Zeitschrift: Commentarii Mathematici Helvetici

Herausgeber: Schweizerische Mathematische Gesellschaft

Band: 20 (1947)

Artikel: Grundzüge einer Zahlentheorie der quadratischen Formen im rationalen Zahlenkörper. I.

Autor: Eichler, Martin

DOI: https://doi.org/10.5169/seals-18049

Grundzüge einer Zahlentheorie der quadratischen Formen im rationalen Zahlkörper I.

Von MARTIN EICHLER, Göttingen

Meinem Lehrer HEINRICH BRANDT zum 60. Geburtstag am 8. November 1946 in dankbarer Verehrung gewidmet. Diese Arbeit, die in zwei Teilen erscheinen soll, ist zum großen Teil aus seinen Anregungen erwachsen, mehr als es durch Hinweise auf seine Publikationen zum Ausdruck gebracht werden kann.

Einleitung

Es ist die Aufgabe einer Theorie, die Fülle der Einzeltatsachen eines Wissensgebietes nach ihrem Verhältnis zu wenigen tragenden Fundamentalbegriffen zu ordnen. Diese Fundamentalbegriffe liegen meist nicht offen zutage, sondern man gewinnt sie erst durch Abstraktion. Ein Beispiel hierfür ist die Theorie der binären quadratischen Formen und die aus ihr durch Verallgemeinerung entstandene Zahlentheorie der algebraischen Zahlkörper und der Algebren. Allein die Benennungen der Grundbegriffe wie „irrationale Zahl", „imaginäre Zahl", „Ideal" kennzeichnen schon genügend die Rolle der Abstraktion bei der Entwicklung dieser Gebiete. Während jedoch hier das begriffliche Trägersystem des Gebäudes längst erkannt wurde, hat es lange Zeit gebraucht, bis man auf dem Gebiet der Zahlentheorie der quadratischen Formen beliebiger Variablenzahl ebensoweit war.

Noch in der umfangreichen Gesamtdarstellung von Bachmann (Die Arithmetik der quadratischen Formen, Leipzig und Berlin 1889) findet man meist eine mühsame Betrachtung der einzelnen Erscheinungen. Zahlreiche und wenig übersichtliche Invarianten liefern eine Einteilung der Klassen ganzzahlig äquivalenter Formen in Ordnungen und Geschlechter. Ein auf diesen Unterscheidungsprinzipien gegründeter Weiterbau der Theorie ist bei den schwerfälligen Begriffsbildungen, die manchmal Wesentliches und Unwesentliches nicht genügend zu unterscheiden

erlauben, fast unmöglich. Erst die neuere Zeit hat eine Wandlung gebracht.

Ein einziger Satz von Minkowski, von Hasse in den Jahren 1923|24 erneut aufgegriffen und prägnant formuliert[1]), erlaubt jetzt eine Beherrschung der Theorie, wenn man sich nicht auf ganzzahlige Formen und ganze Werte der Variablen beschränkt, sondern für Koeffizienten und Variable beliebige Zahlen eines Zahlkörpers zuläßt. Hasses gegenüber früher etwas allgemeinere Auffassung des Geschlechtsbegriffes und seine Loslösung vom Ordnungsbegriff brachte eine viel einfachere Theorie der Geschlechter. Gleichzeitig regten Hasses Arbeiten eine Entwicklung an, die in einer Arbeit von Witt im Jahre 1936[2]) ihren Niederschlag fand. Witt bemerkte, daß alle Geschlechtsinvarianten (außer der Variablenzahl) mit der Variablenzahl nicht wesentlich in Beziehung stehen und führte Gesamtheiten von „ähnlichen" Formen ein, welche Formen verschiedener Variablenzahl aber sonst gleicher Geschlechtsinvarianten umfassen[3]). Die Benutzung dieses Begriffes ermöglicht nunmehr einen Aufbau der Geschlechtertheorie in kaum zu übertreffender Eleganz. Hierbei zeigt sich eine Erscheinung, die auch für das Folgende wichtig erscheint: den Gesamtheiten ähnlicher Formen entsprechen gewisse Algebrenklassen im Sinne von R. Brauer, die Theorie der quadratischen Formen tritt hiermit in Beziehung zur Algebrentheorie.

Mit den genannten Arbeiten ist nun erst die algebraische Grundlage für eine Zahlentheorie der quadratischen Formen im eigentlichen Sinne gelegt. Auf ihr wäre unter anderem insbesondere die Lehre von der Darstellung von Zahlen durch Formen und von der Äquivalenz von Formen aufzubauen. Wollte man dies im alten Stile machen, so müßte man jetzt wieder den Anschluß an die alte schwerfällige Geschlechtertheorie suchen

---

[1]) *H. Hasse*, Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen, Journ. reine angew. Math. **152** (1923), S. 129. Über die Äquivalenz von quadratischen Formen im Körper der rationalen Zahlen, ebd. **152** (1923), S. 205. Symmetrische Matrizen im Körper der rationalen Zahlen, ebd. **153** (1924), S. 12. Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper, ebd. **153** (1924), S. 113. Äquivalenz quadratischer Formen in einem beliebigen algebraischen Zahlkörper, ebd. **153** (1924), S. 158.

[2]) *E. Witt*, Theorie der quadratischen Formen in beliebigen Körpern, Journ. reine angew. Math. **176** (1937), S. 31—44.

[3]) Schon vorher hatte *H. Brandt* das Vorteilhafte einer solchen Betrachtungsweise erkannt, allerdings ohne einen geschlossenen Aufbau der Geschlechtertheorie auf dieser Grundlage der Öffentlichkeit vorzulegen: Diskriminante einer quadratischen Form, Verh. Intern. Mathematikerkongreß Zürich 1932, II, S. 10—11; s. besonders die unter [11]) zitierte Arbeit, Nr. 9.

und hätte somit nur geringen Gewinn von den neueren Ergebnissen. Man weiß aber auch, daß sich die Zahlentheorie der Formen vielfach in mancherlei einzelne Teilergebnisse und Verfahren verlief. Nun haben aber gerade in diesem Zusammenhang neuere Arbeiten von Hecke[4]) und Siegel[5]) Tatsachen allgemeiner Gültigkeit aufgezeigt, die früher nicht bemerkt wurden, und die wiederum, und zwar diesmal von ganz anderer Seite her, auf eine gewisse Parallelität zwischen der Formentheorie und der Algebrentheorie hinweisen.

Jetzt sind es zwei Ideen von Brandt, die weiter führen. Seine Zahlentheorie der quaternären Formen hatte im Jahre 1928 den entscheidenden Anstoß zur Entwicklung einer allgemeinen Zahlentheorie der hyperkomplexen Systeme gegeben[6]). Er ging von dem Grundsatz aus, daß die Zahlentheorie sämtlicher Formenklassen einer Ordnung gleichzeitig zu entwickeln sei. Die verschiedenen Klassen einer Ordnung sind verknüpfbar durch lineare Substitutionen, welche eine Form in das Vielfache einer anderen überführen. Solche Substitutionen werden im Falle kompositionsfähiger Formen durch die Kompositionstheorie geliefert, sie entsprechen den Idealen der Algebren. Jedoch ist ihre Existenz durchaus nicht an die Möglichkeit einer Komposition geknüpft. Man hat es hier also mit der sinngemäßen Übertragung des Idealbegriffes aus der Zahlentheorie der Algebren in die Formentheorie zu tun. In zwei kleineren Noten habe ich diesen Begriff bei zwei Aufgaben benutzt: Erstens versuchte ich mit seiner Hilfe, die genannte Entdeckung von Hecke über die Darstellung von Zahlen durch gewisse Systeme definiter quadratischer Formen begrifflich zu klären, was damals, wenn auch nur in bescheidenem Umfang gelang[7]). Zweitens zeigte ich, wie dieser Begriff es erlaubt, einen gewissen Gedankengang aus der Algebrentheorie in die Formentheorie zu über-

---

[4]) *E. Hecke*, Analytische Arithmetik der positiven quadratischen Formen, Kgl. Danske Vidensk. Selsk., Math.-fys. Medd. XVII, 12 (1940). An dieser Stelle findet man eine vollständige Übersicht über die Resultate Heckes in dieser Richtung nebst weiteren Literaturhinweisen. Für die Normenformen von Quaternionenalgebren wurden Heckes Resultate direkt, d. h. ohne Verwendung analytischer Hilfsmittel bewiesen durch *H. Brandt*, Über die Zerlegungsgesetze der rationalen Zahlen in Quaternionenkörpern, Math. Ann. **117** (1941), S. 899—908; s. auch [27]).

[5]) *C.L. Siegel*, Über die analytische Theorie der quadratischen Formen, Annals of. Math. **36** (1935), S. 527—606. Formes quadratiques et modules des courbes algébriques, Bull. Sci. Math. 2e série, LXI (1937), S. 1—21. Weitere, hier nicht mehr aufgeführte Arbeiten beziehen sich auf indefinite Formen und Formen in algebraischen Zahlkörpern.

[6]) *H. Brandt*, Idealtheorie in Quaternionenalgebren, Math. Annalen **99** (1928), S. 1—29.

[7]) *M. Eichler*, Über gewisse Anzahlformen in der Theorie der quadratischen Formen, Sitz.-Ber. Bayer. Akad. Wiss., Math.-Nat. Abt. 1943, S. 1—24.

tragen; hiernach stehen der Satz von A. Meyer [8]), daß die Klassenzahl der indefiniten Formen bei mehr als zwei Veränderlichen i. a. mit der Geschlechterzahl übereinstimmt, und der Satz, daß die Idealklassenzahl einer normalen einfachen Algebra über einem algebraischen Zahlkörper i. a. gleich der Idealklassenzahl ihres Zentrums ist [9]), in engster verwandtschaftlicher Beziehung [10]).

Die zweite Idee von Brandt ist die, daß man eine besondere Art von Formen vor allen anderen bevorzugt behandeln soll; es sind dies die *Stammformen*, welche bei der immer wieder von neuem auftretenden Parallelität von Formen- und Algebrentheorie den maximalen Ordnungen entsprechen, während die übrigen Formen den nicht maximalen Ordnungen entsprechen [11]). Ich werde mich im folgenden ausschließlich auf sie beschränken.

In der vorliegenden Arbeit soll nun die schon früher [7]) [10]) angekündigte ausführliche Behandlung der berührten Themen erfolgen. Dabei erweist es sich als ratsam, die Theorie der Geschlechter, wie sie sich nach der genannten Arbeit von Witt darstellt, nochmals in veränderter Form zu bringen. Und zwar werde ich die Formentheorie nicht *auf* die Theorie der Algebren, sondern *parallel neben* ihr aufbauen. Dies Vorgehen hat einerseits den didaktischen Vorteil, daß die Algebrentheorie nicht vorausgesetzt zu werden braucht, zweitens ermöglicht es einen bequemeren Anschluß des Folgenden. Eine Übersicht über den weiteren Gedankengang soll die nachstehende Gliederung liefern; eine genauere Aufzählung aller angeschnittenen Einzelprobleme würde zu weit führen. Es erwies sich als möglich, mit wenigen Voraussetzungen auszukommen, wodurch die gewählte Überschrift der Arbeit eine gewisse Rechtfertigung erfährt.

---

[8]) *A. Meyer*, Zur Theorie der unbestimmten ternären quadratischen Formen, Diss. Zürich 1871. Ferner: Journ. reine angew. Math. **108** (1891), S. 125—139. Ebd. **113** (1894), S. 186—206. Ebd. **114** (1895), S. 233—254. Ebd. **115** (1895), S. 150—182. Ebd. **116** (1896), S. 307—325. Diese Arbeiten beziehen sich auf ternäre Formen. Die Übertragung auf Formen beliebiger Variablenzahl findet sich in der Viertelsjahrsschrift Naturf. Ges. Zürich **36** (1891), S. 241—250.

[9]) *M. Eichler*, Bestimmung der Idealklassenzahl in gewissen normalen einfachen Algebren, Journ. reine angew. Math. **176** (1937), S. 192—202. Über die Idealklassenzahl hyperkomplexer Systeme, Math. Zeitschr. **43** (1938), S. 481–494.

[10]) *M. Eichler*, Zur Theorie der quadratischen Formen gerader Variablenzahl, Speiserfestschrift Zürich 1945, S. 34.

[11]) *H. Brandt*, Zur Zahlentheorie der quadratischen Formen, Jahresbericht Deutsche Math.-Vereing. **47** (1937), S. 149—159.

Inhaltsübersicht

Bemerkungen zur Formelschreibweise

Betrachtet werden quadratische Formen

$$f(x_1, \ldots, x_n) = \tfrac{1}{2} \sum_{i,k=1}^{n} f_{ik}\, x_i\, x_k \;, \qquad f_{ik} = f_{ki} \;.$$

Die Variablenzahl heißt stets n. Bezeichnet $\mathfrak{F}$ die Matrix mit den Elementen f_{ik}, $\mathfrak{x}$ die einspaltige Matrix mit den Elementen x_i, und wird schließlich der Spiegelungsprozeß wie üblich durch einen Punkt angedeutet, so ist in Matrizenschreibweise

$$f(x_1, \ldots, x_n) = \tfrac{1}{2}\, \dot{\mathfrak{x}}\, \mathfrak{F}\, \mathfrak{x} \;.$$

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

Handelt es sich um ganzzahlige Formen, so sind die f_{ik} ganz und die f_{ii} sogar gerade. Eine Kongruenz

$$\mathfrak{F} \equiv \mathfrak{G} \bmod m$$

für zwei ganzzahlige Formen $\mathfrak{F}$ und $\mathfrak{G}$ habe stets die Bedeutung, daß $\frac{1}{m}(\mathfrak{F}-\mathfrak{G})$ die Matrix einer ganzzahligen quadratischen Form ist. Diese Bemerkung ist von Bedeutung, wenn es sich um uneigentlich primitive Formen und geraden Modul m handelt: durch die getroffene Verabredung entfällt die Schwierigkeit der Unterscheidung zwischen eigentlich und uneigentlich primitiven Formen.

Mit großen deutschen Buchstaben bezeichne ich quadratische Matrizen überhaupt, wobei die Reihenzahl eventuell durch einen oberen Index in Klammern angedeutet wird. Rechteckige Matrizen sollen durch kleine deutsche Buchstaben bezeichnet werden, zur Angabe von Zeilen- und Spaltenanzahl wird, falls erforderlich, ein oberes Indexpaar in Klammern benutzt. Speziell sei $\mathfrak{E}^{(n)}$ die n-reihige Einheitsmatrix, $\mathfrak{o}^{(n,m)}$ die Nullmatrix von n Zeilen und m Spalten, $\mathfrak{O}^{(n)} = \mathfrak{o}^{(n,n)}$. Ferner sei

$$\mathfrak{F}_0^{(2m)} = \begin{pmatrix} \mathfrak{O}^{(m)} & \mathfrak{E}^{(m)} \\ \mathfrak{E}^{(m)} & \mathfrak{O}^{(m)} \end{pmatrix} = \begin{pmatrix} & \mathfrak{E}^{(m)} \\ \mathfrak{E}^{(m)} & \end{pmatrix} .$$

Tritt die Nullmatrix als Teil einer größeren Matrix auf, so wird sie i. a. ausgelassen werden.

Unter der *Diskriminante*[12]) einer Form $\mathfrak{F}^{(2m)}$ von gerader Variablenanzahl wird die Determinante der Matrix $\mathfrak{F}^{(2m)}$ verstanden, wozu noch ein Vorzeichen kommt; sie wird stets mit dem Buchstaben $D = D(\mathfrak{F}^{(2m)})$ bezeichnet:

$$D(\mathfrak{F}^{(2m)}) = (-1)^m \, | \, \mathfrak{F}^{(2m)} \, | \, .$$

Bei ungerader Variablenzahl dagegen kommt hierzu noch der Faktor $\frac{1}{2}$:

$$D(\mathfrak{F}^{(2m+1)}) = \frac{(-1)^m}{2} \, | \, \mathfrak{F}^{(2m+1)} | \, .$$

I. Die Theorie der Geschlechter

§ 1. Die Einteilungsprinzipien

1. Wenn auch in dieser Arbeit die Theorie der quadratischen Formen nur im rationalen Zahlkörper entwickelt werden soll, so kann doch zur Erörterung der Einteilungsprinzipien ein allgemeiner Grundkörper k als gegeben gedacht werden, dem die Koeffizienten aller hier auftretender Formen und Matrizen angehören sollen.

[12]) Nach wiederholtem Vorschlag von *H. Brandt*, s. [11]).

Zwei Formen $\mathfrak{F}_1$, $\mathfrak{F}_2$ heißen *äquivalent*, wenn mit einer ganzzahligen Matrix $\mathfrak{S}$ in k, deren Determinante eine Einheit ist, die Gleichung

$$\mathfrak{F}_1 = \dot{\mathfrak{S}}\, \mathfrak{F}_2\, \mathfrak{S} \tag{1}$$

gilt. Ich möchte mir erlauben, in der Definition nun anders als üblich folgendermaßen fortzufahren: $\mathfrak{F}_1$ und $\mathfrak{F}_2$ heißen *verwandt*, wenn (1) mit einer nicht notwendig ganzzahligen Matrix $\mathfrak{S}$ gilt, deren Determinante auch keine Einheit zu sein braucht. Diese Beziehungen der Formen zueinander sind reflexiv, symmetrisch und transitiv. Die Gesamtheiten der äquivalenten und verwandten Formen heißen *Klassen* und *Geschlechter*. Für Äquivalenz und Verwandtschaft wird die Schreibweise

$$\mathfrak{F}_1 \cong \mathfrak{F}_2\ , \qquad \mathfrak{F}_1 \approx \mathfrak{F}_2$$

gebraucht. Liegt in k keine Ganzheitsdefinition vor, so entfällt natürlich der Äquivalenzbegriff.

Beide Male wurde hier die begrifflich einfachste Eigenschaft zur Definition herangezogen, damit wird der Theorie die Aufgabe zugewiesen, Kriterien für Äquivalenz und Verwandtschaft aufzustellen. Diesem deduktiven Verfahren steht das induktive gegenüber; leider hat man sich daran gewöhnt, den Äquivalenzbegriff deduktiv, den Geschlechtsbegriff induktiv einzuführen. Es ist an der Zeit, diese Inkonsequenz zu beseitigen!

2. Einem Geschlecht quadratischer Formen in n Variablen kann man einen metrischen Raum R_n zuordnen[2]): sind n Basisvektoren $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$ gegeben, so definiere man als die *Norm* eines Vektors

$$\mathfrak{x} = \mathfrak{e}_1 x_1 + \cdots + \mathfrak{e}_n x_n$$

den Ausdruck

$$N(\mathfrak{x}) = \mathfrak{F}(x_1, \ldots, x_n)\ ,$$

wo $\mathfrak{F}$ eine Form des Geschlechts ist. Gegenstand der eigentlichen Zahlentheorie sind die Gesamtheiten der Vektoren $\mathfrak{x}$, deren Normen ganzzahlig oder bis auf einen konstanten Faktor ganzzahlig sind. Diese Gesamtheiten bilden Moduln in bezug auf den Ring $\mathfrak{o}$ der ganzen Zahlen von k, d. h. $\mathfrak{o}$-Moduln. Ein solcher Modul soll ein *Gitter* heißen, wenn er vom Rang n ist.

Ein maximales, d. h. nicht mehr erweiterungsfähiges Gitter von Vektoren, deren Normen ganzzahlig sind, heißt ein *Kerngitter*. Besitzt es eine Basis $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, was z. B. stets der Fall ist, wenn in k die Idealklassenzahl gleich 1 ist, so ist die quadratische Form

$$N(\mathfrak{a}_1 x_1 + \cdots + \mathfrak{a}_n x_n) = \frac{1}{2} \sum \frac{\partial^2 N}{\partial x_i\, \partial x_k}\, x_i x_k$$

eine Kernform in der Terminologie von Brandt[11]). Jedes Gitter ist in einem Kerngitter enthalten, und das „Volumen" der einzelnen Gittermaschen eines Kerngitters teilt das Volumen der Gittermaschen sämtlicher in ihm enthaltener Gitter. (Das Maschenvolumen ist zunächst durch die gegebene Metrik nur dann definiert, wenn eine Basis existiert; allgemein hat man es als den größten gemeinsamen Teiler der Maschenvolumina sämtlicher Teilgitter mit Basis zu definieren; es ist i. a. kein Hauptideal.)

Kerngitter sind auch diejenigen maximalen Gitter, deren Vektoren ganzzahlige Vielfache eines gegebenen (ganzen oder gebrochenen) Ideals $\mathfrak{f}$ als Normen haben; sie gehören jedoch i. a. zu einer anderen Metrik, wenn nämlich die ursprüngliche Form $\mathfrak{F}$ und die Form $\mathfrak{f} \cdot \mathfrak{F}$ nicht zum gleichen Geschlecht gehören. In einer Gesamtheit solchermaßen in Beziehung stehender Gitter gibt es gewisse, die dadurch ausgezeichnet sind, daß ihr Grundmaschenvolumen der größte gemeinsame Teiler der Grundmaschenvolumina sämtlicher dieser Gitter ist. Sie heißen *Stammgitter* und ihr Grundmaschenvolumen die *Stammdiskriminante*. Der Existenzbeweis für die Stammgitter zu einem Formengeschlecht wäre zwar noch zu erbringen, was aber durch ganz elementare Schlüsse möglich ist, so daß ich ihn wohl übergehen darf. Besitzt ein Stammgitter eine Basis, was stets der Fall ist, wenn k die Idealklassenzahl 1 hat, so ist seine Normenform eine *Stammform*[11]).

Der Gedanke, die Kern- und Stammgitter bei der Entwicklung der Zahlentheorie zu bevorzugen, bedarf keiner besonderen Rechtfertigung mehr, da Brandt oft genug auf ihn hingewiesen hat.

Wenn die Idealklassenzahl von k größer als 1 ist, so gibt es Formen, die nicht mit einer Kernform oder dem Vielfachen einer Stammform verwandt sind. Jedoch kann man sich in diesem Falle helfen, indem man *Kern-* und *Stammformen hinsichtlich eines Primideals* $\mathfrak{p}$ betrachtet, d. h. solche Formen, die bei Erweiterung von k zu dem $\mathfrak{p}$-adischen Zahlkörper $k_{\mathfrak{p}}$ Kern- bzw. Stammformen bleiben.

In dieser Arbeit werden hauptsächlich Gesamtheiten von Stammformen im rationalen Zahlkörper von gleicher Variablenzahl, gleicher Diskriminante und von gleichem Sylvesterschen Trägheitsindex eine Rolle spielen. Eine solche Gesamtheit soll kurz ein *Formensystem* heißen. Die zu entwickelnde Zahlentheorie verknüpft sämtliche Formen eines solchen Systems miteinander. Beispiele für Formensysteme sind die Normenformen sämtlicher Ideale eines quadratischen Zahlkörpers oder einer rationalen Quaternionenalgebra; in diesen Beispielen ist einem Formensystem jeweils ein hyperkomplexes Zahlensystem umkehrbar eindeutig zugeordnet.

3. Das gröbste Einteilungsprinzip verdankt man dem Einfluß der Algebrentheorie, es ist das der Ähnlichkeit von Formen. Zwei Formen $\mathfrak{F}_1(x_1, \ldots, x_{n_1})$ und $\mathfrak{F}_2(x_1, \ldots, x_{n_2})$ in n_1 und n_2 Variablen heißen *ähnlich*[2]), wenn $n_1 \equiv n_2 \bmod 2$ und wenn

$$\mathfrak{F}_1(x_1, \ldots, x_{n_1}) - \mathfrak{F}_2(x_{n_1+1}, \ldots, x_{n_1+n_2}) \approx \mathfrak{F}_0^{(n_1+n_2)}$$

ist; hinsichtlich $\mathfrak{F}_0^{(2m)}$ vgl. die Bemerkungen zur Formelschreibweise. Die Gesamtheit ähnlicher Formen bildet einen *Formentyp* oder *Typ* schlechthin. Für zwei ähnliche Formen wird $\mathfrak{F}_1 \sim \mathfrak{F}_2$ geschrieben.

Zwischen den Formentypen läßt sich eine Addition folgendermaßen erklären: sind zwei Typen durch je einen Repräsentanten $\mathfrak{F}_1(x_1, \ldots, x_{n_1})$ und $\mathfrak{F}_2(x_1, \ldots, x_{n_2})$ gegeben, so wird die Summe als der Typ der Form $\mathfrak{F}_1(x_1, \ldots, x_{n_1}) + \mathfrak{F}_2(x_{n_1+1}, \ldots, x_{n_1+n_2})$ definiert. Es gilt der folgende Satz von Witt[2]):

I. Hauptsatz. *Die Ähnlichkeitsbeziehung ist reflexiv, symmetrisch und transitiv.*

Bezüglich der eben erklärten Addition bilden die Formentypen eine Abelsche Gruppe, das Einheitselement ist der Typ der Formen $\mathfrak{F}_0^{(2m)}$, $m = 0, 1, \ldots$

Verschwinden die Diskriminanten zweier Formen $\mathfrak{F}_1$ *und* $\mathfrak{F}_2$ *gleicher Variablenzahl nicht, so ist dann und nur dann* $\mathfrak{F}_1 \approx \mathfrak{F}_2$, *wenn* $\mathfrak{F}_1 \sim \mathfrak{F}_2$ *ist.*

Die Gruppe der Formentypen soll kurz die Wittsche Gruppe heißen; sie ist das Analogon der Brauerschen Algebrenklassengruppe. Witt erklärt l. c. auch eine Multiplikation der Formentypen, die jedoch weniger Bedeutung zu haben scheint.

§ 2. Die lokalen Invarianten der Formentypen

1. Die Hauptaufgabe des ersten Abschnittes ist die Aufstellung eines vollständigen Invariantensystems gegenüber Transformationen (1) mit beliebigen rationalen Koeffizienten. Es ist praktisch, die Formen hierbei auf Diagonalgestalt

$$\mathfrak{F}(x_1, \ldots) = \tfrac{1}{2} \sum_i a_i x_1^2$$

transformiert anzunehmen und dann kurz mit dem Symbol $(a_1, a_2, \ldots)$ zu bezeichnen. Dieses sei nicht dem Geschlecht, sondern dem Typ zugeordnet, d. h. es sei

$$\begin{aligned}(a_1, a_2, a_3, \ldots, a_n) &= (a_2, a_1, a_3, \ldots, a_n) \\ &= (a_1, a_2, a_3, \ldots, a_n, b, -b) = \ldots\end{aligned}$$

Formentypen werden auch mit großen griechischen Buchstaben bezeichnet, handelt es sich um Typen in einem p-adischen Zahlkörper, so soll dies durch den oberen Index p angedeutet werden; für die symbolische unendliche Primstelle p_∞, der die gewöhnliche archimedische Bewertung des rationalen Zahlkörpers entspricht, gebrauche ich kurz ∞ als oberen Index. Eine Verwechslung mit Potenzen ist nicht möglich, da solche nicht vorkommen. Wenn ein rationaler Formentyp X bei Erweiterung des rationalen Zahlkörpers k zu k_p mit einem p-adischen Formentyp Ξ^p zusammenfällt, wird kurz

$$X \sim \Xi^p \bmod p$$

geschrieben. Ist X ein rationaler Formentyp, so bedeute X^p stets den p-adischen Typ, mit dem X bei Erweiterung von k zu k_p zusammenfällt.

Die Vorgehensweise ist nun die, zuerst die Invarianten der Formentypen für alle Primstellen anzugeben. Aus diesen werden dann vollständige Invariantensysteme für die Geschlechter aufgebaut werden. Dabei wird der Schwerpunkt der Untersuchungen bei den Formen und Typen gerader Variablenzahl liegen; man kann ja jedem Typ X ungerader Variablenzahl den Typ $X + (1)$ gerader Variablenzahl zuordnen, diese Zuordnung ist nicht nur eindeutig, sondern nach dem I. Hauptsatz auch eindeutig umkehrbar.

2. Für die unendliche Primstelle p_∞, für welche k_{p_∞} der Körper aller reellen Zahlen ist, besitzt ein Typ X als einzige Invariante die *Signatur* σ, d. h. die Differenz der Anzahlen der positiven und negativen Zahlen a_ν in der Darstellung $X \sim (a_1, \ldots)$. Bezeichnet Γ den Typ

$$\Gamma = (1,\ 1)\ , \tag{2}$$

so gilt also stets für einen Typ X gerader Variablenzahl

$$X \sim \frac{\sigma}{2}\,\Gamma \mod p_\infty\ . \tag{3}$$

Die Wittsche Gruppe der p-adischen Formentypen für $p = p_\infty$ ist die unendliche zyklische Gruppe.

3. Es sei nun p eine ungerade Primzahl. Man kann jeden Typ durch eine solche Kernform repräsentieren, welche die Zahl 0 nicht eigentlich darstellt[13]), den Typ ausgenommen, welcher dem Einheitselement der Wittschen Gruppe entspricht. Eine elementare Diskussion liefert folgende 8 Typen gerader Variablenzahl, wobei ν einen quadratischen Nichtrest mod p bedeutet:

[13]) s. [2]), Satz 5 und [11]), Nr. 9.

$$
\begin{aligned}
E^p &= (1\,,\ -1)\,, & \Pi^p &= (1\,,\ -p)\,,\\
H^p &= (1\,,\ -\nu)\,, & P^p &= (\nu\,,\ -p)\,,\\
T^p &= (1\,,\ -\nu\,,\ p\,,\ -\nu p)\,, & M^p &= (\nu\,,\ -\nu p)\,,\\
\Theta^p &= (p\,,\ -\nu p)\,, & N^p &= (1\,,\ -\nu p)\ .
\end{aligned}
\tag{4}
$$

Die Wittsche Gruppe wird durch die nachstehende symmetrisch zu ergänzende Gruppentafel beschrieben:

$$
\begin{array}{cccc:cccc}
E^p & H^p & T^p & \Theta^p & \Pi^p & P^p & M^p & N^p\\
H^p & E^p & \Theta^p & T^p & P^p & \Pi^p & N^p & M^p\\
T^p & & E^p & H^p & M^p & N^p & \Pi^p & P^p\\
\Theta^p & & & E^p & N^p & M^p & P^p & \Pi^p\\
\hdashline
\Pi^p & & & & E^p & H^p & T^p & \Theta^p\\
P^p & & & & & E^p & \Theta^p & T^p\\
M^p & & & & & & E^p & H^p\\
N^p & & & & & & & E^p
\end{array}
\qquad \text{für } p \equiv 1 \bmod 4. \tag{5}
$$

$$
\begin{array}{cccc:cccc}
E^p & H^p & T^p & \Theta^p & \Pi^p & P^p & M^p & N^p\\
H^p & E^p & \Theta^p & T^p & P^p & \Pi^p & N^p & M^p\\
T^p & & E^p & H^p & M^p & N^p & \Pi^p & P^p\\
\Theta^p & & & E^p & N^p & M^p & P^p & \Pi^p\\
\hdashline
\Pi^p & & & & T^p & \Theta^p & E^p & H^p\\
P^p & & & & & T^p & H^p & E^p\\
M^p & & & & & & T^p & \Theta^p\\
N^p & & & & & & & T^p
\end{array}
\qquad \text{für } p \equiv 3 \bmod 4. \tag{6}
$$

Es handelt sich um Abelsche Gruppen mit den Invarianten 2, 2, 2 (für $p \equiv 1 \bmod 4$) bzw. 2, 4 (für $p \equiv 3 \bmod 4$). Erzeugendensysteme sind H^p, T^p, Π^p bzw. H^p, Π^p.

4. Bei der Aufstellung der p-adischen Invarianten für $p = 2$ bleibt man am besten bei der Angabe der Formen in Diagonalengestalt, auch wenn es sich dabei i. a. nicht mehr um Kernformen handelt. Die Typen gerader Variablenzahl sind

$$
\left.
\begin{aligned}
E^2 &= (1,\ -1) = (3,\ -3) = (5,\ -5) = (7,\ -7) = (2,\ -2)\\
&= (3.2,\ -3.2) = (5.2,\ -5.2) = (7.2,\ -7.2)\ ,\\
E_*^2 &= (1,\ -5) = (5,\ -1) = (3,\ -7) = (7,\ -3)\ ,\\
H^2 &= (1,\ -7) = (5,\ -3) = (2,\ -7.2) = (5.2,\ -3.2)\ ,
\end{aligned}
\right\} \tag{7}
$$

$$
\left.\begin{aligned}
H_*^2 &= (1,\ -3) = (5,\ -7) = (3.2,\ -2) = (7.2,\ -5.2)\ ,\\
T^2 &= (1,\ 1,\ 1,\ 1) = (2,\ 2,\ 2,\ 2) = \cdots = (7,\ 7,\ 7,\ 7)\\
&= (1,\ 1,\ 2,\ 2) = (1,\ 1,\ 5,\ 5) = \text{usw.},\\
T_*^2 &= (3.2,\ -7.2) = (7.2,\ -3.2) = (2,\ -5.2) =\\
&= (5.2,\ -2) = (1,\ 5,\ 5,\ 5) = (1,\ 1,\ 1,\ 5) = \text{usw.}\\
\Theta^2 &= (3,\ -5) = (7,\ -1) = (3.2,\ -5.2) = (7.2,\ -2)\ ,\\
\Theta_*^2 &= (3,\ -1) = (7,\ -5) = (2,\ -3.2) = (5.2,\ -7.2)\ ,\\
\Pi^2 &= (1,\ -2) = (-1,\ 2)\ ,\\
\Pi_*^2 &= (5,\ -2) = (-5,\ 2)\ ,\\
P^2 &= (1,\ -7.2) = (-5,\ 3.2)\ ,\\
P_*^2 &= (5,\ -7.2) = (-1,\ 3.2)\ ,\\
M^2 &= (5,\ -5.2) = (-5,\ 5.2)\ ,\\
M_*^2 &= (1,\ -5.2) = (-1,\ 5.2)\ ,\\
N^2 &= (5,\ -3.2) = (-1,\ 7.2)\ ,\\
N_*^2 &= (1,\ -3.2) = (-5,\ 7.2)\ .
\end{aligned}\right\} \qquad (7)
$$

Die Gruppentafel ist

$$
\left.\begin{array}{cccccccc:cccccccc}
E^2 & E_*^2 & H^2 & H_*^2 & T^2 & T_*^2 & \Theta^2 & \Theta_*^2 & \Pi^2 & \Pi_*^2 & P^2 & P_*^2 & M^2 & M_*^2 & N^2 & N_*^2\\
E_*^2 & E^2 & H_*^2 & H^2 & T_*^2 & T^2 & \Theta_*^2 & \Theta^2 & \Pi_*^2 & \Pi^2 & P_*^2 & P^2 & M_*^2 & M^2 & N_*^2 & N^2\\
H^2 & & T^2 & T_*^2 & \Theta^2 & \Theta_*^2 & E^2 & E_*^2 & P^2 & P_*^2 & M^2 & M_*^2 & N^2 & N_*^2 & \Pi^2 & \Pi_*^2\\
H_*^2 & & & T^2 & \Theta_*^2 & \Theta^2 & E_*^2 & E^2 & P_*^2 & P^2 & M_*^2 & M^2 & N_*^2 & N^2 & \Pi_*^2 & \Pi^2\\
T^2 & & & & E^2 & E_*^2 & H^2 & H_*^2 & M^2 & M_*^2 & N^2 & N_*^2 & \Pi^2 & \Pi_*^2 & P^2 & P_*^2\\
T_*^2 & & & & & E^2 & H_*^2 & H^2 & M_*^2 & M^2 & N_*^2 & N^2 & \Pi_*^2 & \Pi^2 & P_*^2 & P^2\\
\Theta^2 & & & & & & T^2 & T_*^2 & N^2 & N_*^2 & \Pi^2 & \Pi_*^2 & P^2 & P_*^2 & M^2 & M_*^2\\
\Theta_*^2 & & & & & & & T^2 & N_*^2 & N^2 & \Pi_*^2 & \Pi^2 & P_*^2 & P^2 & M_*^2 & M^2\\
\hdashline
\Pi^2 & & & & & & & & E^2 & E_*^2 & H^2 & H_*^2 & T^2 & T_*^2 & \Theta^2 & \Theta_*^2\\
\Pi_*^2 & & & & & & & & & E^2 & H_*^2 & H^2 & T_*^2 & T^2 & \Theta_*^2 & \Theta^2\\
P^2 & & & & & & & & & & T^2 & T_*^2 & \Theta^2 & \Theta_*^2 & E^2 & E_*^2\\
P_*^2 & & & & & & & & & & & T^2 & \Theta_*^2 & \Theta^2 & E_*^2 & E^2\\
M^2 & & & & & & & & & & & & E^2 & E_*^2 & H^2 & H_*^2\\
M_*^2 & & & & & & & & & & & & & E^2 & H_*^2 & H^2\\
N^2 & & & & & & & & & & & & & & T^2 & T_*^2\\
N_*^2 & & & & & & & & & & & & & & & T^2
\end{array}\right\} \qquad (8)
$$

Die Tabelle ist symmetrisch zu ergänzen. Es handelt sich also um eine Abelsche Gruppe mit den Invarianten 2, 4, 2; ein Erzeugendensystem ist E_*^2, H^2, Π^2.

5. Die Typen ungerader Variablenzahl in k_p werden in der Form $X^p + (1)$ dargestellt, wo X^p sämtliche Typen gerader Variablenzahl durchläuft. Ihre Anzahl ist also genau so groß. Jeder dieser Typen läßt sich wiederum durch eine die Null nicht eigentlich darstellende Form repräsentieren[13]; diese hat jetzt die Variablenzahl 1 oder 3.

Zugleich mit der Aufstellung sämtlicher p-adischen Formentypen bzw. ihrer unären, binären, ternären oder quaternären Repräsentanten sind deren arithmetische Grundeigenschaften in k_p zu diskutieren. Es ergibt sich dabei zunächst durch eine elementare Einzelbetrachtung der möglichen Fälle für die Formen, welche die Null nicht eigentlich darstellen, der

Hilfssatz 1. Eine Form $\mathfrak{F}$ in k_p in n Variablen ist mit genau einer Kernform $\mathfrak{F}_1$ verwandt. Dabei ist $D(\mathfrak{F}_1)$ durch eine Primzahl $p>2$ höchstens zweimal teilbar. Für $n \equiv 1 \bmod 2$ gilt dasselbe auch für $p = 2$, für $n \equiv 0 \bmod 2$ dagegen ist $D(\mathfrak{F}_1)$ durch 2 entweder keinmal, zweimal oder dreimal teilbar.

Dieser Hilfssatz läßt sich leicht auf sämtliche übrigen Formen übertragen. Diese sind verwandt mit je einer Form

$$\mathfrak{F} = \mathfrak{F}_0^{(2m)} + \mathfrak{F}_1 \,, \tag{9}$$

wo die Summe im Sinne der Wittschen Gruppe, also nicht als Matrizensumme zu verstehen ist, und $\mathfrak{F}_1$ eine die Null nicht eigentlich darstellende Kernform ist. Hierbei gilt

$$D(\mathfrak{F}) = D(\mathfrak{F}_1) \,. \tag{10}$$

Man braucht nun nur zu beweisen, daß diese Formen (9) auch Kernformen sind, wenn $\mathfrak{F}_1$ Kernform ist. Wäre $\mathfrak{F}$ nicht Kernform, so wäre $\mathfrak{F}$ in einer Kernform $\mathfrak{F}'$ eigentlich enthalten, es wäre also $D(\mathfrak{F}')$ mindestens zweimal weniger durch p teilbar als $D(\mathfrak{F})$. D. h. nach Hilfssatz 1 für $\mathfrak{F}_1$, daß $D(\mathfrak{F}')$ zu p prim ist oder aber, falls $p = 2$, $n \equiv 0 \bmod 2$ und $D(\mathfrak{F}) \equiv 0 \bmod 8$ war, genau einmal durch 2 teilbar. Das letztere kann bekanntlich nicht zutreffen. Wenn nun aber $D(\mathfrak{F}')$ zu p teilerfremd ist, so müßte $\mathfrak{F}'$ mit einer Form $\mathfrak{F}_0^{(2m')} + \mathfrak{F}_1'$ verwandt sein, wo $D(\mathfrak{F}_1')$ auch zu p prim ist. Dabei ist aber andererseits $\mathfrak{F}_1' \approx \mathfrak{F}_1$, was einen Widerspruch darstellt. Der Hilfssatz 1 ist damit in vollem Umfange bewiesen.

Ist eine ganzzahlige Form $\mathfrak{F}$ im Körper k der rationalen Zahlen gegeben, so kann man für die einzelnen Primteiler p von $D(\mathfrak{F})$ nacheinander $\mathfrak{F}$ enthaltende ganzzahlige Formen aufsuchen, die bezüglich p Kernformen sind. Das Verfahren bricht bei einer Kernform ab. Diese braucht nun aber nicht mehr durch $\mathfrak{F}$ eindeutig festgelegt zu sein, doch ist ihre Diskriminante, die *Kerndiskriminante*, auch jetzt noch eindeutig bestimmt, und für ihre Teilbarkeit durch Primzahlen gilt der Hilfssatz 1.

Auf Grund der bewiesenen Invarianz der Kerndiskriminante bei Übergang zu ähnlichen Formen führe ich die folgende Definition ein: Eine Form $\mathfrak{F}$ oder ein Formentyp X im rationalen Zahlkörper sei *an der Stelle* p (rationale Primzahl) *verzweigt*, wenn p die Kerndiskriminante teilt; p sei eine *Verzweigungsstelle erster oder zweiter Art*, je nachdem p in der Kerndiskriminante in ungerader oder gerader Vielfachheit aufgeht. Es ist also p eine Verzweigungsstelle 1. Art für die Typen Π^p, P^p, M^p, N^p, eine Verzweigungsstelle 2. Art für die Typen T^p, Θ^p und keine Verzweigungsstelle für die Typen E^p, H^p; im Falle $p = 2$ sind die mit einem Stern versehenen zugleich mit denen gleichen Buchstabens und ohne Stern mitzuzählen, nur H^2, H^2_* gehören jetzt in die 2. Gruppe.

Eine Erklärung darüber, wann die unendliche Primstelle p_∞ Verzweigungsstelle ist und von welcher Art, könnte der Vollständigkeit halber hinzugefügt werden. Eine Bedeutung hat eine solche Erklärung nicht, und ich unterlasse sie daher.

§ 3. Das erste vollständige Invariantensystem

1. *Hilfssatz 2.* Ist $p > 2$ eine Primzahl oder $p = p_\infty$ die unendliche Primstelle, so gibt es im rationalen Zahlkörper einen Formentyp Ω_p, welcher folgende Eigenschaften besitzt und durch sie eindeutig gekennzeichnet ist:

$$\Omega_p \sim E^q \bmod q \ , \tag{11}$$

$$\Omega_p \sim T^p \bmod p \ , \tag{12}$$

$$\Omega_p \sim T^2 \bmod 2 \ ; \tag{13}$$

dabei durchlaufe q alle von 2 und p verschiedenen Primstellen des rationalen Zahlkörpers einschließlich der unendlichen ($T^\infty = 2\Gamma$).

Beweis. Für $p = p_\infty$ ist $\Omega_{p\infty} = (1, 1, 1, 1) = 2\Gamma$, für eine Primzahl p der Form $4k + 3$ ist $\Omega_p = (1, 1, -p, -p)$ dieser Formentyp, wie man unmittelbar einsieht.

Es sei nun $p \equiv 1 \bmod 4$. Es werde vollständige Induktion angesetzt und der Hilfssatz für alle kleineren Primzahlen als p bereits als richtig

angenommen. Es sei r der kleinste positive quadratische Nichtrest mod p; offenbar ist r eine Primzahl. Ist $r = 2$, so ist $\Omega_p = (1, -2, p, -2p)$ der verlangte Typ. Ist $r > 2$, so gibt es nach der Voraussetzung ein Ω_r, und es ist

$$\Omega_p = \begin{cases} (1, -r, p, -rp) & \text{für } r \equiv 3 \bmod 4 \ , \\ (1, -r, p, -rp) + \Omega_r & \text{für } r \equiv 1 \bmod 4 \ . \end{cases}$$

Das Erfülltsein von (11) bis (13) läßt sich in jedem Falle durch Benutzung von (5), (6), (8) und des quadratischen Reziprozitätsgesetzes leicht verifizieren.

Hilfssatz 3[14]). Eine Form $\mathfrak{F}$ in $n > 4$ Variablen stellt die Null im rationalen Zahlkörper dann und nur dann eigentlich dar, wenn sie indefinit ist.

2. Es bezeichne E das Einheitselement der Wittschen Gruppe im rationalen Zahlkörper k, nämlich den Typ, dem die Formen $\mathfrak{F}_0^{(2m)}$ angehören. Ferner sei für eine Primzahl $p \geqq 2$

$$\Phi_p = (1, -p) \ . \tag{14}$$

Durch die Formentypen Γ (Gl. (2)), Ω_p (Hilfssatz 2) und Φ_p wird die volle Wittsche Gruppe der Formentypen gerader Variablenzahl in k erzeugt. Es gilt nämlich der

Satz 1. Es sei X ein Formentyp gerader Variablenzahl der Signatur σ. Dann ist

$$X = \Sigma \Phi_{p_1} + \Sigma \Omega_{p_2} + \Sigma(\Phi_{p_3} + \Omega_{p_3}) + \frac{\sigma}{2} \Gamma \tag{15}$$

wobei der letzte Term als $\frac{\sigma}{2}$-malige Addition von Γ aufzufassen ist. Hier durchläuft p_1 sämtliche ungeraden Verzweigungsstellen 1. Art, für welche

$$X \sim \Pi^{p_1}, P^{p_1} \bmod p_1 \tag{16}$$

ist, sowie $p_1 = 2$, falls 2 eine Verzweigungsstelle 1. Art ist; p_2 durchläuft sämtliche ungeraden Verzweigungsstellen 2. Art:

$$X \sim T^{p_2}, \Theta^{p_2} \bmod p_2 \ ; \tag{17}$$

p_3 durchläuft sämtliche ungeraden Verzweigungsstellen 1. Art, für die

$$X \sim M^{p_3}, N^{p_3} \bmod p_3 \tag{18}$$

ist.

[14]) s. die erste der unter [1]) zitierten Arbeiten.

Beweis. Die Differenz beider Seiten von (15) werde mit Ξ bezeichnet. Es ist $\Xi = E$ zu zeigen. Nach (5), (6), (11), (12), (14) hat Ξ keine ungeraden Verzweigungsstellen mehr. Nach (8), (13), (14) ist $p = 2$ entweder keine Verzweigungsstelle oder eine Verzweigungsstelle 2. Art. Die Signatur von Ξ ist Null. Die Kerndiskriminante von Ξ ist demnach 1 oder 4.

Ist $\Xi \neq E$, so werde in Ξ eine Form f von möglichst kleiner Variablenzahl gesucht, es ist eine Form, welche die Null nicht eigentlich darstellt[13]). Ihre Variablenzahl ist nach Hilfssatz 3 also 4 oder 2. Es beschränkt die Allgemeinheit nicht, wenn man f als Kernform annimmt.

Ist die Variablenzahl 4, so ist f Normenform einer Idealklasse einer rationalen Quaternionenalgebra, da die Diskriminante ein Quadrat ist. Es kommen dabei wegen des Wertes der Diskriminante nur die Matrixalgebra und die Hamiltonsche in Frage. Die erste scheidet aus, da dann f die Null eigentlich darstellen würde, die zweite, da f nicht definit ist. — Ist die Variablenzahl 2, so stellt f die Null ebenfalls eigentlich dar, da die Diskriminante ein Quadrat ist. Mithin muß $\Xi = E$ sein, und der Satz 1 ist bewiesen.

3. Der Satz 1 lehrt unter anderem, daß zwischen den lokalen Invarianten X^p eines rationalen Formentyps X gewisse Bindungen bestehen müssen. Um diese Bindungen aufzustellen, werden homomorphe Abbildungen der Wittschen Gruppen in k und k_p auf Untergruppen der Wittschen Gruppen in k_q vorgenommen. Sie werden durch das Symbol $[X^p]^q$ beschrieben, zu einem Formentyp X wird demnach zuerst die p-adische Invariante X^q gebildet, und dieser wird dann das Bild $[X^p]^q$ zugeordnet, welches ein q-adischer Formentyp ist. Ich werde diese Abbildungen für Typen gerader Variablenzahl angeben und vervollständige sie durch die Festsetzung

$$[(X + (1))^p]^q = [X^p]^q + (1)^q \tag{19}$$

für die Typen ungerader Variablenzahl.

Es sei

$$[X^\infty]^q = \begin{cases} E^q \text{ für } \left(\dfrac{(-1)^{\frac{\sigma}{2}}}{q}\right) = 1\ , \\ H^q \text{ für } \left(\dfrac{(-1)^{\frac{\sigma}{2}}}{q}\right) = -1\ , \end{cases} \qquad (q > 2) \tag{20}$$

$$[X^\infty]^2 = \begin{cases} E^2 & \text{für} \quad \sigma \equiv 0 \bmod 8 \ , \\ \Theta^2 & \text{für} \quad \sigma \equiv 2 \bmod 8 \ , \\ T^2 & \text{für} \quad \sigma \equiv 4 \bmod 8 \ , \\ H^2 & \text{für} \quad \sigma \equiv 6 \bmod 8 \ , \end{cases} \tag{21}$$

$$[X^p]^q = \begin{cases} E^q & \text{für} \quad \left(\frac{p}{q}\right) = 1, \ X \text{ beliebig}, \\ E^q & \text{für} \quad \left(\frac{p}{q}\right) = -1, \ X \sim E^p, H^p, T^p, \Theta^p \bmod p, \\ H^q & \text{für} \quad \left(\frac{p}{q}\right) = -1, \ X \sim \Pi^p, P^p, M^p, N^p \bmod p \ , \\ & \qquad\qquad (q \neq 2, \ q \neq p) \end{cases} \tag{22}$$

hierbei werden im Falle $p = 2$ die Typen $E^2_*, H^2_*, \ldots$ bzw. $\Pi^2_*, P^2_*, \ldots$ mit zu $E^2, H^2, \ldots$ bzw. $\Pi^2, P^2, \ldots$ gerechnet;

$$[X^p]^p = \begin{cases} E^p \text{ für } X \sim E^p, T^p, \Pi^p, M^p \bmod p \ , \\ H^p \text{ für } X \sim H^p, \Theta^p, P^p, N^p \bmod p \ ; \end{cases} \quad (p>2) \tag{23}$$

das Symbol $[X^p]^2$ für $p>2$ wird am bequemsten durch nachstehende Tabelle erklärt:

$X \sim$	E^p, H^p	Π^p, P^p	T^p, Θ^p	M^p, N^p	$\bmod p$
$[X^p]^2 =$	E^2	E^2	T^2	T^2	für $p \equiv 1 \bmod 8$,
	E^2	E^2_*	T^2	T^2_*	für $p \equiv 5 \bmod 8$,
	E^2	Θ^2	T^2	H^2	für $p \equiv 7 \bmod 8$,
	E^2	Θ^2_*	T^2	H^2_*	für $p \equiv 3 \bmod 8$,

(24)

$$[X^2]^2 = \begin{cases} X^2 & \text{für } X \sim E^2, \ E^2_*, \ H^2, \ H^2_*, \ T^2, \ T^2_*, \ \Theta^2, \ \Theta^2_* \bmod 2 \ , \\ X^2+\Pi^2 & \text{für } X \sim \Pi^2, \ \Pi^2_*, \ P^2, \ P^2_*, \ M^2, \ M^2_*, \ N^2, \ N^2_* \bmod 2 \ , \end{cases} \tag{25}$$

wobei X^2 der durch $X \sim X^2 \bmod 2$ erklärte 2-adische Typ ist.

Man überzeuge sich zunächst davon, daß hierbei stets

$$[(X_1 + X_2)^p]^q = [X_1^p]^q + [X_2^p]^q \tag{26}$$

gilt. Für Typen gerader Variablenzahl gelten ferner die folgenden *Summenrelationen:*

$$\sum_p [X^p]^q = E^q \ , \qquad (q = 2, 3, 5, \ldots) \tag{27}$$

die Summen sind über sämtliche Primstellen p einschließlich der unendlichen zu erstrecken; sie haben einen Sinn, da nur endlich viele der Summanden von E^q verschieden sind. Man braucht nach (15) diese Relationen nur für die speziellen Typen Γ, Ω_p, Φ_p zu beweisen, was eine Reihe elementarer Einzeldiskussionen erfordert. Weitere Relationen als (27) bestehen zwischen den lokalen Invarianten X^p eines rationalen Formentyps X nicht mehr, wie aus dem folgenden Satz hervorgeht. Eine kurze Bemerkung werde diesem Satz noch vorausgeschickt:

Offenbar liegt mit den p-adischen Invarianten X^p eines rationalen Typs X gerader Variablenzahl auch seine Kerndiskriminante $\Delta(X)$ fest, und zwar ist sie

$$\Delta(X) = (-1)^{\frac{\sigma}{2}} \prod_p p^{\varrho_p} \tag{28}$$

das Produkt ist über sämtliche Verzweigungsstellen p von X zu erstrecken, wobei ϱ_p die Art der Verzweigungsstelle ist und im Falle $p = 2$, $\varrho_2 = 1$ durch $\varrho_2 = 3$ zu ersetzen ist. Mit anderen Worten ist für $p > 2$: $\varrho_p = 0$, für $X^p = E^p, H^p$, $\varrho_p = 2$ für $X^p = T^p, \Theta^p$ und $\varrho_p = 1$ für $X^p = \Pi^p, P^p, M^p, N^p$; für $p = 2$ ist $\varrho_2 = 0$ für $X^2 = E^2, E_*^2$, $\varrho_2 = 2$ für $X^2 = H^2, H_*^2, T^2, T_*^2, \Theta^2, \Theta_*^2$ und $\varrho_2 = 3$ in den übrigen Fällen. Die Summenrelationen (27) für ein $q > 2$ lassen sich jetzt auch so ausdrücken:

$$\left(\frac{\Delta(X) q^{-\varrho_q}}{q}\right) = \left(\frac{(-1)^{\frac{\sigma}{2}}}{q}\right) \prod_{p \neq p} \left(\frac{p^{\varrho_p}}{q}\right), \tag{29}$$

sie geben also lediglich eine elementare Eigenschaft des Legendresymbols wieder.

4. **II. Hauptsatz.** *Die Variablenzahl und der p-adische Typ X^p für jede Stelle p bilden ein vollständiges System von Geschlechtsinvarianten*[15]).

Zwischen den Invarianten bestehen bei gerader Variablenzahl die Summenrelationen (27), *bei ungerader Variablenzahl*

$$\sum_p \left([X^p]^q + (1)\right) = E^q \,. \tag{27'}$$

Die aus X^∞ berechenbare Signatur σ ist $\equiv n \bmod 2$. Es ist $n \geqq |\sigma|$ sowie $n \geqq 3, 4$, falls unter den X^p ein ternärer oder quaternärer Typ vorkommt. Nur für endlich viele p ist $X^p \neq E^p, H^p$.

---

[15]) Äquivalent mit diesem Invariantensystem ist auch das folgende: n, $[X^p]^q$ für p, $q \neq p$.

Zu jedem System p-adischer Invarianten und einer Zahl $n>0$ gibt es ein Geschlecht quadratischer Formen, wenn die angegebenen Bedingungen erfüllt sind.

Beweis. Der II. Hauptsatz enthält gleichzeitig einen Satz über die Invariantensysteme von Typen. Dieser auf die Variablenzahl n nur insofern Bezug nehmende Teil, als die Fälle $n \equiv 0 \bmod 2$ und $n \equiv 1 \bmod 2$ unterschieden werden, leitet sich im Falle $n \equiv 1 \bmod 2$ aus dem Fall $n \equiv 0 \bmod 2$ in selbstverständlicher Weise her. Man hat also nur noch $n \equiv 0 \bmod 2$ ins Auge zu fassen.

Zunächst wird nun der Nachweis geführt, daß es zu einem die Summenrelationen (27) erfüllenden System von Invarianten X^p gerader Variablenzahl einen rationalen Formentyp X gerader Variablenzahl mit gerade diesen Invarianten gibt. Dazu bilde ich die Summe (15), wobei die Summanden entsprechend der Erklärung in Satz 1 zu nehmen sind, und behaupte, der so entstehende rationale Formentyp hat die gegebenen Invarianten X^p. Ersichtlich hat die Signatur den vorgeschriebenen Wert, es ist also

$$X \sim X^\infty \bmod p_\infty \ .$$

Es sei p eine ungerade Primzahl, dann kann nach dem Bildungsgesetz der Summe (17) schon entschieden werden, welchem der folgenden Paare von Formentypen: E^p, H^p; T^p, Θ^p; Π^p, P^p; M^p, N^p X in k_p angehört. Die genaue Festlegung von X innerhalb jedes dieser Paare ist durch das Legendresymbol (29) möglich, welches nach der Bemerkung in Nr. 3 zugleich mit den X^p zur Verfügung steht. Der Typ von X in k_p ist somit durch das Bildungsgesetz der Summe (15) aus den X^p in eindeutiger Weise berechenbar, und folglich

$$X \sim X^p \bmod p \ .$$

Daß auch der 2-adische Typ von X bei der Summendarstellung (15) in richtiger Weise festgelegt wird, folgt aus der Tatsache, daß der Wert von $[X^2]^2$ nach (27) für $q = 2$ berechnet werden kann, und daß damit wegen (25) die Invariante X^2 zunächst zweideutig festliegt; sie wird schließlich durch $[X^2]^2$ und die Kerndiskriminante eindeutig fixiert, und dann kann nur

$$X \sim X^2 \bmod 2$$

sein.

Jetzt muß man zeigen, daß ein gegebener Formentyp X eine Form $\mathfrak{F}$ beliebig gegebener Variablenzahl enthält, wenn nicht die genannten Aus-

nahmen vorliegen. Dieser Nachweis macht keine Schwierigkeit: man gehe von einer Form $\mathfrak{F}$ in X von größerer Variablenzahl als n aus. Wenn $\mathfrak{F}$ die Zahl Null eigentlich darstellt, kann man die Variablenzahl um 2 erniedrigen[13]; diese Schlußweise ist genügend oft zu wiederholen.

Endlich müßte man umgekehrt beweisen, daß Formen mit gleichem Invariantensystem verwandt sind; diese Tatsache ist von selber klar.

§ 4. Das zweite vollständige Invariantensystem

1. Das in § 3 aufgestellte Invariantensystem der Geschlechter ist für die Anwendung in der Zahlentheorie noch zu unhandlich; ich leite aus ihm daher ein zweites her, welches einen bequemeren Anschluß der eigentlichen zahlentheoretischen Untersuchungen gestattet. Es unterscheidet sich übrigens einerseits von dem System der Invarianten, auf das in der älteren Theorie der Geschlechtsbegriff gestützt wurde, nicht wesentlich; andererseits ist es aber doch viel einfacher, da der hier zugrunde gelegte Geschlechtsbegriff nicht an den alten Ordnungsbegriff geknüpft ist und somit eine ganze Anzahl von Invarianten wegfallen.

Zunächst beschränke ich mich auf gerade Variablenzahl. Diese, die Signatur σ, die Kerndiskriminante $\Delta(X)$ und das System der *Charaktere*

$$\left.\begin{aligned} \chi_p(X) &= \begin{cases} 1 & \text{für } X \sim E^p, H^p, \Pi^p, N^p \bmod p, \\ -1 & \text{für } X \sim T^p, \Theta^p, P^p, M^p \bmod p, \end{cases} \quad p>2, \\ \chi_2(X) &= \begin{cases} 1 & \text{für } X \sim E^2, E_*^2, H^2, H_*^2, \Pi^2, N_*^2, P^2, M_*^2 \bmod 2, \\ -1 & \text{für } X \sim T^2, T_*^2, \Theta^2, \Theta_*^2, \Pi_*^2, N^2, P_*^2, M^2 \bmod 2. \end{cases} \end{aligned}\right\} \tag{30}$$

sind Invarianten. Aus ihnen lassen sich die X^p in eindeutiger Weise gewinnen, wie nun zu zeigen ist.

Mit $\Delta(X)$, das in der Form (28) gegeben sei, sind auch die Symbole

$$\delta_p(X) = \begin{cases} \left(\dfrac{\Delta(X)\,p^{-e_p}}{p}\right) & \text{für } p>2, \\ 1 & \text{für } p=2,\ \Delta(X)2^{-e_2} \equiv 1 \bmod 4, \\ -1 & \text{für } p=2,\ \Delta(X)2^{-e_2} \equiv -1 \bmod 4 \end{cases} \tag{31}$$

gegeben.

Man bekommt nun X^p aus folgender Tabelle:

		$p>2$		$p=2$			
				$\left(\frac{2}{\Delta(X)\,2^{-\varrho_2}}\right)=1$		$\left(\frac{2}{\Delta(X)\,2^{-\varrho_2}}\right)=-1$	
		$\chi_p(X)=1$	$\chi_p(X)=-1$	$\chi_2(X)=1$	$\chi_2(X)=-1$	$\chi_2(X)=1$	$\chi_2(X)=-1$
ϱ_p	$\delta_p(X)$	X^p		X^2			
0	1	E^p	—	E^2	—	E_*^2	—
	-1	H^p	—	—	—	—	—
1 bzw. 3	1	Π^p	M^p	Π^2	M^2	M_*^2	Π_*^2
	-1	N^p	P^p	P^2	N^2	N_*^2	P_*^2
2	1	—	T^p	—	T^2	—	T_*^2
	-1	—	Θ^p	H^2	Θ^2	H_*^2	Θ_*^2

(32)

Aus den Lücken in der Tabelle erkennt man, daß $\Delta(X)$ und die $\chi_p(X)$ nicht völlig beliebig vorgegeben werden können, es bestehen vielmehr gewisse Bindungen. Außer den angegebenen gilt noch die wichtige *Produktrelation*

$$\Pi\,\chi_p(X) = (-1)^{\frac{\sigma}{4}\left(\frac{\sigma}{2}-1\right)}, \tag{33}$$

zu erstrecken über sämtliche Primzahlen $p \geqq 2$, wo jedoch nur für endlich viele p, nämlich höchstens die Teiler von $\Delta(X)$ von 1 verschiedene Faktoren stehen.

Diese Formel läßt sich für die Typen Γ, Ω_p, Φ_p leicht verifizieren. Allgemein beweist man (33) durch Bezugnahme auf (15); es ist zu zeigen: gilt (33) für X_1, so auch für $X = X_1 + X_2$, wenn X_2 einer der Typen Γ, Ω_p, Φ_p ist ($p>2$). Die linke Seite von (33) werde dazu mit $P(X)$ bezeichnet.

Es sei $X_2 = \Gamma$. Jetzt ändern sich bei Addition von X_2 höchstens die Faktoren $\chi_p(X)$, wo $p \not\equiv 1 \bmod 4$ ist, da nur dann $X_2 \not\sim E^p \bmod p$ ist. Sämtliche $\chi_p(X)$ mit $p \equiv 3 \bmod 4$ gehen in die entgegengesetzten Werte über, wenn p genau einmal in der Kerndiskriminante von X_1 aufgeht, sonst bleibt $\chi_p(X)$ ungeändert. $\chi_2(X)$ ändert sich, wenn $X_1 \sim H^2$,

H_*^2, Θ^2, Θ_*^2, P^2, P_*^2, N^2, N_*^2 mod 2, also wenn $\Delta(X_1)\,2^{-\varrho_2} \equiv 3 \bmod 4$ ist, in den übrigen Fällen, also für $\Delta(X_1)\,2^{-\varrho_2} \equiv 1 \bmod 4$ bleibt $\chi_2(X)$ ungeändert. Da

$$\Delta(X_1)\,2^{-\varrho_2} \equiv (-1)^{\frac{\sigma}{2}-1}\,\Pi p \qquad \bmod 4$$

ist, wo p die ungeraden Verzweigungsstellen 1. Art durchläuft, gilt nunmehr

$$P(X) = (-1)^{\frac{\sigma}{2}} P(X_1)\ ,$$

in Übereinstimmung mit (33).

Es sei $X_2 = \Omega_p$. Jetzt gilt

$$\chi_p(X_1 + X_2) = \chi_p(X_1)\cdot\chi_p(X_2) \quad \text{für} \quad X_2 \sim E^p, T^p \mod p\ . \tag{34}$$

Da (33) für X_1 und X_2 gilt, und da X_1 und X die gleiche Signatur σ, X_2 dagegen die Signatur 0 haben, gilt (33) auch für X.

Es sei $X_2 = \Phi_p$, $p \equiv 1 \bmod 4$. Ist q eine ungerade in der Kerndiskriminante $\Delta(X_1)$ von X_1 aufgehende Primzahl, so ändert $\chi_q(X)$ dann und nur dann das Vorzeichen, wenn q Verzweigungsstelle 1. Art ist und $\left(\frac{p}{q}\right) = -1$. $\chi_2(X)$ ändert sich, wenn 2 eine Verzweigungsstelle 1. Art ist und $p \equiv 5 \bmod 8$ ist, sonst nicht. Also erhält $P(X)$ zunächst einmal den Faktor

$$\left(\frac{2^{\varrho_2}}{p}\right) \prod_{q\neq 2,\, q\neq p} \left(\frac{p}{q}\right)\ .$$

Es kommt aber noch der weitere Charakter $\chi_p(X)$ hinzu, wenn

$$(\Delta(X_1), p) = 1$$

war, er hat dann den Wert $\left(\frac{\Delta(X_1)}{p}\right)$. Mithin ist

$$P(X) = P(X_1)\left(\frac{\Delta(X_1)}{p}\right)\left(\frac{2^{\varrho_2}}{p}\right) \prod_{q\neq 2,\, q\neq p} \left(\frac{p}{q}\right)\ ,$$

das ist nach dem Reziprozitätsgesetz

$$P(X) = P(X_1)\ .$$

Da die Signatur sich nicht ändert, bleibt (33) mithin bei Addition dieses X_2 bestehen.

Schließlich sei $X_2 = \Phi_p$, $p \equiv 3 \bmod 4$. Ist q wieder eine Verzweigungsstelle 1. Art von X_1 und $\left(\frac{p}{q}\right) = -1$, so ändert sich $\chi_q(X)$, und nur dann. $\chi_2(X)$ ändert sich in der gleichen Art wie bei Addition von Γ, es kommt allerdings noch der Faktor $\left(\frac{2^{e_2}}{p}\right)$ hinzu. Wieder tritt gegebenenfalls $\chi_p(X)$ als neuer Charakter auf, er hat den Wert $\left(\frac{\Delta(X_1)}{p}\right)$. Es ist mithin

$$P(X) = P(X_1)\left(\frac{\Delta(X_1)}{p}\right)\left(\frac{2^{e_2}}{p}\right)(-1)^{\alpha} \prod_{q \neq 2,\, q \neq p} \left(\frac{p}{q}\right), \quad \alpha = \tfrac{1}{2}\left(\Delta(X_1)\, 2^{-e_2} - 1\right).$$

Nach dem Reziprozitätsgesetz ist also wieder

$$P(X) = P(X_1) ,$$

womit (33) allgemein bewiesen ist.

Weitere Bindungen zwischen den Invarianten gibt es nicht. Hierzu ist zu zeigen, daß es zu jedem System von Größen σ, $\Delta(X)$, $\chi_p(X)$, welches mit ihnen verträglich ist, einen Formentyp X gibt. Um dies zu beweisen, berechne man die p-adischen Invarianten X^p aus der Tabelle (32) und setze X in Form der Summe (15) an, wobei die Summanden entsprechend Satz 1 zu nehmen sind. Signatur und Kerndiskriminante des so konstruierten rationalen Typs haben dann offenbar schon die vorgeschriebenen Werte. Es ist nur nachzuweisen, daß dasselbe auch für die Charaktere zutrifft.

Es sei zunächst q eine ungerade Primzahl. Die Summenrelation (27) für q ist, wie in § 3, Nr. 3, erkannt wurde, mit (29) identisch und kann daher als stets erfüllt angenommen werden, wenn $\Delta(X)$ die Form (28) hat. Die Bildung von X als Summe (15) legt den q-adischen Typ von X bereits auf eins der Typenpaare: E^q, H^q; T^q, Θ^q; Π^q, P^q; M^q, N^q fest. Die Werte von σ und $\Delta(X)$ erlauben nach (20) und (22) die Berechnung von $[X^\infty]^q$ und $[X^p]^q$; jetzt kann man nach der bereits als gültig nachgewiesenen Gleichung (27) für q das Symbol $[X^q]^q$ berechnen, und schließlich nach (23) den q-adischen Typ von X innerhalb der genannten Paare eindeutig fixieren. Dies alles geschieht in völliger Übereinstimmung mit den aus (32) entnommenen Werten für die lokalen Invarianten, es hat also X^q und damit $\chi_q(X)$ den vorgeschriebenen Wert für jede ungerade Primzahl q. Der Charakter $\chi_2(X)$ muß dann wegen der Produktrelation (33) ebenfalls den vorgeschriebenen Wert haben. Damit ist, zunächst für gerade Variablenzahl, das Folgende gezeigt:

III. Hauptsatz. *Variablenzahl n, Signatur σ, Kerndiskriminante $\Delta(X)$ und das System der Charaktere $\chi_p(X)$ bilden ein vollständiges System von Invarianten gegenüber rationaler Transformation. Die Invarianten unterliegen folgenden Bedingungen.*

1) *Die im II. Hauptsatz genannten Bedingungen für n.*

2) *$\Delta(X)$ ist bei geradem n ein Produkt* (28), *wobei $\varrho_p \leqq 2$ für $p > 2$ und $\varrho_2 = 0$, 2 oder 3 ist. Bei ungeradem n ist $\Delta(X)$ ein Produkt*

$$\Delta(X) = (-1)^{\frac{\sigma-1}{2}} \Pi p^{\varrho_p} \tag{35}$$

mit $\varrho_p \leqq 2$ für $p \geqq 2$.

3) *Wird $\delta_p(X)$ aus $\Delta(X)$ gemäß* (31) *berechnet, so sind nur solche Invariantenkombinationen möglich, für welche die Tabelle* (32) *keine Leerstelle hat.*

4. *Es gilt die Produktrelation* (33) *bzw.* (36).

Für Typen X ungerader Variablenzahl definiere man

$$\chi_p(X) = \chi_p(X + (1)) ,$$

was mit (34) im Einklang steht. Die an dritter und vierter Stelle genannten Bedingungen für die Invarianten übertragen sich damit auch auf ungerade Variablenzahl, die Produktrelation wird

$$\Pi \chi_p(X) = (-1)^{\frac{\varrho^2-1}{8}} . \tag{36}$$

Die Gestalt (35) der Kerndiskriminante ergibt sich aus Hilfssatz 1. Der Existenznachweis wird für $X - (1)$ an Stelle von X geführt.

2. Die Primteiler der Kerndiskriminante werden eingeteilt in *Kerndiskriminantenprimteiler erster* und *zweiter Art.* Diese Einteilung möge für ungerade Primzahlen mit der Einteilung in Verzweigungsstellen 1. und 2. Art übereinstimmen, die Primzahl 2 dagegen sei ein Kerndiskriminantenprimteiler 1. Art stets dann, wenn $\Delta(X)$ gerade ist, ausgenommen in den Fällen, wo X bzw. $X - (1) \sim T^2$ oder T_*^2 mod 2 ist, dann heiße 2 ein Kerndiskriminantenprimteiler 2. Art. Diese Einteilung hängt mit den Lücken in der Tabelle (32) zusammen; sie ist so gewählt worden, daß für die Kerndiskriminantenprimteiler p erster Art die Charaktere $\chi_p(X)$ beliebig vorgeschrieben werden können, während sie für alle übrigen Primzahlen bereits durch $\Delta(X)$ festgelegt sind. Damit ist gezeigt:

Satz 2. Es gibt bei a Kerndiskriminantenprimteilern 1. Art entweder gar kein oder 2^{a-1} Geschlechter mit vorgeschriebener Kerndiskriminante $\Delta(X)$, Signatur σ und Variablenzahl n[16]).

Satz 3. Ein Formentyp X gerader Variablenzahl gestattet eine Darstellung

$$X = X_2 + X_4 + \Psi \ , \tag{37}$$

wo X_2 eine binäre Form, X_4 eine quaternäre Form mit quadratischer Diskriminante (also die Normenform einer Idealklasse einer rationalen Quaternionenalgebra) und Ψ eine definite Form der Kerndiskriminante 1, deren Variablenzahl durch 8 teilbar ist, enthält. Dabei setzt sich $\Delta(X_2)$ aus den Kerndiskriminantenprimteilern 1. Art zusammen, und es ist für diese

$$\chi_p(X_2) = \begin{cases} \chi_p(X) & \text{für} \quad p \nmid \Delta(X_4) \ , \\ -\chi_p(X) & \text{für} \quad p \mid \Delta(X_4) \ . \end{cases} \tag{38}$$

Ein Formentyp ungerader Variablenzahl gestattet die Darstellung

$$X = X_1 + X_2 + \Psi \ , \tag{39}$$

wo X_1 eine unäre, X_2 eine binäre und Ψ eine definite Form mit der Kerndiskriminante 1 enthält.

Beweis. Die Normaldarstellung (37) bei gerader Variablenzahl erhält man aus (15), wenn man diese Formel so schreibt:

$$X = \left(\sum \Phi_{p_1} + \sum \Phi_{p_3} + \frac{\sigma_1}{2} \Gamma \right) + \left(\sum \Omega_{p_2} + \sum \Omega_{p_3} + 2\frac{\sigma_2}{2} \right) + \frac{\sigma - \sigma_1 - 2\sigma_2}{2} \Gamma \ ,$$

dabei seien $\frac{\sigma_1}{2}, \frac{\sigma_2}{2}$ gleich 0 oder ± 1 und so gewählt, daß

$$\frac{\sigma - \sigma_1 - 2\sigma_2}{2} \equiv 0 \mod 4 \tag{40}$$

gilt. Die Terme in der ersten Klammer geben einen Typ X_2 an, welcher nach dem II. Hauptsatz eine binäre Form enthält, die im zweiten einen Typ X_4, für den

$$X_4 = \begin{cases} E^p \bmod p & \text{für} \quad p \nmid \Delta(X_4) \ , \\ T^p \bmod p & \text{für} \quad p \mid \Delta(X_4) \end{cases} \qquad (p \geqq 2) \tag{41}$$

---

[16]) Wenn $\Delta \equiv 4 \bmod 8$ ist, gibt es 2^{a-1} dieser Geschlechter. Dazu kommen noch 2^{a-2} Geschlechter solcher Formen, für die 2 ein Kerndiskriminantenprimteiler 2. Art ist.

gilt, und der restliche Typ Ψ ist wegen (40)

$$\Psi = \frac{\sigma - \sigma_1 - 2\sigma_2}{2} \Gamma \sim E^p \bmod p \ . \qquad (p \geqq 2) \qquad (42)$$

Die Aussage über $\Delta(X_2)$ ergibt sich nun ohne weiteres, und ebenso (38), denn nach (34), (41), (42) ist $\chi_p(X_2) = \chi_p(X) \cdot \chi_p(X_4)$.

Ist die Variablenzahl ungerade, so bilde man die Normaldarstellung (37) zunächst für den Typ $X + (1)$, also

$$X = X_2 + X_4 - (1) + \Psi \ .$$

Es sei a eine ganze rationale zu $\Delta(X_2)$ teilerfremde Zahl, und zwar ein quadratischer Nichtrest für jeden ungeraden Primteiler von $\Delta(X_4)$ und $a \equiv 7 \bmod 8$, falls $\Delta(X_4)$ gerade ist. Dann ist

$$X_2' = X_4 - (1, a)$$

ein Typ, welcher für kein p mit T^p ähnlich ist, und dasselbe gilt für die beiden weiteren Typen

$$X_2'' = X_2 + X_2' \ , \qquad X_2''' = X_2'' - 2X_4 \ .$$

Sind σ_2, σ_4 die Signaturen von X_2, X_4, so haben X_2'', X_2''' die Signaturen $\sigma_2'' = \sigma_2 + \sigma_4 - 1 - \operatorname{sign}(a)$, $\sigma_2''' = \sigma_2 - \sigma_4 - 1 - \operatorname{sign}(a)$. Durch passende Wahl des Vorzeichens von a kann erreicht werden, daß $|\sigma_2''| \leqq 2$ oder $|\sigma_2'''| \leqq 2$ ist. Dann enthält X_2'' oder X_2''' nach dem II. Hauptsatz eine binäre Form. Es ist also eine der Darstellungen

$$X = (a) + X_2'' + \Psi = (a) + X_2'' + (\Psi + 2X_4)$$

von der behaupteten Art, da $2X_4$ und also auch $\Psi + 2X_4$ die Kerndiskrinante 1 hat. Der Satz 3 ist damit in vollem Umfange bewiesen.

§ 5. Stammformen

1. Da von jetzt ab die Stammformen im Mittelpunkt der Untersuchungen stehen sollen, stelle ich hier ihre Grundeigenschaften kurz zusammen; diese fallen bei gerader und ungerader Variablenzahl recht verschieden aus.

Eine Form ist offenbar dann und nur dann Stammform, wenn sie es hinsichtlich jeder Primzahl ist.

Eine Stammform $\mathfrak{F}$ ist zugleich auch Kernform. Schreibt man sie in der Gestalt (9), wo $\mathfrak{F}_1$ eine Kernform von möglichst kleiner Variablenzahl ist, so wird sich zeigen (zunächst für gerade Variablenzahl): $\mathfrak{F}$ ist dann und nur dann Stammform, wenn $\mathfrak{F}_1$ es ist.

Ist $\mathfrak{F}_1$ nicht Stammform, sondern verwandt mit $t\mathfrak{F}_1'$, wo $\mathfrak{F}_1'$ Stammform ist, so kann man durch Anwendung der Substitution

$$\begin{aligned} x_\nu' &= x_\nu \qquad (\nu = 1, 2, \ldots, m) \\ x_\nu' &= t\, x_\nu \qquad (\nu = m+1,\ m+2, \ldots, 2m) \end{aligned} \tag{43}$$

auf die ersten $2m$ Variablen und Abspaltung des Teilers t sehen, daß $\mathfrak{F}$ mit $\mathfrak{F}_0^{(2m)} + \mathfrak{F}_1'$ verwandt ist. Wenn also $\mathfrak{F}$ Stammform ist, so ist es auch $\mathfrak{F}_1$.

Die Variablenzahl sei nun gerade. Dann ändert sich die Diskriminante bei rationaler Transformation und Abspaltung von gemeinsamen Koeffiziententeilern um quadratische Faktoren. Ist jetzt $D(\mathfrak{F}_1)$ durch $p>2$ nur einmal teilbar, so ist es auch $D(\mathfrak{F})$, also $\mathfrak{F}$ ist Stammform. Das gleiche gilt für $p = 2$, wenn $D(\mathfrak{F}_1)$ durch 8 teilbar ist, denn wäre $\mathfrak{F}$ nicht Stammform, so gäbe es eine Form, deren Diskriminante nur einmal durch 2 teilbar ist, aber eine solche kann es offenbar bei gerader Variablenzahl nicht geben.

Es sei $D(\mathfrak{F}_1)$ und damit $D(\mathfrak{F})$ zweimal durch p teilbar, und $\mathfrak{F}$ sei nicht Stammform, jedoch Kernform; $\mathfrak{F}_1$ dagegen sei Stammform. Dann ist also $\mathfrak{F}$ mit dem p-fachen einer Form $\mathfrak{F}'$ mit $(D(\mathfrak{F}'), p) = 1$ verwandt. Diese ist dann vom Typ E^p oder H^p $(p>2)$ bzw. E_*^2 $(p = 2)$. Im ersteren Falle ist dann $p\mathfrak{F}' \approx \mathfrak{F}'$ und andererseits nach der Voraussetzung $p\mathfrak{F}' \approx \mathfrak{F}$, also $\mathfrak{F} \approx \mathfrak{F}'$, was aber der Annahme widerspricht, daß $\mathfrak{F}$ Kernform sein sollte. Im letzteren Falle wäre $\mathfrak{F} \approx p\mathfrak{F}'$ und $\mathfrak{F}_1$ vom Typ Θ^p $(p>2)$ bzw. T_*^2 $(p = 2)$, und auch jetzt ist $\mathfrak{F}_1$ nicht Stammform.

Aus dieser Schlußweise geht gleichzeitig hervor, daß Θ^p $(p>2)$ bzw. T_*^2 $(p = 2)$ die einzigen p-adischen Typen gerader Variablenzahl sind, welche keine p-adischen Stammformen enthalten.

Satz 4. Eine Kernform gerader Variablenzahl ist dann und nur dann Stammform, wenn sie für jeden Primteiler p ihrer Diskriminante in k_p nicht dem Typ Θ^p $(p>2)$ bzw. T_*^2 $(p = 2)$ angehört.

2. Bei ungerader Variablenzahl herrschen andere Verhältnisse. Zunächst kann jedoch $\mathfrak{F}$ wieder in der Gestalt (9) geschrieben werden, wo $\mathfrak{F}_1$ eine unäre oder ternäre Form ist. Diese kann man rational in folgende Gestalt transformieren:

$$\mathfrak{F}_1(x_{2m+1}, x_{2m+2}, x_{2m+3}) = \mathfrak{G}(x_{2m+1}, x_{2m+2}) + ax_{2m+3}^2 , \qquad (44)$$

falls $\mathfrak{F}_1$ nicht unär war; aber auch diesen Fall kann man mit erfassen, wenn man jetzt $\mathfrak{G} = x_{2m+1} \cdot x_{2m+2}$ nimmt (der triviale Fall, daß $\mathfrak{F}$ die Variablenzahl 1 hat, bleibt allerdings ausgeschlossen).

Bei dieser Darstellung (44) kann man im Falle $p > 2$ erreichen, daß $\mathfrak{G}$ den Koeffiziententeiler p hat, wenn $D(\mathfrak{F}_1)$ durch p^2 teilbar ist, und daß a durch p teilbar ist, wenn p nur einmal in $D(\mathfrak{F}_1)$ aufgeht. Jetzt kann man durch Anwendung der Substitution (43) mit $t = p$, ergänzt durch $x'_{2m+3} = p\, x_{2m+3}$, und Abspaltung des Teilers p den ersteren Fall in letzteren überführen. Liegt der letztere Fall vor, und ist $D(\mathfrak{G})$ quadratischer Rest mod p, so kann man wegen

$$\mathfrak{F}_0^{(2m)} + \mathfrak{G} \cong \mathfrak{F}_0^{(2m+2)}$$

nochmals eine Substitution der Determinante p^{m+1} auf $x_1, \ldots, x_{2m+2}$ anwenden und den Teiler p abspalten, so daß eine ganzzahlige Form entsteht, deren Diskriminante nicht mehr durch p teilbar ist.

Wenn hingegen $D(\mathfrak{G})$ quadratischer Nichtrest ist, so behaupte ich, daß $\mathfrak{F}$ Stammform ist: wäre nämlich $\mathfrak{F}$ nur Kernform, aber keine Stammform, so hätte man $\mathfrak{F} \approx p\,\mathfrak{F}'$ mit $(D(\mathfrak{F}'), p) = 1$. $\mathfrak{F}'$ wäre vom Typ (b) oder $H^p + (b)$ mit $(b, p) = 1$, also $\mathfrak{F}$ vom Typ $(b\,p)$ oder $\Theta^p + (b\,p)$. Es ist $\mathfrak{F} \sim \mathfrak{F}_1$, also wäre

$$\mathfrak{F}_1 \sim H^p + (a) = (b\,p) \quad \text{oder} \quad = \Theta^p + (b\,p) ,$$

wo a einmal durch p teilbar ist. Diese Gleichung besagt nach (4) bis (6):

$$H^p = E^p \quad \text{oder} \quad = \Theta^p ,$$

sie enthält also einen Widerspruch.

Nach der Festsetzung $\chi_p(X) = \chi_p(X + (1))$ für die Typen ungerader Variablenzahl und (30) ergibt sich für den zuletzt betrachteten Fall $\chi_p(\mathfrak{F}) = -1$. Damit ist, zunächst für die ungeraden Primzahlen, das folgende gezeigt:

Satz 5[17]**.** Eine Kernform $\mathfrak{F}$ ungerader Variablenzahl ist dann und nur dann Stammform, wenn ihre Diskriminante D quadratfrei ist, und wenn für jeden Primteiler p von D

$$\chi_p(\mathfrak{F}) = -1$$

[17]) Der Satz stammt von *H. Brandt.*

gilt. Die Anzahl der Primteiler von D ist gerade oder ungerade, je nachdem für die Signatur $\sigma \equiv 1, 7 \bmod 8$ oder $\sigma \equiv 3, 5 \bmod 8$ gilt.

Es sei jetzt $p = 2$. Die Kerndiskriminante ist höchstens zweimal durch 2 teilbar (Hilfssatz 1), also liegt bei gerader Kerndiskriminante in (44) einer der folgenden Fälle vor:

$$\begin{aligned} &1) \quad \mathfrak{G} \sim T_*^2 \sim 2E_*^2 && \bmod 2,\ a \text{ ungerade} ; \\ &2) \quad \mathfrak{G} \sim H^2, H_*^2, \Theta^2, \Theta_*^2 && \bmod 2,\ a \text{ ungerade} ; \\ &3) \quad \mathfrak{G} \sim E^2, E_*^2 && \bmod 2,\ a \text{ gerade} \quad . \end{aligned}$$

Im 1. Falle ist obige Schlußweise für $p > 2$ übertragbar, welche den 1. auf den 3. Fall zurückführt. Im 2. Falle ist eine Einzeldiskussion mit Hilfe der Tabelle (7) erforderlich; jetzt ist $\mathfrak{F}$ mit einer Form des 3. Falles oder dem Doppelten einer solchen Form ähnlich, nach dem I. Hauptsatz also verwandt. Damit bleibt der 3. Fall allein zu diskutieren übrig.

Bei gerader Kerndiskriminante kann also $\mathfrak{F}$ höchstens dann Stammform sein, wenn $\mathfrak{G}$ in (44) vom Typ E^2 oder E_*^2 ist und a einmal durch 2 teilbar, und jetzt ergibt die Übertragung der Schlußweise für $p > 2$, daß $\mathfrak{F}$ dann und nur dann Stammform ist, wenn $\mathfrak{G} \sim E_*^2$ ist. Der Charakter $\chi_2(\mathfrak{F})$ ist in diesem Falle gleich -1. Hiermit ist der Satz 5 bis auf die Aussage über die Anzahl der Teiler von D bewiesen. Diese letzte Aussage erhält man durch Bildung des Produktes aller Charaktere, es muß nach dem III. Hauptsatz den Wert (36) haben, woraus sich auch die letzte Behauptung ergibt.

Man erkennt, daß die Stammdiskriminante (§ 1, Nr. 2) sowohl bei gerader wie bei ungerader Variablenzahl eine Invariante des Geschlechts, ja sogar des Typs ist.

II. Idealtheorie der Formensysteme

§ 6. Die Transformatoren und Ideale

1. Ein System von Stammformen gleicher Variablenzahl n, Signatur σ und Diskriminante D sei vorgelegt, es seien $1, \mathfrak{F}_1, \ldots, \mathfrak{F}_h$ je ein Vertreter aus jeder Formenklasse dieses Systems. Eine Matrix $\mathfrak{T}_{ik}$ mit rationalen Koeffizienten heißt ein *Transformator*[18]), der *links zu* $\mathfrak{F}_1$ und *rechts zu* $\mathfrak{F}_k$ *gehört*, wenn

$$\dot{\mathfrak{T}}_{ik}\, \mathfrak{F}_i\, \mathfrak{T}_{ik} = t \cdot \mathfrak{F}_k \tag{45}$$

[18]) Diese Bezeichnung habe ich a. a. O.[7]) vorgeschlagen.

gilt, wo t eine rationale Zahl ist, diese heißt die *Norm von* $\mathfrak{T}_{ik}$: $t = N(\mathfrak{T}_{ik})$. Durch Determinantenbildung folgt

$$N(\mathfrak{T}_{ik}) = |\mathfrak{T}_{ik}|^{\frac{2}{n}} , \tag{46}$$

bei ungerader Variablenzahl muß also t stets eine Quadratzahl sein. Die Gleichung (45) kann man auch in symmetrischerer Form schreiben:

$$\mathfrak{F}_i \mathfrak{T}_{ik} = \tilde{\mathfrak{F}}_{ik} \mathfrak{F}_k \quad \text{mit} \quad \tilde{\mathfrak{T}}_{ik} = \dot{\mathfrak{T}}_{ik}^{-1} N(\mathfrak{T}_{ik}) . \tag{47}$$

$\mathfrak{T}^{-1}$ heißt der zu $\mathfrak{T}_{ik}$ *inverse* oder *reziproke Transformator*, er gehört rechts zu $\mathfrak{F}_i$ und links zu $\mathfrak{F}_k$. Sind $\mathfrak{F}_i$, $\mathfrak{F}_j$, $\mathfrak{F}_k$ drei Formen des Systems und $\mathfrak{T}_{ij}$ $\mathfrak{T}_{jk}$ Transformatoren, deren Zugehörigkeit zu diesen Formen durch die Indizes angedeutet ist, so kann man das *Produkt*

$$\mathfrak{T}_{ik} = \mathfrak{T}_{ij} \mathfrak{T}_{jk} \tag{48}$$

bilden; es ist ein Transformator, der links zu $\mathfrak{F}_i$ und rechts zu $\mathfrak{F}_k$ gehört.

Ein Transformator heißt *ganz*, wenn seine Koeffizientenmatrix aus ganzen Zahlen besteht. Sind $\mathfrak{T}_{ik}$ und $\mathfrak{T}_{ik}^{-1}$ ganz, so heißt $\mathfrak{T}_{ik}$ eine *Einheit*; für eine Einheit $\mathfrak{T}_{ik}$ stimmen die Formen $\mathfrak{F}_i$ und $\mathfrak{F}_k$ überein. Zwei Transformatoren $\mathfrak{T}_{ik}$ und $\mathfrak{T}'_{ik}$ heißen *rechtsseitig* bzw. *linksseitig assoziiert*, wenn es eine Einheit $\mathfrak{T}_{ii}$ bzw. $\mathfrak{T}_{kk}$ gibt, daß

$$\mathfrak{T}_{ik} = \mathfrak{T}_{ii} \mathfrak{T}'_{ik} \quad \text{bzw.} \quad = \mathfrak{T}'_{ik} \mathfrak{T}_{kk}$$

ist. Die Gesamtheiten rechtsseitig bzw. linksseitig assoziierter Transformatoren heißen *Rechtsideale* bzw. *Linksideale*; sie werden mit $[\mathfrak{T}_{ik})$ bzw. $(\mathfrak{T}_{ik}]$ bezeichnet. Als die *Norm* dieser Ideale ist selbstverständlich $N(\mathfrak{T}_{ik})$ zu definieren. Eine lineare Substitution $\mathfrak{T}_i$, welche $\mathfrak{F}_i$ in das t-fache einer Form $\mathfrak{F}$ gleicher Diskriminante transformiert, *erzeugt* ein Linksideal $(\mathfrak{T}_i]$ für $\mathfrak{F}_i$; dieses enthält mindestens einen Transformator $\mathfrak{T}_{ik} = \mathfrak{T}_i \mathfrak{U}$, wo $\mathfrak{U}$ eine unimodulare Substitution ist, welche $\mathfrak{F}$ in eine der Formen $\mathfrak{F}_k$ transformiert.

Ein ganzer Transformator $\mathfrak{T}_{ik}$ heißt *durch* einen ganzen Transformator $\mathfrak{T}_{ij}$ *von links teilbar*, wenn (48) mit einem ebenfalls ganzen $\mathfrak{T}_{jk}$ gilt, $\mathfrak{T}_{ij}$ heißt ein *Linksteiler* von $\mathfrak{T}_{ik}$. Ebenso ist $\mathfrak{T}_{ik}$ *durch* $\mathfrak{T}_{jk}$ *von rechts teilbar*, $\mathfrak{T}_{jk}$ ein *Rechtsteiler* von $\mathfrak{T}_{ik}$. Die Teilbarkeit ist eigentlich eine Eigenschaft der Ideale: jeder Transformator aus dem Linksideal $(\mathfrak{T}_{ij}]$ ist ein Linksteiler jedes Transformators aus dem Linksideal $(\mathfrak{T}_{ik}]$, und ebenso

ist jeder Transformator aus dem Rechtsideal $[\mathfrak{T}_{jk})$ ein Rechtsteiler jedes Transformators aus dem Rechtsideal $[\mathfrak{T}_{ik})$. Man könnte sagen: $(\mathfrak{T}_{ij}]$ ist ein Linksteiler von $(\mathfrak{T}_{ik}]$, $[\mathfrak{T}_{jk})$ ist ein Rechtsteiler von $[\mathfrak{T}_{ik})$. Anders als in der Idealtheorie der Algebren ist nicht jedes Linksideal zugleich ein Rechtsideal, und eine Multiplikation der Ideale hat anscheinend keinen Sinn. Jedoch gilt auch hier: die Anzahl der ganzen Ideale von gegebener Norm ist endlich, während es bei indefiniten Formen stets unendlich viele ganze Transformatoren gegebener Norm gibt.

Ein nur durch sich selbst und durch Einheiten teilbarer ganzer Transformator heißt ein *Primtransformator*, das durch ihn erzeugte Links- bzw. Rechtsideal ein *Primideal*. Jeder ganze Transformator läßt sich als Produkt von Primtransformatoren schreiben. Natürlich ist die Zerlegung i. a. nicht eindeutig. Jedoch überträgt sich die Eindeutigkeit der Primzerlegung im rationalen Zahlkörper, wenn man *primäre Transformatoren* einführt, das sind solche ganzen Transformatoren, deren Normen Potenzen von rationalen Primzahlen sind. Wie leicht zu sehen ist, gilt dann[19]:

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

2. Die Definitionen sind noch im Anschluß an die geometrischen Begriffsbildungen in § 1, Nr. 2, zu vervollständigen. Jeder der Formen $\mathfrak{F}_i$ werde ein Gitter $\mathfrak{J}_i$ in einem n-dimensionalen metrischen Raume R_i zugeordnet, dadurch daß für jeden Vektor $\mathfrak{t}_i$ aus $\mathfrak{J}_i$ vermittels

$$N(\mathfrak{t}_i) = \tfrac{1}{2}\dot{\mathfrak{t}}_i \mathfrak{F}_i \mathfrak{t}_i$$

eine *Norm* $N(\mathfrak{t}_i)$ definiert wird (hierbei wird $\mathfrak{t}_i$ gleichzeitig als eine einspaltige Matrix aufgefaßt, deren Elemente die Komponenten des Vektors $\mathfrak{t}_i$ sind). Ein ganzer Transformator $\mathfrak{T}_{ik}$ bildet vermöge der Gleichung

$$\mathfrak{t}_i = \mathfrak{T}_{ik}\mathfrak{t}_k \tag{49}$$

das Gitter $\mathfrak{J}_k$ auf ein Teilgitter von $\mathfrak{J}_i$ ab.

Besteht (49) mit ganzzahligen Vektoren $\mathfrak{t}_i$, $\mathfrak{t}_k$ (d. h. $\mathfrak{t}_i \subset \mathfrak{J}_i$, $\mathfrak{t}_k \subset \mathfrak{J}_k$) und ganzem $\mathfrak{T}_{ik}$, so heiße $\mathfrak{t}_i$ *durch* $\mathfrak{T}_{ik}$ *teilbar*; $\mathfrak{t}_i$ ist dann durch jeden Transformator aus dem Linksideal $(\mathfrak{T}_{ik}]$, d. h. kurz durch $(\mathfrak{T}_{ik}]$ teilbar. Eine notwendige Bedingung der Teilbarkeit ist die Teilbarkeit der Normen, denn es folgt aus (49):

$$N(\mathfrak{t}_i) = N(\mathfrak{T}_{ik})N(\mathfrak{t}_k)\ . \tag{50}$$

---

[19]) s. [7]), § 2.

Anders als in der Zahlentheorie der algebraischen Zahlkörper, wo die Gitterpunkte den ganzen Zahlen entsprechen, gibt es jetzt i. a. mehrere ganze Ideale $(\mathfrak{T}_{ik}]$ der Norm t, welche einen Vektor $\mathfrak{t}_i$ teilen, dessen Norm durch t teilbar ist; diese Anzahl wird sich als eine Funktion der Zahl t herausstellen, welche für das Formensystem charakteristisch ist. Interessant sind in diesem Zusammenhang die Verhältnisse bei nicht kommutativen einfachen Algebren, wo diese Anzahl bereits größer als 1 ist, jedoch noch leicht zu übersehen; vgl. hiezu § 8, Nr. 6.

3. Von besonderer Wichtigkeit ist der

Satz 6. *Die Norm eines Primtransformators ist eine rationale Primzahl p oder deren Quadrat p^2. Der erstere Fall liegt vor, wenn die Variablenzahl n gerade und D durch p teilbar oder ein quadratischer Rest mod p ist, der zweite, wenn n gerade und D ein quadratischer Nichtrest mod p ist oder wenn n ungerade ist.*

Entsprechend den beiden Möglichkeiten kann man die Primtransformatoren und natürlich auch die Primideale in *Primtransformatoren* bzw. *Primideale ersten* und *zweiten Grades* einteilen.

Der nicht ganz einfache Beweis für Satz 6 wird den Rest dieses Paragraphen ausfüllen. Er darf offenbar in der p-adischen Erweiterung k_p von k geführt werden, wo p irgendeine rationale Primzahl ist; hierbei kann man von der Möglichkeit Gebrauch machen, die Formen auf eine einfache Normalgestalt zu transformieren.

Es sei $\mathfrak{T}_{ik}$ ein ganzer Transformator der Norm p^δ. Mit zwei unimodularen Matrizen $\mathfrak{U}$, $\mathfrak{V}$ gelte

$$\mathfrak{T}_{ik} = \mathfrak{U} \begin{pmatrix} p^{\delta_1} & & & \\ & \ddots & & \\ & & p^{\delta_2} & \\ & & & \ddots \end{pmatrix} \mathfrak{V} ,$$

wo $p^{\delta_1}, \ldots$ (r_1-mal), $p^{\delta_2}, \ldots$ (r_2-mal), $\ldots, p^{\delta_m}, \ldots$ (r_m-mal) mit

$$\delta_1 < \delta_2 < \cdots < \delta_m$$

das System der Elementarteiler von $\mathfrak{T}_{ik}$ ist. Dabei ist also

$$r_1 \delta_1 + r_2 \delta_2 + \cdots + r_m \delta_m = \frac{n}{2} \delta . \tag{51}$$

Indem man $\mathfrak{F}_i$ mit $\mathfrak{U}$, $\mathfrak{F}_k$ mit $\mathfrak{V}^{-1}$ transformiert, kommt man zu zwei Formen $\mathfrak{F}'_i$, $\mathfrak{F}'_k$ und einem Transformator $\mathfrak{T}'_{ik}$ in Diagonalgestalt, welcher

$\mathfrak{F}_i'$ in $p \cdot \mathfrak{F}_k'$ transformiert. Es beschränkt die Allgemeinheit also nicht, wenn man gleich $\mathfrak{T}_{ik}$ in dieser Gestalt voraussetzt.

Ist $\delta_1 > 0$, so ist $p\,\mathfrak{E}^{(n)}$ ein Teiler von $\mathfrak{T}_{ik}$, es ist also zu zeigen, daß $p\,\mathfrak{E}^{(n)}$ je nach den in Satz 6 genannten Umständen zerlegbar ist oder nicht. Bei ungeradem n ist $p\,\mathfrak{E}^{(n)}$ offenbar nicht weiter zerlegbar, denn $p\,\mathfrak{E}^{(n)}$ hat die Norm p^2, und die Norm jedes Transformators muß eine Quadratzahl sein. Bei geradem n hingegen ist nach § 5, Nr. 1:

$$\mathfrak{F}_i \cong \begin{pmatrix} \mathfrak{F}_0^{(n-2)} & \\ & \mathfrak{G}^{(2)} \end{pmatrix} \quad \text{oder} \quad \mathfrak{F}_i \cong \begin{pmatrix} \mathfrak{F}_0^{(n-4)} & \\ & \mathfrak{G}^{(4)} \end{pmatrix},$$

wo $\mathfrak{G}^{(2)}$ eine binäre p-adische Stammform und $\mathfrak{G}^{(4)}$ die einzige quaternäre p-adische Stammform ist; sie gehört zum Typ T^p. Die Diskriminante von $\mathfrak{G}^{(2)}$ bzw. $\mathfrak{G}^{(4)}$ stimmt mit D überein. Man kann nun stets eine ganzzahlige Matrix $\mathfrak{P}^{(2)}$ bzw. $\mathfrak{P}^{(4)}$ angeben, welche $\mathfrak{G}^{(2)}$ bzw. $\mathfrak{G}^{(4)}$ in das p-fache einer Form gleicher Diskriminante transformiert, mit alleiniger Ausnahme des Falles, daß $\mathfrak{F}_i$ von der ersten Form ist und $\mathfrak{G}^{(2)}$ zum Typ H^p $(p>2)$ oder E_*^2 $(p=2)$ gehört, d. h. also, daß $\left(\frac{D}{p}\right) = -1$ ist. Dann erzeugt die lineare Substitution

$$\mathfrak{P}^{(n)} = \begin{pmatrix} \mathfrak{E}^{\left(\frac{n}{2}-1\right)} & & \\ & p\,\mathfrak{E}^{\left(\frac{n}{2}-1\right)} & \\ & & \mathfrak{P}^{(2)} \end{pmatrix} \text{ bzw. } = \begin{pmatrix} \mathfrak{E}^{\left(\frac{n}{2}-2\right)} & & \\ & p\,\mathfrak{E}^{\left(\frac{n}{2}-2\right)} & \\ & & \mathfrak{P}^{(4)} \end{pmatrix}$$

ein Primlinksideal $(\mathfrak{P}^{(n)}]$ der Norm p, das links zu $\mathfrak{F}_i$ gehört, und das $p\,\mathfrak{E}^{(n)}$ von links teilt.

Ist umgekehrt $\mathfrak{P}^{(n)}$ eine solche Substitution, so besteht ihr Elementarteilersystem offenbar nur aus 1 und p, und zwar muß wegen (51) jede dieser Zahlen $\frac{n}{2}$-mal vorkommen. Wiederum beschränkt es die Allgemeinheit nicht, wenn man

$$\mathfrak{P}^{(n)} = \begin{pmatrix} \mathfrak{E}^{\left(\frac{n}{2}\right)} & \\ & p\,\mathfrak{E}^{\left(\frac{n}{2}\right)} \end{pmatrix}$$

annimmt. Es muß nun

$$\mathfrak{F}_i = \begin{pmatrix} \mathfrak{F}_{11}^{\left(\frac{n}{2}\right)} & \mathfrak{F}_{12}^{\left(\frac{n}{2}\right)} \\ \dot{\mathfrak{F}}_{12}^{\left(\frac{n}{2}\right)} & \mathfrak{F}_{22}^{\left(\frac{n}{2}\right)} \end{pmatrix}, \qquad \mathfrak{F}_{11}^{\left(\frac{n}{2}\right)} \equiv \mathfrak{O}^{\left(\frac{n}{2}\right)} \bmod p$$

sein, und Determinantenbildung ergibt

$$D \equiv \left| \mathfrak{F}_{12}^{\left(\frac{n}{2}\right)} \right|^2 \bmod p \ ,$$

es kann also nicht $\left(\frac{D}{p}\right) = -1$ sein.

Die Zerlegung des Transformators $p\,\mathfrak{E}^{(n)}$ steht also im Einklang mit der Behauptung.

4. Nicht jeder Primtransformator braucht ein Teiler von $p\,\mathfrak{E}^{(n)}$ zu sein, es ist nun zu zeigen, daß die Behauptung auch für die übrigen Primtransformatoren zutrifft. Die oben erklärte Zahl δ_1 darf jetzt gleich Null angenommen werden. Ich zeige zunächst:

$$r_1 = r_m \ , \qquad \delta_m = \delta \ , \tag{52}$$

d. h. der letzte Elementarteiler ist gleich der Norm, er tritt ebenso oft auf wie der erste.

Wegen

$$\dot{\mathfrak{T}}_{ik}\,\mathfrak{F}_i\,\mathfrak{T}_{ik} \equiv \mathfrak{O}^{(n)} \bmod p$$

gelten für die Elemente f_{ik} der Matrix $\mathfrak{F}_i$ folgende Kongruenzen (für $p=2$ beachte man die „Bemerkungen zur Formelschreibweise" in der Einleitung!):

$$\left.\begin{array}{lll} f_{ik} \equiv 0 \bmod p^{\delta} & \text{für } i = 1,\ldots,r_1 ; & k = 1,\ldots,r_1 \ , \\ f_{ik} \equiv 0 \bmod p^{\delta-\delta_2} & \text{für } i = 1,\ldots,r_1 ; & k = r_1+1,\ldots,r_1+r_2 \ , \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & & \\ f_{ik} \equiv 0 \bmod p^{\delta-\delta_m} & \text{für } i = 1,\ldots,r_1 ; & k = n-r_m+1,\ldots,n \ . \end{array}\right\} \tag{53}$$

Hiernach ist stets $\delta \geqq \delta_m$.

Ist $\delta = 1$, so kann nur $\delta_m = 1$ sein, und nach (51) $r_1 = r_2 = \frac{n}{2}$, d. h. (52) ist in diesem Falle richtig. Von jetzt ab sei $\delta > 1$. Dann sind die in (53) zuerst genannten Zahlen f_{ik} jedenfalls durch p^2 teilbar.

Wäre nun $\delta > \delta_m$ oder zwar $\delta = \delta_m$ aber $r_m < r_1$, so wären die r_1 ersten Zeilen von $\mathfrak{F}_i$ mod p linear abhängig. Jetzt könnte man auf $\mathfrak{F}_i$ eine unimodulare Substitution

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{S}_1^{(r_1)} & \\ & \mathfrak{E}^{(n-r_1)} \end{pmatrix}$$

ausüben, welche $\mathfrak{F}_1$ in eine äquivalente Form $\mathfrak{F}_i'$ überführt, wobei die ganze erste Zeile der Koeffizientenmatrix von $\mathfrak{F}_i'$ durch p teilbar ist. Wegen der besonderen Gestalt von $\mathfrak{S}$ und der Teilbarkeit der f_{ik} für i, $k = 1, \ldots, r_1$ durch p^2 wäre der Koeffizient von $\mathfrak{F}_i'$ mit dem Indexpaar 11 sogar durch p^2 teilbar. Dann könnte aber $\mathfrak{F}_i'$ und damit auch $\mathfrak{F}_i$ keine Stammform sein, im Gegensatz zu der Voraussetzung. Mithin ist $\delta_m = \delta$ und $r_m \geqq r_1$. Ersetzt man $\mathfrak{F}_i$ durch $\mathfrak{F}_k$, $\mathfrak{T}_{ik}$ durch $p^{\delta} \cdot \mathfrak{T}_{ik}^{-1}$, so vertauschen r_1 und r_m ihre Rollen, es ist also auch $r_m \leqq r_1$, womit (52) bewiesen ist. Es ist gleichzeitig gezeigt, daß der Rang der Matrix der r_1 ersten Zeilen von $\mathfrak{F}_i$ mod p gleich r_1 ist.

Nach dieser Vorbereitung teile man $\mathfrak{F}_i$ folgendermaßen in Teilmatrizen auf:

$$\mathfrak{F}_i = \begin{pmatrix} \mathfrak{F}_{11}^{(r_1)} & \mathfrak{f}_{12}^{(r_1, n-2r_1)} & \mathfrak{f}_{13}^{(r_1, r_1)} \\ \dot{\mathfrak{f}}_{12} & \mathfrak{F}_{22}^{(n-2r_1)} & \mathfrak{f}_{23}^{(n-2r_1, r_1)} \\ \dot{\mathfrak{f}}_{13} & \dot{\mathfrak{f}}_{23} & \mathfrak{F}_{33}^{(r_1)} \end{pmatrix}, \tag{54}$$

dabei ist nach (53)

$$\mathfrak{F}_{11}^{(r_1)} \equiv \mathfrak{O}^{(r_1)} \mod p^2, \quad \mathfrak{f}_{12}^{(r_1, n-2r_1)} \equiv \mathfrak{o}^{(r_1, n-2r_1)} \mod p, \quad (|\mathfrak{f}_{13}^{(r_1, r_1)}|, p) = 1. \tag{55}$$

Nach (54), (55) definiert

$$\mathfrak{D} = \begin{pmatrix} \mathfrak{E}^{(r_1)} & & \\ & p\,\mathfrak{E}^{(n-2r_1)} & \\ & & p^2\,\mathfrak{E}^{(r_1)} \end{pmatrix}$$

ein Linksideal $(\mathfrak{D}]$ der Norm p^2, welches links zu $\mathfrak{F}_i$ gehört und $\mathfrak{T}_{ik}$ von links teilt. Es ist für $n = 2r_1$ in ersichtlicher Weise zerlegbar, in diesem Falle ist also nichts mehr zu beweisen.

Folglich bleibt jetzt noch zu zeigen übrig: $(\mathfrak{D}]$ ist weiter zerlegbar, wenn n gerade, $> 2r_1$ und $\left(\frac{D}{p}\right) \neq -1$ ist. Wegen (54), (55) ist

$$\left(\frac{D}{p}\right) = \left(\frac{D(\mathfrak{F}_{22}^{(n-2r_1)})}{p}\right),$$

hat dieses Symbol den Wert 1, so gibt es nach Nr. 3 ein Primlinksideal der Norm p für die Form $\mathfrak{F}_{22}^{(n-2r_1)}$, es werde erzeugt durch eine Substitution $\mathfrak{P}^{(n-2r_1)}$, welche ein Teiler von $p\,\mathfrak{E}^{(n-2r_1)}$ ist, folglich erzeugt

$$\mathfrak{P}^{(n)} = \begin{pmatrix} \mathfrak{E}^{(r_1)} & & \\ & \mathfrak{P}^{(n-2r_1)} & \\ & & p\,\mathfrak{E}^{(r_1)} \end{pmatrix}$$

ein Primlinksideal $(\mathfrak{P}^{(n)}]$ der Norm p für $\mathfrak{F}_i$, welches $(\mathfrak{D}]$ teilt.

Dieselbe Schlußweise ist richtig, wenn $D(\mathfrak{F}_{22}^{(n-2r_1)}) \equiv 0 \bmod p$ ist, und wenn man nur noch nachweist, daß $\mathfrak{F}_{22}^{(n-2r_1)}$ eine Stammform ist.

5. Zu diesem Nachweis beachte man zunächst: sind $\mathfrak{F}$, $\mathfrak{G}$ irgend zwei ganzzahlige Formen, so ist $\mathfrak{F}$ dann und nur dann eine p-adische Stammform, wenn $\mathfrak{F} + p\,\mathfrak{G}$ eine p-adische Stammform ist. Die ganz elementare Begründung hierfür darf übergangen werden. Man transformiere nun $\mathfrak{F}_i$ mit

$$\begin{pmatrix} \mathfrak{E}^{(r_1)} & & \\ & \mathfrak{E}^{(n-2r_1)} & \\ & -p\,\mathfrak{U}^{(r_1,n-2r_1)} & \mathfrak{E}^{(r_1)} \end{pmatrix},$$

wo $\mathfrak{U}^{(r_1,n-2r_1)}$ aus dem Kongruenzensystem

$$\frac{1}{p}\,\mathfrak{f}_{12}^{(r_1,n-2r_1)} \equiv \mathfrak{f}_{13}^{(r_1,r_1)}\,\mathfrak{U}^{(r_1,n-2r_1)} \bmod p$$

zu bestimmen ist, welches nach (55) auch wirklich eine ganzzahlige Auflösung besitzt. $\mathfrak{F}_i$ geht dann in ähnliche Gestalt über, wobei jedoch an Stelle von (55) sogar

$$\mathfrak{F}_{11}^{(r_1)} \equiv \mathfrak{D}^{(r_1)} \bmod p^2\,, \quad f_{12}^{(r_1,n-2r_1)} \equiv \mathfrak{d}^{(r_1,n-2r_1)} \bmod p^2 \qquad (56)$$

gilt. Die neue „innere" Teilmatrix $\mathfrak{F}_{22}^{(n-2r_1)}$ ist der alten mod p kongruent, also zugleich mit dieser die Koeffizientenmatrix einer Stammform oder nicht.

Wäre $\mathfrak{F}_{22}^{(n-2r_1)}$ keine Kernform, so gäbe es eine Substitution $\mathfrak{U}^{(n-2r_1)}$, welche $\mathfrak{F}_{22}^{(n-2r_1)}$ in eine ganzzahlige Form kleinerer Diskriminante transformiert, wobei $p \cdot \mathfrak{U}^{(n-2r_1)}$ ganzzahlig ist. Dann transformierte

$$\mathfrak{U}^{(n)} = \begin{pmatrix} \frac{1}{p}\mathfrak{E}^{(r_1)} & & \\ & \mathfrak{U}^{(n-2r_1)} & \\ & & p\mathfrak{E}^{(r_1)} \end{pmatrix}$$

wegen (56) die Form $\mathfrak{F}_i$ in eine ganzzahlige Form kleinerer Diskriminante, was jedoch der Stammformeneigenschaft von $\mathfrak{F}_i$ widerspricht. Wäre $\mathfrak{F}_i$ wohl Kernform aber nicht Stammform, so wäre nach § 5, Nr. 1

$$\mathfrak{F}_{22}^{(n-2r_1)} \cong \begin{pmatrix} \mathfrak{F}_0^{(n-2r_1-2)} & & \\ & p & \\ & & -vp \end{pmatrix},$$

wo v ein quadratischer Nichtrest mod p ist ($v = 5$ für $p = 2$). Nimmt man $\mathfrak{F}_{22}^{(n-2r_1)}$ in dieser Gestalt an, so transformierte nun

$$\begin{pmatrix} \mathfrak{E}^{\left(\frac{n}{2}-1\right)} & & \\ & p\mathfrak{E}^{\left(\frac{n}{2}-r_1-1\right)} & \\ & & \mathfrak{E}^{(r_1+2)} \end{pmatrix}$$

die Form $\mathfrak{F}_i$ in das p-fache einer anderen, deren Diskriminante dann ersichtlich weniger oft durch p teilbar sein müßte, was auch einen Widerspruch darstellt. Damit ist der Beweis des Satzes 6 vollständig.

§ 7. Klassen und Geschlechter von Transformatoren

1. Zwei Transformatoren $\mathfrak{T}_{ik}$ und $\mathfrak{T}_{jl}$ sollen *äquivalent* heißen, wenn sie links und rechts zu den gleichen Formen gehören, d. h. wenn $i = j$, $k = l$ ist. Transformatoren $\mathfrak{T}_{ii}$, welche links und rechts zur selben Form gehören, heißen *Haupttransformatoren*. Diese bilden jeweils eine Gruppe. Die Gesamtheiten äquivalenter Transformatoren werden *Transformatorenklassen* genannt.

Zwischen den Transformatorenklassen läßt sich eine Multiplikation erklären, indem man aus ihnen einzelne Repräsentanten herausgreift und diese multipliziert. In diesem Zusammenhang gilt

Satz 7. *Die Transformatoren eines Systems von Stammformen gleicher Variablenzahl, Signatur und Diskriminante bilden ein Gruppoid. Die Transformatorenklassen bilden ein Gruppoid von der Ordnung 1 und vom Rang h, wenn h die Anzahl der Formenklassen in diesem System ist.*

2. Der Beweis ist selbstverständlich bis auf die Tatsache, daß es zu zwei Formen $\mathfrak{F}_i$, $\mathfrak{F}_k$ des Systems stets einen links zu $\mathfrak{F}_i$ und rechts zu $\mathfrak{F}_k$ gehörigen Transformator $\mathfrak{T}_{ik}$ gibt. Gehören $\mathfrak{F}_i$ und $\mathfrak{F}_k$ dem gleichen Geschlecht an, so ist auch diese Tatsache klar. Nach Satz 5 ist Satz 7 also bereits für ungerade Variablenzahl bewiesen.

Um den Satz 7 allgemein zu beweisen, teile ich bei gerader Variablenzahl die Transformatoren in *Geschlechter* ein, indem ich ihnen mittels

$$\psi_p(\mathfrak{T}_{ik}) = \frac{\chi_p(\mathfrak{F}_i)}{\chi_p(\mathfrak{F}_k)} \tag{57}$$

ein System von *Charakteren* für alle Diskriminantenprimteiler 1. Art zuordne. Wegen (33) gilt für sie die *Produktrelation*

$$\prod_p \psi_p(\mathfrak{T}_{ik}) = 1 \ . \tag{58}$$

Transformatoren mit gleichen Charakteren bilden ein Geschlecht; ein solches umfaßt stets (eine oder mehrere) volle Klassen. Ebenso wie für die Transformatorenklassen kann man auch für die Geschlechter eine Multiplikation erklären, dabei gilt der

Satz 8. Die Geschlechter der Transformatoren bilden eine Abelsche Gruppe der Ordnung 2^{a-1} und des Typs $(2, \ldots, 2)$ bei a Diskriminantenprimteilern 1. Art.

Beweis. Die Behauptungen sind klar bis auf die Aussage über die Anzahl der Geschlechter. Nach (58) kann sie offenbar nicht größer als angegeben sein. Es ist also, wie üblich in der Theorie der algebraischen Zahlkörper, zu beweisen, daß alle denkbaren Geschlechter wirklich existieren.

Es sei p eine ungerade Primzahl, welche in der Diskriminante genau einmal aufgeht, und $\mathfrak{T}_{ik}$ ein ganzer Transformator mit zu p teilerfremder Norm. Dann ist

$$\chi_p(\mathfrak{F}_i) = \chi_p\big(N(\mathfrak{T}_{ik}) \cdot \mathfrak{F}_k\big) \ ,$$

nach (57) und (30) also

$$\psi_p(\mathfrak{T}_{ik}) = \left(\frac{N(\mathfrak{T}_{ik})}{p}\right) \ . \tag{59}$$

Die Diskriminante hat die Gestalt

$$D = (-1)^{\frac{\sigma}{2}} 2^{\varrho_2} P A^2 \ , \tag{60}$$

wo P das Produkt der ungeraden Diskriminantenprimteiler 1. Art ist und A eine zu $2P$ teilerfremde ganze Zahl.

Ein System von a Zahlen $\psi_p = \pm 1$ mit dem Produkt 1 sei vorgegeben, wo p die a Diskriminantenprimteiler 1. Art durchlaufen möge. Es werde nun eine Primzahl q bestimmt, welche den Kongruenzen

$$\left(\frac{q}{p}\right) = \psi_p \tag{61}$$

für alle ungeraden p und

$$q \equiv \begin{cases} 1 \bmod 4 & \text{für } \varrho_2 = 0\ , \\ 1 \bmod 8 & \text{für } \varrho_2 = 3\ , \quad \psi_2 = \ \ 1\ , \\ 5 \bmod 8 & \text{für } \varrho_2 = 3\ , \quad \psi_2 = -1\ , \\ 1 \bmod 4 & \text{für } \varrho_2 = 2\ , \quad \psi_2 = \ \ 1\ , \\ 3 \bmod 4 & \text{für } \varrho_2 = 2\ , \quad \psi_2 = -1 \end{cases} \tag{62}$$

genügt. Der letzte Fall kann offenbar nur dann eintreten, wenn

$$(-1)^{\frac{\sigma}{2}} P \equiv 3 \bmod 4 \tag{63}$$

ist, denn sonst wäre D nicht Stammdiskriminante. Nach (60) bis (63) und dem quadratischen Reziprozitätsgesetz ist dann

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

und nach Satz 6 gibt es einen ganzen Transformator $\mathfrak{T}_{ik}$ mit der Norm q. Er erfüllt für sämtliche ungeraden Diskriminantenprimteiler 1. Art wegen (59) und (61) die Gleichungen

$$\psi_p(\mathfrak{T}_{ik}) = \psi_p\ ,$$

nach der Produktrelation also auch für $p = 2$. Aus dieser Schlußweise geht die Richtigkeit des Satzes 8 hervor.

Mit Satz 8 schließt sich gleichzeitig die letzte Lücke im Beweis für Satz 7: es gibt hiernach ebensoviele Geschlechter von Transformatoren wie Formengeschlechter (Satz 2), mithin sind letztere sämtlich durch geeignete Transformatoren untereinander verbunden.

§ 8. Die Primideale ersten Grades

1. In diesem Paragraphen werden eine Reihe von elementaren Einzeltatsachen der Theorie der quadratischen Formen in dem Restklassenring der ganzen Zahlen nach einer Primzahlpotenz p^α gebracht, wobei

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

und die Variablenzahl $n = 2m$ gerade ist. Es handelt sich also um die Zahlentheorie der speziellen Form $\mathfrak{F}_0^{(2m)}$ bzw. ihrer Klasse.

Eine ganzzahlige Matrix $\mathfrak{U}$ heißt eine *Einheit von* $\mathfrak{F}$ *mod* p^α, wenn

$$\dot{\mathfrak{U}}\,\mathfrak{F}\,\mathfrak{U} \equiv \mathfrak{F} \mod p^\alpha$$

ist. Die Einheiten mod p^α bilden eine Gruppe. Ihre Ordnung ist für $\alpha = 1$, $p > 2$ bekanntlich[20]) gleich

$$2p^{m(m-1)}(p^m - 1)\prod_{k=1}^{m-1}(p^{2k} - 1)\,. \tag{64}$$

Zwei ganzzahlige Vektoren $\mathfrak{x}$ und $\mathfrak{y}$ sollen *mod* p^α *äquivalent* heißen, wenn es eine Einheit $\mathfrak{U}$ von $\mathfrak{F}$ mod p gibt, so daß

$$\mathfrak{y} = \mathfrak{U}\,\mathfrak{x}$$

gilt. Ich beweise zunächst den

Hilfssatz 4. Zwei ganzzahlige, vom Nullvektor mod p verschiedene Vektoren $\mathfrak{x}$ und $\mathfrak{y}$ sind dann und nur dann mod p äquivalent, wenn

$$N(\mathfrak{x}) \equiv N(\mathfrak{y}) \mod p$$

ist.

Beweis. Daß die genannte Bedingung notwendig ist, ist klar. Es beschränkt die Allgemeinheit nicht, wenn man $\mathfrak{F} = \mathfrak{F}_0^{(2m)}$ annimmt. Es gibt jetzt folgende speziellen Einheiten von $\mathfrak{F}$ mod p:

$$\mathfrak{U} \equiv \begin{pmatrix} \mathfrak{B} & \\ \dot{\mathfrak{B}}^{-1}\mathfrak{S} & \dot{\mathfrak{B}}^{-1} \end{pmatrix} \mod p\,, \tag{65}$$

wo $\mathfrak{B}$ und $\mathfrak{S}$ m-reihige quadratische Matrizen sind und

$$\mathfrak{S} + \dot{\mathfrak{S}} \equiv \mathfrak{O}^{(m)} \mod p\,, \tag{66}$$

d. h. für $p = 2$ nach der eingangs getroffenen Verabredung: $\frac{1}{2}(\mathfrak{S} + \dot{\mathfrak{S}})$ ist eine symmetrische Matrix mit geraden Diagonalengliedern. Eine weitere Einheit von $\mathfrak{F} = \mathfrak{F}_0^{(2m)}$ ist $\mathfrak{F}_0^{(2m)}$ selbst.

Durch Anwendung einer Einheit (65) mit $\mathfrak{S} = \mathfrak{O}^{(m)}$ auf $\mathfrak{x}$ kann man

---

[20]) Vgl. etwa *B. L. van der Waerden*, Gruppen von linearen Transformationen, Ergebn. d. Math. IV, 2, Berlin 1935, S. 15. Dort liegt offensichtlich (z. B. für $n = 2$) ein Druckfehler vor. Das Original: *L. E. Dickson*, Linear Groups, Leipzig und Berlin 1901, nach dem v. d. Waerden zitiert, ist mir leider nicht zugänglich.

bei passender Wahl von $\mathfrak{B}$ zunächst erreichen, daß die Komponenten $x_2, \ldots, x_m$ durch p teilbar werden. Dann ist

$$N(\mathfrak{x}) \equiv x_1 x_{m+1} \mod p \,. \tag{67}$$

Ist auch $x_1 \equiv 0 \mod p$, so transformiere man jetzt $\mathfrak{x}$ mit der Einheit $\mathfrak{F}_0^{(2m)}$, wodurch $x_1, x_2, \ldots$ mit $x_{m+1}, x_{m+2}, \ldots$ vertauscht werden. Eine weitere Transformation mit einer Einheit (65) mit $\mathfrak{S} = \mathfrak{D}^{(m)}$ und geeignetem $\mathfrak{B}$ macht schließlich $x_2 \equiv \cdots \equiv x_{2m} \equiv 0 \mod p$, wobei auch noch $x_1 \equiv 1 \mod p$ erreicht werden kann, falls nicht $\mathfrak{x}$ der Nullvektor mod p war.

Ist dagegen $x_1 \not\equiv 0 \mod p$, so kann man $\mathfrak{x}$ mit einer Einheit (65) mit $\mathfrak{B} = \mathfrak{E}^{(m)}$ und geeignetem $\mathfrak{S}$ so transformieren, daß auch $x_{m+2}, \ldots, x_{2m}$ durch p teilbar werden. Dabei muß $\mathfrak{S}$ so bestimmt werden, daß die erste Spalte $s_{11}, s_{21}, \ldots, s_{m1}$ folgende Werte hat:

$$s_{11} \equiv 0 \,, \quad s_{21} x_1 \equiv -x_{m+2}, \ldots, s_{m1} x_1 \equiv -x_{2m} \mod p \,,$$

was mit (66) verträglich ist. Wenn die Norm von $\mathfrak{x}$ durch p teilbar ist, so ist jetzt wegen (67) auch $x_{m+1} \equiv 0 \mod p$, es liegt dann der schon behandelte Fall vor. Anderenfalls kann man endlich noch eine Substitution (65) mit $\mathfrak{B} = \frac{1}{x_1} \mathfrak{E}^{(m)}$, $\mathfrak{S} = \mathfrak{D}^{(m)}$ anwenden, dann erhält man die endgültige Normalform:

$$x_1 \equiv 1 \,, \quad x_2 \equiv \cdots \equiv x_m \equiv 0 \,, \quad x_{m+1} \equiv N(\mathfrak{x}) \,, \quad x_{m+2} \equiv \cdots \equiv x_{2m} \equiv 0 \mod p \,. \tag{68}$$

Der Hilfssatz 4 ist hiermit bewiesen, da jeder ganzzahlige Vektor solch einem Normalvektor mod p äquivalent ist.

2. Die Überlegungen sind fast wörtlich übertragbar auf Kongruenzen mod p^α. Dazu werde noch folgender Begriff eingeführt: ein ganzzahliger Vektor möge *primitiv* heißen, wenn seine Komponenten ohne gemeinsamen Teiler sind. Primitive Vektoren sind mit Normalvektoren der Gestalt (68) auch mod p^α äquivalent, und es gilt der

Hilfssatz 5. Zwei ganzzahlige primitive Vektoren $\mathfrak{x}$ und $\mathfrak{y}$ sind dann und nur dann mod p^α äquivalent, wenn

$$N(\mathfrak{x}) \equiv N(\mathfrak{x}) \mod p^\alpha$$

ist.

3. Wird $\mathfrak{F}$ in der Gestalt $\mathfrak{F}_0^{(2m)}$ angesetzt, so ist

$$\mathfrak{P}_0 = \begin{pmatrix} \mathfrak{E}^{(m)} & \\ & p\,\mathfrak{E}^{(m)} \end{pmatrix}$$

ein spezieller Haupttransformator der Norm p für $\mathfrak{F}$. Es sei $\mathfrak{P}$ eine ganzzahlige lineare Substitution, welche ein Primlinksideal $(\mathfrak{P}]$ der Norm p für $\mathfrak{F}$ erzeugt. Es gibt dann zwei unimodulare Matrizen $\mathfrak{U}$ und $\mathfrak{V}$ so, daß

$$\mathfrak{P} = \mathfrak{U}\,\mathfrak{P}_0\,\mathfrak{V} \tag{69}$$

gilt. Man transformiere $\mathfrak{F}$ mit $\mathfrak{U}$:

$$\mathfrak{F}' = \dot{\mathfrak{U}}\,\mathfrak{F}\,\mathfrak{U} = \begin{pmatrix} \mathfrak{F}_{11} & \mathfrak{F}_{12} \\ \dot{\mathfrak{F}}_{12} & \mathfrak{F}_{22} \end{pmatrix},$$

hier seien $\mathfrak{F}_{11}$, $\mathfrak{F}_{12}$, $\mathfrak{F}_{22}$ m-reihige Matrizen. Da $(\mathfrak{P}]$ ein Linksideal für $\mathfrak{F}$ ist, ist $\mathfrak{P}_0$ ein solches für $\mathfrak{F}'$, also gilt

$$\mathfrak{F}_{11} \equiv \mathfrak{O}^{(m)} \bmod p\,, \qquad |\,\mathfrak{F}_{12}\,| \equiv \pm 1 \bmod p\,.$$

Es sei nun $\mathfrak{T} = \mathfrak{T}^{(m)}$ eine Lösung der Kongruenz

$$\mathfrak{T} + \dot{\mathfrak{T}} + \dot{\mathfrak{F}}_{12}^{-1}\,\mathfrak{F}_{22}\,\mathfrak{F}_{12} \equiv \mathfrak{O}^{(m)} \mod p\,, \tag{70}$$

zu deren Verständnis im Falle $p = 2$ noch besonders auf die „Bemerkungen zur Formelschreibweise" hingewiesen sei; sie besitzt stets eine ganzzahlige Auflösung. Mit ihr bilde ich die $2m$-reihige Matrix

$$\mathfrak{U}' = \begin{pmatrix} \mathfrak{E}^{(m)} & \mathfrak{T} \\ & \mathfrak{F}_{12}^{-1} \end{pmatrix}.$$

Der Hauptnenner ihrer Koeffizienten ist zu p teilerfremd; dasselbe gilt auch für die Matrix

$$\mathfrak{V}' = \mathfrak{P}_0^{-1}\,\mathfrak{U}'\,\mathfrak{P}_0$$

und die hierzu inverse. Mit

$$\mathfrak{U}_1 = \mathfrak{U}\,\mathfrak{U}'\,, \qquad \mathfrak{V}_1 = \mathfrak{V}'^{-1}\,\mathfrak{V}$$

gilt nun nach (69)

$$\mathfrak{P} = \mathfrak{U}_1\,\mathfrak{P}_0\,\mathfrak{V}_1$$

oder

$$(\mathfrak{P}] = (\mathfrak{U}_1\,\mathfrak{P}_0] \tag{71}$$

und nach (70) wegen $\mathfrak{F} = \mathfrak{F}_0^{(2m)}$

$$\dot{\mathfrak{U}}_1\,\mathfrak{F}\,\mathfrak{U}_1 \equiv \mathfrak{F} \mod p\,. \tag{72}$$

Da nach (72) stets $|\mathfrak{U}_1| \equiv \pm 1 \mod p$ ist, gibt es eine ganzzahlige Matrix $\mathfrak{U}_1'$ der Determinante ± 1, welche der Kongruenz

$$\mathfrak{U}_1' \equiv \mathfrak{U}_1 \mod p$$

genügt. Es folgt aus diesen Schlüssen der

Hilfssatz 6. Zu zwei Primlinksidealen $(\mathfrak{P}_1]$ und $(\mathfrak{P}_2]$ der Norm p für $\mathfrak{F}$ gibt es eine ganzzahlige Matrix $\mathfrak{U}_1$ der Determinante ± 1, welche der Kongruenz (72) genügt, so daß

$$(\mathfrak{P}_1] = (\mathfrak{U}_1\, \mathfrak{P}_2]$$

ist.

4. Die Ergebnisse von Nr. 3 sind nun zu verallgemeinern. Ein Transformator oder ein Ideal heiße *normal*, wenn das Elementarteilersystem der Matrix bzw. Matrizen, welche den Transformator bzw. das Ideal erzeugen, höchstens zwei verschiedene Zahlen enthält. Handelt es sich nicht um ein rationales Vielfaches der Einheitsmatrix, so sind offenbar m Elementarteiler gleich einer Zahl a, die anderen m Elementarteiler sind gleich einer anderen Zahl b. Ein ganzer Transformator oder ein ganzes Ideal heiße ferner *primitiv*, wenn nicht alle Koeffizienten der erzeugenden Matrizen einen gemeinsamen Teiler haben. Bei ganzen normalen primitiven Transformatoren und Idealen ist der erste Elementarteiler gleich 1, der zweite gleich der Norm. Die Überlegungen von Nr. 3 sind zum Beweis des folgenden Hilfssatzes fast wörtlich übertragbar; an die Stelle von $\mathfrak{P}_0$ tritt dabei stets die Potenz $\mathfrak{P}_0^\alpha$ von $\mathfrak{P}_0$:

Hilfssatz 7. Zu zwei ganzen primitiven normalen Linksidealen $(\mathfrak{P}_1]$ und $(\mathfrak{P}_2]$ der Norm p^α für $\mathfrak{F}$ gibt es eine ganzzahlige Matrix $\mathfrak{U}_1$ der Determinante ± 1, welche der Kongruenz

$$\dot{\mathfrak{U}}_1\, \mathfrak{F}\, \mathfrak{U}_1 \equiv \mathfrak{F} \mod p^\alpha \tag{73}$$

genügt, so daß

$$(\mathfrak{P}_1] = (\mathfrak{U}_1\, \mathfrak{P}_2]$$

ist.

5. Es sind nun einige Anzahlen zu berechnen, und zwar:

1) $\varrho(p^\alpha)$: die Anzahl der ganzen primitiven normalen Ideale der Norm p^α für $\mathfrak{F}$.

2) $\nu(p^\alpha)$: die Anzahl solcher Ideale, welche einen gegebenen ganzzahligen primitiven Vektor teilen, dessen Norm durch p^α teilbar ist.

3) $\delta(p^\alpha)$: die Anzahl der ganzzahligen primitiven Vektoren mod p^α, deren Norm durch p^α teilbar ist.

4) $\mu(p^\alpha)$: die Anzahl solcher Vektoren, welche durch ein gegebenes ganzes primitives normales Ideal der Norm p^α für $\mathfrak{F}$ teilbar sind.

Die Anzahlen $\nu(p^\alpha)$, $\mu(p^\alpha)$ hängen ihrer Definition nach zwar noch von einem speziellen Vektor bzw. einem speziellen Ideal ab, sie sind jedoch nach den Hilfssätzen 5 und 7 Invarianten des Formensystems allein. Nachdem diese Tatsache festgestellt ist, erkennt man zwischen den erwähnten Anzahlen sofort die Beziehung

$$\nu(p^\alpha)\,\frac{\delta(p^\alpha)}{\mu(p^\alpha)} = \varrho(p^\alpha)$$

oder

$$\frac{\varrho(p^\alpha)}{\nu(p^\alpha)} = \frac{\delta(p^\alpha)}{\mu(p^\alpha)}\ . \tag{74}$$

Hauptsächlich dieser Quotient wird weiter unten eine Rolle spielen.

Die beiden letzten Anzahlen lassen sich ganz elementar berechnen, bei der Berechnung von $\mu(p^\alpha)$ darf für das genannte Ideal ein spezielles, und zwar am bequemsten $\mathfrak{P}_0^\alpha$ eingesetzt werden:

$$\delta(p^\alpha) = p^{(\alpha-1)(2m-1)}(p^m-1)(p^{m-1}+1)\ ,\quad \mu(p^\alpha) = p^{(\alpha-1)m}(p^m-1)\ . \tag{75}$$

Nach (74) und (75) ist also

$$\frac{\varrho(p^\alpha)}{\nu(p^\alpha)} = p^{(\alpha-1)(m-1)}(p^{m-1}+1)\ . \tag{76}$$

6. Die Anzahl $\varrho(p^\alpha)$ ist nach Hilfssatz 7 offenbar gleich der Ordnung der Gruppe sämtlicher Einheiten von $\mathfrak{F}_0^{(2m)}$ mod p^α, dividiert durch die Ordnung der Gruppe derjenigen dieser Einheiten $\mathfrak{U}$, für welche

$$(\mathfrak{U}\,\mathfrak{P}_0^\alpha] = (\mathfrak{P}_0^\alpha]$$

ist, d. h. für welche

$$\mathfrak{P}_0^{-\alpha}\,\mathfrak{U}\,\mathfrak{P}_0^\alpha$$

ganzzahlig ist. Diese $\mathfrak{U}$ müssen von folgender Gestalt sein:

$$\mathfrak{U} \equiv \begin{pmatrix} \mathfrak{B}_1 & \mathfrak{B}_1\mathfrak{T} \\ & \mathfrak{B}_2 \end{pmatrix} \bmod p^\alpha\ ,$$

wo $\mathfrak{B}_1$, $\mathfrak{B}_2$, $\mathfrak{T}$ m-reihige Matrizen sind. Es sind Einheiten mod p^α, falls

$$\mathfrak{B}_2 \equiv \dot{\mathfrak{B}}_1^{-1}\ ,\qquad \mathfrak{T} + \dot{\mathfrak{T}} \equiv \mathfrak{O}^{(m)} \qquad \bmod p^\alpha$$

gilt. Die Ordnung dieser Gruppe ist für $\alpha = 1$ gleich $p^{\frac{1}{2}m(m-1)}$-mal der Ordnung der vollen linearen Gruppe vom Grade m, also gleich

$$p^{m(m-1)}(p-1)\ldots(p^m-1)\ .$$

Da (64) die Ordnung der Einheitengruppe mod p für $p>2$ ist, hat man jetzt für $\alpha = 1$, $p>2$, $m \geqq 2$:

$$\varrho(p) = 2(p+1)\ldots(p^{m-1}+1) = (p^0+1)(p^1+1)\ldots(p^{m-1}+1) \qquad (77)$$

und

$$\nu(p) = 2(p+1)\ldots(p^{m-2}+1) = (p^0+1)(p^1+1)\ldots(p^{m-2}+1)\ . \qquad (78)$$

Für $m = 1$ hat man $\varrho(p) = 2$, $\nu(p) = 1$; hiermit kommt der folgende Sachverhalt zum Ausdruck: In einem quadratischen Zahlkörper, dessen Diskriminante mod p ein quadratischer Rest ist, gibt es zwei Primideale der Norm p. Eine primitive ganze Zahl, deren Norm durch p teilbar ist, ist durch genau eines von diesen teilbar. Im Falle $m = 2$ ist $\varrho(p) = 2(p+1)$, $\nu(p) = 2$; hiermit kommt der folgende Sachverhalt zum Ausdruck: es gibt für eine Maximalordnung $\mathfrak{J}$ einer Quaternionenalgebra, deren Diskriminante zu p teilerfremd ist, $2(p+1)$ Primideale der Norm p. Eine ganze primitive Zahl α aus $\mathfrak{J}$, deren Norm durch p teilbar ist, ist in zweien von diesen Idealen enthalten; diese Ideale sind offenbar das Linksideal $\mathfrak{P}_1 = \mathfrak{J}\alpha + \mathfrak{J}p$ und das Rechtsideal $\mathfrak{P}_2 = \alpha\mathfrak{J} + p\mathfrak{J}$.

§ 9. Die Primideale zweiten Grades

1. Die Überlegungen des § 8 sind nun soweit als möglich auf den Fall zu übertragen, wo D mod p ein quadratischer Nichtrest bei gerader Variablenzahl n ist, oder wo die Variablenzahl n ungerade ist. Es handelt sich also jetzt um die Zahlentheorie der Formen

$$\mathfrak{F} = \begin{pmatrix} \mathfrak{F}_0^{(2m)} & & \\ & 2 & \\ & & -2\frac{D}{4} \end{pmatrix} \quad \text{oder} \quad \mathfrak{F} = \begin{pmatrix} \mathfrak{F}_0^{(2m)} & \\ & 2D \end{pmatrix} \quad (n = 2m+r,\ r = 1,2) \qquad (79)$$

je nachdem die Variablenzahl gerade ($r = 2$) oder ungerade ($r = 1$) ist, und zwar im Restklassenring der ganzen Zahlen mod p^α. Dabei soll der Kürze halber der Fall $p = 2$ ausgeschlossen werden; es wäre nicht schwer, die für diesen Fall notwendigen Zusatzüberlegungen anzufügen,

die Ergebnisse dürften sich dabei nicht ändern. Ferner werde durchweg $m > 0$ angenommen.

Hilfssatz 8. Zwei ganzzahlige primitive Vektoren $\mathfrak{x}$ und $\mathfrak{y}$ sind dann und nur dann äquivalent mod p^α, wenn

$$N(\mathfrak{x}) \equiv N(\mathfrak{y}) \mod p^\alpha$$

ist.

Beweis. Die Notwendigkeit der genannten Bedingung ist klar. Um einen ganzzahligen primitiven Vektor $\mathfrak{x}$ auf eine Normalgestalt zu transformieren, kann man zunächst die Einheiten der Teilformen $\mathfrak{F}_0^{(2m)}$ von $\mathfrak{F}$ gemäß (79) benutzen und dadurch erreichen, daß

$$x_2 \equiv \cdots \equiv x_m \equiv x_{m+2} \equiv \cdots \equiv x_{2m} \equiv 0 \mod p^\alpha$$

ist. Dann ist

$$N(\mathfrak{x}) \equiv x_1 x_{m+1} + \begin{Bmatrix} D x_{2m+1}^2 \\ x_{2m+1}^2 - \frac{D}{4} x_{2m+2}^2 \end{Bmatrix} \mod p^\alpha \text{ für } \begin{cases} r = 1, \\ r = 2. \end{cases} \tag{80}$$

Es bleiben nun nur noch die Einheiten der ternären oder quaternären Form

$$\mathfrak{F}_3 = y_1 y_2 + D y_3^2, \qquad \mathfrak{F}_4 = y_1 y_2 + y_3^2 - \frac{D}{4} y_4^2 \tag{81}$$

für $y_1 = x_1$, $y_2 = x_{m+1}$, $y_3 = x_{2m+1}$, $y_4 = x_{2m+2}$ zur Anwendung übrig. Die erstere Form ist mod p^α äquivalent mit $v^2 - uw$, und deren Einheiten sind bekanntlich die Matrizen

$$\begin{pmatrix} \alpha^2 & 2\alpha\gamma & \gamma^2 \\ \alpha\beta & \alpha\delta + \beta\gamma & \gamma\delta \\ \beta^2 & 2\beta\delta & \delta^2 \end{pmatrix} \quad \text{mit} \quad \alpha\delta - \beta\gamma \equiv 1 \mod p^\alpha$$

d. h. u, v, w transformieren sich wie die Koeffizienten der binären Form

$$u\xi^2 + 2v\xi\eta + w\eta^2 \tag{82}$$

bei unimodularer Transformation der Variablen ξ, η. Man kann (82) stets so transformieren, daß $v \equiv 0 \mod p^\alpha$ wird. Mithin gibt es eine Einheit von $\mathfrak{F}$ mod p^α, welche die Kongruenz $x_{2m+1} \equiv 0 \mod p^\alpha$ herstellt. Wendet man nun, falls noch erforderlich, weitere Einheiten der Teilform $\mathfrak{F}_0^{(2m)}$ an, so erhält man die Normalgestalt

$$x_1 \equiv 1,\ x_2 \equiv \cdots \equiv x_m \equiv 0,\ x_{m+1} \equiv N(\mathfrak{x}),\ x_{m+2} \equiv \cdots \equiv 0 \bmod p^\alpha \quad (83)$$

für alle ganzen primitiven Vektoren. Der Hilfssatz 8 ist damit jedenfalls für ungerade Variablenzahl bewiesen. Bei gerader Variablenzahl muß man aus der Form $\mathfrak{F}_4$ in (81) zunächst die ternäre Teilform $y_1 y_2 + y_3^2$ herausgreifen und durch Anwendung einer Einheit von dieser y_3, d. h. x_{2m+1} zu Null mod p^α machen. Sodann wende man eine Einheit der verbliebenen ternären Form $y_1 y_2 - \frac{D}{4} y_4^2$ an und mache $y_4 = x_{2m+2} \equiv 0 \bmod p^\alpha$. Die Normalgestalt (83) ist also auch bei gerader Variablenzahl herstellbar.

2. An Stelle der Normalform (79) werde jetzt die etwas allgemeinere

$$\mathfrak{F} = \begin{pmatrix} \mathfrak{F}_0^{(2m_1)} & \\ & \mathfrak{G}^{(r_1)} \end{pmatrix},\quad \mathfrak{G}^{(r_1)} = \begin{pmatrix} \mathfrak{F}_0^{(r_1-r)} & & \\ & 2 & \\ & & -2\frac{D}{4} \end{pmatrix} \text{ bzw. } \begin{pmatrix} \mathfrak{F}_0^{(r_1-r)} & \\ & 2D \end{pmatrix} \quad (84)$$

$$(n = 2m_1 + r_1 = 2m + r)$$

verwendet; ersichtlich sind die Formen (79) und (84) äquivalent.

Ein Transformator oder ein Ideal soll *halbnormal* heißen, wenn sein Elementarteilersystem aus höchstens 3 Zahlen besteht. Spezielle ganze primitive halbnormale Haupttransformatoren für die Form (84) sind

$$\mathfrak{P}_{r_1} = \begin{pmatrix} \mathfrak{E}^{(m_1)} & & \\ & p^2\mathfrak{E}^{(m_1)} & \\ & & p\mathfrak{E}^{(r_1)} \end{pmatrix} \quad (85)$$

und deren Potenzen; sie vertreten die Rolle, die $\mathfrak{P}_0$ und dessen Potenzen in § 8 spielten, normale Ideale und Transformatoren der Norm $p^{2\alpha}$ für $\mathfrak{F}$ gibt es in dem vorliegenden Falle nicht.

Es sei $(\mathfrak{P}]$ ein ganzes primitives halbnormales Ideal der Norm $p^{2\alpha}$, der mittlere Elementarteiler trete r_1-mal auf. Dann gibt es zwei unimodulare Matrizen $\mathfrak{U}$ und $\mathfrak{V}$, so daß

$$\mathfrak{P} = \mathfrak{U}\,\mathfrak{P}_{r_1}^{\alpha}\,\mathfrak{V} \quad (86)$$

ist. Man setze

$$\mathfrak{F}' = \dot{\mathfrak{U}}\,\mathfrak{F}\,\mathfrak{U} = \begin{pmatrix} \mathfrak{F}'_{11} & \mathfrak{F}'_{12} & \mathfrak{f}'_{13} \\ \dot{\mathfrak{F}}'_{12} & \mathfrak{F}'_{22} & \mathfrak{f}'_{23} \\ \dot{\mathfrak{f}}'_{13} & \dot{\mathfrak{f}}'_{23} & \mathfrak{F}'_{33} \end{pmatrix}, \quad (87)$$

diese Aufspaltung in Teilmatrizen sei derart, daß $\mathfrak{F}'_{11}$, $\mathfrak{F}'_{12}$, $\mathfrak{F}'_{22}$ das Format $m_1 \times m_1$, $\mathfrak{f}'_{13}$, $\mathfrak{f}_{23}$ das Format $m_1 \times r_1$ und $\mathfrak{F}_{33}$ das Format $r_1 \times r_1$ haben. Nun ist $(\mathfrak{P}^{\alpha}_{r_1}]$ ein Ideal für $\mathfrak{F}'$, also

$$\mathfrak{F}'_{11} \equiv \mathfrak{O}^{(m_1)} \bmod p^{2\alpha}, \quad \mathfrak{f}'_{13} \equiv v^{(m_1, r_1)} \bmod p^{\alpha}, \tag{88}$$

$$D \equiv \left|\mathfrak{F}'_{12}\right|^2 D(\mathfrak{F}'_{33}) \bmod p^{2\alpha}. \tag{89}$$

Es sei jetzt $\mathfrak{U}'$ eine ganzzahlige Matrix mit

$$\mathfrak{U}' \equiv \begin{pmatrix} \mathfrak{U}_{11} & \mathfrak{U}_{12} & \mathfrak{u}_{13} \\ & \mathfrak{U}_{22} & p^{\alpha}\mathfrak{u}_{23} \\ p^{\alpha}\mathfrak{u}_{31} & \mathfrak{u}_{32} & \mathfrak{U}_{33} \end{pmatrix} \bmod p^{2\alpha}, \tag{90}$$

deren Teilmatrizen dieselben Formate haben wie die Teilmatrizen von $\mathfrak{F}'$, und

$$\mathfrak{F}'' = \dot{\mathfrak{U}}' \mathfrak{F}' \mathfrak{U}'. \tag{91}$$

Zerlegt man $\mathfrak{F}''$ in derselben Weise in Teilmatrizen wie (87), so erhält man nach (87), (88), (90) folgende Kongruenzensysteme:

Für

$$\mathfrak{U}_{11} \equiv \mathfrak{U}_{22} \equiv \mathfrak{E}^{(m_1)}, \quad \mathfrak{U}_{12} \equiv \mathfrak{O}^{(m_1)}, \quad \mathfrak{u}_{13} \equiv \mathfrak{u}_{23} \equiv \mathfrak{o}^{(m_1, r_1)} \bmod p^{2\alpha}$$

ist

$$\mathfrak{f}''_{13} \equiv (\mathfrak{f}'_{13} + p^{\alpha}\dot{\mathfrak{u}}_{31}\mathfrak{F}'_{33})\,\mathfrak{U}_{33}, \quad \mathfrak{f}'_{23} \equiv (\mathfrak{f}'_{23} + \dot{\mathfrak{u}}_{32}\mathfrak{F}'_{33})\,\mathfrak{U}_{33}, \quad \mathfrak{F}''_{33} \equiv \dot{\mathfrak{U}}_{33}\mathfrak{F}'_{33}\mathfrak{U}_{33} \bmod p^{2\alpha}.$$

Wegen (88), (89) kann man nun $\mathfrak{u}_{31}$, $\mathfrak{u}_{32}$, $\mathfrak{U}_{33}$ so bestimmen, daß

$$\mathfrak{f}''_{13} \equiv \mathfrak{f}''_{23} \equiv \mathfrak{v}^{(m_1, r_1)}, \quad \mathfrak{F}''_{33} \equiv \mathfrak{G}^{(r_1)} \bmod p^{2\alpha}$$

gilt. Sind diese Kongruenzen erfüllt, so setze man $\mathfrak{u}_{13} = \mathfrak{u}_{23} = \mathfrak{o}^{(m_1, r_1)}$, $\mathfrak{u}_{31} = \mathfrak{u}_{32} = \mathfrak{o}^{(r_1, m_1)}$, $\mathfrak{U}_{33} = \mathfrak{E}^{(r_1)}$ und kann dann $\mathfrak{U}_{11}$, $\mathfrak{U}_{12}$, $\mathfrak{U}_{22}$ nach dem Gedanken von § 8, Nr. 3 so bestimmen, daß

$$\mathfrak{F}''_{11} \equiv \mathfrak{F}''_{22} \equiv \mathfrak{O}^{(m_1)}, \quad \mathfrak{F}''_{12} \equiv \mathfrak{E}^{(m_1)} \bmod p^{2\alpha}$$

wird, dann ist also

$$\mathfrak{F}'' \equiv \mathfrak{F} \bmod p^{2\alpha}, \tag{92}$$

wenn $\mathfrak{F}$ in der Normalgestalt (84) angenommen wurde. Man setze weiterhin

$$\mathfrak{U}_1 = \mathfrak{U}\,\mathfrak{U}' \,, \qquad \mathfrak{B}_1 = \mathfrak{P}_{r_1}^{-\alpha}\,\mathfrak{U}'^{-1}\,\mathfrak{P}_{r_1}^{\alpha}\,\mathfrak{B} \,, \tag{93}$$

dann ist nach (86)

$$\mathfrak{P} = \mathfrak{U}_1\,\mathfrak{P}_{r_1}^{\alpha}\,\mathfrak{B}_1 \tag{94}$$

und nach (87), (91) bis (93)

$$\dot{\mathfrak{U}}_1\,\mathfrak{F}\,\mathfrak{U}_1 \equiv \mathfrak{F} \mod p^{2\alpha} \,. \tag{95}$$

Nach (85), (90), (93) ist $\mathfrak{B}_1$ eine Matrix, deren Koeffizienten zu p teilerfremde Nenner haben, also folgt aus (94)

$$(\mathfrak{P}] = (\mathfrak{U}_1\,\mathfrak{P}_{r_1}^{\alpha}] \,.$$

Wie in § 8, Nr. 3 kann man endlich sicherstellen, daß $\mathfrak{U}_1$ eine ganzzahlige Matrix der Determinante ± 1 ist. Also gilt der

Hilfssatz 9. Es seien $\mathfrak{P}_1$ und $\mathfrak{P}_2$ zwei ganze primitive halbnormale Ideale für $\mathfrak{F}$ mit dem gleichen Elementarteilersystem. Dann gibt es eine ganzzahlige Matrix $\mathfrak{U}_1$ der Determinante ± 1, welche (95) erfüllt, so daß

$$(\mathfrak{P}_1] = (\mathfrak{U}_1\,\mathfrak{P}_2]$$

ist.

3. Wiederum sind einige Anzahlformeln zu berechnen, und zwar:

1) $\varrho(p^{2\alpha}, r_1)$: die Anzahl der ganzen primitiven halbnormalen Ideale der Norm $p^{2\alpha}$, wobei der mittlere Elementarteiler genau r_1-mal auftritt.

2) $\nu(p^{2\alpha}, r_1)$: die Anzahl der Ideale dieser Art, welche einen gegebenen ganzzahligen primitiven Vektor teilen, dessen Norm durch $p^{2\alpha}$ teilbar ist.

3) $\delta(p^{2\alpha})$: die Anzahl der ganzzahligen primitiven Vektoren mod $p^{2\alpha}$, deren Norm durch $p^{2\alpha}$ teilbar ist.

4) $\mu(p^{2\alpha}, r_1)$: die Anzahl der Vektoren dieser Art, welche durch ein gegebenes ganzes primitives normales Ideal der Norm $p^{2\alpha}$ teilbar sind, dessen mittlerer Elementarteiler genau r_1-mal auftritt.

Wie in § 8 folgt auch hier, daß diese Anzahlen sämtlich Invarianten des Formensystems sind, und daß die Gleichung

$$\frac{\varrho(p^{2\alpha}, r_1)}{\nu(p^{2\alpha}, r_1)} = \frac{\delta(p^{2\alpha})}{\mu(p^{2\alpha}, r_1)} \tag{96}$$

gilt.

Eine ganz elementare Rechnung liefert

$$\mu(p^{2\alpha}, r_1) = p^{(2\alpha-1)m_1+\alpha r_1}(p^{m_1} - 1) \ . \tag{97}$$

Etwas schwieriger berechnet sich $\delta(p^{2\alpha})$. Zunächst sei $r = 2$, $\alpha = 1$; $\delta(p^2)$ ist gleich der Lösungszahl $\bmod p^2$ der Kongruenz

$$\mathfrak{a}\,\mathfrak{b} + x^2 - \frac{D}{4}y^2 \equiv 0 \mod p^2$$

wo $\mathfrak{a}$ und $\mathfrak{b}$ Vektoren von m ganzzahligen Komponenten und $\mathfrak{a}\,\mathfrak{b}$ deren skalares Produkt bedeuten. Diese Lösungsanzahl setzt sich zusammen aus der Lösungsanzahl δ_1 von

$$\mathfrak{a}\,\mathfrak{b} \equiv a \bmod p^2$$

bei festem zu p teilerfremdem a und der Anzahl δ_2 der primitiven Lösungen derselben Kongruenz mit $a = 0$. Die erstere Anzahl ist $p^2(p^2 - 1)$-mal zu zählen entsprechend der Anzahl der Lösungen $\bmod p^2$ von

$$x^2 - \frac{D}{4}y^2 \equiv -a \not\equiv 0 \mod p \ ,$$

die zweite p^2-mal entsprechend der Anzahl der Lösungen $\bmod p^2$ von

$$x^2 - \frac{D}{4}y^2 \equiv 0 \mod p^2 \ ,$$

wobei zu beachten ist, daß D ein quadratischer Nichtrest $\bmod p$ sein sollte. Man findet leicht

$$\delta_1 = p^{3m-2}(p^m - 1) \ ,$$
$$\delta_2 = p^{2m-1}(p^m - 1)(p^{m-1} + 1) \ .$$

Es ist mithin

$$\delta(p^2) = \delta_1 p^2(p^2 - 1) + \delta_2 p^2 = p^{2m+1}(p^m - 1)(p^{m+1} + 1) \ .$$

Ist $\mathfrak{a}_\beta$, $\mathfrak{b}_\beta$, x_β, y_β eine primitive Lösung von

$$\mathfrak{a}_\beta\,\mathfrak{b}_\beta + x_\beta^2 - \frac{D}{4}y_\beta^2 \equiv 0 \mod p^\beta \ ,$$

so erhält man eine Lösung derselben Kongruenz mit $\beta + 1$ an Stelle von β durch den Ansatz $\mathfrak{a}_{\beta+1} = \mathfrak{a}_\beta + p^\beta \mathfrak{a}'$ usw. Hierbei muß für $\mathfrak{a}'$ usw. eine einzige lineare Kongruenz mod p bestehen, welche nicht identisch erfüllt ist und daher p^{2m+1} verschiedene Lösungen besitzt. Mithin wird

$$\delta(p^{2\alpha}) = p^{(2\alpha-1)(2m+1)}(p^m - 1)(p^{m+1} + 1) \quad (r = 2) \; . \tag{98}$$

Der Gedankengang verläuft bei ungerader Variablenzahl völlig analog und liefert

$$\delta(p^{2\alpha}) = p^{(2\alpha-1)\,2m}(p^m - 1)(p^m + 1) \; . \quad (r = 1) \tag{99}$$

Nach (96) bis (99) wird für $r_1 = r$:

$$\frac{\varrho(p^{2\alpha}, r)}{\nu(p^{2\alpha}, r)} = \begin{cases} p^{(2\alpha-1)\,m-\alpha}(p^m + 1) & \text{für} \quad r = 1 \; , \\ p^{(2\alpha-1)\,m-1}(p^{m+1} + 1) & \text{für} \quad r = 2 \; . \end{cases} \tag{100}$$

4. Zum Schluß ist noch die Anzahl $\lambda(p^2; N)$ der ganzen primitiven halbnormalen Ideale $(\mathfrak{P}]$ der Norm p^2 zu berechnen, deren mittlerer Elementarteiler r-mal auftritt ($r = 1$ für ungerade und $r = 2$ für gerade Variablenzahl), und welche einen gegebenen Vektor $p\mathfrak{x}$ teilen, wo $\mathfrak{x}$ ein ganzzahliger primitiver Vektor der Norm N ist:

$$p\,\mathfrak{x} = \mathfrak{P}\,\mathfrak{y} \; .$$

Zufolge der Hilfssätze 8 und 9 hängt diese Anzahl nur von der Norm N von $\mathfrak{x}$ ab; ja sogar nur von dem Legendresymbol $\left(\frac{N}{p}\right)$; dasselbe gilt für die Anzahl $\varkappa(p^2; N)$ der primitiven Vektoren mod p, die mit einem solchen $\mathfrak{P}$ in dieser Beziehung stehen. Ist $\delta(p; N)$ die Anzahl aller ganzzahligen primitiven Vektoren mod p mit der Norm N, so gilt offenbar

$$\delta(p; N)\,\frac{\lambda(p^2; N)}{\varkappa(p^2; N)} = \varrho(p^2, r) \tag{101}$$

oder

$$\frac{\lambda(p^2; N)}{\nu(p^2, r)} = \frac{\varrho(p^2, r)}{\nu(p^2, r)}\;\frac{\varkappa(p^2; N)}{\delta(p; N)} \; . \tag{102}$$

Ferner ist abgesehen von dem trivialen Fall $n = 1$:

$$\delta(p; N) = \begin{cases} (p^m - 1)(p^m + 1) & \text{für } N \equiv 0 \bmod p \; , \\ p^m\left(p^m + \left(\frac{DN}{p}\right)\right) & \text{für } N \not\equiv 0 \bmod p \; , \end{cases} \quad r = 1 \; , \\ \begin{cases} (p^m - 1)(p^{m+1} + 1) & \text{für } N \equiv 0 \bmod p \; , \\ p^m(p^{m+1} + 1) & \text{für } N \not\equiv 0 \bmod p \; , \end{cases} \quad r = 2 \; , \end{cases} \tag{103}$$

wie man ganz leicht verifizieren kann, und ebenso

$$\varkappa(p^2; N) = \begin{cases} (p^m - 1) & \text{für } N \equiv 0 \bmod p\,,\ r \text{ beliebig,} \\ p^m\left(1 + \left(\frac{DN}{p}\right)\right) & \text{für } N \not\equiv 0 \bmod p\,,\ r = 1\,, \\ p^m(p+1) & \text{für } N \not\equiv 0 \bmod p\,,\ r = 2\,. \end{cases} \tag{104}$$

Nach (100) und (102) bis (104) ist dann

$$\frac{\lambda(p^2; N)}{\nu(p^2, r)} = \begin{cases} p^{m-1} & \text{für } N \equiv 0 \bmod p\,,\ r \text{ beliebig,} \\ p^{m-1}\left(1 + \left(\frac{DN}{p}\right)\right) & \text{für } N \not\equiv 0 \bmod p\,,\ r = 1\,, \\ p^{m-1}(p+1) & \text{für } N \not\equiv 0 \bmod p\,,\ r = 2\,. \end{cases} \tag{105}$$

(Eingegangen den 19. September 1946.)