

# Geschlechter quadratischer Formen.

Von *Hel Braun* in Göttingen.

## § 1. Einleitung.

Es war seit einigen Jahren erwünscht die Theorie der Geschlechter quadratischer Formen mit mehr als zwei Variablen so zu entwickeln, daß ihre Ergebnisse bequem auf andere Fragen aus der Theorie der quadratischen Formen angewandt werden können. Im vorliegenden Aufsatz wird gezeigt auf welche Art das geschehen kann. Es ist dabei vorteilhaft von der folgenden Definition eines Geschlechts auszugehen:

$\mathfrak{S}_1$  und  $\mathfrak{S}_2$  seien symmetrische Matrizen mit ganzen rationalen Elementen. Man nennt  $\mathfrak{S}_1$  äquivalent  $\mathfrak{S}_2$ , in Zeichen:  $\mathfrak{S}_1 \sim \mathfrak{S}_2$ , wenn  $\mathfrak{S}_1$  durch  $\mathfrak{S}_2$  und umgekehrt auch  $\mathfrak{S}_2$  durch  $\mathfrak{S}_1$  darstellbar ist; das heißt also: wenn es zwei ganze Matrizen  $\mathfrak{U}$  und  $\mathfrak{V}$  gibt (deren Transponierte  $\mathfrak{U}'$  und  $\mathfrak{V}'$  seien), so daß

$$(*) \quad \mathfrak{U}' \mathfrak{S}_1 \mathfrak{U} = \mathfrak{S}_2, \quad \mathfrak{V}' \mathfrak{S}_2 \mathfrak{V} = \mathfrak{S}_1$$

ist. Äquivalente Matrizen bilden eine Klasse.

Nun sei  $q$  irgendeine natürliche Zahl. Man nennt dann  $\mathfrak{S}_1$  äquivalent  $\mathfrak{S}_2$  modulo  $q$ , in Zeichen:  $\mathfrak{S}_1 \sim \mathfrak{S}_2 \pmod{q}$ , wenn

$$\mathfrak{U}' \mathfrak{S}_1 \mathfrak{U} \equiv \mathfrak{S}_2 \pmod{q}, \quad \mathfrak{V}' \mathfrak{S}_2 \mathfrak{V} \equiv \mathfrak{S}_1 \pmod{q}$$

ist mit ganzem  $\mathfrak{U}$  und  $\mathfrak{V}$ . Alle modulo  $q$  äquivalenten Matrizen bilden eine *Klasse modulo  $q$* .

Ganz entsprechend nennt man  $\mathfrak{S}_1$  und  $\mathfrak{S}_2$  reell äquivalent, wenn die beiden Gleichungen (\*) mit reellem  $\mathfrak{U}$  und  $\mathfrak{V}$  bestehen.

Man faßt jetzt alle diejenigen symmetrischen ganzzahligen  $\mathfrak{S}_1, \mathfrak{S}_2, \dots$  zu einem Geschlecht zusammen, die nach jedem natürlichen Modul und außerdem reell äquivalent sind. Alle Matrizen einer Klasse gehören trivialerweise zum selben Geschlecht, aber im allgemeinen besteht ein Geschlecht aus mehreren Klassen. Man kann nun zeigen, daß es in jeder Klasse Matrizen gibt deren Determinante  $\neq 0$  ist. Deswegen wird von jetzt ab immer angenommen, die Determinanten der betrachteten symmetrischen Matrizen seien von Null verschieden. Es ist sofort zu sehen, daß unter dieser Voraussetzung zwei symmetrische ganzzahlige Matrizen  $\mathfrak{S}_1$  und  $\mathfrak{S}_2$  dann und nur dann zur selben Klasse gehören, wenn sie durch unimodulare Transformation auseinander hervorgehen; wenn also  $\mathfrak{S}_1 = \mathfrak{U}' \mathfrak{S}_2 \mathfrak{U}$  ist, mit ganzzahligem  $\mathfrak{U}$ , dessen Determinante den Wert  $+1$  oder  $-1$  hat.

Alle diese für symmetrische Matrizen ausgesprochenen Definitionen und Sätze sind sinngemäß zu übertragen auf die mit diesen Matrizen gebildeten quadratischen Formen.

Gauß ist in seinen Untersuchungen über binäre quadratische Formen von einer anderen Geschlechtsdefinition ausgegangen. Er hat dabei vorausgesetzt, daß die Elemente der gegebenen symmetrischen zweireihigen Matrix  $\mathfrak{S}$  teilerfremd sind, daß also  $\mathfrak{S}$  primitiv ist. Das Geschlecht von  $\mathfrak{S}$  hat er festgelegt durch die Determinante und durch

endlich viele Legendresche quadratische Restsymbole, die Geschlechtscharaktere. Gauß zeigte, daß zu vorgegebenem Charaktersystem genau dann ein Geschlecht primitiver Formen der vorgeschriebenen Determinante gehört, wenn das Produkt über sämtliche Charaktere den Wert  $+1$  hat. Dieser Gaußsche Satz wurde auf ternäre Formen von Eisenstein und Smith, auf quadratische Formen mit mehr als drei Variablen von Minkowski übertragen. Wenn man für Formen mit mehr als zwei Variablen ein endliches vollständiges System von Geschlechtsinvarianten aufstellen will, die den Gaußschen Invarianten entsprechen, so hat man die Elementarteiler und das dyadische Verhalten der Formen des Geschlechts wesentlich zu beachten. Infolgedessen kommt man zwangsläufig zu Fallunterscheidungen, die alle Resultate unübersichtlich und unhandlich machen.

Es erscheint deshalb vernünftig ein anderes vollständiges endliches System von Geschlechtsinvarianten zum Ausgangspunkt zu nehmen, wenn man die Geschlechtertheorie so entwickeln will, daß ihre Sätze bequem anwendbar sind. Zu diesem System wird man durch folgende Überlegung geführt:

Die Signatur einer  $m$ -reihigen symmetrischen Matrix  $\mathfrak{S}$  sei so erklärt: Man kann bekanntlich  $\mathfrak{S}$  reell in eine Diagonalmatrix transformieren deren Diagonalelemente die Werte  $+1$  oder  $-1$  haben. Es sei  $\mu$  die Anzahl der Diagonalelemente  $+1$ , also  $m - \mu$  die Anzahl der Diagonalelemente  $-1$ . Dann nennt man das Zahlenpaar  $\mu, m - \mu$  die Signatur von  $\mathfrak{S}$ . Die Signatur ist nach dem Trägheitsgesetz eine Geschlechtsinvariante. Man sieht leicht ein, daß auch der absolute Betrag der Determinante eine Geschlechtsinvariante ist; dieser absolute Betrag sei mit  $D$  bezeichnet. Ferner sei  $8D^3 = q_0$  gesetzt. Dann gilt der

- Satz I.**       $(\alpha)$  Signatur  $\mu, m - \mu$   
                   $(\beta)$  absoluter Betrag  $D$  der Determinante  
                   $(\gamma)$  Klasse modulo  $q_0$

bilden ein vollständiges endliches System von Geschlechtsinvarianten.

Dabei läßt sich die Klasse modulo  $q_0$  festlegen durch irgendeine ihr angehörige ganze  $m$ -reihige symmetrische Matrix. Satz I besagt in anderen Worten:  $\mathfrak{S}_1$  und  $\mathfrak{S}_2$  gehören dann und nur dann zum selben Geschlecht, wenn sie gleiche Signatur haben, der absolute Betrag ihrer Determinanten der gleiche ist und die Äquivalenz  $\mathfrak{S}_1 \sim \mathfrak{S}_2 \pmod{q_0}$  erfüllt ist. Dieser Satz war bereits Minkowski <sup>1)</sup> bekannt, einen Beweis findet man bei Siegel <sup>2)</sup>.

Jetzt bleibt noch die Frage offen: Wann kann zu gegebenen Invarianten  $(\alpha), (\beta), (\gamma)$  ein Geschlecht quadratischer Formen gefunden werden?

Im folgenden wird sich zeigen, daß diese Frage in einfacher Weise beantwortet werden kann. Zuerst wird man nämlich sehen, daß zwischen den Invarianten  $(\alpha), (\beta), (\gamma)$  zwei Relationen bestehen müssen. Erstens muß für die Repräsentanten  $\mathfrak{S}$  der Klasse modulo  $q_0$  die Kongruenz

$$(\delta) \quad |\mathfrak{S}| \equiv x^2 (-1)^{m-\mu} D \pmod{q_0}$$

durch ein zu  $q_0$  teilerfremdes  $x$  lösbar sein. Zweitens muß für jedes  $\mathfrak{S}$  der Klasse modulo  $q_0$  die Relation

$$(\varepsilon) \quad \sum_{\mathfrak{x}(q_0)} e^{\frac{2\pi i}{q_0} \mathfrak{x} \mathfrak{S} \mathfrak{x}} = e^{\frac{\pi i}{4} (2\mu - m)} (2q_0)^{\frac{m}{2}} D^{\frac{1}{2}}$$

bestehen. Dabei wird in der Gaußschen Summe über die sämtlichen Elemente  $x_1, x_2, \dots, x_m$  der Spalte  $\mathfrak{x}$  summiert, die unabhängig voneinander ein volles Restsystem mod  $q_0$  durch-

<sup>1)</sup> H. Minkowski, Gesammelte Abhandlungen 1 (Leipzig 1911), 158.

<sup>2)</sup> C. L. Siegel, Über die analytische Theorie der quadratischen Formen (in der Folge kurz mit S. bezeichnet), Annals of Math. **36** (1935), 548.

laufen. Es ist einfach zu sehen, daß die Relation  $(\delta)$  bestehen muß. Daß auch  $(\varepsilon)$  erfüllt ist, wenn das Geschlecht existiert, ist leicht zu sehen, wenn man die Reziprozitätsformel für die Gaußschen Summen anwendet. Schwieriger ist dann, den Satz II zu beweisen, der kurz als *Geschlechtersatz* bezeichnet werden soll:

**Satz II.** *Zu gegebenen Invarianten  $(\alpha)$ ,  $(\beta)$ ,  $(\gamma)$  existiert, falls die Relationen  $(\delta)$  und  $(\varepsilon)$  erfüllt sind, ein Geschlecht quadratischer Formen.*

Dieser Satz wird im vierten und fünften Paragraphen bewiesen.

Man beachte übrigens, daß  $q_0 = 8D^3$  nicht der kleinste Modul ist, für den Signatur, absoluter Betrag der Determinante und Klasse modulo  $q_0$  das Geschlecht vollständig bestimmen. Es ist nur bequem, beim Beweis von Satz I vorauszusetzen, daß  $q_0 = 8D^3$ , oder allgemeiner, daß  $q_0$  ein fester, durch  $8D^3$  teilbarer Modul ist. Dann kann man nämlich im Beweis von Satz I von den Elementarteilern absehen. Minkowski hat behauptet, daß Satz I gilt, wenn  $q_0$  nur durch  $2D$  teilbar ist. Vermutlich kann auch diese Bedingung noch durch eine geringere ersetzt werden, in der dann allerdings die Elementarteiler explizit auftreten. Beim Beweis des Geschlechtersatzes wird von  $q_0$  nur verlangt, daß es durch  $8DP$  teilbar ist, wobei  $P$  das Produkt über die ungeraden Primteiler von  $D$  bedeutet.

Da die beiden Existenzkriterien  $(\delta)$  und  $(\varepsilon)$  eine sehr einfache Gestalt haben, ist es möglich, ohne viel Rechnung aus dem Geschlechtersatz einen weiteren, von Siegel auf anderem Wege bereits bewiesenen Existenzsatz herzuleiten. Dieser Satz bezieht sich nicht mehr auf äquivalente Matrizen, sondern auf irgendwelche ganzzahlige symmetrische Matrizen, die verschiedenen Rang haben können. Man geht deshalb aus von einer ganzen  $m$ -reihigen symmetrischen Matrix  $\mathfrak{S}$  und einer ganzen  $n$ -reihigen symmetrischen Matrix  $\mathfrak{I}$ , wobei  $n \leq m$  sei. Ferner nimmt man an es sei  $|\mathfrak{S}| \cdot |\mathfrak{I}| \neq 0$ . Man betrachtet dann einerseits die Kongruenz

$$(**) \quad \mathfrak{X}' \mathfrak{S} \mathfrak{X} \equiv \mathfrak{I} \pmod{q}$$

für jedes natürliche  $q$  und andererseits die Gleichung

$$(***) \quad \mathfrak{X}' \mathfrak{S} \mathfrak{X} = \mathfrak{I}.$$

Dabei muß  $\mathfrak{X}$   $m$ -zeilig und  $n$ -spaltig sein. Über die Beziehungen zwischen der Lösbarkeit von  $(**)$  und  $(***)$  in rationalen  $\mathfrak{X}$  gibt der *Hasse-Legendresche Satz* Aufschluß. Dieser Satz besagt:

*Die Gleichung  $(***)$  ist dann und nur dann mit rationalem  $\mathfrak{X}$  lösbar, wenn  $(**)$  für jedes natürliche  $q$  mit rationalem  $\mathfrak{X}$  und  $(***)$  mit reellem  $\mathfrak{X}$  lösbar ist.*

Man fragt nun danach, ob auch  $(***)$  ganz-rational lösbar ist, wenn  $(**)$  für jedes  $q$  mit ganzem  $\mathfrak{X}$  und  $(***)$  reell lösbar ist. Das Beispiel

$$\mathfrak{S} = \begin{pmatrix} 2 & 0 \\ 0 & 7 \end{pmatrix}, \quad \mathfrak{I} = (1)$$

zeigt, daß dies nicht immer der Fall ist. Es gilt aber folgender

**Satz III.** *Vorausgesetzt sei, daß  $(**)$  für jedes  $q$  mit ganzem  $\mathfrak{X}$  und  $(***)$  reell lösbar ist. Dann gibt es im Geschlecht von  $\mathfrak{S}$  ein  $\mathfrak{S}^*$ , für das*

$$\mathfrak{X}' \mathfrak{S}^* \mathfrak{X} = \mathfrak{I}$$

*mit ganzem  $\mathfrak{X}$  lösbar ist.*

Siegel hat diesen Satz unter Benutzung des Hasse-Legendreschen Satzes bewiesen <sup>3)</sup>. Im sechsten Paragraphen des vorliegenden Aufsatzes soll gezeigt werden, wie man diesen Satz ohne Verwendung der rationalen Theorie der quadratischen Formen aus dem Geschlechtersatz ableiten kann. Der so gefundene Beweis von Satz III ist dann einheitlicher als der

<sup>3)</sup> S., 550.

Siegelsche, weil man direkt von der mod  $q$  ganzzahligen Lösbarkeit von (\*\*) auf die ganzzahlige Lösbarkeit von  $\mathfrak{X}'\mathfrak{S}^*\mathfrak{X} = \mathfrak{X}$  schließt.

Es sei noch bemerkt, daß der Vorteil des Geschlechtersatzes gegenüber den bisherigen Resultaten der Geschlechtertheorie darin liegt, daß weder Elementarteiler noch quadratische Restsymbole explizit vorkommen. Infolgedessen ist es nicht nötig, bei der Formulierung dieses Satzes Fallunterscheidungen zu machen, was bei den bisherigen Sätzen der Geschlechtertheorie immer nötig war. Ferner wird es aus dem gleichen Grund auch nicht allzu schwierig sein, den Geschlechtersatz auf quadratische Formen in algebraischen Zahlkörpern zu übertragen.

## § 2. Hilfsbetrachtungen über Gaußsche Summen.

Beim Beweis des Geschlechtersatzes sind die Gaußschen Summen von Bedeutung weil sie bestimmte Invarianzeigenschaften und eine Reziprozitätsformel haben.

Man definiert für die quadratische Form  $\mathfrak{x}'\mathfrak{S}\mathfrak{x}$  mit der ganzen  $m$ -reihigen symmetrischen Matrix  $\mathfrak{S}$  und der variablen  $m$ -gliedrigen Spalte  $\mathfrak{x}$ , deren Elemente  $x_1, x_2, \dots, x_m$  seien, die Gaußsche Summe  $G_q(\mathfrak{S})$  durch

$$(1) \quad G_q(\mathfrak{S}) = \sum_{\mathfrak{x}(q)} e^{\frac{2\pi i}{q} \mathfrak{x}'\mathfrak{S}\mathfrak{x}}.$$

Dabei ist  $q$  irgendein fester natürlicher Modul, und die Elemente von  $\mathfrak{x}$  durchlaufen unabhängig voneinander ein volles Restsystem mod  $q$ . Die Summe  $G_q(\mathfrak{S})$  ändert sich nicht, wenn man die Elemente von  $\mathfrak{S}$  und  $\mathfrak{x}$  durch andere Repräsentanten ihrer Restklasse mod  $q$  ersetzt. Ist ferner  $\mathfrak{B}$  eine  $m$ -reihige Matrix, deren Determinante zu  $q$  teilerfremd ist, also eine mod  $q$  ganzzahlig umkehrbare Matrix, so gilt

$$(2) \quad G_q(\mathfrak{S}) = G_q(\mathfrak{B}'\mathfrak{S}\mathfrak{B}).$$

Denn mit  $\mathfrak{x}$  durchläuft auch  $\mathfrak{B}\mathfrak{x}$  ein volles Restsystem mod  $q$ . Man nennt Matrizen  $\mathfrak{B}$  mit dieser Eigenschaft unimodular mod  $q$ . Deshalb kann man Formel (2) auch so aussprechen:  $G_q(\mathfrak{S})$  ist invariant gegenüber mod  $q$  unimodularer Transformation von  $\mathfrak{S}$ .

In der Folge werden noch einige andere Eigenschaften von  $G_q(\mathfrak{S})$  benutzt, die ebenfalls leicht aufzuweisen sind. Man sieht ohne weiteres, daß bei beliebigem natürlichem  $a$

$$(3) \quad G_{aq}(a\mathfrak{S}) = a^m G_q(\mathfrak{S})$$

ist. Ferner ist für  $q = rk$  mit  $(r, k) = 1$

$$(4) \quad G_q(\mathfrak{S}) = G_r(k\mathfrak{S}) G_k(r\mathfrak{S}).$$

Um das nachzuprüfen, braucht man nur in (1)

$$\mathfrak{x} = r\mathfrak{y} + k\mathfrak{z}$$

einzutragen, wo  $\mathfrak{y}$  und  $\mathfrak{z}$   $m$ -gliedrige variable Spalten bedeuten. Wenn nämlich die Elemente von  $\mathfrak{y}$  ein volles Restsystem mod  $k$  und die Elemente von  $\mathfrak{z}$  ein volles Restsystem mod  $r$  durchlaufen, so durchlaufen die Elemente von  $\mathfrak{x}$  ein volles Restsystem mod  $q$ . Bei dieser Substitution wird

$$(r\mathfrak{y} + k\mathfrak{z})'\mathfrak{S}(r\mathfrak{y} + k\mathfrak{z}) = r^2\mathfrak{y}'\mathfrak{S}\mathfrak{y} + 2rk\mathfrak{y}'\mathfrak{S}\mathfrak{z} + k^2\mathfrak{z}'\mathfrak{S}\mathfrak{z}.$$

Da  $2\mathfrak{y}'\mathfrak{S}\mathfrak{z}$  für ganzes  $\mathfrak{y}$  und  $\mathfrak{z}$  stets ganz ist, erhält man aus (1) sofort (4).

Nun sei  $\mathfrak{S}$  einreihig, und zwar  $\mathfrak{S} = qd$ , wobei  $d$  eine ganze von Null verschiedene Zahl bedeutet. Weiter sei  $p$  eine zu  $2qd$  teilerfremde Primzahl, und  $\left(\frac{d}{p}\right)$  bedeute das Legendresche quadratische Restsymbol. Dann ist

$$(5) \quad G_p(qd) = \left(\frac{d}{p}\right) G_p(q).$$

Einen einfachen Beweis dieser Formel findet man z. B. bei Bachmann <sup>4)</sup>.

<sup>4)</sup> P. Bachmann, Die analytische Zahlentheorie (Leipzig 1894), 155.

Während man die bisherigen Formeln über Gaußsche Summen durch algebraische Umformungen erhält, braucht man zum Beweis der folgenden Reziprozitätsformel analytische Hilfsmittel. Der absolute Betrag der Determinante von  $\mathfrak{S}$  sei mit  $s$  bezeichnet. Wie in der Einleitung bedeute das Zahlenpaar  $\mu, m - \mu$  die Signatur von  $\mathfrak{S}$ ; weiter sei  $\mu - (m - \mu) = \sigma$  gesetzt. Man nennt  $\mathfrak{S}$  gerade oder ungerade, je nachdem die quadratische Form  $\mathfrak{x}'\mathfrak{S}\mathfrak{x}$  nur gerade Zahlen darstellt oder auch ungerade. Sind jetzt  $a$  und  $b$  natürliche Zahlen derart, daß  $ab$  gerade ist bei ungeradem  $\mathfrak{S}$ , dann gilt die Reziprozitätsformel

$$(6) \quad b^{-\frac{m}{2}} \sum_{\mathfrak{x}(b)} e^{\frac{\pi i a}{b} \mathfrak{x}'\mathfrak{S}\mathfrak{x}} = e^{\frac{\pi i}{4} \sigma} a^{-\frac{m}{2}} s^{\frac{1}{2} - m} \sum_{\mathfrak{x}(sa)} e^{-\frac{\pi i b}{a} \mathfrak{x}'\mathfrak{S}^{-1}\mathfrak{x}}.$$

Diese Formel wurde von Krazer bewiesen<sup>5)</sup>. Der Beweis sei hier noch einmal kurz angegeben, weil die Formel für die weiteren Überlegungen grundlegend ist.

*Beweis.* Für variables positives  $\lambda$  wird

$$\lambda \mathfrak{S} - i \frac{a}{b} \mathfrak{S} = \mathfrak{T}$$

gesetzt, wobei  $\mathfrak{S}$  die Einheitsmatrix bedeutet. Ferner sei

$$(7) \quad f(\lambda) = \sum_{\mathfrak{x}} e^{-\pi \mathfrak{x}'\mathfrak{T}\mathfrak{x}},$$

wo  $\mathfrak{x}$  alle ganzen  $m$ -gliedrigen Spalten durchläuft. Weil  $\lambda > 0$  ist, konvergiert diese Reihe absolut. Aus der Transformationsformel der  $\vartheta$ -Funktion ergibt sich dann, daß  $f(\lambda)$  auch die Entwicklung

$$f(\lambda) = |\mathfrak{T}|^{-\frac{1}{2}} \sum_{\mathfrak{x}} e^{-\pi \mathfrak{x}'\mathfrak{T}^{-1}\mathfrak{x}}$$

hat. Man rechnet sich aus, daß dabei

$$\mathfrak{T}^{-1} = i \frac{b}{a} \mathfrak{S}^{-1} + \lambda \frac{b^2}{a^2} \mathfrak{S}^{-2} (\mathfrak{S} - \lambda \mathfrak{T}^{-1})$$

ist. Nun macht man die Substitution  $\mathfrak{x} = \mathfrak{x}_1 + s a \mathfrak{x}$  und läßt  $\mathfrak{x}_1$  alle Reste mod  $sa$  und  $\mathfrak{x}$  wieder alle ganzen Spalten durchlaufen. Dann wird

$$f(\lambda) = |\mathfrak{T}|^{-\frac{1}{2}} \sum_{\mathfrak{x}_1(sa)} e^{-\pi i \frac{b}{a} \mathfrak{x}_1' \mathfrak{S}^{-1} \mathfrak{x}_1} \sum_{\mathfrak{x}} e^{-\pi \lambda b^2 s^2 (a^{-1} s^{-1} \mathfrak{x}_1 + \mathfrak{x})' \mathfrak{S}^{-2} (\mathfrak{S} - \lambda \mathfrak{T}^{-1}) (a^{-1} s^{-1} \mathfrak{x}_1 + \mathfrak{x})}.$$

Deshalb wird für  $\lambda \rightarrow 0$

$$f(\lambda) \sim |\mathfrak{T}|^{-\frac{1}{2}} (b^2 \lambda)^{-\frac{m}{2}} s^{1-m} \sum_{\mathfrak{x}_1(sa)} e^{-\pi i \frac{b}{a} \mathfrak{x}_1' \mathfrak{S}^{-1} \mathfrak{x}_1}.$$

Dabei ist noch der Wert von  $|\mathfrak{T}|^{-\frac{1}{2}}$  für  $\lambda \rightarrow 0$  zu bestimmen. Zu diesem Zweck transformiert man  $\lambda \mathfrak{S} - i \frac{a}{b} \mathfrak{S}$  mit einer solchen reellen orthogonalen Matrix  $\mathfrak{D}$ , für die  $\mathfrak{D}' \mathfrak{S} \mathfrak{D} = \mathfrak{D}$  ist, wobei  $\mathfrak{D}$  eine Diagonalmatrix bedeutet. Die Diagonalelemente von  $\mathfrak{D}$  seien mit  $d_1, d_2, \dots, d_m$  bezeichnet. Dann wird

$$\left| \lambda \mathfrak{S} - i \frac{a}{b} \mathfrak{S} \right| = \left| \lambda \mathfrak{S} - i \frac{a}{b} \mathfrak{D} \right| = \prod_{k=1}^m \left( \lambda - i \frac{a}{b} d_k \right).$$

Da  $\lambda$  positiv war, wird für  $\lambda \rightarrow 0$

$$|\mathfrak{T}|^{-\frac{1}{2}} \sim s^{-\frac{1}{2}} \left( \frac{b}{a} \right)^{\frac{m}{2}} e^{\frac{\pi i}{4} \sigma}.$$

<sup>5)</sup> A. Krazer, Zur Theorie der mehrfachen Gaußschen Summen, H. Weber-Festschrift (Leipzig 1912), 181.

Andrerseits erhält man aus (7) für  $\lambda = 0$

$$f(\lambda) \sim (b^2 \lambda)^{-\frac{m}{2}} \sum_{\mathfrak{z}(b)} e^{\pi i \frac{a}{b} \mathfrak{z}' \mathfrak{z}}.$$

Aus den drei asymptotischen Gleichungen folgt jetzt sofort die Richtigkeit der Formel (6).

Aus der Reziprozitätsformel (6) folgt eine weitere für den Beweis des Geschlechtersatzes wichtige Formel. Es ist dabei zweckmäßig den Nenner einer rationalen Matrix zu definieren. Man nennt die symmetrische Matrix  $\mathfrak{M} = (m_{kl})$  halbganz, wenn die quadratische Form  $\mathfrak{z}' \mathfrak{M} \mathfrak{z}$  ganz ist für alle ganzen  $\mathfrak{z}$ , wenn also  $m_{kk}$  und  $2m_{kl}$  ( $l \neq k$ ) ganz sind. Für beliebiges rationales symmetrisches  $\mathfrak{M}$  sei dann unter dem Nenner  $\nu$  von  $\mathfrak{M}$  die kleinste natürliche Zahl verstanden, so daß  $\nu \mathfrak{M}$  halbganz ist.

$\mathfrak{S}$  sei wieder unsere ganze symmetrische Matrix,  $\mathfrak{C}$  irgendeine ganze  $m$ -reihige Matrix derart, daß der absolute Betrag  $c$  ihrer Determinante  $> 0$  ist, und  $q$  sei wieder eine natürliche Zahl. Es wird dann  $\mathfrak{Z} = \mathfrak{C}' \mathfrak{S} \mathfrak{C}$  gesetzt und behauptet:

Ist der Nenner von  $\frac{q}{4} \mathfrak{Z}^{-1}$  teilerfremd zu  $c$ , so gilt

$$(8) \quad G_q(\mathfrak{Z}) = c G_q(\mathfrak{S}).$$

Beweis. Aus (6) folgt

$$G_q(\mathfrak{Z}) = e^{\frac{\pi i}{4} \sigma} \left( \frac{q}{2} \right)^{\frac{m}{2}} (c^2 s)^{\frac{1}{2} - m} \sum_{\mathfrak{z}(2c^2 s)} e^{-\pi i \frac{q}{2} \mathfrak{z}' \mathfrak{Z}^{-1} \mathfrak{z}}.$$

Den Nenner von  $\frac{q}{4} \mathfrak{Z}^{-1}$  bezeichnet man mit  $f$  und ersetzt in der rechten Summe  $\mathfrak{z}$  durch  $\mathfrak{z}^* + f \mathfrak{y}$ , wo  $\mathfrak{y}$  eine beliebige ganze  $m$ -gliedrige Spalte bedeutet. Dann wird

$$e^{-\pi i \frac{q}{2} \mathfrak{z}' \mathfrak{Z}^{-1} \mathfrak{z}} = e^{-\pi i \frac{q}{2} \mathfrak{z}'^* \mathfrak{Z}^{-1} \mathfrak{z}^*}.$$

Also wird auch

$$\sum_{\mathfrak{z}(2c^2 s)} e^{-\pi i \frac{q}{2} \mathfrak{z}' \mathfrak{Z}^{-1} \mathfrak{z}} = \left( \frac{2c^2 s}{f} \right)^m \sum_{\mathfrak{z}(f)} e^{-\pi i \frac{q}{2} \mathfrak{z}' \mathfrak{Z}^{-1} \mathfrak{z}}.$$

Weil aber  $f$  zu  $c$  teilerfremd sein sollte, kann man nach Formel (2) in der rechten Summe  $\mathfrak{z}$  durch  $\mathfrak{C}' \mathfrak{z}$  ersetzen. Jetzt wendet man noch auf  $G_q(\mathfrak{S})$  die Reziprozitätsformel (6) an und beachtet, daß

$$\sum_{\mathfrak{z}(2s)} e^{-\pi i \frac{q}{2} \mathfrak{z}' \mathfrak{S}^{-1} \mathfrak{z}} = \left( \frac{2s}{f} \right)^m \sum_{\mathfrak{z}(f)} e^{-\pi i \frac{q}{2} \mathfrak{z}' \mathfrak{S}^{-1} \mathfrak{z}}$$

besteht. Durch Eintragen ergibt sich sofort die Formel (8).

### § 3. Hilfsbetrachtungen über Kongruenzen.

Es sei wieder  $d$  eine ganze von Null verschiedene Zahl,  $P$  sei das Produkt über die verschiedenen ungeraden Primteiler von  $d$ , und es sei  $|d| = D$  gesetzt.  $\mathfrak{S}$  habe dieselbe Bedeutung wie bisher. Über den natürlichen Modul  $q$  soll jetzt vorausgesetzt werden:

$$8DP \mid q.$$

Dann besagt

Hilfssatz 1. Es sei  $r$  eine natürliche Zahl die keine anderen Primfaktoren enthält als  $q$ . Gibt es dann ein zu  $q$  teilerfremdes  $x_0$  so daß

$$(9) \quad |\mathfrak{S}| \equiv dx_0^2 \pmod{q}$$

besteht, so ist auch die Kongruenz

$$(10) \quad |\mathfrak{S}| \equiv dx^2 \pmod{qr}$$

mit einem zu  $q$  teilerfremden  $x$  lösbar.

Den Beweis braucht man nur für den Fall zu führen, daß  $r$  Primzahl ist. Aus (9) entnimmt man  $|\mathfrak{S}| = dx_0^2 + qc$  mit ganzem  $c$ . Man setzt

$$x = x_0 + \frac{q}{2d} y$$

mit ganzem  $y$ . Nach (10) soll dann gelten:

$$dx_0^2 + qc \equiv dx_0^2 + qx_0 y + \frac{q^2}{4d} y^2 \pmod{qr}.$$

Wegen der Teilbarkeitsvoraussetzung über  $q$  ist  $\frac{q}{4rd}$  ganz; daher wird

$$c \equiv x_0 y \pmod{r}.$$

Diese Kongruenz hat eine Lösung  $y$ , weil ja  $(x_0, q) = 1$ , also auch  $(x_0, r) = 1$  ist. Damit ist Hilfssatz 1 bewiesen.

Man sagt, eine Zahl  $k$  wird durch  $\mathfrak{x}'\mathfrak{S}\mathfrak{x} \pmod{q}$  *primitiv* dargestellt, wenn  $\mathfrak{x}'\mathfrak{S}\mathfrak{x} \equiv k \pmod{q}$  ist, mit ganzem  $\mathfrak{x}$  und so, daß  $(x_1, x_2, \dots, x_m, q) = 1$  ist.

Nun sei  $m \geq 2$ , und es gelte

$$|\mathfrak{S}| \equiv d \pmod{q}.$$

Weiter sei angenommen, daß es eine natürliche zu  $q$  teilerfremde Zahl  $k$  gibt, die durch  $\mathfrak{x}'\mathfrak{S}\mathfrak{x}$  modulo  $q$  darstellbar ist. Im Fall  $m = 2$  sei außerdem  $k$  Primzahl, und das Legendresche Symbol  $\left(\frac{-d}{k}\right)$  habe den Wert  $+1$ . Dann besagt

*Hilfssatz 2. Bei gegebenem natürlichem Exponenten  $b$  gibt es eine ganze symmetrische Matrix  $\mathfrak{S}_1$  mit den Eigenschaften*

- 1)  $\mathfrak{S}_1 \equiv \mathfrak{S} \pmod{q}$ ,
- 2)  $|\mathfrak{S}_1| \equiv d \pmod{qk^b}$ ,
- 3)  $k$  ist durch  $\mathfrak{x}'\mathfrak{S}_1\mathfrak{x} \pmod{qk^b}$  primitiv darstellbar.

*Beweis.* Mit  $\mathfrak{S}_2$  bezeichne man die Diagonalmatrix mit den Diagonalelementen  $d, 1, \dots, 1$ . Man wähle  $\xi$  und  $\eta$  so, daß die Kongruenzen

$$q\xi \equiv 1 \pmod{k^b}, \quad k^b\eta \equiv 1 \pmod{q}$$

erfüllt sind, und setze

$$\mathfrak{S}_1 = k^b\eta\mathfrak{S} + q\xi\mathfrak{S}_2.$$

Dann hat  $\mathfrak{S}_1$  die Eigenschaften 1) und 2). Man hat nur noch festzustellen, daß  $k$  durch  $\mathfrak{x}'\mathfrak{S}_1\mathfrak{x} \pmod{k^b}$  primitiv darstellbar ist, denn dann ist für  $\mathfrak{S}_1$  auch 3) erfüllt.

Zunächst sei  $b = 1$ . Die Kongruenz

$$dx_1^2 + x_2^2 + \dots + x_m^2 \equiv k \pmod{k}$$

ist für  $m = 2$  wegen  $\left(\frac{-d}{k}\right) = +1$ ,  $k$  Primzahl, primitiv lösbar. Sie ist aber auch für  $m > 2$  primitiv lösbar, weil sogar stets

$$dx_1^2 + x_2^2 + x_3^2 \equiv k \pmod{k}$$

primitiv lösbar ist.

Jetzt sei  $b > 1$  und  $dx_1^2 + x_2^2 + \dots + x_m^2 \equiv k \pmod{k^{b-1}}$  lösbar unter der Bedingung  $(x_1, x_2, \dots, x_m, k) = 1$ . Dann setzt man  $x_* + k^{b-1}y_*$  statt  $x_*$  und erhält

$$\begin{aligned} d(x_1 + k^{b-1}y_1)^2 + (x_2 + k^{b-1}y_2)^2 + \dots + (x_m + k^{b-1}y_m)^2 \\ \equiv dx_1^2 + x_2^2 + \dots + x_m^2 + 2k^{b-1}(dx_1y_1 + x_2y_2 + \dots + x_my_m) \pmod{k^b}. \end{aligned}$$

Man hat jetzt nur noch  $y_1, y_2, \dots, y_m$  so zu wählen, daß

$$2(dx_1y_1 + x_2y_2 + \dots + x_my_m) \equiv -\frac{dx_1^2 + x_2^2 + \dots + x_m^2 - k}{k^{b-1}} \pmod{k}$$

ist. Das ist möglich weil  $(2x_1, 2x_2, \dots, 2x_m, k) = 1$  ist. Also ist  $k$  durch  $x' \mathfrak{S}_2 x \pmod{k^b}$  primitiv darstellbar für beliebiges natürliches  $b$ .

#### § 4. Der Geschlechtersatz.

Zunächst soll die in der Einleitung gestellte Frage etwas anders formuliert werden. Gegeben sei das Zahlenpaar  $\mu, m - \mu$ , wobei  $\mu$  und  $m - \mu$  ganze Zahlen  $\geq 0$  sind. Weiter sei die natürliche Zahl  $D$  gegeben und

$$(-1)^{m-\mu} D = d$$

gesetzt. Drittens sei eine Klasse von symmetrischen  $m$ -reihigen Matrizen nach einem festen Modul  $q$  gegeben, wobei  $q$  der Teilbarkeitsbedingung

$$(11) \quad 8DP \mid q$$

genügen soll. Dabei bedeutet  $P$  wie im vorigen Paragraphen das Produkt über alle ungeraden Primteiler von  $D$ . Die Bedingung (11) muß erfüllt sein, weil später der Hilfssatz 1 angewandt wird. Die Gesamtheit der Matrizen der gegebenen Klasse modulo  $q$  soll zur Abkürzung mit  $\mathfrak{S}(q)$  bezeichnet werden; diese Klasse denkt man sich durch einen beliebigen Repräsentanten  $\mathfrak{S}$  festgelegt. Unsere Frage lautet jetzt so:

Wann gibt es eine ganze symmetrische Matrix  $\mathfrak{S}_0$  mit den Eigenschaften:

- 1)  $\mathfrak{S}_0$  gehört zu  $\mathfrak{S}(q)$ , 2)  $\mathfrak{S}_0$  hat die Signatur  $\mu, m - \mu$ , 3)  $|\mathfrak{S}_0| = d$ ?

Diese Frage ist für  $q = 8D^3$  gleichbedeutend mit der in der Einleitung gestellten Frage: Wann gehört zu gegebenen Invarianten  $(\alpha), (\beta), (\gamma)$  ein Geschlecht quadratischer Formen?

Man nimmt zunächst an, das gesuchte  $\mathfrak{S}_0$  existiert. Dann muß für jedes  $\mathfrak{S}$  aus  $\mathfrak{S}(q)$  nach Definition der Äquivalenz mod  $q$  (siehe § 1)

$$\mathfrak{U}'\mathfrak{S}\mathfrak{U} \equiv \mathfrak{S}_0 \pmod{q}, \quad \mathfrak{V}'\mathfrak{S}_0\mathfrak{V} \equiv \mathfrak{S} \pmod{q}$$

sein mit ganzem  $\mathfrak{U}$  und  $\mathfrak{V}$ . Durch Determinantenbildung folgt  $|\mathfrak{V}|^2 d \equiv |\mathfrak{S}| \pmod{q}$  und  $|\mathfrak{U}|^2 |\mathfrak{S}| \equiv d \pmod{q}$ , also auch  $|\mathfrak{U}|^2 |\mathfrak{V}|^2 \equiv 1 \pmod{\frac{q}{D}}$ . Da nach (11) die Zahl  $q$  durch  $8DP$  teilbar ist, müssen  $|\mathfrak{U}|$  und  $|\mathfrak{V}|$  zu  $q$  teilerfremd sein. Deshalb muß für jedes  $\mathfrak{S}$  aus  $\mathfrak{S}(q)$  die Kongruenz

$$(12) \quad |\mathfrak{S}| \equiv dx^2 \pmod{q}$$

mit einem zu  $q$  teilerfremden  $x$  lösbar sein. Damit ist eine erste notwendige Bedingung für die Existenz von  $\mathfrak{S}_0$  gefunden. Um eine zweite zu finden, betrachtet man die durch (1) definierte Gaußsche Summe  $G_q(\mathfrak{S})$ . Wenn  $\mathfrak{S}_0$  existiert, ist nach Formel (6), angewandt mit  $a = 2$  und  $b = q$ ,

$$G_q(\mathfrak{S}_0) = e^{\frac{\pi i}{4}\sigma} \left(\frac{q}{2}\right)^{\frac{m}{2}} D^{\frac{1}{2}-m} \sum_{x \pmod{2D}} e^{-\frac{\pi i q}{2} x^2 \mathfrak{S}_0^{-1} x}$$

mit  $\sigma = \mu - (m - \mu)$ . Da aber  $q$  der Bedingung (11) genügt, ist die rechte Summe gleich der Anzahl ihrer Elemente. Daraus folgt

$$G_q(\mathfrak{S}_0) = e^{\frac{\pi i}{4}\sigma} (2q)^{\frac{m}{2}} D^{\frac{1}{2}}.$$

Andererseits ist  $G_q(\mathfrak{S}_0)$  nur von der Restklasse von  $\mathfrak{S}_0 \pmod{q}$  abhängig, und es besteht für alle  $\mathfrak{S}$  aus  $\mathfrak{S}(q)$  die Kongruenz  $\mathfrak{S} \equiv \mathfrak{V}'\mathfrak{S}_0\mathfrak{V} \pmod{q}$  mit mod  $q$  unimodularen  $\mathfrak{V}$ . Also

ist nach Formel (2) für jedes  $\mathfrak{S}$  aus  $\mathfrak{S}(q)$

$$G_q(\mathfrak{S}_0) = G_q(\mathfrak{S}).$$

Angenommen also, das gesuchte  $\mathfrak{S}_0$  existiert, dann muß für beliebiges  $\mathfrak{S}$  aus  $\mathfrak{S}(q)$

$$(13) \quad G_q(\mathfrak{S}) = e^{\frac{\pi i}{4} \sigma} (2q)^{\frac{m}{2}} D^{\frac{1}{2}}$$

sein.

Es ergab sich also: Wenn das gesuchte  $\mathfrak{S}_0$  existiert, dann besteht für beliebiges  $\mathfrak{S}$  aus  $\mathfrak{S}(q)$  die Kongruenz (12) mit zu  $q$  teilerfremdem  $x$  und die Relation (13). Nun ist zu zeigen, daß keine weiteren Relationen zwischen den drei Bestimmungsstücken Signatur, absoluter Betrag der Determinante  $D$  und Klasse  $\mathfrak{S}(q)$  bestehen. Es ist also zu beweisen, daß der in der Einleitung für  $q = 8D^3$  bereits formulierte *Geschlechtersatz* richtig ist:

*Gegeben seien das Zahlenpaar  $\mu, m - \mu$  und die natürlichen Zahlen  $D$  und  $q$ , ferner eine Klasse  $\mathfrak{S}(q)$ . Die Bedingungen (11), (12) und (13) seien erfüllt. Dann gibt es in der Klasse  $\mathfrak{S}(q)$  eine ganze symmetrische Matrix  $\mathfrak{S}_0$  mit der Signatur  $\mu, m - \mu$  und der Determinante  $d$ .*

Dem Beweis werden einige Betrachtungen vorausgeschickt; dabei wird immer angenommen, daß  $\mu, m - \mu, D, q$  und  $\mathfrak{S}(q)$  gegeben und die Bedingungen (11), (12) und (13) erfüllt sind.

Man nimmt zunächst an, es sei  $\mu = 0$  gegeben. Indem man in (13) zum Konjugiert-komplexen übergeht, ergibt sich, daß alle drei Bedingungen auch für  $-\mathfrak{S}(q)$  anstelle  $\mathfrak{S}(q)$ ,  $\mu = m$  anstelle  $\mu = 0$ ,  $(-1)^m d$  anstelle  $d$  erfüllt sind. Man nehme an, der Geschlechtersatz sei für  $\mu = m$  bewiesen. Dann existiert ein  $-\mathfrak{S}_0$  in  $-\mathfrak{S}(q)$  mit der Signatur  $m, 0$  und der Determinante  $(-1)^m d$ . Also ist  $\mathfrak{S}_0$  eine Matrix aus  $\mathfrak{S}(q)$ ,  $\mathfrak{S}_0$  hat außerdem die Signatur  $0, m$  und die Determinante  $d$ . Es genügt deshalb den Geschlechtersatz für  $\mu > 0$  zu beweisen.

Mit  $\lambda$  bezeichnet man jetzt den größten gemeinsamen Teiler aller Elemente eines  $\mathfrak{S}$  aus  $\mathfrak{S}(q)$  mit  $q$ . Dann ist  $\lambda$  eine Invariante unserer Klasse modulo  $q$ . Für den Moment sei

$$\mathfrak{S} = \lambda \mathfrak{I}, \quad q = \lambda q_1, \quad D = \lambda^m D_1, \quad d = \lambda^m d_1,$$

weiter sei  $P_1$  das Produkt aller ungeraden Primteiler von  $D_1$ . Dann ist  $P_1$  Teiler von  $P$ , und aus (11) entnimmt man

$$8D_1 P_1 \mid q_1.$$

Daraus, daß Bedingung (13) erfüllt ist, folgt dann unter Anwendung von (3)

$$G_{q_1}(\mathfrak{I}) = e^{\frac{\pi i}{4} \sigma} (2q_1)^{\frac{m}{2}} D_1^{\frac{1}{2}}.$$

Ferner ergibt sich aus (12) und aus Hilfssatz 1, daß die Kongruenz

$$|\mathfrak{I}| \equiv d_1 x^2 \pmod{q_1}$$

mit einem zu  $q_1$  teilerfremden  $x$  lösbar ist. Angenommen nun der Geschlechtersatz sei für  $\lambda = 1$  bewiesen, dann kann man ihn für  $\mathfrak{I}, q_1$  und  $D_1$  anstelle  $\mathfrak{S}, q$  und  $D$  anwenden. Also existiert ein ganzes  $\mathfrak{I}_0$  mit  $|\mathfrak{I}_0| = d_1$  und der Signatur  $\mu, m - \mu$ , so daß außerdem  $\mathfrak{I} \equiv \mathfrak{U}' \mathfrak{I}_0 \mathfrak{U} \pmod{q_1}$  mit irgendeinem mod  $q_1$  unimodularen  $\mathfrak{U}$  besteht. Dann ist  $\mathfrak{U}$  auch unimodular mod  $q$ . Nun setzt man  $\mathfrak{S}_0 = \lambda \mathfrak{I}_0$  und prüft nach, daß  $\mathfrak{S}_0$  die gewünschten Eigenschaften hat. Infolgedessen darf für den weiteren Beweis vorausgesetzt werden, daß für die gegebene Klasse mod  $q$  die Zahl  $\lambda = 1$  ist.

Es war vorausgesetzt worden, daß die Kongruenz (12) lösbar ist. Angenommen für ein  $\mathfrak{S}_1$  aus  $\mathfrak{S}(q)$  sei speziell  $|\mathfrak{S}_1| \equiv da^2 \pmod{q}$ , mit einem gewissen zu  $q$  teilerfremden

$a$ , und es sei  $ab \equiv 1 \pmod{q}$ . Dann erhält man einen neuen Repräsentanten  $\mathfrak{S}$  von  $\mathfrak{S}(q)$ , wenn man auf  $\mathfrak{S}_1$  die mod  $q$  unimodulare Transformation mit derjenigen Diagonalmatrix ausübt, deren erstes Diagonalelement  $b$ , deren übrige 1 sind. Dann wird

$$(14) \quad |\mathfrak{S}| \equiv d \pmod{q}.$$

Durch eine weitere mod  $q$  unimodulare Transformation von  $\mathfrak{S}$ , deren Determinante  $\equiv 1 \pmod{q}$  ist, kann man in bekannter Weise erreichen, daß das erste Element der neuen Matrix entweder zu  $q$  teilerfremd ist, oder mit  $q$  nur den Teiler 2 gemeinsam hat; es war ja vorausgesetzt, daß  $\lambda = 1$  ist. Der letzte Fall tritt dabei nur dann stets ein, wenn  $\mathfrak{S}$  gerade ist. Weil  $q$  gerade ist, sind dann alle Matrizen der Klasse  $\mathfrak{S}(q)$  gerade. Falls das erste Element von  $\mathfrak{S}$  zu  $q$  teilerfremd ist, kann man nach dem Dirichletschen Satz über die Primzahlen in arithmetischen Reihen  $\mathfrak{S}$  in seiner Restklasse mod  $q$  noch so abändern, daß das erste Element eine positive Primzahl wird. Für  $m > 2$  braucht man diese letzte Abänderung von  $\mathfrak{S}$  nicht notwendig vorzunehmen, für  $m = 2$  muß sie beim folgenden Beweis gemacht werden, weil Hilfssatz 2 angewandt wird.

Nun seien die Repräsentanten der gegebenen Klasse gerade ( $m \geq 2$ ). Dabei wird weiter angenommen, daß für einen Repräsentanten  $\mathfrak{S}$  das erste Element mit  $q$  nur den Teiler 2 gemeinsam hat. Diese Voraussetzung kann man machen, weil nur noch der Fall  $\lambda = 1$  zu behandeln ist. Mit  $\mathfrak{D}$  bezeichne man die Diagonalmatrix mit den Diagonalelementen 2, 1, ..., 1. Die Matrix  $\mathfrak{I}$  sei jetzt definiert durch

$$(15) \quad \mathfrak{D}\mathfrak{I}\mathfrak{D} = 2\mathfrak{S}.$$

$\mathfrak{I}$  ist dann eine ganze Matrix deren erstes Element zu  $q$  teilerfremd ist. Weiter ist für  $\mathfrak{I}$  die Kongruenz

$$|\mathfrak{I}| \equiv 2^{m-2} dx^2 \pmod{2^{m-2}q}, \quad (x, q) = 1,$$

lösbar, weil (12) erfüllt sein soll. Man setzt zur Abkürzung  $2^{m-2}d = d^*$  und  $2^c q = q^*$ , wo  $c$  eine beliebige natürliche Zahl bedeutet. Aus Hilfssatz 1 folgt, daß auch die Kongruenz

$$(16) \quad |\mathfrak{I}| \equiv d^* x^2 \pmod{q^*}, \quad (x, q) = 1,$$

lösbar ist. Wir wollen, je nachdem ob  $m$  ungerade oder gerade ist  $c = m$  oder  $c = m + 1$  wählen, so daß  $c$  immer eine ungerade Zahl  $\geq m$  ist. Nun betrachtet man die Summe  $G_q(\mathfrak{S})$ . Die Anwendung von Formel (3) mit  $a = 2^c$  ergibt

$$2^{m-1} G_q(\mathfrak{S}) = \left(\frac{1}{2}\right)^{1+m(c-1)} G_{q^*}(2^c \mathfrak{S}).$$

Weil Bedingung (13) erfüllt sein soll, folgt dann

$$(17) \quad \left(\frac{1}{2}\right)^{1+m(c-1)} G_{q^*}(2^c \mathfrak{S}) = e^{\frac{\pi i}{4} \sigma} D^{\frac{1}{2}} q^{\frac{m}{2}} 2^{\frac{3m}{2}-1} = e^{\frac{\pi i}{4} \sigma} 2^m q^{\frac{m}{2}} D^{\frac{1}{2} *}$$

mit  $D^* = 2^{m-2} D$ . Der Definitionsgleichung (15) entnimmt man

$$G_{q^*}(2^{c-1} \mathfrak{D}\mathfrak{I}\mathfrak{D}) = G_{q^*}(2^c \mathfrak{S}).$$

Nun kann man die Formel (8) mit  $2^{\frac{c-1}{2}} \mathfrak{D}$  und  $\mathfrak{I}$  anstelle  $\mathfrak{U}$  und  $\mathfrak{S}$ ,  $2^c \mathfrak{S}$  und  $q^*$  anstelle  $\mathfrak{X}$  und  $q$  anwenden. Es ist nämlich  $|\mathfrak{S}| = dx^2 + qy$ , wo  $y$  eine von  $\mathfrak{S}$  abhängige ganze Zahl bedeutet und  $(x, q) = 1$  ist. Also ist der Nenner von  $\frac{q}{4} \mathfrak{S}^{-1}$  Teiler des Nenners von

$$\frac{q}{4d} : \left(x^2 + \frac{qy}{d}\right).$$

Wegen Bedingung (11) ist dieser Nenner ungerade, also ist die Anwendung von Formel

(8) mit  $\mathfrak{C} = 2^{\frac{c-1}{2}} \mathfrak{D}$  gestattet. Daraus ergibt sich

$$G_{q^*}(2^c \mathfrak{C}) = 2^{1+m \frac{c-1}{2}} G_{q^*}(\mathfrak{I}).$$

Deshalb folgt aus (17)

$$(18) \quad G_{q^*}(\mathfrak{I}) = e^{\frac{\pi i}{4} \sigma} (2q^*)^{\frac{m}{2}} D^{\frac{1}{2}}.$$

Daraus, daß (11) erfüllt sein soll und  $c \geq m$  ist, folgt ferner

$$(19) \quad 8PD^* \mid q^*.$$

Man nimmt nun an, der Geschlechtersatz sei für die Klasse  $\mathfrak{I}(q^*)$  bereits bewiesen. Weil die Bedingungen (16), (18) und (19) erfüllt sind, entnimmt man aus dem Geschlechtersatz, daß es ein ganzes  $\mathfrak{I}_0$  mit der Determinante  $d^*$  und der Signatur  $\mu, m - \mu$  gibt, für das die Kongruenz  $\mathfrak{I} \equiv \mathfrak{U}' \mathfrak{I}_0 \mathfrak{U} \pmod{q^*}$  mit einem mod  $q^*$  unimodularen  $\mathfrak{U}$  erfüllt ist. Aus (15) ergibt sich dann

$$2\mathfrak{C} \equiv \mathfrak{D} \mathfrak{U}' \mathfrak{I}_0 \mathfrak{U} \pmod{q^*}.$$

Aus der Elementarteilertheorie entnimmt man, daß es zwei unimodulare Matrizen  $\mathfrak{B}_1$  und  $\mathfrak{B}_2$  derart gibt, daß  $\mathfrak{U} \mathfrak{D} = \mathfrak{B}_1 \mathfrak{D}^* \mathfrak{B}_2$  ist. Dabei bedeutet  $\mathfrak{D}^*$  eine ganze Diagonalmatrix, deren Determinante durch 2 aber nicht durch 4 teilbar ist. Man kann sich  $\mathfrak{B}_1$  und  $\mathfrak{B}_2$  so gewählt denken, daß das erste Diagonalelement von  $\mathfrak{D}^*$  gerade ist. Dann kann man auch schreiben:

$$\mathfrak{U} \mathfrak{D} = \mathfrak{B}_1 \mathfrak{D} \mathfrak{U}_1,$$

wo jetzt  $\mathfrak{U}_1$  eine ganze Matrix bedeutet, deren Determinante zu  $q^*$  teilerfremd sein muß, weil  $(\mid \mathfrak{U} \mid, q^*) = 1$  ist. Das trägt man in die letzte Kongruenz ein und erhält

$$\mathfrak{C} \equiv \frac{1}{2} \mathfrak{U}_1' \mathfrak{D} \mathfrak{B}_1' \mathfrak{I}_0 \mathfrak{B}_1 \mathfrak{D} \mathfrak{U}_1 \pmod{\frac{q^*}{2}}.$$

Setzt man noch

$$\frac{1}{2} \mathfrak{D} \mathfrak{B}_1' \mathfrak{I}_0 \mathfrak{B}_1 \mathfrak{D} = \mathfrak{C}_0,$$

so ist  $\mathfrak{C}_0$  ganz und gehört zur Klasse  $\mathfrak{C}(q)$  weil  $\mathfrak{C} \equiv \mathfrak{U}_1' \mathfrak{C}_0 \mathfrak{U}_1 \pmod{\frac{q^*}{2}}$  und  $q$  Teiler von  $\frac{q^*}{2}$  ist. Wie man sofort sieht, hat außerdem  $\mathfrak{C}_0$  die Determinante  $d$  und die Signatur  $\mu, m - \mu$ . Ist also der Geschlechtersatz richtig für die Klasse  $\mathfrak{I}(q^*)$ , deren Matrizen ungerade sind, dann ist er auch richtig für die Klasse  $\mathfrak{C}(q)$ .

### § 5. Der Induktionsschluß.

Für  $m = 1$  ist der Geschlechtersatz trivialerweise richtig. Man hat nur  $\mathfrak{C}_0 = d$  zu setzen; dann gehört  $\mathfrak{C}_0$  zur Klasse  $\mathfrak{C}(q)$  weil Bedingung (12) hier  $\mathfrak{C} \sim d \pmod{q}$  bedeutet.

Von jetzt ab sei  $m \geq 2$ . Vorausgesetzt wird wieder, daß die Zahlen  $\mu, m - \mu, D, q$  und die Klasse  $\mathfrak{C}(q)$  gegeben und die Bedingungen (11), (12) und (13) erfüllt sind. Aus den letzten Abschnitten des vorigen Paragraphen entnimmt man dann:

Für den weiteren Beweis kann man voraussetzen, daß  $0 < \mu$  ist. Ferner kann man annehmen, daß für ein geeignetes  $\mathfrak{C}$  aus  $\mathfrak{C}(q)$  auch Bedingung (14) erfüllt ist und  $\mathfrak{C}$  eine positive zu  $q$  teilerfremde Primzahl  $p$  zum ersten Element hat. Man kann weiter annehmen, das zweite Element  $s_{12}$  sei zu  $p$  teilerfremd.

Unter diesen Voraussetzungen wird der Beweis mittels Induktion nach  $m$  geführt. Dabei wird von den Formeln (6) und (8), von Hilfssatz 2 und von der Formel für die

quadratische Ergänzung Gebrauch gemacht. Diese letzte Formel besagt, daß es eine  $(m-1)$ -reihige ganze symmetrische Matrix  $\xi$  derart gibt, daß

$$p\xi' \xi - (px_1 + s_{12}x_2 + \cdots + s_{1m}x_m)^2 = \eta' \xi \eta$$

ist, wobei die Variablen  $x_2, x_3, \dots, x_m$  zu der Spalte  $\eta$  zusammengefaßt sind. Man erkennt sofort, daß mit

$$\mathfrak{F} = \begin{pmatrix} p & s_{12}, \dots, s_{1m} \\ n & \xi \end{pmatrix}$$

zwischen  $\xi$  und  $\xi$  die Beziehung

$$(20) \quad p\xi = \mathfrak{F}' \begin{pmatrix} 1 & n' \\ n & \xi \end{pmatrix} \mathfrak{F}$$

besteht. Dabei bedeutet  $n$  die Nullspalte.

Weil  $(p, q) = 1$  ist, kann man, unter Anwendung von (2) mit  $\mathfrak{B} = p\xi$ , schreiben:

$$G_q(\xi) = \sum_{\xi(\eta)} e^{\frac{2\pi i}{q} p(px_1 + s_{12}x_2 + \cdots + s_{1m}x_m)^2 + \frac{2\pi i}{q} \eta' \xi \eta}.$$

Außerdem ändert sich wegen (2) der Wert von  $G_q(\xi)$  nicht, wenn man die Spalte  $\xi$  der mod  $q$  unimodularen Transformation

$$px_1 + s_{12}x_2 + \cdots + s_{1m}x_m = x, \quad \eta = \eta$$

unterwirft. Also ist folgende Gleichung richtig:

$$(21) \quad G_q(\xi) = G_q(p\xi) G_q(p).$$

Die Summe  $G_q(p\xi)$  soll unter Anwendung von (4) mit der Summe  $G_{p'}(\xi)$  in Zusammenhang gebracht werden. Zu diesem Zweck beachte man, daß aus der Formel für die quadratische Ergänzung folgt:

$$G_p(q\xi) = \sum_{\xi(p)} e^{-\frac{2\pi i}{p} q(s_{12}x_2 + \cdots + s_{1m}x_m)^2}.$$

Hierin ist die Substitution

$$s_{12}x_2 + \cdots + s_{1m}x_m = x, \quad x_3 = x_3, \dots, x_m = x_m$$

gestattet, ohne daß sich der Wert der Summe ändert; es war ja  $(s_{12}, p) = 1$  vorausgesetzt. Also wird

$$G_p(q\xi) = p^{m-2} G_p(-q).$$

Nun wendet man für die Summe  $G_q(p\xi)$  in (21) die Formel (4) an und formt außerdem  $G_q(p)$  mit Hilfe der Reziprozitätsformel (6) um. Dann geht (21) über in

$$G_q(\xi) = e^{\frac{\pi i}{4}} (2q)^{\frac{1}{2}} p^{\frac{3}{2}-m} G_{pq}(\xi).$$

Nach Voraussetzung ist für  $\xi$  die Bedingung (13) erfüllt, so daß sich aus der letzten Gleichung

$$(22) \quad G_{p'}(\xi) = e^{\frac{\pi i}{4}(\sigma-1)} (2pq)^{\frac{m-1}{2}} D^{\frac{1}{2}}$$

ergibt, mit  $p^{m-2} D = D^*$ .

Man unterbricht jetzt den Gedankengang und nimmt zunächst an es sei  $m = 2$ . Dann ist zu zeigen, daß aus (21)

$$\left(\frac{-d}{p}\right) = +1$$

folgt, wo wieder  $\left(\frac{-d}{p}\right)$  das Legendresche Symbol bedeutet. Nach Definition ist jetzt

$\xi = ps_{22} - s_{12}^2$ , weswegen aus Bedingung (14) sofort  $H = |\xi| \equiv d \pmod{q}$  folgt.

Also besagt hier Formel (21)

$$(23) \quad G_q(\mathfrak{S}) = G_q(pd) G_q(p).$$

Auf der linken Seite trägt man den Wert aus (13) ein. Dann wendet man auf die erste der beiden rechtsstehenden Summen die Formel (6) an. Man beachte dabei, daß  $2\mu - 2 - (-1)^\mu = 1$  ist, weil  $\mu$  nur die Werte 1 und 2 haben kann. Auf diese Weise ergibt sich

$$e^{\frac{\pi i}{4}} (8pq)^{\frac{1}{2}} D = G_q(p) \sum_{x(2pD)} e^{-\frac{\pi i q}{2ip} x^2}.$$

Indem man die letzte der beiden Summen erst unter Benutzung von (3) und dann von (2) umformt, ergibt sich

$$(24) \quad e^{\frac{\pi i}{4}} (2pq)^{\frac{1}{2}} = G_q(p) G_p(-dq).$$

Andrerseits ist nach Formel (5)

$$G_p(-dq) = \left(\frac{-d}{p}\right) G_p(q),$$

und nach (4) geht deshalb (24) über in

$$(25) \quad e^{\frac{\pi i}{4}} (2pq)^{\frac{1}{2}} = \left(\frac{-d}{p}\right) G_{pq}(1).$$

Nun rechnet man  $G_{pq}(1)$  mittels Formel (6) aus und findet so, daß aus (25) folgt:

$$\left(\frac{-d}{p}\right) = +1.$$

Es sei wieder  $m \geq 2$ . Weil für  $m = 2$  das Symbol  $\left(\frac{-d}{p}\right)$  den Wert  $+1$  hat, entnimmt man aus Hilfssatz 2, daß es in  $\mathfrak{S}(q)$  ein  $\mathfrak{S}$  gibt mit der Eigenschaft

$$(26) \quad |\mathfrak{S}| \equiv d \pmod{p^b q},$$

bei irgendeinem festen natürlichen  $b$ , das später noch näher festgelegt werden soll. Ferner stellt  $\mathfrak{x}'\mathfrak{S}\mathfrak{x}$  die Zahl  $p \bmod p^b q$  primitiv dar, so daß man annehmen kann,  $\mathfrak{S}$  habe wieder  $p$  zum ersten Element. Ferner ist nach (26) mindestens eine der Zahlen  $s_{11}, s_{12}, \dots, s_{1m}$  zu  $p$  teilerfremd; wegen  $s_{11} = p$  kann man  $(s_{12}, p) = 1$  voraussetzen. Deshalb kann man nachträglich den zu Beginn des Paragraphen gewählten Repräsentanten  $\mathfrak{S}$  aus  $\mathfrak{S}(q)$  so festgelegt denken, daß  $\mathfrak{S}$  der Bedingung (26) genügt und wieder  $p$  zum ersten Element hat.

Man braucht diese Eigenschaften von  $\mathfrak{S}$  um mit Hilfe der Formel (8) die Gleichung (22) umformen zu können. Man setzt zu diesem Zweck  $m = u$  oder  $m + 1 = u$ , je nachdem  $m$  ungerade oder gerade ist. Weiter setzt man  $p^u q = q^*$ . Nach Formel (3) ist dann

$$G_{q^*}(p^{u-1} \mathfrak{S}) = p^{(u-1)(m-1)} G_{pq}(\mathfrak{S}).$$

Nun wendet man Formel (8) mit  $\mathfrak{S}, q^*$  und  $p^{\frac{u-1}{2}} \mathfrak{E}$  anstelle  $\mathfrak{S}, q$  und  $\mathfrak{E}$  an. Danach ist

$$G_{q^*}(p^{u-1} \mathfrak{S}) = p^{\frac{(u-1)(m-1)}{2}} G_{q^*}(\mathfrak{S}).$$

Man hat allerdings noch nachzuweisen, daß der Nenner  $\nu$  von  $\frac{qp}{4} \mathfrak{S}^{-1}$  zu  $p$  teilerfremd ist.

Nach Formel (20) ist

$$\mathfrak{S} \mathfrak{S}^{-1} \mathfrak{S}' = \begin{pmatrix} p & \nu' \\ \nu & p \mathfrak{S}^{-1} \end{pmatrix}.$$

Andrerseits folgt aus Formel (26)

$$|\mathfrak{S}| = d \left( 1 + \frac{qp^by}{d} \right)$$

mit irgendeinem ganzen von  $\mathfrak{S}$  abhängigen  $y$ . Also ist  $\nu$  Teiler des Nenners von

$$\frac{q}{4d} : \left( 1 + \frac{qp^by}{d} \right),$$

infolgedessen ist  $(\nu, p) = 1$ . Aus (22) folgt deshalb

$$(27) \quad G_{q^*}(\mathfrak{S}) = e^{\frac{\pi i}{4}(\sigma-1)} (2q^*)^{\frac{m-1}{2}} D^{*\frac{1}{2}}.$$

Das in (26) noch willkürliche  $b$  legt man jetzt durch die Bedingung

$$b = u + 2 - m$$

fest. Es ergibt sich zunächst aus (20), daß  $|p\mathfrak{S}| = p^2 |\mathfrak{S}|$  ist, weswegen aus (26) folgt

$$(28) \quad |\mathfrak{S}| \equiv d^* \pmod{q^*}$$

mit  $d^* = p^{m-2}d$ . Da ferner die Teilbarkeitsbedingung (11) erfüllt sein sollte und  $u \geq m$  ist, erkennt man auch

$$(29) \quad 8D^*P^* | q^*,$$

wobei  $P^* = pP$  das Produkt über die ungeraden Primteiler von  $D^* = p^{m-2}D$  ist.

Nun nimmt man an, der Geschlechtersatz sei für  $m-1$  anstelle  $m$  bewiesen. Dann folgt aus (27), (28) und (29), daß eine ganze symmetrische Matrix  $\mathfrak{S}_0$  existiert mit den Eigenschaften

1)  $|\mathfrak{S}_0| = d^*$ , 2) Signatur von  $\mathfrak{S}_0$  ist  $\mu-1$ ,  $m-\mu$ , 3)  $\mathfrak{S} \equiv \mathfrak{U}'\mathfrak{S}_0\mathfrak{U} \pmod{q^*}$ ,  
wobei  $(|\mathfrak{U}|, q^*) = 1$  ist. Setzt man noch zur Abkürzung

$$\begin{pmatrix} 1 & \mathfrak{n}' \\ \mathfrak{n} & \mathfrak{U} \end{pmatrix} \mathfrak{F} = \mathfrak{B},$$

so folgt aus (20)

$$(30) \quad p\mathfrak{S} \equiv \mathfrak{B}' \begin{pmatrix} 1 & \mathfrak{n}' \\ \mathfrak{n} & \mathfrak{S}_0 \end{pmatrix} \mathfrak{B} \pmod{q^*}.$$

Ähnlich wie am Ende des vierten Paragraphen zeigt man, daß es eine unimodulare Matrix  $\mathfrak{B}_1$ , eine ganze Diagonalmatrix  $\mathfrak{P}$  mit der Determinante  $p$  und eine mod  $q^*$  unimodulare Matrix  $\mathfrak{U}_1$  derart gibt, daß

$$\mathfrak{B} = \mathfrak{B}_1 \mathfrak{P} \mathfrak{U}_1$$

ist. Nun setzt man

$$p\mathfrak{S}_0 = \mathfrak{P}' \mathfrak{B}'_1 \begin{pmatrix} 1 & \mathfrak{n}' \\ \mathfrak{n} & \mathfrak{S}_0 \end{pmatrix} \mathfrak{B}_1 \mathfrak{P}.$$

Trägt man das in (30) ein, so ergibt sich

$$(31) \quad p\mathfrak{S} \equiv p\mathfrak{U}'_1 \mathfrak{S}_0 \mathfrak{U}_1 \pmod{q^*}.$$

Dabei ist  $\mathfrak{S}_0$  ganz, weil  $p\mathfrak{S}_0$  ganz und nach (31) alle Elemente von  $p\mathfrak{S}_0$  durch  $p$  teilbar sind. Nach (31) ist weiter  $\mathfrak{S}_0 \sim \mathfrak{S} \pmod{q}$ , weil  $q$  Teiler von  $\frac{q^*}{p}$  ist. Endlich rechnet man sofort nach, daß  $\mathfrak{S}_0$  die Determinante  $d$  und die Signatur  $\mu, m-\mu$  hat. Damit ist der Geschlechtersatz bewiesen.

## § 6. Anwendung des Geschlechtersatzes.

Man geht jetzt zurück auf die Gleichungen (\*\*) und (\*\*\*) der Einleitung. Darin war  $\mathfrak{S}$  ganz, symmetrisch,  $m$ -reihig und  $\mathfrak{I}$  ganz, symmetrisch,  $n$ -reihig. Die Determinanten von  $\mathfrak{S}$  und  $\mathfrak{I}$  seien  $S$  und  $T$ ; die absoluten Beträge von  $S$  und  $T$  seien  $s$  und  $t$  ( $st \neq 0$ ).

Die Signatur von  $\mathfrak{S}$  sei wieder  $\mu, m - \mu$ , diejenige von  $\mathfrak{I}$  sei  $\nu, n - \nu$ ; man nennt dann  $\sigma = \mu - (m - \mu)$  den Index von  $\mathfrak{S}$  und ebenso  $\tau = \nu - (n - \nu)$  den Index von  $\mathfrak{I}$ . Das Ziel ist, den in der Einleitung formulierten Satz III zu beweisen. Von vornherein wird deshalb

$$(32) \quad 0 \leq \mu - \nu \leq m - n$$

angenommen, weil für Satz III angenommen war, daß  $\mathfrak{X}'\mathfrak{S}\mathfrak{X} = \mathfrak{I}$  mit reellem  $\mathfrak{X}$  lösbar ist. Das ist aber dann und nur dann der Fall, wenn die Ungleichung (32) erfüllt ist.

Zunächst betrachtet man die Kongruenz

$$(33) \quad \mathfrak{X}'\mathfrak{S}\mathfrak{X} \equiv \mathfrak{I} \pmod{q},$$

wobei jetzt  $q$  eine feste natürliche Zahl sein soll, die der Bedingung

$$(34) \quad (2st^m)^4 \mid q$$

genügt. Man bezeichnet als *mod  $q$  primitive Lösung* von (33) eine solche Lösung, die man durch hinzufügen von  $m - n$  Spalten zu einer *mod  $q$  unimodularen Matrix* ergänzen kann.

Man nimmt nun zunächst an, es sei  $n < m$  und es existierte eine *mod  $q$  primitive Lösung*  $\mathfrak{X} = \mathfrak{C}$  von (33), wobei jetzt  $\mathfrak{C}$  eine andere Bedeutung hat als bisher. Man kann dann  $\mathfrak{C}$  zu einer *mod  $q$  unimodularen Matrix*  $\mathfrak{U}$  ergänzen. Dabei ist  $\mathfrak{U}$  durch  $\mathfrak{C}$  nicht eindeutig festgelegt; man greift für die weiteren Überlegungen unter allen möglichen  $\mathfrak{U}$  ein festes heraus. Nun setzt man

$$(35) \quad \mathfrak{S}_1 = \mathfrak{U}'\mathfrak{S}\mathfrak{U} \equiv \begin{pmatrix} \mathfrak{I} & \mathfrak{D} \\ \mathfrak{D} & \mathfrak{R} \end{pmatrix} \pmod{q},$$

wobei  $\mathfrak{D}$  ganz,  $(m - n)$ -spaltig und  $n$ -zeilig,  $\mathfrak{R}$  ganz, symmetrisch und  $(m - n)$ -reihig ist. Weil  $\mathfrak{D}$  und  $\mathfrak{R}$  sich aus  $\mathfrak{U}$  bestimmen, sind sie noch von der Wahl von  $\mathfrak{U}$  abhängig. Setzt man noch

$$(36) \quad \mathfrak{G} = t \begin{pmatrix} \mathfrak{C} & \mathfrak{I}^{-1}\mathfrak{D} \\ \mathfrak{R} & \mathfrak{C} \end{pmatrix}, \quad t\mathfrak{S} \equiv t(\mathfrak{R} - \mathfrak{D}'\mathfrak{I}^{-1}\mathfrak{D}) \pmod{q},$$

wo  $\mathfrak{R}$  die Nullmatrix bedeutet, so ist  $\mathfrak{G}$   $m$ -reihig und ganz und  $t\mathfrak{S}$   $(m - n)$ -reihig, ganz und symmetrisch. Man rechnet sofort nach, daß die wichtige Kongruenz

$$(37) \quad t^2\mathfrak{S}_1 \equiv \mathfrak{G}' \begin{pmatrix} \mathfrak{I} & \mathfrak{R} \\ \mathfrak{R} & \mathfrak{S} \end{pmatrix} \mathfrak{G} \pmod{q}$$

besteht. Um später für  $n < m$  Satz III beweisen zu können, zeigt man zunächst, daß aus dem Geschlechtersatz folgt:

**Satz IV.** *Man nehme an, es existiert eine primitive Lösung  $\mathfrak{X} = \mathfrak{C}$  von (33) zu der die Matrix  $\mathfrak{S}$  durch (35) und (36) definiert ist. Dann existiert eine Matrix  $\mathfrak{S}_0$  vom Index  $\delta - \tau$  mit den weiteren Eigenschaften*

$$1) \ t\mathfrak{S}_0 \text{ ist ganz,} \quad 2) \ t\mathfrak{S}_0 \sim t\mathfrak{S} \pmod{q}, \quad 3) \ |\mathfrak{S}_0| = ST^{-1}.$$

Weil  $\mathfrak{D}$  und  $\mathfrak{R}$  von der speziellen Ergänzung von  $\mathfrak{C}$  zu  $\mathfrak{U}$  abhängen, ist auch  $\mathfrak{S}$  davon abhängig. Man kann aber zeigen, daß jede beliebige Ergänzung von  $\mathfrak{C}$  zu  $\mathfrak{U}^*$  vermöge (35) und (36) zu einer solchen Matrix  $\mathfrak{S}^*$  führt, für die  $t\mathfrak{S}^* \sim t\mathfrak{S} \pmod{q}$  ist <sup>6)</sup>. Deshalb ist das in Satz IV auftretende  $\mathfrak{S}_0$  nicht mehr von der speziellen Wahl von  $\mathfrak{U}$  abhängig, sondern allein durch  $\mathfrak{C}$  bestimmt.

Dem Beweis von Satz IV sei noch folgendes vorausgeschickt:

Dieser Satz ist bereits bekannt; Siegel hat ihn zuerst bewiesen <sup>7)</sup>. Er zeigt nämlich zuerst, daß Satz III in einer gewissen Verschärfung richtig ist. Wie in der Einleitung schon

<sup>6)</sup> S., 539,      <sup>7)</sup> S., 559–560.

bemerkt wurde, benutzt er dabei den Hasse-Legendreschen Satz aus der rationalen Theorie der quadratischen Formen. Erst unter Anwendung dieses Satzes konnte Siegel die Sätze III und IV beweisen. Bei dem Beweis des Siegelschen Hauptsatzes aus der analytischen Theorie der quadratischen Formen <sup>8)</sup> braucht übrigens Siegel nicht Satz III, sondern nur Satz IV. Zur Vereinheitlichung des Siegelschen Beweises dieses Hauptsatzes genügt es deshalb, Satz IV zu beweisen, ohne von der rationalen Theorie der quadratischen Formen Gebrauch zu machen. Es wäre also in diesem Zusammenhang nicht nötig, zu zeigen, daß Satz III richtig ist; am Schluß soll jedoch noch gezeigt werden, daß für  $m > n$  Satz III durch eine einfache Rechnung aus Satz IV folgt. Für  $m = n$  wird Satz III ohne weiteres mit Hilfe von Satz I bewiesen. Beim Beweis von Satz IV werden die Betrachtungen aus dem zweiten Paragraphen, der Hilfssatz 1 und der Geschlechtersatz benutzt.

*Beweis.* Aus der Kongruenz (37) folgt durch Determinantenbildung

$$(38) \quad t^{2m} S x^2 \equiv t^{m+n} T |t\mathfrak{L}| \pmod{q}, \quad x = |U|.$$

Wegen (34) ist hier die Anwendung von Hilfssatz 1 gestattet, woraus folgt, daß

$$(39) \quad |t\mathfrak{L}| \equiv x^2 t^{m-n} S T^{-1} \pmod{q}$$

mit zu  $q$  teilerfremdem  $x$  lösbar ist.

Nun setzt man zur Abkürzung  $q = rt$  und

$$\begin{pmatrix} \mathfrak{L} & \mathfrak{N} \\ \mathfrak{N} & \mathfrak{L} \end{pmatrix} = \mathfrak{L}$$

und betrachtet die Gaußsche Summe  $G_r(\mathfrak{G}'\mathfrak{L}\mathfrak{G})$ . Darin ist wegen (37) die Matrix  $\mathfrak{G}'\mathfrak{L}\mathfrak{G}$  ganz. Die Anwendung der Formel (3) mit  $a = t$  ergibt

$$(40) \quad G_r(\mathfrak{G}'\mathfrak{L}\mathfrak{G}) = t^{-m} G_q(t\mathfrak{G}'\mathfrak{L}\mathfrak{G}).$$

Auf diese Summe wendet man noch Formel (8) mit  $\mathfrak{G}$  und  $t\mathfrak{L}$  anstelle  $\mathfrak{C}$  und  $\mathfrak{S}$  an. Das ist gestattet, weil die Kongruenz (38) besteht und  $q$  der Bedingung (34) genügt. Also wird

$$(41) \quad G_q(t\mathfrak{G}'\mathfrak{L}\mathfrak{G}) = t^m G_q(t\mathfrak{L}).$$

Nun folgt aus (37), (40) und (41)

$$G_r(t^2\mathfrak{S}) = G_q(t\mathfrak{L}) G_q(t\mathfrak{L}).$$

Auf  $G_r(t^2\mathfrak{S})$  und  $G_q(t\mathfrak{L})$  wendet man schließlich die Reziprozitätsformel (6) an und erhält

$$(42) \quad G_q(t\mathfrak{L}) = e^{\frac{\pi i}{4}(\sigma-\tau)} (2q)^{\frac{m-n}{2}} (st^{m-n-1})^{\frac{1}{2}}.$$

Den Formeln (34), (39) und (42) entnimmt man, daß mit  $m - n$ ,  $\sigma - \tau$ ,  $t\mathfrak{L}$  und  $t^{m-n}ST$  anstelle  $m$ ,  $\sigma$ ,  $\mathfrak{S}$  und  $d$  die Bedingungen (11), (12) und (13) aus dem vierten Paragraphen erfüllt sind. Nach dem Geschlechtersatz existiert also eine  $(m - n)$ -reihige ganze symmetrische Matrix  $t\mathfrak{L}_0$  mit den Eigenschaften

$$t\mathfrak{L}_0 \sim t\mathfrak{L} \pmod{q}, \quad \text{Index von } \mathfrak{L}_0 \text{ ist } \sigma - \tau, \quad |\mathfrak{L}_0| = ST^{-1}.$$

Damit ist Satz IV bewiesen. Man beachte dabei, daß die Voraussetzung (32) notwendig war, damit das  $(m - n)$ -reihige  $\mathfrak{L}_0$  den Index  $\sigma - \tau$  haben kann.

Es sei jetzt nicht mehr der Fall  $m = n$  ausgeschlossen. Um Satz III zu beweisen, geht man wieder von der Kongruenz (33) aus, worin  $q$  der Bedingung (34) genügt. In Satz III war vorausgesetzt, daß eine Lösung  $\mathfrak{X} = \mathfrak{C}$  von (\*\*\*) für alle natürlichen  $q$ , also speziell eine Lösung von (33) existiert. Dieses  $\mathfrak{C}$  braucht jetzt nicht notwendig mod  $q$  primitiv zu sein. Es sei daran erinnert, daß nach Definition  $\mathfrak{C} \pmod{q}$  primitiv ist, wenn es durch Hinzufügen von  $m - n$  Spalten zu einer mod  $q$  unimodularen Matrix er-

<sup>8)</sup> S., 555.

gänzt werden kann. Dieses ist dann und nur dann der Fall, wenn der größte gemeinsame Teiler aller  $n$ -reihigen Unterdeterminanten von  $\mathfrak{C}$  zu  $q$  teilerfremd ist. Im allgemeinen ist das nicht erfüllt; einer Siegelschen Überlegung kann man aber immer folgendes entnehmen <sup>9)</sup>:

Es gibt eine ganze umkehrbare Matrix  $\mathfrak{R}$  derart, daß  $\mathfrak{C}\mathfrak{R}^{-1} = \mathfrak{B}$  ganz und primitiv ist. Deshalb ist  $|\mathfrak{B}'\mathfrak{C}\mathfrak{B}|$  eine ganze Zahl, also geht der absolute Betrag  $k$  von  $|\mathfrak{R}|$  zum Quadrat in  $|\mathfrak{C}'\mathfrak{C}|$  auf. Angenommen es sei  $k = k_1 r$ , wo  $k_1$  nur solche Primfaktoren enthält, die in  $q$  aufgehen, und  $(r, q) = 1$  ist. Indem man in (33) zu den Determinanten übergeht und beachtet, daß (34) erfüllt ist, sieht man daß

$$k_1^2 \mid t.$$

Unter Benutzung der Elementarteilertheorie kann man schreiben

$$\mathfrak{R} = \mathfrak{U}_1 \mathfrak{R}_1,$$

wo  $|\mathfrak{R}_1| = k_1$  und  $(|\mathfrak{U}_1|, q) = 1$  ist. Man setzt noch  $k_1^2 q_1 = q$ ,  $\mathfrak{B}\mathfrak{U}_1 = \mathfrak{A}$  und

$$\mathfrak{I}_1 = \mathfrak{R}_1^{-1} \mathfrak{I} \mathfrak{R}_1^{-1}.$$

$\mathfrak{I}_1$  ist dann eine ganze Matrix und (33) geht über in

$$(43) \quad \mathfrak{A}'\mathfrak{C}\mathfrak{A} \equiv \mathfrak{I}_1 \pmod{q_1}.$$

Infolgedessen erhält man aus jeder beliebigen Lösung  $\mathfrak{C}$  von (33) eine primitive Lösung  $\mathfrak{A}$  von (43). Dabei ist analog zu (34) die Teilbarkeitsbedingung

$$(2st_1^m)^4 \mid q_1$$

erfüllt, wo  $t_1$  den absoluten Betrag der Determinante von  $\mathfrak{I}_1$  bezeichnet. Man beachte noch, daß die Signaturen von  $\mathfrak{I}$  und  $\mathfrak{I}_1$  die gleichen sind. Angenommen nun, es sei bereits bewiesen, daß aus der Existenz eines primitiven  $\mathfrak{A}$ , das der Kongruenz (43) genügt, die Existenz eines ganzen  $\mathfrak{U}_1$  derart folgt, daß für ein zum Geschlecht von  $\mathfrak{C}$  gehöriges  $\mathfrak{C}^*$

$$\mathfrak{A}'\mathfrak{C}^*\mathfrak{A} = \mathfrak{I}_1$$

gilt. Dann folgt sofort durch Transformation mit  $\mathfrak{R}_1$ , daß Satz III richtig ist.

Hiermit hat sich gezeigt, daß man nur noch folgendes beweisen muß: *Angenommen, es existiert eine mod  $q$  primitive Lösung  $\mathfrak{C}$  von (33), dann gibt es ein ganzes  $\mathfrak{C}_1$  derart, daß*

$$(44) \quad \mathfrak{C}_1'\mathfrak{C}^*\mathfrak{C}_1 = \mathfrak{I}$$

ist.

Zuerst sei  $m = n$ . Dann wird angenommen, es existiert ein mod  $q$  unimodulares  $\mathfrak{C}$  derart, daß (33) erfüllt ist. Daraus folgt  $|\mathfrak{C}|^2 S \equiv T \pmod{q}$ , und aus (34) ergibt sich, daß  $s = t$  ist. Wegen (32) haben außerdem  $\mathfrak{C}$  und  $\mathfrak{I}$  dieselbe Signatur. Nach Satz I gehören deshalb  $\mathfrak{C}$  und  $\mathfrak{I}$  zum selben Geschlecht, und (44) ist mit  $\mathfrak{C}^* = \mathfrak{I}$ ,  $\mathfrak{C}_1 = \mathfrak{C}$  erfüllt.

Jetzt sei  $m > n$ . Man nimmt an, es liege eine mod  $q$  primitive Lösung  $\mathfrak{C}$  von (33) vor und  $\mathfrak{C}$  sei zu einer mod  $q$  unimodularen Matrix  $\mathfrak{U}$  ergänzt. Dann gelten die Formeln (35), (36) und (37). Aus Satz IV ergibt sich ferner, daß eine ganze Matrix  $t\mathfrak{H}_0$  existiert, mit der Determinante  $t^{m-n}ST^{-1}$  und dem Index  $\sigma - \tau$ , für welche die Kongruenz

$$(45) \quad t\mathfrak{H} \equiv t\mathfrak{U}_2'\mathfrak{H}_0\mathfrak{U}_2 \pmod{q}$$

mit einem mod  $q$  unimodularen  $\mathfrak{U}_2$  erfüllt ist. Setzt man bei  $n$ -reihigem  $\mathfrak{C}$  noch

$$(46) \quad \mathfrak{B} = \begin{pmatrix} \mathfrak{C} & \mathfrak{N} \\ \mathfrak{N} & \mathfrak{U}_2 \end{pmatrix},$$

so ist auch  $\mathfrak{B}$  unimodular mod  $q$ , und es folgt durch Eintragen von (45) und (46)

<sup>9)</sup> S., 532.

in (37)

$$(47) \quad t^2 \mathfrak{S}_1 = \mathfrak{U}' \mathfrak{W}' \begin{pmatrix} \mathfrak{I} & \mathfrak{N} \\ \mathfrak{N} & \mathfrak{H}_0 \end{pmatrix} \mathfrak{W} \mathfrak{U} \pmod{q}.$$

Der Elementarteilertheorie entnimmt man wieder, daß sich  $\mathfrak{W} \mathfrak{U}$  auch in der Form

$$(48) \quad \mathfrak{W} \mathfrak{U} = \mathfrak{B}_1 \mathfrak{D} \mathfrak{B}_1$$

schreiben läßt, wobei  $\mathfrak{B}_1$  unimodular,  $\mathfrak{B}_1 \pmod{q}$  unimodular ist und  $\mathfrak{D}$  eine ganze Diagonalmatrix mit  $|\mathfrak{D}| = t^m$  bedeutet. Setzt man noch

$$(49) \quad \mathfrak{D} \mathfrak{B}_1' \begin{pmatrix} \mathfrak{I} & \mathfrak{N} \\ \mathfrak{N} & \mathfrak{H}_0 \end{pmatrix} \mathfrak{B}_1 \mathfrak{D} = t^2 \mathfrak{S}^*,$$

so folgt sofort aus (47)

$$(50) \quad \mathfrak{S} \sim \mathfrak{S}^* \pmod{\frac{q}{t^2}}.$$

Die Elemente von  $\mathfrak{H}_0$  können im Nenner nur Teiler von  $t$  haben, also die Elemente von  $\mathfrak{S}^*$  im Nenner nur Teiler von  $t^3$ . Andererseits ist aber (50) erfüllt, woraus folgt, daß  $\mathfrak{S}^*$  ganz ist. Weil  $|\mathfrak{H}_0| = S T^{-1}$  und  $|\mathfrak{D}| = t^m$  ist, folgt aus (49), daß  $|\mathfrak{S}^*| = S$  ist. Weil  $\mathfrak{H}_0$  den Index  $\sigma - \tau$  hat, folgt weiter, daß  $\mathfrak{S}^*$  den Index  $\sigma$  hat. Hieraus und aus der Äquivalenz (50) folgt unter Anwendung von Satz I (§ 1), daß  $\mathfrak{S}^*$  zum Geschlecht von  $\mathfrak{S}$  gehört.

Man bezeichnet nun mit  $\mathfrak{C}_1$  die ersten  $n$  Spalten von  $\mathfrak{B}_1$ ; dann ist  $\mathfrak{C}_1$  ganz, und man hat noch zu zeigen, daß  $\mathfrak{C}_1$  der Gleichung (44) genügt. Zu diesem Zweck beachtet man, daß nach (48) und (49)

$$\mathfrak{B}_1' \mathfrak{S}^* \mathfrak{B}_1 = t^{-2} \mathfrak{U}' \mathfrak{W}' \begin{pmatrix} \mathfrak{I} & \mathfrak{N} \\ \mathfrak{N} & \mathfrak{H}_0 \end{pmatrix} \mathfrak{W} \mathfrak{U}$$

gilt. Andererseits entnimmt man aus (36) und (46)

$$t^{-1} \mathfrak{W} \mathfrak{U} = \begin{pmatrix} \mathfrak{C} & \mathfrak{I}^{-1} \mathfrak{D} \\ \mathfrak{N} & \mathfrak{U}_2 \end{pmatrix}.$$

Trägt man das in die vorhergehende Gleichung ein, dann erkennt man sofort, daß die ersten  $n$  Spalten  $\mathfrak{C}_1$  von  $\mathfrak{B}_1$  der Gleichung (44) genügen.

Damit ist Satz III bewiesen. Will man noch zeigen, daß die von Siegel bewiesene Verschärfung dieses Satzes gilt, so muß man von zwei weiteren Hilfsbetrachtungen Gebrauch machen<sup>10)</sup>. Das bereitet keine besonderen Schwierigkeiten, weswegen hier nicht weiter darauf eingegangen wird, zumal bei der Anwendung der Überlegungen dieses letzten Paragraphen auf den Beweis des Siegelschen Hauptsatzes nur von Satz IV Gebrauch gemacht wird.

<sup>10)</sup> S., 534, Hilfssatz 6; 548, Hilfssatz 19.

Eingegangen 31. März 1939.