch die Formen des i-ten Geschlechtes und $e_k\mathfrak{d}(1)$ das Darstellungsmaß der Zahl 1 durch die Formen des k-ten Geschlechtes, wobei dieses nach der Regel von § 10, Nr. 2 zu bestimmen ist. Es ist bemerkenswert, wie sich hier die multiplikative Eigenschaft (142) des wesentlichen Teiles $x(t)$ des Darstellungsmaßes auf die Primzerlegung der Transformatoren und Ideale gründet, während bei Siegel[5]) diese Eigenschaft aus formal ganz anderen Vorstellungen hergeleitet wird.

IV. Haupttransformatoren und Einheiten, insbesondere bei indefiniten Formen

§ 12. Quadratische Formen und algebraische Zahlkörper; der Satz von Wedderburn

1. Wie die einfachen nichtkommutativen Algebren stehen auch die quadratischen Formen mit algebraischen Zahlkörpern in Beziehung, und zwar auf eine zweifache Art. Das gilt besonders für gerade Variablenzahl. Ein algebraischer Zahlkörper k heiße ein *Zerfällungskörper* der Form $\mathfrak{F}^{(2m)}$, wenn in k: $\mathfrak{F}^{(2m)} \approx \mathfrak{F}_0^{(2m)}$ wird. Es gilt der

Satz 11. Ein algebraischer Zahlkörper k ist dann und nur dann Zerfällungskörper einer Form $\mathfrak{F}$ in $n = 2m$ Variablen, wenn

1) $\sqrt{D(\mathfrak{F})}$ in k enthalten ist,

2) jedes Primideal in k, welches in der Kerndiskriminante von $\mathfrak{F}$ aufgeht, entweder geraden Grad oder gerade Verzweigungsordnung hat,

3) k im Falle nicht verschwindender Signatur total imaginär ist.

Beweis. Ein algebraischer Zahlkörper ist offenbar Zerfällungskörper für alle Formen eines Typs gleichzeitig. Ein Typ X gerader Variablenzahl werde gemäß Satz 3 in der Form (37) dargestellt. Dann sind die Bedingungen 1) und 2) für die Zerfällung der Typen X_2 und X_4 durch k notwendig und hinreichend bei verschwindender Signatur; hinsichtlich X_4 und der Bedingung 2) hat man dabei die bekannten Zerfällungsbedingungen für Quaternionenalgebren heranzuziehen, denn X_4 ist die Normenform einer Quaternionenalgebra. Die Bedingung 3) kommt bei nicht verschwindender Signatur hinzu, sie ist gleichzeitig die Bedingung für die Zerfällung von Ψ.

2. Eine andere Beziehung zwischen quadratischen Formen und algebraischen Zahlkörpern gründet sich auf die Haupttransformatoren. Zunächst gilt der

Hilfssatz 11. Ein Haupttransformator $\mathfrak{T}$ für eine Form $\mathfrak{F}$ läßt sich in einem Körper k der Charakteristik $\neq 2$ vollständig ausreduzieren, d. h. auf folgende Normalgestalt transformieren:

$$\mathfrak{C}^{-1}\mathfrak{T}\mathfrak{C} = \begin{pmatrix} \mathfrak{T}_1 & & \\ & \mathfrak{T}_2 & \\ & & \ddots \end{pmatrix},$$

wo die $\mathfrak{T}_i$ Matrizen mit in k irreduziblen charakteristischen Gleichungen sind. Die Form $\mathfrak{F}$ geht dabei in eine Summe von Teilformen ohne gemeinsame Variable über:

$$\dot{\mathfrak{C}}\,\mathfrak{F}\,\mathfrak{C} = \begin{pmatrix} \mathfrak{F}_1 & & \\ & \mathfrak{F}_2 & \\ & & \ddots \end{pmatrix}.$$

Der *Beweis* folgt einem bekannten Gedankengang[23]). Zunächst ist $\mathfrak{T}$ in „halbreduzierte" Gestalt transformierbar. Darauf transformiere man die Form $\dot{\mathfrak{C}}\,\mathfrak{F}\,\mathfrak{C}$ durch eine Dreiecksmatrix $\mathfrak{C}'$ in eine Form $\mathfrak{F}'$, deren Matrix nur Diagonalenelemente enthält. $\mathfrak{T}' = \mathfrak{C}'^{-1}\,\mathfrak{C}^{-1}\,\mathfrak{T}\,\mathfrak{C}\,\mathfrak{C}'$ behält dabei die halbreduzierte Gestalt bei. Andererseits ist $\mathfrak{T}'$ ein Haupttransformator für $\mathfrak{F}'$, das ist nur dann möglich, wenn $\mathfrak{T}'$ sogar vollständig ausreduziert ist.

Man kann leicht Haupttransformatoren der Norm t bilden, indem man die Form $\mathfrak{F}$ mittels einer Substitution $\mathfrak{S}$ in eine „Diagonalform" $\mathfrak{F}_1$ transformiert. Haupttransformatoren der Norm t für $\mathfrak{F}_1$ sind

$$\mathfrak{T}_1 = \begin{pmatrix} \pm\sqrt{t} & & \\ & \pm\sqrt{t} & \\ & & \ddots \end{pmatrix},$$

also $\mathfrak{T} = \mathfrak{S}\,\mathfrak{T}_1\,\mathfrak{S}^{-1}$ sind solche für die Form $\mathfrak{F}$. Jedoch sind diese trivial. Ich definiere daher: ein Haupttransformator der Norm t heiße *regulär*, wenn höchstens einer seiner Eigenwerte gleich $\pm\sqrt{t}$ ist, sonst *singulär*. Es wird sich zeigen, daß ein regulärer Haupttransformator bei ungerader Variablenzahl stets einen Eigenwert $\pm\sqrt{t}$ hat.

Es soll ferner im Anschluß an Hilfssatz 11 zwischen *„reduziblen"* und *„irreduziblen"* Haupttransformatoren unterschieden werden. Ein irreduzibler Haupttransformator ist offenbar auch stets regulär, außer eventuell bei der Variablenzahl 2, wo es irreduzible Haupttransformatoren mit den Eigenwerten $\pm\sqrt{t}$ geben kann.

3. Es sei $\mathfrak{T}$ ein irreduzibler Haupttransformator der Norm t für die Form $\mathfrak{F}$. Der Körper K entstehe durch Adjunktion sämtlicher Eigenwerte $\tau_1, \ldots, \tau_n$ von $\mathfrak{T}$ zum rationalen Zahlkörper k_0. Es gibt nach Hilfssatz 11 in K eine Matrix $\mathfrak{C}$, so daß

$$\mathfrak{C}^{-1}\,\mathfrak{T}\,\mathfrak{C} = \begin{pmatrix} \tau_1 & & \\ & \tau_2 & \\ & & \ddots \end{pmatrix} \tag{144}$$

[23]) *A. Speiser*, Die Gruppen von endlicher Ordnung, 3. Aufl. Berlin 1937, § 51.

ist; dabei ist in bekannter Weise die i-te Spalte $\mathfrak{c}_i$ von $\mathfrak{C}$ als eine nicht triviale Lösung des linearen Gleichungssystems

$$(\mathfrak{T} - \tau_i \mathfrak{E}^{(n)})\, \mathfrak{c}_i = \mathfrak{o}^{(n,1)}$$

definiert. Man darf ohne Beschränkung der Allgemeinheit annehmen, daß die $\mathfrak{c}_i$ algebraisch konjugiert sind.

Setzt man

$$\mathfrak{F}' = \dot{\mathfrak{C}}\, \mathfrak{F}\, \mathfrak{C} = (f'_{ik}) \ ,$$

so ist $\mathfrak{T}'$ ein Haupttransformator für $\mathfrak{F}'$, also

$$f'_{ik}\, \tau_i\, \tau_k = t\, f'_{ik} \ .$$

Da $\mathfrak{T}$ irreduzibel sein sollte, sind alle τ_i voneinander verschieden, also hat diese Gleichung zur Folge, daß es für jedes i genau ein $k = \varphi(i)$ gibt, so daß $f'_{ik} \neq 0$ ist; dabei ist

$$\tau_i\, \tau_{\varphi(i)} = t \ . \tag{145}$$

Ist für ein i: $\varphi(i) = i$, so folgt aus (145) $\tau_i = \pm \sqrt{t}$. Von jetzt ab möge $\mathfrak{T}$ als regulär angenommen werden, dann entfällt also diese Möglichkeit, d. h. es ist stets $\varphi(i) \neq i$. Nach (145) ist aber auch $\varphi(\varphi(i)) = i$, folglich muß die Variablenzahl gerade sein. Bei geeigneter Numerierung ist nun $\varphi(i) = i \pm m$, und $\mathfrak{F}'$ hat die Gestalt

$$\mathfrak{F}' = \begin{pmatrix} & & v_1 & & \\ & & & \ddots & v_m \\ v_1 & & & & \\ & \ddots & v_m & & \end{pmatrix} \tag{146}$$

mit gewissen von Null verschiedenen Zahlen $v_1, \ldots, v_m$ in K. Ich behaupte: $k_i = k_0\left(\tau_i + \frac{t}{\tau_i}\right)$, $k_i = k_0(\tau_i)$ sind Körper der Grade m und $2m$ über k_0, v_i ist in k_i enthalten. Der Beweis ist ganz einfach: $\tau_i \to \tau_{\varphi(i)} = \frac{t}{\tau_i}$ ist ein Automorphismus von K bezüglich k_0, daher ist k_i ein Unterkörper vom Index 2 in k'_i. Sämtliche Automorphismen σ von K/k_0 permutieren die Spalten von $\mathfrak{C}$, sie erzeugen also eine Permutation der Zeilen und Spalten von $\mathfrak{F}'$, d. h. eine Permutation der v_i. Ist σ ein solcher Automorphismus, der τ_i fest läßt $(i \leqq m)$, so läßt er auch τ_{i+m} fest. Also läßt σ die i-te und die $(i + m)$-te Spalte von $\mathfrak{C}$ fest, also

auch die i-te und die $(i+m)$-te Spalte von $\mathfrak{F}'$, d. h. die Zahl ν_i. Wenn σ die Eigenwerte τ_i und τ_{i+m} vertauscht, so wird in $\mathfrak{F}'$ die i-te und $(i+m)$-te Zeile und die i-te und $(i+m)$-te Spalte vertauscht, also bleibt ν_i ebenfalls fest, d. h. ν_i liegt in k_i, was zu beweisen war.

Wenn die einzelnen Spalten von $\mathfrak{C}$ algebraisch konjugiert sind, so sind es auch die Zeilen von $\mathfrak{C}^{-1}$. Die Zahlen $\omega_{i1}, \ldots, \omega_{in}$ mögen die i-te Zeile von $\mathfrak{C}^{-1}$ bilden $(i \leqq m)$, sie liegen in k_i, und es ist

$$\tfrac{1}{2}\dot{\mathfrak{x}}\,\mathfrak{F}\,\mathfrak{x} = \sum_{i=1}^{m} \nu_i(\omega_{i1}\,x_1 + \cdots + \omega_{in}\,x_n)(\omega_{i+m,1}\,x_1 + \cdots + \omega_{i+m,n}\,x_n) \ .$$

Hierfür kann man kürzer schreiben:

$$\tfrac{1}{2}\dot{\mathfrak{x}}\,\mathfrak{F}\,\mathfrak{x} = Sp\big(\nu\, n(\omega_1\,x_1 + \cdots + \omega_n\,x_n)\big) \ , \tag{147}$$

wenn folgendes festgesetzt wird: es sei $\omega_j = \omega_{1j}$, $\nu = \nu_1$, n die Norm von $k' = k'_1$ bezüglich $k = k_1$ und S_p die Spur von k bezüglich k_0.

Die Ausführung des Haupttransformators $\mathfrak{T}$ geschieht nun einfach durch Multiplikation von $\omega_1\,x_1 + \cdots + \omega_n\,x_n$ mit der Zahl $\tau = \tau_1$.

Ist $\mathfrak{T}$ nicht irreduzibel, aber regulär, so wird $\mathfrak{T}$ nach Hilfssatz 11 bei geeigneter Variablentransformation eine Summe von Formen $\mathfrak{F}_j$ ohne gemeinsame Variable, und $\mathfrak{T}$ entspricht einem System regulärer irreduzibler Haupttransformatoren $\mathfrak{T}_j$ der $\mathfrak{F}_j$. Man bekommt also eine Darstellung von $\mathfrak{F}$ in der allgemeinen Form

$$\tfrac{1}{2}\dot{\mathfrak{x}}\,\mathfrak{F}\,\mathfrak{x} = \sum_{j} Sp\big(\nu_j\, n(\omega_{j1}\,x_{j1} + \cdots + \omega_{jn_j}\,x_{jn_j})\big) + f\,x_n^2 \ , \tag{148}$$

wo das Glied $f x_n^2$ nur bei ungerader Variablenzahl steht; es entspricht dem in diesem Falle einzigen Eigenwert $\pm\sqrt{t}$.

Es liegt nahe, einen Körper k' einen *Darstellungskörper* für $\mathfrak{F}$ zu nennen, wenn eine Darstellung (148) in ihm möglich ist, wobei $\omega_{j1}, \ldots, \omega_{jn_j}$ die Basis eines Unterkörpers k'_j von k' bilden und die ν_j einem Unterkörper k_j von k'_j vom Index 2 angehören. Mit dieser Begriffsbezeichnung können die letzten Ergebnisse folgendermaßen formuliert werden:

Satz 12. Der Ring aller rationalen mit einem regulären Haupttransformator $\mathfrak{T}$ vertauschbaren Matrizen ist eine direkte Summe von Körpern; deren Kompositum ist ein Darstellungskörper. Der Körper aller Eigenwerte von $\mathfrak{T}$ ist ein Zerfällungskörper.

Die Darstellung (147) bzw. (148) hat gewisse Ähnlichkeit mit der Darstellung einer einfachen nicht kommutativen Algebra als ein verschränktes Produkt. Auch der Satz 12 erinnert an ein ähnliches Verhalten solcher

Algebren: maximale kommutative Unterkörper sind gleichzeitig Zerfällungskörper.

4. In diesen Zusammenhang gehört die Verallgemeinerung eines bekannten Satzes von *Wedderburn:*

Satz 13. *Sind $\mathfrak{T}_1, \mathfrak{T}_2$ zwei Haupttransformatoren einer Form $\mathfrak{F}$ in einem Körper k_0 der Charakteristik $\neq 2$ mit denselben Eigenwerten, so gibt es in einem Erweiterungskörper k von k_0 einen Haupttransformator $\mathfrak{S}$ von $\mathfrak{F}$ derart, daß*

$$\mathfrak{T}_1 = \mathfrak{S}^{-1}\,\mathfrak{T}_2\,\mathfrak{S} \tag{149}$$

ist. Sind alle Eigenwerte verschieden, und ist k_0 ein endlicher Körper, so gibt es ein solches $\mathfrak{S}$ bereits in k_0.

Beweis. Nach Hilfssatz 11 einerseits und dem Satz von Wedderburn andererseits gibt es eine Matrix $\mathfrak{R}$ in k_0, so daß

$$\mathfrak{T}_1 = \mathfrak{R}^{-1}\,\mathfrak{T}_2\,\mathfrak{R} \tag{150}$$

gilt. $\mathfrak{T}_1$ ist dann ein Haupttransformator für die beiden Formen $\mathfrak{F}$ und $\mathfrak{F}_1 = \dot{\mathfrak{R}}\,\mathfrak{F}\,\mathfrak{R}$.

Es seien zunächst alle Eigenwerte von $\mathfrak{T}_1$ verschieden. Wird $\mathfrak{T}_1$ mittels einer Matrix $\mathfrak{C}$ auf die Diagonalform (144) transformiert, so haben nach der Schlußweise von Nr. 3 die Matrizen $\mathfrak{F}' = \dot{\mathfrak{C}}\,\mathfrak{F}\,\mathfrak{C}$ und $\mathfrak{F}_1' = \dot{\mathfrak{C}}\,\mathfrak{F}_1\,\mathfrak{C}$ in jeder Zeile an genau einer Stelle einen von Null verschiedenen Koeffizienten, und zwar an derselben Stelle. Folglich gibt es eine Diagonalmatrix $\mathfrak{D}$, daß

$$\mathfrak{F}' = \dot{\mathfrak{D}}\,\mathfrak{F}_1'\,\mathfrak{D} \tag{151}$$

ist. Nun ist $\mathfrak{D}$ mit der Matrix (144) vertauschbar, $\mathfrak{C}\mathfrak{D}\mathfrak{C}^{-1}$ also mit $\mathfrak{T}_1$. Nach (151) ist $\mathfrak{S} = \mathfrak{R}\,\mathfrak{C}\,\mathfrak{D}\,\mathfrak{C}^{-1}$ ein Haupttransformator für $\mathfrak{F}$, und da $\mathfrak{C}\,\mathfrak{D}\,\mathfrak{C}^{-1}$ mit $\mathfrak{T}_1$ vertauschbar ist, folgt (149) aus (150).

Wenn nicht alle Eigenwerte verschieden sind, so zerfallen $\mathfrak{F}'$ und $\mathfrak{F}_1'$ in gleicher Weise in „Kästchen": sind f_{ik}' die Koeffizienten von $\mathfrak{F}'$, so ist $f_{ik}' \neq 0$ für $i_1 \leqq i \leqq i_2$ und $k_1 \leqq k \leqq k_2$; dagegen $f_{ik}' = 0$ für $i < i_1$ oder $i > i_2$ und $k_1 \leqq k \leqq k_2$ sowie für $i_1 \leqq i \leqq i_2$ und $k < k_1$ oder $k > k_2$. Dabei sind diese Indexintervalle die größten der Art, daß bei geeigneter Numerierung der Eigenwerte $\tau_{i_1} = \cdots = \tau_{i_2}$, $\tau_{k_1} = \cdots = \tau_{k_2}$ usw. ist. Wie im Falle von lauter verschiedenen Eigenwerten kann man $\mathfrak{F}_1'$ mittels einer Matrix $\mathfrak{D}$ in $\mathfrak{F}'$ überführen, welche aus lauter quadratischen Kästchen längs der Hauptdiagonalen besteht, deren Kantenlängen $i_2 - i_1 + 1$, $k_2 - k_1 + 1$ usw. sind. Die Matrix $\mathfrak{D}$ ist dann wieder mit $\mathfrak{T}_1'$ vertauschbar, und der Beweis kann wie oben zu Ende geführt werden.

Nun sei k_0 ein endlicher Körper und alle τ_i seien verschieden. Zunächst werde $\mathfrak{T}$ in k_0 gemäß Hilfssatz 11 vollständig ausreduziert, wobei gleichzeitig $\mathfrak{F}$ eine Summe von variablenfremden Teilformen wird. Dabei zerfällt auch $\mathfrak{F}_1$ automatisch in gleicher Weise in variablenfremde Teilformen, wie man sofort einsieht, wenn man die einzelnen irreduziblen Bestandteile von $\mathfrak{T}_1$ kästchenweise auf Diagonalform transformiert und dann feststellt, daß $\mathfrak{F}'$ und $\mathfrak{F}_1'$ nur an entsprechenden Stellen von Null verschiedene Koeffizienten haben. Aus diesem Grunde genügt es, die letzte Behauptung von Satz 13 für irreduzible Transformatoren zu beweisen.

Es möge sich zuerst um irreduzible reguläre Transformatoren handeln. Man transformiere $\mathfrak{F}_1$ mittels einer Matrix $\mathfrak{C}$, deren Spalten als algebraisch konjugiert bezüglich k_0 angenommen werden dürfen, in die Gestalt (144). Dann kann man $\mathfrak{F}'$ nach Nr. 3 in der Gestalt (146) voraussetzen, und auch $\mathfrak{F}_1'$ hat diese Gestalt mit v_i^* an Stelle von v_i. Da k_0 ein endlicher Körper sein sollte, ist jetzt $\frac{v_i}{v_i^*}$ die Norm einer Zahl μ_i aus $k_i' = k_0(\tau_i)$ bezüglich $k_i = k_0\left(\tau_i + \frac{t}{\tau_i}\right)$. Dann leistet die Matrix

$$\mathfrak{D} = \begin{pmatrix} \mu_1 & & & \\ & \ddots & & \\ & & \mu_m & \\ & & & \mu_1' \\ & & & & \ddots \\ & & & & & \mu_m' \end{pmatrix},$$

wo μ_i' zu μ_i bezüglich k_i konjugiert ist, die Transformation (151). $\mathfrak{C}\mathfrak{D}\mathfrak{C}^{-1}$ hat Koeffizienten in k_0, da die Spalten von $\mathfrak{C}$ bezüglich k_0 konjugiert sind, die Koeffizienten der oben konstruierten Matrix $\mathfrak{S}$ fallen also in k_0.

Endlich möge $\mathfrak{T}_1$ die Eigenwerte $\pm\sqrt{t}$ haben. Wenn t eine Quadratzahl in k_0 ist, so haben $\mathfrak{T}_1$ und $\mathfrak{T}_2$ als irreduzible Transformatoren die Reihenzahl 1, so daß nichts mehr zu beweisen ist. Ist t keine Quadratzahl, so haben $\mathfrak{T}_1$ und $\mathfrak{T}_2$ die Reihenzahl 2. Jetzt ist $\mathfrak{F} \simeq x^2 - t\,y^2$. Sämtliche Transformatoren dieser Form sind von der Art, daß sie $\xi = x + y\sqrt{t}$ mit einer Zahl $r + s\sqrt{t}$ multiplizieren und eventuell $\sqrt{t}$ mit $-\sqrt{t}$ vertauschen. Die einzigen Transformatoren mit den Eigenwerten $\pm\sqrt{t}$ sind

$$\begin{pmatrix} & \pm t \\ \pm 1 & \end{pmatrix},$$

für welche man die Behauptung direkt verifizieren kann.

§ 13. Die Einheiten indefiniter Formen

1. Von hier ab bis zum Schluß folge ich einem schon früher skizzierten Gedankengang[24]), der aber in einigen Punkten zu berichtigen ist. Gefragt wird nach dem Restverhalten der Einheiten indefiniter Stammformen nach Primzahlen und nach der Klassenzahl der Transformatoren oder der Formen. Beide Fragen stehen in engem Zusammenhang. Im Falle von Quaternionenalgebren und ihren Normenformen handelt es sich um eine Fragestellung, die sowohl in der Sprache der Algebrentheorie wie in der Sprache der Formentheorie formuliert und gelöst werden kann. Bekanntlich wurde zuerst in der Formentheorie bewiesen, daß die Klassenzahl in einem Geschlecht gleich eins ist[8]). Auf die Anregung von Herrn Brandt hin wurde dann von mir ein neuer Beweis mit Mitteln der Algebrentheorie gesucht und gefunden, der sich als tragfähig für alle normalen einfachen Algebren erwies. Dieser Beweisgedanke soll nun in die Sprache der Formentheorie zurückübersetzt werden. Daß dieses, wenn auch noch mit einigen Schwierigkeiten möglich ist, ist eine schöne Bestätigung der mehrfach ausgesprochenen These, daß Algebrentheorie und Formentheorie eng verwandt sind.

Die Einheiten $\mathfrak{U}_p$ von $\mathfrak{F}$ mod p (s. § 8, Nr. 1) mit $|\mathfrak{U}_p| \equiv 1 \bmod p$ bilden eine Gruppe $O(\mathfrak{F})$, die im wesentlichen einfach ist. Im einzelnen gilt folgendes[25]): p sei teilerfremd zu $2D(\mathfrak{F})$, die Variablenzahl n sei stets größer als 2. Dann besteht das Zentrum Z_n von $O(\mathfrak{F})$ aus den Matrizen $\pm\mathfrak{E}^{(n)}$ bei geradem n, sonst nur aus dem Einselement. Die Einheiten mod p permutieren die „Punkte" der „Fläche" $\frac{1}{2}\dot{\mathfrak{x}}\,\mathfrak{F}\,\mathfrak{x} \equiv 1 \bmod p$. Diejenigen $\mathfrak{U}_p$, welche eine gerade Permutation dieser Punkte hervorrufen, bilden eine Untergruppe $O_1(\mathfrak{F})$ vom Index 2 in $O(\mathfrak{F})$. Wenn $n > 4$ ist, so ist die Faktorgruppe $O_1(\mathfrak{F})/(Z_n \cap O_1(\mathfrak{F}))$ einfach.

Für $n = 3$ und $n = 4$ herrschen besondere Verhältnisse. Für $n = 4$ werde $\left(\frac{D}{p}\right) = 1$ angenommen, was besonders bequem aber nicht unbedingt notwendig ist; $\mathfrak{F}$ ist dann der Form $x_1 x_2 - x_3 x_4 \bmod p$ äquivalent. Es bezeichne L_2 die Gruppe der nichtsingulären zweireihigen Matrizen $\mathfrak{M}^{(2)}$ mod p, L_2' die Gruppe derjenigen $\mathfrak{M}^{(2)}$, deren Determinante mod p ein quadratischer Rest ist, $\mathfrak{L}_2$ die Gruppe der $\mathfrak{M}^{(2)}$ mit $|\mathfrak{M}^{(2)}| \equiv 1 \bmod p$, Z_2 die Gruppe der $\mathfrak{M}^{(2)} \equiv \mu\,\mathfrak{E}^{(2)} \bmod p$. Es ist offenbar $L_2' \cong Z_2 \times \mathfrak{L}_2$.

---

[24]) A. a. O.[10]). Zur Zeit der Abfassung dieser Note war ich Soldat und von jeder Literatur abgeschnitten. Dabei habe ich einen Satz über die Einfachheit der orthogonalen Gruppen mod p aus dem Gedächtnis falsch zitiert. Die Überlegungen von damals sind daher nur als grobe Skizze aufrechtzuerhalten und werden hier nun lückenlos ausgeführt.

[25]) s. [20]), §§ 6, 7.

Mit diesen Bezeichnungen ist für $n = 3 : O(\mathfrak{F}) \cong L_2/Z_2, O_1(\mathfrak{F}) \cong L_2'/Z_2 \cong \mathfrak{L}_2$. Für $n = 4$ ist $O(\mathfrak{F})$ isomorph mit der Gruppe von Paaren $\mathfrak{M}_1^{(2)}$, $\mathfrak{M}_2^{(2)}$ aus L_2, deren Determinanten das Produkt 1 mod p ergeben. Eine Untergruppe $O'(\mathfrak{F})$ vom Index 2 erhält man, wenn $\mathfrak{M}_1^{(2)}$ und $\mathfrak{M}_2^{(2)}$ aus L_2 genommen werden, und dann ist $O'(\mathfrak{F}) = \mathfrak{L}_2 \times \mathfrak{L}_2$. Es ist $O'(\mathfrak{F}) = O_1(\mathfrak{F})$; denn sowohl $O'(\mathfrak{F})$ wie $O_1(\mathfrak{F})$ enthalten die Quadrate sämtlicher Elemente aus $O(\mathfrak{F})$, und da $O'(\mathfrak{F})$ das direkte Produkt zweier einfacher Gruppen ist, wird $O'(\mathfrak{F})$ durch die Quadrate sämtlicher Elemente von $O(\mathfrak{F})$ erzeugt; es gilt also $O'(\mathfrak{F}) \supset O_1(\mathfrak{F})$ und folglich $O'(\mathfrak{F}) = O_1(\mathfrak{F})$, da $O_1(\mathfrak{F})$ in $O(\mathfrak{F})$ den Index 2 hat. Für $n = 4$ ist also $O_1(\mathfrak{F})$ das direkte Produkt zweier einfacher Gruppen, die beide mit der orthogonalen Gruppe $O_1(\mathfrak{F})$ für $n = 3$ isomorph sind.

Das nächste Ziel ist nun der folgende wichtige

Hilfssatz 12. *Es sei $\mathfrak{F}$ eine indefinite Stammform der Diskriminante D in $n > 2$ Variablen, p eine zu $2D$ teilerfremde Primzahl und $\mathfrak{U}_p$ eine Einheit von $\mathfrak{F}$ mod p aus der Untergruppe $O_1(\mathfrak{F})$; für $n = 4$ werde noch $\left(\frac{D}{p}\right) = 1$ vorausgesetzt. Nimmt man eventuell endlich viele Primzahlen p aus, so gibt es jetzt eine Einheit $\mathfrak{U}$ von $\mathfrak{F}$, welche der Kongruenz*

$$\mathfrak{U} \equiv \mathfrak{U}_p \bmod p$$

genügt.

Es bleibt die Frage offen, welche der Voraussetzungen wohl entbehrlich sein könnten. Zunächst darf man die Einschränkung fallen lassen, daß die Behauptung für endlich viele Ausnahmeprimzahlen nicht zutreffen könnte. Jedoch müßte man dazu ein tiefer eindringendes Beweisverfahren verwenden, während hier gerade besonderer Wert auf Kürze gelegt wird. Wahrscheinlich ist $\left(\frac{D}{p}\right) = 1$ im Falle $n = 4$ entbehrlich, ohne diese Voraussetzung wird nur die Struktur der Gruppe $O(\mathfrak{F})$ noch unübersichtlicher. Vermutlich gilt der Satz auch dann, wenn p in D aufgeht. Dagegen kann die Voraussetzung, daß der Untergruppe $O_1(\mathfrak{F})$ angehören soll, zwar gegebenenfalls durch eine andere ersetzt aber nicht einfach fallen gelassen werden[26]).

2. Zur Vorbereitung auf den Beweis dient der folgende

Hilfssatz 13. Es sei p eine zu $2D$ teilerfremde Primzahl und $\mathfrak{U}_p$ eine Einheit mod p. Dann gibt es einen Transformator $\mathfrak{T}$ von $\mathfrak{F}$ der Norm 1 mit

$$\mathfrak{T} \equiv \mathfrak{U}_p \bmod p \ .$$

[26]) Für $n = 3$ gilt: diese Voraussetzung ist dann und nur dann entbehrlich, wenn es unter den Primteilern der Diskriminante und der Zahl -1 einen quadratischen Nichtrest mod p gibt.

Beweis. Ich knüpfe an eine bekannte Parameterdarstellung der Einheiten quadratischer Formen an. Führt man mittels

$$\mathfrak{M}^* = \mathfrak{F}^{-1}\,\dot{\mathfrak{M}}\,\mathfrak{F}$$

eine allgemeine Matrizenoperation ein, so gilt

$$\mathfrak{U}_p^{-1} \equiv \mathfrak{U}^* \bmod p\ . \tag{152}$$

$\mathfrak{U}_p$ möge nicht den Eigenwert $-1 \bmod p$ haben, dann läßt sich

$$\mathfrak{C}_p \equiv (\mathfrak{E} - \mathfrak{U}_p)(\mathfrak{E} + \mathfrak{U}_p)^{-1} \bmod p$$

bilden, und aus (152) folgt

$$\mathfrak{C}_p^* \equiv -\,\mathfrak{C}_p \bmod p$$

und

$$\mathfrak{U}_p \equiv (\mathfrak{E} + \mathfrak{C}_p)^{-1}(\mathfrak{E} - \mathfrak{C}_p) \bmod p\ .$$

Es sei nun $\mathfrak{C} \equiv \mathfrak{C}_p \bmod p$ eine Matrix mit rationalen Koeffizienten, welche der Gleichung $\mathfrak{C}^* = -\,\mathfrak{C}$ genügt. Dann ist

$$\mathfrak{T} = (\mathfrak{E} + \mathfrak{C})^{-1}(\mathfrak{E} - \mathfrak{C})$$

ein Transformator von $\mathfrak{F}$ der im Hilfssatz verlangten Art.

Jetzt möge $\mathfrak{U}_p$ den Eigenwert $-1 \bmod p$ genau a-mal haben. Dann gibt es nach Hilfssatz 11 eine Matrix $\mathfrak{S}$, so daß

$$\mathfrak{S}^{-1}\mathfrak{U}_p\mathfrak{S} \equiv \begin{pmatrix} \mathfrak{V}_p^{(n-a)} & \\ & -\,\mathfrak{E}^{(a)} \end{pmatrix} \bmod p\ ,\quad \mathfrak{F}' = \dot{\mathfrak{S}}\mathfrak{F}\mathfrak{S} \equiv \begin{pmatrix} \mathfrak{G}^{(n-a)} & \\ & \mathfrak{H}^{(a)} \end{pmatrix} \bmod p \tag{153}$$

ist, wo $\mathfrak{V}_p^{(n-a)}$ eine Einheit von $\mathfrak{G}^{(n-a)} \bmod p$ ist. Es sei

$$\mathfrak{F}' = \begin{pmatrix} \mathfrak{G}^{(n-a)} & \mathfrak{h}^{(n-a,a)} \\ \dot{\mathfrak{h}} & \mathfrak{H}^{(a)} \end{pmatrix}\ ,\quad \mathfrak{S}' = \begin{pmatrix} \mathfrak{E}^{(n-a)} & \\ -\,\mathfrak{H}^{-1}\dot{\mathfrak{h}} & \mathfrak{E}^{(a)} \end{pmatrix}\ ,\quad (\mathfrak{H} = \mathfrak{H}^{(a)})\ ,$$

dabei ist $\mathfrak{H}^{-1}\dot{\mathfrak{h}} \equiv \mathfrak{o}^{(a,n-a)} \bmod p$. Man kann nun $\mathfrak{S}$ durch $\mathfrak{S}\mathfrak{S}'$ ersetzen; die erste Kongruenz (153) bleibt dabei bestehen, an Stelle der zweiten tritt sogar die Gleichheit:

$$\dot{\mathfrak{S}}\mathfrak{F}\mathfrak{S} = \begin{pmatrix} \mathfrak{G}^{(n-a)} & \\ & \mathfrak{H}^{(a)} \end{pmatrix}\ .$$

Nach dem bereits Bewiesenen gibt es jetzt einen Transformator $\mathfrak{T}^{(n-a)}$ für $\mathfrak{G}^{(n-a)}$ mit

$$\mathfrak{T}^{(n-a)} \equiv \mathfrak{B}_p^{(n-a)} \bmod p \ ,$$

und jetzt ist

$$\mathfrak{T} = \mathfrak{T}^{(n)} = \mathfrak{S} \begin{pmatrix} \mathfrak{T}^{(n-a)} & \\ & -\mathfrak{E}^{(a)} \end{pmatrix} \mathfrak{S}^{-1}$$

ein Transformator von $\mathfrak{F}$ der verlangten Art.

3. Nun der Beweis für Hilfssatz 12, zunächst im Falle $n \neq 4$. Es durchlaufe $\mathfrak{U}_p$ die Gruppe $O(\mathfrak{F})$, $\mathfrak{T}_1, \ldots, \mathfrak{T}_N$ seien die hierzu gemäß Hilfssatz 13 konstruierten Transformatoren von $\mathfrak{F}$ und T eine ganze Zahl derart, daß $T\mathfrak{T}_1, \ldots, T\mathfrak{T}_N$ ganz sind.

Die Gruppe E der Einheiten von $\mathfrak{F}$ ist bekanntlich unendlich. Die „Hauptkongruenzuntergruppe" E_T der Einheiten $\mathfrak{U} \equiv \mathfrak{E}^{(n)} \bmod T^n$ hat in E einen endlichen Index, sie ist also auch eine unendliche Gruppe. Es gibt nun höchstens endlich viele Primzahlen p derart, daß jede Einheit $\mathfrak{U}$ aus $\mathfrak{E}_T$ einer der Kongruenzen $\mathfrak{U} \equiv \pm \mathfrak{E}^{(n)} \bmod p$ genügt. Es sei p eine Primzahl, für welche dies nicht zutrifft und $\mathfrak{U}$ eine Einheit von $\mathfrak{F}$, welche den Kongruenzen

$$\mathfrak{U} \not\equiv \pm \mathfrak{E}^{(n)} \bmod p \ , \qquad \mathfrak{U} \equiv \mathfrak{E}^{(n)} \bmod T^n \tag{154}$$

genügt. Dann erzeugt $\mathfrak{U}$ mitsamt allen Konjugierten $\mathfrak{U}_i = \mathfrak{T}_i^{-1} \mathfrak{U} \mathfrak{T}_i$ und eventuell $-\mathfrak{E}^{(n)}$ die ganze Gruppe $O(\mathfrak{F})$ oder wenigstens $O_1(\mathfrak{F})$, da letztere, mod ihrem Zentrum genommen, einfach ist. Wegen (154) sind die $\mathfrak{U}_i$ ganz, womit der Hilfssatz 12 für $n \neq 4$ bewiesen ist.

4. Um den Hilfssatz 12 auch für $n = 4$ zu beweisen, mache ich zunächst auf Folgendes aufmerksam: wird die Zahl T in Nr. 3 noch mit einer ganzen Zahl S multipliziert, so ergibt die Schlußweise die Existenz einer Einheit $\mathfrak{U}$ von $\mathfrak{F}$, welche bei gegebenem $\mathfrak{U}_p$ den beiden Kongruenzen

$$\mathfrak{U} \equiv \mathfrak{U}_p \bmod p \ , \qquad \mathfrak{U} \equiv \mathfrak{E}^{(n)} \bmod S^n$$

genügt.

Es sei nun $\mathfrak{F}$ eine Stammform in 4 Variablen. Es gibt eine Substitution $\mathfrak{S}$, welche $\mathfrak{F}$ in eine Diagonalform transformiert. Durch Streichung einer Variablen kann man auf mindestens zwei Arten eine ternäre indefinite Form erhalten, diese werden durch ein $\mathfrak{S}'$ in ein Vielfaches einer Stammform transformiert, so daß $\mathfrak{S}_1 = \mathfrak{S}\mathfrak{S}'$ folgendes leistet:

$$\dot{\mathfrak{S}}_1 \mathfrak{F} \mathfrak{S} = \begin{pmatrix} t_1 \mathfrak{F}_1 & \\ & 2f_1 \end{pmatrix} ,$$

wo $\mathfrak{F}_1$ eine indefinite Stammform ist. Es gibt also mindestens zwei solche

Transformationen $\mathfrak{S}_1$, $\mathfrak{S}_2$, welche auf die beschriebene Art je eine ternäre indefinite Stammform $\mathfrak{F}_1$, $\mathfrak{F}_2$ abspalten, und zwar so, daß $\mathfrak{F}_1$ und $\mathfrak{F}_2$ nicht drei gemeinsame Variable haben.

Nun sei s eine ganze Zahl der Art, daß $s\,\mathfrak{S}_1$ und $s\,\mathfrak{S}_2$ ganzzahlig sind, und S sei das Produkt der Determinanten $|\,s\,\mathfrak{S}_1\,|$ und $|\,s\mathfrak{S}_2\,|$. Nachdem der Hilfssatz 12 für ternäre Formen schon bewiesen ist und sogar mit der eben erwähnten Erweiterung, liefern die Restklassen mod p der Einheiten $\mathfrak{U}_1$, $\mathfrak{U}_2$ von $\mathfrak{F}_1$, $\mathfrak{F}_2$, welche den Kongruenzen

$$\mathfrak{U}_1 \equiv \mathfrak{U}_2 \equiv \mathfrak{E}^{(3)} \bmod S \tag{155}$$

genügen, bereits die vollen Gruppen $O_1(\mathfrak{F}_1)$, $O_1(\mathfrak{F}_2)$.

Wegen (155) sind

$$\mathfrak{V}_1 = \mathfrak{S}_1 \begin{pmatrix} \mathfrak{U}_1 & \\ & 1 \end{pmatrix} \mathfrak{S}_1^{-1}\,, \qquad \mathfrak{V}_2 = \mathfrak{S}_2 \begin{pmatrix} \mathfrak{U}_2 & \\ & 1 \end{pmatrix} \mathfrak{S}_2^{-1}$$

Einheiten von $\mathfrak{F}$. Die $\mathfrak{V}_1$, $\mathfrak{V}_2$ erzeugen, mod p genommen, mit $O_1(\mathfrak{F})$ bzw. $O_1(\mathfrak{F}_2)$ isomorphe Untergruppen $\overline{O}_1$, $\overline{O}_2$ von $O(\mathfrak{F})$, und zwar sind $\overline{O}_1$ und $\overline{O}_2$ verschieden. Da nun $O_1(\mathfrak{F})$ ein direktes Produkt zweier einfachen Gruppen ist, erzeugen $\overline{O}_1$ und $\overline{O}_2$ die Gruppe $O_1(\mathfrak{F})$, wenn nicht sogar die ganze Gruppe $O(\mathfrak{F})$. Damit ist der Hilfssatz 12 vollständig bewiesen.

§ 14. Das Normenäquivalenzkriterium und der Satz von A. Meyer

1. Als das *Normenäquivalenzkriterium* bezeichne ich den

Satz 14. *Zwei Transformatoren $\mathfrak{T}_{12}$, $\mathfrak{T}_{13}$, welche links zu derselben indefiniten Stammform $\mathfrak{F}$ in $n>3$ Variablen gehören, sind dann und nur dann äquivalent, wenn sie zum gleichen Geschlecht gehören.*

Wann die Voraussetzung des Satzes zutrifft, kann man nach § 7 (Gl. (59)) durch Vergleich des quadratischen Restverhaltens der Normen nach den ungeraden Diskriminantenprimteilern erster Art feststellen, womit der Name des Satzes gerechtfertigt ist. Gleichzeitig soll er an den oben erwähnten Satz aus der Algebrentheorie erinnern. Mit dem Normenäquivalenzkriterium gleichbedeutend ist der Satz von A. Meyer [8]:

Satz 15. *Zwei indefinite Stammformen des gleichen Geschlechts in $n>3$ Variablen sind äquivalent.*

Meyer beweist diesen Satz zwar für eine weitere Gesamtheit von Formen, jedoch haben seine einschränkenden Voraussetzungen über die Ord-

nungsinvarianten zur Folge, daß der Beweis für Stammform nicht gültig ist. Er beweist den Satz zunächst für $n = 3$ und überträgt das Ergebnis dann von n auf $n + 1$.

In diesem Zusammenhang besteht die Möglichkeit, den Beweis auf zweierlei Art zu führen. Erstens kann man den Satz zunächst für $n = 3$ auf Grund des bekannten Zusammenhanges zwischen Quaternionenalgebren und ternären Formen[27]) auf das Normenäquivalenzkriterium für Quaternionenalgebren stützen und dann mit Meyer vollständige Induktion durchführen. Will man aber das Normenäquivalenzkriterium im hyperkomplexen Falle nicht voraussetzen, so kann man einen zweiten Weg gehen, den ich auch hier einschlagen werde: der Satz wird gleich für beliebiges gerades n bewiesen. Für ungerades $n > 4$ ist dann wieder vollständige Induktion anzuwenden, für die ich auf Meyer verweise[28]). Für $n = 3$ kann der bekannte Zusammenhang zwischen ternären Formen der Diskriminante D und quaternären Formen der Diskriminante D^2 ausgenutzt werden[27]).

2. Dem Beweis der Sätze 14 und 15 ist ein Hilfssatz vorauszuschicken; es mögen dabei alle ungeraden Primzahlen p mit $\left(\frac{D}{p}\right) = 1$, $p \equiv 3 \bmod 4$ *zulässig* heißen, die nicht in der in Hilfssatz 12 genannten Ausnahmemenge vorkommen.

Hilfssatz 14. Für zwei verwandte Stammformen $\mathfrak{F}_1$, $\mathfrak{F}_2$ der gemeinsamen Diskriminante D und der geraden Variablenzahl $n = 2m$ gibt es eine Substitution $\mathfrak{S}$ mit

$$\mathfrak{F}_1 = \dot{\mathfrak{S}}\, \mathfrak{F}_2\, \mathfrak{S} \;, \tag{156}$$

deren Koeffizienten nur zulässige Primzahlen und Potenzprodukte von solchen als Nenner haben (im Falle $n = 2$ sei $D \neq -4$).

Beweis. Es sei zunächst $m = 1$. Dann stellen $\mathfrak{F}_1$ und $\mathfrak{F}_2$ die Normen der Ideale aus je einer Idealklasse des quadratischen Zahlkörpers $k_0(\sqrt{D})$ dar, diese beiden Klassen gehören dem gleichen Geschlecht an. Die Ideale $\mathfrak{f}_1$, $\mathfrak{f}_2$ mögen diese Klassen repräsentieren, dann gilt nach dem Hauptgeschlechtssatz

$$\mathfrak{f}_1 \sim \mathfrak{f}_2\, \mathfrak{s}^{1-\sigma} \;, \tag{157}$$

---

[27]) *H. Brandt*, Zur Zahlentheorie der Quaternionen, Jahresbericht Deutsche Math.-Vereing. **53** (1943), S. 23—57.

[28]) s. die letzte unter [8]) zitierte Arbeit. Ich setze dabei voraus, daß sich Meyers Schlußweise, die zunächst nicht für Stammformen ausgeführt wird, auf diese übertragen läßt. Leider ist mir die Arbeit nicht zugänglich. Jedoch habe ich selber einen Gedankengang für die vollständige Induktion, der das Verlangte leistet.

wo σ der Automorphismus von $k_0(\sqrt{D})$ ist, der $\sqrt{D}$ und $-\sqrt{D}$ vertauscht. Zu zeigen ist, daß (157) mit einem ganzen Ideal $\mathfrak{s}$ gilt, dessen Norm aus lauter zulässigen Primzahlen zusammengesetzt ist. Die durch das Ideal $\mathfrak{s}$ bestimmte Klasse enthält nun unendlich viele Primideale ersten Grades. Wird $\mathfrak{s}$ als ein solches genommen, nach welchem -1 ein quadratischer Nichtrest ist, und das zu den endlich vielen Ausnahmen nicht gehört, so ist seine Norm eine zulässige Primzahl, denn es ist ja $\left(\frac{D}{n(\mathfrak{s})}\right) = 1$, und der Hilfssatz ist für $m = 1$ bewiesen.

Allgemein wird der Beweis mittels vollständiger Induktion bezüglich m geführt. Ich benutze dabei, daß jede primitive binäre Form unendlich viele Primzahlen darstellt; und dieses sieht man bekanntlich so ein: die Form stellt die Normen von Ringidealen für einen (eventuell von der Hauptordnung verschiedenen) Ring ganzer Zahlen aus einem quadratischen Zahlkörper dar. Die Ringideale bilden eine Gruppe[29]), ihre Klassen bilden eine endliche Gruppe, und die analytische Schlußweise, daß jede Idealklasse unendlich viele Primideale ersten Grades enthält, ist allgemein für Ringideale gültig. Da offenbar jede primitive Form in $n \geqq 2$ Variablen eine primitive binäre Form darstellt, so stellt eine jede solche Form in $n \geqq 2$ Variablen unendlich viele Primzahlen dar. Bei indefiniten Formen kann man auch noch deren Vorzeichen vorschreiben.

Einer Form in n Variablen wird folgendermaßen eine *adjungierte Form* $\tilde{\mathfrak{F}}$ zugeordnet: die Matrix $\tilde{\mathfrak{F}}$ ist die Matrix der $(n-1)$-reihigen Unterdeterminanten von $\mathfrak{F}$, falls n gerade ist, bei ungeradem n dagegen die doppelt genommene Matrix der $(n-1)$-reihigen Unterdeterminanten. Es ist also $\tilde{\tilde{\mathfrak{F}}} = |\mathfrak{F}|\mathfrak{F}$ bzw. $= 4|\mathfrak{F}|\mathfrak{F}$, je nachdem ob n gerade oder ungerade ist. Die adjungierte Form einer Stammform ist stets ganzzahlig und primitiv. Zu jeder Darstellung einer Zahl d durch $\tilde{\mathfrak{F}}$ gehört eine Darstellung einer Form $\mathfrak{G}$ in $n-1$ Variablen durch $\mathfrak{F}$, deren Diskriminante $-(-1)^{\frac{n}{2}} d$ bzw. $(-1)^{\frac{n-1}{2}} d$ ist.

Wenn nun $\mathfrak{F}_1$, $\mathfrak{F}_2$ die beiden gegebenen Stammformen in n Variablen sind, so stellen ihre adjungierten Formen je eine ungerade Primzahl dar, sie stellen selbst also je eine Form $\mathfrak{F}_1^{(n-1)}$, $\mathfrak{F}_2^{(n-1)}$ in $n-1$ Variablen von Primzahldiskr minante dar. Sind $\mathfrak{F}_1$, $\mathfrak{F}_2$ indefinit, so kann man durch geeignete Vorgabe des Vorzeichens der Diskriminanten von $\mathfrak{F}_1^{(n-1)}$, $\mathfrak{F}_2^{(n-1)}$ erreichen, daß diese Formen wieder indefinit sind. Sind jedoch

---

[29]) *Dirichlet-Dedekind*, Vorlesungen über Zahlentheorie, 4. Aufl. Braunschweig 1894, § 187.

$\mathfrak{F}_1, \mathfrak{F}_2$ definit, so sind auch $\mathfrak{F}_1^{(n-1)}$, $\mathfrak{F}_2^{(n-1)}$ definit, jedoch von gleichem Vorzeichen. Die Formen $\widetilde{\mathfrak{F}_1^{(n-1)}}$, $\widetilde{\mathfrak{F}_2^{(n-1)}}$ sind wieder primitiv, also stellen $\mathfrak{F}_1^{(n-1)}$, $\mathfrak{F}_2^{(n-1)}$ je eine Form $\mathfrak{F}_1^{(n-2)}$, $\mathfrak{F}_2^{(n-2)}$ in $n-2$ Variablen und von Primzahldiskriminante dar, usw. Man kommt so zu zwei ternären Formen $\mathfrak{F}_1^{(3)}$, $\mathfrak{F}_2^{(3)}$ mit den Diskriminanten q_1, q_2, wo $|q_1|$, $|q_2|$ zwei verschiedene ungerade Primzahlen sind. Es beschränkt die Allgemeinheit nicht, wenn man annimmt, daß $\mathfrak{F}_1^{(3)}$, $\mathfrak{F}_2^{(3)}$ nicht definit von entgegengesetztem Vorzeichen sind.

Dieselbe Schlußweise zeigt, daß $\mathfrak{F}_1^{(3)}$, $\mathfrak{F}_2^{(3)}$ je eine binäre Form $\mathfrak{G}_1$, $\mathfrak{G}_2$ darstellen, deren Diskriminanten ungerade Primzahlen sind. Dann stellen $\mathfrak{G}_1$, $\mathfrak{G}_2$ je eine Primzahl p_1, $p_2 \neq p_1$ dar, wobei

$$p_1 q_1 \equiv p_2 q_2 \equiv 1 \bmod 4 \tag{158}$$

ist. Die Zahlen p_1, p_2 werden auch durch $\mathfrak{F}_1^{(3)}$, $\mathfrak{F}_2^{(3)}$ dargestellt. Somit stellen $\widetilde{\mathfrak{F}_1^{(3)}}$, $\widetilde{\mathfrak{F}_2^{(3)}}$ je eine binäre Form $\mathfrak{H}_1$, $\mathfrak{H}_2$ der Diskriminanten $-4p_1q_1$, $-4p_2q_2$ dar, das sind nach (158) Stammdiskriminanten, $\mathfrak{H}_1$, $\mathfrak{H}_2$ sind also Stammformen. Wieder darf man ohne Beschränkung der Allgemeinheit annehmen, daß $\mathfrak{G}_1$, $\mathfrak{G}_2$ und $\mathfrak{H}_1$, $\mathfrak{H}_2$ nicht definit von entgegengesetztem Vorzeichen sind.

Jetzt behaupte ich, $\mathfrak{H}_1$, $\mathfrak{H}_2$ stellen gemeinsam eine zulässige Primzahl p dar: Die durch $\mathfrak{H}_1$, $\mathfrak{H}_2$ dargestellten ungeraden Zahlen sind als negativ genommene binäre Diskriminanten $\equiv 3 \bmod 4$, mithin gehören $\mathfrak{H}_1$, $\mathfrak{H}_2$ einem der 2-adischen Typen Θ^2, Θ_*^2 an. Die Form

$$\mathfrak{H}(x_1, x_2, x_3, x_4) = \mathfrak{H}_1(x_1, x_2) - \mathfrak{H}_2(x_3, x_4)$$

gehört also nicht dem Typ T^2 an. Da die ungeraden Diskriminantenprimteiler von $\mathfrak{H}_1$, $\mathfrak{H}_2$ verschieden sind, gehört $\mathfrak{H}$ für kein p zum Typ T^p. Da $\mathfrak{H}_1$, $\mathfrak{H}_2$ nicht definit von entgegengesetztem Vorzeichen sind, ist $\mathfrak{H}$ indefinit. $\mathfrak{H}$ ist also für jede Primstelle mit einer Form in weniger als 4 Variablen ähnlich und stellt daher nach dem II. Hauptsatz die Null eigentlich dar. Es gibt folglich eine durch $\mathfrak{H}_1$, $\mathfrak{H}_2$ gemeinsam dargestellte ganze Zahl h.

Nun stellen $\mathfrak{H}_1$, $\mathfrak{H}_2$ die Normen der Ideale aus je einer Idealklasse der quadratischen Zahlkörper

$$k_1 = k_0\left(\sqrt{D(\mathfrak{H}_1)}\right), \qquad k_2 = k_0\left(\sqrt{D(\mathfrak{H}_2)}\right)$$

dar. Es gibt je einen Repräsentanten $\mathfrak{h}_1$, $\mathfrak{h}_2$ dieser Klassen in k_1, k_2, wobei $n(\mathfrak{h}_1) = n(\mathfrak{h}_2) = h$ ist. Es sei

$$\mathfrak{h}_1 = h_1 \mathfrak{g}_1 \ , \qquad \mathfrak{h}_2 = h_2 \mathfrak{g}_2 \ ,$$

wo h_1, h_2 ganze rationale Zahlen und $\mathfrak{g}_1$, $\mathfrak{g}_2$ ganze primitive Ideale sind. Durch einen gemeinsamen rationalen Teiler darf man $\mathfrak{h}_1$, $\mathfrak{h}_2$ ohne Beschränkung der Allgemeinheit teilen und folglich $(h_1, h_2) = 1$ annehmen. Jetzt behaupte ich, daß es in dem Vereinigungskörper $k = k_1 k_2$ ein Ideal $\mathfrak{h}$ gibt, dessen Normen bezüglich k_1, k_2 gleich $\mathfrak{h}_1$, $\mathfrak{h}_2$ sind. Man setze zum Beweise die obige Zerlegung von $\mathfrak{h}_1$, $\mathfrak{h}_2$ fort:

$$\mathfrak{h}_1 = h_1 \mathfrak{k}_1^2 \mathfrak{l}_1 \ , \qquad \mathfrak{h}_2 = h_2 \mathfrak{k}_2^2 \mathfrak{l}_2 \ ,$$

wobei

$$n_{k_1/k_0}(\mathfrak{k}_1) = h_2 \ , \quad n_{k_2/k_0}(\mathfrak{k}_2) = h_1 \ , \quad n_{k_1/k_0}(\mathfrak{l}_1) = n_{k_2/k_0}(\mathfrak{l}_2)$$

ist, was sich durch Normenvergleich ergibt. Ersichtlich gibt es in k ein Ideal $\mathfrak{l}$ mit

$$n_{k/k_1}(\mathfrak{l}) = \mathfrak{l}_1 \ , \quad n_{k/k_2}(\mathfrak{l}) = \mathfrak{l}_2 \ ,$$

und das verlangte Ideal $\mathfrak{h}$ ist

$$\mathfrak{h} = \mathfrak{k}_1 \mathfrak{k}_2 \mathfrak{l} \ .$$

In der Klasse von $\mathfrak{h}$ in k gibt es nun endlich viele Primideale $\mathfrak{p}$ ersten Grades, nach welchen die Zahl D ein quadratischer Rest und -1 ein quadratischer Nichtrest ist, ihre Normen sind bis auf endlich viele Ausnahmen zulässige Primzahlen p. Die Primideale ersten Grades

$$\mathfrak{p}_1 = n_{k/k_1}(\mathfrak{p}) \ , \quad \mathfrak{p}_2 = n_{k/k_2}(\mathfrak{p}) \qquad (n(\mathfrak{p}_1) = n(\mathfrak{p}_2) = p)$$

sind mit $\mathfrak{h}_1$, $\mathfrak{h}_2$ äquivalent, also stellen $\mathfrak{H}_1$, $\mathfrak{H}_2$ wirklich eine (ja sogar unendlich viele) zulässige Primzahl p gemeinsam dar.

Damit stellen auch $\widetilde{\mathfrak{F}}_1^{(3)}$, $\widetilde{\mathfrak{F}}_2^{(3)}$ eine zulässige Primzahl p gemeinsam dar, also $\mathfrak{F}_1^{(3)}$, $\mathfrak{F}_2^{(3)}$ und damit auch $\mathfrak{F}_1$, $\mathfrak{F}_2$ stellen je eine binäre Form $\mathfrak{F}_1^{(2)}$, $\mathfrak{F}_2^{(2)}$ derselben Primzahldiskriminante p dar. Sind $\mathfrak{F}_1$, $\mathfrak{F}_2$ indefinit, so kann man wiederum das Vorzeichen von p so festlegen, daß auch diese binären Formen indefinit sind; sonst sind sie zusammen mit $\mathfrak{F}_1$, $\mathfrak{F}_2$ definit von gleichem Vorzeichen. $\mathfrak{F}_1^{(2)}$, $\mathfrak{F}_2^{(2)}$ gehören als binäre Formen derselben Primzahldiskriminante und derselben Signatur demselben Geschlecht an.

Es sei

$$\mathfrak{F}_1 = \begin{pmatrix} \mathfrak{F}_1^{(2)} & \mathfrak{f}_1^{(2,n-2)} \\ \dot{\mathfrak{f}}_1 & \mathfrak{G}_1^{(n-2)} \end{pmatrix} \ , \qquad \mathfrak{F}_2 = \begin{pmatrix} \mathfrak{F}_2^{(2)} & \mathfrak{f}_2^{(2,n-2)} \\ \dot{\mathfrak{f}}_2 & \mathfrak{G}_2^{(n-2)} \end{pmatrix} \ .$$

Nun transformiere man $\mathfrak{F}_1$, $\mathfrak{F}_2$ mit

$$\mathfrak{S}_1 = \begin{pmatrix} \mathfrak{E}^{(2)} & -(\mathfrak{F}_1^{(2)})^{-1}\,\mathfrak{f}_1^{(2,n-2)} \\ & \mathfrak{E}^{(n-2)} \end{pmatrix}, \quad \mathfrak{S}_2 = \begin{pmatrix} \mathfrak{E}^{(2)} & -(\mathfrak{F}_2^{(2)})^{-1}\,\mathfrak{f}_2^{(2,n-2)} \\ & \mathfrak{E}^{(n-2)} \end{pmatrix}$$

in

$$\mathfrak{F}_1' = \dot{\mathfrak{S}}_1 \mathfrak{F}_1 \mathfrak{S}_1 = \begin{pmatrix} \mathfrak{F}_1^{(2)} & \\ & \mathfrak{G}_1'^{(n-2)} \end{pmatrix}, \quad \mathfrak{F}_2' = \dot{\mathfrak{S}}_2 \mathfrak{F}_2 \mathfrak{S}_2 = \begin{pmatrix} \mathfrak{F}_2^{(2)} & \\ & \mathfrak{G}_2'^{(n-2)} \end{pmatrix}.$$

Dabei sind $\mathfrak{G}_1'^{(n-2)}$, $\mathfrak{G}_2'^{(n-2)}$ nach dem I. Hauptsatz verwandt. Nach der Induktionsannahme sind $\mathfrak{F}_1'$, $\mathfrak{F}_2'$ durch ein $\mathfrak{S}'$ ineinander transformierbar, wobei nur zulässige Primzahlen als Nenner auftreten. $\mathfrak{S} = \mathfrak{S}_2 \mathfrak{S}' \mathfrak{S}_1^{-1}$ leistet dann die Transformation (156), auch hierbei kommen nur zulässige Nenner vor, da $|\mathfrak{F}_1^{(2)}| = |\mathfrak{F}_2^{(2)}|$ eine zulässige Primzahl sein sollte. Damit ist der Hilfssatz 14 bewiesen.

3. Der Beweis für die Sätze 14 und 15 verläuft nun folgendermaßen: es sei $\mathfrak{S}$ die in Hilfssatz 14 genannte Substitution und T der Hauptnenner ihrer Koeffizienten. Dann ist $\mathfrak{T}_{21} = \mathfrak{S} T$ ein ganzer Transformator der Norm T^2, und T ist aus lauter zulässigen Primzahlen zusammengesetzt. $\mathfrak{T}_{21}$ gestattet also eine Zerlegung

$$\mathfrak{T}_{21} = \mathfrak{P}_{2j_1}\,\mathfrak{P}_{j_1 i_1}\,\mathfrak{P}_{i_1 j_2}\,\mathfrak{P}_{j_2 i_2} \cdots ,$$

in lauter Primtransformatoren ersten Grades, von denen je zwei aufeinanderfolgende immer gleiche Norm haben:

$$N(\mathfrak{P}_{2j_1}) = N(\mathfrak{P}_{j_1 i_1}), \qquad N(\mathfrak{P}_{i_1 j_2}) = N(\mathfrak{P}_{j_2 i_2}), \qquad \text{usw.}$$

Ich werde beweisen, daß die Formen $\mathfrak{F}_2$ und $\mathfrak{F}_{i_1}$, zu denen $\mathfrak{P}_{2j_1}$ und $\mathfrak{P}_{j_1 i_1}$ links und rechts gehören, äquivalent sind. Wiederholung der gleichen Schlußweise ergibt dann die Behauptung.

Es ist also zu beweisen, daß die beiden Linksideale $(\mathfrak{P}_{j_1 i_1}]$, $(\mathfrak{P}_{j_1 2}]$ äquivalent sind, wo $\mathfrak{P}_{j_1 2} = N(\mathfrak{P}_{2j_1})\,\mathfrak{P}_{2j_1}^{-1}$ ist. Hierzu wird der Hilfssatz 6 herangezogen, demzufolge gibt es eine Einheit $\mathfrak{U}_p$ von $\mathfrak{F}_{j_1}$ mod $p = N(\mathfrak{P}_{2j_1})$ derart, daß

$$(\mathfrak{P}_{j_1 i_1}] = (\mathfrak{U}_p\,\mathfrak{P}_{j_1 2}] \tag{159}$$

ist. Die Einheit $\mathfrak{U}_p$ ist hierdurch noch nicht eindeutig festgelegt, sondern nur bis auf rechtsseitige Multiplikation mit einer weiteren Einheit $\mathfrak{V}_p$, für welche

$$(\mathfrak{P}_{j2}] = (\mathfrak{V}_p\,\mathfrak{P}_{j_1 2}]$$

gilt. Nimmt man

$$\mathfrak{F}_{j_1} \equiv \mathfrak{F}_0^{(2m)} \bmod p \ , \qquad \mathfrak{P}_{j_1 2} = \mathfrak{P}_0$$

an (vgl. § 8, Nr. 3), was die Allgemeinheit nicht beeinträchtigt, so hat also $\mathfrak{V}_p$ die Gestalt

$$\mathfrak{V}_p \equiv \begin{pmatrix} \mathfrak{V} & \mathfrak{S} \\ & \mathfrak{W} \end{pmatrix} \bmod p \ ,$$

wo $\mathfrak{V}$, $\mathfrak{S}$, $\mathfrak{W}$ n-reihige Matrizen sind. Ein spezielles $\mathfrak{V}_p$ dieser Art ist

$$\mathfrak{V}_p = \begin{pmatrix} -1 & & & \\ & \mathfrak{E}^{(m-1)} & & \\ & & -1 & \\ & & & \mathfrak{E}^{(m-1)} \end{pmatrix} , \tag{160}$$

es gehört nicht zu der in § 13, Nr. 1 definierten Gruppe $O_1(\mathfrak{F}_{j_1})$. Nämlich auf der Fläche $\frac{1}{2}\dot{\mathfrak{x}}\mathfrak{F}_{j_1}\mathfrak{x} \equiv 1 \bmod p$ liegt stets eine gerade Anzahl von Punkten mit gegebenen Koordinaten x_1, x_{m+1}, ausgenommen wenn $x_1 x_{m+1} = 1 \bmod p$ ist; denn die Punkte lassen sich zu Paaren anordnen, deren Koordinaten $x_2, \ldots, x_m$, $x_{m+2}, \ldots, x_{2m}$ entgegengesetzt gleich mod p sind, dabei ist allein $x_1, O, \ldots, O$, $x_{m+1}, O, \ldots, O$ nicht mit erfaßt. Die Anzahl dieser Ausnahmepunkte ist $p - 1$. Die Einheit (160) vertauscht nun sämtliche Punkte, deren 1-te und $(m+1)$-te Koordinaten x_1, x_{m+1} sind, mit denjenigen, deren entsprechende Koordinaten $-x_1$, $-x_{m+1}$ sind. Als Permutation geschrieben zerfällt also $\mathfrak{V}_p$ in $\frac{p-1}{2}$ + eine gerade Anzahl von Zweierzyklen. Das ist eine ungerade Anzahl, da p als zulässige Primzahl $\equiv 3 \bmod 4$ ist. $\mathfrak{V}_p$ gehört also in der Tat nicht zu $O_1(\mathfrak{F}_{j_1})$. Jetzt kann man gegebenenfalls durch Multiplikation von $\mathfrak{U}_p$ mit $\mathfrak{V}_p$ erreichen, daß $\mathfrak{U}_p$ stets zu $O_1(\mathfrak{F}_{j_1})$ gehört. Dann gibt es nach Hilfssatz 12 stets eine wirkliche Einheit $\mathfrak{U}$ von $\mathfrak{F}$ mit

$$\mathfrak{U} \equiv \mathfrak{U}_p \bmod p \ ,$$

mit ihr gilt ebenfalls (159), es ist also

$$p\,\mathfrak{F}_{i_1} = \dot{\mathfrak{P}}_{j_1 i_1}\,\mathfrak{F}_{j_1}\,\mathfrak{P}_{j_1 i_1} \cong \dot{\mathfrak{P}}_{j_1 2}\,\mathfrak{F}_{j_1}\,\mathfrak{P}_{j_1 2} = p\,\mathfrak{F}_2 \ ,$$

was zu beweisen war.

(Eingegangen den 19. September 1946.)