SUB | NIEDERSÄCHSISCHE STAATS- UND UNIVERSITÄTSBIBLIOTHEK GÖTTINGEN

Werk

Titel: Vorlesungen über Zahlentheorie
Autor: Dirichlet, Peter
Verlag: Vieweg
Ort: Braunschweig
Jahr: 1871
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN30976923X
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN30976923X
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

LOG Id: LOG_0189
LOG Titel: §, 170. Composition der quadratischen Formen
LOG Typ: chapter

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.
Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.
Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

wo x und z willkürliche ganze rationale Zahlen bedeuten. Da aus (5)

$$N(\nu) = x^2 + bxz + acz^2$$

folgt, so sind die Norm und Determinante von $\mathfrak{n}$ resp. $= 1$ und d.

Bezeichnet man ganz allgemein die Anzahl der in einem Modul $\mathfrak{b}$ enthaltenen Zahlen, welche in Bezug auf einen Modul $\mathfrak{a}$ incongruent sind, mit $(\mathfrak{b}, \mathfrak{a})$, so ergiebt sich aus

$$g = h\alpha + k\beta$$

$$g\frac{\alpha\beta}{\alpha} = -ck\alpha + (ah + bk)\beta$$

nach leicht zu beweisenden allgemeinen Sätzen*)

$$(\mathfrak{n}, \mathfrak{m}) = \frac{g^2}{u}, \quad (\mathfrak{m}, \mathfrak{n}) = \frac{e}{u}, \quad (\mathfrak{n}, \mathfrak{m}) = m(\mathfrak{m}, \mathfrak{n}),$$

wo u den grössten gemeinschaftlichen Divisor von g und e bedeutet. Ist $\mathfrak{m}$ ein Ideal, also ein Vielfaches von $\mathfrak{n}$, so ist $(\mathfrak{m}, \mathfrak{n}) = 1$, $(\mathfrak{n}, \mathfrak{m}) = m$.

§. 170.

Sind $\mathfrak{m}$, $\mathfrak{m}'$ zwei Moduln von der eben betrachteten Beschaffenheit, deren Zahlen μ, μ' demselben quadratischen Körper Ω angehören, so bilden alle Producte $\mu\mu'$ und deren Summen wieder einen solchen Modul $\mathfrak{m}'' = \mathfrak{m}\mathfrak{m}'$. Uebertragen wir die vorhergehenden Bezeichnungen durch Accentuation von $\mathfrak{m}$ auf $\mathfrak{m}'$ und $\mathfrak{m}''$, so müssen *erstens*, weil alle Producte $\mu\mu'$ in $\mathfrak{m}''$ enthalten sind, acht ganze rationale Zahlen $p, q \ldots p''', q'''$ existiren, welche den Gleichungen

$$\begin{aligned} \alpha\alpha' &= p\alpha'' + q\beta'' \\ \alpha\beta' &= p'\alpha'' + q'\beta'' \\ \beta\alpha' &= p''\alpha'' + q''\beta'' \\ \beta\beta' &= p'''\alpha'' + q'''\beta'' \end{aligned} \tag{1}$$

*) Vergl. §. 161. Anm. — Ich erwähne hier nur noch Folgendes. Nennt man zwei Moduln $\mathfrak{a}$, $\mathfrak{b}$ verwandt, wenn $(\mathfrak{a}, \mathfrak{b})$ und $(\mathfrak{b}, \mathfrak{a})$ endlich sind, so sind zwei mit $\mathfrak{a}$ verwandte Moduln $\mathfrak{b}$, $\mathfrak{c}$ auch mit einander verwandt, und es ist

$$(\mathfrak{a}, \mathfrak{b})\,(\mathfrak{b}, \mathfrak{c})\,(\mathfrak{c}, \mathfrak{a}) = (\mathfrak{b}, \mathfrak{a})\,(\mathfrak{c}, \mathfrak{b})\,(\mathfrak{a}, \mathfrak{c}),$$

wovon man sich leicht durch die Betrachtung der kleinsten gemeinschaftlichen Vielfachen und grössten gemeinschaftlichen Theiler überzeugt.

genügen. Setzen wir zur Abkürzung*) die aus ihnen gebildeten partialen Determinanten

$$\begin{aligned} pq' - qp' = P, \quad pq'' - qp'' = Q, \quad pq''' - qp''' = R, \\ p''q''' - q''p''' = U, \quad p'q''' - q'p''' = T, \quad p'q'' - q'p'' = S, \end{aligned} \tag{2}$$

so ist

$$RS = QT - PU, \tag{3}$$

und durch Elimination von α'', β'' aus je drei der Gleichungen (1) erhält man

$$\begin{aligned} * \quad U\alpha\beta' - T\beta\alpha' + S\beta\beta' &= 0 \\ - U\alpha\alpha' \quad * \quad + R\beta\alpha' - Q\beta\beta' &= 0 \\ T\alpha\alpha' - R\alpha\beta' \quad * \quad + P\beta\beta' &= 0 \\ - S\alpha\alpha' + Q\alpha\beta' - P\beta\alpha' \quad * \quad &= 0. \end{aligned} \tag{4}$$

Eliminirt man T aus der ersten und dritten, ferner U aus der ersten und zweiten dieser Gleichungen, so erhält man

$$\begin{aligned} P\beta^2 - (R - S)\alpha\beta + U\alpha^2 &= 0, \\ Q\beta'^2 - (R + S)\alpha'\beta' + T\alpha'^2 &= 0, \end{aligned}$$

und folglich muss (zufolge (5) in §. 169)

$$\begin{aligned} P = an', \quad R - S = bn', \quad U = cn', \\ Q = a'n, \quad R + S = b'n, \quad T = c'n \end{aligned} \tag{5}$$

sein, wo n, n' ganze rationale, von Null verschiedene Zahlen bedeuten (denn n' muss eine ganze Zahl sein, weil a, b, c keinen gemeinschaftlichen Theiler haben, und wäre $n' = 0$, also auch $P = 0$, so wären α', β' zufolge (1) nicht unabhängig von einander); hierdurch nimmt die erste der Gleichungen (4) die Form

$$(b\beta - 2c\alpha)\beta' n' = (b'\beta' - 2c'\alpha')\beta n$$

an, mithin ist (zufolge (5) in §. 169)

$$n' \sqrt{d} = n \sqrt{d'}, \tag{6}$$

und hiermit sind die vier Gleichungen (4) vollständig befriedigt. Das Product dd' ist, wie zu erwarten war, eine Quadratzahl.

Da *zweitens* alle Zahlen μ'' des Moduls $\mathfrak{m}''$ durch Addition von Producten $\mu\mu'$ entstehen, so existiren acht ganze rationale Zahlen $u, v \ldots u''', v'''$, welche den Bedingungen

*) Die Bezeichnungen schliessen sich an die an, welche *Gauss* in den artt. 235, 236 der *Disquisitiones Arithmeticae* gewählt hat; die nothwendigen Modificationen sind leicht zu erkennen.

$$\begin{aligned} \alpha'' &= u\alpha\alpha' + u'\alpha\beta' + u''\beta\alpha' + u'''\beta\beta' \\ \beta'' &= v\alpha\alpha' + v'\alpha\beta' + v''\beta\alpha' + v'''\beta\beta' \end{aligned} \tag{7}$$

genügen. Substituirt man hierin die Gleichungen (1), und berücksichtigt, dass die Zahlen α'', β'' von einander unabhängig sind, so folgt

$$\begin{aligned} pu + p'u' + p''u'' + p'''u''' &= 1 \\ qu + q'u' + q''u'' + q'''u''' &= 0 \end{aligned} \tag{8}$$

und

$$\begin{aligned} pv + p'v' + p''v'' + p'''v''' &= 0 \\ qv + q'v' + q''v'' + q'''v''' &= 1. \end{aligned} \tag{9}$$

Bildet man die Determinante aus diesen vier Summen, so erhält man eine Gleichung von der Form

$$PP_1 + QQ_1 + RR_1 + SS_1 + TT_1 + UU_1 = 1, \tag{10}$$

wo die Determinanten $P_1 \ldots U_1$ auf dieselbe Weise aus den Zahlen $u, v \ldots u''', v'''$ gebildet sind, wie $P \ldots U$ aus $p, q \ldots p''', q'''$, und hieraus folgt, dass die sechs Zahlen (2) keinen gemeinschaftlichen Theiler haben. Dasselbe Resultat erhält man auch auf folgendem Wege; eliminirt man jede der vier Zahlen u, u', u'', u''' aus den beiden Gleichungen (8), so folgt

$$\begin{aligned} q &= \ * \ - Pu' - Qu'' - Ru''' \\ q' &= Pu \ * \ - Su'' - Tu''' \\ q'' &= Qu + Su' \ * \ - Uu''' \\ q''' &= Ru + Tu' + Uu'' \ * \end{aligned} \tag{11}$$

ebenso erhält man aus (9) die Gleichungen

$$\begin{aligned} p &= \ * \ Pv' + Qv'' + Rv''' \\ p' &= -Pv \ * \ + Sv'' + Tv''' \\ p'' &= -Qv - Sv' \ * \ + Uv''' \\ p''' &= -Rv - Tv' - Uv'' \ * \end{aligned} \tag{12}$$

Aus (11) folgt, dass jeder gemeinschaftliche Theiler der sechs Determinanten (2) in den vier Zahlen q, q', q'', q''', mithin zufolge (9) auch in der Zahl 1 aufgeht, was zu beweisen war. Hieraus ergiebt sich leicht mit Rücksicht auf (3), dass auch die sechs Zahlen (5) keinen gemeinschaftlichen Theiler haben; geht nämlich e in P, Q, $R - S$, $R + S$, T, U auf, so sind die Zahlen $2R$, $2S$ ebenfalls theilbar durch e, und die Quotienten $2R:e$ und $2S:e$ sind ent-

weder beide gerade oder beide ungerade, weil ihre Summe gerade ist; wären sie nun beide ungerade, so wäre auch ihr Product $4RS:e^2$ ungerade, was gegen die Gleichung (3) streitet, der zufolge RS durch e^2 theilbar ist; mithin sind R und S durch e theilbar, und folglich ist $e = \pm 1$. Es ergiebt sich daher, dass n und n' *relative Primzahlen* sind.

Durch Elimination der vier Zahlen α, β, α', β' aus den Gleichungen (1) erhält man

$$(p'\alpha'' + q'\beta'')\,(p''\alpha'' + q''\beta'') = (p\alpha'' + q\beta'')\,(p'''\alpha'' + q'''\beta'')$$

oder

$$L\beta''^2 - M\alpha''\beta'' + N\alpha''^2 = 0, \tag{13}$$

wenn man zur Abkürzung

$$\begin{gathered} q'q'' - qq''' = L, \quad p'p'' - pp''' = N, \\ pq''' + qp''' - p'q'' - q'p'' = M \end{gathered} \tag{14}$$

setzt. Wir zeigen zunächst, dass diese drei Zahlen durch nn' theilbar sind; da nämlich zufolge (5)

$$Q \equiv 0, \quad S \equiv -R, \quad T \equiv 0 \pmod{n}$$

ist, so ergiebt sich aus (11) und (12) in Bezug auf denselben Modul

$$\begin{aligned} q &\equiv -Pu' - Ru''', & p &\equiv Pv' + Rv''' \\ q' &\equiv Pu + Ru'', & p' &\equiv -Pv - Rv'' \\ q'' &\equiv -Ru' - Uu''', & p'' &\equiv Rv' + Uv''' \\ q''' &\equiv Ru + Uu'', & p''' &\equiv -Rv - Uv'' \end{aligned}$$

und hieraus

$$L \equiv (PU - R^2)\,(u'u'' - uu'''), \quad N \equiv (PU - R^2)\,(v'v'' - vv'''),$$
$$M \equiv (PU - R^2)\,(u'v'' + v'u'' - uv''' - vu'''),$$

nun ist aber zufolge (3) $PU \equiv R^2 \pmod{n}$, folglich sind L, M, N theilbar durch n; da ferner auf dieselbe Weise sich zeigen lässt, dass sie auch durch n' theilbar sind, so müssen sie, weil n, n' relative Primzahlen sind, auch durch nn' theilbar sein; was zu beweisen war.

Führt man endlich die unabhängigen Variabeln x, y, x', y' und die bilinearen Functionen

$$\begin{aligned} x'' &= pxx' + p'xy' + p''yx' + p'''yy' \\ y'' &= qxx' + q'xy' + q''yx' + q'''yy' \end{aligned} \tag{15}$$

ein, so ergiebt sich durch Elimination von xx', xy', yx', yy'

$$\begin{aligned} py'' - qx'' &= \quad * \quad Pxy' + Qyx' + Ryy' \\ p'y'' - q'x'' &= -Pxx' \quad * \quad + Syx' + Tyy' \\ p''y'' - q''x'' &= -Qxx' - Sxy' \quad * \quad + Uyy' \\ p'''y'' - q'''x'' &= -Rxx' - Txy' - Uyx' \quad * \end{aligned}$$

und hieraus folgt

$$\begin{aligned} &(p'y'' - q'x'')\,(p''y'' - q''x'') - (py'' - qx'')\,(p'''y'' - q'''x'') \\ &= (Px^2 + (R - S)\,xy + Uy^2)\,(Qx'^2 + (R + S)\,x'y' + Ty'^2), \end{aligned} \tag{16}$$

d. h.

$$\begin{aligned} &Lx''^2 + Mx''y'' + Ny''^2 \\ &= nn'(ax^2 + bxy + cy^2)\,(a'x'^2 + b'x'y' + c'y'^2). \end{aligned} \tag{17}$$

Da diese Gleichung eine Identität in Bezug auf die Variabeln x, y, x', y' wird, sobald x'', y'' durch die Ausdrücke (15) ersetzt werden, so muss, wenn enn' den grössten gemeinschaftlichen Divisor von L, M, N bedeutet, e in allen neun Producten aa', $ab' \ldots cc'$ aufgehen; diese letzteren haben aber keinen gemeinschaftlichen Theiler, weil dasselbe sowohl von den Zahlen a, b, c, wie von den Zahlen a', b', c' gilt; mithin ist $e = 1$, also nn' *der grösste gemeinschaftliche Theiler von* L, M, N. Nun ist ferner in Folge der bilinearen Substitution (15)

$$x''\alpha'' + y''\beta'' = (x\alpha + y\beta)\,(x'\alpha' + y'\beta'),$$

folglich auch

$$N(x''\alpha'' + y''\beta'') = N(x\alpha + y\beta)\,N(x'\alpha' + y'\beta'),$$

also

$$\begin{aligned} &m''(a''x''^2 + b''x''y'' + c''y''^2) = \\ &mm'(ax^2 + bxy + cy^2)\,(a'x'^2 + b'x'y' + c'y'^2); \end{aligned}$$

mithin ergiebt sich durch Vergleichung mit (17)

$$nn'm''(a''x''^2 + b''x''y'' + c''y''^2) = mm'(Lx''^2 + Mx''y'' + Ny''^2);$$

diese Gleichung, welche eine Identität in Bezug auf die Variabeln x, y, x', y' wird, sobald x'', y'' durch die Ausdrücke (15) ersetzt werden, muss deshalb auch eine Identität in Bezug auf x'', y'' sein; da ferner m, m', m'' positiv sind, und die Zahlen a'', b'', c'' keinen gemeinschaftlichen Theiler haben, so ergiebt sich

$$m'' = mm' \tag{18}$$

und

$$L = a''nn', \quad M = b''nn', \quad N = c''nn', \tag{19}$$

also

$$\begin{gathered} a''x''^2 + b''x''y'' + c''y''^2 \\ = (ax^2 + bxy + cy^2)\ (a'x'^2 + b'x'y' + c'y'^2). \end{gathered} \tag{20}$$

Da endlich aus der Definition der Grössen (2) und (14), oder auch aus (16) sich leicht ergiebt, dass

$$\begin{gathered} M^2 - 4LN \\ = (R-S)^2 - 4PU = (R+S)^2 - 4QT \end{gathered}$$

ist, so folgt hieraus schliesslich

$$d''n^2n'^2 = dn'^2 = d'n^2,$$

d. h. die Determinante d'' ist der grösste gemeinschaftliche Theiler der beiden Determinanten

$$d = d''n^2, \quad d' = d''n'^2, \tag{21}$$

woraus sich leicht ergiebt, dass die Ordnung $\mathfrak{n}''$ des Productmoduls $\mathfrak{m}'' = \mathfrak{m}\mathfrak{m}'$ auch das Product nn' aus den Ordnungen $\mathfrak{n}$, $\mathfrak{n}'$ von $\mathfrak{m}$, $\mathfrak{m}'$ ist. Ist ferner $\mathfrak{m}'$ das System $\mathfrak{o}$ aller ganzen Zahlen des Körpers Ω, so wird $\mathfrak{m}''$ ein Ideal im engeren Sinne des Wortes, nämlich der grösste gemeinschaftliche Theiler der beiden Ideale $\mathfrak{i}(\alpha)$, $\mathfrak{i}(\beta)$ oder aller Ideale $\mathfrak{i}(\mu)$; zugleich ist $m' = 1$, $m'' = m = N(\mathfrak{m}'')$, und $d' = d'' = \Delta(\Omega)$.

Wir stellen uns jetzt noch die Aufgabe, die Zahlen α'', β'' zu finden, wenn die Zahlen α, β, α', β', also auch a, b, c, $\sqrt{d}$, a', b', c', $\sqrt{d'}$ gegeben sind; die nachfolgende Lösung ist, abgesehen von geringfügigen Aenderungen, der eleganten Methode entlehnt, welche von *Gauss* zu ähnlichem Zweck angewandt ist und sich in hohem Grade verallgemeinern lässt (vergl. §. 161, Anm.). Die beiden relativen Primzahlen n, n' sind durch (6), und folglich die sechs ganzen Zahlen $P \ldots U$ durch (5) (bis auf einen gemeinschaftlichen Factor ± 1) aus den Daten vollständig bestimmt, und zwar so, dass sie die Gleichungen (3), (4) befriedigen und keinen gemeinschaftlichen Theiler haben*). Nun wähle man, durch die Gleichungen (11) geleitet, vier ganze rationale Zahlen $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$, $\mathfrak{Q}'''$ willkürlich, nur mit der einzigen Beschränkung, dass die folgenden vier Zahlen

*) Dass R und S (zufolge (5)) *ganze* Zahlen werden und keinen gemeinschaftlichen Theiler mit P, Q, T, U haben, geht unmittelbar aus der Gewissheit hervor, dass der Modul $\mathfrak{m}''$ und die Basiszahlen α'', β'' *existiren*; es lässt sich aber auch sehr leicht aus (5) und (6) beweisen, natürlich unter der Voraussetzung, dass dd' eine Quadratzahl ist.

$$\begin{aligned} * \quad P\mathfrak{Q}' + Q\mathfrak{Q}'' + R\mathfrak{Q}''' &= rq \\ -P\mathfrak{Q} \quad * \quad + S\mathfrak{Q}'' + T\mathfrak{Q}''' &= rq' \\ -Q\mathfrak{Q} - S\mathfrak{Q}' \quad * \quad + U\mathfrak{Q}''' &= rq'' \\ -R\mathfrak{Q} - T\mathfrak{Q}' - U\mathfrak{Q}'' \quad * \quad &= rq''' \end{aligned} \tag{22}$$

nicht sämmtlich verschwinden und folglich einen grössten gemeinschaftlichen Divisor r besitzen; nachdem hierdurch vier ganze Zahlen q, q', q'', q''' ohne gemeinschaftlichen Theiler gewonnen sind, wähle man (nach §. 24) vier ganze rationale Zahlen v, v', v'', v''' so, dass

$$qv + q'v' + q''v'' + q'''v''' = 1 \tag{23}$$

wird, und bestimme die Zahlen p, p', p'', p''' durch die Gleichungen (12); endlich wähle man sechs ganze rationale Zahlen P', Q', R', S', T', U' (nach §. 24) so, dass

$$PP' + QQ' + RR' + SS' + TT' + UU' = 1 \tag{24}$$

wird, setze hierauf

$$\begin{aligned} u \quad &= \quad * \quad P'q' + Q'q'' + R'q''' \\ u' &= -P'q \quad * \quad + S'q'' + T'q''' \\ u'' &= -Q'q - S'q' \quad * \quad + U'q''' \\ u''' &= -R'q - T'q' - U'q'' \quad * \end{aligned} \tag{25}$$

und bestimme die Zahlen α'', β'' durch die Gleichungen (7), so bilden dieselben eine Basis des Moduls $\mathfrak{m}''$, d. h. sie genügen den Gleichungen (1).

Um sich hiervon zu überzeugen, bemerke man zunächst, dass aus (22) mit Rücksicht auf (3) die Relationen

$$\begin{aligned} * \quad Uq' - Tq'' + Sq''' &= 0 \\ -Uq \quad * \quad + Rq'' - Qq''' &= 0 \\ Tq - Rq' \quad * \quad + Pq''' &= 0 \\ -Sq + Qq' - Pq'' \quad * \quad &= 0 \end{aligned}$$

folgen; mit Hülfe derselben ergiebt sich aus (12) und (23)

$$\begin{aligned} pq' - qp' &= (Pv' + Qv'' + Rv''')q' - (-Pv + Sv'' + Tv''')q \\ &= P(qv + q'v') + (Qq' - Sq)v'' + (Rq' - Tq)v''' \\ &= P(qv + q'v' + q''v'' + q'''v''') = P, \end{aligned}$$

und auf ähnliche Weise erhält man die fünf anderen Gleichungen (2). Mithin folgt die erste der beiden Gleichungen (8), wenn man die Gleichungen (25) mit p, p', p'', p''' multiplicirt und mit Rück-

sicht auf (24) addirt; die zweite Gleichung (8) ergiebt sich unmittelbar aus (25), wenn man mit q, q', q'', q''' multiplicirt und addirt. Es gelten daher auch die aus (8) und (2) abgeleiteten Gleichungen (11). Von den Gleichungen (9) findet die zweite zufolge (23) Statt, während die erste sich aus (12) ergiebt, wenn man mit v, v', v'', v''' multiplicirt und addirt. Setzt man ferner zur Abkürzung

$$uv' - vu' = P_1, \quad uv'' - vu'' = Q_1, \quad uv''' - vu''' = R_1,$$
$$u''v''' - v''u''' = U_1, \quad u'v''' - v'u''' = T_1, \quad u'v'' - v'u'' = S_1,$$

so ergiebt sich die Gleichung (10) entweder auf die dort angegebene Weise aus (8) und (9), oder auch aus (12), wenn man mit u, u', u'', u''' multiplicirt und unter Rücksicht auf (8) addirt. Substituirt man ferner für p, q ihre Ausdrücke aus (12) und (11), so erhält man

$$\begin{aligned} pu + qv &= PP_1 + QQ_1 + RR_1 \\ pu' + qv' &= QS_1 + RT_1 \\ pu'' + qv'' &= -PS_1 + RU_1 \\ pu''' + qv''' &= -PT_1 - QU_1. \end{aligned}$$

Multiplicirt man diese Gleichungen mit $\alpha\alpha', \alpha\beta', \beta\alpha', \beta\beta'$ und addirt, so folgt aus den Definitionen (7) mit Rücksicht auf (4) und (10) die erste der Gleichungen (1); da die anderen sich auf ganz ähnliche Art ergeben, so bilden die durch die Gleichungen (7) definirten Zahlen α'', β'' in der That eine Basis des Productes $\mathfrak{m}'' = \mathfrak{m}\mathfrak{m}'$, was zu beweisen war.

Wir bemerken zum Schluss, dass man für die ersten Basiszahlen $\alpha, \alpha', \alpha''$ stets die kleinsten positiven ganzen rationalen Zahlen g, g', g'' wählen kann, welche in den Moduln $\mathfrak{m}, \mathfrak{m}', \mathfrak{m}''$ enthalten sind; dann wird $q = 0$, und die Bestimmung von $\mathfrak{m}''$ aus $\mathfrak{m}$ und $\mathfrak{m}'$ lässt sich auf ein System von Congruenzen reduciren, ähnlich wie in dem speciellen Falle, welcher in den §§. 145, 146 behandelt ist*).

*) Vergl. *Arndt: Auflösung einer Aufgabe in der Composition der quadratischen Formen.* Crelle's Journal LVI.