Die trinären Zahlformen und Zahlwerthe.

Von W. Šimerka,
suppl. Gymnasiallehrer zu Budweis.

(Vorgelegt in der Sitzung vom 12. Mai 1859.)

Der Gegenstand dieser Abhandlung hat, als eine interessante Partie der Zahlentheorie, bald die Aufmerksamkeit der Mathematiker wie Fermat, Gauss und Legendre erregt. Auch ich befasse mich schon eine geraume Zeit mit demselben, und fand, nachdem ich die Periodicität der quadratischen Zahlformen [1]) entdeckt hatte, zwischen diesen beiden Theorien einen wichtigen Zusammenhang, so dass ich in den Stand gesetzt wurde, aus einer Lösung der Gleichung $x^2 + y^2 + z^2 = D$ alle übrigen abzuleiten. Hiedurch erlitt aber auch dieser Theil der unbestimmten Analytik eine solche Veränderung, dass ich ihn ganz neu überarbeiten musste, was ich hier mit möglichst kurzer Fassung der bereits bekannten Sätze der Öffentlichkeit übergebe.

I. Von den trinären Verhältnissen bei einer einzigen Determinante.

1. Bezeichnung und Benennung der trinären Grössen.

Dem Ausdrucke

$$(mx + ny)^2 + (m'x + n'y)^2 + (m''x + n''y)^2$$

kann nach dem jetzigen Stande der unbestimmten Analytik statt des Legendre'schen *la forme trinaire du diviseur quadratique de la formule $t^2 + Du^2$* — der zweckmässigere Name „eine trinäre Zahlform" (d. i. eine trinäre Gestalt einer quadratischen Zahlform) bei-

[1]) XXXI. Bd., Nr. 18, J. 1858 dieser Sitzungsberichte.

gelegt werden; die Grössen m, m', m'', n, n', n'' mögen dann trinäre Coëfficienten heissen.

Diese trinären Zahlformen sind von zweierlei Art, nämlich eigentliche, wenn die drei Wurzeln

$$mx + ny,\ m'x + n'y,\ m''x + n''y$$

keinen gemeinsamen Theiler haben können, mögen die relativen Primzahlen x, y was immer für Werthe besitzen. Im entgegengesetzten Falle heisst die Form eine uneigentliche.

Zur Bezeichnung dieser Formen kann man sich in Fällen, wo an den Werthen von x, y nichts gelegen ist, des Symbols

$$\begin{Bmatrix} m & & m' & & m'' \\ n & . & n' & . & n'' \end{Bmatrix}$$

bedienen; wird daher der Kürze wegen

$$\begin{aligned} p &= m^2 + m'^2 + m''^2 \\ q &= mn + m'n' + m''n'' \\ r &= n^2 + n'^2 + n''^2 \end{aligned} \tag{1}$$

gesetzt, so ergibt sich

$$\begin{Bmatrix} m & & m' & & m'' \\ n & . & n' & . & n'' \end{Bmatrix} = px^2 + 2q\,xy + ry^2 = (p, 2q, r) \tag{2}$$

Eine ganz besondere Bedeutung haben bei diesen Untersuchungen die Grössen

$$\alpha = m'n'' - m''n',\quad \alpha' = m''n - mn'',\quad \alpha'' = mn' - m'n \tag{3}$$

Ihr Bau als Differenzen von Querproducten wird ersichtlich, wenn man die trinären Coëfficienten unter der Gestalt

$$\begin{matrix} m' & & m'' & & m & & m' \\ n' & . & n'' & . & n & . & n' \end{matrix}$$

ansetzt; nimmt man übrigens α''', m''', n''' für α, m, n an, so entsteht aus jeder der Grössen α, α', α'', α die nächst folgende durch Erhöhung der Striche.

Die Gleichungen (3) geben

$$\begin{aligned} \alpha^2 + \alpha'^2 + \alpha''^2 = &\ (m^2 + m'^2 + m''^2)\ (n^2 + n'^2 + n''^2) \\ &- (mn + m'n' + m''n'')^2 \end{aligned}$$

oder nach (1)

(4) $$D = pr - q^2 = \alpha^2 + \alpha'^2 + \alpha''^2$$

Die Grössen α, α', α'' heissen die trinären Zahlwerthe oder kurz trinäre Werthe von D; man nennt sie eigentlich, wenn sie keinen gemeinsamen Theiler besitzen, sonst sind sie uneigentlich. Statt des Ausdruckes „eine Art trinärer Werthe" d. h. eine Art die Determinante D in die Summe dreier Quadrate zu zerlegen, kann man kurz „eine trinäre Art" gebrauchen. Den Zusammenhang der trinären Werthe α, α', α'' mit der trinären Form, aus der sie entstanden sind, kann man der Übersicht halber mit

(5) $$\begin{Bmatrix} m & \cdot & m' & \cdot & m'' \\ n & & n' & & n'' \end{Bmatrix} = <\alpha,\, \alpha',\, \alpha''>$$

andeuten, welcher Bezeichnungsweise man sich bei allen auf gleiche Art gebildeten Grössen wird bedienen können.

Steht in einer trinären Zahlform ein Coëfficientenpaar auf der eben so vielten Stelle, die in $<\alpha, \alpha', \alpha''>$ ein trinärer Werth einnimmt, so kann man offenbar diese zwei Grössen gleichstellig nennen, so dass etwa $\frac{m}{n}$ mit α gleichstellig, hingegen $\frac{m'}{n'}$ mit α und α'' ungleichstellig sein wird.

1. Anmerkung. Weil Legendre[1]) bei den quadratischen Zahlformen die Vorzeichen der Mittelglieder nicht berücksichtigte, so hatte er auch keinen Grund bei den trinären Zahlformen streng auf die Vorzeichen zu achten, und desshalb nimmt er in seiner VIII. Tabelle alle Werthe von m, m', m'' positiv, indem er statt $(-my + nz)^2$ dem mathematischen Schreibegebrauche entsprechender $(my - nz)^2$ setzt. Aus diesem Grunde war es ihm einerlei, ob die trinären Zahlwerthe positiv oder negativ zum Vorschein kamen. So hat er z. B. bei $D = 90$

$$9y^2 + 6yz + 11z^2 = (2y + 3z)^2 + (2y - z)^2 + (y - z)^2$$

oder nach der hier eingeführten Bezeichnungsweise

$$(9, 6, 11) = \begin{Bmatrix} 2 & \cdot & 2 & \cdot & 1 \\ 3 & & -1 & & -1 \end{Bmatrix}$$

---

[1]) Essai sur la theorie des nombres. 2. edit.

so dass man

$$\alpha = -1,\ \alpha' = 5,\ \alpha'' = -8$$

erhält; will man α, α', α'' positiv haben, so muss

$$(9, 6, 11) = \begin{Bmatrix} 2 & . & -2 & . & 1 \\ 3 & & 1 & & -1 \end{Bmatrix}$$

gesetzt werden.

2. Anmerkung. Lässt sich die Form $px^2 + 2qxy + ry$ in die Summe dreier Quadrate zerlegen, d. h. kann man ihr eine trinäre Gestalt geben, so ist kein Grund vorhanden, warum man sie nicht der Kürze wegen eine trinäre nennen dürfte.

2. Negative Sätze über die Existenz der trinären Formen und Werthe.

Nach 1. lassen sich nachstehende zum Theil bereits bekannte (Legendre Nr. 263 etc.), zum Theil leicht ersichtliche Sätze auf folgende Art stylisiren:

a) Alle Zahlen einer trinären Form haben trinäre Werthe; und kommt in einer quadratischen Zahlform eine Grösse vor, der sich keine trinären Werthe geben lassen, so kann diese Form keine trinäre sein.

b) Erscheint in einer quadratischen Form eine Zahl, die nur uneigentliche trinäre Werthe besitzt, so ist diese Form entweder keine trinäre oder höchstens eine uneigentliche.

c) Eine Determinante, die keine trinären Werthe hat, kann auch keine trinären Formen besitzen. Dass uneigentliche trinäre Werthe nur bei uneigentlichen trinären Formen und umgekehrt vorkommen, lehrt der Verfolg dieser Abhandlung.

d) Keine Zahl von der Gestalt $4^\alpha\,(8k-1)$, wobei auch $\alpha = 0$ sein kann, hat trinäre Werthe; eben so kann auch eine durch 4 theilbare Zahl keine eigentlichen trinären Werthe besitzen. Daher kann keine quadratische Zahlform, worin eine Grösse von der Gestalt $8k - 1$ oder allgemein $4^\alpha\,(8k - 1)$ vorkommt, nach *a)* trinär sein. Ebenso können auch Determinanten von der Gestalt $4^\alpha\,(8k - 1)$ keine trinären Formen haben.

e) Determinanten von der Gestalt $4k$ können nur uneigentliche trinäre Formen haben, da in jeder ihrer quadratischen Zahlformen Grössen von der Gestalt $4k'$ vorkommen.

f) Es lässt sich keine quadratische Zahlform mit einem unpaaren mittleren Coëfficienten in eine trinäre verwandeln.

g) Uneigentliche trinäre Werthe können nur Zahlen von der Gestalt kl^2 besitzen.

h) Keine eigentliche quadratische Zahlform der Determinante $8k + 3$ kann trinär sein, sondern nur eine uneigentliche von der Gestalt $(2p, 2q, 2r)$, wobei p, q, r ungerade sind.

i) Bei der Determinante $4k + 1$ können nur jene quadratischen Formen trinär sein, welche Zahlen von der Gestalt $4\varphi + 1$ enthalten; kommt in einer Form die Zahl $4\varphi - 1$ vor, so enthält ein solcher Ausdruck auch Grössen von der Gestalt $8\varphi - 1$, und kann desshalb nicht trinär sein. Übrigens muss noch nicht jede Form, welche Zahlen von der Gestalt $4\varphi + 1$ enthält, schon desswegen zu den trinären gehören.

k) Eigentliche trinäre Zahlformen können daher nur bei den Determinanten $4k + 1$, $4k + 2$ und $8k + 3$ vorkommen; und dass sich dieser Fall bei jeder Determinante wirklich ereignet, lehrt der Verfolg dieser Theorie.

3. Umwandlung der trinären Formen.

Hat man

$$px^2 + 2qxy + ry^2 = (mx + ny)^2 + (m'x + n'y)^2 + (m''x + n''y)^2$$

dann

$$\alpha = m'n'' - m''n', \quad \alpha' = m''n - mn'', \quad \alpha'' = mn' - m'n,$$

und wird

$$x = fx' + gy', \quad y = f'x' + g'y',$$

wobei $fg' - f'g = 1$ ist, gesetzt, so erhält man die neue Gleichung

$$p'x'^2 + 2q'x'y' + r'y'^2 = (ax' + by')^2 + (a'x' + b'y')^2 + (a''x' + b''y')^2 \; V,$$

worin

$$D = pr - q^2 = p'r' - q'^2$$

und

$$\begin{matrix} a = mf + nf'', & a' = m'f + n'f', & a'' = m''f + n''f' \\ b = mg + ng', & b' = m'g + n'g', & b'' = m''g + n''g' \end{matrix} \qquad (6)$$

sich ergibt. Bezeichnet man die trinären Werthe, welche diese so veränderte Form $\begin{Bmatrix} a & . & a' & . & a'' \\ b & & b' & & b'' \end{Bmatrix}$ nach Gleichung (3) liefert, mit β, β', β'', so ist

$$\begin{aligned} \beta = a'b'' - a''b' = m'm''fg + m'n''fg' + m''n'f'g + n'n''f'g' \\ - m'm''fg - m''n'fg' - m'n''f'g - n'n''f'g' \end{aligned}$$

also

$$\beta = (m'n'' - m''n')\,(fg' - f'g) = \alpha.$$

Eben so findet man $\beta' = \alpha'$ und $\beta'' = \alpha''$. Durch die Umwandlung der quadratischen und trinären Zahlform erleidet daher weder die Grösse der trinären Werthe, noch ihre Anordnung oder ihr Vorzeichen irgend eine Veränderung.

Bei diesem Verfahren gewährt die im Crelle'schen Journal übliche Bezeichnung der Übergangsgleichungen

$$x = fx' + gy', \quad y = f'x' + g'y'$$

durch das Symbol $\begin{pmatrix} f & . & g \\ f' & & g' \end{pmatrix}$, wie aus der Gleichung (6) erhellet, viel Bequemlichkeit.

Die Kürzung dieser Formen wird auf eine ähnliche Art vorgenommen, wie die der quadratischen; ist nämlich in

$$(p, 2q, r) = \begin{Bmatrix} m & . & m' & . & m'' \\ n & & n' & & n'' \end{Bmatrix}, \quad 2q > p,$$

und heisst λ die grösste in $\frac{q}{p}$ enthaltene ganze Zahl, so kürzt man mittelst des Ausdruckes $\begin{pmatrix} 1 & . & -\lambda \\ 0 & & 1 \end{pmatrix}$; wäre jedoch $2q > r$, so sucht man λ aus $\frac{q}{r}$ und operirt mittelst $\begin{pmatrix} 1 & . & 0 \\ -\lambda & & 1 \end{pmatrix}$. Wollte man die oberen trinären Coëfficienten mit den unteren, somit auch p mit r vertauschen, so ist dies mittelst $\begin{pmatrix} 0 & . & 1 \\ -1 & & 0 \end{pmatrix}$ oder $\begin{pmatrix} 0 & . & -1 \\ 1 & & 0 \end{pmatrix}$ vorzunehmen, wo also bei einer dieser Coëfficientenclassen die Vorzeichen geändert werden müssen.

Hierdurch ist man in den Stand gesetzt, jeder trinären Form die einfachste Gestalt zu geben, und braucht in vielen Fällen die zugehörigen quadratischen Formen gar nicht zu verrechnen. So übergeht z. B.

$$\begin{Bmatrix} -4 & . & 4 & . & -3 \\ -9 & & 6 & & -4 \end{Bmatrix} \text{ mittelst } \begin{pmatrix} 1 & . & -2 \\ 0 & & 1 \end{pmatrix} \text{ in}$$

$$\begin{Bmatrix} -4 & . & 4 & . & -3 \\ -1 & & -2 & & 2 \end{Bmatrix} \text{ dies wieder bei } \begin{pmatrix} 1 & . & 0 \\ 1 & & 1 \end{pmatrix} \text{ in}$$

$$\begin{Bmatrix} -5 & . & 2 & . & -1 \\ -1 & & -2 & & 2 \end{Bmatrix} \text{ woraus man durch } \begin{pmatrix} 0 & . & 1 \\ -1 & & 0 \end{pmatrix} \text{ zu}$$

$$\begin{Bmatrix} 1 & . & 2 & . & -2 \\ -5 & & 2 & & -1 \end{Bmatrix} = \langle 2, 11, 12 \rangle = (9, 2, 30) \text{ gelangt.}$$

Anmerkung. Die Gleichungen

$$x = fx' + gy' \quad , \quad y = f'x' + g'y'$$

übergehen, wie man leicht ersehen kann, in

$$x' = g'x - gy \quad , \quad y' = -f'x + fy.$$

Wird demnach die Transformation von

$$\begin{Bmatrix} m & . & m' & . & m'' \\ n & & n' & & n'' \end{Bmatrix} \text{ in } \begin{Bmatrix} a & . & a' & . & a'' \\ b & & b' & & b'' \end{Bmatrix}$$

durch $\begin{pmatrix} f & . & g \\ f' & & g' \end{pmatrix}$ angedeutet, so ist umgekehrt der Übergang letzterer Form in die erstere mit $\begin{pmatrix} g' & . & -g \\ -f' & & f \end{pmatrix}$ vorzunehmen. Dass dies auch von den quadratischen Zahlformen gilt, bedarf wohl keines Beweises.

4. Permutation und Zeichenänderung bei den trinären Grössen.

a) Das Erste, was in dieser Beziehung in die Augen fällt ist, dass man bei den trinären Formen die Vorzeichen aller Coëfficienten in die entgegengesetzten verwandeln, d. h.

$$\begin{Bmatrix} m & . & m' & . & m'' \\ n & & n' & & n'' \end{Bmatrix} = \begin{Bmatrix} -m & . & -m' & . & -m'' \\ -n & & -n' & & -n'' \end{Bmatrix}$$

setzen kann, indem dadurch nach den Gleichungen (1) und (3) weder die Werthe noch die Vorzeichen von p, q, r und α, α', α'' eine Veränderung erleiden.

Dieses Verfahrens wird man sich bedienen, um unter den trinären Coëfficienten die wenigsten — Zeichen zu erhalten, oder falls die Zeichen in gleicher Anzahl erscheinen würden, um m, und wenn dieses $= 0$ wäre, um n positiv zu machen; so dass etwa statt

$$\begin{Bmatrix} -2 & & 1 & & 0 \\ -1 & \cdot & -3 & \cdot & 1 \end{Bmatrix}, \quad \begin{Bmatrix} -1 & & -1 & & 1 \\ 2 & \cdot & -2 & \cdot & 1 \end{Bmatrix}, \quad \begin{Bmatrix} 0 & & 2 & & -1 \\ -3 & \cdot & 0 & \cdot & 1 \end{Bmatrix}$$

beziehungsweise

$$\begin{Bmatrix} 2 & & -1 & & 0 \\ 1 & \cdot & 3 & \cdot & -1 \end{Bmatrix}, \quad \begin{Bmatrix} 1 & & 1 & & -1 \\ -2 & \cdot & 2 & \cdot & -1 \end{Bmatrix}, \quad \begin{Bmatrix} 0 & & -2 & & 1 \\ 3 & \cdot & 0 & & -1 \end{Bmatrix}$$

zu schreiben sein wird.

b) Ferner kann man in dem Ausdrucke

$$\begin{Bmatrix} m & & m' & & m'' \\ n & \cdot & n' & \cdot & n'' \end{Bmatrix} = < \alpha, \alpha', \alpha'' >$$

sämmtliche Glieder um einen Strich erhöhen oder gegen links verschieben, so dass derselbe in

$$\begin{Bmatrix} m' & & m'' & & m \\ n' & \cdot & n'' & \cdot & n \end{Bmatrix} = < \alpha', \alpha'', \alpha >$$

oder weiterhin in

$$\begin{Bmatrix} m'' & & m & & m' \\ n'' & \cdot & n & \cdot & n' \end{Bmatrix} = < \alpha'', \alpha, \alpha' >$$

übergeht, wobei keine Grösse ihre frühere Stellung behält. Dabei erleidet p, q, r keine Veränderung, und α, α', α'' werden nur versetzt. Diese Verschiebung werden wir eine gerade nennen. Sie dient dazu, um die trinären Werthe α, α', α'' so zu ordnen, dass sie numerisch betrachtet entweder steigen oder fallen.

So übergeht z. B.

$$\begin{Bmatrix} 0 & & 2 & & -1 \\ -1 & \cdot & 2 & \cdot & 3 \end{Bmatrix} = < 8, 1, 2 >, \quad \begin{Bmatrix} 1 & & 1 & & -1 \\ -2 & \cdot & 3 & \cdot & 0 \end{Bmatrix} = < 3, 2, 5 >$$

in

$$\begin{Bmatrix} 2 & & -1 & & 0 \\ 2 & \cdot & 3 & \cdot & -1 \end{Bmatrix} = < 1, 2, 8 >, \quad \begin{Bmatrix} -1 & & 1 & & 1 \\ 0 & \cdot & -2 & \cdot & 3 \end{Bmatrix} = < 5, 3, 2 >$$

c) Ändert eines der Coëfficientenpaare $\frac{m}{n}, \frac{m'}{n'}, \frac{m''}{n''}$ die Vorzeichen, so werden hiedurch auch bei zwei mit ihm ungleichstelligen trinären Werthen die Vorzeichen geändert, da man offenbar

$$\left\{\begin{matrix} -m & & m' & & m'' \\ -n & \cdot & n' & \cdot & n'' \end{matrix}\right\} = < \alpha, -\alpha', -\alpha'' >$$

erhält, was auch in den übrigen zwei Fällen geschieht. Kommen daher unter den Grössen α, α', α'' zwei negative vor, so können sie positiv gemacht werden. Auf diese Art übergeht z. B.

$$\left\{\begin{matrix} 1 & & 2 & & 2 \\ 0 & \cdot & -1 & \cdot & 3 \end{matrix}\right\} = < 8, -3, -1 >$$

in

$$\left\{\begin{matrix} -1 & & 2 & & 2 \\ 0 & \cdot & -1 & \cdot & 3 \end{matrix}\right\} = < 8, 3, 1 >$$

d) Durch die Versetzung von zwei Paaren der Grössen $\frac{m}{n}, \frac{m'}{n'}, \frac{m''}{n''}$ d. h. durch eine der unter *b)* angeführten entgegengesetzte oder verkehrte Verschiebung, werden auch die gleichstelligen trinären Werthe α, α', α'' versetzt, und es ändern überdies alle drei ihre Vorzeichen; was unter obiger Voraussetzung aus

$$\left\{\begin{matrix} m'' & & m' & & m \\ n'' & \cdot & n' & \cdot & n \end{matrix}\right\} = < -\alpha'', -\alpha', -\alpha >$$

erhellet.

Mittelst dieses Satzes kann man, wenn α, α', α'' sämmtlich negativ sind, dieselben positiv machen, ohne dass hiedurch die quadratische Zahlform $(p, 2q, r)$ eine Veränderung erleidet. Aus

$$\left\{\begin{matrix} 1 & & 1 & & -2 \\ 2 & \cdot & -3 & \cdot & -1 \end{matrix}\right\} = < -7, -3, -5 >$$

erhält man

$$\left\{\begin{matrix} 1 & & -2 & & 1 \\ 2 & \cdot & -1 & \cdot & -3 \end{matrix}\right\} = < 7, 5, 3 >;$$

die quadratische Zahlform ist in beiden Fällen $(6, 2, 14)$.

Wäre von den trinären Werthen blos einer negativ, so ist er leicht positiv zu machen; man verschiebt die Grössen verkehrt und ändert beim gleichstelligen Paare der trinären Coëfficienten die Zeichen. So übergeht

$$\begin{Bmatrix} 1 & 1 & 1 \\ -4 & \cdot 2 & \cdot 3 \end{Bmatrix} = < 1, -7, 6 > \text{ in } \begin{Bmatrix} 1 & 1 & -1 \\ -4 & \cdot 3 & \cdot -2 \end{Bmatrix} = < 1, 6, 7 >$$

e) Der Ausdruck

$$(p, 2q, r) = \begin{Bmatrix} m & & m' & & m'' \\ n & \cdot & n' & \cdot & n'' \end{Bmatrix} = < \alpha, \alpha', \alpha'' >$$

übergeht in

$$(p, -2q, r) = \begin{Bmatrix} m & & m' & & m'' \\ -n & \cdot & -n' & \cdot & -n'' \end{Bmatrix} = < -\alpha, -\alpha', -\alpha'' >$$

oder nach *d)* in

$$(p, -2q, r) = \begin{Bmatrix} m'' & & m' & & m \\ -n'' & \cdot & -n' & \cdot & -n \end{Bmatrix} = < \alpha'', \alpha', \alpha >.$$

Gehört demnach $< \alpha, \alpha', \alpha'' >$ einer positiven quadratischen Form an, so wird $< \alpha'', \alpha', \alpha >$ ihrer negativen zukommen. Bei Schluss- und Mittelformen braucht man daher weder auf die Stellung noch auf die Vorzeichen von α, α', α'' Rücksicht zu nehmen.

f) Hiebei wirft sich auch die Frage auf: wie viele Versetzungen mit Zeichenänderung man bei $< \alpha, \alpha', \alpha'' >$ vornehmen kann, ohne dass $(p, 2q, r)$ geändert wird? Dabei sind drei Fälle zu unterscheiden, u. z.

α. wenn α, α', α'' sämmtlich von einander verschieden sind, und weder einer Mittelform noch einer Schlussform zugehören, so kann die Anordnung derselben auf eine 24fache Art stattfinden. Ist nämlich α am ersten Platze und alle Zeichen positiv, so hat man blos die Versetzung $< \alpha, \alpha', \alpha'' >$. Bleibt α am ersten Platze und wird bei einer der Grössen das Zeichen geändert, so muss α' mit α'' versetzt werden; dies gibt

$$< -\alpha, \alpha'', \alpha' >, \quad < \alpha, -\alpha'', \alpha' >, \quad < \alpha, \alpha'', -\alpha' >.$$

Ferner kann man α, α', α'' an ihren Stellen belassen, und bei je zweien die Zeichen verändern; dies liefert

$< -\alpha, -\alpha', \alpha'' >$, $< -\alpha, \alpha', -\alpha'' >$, $< \alpha, -\alpha', -\alpha'' >$

Endlich kann α' mit α'' versetzt und bei allen drei Grössen das Zeichen geändert werden, was $< -\alpha, -\alpha'', -\alpha' >$ gibt. Man findet also aus $< \alpha, \alpha', \alpha'' >$ acht Versetzungen, bei denen α stets die erste Stelle einnimmt. Eben so geben $< \alpha', \alpha'', \alpha >$ und $< \alpha'', \alpha, \alpha' >$, wenn beziehungsweise die erste Stelle stets mit α' und α'' besetzt wird, je zu acht Versetzungen, so dass man die obangesetzte Zahl erhält.

β. Es sind oft α, α', α'' sämmtlich von einander verschieden, und gehören einer Mittelform an. Dann kann die Versetzung offenbar auf 48fache Art vorgenommen werden, da man hier das Vorzeichen von $2q$ in $(p, 2q, r)$ nicht zu beachten braucht. Dieses kann sich, wie die Folge lehren wird, blos bei Formen von den Gestalten $(2p, 2p, r)$, $(p, 2q, p)$ und (p, r), wenn $p > 2$ und $< \frac{1}{2} D$ ist, ereignen. Weil diese Formen auch andere Eigenthümlichkeiten besitzen, und da die Determinante mittelst derselben in zwei Factoren zerlegt (gespalten) wird, so legt ihnen Legendre den Namen bifid bei. Es zerfallen daher die Mittelformen in bifide und nicht bifide; zu den letzteren gehört $(2, 2, d)$ und $(2, d)$.

γ. Was die trinären Werthe $< 0, \alpha, \alpha' >$, $< \alpha, \alpha, \alpha' >$ anbelangt, gehören sie beziehungsweise zu

$$\begin{Bmatrix} 1 & 0 & 0 \\ 0 \cdot & \alpha' \cdot & -\alpha \end{Bmatrix} = (1, D), \quad \begin{Bmatrix} 1 & -1 & 0 \\ \alpha' \cdot & 0 \cdot & -\alpha \end{Bmatrix} = (2, 2\alpha', \alpha^2 + \alpha'^2),$$

und der Verlauf wird zeigen, dass quadratische Formen von der Gestalt $(1, D)$, $(2, d)$, $(2, 2, d)$ keine anderen trinären Formen und Werthe haben können. Die Anzahl der Versetzungen beträgt hier 24, da eines Theils das Vorzeichen von 0 nicht in Anschlag gebracht werden kann, und andern Theils α mit sich selbst versetzt werden darf, so dass immer zwei Versetzungen einander gleich werden.

1. Anmerkung. Mittelst der hier angeführten Regeln wird es leicht zu trinären wie immer geordneten und mit was immer für Vorzeichen versehenen Werthen einer Determinante mit Hilfe einer Tabelle, worin diese Grössen wohlgeordnet vorkommen, die Anordnung der trinären Coëfficienten zu finden. So hätte man z. B. zu $< 3, -5, 2 >$ die Coëfficienten anzugeben. In der Tabelle wäre bei

$$D = 38 \begin{Bmatrix} -1 & & 1 & & 1 \\ 0 & \cdot & -2 & \cdot & 3 \end{Bmatrix} = < 5, 3, 2 >$$

was

$$\begin{Bmatrix} 1 & & 1 & & 1 \\ -2 & \cdot & 0 & \cdot & 3 \end{Bmatrix} = < 3, -5, 2 >$$

gibt.

2. Anmerkung. Bei der Veränderung der trinären Arten hat man daher drei besondere Beziehungen zu beachten. Die erste derselben kann man Zeichnung (Zeichenänderung) nennen; sie findet Statt, wenn die trinären Werthe dieselbe Stellung behalten und nur in zwei Vorzeichen von einander verschieden sind. Hier gehört jede trinäre Art zu einer Gruppe von vier Complexionen. Eine zweite dieser Beziehungen ist die Verschiebung (Pkt. *b*), mittelst welcher $<\alpha, \alpha', \alpha''>$, $<\alpha', \alpha'', \alpha>$, $<\alpha'', \alpha, \alpha'>$ eine Gruppe bilden.

Die dritte kann füglich Verrückung (statt verkehrte Verschiebung) heissen, und um systemmässig zu verfahren, kann man annehmen, dass $<\alpha, \alpha', \alpha''>$ in dieser Hinsicht blos in $<-\alpha'', -\alpha', -\alpha>$ übergehe.

3. Anmerkung. Die weitere Entwicklung der hier angeführten Gedanken führte mich zur Lösung bestimmter Gleichungen des ersten Grades mit n Unbekannten mittelst der Permutationslehre (XXXIII. Band, S. 277 dieser Sitzungsberichte).

5. Verhältnisse zwischen den quadratischen Coëfficienten und den trinären Grössen.

a) Aus der Gleichung (3) folgt

$$m\alpha + m'\alpha' + m''\alpha'' = m\,(m'n'' - m''n') + m'\,(m''n - mn'') \\ + m''\,(mn' - m'n)$$

d. i. auch

$$m\alpha + m'\alpha' + m''\alpha'' = 0. \qquad (7)$$

Eben so findet man $n\alpha + n'\alpha' + n''\alpha'' = 0$. Daher besitzt jede in der Form $(p, 2q, r)$ enthaltene Zahl $N = a^2 + a'^2 + a''^2$ nach Gleichung (6) die Eigenschaft, dass bei derselben

(8) $$a\alpha + a'\alpha' + a''\alpha'' = 0$$

wird.

b) Die Gleichungen (3) zeigen, dass diejenigen Theiler, die m mit n, m' mit n' und m'' mit n'' gemeinschaftlich haben, beziehungsweise auch die Paare $\alpha'\alpha''$, $\alpha\alpha''$, $\alpha\alpha'$ haben müssen. Eben so ist umgekehrt aus den Gleichungen (7) ersichtlich, dass die gemeinschaftlichen Factoren von $\alpha\alpha'$, $\alpha\alpha''$, $\alpha'\alpha''$ beziehungsweise auch $m''n''$, $m'n'$, mn theilen werden, vorausgesetzt, dass man es hier mit eigentlichen trinären Formen und Werthen zu thun hat.

c) Aus den Gleichungen (3) folgt ferner

$$\alpha^2 + \alpha'^2 = (m'n'' - m''n')^2 + (m''n - mn'')^2 = (m^2 + m'^2 + m''^2)\, n''^2$$
$$- 2\,(mn + m'n' + m''n'')\, n''m'' + (n^2 + n'^2 + n''^2)\, m''^2,$$

so dass man

(9) $$\alpha^2 + \alpha'^2 = pn''^2 - 2qn''m'' + rm''^2$$

erhält, was bei

$$\alpha = ac \quad , \quad \alpha' = a'c,$$

somit nach *b)*

$$m'' = \mu''c \quad , \quad n'' = \nu''c$$

in

(10) $$a^2 + a'^2 = p\nu''^2 - 2q\nu''\mu'' + r\mu''^2$$

übergeht. Ähnliches ergibt sich auch für $\alpha^2 + \alpha''^2$ und $\alpha'^2 + \alpha''^2$, so wie bei $a^2 + a''^2$ und $a'^2 + a''^2$.

d) Ferner erhält man auch

$$m'\alpha'' - m''\alpha' = m'(mn' - m'n) - m''(m''n - mn'')$$
$$= m\,(m'n' + m''n'') - n\,(m'^2 + m''^2)$$

was in Folge der Gleichung (1) in $m'\alpha'' - m''\alpha' = qm - pn$ übergeht, so dass man mittelst höherer Streichung auch zu

$$m''\alpha - m\alpha'' = qm' - pn', \quad m\alpha' - m'\alpha = qm'' - pn''$$

gelangt. Wird nun der Kürze halber

$$\eta = m'\alpha'' - m''\alpha', \quad \eta' = m''\alpha - m\alpha'', \quad \eta'' = m\alpha' - m'\alpha \tag{11}$$

gesetzt, so hat man

$$\eta = qm - pn, \quad \eta' = qm' - pn', \quad \eta'' = qm'' - pn'' \tag{12}$$

und es kann überdies nach Analogie der Gleichung (5) und in Folge der Gleichung (7)

$$< \eta, \eta', \eta'' > = \left\{ \begin{matrix} m & m' & m'' \\ \alpha & \alpha' & \alpha'' \end{matrix} \right\} = (p, D) \tag{13}$$

genommen werden, so dass sich nach Gleichung (4)

$$pD = \eta^2 + \eta'^2 + \eta''^2 \tag{14}$$

ergibt.

Ist, wie es sich im Verlaufe einmal ereignet, $p, q, m, m', m'', \alpha, \alpha', \alpha''$ bekannt, so findet man

$$n = \frac{mq - \eta}{p}, \quad n' = \frac{m'q - \eta'}{p}, \quad n'' = \frac{m''q - \eta''}{p}. \tag{15}$$

e) Aus dem eben Angeführten ergibt sich weiterhin

$$\eta\eta' + \alpha\alpha' p = - mm'D. \tag{16}$$

Setzt man nämlich rücksichtlich des Beweises $\eta\eta' + \alpha\alpha' p = X$, so hat man nach Gleichung (11)

$$\begin{aligned} X &= (m'\alpha'' - m''\alpha')\ (m''\alpha - m\alpha'') + \alpha\alpha'\ (m^2 + m'^2 + m''^2) \\ &= (m\alpha' + m'\alpha)\ m''\alpha'' - mm'\alpha''^2 + m^2\alpha\alpha' + m'^2\ \alpha\alpha' \end{aligned}$$

Die Gleichung (7) liefert jedoch

$$(m\alpha' + m'\alpha)\ m''\alpha'' = -\ (m\alpha' + m'\alpha)\ (m\alpha + m'\alpha'),$$

so dass

$$X = - mm'\alpha''^2 - mm'\alpha'^2 - mm'\alpha^2 = - mm'D$$

wird, woraus der obige Satz hervorgeht.

f) Es wäre zu wünschen, dass man einer jeden quadratischen Zahlform $(p, 2q, r)$, bei der dies überhaupt möglich ist, leicht die trinäre Gestalt geben könnte. Bis jetzt gehört aber diese Aufgabe zu den schwierigeren in der unbestimmten Analytik. Ist jedoch p eine nicht gar grosse Zahl, so dass es entweder nur eine oder einige wenige trinäre Arten, die hier für m, m', m'' zu nehmen sind, besitzt, so kann man n, n', n'' auf folgende Weise ermitteln: Nach Gleichung (9) hat man

$$D - \alpha^2 = pn^2 - 2qnm + rm^2$$

also

$$\alpha^2 = D - rm^2 - (pn^2 - 2qm \,.\, n),$$

woraus mittelst Reihen des zweiten Grades die Unbekannten n, α zu ermitteln sind. Ist dies geschehen, so ergibt sich

$$n' = \frac{m'(q - mn) - m''\alpha}{p - m^2} \text{ und } n'' = \frac{m''(q - mn) + m'\alpha}{p - m^2}$$

wobei das Vorzeichen von α so zu nehmen ist, dass n', n'' ganze Zahlen werden.

Es folgt nämlich aus den Gleichungen (11) (12)

$$n'p - m'q = m\alpha'' - m''\alpha = m(mn' - m'n) - m''\alpha$$

oder

$$n'(p - m^2) = m'(q - mn) - m''\alpha,$$

was n' gibt. Eben so lässt sich auch die Gleichung für n'' erweisen.

Es wäre z. B. bei $D = 734$ die Form $(22, 12, 35)$; so hat man hier $m = 3$, $m' = 3$, $m'' = 2$ und die zu lösende Gleichung ist

$$\alpha^2 = 419 - (22n^2 - 36n),$$

der bei $n = 5$ und $\alpha = \pm 7$ Genüge geleistet wird; daher findet man $n' = -1$, $n'' = -3$ und $\alpha = -7$, so dass

$$(22, 12, 35) = \begin{Bmatrix} 3 & . & 3 & . & 2 \\ 5 & & -1 & & -3 \end{Bmatrix} = \langle -7, 19, -18 \rangle$$

oder geordnet

$$\begin{Bmatrix} -3 & . & 2 & . & 3 \\ 1 & & -3 & & 5 \end{Bmatrix} = \langle 19, 18, 7 \rangle$$

zum Vorschein kommt.

6. Methoden, aus den trinären Werthen die trinären Formen zu finden.

Hier handelt es sich darum, aus den Grössen α, α', α'' die Coëfficienten m, m', m'' und n, n', n'' zu bestimmen. Sind, wie es meistens geschieht, von den drei Grössen m, m', m'' zwei etwa m', m'' prim zu einander, oder kann man sie prim machen, so reicht hiezu die Gleichung (7) und eine der Gleichungen (3) etwa $m'n'' - m''n' = \alpha$ aus; man erhält nämlich hieraus $\alpha \equiv m'n''$, $\alpha m + \alpha' m' \equiv 0$ (Mod. m''), dies gibt ferner $mm'n'' + \alpha' m' \equiv 0$, und da m', m'' relative Primzahlen sind, $mn'' + \alpha' \equiv 0$ (Mod. m'') was $n = \frac{\alpha' + mn''}{m''}$ als eine ganze Zahl liefert, wie es die zweite der Gleichungen (3) fordert. Substituirt man die Werthe von α, α' in die Gleichung (7), so gibt sie $\alpha'' = mn' - m'n$, und eben so zeigt es sich, dass $\alpha n + \alpha' n' + \alpha'' n'' = 0$ blos eine Folge der obigen zwei Gleichungen ist.

Nur dann würden die zwei angeführten Gleichungen zur vollständigen Bestimmung der trinären Coëfficienten nicht ausreichen, wenn man etwa $m' = c\mu'$, $m'' = c\mu''$ also auch $\alpha = ca$ erhalten würde. In diesem Falle übergeht die Gleichung $m'n'' - m''n' = \alpha$ in $\mu'n'' - \mu''n' = a$, was etwa $n' = \mu't + \nu'$, $n'' = \mu''t + \nu''$ liefert, wobei ν', ν'' sich als bekannt ergeben, t aber noch zu bestimmen ist. Dies geschieht mittelst $\alpha' = m''n - mn''$, woraus man $\alpha' \equiv - mn''$ (Mod. c) oder $\alpha' \equiv - m\mu''t - mn''$ oder $m\mu''t \equiv -(\alpha' + m\nu'')$ zur Berechnung von t erlangt. Es wird daher am gerathensten sein, m', m'' als prim zu einander zu nehmen.

Da nun fünf Grössen blos durch zwei Gleichungen zu bestimmen sind, so kann man einer dieser Gleichungen durch Annahme Genüge leisten, die zweite muss hingegen als diophantisch verrechnet werden. Den sechsten Coëfficienten findet man aus einer der Gleichungen (3).

Dies vorausgeschickt kann man die gegebene Aufgabe nach folgenden Methoden lösen:

I. Methode. Diese ist der Legendre'schen (Nr. 270, 271) ähnlich, und beruht im nachstehenden Verfahren: Sind π, ρ, σ beziehungsweise die grössten gemeinsamen Theiler von

$$\alpha'\alpha'', \quad \alpha\alpha'', \quad \alpha\alpha'$$

so kann man

$$\alpha = \rho\sigma a, \quad \alpha' = \pi\sigma a', \quad \alpha'' = \pi\rho a''$$

setzen; in Folge dessen ist nach 5. *b)*

$$m = \pi\mu, \quad m' = \rho\mu', \quad m'' = \sigma\mu''.$$

Der Gleichung $mn' - m'n = \alpha''$ leistet man dadurch Genüge, dass $n = o$, $n' = \rho a''$, $\mu = 1$ gesetzt wird. Die Gleichung (7) übergeht in

$$a + a'\mu' + a''\mu'' = 0$$

und liefert die Werthe von μ', μ''. Was n'' anbelangt, findet man es aus der zweiten der Gleichungen (3) $= - \sigma a'$. Man gelangt daher zu

$$< \alpha, \alpha', \alpha'' > = \begin{Bmatrix} \pi & . & \rho\mu' & . & \sigma\mu'' \\ 0 & . & \rho a'' & . & -\sigma a' \end{Bmatrix}$$

So sind z. B. bei $D = 2569$ die trinären Werthe $< 12, 20, 45 >$, folglich hat man

$$\pi = 5, \ \rho = 3, \ \sigma = 4,$$

daher auch

$$a = 1, \ a' = 1, \ a'' = 3,$$

und es gibt die Gleichung $1 + \mu' + 3\mu'' = 0$, $\mu' = -1$, $\mu'' = 0$. Somit ist die trinäre Form $\begin{Bmatrix} 5 & . & -3 & . & 0 \\ 0 & . & 9 & . & -4 \end{Bmatrix}$, welche gekürzt die Gestalt

$$(34, 14, 77) = \begin{Bmatrix} 5 & . & -3 & . & 0 \\ 5 & . & 6 & . & -4 \end{Bmatrix} = < 12, 20, 45 >$$

erhält.

Diese Methode wird dann von Vortheil sein, wenn α, α', α'' etwas grössere gemeinsame Theiler besitzen.

II. Methode. Der Gleichung (7) kann dadurch Genüge geleistet werden, dass man

$$m = -\frac{\alpha'}{h}, \quad m' = \frac{\alpha}{h}, \quad m'' = 0$$

setzt, wo h den grössten gemeinschaftlichen Theiler von α, α' vorstellt, so dass also m, m' prim zu einander sind. Bestimmt man hierauf n, n' aus $mn' - m'n = 1$, so ist

$$<\alpha, \alpha', \alpha''> = \left\{\begin{matrix} m & & m' & & 0 \\ & \cdot & & \cdot & \\ \alpha''n & & \alpha''n' & & h \end{matrix}\right\}.$$

Wollte man auch zugleich die quadratische Zahlform haben, so ist dieselbe, wenn $q = mn + m'n'$, dann $r = n^2 + n'^2$ gesetzt wird

$$= (m^2 + m'^2, 2\alpha''q, h^2 + r\alpha''^2).$$

Bei $D = 286$ ist z. B. die trinäre Art $<6, 9, 13>$, daher bei $\alpha = 6$, $\alpha' = 9$, $h = 3$, $m = -3$, $m' = 2$, $n = 1$, $n' = -1$ also die trinäre Form

$$\left\{\begin{matrix} -3 & & 2 & & 0 \\ & \cdot & & \cdot & \\ 13 & & -13 & & 3 \end{matrix}\right\}$$

oder gekürzt

$$<6, 9, 13> = \left\{\begin{matrix} 3 & & -2 & & 0 \\ & \cdot & & \cdot & \\ 2 & & 3 & & -3 \end{matrix}\right\} = (13, 22).$$

Am brauchbarsten ist diese Methode dann, wenn α, α' entweder klein sind, oder einen grossen gemeinsamen Theiler besitzen.

III. Methode. Ist h der grösste gemeinschaftliche Theiler von $\alpha' - \alpha''$, $\alpha'' - \alpha$, $\alpha - \alpha'$, so wird der Gleichung (7) entsprochen bei

$$m = \frac{\alpha' - \alpha''}{h}, \quad m' = \frac{\alpha'' - \alpha}{h}, \quad m'' = \frac{\alpha - \alpha'}{h};$$

zwei von den Coëfficienten n, n', n'' gibt eine der Gleichungen (3) und den dritten findet man aus $n + n' + n'' = -h$; aus

$$\alpha = \frac{\alpha'' - \alpha}{h} n'' - \frac{\alpha - \alpha'}{h} n'$$

folgt nämlich $\alpha h = \alpha'n' + \alpha''n'' - \alpha(n' + n'')$, da man aber nach Gleichung (7) $\alpha'n' + \alpha''n'' = -\alpha n$ hat, so ist

$$\alpha h = -\alpha(n + n' + n''):$$

was den obigen Ausdruck liefert. So erhält man bei $D = 819$ aus

$$< 13, 17, 19 > \; h = 2 \quad \begin{matrix} m = -1, & m' = 3, & m'' = -2 \\ n = -5, & n' = -4, & n'' = 7 \end{matrix}$$

was gekürzt

$$(14, 14, 62) = \begin{Bmatrix} 1 & . & -3 & . & 2 \\ 7 & & -2 & & -3 \end{Bmatrix} = < 13, 17, 19 >$$

gibt.

Dieses Verfahren ist bedeutend bequem, besonders wenn $\alpha, \alpha', \alpha''$ grosse nicht weit von einander abstehende Zahlen sind.

Von untergeordneter Bedeutung ist die IV. Methode. Hier wird

$$m = \frac{\alpha' - \alpha''}{h}, \quad m' = -\frac{\alpha + \alpha''}{h}, \quad m'' = \frac{\alpha + \alpha'}{h}$$

gesetzt, und zur Berechnung des dritten der unteren Coëfficienten dient $n - n' - n'' = h$. Die Ableitung ist dieselbe wie bei der dritten Methode.

Ähnliches gilt bei der V. Methode. Man hat da

$$m = -\frac{\alpha' + \alpha''}{h}, \quad m' = \frac{\alpha}{h}, \quad m'' = \frac{\alpha}{h};$$

n und n'' findet man aus $m''n - mn'' = \alpha'$ und $n' = n'' - h$. An diese reiht sich noch eine VI. Methode, worin

$$m = \frac{\alpha''}{h}, \quad m' = -\frac{\alpha''}{h}, \quad m'' = \frac{\alpha' - \alpha}{h}$$

genommen, n und n'' aus $m''n - mn'' = \alpha'$ berechnet wird, und $n' = h - n$ sich ergibt.

1. Anmerkung. Eine Methode aufzufinden, bei der man keine diophantische Gleichung zu lösen hätte, gelang es mir trotz vieler Mühe nicht; so eine Gleichung scheint daher zum Wesen dieser Verrechnungen zu gehören.

2. Anmerkung. Ausser der ersten sind alle diese Methoden auch bei uneigentlichen trinären Werthen brauchbar. Nebst dem lassen sie sich in ein allgemeines Verfahren zusammenfassen; setzt man nämlich

$$m = \frac{\alpha' t + \alpha'' u}{h}, \quad m' = \frac{\alpha t' + \alpha'' u'}{h}, \quad m'' = \frac{\alpha t'' + \alpha' u''}{h}$$

so wird der Gleichung

$$\alpha\,(\alpha' t + \alpha'' u) + \alpha'\,(\alpha t' + \alpha'' u') + \alpha''\,(\alpha t'' + \alpha' u'') = 0$$

entsprochen bei

$$t + t' = t'' + u = u' + u'' = 0$$

und die angeführten Methoden hängen von der Bestimmung der Grössen t, t', t'', u, u', u'' ab, so dass man z. B. für die V. Methode

$$t = -1, \quad u = -1, \quad t' = 1, \quad u' = 0, \quad t'' = 1, \quad u'' = 0$$

hat. Die obige Anordnung dieser Methoden rührt von dem Grade ihrer Brauchbarkeit her.

7. Zu einer eigentlichen trinären Art gehört nur eine trinäre Form.

Dieser Satz will sagen, dass man aus $< \alpha, \alpha', \alpha'' >$, wenn diese Grössen keinen gemeinsamen Theiler haben, mag man nach welcher Methode immer verfahren, oder die unbestimmten Grössen in der diophantischen Gleichung wie immer nehmen, stets zu einer und derselben trinären Form gelangt, d. h. dass sich die verschiedenen Gestalten der Resultate stets in einander umwandeln lassen. Findet man nämlich aus den obangeführten trinären Werthen die zwei Formen

$$\begin{Bmatrix} m & & m' & & m'' \\ n & \cdot & n' & \cdot & n'' \end{Bmatrix}, \quad \begin{Bmatrix} M & & M' & & M'' \\ N & \cdot & N' & \cdot & N'' \end{Bmatrix},$$

so haben für beide Classen von Coëfficienten die Gleichungen in 1. und 5. ihre Richtigkeit, und bei diesem Umstande sind nicht nur

$$f = \frac{M'n'' - M''n'}{\alpha} = \frac{M''n - Mn''}{\alpha'} = \frac{Mn' - M'n}{\alpha''}$$

$$g = \frac{N'n'' - N''n'}{\alpha} = \frac{N''n - Nn''}{\alpha'} = \frac{Nn' - N'n}{\alpha''}$$

$$f' = \frac{m'M'' - m''M'}{\alpha} = \frac{m''M - mM''}{\alpha'} = \frac{mM' - m'M}{\alpha''}$$

$$g' = \frac{m'N'' - m''N'}{\alpha} = \frac{m''N - mN''}{\alpha'} = \frac{mN' - m'N}{\alpha''}$$

wirkliche Gleichungen, sondern die Grössen f, g, f', g' sind auch ganze Zahlen.

Um den ersten Theil darzuthun, kann man sich der Deutlichkeit halber einer Beweisart bedienen, die in der Algebra zwar selten üblich, jedoch immerhin zulässig ist. Man setze die ersten Glieder der ersten Gleichung unter die Frage, dann ist

$$\alpha' M' n'' - \alpha' M'' n' = \alpha M'' n - \alpha M n''?$$

dies gibt auch

$$n''(\alpha M + \alpha' M') = M''(\alpha n + \alpha' n')?$$

woraus man nach Gleichung (7) $-n''\alpha'' M'' = -M''\alpha'' n''$ erhält, so dass das Fragezeichen verschwindet; und da nichts im Wege steht, wesshalb man in den Gleichungen nicht zurück gehen könnte, so wird auch die erste richtig sein. Auf dieselbe Art lässt sich erweisen, dass $\frac{M''n - Mn''}{\alpha'} = \frac{Mn' - M'n}{\alpha''}$, und dass auch die übrigen Formeln richtig sind.

Die Grössen f, g, f', g' sind aber auch ganze Zahlen; nimmt man nämlich an, dass $f = \frac{\varphi}{\psi}$ wäre, wo φ, ψ prim zu einander sind, und setzt man Kürze halber

$$L = M'n'' - M''n', \; L' = M''n - Mn'', \; L'' = Mn' - M'n,$$

dann hat man nach den obigen Gleichungen

$$\alpha\varphi = L\psi, \quad \alpha'\varphi = L'\psi, \quad \alpha''\varphi = L''\psi,$$

und es müssten gegen die Annahme α, α', α'' den gemeinsamen Theiler ψ haben. Eben so zeigt es sich, dass g, f', g' ganze Zahlen sein müssen.

Aus den angeführten vier Gleichungen folgt weiter

$$\begin{aligned}
\alpha f \,.\, \alpha' g' - \alpha' f'' \,.\, \alpha g &= (M'n'' - M''n')(m''N - mN'') \\
&\quad - (m''M - mM'')(N'n'' - N''n') \\
&= m''n''(M'N - MN') - mn''(M'N'' - M''N') - m''n'(M''N - MN'') \\
&= -m''n''\alpha'' - mn''\alpha - m''n'\alpha' = n''(m\alpha + m'\alpha') - mn''\alpha - m''n'\alpha' \\
&= m'n''\alpha' - m''n'\alpha' = \alpha\alpha'
\end{aligned}$$

also

$$fg' - f'g = 1.$$

Ferner findet man auch aus jenen Formeln

$$mf + nf' = \frac{1}{\alpha'} (mnM'' - mn'' M + m''nM - mnM'') = M$$

und eben so ergibt sich

$$m'f + n'f' = M' \; . \; m''f + n''f' = M''$$
$$mg + ng' = N. \; m'g + m'g' = N', \; m''g + n''g' = N''$$

Es ist daher die Form $\left\{\begin{matrix} M & . & M' & . & M'' \\ N & & N' & & N'' \end{matrix}\right\}$ wie es aus Gleichung (6) zu ersehen, aus $\left\{\begin{matrix} m & . & m' & . & m'' \\ n & & n' & & n'' \end{matrix}\right\}$ mittelst des Ausdrucks $\left(\begin{matrix} f & . & g \\ f' & & g' \end{matrix}\right)$ abgeleitet, und eine kann auf die andere leicht gebracht werden.

Die Grössen f, g, f', g' findet man am bequemsten mittelst der Formeln

$$\left\{\begin{matrix} M & . & M' & . & M'' \\ n & & n' & & n'' \end{matrix}\right\} = <\alpha f, \alpha' f, \alpha'' f>$$

$$\left\{\begin{matrix} N & . & N' & . & N'' \\ n & & n' & & n'' \end{matrix}\right\} = <\alpha g, \alpha' g, \alpha'' g>$$

$$\left\{\begin{matrix} m & . & m' & . & m'' \\ M & & M' & & M'' \end{matrix}\right\} = <\alpha f', \alpha' f', \alpha'' f'>$$

$$\left\{\begin{matrix} m & . & m' & . & m'' \\ N & & N' & & N'' \end{matrix}\right\} = <\alpha g', \alpha' g'. \alpha'' g'>$$

So liefert z. B. bei $<2, 3, 5>$ die erste Methode $\left\{\begin{matrix} 1 & . & 1 & . & -1 \\ 0 & & 5 & & -3 \end{matrix}\right\}$ und die zweite $\left\{\begin{matrix} -3 & . & 2 & . & 0 \\ 5 & & -5 & & 1 \end{matrix}\right\}$, die Verwandlung geschieht hier mittelst $\left(\begin{matrix} -3 & . & 5 \\ 1 & & -2 \end{matrix}\right)$.

1. Anmerkung. Hieraus folgt nicht, dass zu einer quadratischen Zahlform nicht mehrere trinäre gehören könnten. Wie gross die Anzahl der trinären Formen und somit auch trinärer Arten ist, die zu einer quadratischen Zahlform gehören, wird der Gegenstand weiterer Untersuchungen sein.

2. Anmerkung. Nach diesem Satze kann ich nicht anders als die Ansicht (Legendre Nr. 273), dass eine und dieselbe Art eigentlicher trinärer Werthe zu zwei trinären Formen gehören könne, für unstatthaft erklären. Legendre führt als Beispiel an, dass $5y^2 + 4yz + 5z^2$ die zwei trinären Formen $(2y + z)^2 + y^2 + 4z^2$ und $(y + 2z)^2 + z^2 + 4y^2$, welche den Werthen $< 4, 2, 1 >$ zugehören, besitze. Nach der hier eingeführten Bezeichnungsweise ist jedoch

$$\begin{Bmatrix} 2 & & 1 & & 0 \\ 1 & \cdot & 0 & \cdot & 2 \end{Bmatrix} = < 2, -4, -1 >$$

und

$$\begin{Bmatrix} 1 & & 0 & & 2 \\ 2 & \cdot & 1 & \cdot & 0 \end{Bmatrix} = < -2, 4, 1 >$$

Soll aber die zweite Form zu den Werthen der ersten gehören, so müssen darin die Zeichen geändert werden, so dass eigentlich

$$\begin{Bmatrix} 1 & & 0 & & 2 \\ -2 & \cdot & -1 & \cdot & 0 \end{Bmatrix} = < 2, -4, -1 >$$

zu setzen ist, was bei $\begin{pmatrix} 0 & & 1 \\ -1 & \cdot & 0 \end{pmatrix}$ in die erste übergeht.

Folgesatz. Hat man demnach bei den trinären Werthen $\alpha, \alpha', \alpha''$ sowohl die Ordnung als auch die Vorzeichen bestimmt, und ist die Form $(p, 2q, r) = \begin{Bmatrix} m & & m' & & m'' \\ n & \cdot & n' & \cdot & n'' \end{Bmatrix}$ eine reducirte, so kann keiner der trinären Coëfficienten mehr als einen Werth besitzen.

Wird dann $(p, 2q, r)$ in eine andere quadratische und daher auch trinäre Form

$$(p', 2q', r') = \begin{Bmatrix} a & & a' & & a'' \\ b & \cdot & b' & \cdot & b'' \end{Bmatrix}$$

verwandelt, so werden auch hier die Coëfficienten blos je einen Werth haben können.

Dies ist Grund genug, dass man in Perioden und Periodensystemen, wenn

$$fe = (p, 2q, r), \text{ auch } fe = \begin{Bmatrix} m & & m' & & m'' \\ n & \cdot & n' & \cdot & n'' \end{Bmatrix} \text{ und } fe = < \alpha, \alpha', \alpha'' >$$

setzen darf, falls nur $< \alpha, \alpha', \alpha'' >$ eigentliche trinäre Werthe sind,

8. Kennzeichen der uneigentlichen trinären Formen.

Jede uneigentliche trinäre Form und nur sie hat uneigentliche trinäre Werthe, so dass in dieser Hinsicht die trinären Werthe ein charakteristisches Kennzeichen der Formen sind. Ist nämlich in

$$px^2 + 2qxy + ry^2 = (mx + ny)^2 + (m'x + n'y)^2 + (m''x + n''y)^2$$

die trinäre Form eine uneigentliche, so müssen die drei Wurzeln nach 1. für gewisse Werthe von x, y einen gemeinschaftlichen Theiler haben; es kann daher etwa

$$mx + ny = ga, \quad m'x + n'y = ga', \quad m''x + n''y = ga''$$

gesetzt werden. Hat x mit g den grössten gemeinschaftlichen Divisor h, d. h. ist $x = hx'$, $g = hg'$, so muss, weil x, y prim zu einander sind, wie dies überall bei den quadratischen Formen vorausgesetzt wird, n, n', n'' durch h theilbar sein, und man hat

$$n = hb, \quad n' = hb', \quad n'' = hb'';$$

daraus folgt

$$\alpha = m'n'' - m''n' = h\,(m'b'' - m''b') = hk,$$

und eben so $\alpha' = hk'$, $\alpha'' = hk''$, wobei also

$$k = m'b'' - m''b', \quad k' = m''b - mb'', \quad k'' = mb' - m'b$$

vorstellt. Werden ferner die obigen Wurzeln durch h abgekürzt, so ist

$$mx' + by = g'a, \quad m'x' + b'y = g'a', \quad m''x' + b''y = g'a''.$$

Eliminirt man y aus diesen Gleichungen, so gibt die zweite und dritte $(m'b'' - m''b')\;x' = g'\;(a'b'' - a''b') = kx'$, und da g', x' prim zu einander sind, so muss k durch g' aufgehen, und man hat $k = g'\beta$, folglich $\alpha = hk = hg'\beta$ oder $\alpha = g\beta$. Eben so erhält man aus der ersten und dritten der obigen Gleichungen $\alpha' = g\beta'$, dann aus der ersten und zweiten $\alpha'' = g\beta''$. Somit haben die trinären Werthe einen gemeinschaftlichen Factor und zwar denselben, der die drei Wurzeln der trinären Form theilt.

Auch die propositio inversa dieses Satzes lässt sich erweisen, nämlich dass die Wurzeln $mx + ny$, $m'x + n'y$, $m''x + n''y$ für gewisse Werthe von x, y den gemeinsamen Theiler g erhalten, wenn $\alpha = g\beta$, $\alpha' = g\beta'$, $\alpha'' = g\beta''$. Es haben nämlich die Gleichungen (11) und (12) auch bei uneigentlichen trinären Formen Giltigkeit, so dass $qm - pn = m'\alpha'' - m''\alpha' = gk$, daher auch $qm' - pn' = gk'$ und $qm'' - pn'' = gk''$ zum Vorschein kommt. Sind nun t, t' was immer für ganze Zahlen, so ergibt sich bei $x = gt + q$, $y = gt' - p$ $mx + ny = g\,(mt + nt' + k) = gA$ und eben so $m'x + n'y = gA'$, $m''x + n''y = gA''$.

Anmerkung. Es steht nichts im Wege, warum nicht eine quadratische Zahlform in eine eigentliche und zugleich auch in eine uneigentliche trinäre zerlegt werden könnte; so ist z. B.

$$(5, 9) = \begin{Bmatrix} 2 & \cdot & -1 & \cdot & 0 \\ 1 & & 2 & & -2 \end{Bmatrix} = <2.\ 4,\ 5>$$

$$(5, 9) = \begin{Bmatrix} 0 & \cdot & -2 & \cdot & 1 \\ 3 & & 0 & & 0 \end{Bmatrix} = <0,\ 3,\ 6>$$

Folgesatz. Die Form $(pl,\ 2ql,\ rl)$ kann nur in eine uneigentliche trinäre verwandelt werden. Ist nämlich l gerade, so folgt dies aus 2., da die Determinante durch 4 theilbar ist. Was jedoch ein ungerades l anbelangt, so gibt die Gleichung (9)

$$\alpha'^2 + \alpha''^2 = D - \alpha^2 \equiv 0 \text{ (Mod. } l);$$

wäre daher auch $l = k^2 l'$, und l' durch kein Quadrat theilbar, so muss wenigstens $\alpha \equiv 0$ (Mod. kl') sein, was auch offenbar wegen $\alpha^2 + \alpha''^2 = D - \alpha'^2 \equiv 0$ (Mod. l) von α' und α'' gelten wird.

So hat man z. B.

$$(27,\ 18,\ 45) = \begin{Bmatrix} 5 & \cdot & 1 & \cdot & -1 \\ 0 & & 6 & & -3 \end{Bmatrix} = <3,\ 15,\ 30>$$

9. Wie viele und welche quadratischen und trinären Formen haben dieselben uneigentlichen trinären Werthe?

Soll diese Abhandlung so viel als möglich vollständig sein, so darf auch die obangeführte Frage nicht übergangen werden. Die Antwort hierauf lautet: Haben die uneigentlichen trinären Werthe α, α', α'' den grössten gemeinsamen Theiler S, so dass also DS^2 die Determinante ist, dann kommen dieselben in

$$k = \left[s - \left(\frac{-D}{s}\right)\right]\left[s' - \left(\frac{-D}{s'}\right)\right]\left[s'' - \left(\frac{-D}{s''}\right)\right] \text{u. s. w.}$$

von einander verschiedenen quadratischen und trinären Formen vor, falls $S = ss's'' \ldots$ und $s, s', s'', \ldots$ Primzahlen sind. Die Grösse $\left(\frac{-D}{s}\right)$ ist nach Legendre $\equiv (-D)^{\frac{s-1}{2}}$ (Mod. s), und wird $= 0$ genommen, wenn $s = 2$ oder ein Theiler von D ist. Was den Fall anbelangt, wo $D = 1$ und S eine Primzahl bedeutet, so erscheinen die trinären Werthe $< 0, 0, S >$ in $2k$ Formen, falls $k = \frac{S \pm 1}{4}$ eine ganze Zahl ist.

Man hat hier nämlich $\alpha = \beta S$, $\alpha' = \beta' S$, $\alpha'' = \beta'' S$, und β, β', β'' sind eigentliche trinäre Werthe der Determinante D, so dass man nach 6. zu dem Ausdrucke

$$(p, 2q, r) = \left\{ \begin{matrix} m & . & m' & . & m'' \\ n & & n' & & n'' \end{matrix} \right\} = < \beta, \beta', \beta'', >$$

gelangt. Hieraus erhält man nach Lipschitz[1]) mittelst der Substitutionen

$$\begin{pmatrix} 1 & . & 0 \\ 0 & & s \end{pmatrix}, \begin{pmatrix} 0 & . & -s \\ 1 & & 0 \end{pmatrix}, \begin{pmatrix} 1 & . & -s \\ 1 & & 0 \end{pmatrix}, \begin{pmatrix} 2 & . & -s \\ 1 & & 0 \end{pmatrix} \cdot \cdot \begin{pmatrix} s-1 & . & -s \\ 1 & & 0 \end{pmatrix}$$

bei den obigen Annahmen im Ganzen $s - \left(\frac{-D}{s}\right)$ neue, von einander verschiedene, quadratische Formen. Jeder dieser quadratischen Formen entspricht auch eine trinäre, etwa $\left\{ \begin{matrix} M & . & M' & . & M'' \\ N & & N' & & N'' \end{matrix} \right\}$, da man bei der ersten Substitution

$$M = m \ , \ M' = m' \ , \ M'' = m''$$

und

$$N = ns \ , \ N' = n's \ , \ N'' = n''s,$$

bei jeder der übrigen aber, die man im Allgemeinen mit $\begin{pmatrix} v & . & -s \\ 1 & & 0 \end{pmatrix}$ bezeichnen kann

[1]) Crelle's Journal. Bd. LIII, Nr. 14.

$$M = mv + n, \quad M' = m'v + n', \quad M'' = m''v + n''$$
$$N = -ms, \quad N' = -m's, \quad N'' = -m''s$$

erhält. In allen Fällen sind daher βs, $\beta' s$, $\beta'' s$ trinäre Werthe der Determinante Ds^2.

Verfährt man mit der Primzahl s' gerade so, wie mit s, so erhält man aus jeder quadratischen, und eben so aus jeder trinären Form der Determinante Ds^2 wieder $s' - \left(\frac{-D}{s'}\right)$ Formen zur Determinante $Ds^2s'^2$, u. s. w. bis man zur obangesetzten Menge gelangt.

So kommen z. B. bei $DS^2 = 2475$ wegen $D = 11$, $S = 15$ die trinären Werthe $< 15, 15, 45 >$ in acht quadratischen Formen vor.

II. Reciprocität der trinären Grössen.

10. Von den Reciprocitäts-Verhältnissen überhaupt.

Da dieser Gegenstand in seiner Allgemeinheit bisher noch nicht genügend erörtert ist, was vor der Auffindung der Periodicität der quadratischen Zahlformen nicht leicht geschehen konnte; so wird es nicht am unrechten Orte sein, hier darüber mehr anzuführen, als gerade der Zweck dieser Abhandlung erheischt.

a) Eine Hauptrolle spielt hiebei das von Legendre aufgestellte und von Gauss gründlich erwiesene Reciprocitätsgesetz. Nach demselben besteht zwischen zwei ungeraden Primzahlen k, p das Verhältniss, dass

$$\left(\frac{k}{p}\right) = (-1)^{\frac{k-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{k}\right),$$

wenn Kürze halber $\left(\frac{k}{p}\right)$ den kleinsten Rest, den $k^{\frac{p-1}{2}}$ nach dem Mod. p gibt, bedeutet, so dass also $\left(\frac{k}{p}\right)$ entweder $+1$ oder -1 ist. Was $k = 2$ anbelangt, ist bei $p = 8\varphi \pm 1$ stets $\left(\frac{2}{p}\right) = 1$, bei $p = 8\varphi \pm 3$ hingegen $\left(\frac{2}{p}\right) = -1$.

Nach dieser Bemerkung und den bei Legendre Nr. 135 angeführten Sätzen wird es dann leicht von zwei relativen Primzahlen a, b zu entscheiden, ob die eine ein quadratischer Rest nach der andern ist, oder nicht. Heisst nämlich b' welche immer in b aufgehende Primzahl, so findet ersteres Statt, wenn man stets $\left(\frac{a}{b'}\right) = 1$ hat, sonst stellt a einen Nichtrest nach b vor.

Der Ausdruck „a ist ein quadratischer Rest oder Nichtrest nach b" — ist identisch mit dem Satze: „b ist eine bei der positiven Determinante a vorkommende Zahl oder nicht." Ist nämlich a ein quadratischer Rest nach b, so gilt die Congruenz $a \equiv c^2$ (Mod. b); diese liefert die Gleichung $a = c^2 + bd$, woraus man die Form $(b, 2c, -d)$ erhält, die b enthält, und zur positiven Determinante a gehört. Wäre $a = c^2 + 4bd$, so hat man auch die Form $(b, c, -d)$, wo c ungerade ist.

Dasselbe findet auch bei der negativen Determinante a Statt, wo b eine ihrer Formzahlen ist oder nicht ist, wenn $-a$ einen Rest oder Nichtrest nach b vorstellt; indem aus $-a \equiv c^2$ (Mod. b) die Gleichung $a = bd - c^2$ und weiterhin die Form $(b, 2c, d)$ hervorgeht.

b) Legendre nennt einen reciproken Theiler denjenigen quadratischen Theiler der Form $t^2 + Du^2$, der die Eigenschaft besitzt, dass für jede in jenem Theiler enthaltene Zahl N umgekehrt D ein Theiler von $t^2 + Nu^2$ sei. Im Gegentheil nennt er einen quadratischen Theiler nicht reciprok, wenn er diese Eigenschaft nicht besitzt.

Dieser Begriff ist jedoch offenbar zu enge. Warum sollten nur quadratische Formen (nach Legendre quadratische Theiler von $t^2 + Du^2$) reciprok sein, und nicht Zahlen überhaupt? Oder ist dies blos bei negativen Determinanten der Fall und nicht auch bei positiven?

Es wird daher am zweckmässigsten sein, D und N dann reciprok zu nennen, wenn N eine in den quadratischen Formen der Determinante D vorkommende Zahl ist, und wenn zugleich auch D bei der Determinante N erscheint.

Ist keine von den Grössen D, N durch 4 theilbar und sind sie entweder selbst oder ihre Hälften prim zu einander, so sind sie nach *a)* reciprok, wenn sie wechselweise quadratische Reste nach einander sind. Ist eine ein Nichtrest nach der andern, so kommt ihnen diese Eigenschaft nicht zu. Wäre eine von ihnen durch 4 theilbar, so wie auch wenn beide einen ungeraden Theiler gemein hätten, dann müsste ihre Reciprocität anderweitig erwiesen werden.

c) Nach dieser Definition der Reciprocität wird es zwei Hauptfälle derselben geben; entweder sind D, N sogenannte negative Determinanten quadratischer Zahlformen, und dieser Umstand ist bei den trinären Formen von grosser Bedeutung; oder stellen D, N positive Determinanten vor. Man könnte wohl noch einen dritten Fall unterscheiden, nämlich wenn D positiv und N negativ wäre; dieser ist jedoch im vorhergehenden enthalten, da in den Formen positiver Determinanten auch negative Zahlen vorkommen, wo hingegen die Formen negativer Determinanten blos positive Zahlen enthalten können.

d) Ist in der Form $px^2 + 2qxy + ry^2$, mag dieselbe einer positiven oder negativen Determinante angehören, p zu D oder $\frac{1}{2} D$ prim und zugleich auch mit D reciprok, so besitzen alle zu D und falls es gerade wäre, alle zu $\frac{1}{2} D$ relativen Primzahlen diese letztere Eigenschaft, und es kann diese Form eine reciproke genannt werden. Umgekehrt ist eine Form nicht reciprok, wenn darin eine nicht reciproke Zahl vorkommt, die zu D oder $\frac{1}{2} D$ prim ist. Ist nämlich $N = px^2 + 2qxy + ry^2$, so erhält man

$$pN = (px + qy)^2 \mp Dy^2 = k^2 \mp Dy^2.$$

Stellt nun d was immer für eine in D aufgehende ungerade Primzahl vor, so erhält man

$$\left(\frac{pN}{d}\right) = \left(\frac{k^2}{d}\right) = 1 \text{ also } \left(\frac{\pm N}{d}\right) = \left(\frac{\pm p}{d}\right)$$

Ist daher $\left(\frac{\pm p}{d}\right) = 1$, so stellt $\pm p$ also auch $\pm N$ einen quadratischen Rest nach d demnach auch nach D vor, und es ist nicht nur N eine Zahl der Determinante D, sondern auch umgekehrt D eine Zahl von $\pm N$, d. h. D und N sind reciprok. Wäre jedoch $\left(\frac{\pm p}{d}\right) = -1$, so kann weder p noch N zu D reciprok sein.

So findet man bei $D = 99$ die Form $2x^2 + 2xy + 50y^2$ als reciprok; es hat nämlich d hier die Werthe 3 und 11, und man erhält $\left(\frac{-2}{3}\right) = \left(\frac{-2}{11}\right) = 1$.

Eben so sind bei der positiven Determinante $D = 106$ alle positiven und negativen Zahlen der Form $7x^2 + 2xy - 15y^2$ mit Ausnahme der durch 53 theilbaren zu 106 reciprok, weil $\left(\frac{7}{53}\right) = 1$ ist.

c) Haben zwei Zahlen D und N einen gemeinschaftlichen Theiler, so können sie reciprok sein ohne dass desshalb die Formen, in denen sie vorkommen, diese Eigenschaft besitzen müssten. So findet man bei $D = 15$, $N = 51$

$$51 = -x^2 + 15\,y^2 \text{ bei } x = 3,\, y = 2$$

und

$$15 = -x^2 + 51\,y^2 \text{ für } x = 6,\, y = 1,$$

wo weder die eine noch die andere Form reciprok ist, da z. B. die erstere bei $x = 2$, $y = 1$, $N' = 11$ gibt, und $\left(\frac{11}{3}\right) = -1$ liefert. Ähnliches kommt bei den negativen Determinanten $D = 21$, $N = 66$ vor.

Die negativen Determinanten haben, wie sich weiterhin ergeben wird, die Eigenschaft, dass auch Zahlen, die zu D oder $\frac{1}{2}D$ nicht prim sind, die Reciprocität besitzen, wenn sie in reciproken Formen vorkommen. Bei positiven Determinanten ist dies jedoch nicht immer der Fall. So ist z. B. bei $D = 34$ die Form $-2x^2 + 17y^2$ reciprok, und doch lässt sich die Gleichung $34 = x^2 - 17y^2$ nicht in ganzen Zahlen lösen.

f) Wird der 15. Abschnitt meiner im XXXI. Bande, Nr. 18 dieser Berichte vorkommenden Abhandlung mit Bezug auf *c)* allgemeiner aufgefasst, so ist im Periodensysteme die Form $fn + 2m$ reciprok oder nicht reciprok, wenn es fn beziehungsweise ist. Sind nun D, N relative Primzahlen, so erhält man aus $N = x^2 - Dy^2$ für jede Primzahl d, die in D aufgeht $\left(\frac{N}{d}\right) = \left(\frac{x^2}{d}\right) = 1$. Demnach sind bei positiven Determinanten nicht nur alle Schlussformen sondern überhaupt alle Formen mit geraden Zeigern reciprok. So hat z. B. $D = 79$ eine Periode von sechs Gliedern, nämlich

$$f1 = (3,2,-26), f2 = (5,4,-15), f3 = (-1,79), f6 = (1,-79)$$

hievon sind $f2$, $f6$ reciprok, $f1$, $f3$ aber nicht. Nur im ersten Reciprocitätsfalle erscheinen reciproke Formen auch mit unpaaren Zeigern.

Diesen Satz findet man im Crelle'schen Journal, 56. Band, 1. Heft, Seite 73 von Arndt mit den Worten: „Durch eine gegebene eigentlich primitive (positive) Form von der durch kein Quadrat theilbaren Determinante D, kann, wenn sie im Hauptgeschlecht ist, immer ein Quadrat dargestellt werden, welches zugleich prim gegen D ist" — ausgedrückt. Die vorstehende Theorie liefert ihn offenbar kürzer und allgemeiner.

Anmerkung. Mehreres über diesen Gegenstand, besonders was die linearen Formen der reciproken und nicht reciproken Grössen anbelangt, hoffe ich in einer eigenen Abhandlung über die Congruenzen höherer Grade (die Potenzrestenperioden), wo dergleichen Sätze deutlicher erörtert werden können, demnächst zu veröffentlichen.

II. Die eigentlichen trinären Formen sind reciprok.

Lässt sich der Form $(p, 2q, r)$ bei der Determ. $D = pr - q^2$, wo p zu D oder $\frac{1}{2} D$ prim ist, eine trinäre Gestalt geben, so folgt aus Gleichung (9) $\alpha'^2 + \alpha''^2 = pn^2 - 2qnm + rm^2$, was auch in $p(D - \alpha^2) = (pn - qm^2) + Dm^2$ und nach Gleichung (12) in $D(p - m^2 - p\alpha^2 = \eta^2$ übergeht. Diese Gleichung gibt, wenn d was immer für eine in D aufgehende Primzahl darstellt, die Congruenz $-p\alpha^2 \equiv \eta^2$ (Mod. d). Eben so erhält man bei demselben Modell auch $-p\alpha'^2 \equiv \eta'^2$, $-p\alpha''^2 \equiv \eta''^2$. Ist nun die trinäre Form eine eigentliche, so können nach 8. die Grössen α, α', α'' nicht zugleich durch d theilbar sein; wäre daher α zu d prim, so hat man $\left(\frac{-p\alpha^2}{d}\right) = \left(\frac{\eta^2}{d}\right) = 1$, also auch $\left(\frac{-p}{d}\right) = 1$. Dasselbe ereignet sich bei jedem Werthe von d; es ist also $-p$ ein quadratischer Rest nach D, und D ist in den Formen der negativen Determinante p enthalten, d. h. p und D sind reciprok, was die Form $(p, 2q, r)$ als eine reciproke charakterisirt. Was die uneigentlichen trinären Formen anbelangt, so lassen sich bei ihnen obige Schlüsse nicht anwenden, dieselben können daher trinär sein, ohne desshalb reciprok sein zu müssen, wie sich dies z. B. bei

$$D = 275, (18, 14, 18) = \left\{\begin{matrix} 1 \\ 4 \end{matrix} \cdot \begin{matrix} -4 \\ -1 \end{matrix} \cdot \begin{matrix} 1 \\ -1 \end{matrix}\right\} = \langle 5, 5, 15 \rangle$$

wegen $\left(\frac{-18}{5}\right) = -1$ ereignet.

Daraus erhellet auch, dass nur reciproke Formen eigentlich trinär sein können. Die propositio inversa — nämlich dass jede reciproke Form auch eine eigentliche trinäre ist, d. h. dass eigentlich trinär und reciprok (bei negativen Determinanten) gleichbedeutende Ausdrücke sind, ist zwar auch richtig, muss jedoch eigens erwiesen werden.

12. Reciprocitäts-Verhältnisse der trinären Formen.

Nach der ersten Anmerkung in 7. können zu einer quadratischen Zahlform mehrere trinäre Formen, daher auch mehrere trinäre Arten gehören; es wird demnach deutlicher sein, von der Reciprocität der trinären Arten als von derselben Eigenschaft der quadratischen Zahlformen, denen jene trinären Arten zugehören, zu handeln.

a) In dieser Beziehung enthält die Gleichung

$$\alpha A + \alpha' A' + \alpha'' A'' = 0$$

das charakteristische Merkmal der Reciprocität der trinären Art $\langle \alpha, \alpha', \alpha'' \rangle$ bei der Determinante D mit $\langle A, A', A'' \rangle$ bei N; denn dieselbe hat erstens ihre Giltigkeit, so oft N eine Zahl von der Form $(p, 2q, r) = \langle \alpha, \alpha', \alpha'' \rangle$ ist, und zweitens besteht die obige Gleichung, so ist $N = A^2 + A'^2 + A''^2$ eine Zahl aus der Form $(p, 2q, r) = \langle \alpha, \alpha', \alpha'' \rangle$ und umgekehrt $D = \alpha^2 + \alpha'^2 + \alpha''^2$ eine Grösse, die in $(a, 2b, c) = \langle A, A', A'' \rangle$ vorkommt.

Was den ersten Theil anbelangt, so ist aus Gleichung (8) leicht zu ersehen, dass wenn bei der Determinante D in der Form

$$(p, 2q, r) = \left\{\begin{matrix} m \\ n \end{matrix} \cdot \begin{matrix} m' \\ n' \end{matrix} \cdot \begin{matrix} m'' \\ n'' \end{matrix}\right\} = \langle \alpha, \alpha', \alpha'' \rangle$$

die Zahl $N = pf^2 + 2qfg + rg^2$ erscheint, die Werthe

$$A = mf + ng, \quad A' = m'f + n'g, \quad A'' = m''f + n''g$$

der angeführten Bedingung genügen.

Dem zu Folge bleibt nur der zweite Theil oder die propositio inversa zu erweisen übrig, und es sind in dieser Beziehung bei der üblichen Bedeutung der trinären Coëfficienten nach einer, der in 7. auseinander gesetzten, ganz analogen Schlussweise nicht nur

$$f = \frac{A'n'' - A''n'}{\alpha} = \frac{A''n - An''}{\alpha'} = \frac{An' - A'n}{\alpha''}$$
$$g = \frac{A''m' - A'm''}{\alpha} = \frac{Am'' - A''m}{\alpha'} = \frac{A'm - Am'}{\alpha''}$$

vollkommene Gleichungen, sondern auch f, g ganze Zahlen. Hieraus folgt $An' - A'n = \alpha''f$ und $A'm - Am' = \alpha''g$, woraus sich durch Elimination von A', $A\,(mn' - m'n) = \alpha''A = \alpha''\,(fm + gn)$ oder $A = fm + gn$, daher auch $A' = fm' + gn'$, $A'' = fm'' + gn''$ ergibt. Es ist also

$$A^2 + A'^2 + A''^2 = (m^2 + m'^2 + m''^2)\,f^2 + 2\,(mn + m'n' + m''n'')\,fg + (n^2 + n'^2 + n''^2)\,g^2$$

oder

$$N = pf^2 + 2q\,fg + rg^2.$$

Auf dieselbe Art folgt auch aus der Form

$$(a, 2b, c) = \left\{ \begin{matrix} \mu \\ \nu \end{matrix} \;.\; \begin{matrix} \mu' \\ \nu' \end{matrix} \;.\; \begin{matrix} \mu'' \\ \nu'' \end{matrix} \right\} = \langle A, A', A'' \rangle$$

bei $N = ac - b^2$, wenn

$$\varphi = \frac{\alpha'\nu'' - \alpha''\nu'}{A} = \frac{\alpha''\nu - \alpha\nu''}{A'} = \frac{\alpha\nu' - \alpha'\nu}{A''}$$

und

$$\psi = \frac{\alpha''\mu' - \alpha'\mu''}{A} = \frac{\alpha\mu'' - \alpha''\mu}{A'} = \frac{\alpha'\mu - \alpha\mu'}{A''}$$

gesetzt wird, $\alpha = \mu\varphi + \nu\psi$, $\alpha' = \mu'\varphi + \nu'\psi$, $\alpha'' = \mu''\varphi + \nu''\psi$, so dass

$$D = a\varphi^2 + 2b\,\varphi\psi + c\psi^2.$$

So sind bei $D = 77$, $N = 41$ die Formen

$$\langle 2, 3, 8 \rangle = \left\{\begin{matrix} 1 & & 2 & & -1 \\ -3 & \cdot & 2 & \cdot & 0 \end{matrix}\right\} = (6, 2, 13)$$

$$\langle -1, 6, -2 \rangle = \left\{\begin{matrix} -2 & & 0 & & 1 \\ 2 & \cdot & 1 & \cdot & 2 \end{matrix}\right\} = (5, -4, 9)$$

reciprok, und es ist $f = 2$, $g = 1$, $\varphi = 2$, $\psi = 3$; man findet aber auch noch

$$\langle 4, 5, 6 \rangle = \left\{\begin{matrix} 1 & & -2 & & 1 \\ 3 & \cdot & 0 & \cdot & -2 \end{matrix}\right\} = (6, 2, 13)$$

$$\langle 5, -4, 0 \rangle = \left\{\begin{matrix} 0 & & 0 & & -1 \\ 4 & \cdot & 5 & \cdot & 0 \end{matrix}\right\} = (1, 41);$$

woraus man ersieht, dass $(6, 2, 13)$ mit $(5, -4, 9)$ und $(1, 41)$ zugleich reciprok ist, dass hingegen der trinären Art $\langle 2, 3, 8 \rangle$ blos $\langle -1, 6, -2 \rangle$ und eben so $\langle 4, 5, 6 \rangle$ blos $\langle 5, -4, 0 \rangle$ entspricht.

Bei Legendre (Nr. 283) kommt dieser Satz mit folgenden Worten ausgedrückt vor: Ist die Zahl N in einem trinären Theiler der Form $t^2 + Du^2$ enthalten, so kommt wieder umgekehrt die Zahl D in einem trinären Theiler der Form $t^2 + Nu^2$ vor, und es sind überdies die correspondirenden trinären Werthe von N und D dieselben, mag man N als Theiler von $t^2 + Du^2$ oder D als Theiler von $t^2 + Nu^2$ ansehen. — Übrigens überzeugt man sich leicht, dass hier sowohl die Auffassung als auch die Durchführung des besagten Theorems eine ganz andere ist.

b) Eine Folge des eben behandelten Satzes ist die, dass wenn von zwei reciproken quadratischen Formen eine trinär ist, die andere auch trinär sein muss; wäre nämlich das Erstere bei $(p, 2q, r)$ der Fall, und hätte man $N = pf^2 + 2q\,fg + rg^2$, so ergeben sich hieraus bei der Determinante N die trinären Werthe A, A', A'', welche die Form $(a, 2b, c) = \left\{\begin{matrix} \mu & & \mu' & & \mu'' \\ \nu & \cdot & \nu' & \cdot & \nu'' \end{matrix}\right\}$ liefern.

c) Die Reciprocitätswerthe, d. i. die Grössen f, g, φ, ψ, mittelst welcher N in der reciproken Form von D und umgekehrt enthalten ist, lassen sich nach der hier üblichen Bezeichnungsweise mittelst der Ausdrücke

$$\left\{\begin{matrix} A & . & A' & . & A'' \\ n & & n' & & n'' \end{matrix}\right\} = < \alpha f,\ \alpha' f,\ \alpha'' f >$$

$$\left\{\begin{matrix} m & . & m' & . & m'' \\ A & & A' & & A'' \end{matrix}\right\} = < \alpha g,\ \alpha' g,\ \alpha'' g >$$

$$\left\{\begin{matrix} \alpha & . & \alpha' & . & \alpha'' \\ \nu & & \nu' & & \nu'' \end{matrix}\right\} = < A\varphi,\ A'\varphi,\ A''\varphi >$$

$$\left\{\begin{matrix} \mu & . & \mu' & . & \mu'' \\ \alpha & & \alpha' & & \alpha'' \end{matrix}\right\} = < A\psi,\ A'\psi,\ A''\psi >$$

leicht bestimmen; übrigens findet man für dieselben auch nach *a)* die Formeln

$$-\frac{f}{g} = \frac{n\mu + n'\mu' + n''\mu''}{m\mu + m'\mu' + m''\mu''} = \frac{n\nu + n'\nu' + n''\nu''}{m\nu + m'\nu' + m''\nu''}$$

$$-\frac{\varphi}{\psi} = \frac{m\nu + m'\nu' + m''\nu''}{m\mu + m'\mu' + m''\mu''} = \frac{n\nu + n'\nu' + n''\nu''}{n\mu + n'\mu' + n''\mu''}$$

wobei die Brüche nöthigen Falls abzukürzen sind, damit $\frac{f}{g}$, $\frac{\varphi}{\psi}$ mit den kleinsten Zahlen erscheinen.

d) Übersichtlich lässt sich das Reciprocitäts-Verhältniss von D, N mittelst der Gleichungen

$$D = Nr - q^2,\ (N, 2q, r) = \left\{\begin{matrix} A & . & A' & . & A'' \\ n & & n' & & n'' \end{matrix}\right\} = < \alpha, \alpha', \alpha'' >$$

$$N = Dc - b^2,\ (D, 2b, c) = \left\{\begin{matrix} \alpha & . & \alpha' & . & \alpha'' \\ \nu & & \nu' & & \nu'' \end{matrix}\right\} = < A, A', A'' >$$

darstellen, wo $f = \varphi = 1$ und $g = \psi = 0$ wird. Dabei kommt noch der Umstand vor, dass stets $n\nu + n'\nu' + n''\nu'' = -1$ ist; denn aus den Gleichungen

$$A = \alpha'\nu'' - \alpha''\nu',\ \ \alpha' = A''n - An'',\ \ \alpha'' = An' - A'n$$

folgt $A = A''\nu''n - An''\nu'' - An'\nu' + A'n\nu'$, was wegen

$$A''\nu'' + A'\nu' = -A\nu,\ \ A = -A\,(n\nu + n'\nu' + n''\nu'')$$

gibt.

13. Eigenthümlichkeit der Formen von der Gestalt (p, pk, r).

a) Der Gleichung $N = px^2 + pk\,xy + ry^2$ kann man, mag p was immer für eine ganze positive oder negative Zahl sein, auch die Gestalt $N = p(x + ky)^2 - pk(x + ky)\,y + ry^2$ geben; ist sie daher bei $x = f$, $y = g$ lösbar, so wird dies auch bei $x = f + gk$ und $y = -g$ stattfinden; oder mit anderen Worten, jede Grösse, die darin mit $\frac{f}{g}$ vorkommt, wird auch das Werthepaar $\frac{f + gk}{-g}$ besitzen, und nur für $g = 0$ übergehen beide Paare in $\frac{1}{0}$, da bekanntlich bei diesen Untersuchungen x, y stets prim zu einander sind.

Besonders auffallend erscheint dieser Umstand bei $N = P$, $2P$ oder überhaupt P^m, $2P^m$, wenn die besagte Form einer negativen Determinante angehört, und die ungerade Primzahl P in D nicht aufgeht. Hat dann die obige Form eine Gestalt, an der man es nicht absieht, dass sie eine Schluss- oder Mittelform ist, so kommt in derselben N mit zwei von einander verschiedenen Werthepaaren vor, wo es in jedem andern Falle nur e i n Werthepaar besitzen kann. So ist z. B. $11x^2 + 36xy + 30y^2 = 101$ lösbar bei $-\frac{11}{5}$ und $-\frac{17}{9}$. Mehr als zweimal kann N, wenn es die obigen Eigenschaften besitzt, in (p, pk, r) nicht vorkommen; denn die Gleichung $Nc - b^2 = D$ ist nur für e i n $b < \frac{1}{2} D$ lösbar, was die Doppelform $(N, \pm 2b, c)$ liefert.

A n m e r k u n g. Die weitere Erörterung dieses Satzes besonders in Hinsicht der positiven Determinanten gehört in die Lehre von den unbestimmten Gleichungen.

b) Ist die obangeführte Form eine trinäre, und hat man

$$(p, pk, r) = \begin{Bmatrix} m & . & m' & . & m'' \\ n & & n' & & n'' \end{Bmatrix} = \langle \alpha, \alpha', \alpha'' \rangle,$$

so ergeben sich hieraus für jedes $N = pf^2 + pkfg + rg^2$ zwei Arten trinärer Werthe, nämlich eine bei $x = f$, $y = g$ und die zweite bei $x = f + gk$, $y = -g$; sie sind

$$A = mf + ng, \qquad A' = m'f + n'g, \qquad A'' = m''f + n''g$$
$$B = m(f+gk) - ng,\ B' = m'(f+gk) - n'g,\ B'' = m''(f+gk) - n''g.$$

Die trinäre Art $\langle \alpha, \alpha', \alpha'' \rangle$ ist demnach sowohl mit $\langle A, A', A'' \rangle$ als auch mit $\langle B, B', B'' \rangle$ reciprok, und besitzt daher, so oft diese zwei trinären Arten von einander verschieden sind, doppelte Reciprocität.

c) Die trinären Arten $<A, A', A''>$, $<B, B', B''>$ sind gleich, wenn $p < 3$ ist, oder mit anderen Worten: die Formen $(1, D)$, $(2, d)$ und $(2, 2, d)$ liefern, wenn sie trinär sind, zu einem Werthepaar $\frac{f}{g}$ auch nur eine trinäre Form für N.

Rücksichtlich der ersten Form hat man nach 6.

$$(1, D) = \begin{Bmatrix} 1 & . & 0 & . & 0 \\ 0 & & n & & -m \end{Bmatrix} = <0, m, n>$$

hieraus folgt für $k = 0$

$$\begin{aligned} A &= f, & A' &= gn, & A'' &= -gm \\ B &= f, & B' &= -gn, & B'' &= gm \end{aligned}$$

Eben so ergibt sich aus

$$(2, d) = \begin{Bmatrix} 1 & . & -1 & . & 0 \\ n & & n & & -m \end{Bmatrix} = <m, m, 2n>$$

wegen $k = 0$

$$\begin{aligned} A &= f + gn, & A' &= -f + gn, & A'' &= -gm \\ B &= f - gn, & B' &= -f - gn, & B'' &= gm \end{aligned}$$

und aus

$$(2, 2, d) = \begin{Bmatrix} 1 & . & -1 & . & 0 \\ n+1 & & n & & -m \end{Bmatrix} = <m, m, 2n+1>$$

bei $k = 1$

$$\begin{aligned} A &= f + g + gn, & A' &= -f + gn. & A'' &= -gm \\ B &= f - gn, & B' &= -f - g - gn, & B'' &= gm. \end{aligned}$$

In allen drei Fällen sind daher diese trinären Arten einander gleich und zwar in der Weise, dass sie sich, nach 4. betrachtet, nicht einmal im Vorzeichen des Mittelgliedes der quadratischen Zahlform, welcher sie angehören, von einander unterscheiden.

d) Ist $p > 2$ und $N > \frac{2}{3} D$, so sind die trinären Arten $<A, A', A''>$, $<B, B', B''>$ stets unter einander verschieden.

Um diesen Satz darzuthun, kann man sich des von Legendre (Nr. 285) erwiesenen Theorems bedienen, das in die hier übliche Ausdrucksweise übersetzt lautet: „Lässt sich der Form $px^2 + 2qxy + ry^2$, die der Determinante D angehört, auf mehrfache Art eine trinäre Gestalt geben, und wird hiebei $x = f$, $y = g$ gesetzt, so sage ich, dass die trinären Werthe der Zahl $N = pf^2 + 2qfg + rg^2$ sämmtlich von einander verschieden sind, oder dass im Gegentheil N nicht $\frac{2}{3}$ D übersteigen könne."

Man kann nämlich hier der Zahlform (p, pk, r) ausser der trinären Gestalt $\left\{\begin{matrix} m \\ n \end{matrix} \cdot \begin{matrix} m' \\ n' \end{matrix} \cdot \begin{matrix} m'' \\ n'' \end{matrix}\right\}$ noch die zweite

$$\left\{\begin{matrix} m \\ mk - n \end{matrix} \cdot \begin{matrix} m' \\ m'k - n' \end{matrix} \cdot \begin{matrix} m'' \\ m''k - n'' \end{matrix}\right\}$$

geben; denn es ist

$$2\ (m^2 + m'^2 + m''^2)\ k - 2\ (mn + m'n' + m''n'') = 2pk - pk$$

und

$$(m^2 + m'^2 + m''^2)\,k^2 - 2\,(mn + m'n' + m''n'')\,k + n^2 + n'^2 + n''^2 = r$$

und beide trinären Formen sieht Legendre als wesentlich von einander verschieden an, so dass man seinen Ausdruck $\left\{\begin{matrix} \mu \\ \nu \end{matrix} \cdot \begin{matrix} \mu' \\ \nu' \end{matrix} \cdot \begin{matrix} \mu'' \\ \nu'' \end{matrix}\right\}$ für eine Versetzung der zweiten trinären Form ansehen kann.

Dies ist eine zweite Eigenthümlichkeit der bifiden Formen (4. β), wodurch sie sich von allen anderen unterscheiden.

Anmerkung. Hieraus folgt jedoch nicht, dass man bei bifiden Formen durch die obige Substitution immer, so oft $N < \frac{2}{3} D$ ist, blos eine trinäre Art für N erhält, da $\frac{2}{3} D$ nur die Grenze ist, über welche hinaus obbesagte Gleichheit nicht stattfinden kann. So ergibt sich bei $D = 235$ aus

$$(10,\ 10,\ 26) = \left\{\begin{matrix} 3 \\ 3 \end{matrix} \cdot \begin{matrix} -1 \\ 4 \end{matrix} \cdot \begin{matrix} 0 \\ -1 \end{matrix}\right\} = \langle 1,\ 3,\ 15 \rangle$$

für $f = 2$, $g = 1$ also $N = 86$, $\langle 9, 2, -1 \rangle$ und $\langle 6, -7, 1 \rangle$

14. Jede reciproke Form ist eine trinäre.

Dieser Satz gilt bei den Determinanten 1, 2, 3; denn man hat bei

$$D = 1,\ (1,\ 1) = \begin{Bmatrix} 1 & & 0 & & 0 \\ & \cdot & & \cdot & \\ 0 & & 1 & & 0 \end{Bmatrix} = < 0,\ 0,\ 1 >$$

$$D = 2,\ (1,\ 2) = \begin{Bmatrix} 1 & & 0 & & 0 \\ & \cdot & & \cdot & \\ 0 & & 1 & & -1 \end{Bmatrix} = < 0,\ 1,\ 1 >$$

$$D = 3,\ (2,\ 2,\ 2) = \begin{Bmatrix} 1 & & 0 & & -1 \\ & \cdot & & \cdot & \\ 0 & & 1 & & -1 \end{Bmatrix} = < 1,\ 1,\ 1 >$$

und diese Determinanten haben sonst keine anderen reciproken Formen. Es ist daher immerhin erlaubt anzunehmen, dass er seine Giltigkeit bei allen reciproke Formen besitzenden Determinanten von 1 bis zu einer gewissen Grenze M habe. Wäre nun N die zunächst höhere Zahl, bei der eine reciproke Form etwa $(a,\ 2b,\ c)$ vorkommt, so wird es darin nach Legendre (Nr. 410 etc.) eine Zahl D geben, die kleiner als N und zu N oder $\frac{1}{2}N$ prim ist. Diese ist daher mit N reciprok, und es kommt N in einer ihrer reciproken Formen, d. i. etwa in $(p,\ 2q,\ r)$ vor. Aber $(p,\ 2q,\ r)$ ist zugleich auch trinär, weil der Annahme gemäss $D \leqq M$ ist; folglich muss nach 12. *b)* auch $(a,\ 2b,\ c)$ trinär sein. Somit besitzt jede reciproke Form bei N und daher auch bei jeder höheren Determinante die obige Eigenschaft.

Anmerkung. Da jede in einer reciproken Form negativer Determinante vorkommende Zahl, wenn sie auch nicht zur Determinante prim wäre, der Bedingungsgleichung in 12. *a)* Genüge leistet, so sind in den reciproken Formen alle Zahlen reciprok. Desshalb ist es blos in theoretischer Beziehung nothwendig, dass D zu N oder $\frac{1}{2}N$ prim sei.

15. Folgesätze.

a) Mittelst der Theorie der sogenannten linearen Theiler von $t^2 + Du^2$ lässt sich nachweisen, dass jede Zahl D von einer der drei Gestalten $4\varphi + 1$, $4\varphi + 2$ und $8\varphi + 3$ reciproke Grössen besitze; sie wird daher auch reciproke d. i. trinäre Formen und trinäre Werthe haben, und lässt sich in die Summe aus drei Quadraten zerlegen.

b) Weil reciprok und trinär gleichbedeutende Ausdrücke sind, so kann eine Determinante von der Gestalt $8\varphi + 7$ keine reciproken Formen haben, da sie keine trinären Werthe besitzt.

c) Da die reciproken Formen der Determinante $8\varphi + 3$ die Gestalt $(2p, 2q, 2r)$, wo p, q, r ungerade sind, besitzen, und die Formen von $4\varphi + 1$ und $4\varphi + 2$, wenn x, y prim zu einander sind, keine durch 4 theilbare Zahl enthalten; so kann ein ungerades oder doppelt ungerades N nicht mit $4D$ in der eigentlichen Bedeutung reciprok sein.

d) Jede Zahl lässt sich in die Summe von vier Quadraten zerlegen. Ein Satz, den schon Fermat entdeckt hat.

16. Jede eigentliche quadratische Zahlform enthält unendlich viele Primzahlen.

In der Form $ax^2 + bxy + cy^2$ werden um so sicherer Primzahlen vorkommen, wenn schon $ax^2 + bx + c$ derartige Grössen besitzt. Hat man nun die Gleichung $ax^2 + bx + c = pz$, wo p eine ungerade Primzahl ist, so lassen sich in $x \equiv 0, 1, 2, \ldots (p-1)$ (Mod. p) nicht mehr und nicht weniger als zwei Werthe von x finden, die ihr genügen; es verbleiben also in jenen Grenzen noch $p - 2$ Werthe für x, bei denen die Form keine durch p theilbare Zahl enthält. Setzt man daher für x nach einander alle natürlichen Zahlen von 0 bis w, wo w sehr gross gedacht werden kann, so ist bei einem positiven x die Anzahl der durch p untheilbaren Werthe von $ax^2 + bx + c$ gleich

$$\frac{w}{p}(p-2) = w\left(1 - \frac{2}{p}\right).$$

Es kann zwar auch x negativ genommen werden, da jedoch die obige Form manchmal dieselben Zahlen liefert, die bei einem positiven x vorkommen, so mag dieser Fall hier unberührt bleiben. Unter den obigen $w\left(1 - \frac{2}{p}\right)$ Werthen sind ihrer in Bezug auf eine andere Primzahl p' stets von $x \equiv 0$ bis $x \equiv p' - 1$ (Mod. p') abermals $p' - 2$ untheilbar, daher enthält die Form zum wenigsten $w\left(1 - \frac{2}{p}\right)\left(1 - \frac{2}{p'}\right)$ Werthe, die zu pp' prim sind. Verfährt man so fort, und heisst s die Anzahl der Werthe obiger Form, die sich durch keine der Primzahlen 2, p, p', p'', ... theilen lassen, so erhält man, weil von ihnen offenbar nicht mehr als die Hälfte gerade sein kann, den Ausdruck

$$s \overline{\gtrless} \frac{w}{2}\left(1-\frac{2}{p}\right)\left(1-\frac{2}{p'}\right)\left(1-\frac{2}{p''}\right)\cdot\;\cdot\;\cdot\;\cdot$$

Nimmt man hier den äussersten Fall an, nämlich dass $p, p', p'', \ldots$ alle Primzahlen ohne Unterschied darstellen, so ist offenbar

$$s > \frac{1}{2}w\frac{1}{3}\times\frac{3}{5}\times\frac{5}{7}\times\frac{9}{11}\times\frac{11}{13}\cdot\;\cdot\;\cdot\;\cdot$$

d. i. auch

$$\frac{7}{9}\times\frac{13}{15}\times\frac{19}{21}\times\;\cdot\;\cdot\;\times s > \frac{1}{2}w\frac{1}{3}\times\frac{3}{5}\times\frac{5}{7}\times\frac{7}{9}\times\;\cdot\;\cdot$$

und heisst P die grösste Primzahl, die hier als Theiler vorkommt, so wird man

$$\frac{7}{9}\times\frac{13}{15}\times\frac{19}{21}\times\;\cdot\;\cdot\;\cdot\;\cdot\; s > \frac{w}{2P}$$

haben, wo die Grössen 7, 13, 19, ... und 9, 15, 21, ... für arithmetische Progressionen angesehen werden können. Es kommen nämlich unter jenen Brüchen in den Nennern alle theilbaren ungeraden Zahlen vor; die Zahlform wird aber um so sicherer Primzahlen enthalten, wenn selbst unter dieser Voraussetzung sich $s > 1$ ergibt. Was P anbelangt, so muss, falls es die grösste für einen bestimmten Werth von w in $aw^2 + bw + c$ aufgehende Primzahl ist, die Gleichung $aw^2 + bw + c = P(P + \rho)$, wo $\rho \overline{\gtrless} 0$, $P + \rho$ aber eine Primzahl vorstellt, bestehen. Hieraus erhält man, da w somit auch P sehr gross ist, $aw^2 = P^2$, also $P = w\sqrt{a}$.

Man gelangt somit zu

$$s > \frac{1}{2\sqrt{a}}\times\frac{9\times15\times21\times\;\cdot\;\cdot\;\cdot\;\cdot}{7\times13\times19\times\;\cdot\;\cdot\;\cdot\;\cdot},$$

nimmt man hier die natürlichen Logarithmen, die mit $\lambda o \gamma$ bezeichnet werden können, so ist

$$\lambda o\gamma\, s > -\lambda o\gamma\, 2\sqrt{a} + \lambda o\gamma\, 9 + \lambda o\gamma\, 15 + \lambda o\gamma\, 21 \ldots\ldots$$
$$-\lambda o\gamma\, 7 - \lambda o\gamma\, 13 - \lambda o\gamma\, 19 - \ldots\ldots$$

und bedient man sich hiebei des combinatorischen Integrals

$$\lambda o\gamma\, s > -\lambda o\gamma\, 2\sqrt{a} + \overset{r}{\underset{1}{\mathfrak{S}}}\, \lambda o\gamma\,(3 + 6r) - \overset{r}{\underset{1}{\mathfrak{S}}}\, \lambda o\gamma\,(1 + 6r)$$

oder

$$\lambda o\gamma\, s > -\lambda o\gamma\, 2\sqrt{a} + \overset{r}{\underset{1}{\mathfrak{S}}}\, \lambda o\gamma \left(1 + \frac{2}{6r+1}\right).$$

Da aber, wie bekannt,

$$\lambda o\gamma\,(1 + u) = u - \tfrac{1}{2}u^2 + \tfrac{1}{3}u^3 - \tfrac{1}{4}u^4 + \ldots$$

ist, so erhält man bei $u = \dfrac{2}{6r+1}$

$$\overset{r}{\underset{1}{\mathfrak{S}}}\, \lambda o\gamma \left(1 + \frac{2}{6r+1}\right) = \overset{r}{\underset{1}{\mathfrak{S}}} \left[\frac{2}{6r+1} - \frac{1}{2}\left(\frac{2}{6r+1}\right)^2\right.$$
$$\left. + \frac{1}{3}\left(\frac{2}{6r+1}\right)^3 - \frac{1}{4}\left(\frac{2}{6r+1}\right)^4 \ldots\right] = \overset{r}{\underset{1}{\mathfrak{S}}}\, \frac{12r}{(6r+1)^2} + L,$$

wo L als die Summe von $\dfrac{1}{3}\left(\dfrac{2}{6r+1}\right)^3 - \dfrac{1}{4}\left(\dfrac{2}{6r+1}\right)^4 + \ldots$ positiv ist, und man gelangt zu

$$\overset{r}{\underset{1}{\mathfrak{S}}}\, \lambda o\gamma \left(1 + \frac{2}{6r+1}\right) > \overset{r}{\underset{1}{\mathfrak{S}}}\, \frac{12r}{(6r+1)^2} = \frac{1}{k}\, \overset{r}{\underset{1}{\mathfrak{S}}}\, \frac{12kr}{(6r+1)^2}$$

Ist aber $k = 5$, so hat man $\dfrac{12kr}{(6r+1)^2} > \dfrac{1}{r}$, folglich auch $\overset{r}{\underset{1}{\mathfrak{S}}}\, \dfrac{12kr}{(6r+1)^2} > \overset{r}{\underset{1}{\mathfrak{S}}}\, \dfrac{1}{r}$, wo dann auch $\lambda o\gamma\, s > -\lambda o\gamma\, 2\sqrt{a} + \dfrac{1}{5}\, \overset{r}{\underset{1}{\mathfrak{S}}}\, \dfrac{1}{r}$.

Da aber die obige Formel allgemein gilt, so gibt sie für $u = -1$

$$\lambda o\gamma\, 0 = -\infty = -\left(1 + \frac{1}{2} + \frac{1}{3} + \ldots\right) = -\overset{r}{\underset{1}{\mathfrak{S}}}\, \frac{1}{r},$$

wesshalb $\overset{r}{\underset{1}{\mathfrak{S}}}\, \dfrac{1}{r}$ unendlich wird, so dass $-\lambda o\gamma\, 2\sqrt{a}$ gegen $\dfrac{1}{5}\, \overset{r}{\underset{1}{\mathfrak{S}}}\, \dfrac{1}{r}$

verschwindet, daher $\lambda\mathfrak{z}\gamma$ s und um so mehr s trotz aller Beschränkungen grösser werden kann, als jede angebbare Zahl.

Folgesätze. *a)* Die Form $(2p, 2q, 2r)$ bei $D = 8\varphi + 3$ wird unter andern auch doppelte Primzahlen enthalten, vorausgesetzt dass p, q, r relativ prim sind.

b) Jede eigentliche quadratische Zahlform enthält auch Potenzen aus Primzahlen, was aus den Perioden dieser Zahlformen leicht zu ersehen ist.

c) Auf eine ähnliche Art lässt sich darthun, dass die lineare Form $ax + b$ wo a, b prim zu einander sind, Primzahlen enthält. In diesem Falle ist nämlich $s \overline{\overline{>}}\, w \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times \frac{6}{7} \ldots$

folglich um so mehr $s \overline{\overline{>}}\, \frac{1}{2} w \times \frac{1}{3} \times \frac{3}{5} \times \frac{5}{7} \times \ldots$, wo dann der Beweis denselben Gang wie oben verfolgt.

Anmerkung. Aus vielen Beispielen lässt sich der Satz abstrahiren, dass bei jeder Determinante, die sich nicht durch 4 theilen lässt, in jeder eigentlichen quadratischen Zahlform entweder eine Primzahl oder doppelte Primzahl, Potenz oder doppelte Potenz vorkommt, die kleiner als D und zu D oder $\frac{1}{2}D$ prim ist. In dieser Abhandlung reicht jedoch das vorstehende Theorem als Prämisse aus. Es ist zwar an sich auch ohne Beweis sehr wahrscheinlich; doch pflegen ähnliche Sätze in der Mathematik nicht als Axiome angenommen zu werden.

17. Auf wie vielfache Art lässt sich eine reciproke Zahlform in eine trinäre verwandeln?

a) Ist die Determinante D eine Primzahl oder das Doppelte einer Primzahl, so weist Legendre (Nr. 278 etc.) nach, dass bei ihr einer quadratischen Zahlform nie zwei trinäre entsprechen können. Nach 14. ist aber jede reciproke Form auch eine trinäre; daher lässt sich bei dieser Determinante jede reciproke Form nicht mehr und nicht weniger als einmal in eine trinäre verwandeln.

Dasselbe geschieht auch, wenn D die Potenz aus einer ungeraden Primzahl oder das Doppelte einer solchen Grösse ist; übrigens kann dieser Fall auch zum folgenden Punkte bezogen werden.

b) Besteht D aus i Factoren, die entweder Primzahlen oder Potenzen aus Primzahlen sind, und wobei 2 für keinen Factor angesehen wird, so lässt sich jede nicht bifide reciproke Form auf 2^{i-1}-fache Weise in die Summe aus drei Quadraten zerlegen. Ist nämlich $(p, 2q, r)$ die gegebene Form, so kommt in derselben nach 16. eine Primzahl oder doppelte Primzahl N vor. Wird diese als Determinante angesehen, so enthält sie in ihren Formen laut der Multiplicationsregel, wenn in dieser Hinsicht die Vorzeichen der Mittelglieder unberücksichtigt bleiben, 2^{i-1} Mal die Grösse D. Ein Product aus zwei Factoren erscheint nämlich entweder in zwei verschiedenen Formen oder doch wenigstens bei zwei verschiedenen Werthen von f, g. Ein Product aus drei Factoren befindet sich in vier Formen, oder wenn dies nicht der Fall wäre, so hat es doch vier Werthe für f, g u. s. w. Nun liefert aber jedes Werthepaar eine trinäre Form für D, daher kann $(p, 2q, r)$ nicht mehr als 2^{i-1} trinäre Formen haben. Es können ihrer aber auch nicht weniger vorkommen; würde man nämlich bei N aus den Formen, die den trinären Arten $<\beta, \beta', \beta''>$ $<\gamma, \gamma', \gamma''>$ zugehören, für D blos

$$<\alpha, \alpha', \alpha''> = \begin{Bmatrix} m & . & m' & . & m'' \\ n & & n' & & n'' \end{Bmatrix} = (p, 2q, r)$$

erhalten, so müsste wieder umgekehrt nach 12.

$$\begin{array}{lll} \beta = m\varphi + n\psi, & \beta' = m'\varphi + n'\psi, & \beta'' = m''\varphi + n''\psi \\ \gamma = m\varphi' + n\psi', & \gamma' = m'\varphi' + n'\psi', & \gamma'' = m''\varphi' + n''\psi' \end{array}$$

zum Vorschein kommen, und man hätte

$$N = p\varphi^2 + 2q\varphi\psi + r\psi^2 = p\varphi'^2 + 2q\varphi'\psi' + r\psi'^2;$$

daher würde N in der Form $(p, 2q, r)$ zweimal vorkommen, und wäre also entweder ein Product aus zwei Factoren, oder müsste $(p, 2q, r)$ bifid sein. Beides widerstreitet aber den Annahmen.

c) Ist die reciproke Form eine bifide, und besteht D aus i Factoren, so lässt sie sich blos auf 2^{i-2}fache Art in drei Quadrate zerlegen. Da jede quadratische Zahlform unendlich viele Primzahlen und doppelte Primzahlen enthält, so kommt auch hier eine Zahl $N > \frac{2}{3} D$ vor und zwar nach 13. mit zwei Werthepaaren, aus deren jedem eine eigene trinäre Form für N hervorgeht. Aus diesem Grunde lassen sich auch bei der Determinante N zu den Werthen $<\beta, \beta', \beta''>$ noch $<\gamma, \gamma', \gamma''>$ finden, die für D zugleich $<\alpha, \alpha', \alpha''>$ liefern.

Daher kommt hier nur die Hälfte trinärer Arten und trinärer Formen vor, als dies sonst in jedem andern Falle geschehen würde.

Anmerkung. Es bedurfte bei mir einer langen Überlegung, bevor ich mich entschloss im vorstehenden Punkte von der üblichen Auffassung dieses Lehrsatzes abzuweichen. Nach Legendre (Nr. 302) hat nämlich jede reciproke Form 2^{i-1} trinäre Gestalten, wenn D aus i Factoren besteht. Hiezu fügt er in Nr. 314, Art. X, die Bemerkung bei, dass die bifiden Formen ihre trinären Werthe paarweise gleich haben. Aber nach 7. können nicht zu einer Art eigentlicher trinärer Werthe zwei trinäre Formen gehören; daher ist die obige Verschiedenheit nur eine scheinbare. Auch der Umstand kann hier nicht berücksichtigt werden, dass wenn etwa $<\alpha, \alpha', \alpha''>$ zu (p, pk, r) gehört, umgekehrt $<\alpha'', \alpha', \alpha>$ der Form $(p, -pk, r)$ entsprechen würde, da ja hier das Vorzeichen von pk gleichgiltig ist. Übrigens verhält sich eine trinäre Art in bifiden Formen beinahe überall so, wie zwei Arten bei anderen Formen, was der Grund sein mag, dass man sie als zu zwei trinären Formen gehörig angesehen hat.

18. Es ist eine gegebene reciproke Form in trinäre Formen zu zerlegen.

Ist $(p, 2q, r)$ bei der Determinante D die gegebene Form, daher p zu D reciprok, so suche man, wenn p mehrere reciproke Formen besitzt, etwa mittelst der Multiplication und Periodenverrechnung diejenigen von ihnen auf, die D enthalten, so dass die Gleichung $ax^2 + 2bxy + cy^2 = D$, bei $p = ac - b^2$ vollständig für alle Werthe von a, b, c und x, y gelöst erscheint. Ist dann

$$(a, 2b, c) = \left\{ \begin{matrix} \mu & . & \mu' & . & \mu'' \\ \nu & . & \nu' & . & \nu'' \end{matrix} \right\} = <m, m', m''>$$

und $x = f$, $y = g$, so ergeben sich

$$\alpha = \mu f + \nu g,\ \ \alpha' = \mu' f + \nu' g,\ \ \alpha'' = \mu'' f + \nu'' g$$

als trinäre Werthe von D, und es werden die Coëfficienten n, n', n'' nach Gleichung (15), da das Vorzeichen von q aus $\alpha, \alpha', \alpha''$ und m, m', m'' nicht ersichtlich ist, mittelst der Formeln

$$n = -\frac{1}{p}(\eta \mp mq),\ \ n' = -\frac{1}{p}(\eta' \mp m'q),\ \ n'' = -\frac{1}{p}(\eta'' \mp m''q),$$

wobei sich η, η', η'' aus Gleichung (13) ergibt, bestimmt, so dass man zu

$$(p, 2q, r) = \begin{Bmatrix} m & . & m' & . & m'' \\ n & & n' & & n'' \end{Bmatrix} = <\alpha, \alpha', \alpha''>$$

gelangt, welchem Ausdrucke man dann, wo nöthig nach 4. die regelrechte Gestalt geben kann.

Würde man die trinären Formen von $(a, 2b, c)$ nicht kennen, so werden sie auf dieselbe Art gefunden, was wegen $p < 2\sqrt{\frac{D}{3}}$ viel weniger Mühe kostet.

Übrigens ist nach 14. zur vollständigen Lösung nicht nöthig, dass p, D prim zu einander sind; denn jede trinäre Art der Zahlform $(p, 2q, r)$ ist nach 12. mit einer Art der Determinante p reciprok, wesshalb auch für jedes dieser Reciprocitätsverhältnisse die Grössen f, g vorhanden sein müssen. Beträgt dann die Anzahl der Paare von f, g nicht 2^{i-1}, so hat wieder $(a, 2b, c)$ mehrere trinäre Formen, oder ist es bifid, daher die Aufgabe immer vollständig lösbar. Die meiste Schwierigkeit macht übrigens die Gleichung

$$ax^2 + 2bxy + cy^2 = D,$$

die ich zum Gegenstande späterer Untersuchungen zu machen gedenke, da die Periodicität der quadratischen Zahlformen bei ihrer vollständigen Lösung eine bedeutende Rolle spielt. Dieses Verfahren mögen zwei Beispiele verdeutlichen:

1. Beispiel. Legendre befasst sich in Nr. 313 mit der Form $(50, 30, 189)$ bei $D = 9225 = 3^2 . 5^2 . 41$, die demnach vier trinäre Arten besitzt. Er gibt ihr, um sein Verfahren zu versinnlichen, die Gestalt $(209, 70, 50)$, weil 209 zu 9225 prim ist. Nehmen wir jedoch $p = 50$ an, so hat man hier die zwei trinären Formen

$$(6, -4, 9) = \begin{Bmatrix} 1 & . & -2 & . & 1 \\ 2 & & 1 & & -2 \end{Bmatrix} = <3, 4, 5>$$

und

$$(1, 50) = \begin{Bmatrix} 1 & . & 0 & . & 0 \\ 0 & & 7 & & -1 \end{Bmatrix} = <0, 1, 7>;$$

in der ersten Form kommt D mit den Werthen

$$f = 36,\ 36,\ 16$$
$$g = -7,\ 23,\ 33$$

und in der letzteren mit $f = 95$, $g = 2$ vor, dies gibt als trinäre Arten für (50, 30, 189) beziehungsweise

$$<22, -79, 50>,\ <82, -49, -10>,\ <82, 1, -50>,\ <95, 14, -2>$$

denen die trinären Formen

$$\left\{\begin{matrix} 3 & 4 & 5 \\ -11\cdot & 2\cdot & 8 \end{matrix}\right\},\quad \left\{\begin{matrix} 3 & 4 & 5 \\ -5\cdot & -10\cdot & 8 \end{matrix}\right\},\quad \left\{\begin{matrix} 3 & 4 & 5 \\ 5\cdot & -10\cdot & 8 \end{matrix}\right\},\quad \left\{\begin{matrix} 0 & 1 & 7 \\ 2\cdot & -13\cdot & 4 \end{matrix}\right\}$$

zugehören. Werden diese Grössen gehörig geordnet, so sind

$$\left\{\begin{matrix} 3 & 5 & -4 \\ -11\cdot & 8\cdot & -2 \end{matrix}\right\} = <22, 50, 79>;\quad \left\{\begin{matrix} 5 & 4 & -3 \\ -8\cdot & 10\cdot & -5 \end{matrix}\right\} = <10, 49, 82>;$$
$$\left\{\begin{matrix} 3 & -5 & 4 \\ 5\cdot & -8\cdot & -10 \end{matrix}\right\} = <82, 50, 1>;\quad \left\{\begin{matrix} 7 & -1 & 0 \\ 4\cdot & 13\cdot & -2 \end{matrix}\right\} = <2, 14, 95>$$

die vier gesuchten Ausdrücke.

2. Beispiel. Es wäre bei $D = 4758 = 2 \times 3 \times 13 \times 61$ die reciproke Form (66, 36, 77). Hier sind bei $p = 66$ zwei trinäre Formen, nämlich (2, 33) worin D mit $f = 27$, $g = 10$ und (6, 11) wo es mit $f = 23$, $g = 12$ vorkommt; daher hier nur zwei Paare dieser Grössen erscheinen. Es hat jedoch erstere Form zwei trinäre Gestalten, nämlich

$$\left\{\begin{matrix} 1 & -1 & 0 \\ 4\cdot & 4\cdot & -1 \end{matrix}\right\} = <1, 1, 8>;\quad \left\{\begin{matrix} 0 & 1 & -1 \\ -5\cdot & 2\cdot & 2 \end{matrix}\right\} = <4, 5, 5>$$

welche die Werthe $<67, 13, -10>$, $<-50, 47, -7>$ liefern. Die zweite Form ist eine bifide und hat

$$\left\{\begin{matrix} 1 & -2 & 1 \\ 3\cdot & 1\cdot & -1 \end{matrix}\right\} = <1, 4, 7>,$$

daher kann hier auch noch $f = 23$, $g = -12$ genommen werden, und man erhält $<59, -34, 11>$, $<-13, -58, 35>$. Sucht man hiezu die Coëfficienten n, n', n'' auf, und ordnet die Resultate, so kommt

$$\left\{\begin{matrix} 8 & -1 & -1 \\ 3\cdot & 8\cdot & -2 \end{matrix}\right\} = <10, 13, 67>,\quad \left\{\begin{matrix} 5 & -5 & 4 \\ 8\cdot & 2\cdot & -3 \end{matrix}\right\} = <7, 47, 50>$$
$$\left\{\begin{matrix} 7 & -4 & 1 \\ 6\cdot & 5\cdot & -4 \end{matrix}\right\} = <11, 34, 59>,\quad \left\{\begin{matrix} 4 & -7 & 1 \\ 3\cdot & -2\cdot & -8 \end{matrix}\right\} = <58, 35, 13>$$

zum Vorschein.

19. Trinäre Formen allgemeiner Determinanten.

Ist die niedrigste in der reciproken Form $(p, 2q, r)$ vorkommende Zahl p bedeutend klein, so hat sie entweder nur einen oder einige wenige trinäre Werthe, und man ist nach den angeführten Lehrsätzen im Stande, einen allgemeinen Ausdruck für alle reciproken Formen, welche die Zahl p enthalten, aufzustellen, mittelst dessen es dann leicht wird, jenen Formen die trinäre Gestalt zu geben. Hiebei ereignet es sich auch oft, dass man es an den trinären Werthen absieht, zu welcher quadratischen Zahlform sie gehören, ohne sie erst nach 6. verrechnen zu müssen; so dass eine tabellarische Übersicht dieses Umstandes immerhin bedeutende Vortheile gewährt. Dies mag ein Beispiel erläutern. Bei welchen Determinanten und in welchen trinären Formen kommt $p = 6$ vor? Die Determinante 6 hat

$$(2, 3) = \left\{\begin{matrix} 1 & \cdot & -1 & \cdot & 0 \\ 1 & & 1 & & -1 \end{matrix}\right\} = \langle 1, 1, 2 \rangle,$$

daher wird $p = 6$ bei jedem $D = 2a^2 + 3b^2$ in einer trinären Form erscheinen, wo zugleich

$$\alpha = a + b,\ \alpha' = -a + b,\ \alpha'' = -b.$$

Jener Ausdruck ist demnach

$$\left\{\begin{matrix} 1 & \cdot & 1 & \cdot & 2 \\ n & & n' & & n'' \end{matrix}\right\} = \langle a + b, -a + b, -b \rangle.$$

Aus $n'' - 2n' = a + b$ folgt $n'' = a - b$, $n' = -b$, und $2n - n'' = -a + b$ gibt $n = 0$, so dass man

$$\left\{\begin{matrix} 1 & \cdot & 1 & \cdot & 2 \\ 0 & & -b & & a-b \end{matrix}\right\} = \langle a + b, -a + b, -b \rangle$$

oder

$$\left\{\begin{matrix} -1 & \cdot & 1 & \cdot & 2 \\ 0 & & -b & & a-b \end{matrix}\right\} = \langle a+b, a-b, b \rangle = (6, 4a-6b, a^2-2ab+2b^2)$$

erhält. Um hier für das Mittelglied der quadratischen Form die kleinste Zahl zu erhalten, setze man $2a - 3b = 6c + q$, wo $q \overset{=}{<} 3$ gemacht werden kann, und man gelangt bei $x = x' - cy$ zu

$$(6,\,2q,\,r) = \begin{Bmatrix} -1 & 1 & 2 \\ c & -b-c & a-b-2c \end{Bmatrix} = \langle a+b,\ a-b,\ b\rangle$$

Die trinären Werthe $a-b$, b, $a+b$ bilden hier eine arithmetische Progression und es lassen sich aus

$$\alpha'' = b = \frac{\alpha \mp \alpha'}{2},\ a = \frac{\alpha \pm \alpha'}{2}$$

die Grössen a, b ermitteln.

Auf eine ähnliche Art gelangt man zur nachstehenden

Tabelle.

$$p = 1,\ D = a^2 + b^2,\ \begin{Bmatrix} 1 & 0 & 0 \\ 0 & b & -a \end{Bmatrix} = \langle 0,\ a,\ b\rangle$$

$$q = 0 \quad \alpha = 0 \quad \alpha' = a \quad \alpha'' = b$$

$$p = 2,\ D = a^2 + 2b^2,\ \begin{Bmatrix} 0 & 1 & -1 \\ -b & a-c & c \end{Bmatrix} = \langle a,\ b,\ b\rangle$$

$$a = 2c + q,\ \ \alpha' = \alpha'' = b,\ \ \alpha = a$$

$$p = 3,\ D = 2a^2 + 2ab + 2b^2,\ \begin{Bmatrix} 1 & -1 & 1 \\ b-c & c & -a-c \end{Bmatrix} = \langle a,\ a+b,\ b\rangle$$

$$b - a = 3c + q,\ \ \alpha' = \alpha + \alpha'',\ \ \alpha = a,\ \ \alpha'' = b$$

$$p = 5,\ D = a^2 + 5b^2,\ \begin{Bmatrix} 0 & -2 & 1 \\ b & 2c-a & -c \end{Bmatrix} = \langle a,\ b,\ 2b\rangle$$

$$2a = 5c + q,\ \ \alpha' = \frac{\alpha''}{2} = b,\ \ \alpha = a$$

$$p = 6,\ D = 2a^2 + 3b^2,\ \begin{Bmatrix} -1 & 1 & 2 \\ c & -b-c & a-b-2c \end{Bmatrix} = \langle a+b,\ a-b,\ b\rangle$$

$$2a - 3b = 6c + q,\ \ \alpha'' = b = \frac{\alpha \mp \alpha'}{2},\ \ a = \frac{\alpha \pm \alpha'}{2}$$

$$p = 9,\ D = 2a^2 + 2ab + 5b^2,\ \begin{Bmatrix} 2 & -2 & 1 \\ a+b-2c & 2c-a & -c \end{Bmatrix} = \langle a,\ a+b,\ 2b\rangle$$

$$4a + 2b = 9c + q,\ \alpha'' = 2\,(\alpha' \pm \alpha),\ a = \alpha,\ \ b = \frac{\alpha''}{2}$$

$$p = 10,\ D = a^2 + 10b^2,\ \begin{Bmatrix} 0 & -3 & 1 \\ b & 3c-a & -c \end{Bmatrix} = \langle a,\ b,\ 3b\rangle$$

$$3a = 10c + q,\ \ \alpha' = \frac{\alpha''}{3} = b,\ \ a = \alpha$$

$$p = 11,\ D = 2a^2 + 2ab + 6b^2,\ \left\{\begin{matrix} -1 & & 1 & & 3 \\ c & \cdot & -b-c & \cdot & a-b-3c \end{matrix}\right\}$$

$$= \langle a + 2b,\ a - b,\ b \rangle$$

$$3a - 4b = 11c + q,\ \alpha'' = \frac{\alpha \mp \alpha'}{3} = b,\ a = \alpha' \pm \alpha''$$

$$p = 13,\ D = a^2 + 13b^2,\ \left\{\begin{matrix} 0 & & -3 & & 2 \\ b & \cdot & a+3c & \cdot & -a-2c \end{matrix}\right\} = \langle a,\ 2b,\ 3b \rangle$$

$$-5a = 13c + q,\ \frac{\alpha'}{2} = \frac{\alpha''}{3} = b,\ a = \alpha$$

$$p = 14,\ D = 3a^2 + 2ab + 5b^2$$

$$\left\{\begin{matrix} -3 & & 2 & & 1 \\ a-b+3c & \cdot & -a-2c & \cdot & -c \end{matrix}\right\} = \langle a.\ a - b,\ a + 2b \rangle$$

$$-5a + 3b = 14c + q.\ \alpha = \frac{\alpha'' \pm 2\alpha'}{3} = a.\ b = a \mp a'.$$

Anmerkung. Einen ähnlichen Gegenstand behandelt Legendre in Nr. 307 — 312 als Bestandtheil des zweiten Beweises, dass jede reciproke Form sich in 2^{i-1} trinäre zerlegen lasse, wenn D aus i Factoren besteht; hier ist es von einer andern Seite aufgefasst und als Folge der Reciprocität durchgeführt, so dass alle speciellen Fälle und Kunstgriffe möglichst vermieden wurden.

III. Überschreitung der trinären Arten.

20. Erörterung dieses Verfahrens.

Lässt sich zu den trinären Werthen $\langle \alpha,\ \alpha',\ \alpha'' \rangle$ der Determinante D eine Grösse $p = m^2 + m'^2 + m''^2$, wo m, m', m'' prim zu einander sind, so finden, dass in der Gleichung

$$\alpha m + \alpha' m' + \alpha'' m'' = ph \tag{17}$$

h eine ganze Zahl oder höchstens die Hälfte einer ungeraden Zahl wird, und bestimmt man β, β', β'' aus

$$\beta = 2hm - \alpha,\ \beta' = 2hm' - \alpha',\ \beta'' = 2hm'' - \alpha'', \tag{18}$$

so sind diese Grössen auch trinäre Werthe der Determinante D. Es geben nämlich diese Gleichungen

$$\beta^2 + \beta'^2 + \beta''^2 = 4h^2(m^2 + m'^2 + m''^2)$$
$$- 4h(\alpha m + \alpha' m' + \alpha'' m'') + \alpha^2 + \alpha'^2 + \alpha''^2.$$

was nach Gleichung (17) in

(19) $$D = \beta^2 + \beta'^2 + \beta''^2$$

übergeht.

Eben so erhält man aus den Gleichungen (18)

$$\beta m + \beta' m' + \beta'' m'' = 2h(m^2 + m'^2 + m''^2) - (\alpha m + \alpha' m' + \alpha'' m'')$$

oder

(20) $$\beta m + \beta' m' + \beta'' m'' = ph.$$

Werden daher die Werthe β, β', β'' so behandelt wie $<\alpha, \alpha', \alpha''>$, so erhält man wieder letztere Form zum Resultate. Man kann jedoch bei β, β', β'' oder m, m', m'' Versetzungen und Zeichenänderungen (4.) vornehmen, und erhält in vielen Fällen wieder eine neue trinäre Art für D.

Auf diese Weise lassen sich aus $<\alpha, \alpha', \alpha''>$, wenn die Grössen p entsprechend gewählt werden, alle trinären Arten der Determinante D finden. Überdies liefert dieses Verfahren eine hellere Einsicht in den Zusammenhang der trinären Arten unter einander und in ihr Verhältniss zur Formenperiode.

Die Grösse p, welche in diesem Falle keine Zahl der zu $<\alpha, \alpha', \alpha''>$ gehörigen quadratischen Form sein muss, nenne ich den Schreiter, und diese Methode aus einer gegebenen trinären Art andere abzuleiten, die Überschreitung, welche Benennungen im Verlaufe dieser Abhandlung begründet erscheinen.

Anmerkung. Die angeführten Gleichungen behalten ihre Richtigkeit, auch wenn

$$h = \frac{1}{p}(\alpha m + \alpha' m' + \alpha'' m'')$$

keine ganze Zahl wäre. Dann sind aber, den Fall von $h = \frac{2h'+1}{2}$ ausgenommen, β, β', β'' keine ganzen Zahlen, wie dies bei trinären Werthen erforderlich ist, so dass man diesen Fall nur dann in Betracht zu ziehen hätte, wenn D überhaupt in die Summe aus drei Quadraten von rationellen Wurzeln zu zerlegen wäre.

21. Es ist eine uneigentliche trinäre Art in eine eigentliche zu verwandeln.

Sind $<\alpha p, \alpha' p, \alpha'' p>$ die gegebenen uneigentlichen trinären Werthe, so ist zur Lösbarkeit dieser Aufgabe erforderlich, dass p ungerade sei, da man sonst hier $4D$ zur Determinante hätte, die keine eigentlichen trinären Werthe besitzt. Wäre nun $p = m^2 + m'^2 + m''^2$, so kann diese Grösse als Schreiter angesehen werden, und man erhält $h = \alpha m + \alpha' m' + \alpha'' m''$, wo die Vorzeichen von m, m', m'' so zu nehmen sind, dass h mit p keinen gemeinschaftlichen Theiler erhalte; dann ist

$$\beta = 2hm - \alpha p, \quad \beta' = 2hm' - \alpha' p, \quad \beta'' = 2hm'' - \alpha'' p.$$

Wäre hingegen p von der Form $8\varphi - 1$, daher nicht in drei Quadrate zerlegbar, so muss dies bei $2p$ geschehen, wo man also $2p = m^2 + m'^2 + m''^2$ zum Schreiter nehmen kann. In diesem Falle ergibt sich, falls man für h den obigen Werth behält,

$$\beta = hm - \alpha p, \quad \beta' = hm' - \alpha' p, \quad \beta'' = hm'' - \alpha'' p.$$

Aus 4. ist ersichtlich, dass die Anzahl der Arten $<\beta, \beta', \beta''>$ 24 nicht übersteigen könne.

Auch ist es klar, dass die Aufgabe aus $D = \alpha^2 + \alpha'^2 + \alpha''^2$ und p oder $2p = m^2 + m'^2 + m''^2$ eigentliche trinäre Werthe von Dp^2 zu finden — nur eine andere Version der angeschriebenen ist, da in diesem Falle die Determinante Dp^2 offenbar die uneigentliche trinäre Art $<\alpha p, \alpha' p, \alpha'' p>$ besitzt.

Eine eigenthümliche Folge dieser Sätze ist ferner die, dass $<0, 0, D>$ bei

$$p = D = \alpha^2 + \alpha'^2 + \alpha''^2$$

wegen $h = \alpha''$,

$$D^2 = (2\alpha\alpha'')^2 + (2\alpha'\alpha'')^2 + (2\alpha''^2 - D)^2$$

liefert, und dass man eben so aus $2D = \alpha^2 + \alpha'^2 + \alpha''^2$

$$D^2 = (\alpha\alpha'')^2 + (\alpha'\alpha'')^2 + (\alpha''^2 - D)^2$$

erhält; wodurch man mehrere trinäre Werthe einer quadratischen Determinante leicht ermitteln kann.

22. Hilfsgrössen zur Überschreitung und ihre Verhältnisse.

Die Zahlen $\alpha + \beta$, $\alpha' + \beta'$, $\alpha'' + \beta''$ sind in dem normalen Falle, wo h eine ganze Zahl ist, nach Gleichung (18) gerade, was daher auch bei $\beta - \alpha$, $\beta' - \alpha'$, $\beta'' - \alpha''$ stattfinden wird, und man kann, wenn dieselben den gemeinsamen Theiler $2k$ haben,

$$(21) \qquad g = \frac{\beta - \alpha}{2k}, \quad g' = \frac{\beta' - \alpha'}{2k}, \quad g'' = \frac{\beta'' - \alpha''}{2k}$$

setzen, so dass g, g', g'' relativ prim werden. Diese Gleichungen geben

$$mg + m'g' + m''g'' = \frac{1}{2k}\left[\beta m + \beta' m' + \beta'' m'' - (\alpha m + \alpha' m' + \alpha'' m'')\right]$$

folglich nach Gleichung (17) und (20)

$$(22) \qquad mg + m'g' + m''g'' = 0$$

und die trinären Arten $<m, m', m''>$, $<g, g', g''>$ sind nach 12. reciprok, so dass sowohl

$$(23) \qquad <g, g', g''> = \begin{Bmatrix} m & . & m' & . & m'' \\ n & . & n' & . & n'' \end{Bmatrix} = (p, 2q, r),$$

wobei

$$(24) \qquad d = g^2 + g'^2 + g''^2 = pr - q^2,$$

als auch

$$(25) \qquad <m, m', m''> = \begin{Bmatrix} g & . & g' & . & g'' \\ \nu & . & \nu' & . & \nu'' \end{Bmatrix} = (d, 2q', r')$$

und

$$(26) \qquad p = dr' - q'^2$$

zum Vorschein kommt.

Es sind daher p, d reciproke Zahlen, welches Verhältniss zwischen p, D nicht vorkommen muss.

Ferner geben die Gleichungen (21) mit Rücksicht auf die Gleichung (18)

$$(27) \quad \begin{cases} \alpha = hm - gk, & \alpha' = hm' - g'k, \quad \alpha'' = hm'' - g''k \\ \beta = hm + gk, & \beta' = hm' + g'k, \quad \beta'' = hm'' + g''k \end{cases}$$

so dass man weiterhin $D = \alpha^2 + \alpha'^2 + \alpha''^2$

$$= h^2(m^2+m'^2+m''^2) - 2hk(mg+m'g'+m''g'') + k^2(g^2+g'^2+g''^2)$$

erhält, was wegen Gleichung (22) und (24) in

$$D = ph^2 + dk^2 \tag{28}$$

übergeht, und wenn d eliminirt wird,

$$D = p\,(h^2 + rk^2) - (kq)^2$$

liefert, so dass dann

$$(p,\ 2kq,\ h^2 + rk^2) \tag{29}$$

diejenige Form ist, aus der man den Formenzeiger für p in Hinsicht der Perioden bestimmen kann.

Wird aus der Gleichung (28) der Schreiter p mittelst Gleichung (26) eliminirt, so ergibt sich

$$D = d\,(k^2 + r'h^2) - (hq')^2,$$

woraus wieder

$$(d,\ 2hq',\ k^2 + r'h^2) \tag{30}$$

als die zur Gegengrösse des Schreiters gehörige Form der Determinante D hervorgeht. Ferner erhält man aus Gleichung (27)

$$\alpha g + \alpha' g' + \alpha'' g'' = h\,(mg + m'g' + m''g'') - (g^2 + g'^2 + g''^2)\,k$$

oder

so wie auch

$$\left.\begin{aligned} \alpha g + \alpha' g' + \alpha'' g'' &= -\,dk \\ \beta g + \beta' g' + \beta'' g'' &= dk \end{aligned}\right\} \tag{31}$$

und werden die Gleichungen (27) mit einander multiplicirt, so ist die Summe der Producte

$$\alpha\beta + \alpha'\beta' + \alpha''\beta'' = h^2\,(m^2 + m'^2 + m''^2) - k^2\,(g^2 + g'^2 + g''^2),$$

oder

$$\alpha\beta + \alpha'\beta' + \alpha''\beta'' = ph^2 - dk^2. \tag{32}$$

Bestimmt man ferner die Grössen γ, γ', γ'' mittelst des Ausdruckes

(33) $$(p, d) = \left\{\begin{matrix} m & . & m' & . & m'' \\ g & & g' & & g'' \end{matrix}\right\} = <\eta, \eta', \eta''>$$

so folgt aus der Gleichung (12)

(34) $$\eta = qm - pn, \quad \eta' = qm' - pn', \quad \eta'' = qm'' - pn''$$

und man hat

(35) $$q = \frac{pn + \eta}{m} = \frac{pn' + \eta'}{m'} = \frac{pn'' + \eta''}{m''}$$

mittelst welcher Formel sich n, n', n'' leichter finden lassen, als durch Gleichung (23). Überdies erhält man hier $q \overline{\overline{<}} \frac{1}{2} p$; es ist nämlich nur n so zu bestimmen, dass $\frac{pn + \eta}{m}$ eine ganze Zahl und $\overline{\overline{<}} \frac{1}{2} p$ wird. Dann sind die Gleichungen (35) auch desshalb vortheilhaft, weil sie q geben ohne erst n', n'' verrechnen zu müssen. Weiterhin folgt aus Gleichung (27)

$$\alpha' m'' - \alpha'' m' = m''(hm' - g'k) - m'(hm'' - g''k) = k(m'g'' - m''g')$$

und nach Gleichung (33)

(36) $$\alpha' m'' - \alpha'' m' = k\eta.$$

Eben so erhält man aus Gleichung (33)

$$\begin{aligned} \alpha''\eta' - \alpha'\eta'' &= \alpha''(m''g - mg'') - \alpha'(mg' - m'g) \\ &= g(\alpha' m' + \alpha'' m'') - m(\alpha' g' + \alpha'' g''), \end{aligned}$$

was nach Gleichung (17) und (31) in

$$g(ph - \alpha m) + m(dk + \alpha g) = dkm + phg$$

oder

(37) $$\alpha''\eta' - \alpha'\eta'' = dkm + phg$$

übergeht. Aus diesem letzteren Resultate folgt wieder nach Gleichung (27) und (28)

$$\alpha''\eta' - \alpha'\eta'' = \frac{1}{k}(ph \,.\, gk + m \,.\, dk^2) =$$

$$= \frac{1}{k}[ph(hm - \alpha) + m(D - ph^2)] = \frac{1}{k}(mD - ph\alpha)$$

oder

$$\alpha'\eta'' - \alpha''\eta' = \frac{\alpha hp - mD}{k} \tag{38}$$

Es ist aber auch nach Gleichung (34)

$$\begin{aligned}\alpha'\eta'' - \alpha''\eta' &= \alpha'(qm'' - pn'') - \alpha''(qm' - pn') \\ &= q(\alpha'm'' - \alpha''m') + p(n'\alpha'' - n''\alpha') = kq\eta + p\varphi\end{aligned}$$

laut Gleichung (36) wenn zur Abkürzung $\varphi = n'\alpha'' - n''\alpha'$ gesetzt wird. Hieraus folgt nach Gleichung (38)

$$\frac{\alpha hp - mD}{k} = kq\eta + p\varphi \text{ oder } kq\eta = \frac{p(\alpha h - k\varphi) - mD}{k}$$

was bei $\psi = \alpha h - k\varphi$, die Gleichung

$$kq = \frac{p\psi - mD}{k\eta} \tag{39}$$

liefert, welche ebenfalls zur Bestimmung von kq dient, und wobei $k\eta$ aus Gleichung (36) zu ermitteln ist. Wäre $\eta = 0$, oder hätte es mit p einen gemeinsamen Theiler, so suche man kq aus $\frac{p\psi - m'D}{k\eta'}$ oder aus $\frac{p\psi - m''D}{k\eta''}$, wobei ψ so zu nehmen ist, dass die Brüche zu ganzen Zahlen werden.

Ferner ist nach Gleichung (33)

$$\begin{aligned}\beta''\eta' - \beta'\eta'' &= \beta''(m''g - mg'') - \beta'(mg' - m'g) \\ &= g(\beta'm' + \beta''m'') - m(\beta'g' + \beta''g'').\end{aligned}$$

was nach Gleichung (20) und (31)

$$= g(ph - \beta m) - m(dk - \beta g),$$

daher

$$\beta''\eta' - \beta'\eta'' = phg - dkm. \tag{40}$$

Laut Gleichung (33) ist

$$\left\{\begin{matrix} g & . & g' & . & g'' \\ m & & m' & & m'' \end{matrix}\right\} = \langle -\eta, -\eta', -\eta'' \rangle,$$

woraus man in Hinsicht der Gleichungen (23) und (12)

(41) $$\begin{cases} \eta = d\nu - gq', \quad \eta' = d\nu' - g'q', \quad \eta'' = d\nu'' - g''q \\ \text{oder} \\ q' = \dfrac{d\nu - \eta}{g} = \dfrac{d\nu' - \eta'}{g'} = \dfrac{d\nu'' - \eta''}{g''} \end{cases}$$

erhält.

Überdies folgt aus Gleichung (27)

$$\alpha' g'' - \alpha'' g' = g''(hm' - g'k) - g'(hm'' - g''k) = h(m'g'' - m''g')$$

und nach Gleichung (33)

(42) $$\alpha' g'' - \alpha'' g' = h\eta.$$

Aus Gleichung (37) hat man

$$\alpha''\eta' - \alpha'\eta'' = \frac{1}{h}\,(g \cdot ph^2 + dk \cdot mh).$$

Dies übergeht nach Gleichung (28) und (27) in

$$= \frac{1}{h}\,[g\,(D - dk^2) + dk\,(\alpha + gk)],$$

wesshalb auch

(43) $$\alpha''\eta' - \alpha'\eta'' = \frac{dk\alpha + gD}{h}.$$

Hierauf folgt aus Gleichung (41)

$$\begin{aligned} \alpha''\eta' - \alpha'\eta'' &= \alpha''\,(d\nu' - g'q') - \alpha'\,(d\nu'' - g''q') \\ &= d\,(\alpha''\nu' - \alpha'\nu'') + q'\,(\alpha'g'' - \alpha''g'), \end{aligned}$$

welcher Ausdruck nach Gleichung (43) und (42)

$$\frac{dk\alpha + gD}{h} = d\,(\alpha''\nu' - \alpha'\nu'') + hq'\eta,$$

d. i.

$$hq'\eta = \frac{d\,[\alpha k - h\,(\alpha''\nu' - \alpha'\nu'')] + gD}{h}$$

und bei

(44) $$\psi' = \alpha k - h\,(\alpha''\nu' - \alpha'\nu''), \quad hq' = \frac{d\psi' + gD}{h\eta}$$

gibt, so dass dann die Gleichungen 41, 42, 43 und 44 jenen unter (34, 35) 36, 38 und 39 entsprechen.

Die Gleichung (42) gibt mit α multiplicirt

$$h\alpha\eta = \alpha\alpha' g'' - \alpha\alpha'' g'.$$

und durch höhere Streichung erhält man hieraus

$$h\alpha'\eta' = \alpha'\alpha'' g - \alpha\alpha' g'', \quad h\alpha''\eta'' = \alpha\alpha'' g' - \alpha'\alpha'' g;$$

daher liefert ihre Summe $\alpha\eta + \alpha'\eta' + \alpha''\eta'' = 0$. Hiezu erhält man aus den Gleichungen (21) mit Rücksicht auf Gleichung (33)

$$0 = g\eta + g'\eta' + g''\eta'' = \frac{1}{2k}\left[\beta\eta + \beta'\eta' + \beta''\eta'' - (\alpha\eta + \alpha'\eta' + \alpha''\eta'')\right]$$

folglich auch

$$\beta\eta + \beta'\eta' + \beta''\eta'' = 0.$$

Es ist demnach die trinäre Art $<\eta, \eta', \eta''>$ nicht nur mit $<m, m', m''>$, $<g, g', g''>$ sondern auch mit $<\alpha, \alpha', \alpha''>$ und $<\beta, \beta', \beta''>$ reciprok. Nimmt man daher, um im Allgemeinen zu handeln, an, die Grössen η, η', η'' hätten π zum grössten gemeinschaftlichen Theiler, und setzt desshalb

$$\eta = \pi\varepsilon, \quad \eta' = \pi\varepsilon', \quad \eta'' = \pi\varepsilon'', \tag{45}$$

so folgt aus 12:

$$\left.\begin{aligned} <\alpha, \alpha', \alpha''> &= \begin{Bmatrix} \varepsilon & . & \varepsilon' & . & \varepsilon'' \\ \gamma & & \gamma' & & \gamma'' \end{Bmatrix} = (P, 2Q, R) \\ <\beta, \beta', \beta''> &= \begin{Bmatrix} \varepsilon & . & \varepsilon' & . & \varepsilon'' \\ \delta & & \delta' & & \delta'' \end{Bmatrix} = (P, 2Q', R') \end{aligned}\right\} \tag{46}$$

Aus der Annahme, dass η, η', η'' den gemeinsamen Theiler π haben, folgt weiterhin, dass jenen Divisor auch p, d, D, q, q' haben muss, d. h. dass man

$$p = \pi p', \quad d = \pi d', \quad D = \pi D', \quad q = \pi q^0, \quad q' = \pi q'' \tag{47}$$

zu setzen habe, wobei freilich $\pi = 1$ der gewöhnliche Fall ist. Was p anbelangt, folgt aus Gleichung (33)

$$m'g'' - m''g' = \pi\varepsilon, \quad m''g - mg'' = \pi\varepsilon', \quad mg' - m'g = \pi\varepsilon''$$

und verbindet man hiemit $mg + m'g' + m''g'' = 0$, so erhält man, wenn die zweite, dritte und vierte beziehungsweise mit $m'', -m', m$ multiplicirt wird, zur Summe

$$g(m^2 + m'^2 + m''^2) = \pi(\varepsilon' m'' - \varepsilon'' m') = pg.$$

Eben so gibt die erste, dritte und vierte dieser Gleichungen

$$\pi(\varepsilon'' m - \varepsilon m'') = pg'.$$

so wie man auch zu

$$\pi(\varepsilon m' - \varepsilon' m) = pg''$$

gelangt. Demnach haben die Zahlen pg. pg', pg'' den gemeinschaftlichen Theiler π, wodurch p aufgehen muss, weil g, g', g'' prim zu einander sind. Auf eine ähnliche Art findet man aus den vier angeführten Gleichungen, dass dm, dm', dm'' sämmtlich durch π theilbar sind, dass demnach $d = \pi d'$. Nach Gleichung (35) hat diesen Divisor q, nach Gleichung (41) q', und nach Gleichung (28) die Determinante D.

Was P anbelangt, ist nach Gleichung (46)

$$P = \varepsilon^2 + \varepsilon'^2 + \varepsilon''^2 = \frac{1}{\pi^2}(\eta^2 + \eta'^2 + \eta''^2),$$

(48) daher laut Gleichung (33) $= \frac{pd}{\pi^2}$. folglich $P = p'd'$.

1. Anmerkung. Was den Fall anbelangt, wenn $h = \frac{h'}{2}$ und h' ungerade, so kann er sich nach Gleichung (17) nur bei $p = 2p''$ ereignen, wo p'' ungerade ist, da m, m', m'' eigentliche trinäre Werthe darstellen. Bei diesem Umstande wird nach Gleichung (18) unter den Grössen $\alpha + \beta$, $\alpha' + \beta'$, $\alpha'' + \beta''$ wenigstens eine ungerade vorkommen, die daher auch unter $\beta - \alpha$, $\beta' - \alpha'$, $\beta'' - \alpha''$ erscheint, wesshalb nach Gleichung (21) $k = \frac{k'}{2}$ und k' ungerade ist. Nach Gleichung (28) muss dann wegen $4D = ph'^2 + dk'^2, d = 2d''$ sein, daher wegen Gleichung (24), (26) q und q' gerade sein werden, wesshalb auch kq und hq' ganze Zahlen sind. Ferner folgt aus den Gleichungen (34), dass η, η', η'' gerade sind, daher wird die Gleichung (39) immer lösbar sein. Es bietet somit der oberwähnte Fall bei diesem Verfahren keine Schwierigkeiten.

2. Anmerkung. Von besonderer Wichtigkeit ist, wie die Folge zeigt, die Gleichung (39). Da es in derselben nur auf die Bestimmung von kq ankommt, wofür man blos den Rest nach dem

Model p zu kennen braucht, so kann man wegen der Congruenz $kq\ .\ k\eta \equiv -mD$ sowohl aus $k\eta$ als auch aus mD die Reste nach p nehmen und zwar auch dann, wenn der Schreiter $2p$ wäre.

23. Die Überschreitung in der Formenperiode.

Würde dieses Verfahren blos zum Aufsuchen unbekannter trinärer Arten von D aus bekannten dienen, so wäre die Vorsicht überflüssig, mit welcher im Vorbehandelten entgegengesetzte trinäre Formen und Arten von einander unterschieden wurden, und die sich besonders bei der Bestimmung des Mittelgliedes in der zum Schreiter und seiner Gegengrösse gehörigen quadratischen Zahlformen im vorigen Nr. zeigt. Die Überschreitung steht aber in einer ganz besonderen Beziehung zur Formenperiode, und zwar der Art, dass wenn θ die Periodenlänge ist, und man

$$ft = <\alpha, \alpha', \alpha''> \qquad fu = <\beta, \beta', \beta''>$$
$$fv = (p, 2kq, h^2 + rk^2) \qquad fw = (d, 2hq', k^2 + r'h^2)$$

hat, die Formenzeiger mittelst der Congruenz

$$u \equiv t + 2v \equiv -t + 2w \ (\text{Mod. } \theta) \tag{49}$$

zusammenhängen.

Beweis. Vorerst ist zu erwähnen nöthig, dass in der Gleichung (48) p', d' prim zu einander sind. Hätten sie nämlich die Primzahl ρ zum gemeinsamen Theiler, so geht dieselbe auch in p, d auf, und es sind laut Gleichung (33) und 8. (Folgesatz) auch η, η', η'' mittelst derselben theilbar, so dass also ρ zur Grösse π gehört. Ferner folgt aus den Gleichungen (46) nach 5. Gleichung (12)

$$Q\varepsilon = P\gamma + \varepsilon'\alpha'' - \varepsilon''\alpha'$$

und

$$Q'\varepsilon = P\delta + \varepsilon'\beta'' - \varepsilon''\beta'$$

und da man nach den Gleichungen (37), (40), (47)

$$\varepsilon'\alpha'' - \varepsilon''\alpha' = ghp' + kmd', \quad \varepsilon'\beta'' - \varepsilon''\beta' = ghp' - kmd'$$

hat, so ist laut Gleichung (48)

$$Q\varepsilon = d'p'\gamma + ghp' + kmd', \quad Q'\varepsilon = d'p'\delta + ghp' - kmd'. \tag{50}$$

Diese zwei Gleichungen geben für Model p' die Congruenz

$$Q\varepsilon \equiv - Q'\varepsilon \equiv kmd';$$

aus Gleichung (28) folgt jedoch $k^2d' \equiv D'$ oder

$$- mk^2d' \equiv p'\psi - mD',$$

d. i. nach Gleichung (39)

$$- mkd' \equiv \frac{p'\psi - mD'}{k} \equiv \varepsilon kq,$$

also $- Q\varepsilon \equiv Q'\varepsilon \equiv kq\varepsilon$, und mittelst Erhöhung der Striche gelangt man auch zu

$$- Q\varepsilon' \equiv Q'\varepsilon' \equiv kq\varepsilon', \quad - Q\varepsilon'' \equiv Q'\varepsilon'' \equiv kq\varepsilon''.$$

Multiplicirt man von diesen Congruenzen die erste mit X, die zweite mit Y und die dritte mit Z, und bezeichnet $\varepsilon X + \varepsilon' Y + \varepsilon'' Z$ mit H, so gibt ihre Summe $- QH \equiv Q'H \equiv kqH$, und nimmt man X, Y, Z so, dass H zu p' prim wird, was immer möglich ist, indem $\varepsilon, \varepsilon', \varepsilon''$ keinen gemeinschaftlichen Theiler haben, so ist

(51) $$- Q \equiv Q' \equiv kq \text{ (Mod. } p').$$

Auf ähnliche Weise verfährt man mit den Gleichungen (50) rücksichtlich d', sie geben nämlich beim (Mod. d') $Q\varepsilon \equiv Q'\varepsilon \equiv ghp'$. Hierauf folgt aus Gleichung (28)

$$h^2p' \equiv D' \text{ also } gh^2p' \equiv d'\psi' + gD'$$

und nach Gleichung (44)

$$ghp' \equiv \frac{d'\psi' + gD'}{h} \equiv hq'\varepsilon,$$

was $Q\varepsilon \equiv Q'\varepsilon \equiv hq'\varepsilon$ also auch $Q\varepsilon' \equiv Q'\varepsilon' \equiv hq'\varepsilon'$ und $Q\varepsilon'' \equiv Q'\varepsilon'' \equiv hq'\varepsilon''$ folglich

(52) $$Q \equiv Q' \equiv hq' \text{ (Mod. } d')$$

liefert.

Nach der Lehre von der Bestimmbarkeit der Formen in den Perioden hat man

$$fr = p = \pi p', \quad fr = d = \pi d',$$

wobei π einer Mittelform angehört. Die Congruenzen (51) und (52) geben mit Rücksicht der Gleichung (46)

$$ft = \frac{d'}{p'} = \frac{\pi d'}{\pi p'},\ fu = p'd' = \pi p' \,.\, \pi d'$$

also

$$ft = f(w - v),\ fu = f(w + v) \text{ oder } t \equiv w - v,\ u \equiv w + v \text{ (Mod. } \theta),$$

woraus man den obigen Satz erhält.

Anmerkung. Vergleicht man die Kürze des hier aufgestellten Satzes mit seinem Beweise, so zeigt es sich, dass Gauss vollkommen Recht hat, wenn er in *Disquisitiones arithmeticae* §. 287, III, schreibt: *Haecce theoremata, ni vehementer fallimur, ad pulcherrima in theoria formarum binariarum sunt referrenda, eo magis, quod licet summa simplicitate gaudeant, tamen tam recondita sint, ut ipsarum demonstrationem rigorosam absque tot aliarum disquisitionum subsidio condere non liceat.*

24. Folgesätze.

a) Das erste, was man zu thun hat, wenn $ft = \langle\alpha, \alpha', \alpha''\rangle$ mittelst $p = m^2 + m'^2 + m''^2$ zu überschreiten kommt, ist, die trinäre Art so einzurichten, dass der Gleichung (17) entsprochen wird. Dabei ist es am gerathensten α, α', α'' zu versetzen, und m, m', m'' unverändert zu lassen, indem man dann nach 4. leicht sieht, ob hier $+\,t$ oder $-\,t$ zu nehmen ist, und man kann dann nöthigen Falls die Zeichen von α, α', α'' verändern; im Gegentheil würde sich diese Untersuchung mit der nächst folgenden verflechten. Statt der Grössen α, α', α'' kann man sich auch blos der Reste nach dem Model p, oder wenn p gerade wäre, nach $\frac{1}{2}p$ bedienen, aus der Anordnung dieser Reste ersieht man auch die Ordnung der trinären Werthe.

Ferner handelt es sich, wenn auch mittelst der Periodenverrechnung in $fv = p$, wo p am bequemsten eine Primzahl oder doppelte Primzahl ist, die Grösse v bekannt wäre, um das Vorzeichen derselben. Da sucht man nach Gleichung (36) $k\eta$ aus

$$\begin{Bmatrix} \alpha & . & \alpha' & . & \alpha'' \\ m & & m' & & m'' \end{Bmatrix} = \langle k\eta, k\eta', k\eta''\rangle$$

und es gibt die Gleichung (39)

$$kq \equiv \frac{p\psi - mD}{kq} \text{ (Mod. } p),$$

wo dann nach dem Reste, den kq beim Mod. p gibt, das Vorzeichen von v bestimmt wird. Will man aus $<\beta, \beta', \beta''>$ ein neues Resultat erhalten, so muss diese trinäre Art nach 20. wieder entsprechend versetzt werden.

Beispiel. Bei $D = 398$ wäre $f\,3 = <18, 7, 5>$ $f\,13 = (11, 6, 37)$ und $0 = 20$ bekannt, daher $t = 3$, $v = 13$, also $2v \equiv 6$. Hier ist daher $m = 1$, $m' = 1$, $m'' = 3$ und die Reste aus $\alpha, \alpha', \alpha''$ sind $-4, -4, 5$, welche in der Gestalt $5, -4, -4$ mit $1, 1, 3$ verbunden $5 - 4 - 12 = -11$ geben; es kann demnach auch $f3 = <5, 18, 7>$ zum Überschreiten genommen werden, dann ist $h = 4$, und

$$kq \equiv \frac{11\psi - 398}{47} \equiv \frac{11\psi - 2}{47} \text{ (Mod. } 11),$$

bei $\psi = 13$ wird $kq = 3$, daher v positiv zu nehmen, und man hat

$$f9 = <\beta, \beta', \beta''> = <3, -10, 17>.$$

Wegen weiterer Überschreitung findet man

$$f9 = <17, -3, 10>, h = 4$$

und $f15 = <-9, 11, 14>$. Dabei ist es nicht mehr nöthig kq zu suchen, weil man, wenn v negativ wäre, $f3$ erhalten müsste. Weiterhin gibt

$$f15 = <-11, -9, 14> \; h = 2 \text{ und } f21 = f1 = <15, 13, -2>$$
$$f1 = <-15, -2, 13> \; h = 2 \;\;\text{„}\;\; f7 = <19, 6, -1>.$$

Aus $f7$ bekäme man $f13 = f-7$, also kein neues Resultat. Übrigens hat $D = 398$ keine anderen trinären Werthe; die Schlussform (1, 398) ist nämlich wegen $\left(\frac{-1}{199}\right) = -1$ nicht reciprok, daher kommen hier die trinären Arten mit ungeraden Zeigern, nämlich

$f1 = <2, 13, 15>$, $f3 = <18, 7, 5>$, $f5 = <9, 11, 14>$, $f7 = <1, 6, 19>$, $f9 = <17, 10, 3>$ vor.

Weil hier bei $f1$, $2 + 13 = 15$, so muss nach $19. f \pm 1$ der Primzahl 3 zugehören.

b) Es geschieht aber nicht immer, dass man mittelst eines einzigen Schreiters alle trinären Arten findet. Einmal liegt der Grund darin, dass bei $p = fv$ der Zeiger v zu θ oder $\frac{1}{2}\theta$ nicht prim ist; denn wäre $\theta = \pi\theta'$ und $v = \pi v'$, so haben die Resultate

$$t,\ t + 2\pi v',\ t + 4\pi v',\ \ldots.$$

zu Zeigern, wo jedes $T \equiv t$ (Mod. 2π). Ein anderes Mal geschieht es wieder, dass man ausser der Gleichung $\alpha m + \alpha' m' + \alpha'' m'' = ph$ bei allen möglichen Versetzungen und Zeichenänderungen von $\alpha, \alpha', \alpha''$ keine durch p theilbare Zahl findet, wo daher die Operation abbricht. Zahlen, bei denen so ein Abbrechen nicht vorkommt, kann man doppelt schreitend nennen, und es gibt wirklich mehrere derartige Grössen; ausser ihnen wird es einfache Schreiter geben so wie auch Grössen, die für eine gegebene Form $<\alpha, \alpha', \alpha''>$ zu Schreitern unbrauchbar sind. Dass kleine Schreiter bequemer sein werden als grosse, ist von selbst einleuchtend.

c) Die mittelst dieses Verfahrens bei einem doppelten Schreiter gefundenen trinären Arten haben in der Periode die Zeiger $t, t + 2v, t + 4v, \ldots.$ Dies ist eine arithmetische Progression, welche nur dann die Glieder der Periode der Reihe nach darstellen kann, wenn $t = 1$ und $2v \equiv 1$ (Mod. θ) ist, was blos bei der Primzahl $D = 8\varphi + 3$ geschehen kann. In allen andern Fällen erscheint da die Hälfte der Glieder überschritten, welchem Umstande ich den Namen für diese Operation entnommen habe, da sich sonst kein passenderer darbot.

d) Die Zeiger der durch Überschreitung entstandenen trinären Arten bilden, wenn man sie mit den kleinsten Zahlen schreibt, eine Periode, und diese ist doppelt, entweder kehren da die Glieder mit dem entgegengesetzten Vorzeichen um, wie dies im Beispiele bei *a)* der Fall ist, wo man 3, 9, —5, 1, 7, —7, —1, 5, —9, —3: 3, 9 etc. hat, oder geschieht dies nicht, wie bei $D = 734$, wo $\theta = 40$ ist, wenn $t = 3$ und $2v = 8$ genommen wird, dass man 3, 11, 19, —13, —5: 3, . . . erhält.

e) Mit dem hier erwiesenen Satze stimmt auch der Umstand überein, dass $fu = <\beta, \beta', \beta''>$, wenn die Werthe m, m', m'' unverändert bleiben, zum Resultate $ft = <\alpha, \alpha', \alpha''>$ liefert. Es ist nämlich

$$\beta' m'' - \beta'' m' = m''(2hm' - \alpha') - m'(2hm'' - \alpha'')$$
$$= -(\alpha' m'' - \alpha'' m') = -kq,$$

folglich ist nach Gleichung (39)

$$\frac{p\psi - mD}{-kq} = -kq,$$

und wäre fu' die aus fu resultirende Grösse, so ist $u' = u - 2v = t$.

f) Es wäre unnütz $p = 1$ oder $p = 2$ zu Schreitern zu nehmen, da hiedurch keine neue trinäre Art zum Vorschein kommt. Aus $<\alpha, \alpha', \alpha''>$ erhält man nämlich bei

$$m = 0, \ m' = 0, \ m'' = 1, \ h = \alpha''$$

also

$$\beta = -\alpha, \ \beta' = -\alpha', \ \beta'' = \alpha''.$$

Eben so ist bei

$$m = 0, \ m' = 1, \ m'' = 1, \ h = \frac{1}{2}(\alpha' + \alpha''),$$

daher

$$\beta = -\alpha, \ \beta' = \alpha'', \ \beta'' = \alpha'.$$

In beiden Fällen zeigt sich aber das Überschreitungsgesetz richtig, indem hier $v = 0$ oder $\frac{1}{2}0$ vorkommt. Der kleinste brauchbare Schreiter ist daher 3, an den sich 5, 6, 9, 10 u. s. w. anschliesst.

g) Die Überschreitung von $<-\alpha, -\alpha', -\alpha''>$ mittelst $p = m^2 + m'^2 + m''^2$ führt zu keinem neuen Resultate; es ist hier nämlich $-\alpha m - \alpha' m' - \alpha'' m'' = -ph$ also

$$-2hm + \alpha = -\beta, \ -2hm' + \alpha' = -\beta', \ -2hm'' + \alpha'' = -\beta'',$$

wie dies auch aus Gleichung (49) wegen $\frac{p\psi - mD}{-kq} = -kq$ hervorgeht.

25. Hilfsmittel zum Überschreiten.

a) Es ist schon erwähnt worden, dass man sich, um der Gleichung (17) zu genügen, blos der Reste von $\alpha, \alpha', \alpha''$ nach Mod. p bedienen kann. Dabei ereignet sich überdies noch der Umstand, dass man in der Schreiterform $(p, 2kq, r'')$ auch zu demselben Werth von kq gelangt. Hätte man nämlich

$$<\alpha + p\varphi, \alpha' + p\varphi', \alpha'' + p\varphi''>,$$

wo φ, φ', φ'' was immer für ganze Zahlen sind, so ist die Determinante dieser trinären Art

$$D' = D + 2p(\alpha\varphi + \alpha'\varphi' + \alpha''\varphi'') + p^2(\varphi^2 + \varphi'^2 + \varphi''^2).$$

Ist ferner $(p, 2q'', \rho)$ die Form des Schreiters bei D', so wird man nach Gleichung (39) $q'' = \frac{p\psi' - mD'}{k\eta + pl}$ erhalten, wenn Kürze halber $\varphi'm'' - \varphi''m' = l$ gesetzt wird, indem

$$(\alpha' + p\varphi')m'' - (\alpha'' + p\varphi'')m' = \alpha'm'' - \alpha''m' + p(\varphi'm'' - \varphi''m')$$

liefert. Macht man ferner

$$\psi' = \psi'' + 2m(\alpha\varphi + \alpha'\varphi' + \alpha''\varphi'') + p(\varphi^2 + \varphi'^2 + \varphi''^2),$$

so übergeht $p\psi' - mD'$ in $p\psi'' - mD$, wesshalb $q'' = \frac{p\psi'' - mD}{k\eta + pl}$; nimmt man aber weiter $\psi'' = \psi + klq$, so ergibt sich laut Gleichung (39)

$$q'' \equiv \frac{p\psi - mD + klpq}{k\eta + pl} = \frac{k^2q\eta + klpq}{k\eta + pl} = kq.$$

Es sind daher die Reste der Mittelglieder in beiden Fällen gleich.

So hätte man im vorigen Nr. kq kürzer aus der Zusammenstellung $D = 398 \equiv 2$ (Mod. 11)

$$\left.\begin{matrix} 5 & & -4 & & -4 \\ 1 & . & 1 & . & 3 \end{matrix}\right\} kq \equiv \frac{11\psi - 2}{-8} = 3$$

bei $\psi = -2$ gefunden.

Man kann daher, sowohl um die Lösbarkeit der Gleichung (17) zu ermitteln, als auch um kq zu finden, sich statt α, α', α'' der Grössen a, a', a'' bedienen, welche beziehungsweise ihre kleinsten Reste nach dem Mod. p darstellen.

b) Wäre $<\alpha + m\varphi, \alpha' + m'\varphi, \alpha'' + m''\varphi>$ zu überschreiten, so hat man $D' = D + 2hp\varphi + p\varphi^2$, also

$$p\psi' - mD' = p\,(\psi' - 2hm\varphi - m\varphi^2) - mD = p\psi - mD$$

und

$$(\alpha' + m'\varphi)\,m'' - (\alpha'' + m''\varphi)\,m' = \alpha'm'' - \alpha''m' = kq.$$

also

$$\frac{p\psi' - mD'}{kq} = \frac{p\psi - mD}{kq} = kq.$$

Es hat sonach der Schreiter hier in seiner Form dasselbe Mittelglied, das er bei $<\alpha, \alpha', \alpha''>$ besitzt.

Darnach ist man im Stande bei der Determinante $D = p\psi + e$, wo $e < p$ vorkommt, aus einer Art der trinären Reste $<a, a', a''>$ alle übrigen zu finden, nach denen sich dann $<\alpha, \alpha', \alpha''>$ gehörig ordnen lässt.

c) Sind $<a, a', a''>$, $<b, b', b''>$, $<c, c', c''>$ drei nach dem Verfahren in *b)* ermittelte Arten trinärer Reste von der Determinante $D = p\psi + e$, die zu $p = m^2 + m'^2 + m''^2$ gehören, wo daher

$$b = a + m\varphi,\ \ b' = a' + m'\varphi,\ \ b'' = a'' + m''\varphi$$

und

$$c = a + m\varphi',\ \ c' = a' + m'\varphi',\ \ c'' = a'' + m''\varphi'$$

ist, und setzt man $\varphi'' = \varphi - \varphi'$, so ist

$$b - c = m\varphi'',\ \ b' - c' = m'\varphi'',\ \ b'' - c'' = m''\varphi''$$

also

$$a+b-c = a+m\varphi'',\ a'+b'-c' = a'+m'\varphi'',\ a''+b''-c'' = a''+m''\varphi'$$

und es gehört demnach $<a + b - c, a' + b' - c', a'' + b'' - c''>$ zu derselben Classe von Grössen wie die drei obigen.

Hieraus folgt auch, dass $<2a - b, 2a' - b', 2a'' - b''>$ und im Allgemeinen

$$<af - b\,(f-1),\ \ a'f - b'\,(f-1),\ \ a''f - b''\,(f-1)>$$

Grössen derselben Kategorie sind, daher ist es leicht zu entscheiden, ob gewisse trinäre Reste bei m, m', m'' vorkommen oder nicht.

d) Der Rest des Mittelgliedes in der Form des Schreiters nach dem Model $2p$ bei der Überschreitung von $<\alpha b, \alpha' b, \alpha'' b>$ ist

$= 2bkq$. Heisst nämlich z die halbe fragliche Grösse, so erhält man, da hier b^2D, $bk\eta$ statt D, $k\eta$ zu setzen ist, nach Gleichung (39)

$$z \equiv \frac{p\psi' - b^2mD}{bk\eta},$$

was bei $\psi' = b^2\psi$ in

$$z \equiv b\,\frac{p\psi - mD}{k\eta} \equiv bkq$$

übergeht.

Hat daher $D = p\lambda - 1$ beim Schreiter p die trinären Reste $<a, a', a''>$, und will man hieraus trinäre Reste desselben Schreiters für $D' = p\lambda' + e$ finden, so suche man b aus $b^2 \equiv -e$ (Mod. p), und es ist $<ab, a'b, a''b>$, wobei b negativ zu nehmen ist, wenn der kleinste Rest aus bkq (Mod. p) negativ ausfallen würde.

Öfters kommt hingegen der Fall vor, dass man die trinären Reste bei $D = p\lambda - 1$ kennt, und sucht, welche Anordnung die Grössen α, α', α'' bei $D' = p\lambda' + e$ haben müssen, um sich durch p überschreiten zu lassen. Desshalb suche man aus $bb' \equiv 1$, oder falls an b nichts gelegen wäre, aus $b'^2e \equiv -1$ (Mod. p) die Zahl b' auf, womit die Reste aus $<\alpha, \alpha', \alpha''>$ zu multipliciren sind. Kämen diese neuen Reste bei $D = p\lambda - 1$ nicht vor, so lässt sich die gegebene trinäre Art nicht durch p überschreiten.

e) Beim Schreiter $p = m'^2 + m''^2$, wo daher $m = 0$, hängt das Vorzeichen des Mittelgliedes in $(p, 2kq, r'')$ blos von α in der gegebenen trinären Art $<\alpha, \alpha', \alpha''>$ ab, d. h. es ist bei $<\alpha, \alpha', \alpha''>$ und $<\alpha, A', A''>$ gleich, mag A', A'' wie immer beschaffen sein, wenn es nur der Gleichung (17) genügt. Nach *a)* und *b)* hat man nämlich bei

$$<\alpha, \alpha' + m'\varphi + p\varphi', \ \alpha'' + m''\varphi + p\varphi''>$$

dasselbe kq, welches bei $<\alpha, \alpha', \alpha''>$ vorkommt; somit handelt es sich nur darum, ob immer für ganze Werthe von φ, φ', φ'' die Gleichungen

$$A' = \alpha + m'\varphi + p\varphi', \ A'' = \alpha'' + m''\varphi + p\varphi''$$

lösbar sind. Wird die erste mit m', die zweite mit m'' multiplicirt, so gibt ihre Summe

$$m'A' + m''A'' = \alpha'm' + \alpha''m'' + (m'^2 + m''^2)\,\varphi + pm'\varphi' + pm''\varphi''$$

und da man

$$m'A' + m''A'' = ph', \ \alpha'm' + \alpha''m'' = ph$$

hat, so gelangt man zu

$$h' = h + \varphi + m'\varphi' + m''\varphi'',$$

woraus sich φ ergibt; daher handelt es sich weiter nur darum, ob auch φ', φ'' immer ganze Zahlen sein werden. Dazu liefern uns obige Gleichungen

$$m'A'' - m''A' = m'\alpha'' - m''\alpha' + p\,(m'\varphi'' - m''\varphi').$$

Nach Gleichung (34) ist aber η wegen $m = 0$ durch p theilbar, also $m'\alpha'' - m''\alpha' = pkl$ daher auch $m'A'' - m''A' = pk'L$, woraus $m'\varphi'' - m''\varphi' = k'L - kl$ folgt, welche Gleichung immer ganze Werthe für φ', φ'' gibt, da m', m'' wie vorausgesetzt wird, prim zu einander sind.

f) Beim Schreiter $p = m'^2 + m''^2$ geben die trinären Arten $<\alpha, \alpha', \alpha''>$ und $<\alpha, -\alpha'', \alpha'>$ dasselbe Resultat. Bei der ersten hat man nämlich

$$h = \frac{\alpha'm' + \alpha''m''}{p}, \ \beta = -\alpha, \ \beta' = 2hm' - \alpha', \ \beta'' = 2hm'' - \alpha''$$

bei der zweiten hingegen

$$h' = \frac{\alpha'm'' - \alpha''m'}{p}, \ B = -\alpha, \ B' = 2h'm' + \alpha'', \ B'' = 2h'm'' - \alpha'.$$

Es ist daher $B = \beta = -\alpha$, und da ferner

$$m''h - m'h' = \frac{1}{p}\,(\alpha''m''^2 + \alpha''m'^2) = \alpha'',$$

so ergibt sich $2h'm' + \alpha'' = 2hm'' - \alpha''$ oder $B' = \beta''$, und aus

$$h'm'' + hm' = \alpha', \ 2h'm'' - \alpha' = -2hm' + \alpha', \ B'' = -\beta'.$$

g) Die Überschreitung von $<\alpha, \alpha', \alpha''>$ mit $p = m'^2 + m''^2$ und mit $2p = (m' - m'')^2 + (m' + m'')^2$ führt zu einem und demselben Resultate.

Beim ersten Schreiter hat man $hp = \alpha'm' + \alpha''m''$ und $\beta = -\alpha$, $\beta' = 2hm' - \alpha'$, $\beta'' = 2hm'' - \alpha''$, ferner ist nach Gleichung (34) $\eta = -pn$, daher nach Gleichung (36)

$$\alpha''m' - \alpha'm'' = -kq = knp.$$

Beim Schreiter $2p$ erhält man

$$2ph' = \alpha'm' - \alpha'm'' + \alpha''m' + \alpha''m'' = hp + knp,$$

d. i. $2h' = h + kn$. Man kommt demnach zu

$$B = -\alpha = \beta, B' = (h+kn)(m'-m'') - \alpha', B'' = (h+kn)(m'+m'') - \alpha''.$$

Bei diesen Umständen ergibt sich $B' = -\beta''$, $B'' = \beta'$. Rücksichtlich des Ersteren hat man

$$hm' - hm'' + km'n - km''n - \alpha' = -2hm'' + \alpha''?$$

dann nach Gleichung (27)

$$g'k + g''k + km'n - km''n = 0?, \; g' + g'' + m'n - m''n = 0?$$

wobei nach Gleichung (23) wegen $m = 0$ die Frage schwindet. Im zweiten Falle ist

$$hm' + hm'' + km'n + km''n - \alpha'' = 2hm' - \alpha'?$$
$$-g'k + g''k + km'n + km''n = 0?, \; -m'n - m''n + m'n + m''n = 0.$$

Hieraus folgt Doppeltes: Ist 1[tens] p ein doppelter Schreiter, so wäre es Arbeitsverlust mit $2p$ überschreiten zu wollen. 2[tens] Sind hingegen p mit $2p$ zusammengenommen erst doppelt überschreitend, so braucht man blos einen der Ausdrücke $<0, m', m''>$ oder $<0, m' - m'', m' + m''>$ zu berücksichtigen.

h) Auf eine ähnliche Art findet man dass $<\alpha, \alpha', \alpha''>$ mit $p = m^2 + m^2 + m''^2$ und $2p = m''^2 + m''^2 + (-2m)^2$ überschritten zu demselben Resultate führt. Es ist nämlich im ersten Falle $ph = \alpha m + \alpha'm + \alpha''m''$, dann

$$\beta = 2hm - \alpha, \;\; \beta' = 2hm - \alpha', \;\; \beta'' = 2hm'' - \alpha''$$

und im zweiten $2ph' = \alpha m'' + \alpha'm'' - 2\alpha''m$, dann

$$B = 2h'm'' - \alpha, \;\; B' = 2h'm'' - \alpha', \;\; B'' = -4h'm - \alpha''.$$

Wird die Gleichung für h mit $2m$, und jene für h' mit m'' multiplicirt, so erhält man zur Summe der Producte

$$2p\,(hm + h'm'') = p\alpha + p\alpha' \text{ oder } 2\,(hm + h'm'') = \alpha + \alpha',$$

woraus sowohl

$$2h'm'' - \alpha = -(2hm - \alpha') \text{ d. i. } B = -\beta'$$

als auch

$$2h'm'' - \alpha' = -(2hm - \alpha) \text{ oder } B' = -\beta$$

folgt.

Ferner hat man

$$phm'' = \alpha mm'' + \alpha' mm'' + \alpha'' m''^2$$

und

$$2ph'm = \alpha mm'' + \alpha' mm'' - 2\alpha'' m^2,$$

was $phm'' - 2ph'm = \alpha''(2m^2 + m''^2)$ oder $hm'' - 2h'm = \alpha''$ liefert, so dass $-4h'm - \alpha'' = -(2hm'' - \alpha'')$ d. i. $B'' = -\beta''$ zum Vorschein kommt. Die Folgen hievon sind dieselben wie im vorhergehenden Falle.

i) Beim Schreiter $p = m^2 + m^2 + m''^2$ geben die trinären Arten $<\alpha, \alpha', \alpha''>$ und $<-\alpha', -\alpha, -\alpha''>$ wie es aus den Gleichungen (36) und (39) zu ersehen ist, nicht nur gleiche Resultate, sondern auch gleiche Vorzeichen für kq. Dies dient zur Versetzung der trinären Reste $<a, a', a''>$, um so die wenigsten — Zeichen zu erhalten.

k) Die trinäre Art $<\alpha, \alpha', \alpha''>$ lässt sich im Allgemeinen mittelst $p = m^2 + m'^2 + m''^2$, falls dies überhaupt möglich ist, doppelt überschreiten, so oft unter den trinären Resten nach p oder $\frac{1}{2}p$ entweder 0 oder zwei gleiche vorkommen. Gibt nämlich $<0, a', a''>$ ein Resultat, so erhält man aus $<0, -a', -a''>$ das andere, und ist $<0, a', a''>$ schon durch Überschreitung aus einer andern trinären Art entstanden, daher nach 24. *e)* der Rest aus kq gegen die ursprüngliche Form von p negativ, so wird er hier positiv sein. Nur einige besondere Fälle, wie z. B. bei $\alpha = 0$, liefern blos e i n e neue trinäre Art.

Was die Reste $<a, a, a''>$ anbelangt, so können die a mit einander versetzt werden, wobei noch alle drei Grössen negativ zu nehmen sind, damit an $<\alpha, \alpha', \alpha''>$ dem 4. gemäss nichts geändert werde. Dass auch hier nur e i n Resultat zum Vorschein kommt, wenn $m = m'$, oder $\alpha = \alpha'$ wäre, ist leicht zu ersehen.

Überdies können jedoch noch viele andere trinäre Arten doppelt überschreitbar sein.

l) Bei $D = p\varphi - 1$ ist es nicht schwer zu m, m', m'' die trinären Reste zu finden. Es wird nämlich der Gleichung $1 \equiv \frac{p\psi + m}{k\eta}$ dadurch Genüge geleistet, dass man $k\eta \equiv m''a' - m'a'' \equiv m$ (Mod. p) setzt, so dass sich dann a, a', a'' aus

$$m''a' - m'a'' \equiv m,\ ma'' - m''a \equiv m',\ m'a - ma' \equiv m'' \text{ (Mod. } p)$$

ergibt. Bei $p = 17$ findet man z. B. aus

$$m = 2,\ m' = 2,\ m'' = 3;\ a = -7,\ a' = 0, a'' = -1.$$

Anmerkung. Um von einer Zahl p sagen zu können, sie überschreite alle trinären Arten, ist es hinreichend, dies bei einer Classe von Determinanten etwa bei $D = p\varphi - 1$ zu ermitteln, da es dann nach *d)* bei allen andern stattfinden muss. Hieraus folgt zwar noch nicht, dass ein p, welches diese Eigenschaft besitzt, doppelt schreitend sein muss, Beispiele zeigen jedoch, dass es immer geschieht, so oft nur p zu D oder $\frac{1}{2}D$ prim ist.

26. Specielle Fälle des Überschreitens.

Damit diese Operation dem gewünschten Zwecke entspreche, ist es nöthig, die obangeführten allgemeinen Regeln auf besondere Schreiter zu appliciren. Hiebei kann man für p eine Primzahl oder höchstens eine doppelte Primzahl nehmen, um so bei der geringsten Arbeit zum Ziele zu gelangen. Auch kann man vorerst p oder $\frac{1}{2}p$ zu D prim nehmen, und dann die Schreiter, die in D oder $2D$ aufgehen, unter einem behandeln. Der bequemste und kleinste unter allen ist dann der

Schreiter 3. Er kommt bei jedem $D = 3\varphi - 1$ vor, und hat $m = m' = m'' = 1$; daher $h = \frac{1}{3}(\alpha + \alpha' + \alpha'')$. Nimmt man, was v anbelangt, $fv = (3, 2, \varphi)$ oder falls $D = 24\varphi + 11$ wäre, $fv = (6, 2, 4\varphi + 2)$ an, so müssen, wenn $\langle\beta, \beta', \beta''\rangle = ft + 2v$ sein soll, α, α', α'' so gestellt werden, dass einer der Ausdrücke $\langle 0, -1, 1\rangle$, $\langle 1, 0, -1\rangle$, $\langle -1, 1, 0\rangle$ ihre trinären Reste nach dem Mod. 3 darstelle. Ist auf diese Art $\langle\beta, \beta', \beta''\rangle$ gefunden, so hat man, um hieraus ein neues Resultat zu erlangen, die Vorzeichen bei den zwei durch die Primzahl 3 nicht theilbaren trinären Werthen entgegengesetzt zu nehmen.

So hat $D = 362$ für $f1 = (6, 4, 61)$ eine Periode von $\theta = 18$ Gliedern, wo $f8 = 3$, daher man $2v \equiv -2$ hat. Ferner ist $f18 = <0, 1, 19>$; da hier nicht die obigen Reste vorkommen, so wird $f18 = <0, -1, 19>$ zu setzen sein, und aus der angeführten Regel folgt

$$
\begin{array}{rl}
 & h = 6, f-2 = <12, 13, -7> \\
f-2 = <12, -13, 7>, & h = 2, f-4 = <-8, 17, -3> \\
f-4 = <8, -17, -3>, & h = -4, f-6 = <-16, 9, -5> \\
f-6 = <16, 9, 5>, & h = 10, f-8 = <4, 11, 15>
\end{array}
$$

Da man mit $p = 3$ ausreicht, indem diese Grösse doppelt überschreitend ist, so ist es nicht nöthig 6, 9 oder 18 zu Schreitern zu gebrauchen.

Schreiter 5. Dieser erscheint bei $D = 5\varphi - 1$ und $5\varphi + 1$; er hat $m = 0$, $m' = 1$, $m'' = 2$, daher $h = \frac{1}{5}(\alpha' + 2\alpha'')$. Die trinären Reste sind im ersten Falle $<2, 0, 0>$ oder $<2, 1, 2>$ und im zweiten $<-1, 0, 0>$ oder $<-1, 1, 2>$, die auch unter den Gestalten $<2, 2, -1>$, $<2, -2, 1>$, $<2, -1, -2>$ und $<-1, 2, -1>$, $<-1, -2, 1>$, $<-1, -1, -2>$ vorkommen können, ohne jedoch andere Resultate zu liefern.

Um hier von $<\beta, \beta', \beta''>$ zu einer neuen Form zu gelangen, wird beim Überschreiten, wenn $\beta' \equiv \beta'' \equiv 0$ (Mod. 5) ist, $<-\beta, -\beta', \beta''>$; ist jedoch $\beta \equiv \beta'$ oder $\equiv \beta''$, $<\pm\beta', \mp\beta, \beta''>$ oder $<\pm\beta'', \beta', \mp\beta>$ genommen, wobei das Zeichen $\pm$ aus den obigen Resten ersichtlich ist. Daher hat auch hier diese Operation keine Schwierigkeiten.

So hat $D = 1021$ bei $f1 = (7, 2, 146)$, $\theta = 22$, und da $f4 = 5$ also $2v \equiv 8$ ist, so folgt aus

$$
\begin{array}{ll}
f22 = <-11, 0, 30>, & h = 12, \; f8 = <11, 24, 18> \\
f8 = <24, -11, 18>, & h = 5 \quad f16 = <-24, 21, 2> \\
f16 = <-21, -24, 2>, & h = -4, \; f2 = <21, 16, -18>
\end{array}
$$

u. s. w.

Schreiter 14 (Mod. 7). Hier hat man $m = 1$, $m' = 2$, $m'' = 3$ und die trinären Reste können nach dem Mod. 7 genommen werden, da h auch die Hälfte einer ungeraden Zahl sein kann.

Für $D = 7\varphi - 1$ hat man $<0, -3, 2>$, $<1, -1, -2>$, $<-1, 2, -1>$, $<2, 1, 1>$, $<-2, 0, 3>$, $<3, 3, -3>$, $<-3, -2, 0>$.

Bei $D = 7\varphi + 3$ ergeben sie sich $<0, -1, 3>$, $<1, 1, -1>$, $<2, 3, 2>$, $<3, -2, -2>$, $<-3, 0, 1>$, $<-2, 2, -3>$, $<-1, -3, 0>$.

Und bei $D = 7\varphi + 5$, $<0, -2, -1>$, $<1, 0, 2>$, $<2, 2, -2>$, $<3, -3, 1>$, $<-3, -1, -3>$, $<-2, 1, 0>$, $<-1, 3, 3>$.

So kommt bei $D = 866$ für $f1 = 5$, $f3 = 7$, $\theta = 44$, also $2v = 6$, und man erhält aus

$$f44 = <0, 5, -29>, 2h = -11, f6 = <-11, -27, -4>$$
$$f6 = <-11, 4, -27>, h = -6. f12 = <-1, -28, -9>$$
$$f12 = <1, -28, 9>, h = -2. f18 = <-5, 20, -21>$$

u. s. w.

Schreiter 11. In diesem Falle ist $m = m' = 1$, $m'' = 3$ und die trinären Reste bei $D = 11\varphi - 1$ sind

$$<0, -3, 1>, <1, -2, 4>, <2, -1, -4>, <3, 0, -1>$$
$$<4, 1, 2>, <5, 2, 5>, <-5, 3, -3>, <-4, 4, 0>$$
$$<-3, 5, 3>, <-2, -5, 5>, <-1, -4, -2>.$$

Was die übrigen vier Determinanten-Classen anbelangt, so lassen sich ihre trinären Reste leicht auf die angeführten reduciren; ist nämlich $D = 11\varphi + 2, 6, 7, 8$, so hat man beziehungsweise mit $4, 3, -5, -2$ die vorkommenden trinären Reste zu multipliciren und gelangt so zu den Resten der Determinante $11\varphi - 1$, aus deren Anordnung die vorzunehmende Versetzung der gegebenen Form ersichtlich ist. Hätte man z. B. bei $D = 541$ die trinäre Art $<6, 12, 19>$, so gibt sie die Reste $<-5, 1, -3>$, dies mit 4 multiplicirt $<2, 4, -1>$, welche Grössen oben die Anordnung $<2, -1, -4>$ besitzen, so dass man $<6, 19, -12>$ zu setzen hat, und wegen $h = -1$, $<-8, -21, 6>$ erhält.

Schreiter 26 (Mod. 13). Dieser vertritt die Stelle von 13, da letztere Zahl nicht alle Formen überschreitet. Auch werden hier, wie bei 14 Ähnliches vorkommt, die Reste nach der Hälfte d. i. nach 13 genommen. Man hat dann bei $D = 13\varphi - 1$ und $m = 0$, $m' = 1$, $m'' = 5$

$$<5, 0, 0>, <-5, 1, 5>, <-5, 2, -3>, <-5, 3, 2>,$$
$$<-5, 4, -6>, <-5, 5, -1>, <-5, 6, 4>, <-5, -6, -4>,$$
$$<-5, -5, 1>, <-5, -4, 6>, <-5, -3, -2>,$$
$$<-5, -2, 3>, <-5, -1, -5>$$

und für $m = 1$, $m' = 3$, $m'' = 4$

$$<0, -4, 3>, <1, -1, -6>, <2, 2, -2>, <3, 5, 2>,$$
$$<4, -5, 6>, <5, -2, -3>, <6, 1, 1>, <-6, 4, 5>,$$
$$<-5, -6, -4>, <-4, -3, 0>, <-3, 0, 4>, <-2, 3, -5>,$$
$$<-1, 6, -1>.$$

Was die Determinante von der linearen Form $D = 13\varphi + e$ anbelangt, so hat man bei $e = 1, 3, 4, 9, 10$ beziehungsweise mit $b' = -5, -2, -4, -6, -3$ die jeweiligen Reste zu multipliciren.

Schreiter 17. Hier hat man bei $D = 17\varphi - 1$ und $m = 0$, $m' = 1$, $m'' = 4$ die Reste

$$<4, 0, 0>, <4, 1, 4>, <4, 2, 8>, <4, 5, 3>, <4, 6, 7>,$$

bei $m = 2$, $m' = 2$, $m'' = 3$ sind sie

$$<0, 7, 1>, <1, 8, -6>, <2, -8, 4>, <3, -7, -3>,$$
$$<4, -6, 7>, <5, -5, 0>, <6, -4, -7>, <7, -3, 3>$$
$$<8, -2, -4>, <-8, -1, 6>, <-7, 0, -1>,$$
$$<-6, 1, -8>, <-5, 2, 2>, <-4, 3, -5>, <-3, 4, 5>,$$
$$<-2, 5, -2>, <-1, 6, 8>.$$

Hinsichtlich der anderen Classen hat man bei

$$e = 1, 2, 4, 8, 9, 13, 15$$

beziehungsweise mit

$$b' = -4, 5, -2, 6, 7, -8, 3$$

zu multipliciren.

Von den übrigen Primzahlen sind es nur noch 29 und 41, die jede trinäre Art und zwar doppelt überschreiten. Von doppelten Primzahlen besitzen diese Eigenschaft ausser den angeführten 6, 10, 22, 34, 38, 46, 62, 74, 86, 94, 134, 146, bei denen man auf ähnliche Art wie mit 14 und 26 verfährt. Überdies hat manchmal weder p

noch $2p$ die doppelte Überschreitung, sondern erst beide zusammen, so dass sie sich in dieser Beziehung ergänzen. Eine solche Eigenschaft fand ich bei 53 und 106 vor.

Was die Schreiter anbelangt, die in D oder $2D$ aufgehen, so scheinen sie oft eine trinäre Art doppelt überschreiten zu wollen, in der Wirklichkeit ist dies jedoch nicht der Fall; denn wenn auch den Grössen $<\alpha, \alpha', \alpha''>$ eine andere Anordnung gegeben wird, so erhält man schliesslich doch nur ein Resultat. In Ermanglung eines allgemeinen Beweises, der hier übrigens nicht so leicht aufzustellen wäre, mag dies ein specieller Fall erörtern. Bei $p = 14$ hat man $m = 1$, $m' = 2$, $m'' = 3$ und die trinären Reste $<1, 2, 3>$, $<2, -3, -1>$, $<3, -1, 2>$ u. s. w. Wäre nun $<7a + 1, 7b + 2, 7c + 3>$ zu überschreiten, so erhält man bei dieser Anordnung wegen

$$2h = a + 2b + 3c + 2,\ \beta = -6a + 2b + 3c + 1,$$
$$\beta' = 2a - 3b + 6c + 2,\quad \beta'' = 3a + 6b + 2c + 3.$$

Hätte aber dieselbe trinäre Art die Gestalt

$$<7b + 2, -7c - 3, -7a - 1>,$$

so ist $2h = -3a + b - 2c - 1$, was

$$\gamma = -3a - 6b - 2c - 3 = -\beta'',\quad \gamma' = -6a + 2b + 3c + 1 = \beta$$
$$\gamma'' = -2a + 3b - 6c - 2 = -\beta'$$

liefert. Ähnliches geschieht in allen anderen Fällen.

Dieser Schreiter kann man sich, wo es angeht, bedienen, um alle trinären Arten, die zu einer quadratischen Zahlform gehören, zu ermitteln, wenn eine bekannt ist; denn wenn p einer Mittelform angehört, so ist nach 23. stets $t = u$. So hat z. B.

$$D = 1785 = 3 \times 5 \times 7 \times 17$$

bei (26, 6, 69) die trinäre Art $a = <41, 10, 2>$; wird diese mit 3 überschritten, so liefert sie $b = <32, 20, 19>$; a mit 5 überschritten gibt $c = <10, 23, 34>$, und c mit 3, $d = <37, 20, 4>$. Wird a mit 7 behandelt, $e = <4, 13, 40>$; dann e mit 3, $f = <34, 25, 2>$; e mit 5, $g = <40, 11, 8>$, und g mit 3, $h = < 22, 25, 26 >$ (vergl. 17).

Anmerkung. Da es demnach so viele doppelte Schreiter gibt, so ereignet es sich nur bei einer sehr geringen Zahl von Determinanten, dass sich aus einer trinären Art nicht alle andern leicht ermitteln liessen. Daher gibt die Überschreitung ein bequemes Mittel an die Hand, die Gleichung $x^2 + y^2 + z^2 = D$ in ganzen Zahlen zu lösen.

27. Bestimmung der Schreiterform aus ihren beiden trinären Arten.

Zur Vollständigkeit dieser Abhandlung ist es noch nöthig zu untersuchen, welche Relationen zum Vorschein kommen, wenn aus den Werthen von $<\alpha, \alpha', \alpha''>$ $<\beta, \beta', \beta''>$ unter beliebiger Zeichenänderung und Versetzung der letzteren die Grössen m, m', m'' und p nach den Gleichungen in 20. und 22. bestimmt werden. Ist nämlich $ft = <\alpha, \alpha', \alpha''>$, $fu = <\beta, \beta', \beta''>$ und $fv = p$, so ergibt sich $2v \equiv u - t$ (Mod. θ). Da nun θ die Periodenlänge vorstellt, so hat man $v \equiv \frac{1}{2}(u - t)$ oder $\equiv \frac{1}{2}\theta + \frac{1}{2}(u-t)$, und nach dem bisher Behandelten könnte man meinen, es werde bei gewissen Versetzungen $f\frac{1}{2}\theta$ auch eine bifide Form sein können, so dass man hiedurch in den Stand gesetzt würde, jede Zahl in ihre Factoren zu zerlegen. Dass jedoch dieses nicht geschieht, erhellet aus dem Verfolge. Der erste hieher einschlägige Lehrsatz lautet:

α) Die trinäre Art $<\alpha, \alpha', \alpha''>$ liefert mit $<\beta, \beta', \beta''>$ und den hieraus mittelst Zeichnung (2. Anm. 4.) entstandenen Versionen verbunden Schreiter, die zu derselben quadratischen Zahlform gehören; d. h. sucht man aus $<\alpha, \alpha', \alpha''>$, $<\beta, \beta', \beta''>$ mittelst der Gleichungen (18), (21) und (23) die Form $(p\ 2kq,\ h^2 + rk^2)$, und ergibt sich auf eine ähnliche Art aus $<\alpha, \alpha', \alpha''>$, $<\beta, -\beta', -\beta''>$ der Schreiter P, so ist $P = (p,\ 2kq,\ h^2 + rk^2)$ bei $x = \frac{kn}{h'}$ und $y = -\frac{m}{h'}$, wenn h' den grössten gemeinsamen Theiler von m, n darstellt. Es ist nämlich bei diesem Werthe von h' nach den Gleichungen (21) und (23)

$$hm = h'M,\quad g'k = -h'M',\quad g''k = -h'M''$$

zu setzen erlaubt, so dass man

$$M = \frac{\alpha + \beta}{2h'},\ M' = \frac{\alpha' - \beta'}{2h'},\ M'' = \frac{\alpha'' - \beta''}{2h'}$$

erhält, und M, M', M'' sind nach Gleichung (18) die trinären Werthe des Schreiters von $<\alpha, \alpha', \alpha''>$, $<\beta, -\beta', -\beta''>$, wesshalb auch $P = M^2 + M'^2 + M''^2$; und setzt man in der quadratischen Zahlform

$$(p, 2kq, h^2 + rk^2),\ x = \frac{kn}{h'},\ y = -\frac{m}{h'},$$

so folgt hieraus

$$\frac{1}{h'^2}\left[k^2(pn^2 - 2qnm + rm^2) + h^2m^2\right],$$

was nach Gleichung (9), (23) in

$$\frac{1}{h'^2}(k^2g'^2 + k^2g''^2 + h^2m^2) = M^2 + M'^2 + M''^2 = P$$

übergeht. Hiebei ist $h' = \frac{l}{2}$ zu nehmen, wenn h die Hälfte einer ungeraden Zahl wäre. Auf dieselbe Art findet man, dass aus der Verbindung von $<\alpha, \alpha', \alpha''>$ mit $<-\beta, \beta', -\beta''>$ und $<-\beta, -\beta', \beta''>$ der Schreiter P in der besagten Form mit den Werthen $x = \frac{kn'}{h'}, \frac{kn''}{h'}$ und $y = -\frac{m'}{h'}, -\frac{m''}{h'}$ vorkomme, wo h' den gemeinschaftlichen Theiler von m', n' und m'', n'' darstellt.

Werden umgekehrt die analogen aus der Verbindung von $<\alpha, \alpha', \alpha''>$, $<\beta, -\beta', -\beta''>$ hervorgehenden Grössen mit $h', k', M, M', M'', N, N', N'', q', r'$ bezeichnet, so lässt sich auf eine ähnliche Art beweisen, dass

$$p = Px'^2 + 2k'q'x'y' + (h'^2 + r'k'^2)\,y'^2$$

bei

$$x' = \frac{k'N}{h} \text{ und } y' = -\frac{M}{h}.$$

β) Entsteht aus der Verbindung von $<\alpha, \alpha', \alpha''>$ mit $<\beta, \beta', \beta''>$ die Schreiterform $(p, 2kq, h^2 + rk^2)$, so kommt, wenn die letztere trinäre Art die Gestalt $<-\beta'', \beta', \beta>$ erhält, $2\,(p, 2kq, h^2 + rk^2)$ zum Vorschein.

Aus den ersten zwei Ausdrücken ergeben sich mittelst der Gleichungen (18) und (21) die Grössen

$$(a)\quad hm = \tfrac{1}{2}(\beta + \alpha),\ hm' = \tfrac{1}{2}(\beta' + \alpha'),\ hm'' = \tfrac{1}{2}(\beta'' + \alpha'')$$
$$(b)\quad gk = \tfrac{1}{2}(\beta - \alpha),\ g'k = \tfrac{1}{2}(\beta' - \alpha'),\ g''k = \tfrac{1}{2}(\beta'' - \alpha'');$$

und bezeichnet man die aus der Verbindung von $<\alpha, \alpha', \alpha''>$, $<-\beta'', \beta', \beta>$ sich ergebenden ähnlichen Zahlen mit grossen Buchstaben, so ist

$$(c)\quad HM = \tfrac{1}{2}(\alpha - \beta''),\ HM' = \tfrac{1}{2}(\alpha' + \beta'),\ HM'' = \tfrac{1}{2}(\alpha'' + \beta)$$
$$(d)\quad GK = -\tfrac{1}{2}(\beta'' + \alpha),\ G'K = \tfrac{1}{2}(\beta' - \alpha'),\ G''K = \tfrac{1}{2}(\beta - \alpha'')$$

woraus man

$$(e)\qquad <G, G', G''> = \begin{Bmatrix} M & \cdot & M' & \cdot & M'' \\ N & & N' & & N'' \end{Bmatrix} = (P, 2Q, R)$$

und

$$(f)\qquad (P, 2KQ, H^2 + RK^2)$$

zur Schreiterform erhält. Der Gegenstand dieses Abschnittes ist nun zu zeigen, dass

$$(g)\quad \begin{cases} px^2 + 2kqxy + (h^2 + rk^2)\, y^2 = 2P \\ PX^2 + 2KQXY + (H^2 + RK^2)\, Y^2 = 2p \end{cases}$$

bei

$$(h)\quad x = \frac{kn' - h}{H},\ y = -\frac{m'}{H},\ X = \frac{KN' + H}{h},\ Y = -\frac{M'}{h}.$$

In dieser Hinsicht liefern die mittleren Gleichungen *a), b), c), d)*

$$(i)\qquad hm' = HM' \text{ und } g'k = G'K$$

und aus den äusseren erhält man

$$(k)\quad \begin{cases} \alpha = h(m+m'') + H(M-M''), \alpha'' = h(-m+m'') + H(M+M'') \\ gk = -hm'' - H(M - M''),\ g''k = hm - H(M + M'') \\ GK = -h(m + m'') + HM'',\ G''K = h(m - m'') - HM \end{cases}$$

überdies folgt aus der Gleichung (17)

$$\alpha'm' = ph - H(mM - mM'' + m''M + m''M'') - h(m^2 + m''^2),$$

und da man nach Gleichung *i)*

$$ph - h(m^2 + m''^2) = hm'^2 = m'HM'$$

hat, so erhält man in Hinsicht der Gleichungen k), i)

$$\left.\begin{aligned} \alpha m' &= H[Mm' + M'(m + m'') - M''m'] \\ \alpha' m' &= H[-M(m + m'') + M'm' + M''(m - m'')] \\ \alpha'' m' &= H[Mm' - M'(m - m'') + M''m'] \end{aligned}\right\} \quad (l)$$

Wird nun in Folge dessen

$$\begin{aligned} 2pPH^2 - Dm'^2 = H^2 (M^2A + M'^2B + M''^2C + 2MM'A' \\ + 2MM''B' + 2M'M''C') \end{aligned}$$

gesetzt, so ergibt sich

$$\begin{aligned} A = (m - m'')^2,\ B = m'^2,\ C = (m + m'')^2,\ A' = (m - m'')\, m', \\ B' = (m - m'')(m + m''),\ C' = m'(m + m''), \end{aligned}$$

oder

$$2pPH^2 - Dm'^2 = H^2 (mM + m'M' + m''M'' + mM'' - m''M)^2 \quad (m)$$

Da in den Gleichungen (l) α, α', α'' prim zu einander sind, so muss H in m' aufgehen, so dass in (h) die Grösse y, daher nach (i) auch Y eine ganze Zahl wird. Ferner folgt aus (k)

$$gk \equiv - hm'' \text{ (Mod. } H),$$

wobei, wenn H die Hälfte einer ungeraden Zahl ist, der Zähler als Model angesehen wird. Überdies ergibt sich aus der Gleichung (23)

$$gk = km'n'' - km''n' \equiv - km''n' \text{ (Mod. } H)$$

oder $km''n' \equiv hm''$, so dass $\frac{m''(kn' - h)}{H}$ eine ganze Zahl wird. Dieselbe Eigenschaft besitzt, wie man durch ähnliche Schlüsse findet, auch der Ausdruck $\frac{m(kn' - h)}{H}$; da nun die Grössen m, m', m'' prim zu einander sind, so muss $kn' - h$ durch H theilbar sein, und man erhält für x in (h) eine ganze Zahl. Ferner geben die Gleichungen (33), (34) mit Rücksicht auf (k)

$$\begin{aligned} k(pn' - qm') = m.kg'' - m''.kg = h(m^2 + m''^2) \\ - H(mM + mM'' + m''M'' - m'M); \end{aligned}$$

da aber $h(m^2 + m''^2) = ph - m'HM'$, so kommt

$$p\,(kn' - h) - kqm' = -H\,(mM + m'M' + m''M'' + mM'' - m''M)$$

und nach (m)

$$[p\,(kn' - h) - kqm']^2 = 2pPH^2 - Dm'^2$$

zum Vorschein, was nach (h) in $(px + kqy)^2 = 2pP - Dy^2$ übergeht, und laut der Gleichung (29)

$$px^2 + 2kqxy + (h^2 + rk^2)y^2 = 2P$$

liefert.

Eben so ist auch die zweite der Gleichungen unter (g) richtig; aus (e) folgt nämlich

$$G = M'N'' - M''N',$$

daher ist

$$GK \equiv -KM''N' \equiv HM'' \text{ (Mod. } h),$$

also $\dfrac{M''(KN' + H)}{h}$ eine ganze Zahl und da sich dies auch von $\dfrac{M\,(KN' + H)}{h}$ nachweisen lässt, so besitzt diese Eigenschaft auch X.

Die Gleichungen (33), (34) geben überdies

$$-PKN' + QKM' = M''KG - MKG'' = H\,(M^2 + M''^2) - h\,(mM + m''M'' + mM'' - m''M),$$

was wegen

$$H\,(M^2 + M''^2) = PH - hm'M'$$

$$P\,(KN' + H) - KQM' = h\,(mM + m'M' + m''M'' + mM'' - m''M)$$

d. i.

$$(PX + KQY)^2 = 2pP - DY^2,$$

oder

$$PX^2 + 2KQXY + (H^2 + RK^2)\,Y^2 = 2p$$

liefert.

Anmerkung. Hieraus ist in Beziehung zum Punkt α) leicht zu ersehen, welchen Einfluss die Verrückung (2. Anm. 4.) einer trinären Art auf den Schreiter ausübt.

γ) Verbindet man $<\alpha, \alpha', \alpha''>$ auf die oben angeführte Weise mit dem mittelst Verschiebung aus $<\beta, \beta', \beta''>$ entstandenen Ausdrucke $<\beta', \beta'', \beta>$, so gelangt man zu

$$px^2 + 2kqxy + (h^2 + rk^2)\, y^2 = 4P \qquad (n)$$

und

$$PX^2 + 2KQXY + (H^2 + RK^2)\, Y^2 = 4p.$$

wobei

$$x = \frac{h - ks'}{H}, \quad X = \frac{H + KS'}{h}, \quad y = -\,Y = \frac{s}{H} = \frac{S}{h} \qquad (o)$$

wenn Kürze halber

$$=m+m'+m'',\ s'=n+n'+n'',\ S=M+M'+M',\ S'=N+N'+N''.$$

In diesem Falle erhält man statt der Gleichungen (c) (d)

$$HM = \tfrac{1}{2}(\alpha + \beta'),\quad HM' = \tfrac{1}{2}(\alpha' + \beta''),\quad HM'' = \tfrac{1}{2}(\alpha'' + \beta) \qquad (p)$$
$$KG = \tfrac{1}{2}(\beta' - \alpha),\quad KG' = \tfrac{1}{2}(\beta'' - \alpha'),\quad KG'' = \tfrac{1}{2}(\beta - \alpha'') \qquad (q)$$

und es geben die Gleichungen (a), (p)

$$\alpha - \alpha'' = 2hm - 2HM'',\ \alpha' - \alpha = 2hm' - 2HM,\ \alpha'' - \alpha' = 2hm'' - 2HM' \qquad (r)$$

so dass aus ihrer Summe nach der obigen Bezeichnungsweise $hs = HS$ hervorgeht. Um die Grössen α, α', α'' auf eine ähnliche Art wie im vorigen Abschnitte darzustellen, muss der Ausdruck $\alpha m + \alpha' m' + \alpha'' m'' = ph$ zu Hilfe genommen werden, so dass man zu (s)

$$\alpha s = (m^2 - m'^2 + m''^2 + 2mm'')\, h + 2H\,(m'M - m''M'')$$

oder

$$\alpha = (m - m' + m'')\, h + \frac{2H}{s}\,(m'M - m''M'') \qquad (t)$$

gelangt, woraus sich α', α'' durch höhere Streichung finden lassen.

Hat h mit H einen gemeinschaftlichen Theiler cc', so muss ihn auch s und zwar ganz enthalten; hätte nämlich s von demselben nur den Factor c', wäre also $s = c'\sigma$, so müsste in (t) $\dfrac{2\,(m'M - m''M'')}{\sigma}$ eine ganze Zahl sein, daher wäre α, und wenn man diese Schlüsse wiederholt, auch α', α'' durch c theilbar. Da man ferner der Gleichung (t) auch die Gestalt

$$= (s - 2m')\, h + \frac{2h}{S}(m'M - m''M'') = SH - \frac{2h}{S}(m'S + m'M - m$$

geben kann, so wird jenen gemeinsamen Theiler auch S besitzen, und man kann

$$h = ch', \; H = cH', \; s = cs'', \; S = cS''$$

setzen, was nach (s) $H'S'' = h's''$ liefert, und da hier h', H' prim zu einander sind, so müssen $\frac{s''}{H'} = \frac{S''}{h'}$ folglich auch y, Y in (o) ganze Zahlen sein.

Ferner gibt die Gleichung (r) $\alpha' - \alpha'' \equiv -2hm''$ (Mod. H) und da nach Gleichung (s) $h(m + m' + m'') \equiv 0$ (Mod. H) ist, $\alpha' - \alpha'' \equiv hm + hm' - hm''$ d. i. $\alpha' - hm' - (\alpha'' - hm'') \equiv hm$ oder nach Gleichung (27) $g''k - g'k \equiv hm$, was laut Gleichung (23) in $k(mn' - m'n - m''n + mn'') \equiv hm$, und weiterhin in

$$k[-n(s-m) + m(n'+n'')] \equiv km(n+n'+n'') \equiv kms' \equiv hm$$

übergeht, so dass $\frac{m(h-ks')}{H}$, folglich auch $\frac{m'(h-ks')}{H}$, $\frac{m''(h-ks')}{H}$ ganze Zahlen werden.

Da überdies m, m', m'' keinen gemeinschaftlichen Theiler haben, so muss auch $\frac{h-ks'}{H} = x$ eine ganze Zahl sein, wie dies die Gleichung (o) fordert. Eben so gelangt man von $\alpha' - \alpha'' \equiv 2HM'$ (Mod. h) d. i. $\alpha' - \alpha'' \equiv -HM + HM' - HM''$ oder

$$\alpha' - HM' - (\alpha'' - HM'') \equiv -HM \text{ zu } KG'' - KG' \equiv -HM,$$

was in

$$K(MN' - M'N - M''N + MN'') \equiv K[-N(S-M) + M(N'+N'')]$$
$$\equiv KMS' \equiv -HM$$

übergeht, so dass $\frac{M(H+KS')}{h}$ folglich auch X eine ganze Zahl wird. Bei diesen Congruenzen wird, wie leicht zu ersehen ist, statt H, wenn es ein Bruch mit dem Nenner 2 wäre, blos der Zähler zu nehmen sein. Dies vorausgeschickt erhält man wegen $\frac{hs}{H} = S$ aus der Gleichung (t)

$$\alpha y = (m - m' + m'')(M + M' + M'') + 2m'M - 2m''M''$$

oder

$$\left.\begin{array}{l}\alpha y=(\ \ m+m'+m'')M+(\ \ m-m'+m'')M'+(m-m'-m'')M'' \\ \text{daher auch} \\ \alpha' y=(-m+m'-m'')M+(\ \ m+m'+m'')M'+(m+m'-m'')M'' \\ \text{und} \\ \alpha'' y=(-m+m'+m'')M+(-m-m'+m'')M'+(m+m'+m'')M''\end{array}\right\} \quad (u)$$

Setzt man ferner in Folge der Werthe von

$$p=m^2+m'^2+m''^2,\ P=M^2+M'^2+M''^2,\ D=\alpha^2+\alpha'^2+\alpha''^2$$

und der Gleichungen (u)

$$4pP-Dy^2=M^2A+M'^2B+M''^2C+2MM'A'+2MM''B'+2M'M''C'$$

so gibt die Summirung

$$\begin{aligned}A &= (m+m'-m'')^2,\ B=(-m+m'+m'')^2,\ C=(m-m'+m'')^2 \\ A' &= (m+m'-m'')(-m+m'+m''), \\ B' &= (m+m'-m'')(m-m'+m''), \\ C' &= (-m+m'+m'')(m-m'+m'');\end{aligned}$$

daher ist

$$\begin{aligned}4pP-Dy^2 = [(m+m'-m'')M+(-m+m'+m'')M' \\ +(m-m'+m'')M'']^2\end{aligned} \quad (v)$$

Aus den Gleichungen (33) und (34) ergibt sich

$$pn-qm=m''g'-m'g'',\ pn'-qm'=mg''-m''g.$$
$$pn''-qm''=m'g-mg'.$$

wovon die Summe in

$$pks'-qks=m(kg''-kg')+m'(kg-kg'')+m''(kg'-kg)$$

übergeht, welche wieder nach Gleichung (27) weil

$$m(m''-m')+m'(m-m'')+m''(m'-m)=0$$

ist,

$$pks'-qks=m(\alpha'-\alpha'')+m'(\alpha''-\alpha)+m''(\alpha-\alpha')$$

liefert. Multiplicirt man diesen Ausdruck mit $\frac{s}{H}=y$, so gibt er laut der Gleichungen (u)

$$\frac{s}{H}\,(pks' - qks) = 2\,(m''^2 - mm')\,M + 2\,(m^2 - m'm'')\,M + 2\,(m'^2 - mm'')\,M'',$$

und wird diese Formel von

$$\frac{s}{H}\,ph = pS = (m^2 + m'^2 + m''^2)\,(M + M' + M'')$$

subtrahirt,

$$\frac{s}{H}\,[p\,(h - ks') + qks] = [(m + m')^2 - m''^2]\,M + [-m^2 + (m' + m'')^2]\,M' + [(m + m'')^2 - m'^2]\,M'',$$

was auch in

$$px + kqy = (m + m' - m'')\,M + (-m + m' + m'')\,M' + (m - m' + m'')\,M''$$

übergeht, so dass hieraus nach Gleichung (v)

$$(px + kqy)^2 = 4pP - Dy^2 = 4pP - [p\,(h^2 + rk^2) - k^2q^2]\,y^2$$

oder

$$px^2 + 2kqxy + (h^2 + rk^2)\,y^2 = 4P$$

folgt, wie es unter (u) angegeben erscheint.

Es ist aber auch die zweite der daselbst angeführten Gleichungen richtig; denn aus

$$PN - QM = M''G' - M'G'',\ PN' - QM' = MG'' - M''G,\ PN'' - QM'' = M'G - MG'$$

erhält man

$$PKS' - QKS = M\,(KG'' - KG') + M'\,(KG - KG'') + M''\,(KG' - KG)$$

oder

$$PKS' - KQS = M\,(\alpha' - \alpha'') + M'\,(\alpha'' - \alpha) + M''\,(\alpha - \alpha'),$$

welche Gleichung mit $\frac{S}{h} = y$ multiplicirt und nach (u) summirt

$$\frac{S}{h}\,(PKS' - KQS) = m\,(-2M'^2 + 2MM'') + m'\,(-2\,M''^2 + 2MM') + m''\,(2M'M'' - 2M^2)$$

liefert, was zu

$$\frac{S}{h}\, PH = Ps = (M^2 + M'^2 + M''^2)\,(m + m' + m'')$$

addirt

$$\frac{S}{h}\,[P\,(H + KS') - KQS] = m\,[(M + M'')^2 - M'^2]$$
$$+ m'\,[(M + M')^2 - M''^2] + m''\,[(M' + M'')^2 - M^2]$$

gibt, so dass man

$$\begin{aligned} PX + KQY &= m\,(M - M' + M'') + m'\,(M + M' - M'') \\ &+ m''\,(-M + M' + M'') = (m + m' - m'')\,M \\ &+ (-m + m' + m'')\,M' + (m - m' + m'')\,M'' \\ &= \sqrt{4pP - DY^2} \end{aligned}$$

erhält, was schliesslich in

$$PX^2 + 2KQXY + (H^2 + RK^2) = 4p$$

übergeht.

28. Folgesätze.

a) Werden die beiden zu verbindenden trinären Arten auf gleiche Weise verschoben, so ändert sich an h, k nichts, nur m, m', m'' g, g', g'' erscheinen eben so verschoben, daher erhält man dieselbe Schreiterform zum Resultat, welche $<\alpha, \alpha', \alpha''>$ mit $<\beta, \beta', \beta''>$ liefert.

Eben so gibt $<\alpha, -\alpha', -\alpha''>$ $<\beta, -\beta', -\beta''>$ die Schreiterform $(p, 2kq, h^2 + rk^2)$; denn man hat hier nach der üblichen Anordnung

$$<g, -g', -g''> = \begin{Bmatrix} m & . & -m' & . & -m'' \\ n & & -n' & & -n'' \end{Bmatrix} = (p, 2q, r).$$

Aus $<-\alpha, \alpha', \alpha''>$ mit $<-\beta, \beta', \beta'')$ erhält man hingegen

$$<-g, g', g''> = \begin{Bmatrix} -m & . & m' & . & m'' \\ n & & -n' & & -n'' \end{Bmatrix} = (p, -2q, r)$$

also $(p, -2kq, h^2 + rk^2)$, wie dies zum Theile auch aus 23. folgt.

Demnach kann der ersten der zu verbindenden trinären Arten immer die normale Gestalt gegeben werden.

b) Verwechselt man bei dieser Operation die zwei trinären Arten unter einander, d. h. verbindet man $<\beta, \beta', \beta''>$ mit $<\alpha, \alpha', \alpha''>$, so behalten die Grössen m, m', m'', h, k, ihre Werthe g, g', g'' werden aber negativ; man erhält somit

$$<-g, -g', -g''> = \left\{\begin{matrix} m & \cdot & m' & \cdot & m'' \\ -n & & -n' & & -n'' \end{matrix}\right\},$$

und es ist $(p, -2kq, h^2 + rk^2)$ dieselbe nur negative Schreiterform, welche $<\alpha, \alpha', \alpha''>$ mit $<\beta, \beta', \beta''>$ verbunden gibt.

c) Wird bei $D = 4\varphi + 1$ oder $4\varphi + 2$ die trinäre Art $<\alpha, \alpha', \alpha''>$ mit $<\beta, \beta', \beta''>$ unter verschiedenen Versionen der letzteren Grössen (4.) verbunden, so haben auf die Schreiterform die Verschiebungen (27. γ) keinen Einfluss; denn in den Formen dieser Determinante kommen keine Zahlen von der Gestalt $4p$ vor, wesshalb x, y, X, Y gerade sein müssen. Betrachtet man daher sämmtliche 24 Versetzungen, von β, β', β'', so zerfallen sie in zwei Gruppen von je 12 Complexionen. Alle Complexionen einer Gruppe geben mit $<\alpha, \alpha', \alpha''>$ verbunden dasselbe p; ist aber p' die Schreiterform der zweiten Gruppe, so hat man zwischen diesen beiden Grössen die Relation $p' = 2p$. Die eine Gruppe entsteht aus $<\beta, \beta', \beta''>$ die andere hingegen aus $<-\beta'', -\beta', -\beta>$ mittelst Zeichnung und Verschiebung.

d) Was die Determinante $D = 8\varphi + 3$ anbelangt, so entsprechen bei derselben jeder ungeraden quadratischen Zahlform (a, b, c) vier Formen mit geraden Mittelgliedern, nämlich die uneigentliche Form $(2a, 2b, 2c)$, dann die Formen $(a, 2b, 4c)$, $(4a, 2b, c)$, $(4a, -4a + 2b, a - b + c)$; daher gehören zu zwei trinären Arten vier Schreiterformen, und die Versionen von $<\beta, \beta', \beta''>$ zerfallen in 4 Gruppen. Ist nämlich der aus der Verbindung von $<\alpha, \alpha', \alpha''>$ mit $<\beta, \beta', \beta''>$ resultirende Schreiter ungerade, also die Form etwa $p = (a, 2b, 4c)$, so liefert die Verbindung mit $<-\beta'', -\beta', -\beta>$ die Grösse $2p = (2a, 2b, 2c)$, welcher Form nach 27. α), (γ) eine Gruppe von 12 Complexionen angehört. Die übrigen 12 Complexionen geben ungerade Schreiter, und es gehören von ihnen nach α) je vier zu einer Gruppe; werden überdies die Resultate aus der Verbindung von $<\alpha, \alpha', \alpha''>$ mit

$<\beta, \beta', \beta''>$, $<\beta', \beta'', \beta>$, $<\beta'', \beta, \beta'>$ mit p, p', p'' bezeichnet, so herrscht unter diesen Schreiterformen die Beziehung, dass man $p' = ep$, $p'' = ep'$ und eben so auch $p = ep''$ hat, wobei $e = \left(4, 2i, \frac{D+1}{4}\right)$ und $i = \pm 1 \equiv -(\alpha + \alpha' + \alpha'')$ (Mod. 4) bedeutet. Dieser letztere Umstand lässt sich auf folgende Art erweisen:

Nach (γ) hat man

$$4p = p'X^2 + 2KQXY + (H^2 + RK^2)\,Y^2,$$

wobei p in $(p', 2KQ, H^2 + RK^2)$ in Folge der Gleichung (49) auf dieselbe Art bestimmt erscheint, wie in $(p, 2kq, h^2 + rk^2)$, so dass es sich weiterhin nur um die Bestimmbarkeit von 4 oder

$$e = \left(4, 2i, \frac{D+1}{4}\right)$$

handelt. Sucht man desshalb mittelst $\nu X - \mu Y = 1$ die Grössen μ, ν auf, und setzt $t = X\varphi + \mu\psi$, $u = Y\varphi + \nu\psi$, so gelangt man zu

$$p't^2 + 2KQtu + (H^2 + RK^2)u^2 = 4p\varphi^2 + 2A\varphi\psi + B\psi^2,$$

wobei

$$A = \mu p'X + (\mu Y + \nu X)\,KQ + \nu Y\,(H^2 + RK^2).$$

Da aber hier p ungerade ist, so wird auch s, S, h, H, Y unpaar sein, und in der obigen diophantischen Gleichung ist es immerhin erlaubt $\nu \equiv 0$ (Mod. 4), also auch $\mu Y \equiv -1$ oder $\mu \equiv -Y$ und $A \equiv \mu p'X + \mu YKQ$ zu nehmen. Nach der vorletzten Gleichung in 27. ist jedoch $p'X + KQY = sS - 2l$, wenn

$$l = mM' + m'M'' + m''M,$$

daher wegen $hY = -S$ oder $sS = -shY$,

$$p'X + KQY = -shY - 2l, \text{ und } A \equiv shY^2 + 2lY,$$

d. i. $A \equiv sh + 2l$ (Mod. 4), wo es sich in Bezug auf l nur darum handelt, ob es gerade oder ungerade ist.

Um nun zu erweisen, dass $A \equiv i \equiv -(\alpha + \alpha' + \alpha'')$ (Mod. 4), kann man sich offenbar statt $\alpha, \alpha', \alpha'', h, \beta, \beta', \beta''$ blos der Reste nach dem Mod. 4 bedienen, und da ergeben sich in

Betracht dessen, dass p ungerade ist und $h \equiv 1$ genommen werden kann, folgende 8 Fälle als die allgemeinen Repräsentanten der Verbindung von $<\alpha, \alpha', \alpha''>$ mit $<\beta, \beta', \beta''>$ nämlich

$$\left.\begin{matrix}<1, & 1, & 1>\\ <1, & 1, & 1>\end{matrix}\right) \quad \left.\begin{matrix}<1, & 1. & 1>\\ <1, & -1, & -1>\end{matrix}\right) \quad \left.\begin{matrix}< \;1, & 1, & -1\\ < \;1, & 1, & -1\end{matrix}\right) \quad \left.\begin{matrix}< \;1, & 1, & -1>\\ <-1, & -1, & -1>\end{matrix}\right)$$

$$\left.\begin{matrix}<1, & -1, & -1>\\ <1, & 1, & 1>\end{matrix}\right) \quad \left.\begin{matrix}<1, & -1, & -1>\\ <1, & -1, & -1>\end{matrix}\right) \quad \left.\begin{matrix}<-1, & -1, & -1\\ < \;1, & 1, & -1\end{matrix}\right) \quad \left.\begin{matrix}<-1, & -1, & -1>\\ <-1. & -1, & -1>\end{matrix}\right)$$

in denen allen man $A \equiv i$ findet; so ist z. B. im 6. Falle

$$i \equiv 1, \; m \equiv 1, \; m' \equiv -1, \; m'' \equiv -1$$

also $\quad s \equiv -1$, dann $M \equiv 0$. $M' \equiv -1$, $M'' \equiv 0$

und $l \equiv -1$, folglich $A \equiv -1 - 2 \equiv 1 \equiv i$.

Es kann daher in Hinsicht der Bestimmbarkeit der Formen $p' = ep$, folglich auch $p'' = ep$ oder $\frac{p}{e}$ so wie $p = ep''$ gesetzt werden.

So sind die Schreiterformen, welche bei $D = 395$ aus der Verbindung von $<7, 11, 15>$ mit $<1, 13, 15>$, $<13, 15, 1>$, $<15, 1, 13>$ entstehen $(17, 16, 27)$, $(7, 4, 57)$, $(15, 10, 28)$, und man findet wegen $i = -1$, $(7, 4, 57) : (17, 16, 27) =$

$$= (15, 10, 28) : (7, 4, 57) = (17, 16, 27) : (15, 10, 28)$$
$$= (4, -2, 99).$$

e) Wird bei diesen Verbindungen $\beta = \alpha$, $\beta' = \alpha'$, $\beta'' = \alpha''$ gesetzt, so hat man bei der Voraussetzung, dass die trinäre Art eine eigentliche ist,

$$h = 1, \; m = \alpha, \; m' = \alpha', \; m'' = \alpha'', \; g = g' = g'' = 0;$$

daher erhält man $(1, D)$ zur Schreiterform.

Ist demnach $D = 4\varphi + 1$ oder $4\varphi + 2$, so gibt $<\alpha, \alpha', \alpha''>$ mit sich selbst und mit den übrigen 11 hieraus durch Zeichnung und Verschiebung entstandenen Complexionen verbunden die Schlussform zum Resultate; aus der Verbindung mit Versetzungen der zweiten Gruppe kommt hingegen die Form $\left(2, 2\psi, \frac{D + \psi^2}{2}\right)$ zum Vorschein.

Bei $D = 8\varphi + 3$ gehen jedoch $<\alpha, \alpha', \alpha''>$, $<\alpha', \alpha'', \alpha>$, $<\alpha'', \alpha, \alpha'>$ und ihre Zeichnungen beziehungsweise

$$(1, D), \left(4, 2i, \frac{D+1}{2}\right), \left(4, -2i, \frac{D+1}{2}\right)$$

zu Schreiterformen; wo hingegen $<-\alpha'', -\alpha', -\alpha>$ und sämmtliche hieraus mittelst Zeichnung und Verschiebung entstandenen Complexionen Schreiter geben, die in $\left(2, 2, \frac{D+1}{2}\right)$ vorkommen.

f) Nimmt man in 23. $u = -t$ an, und verbindet in Folge dessen $<\alpha, \alpha', -\alpha''>$ mit $<\alpha, \alpha', \alpha''>$, so ergibt sich

$$m = \frac{\alpha}{h}, \; m' = \frac{\alpha'}{h}, \; m'' = 0, \; g = 0, \; g' = 0, \; g'' = 1, \; k = \alpha''$$

und sucht man wegen

$$<0, 0, 1> = \begin{Bmatrix} m & . & m' & . & o \\ n & & n' & & o \end{Bmatrix}, \; n, n' \text{ aus } mn' - m'n = 1,$$

so findet man

$$fu = \left(\frac{\alpha^2+\alpha'^2}{h}, 2\alpha''q, h^2+r\alpha''^2\right) = \begin{Bmatrix} -m' & . & m & . & 0 \\ -\alpha''n' & & \alpha''n & & h \end{Bmatrix} = <\alpha, \alpha', \alpha''>,$$

wenn $q = mn + m'n'$ und $r = n^2 + n'^2$ gesetzt wird. Dass hierin der Grundgedanke zu der in 6. angeführten zweiten Methode $<\alpha, \alpha', \alpha''>$ in eine trinäre Form zu verwandeln, enthalten ist, leuchtet von selbst ein.

g) Sind die trinären Arten $<\alpha, \alpha', \alpha''>$, $<\beta, \beta', \beta''>$ von einander verschieden, gehören sie aber zu derselben quadratischen Zahlform, so ist die Schreiterform eine bifide; denn da hier $t = u$ ist, so muss $2v \equiv 0$ (Mod. θ) sein. fv kann aber nie $(1, D)$ werden, weil darin nach Gleichung (28) blos 1 oder D Schreiter sein könnte und daher die trinären Arten gleich sein müssten. Und kann dieser Umstand bei $(1, D)$ nicht vorkommen, so ereignet er sich auch bei $\left(2, 2\psi, \frac{D+\psi^2}{2}\right)$ oder $\left(4, 2i, \frac{D+1}{4}\right)$ nicht. Daher ist nur der Fall möglich, dass fv eine bifide Form gibt, und man bei einer andern Anordnung der trinären Werthe nebst dem noch $2fv$ oder $4fv$ erhält.

29. Aus einer quadratischen Zahlform, deren Determinante trinär ist, die Quadratwurzel zu ziehen.

Ist $fm = (P, 2Q, R)$ die gegebene Form, und hat man bei was immer für einem Werthe von t, $ft = <\alpha, \alpha', \alpha''>$, so wird $f(t+m)$ eine reciproke daher auch trinäre Zahlform sein, falls nur die Aufgabe überhaupt lösbar ist, und man findet $f(t+m) = <\beta, \beta', \beta''>$. Verbindet man diese beiden trinären Arten mit einander, so erhält man wegen $u = t + m$, $v = \frac{1}{2}m$ oder $\frac{1}{2}(0 + m)$ und

$$fv = (p, 2kq, h^2 + rk^2),$$

welcher Ausdruck zum Quadrate erhoben die obige Form liefert, daher als die Quadratwurzel derselben anzusehen ist.

Am leichtesten ist diese Aufgabe dann zu lösen, wenn

$$f0 = <o, \alpha, \alpha'> \text{ oder } <\alpha, \alpha, \alpha'> \text{ und } fm = f(m+0) = <\beta, \beta', \beta''>$$

bekannt wäre, da man dann nur die beiden gegebenen trinären Arten mit einander zu verbinden hat.

Übrigens gehört dieser Gegenstand mehr in das Bereich der Theorie, indem es in den meisten Fällen schwer ist, zu $f(t + m)$ die trinäre Art zu finden; daher kann auch die weitere Auseinandersetzung dieser Aufgabe füglich unterlassen werden.

30. Bemerkungen über die Zerlegung der Zahlen in ihre Factoren mittelst dieser Theorie.

Entsprechen einer quadratischen Zahlform zwei trinäre Arten, so lässt sich aus ihrer Verbindung nach 28. γ) eine bifide Form ermitteln, wodurch die Determinante in zwei Factoren zerlegt wird. Sind jedoch nicht nur die trinären Arten sondern auch die trinären Formen bekannt, so erreicht man kürzer denselben Zweck auf folgende Weise:

Nach Gleichung (9) hat man $D - \alpha^2 = pn^2 - 2qnm + rm^2$, was auch $pD - p\alpha^2 = (pn - qm)^2 + Dm^2$ gibt, so dass man hieraus nach Gleichung (12) die Congruenz $\eta^2 \equiv -p\alpha^2$ (Mod. D) erhält. Eben so liefert die zweite trinäre Art $<\beta, \beta', \beta''>$, $Y^2 \equiv -p\beta^2$, und es ist das Product dieser beiden Ausdrücke $(\eta Y)^2 \equiv (p\alpha\beta)^2$ oder $(\eta Y + p\alpha\beta)(\eta Y - p\alpha\beta) \equiv 0$, so dass D

mit $\eta Y + p\alpha\beta$ einen, und mit $\eta Y - p\alpha\beta$ den andern Factor gemein hat.

Eine einzige trinäre Art mit sich selbst auf diese Weise verbunden, zerlegt jedoch D nicht in die Factoren, indem nach der Gleichung (16) die Determinante in $\eta\eta' + \alpha\alpha' p$ aufgeht.

Eigenthümlich ist hier der Umstand, dass diese Verbindungsart der Ausdrücke $<\alpha, \alpha', \alpha''>$, $<\beta, \beta', \beta''>$ dieselben Factoren von D liefert, wie die bifide Form in 28. *g)*.

Anmerkung. Würde man eine neue Regel finden, mittelst der sich jede quadratische Zahlform leicht in eine trinäre verwandeln liesse, dann wäre das Problem der Factorenzerlegung gelöst; doch bisher ist dies bei grossen Determinanten sehr schwer, indem die Methode in 5. *f)* nur bei kleinen D brauchbar ist, und jene in 18. die Factoren von D voraussetzt, um die Werthe von f, g zu ermitteln. Wie man leicht sehen kann, war die Auffindung einer allgemeinen leicht anwendbaren Theilbarkeitsregel das Ziel der vorstehenden Untersuchungen. Der besagte Zweck ist zwar nicht erreicht worden, aber es werden diese Zeilen, wenn ja eine solche Regel existirt, sicher ihr Schärflein zur Entdeckung derselben beitragen.