Über die Composition der binären quadratischen Formen

F. Mertens,
M. k. Akad.

1.

Gauss[1] hat die Theorie der Composition der binären quadratischen Formen vornehmlich auf zwei Probleme angewendet: auf die Bestimmung des Verhältnisses der Classenanzahlen, welche für die eigentlich primitive und irgend eine andere Ordnung gelten, und auf die Bestimmung der Anzahl der Geschlechter der eigentlich primitiven Formen. Das erste Problem ist in den Disquisitiones arithmeticae für positive Determinanten nicht vollständig durchgeführt und wurde erst später von Dirichlet mittelst anderer Methoden gelöst. Das zweite Problem, dessen Hauptschwierigkeit in dem Beweise des Satzes besteht, dass jede Classe des Hauptgeschlechts durch Duplication entsteht, wird mit Hilfe der Theorie der ternären quadratischen Formen gelöst.

In dem Folgenden soll eine einfache Lösung des ersten Problems und ein Beweis des genannten Satzes mitgetheilt werden, welche, ähnlich wie bei Arndt[2], aus der Theorie der

---

[1] Gauss, Disquisitiones arithmeticae, Sectio V, art. 256, 287. — Lejeune Dirichlet, De formarum binariarum secundi gradus compositione, 1847. — Dedekind, Vorlesungen über Zahlentheorie, von P. G. Lejeune Dirichlet.

[2] Über die Anzahl der Genera der quadratischen Formen. Crelle's Journal, Bd. 56.

ternären Formen nur einen Hilfssatz von Legendre über die Gleichung

$$ax^2+by^2+cz^2=0$$

erfordert.

2.

Die Lehre von der Composition der binären quadratischen Formen lässt sich auf einen Hilfssatz[1] aus der Theorie der ganzzahligen linear-homogenen Formen gründen.

Ich werde mir hier zur Abkürzung erlauben, eine Summe von Vielfachen mehrerer Grössen als Vielfachsumme dieser Grösse zu bezeichnen und zwei Reihen von Grössen

$$\begin{matrix} A, B, & .E \\ A', B', & E' \end{matrix}$$

gleichstimmig zu nennen, wenn jede Grösse der ersten Reihe als Vielfachsumme der Grössen der zweiten Reihe und ebenso jede Grösse der zweiten Reihe als Vielfachsumme der Grössen der ersten Reihe darstellbar ist.

Wenn p ganzzahlige linear-homogene Formen

$$f_1, f_2, \ldots f_p$$

der n Veränderlichen $x_1, x_2, \ldots x_n$ durch q ähnliche Formen

$$g_1, g_2, \ldots g_q$$

ganzzahlig ausdrückbar und $p \geqq n$, $q \geqq n$ sind, so sind alle Determinanten n^{ter} Ordnung, welche sich aus dem Coëfficientensystem der Formen $f_1, f_2, \ldots f_p$ bilden lassen, Vielfachsummen der Determinanten n^{ter} Ordnung der Formen $g_1, g_2, \ldots g_q$.

Ist nämlich

$$\begin{aligned} f_i &= a_{i1}x_1+a_{i2}x_2+\ldots+a_{in}x_n \\ g_i &= b_{1i}x_1+b_{2i}x_2+\ldots+b_{ni}x_n \\ f_i &= c_{i1}g_1+c_{i2}g_2+\ldots+c_{iq}g_q, \end{aligned}$$

wo $c_{11}, c_{12}, \ldots c_{pq}$ ganze Zahlen bezeichnen, so ergibt sich

$$a_{ik} = c_{i1}b_{k1}+c_{i2}b_{k2}+\ldots+c_{iq}b_{kq}.$$

---

[1] Dedekind, Vorlesungen. 165.

Das Coëfficientensystem der Formen $f_1, f_2, \ldots f_p$ geht daher aus der Zusammensetzung der Systeme

$$\begin{array}{ll} c_{11}, c_{12}, \ldots c_{1q} & b_{11}, b_{12}, \ldots b_{1q} \\ c_{21}, c_{22}, \ldots c_{2q} & b_{21}, b_{22}, \ldots b_{2q} \\ \\ c_{p1}, c_{p2} \ldots c_{pq} & b_{n1}, b_{n2}, \ldots b_{nq} \end{array}$$

hervor und jede Determinante n^{ter} Ordnung der Formen $f_1, f_2, \ldots$ ist demzufolge eine Summe von Producten einer Determinante der Zahlen $c_{11}, c_{12}, \ldots$ also einer ganzen Zahl in eine Determinante n^{ter} Ordnung der Formen $g_1, g_2, \ldots g_q$.

Wenn zwei Systeme $f_1, f_2, \ldots f_p$ und $g_1, g_2, \ldots g_q$ von ganzzahligen linear-homogenen Formen der Veränderlichen $x_1, x_2, \ldots x_n$ gleichstimmig und $p \geqq n$, $q \geqq n$ sind, so sind die Determinanten n^{ter} Ordnung des einen Systems mit denen des anderen gleichstimmig und besitzen demzufolge denselben grössten gemeinschaftlichen Theiler, wenn sie nicht alle $= 0$ sind.

Wenn ein System S von m gegebenen ganzzahligen linear-homogenen Formen

$$f_1, f_2, \ldots f_m$$

der Veränderlichen $x_1, x_2, \ldots x_n$ vom Range n ist, so lässt sich ein und nur ein mit S gleichstimmiges System von n ganzzahligen linear-homogenen Formen

$$\omega_1, \omega_2, \ldots \omega_n$$

der nämlichen Veränderlichen bestimmen, welches folgende Eigenschaften besitzt:

I. ω_k enthält nur die Veränderlichen $x_1, x_2, \ldots x_k$ und das Vorzeichen des Coëfficienten c_{kk} von x_k in ω_k kann beliebig vorgeschrieben werden.

II. Ist $\overline{c_{kk}}$ der Zahlenwerth von c_{kk} und c_{ik} der Coëfficient von x_k in ω_i, so ist für jeden über k liegenden Stellenzeiger i

$$0 \leqq c_{ik} < \overline{c_{kk}}.$$

Zunächst lässt sich ein mit S gleichstimmiges System von n Formen $\varphi_1, \varphi_2, \ldots \varphi_n$ der Veränderlichen $x_1, x_2, \ldots x_n$ aufstellen, welches die Eigenschaft I besitzt.

Es sei zu diesem Ende

$$f_i = a_{i1}x_1 + a_{i2}x_2 + \quad + a_{in}x_n,$$

b_{nn} der mit dem für c_{nn} vorgeschriebenen Vorzeichen behaftete grösste gemeinschaftliche Theiler der Zahlen

$$a_{1n}, a_{2n}, \ldots a_{mn},$$

welche nicht alle $= 0$ sein können, und $\alpha_1, \alpha_2, \ldots \alpha_m$ eine ganzzahlige Lösung der Gleichung

$$a_{1n}\alpha_1 + a_{2n}\alpha_2 + \quad + a_{mn}\alpha_m = b_{nn}.$$

Setzt man

$$\alpha_1 f_1 + \alpha_2 f_2 + \quad . + \alpha_m f_m = \varphi_n,$$

so sind die Differenzen

$$f_1 - \frac{a_{1n}}{b_{nn}}\varphi_n,\ f_2 - \frac{a_{2n}}{b_{nn}}\varphi_n, \ldots f_m - \frac{a_{mn}}{b_{nn}}\varphi_n$$

entweder schon alle $= 0$ oder aber ganzzahlige linear-homogene Formen der $n-1$ Veränderlichen $x_1, x_2, \ldots x_{n-1}$, je nachdem $n = 1$ oder $n > 1$ ist.

Im ersten Falle ist das gegebene System S mit der Form φ_1 gleichstimmig.

Im zweiten Falle sei

$$f_i - \frac{a_{in}}{b_{nn}}\varphi_n = f_i' = a_{i1}'x_1 + a_{i2}'x_2 + \quad + a_{in-1}'x_{n-1}.$$

Die Formen

$$f_1', f_2', \ldots f_m'$$

bilden mit φ_n zusammen ein mit S gleichstimmiges System S_1 und sind vom Range $n-1$. Die Coëfficienten

$$a_{1n-1}', a_{2n-1}', \ldots a_{mn-1}'$$

können daher nicht alle $= 0$ sein und besitzen einen bestimmten grössten gemeinschaftlichen Theiler, welcher, mit dem für $c_{n-1\,n-1}$ vorgeschriebenen Vorzeichen versehen, $= b_{n-1\,n-1}$ sei. Man kann somit auf die Formen $f_1', f_2', \ldots f_m'$ das-

selbe Verfahren wie auf $f_1, f_2, \ldots f_m$ anwenden, indem man eine ganzzahlige Lösung $\beta_1, \beta_2, \ldots$ der Gleichung

$$a'_{1\,n-1}\beta_1 + a'_{2\,n-1}\beta_2 + \ldots + a'_{m\,n-1}\beta_m = b_{n-1\,n-1}$$

ermittelt und die Form

$$\beta_1 f'_1 + \beta_2 f'_2 + \ldots + \beta_m f'_m = \varphi_{n-1}$$

bildet.

Ist $n = 2$, so fallen die Formen

$$f'_1, f'_2, \ldots f'_m$$

mit

$$\frac{a'_{1\,n-1}}{b_{n-1\,n-1}}\varphi_{n-1}, \quad \frac{a'_{2\,n-1}}{b_{n-1\,n-1}}\varphi_{n-1}, \ldots \quad \frac{a'_{m\,n-1}}{b_{n-1\,n-1}}\varphi_{n-1}$$

zusammen und sind mit φ_{n-1} gleichstimmig. Die Formen φ_1, φ_2 sind also mit S_1 und folglich auch mit dem gegebenen System S gleichstimmig.

Ist dagegen $n > 2$, so enthalten die Formen

$$f''_1 = f'_1 - \frac{a'_{1\,n-1}}{b_{n-1\,n-1}}\varphi_{n-1}, \quad f''_2 = f'_2 - \frac{a'_{2\,n-1}}{b_{n-1\,n-1}}\varphi_{n-1}, \ldots$$

nur die $n-2$ Veränderlichen $x_1, x_2 \ldots x_{n-2}$ und bilden mit φ_{n-1} zusammen ein mit $f'_1, f'_2, \ldots f'_m$ gleichstimmiges System. Die Formen

$$\varphi_n, \varphi_{n-1}, f''_1, f''_2, \ldots f''_m$$

bilden daher ein mit S_1 und S gleichstimmiges System S_2.

Wendet man das nämliche Verfahren auf die Formen $f''_1, f''_2, \ldots f''_m$ an und setzt dasselbe nach Bedarf fort, so gelangt man nach n Schritten zu einem mit S gleichstimmigen System von Formen

$$\varphi_1, \varphi_2, \ldots \varphi_n,$$

welche die Eigenschaft I besitzen.

In jedem mit S gleichstimmigen System

$$g_1, g_2, \ldots g_n,$$

welches die Eigenschaft I besitzt, sind die Coëfficienten, welche in $g_1, g_2, \ldots g_n$, beziehungsweise bei $x_1, x_2, \ldots x_n$ stehen, voll-

ständig bestimmt. Es seien, um dies darzuthun, $C_1, C_2, \ldots C_n$ diese Coëfficienten und

$$f_1^0, f_2^0, \ldots f_m^0, g_{\mu+1}^0, g_{\mu+2}^0, \ldots$$

diejenigen Bestandtheile der Formen

$$f_1, f_2, \ldots f_m, g_{\mu+1}, g_{\mu+2}, \ldots g_n,$$

welche die Veränderlichen $x_{\mu+1}, x_{\mu+2}, \ldots x_n$ enthalten. Es leuchtet ein, dass die Formen $f_1^0, f_2^0, \ldots f_m^0$ mit $g_{\mu+1}^0, g_{\mu+2}^0, \ldots g_n^0$ gleichstimmig sind; denn für $\mu = 0$ ist diese Behauptung nichts als die Voraussetzung selbst und für $\mu > 0$ braucht man nur in den Gleichungen zwischen den Formen $f_1, f_2, \ldots$ und $g_1, g_2, \ldots$ die Veränderlichen $x_1, x_2, \ldots x_\mu = 0$ zu setzen, wodurch $g_1, g_2, \ldots g_\mu$ verschwinden. Da die Formen $g_{\mu+1}^0, g_{\mu+2}^0, \ldots g_n^0$ nur die eine Determinante $n-\mu^{\text{ter}}$ Ordnung

$$C_{\mu+1} C_{\mu+2} \ldots C_n$$

besitzen, so muss dieselbe mit den Determinanten $n-\mu^{\text{ter}}$ Ordnung der Formen $f_1^0, f_2^0, \ldots f_m^0$ oder denen des Elementensystems

$$\begin{matrix} a_{1\,\mu+1} a_{2\,\mu+1} \ldots a_{m\,\mu+1} \\ a_{1\,\mu+2} a_{2\,\mu+2} \ldots a_{m\,\mu+2} \\ \ldots \\ a_{1n} \quad a_{2n} \quad \ldots a_{mn} \end{matrix}$$

gleichstimmig sein und daher bis auf das Vorzeichen mit dem grössten gemeinschaftlichen Theiler T_μ derselben zusammenfallen. Es ist also, wenn ε_i die mit dem für c_{ii} vorgeschriebenen Vorzeichen versehene Einheit bezeichnet,

$$C_{\mu+1} C_{\mu+2} \ldots C_n = \varepsilon_{\mu+1} \varepsilon_{\mu+2} \ldots \varepsilon_n T_\mu.$$

Hienach wird

$$C_n = \varepsilon_n T_{n-1}$$

$$C_{n-1} = \varepsilon_{n-1} \frac{T_{n-2}}{T_{n-1}}$$

$$C_1 = \varepsilon_1 \frac{T_0}{T_1}$$

Dass T_μ durch $T_{\mu+1}$ theilbar ist, folgt daraus, dass die Determinanten $n-\mu^{\text{ter}}$ Ordnung des vorstehenden Elementensystems Vielfachsummen der Determinanten $n-\mu-1^{\text{ter}}$ Ordnung des Elementensystems

$$a_{1\,\mu+2}a_{2\,\mu+2}\ldots a_{m\mu+2}$$

$$a_{1\,n}\quad a_{2\,n}\qquad .a_{mn}$$

sind.

Soll nun ein mit S gleichstimmiges System $\omega_1, \omega_2, \ldots \omega_n$ bestimmt werden, welches beide Eigenschaften I und II aufweist, so ist dasselbe auch mit $\varphi_1, \varphi_2, \ldots \varphi_n$ gleichstimmig und man hat

$$\omega_m = h_1\varphi_1 + h_2\varphi_2 + \ldots + h_n\varphi_n,$$

wo $h_1, h_2, \ldots h_n$ ganze Zahlen bezeichnen. Ist $m < n$, so erhellt, indem man nach und nach die Coëfficienten von $x_n, x_{n-1}, \ldots x_{m+1}$ in Betracht zieht, dass

$$h_1 = h_2 = \ldots h_{m+1} = 0$$

und

$$\omega_m = h_1\varphi_1 + h_2\varphi_2 + \ldots + h_m\varphi_m$$

sein muss. Da überdies die Coëfficienten von x_m in ω_m und φ_m zusammenfallen müssen, so ergibt sich $h_m = 1$ und man hat

$$\omega_m = h_1\varphi_1 + h_2\varphi_2 + \ldots + \varphi_m.$$

Ist $m = 1$, so ist $\omega_1 = \varphi_1$ vollständig bestimmt.

Ist aber $m > 1$ und setzt man

$$\varphi_i = b_{i1}x_1 + b_{i2}x_2 + \ldots + b_{ii}x_i,$$

so soll der Coëfficient

$$h_{m-1}b_{m-1\,m-1} + b_{mm-1}$$

von x_{m-1} in ω_m nicht negativ und kleiner als der Zahlenwerth von $b_{m-1\,m-1}$ sein. Derselbe muss daher der echte Rest von b_{mm-1} in Bezug auf den Modul $b_{m-1\,m-1}$ sein, wodurch h_{m-1} vollständig bestimmt ist. Ist $m > 2$, so ergibt sich in derselben Weise, dass der Coëfficient von x_{m-2} in ω_m der echte Rest von $h_{m-1}b_{m-1\,m-2} + b_{mm-2}$ in Bezug auf den Modul $b_{m-2\,m-2}$ sein

muss. Da aber h_{m-1} bereits bestimmt ist, so erhellt, dass auch sowohl der in Rede stehende Coëfficient, als auch h_{m-2} vollständig bestimmt sind. Schliesst man so fort, so ergibt sich, dass $h_1, h_2, \ldots h_{m-1}$ sich immer und nur auf eine Weise so bestimmen lassen, dass ω_m die Eigenschaft II besitzt, und dies gilt für jeden der Werthe $2, 3, \ldots n$ von m.

Überdies ist klar, dass die so bestimmten Formen $\omega_1, \omega_2, \ldots \omega_n$ mit $\varphi_1, \varphi_2, \ldots \varphi_n$ gleichstimmig sind. Denn φ_1 ist ein Vielfaches von ω_1, φ_2 eine Vielfachsumme von ω_2 und φ_1, also auch von ω_2 und ω_1, φ_3 eine Vielfachsumme von ω_3, φ_1, φ_2, also auch von ω_3, ω_2, ω_1 u. s. f.

Das System

$$\omega_1, \omega_2, \ldots \omega_n$$

soll ein reducirtes Formensystem des Systems S genannt werden.

Setzt man

$$\omega_i = p_{i1} f_1 + p_{i2} f_2 + \ldots + p_{im} f_m$$
$$f_i = q_{1i} \omega_1 + q_{2i} \omega_2 + \ldots + q_{ni} \omega_n,$$

so ergibt sich durch Einsetzung der Ausdrücke für $f_1, f_2, \ldots f_m$ in die Gleichung für ω_i

$$\omega_i = (p_{i1} q_{11} + p_{i2} q_{12} + \ldots + p_{im} q_{1m}) \omega_1$$
$$+ (p_{i1} q_{21} + p_{i2} q_{22} + \ldots + p_{im} q_{2m}) \omega_2$$
$$+ (p_{i1} q_{n1} + p_{i2} q_{n2} + \ldots + p_{im} q_{nm}) \omega_n$$

Wegen der linearen Unabhängigkeit von $\omega_1, \omega_2, \ldots \omega_n$ folgt hieraus

$$p_{i1} q_{i1} + p_{i2} q_{i2} + \ldots + p_{im} q_{im} = 1$$

und

$$p_{i1} q_{k1} + p_{i2} q_{k2} + \ldots + p_{im} q_{km} = 0,$$

wenn i und k verschieden sind. Die Zahlen

$$p_{i1}, p_{i2}, \ldots p_{im}$$

ebenso wie die Zahlen

$$q_{i1}, q_{i2}, \ldots q_{im}$$

haben sonach den grössten gemeinschaftlichen Theiler 1.

3.

Es seien

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

zwei binäre quadratische Formen von gleicher Determinante D, deren Theiler m, m' relativ prim vorausgesetzt werden, und es werde zur Abkürzung

$$ax+(b+\sqrt{D})y = f_0$$
$$a'x'+(b'+\sqrt{D})y' = f_0'$$

gesetzt; es soll das Product $f_0 f_0'$ nach den Unbestimmten x, y, x', y' entwickelt und für die Coëfficienten dieser Entwickelung, welche als linear-homogene Functionen von 1 und $\sqrt{D}$ aufzufassen sind, dasjenige reducirte System

$$c_{11}, \qquad c_{21}+c_{22}\sqrt{D}$$

ermittelt werden, in welchem c_{22} positiv ist und c_{11} das Vorzeichen von aa' hat.

Man hat

$$f_0 f_0' = aa'xx'+(ab'+a\sqrt{D})xy'+(a'b+a'\sqrt{D})yx'+ \\ +(D+bb'+(b+b')\sqrt{D})yy',$$

und es handelt sich also um die Bestimmung des reducirten Systems der vier linearen Formen

$$aa', \quad ab'+a\sqrt{D}, \quad a'b+a'\sqrt{D}, \quad D+bb'+(b+b')\sqrt{D}$$

von 1, $\sqrt{D}$ mit den oben genannten Vorzeichenbedingungen.

Bezeichnet ν den grössten gemeinschaftlichen Theiler der Zahlen

$$a, \quad a', \quad b+b',$$

so ergibt sich zunächst $c_{22} = \nu$.

Um c_{11} zu ermitteln, sind die Determinanten zweiter Ordnung des Elementensystems

$$\begin{matrix} aa', & ab', & ba', & D+bb' \\ 0, & a, & a', & b+b' \end{matrix}$$

zu bilden. Dieselben sind:

$$aa'.a, \quad aa'.a', \quad aa'.(b+b'), \quad aa'.(b'-b), \quad aa'.c', \quad aa'.c.$$

Ihr grösster gemeinschaftlicher Theiler ist, wenn vom Vorzeichen abgesehen wird, das Product von aa' in den grössten gemeinschaftlichen Theiler t der sechs Zahlen

$$a, \quad a', \quad b'+b, \quad b'-b, \quad c, \quad c'$$

Da der grösste gemeinschaftliche Theiler m der Zahlen $a, 2b, c$ zu dem grössten gemeinschaftlichen Theiler m' der Zahlen $a', 2b', c'$ relativ prim ist, so haben die Zahlen

$$a, \quad 2b, \quad c, \quad a', \quad 2b', \quad c'$$

den grössten gemeinschaftlichen Theiler 1 und es besteht eine Gleichung

$$a\mathfrak{A}+2b\mathfrak{B}+c\mathfrak{C}+a'\mathfrak{A}'+2b'\mathfrak{B}'+c'\mathfrak{C}'=1,$$

worin $\mathfrak{A}, \mathfrak{B}, \ldots \mathfrak{C}'$ ganze Zahlen sind. Dann besteht aber auch die Gleichung

$$a\mathfrak{A}+a'\mathfrak{A}'+(b'+b)(\mathfrak{B}'+\mathfrak{B})+(b'-b)(\mathfrak{B}'-\mathfrak{B})+c\mathfrak{C}+c'\mathfrak{C}'=1,$$

aus welcher erhellt, dass $t=1$ ist. Der grösste gemeinschaftliche Theiler der sechs obigen Determinanten ist sonach, vom Vorzeichen abgesehen, $= aa'$ und man hat

$$c_{11}c_{22}=aa',$$

also

$$c_{11}=\frac{aa'}{\nu}.$$

Um c_{21} zu ermitteln, hat man eine beliebige Lösung der Gleichung

$$a\alpha+a'\beta+(b+b')\gamma=\nu$$

zu bestimmen, mit Hilfe derselben den Ausdruck

$$\varphi_2=\alpha(ab'+a\sqrt{D})+\beta(ba'+a'\sqrt{D})+\gamma(D+bb'+(b+b')\sqrt{D})$$

zu bilden und hierauf in der Gleichung

$$c_{21}+c_{22}\sqrt{D}=\varphi_2+lc_{11}$$

den Coëfficienten l so zu bestimmen, dass c_{21} nicht negativ und kleiner als der Zahlenwerth von c_{11} ausfällt. c_{21} ist somit der echte Rest der Zahl

$$ab'\alpha+ba'\beta+(D+bb')\gamma$$

in Bezug auf den Modul $\frac{aa'}{\nu}$.

Da ν sowohl in $\frac{aa'}{\nu}$ als auch in ab', ba' und

$$D+bb'=b(b+b')-ac$$

aufgeht, so ist c_{21} durch ν theilbar und das gesuchte reducirte System hat die Gestalt

$$\nu A, \qquad \nu(B+\sqrt{D}),$$

wenn

$$\frac{c_{11}}{c_{22}}=A \qquad \frac{c_{21}}{c_{22}}=B$$

gesetzt wird.

Setzt man

$$\begin{aligned} aa' &= p_1\nu A+q_1\nu(B+\sqrt{D}) \\ ab'+a\sqrt{D} &= p_2\nu A+q_2\nu(B+\sqrt{D}) \\ ba'+a'\sqrt{D} &= p_3\nu A+q_3\nu(B+\sqrt{D}) \\ D+bb'+(b+b')\sqrt{D} &= p_4\nu A+q_4\nu(B+\sqrt{D}) \end{aligned}$$

$$\begin{aligned} p_1xx'+p_2xy'+p_3yx'+p_4yy' &= \mathfrak{X} \\ q_1xx'+q_2xy'+q_3yx'+q_4yy' &= \mathfrak{Y}, \end{aligned}$$

so wird identisch

$$f_0f_0'=\nu(A\mathfrak{X}+(B+\sqrt{D})\mathfrak{Y}).$$

Durch Verwandlung von $\sqrt{D}$ in $-\sqrt{D}$ folgt hieraus die zweite Identität

$$(ax+(b-\sqrt{D})y)(a'x'+(b'-\sqrt{D})y')=\nu(A\mathfrak{X}+(B-\sqrt{D})\mathfrak{Y})$$

und man erhält durch Multiplication derselben mit der vorhergehenden

$$aa'ff'=\nu^2(A^2\mathfrak{X}^2+2AB\mathfrak{X}\mathfrak{Y}+(B^2-D)\mathfrak{Y}^2)$$

oder

$$A^2\mathfrak{X}^2+2AB\mathfrak{X}\mathfrak{Y}+(B^2-D)\mathfrak{Y}^2 = Aff'$$

Da auf Grund dieser Gleichung $(B^2-D)\mathfrak{Y}^2$ durch A theilbar und $\mathfrak{Y}$ eine ganze ganzzahlige primitive Function von x, y, x', y' ist, so muss B^2-D durch A theilbar sein und man hat

$$B^2-D = AC$$

$$A\mathfrak{X}^2+2B\mathfrak{X}\mathfrak{Y}+C\mathfrak{Y}^2 = ff', \qquad (1)$$

wo C eine ganze Zahl bezeichnet.

Da νA, $\nu(B+\sqrt{D})$ Vielfachsummen der vier Coëfficienten von $f_0 f_0'$ sind und in den diesbezüglichen Gleichungen $\sqrt{D}$ durch irgend eine Zahl ersetzt werden darf, so erscheinen, wenn man $\sqrt{D}$ durch b ersetzt, νA und $\nu(B+b)$ als Vielfachsummen der Zahlen

$$aa', \quad a(b+b'), \quad 2ba', \quad 2b(b+b')-ac$$

und somit als Vielfache von νm; es sind also A und $2(B+b)$ und sonach auch $2B$ durch m theilbar. Ebenso erscheinen νA und $\nu(B+b')$, wenn $\sqrt{D}$ durch b' ersetzt wird, als Vielfachsummen von

$$aa', \quad 2b'a, \quad a'(b+b'), \quad 2b'(b+b')-a'c'$$

also als Vielfache von $\nu m'$ und A, $2(B+b')$, also auch $2B$ müssen durch m' theilbar sein. Dann sind aber A, $2B$ durch mm' theilbar und die Identität (1) zeigt, dass mm' auch in C aufgeht. Anderseits zeigt dieselbe Identität, dass das Product von mm' in die primitive Function $\frac{f}{m}\ \frac{f'}{m'}$ Vielfachsummen von A, $2B$, C zu Coëfficienten hat, und es ist somit auch mm' eine Vielfachsumme von A, $2B$, C. Dann ist aber mm' der grösste gemeinschaftliche Theiler der Zahlen A, $2B$, C.

Setzt man

$$AX^2+2BXY+CY^2 = F,$$

so wird die Form F aus den Formen f, f' zusammengesetzt genannt. Sie hat dieselbe Determinante wie f, f', den Theiler mm', ist vollständig bestimmt, von der Reihenfolge, in welcher

die Formen f, f' genommen werden, unabhängig und genügt der Identität

$$F(\mathfrak{X}, \mathfrak{Y}) = f \cdot f'$$

Um die Form F zu bilden, hat man zunächst den grössten gemeinschaftlichen Theiler ν der Zahlen $a, a', b+b'$ und eine Lösung der Gleichung

$$a\alpha + a'\beta + (b+b')\gamma = \nu$$

zu ermitteln; es wird dann $A = \frac{aa'}{\nu^2}$, B der echte Rest der Zahl

$$\frac{ab'}{\nu}\alpha + \frac{ba'}{\nu}\beta + \frac{D+bb'}{\nu}\gamma$$

in Bezug auf den Modul A und C ergibt sich aus der Gleichung

$$C = \frac{B^2 - D}{A}.$$

Die aus zwei Formen f, f' zusammengesetzte Form soll mit $\overline{ff'}$ bezeichnet werden.

Sagt man von einer Form, deren Theiler n ist, dass sie zur Ordnung n gehört, so gehört die Form F zur Ordnung mm' Ist eine der Formen f, f', etwa f, primitiv, so gehören f' und F derselben Ordnung an.

Ist irgend eine Anzahl μ von Formen

$$\begin{aligned} f &= ax^2 + 2bxy + cy^2 \\ f' &= a'x_1^2 + 2b'x_1y_1 + c'y_1^2 \\ f'' &= a''x_2^2 + 2b''x_2y_2 + c''y_2^2 \end{aligned}$$

$$f^{(\mu-1)} = a^{(\mu-1)}x_{\mu-1}^2 + 2b^{(\mu-1)}x_{\mu-1}y_{\mu-1} + c^{(\mu-1)}y_{\mu-1}^2$$

der Determinante D gegeben, deren Theiler $m, m', m'', \ldots m^{(\mu-1)}$ paarweise relativ prim sind, so kann man zunächst irgend zwei Formen f, f' in eine Form

$$F' = A'X_1^2 + 2B'X_1Y_1 + C'Y_1^2,$$

hierauf diese Form F' und irgend eine dritte Form f'', deren Theiler mm' und m'' ebenfalls relativ prim sind, in eine Form

$$F'' = A''X_2^2 + 2B''X_2Y_2 + C''Y_2^2$$

zusammensetzen und so fortfahren, bis man zuletzt die Form

$$F^{(\mu-2)} = A^{(\mu-2)}X_{\mu-2}^2 + 2B^{(\mu-2)}X_{\mu-2}Y_{\mu-2} + C^{(\mu-2)}Y_{\mu-2}^2$$

und die letzte Form $f^{(\mu-1)}$ in eine Form

$$F^{(\mu-1)} = A^{(\mu-1)}X_{\mu-1}^2 + 2B^{(\mu-1)}X_{\mu-1}Y_{\mu-1} + C^{(\mu-1)}Y_{\mu-1}^2$$

zusammensetzt. Die Form $F^{(\mu-1)}$ heisst dann aus den Formen $f, f', f'', \ldots f^{(\mu-1)}$ zusammengesetzt, hat die Determinante D, den Theiler $mm'm'' \ldots m^{(\mu-1)}$ und ist von der Reihenfolge unabhängig, in welcher die Formen $f, f', \ldots f^{(\mu-1)}$ genommen werden. Dieselbe soll mit $\overline{ff' \ldots f^{(\mu-1)}}$ bezeichnet werden.

Es sei zur Abkürzung

$$f_0^{(i)} = a^{(i)}x_i + (b^{(i)} + \sqrt{D})y_i$$
$$F_0^{(i)} = A^{(i)}X_i + (B^{(i)} + \sqrt{D})Y_i$$
$$P = f_0 f_0' f_0'' \ldots f_0^{(\mu-1)}$$

und ν_1 der grösste gemeinschaftliche Theiler der Zahlen a, a', $b+b'$, ν_i derjenige der Zahlen $A^{(i-1)}$, $a^{(i)}$, $B^{(i-1)}+b^{(i)}$. Die Coëfficienten von $f_0 f_0'$ sind mit $\nu_1 A'$, $\nu_1(B' + \sqrt{D})$ oder den Coëfficienten von $\nu_1 F_0'$ gleichstimmig. Daher sind auch die Coëfficienten von $f_0 f_0' f_0''$ und $\nu_1 F_0' f_0''$ gleichstimmig; da aber die Coëfficienten von $F_0' f_0''$ und $\nu_2 F_0''$ gleichstimmig sind, so sind es auch die von $\nu_1 F_0' f_0''$ und $\nu_1\nu_2 F_0''$ und somit auch die von $f_0 f_0' f_0''$ und $\nu_1\nu_2 F_0''$. In derselben Weise ergibt sich, wenn $\mu > 3$ ist, die Gleichstimmigkeit der Coëfficienten von $f_0 f_0' f_0'' f_0'''$ und $\nu_1\nu_2\nu_3 F_0'''$ u. s. f. Es sind also auch die Coëfficienten von P mit denen von $\nu_1\nu_2 \ldots \nu_{\mu-1} F_0^{(\mu-1)}$ gleichstimmig. Hieraus folgt, dass die linearen Formen von 1, $\sqrt{D}$

$$\nu_1\nu_2 \ldots \nu_{\mu-1} A^{(\mu-1)}, \qquad \nu_1\nu_2 \ldots \nu_{\mu-1}(B^{(\mu-1)} + \sqrt{D})$$

ein mit den Coëfficienten von P gleichstimmiges reducirtes System, und zwar dasjenige reducirte System

$$c_{11}, \qquad c_{21} + c_{22}\sqrt{D}$$

bilden, in welchem c_{22} positiv ist und c_{11} das Vorzeichen von $aa' \ldots a^{(\mu-1)}$ hat, da

$$A^{(\mu-1)} = \frac{aa' \ldots a^{(\mu-1)}}{\nu_1^2\nu_2^2 \ldots \nu_{\mu-1}^2}$$

ist. Da dieses System nur von den Coëfficienten von P abhängt, also von der Reihenfolge der Formen $f, f', \ldots f^{(\mu-1)}$ unabhängig und

$$A^{(\mu-1)} = \frac{c_{11}}{c_{22}} \qquad B^{(\mu-1)} = \frac{c_{21}}{c_{22}}$$

ist, so ist auch die Form $F^{(\mu-1)}$ von dieser Reihenfolge unabhängig.

Um $F^{(\mu-1)}$ zu erhalten, kann man auch folgendermassen verfahren. Man theile die gegebenen Formen

$$f, f' \qquad f^{(\mu-1)}$$

irgendwie in zwei Gruppen, und es sei φ die Form, welche aus den Formen der einen Gruppe zusammengesetzt ist, oder auch die Form dieser Gruppe selbst, wenn letztere nur eine einzige Form enthält, und ψ die Form, welche in Bezug auf die Formen der anderen Gruppe eine ähnliche Bedeutung hat; es ist dann

$$F^{(\mu-1)} = \overline{\varphi\psi}.$$

Setzt man nämlich

$$\begin{aligned}
\varphi &= px^2+2qxy+ry^2 \\
\psi &= p'x_1^2+2q'x_1y_1+r'y_1^2 \\
\chi &= \overline{\varphi\psi} = p_1X^2+2q_1XY+r_1Y^2 \\
\varphi_0 &= px+(q+\sqrt{D})y \\
\psi_0 &= p'x_1+(q'+\sqrt{D})y_1 \\
\chi_0 &= p_1X+(q_1+\sqrt{D})Y
\end{aligned}$$

und bezeichnet mit Q_1, Q_2 die Producte der Ausdrücke $f_0, f_0', \ldots$ oder auch eintretendenfalls solche Ausdrücke selbst, welche den Formen der beiden Gruppen entsprechen, so sind die Coëfficienten von Q_1 mit denen von $k\varphi_0$, die von Q_2 mit denen von $k'\psi_0$, also die Coëfficienten von $P = Q_1Q_2$ mit denen von $kk'\varphi_0\psi_0$ und daher auch denen von $kk'k_1\chi_0$ gleichstimmig, wo k, k', k_1 ganze Zahlen bezeichnen. Es ist also

$$p_1 = \frac{c_{11}}{c_{22}} = A^{(\mu-1)} \qquad q_1 = \frac{c_{21}}{c_{22}} = B^{(\mu-1)}.$$

4.

Um irgend eine Form

$$f = (a, b, c)$$

mit der Hauptform

$$g = (1, 0, -D)$$

zusammenzusetzen, hat man

$$\nu = 1 \qquad A = a$$

und kann als Lösung der Gleichung

$$a\alpha + \beta + b\gamma = 1$$

die Zahlen $\alpha = 0$, $\beta = 1$, $\gamma = 0$ nehmen. B wird dann der echte Rest b_0 von b in Bezug auf den Modul a. Es ist daher

$$\overline{fg} = \left(a, b_0, \frac{b_0^2 - D}{a}\right).$$

Nennt man insbesondere eine Form (a, b, c) kurz »schlicht«, wenn b nicht negativ ist und den Zahlenwerth von a nicht erreicht, so ist die aus einer schlichten Form f und der Hauptform zusammengesetzte Form die Form f selbst.

Wenn f primitiv und f' die entgegengesetzte Form $(a, -b, a)$ von f ist, so hat man

$$\nu = \pm a \qquad A = 1$$

und B hat als echter Rest in Bezug auf den Modul 1 den Werth 0. Daher ist

$$\overline{ff'} = (1, 0, -D).$$

Wenn f eine primitive Form und die Formen g, g' verschieden und schlicht sind, so sind auch die Formen $\overline{fg}$, $\overline{fg'}$ verschieden.

5.

Wenn die Formen f, f' theilerfremde Theiler haben und die Form g mit f, die Form g' mit f' äquivalent ist, so ist $\overline{gg'}$ mit $\overline{ff'}$ äquivalent.

Es gehe f in g durch die Substitution $(\alpha, \beta, \gamma, \delta)$, f' in g' durch die Substitution $(\alpha', \beta', \gamma', \delta')$ über und man setze

$$\begin{aligned}
f &= ax^2+2bxy+cy^2\\
f' &= a'x_1^2+2b'x_1y_1+c'y_1^2\\
g &= px^2+2qxy+ry^2\\
g' &= p'x_1^2+2q'x_1y_1+r'y_1^2\\
\overline{ff'} &= F = AX^2+2BXY+CY^2\\
\overline{gg'} &= G = A'X_1^2+2B'X_1Y_1+C'Y_1^2\\
f_0 &= ax+(b+\sqrt{D})y\\
f_0' &= a'x_1+(b'+\sqrt{D})y_1\\
g_0 &= px+(q+\sqrt{D})y\\
g_0' &= p'x_1+(q'+\sqrt{D})y_1\\
F_0 &= AX+(B+\sqrt{D})Y\\
G_0 &= A'X_1+(B'+\sqrt{D})Y_1\\
a\alpha+(b-&\sqrt{D})\gamma = k\\
a'\alpha'+(b'-&\sqrt{D})\gamma' = k'.
\end{aligned}$$

Man hat

$$\begin{aligned}
f_0f_0' &= \nu F_0(\mathfrak{X}, \mathfrak{Y})\\
g_0g_0' &= \nu' G_0(\mathfrak{U}, \mathfrak{V})
\end{aligned}$$

wo ν den grössten gemeinschaftlichen Theiler von a, a', $b+b'$, ν' den von p, p', $q+q'$ und $\mathfrak{X}$, $\mathfrak{Y}$, $\mathfrak{U}$, $\mathfrak{V}$ ganze ganzzahlige Functionen von x, y, x', y' bezeichnen. Gehen $\mathfrak{X}$, $\mathfrak{Y}$ nach Ersetzung von x, y, x', y' durch

$$\alpha x+\beta y, \quad \gamma x+\delta y, \quad \alpha' x_1+\beta' y_1, \quad \gamma' x_1+\delta' y_1$$

in $\mathfrak{X}', \mathfrak{Y}'$ über, so wird identisch

$$\nu F_0(\mathfrak{X}', \mathfrak{Y}') = f_0(\alpha x+\beta y, \gamma x+\delta y) f_0'(\alpha' x_1+\beta' y_1, \gamma' x_1+\delta' y_1).$$

Multiplicirt man mit kk' und beachtet, dass

$$\begin{aligned}
kf_0(\alpha x+\beta y, \gamma x+\delta y) &= ag_0\\
k'f_0'(\alpha' x_1+\beta' y_1, \gamma' x_1+\delta' y_1) &= a'g_0'
\end{aligned}$$

ist, so ergibt sich

$$\nu kk' F_0(\mathfrak{X}', \mathfrak{Y}') = aa' g_0 g_0'.$$

Hienach sind die Coëfficienten von $\nu kk' F_0(\mathfrak{X}', \mathfrak{Y}')$ mit denen von $aa' g_0 g_0'$ und daher auch denen von $aa'\nu'G_0$ gleichstimmig. Man hat also

$$aa'\nu' A' = \nu kk' F_0(\mathfrak{a}, \mathfrak{c})$$
$$aa'\nu'(B' + \sqrt{D}) = \nu kk' F_0(\mathfrak{b}, \mathfrak{d}),$$

wo $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}$ ganze Zahlen bezeichnen.

Aus diesen Gleichungen folgt, wenn man die erste mit der conjugirten Gleichung

$$aa'\nu' A' = \nu f_0(\alpha, \gamma) f_0'(\alpha', \gamma')(A\mathfrak{a} + (B - \sqrt{D})\mathfrak{c})$$

multiplicirt,

$$a^2 a'^2 \nu'^2 A'^2 = \nu^2 . af(\alpha, \gamma) . a' f'(\alpha', \gamma') . AF(\mathfrak{a}, \mathfrak{c})$$

oder den Gleichungen

$$A = \frac{aa'}{\nu^2} \qquad A' = \frac{pp'}{\nu'^2}$$

$$f(\alpha, \gamma) = p \qquad f'(\alpha', \gamma') = p'$$

zufolge

$$A' = F(\mathfrak{a}, \mathfrak{c}).$$

Ferner ergibt sich durch Division der obigen Gleichungen

$$\frac{B' + \sqrt{D}}{A'} = \frac{F_0(\mathfrak{b}, \mathfrak{d})}{F_0(\mathfrak{a}, \mathfrak{c})}$$
$$= \frac{A\mathfrak{a}\mathfrak{b} + B(\mathfrak{a}\mathfrak{d} + \mathfrak{b}\mathfrak{c}) + C\mathfrak{c}\mathfrak{d} + (\mathfrak{a}\mathfrak{d} - \mathfrak{b}\mathfrak{c})\sqrt{D}}{F(\mathfrak{a}, \mathfrak{c})}$$

und der bereits gefundenen Gleichung $A' = F(\mathfrak{a}, \mathfrak{c})$ zufolge

$$B' = A\mathfrak{a}\mathfrak{b} + B(\mathfrak{a}\mathfrak{d} + \mathfrak{b}\mathfrak{c}) + C\mathfrak{c}\mathfrak{d}$$
$$\mathfrak{a}\mathfrak{d} - \mathfrak{b}\mathfrak{c} = 1.$$

Wenn zwei unäquivalente Formen φ, ψ mit einer primitiven Form f zusammengesetzt werden, so sind die resultirenden Formen $\overline{f\varphi}$, $\overline{f\psi}$ ebenfalls unäquivalent. Im Gegenfalle müssten nämlich die Formen $\overline{f'f\varphi}$ und $\overline{f'f\psi}$ äquivalent sein, wo f' die entgegengesetzte Form von f bezeichnet; da aber $\overline{ff'} = (1, 0, -D)$ ist, so müssten auch φ und ψ äquivalent sein.

Unter der Formenclasse, welche aus zwei Classen K, L zusammengesetzt ist, versteht man diejenige Classe, zu welcher die aus zwei den Classen K und L entnommenen Formen f, g zusammengesetzte Form gehört.

6.

Wenn eine Zahl m durch die Form f so dargestellt wird, dass die darstellenden Zahlen ξ, η den grössten gemeinschaftlichen Theiler μ haben, so ist die Form f einer Form $\left(\frac{m}{\mu^2}, r, l\right)$ äquivalent, in welcher r nicht negativ und kleiner als der Zahlenwerth von $\frac{m}{\mu^2}$ ist, und $\frac{\xi}{\mu}, \frac{\eta}{\mu}$ bilden den ersten und dritten Coëfficienten einer und nur einer Substitution $\left(\frac{\xi}{\mu}, \beta, \frac{\eta}{\mu}, \delta\right)$ von der Determinante 1, welche f in $\left(\frac{m}{\mu^2}, r, l\right)$ verwandelt. Nennt man eine schlichte Form $\left(\frac{m}{\mu^2}, r, l\right)$ der Determinante D kurz eine Hilfsform der Zahl m und sagt, dass die Darstellung (ξ, η) aus der Hilfsform $\left(\frac{m}{\mu^2}, r, l\right)$ und der Substitution $\left(\frac{\xi}{\mu}, \beta, \frac{\eta}{\mu}, \delta\right)$ hervorgehe, so gehen demnach alle Darstellungen der Zahl m durch f aus den mit f äquivalenten Hilfsformen und den einzelnen Substitutionen hervor, welche f in diese Hilfsform verwandeln.

Wenn f primitiv und D negativ ist, so gehen aus jeder mit f äquivalenten Hilfsform so viele Darstellungen hervor, als die Pell'sche Gleichung

$$t^2 - Du^2 = 1$$

Lösungen besitzt.

Wenn dagegen D positiv ist, so gehen aus jeder mit f äquivalenten Hilfsform unendlich viele Darstellungen hervor. Setzt man $f = (a, b, c)$ und bezeichnet irgend eine besondere aus einer dieser Hilfsformen hervorgehende Darstellung von m durch f mit (ξ_0, η_0) und mit T, U die kleinste positive Lösung der Pell'schen Gleichung

$$t^2 - Du^2 = 1,$$

so sind alle aus der nämlichen Hilfsform hervorgehenden Darstellungen von m mittelst der Form f durch die Gleichung

$$a\xi+(b+\sqrt{D})\eta = \pm(a\xi_0+(b+\sqrt{D})\eta_0)(T+U\sqrt{D})^e$$

gegeben, wo e alle ganzen Zahlen zu durchlaufen hat. Unter allen diesen aus einer Hilfsform hervorgehenden unendlich vielen Darstellungen gibt es aber nur eine einzige, welche den Bedingungen

$$1 < \frac{a\xi+(b+\sqrt{D})\eta}{\sqrt{\pm am}} \leqq T+U\sqrt{D}$$

genügt.

7.

Durch jede gegebene primitive Form

$$\varphi = Ax^2+Bxy+Cy^2,$$

in welcher B auch ungerade sein kann, lassen sich Zahlen darstellen, welche zu einer gegebenen Zahl M theilerfremd sind. Nimmt man den einzigen Fall aus, wo A, B ungerade und C, M gerade sind, so darf man sogar für y eine beliebige, zu M theilerfremde Zahl setzen, und es lässt sich x noch immer so wählen, dass $\varphi(x, y)$ theilerfremd zu M ausfällt.

Es sei η eine beliebig gewählte, zu M theilerfremde Zahl.

Wenn $M = 1$ ist, so bedarf es keines Beweises, da $\varphi(\xi, \eta)$ für jedes ξ zu M theilerfremd ist.

Ist $M > 1$, so können die Zahlen

$$A+B\eta, \quad 2B\eta, \quad C\eta^2, \quad M$$

keinen Theiler gemein haben. Denn ein solcher Theiler müsste zu η relativ prim sein, also in $C, 2B, A+B\eta$ aufgehen; da er aber wegen der Primitivität von φ zu B theilerfremd sein muss, so könnte er nur $= 2$ sein, und es wären gegen die Annahme M, C gerade, A, B ungerade.

Es gibt also ganze Zahlen $\alpha, \beta, \gamma, \delta$, welche der Gleichung

$$(A+B\eta)\alpha+2B\beta+C\eta^2\gamma+M\delta = 1$$

genügen. Ersetzt man in derselben $A+B\eta, 2B\eta, C\eta^2$ durch

$$\varphi(1, \eta)-\varphi(0, \eta), \quad -3\varphi(0, \eta)+4\varphi(1, \eta)-\varphi(2, \eta), \quad \varphi(0, \eta),$$

so ergibt sich eine Gleichung

$$\alpha'\varphi(0,\eta)+\beta'\varphi(1,\eta)+\gamma'\varphi(2,\eta)+M\delta=1,$$

in welcher α', β', γ', δ ganze Zahlen bezeichnen. Für jeden Primfactor p von M kann man daher eine Zahl ξ angeben, für welche $\varphi(\xi,\eta)$ nicht durch p theilbar ist, da nicht alle drei Resultate $\varphi(0,\eta)$, $\varphi(1,\eta)$, $\varphi(2,\eta)$ durch p theilbar sein können.

Ist nun M eine Primzahlpotenz, so ist der Beweis erbracht.

Enthält M dagegen mehrere verschiedene Primfactoren $p_1, p_2,\ldots$ so ermittle man Zahlen $\xi_1, \xi_2\ldots$ von der Art, dass $\varphi(\xi_1,\eta)$ zu p_1, $\varphi(\xi_2,\eta)$ zu p_2 u. s. w. theilerfremd ausfallen, und eine Zahl ξ, welche den Zahlen $\xi_1, \xi_2,\ldots$ beziehungsweise nach den Moduln $p_1, p_2,\ldots$ congruent ist. Dann ist $\varphi(\xi,\eta)$ der Congruenz

$$\varphi(\xi,\eta)\equiv\varphi(\xi_i,\eta)\qquad(\mathrm{mod}\ p_i)$$

zufolge durch keinen einzigen Primfactor von M theilbar, also zu M theilerfremd.

In dem Ausnahmefalle, wo A, B ungerade, C, M gerade sind, braucht man nur x, y mit einander zu vertauschen.

8.

Aufgabe. Es ist eine schlichte Form F der Ordnung n gegeben; es sollen alle schlichten primitiven Formen ermittelt werden, welche, mit der einfachsten Form ω der Ordnung n zusammengesetzt, F hervorbringen.

Es sei

$$F=n\left(ax^2+\frac{2}{\sigma}bxy+cy^2\right)$$

$$\omega=\left(n,\frac{n(\sigma-1)}{\sigma},\frac{n^2(\sigma-1)^2-D\sigma^2}{n\sigma^2}\right),$$

wo $\sigma=1$ oder $=2$ und b für $\sigma=2$ ungerade ist. Ist

$$f=(A,B,C)$$

irgend eine Lösung der Forderung

$$f\overline{\omega}=F,$$

ν der grösste gemeinschaftliche Theiler der Zahlen A, n, $B + \frac{n(\sigma-1)}{\sigma}$ und $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ eine Lösung der Gleichung

$$A\mathfrak{a} + n\mathfrak{b} + \left(B + \frac{n(\sigma-1)}{\sigma}\right)\mathfrak{c} = \nu,$$

so muss

$$an = \frac{An}{\nu^2},$$

also $A = a\nu^2$ und

$$\frac{nb}{\sigma} \equiv \frac{An(\sigma-1)}{\nu\sigma}\mathfrak{a} + \frac{Bn}{\nu}\mathfrak{b} + \left(\frac{D}{\nu} + \frac{Bn(\sigma-1)}{\nu\sigma}\right)\mathfrak{c} \pmod{an}$$

sein. Zieht man von dieser Congruenz die mit $\frac{B}{\nu}$ multiplicirte Gleichung zwischen $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ ab, so ergibt sich

$$\frac{nb}{\sigma} - B \equiv \left(\frac{n(\sigma-1)}{\sigma} - B\right)\mathfrak{a}\cdot\frac{A}{\nu} - C\mathfrak{c}\cdot\frac{A}{\nu} \pmod{an}$$

$$\equiv 0 \pmod{a\nu}$$

und es ist demnach

$$B = \frac{nb}{\sigma} + sa\nu$$

$$C = \frac{B^2-D}{A} = as^2 + \frac{2}{\sigma}bs\frac{n}{\nu} + c\frac{n^2}{\nu^2},$$

wo s eine ganze Zahl bezeichnet.

Hienach muss jede der gesuchten Lösungen die Gestalt

$$f = \left(a\nu^2,\ \frac{nb}{\sigma} + sa\nu,\ as^2 + \frac{2}{\sigma}bs\frac{n}{\nu} + c\frac{n^2}{\nu^2}\right)$$

haben, wo ν irgend einen Theiler von n bezeichnet.

Umgekehrt genügt jede Form, welche diese Gestalt hat und überdies primitiv und schlicht ist, der Aufgabe. Sind nämlich die Coëfficienten

$$a\nu^2, \qquad 2\left(\frac{nb}{\sigma} + sa\nu\right), \qquad as^2 + \frac{2b}{\sigma}s\frac{n}{\nu} + c\frac{n^2}{\nu^2}$$

mit 1 gleichstimmig, so sind es auch die Zahlen

$$a\nu, \qquad \frac{n}{\nu}, \qquad as$$

und daher auch

$$a\nu, \qquad \frac{n}{\nu}, \qquad as + \frac{n}{\nu} \cdot \frac{b+\sigma-1}{\sigma}.$$

ν ist daher der grösste gemeinschaftliche Theiler der Zahlen

$$a\nu^2, \qquad n, \qquad \frac{n(b+\sigma-1)}{\sigma} + sa\nu.$$

Bezeichnet demnach $(\mathfrak{A}, \mathfrak{B}, \mathfrak{C})$ die Form $\overline{f\omega}$ und α, β, γ eine Lösung der Gleichung

$$a\nu^2\alpha + n\beta + \left(sa\nu + \frac{n(b+\sigma-1)}{\sigma}\right)\gamma = \nu,$$

so hat man

$$\mathfrak{A} = \frac{a\nu^2 . n}{\nu^2} = an$$

$$\mathfrak{B} \equiv a\nu . \frac{n(\sigma-1)}{\sigma}\alpha + \frac{n}{\nu}\left(\frac{nb}{\sigma} + sa\nu\right)\beta +$$

$$+ \left(\frac{D}{\nu} + \left(\frac{nb}{\nu\sigma} + sa\right)\frac{n}{\sigma}(\sigma-1)\right)\gamma \qquad (\mathrm{mod}\ an).$$

Zieht man aber die mit $\frac{nb}{\nu\sigma}$ multiplicirte Gleichung zwischen α, β, γ ab, so folgt

$$\mathfrak{B} - \frac{nb}{\sigma} \equiv -an\left(\alpha\nu\frac{(b-\sigma+1)}{\sigma} - \beta s + \gamma\left(\frac{b-\sigma+1}{\sigma}s + c\frac{n}{\nu}\right)\right) \qquad (\mathrm{mod}\ an)$$

$$\equiv 0 \qquad (\mathrm{mod}\ an).$$

Es ist also $\mathfrak{B} = \frac{nb}{\sigma}$ und daher auch $\mathfrak{C} = nc$.

Durch passende Wahl von ν und s lässt sich erreichen, dass f primitiv ausfällt. Man zerlege n in zwei Factoren μ und ν von der Art, dass μ theilerfremd zu a ist und ν nur Primfactoren von a enthält. Dann ist μ zu $a\nu^2$ theilerfremd, und es

kann nicht gleichzeitig $a\nu^2$ und c gerade, a und b ungerade sein. Nach 7 gibt es daher Zahlen s von der Art, dass

$$\frac{1}{n} F(s, \mu) = as^2 + 2\frac{b}{\sigma} s\frac{n}{\nu} + c\frac{n^2}{\nu^2}$$

zu $a\nu^2$ theilerfremd, also die Form

$$f_0 = \left(a\nu^2, \frac{nb}{\sigma} + sa\nu, as^2 + \frac{2b}{\sigma} s\frac{n}{\nu} + \frac{cn^2}{\nu^2}\right)$$

primitiv ausfällt. Diese Eigenschaft wird nicht zerstört, wenn man s um ein Vielfaches von ν ändert, und man kann demnach bewirken, dass $\frac{nb}{\sigma} + sa\nu$ nicht negativ und kleiner als der Zahlenwerth von $a\nu^2$ wird.

Mit Hilfe der Form f_0 lässt sich die Aufgabe auf den Fall zurückführen, wo die gegebene Form F mit ω selbst zusammenfällt. Ist nämlich f irgend eine Lösung, f_0' die entgegengesetzte Form von f_0 und setzt man $\overline{f_0' f} = \varphi$, so wird

$$f = \overline{f_0 f_0' f} = \overline{f_0 \varphi}$$
$$\overline{\varphi\omega} = \overline{f_0' f\omega} = \overline{f_0' F} = \overline{f_0' f_0 \omega} = \omega.$$

φ ist also eine primitive, schlichte, der Forderung

$$\overline{\varphi\omega} = \omega$$

genügende Form. Ist umgekehrt φ eine solche Form, so genügt $\overline{f_0\varphi}$ der Forderung

$$\overline{f_0\varphi\omega} = \overline{f_0\omega} = F.$$

Man erhält also alle Lösungen der Aufgabe, wenn man f_0 mit allen Formen φ zusammensetzt.

Ist $F = \omega$, handelt es sich also um die vollständige Auflösung der Forderung

$$\overline{\varphi\omega} = \omega,$$

so haben die Formen φ die Gestalt

$$\varphi = \left(\nu^2, n\frac{\sigma - 1}{\sigma} + \nu s, l\right)$$

und fallen mit allen primitiven Hilfsformen von n^2 für die Determinante D zusammen, deren Inbegriff mit $\mathfrak{H}$ bezeichnet werde.

Ist nämlich (ν^2, r, l) eine solche Hilfsform von n^2 und setzt man

$$r = \frac{n(\sigma-1)}{\sigma} + z,$$

so wird

$$0 = \left(z + \frac{n(\sigma-1)}{\sigma}\right)^2 - l\nu^2 - D$$

$$= z^2 + \frac{2n}{\sigma}(\sigma-1)z + n^2\left(ac - \frac{b^2-(\sigma-1)^2}{\sigma^2}\right),$$

also auch

$$0 = \left(\frac{z}{\nu}\right)^2 + \frac{2}{\sigma}\,\frac{n}{\nu}(\sigma-1)\frac{z}{\nu} + \frac{n^2}{\nu^2}\left(ac - \frac{b^2-(\sigma-1)^2}{\sigma^2}\right).$$

$\frac{z}{\nu}$ ist also als Wurzel einer ganzzahligen Gleichung mit höchstem Coëfficienten 1 eine ganze Zahl und man kann $z = \nu s$, also

$$r = \frac{n(\sigma-1)}{\sigma} + \nu s$$

setzen.

Die Formen φ reproduciren sich durch Zusammensetzung. Sind nämlich φ_1, φ_2 irgend zwei Formen des Inbegriffes $\mathfrak{H}$, so hat man

$$\overline{\varphi_1}\omega = \omega \qquad \overline{\varphi_2}\omega = \omega.$$

Hieraus folgt aber

$$\overline{\varphi_1\varphi_2}\omega = \overline{\varphi_1}\omega = \omega$$

Die Form $\overline{\varphi_1\varphi_2}$ muss demnach ebenfalls zu $\mathfrak{H}$ gehören.

Aber auch diejenigen Formen von $\mathfrak{H}$, welche mit der Hauptform

$$H = (1, 0, -D)$$

äquivalent sind und deren Inbegriff mit J bezeichnet werden soll, besitzen dieselbe Eigenschaft. Sind nämlich φ_1, φ_2 Formen von J, so gehört $\overline{\varphi_1\varphi_2}$ zu $\mathfrak{H}$ und ist mit H äquivalent, da φ_1 und φ_2 mit H, also $\overline{\varphi_1\varphi_2}$ mit $H\overline{H} = H$ äquivalent ist.

Setzt man alle Formen von J mit irgend einer Form ψ von $\mathfrak{H}$ zusammen, so gehören die resultirenden Formen wieder zu $\mathfrak{H}$ und bilden alle diejenigen Formen von $\mathfrak{H}$, welche mit ψ äquivalent sind. Ist nämlich φ irgend eine Form von J, so ist dieselbe mit H und daher $\overline{\varphi\psi}$ mit $\overline{H\psi} = \psi$ äquivalent. Ist umgekehrt ϑ eine mit ψ äquivalente Form von $\mathfrak{H}$ und ψ' die entgegengesetzte Form von ψ, so ist $\overline{\vartheta\psi'}$ mit $\overline{\psi\psi'} = H$ äquivalent. Da überdies $\overline{\vartheta\psi'}$ eine schlichte Form ist und der Forderung

$$\overline{\vartheta\psi'\omega} = \overline{\psi'\vartheta\omega} = \overline{\psi'\omega} = \overline{\psi'\psi\omega} = \omega$$

genügt, so ist sie eine Form φ von J und man hat

$$\overline{\vartheta\psi'} = \varphi \qquad \vartheta = \overline{\psi\psi'\vartheta} = \overline{\varphi\psi}.$$

Wählt man daher unter den Formen von $\mathfrak{H}$ die grösstmögliche Anzahl

$$\varphi_0, \varphi_1, \ldots \varphi_{\rho-1}$$

von Formen aus, welche untereinander unäquivalent sind, so lassen sich alle Formen von $\mathfrak{H}$ in die ρ Inbegriffe

$$J\varphi_0, J\varphi_1, \ldots J\varphi_{\rho-1}$$

vertheilen, wenn man den Inbegriff der aus der Zusammensetzung aller Individuen eines Formencomplexes C mit einer Form f hervorgehenden Formen kurz mit Cf bezeichnet.

Ist nun L der Inbegriff der Formen $\varphi_0, \varphi_1, \ldots \varphi_{\rho-1}$ und

$$\omega_0, \omega_1, \omega_2, \ldots \omega_{k-1}$$

ein vollständiges System von Formen der Ordnung n, wo $\omega_0 = \omega$, so ist nach dem Obigen $\mathfrak{H}f_i$ die Gesammtheit aller primitiven Formen f, welche der Forderung

$$\overline{f\omega} = \omega_i$$

genügen, wenn f_i eine besondere Lösung dieser Forderung bezeichnet. Unter den Formen von $\mathfrak{H}f_i$ sind nur die des Inbegriffs Lf_i untereinander unäquivalent und es bestehen also die k Inbegriffe

$$Lf_0, Lf_1, \ldots Lf_{k-1} \qquad (2)$$

aus lauter untereinander unäquivalenten Formen. Diese Inbegriffe besitzen aber überdies die Eigenschaft, dass jede gegebene primitive Form G der Determinante D einer in denselben vorkommenden Form äquivalent sein muss. Denn die Form $\overline{G\omega}$ gehört zur Ordnung n und ist daher einer Form $\omega_i = \overline{f_i\omega}$ äquivalent. Dann ist aber, wenn die entgegengesetzte Form von f_i mit f_i' bezeichnet und $f_i'G = G_1$ gesetzt wird, die Form $\overline{f_i'G\omega} = \overline{G_1\omega}$ mit $\overline{f_i'f_i\omega} = \omega$ äquivalent und man hat eine Identität

$$\omega(\alpha X+\beta Y, \gamma X+\delta Y) = \overline{G_1\omega},$$

worin α, β, γ, δ ganze Zahlen bezeichnen. Anderseits geht $\overline{G_1\omega}$ durch eine Substitution

$$X = \mathfrak{X} \qquad Y = \mathfrak{Y},$$

in welcher $\mathfrak{X}$, $\mathfrak{Y}$ Vielfachsummen von xx', xy', yx', yy' bedeuten, in das Product $G_1(x, y)\,\omega(x', y')$ über und es wird

$$\omega(\alpha\mathfrak{X}+\beta\mathfrak{Y}, \gamma\mathfrak{X}+\delta\mathfrak{Y}) = G_1(x, y)\,\omega(x', y').$$

Für $x' = 1$, $y' = 0$ folgt hieraus

$$\omega(\mathfrak{a}x+\mathfrak{b}y, \mathfrak{c}x+\mathfrak{d}y) = n\,G_1(x, y),$$

wo $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$ ganze Zahlen sind. Da hienach die Form ω durch die Substitution $(\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d})$ in nG_1 übergeht, so hat man zwischen den Determinanten dieser Formen die Gleichung

$$D(\mathfrak{a}\mathfrak{d}-\mathfrak{b}\mathfrak{c})^2 = Dn^2$$

und überdies für $x = \mathfrak{b}$, $y = -\mathfrak{c}$ die Gleichung

$$n(\mathfrak{a}\mathfrak{d}-\mathfrak{b}\mathfrak{c})^2 = n\,G_1(\mathfrak{d}_1-\mathfrak{c}).$$

Es ist demnach

$$G_1(\mathfrak{d}_1-\mathfrak{c}) = n^2$$

oder n^2 durch G_1 darstellbar und G_1 muss demzufolge einer Hilfsform der Zahl n^2, also auch einer der Formen $\varphi_0, \varphi_1, \ldots \varphi_{\rho-1}$, etwa φ_ε äquivalent sein. Dann ist aber G mit der Form $\overline{\varphi_\varepsilon f_i}$ von $f_i L$ äquivalent.

Die obigen k Complexe (2) bilden sonach ein vollständiges System von primitiven Formen für die Determinante D und man hat

$$h = k\rho,$$

wo h die Anzahl aller primitiven Classen bezeichnet.

Es gilt nun noch die Zahl ρ zu ermitteln. Bezeichnet zu diesem Ende $\Theta(n^2)$ die Anzahl aller Formen von $\mathfrak{H}$ und ρ_1 die Anzahl der Formen von J, so ist

$$\rho = \frac{\Theta(n^2)}{\rho_1}.$$

Um ρ_1 zu ermitteln, sei $D = D_1 \frac{n^2}{\sigma^2}$

Ist D negativ und λ die Anzahl der Lösungen der Pell'schen Gleichung

$$t^2 - Du^2 = 1,$$

so ist $\lambda\rho_1$ die Anzahl aller möglichen Darstellungen (ξ, η) der Zahl n^2 durch die Hauptform H. Denn jede solche Darstellung geht aus einer und nur einer mit H äquivalenten Hilfsform der Zahl n^2 oder einer Form von J und einer der H in diese Form verwandelnden Substitution hervor. Aus der Gleichung

$$\xi^2 - D\eta^2 = \xi^2 - D_1 \frac{n^2\eta_1^2}{\sigma^2} = n^2$$

erhellt aber, dass ξ durch $\frac{n}{\sigma}$ theilbar ist. Setzt man demgemäss

$$\xi = \frac{nt_1}{\sigma} \qquad \eta_1 = u_1,$$

so wird $t_1^2 - D_1 u_1^2 = \sigma^2$, und es ist klar, dass die Anzahl aller Darstellungen von n^2 durch H mit der Anzahl λ_1 der Lösungen der Pell'schen Gleichung

$$t_1^2 - D_1 u_1^2 = \sigma^2$$

zusammenfällt. Man hat also

$$\lambda\rho_1 = \lambda_1 \qquad \rho_1 = \frac{\lambda_1}{\lambda}$$

Ist D positiv und T, U die kleinste positive Lösung der Pell'schen Gleichung

$$T^2 - DU^2 = 1,$$

so ist ρ_1 die Anzahl aller Darstellungen (ξ, η) der Zahl n^2 durch H, welche den Bedingungen

$$1 < \frac{\xi + \eta\sqrt{D}}{n} \leqq T + U\sqrt{D}$$

genügen. Denn jede Darstellung (ξ, η) von n^2 durch H geht aus einer und nur einer mit H äquivalenten Hilfsform von n^2 oder einer Form von J hervor und unter allen aus einer bestimmten Hilfsform hervorgehenden Darstellungen gibt es nur eine, welche den vorstehenden Bedingungen genügt.

Die Anzahl ρ_1 der in Rede stehenden Darstellungen lässt sich aber noch in anderer Weise ausdrücken. Da ξ durch $\frac{n}{\sigma}$ theilbar sein muss, so ergibt sich, wenn

$$\xi = \frac{n}{\sigma} t_1 \qquad \eta = u_1$$

gesetzt wird,

$$t_1^2 - D_1 u_1^2 = \sigma^2$$

$$1 < \frac{t_1 + u_1\sqrt{D}}{\sigma} \leqq T + U\sqrt{D}.$$

ρ_1 ist demnach auch die Anzahl aller Lösungen der Pell'schen Gleichung

$$t_1^2 - D_1 u_1^2 = \sigma^2,$$

welche den vorstehenden Ungleichungen genügen. Bezeichnet aber T_1, U_1 die kleinste positive Lösung dieser Gleichung, so ist

$$T + U\sqrt{D} = \left(\frac{T_1 + U_1\sqrt{D}}{\sigma}\right)^e$$

$$\frac{t_1 + u_1\sqrt{D_1}}{\sigma} = \pm\left(\frac{T_1 + U_1\sqrt{D_1}}{\sigma}\right)^{l'}$$

und die Bedingungen für $\frac{t_1 + u_1\sqrt{D_1}}{\sigma}$ gehen, da nur das obere Vorzeichen gelten kann, in

$$1 < \left(\frac{T_1+U_1\sqrt{D_1}}{\sigma}\right)^p \leqq \left(\frac{T_1+U_1\sqrt{D_1}}{\sigma}\right)^e$$

über und ergeben

$$0 < p \leqq e.$$

p kann also nur die Werthe 1, 2,. .e haben und es ist

$$\rho_1 = e = \frac{l(T+U\sqrt{D})}{l\left(\frac{T_1+U_1\sqrt{D_1}}{\sigma}\right)}.$$

e ist der kleinste Exponent, zu welchem $\frac{T_1+U_1\sqrt{D_1}}{\sigma}$ erhoben werden muss, damit in dem Resultate der Coëfficient von $\sqrt{D_1}$ ganz und durch $\frac{n}{\sigma}$ theilbar ausfalle.

Man hat also für eine negative Determinante

$$k = \frac{h\lambda_1}{\lambda\Theta(n^2)}$$

und für eine positive

$$k = \frac{he}{\Theta(n^2)} = \frac{hl(T+U\sqrt{D})}{\Theta(n^2)l\left(\frac{T_1+U_1\sqrt{D_1}}{\sigma}\right)}.$$

Die Bestimmung der Zahl $\Theta(n^2)$ kommt nur in den Fällen

$$n = \sigma = 2 \qquad D \equiv 1 \pmod 4$$

und

$$n > 1 \qquad \sigma = 1$$

in Betracht.

I. Wenn $n = \sigma = 2$ und $D \equiv 1 \pmod 4$ ist, so ist $D_1 = D$ und alle Hilfsformen der Zahl 4 sind

$$(1, 0, -D), \left(4, 1, \frac{1-D}{4}\right), \left(4, 3, \frac{9-D}{4}\right).$$

Die zwei letzten Formen sind jedoch nur dann primitiv, wenn $D \equiv 5 \pmod 8$ ist und es wird

$$\Theta(2^2) = 2-(-1)^{\frac{D^2-1}{8}}$$

Man hat also bei negativer Determinante

$$k = \frac{h\lambda_1}{\lambda\left(2-(-1)^{\frac{D^2-1}{8}}\right)}$$

und bei positiver

$$k = \frac{he}{2-(-1)^{\frac{D^2-1}{8}}} = \frac{h}{2-(-1)^{\frac{D^2-1}{8}}} \cdot \frac{l(T+U\sqrt{D})}{l\left(\frac{T_1+U_1\sqrt{D}}{2}\right)}$$

II. Es sei $\sigma = 1$, $n > 1$, $D = D_1 n^2$.

Damit die Hilfsform $\left(\nu^2, \nu s, s^2 - \frac{D}{\nu^2}\right)$ primitiv ausfalle, ist es nothwendig und hinreichend, dass $s^2 - \frac{D}{\nu^2}$ zu ν theilerfremd sei. Es kommt also nur darauf an, für jeden einzelnen Theiler ν von n die Anzahl der Zahlen der Reihe

$$0^2 - \frac{D}{\nu^2},\ 1^2 - \frac{D}{\nu^2},\ 2^2 - \frac{D}{\nu^2},\ \ldots\ (\nu-1)^2 - \frac{D}{\nu^2}$$

zu ermitteln, welche zu ν theilerfremd sind und es sei zu diesem Ende x_δ die Anzahl aller Zahlen dieser Reihe, welche mit ν den grössten gemeinschaftlichen Theiler δ haben, y_δ die Anzahl der durch δ theilbaren Zahlen der nämlichen Reihe.

Man kann y_δ für einen bestimmten Theiler δ von ν auf zweierlei Weise ausdrücken.

Einerseits kann jede durch δ theilbare Zahl $s^2 - \frac{D}{\nu^2}$ der vorstehenden Reihe mit ν nur einen grössten gemeinschaftlichen Theiler haben, welcher ein Vielfaches von δ, also eine der Zahlen

$$\delta,\ \delta\varepsilon,\ \delta\varepsilon' \ldots$$

ist, wo $1, \varepsilon, \varepsilon', \ldots$ alle Theile von $\frac{\nu}{\delta}$ bezeichnen. Die in Rede stehenden Zahlen zerfallen daher in die x_δ Zahlen, welche mit ν den grössten gemeinschaftlichen Theiler δ haben, in die $x_{\delta\varepsilon}$ Zahlen, welche mit ν den grössten gemeinschaftlichen Theiler $\delta\varepsilon$ haben, u. s. f. und es ist

$$y\delta = x_\delta + x_{\delta\varepsilon} + x_{\delta\varepsilon'} + \ldots$$
$$= \Sigma x_{\delta t},$$

wo die Summe über alle Theiler t von $\frac{\nu}{\delta}$ zu erstrecken ist.

Anderseits ist es für die Theilbarkeit der Zahl $s^2 - \frac{D}{\nu^2}$ durch δ nothwendig und hinreichend, dass der echte Rest s_0 von s in Bezug auf den Modul δ eine nicht negative und δ nicht erreichende Wurzel der Congruenz

$$z^2 \equiv \frac{D}{\nu^2} \pmod{\delta}$$

und $\frac{s - s_0}{\delta}$ eine der Zahlen

$$0, 1, \ldots \frac{\nu}{\delta} - 1$$

sei. Besitzt daher diese Congruenz $\mathfrak{A}_\delta$ nicht negative und δ nicht erreichende Wurzeln $\omega, \omega', .$ so sind

$$\omega, \omega + \delta, \omega + 2\delta, . \quad . \omega + \left(\frac{\nu}{\delta} - 1\right)\delta$$

$$\omega', \omega' + \delta, \omega' + 2\delta, . \quad . \omega' + \left(\frac{\nu}{\delta} - 1\right)\delta$$

genau alle Zahlen der Reihe $0, 1, \ldots \nu - 1$, für welche der Ausdruck $s^2 - \frac{D}{\nu^2}$ durch δ theilbar wird, und es wird demnach

$$y_\delta = \frac{\nu}{\delta}\mathfrak{A}_\delta.$$

Ist aber $\mathfrak{A}_\delta = 0$, so leuchtet diese Gleichung unmittelbar ein.

Man hat also die Gleichung

$$\Sigma x_{\delta t} = \frac{\nu \mathfrak{A}_\delta}{\delta}$$

Da es solcher Gleichungen so viele gibt als Theiler δ von ν, so ergibt sich in bekannter Weise durch deren Auflösung

$$x_1 = \Sigma \frac{\chi(\delta)\nu\mathfrak{A}_\varepsilon}{\delta},$$

wo die Summe über alle Theiler δ von ν zu erstrecken ist und $\chi(\delta)$ den Werth 0, 1,—1 hat, je nachdem δ einen die Einheit übersteigenden quadratischen Theiler oder eine gerade oder ungerade Anzahl von verschiedenen Primfactoren enthält.

Wenn nun δ keinen die Einheit übersteigenden quadratischen Theiler besitzt, so ist, über alle Theiler δ_1 von δ erstreckt,

$$\mathfrak{A}_\varepsilon = \Sigma \left(\frac{D_1 \frac{n^2}{\nu^2}}{\delta_1} \right);$$

hierin ist unter $\left(\frac{D_1 \frac{n^2}{\nu^2}}{\delta_1} \right)$ das Legendre-Jacobi'sche Symbol zu verstehen, welches in dem Falle eines geraden Nenners $\delta_1 = 0$ zu setzen ist. Es ist also auch

$$\chi(\delta)\mathfrak{A}_\varepsilon = \Sigma \chi(\delta) \left(\frac{D_1 \frac{n^2}{\nu^2}}{\delta_1} \right).$$

Diese Formel gilt aber auch noch, wenn δ quadratische Theiler aufweist, da in diesem Falle beide Seiten verschwinden.

Man hat also

$$x_1 = \Sigma \chi(\delta) \left(\frac{D_1 \frac{n^2}{\nu^2}}{\delta_1} \right) \frac{\nu}{\delta},$$

wo die Summe über alle Theiler δ und δ_1 von ν zu erstrecken ist, deren zweiter in dem ersten aufgeht. Setzt man für jedes solches Theilerpaar δ, δ_1

$$\delta = \delta_1\delta_2 \qquad \nu = \delta\delta_3 = \delta_1\delta_2\delta_3,$$

so wird

$$x_1 = \Sigma \chi(\delta_1\delta_2) \left(\frac{D_1 \frac{n^2}{\delta_1^2\delta_2^2\delta_3^2}}{\delta_1} \right) \delta_3,$$

wo die Summe über alle möglichen Theiler δ_1, δ_2, δ_3 von ν zu erstrecken ist, deren Product $= \nu$ ist.

Summirt man alle Anzahlen x_1, welche den einzelnen Theilern ν von n entsprechen, so ergibt sich $\Theta(n^2)$ als Summe aller Ausdrücke

$$\chi(\delta_1\delta_2)\left(\frac{D_1\frac{n^2}{\delta_1^2\delta_2^2\delta_3^2}}{\delta_1}\right)\delta_3,$$

in welchen δ_1, δ_2, δ_3 alle möglichen Theiler von n durchlaufen, deren Product in n aufgeht. Man hat also in diesem Sinne

$$\Theta(n^2) = \Sigma\chi(\delta_1\delta_2)\left(\frac{D_1\frac{n^2}{\delta_1^2\delta_2^2\delta_3^2}}{\delta_1}\right)\delta_3.$$

Man denke sich die Glieder dieser Summe in Gruppen vertheilt, indem man alle Glieder, welche irgend zwei bestimmten Werthen von δ_1 und δ_3 entsprechen, in je eine Gruppe stellt. Man erhält alle Glieder einer Gruppe, wenn man δ_2 alle Theiler von $\frac{n}{\delta_1\delta_3}$ durchlaufen lässt.

Wenn $\frac{n}{\delta_1\delta_3} > 1$, so ist die Summe der Glieder einer solchen Gruppe $= 0$. Sind nämlich δ_1 und $\frac{n}{\delta_1\delta_3}$ nicht theilerfremd, so müssen entweder δ_1 und δ_2, oder δ_1 und $\frac{n}{\delta_1\delta_2\delta_3}$ einen die Einheit übersteigenden Theiler gemein haben und es ist entweder $\chi(\delta_1\delta_2) = 0$ oder $\left(\frac{D_1\frac{n^2}{\delta_1^2\delta_2^2\delta_3^2}}{\delta_1}\right) = 0$, so dass alle Glieder der betreffenden Gruppe verschwinden. Sind aber δ_1 und $\frac{n}{\delta_1\delta_3}$ theilerfremd, so ist δ_1 zu jedem Werthe von δ_2 und $\frac{n}{\delta_1\delta_2\delta_3}$ theilerfremd und man hat

$$\chi(\delta_1\delta_2) = \chi(\delta_1)\chi(\delta_2)$$

$$\left(\frac{D_1\frac{n^2}{\delta_1^2\delta_2^2\delta_3^2}}{\delta_1}\right) = \left(\frac{D_1}{\delta_1}\right)\left(\frac{\frac{n}{\delta_1\delta_2\delta_3}}{\delta_1}\right) = \left(\frac{D_1}{\delta_1}\right),$$

da $\left(\frac{\frac{n}{\delta_1\delta_2\delta_2}}{\delta_1}\right)^2$ den Werth 1 oder 0 hat, je nachdem δ_1 ungerade oder gerade ist. Die Summe der Glieder der Gruppe ist daher

$$= \chi(\delta_1)\left(\frac{D_1}{\delta_1}\right)\Sigma\chi(\delta_2),$$

wo die Summation sich auf alle Theiler δ_2 von $\frac{n}{\delta_1\delta_3}$ bezieht und daher ein verschwindendes Resultat liefert.

Es bleiben also nur diejenigen Gruppen übrig, in welchen $n = \delta_1\delta_3$ ist und welche nur aus einem, dem Theiler $\delta_2 = 1$ entsprechenden Gliede

$$\chi(\delta_1)\left(\frac{D_1}{\delta_1}\right)\delta_3 = \chi(\delta_1)\left(\frac{D_1}{\delta_1}\right)\frac{n}{\delta_1}$$

bestehen, und es wird

$$\Theta(n^2) = \Sigma\chi(\delta_1)\left(\frac{D_1}{\delta_1}\right)\frac{n}{\delta_1}$$

$$= n\Pi\left((1-\left(\frac{D_1}{p}\right)\frac{1}{p}\right)$$

wo das Summenzeichen auf alle Theiler δ_1 von n und das Productzeichen auf alle Primfactoren p von n zu beziehen ist.

9.

Gauss bestimmt die Anzahl der Classen des Hauptgeschlechts, indem er beweist, dass dieselben mit den Classen zusammenfallen, welche aus der Duplication aller primitiven Classen hervorgehen.

Bezeichnet Γ den Inbegriff aller primitiven ambigen Classen der Determinante D und ΓK den Inbegriff aller Classen, welche aus der Zusammensetzung der Classe K mit allen Classen von Γ hervorgehen, so lassen sich alle primitiven Classen in einen oder mehrere Inbegriffe

$$\Gamma K_0, \Gamma K_1, \ldots \Gamma K_{\mu-1}$$

vertheilen. Da aus jeder ambigen Classe durch Duplication die Hauptclasse K_0 entsteht, so bringen alle Classen eines Inbegriffs ΓK_i durch Duplication dieselbe Classe K_i^2 hervor und es können daher durch Duplication aller primitiven Classen nur höchstens die μ Classen

$$K_0^2,\ K_1^2,\ \ldots K_{\mu-1}^2 \tag{3}$$

entstehen. Diese sind aber auch wirklich alle untereinander verschieden. Denn aus der Annahme

$$K_\beta^2 = K_\alpha^2$$

würde

$$(K_\beta K_\alpha')^2 = (K_\alpha K_\alpha')^2 = K_0$$

hervorgehen, wo K_α' die entgegengesetzte Classe von K_α bezeichnet; es wäre also $K_\beta K_\alpha'$ eine ambige Classe L und gegen die Annahme $K_\beta = LK_\alpha$.

Alle Classen (3) gehören dem Hauptgeschlechte an und es erhellt, dass dieselben dieses Geschlecht genau erschöpfen müssen, wenn man darthun kann, dass jede Classe des Hauptgeschlechtes durch Duplication entsteht.

Es ist also zu beweisen, dass jede gegebene primitive Form F des Hauptgeschlechts einer Form $\overline{\varphi\varphi}$ äquivalent ist, welche aus der Duplication einer primitiven Form φ entsteht.

Zu diesem Ende soll zunächst dargethan werden, dass F im Stande ist, Quadratzahlen darzustellen. Man darf hiebei unbeschadet der Allgemeinheit annehmen, dass der erste Coëfficient von F zu $2D$ theilerfremd ist.

Es sei

$$F = AX^2 + 2BXY + CY^2$$

und

$$A = A_0 g^2 \qquad D = D_0 h^2,$$

wo g^2, h^2 die grössten in A, D aufgehenden quadratischen Theiler bezeichnen. Da h zu A_0 theilerfremd ist, so kann man eine Zahl B_0 bestimmen, welche der Congruenz

$$hB_0 \equiv B \pmod{A_0}$$

genügt, und es wird

$$h^2 B_0^2 \equiv B^2 \equiv D \equiv h^2 D_0 \pmod{A_0}.$$

Hebt man h^2 fort, so ergibt sich

$$B_0^2 \equiv D_0 \qquad (\mathrm{mod}\ A_0)$$

und man hat

$$D_0 = B_0^2 - A_0 C_0,$$

wo C_0 eine ganze Zahl bezeichnet. Wird nun

$$A_0 x^2 + 2B_0 xy + C_0 y^2 = f$$
$$hB_0 = B + lA_0$$

gesetzt, so ist identisch

$$F(hx + ly, g^2 y) = g^2 h^2 f(x, y)$$

und es genügt darzuthun, dass die Form f Quadratzahlen darstellt, oder die Gleichung

$$A_0 x^2 + 2B_0 xy + C_0 y^2 - z^2 = 0$$

in ganzen Zahlen x, y, z lösbar ist.

Setzt man

$$x = \xi - B_0 \eta$$
$$y = A_0 \eta$$
$$z = A_0 \zeta$$

so ergibt sich nach Forthebung von A_0 für ξ, η, ζ die Gleichung

$$\xi^2 - D_0 \eta^2 - A_0 \zeta^2 = 0,$$

welche zu den von Lagrange und Legendre gelösten gehört.

Dieselbe erfüllt alle Lösbarkeitsbedingungen. Denn ihre Coëfficienten $1, -D_0, -A_0$ sind ohne quadratischen Theiler, paarweise theilerfremd und nicht von gleichen Vorzeichen. Ferner sind die negativen Producte je zweier

$$-A_0 D_0, \quad A_0, \quad D_0$$

beziehungsweise quadratische Reste von

$$1, \quad D_0, \quad A_0.$$

Dass D_0 Rest von A_0 ist, folgt aus der Gleichung $D_0 = B_0^2 - A_0 C_0$. Dass A_0 Rest von D_0 ist, erhellt unmittelbar, wenn es feststeht, dass A Rest von D ist; denn aus einer Congruenz

$$A = g^2 A_0 \equiv q^2 \qquad (\mathrm{mod}\ D)$$

folgt, wenn $gg_1 \equiv 1 \pmod{D_0}$ ist,

$$A_0(gg_1)^2 \equiv A_0 \equiv (g_1 q)^2 \qquad (\mathrm{mod}\ D_0).$$

Dass aber A Rest von D ist, folgt daraus, dass A eine zu D theilerfremde, durch F darstellbare Zahl und F eine Form des Hauptgeschlechts ist, da A demzufolge nicht nur Rest von den einzelnen etwaigen ungeraden Primfactoren von D, sondern auch von der höchsten, in D aufgehenden Potenz von 2 ist.

Man kann also nach dem Lagrange'schen Verfahren eine ganzzahlige Lösung ξ, η, ζ der obigen Gleichung ermitteln und es ist klar, dass ζ nicht $= 0$ sein kann, da andernfalls aus der Gleichung $\xi^2 - D_0\eta^2 = 0$ auch $\xi = \eta = 0$ folgen würde.

Stellt aber die Form F eine Quadratzahl k^2 dar, so ist sie einer primitiven Hilfsform (m^2, b, c) von k^2 äquivalent, deren erster Coëfficient ein Quadrat ist.

Es lässt sich nun weiter zeigen, dass jede primitive Form $\psi = (m^2, b, c)$, welche zum Hauptgeschlechte gehört und schlicht ist, durch Duplication entsteht.

Es sei μ der grösste gemeinschaftliche Theiler von m und b, der von m und 2 und δ'' der von δ' und $\frac{b+m}{\mu}$. Die Zahl $\mu\delta'\delta''$ kann nur gerade sein, wenn $\delta' = 2$ ist, und ist zu c theilerfremd. Hätten nämlich c und $\mu\delta'\delta''$ einen Primtheiler gemein, so müsste derselbe in μ oder δ', also jedenfalls in m^2, $2b$ und c aufgehen, was der Primitivität der Form ψ widerspricht.

c ist quadratischer Rest von jeder etwa in $\mu\delta'\delta''$ aufgehenden ungeraden Primzahl p. Denn c ist durch ψ darstellbar und p geht in μ, also auch in m, b und $D = b^2 - m^2 c$ auf.

Ist die Zahl $\mu\delta'\delta''$ gerade und 2^π die höchste in derselben aufgehende Potenz von 2, so ist c auch quadratischer Rest von 2^π. Dies bedarf nur eines Beweises, wenn $\pi > 1$, also μ gerade ist. Man hat

$$\frac{D}{\mu^2} = \frac{b^2 - m^2 c}{\mu^2} = \frac{b^2 - m^2}{\mu^2} + \frac{m^2}{\mu^2}(c-1)$$
$$\equiv \delta'' \qquad (\mathrm{mod}\ 2),$$

weil $\frac{b+m}{\mu}$ und $\frac{b-m}{\mu}$ bei ungeradem δ'' beide ungerade sind.

Hieraus folgt aber

$$D \equiv \delta''\mu^2 \equiv \mu\delta'\delta'' + 8\delta'' \frac{1}{2} \cdot \frac{\mu}{2}\left(\frac{\mu}{2} - 1\right) \pmod{2\mu^2}$$

$$\equiv \mu\delta'\delta'' \pmod{8}$$

und es ist also entweder gleichzeitig

$$\mu\delta'\delta'' \equiv 4 \qquad D \equiv 4 \pmod{8} \qquad \pi = 2$$

$$(-1)^{\frac{c-1}{2}} = 1 \qquad c \equiv 1 \pmod{4}$$

oder gleichzeitig

$$\mu\delta'\delta'' \equiv 0 \qquad D \equiv 0 \pmod{8} \qquad \pi > 2$$

$$(-1)^{\frac{c-1}{2}} = 1 \qquad (-1)^{\frac{c^2-1}{8}} = 1 \qquad c \equiv 1 \pmod{8}.$$

Die Congruenz

$$z^2 \equiv c \pmod{\mu\delta'\delta''}) \tag{4}$$

ist daher immer lösbar. Sie ist aber auch so lösbar, dass die Zahl $\frac{b+mz}{\mu\delta''}$ theilerfremd zu μ ausfällt.

Dass diese Zahl für jede Wurzel z der vorstehenden Congruenz ganz ist, folgt daraus, dass in dem Falle $\delta'' = 2$ ungerade, also

$$\frac{b+mz}{\mu} \equiv \frac{b+m}{\mu} \equiv 0 \pmod{\delta''}$$

ist.

Für jede in $\mu\delta'\delta''$ genau aufgehende Primzahlpotenz p^π gibt es zwei ungerade Wurzeln ζ und $-\zeta$ der Congruenz

$$z^2 \equiv c \pmod{p^\pi}$$

und es muss eine der beiden Zahlen $\frac{b+m\zeta}{\mu\delta''}$, $\frac{b-m\zeta}{\mu\delta''}$ zu p theilerfremd sein. Wären nämlich beide durch p theilbar, so wären es auch $\frac{2}{\delta''}\,\frac{b}{\mu}$ und $\frac{2}{\delta''}\,\frac{m}{\mu}$ und daher auch $\frac{2}{\delta''}$, weil $\frac{q}{\mu}$ und $\frac{m}{\mu}$ theilerfremd sind; es müsste also $p = 2$, $\delta'' = 1$ sein,

was unmöglich ist, da $\frac{b+m\zeta}{\mu} \equiv \frac{b+m}{\mu} \equiv \delta''$ (mod 2) ist. Man darf also annehmen, dass $\frac{b+m\zeta}{\mu\delta''}$ zu p theilerfremd ist. Bestimmt man dann eine Zahl z, welche in Bezug auf die einzelnen Primzahlpotenzen p^π von $\mu\delta'\delta''$ der jeweiligen Wurzel ζ congruent ist, so genügt dieselbe der Congruenz (4) und es wird

$$\frac{b+mz}{\mu} \equiv \frac{b}{\mu} + \frac{m}{\mu}\zeta \qquad (\text{mod } p)$$

Die Zahl $\frac{b+mz}{\mu\delta''}$ kann also durch keinen ungeraden Primfactor von μ theilbar sein. Sie muss aber auch ungerade sein, wenn μ gerade ist, da alsdann $2^\pi \geqq 4$, also

$$\frac{b+mz}{\mu} \equiv \frac{b}{\mu} + \frac{m}{\mu}\zeta \qquad (\text{mod } 4)$$

und

$$\frac{b+mz}{\mu\delta''} \equiv \frac{b+m\zeta}{\mu\delta''} \qquad (\text{mod } 2)$$

ist.

Dieselbe Zahl $\frac{b+mz}{\mu\delta''}$ ist aber auch zu $\frac{m}{\mu}$ theilerfremd, weil $\frac{m}{\mu}$ zu $\frac{b}{\mu}$, also auch zu $\frac{b+mz}{\mu}$ und umsomehr zu $\frac{b+mz}{\mu\delta''}$ theilerfremd ist. Wenn aber μ und $\frac{m}{\mu}$ zu $\frac{b+mz}{\mu\delta''}$ theilerfremd sind, so gilt dasselbe von dem Product $\mu\cdot\frac{m}{\mu} = m$. Weil endlich m und $\frac{2}{\delta'}$ theilerfremd sind, so sind es auch m und $\frac{2(b+mz)}{\mu\delta'\delta'}$ und $\mu\delta'\delta''$ ist der grösste gemeinschaftliche Theiler von $m\mu\delta'\delta''$ und $2(b+mz)$.

Setzt man nun

$$l = \frac{(b+mz)^2 - D}{m\mu\delta'\delta''} = z\,\frac{2(b+mz)}{\mu\delta'\delta''} - m\,\frac{z^2-c}{\mu\delta'\delta''}$$

$$\varphi = (m\mu\delta'\delta'',\ b+mz,\ l),$$

so ist φ eine primitive Form, welche, mit sich selbst zusammengesetzt, ψ hervorbringt.

Dass φ primitiv ist, folgt daraus, dass die Coëfficienten $m\mu\delta'\delta''$ und $2(b+mz)$ nur solche Primtheiler gemein haben können, welche in ihrem grössten gemeinschaftlichen Theiler $\mu\delta'\delta''$ aufgehen; ein solcher Primtheiler geht aber in m auf und kann in l nicht aufgehen, weil er weder in z noch in $\frac{2(b+mz)}{\mu\delta'\delta''}$ aufgehen kann.

Wird die Form $\overline{\varphi\varphi}$ mit $(\mathfrak{A}, \mathfrak{B}, \mathfrak{C})$ bezeichnet und eine Lösung der Gleichung

$$m\mu\delta'\delta''\alpha+2(b+mz)\gamma = \mu\delta'\delta''$$

ermittelt, so ist

$$\mathfrak{A} = \left(\frac{m\mu\delta'\delta''}{\mu\delta'\delta''}\right)^2 = m^2$$

$$\mathfrak{B} \equiv \alpha m(b+mz)+\gamma\frac{D+(b+mz)^2}{\mu\delta'\delta''} \pmod{m^2}.$$

Zieht man von dieser Congruenz die mit $\frac{b}{\mu\delta'\delta''}$ multiplicirte Gleichung zwischen α, γ ab, so folgt

$$\mathfrak{B}-b \equiv \alpha m^2 z+\gamma\frac{D-b^2+m^2z^2}{\mu\delta'\delta''}$$

$$\equiv\left(\alpha z+\gamma\frac{z^2-c}{\mu\delta'\delta''}\right)m^2$$

$$\equiv 0 \pmod{m^2}.$$

Es ist also $\mathfrak{B} = b$ und demnach

$$(\mathfrak{A}, \mathfrak{B}, \mathfrak{C}) = \overline{\varphi\varphi} = \psi.$$