Werk

Titel: Vorlesungen über Zahlentheorie

Autor: Dirichlet, Peter

Verlag: Vieweg

Ort: Braunschweig

Jahr: 1871

Kollektion: Mathematica

Werk Id: PPN30976923X

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN30976923X|LOG_0061

OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

Contact

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

Vierter Abschnitt.

Von den quadratischen Formen.

§. 53.

Unter einer *Form* versteht man in der Zahlentheorie im Allgemeinen eine ganze rationale Function von Variabeln, deren Coefficienten ganze Zahlen sind (vergl. §. 39). Je nach dem Grade derselben unterscheidet man *lineare*, *quadratische*, *cubische* Formen u. s. w.; je nach der Anzahl der vorkommenden Variabeln spricht man von *binären*, *ternären* Formen u. s. w. Wir werden uns im Folgenden ausschliesslich mit Ausdrücken von der Form

$$ax^2 + 2bxy + cy^2$$

beschäftigen, wo a, b, c bestimmte, gegebene ganze Zahlen, x und y aber unbestimmte, variabele ganze Zahlen bedeuten; und wir werden diese homogenen binären quadratischen Formen, wo kein Missverständniss zu besorgen ist, kurz Formen nennen.

Wir haben dem Coefficienten des Productes xy der beiden Variabeln gleich die Gestalt einer geraden Zahl $2b$ gegeben, weil die Untersuchung dadurch erleichtert wird; sollte in einer Form dieser Coefficient eine ungerade Zahl sein, so würde es genügen, die ganze Form mit 2 zu multipliciren, um diesen Fall auf den obigen zurückzuführen, und aus den Eigenschaften der so erhaltenen Form würde man mit Leichtigkeit auf die Eigenschaften der ursprünglichen Form zurückschliessen können.

Sind die drei Glieder in der obigen Anordnung geschrieben, so nennt man a den *ersten*, b (nicht $2b$) den *zweiten*, c den *dritten Coefficienten*; a und c fasst man auch wohl unter dem gemeinschaftlichen Namen der *äusseren* Coefficienten zusammen, und nennt dann b im Gegensatz den *mittlern* Coefficienten; ähnlich heisst x die *erste*, y die *zweite Variabele*. Eine solche Form bezeichnet man wohl auch kurz durch das Symbol (a, b, c), wenn es sich nur darum handelt, die Coefficienten anzugeben, von denen allein die Eigenschaften der Form abhängen können.

Wir schliessen nun ein für alle Mal die Fälle aus, in welchen die Form sich in zwei lineare Factoren mit *rationalen* Coefficienten zerfällen lässt, weil diese eine andere und zwar einfachere Behandlung gestatten. Zunächst folgt hieraus, dass in den Formen, mit welchen allein wir uns beschäftigen wollen, keiner der äusseren Coefficienten gleich Null sein wird; da ferner

$$ax^2 + 2bxy + cy^2 = \frac{1}{a}\left((ax + by)^2 - (b^2 - ac)y^2\right)$$

ist, so ergiebt sich weiter, dass die Zahl $b^2 - ac$ nie eine vollständige Quadratzahl sein darf, denn sonst würde die Form

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

$$\frac{1}{a}\left(ax + (b + \sqrt{b^2 - ac})\,y\right)\left(ax + (b - \sqrt{b^2 - ac})\,y\right)$$

ein Product aus zwei linearen Factoren mit rationalen Coefficienten sein. Die Zahl $b^2 - ac$, von welcher, wie wir sehen werden, die Eigenschaften der Form (a, b, c) hauptsächlich abhängen, heisst die *Determinante**) dieser Form; wir werden sie im Folgenden mit dem Buchstaben D bezeichnen. Die unseren Formen (a, b, c) auferlegte Beschränkung besteht also darin, dass D *kein Quadrat* ist.

Euler hat sich zuerst mit solchen Formen, aber nur von specieller Natur, beschäftigt; erst *Lagrange* legte den Grund zu einer allgemeinen Theorie derselben, die dann später von *Legendre*, vor Allen aber durch *Gauss* vervollständigt wurde.

Ihre Entstehung verdankt die ganze Theorie dem Probleme, zu entscheiden, ob eine gegebene Zahl m durch die gegebene Form (a, b, c) *darstellbar* ist, d. h. ob es specielle Werthe von x, y giebt, für welche die Form den Werth m erhält. Doch ist zur vollständigen

*) *Gauss: D. A.* art. 154.

Lösung desselben die Theorie der *Transformation* erforderlich, mit welcher wir uns zunächst beschäftigen wollen.

§. 54.

Ebenso wie die Gleichungen der Curven in der analytischen Geometrie ihre Gestalt ändern, wenn ein anderes Coordinatensystem gewählt wird, so geht eine quadratische Form (a, b, c) durch Einführung zweier neuen Variabeln in eine neue quadratische Form (a', b', c') über. Sind nämlich x, y die Variabeln der Form (a, b, c), und setzt man

$$\begin{aligned} x &= \alpha x' + \beta y', \\ y &= \gamma x' + \delta y', \end{aligned} \tag{1}$$

wo $\alpha, \beta, \gamma, \delta$ vier bestimmte ganze Zahlen, und x', y' die neuen Variabeln bedeuten, so wird

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

und die Coefficienten a', b', c' der neuen quadratischen Form hängen auf folgende Weise von denen der ursprünglichen Form und von den vier Coefficienten $\alpha, \beta, \gamma, \delta$ ab:

$$\begin{aligned} a' &= a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \\ b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ c' &= a\beta^2 + 2b\beta\delta + c\delta^2. \end{aligned} \tag{2}$$

Man drückt den Zusammenhang der beiden Formen kurz so aus: die Form $ax^2 + 2bxy + cy^2$ geht durch die *Transformation* oder *Substitution* (1) in die Form $a'x'^2 + 2b'x'y' + c'y'^2$ über. Die Zahlen $\alpha, \beta, \gamma, \delta$ heissen der Reihe nach der *erste, zweite, dritte, vierte Coefficient* der Substitution. Da die Wahl der Buchstaben zur Bezeichnung der Variabeln von ganz untergeordneter Bedeutung ist, und die Natur der Formen und Substitutionen nur von den Coefficienten abhängt, so drückt man sich häufig noch kürzer so aus: die Form (a, b, c) geht durch die Substitution $\alpha, \beta, \gamma, \delta$ oder $\left(\begin{smallmatrix}\alpha, & \beta \\ \gamma, & \delta\end{smallmatrix}\right)$ in die Form (a', b', c') über; und diese Ausdrucksweise soll nicht mehr oder weniger sagen, als dass die drei Gleichungen (2) Statt finden. Hierbei ist wohl auf die Stellung der Coefficienten der Formen sowohl, wie derjenigen der Substi-

tution zu achten; behalten wir die eben eingeführten Bezeichnungen bei, so müssen wir z. B. sagen, dass gleichzeitig die Form

$$(a, b, c) \text{ durch die Substitution } \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \text{ in } (a', b', c'),$$

$$(a, b, c) \quad „ \quad „ \quad „ \quad \begin{pmatrix} \beta, & \alpha \\ \delta, & \gamma \end{pmatrix} \quad „ \quad (c', b', a'),$$

$$(c, b, a) \quad „ \quad „ \quad „ \quad \begin{pmatrix} \gamma, & \delta \\ \alpha, & \beta \end{pmatrix} \quad „ \quad (a', b', c'),$$

$$(c, b, a) \quad „ \quad „ \quad „ \quad \begin{pmatrix} \delta, & \gamma \\ \beta, & \alpha \end{pmatrix} \quad „ \quad (c', b', a')$$

übergeht.

Es leuchtet ein, dass jede durch die zweite Form (a', b', c') darstellbare Zahl auch durch die erste Form (a, b, c) dargestellt werden kann; denn wird die Zahl m durch (a', b', c') dargestellt, indem den Variabeln x', y' die speciellen Werthe r', s' ertheilt werden, so setze man

$$r = \alpha r' + \beta s', \quad s = \gamma r' + \delta s',$$

und es wird die Form (a, b, c) dieselbe Zahl m darstellen, sobald $x = r$, $y = s$ gesetzt wird. Man sagt deshalb auch: die Form (a, b, c) *enthält* die Form (a', b', c'), oder deutlicher: die Form (a', b', c') ist unter der Form (a, b, c) *enthalten**); eben weil sämmtliche durch (a', b', c') darstellbare Zahlen unter den durch (a, b, c) darstellbaren enthalten sind**).

Von besonderer Wichtigkeit ist die Relation, in welcher die Determinante

$$D' = b'^2 - a'c'$$

der neuen Form zu der der früheren steht; substituirt man für a', b', c' ihre Ausdrücke gemäss den Gleichungen (2), so findet man nach leichten Reductionen

$$D' = (\alpha\delta - \beta\gamma)^2 D;$$

die neue Determinante ist daher stets gleich der alten, multiplicirt mit einer Quadratzahl; beide Determinanten haben also auch dasselbe Vorzeichen. Da wir von vorn herein Formen ausschliessen, deren

*) *Gauss: D. A.* art. 157.

**) Ueber die Umkehrung dieses Satzes siehe *Schering: Théorèmes relatifs aux formes binaires quadratiques qui représentent les mêmes nombres*, Journal de Mathématiques publ. p. Liouville T. IV. 2e série. 1859.

Determinanten $= 0$ sind, so betrachten wir deshalb auch nur solche Substitutionen $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$, für welche die Coefficientenverbindung $\alpha\delta - \beta\gamma$ (die sogenannte *Determinante der Substitution*) einen von Null verschiedenen Werth hat. Hieran knüpft sich jedoch noch eine wichtige Unterscheidung; je nachdem nämlich dieser Ausdruck $\alpha\delta - \beta\gamma$ einen positiven oder negativen Werth hat, soll die Substitution $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ eine *eigentliche* oder *uneigentliche* heissen, und diese Ausdrucksweise soll auf die Beziehung zwischen den Formen (a, b, c) und (a', b', c') übertragen werden, indem wir sagen, dass die Form (a', b', c') *eigentlich* oder *uneigentlich* unter der Form (a, b, c) *enthalten* sei, je nachdem die Substitution $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$, durch welche die letztere in die erstere übergeht, eigentlich oder uneigentlich ist. Um Missverständnisse zu vermeiden, fügen wir sogleich hinzu, dass eine Form eine andere sowohl eigentlich als auch uneigentlich enthalten kann; denn es tritt häufig der Fall ein, dass eine Form einmal durch eine eigentliche, ein anderes Mal durch eine uneigentliche Substitution in eine und dieselbe zweite Form transformirt wird. So z. B. geht die Form (3, 13, 18) durch die eigentliche Substitution $\left(\begin{smallmatrix}+1, & 0\\ -1, & +1\end{smallmatrix}\right)$, und ebenso durch die uneigentliche Substitution $\left(\begin{smallmatrix}+1, & +2\\ -1, & -3\end{smallmatrix}\right)$ in die andere Form $(-5, -5, 18)$ über; die erstere enthält daher die letztere sowohl eigentlich als auch uneigentlich.

Man nennt ferner zwei Substitutionen *gleichartig*, wenn sie beide eigentlich, oder beide uneigentlich sind, *ungleichartig*, wenn die eine eigentlich, die andere uneigentlich ist.

§. 55.

Behalten wir die vorhergehenden Bezeichnungen bei, und nehmen wir an, dass die Form

$$(a', b', c') = a' x'^2 + 2 b' x' y' + c' y'^2$$

durch eine neue Substitution

$$x' = \alpha' x'' + \beta' y''$$
$$y' = \gamma' x'' + \delta' y''$$

in die Form

$$(a'', b'', c'') = a'' x''^2 + 2 b'' x'' y'' + c'' y''^2$$

übergeht, so geht offenbar die erste Form (a, b, c) durch die Substitution

$$x = \alpha(\alpha' x'' + \beta' y'') + \beta(\gamma' x'' + \delta' y'')$$
$$y = \gamma(\alpha' x'' + \beta' y'') + \delta(\gamma' x'' + \delta' y'')$$

oder

$$x = (\alpha\alpha' + \beta\gamma') x'' + (\alpha\beta' + \beta\delta') y''$$
$$y = (\gamma\alpha' + \delta\gamma') x'' + (\gamma\beta' + \delta\delta') y''$$

in die dritte Form (a'', b'', c'') über. Hieraus folgt der Satz:

Enthält eine Form eine zweite, diese wieder eine dritte, so enthält auch die erste Form die dritte.

Bezeichnet man nun die Coefficientenverbindung

$$(\alpha\alpha' + \beta\gamma')(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')(\gamma\alpha' + \delta\gamma')$$

mit ε, so ist nothwendig die Determinante der dritten Form $D'' = \varepsilon^2 D$; da aber andererseits

$$D' = (\alpha\delta - \beta\gamma)^2 D,\ D'' = (\alpha'\delta' - \beta'\gamma')^2 D',$$

also auch

$$D'' = (\alpha\delta - \beta\gamma)^2 (\alpha'\delta' - \beta'\gamma')^2 D,$$

und D von Null verschieden ist, so schliessen wir hieraus, dass

$$\varepsilon^2 = (\alpha\delta - \beta\gamma)^2 (\alpha'\delta' - \beta'\gamma')^2$$

ist, und man überzeugt sich leicht durch Vergleichung beider Seiten, dass die Quadratwurzel in folgender Weise auszuziehen ist:

$$\varepsilon = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma').$$

Aus dieser Gleichung (welche einen der einfachsten Sätze der Determinantentheorie enthält) folgt noch eine wesentliche Vervollständigung des obigen Satzes, nämlich:

Die erste Form enthält die dritte eigentlich oder uneigentlich, je nachdem die erste die zweite in derselben oder in entgegengesetzter Art enthält, wie die zweite die dritte.

Fährt man in derselben Weise fort und transformirt die dritte Form in eine vierte, diese in eine fünfte u. s. f., so ergiebt sich unmittelbar der allgemeine Satz: *Wenn von einer Reihe von Formen jede die nächstfolgende enthält, so enthält die erste Form auch die letzte, und zwar eigentlich oder uneigentlich, je nachdem die Anzahl der hierbei auftretenden uneigentlichen Substitutionen gerade oder ungerade ist.*

Die Substitution, durch welche die erste Form unmittelbar in die letzte transformirt wird, heisst *zusammengesetzt* aus den einzelnen successiven Substitutionen; um die Zusammensetzung von

zwei Substitutionen anzudeuten, wollen wir uns bisweilen der Bezeichnung

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}\begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix} = \begin{pmatrix}\alpha\alpha'+\beta\gamma', & \alpha\beta'+\beta\delta'\\ \gamma\alpha'+\delta\gamma', & \gamma\beta'+\delta\delta'\end{pmatrix}$$

bedienen; offenbar ist es im Allgemeinen nicht erlaubt, die Ordnung der beiden successiven Substitutionen umzukehren, weil hierdurch auch die resultirende Substitution geändert würde. So ist z. B. $\left(\begin{smallmatrix}+1, & 0\\ -1, & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}+1, & +2\\ -1, & -3\end{smallmatrix}\right) = \left(\begin{smallmatrix}+1, & +2\\ -2, & -5\end{smallmatrix}\right)$, dagegen $\left(\begin{smallmatrix}+1, & +2\\ -1, & -3\end{smallmatrix}\right)\left(\begin{smallmatrix}+1, & 0\\ -1, & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}-1, & +2\\ +2, & -3\end{smallmatrix}\right)$.

Dagegen ist es bei drei successiven Substitutionen S, S', S'' gleichgültig, ob man erst S und S' zusammensetzt, und dann das Resultat SS' mit S'' verbindet, oder ob man S mit dem Resultat $S'S''$ der zweiten und dritten Substitution zusammensetzt; in Zeichen:

$$(SS')S'' = S(S'S'').$$

Dies folgt unmittelbar aus dem Begriffe dieser Zusammensetzung; denn sind (x, y), (x', y'), (x'', y'') und (x''', y''') die successiven Variabeln, so ist es für die Ausdrücke von x, y durch x''', y''' gleichgültig, ob man die Variabeln x'', y'' oder die Variabeln x', y' als Zwischenglieder einschiebt.

Ferner ist für die Folge zu bemerken, dass die Substitution $\left(\begin{smallmatrix}1, & 0\\ 0, & 1\end{smallmatrix}\right)$ bei der Zusammensetzung stets fortgelassen werden darf, da sie keine Aenderung hervorbringt.

Endlich leuchtet ein, dass der obige Satz auch so ausgesprochen werden kann: *Die aus den Substitutionen S, S', S'' . . . zusammengesetzte Substitution $SS'S''$ . . . ist eigentlich oder uneigentlich, je nachdem die Anzahl der unter ihnen befindlichen uneigentlichen Substitutionen gerade oder ungerade ist.*

§. 56.

Besonders wichtig ist nun die Frage: wann enthalten zwei Formen sich gegenseitig? Offenbar ist dann das System aller durch die eine Form darstellbaren Zahlen identisch mit dem System derjenigen Zahlen, welche durch die andere Form dargestellt werden können. Zwei solche Formen werden wir *äquivalent**) nennen. Sind D, D' ihre Determinanten, so muss sowohl $D' : D$, als auch

*) *Gauss*: *D. A.* art. 157.

$D:D'$, eine ganze Quadratzahl, also eine ganze positive Zahl sein, und hieraus folgt als eine für die Aequivalenz zweier Formen *erforderliche* Bedingung, dass ihre Determinanten D und D' gleich sein müssen.

Diese Bedingung ist aber umgekehrt *nicht hinreichend*, um auf die Aequivalenz schliessen zu können. Dies ist erst dann gestattet, wenn man ausserdem weiss, dass die eine der beiden Formen die andere enthält. In der That, wenn die beiden Formen (a, b, c) und (a', b', c') gleiche Determinanten haben, und wenn ausserdem die erstere durch die Substitution

$$x = \alpha x' + \beta y'$$
$$y = \gamma x' + \delta y'$$

in die letztere übergeht, so folgt aus der Relation

$$D' = (\alpha\delta - \beta\gamma)^2 D$$

und der Gleichheit von D' und D die Gleichung

$$\alpha\delta - \beta\gamma = \pm 1$$

und hieraus, wenn man zur Abkürzung $\alpha\delta - \beta\gamma = \pm 1 = \varepsilon$ setzt,

$$x' = +\varepsilon\delta x - \varepsilon\beta y$$
$$y' = -\varepsilon\gamma x + \varepsilon\alpha y$$

und es geht daher durch diese Substitution mit ganzzahligen Coefficienten die Form (a', b', c') in die Form (a, b, c) über; also sind in der That beide Formen einander äquivalent. Die Substitutionen

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \text{ und } \begin{pmatrix} +\varepsilon\delta, & -\varepsilon\beta \\ -\varepsilon\gamma, & +\varepsilon\alpha \end{pmatrix},$$

deren jede die *inverse* der andern heisst, und durch deren Zusammensetzung immer die Substitution $\left(\begin{smallmatrix} 1, & 0 \\ 0, & 1 \end{smallmatrix}\right)$ entsteht, sind offenbar entweder beide eigentlich, oder beide uneigentlich; je nachdem das Eine oder das Andere Statt findet, sollen die beiden Formen *eigentlich* oder *uneigentlich äquivalent**) heissen.

Sowie wir eben gesehen haben, dass die eine von zwei äquivalenten Formen in die andere immer durch eine Substitution $\left(\begin{smallmatrix} \alpha, & \beta \\ \gamma, & \delta \end{smallmatrix}\right)$ übergeht, in welcher $\alpha\delta - \beta\gamma = \pm 1$ ist, so leuchtet auch umgekehrt ein, dass durch jede solche Substitution eine beliebige Form nothwendig in eine ihr äquivalente transformirt wird; denn die Determinanten beider Formen sind einander gleich. Hierin

*) *Gauss: D. A.* art. 158.

besteht also die *erforderliche und hinreichende* Bedingung für die Aequivalenz zweier Formen.

Aus dem Begriffe der Aequivalenz ergiebt sich unmittelbar, dass jede Form sich selbst eigentlich äquivalent ist; denn sie geht durch die eigentliche Substitution $\left(\begin{smallmatrix}1, & 0\\ 0, & 1\end{smallmatrix}\right)$ in sich selbst über. Dies ist nur ein specieller Fall des folgenden Satzes, welcher sehr oft zur Anwendung kommen wird: *Wenn zwei Formen* (a, b, c) *und* (a, b', c') *von gleicher Determinante* D *denselben ersten Coefficienten* a *haben, und wenn ihre mittleren Coefficienten* b, b' *einander congruent sind in Bezug auf den Modul* a, *so dass* $b' = a\beta + b$; *so sind die beiden Formen eigentlich äquivalent, und die erstere geht durch die eigentliche Substitution* $\left(\begin{smallmatrix}1, & \beta\\ 0, & 1\end{smallmatrix}\right)$ *in die letztere über.*

Ferner bemerke man folgende Fälle der uneigentlichen Aequivalenz: Zwei *entgegengesetzte**) Formen (*formae oppositae*), d. h. zwei Formen (a, b, c) und $(a, -b, c)$, welche sich nur durch das Vorzeichen des mittlern Coefficienten unterscheiden, sind stets *uneigentlich* äquivalent, indem die eine durch die Substitution $\left(\begin{smallmatrix}1, & 0\\ 0, & -1\end{smallmatrix}\right)$ in die andere übergeht. Dasselbe gilt von zwei *Gefährten***) (*formae sociae*), d. h. von zwei Formen (a, b, c) und (c, b, a), welche dieselben Coefficienten, nur in umgekehrter Folge, haben; die eine geht in die andere durch die Substitution $\left(\begin{smallmatrix}0, & \pm 1\\ 1, & \pm 0\end{smallmatrix}\right)$ über.

Aus diesen beiden Fällen folgt wieder durch Zusammensetzung, dass die beiden Formen (a, b, c) und $(c, -b, a)$ *eigentlich* äquivalent sind; denn die erstere geht in die letztere durch die Substitution $\left(\begin{smallmatrix}0, & 1\\ -1, & 0\end{smallmatrix}\right)$ über.

§. 57.

Auch hier bei der Aequivalenz schliesst die eine Art derselben die andere nicht aus; es kommt häufig der Fall vor, dass zwei Formen einander sowohl eigentlich als uneigentlich äquivalent sind; in dem oben (§. 54) angeführten Beispiel sind wirklich die beiden Formen (3, 13, 18) und (— 5, — 5, 18) eigentlich und uneigentlich äquivalent; die erstere geht durch die Substitutionen

*) *Gauss: D. A.* art. 159.
**) *Gauss: D. A.* art. 187.

$\left(\begin{smallmatrix}+1, & 0\\ -1, & 1\end{smallmatrix}\right)$ und $\left(\begin{smallmatrix}+1, & +2\\ -1, & -3\end{smallmatrix}\right)$ in die letztere über, und umgekehrt diese in jene durch die inversen Substitutionen $\left(\begin{smallmatrix}1, & 0\\ 1, & 1\end{smallmatrix}\right)$ und $\left(\begin{smallmatrix}+3, & +2\\ -1, & -1\end{smallmatrix}\right)$.

Wenn zwei Formen sowohl eigentlich als uneigentlich äquivalent sind, so ist jede von ihnen sich selbst uneigentlich äquivalent.

Denn, wenn die Form (a, b, c) durch jede der beiden Substitutionen

$$\left(\begin{smallmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{smallmatrix}\right) \text{ und } \left(\begin{smallmatrix}\alpha'', & \beta''\\ \gamma'', & \delta''\end{smallmatrix}\right),$$

in denen

$$\alpha'\delta' - \beta'\gamma' = +1, \quad \alpha''\delta'' - \beta''\gamma'' = -1,$$

in die Form (a', b', c') übergeht, so geht (a', b', c') durch jede der beiden inversen Substitutionen

$$\left(\begin{smallmatrix}+\delta', & -\beta'\\ -\gamma', & +\alpha'\end{smallmatrix}\right) \text{ und } \left(\begin{smallmatrix}-\delta'', & +\beta''\\ +\gamma'', & -\alpha''\end{smallmatrix}\right)$$

in (a, b, c) über; und hieraus folgt, dass (a, b, c) durch jede der beiden zusammengesetzten, und zwar nothwendig uneigentlichen Substitutionen

$$\left(\begin{smallmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{smallmatrix}\right)\left(\begin{smallmatrix}-\delta'', & +\beta''\\ +\gamma'', & -\alpha''\end{smallmatrix}\right) \text{ und } \left(\begin{smallmatrix}\alpha'', & \beta''\\ \gamma'', & \delta''\end{smallmatrix}\right)\left(\begin{smallmatrix}+\delta', & -\beta'\\ -\gamma', & +\alpha'\end{smallmatrix}\right)$$

in sich selbst übergeht. So z. B. geht die Form (3, 13, 18) durch die uneigentlichen Substitutionen $\left(\begin{smallmatrix}+1, & 0\\ -1, & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}+3, & +2\\ -1, & -1\end{smallmatrix}\right) = \left(\begin{smallmatrix}+3, & +2\\ -4, & -3\end{smallmatrix}\right)$ und $\left(\begin{smallmatrix}+1, & +2\\ -1, & -3\end{smallmatrix}\right)\left(\begin{smallmatrix}1, & 0\\ 1, & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}+3, & +2\\ -4, & -3\end{smallmatrix}\right)$ in sich selbst über.

Es ist kein Zufall, dass diese beiden auf verschiedene Art zusammengesetzten Substitutionen identisch ausfallen; setzt man nämlich

$$\left(\begin{smallmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{smallmatrix}\right)\left(\begin{smallmatrix}-\delta'', & +\beta''\\ +\gamma'', & -\alpha''\end{smallmatrix}\right) = \left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right),$$

so findet man zunächst

$$\left(\begin{smallmatrix}\alpha'', & \beta''\\ \gamma'', & \delta''\end{smallmatrix}\right)\left(\begin{smallmatrix}+\delta', & -\beta'\\ -\gamma', & +\alpha'\end{smallmatrix}\right) = \left(\begin{smallmatrix}-\delta, & +\beta\\ +\gamma, & -\alpha\end{smallmatrix}\right),$$

und wir haben daher, um die Identität dieser beiden Substitutionen nachzuweisen, nur noch zu zeigen, dass in jeder uneigentlichen Substitution $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$, durch welche eine Form in sich selbst übergeht, stets der erste und vierte Coefficient einander gleich, aber entgegengesetzt sind. Dies geschieht leicht auf folgende Weise. Wenn die Form (a, b, c) durch die uneigentliche Substitution $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ in sich selbst übergeht, so ist

$$a\alpha^2 + (2b\alpha + c\gamma)\gamma = a$$
$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b$$
$$\alpha\delta - \beta\gamma = +1.$$

Die zweite dieser drei Gleichungen geht, wenn man der dritten gemäss $\beta\gamma$ durch $\alpha\delta + 1$ ersetzt, in folgende über:

$$a\alpha\beta + (2b\alpha + c\gamma)\delta = 0;$$

eliminirt man aus dieser und aus der ersten jener drei Gleichungen die Grösse $2b\alpha + c\gamma$, so erhält man, wenn man den Factor a wegwirft (der ja von Null verschieden ist, weil sonst die Determinante D eine Quadratzahl wäre), die Relation

$$(\alpha^2 - 1)\delta = \alpha\beta\gamma,$$

woraus mit Rücksicht auf $\alpha\delta - \beta\gamma = -1$ wirklich folgt, dass $\delta = -\alpha$ ist, was zu beweisen war.

§. 58.

Jede uneigentliche Substitution, durch welche eine Form (a, b, c) in sich selbst übergeht, ist daher nothwendig von der Form $\left(\begin{smallmatrix}\alpha, & +\beta\\ \gamma, & -\alpha\end{smallmatrix}\right)$, und es ist also gleichzeitig $\alpha^2 + \beta\gamma = 1$. Von besonderm Interesse ist der specielle Fall $\gamma = 0$; dann ist $\alpha = \pm 1$ und entsprechend $\pm a\beta = 2b$; eine solche Form, deren doppelter mittlerer Coefficient durch den ersten theilbar ist, soll eine *ambige* Form (*forma anceps*) heissen*). Und umgekehrt ist leicht zu sehen, dass jede ambige Form sich selbst uneigentlich äquivalent ist; denn wenn (a, b, c) eine solche Form, und also $2b = a\beta$ ist, so geht (a, b, c) wirklich durch die uneigentliche Substitution $\left(\begin{smallmatrix}1, & +\beta\\ 0, & -1\end{smallmatrix}\right)$ in sich selbst über. Dasselbe gilt offenbar von jeder Form, welche einer ambigen Form äquivalent ist; aber es besteht auch der umgekehrte Satz: **)

Wenn eine Form sich selbst uneigentlich äquivalent ist, so giebt es stets eine ihr äquivalente ambige Form.

Beweis. Es sei φ eine solche Form, welche durch die uneigentliche Substitution $\left(\begin{smallmatrix}\alpha, & +\beta\\ \gamma, & -\alpha\end{smallmatrix}\right)$ in sich selbst übergeht; ist $\gamma = 0$, so wissen wir, dass φ selbst eine ambige Form, und folglich der Satz richtig ist. Ist aber γ von Null verschieden, so suchen wir eine eigentliche Substitution $\left(\begin{smallmatrix}\lambda, & \mu\\ \nu, & \varrho\end{smallmatrix}\right)$, durch welche die Form φ in eine ihr äquivalente ambige Form übergeht, die wir mit ψ bezeichnen wollen. Da also $\lambda\varrho - \mu\nu = +1$, und folglich ψ durch die

*) *Gauss*: *D. A.* art. 163. Vergl. *Kummer* im Monatsbericht der Berliner Akademie vom 18. Februar 1858.

**) *Gauss*: *D. A.* art. 164.

inverse Substitution $\left(\begin{smallmatrix}\pm\varrho, & \mp\mu\\ -\nu, & +\lambda\end{smallmatrix}\right)$ in φ übergeht, so muss ψ durch die offenbar uneigentliche, aus den drei successiven Substitutionen

$$\begin{pmatrix}+\varrho, & -\mu\\ -\nu, & +\lambda\end{pmatrix},\quad \begin{pmatrix}\alpha, & +\beta\\ \gamma, & -\alpha\end{pmatrix},\quad \begin{pmatrix}\lambda, & \mu\\ \nu, & \varrho\end{pmatrix}$$

zusammengesetzte Substitution in sich selbst übergehen. Der dritte Coefficient dieser Substitution ist

$$\gamma\lambda^2 - 2\alpha\lambda\nu - \beta\nu^2,$$

und es kommt nur darauf an, zwei relative Primzahlen λ, ν so zu bestimmen, dass dieser Coefficient $= 0$ wird; denn dann ist ψ eine ambige Form. Diese Forderung reducirt sich, wenn man mit γ multiplicirt und bedenkt, dass $\alpha^2 + \beta\gamma = 1$ ist, auf die folgende:

$$(\gamma\lambda - \alpha\nu)^2 - \nu^2 = 0;\ \frac{\lambda}{\nu} = \frac{\alpha \pm 1}{\gamma} = \frac{-\beta}{\alpha \mp 1};$$

da unserer Annahme nach γ von Null verschieden ist, so kann man also λ und ν dieser Forderung gemäss bestimmen, und zwar als relative Primzahlen, wenn man den Bruch $(\alpha \pm 1) : \gamma$ auf seine kleinste Benennung $\lambda : \nu$ bringt. Dies Letztere ist erforderlich, weil ja die vier Coefficienten λ, μ, ν, ϱ der Gleichung $\lambda\varrho - \mu\nu = 1$ genügen müssen. Sobald nun λ und ν auf dem angegebenen Wege bestimmt sind, so kann man dann unendlich viele Werthenpaare für ϱ und μ (nach §. 24) finden, welche diese letzte Forderung erfüllen. Auf diese Weise ist also wirklich aus $\left(\begin{smallmatrix}\alpha, & \pm\beta\\ \gamma, & \mp\alpha\end{smallmatrix}\right)$ eine eigentliche Substitution $\left(\begin{smallmatrix}\lambda, & \mu\\ \nu, & \varrho\end{smallmatrix}\right)$ gefunden, welche die gegebene Form φ in eine ihr äquivalente ambige Form ψ transformirt, und hierdurch der obige Satz bewiesen.

Nehmen wir als Beispiel die obige Form (3, 13, 18), welche durch die uneigentliche Substitution $\left(\begin{smallmatrix}\pm 3, & \pm 2\\ -4, & -3\end{smallmatrix}\right)$ in sich selbst übergeht; wir haben also nur

$$\frac{\lambda}{\nu} = \frac{3 \pm 1}{-4}$$

zu setzen; nehmen wir das obere Zeichen, so ist $\lambda = \pm 1$, $\nu = \mp 1$ zu setzen, und entsprechend $\varrho + \mu = \pm 1$. Nehmen wir die obern Zeichen und $\varrho = 1$, $\mu = 0$, so erhalten wir die Substitution $\left(\begin{smallmatrix}+1, & 0\\ -1, & 1\end{smallmatrix}\right)$, durch welche, wie schon oben bemerkt ist, die Form (3, 13, 18) in die Form (— 5, — 5, 18) übergeht, welche in der That eine ambige Form ist.

Ferner: Die Form (7, 1, — 1) geht durch die uneigentliche

Substitution $\left(\begin{smallmatrix}+2, & +1\\ -3, & -2\end{smallmatrix}\right)$ in sich selbst über; in diesem Fall haben wir also

$$\frac{\lambda}{\nu} = \frac{2 \pm 1}{-3}$$

zu setzen; nehmen wir der Einfachheit halber wieder das obere Zeichen, so können wir wieder $\lambda = 1$, $\nu = -1$, $\varrho = 1$, $\mu = 0$ setzen; und in der That geht die Form $(7, 1, -1)$ durch die Substitution $\left(\begin{smallmatrix}+1, & 0\\ -1, & 1\end{smallmatrix}\right)$ in die ambige Form $(4, 2, -1)$ über.

§. 59.

Wir verlassen hiermit diesen interessanten Gegenstand und beschäftigen uns von jetzt an ausschliesslich mit der *eigentlichen* Aequivalenz; nur diese soll im Folgenden gemeint sein, wenn schlechthin von Aequivalenz gesprochen wird; ebenso soll unter Substitution immer nur noch die *eigentliche* Substitution verstanden sein. Werden daher zwei Formen f, f' äquivalent genannt, so bedeutet dieser Ausdruck stets (§. 56), dass eine Substitution $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ existirt, deren Coefficienten der Bedingung $\alpha\delta - \beta\gamma = +1$ genügen, und durch welche f in f' übergeht; umgekehrt geht dann f' in f über durch die inverse Substitution $\left(\begin{smallmatrix}\delta, & -\beta\\ -\gamma, & \alpha\end{smallmatrix}\right)$, deren Coefficienten derselben Bedingung $\delta\alpha - (-\beta)(-\gamma) = +1$ genügen. Aus dem allgemeinen Satze des §. 55 geht nun folgender specielle hervor: *Sind zwei Formen einer dritten äquivalent, so sind sie auch einander äquivalent*; und dieser Satz bildet die Grundlage für den wichtigsten Begriff in der ganzen Theorie der quadratischen Formen.

Es sei f eine bestimmte gegebene Form von der Determinante D, und F der Inbegriff aller der Formen $f, f', f'' \ldots$, welche mit f äquivalent sind; zufolge des eben erwähnten Satzes sind nun je zwei in dem System F vorkommende Formen f', f'' ebenfalls äquivalent; ist daher f' irgend eine in F vorkommende Form, so ist das System aller mit f' äquivalenten Formen identisch mit dem System F. Ein solches System unter einander äquivalenter Formen soll eine *Classe von Formen* *) oder eine *Formenclasse* heissen, und es leuchtet ein, dass durch irgend ein Individuum einer solchen Classe alle anderen derselben Classe angehörenden Formen vollständig be-

*) *Gauss: D. A.* art. 223.

stimmt sind; man kann daher immer ein solches Individuum als *Repräsentanten der Formenclasse* ansehen.

Es würde nicht schwer sein zu beweisen, dass es in jeder solchen Formenclasse unendlich viele Individuen giebt, d. h. dass die Anzahl der Formen, in welche eine gegebene Form f durch die unendlich vielen verschiedenen Substitutionen $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ übergeht, in denen $\alpha\delta - \beta\gamma = +1$, unendlich gross ist, obgleich es vorkommen kann, und zwar bei positiven Determinanten immer vorkommt, dass unendlich viele von diesen Substitutionen die Form f nur in eine und dieselbe Form f' transformiren; allein dieser Nachweis hat für uns zunächst kein Interesse. Von grösserer Wichtigkeit und von dem grössten Interesse ist dagegen die folgende Betrachtung.

Denkt man sich alle Formen von einer und derselben Determinante D in ihre verschiedenen Classen eingetheilt, und wählt man aus jeder Classe nach Belieben eine Form als Repräsentanten derselben, so erhält man ein sogenanntes *vollständiges System nicht äquivalenter Formen* für diese Determinante D; die fundamentale und vollständig charakteristische Eigenschaft eines solchen vollständigen Formensystems S besteht darin, dass jede beliebige Form von der Determinante D stets einer, aber auch nur einer von den in diesem System S enthaltenen Formen äquivalent ist. Die Anzahl dieser verschiedenen Classen (und also auch ihrer Repräsentanten in dem vollständigen Formensystem S) ist nun, wie sich zunächst für negative, später auch für positive Determinanten herausstellen wird, eine *endliche*, und wir bezeichnen absichtlich schon jetzt die genaue Bestimmung dieser *Classenanzahl für eine gegebene Determinante*, welche innig mit den schönsten algebraischen und analytischen Untersuchungen dieses Jahrhunderts verknüpft ist, als die letzte und hauptsächlichste von uns zu lösende Aufgabe.

Der Weg zu diesem Ziele wird gebahnt durch die Lösung der beiden folgenden Hauptprobleme in der Theorie der Aequivalenz:

I. *Zu entscheiden, ob zwei gegebene Formen von gleicher Determinante äquivalent sind, also derselben Classe angehören, oder nicht.*

II. *Alle Substitutionen zu finden, durch welche die eine von zwei gegebenen äquivalenten Formen in die andere übergeht.*

Es wird aber gut sein, die Beschäftigung mit diesen beiden Problemen dadurch zu motiviren, dass wir zeigen, wie die Theorie der *Darstellung* der Zahlen durch quadratische Formen vollständig

auf dieselben zurückgeführt werden kann; und so schicken wir im Folgenden einige Hauptsätze dieser Theorie voraus.

§. 60.

Man nennt, wie schon im Anfang dieses Abschnittes erwähnt ist, eine ganze Zahl m *darstellbar* durch die quadratische Form (a, b, c), wenn es zwei ganze Zahlen x, y giebt, welche der Gleichung

$$ax^2 + 2bxy + cy^2 = m \qquad (1)$$

genügen. Wir können uns aber zunächst auf sogenannte *eigentliche Darstellungen* (x, y) beschränken, in welchen die beiden *darstellenden Zahlen* x, y *relative Primzahlen* sind; denn ist δ der grösste gemeinschaftliche Divisor von x und y, so ist m nothwendig theilbar durch δ^2; setzt man nun $x = x'\delta$, $y = y'\delta$ und $m = m'\delta^2$, so wird m' offenbar durch die Form (a, b, c) dargestellt, wenn x' und y' als darstellende Zahlen genommen werden. Da nun die letztern relative Primzahlen sind, so erkennt man leicht, dass, sobald alle eigentlichen Darstellungen der Zahlen bekannt sind, hieraus die übrigen (*uneigentlichen*) Darstellungen leicht gefunden werden können; wir schliessen daher die letztern von unserer jetzigen Betrachtung ganz aus. Dies vorausgeschickt, schreiten wir zur Erforschung der erforderlichen und hinreichenden Bedingungen für die Darstellbarkeit einer gegebenen Zahl m durch eine gegebene Form (a, b, c).

1. Wir nehmen also an, die obige Darstellung (1) der Zahl m durch die Form (a, b, c) von der Determinante $D = b^2 - ac$ sei eine eigentliche, d. h. x und y seien relative Primzahlen. Dann giebt es (nach §§. 22, 24) immer unendlich viele Paare von ganzen Zahlen ξ, η, welche der unbestimmten Gleichung ersten Grades

$$x\eta - y\xi = +1 \qquad (2)$$

Genüge leisten. Wählen wir ein solches Paar ξ, η nach Belieben aus, so geht (nach §. 56) die Form (a, b, c) durch die Substitution $\begin{pmatrix} x, & \xi \\ y, & \eta \end{pmatrix}$ in eine äquivalente Form (m, n, l) über, deren erster Coefficient zufolge (1) die dargestellte Zahl m ist; der mittlere Coefficient wird

$$n = (ax + by)\xi + (bx + cy)\eta, \qquad (3)$$

und der dritte Coefficient l ergiebt sich, da beide Formen (nach §. 56) dieselbe Determinante haben, aus der Gleichung $n^2 - ml = D$ (denn m kann nicht $= 0$ sein, weil sonst D ein Quadrat wäre). Da nun dieser dritte Coefficient l nothwendig eine ganze Zahl ist, so folgt, *dass D quadratischer Rest von m, und dass $z = n$ eine Wurzel der Congruenz*

$$z^2 \equiv D \pmod{m} \tag{4}$$

ist.

2. Gesetzt nun, man nimmt statt der beiden Zahlen ξ, η irgend ein anderes Paar von Zahlen ξ', η', welche derselben Bedingung (2) genügen, so geht die Form (a, b, c) durch die Substitution $\left(\begin{smallmatrix} x, & \xi' \\ y, & \eta' \end{smallmatrix}\right)$ ebenfalls in eine äquivalente Form (m, n', l') über, und man erhält wieder eine Wurzel

$$n' = (ax + by)\xi' + (bx + cy)\eta'$$

der Congruenz (4). Es ist nun von Wichtigkeit zu untersuchen, in welcher Beziehung diese zu der früheren steht. Da der Voraussetzung nach $x\eta - y\xi = 1 = x\eta' - y\xi'$, also auch $x(\eta' - \eta) = y(\xi' - \xi)$ ist, und x und y relative Primzahlen sind, so muss $\xi' - \xi$ durch x theilbar sein; nennen wir den Quotienten v, so folgt

$$\xi' = \xi + xv, \quad \eta' = \eta + yv;$$

alle denkbaren Auflösungen der Gleichung (2) sind daher in diesen Formeln enthalten, in welchen v jede beliebige ganze Zahl bedeutet, und umgekehrt, jedem ganzzahligen Werthe von v entsprechen zwei Zahlen ξ', η', welche der Gleichung (2) genügen. (Dies gilt selbst dann noch, wenn eine der beiden Zahlen x, y gleich Null, und folglich die andere $= \pm 1$ ist.) Substituirt man nun die vorstehenden Ausdrücke in den von n', so erhält man, mit Berücksichtigung von (1) und (3), das Resultat

$$n' = n + mv, \quad \text{also } n' \equiv n \pmod{m}.$$

Hieraus folgt, dass alle Wurzeln n der Congruenz (4), welche auf die obige Art aus einer gegebenen eigentlichen Darstellung (x, y) der Zahl m durch die Form (a, b, c) abgeleitet werden können, die sämmtlichen Individuen einer und derselben Zahlclasse (mod. m) sind, also nur eine und dieselbe Wurzel dieser Congruenz bilden (§. 21); jedes Individuum dieser Zahlclasse wird, wenn v alle ganzen Zahlen durchläuft, d. h. wenn man der Reihe nach alle Auflösungen ξ, η der Gleichung (2) betrachtet, ein Mal und auch nur ein Mal erzeugt. Man sagt daher, die Darstellung (x, y) der Zahl m *gehöre*

zu dieser Wurzel n (mod. m) der Congruenz (4), weil durch den angegebenen Process nur diese und keine andere Wurzel derselben zum Vorschein kommt.

Zugleich leuchtet ein, dass die Form (a, b, c) durch die sämmtlichen Substitutionen $\left(\begin{smallmatrix} x, & \xi \\ y, & \eta \end{smallmatrix}\right)$, deren erster und dritter Coefficient die beiden darstellenden Zahlen x und y sind, in unendlich viele äquivalente Formen (m, n, l) übergeht (vergl. §. 56), deren gemeinschaftlicher erster Coefficient die dargestellte Zahl m ist, während der mittlere Coefficient n alle Zahlen einer völlig bestimmten Classe (mod. m), und zwar jedes Individuum derselben nur ein Mal, durchläuft *).

3. Das Vorhergehende reicht hin, um übersehen zu können, dass die *Aufgabe, alle eigentlichen Darstellungen einer gegebenen Zahl m durch eine gegebene Form* (a, b, c) *zu finden*, auf die Lösung der beiden Probleme zurückkommt, die wir am Schluss des vorigen Paragraphen aufgestellt haben. Man untersuche zunächst, ob D quadratischer Rest von m ist oder nicht; im letztern Fall

---

*) Es liegt nahe, die Zahlclasse n (mod. m) unmittelbar aus der gegebenen Darstellung (x, y) selbst zu bestimmen, ohne Zuziehung der Zahlen ξ, η. Die Auflösung der beiden Gleichungen (2) und (3), welche beide vom ersten Grade in Bezug auf ξ, η sind, giebt

$$m\eta = ax + (b+n)y, \quad -m\xi = (b-n)x + cy,$$

und hieraus folgen die Congruenzen

$$-yn \equiv ax + by, \quad xn \equiv bx + cy \pmod{m},$$

durch welche die Zahlclasse n (mod. m), wie man leicht erkennt, vollständig bestimmt ist. —

Wir schalten an dieser Stelle noch folgenden Satz ein, von welchem wir später Gebrauch machen werden: Giebt es zwei ganze Zahlen x, y, welche den Bedingungen

$$ax^2 + 2bxy + cy^2 = m$$
$$ax + (b+n)y \equiv 0, \quad (b-n)x + cy \equiv 0 \pmod{m}$$

genügen, wo m, n, a, b, c gegebene Zahlen bedeuten, deren erste von Null verschieden ist, so ist die Form (a, b, c) mit einer Form (m, n, l) äquivalent, deren erste beide Coefficienten m, n sind. Denn setzt man die auf der linken Seite der beiden Congruenzen befindlichen Ausdrücke resp. gleich $m\eta, -m\xi$, so ergiebt sich durch Multiplication mit x, y und Addition $m(x\eta - y\xi) = m$, also $x\eta - y\xi = +1$, woraus dann das Uebrige leicht folgt. Dass ferner umgekehrt, wenn zwei Formen (a, b, c) und (m, n, l) äquivalent sind, stets zwei Zahlen x, y existiren, welche den vorstehenden Bedingungen genügen, leuchtet aus dem Obigen unmittelbar ein. Mithin ist die Existenz zweier solcher Zahlen x, y vollkommen charakteristisch für die Aequivalenz der beiden Formen.

ist m durch keine einzige Form der Determinante D eigentlich darstellbar; im erstern Fall bestimme man alle incongruenten Wurzeln der Congruenz (4), und verfahre mit jeder einzelnen, wie folgt. Es sei n ein bestimmter Repräsentant einer bestimmten Wurzel, und zwar $n^2 = D + ml$, so ist (m, n, l) eine bestimmte Form von der Determinante D. Giebt es nun eine Darstellung (x, y) der Zahl m durch (a, b, c), welche zu der durch n repräsentirten Wurzel der Congruenz (4) gehört, so ist die Form (a, b, c) äquivalent mit (m, n, l), und die Darstellung (x, y) liefert eine und nur eine Substitution $\left(\begin{smallmatrix} x, & \xi \\ y, & \eta \end{smallmatrix}\right)$, durch welche die erstere in die letztere übergeht. Es muss daher zunächst entschieden werden, ob die beiden gegebenen Formen (a, b, c) und (m, n, l) von der Determinante D äquivalent sind, oder nicht — dies ist das *erste* der beiden genannten Probleme; gesetzt nun, die beiden Formen erweisen sich als nicht äquivalent, so existirt keine einzige zu dieser Wurzel n gehörige Darstellung der Zahl m durch die Form (a, b, c). Zeigt es sich aber, dass die beiden Formen äquivalent sind, so müssen alle Substitutionen $\left(\begin{smallmatrix} x, & \xi \\ y, & \eta \end{smallmatrix}\right)$ aufgesucht werden, durch welche (a, b, c) in (m, n, l) übergeht — dies ist das *zweite* Problem. Der erste und dritte Coefficient (x und y) einer jeden solchen Substitution bilden dann auch wirklich eine eigentliche zu der Wurzel n gehörige Darstellung der Zahl m durch (a, b, c), und da, wie schon bemerkt, aus jeder solchen Darstellung (x, y) umgekehrt eine und nur eine solche Substitution $\left(\begin{smallmatrix} x, & \xi \\ y, & \eta \end{smallmatrix}\right)$ entspringt, so erhält man durch die sämmtlichen Substitutionen der angegebenen Art auch *alle* zu n gehörigen Darstellungen, und jede nur *ein Mal*. Genau in derselben Weise verfährt man mit den übrigen Wurzeln der Congruenz (4), deren Anzahl, falls m und D relative Primzahlen sind, nach §. 37 zu bestimmen ist.

§. 61.

Nachdem wir uns in der vorhergehenden Digression davon überzeugt haben, dass in der That die Theorie der Darstellung vollständig auf die beiden (in §. 59) erwähnten Probleme der Lehre von der Aequivalenz zurückgeführt werden kann, so wenden wir uns nun zu der Lösung derselben. Das *erste*, zu erkennen, ob zwei Formen von gleicher Determinante äquivalent sind oder nicht, erfordert von vorn herein ganz verschiedene Methoden, je nachdem

die Determinante *positiv* oder *negativ* ist; in beiden Fällen ist aber die Lösung von der Art, dass, wenn die Aequivalenz der beiden Formen erkannt wird, zu gleicher Zeit auch eine Transformation der einen in die andere gefunden wird. Da also bei zwei wirklich äquivalenten Formen immer eine solche Transformation durch die Lösung der ersten Aufgabe gefunden ist, so besteht das *zweite* Problem nur noch darin, aus *einer* solchen Transformation *alle anderen* zu finden; und da die Lösung desselben zunächst nicht von dem Vorzeichen der Determinante abhängt, sondern für positive wie für negative Determinanten Anfangs eine gleichmässige Behandlung zulässt, so stellen wir es dem andern voran.

Unsere Aufgabe ist also die, aus *einer* Substitution L, durch welche eine Form φ in eine äquivalente Form ψ übergeht, *alle* Substitutionen S zu finden, welche denselben Erfolg haben. Wir können dieselbe sogleich durch einige Bemerkungen bedeutend vereinfachen, indem wir sie auf den einfachsten Fall reduciren, in welchem beide Formen identisch sind. Denn gesetzt, wir kennen *alle* Substitutionen T, durch welche die Form φ in sich selbst übergeht, so geht φ offenbar durch alle Substitutionen TL in die andere Form ψ über. Alle diese Substitutionen TL gehören also zu den gesuchten Substitutionen S. Jetzt behaupten wir auch umgekehrt, dass auf diese Weise alle Substitutionen S erzeugt werden, und jede nur ein einziges Mal; denn bezeichnen wir mit L' die inverse Substitution von L (durch welche also die Form ψ in die Form φ zurückkehrt), so ist jede in der Form SL' enthaltene Substitution eine solche, durch welche die Form φ in sich selbst übergeht, und gehört mithin zu den mit T bezeichneten Substitutionen, so dass wir $SL' = T$ setzen können. Da nun die aus L' und L zusammengesetzte Substitution $L'L = \left(\begin{smallmatrix} 1, & 0 \\ 0, & 1 \end{smallmatrix}\right)$ ist, so folgt hieraus $SL'L = S = TL$, also wird wirklich jede Substitution S auf die angegebene Art erzeugt. Dass endlich jede Substitution S nur ein einziges Mal erzeugt wird, leuchtet hieraus ebenfalls ein; ist nämlich $TL = S$, so ist $T = SL'$, also ist die Substitution T, durch welche eine bestimmte Substitution S erzeugt wird, immer eine vollkommen bestimmte, so dass zwei verschiedene Substitutionen T auch zwei verschiedene Substitutionen S erzeugen.

Da also der Complex der Substitutionen S vollständig mit dem Complex der Substitutionen TL übereinstimmt, wo L die gegebene Substitution bedeutet, durch welche die Form φ in die äquivalente Form ψ übergeht, so kommt es nur noch darauf an,

alle Substitutionen T zu finden; unser Problem ist daher auf das folgende zurückgeführt:

Alle Substitutionen zu finden, durch welche eine Form in sich selbst übergeht.

Bevor wir zur Lösung desselben schreiten, stellen wir eine Betrachtung an, welche für die Folge von grosser Wichtigkeit ist. Bedeutet σ den grössten (positiven) gemeinschaftlichen Theiler der drei Zahlen a, $2b$, c, so leuchtet ein, dass alle durch die Form (a, b, c) darstellbaren Zahlen durch σ theilbar sind, und wir wollen, wo kein Missverständniss zu besorgen ist, diese Zahl σ kurz *den Theiler der Form* (a, b, c) nennen. Dann sind zwei Fälle möglich:

1. Ist $2b : \sigma$ eine gerade Zahl, so geht σ in b, und folglich σ^2 in der Determinante $D = b^2 - ac$ auf; und umgekehrt, wenn σ^2 in D aufgeht, so ist b durch σ theilbar, also $2b : \sigma$ eine gerade Zahl; zugleich ist dann σ der grösste gemeinschaftliche Theiler der drei Coefficienten a, b, c.

2. Ist $2b : \sigma$ eine ungerade Zahl, so ist σ jedenfalls gerade, und σ^2 geht nicht in D, wohl aber in $4D$ auf, und zwar ist

$$\frac{4D}{\sigma^2} = \left(\frac{2b}{\sigma}\right)^2 - 4\frac{a}{\sigma}\frac{c}{\sigma} \equiv 1 \pmod 4,$$

also $4D \equiv \sigma^2 \pmod{4\sigma^2}$; und umgekehrt, wenn $4D \equiv \sigma^2 \pmod{4\sigma^2}$, so ist auch $(2b)^2 \equiv \sigma^2 \pmod{4\sigma^2}$, folglich $2b : \sigma$ eine ungerade Zahl; zugleich ist $\frac{1}{2}\sigma$ der grösste gemeinschaftliche Theiler der drei Coefficienten a, b, c.

Der Theiler σ einer jeden Form von der Determinante D genügt daher entweder der Bedingung $D \equiv 0 \pmod{\sigma^2}$, oder dieser $4D \equiv \sigma^2 \pmod{4\sigma^2}$; umgekehrt, ist σ eine positive Zahl, welche der einen oder andern dieser Bedingungen genügt, so existiren auch Formen (a, b, c) von der Determinante D, deren Theiler σ ist; je nachdem nämlich σ der ersten oder der zweiten Bedingung genügt, ist

$$\left(\sigma, 0, \frac{-D}{\sigma}\right) \quad \text{oder} \quad \left(\sigma, \tfrac{1}{2}\sigma, \frac{\sigma^2 - 4D}{4\sigma}\right)$$

eine Form von der Determinante D und vom Theiler σ, und zwar die sogenannte *einfachste* solche Form (*forma simplicissima*); die einfachste Form $(1, 0, -D)$ vom Theiler 1 heisst die *Hauptform* (*forma principalis*) der Determinante D*).

*) *Gauss: D. A.* artt. 231, 25.

Der grösste gemeinschaftliche Theiler τ der drei Coefficienten a, b, c einer Form (a, b, c) ist im ersten Fall $= \sigma$, im zweiten $= \frac{1}{2}\sigma$; ist nun $\tau = 1$, so heisst die Form eine *ursprüngliche**) (*forma primitiva*), und zwar, wenn $\sigma = 1$ ist, eine Form der *ersten Art***) (*forma proprie primitiva* oder *forma propria* nach *Gauss*), dagegen, wenn $\sigma = 2$ und also $D \equiv 1 \pmod 4$ ist, eine Form der *zweiten Art* (*forma improprie primitiva* oder *forma impropria*). Ist ferner $\tau > 1$, und $a = \tau a'$, $b = \tau b'$, $c = \tau c'$, $b'b' - a'c' = D'$, $D = \tau^2 D'$, so heisst die Form (a, b, c) *abgeleitet* (*derivata*) aus der ursprünglichen Form (a', b', c') der Determinante D'.

Aus den Formeln der Transformation [§. 54, (2)] geht nun hervor, dass, wenn eine Form (a', b', c') unter einer Form (a, b, c) enthalten ist, jeder gemeinschaftliche Theiler der Zahlen a, $2b$, c auch gemeinschaftlicher Theiler der Zahlen a', $2b'$, c' sein muss, woraus unmittelbar folgt, dass je zwei äquivalente Formen denselben Theiler σ besitzen; mithin kommt dieser Theiler allen zu einer und derselben Classe gehörigen Formen gemeinschaftlich zu, und kann daher füglich *der Theiler der Formenclasse* genannt werden. Dasselbe gilt offenbar von dem grössten gemeinschaftlichen Theiler τ der Coefficienten a, b, c einer jeden zu einer bestimmten Classe gehörigen Form (a, b, c). Hiernach leuchtet von selbst ein, was unter der *einfachsten Classe vom Theiler* σ, unter der *Hauptclasse*, unter einer *ursprünglichen Classe der ersten oder zweiten Art*, oder unter einer *abgeleiteten Classe* zu verstehen ist. Endlich bildet der Inbegriff aller Formen von gleicher Determinante D und von gleichem Theiler σ eine sogenannte *Ordnung****) (*ordo*), und aus dem Vorhergehenden folgt, dass dieselbe der Complex aller *Classen* der Determinante D ist, welche den Theiler σ haben.

§. 62.

Es sei nun $\left(\begin{smallmatrix}\lambda, & \mu\\ \nu, & \varrho\end{smallmatrix}\right)$ irgend eine Substitution, durch welche die Form (a, b, c) von der Determinante D und vom Theiler σ in sich selbst übergeht, so ist zunächst

$$\lambda\varrho - \mu\nu = 1 \qquad (1)$$

*) *Gauss: D. A.* art. 226.

**) *Dirichlet*: *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres.* 2e partie. §. 7. Crelle's Journal XXI.

***) *Gauss: D. A.* art. 226.

und ferner (nach §. 54)

$$a\lambda^2 + 2b\lambda\nu + c\nu^2 = a; \qquad (2)$$

$$a\lambda\mu + b(\lambda\varrho + \mu\nu) + c\nu\varrho = b; \qquad (3)$$

da aus diesen drei Gleichungen schon folgt, dass (a, b, c) in eine äquivalente Form übergeht, deren erster und zweiter Coefficient a und b sind, so ist der letzte Coefficient c' der neuen Form wegen der Gleichheit der Determinanten nothwendig $= c$; und folglich drücken diese Gleichungen vollständig aus, dass $\left(\begin{smallmatrix}\lambda & \mu\\ \nu & \varrho\end{smallmatrix}\right)$ eine Substitution der verlangten Art ist (dies würde nicht ebenso vollständig geschehen, wenn man die Gleichung $\lambda\varrho - \mu\nu = 1$ durch die andere Gleichung $a\mu^2 + 2b\mu\varrho + c\varrho^2 = c$ ersetzen wollte; denn dann würde man rückwärts nur schliessen können, dass $\lambda\varrho - \mu\nu = \pm 1$ ist).

Wir behandeln diese drei Gleichungen mit den vier Unbekannten λ, μ, ν, ϱ auf folgende Weise.

Wird $\lambda\varrho$ durch $\mu\nu + 1$ ersetzt, so nimmt die Gleichung (3) die Form

$$a\lambda\mu + 2b\mu\nu + c\nu\varrho = 0$$

an; verbindet man hiermit die Gleichung (2) und eliminirt einmal $2b$, dann c, so erhält man unter Berücksichtigung der Gleichung (1) die beiden folgenden:

$$a\mu + c\nu = 0; \quad a(\lambda - \varrho) + 2b\nu = 0.$$

Da a von Null verschieden ist (weil sonst D eine Quadratzahl wäre), so kann man folglich

$$\nu = \frac{a}{\sigma}u, \quad \mu = -\frac{c}{\sigma}u, \quad \lambda - \varrho = -\frac{2b}{\sigma}u \qquad (4)$$

setzen, worin u eine neue unbekannte, aber *ganze* Zahl bedeutet, weil ν, μ, $\lambda - \varrho$ ganze Zahlen sind, und σ der grösste gemeinschaftliche Divisor von a, c, $2b$ ist. Setzen wir diese Ausdrücke für μ und ν in die Gleichung (1), so erhalten wir

$$\lambda\varrho = -\frac{ac}{\sigma^2}u^2 + 1,$$

und hieraus in Verbindung mit dem vorstehenden Ausdruck für $\lambda - \varrho$ die Gleichung

$$(\lambda + \varrho)^2 = (\lambda - \varrho)^2 + 4\lambda\varrho = \frac{4(Du^2 + \sigma^2)}{\sigma^2}$$

oder

$$\left(\frac{\sigma(\lambda + \varrho)}{2}\right)^2 = Du^2 + \sigma^2.$$

Hieraus ergiebt sich, dass $\frac{1}{2}\sigma(\lambda+\varrho)$ jedenfalls eine *ganze* Zahl sein muss, die wir mit t bezeichnen wollen, so dass

$$\lambda+\varrho=\frac{2t}{\sigma} \text{ und } t^2=Du^2+\sigma^2 \qquad (5)$$

ist.

Wir können die vorstehende Untersuchung mit Rücksicht auf (4) und (5) in Folgendem zusammenfassen*):

Ist $\left(\begin{smallmatrix}\lambda, & \mu\\ \nu, & \varrho\end{smallmatrix}\right)$ *eine Substitution, durch welche die Form* (a, b, c) *von der Determinante* D *und vom Theiler* σ *in sich selbst übergeht, so ist stets*

$$\begin{aligned}\lambda&=\frac{t-bu}{\sigma}, & \mu&=-\frac{cu}{\sigma}\\ \nu&=\frac{au}{\sigma}, & \varrho&=\frac{t+bu}{\sigma}\end{aligned} \qquad (I)$$

wo t, u *zwei ganze Zahlen bedeuten, welche der unbestimmten Gleichung*

$$t^2-Du^2=\sigma^2 \qquad (II)$$

Genüge leisten.

Aber dieser Satz lässt sich auch umkehren:

Sind t, u *zwei ganze der Gleichung* (II) *genügende Zahlen, so sind die durch die Gleichungen* (I) *bestimmten Zahlen* $\lambda, \mu, \nu, \varrho$ *die ganzzahligen Coefficienten einer Substitution* $\left(\begin{smallmatrix}\lambda, & \mu\\ \nu, & \varrho\end{smallmatrix}\right)$, *durch welche die Form* (a, b, c) *in sich selbst übergeht.*

Dies ergiebt sich auf folgende Weise. Zunächst ist zu beweisen, dass $\lambda, \mu, \nu, \varrho$ *ganze* Zahlen werden; da σ in a und in c aufgeht, so sind ν und μ ganze Zahlen; da ferner σ^2 in $4D$ und zufolge (II) auch in $4t^2$ aufgeht, so ist $2t$ theilbar durch σ, und da σ auch in $2b$ aufgeht, so sind 2λ und 2ϱ ebenfalls ganze Zahlen, deren Summe $= 4t : \sigma$, also eine gerade Zahl ist; mithin sind 2λ und 2ϱ entweder beide gerade oder beide ungerade; da aber ihr Product

$$= 4\frac{t^2-b^2u^2}{\sigma^2} = 4\frac{\sigma^2-acu^2}{\sigma^2} = 4\left(1-\frac{a}{\sigma}\frac{c}{\sigma}u^2\right)$$

gerade ist, so sind 2λ und 2ϱ gerade Zahlen, also λ und ϱ ganze Zahlen.

Nachdem dieser erste Punct sichergestellt ist, findet man leicht durch wirkliche Substitution der Ausdrücke (I) unter Berücksichtigung der Gleichung (II), dass die drei Relationen (1),

*) Vergl. *Gauss*: *D. A.* art. 162.

(2) und (3) identisch erfüllt sind, dass also in der That die Form (a, b, c) durch die Substitution $\left(\begin{smallmatrix}\lambda & \mu\\ \nu & \varrho\end{smallmatrix}\right)$ in sich selbst übergeht.

Aus jeder bekannten Substitution $\left(\begin{smallmatrix}\lambda & \mu\\ \nu & \varrho\end{smallmatrix}\right)$ kann daher (z. B. durch die Gleichungen $u = \sigma\nu : a$, $t = \sigma\lambda + bu$) eine Auflösung t, u der Gleichung (II) gefunden werden, und umgekehrt. Es ist aber wichtig, zu bemerken, dass zwei verschiedenen Substitutionen auch zwei verschiedene Auflösungen der Gleichung (II) entsprechen, und umgekehrt zwei verschiedenen Auflösungen der Gleichung (II) auch zwei verschiedene Transformationen der Form (a, b, c) in sich selbst. Denn die Relationen (I) sind derartig, dass gegebenen Werthen t, u ein und nur ein System von Werthen λ, μ, ν, ϱ, und umgekehrt gegebenen Werthen von $\lambda, \mu, \nu, \varrho$ ein und nur ein System von Werthen t, u entspricht.

Hiermit ist also unser Problem nicht vollständig gelöst, sondern nur auf das andere reducirt:

Alle ganzzahligen Auflösungen der unbestimmten Gleichung (II) *zu finden.*

Dieses letztere bietet nun nicht die geringste Schwierigkeit dar, sobald die Determinante D *negativ* ist. Wenn nämlich Δ ihr absoluter Werth, also $D = -\Delta$ ist, so hat die Gleichung (II)

$$t^2 + \Delta u^2 = \sigma^2$$

nur eine *endliche* Anzahl von Auflösungen t, u; und zwar ist, wenn

1. $D \equiv 0 \pmod{\sigma^2}$, die Anzahl der Auflösungen der Gleichung immer $= 2$, sobald $\Delta > \sigma^2$ ist; diese Auflösungen sind offenbar

$$t = +\sigma, \quad u = 0 \quad \text{und} \quad t = -\sigma, \quad u = 0;$$

im Fall $\Delta = \sigma^2$ ist aber die Anzahl der Auflösungen $= 4$; diese sind

$$t = \sigma, \quad u = 0; \quad t = -\sigma, \quad u = 0;$$
$$t = 0, \quad u = 1; \quad t = 0, \quad u = -1.$$

2. Ist $4D \equiv \sigma^2 \pmod{4\sigma^2}$ und folglich $4\Delta \equiv 3\sigma^2 \pmod{4\sigma^2}$, so ist die Anzahl der Auflösungen der Gleichung stets $= 2$, so oft $4\Delta > 3\sigma^2$, also $4\Delta \geqq 7\sigma^2$; diese sind

$$t = \sigma, \quad u = 0; \quad \text{und } t = -\sigma, \quad u = 0;$$

im Fall $4\Delta = 3\sigma^2$ ist aber die Anzahl der Auflösungen $= 6$; diese sind

$$t = +\sigma, u = 0; \quad t = +\tfrac{1}{2}\sigma, u = +1; \quad t = +\tfrac{1}{2}\sigma, u = -1;$$
$$t = -\sigma, u = 0; \quad t = -\tfrac{1}{2}\sigma, u = -1; \quad t = -\tfrac{1}{2}\sigma, u = +1.$$

§. 63.

Bei weitem schwieriger ist die Theorie der Gleichung (II) für den Fall einer *positiven* Determinante D, und hierin zeigt sich zuerst die grosse Verschiedenheit in der Natur der Formen von positiver und derer von negativer Determinante. Wir lassen daher diese Untersuchung für jetzt fallen, um sie später (in §. 83) wieder aufzunehmen, nachdem das andere in §. 59 erwähnte Problem der Lehre von der Aequivalenz seine Lösung gefunden haben wird. Auch bei diesem stellt sich etwas Aehnliches heraus, indem es durchaus nothwendig wird, die Formen von positiver und negativer Determinante vollständig gesondert zu behandeln; und da auch hier die Formen von negativer Determinante weit weniger Schwierigkeiten darbieten, so behandeln wir diese zunächst.

Um aber den Gang der Untersuchung nicht zu unterbrechen, schicken wir eine Bemerkung voraus, welche sich gleichmässig auf Formen von positiver wie von negativer Determinante bezieht. Offenbar geht eine Form (a, b, a'), in welcher wir absichtlich den letzten Coefficienten nicht mit c, sondern mit a' bezeichnen, durch eine Substitution von der Form $\left(\begin{smallmatrix} 0, & 1 \\ -1, & \delta \end{smallmatrix}\right)$ in eine äquivalente Form über, deren Coefficienten

$$a',\ b' = -b - a'\delta,\ a'' = a + 2b\delta + a'\delta^2$$

sind; diese Form (a', b', a'') soll der Form (a, b, a') *nach rechts benachbart**), und ebenso soll die letztere (a, b, a') der andern (a', b', a'') *links benachbart* heissen. Das Charakteristische der Beziehung zweier solcher benachbarter Formen φ und φ' (*formae contiguae*) besteht *erstens* darin, dass sie dieselbe Determinante haben, *zweitens*, dass der letzte Coefficient a' der einen Form φ zugleich der erste Coefficient der andern Form φ' ist, *drittens*, dass die Summe ihrer mittlern Coefficienten $b + b'$ durch diesen gemeinschaftlichen Coefficienten a' theilbar ist. Denn haben zwei Formen φ und φ' diese drei Eigenschaften, und setzt man $b + b' = -a'\delta$, so geht in der That die Form φ durch die Substitution

$$\left(\begin{smallmatrix} 0, & 1 \\ -1, & \delta \end{smallmatrix}\right)$$

*) *Gauss: D. A.* art. 160.

in eine neue Form über, deren erste beide Coefficienten a', b' mit denen der Form φ' übereinstimmen; und da die neue Form jedenfalls der Form φ äquivalent ist, also auch dieselbe Determinante wie φ und folglich auch wie φ' hat, so muss sie mit φ' identisch sein *).

§. 64.

Wir wenden uns nun zu der Untersuchung, ob zwei gegebene Formen von gleicher *negativer* Determinante $D = -\Delta$ äquivalent sind oder nicht. Zunächst ist zu bemerken, dass die beiden äusseren Coefficienten a und c einer solchen Form

$$\varphi = ax^2 + 2bxy + cy^2$$

nothwendig gleiche Vorzeichen haben, da $ac = b^2 + \Delta$ positiv ist; da ferner

$$a\varphi = (ax + by)^2 + \Delta y^2$$

ist, so zeigt sich, dass alle durch die Form φ darstellbaren Zahlen dasselbe Vorzeichen haben wie a und c. Sind daher (a, b, c) und (a', b', c') äquivalente Formen, so haben die äusseren Coefficienten a', c' der letztern Form dasselbe Zeichen wie die der erstern. Da ferner aus der Aequivalenz dieser beiden Formen auch die der beiden Formen $(-a, -b, -c)$ und $(-a', -b', -c')$ folgt, so können wir uns im Folgenden auf die Betrachtung der sogenannten *positiven* Formen beschränken, in welchen die beiden äusseren Coefficienten das *positive* Vorzeichen haben.

Um nun über die Aequivalenz zweier Formen dieser Art zu entscheiden, vergleicht man sie nicht direct mit einander, sondern

*) Der letzte Grund, weshalb die Substitutionen von der Form $\left(\begin{smallmatrix} 0, & 1 \\ -1, & \delta \end{smallmatrix}\right)$ eine so wichtige Rolle spielen, besteht darin, dass aus ihnen alle anderen sich zusammensetzen lassen; man kann die Coefficienten δ in ihrer Aufeinanderfolge noch gewissen Beschränkungen, namentlich in Bezug auf ihre Vorzeichen, unterwerfen, in der Art, dass jede beliebige Substitution sich auch nur auf eine einzige Weise aus solchen einfachen Substitutionen zusammensetzen lässt. Eine wichtige Anwendung findet diese Bemerkung z. B. in der Theorie der unendlich vielen Formen der ϑ-Functionen. Man erkennt ferner leicht, dass auch der in §. 23 behandelte Algorithmus in der Theorie dieser Substitutionen und ihrer Zusammensetzung enthalten ist. Man vergleiche ferner §. 81.

mit sogenannten *reducirten**) Formen. Man nennt eine Form (A, B, C) von negativer Determinante (und positiven äusseren Coefficienten) eine reducirte, wenn der letzte Coefficient C nicht kleiner ist als der erste A, und der erste A wieder nicht kleiner als der absolute Werth des doppelten mittlern Coefficienten $2B$, in Zeichen, wenn

$$C \geqq A \geqq 2(B)$$

ist, wo (B) den absoluten Werth von B bedeuten soll. Wir beweisen nun zunächst folgenden Satz:

Jede Form von negativer Determinante ist einer reducirten Form äquivalent.

Zu dem Zweck betrachte man die der gegebenen Form (a, b, a') nach rechts benachbarten Formen (a', b', a''); unter diesen wird es immer eine (bisweilen auch zwei) geben, in welchen wenigstens die eine Bedingung $a' \geqq 2(b')$ erfüllt ist. Denn unter allen mit $-b$ nach dem Modul a' congruenten Zahlen giebt es eine b', deren absoluter Werth am kleinsten, und zwar kleiner oder wenigstens nicht grösser als $\frac{1}{2}a'$ ist (falls a' gerade und $b \equiv \frac{1}{2}a'$ (mod. a') ist, würde es zwei solche Zahlen b' geben, nämlich $\pm \frac{1}{2}a'$), so dass jedenfalls $b' \equiv -b$ (mod. a') und ausserdem $2(b') \leqq a'$ ist. Ist b' auf diese Weise gefunden, und $b + b' = -a'\delta$, so geht die Form (a, b, a') durch die Substitution

$$\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$$

in die nach rechts benachbarte Form (a', b', a'') über, in welcher $2(b') \leqq a'$ ist. Wenn nun gleichzeitig sich herausstellt, dass $a' \leqq a''$ ist, so ist (a', b', a'') eine reducirte Form und der Process geschlossen. Findet sich aber, dass das Gegentheil

$$a' > a''$$

Statt findet, so ist (a', b', a'') noch keine reducirte Form. Mit dieser verfahre man ebenso wie mit (a, b, a'), d. h. man transformire sie in eine nach rechts benachbarte Form (a'', b'', a'''), in welcher $2(b'') \leqq a''$ ist; sobald dann gleichzeitig $a'' \leqq a'''$ ist, so ist (a'', b'', a''') reducirt, folglich der Process geschlossen; ist dies aber nicht der Fall, also

$$a'' > a''',$$

---

*) *Gauss: D. A.* art. 171. Die Bedingung $A \leqq \sqrt{\frac{4}{3}D}$ ist schon eine Folge der beiden anderen (vergl. §. 65).

so setze man den Process in derselben Weise fort. Immer aber wird er nach einer *endlichen* Anzahl von Operationen schliessen; denn wäre dies nicht der Fall, so hätte man eine nie abbrechende Reihe von positiven ganzen Zahlen

$$a', a'', a''' \ldots a^{(n)}, a^{(n+1)} \ldots,$$

in welcher jede folgende mindestens um eine Einheit kleiner wäre, als die unmittelbar vorausgehende, was unmöglich ist, da es immer nur eine endliche Anzahl ganzer positiver Zahlen giebt, welche kleiner sind als eine gegebene.

Auf diese Weise ist bewiesen, dass man endlich zu einer Form $(a^{(n)}, b^{(n)}, a^{(n+1)})$ gelangen muss, in welcher nicht nur $2(b^{(n)}) \leqq a^{(n)}$, sondern auch $a^{(n)} \leqq a^{(n+1)}$ ist.

Zugleich ergiebt sich jedesmal durch die wirkliche Ausführung der Operationen eine Substitution, welche aus den successiven Substitutionen von der Form

$$\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$$

zusammengesetzt ist, und durch welche die gegebene Form (a, b, a') in die ihr äquivalente reducirte Form $(a^{(n)}, b^{(n)}, a^{(n+1)})$ übergeht.

Nehmen wir als Beispiel die Form (200, 100, 51), deren Determinante $D = -200$ ist, so haben wir $b' \equiv -100 \pmod{51}$ zu setzen und finden hieraus $b' = 2$ und $\delta = -2$; die Substitution, durch welche die gegebene Form (200, 100, 51) transformirt werden muss, ist daher gefunden; da wir aber den ersten und zweiten Coefficienten a' und b' und die Determinante D kennen, so brauchen wir diese Transformation nicht wirklich auszuführen, sondern wir berechnen den letzten Coefficienten a'' durch die Formel

$$a'' = \frac{b'^2 - D}{a'} = a + (b - b')\delta;$$

in unserm Fall finden wir also $a'' = 4$. Die benachbarte Form ist daher (51, 2, 4); sie ist nicht reducirt, weil der letzte Coefficient kleiner ist als der erste. Wir wiederholen daher dieselbe Operation, indem wir $b'' \equiv -2 \pmod{4}$ und folglich $b'' = \pm 2$ setzen, wo beide Zeichen zulässig sind; dann ergiebt sich $\delta' = -1$ oder $= 0$, je nachdem das obere oder untere Zeichen genommen wird, und ausserdem $a''' = 51$; also ist die neue Form $(4, \pm 2, 51)$, und diese ist, mag man das obere oder das untere Zeichen wählen, reducirt. Ferner geht die gegebene Form (200, 100, 51) durch die Substitution

$$\begin{pmatrix} 0, & +1 \\ -1, & -2 \end{pmatrix} \begin{pmatrix} 0, & +1 \\ -1, & -1 \end{pmatrix} = \begin{pmatrix} -1, & -1 \\ +2, & +1 \end{pmatrix}$$

in die Form (4, 2, 51), dagegen durch die Substitution

$$\begin{pmatrix} 0, & +1 \\ -1, & -2 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} -1, & +0 \\ +2, & -1 \end{pmatrix}$$

in die Form $(4, -2, 51)$ über. Man sieht aus diesem Beispiele wie einfach der angegebene Algorithmus sich gestaltet.

§. 65.

Wir sehen ferner an dem eben behandelten Beispiele, dass eine und dieselbe Form zwei verschiedenen reducirten Formen äquivalent sein kann, woraus folgt, dass auch zwei verschiedene reducirte Formen unter einander äquivalent sein, also derselben Classe angehören können. Da es von grosser Wichtigkeit ist, dies allgemein zu untersuchen, so stellen wir uns die Frage:

Wann sind zwei reducirte Formen (a, b, c) *und* (a', b', c') *von gleicher negativer Determinante* $D = -\Delta$ *einander äquivalent?*

Zunächst ziehen wir einige Folgerungen aus den beiden Bedingungen

$$2(b) \leqq a, \quad a \leqq c,$$

welche ausdrücken, dass die Form (a, b, c) eine reducirte ist. Es ergiebt sich nämlich aus der erstern $4b^2 \leqq a^2$, aus der letztern $a^2 \leqq ac$, also auch $4b^2 \leqq ac$ oder $3b^2 \leqq ac - b^2$, folglich

$$(b) \leqq \sqrt{\tfrac{1}{3}\Delta}.$$

Hieraus folgt weiter, dass $3ac = 3\Delta + 3b^2 \leqq 4\Delta$ und, da $a^2 \leqq ac$ ist, dass

$$a \leqq \sqrt{\tfrac{4}{3}\Delta}$$

ist.

Nehmen wir jetzt an, die beiden reducirten Formen (a, b, c), (a', b', c') seien äquivalent, so dürfen wir, ohne die Allgemeinheit zu beeinträchtigen, voraussetzen, dass

$$a' \leqq a$$

ist. Es sei nun $\left(\begin{smallmatrix} \alpha, & \beta \\ \gamma, & \delta \end{smallmatrix}\right)$ die Substitution, durch welche (a, b, c) in (a', b', c') übergeht, also

$$1 = \alpha\delta - \beta\gamma \tag{1}$$

$$a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \tag{2}$$

$$b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta. \tag{3}$$

Multipliciren wir die Gleichung (2) mit a, so ergiebt sich

$$aa' = (a\alpha + b\gamma)^2 + \Delta\gamma^2;$$

da nun sowohl a, als auch $a' \leqq \sqrt{\frac{4}{3}\Delta}$, und also

$$aa' \leqq \tfrac{4}{3}\Delta$$

ist, so folgt, dass in der vorstehenden Gleichung γ^2 entweder $= 0$ oder $= 1$ sein muss; denn wäre $\gamma^2 \geqq 4$, so wäre $aa' \geqq 4\Delta$, was mit der Bedingung $aa' \leqq \frac{4}{3}\Delta$ streitet. Wir unterscheiden nun diese beiden Fälle:

I. $\gamma = 0$.

Dann lauten die drei obigen Gleichungen folgendermaassen:

$$\alpha\delta = 1;\ a' = a\alpha^2;\ b' = a\alpha\beta + b;$$

aus der ersten folgt $\alpha = \delta = \pm 1$; also ist $a' = a$, und die dritte Gleichung lehrt, dass $b' - b = \pm a\beta$ durch $a = a'$ theilbar ist; da nun aber $(b) \leqq \frac{1}{2}a$ und $(b') \leqq \frac{1}{2}a'$, also auch $(b') \leqq \frac{1}{2}a$ ist, so sind nur zwei Fälle möglich: entweder ist $b' - b = 0$, also $b' = b$ und folglich, da schon $a' = a$ ist, auch $c' = c$, d. h. die Formen sind identisch, in welchem Fall sich die Aequivalenz von selbst versteht; oder es ist der absolute Werth von $b' - b$, da er unmöglich grösser als a sein kann und doch durch a theilbar sein muss, gleich a; in diesem Fall muss eine der beiden Zahlen b, b' gleich $+\frac{1}{2}a$, die andere gleich $-\frac{1}{2}a$, und also $c' = c$ sein; wir werden daher auf zwei nicht identische ambige Formen $(a, \frac{1}{2}a, c)$ und $(a, -\frac{1}{2}a, c)$ geführt. Diese sind aber in der That äquivalent, und die erstere geht in die letztere durch die Substitution $\left(\begin{smallmatrix}1 & -1\\ 0 & +1\end{smallmatrix}\right)$ über.

II. $\gamma = \pm 1$.

In diesem Fall lautet die Gleichung (2) folgendermaassen

$$a' = a\alpha^2 \pm 2b\alpha + c;$$

da wir angenommen haben, dass a' nicht grösser als a, und folglich auch nicht grösser als c ist, so folgt, dass

$$a\alpha^2 \pm 2b\alpha \leqq 0$$

ist. Da nun andererseits $2(b) \leqq a$ und stets $(\alpha) \leqq \alpha^2$, also auch der absolute Werth von $2b\alpha$ nicht grösser ist als $a\alpha^2$, so ist ganz gewiss

$$a\alpha^2 \pm 2b\alpha \geqq 0.$$

Es kann also $a\alpha^2 \pm 2b\alpha$ weder positiv noch negativ sein, und folglich ist

$$a\alpha^2 \pm 2b\alpha = 0,$$

also $a' = c$; da aber $a' \leqq a$ und $a \leqq c$, so folgt weiter, dass sowohl $a' = a$, als auch $c = a$ ist. Nun kann man die Gleichung (3) mit Hülfe der Gleichung (1) in die Form

$$b + b' = a\alpha\beta + 2b\alpha\delta \pm c\delta$$

bringen, und da $c = a$, und $2b\alpha = \mp a\alpha^2$ ist, so ergiebt sich

$$b + b' = a(\alpha\beta \mp \alpha^2\delta \pm \delta)$$

d. h. $b + b'$ ist theilbar durch a. Hieraus folgt ganz ähnlich wie im Fall I, dass $b + b'$ entweder $= 0$, oder dass der absolute Werth von $b + b'$ gleich a sein muss. Im letztern Fall müssten b und b' einander gleich, nämlich $= \pm \frac{1}{2}a$ sein, dann erhielte man also wieder den Fall zweier identischen Formen, der kein Interesse darbietet. Im erstern Fall dagegen ist $b' = -b$, folglich da $a' = a$, und auch $c = a$ ist, auch $c' = c = a$; wir haben daher folgende zwei Formen (a, b, a) und $(a, -b, a)$, welche (wenn b von Null verschieden ist) nicht identisch sind; diese sind wirklich äquivalent, und die erstere geht in die letztere durch die Substitution $\left(\begin{smallmatrix} 0, & -1 \\ 1, & 0 \end{smallmatrix}\right)$ über.

Wir fassen das Resultat der Untersuchung in Folgendem zusammen:

Die beiden einzigen Fälle, in denen zwei nicht identische reducirte Formen derselben Classe angehören, sind die folgenden: die Formen $(a, \frac{1}{2}a, c)$ *und* (a, b, a) *gehen resp. durch die Substitutionen*

$$\begin{pmatrix} 1, & -1 \\ 0, & +1 \end{pmatrix} \text{ und } \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}$$

in die entgegengesetzten Formen $(a, -\frac{1}{2}a, c)$ *und* $(a, -b, a)$ *über.*

§. 66.

Hiermit ist nun auch die Aufgabe gelöst, zu entscheiden, ob zwei Formen von gleicher negativer Determinante äquivalent sind oder nicht. Sind φ und ψ die beiden Formen, so transformire man jede derselben, falls sie noch nicht reducirt sein sollte, nach

der oben (§. 64) angegebenen Methode in eine reducirte Form, φ in φ', ψ in ψ'. Stellt sich dann heraus, dass φ' und ψ' identisch ausfallen, oder dass sie einen der beiden eben untersuchten Fälle darbieten, in welchen zwei nicht identische reducirte Formen dennoch äquivalent sind (was durch den Anblick der beiden Formen augenblicklich erkannt wird), so sind die gegebenen Formen φ und ψ gewiss äquivalent. Und zugleich ergiebt sich eine Substitution, durch welche die eine Form in die andere übergeht; denn durch den Process der Reduction ergeben sich Substitutionen S, durch welche φ in φ', und T, durch welche ψ in ψ' übergeht. Sind daher φ' und ψ' identisch, so geht, wenn T' die inverse Substitution von T bedeutet, die Form φ durch die zusammengesetzte Substitution ST' in die Form ψ über. Sind dagegen φ' und ψ' nicht identisch, aber doch äquivalent, so ist, wie wir oben gesehen haben, immer eine Substitution U bekannt, durch welche φ' in ψ' übergeht; und dann geht φ durch die zusammengesetzte Substitution SUT' in ψ über.

Zeigt sich aber, dass die Formen φ' und ψ' nicht identisch sind, und dass sie auch keinen der beiden im vorigen Paragraphen erwähnten singulären Fälle darbieten, sind also diese beiden reducirten Formen nicht äquivalent, so sind auch die beiden gegebenen Formen φ und ψ nicht äquivalent, wie unmittelbar aus §. 59 folgt.

Hiermit sind für negative Determinanten die beiden in §. 59 aufgestellten Probleme der Lehre von der Aequivalenz vollständig gelöst: soeben das erstere, welches darin besteht, über die Aequivalenz oder Nichtäquivalenz zweier gegebenen Formen zu entscheiden; und zugleich haben wir jedesmal, wenn die Entscheidung für die erstere lautet, auch eine Substitution zu finden gelehrt, durch welche die eine Form in die andere übergeht. Das zweite Problem, aus einer gegebenen Substitution, durch welche eine gegebene Form in eine (hierdurch schon völlig bestimmte) äquivalente Form übergeht, alle Substitutionen zu finden, durch welche die erstere Form in dieselbe zweite Form übergeht, ist in den §§. 61, 62 ebenfalls vollständig gelöst.

§. 67.

Die Theorie der reducirten Formen setzt uns nun auch in den Stand, für jede gegebene *negative* Determinante ein *vollständiges System nicht-äquivalenter Formen* (§. 59) aufzustellen, wobei wir uns wieder auf solche Formen beschränken wollen, deren äussere Coefficienten positiv sind. Da nämlich jede Form von negativer Determinante $D = -\Delta$ einer reducirten Form und im Allgemeinen auch nur einer solchen reducirten Form äquivalent ist, so brauchen wir, um ein vollständiges Formensystem zu erhalten, nur die sämmtlichen reducirten Formen aufzusuchen und jedesmal, wenn zwei solche nicht identische Formen einen der beiden in §. 65 erwähnten Fälle darbieten, eine von ihnen nach Belieben fortzulassen, die andere beizubehalten. Dass die Anzahl der so übrig bleibenden nicht äquivalenten reducirten Formen endlich ist, ergiebt sich leicht aus den Bedingungen

$$2(b) \leqq a \leqq c,$$

denen eine reducirte Form (a, b, c) genügen muss, und der hieraus (in §. 65) gezogenen Folgerung

$$(b) \leqq \sqrt{\tfrac{1}{3}\Delta}.$$

Bezeichnet man nämlich die grösste ganze in $\sqrt{\frac{1}{3}\Delta}$ enthaltene Zahl mit λ (so dass $\lambda \leqq \sqrt{\frac{1}{3}\Delta} < \lambda + 1$), so kann der mittlere Coefficient b keine andern, als die folgenden $2\lambda + 1$ Werthe

$$0, \pm 1, \pm 2 \ldots \pm \lambda$$

haben; und wenn man dem mittlern Coefficienten b irgend einen dieser Werthe beigelegt hat, so ist $ac = b^2 + \Delta$; also hat man die Zahl $b^2 + \Delta$ auf alle mögliche Arten in zwei positive Factoren zu zerlegen, und jedesmal denjenigen, welcher den andern an Grösse nicht übertrifft, für a, den letztern für c zu nehmen; stellt sich dann gleichzeitig heraus, dass $2(b) \leqq a$ ist, so ist die so gebildete Form wirklich eine reducirte und deshalb aufzuschreiben, im entgegengesetzten Fall aber fortzulassen. Auf diese Weise erhält man nothwendig alle reducirten Formen; ihre Anzahl ist aber nothwendig eine endliche, denn die Anzahl aller Zerlegungen der $(2\lambda + 1)$ Zahlen von der Form $(b^2 + \Delta)$ in zwei Factoren ist selbst endlich. Wir haben daher das Resultat:

Die Anzahl aller nicht äquivalenten reducirten Formen von negativer Determinante, d. h. die Classenanzahl selbst ist endlich.

Beispiel 1: Für die Determinante $D = -12$ ist $\Delta = 12$; hieraus $\lambda = \sqrt{\frac{1}{3}\Delta} = 2$; wir haben daher b folgende Werthe durchlaufen zu lassen

$$0, \pm 1, \pm 2,$$

und dann die Zahlen $b^2 + \Delta$, d. h. die Zahlen

$$12, 13, 16$$

auf alle möglichen Arten in zwei Factoren zu zerlegen; es ist

$$12 = 1 \cdot 12 = 2 \cdot 6 = 3 \cdot 4$$
$$13 = 1 \cdot 13$$
$$16 = 1 \cdot 16 = 2 \cdot 8 = 4 \cdot 4.$$

Dies giebt, indem der erste Factor immer $= a$, der zweite $= c$ gesetzt wird, die eilf Formen

$$(1, 0, 12), \quad (2, 0, 6), \quad (3, 0, 4);$$
$$(1, \pm 1, 13);$$
$$(1, \pm 2, 16), \quad (2, \pm 2, 8), \quad (4, \pm 2, 4).$$

Von diesen sind die folgenden nicht reducirt

$$(1, \pm 1, 13), \quad (1, \pm 2, 16), \quad (2, \pm 2, 8),$$

weil in ihnen die Bedingung $2(b) \leqq a$ nicht erfüllt ist; als wirklich reducirte Formen bleiben daher nur die folgenden fünf übrig

$$(1, 0, 12), \quad (2, 0, 6), \quad (3, 0, 4), \quad (4, \pm 2, 4);$$

allein die beiden Formen (4, 2, 4) und (4, −2, 4) gehören unter die Ausnahmefälle des §. 65, sind also äquivalent. Mithin enthält das vollständige Formensystem nur *vier* Formen, nämlich

$$(1, 0, 12), \quad (2, 0, 6), \quad (3, 0, 4), \quad (4, 2, 4),$$

die als Repräsentanten ebenso vieler Classen gelten. Von diesen vier Formen sind nur die beiden folgenden

$$(1, 0, 12), \quad (3, 0, 4)$$

ursprünglich, und zwar sind (da D nicht $\equiv 1 \pmod 4$ ist) beide von der ersten Art.

Beispiel 2: Ist $D = -35$, also $\Delta = +35$, so ist $\lambda = 3$ also kann b nur die sieben Werthe

$$0, \pm 1, \pm 2, \pm 3$$

durchlaufen; diesen entsprechen die Zahlen $b^2 + \Delta$:

$$35,\ 36,\ 39,\ 44;$$

die Zerlegungen derselben in zwei Factoren sind folgende:

$$35 = 1 \cdot 35 = 5 \cdot 7$$
$$36 = 1 \cdot 36 = 2 \cdot 18 = 3 \cdot 12 = 4 \cdot 9 = 6 \cdot 6$$
$$39 = 1 \cdot 39 = 3 \cdot 13$$
$$44 = 1 \cdot 44 = 2 \cdot 22 = 4 \cdot 11.$$

Aber von den 22 entsprechenden Formen erfüllen nur die folgenden 10 die Bedingung $2(b) \leqq a$:

$$(1, 0, 35),\quad (5, 0, 7),\quad (2, \pm 1, 18)$$
$$(3, \pm 1, 12),\quad (4, \pm 1, 9),\quad (6, \pm 1, 6).$$

Da ferner die beiden Formen $(2, \pm 1, 18)$ den Fall I, die beiden Formen $(6, \pm 1, 6)$ den Fall II des §. 62 darbieten, so existiren nur *acht* nicht äquivalente reducirte Formen

$$(1, 0, 35),\quad (5, 0, 7),\quad (2, 1, 18)$$
$$(3, \pm 1, 12),\quad (4, \pm 1, 9),\quad (6, 1, 6);$$

diese sind alle ursprünglich; sechs, nämlich

$$(1, 0, 35),\quad (5, 0, 7),\quad (3, \pm 1, 12),\quad (4, \pm 1, 9)$$

sind von der ersten, die beiden andern

$$(2, 1, 18),\quad (6, 1, 6)$$

sind von der zweiten Art.

Beispiel 3: Ist $D = -48 = -\Delta$, so ist $\lambda = 4$, so dass b folgende Zahlen

$$0, \pm 1, \pm 2, \pm 3, \pm 4$$

durchlaufen muss; die Zerlegungen der entsprechenden Zahlen $b^2 + \Delta$ sind folgende:

$$48 = 1 \cdot 48 = 2 \cdot 24 = 3 \cdot 16 = 4 \cdot 12 = 6 \cdot 8$$
$$49 = 1 \cdot 49 = 7 \cdot 7$$
$$52 = 1 \cdot 52 = 2 \cdot 26 = 4 \cdot 13$$
$$57 = 1 \cdot 57 = 3 \cdot 19$$
$$64 = 1 \cdot 64 = 2 \cdot 32 = 4 \cdot 16 = 8 \cdot 8.$$

Von den entsprechenden 27 Formen sind nur folgende eilf reducirt:

$$(1, 0, 48),\quad (2, 0, 24),\quad (3, 0, 16),\quad (4, 0, 12),$$
$$(6, 0, 8),\quad (7, \pm 1, 7),\quad (4, \pm 2, 13),\quad (8, \pm 4, 8).$$

Unter diesen besteht jedes der drei Paare $(7, \pm 1, 7)$, $(4, \pm 2, 13)$,

$(8, \pm 4, 8)$ aus je zwei äquivalenten Formen; also bleiben nur *acht* nicht äquivalente Formen

$$(1, 0, 48), \quad (2, 0, 24), \quad (3, 0, 16), \quad (4, 0, 12),$$
$$(6, 0, 8), \quad (7, 1, 7), \quad (4, 2, 13), \quad (8, 4, 8).$$

Ursprünglich von der ersten Art sind die folgenden vier:

$$(1, 0, 48), \quad (3, 0, 16), \quad (7, 1, 7), \quad (4, 2, 13),$$

die anderen vier sind derivirte Formen.

§. 68.

Um schon jetzt einen Begriff von der Fruchtbarkeit dieser Untersuchungen zu geben, verbinden wir in einigen Beispielen die gewonnenen Resultate mit der in §. 60 vorausgeschickten Theorie der Darstellung der Zahlen durch bestimmte quadratische Formen, bemerken jedoch gleich, dass die folgenden Sätze nur specielle Fälle eines grossen allgemeinen Satzes sind.

Die Formen der Determinante $D = -1$ bilden nur eine einzige Classe, denn es giebt für diese Determinante, wie man leicht erkennt, nur die einzige reducirte Form

$$(1, 0, 1) = x^2 + y^2.$$

Wir fragen nun nach dem System der durch diese Form darstellbaren, d. h. also in zwei Quadrate zerlegbaren Zahlen m; um aber die frühere Theorie unmittelbar anwenden zu können, lassen wir nur *eigentliche* Darstellungen (x, y) gelten, in denen die beiden darstellenden Zahlen x, y relative Primzahlen sind; ferner wollen wir uns der Einfachheit halber auf *ungerade* darstellbare Zahlen m beschränken. Es sei also m eine solche darstellbare ungerade Zahl, so ist zunächst m positiv. Da ferner die Determinante -1 quadratischer Rest von m ist, so müssen alle in m aufgehenden Primzahlen von der Form $4h + 1$ sein. Umgekehrt, ist diese Bedingung erfüllt, so ist die Determinante -1 quadratischer Rest von m, und die Congruenz

$$z^2 \equiv -1 \pmod{m}$$

hat im Ganzen (nach §. 37) 2^μ incongruente Wurzeln, wenn μ die Anzahl dieser von einander verschiedenen in m aufgehenden Primzahlen bedeutet (dies gilt selbst für den Fall, in welchem $\mu = 0$,

$m = 1$ ist). Es sei n ein bestimmter Repräsentant einer bestimmten dieser Wurzeln, und $n^2 + 1 = ml$, so bilde man die quadratische Form (m, n, l) von der Determinante -1; da nur eine einzige Formenclasse existirt, so ist diese Form der reducirten Form $(1, 0, 1)$ nothwendig äquivalent, und man wird durch die in §. 66 angegebene Methode eine, und hieraus nach §§. 61, 62 alle Transformationen finden, durch welche $(1, 0, 1)$ in (m, n, l) übergeht. Die Anzahl dieser von einander verschiedenen Transformationen $\binom{x, \xi}{y, \eta}$ ist (nach §§. 61, 62) stets $= 4$; ebenso viele Darstellungen (x, y) der Zahl m existiren daher, welche zu derjenigen Wurzel gehören, deren Repräsentant n ist. Und da dasselbe Raisonnement auf jede der 2^μ Wurzeln der obigen Congruenz passt, so existiren im Ganzen

$$4 \cdot 2^\mu = 2^{\mu+2}$$

verschiedene Darstellungen der Zahl m.

Stellt man aber die Frage, auf wie viele verschiedene Arten eine solche Zahl m in zwei Quadrate zerlegt werden kann, ohne Rücksicht auf die Ordnung der beiden Quadrate und auf die Vorzeichen ihrer Wurzeln, so liefern je acht verschiedene Darstellungen von der Form

$$(\pm x, \pm y) \quad \text{und} \quad (\pm y, \pm x)$$

nur eine einzige Zerlegung $m = x^2 + y^2$ (von diesen acht Darstellungen gehören vier, nämlich

$$(x, y), (-x, -y), (-y, x), (y, -x)$$

zu einer, und die anderen vier

$$(x, -y), (-x, y), (-y, -x), (y, x)$$

zu der ihr entgegengesetzten Wurzel); folglich ist die Anzahl dieser verschiedenen Zerlegungen

$$= 2^{\mu-1},$$

mit einziger Ausnahme des Falles $m = 1$, weil dann nicht acht, sondern nur vier verschiedene Darstellungen

$$(\pm 1, 0) \quad \text{und} \quad (0, \pm 1)$$

existiren, die sich zu der einzigen Zerlegung $1 = 1^2 + 0^2$ vereinigen.

In diesem allgemeinen Resultat ist als specieller Fall der

berühmte von *Fermat* aufgestellte, zuerst von *Euler**) bewiesene Satz enthalten:

Jede (positive) Primzahl von der Form $4h+1$ *lässt sich stets, und zwar nur auf eine einzige Weise in zwei Quadrate zerfällen.*

Die Bedingung, dass die Quadrate keinen gemeinschaftlichen Factor haben, fällt hier fort, da sie sich von selbst versteht.

Beispiel 1: Die Zahl 37 ist eine Primzahl von der Form $4h+1$; die beiden Wurzeln der Congruenz $z^2 \equiv -1 \pmod{37}$ findet man (z. B. mit Hülfe des Wilson'schen Satzes) $\equiv \pm 6$; nimmt man $n = 6$, so hat man die Form (37, 6, 1) zu betrachten, welche durch die Substitution $\left(\begin{smallmatrix} 0, & +1 \\ -1, & -6 \end{smallmatrix}\right)$ in die reducirte Form (1, 0, 1) übergeht; umgekehrt geht also (1, 0, 1) durch die inverse Substitution $\left(\begin{smallmatrix} -6, & -1 \\ +1, & 0 \end{smallmatrix}\right)$ in (37, 6, 1) über. Also ist die gesuchte Zerlegung folgende: $37 = 6^2 + 1^2$; es ist nicht nöthig, die vier zu dieser Wurzel $+6$, und die anderen vier zu der entgegengesetzten Wurzel -6 gehörenden Darstellungen hier einzeln aufzuschreiben.

Beispiel 2: Die Zahl $m = 65 = 5 \cdot 13$ ist das Product aus den beiden Primzahlen 5 und 13, welche beide die Form $4h+1$ haben. Mithin giebt es $2^4 = 16$ verschiedene Darstellungen, also nur zwei verschiedene Zerlegungen der Zahl 65. Die vier Wurzeln der Congruenz $z^2 \equiv -1 \pmod{65}$ sind ± 8 und ± 18; wir bilden daher die beiden Formen (65, 8, 1) und (65, 18, 5), welche durch die Substitutionen $\left(\begin{smallmatrix} 0, & +1 \\ -1, & -8 \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} -1, & -2 \\ +4, & +7 \end{smallmatrix}\right)$ in die reducirte Form (1, 0, 1) übergehen; die inversen Substitutionen sind $\left(\begin{smallmatrix} -8, & -1 \\ +1, & 0 \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} +7, & +2 \\ -4, & -1 \end{smallmatrix}\right)$, und folglich sind die beiden gesuchten Zerlegungen folgende:

$$65 = 8^2 + 1^2 = 7^2 + 4^2.$$

§. 69.

Alle Formen der Determinante $D = -2$ bilden ebenfalls nur eine einzige Classe, da nur eine einzige reducirte Form

$$(1, 0, 2) = x^2 + 2y^2$$

vorhanden ist. Wir fragen auch hier wieder nach allen durch

*) *Demonstratio theorematis Fermatiani, omnem numerum primum formae* $4n+1$ *esse summam duorum quadratorum*, Nov. Comm. Petrop. V. p. 3.

diese Form darstellbaren *ungeraden* Zahlen m; die erste Bedingung ist die, dass -2 quadratischer Rest von m sein muss; dazu ist erforderlich und hinreichend, dass für jede in m aufgehende (also ungerade) Primzahl p

$$\left(\frac{-2}{p}\right) = +1,$$

also p von einer der beiden Formen $8h+1$ oder $8h+3$ sei. Umgekehrt: sind die sämmtlichen μ in m aufgehenden Primzahlen p alle von der Form $8h+1$ oder $8h+3$, so hat die Congruenz

$$z^2 \equiv -2 \pmod{m}$$

stets 2^μ incongruente Wurzeln. Ist n ein bestimmter Repräsentant einer solchen Wurzel, und $n^2+2 = ml$, so ist die Form (m, n, l) nothwendig der Form $(1, 0, 2)$ äquivalent; man findet daher (nach §. 66) eine Substitution $\left(\begin{smallmatrix} x, & \xi \\ y, & \eta \end{smallmatrix}\right)$, durch welche die letztere in die erstere übergeht; ausser dieser existirt (nach §. 62) nur noch die andere $\left(\begin{smallmatrix} -x, & -\xi \\ -y, & -\eta \end{smallmatrix}\right)$, welche dieselbe Eigenschaft hat; es giebt daher zwei verschiedene Darstellungen (x, y) und $(-x, -y)$ der Zahl m, die zu dieser Wurzel gehören. Im Ganzen giebt es daher

$$2 \cdot 2^\mu = 2^{\mu+1}$$

verschiedene Darstellungen der Zahl m durch die Form $(1, 0, 2)$.

Man erkennt ferner leicht, dass, wenn die beiden Darstellungen $\pm(x, y)$ zu der Wurzel n gehören, entsprechend die beiden Darstellungen $\pm(x, -y)$ zu der entgegengesetzten Wurzel $-n$ gehören. Je vier solche Darstellungen geben eine und dieselbe Zerlegung der Zahl m in ein Quadrat und ein doppeltes Quadrat; mithin ist die Anzahl aller verschiedenen Zerlegungen

$$= 2^{\mu-1};$$

die einzige Ausnahme bildet wieder der Fall, in welchem $\mu = 0$, also $m = 1$ ist; denn dann vereinigen sich die zwei verschiedenen Darstellungen ($+n$ ist $\equiv -n \pmod{1}$) zu der einzigen Zerlegung $1 = 1^2 + 2 \cdot 0^2$. Der interessanteste specielle Fall ist wieder der, in welchem $\mu = 1$ ist:

Jede Primzahl p von einer der beiden Formen $8h+1$ oder $8h+3$ lässt sich stets und nur auf eine einzige Weise in ein Quadrat und ein doppeltes Quadrat zerlegen.

Beispiel 1: Ist $m = 41$, so ist die Bedingung erfüllt; μ ist $= 1$; die beiden Wurzeln der Congruenz $z^2 \equiv -2 \pmod{41}$ sind ± 11; die Form $(41, 11, 3)$ geht durch die Substitution $\left(\begin{smallmatrix} -1, & -1 \\ +4, & +3 \end{smallmatrix}\right)$ in

die Form (1, 0, 2) über, diese also rückwärts in jene durch die Substitution $\left(\begin{smallmatrix}+3, & +1\\ -4, & -1\end{smallmatrix}\right)$; also ist $x = 3$, $y = -4$, und folglich

$$41 = 3^2 + 2 \cdot 4^2.$$

Beispiel 2: Ist $m = 33 = 3 \cdot 11$, so ist die Bedingung erfüllt; μ ist $= 2$, und folglich muss es zwei verschiedene Zerlegungen geben. Die Wurzeln der Congruenz $z^2 \equiv -2 \pmod{33}$ sind ± 8 und ± 14: wir bilden daher die beiden Formen (33, 8, 2) und (33, 14, 6), welche resp. durch die Substitutionen

$$\begin{pmatrix}-1, & 0\\ +4, & -1\end{pmatrix} \text{ und } \begin{pmatrix}-1, & +2\\ +2, & -5\end{pmatrix}$$

in die Form (1, 0, 2) übergehen; die inversen Substitutionen sind

$$\begin{pmatrix}-1, & 0\\ -4, & -1\end{pmatrix} \text{ und } \begin{pmatrix}-5, & -2\\ -2, & -1\end{pmatrix}$$

und folglich ist

$$33 = 1^2 + 2 \cdot 4^2 = 5^2 + 2 \cdot 2^2.$$

§. 70.

Alle Formen der Determinante $D = -3$ bilden *zwei* Classen, als deren Repräsentanten man die reducirten Formen

$$(1, 0, 3) = x^2 + 3y^2$$

und

$$(2, 1, 2) = 2x^2 + 2xy + 2y^2$$

annehmen kann; sie sind resp. von der ersten und zweiten Art. Ungerade Zahlen können offenbar nur durch die erstere dargestellt werden; es sei daher m eine ungerade und der Einfachheit wegen durch 3 nicht theilbare Zahl; damit sie durch die Form (1, 0, 3) darstellbar sei, ist erforderlich, dass, wenn p irgend eine in ihr aufgehende Primzahl ist,

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = +1,$$

folglich p von der Form $3h + 1$ sei. Umgekehrt, sobald diese Bedingung für alle μ in m aufgehenden Primzahlen p erfüllt ist, so hat die Congurenz

$$z^2 \equiv -3 \pmod{m}$$

stets 2^μ incongruente Wurzeln; ist n ein bestimmter Repräsentant

einer solchen, und $n^2 + 3 = ml$, so ist die Form (m, n, l) von der ersten Art (da m ungerade ist) und folglich der Form $(1, 0, 3)$ äquivalent. Es giebt also (nach §. 62) zwei Substitutionen

$$\begin{pmatrix} x, & \xi \\ y, & \eta \end{pmatrix} \text{ und } \begin{pmatrix} -x, & -\xi \\ -y, & -\eta \end{pmatrix}$$

durch welche die Form $(1, 0, 3)$ in die Form (m, n, l) übergeht, und folglich auch zwei Darstellungen (x, y) und $(-x, -y)$ der Zahl m, welche zu dieser Wurzel gehören. Im Ganzen giebt es daher

$$2 \cdot 2^{\mu} = 2^{\mu+1}$$

verschiedene Darstellungen einer solchen Zahl m durch die Form $(1, 0, 3)$, die sich aber wieder auf nur

$$\tfrac{1}{4} \cdot 2^{\mu+1} = 2^{\mu-1}$$

verschiedene Zerlegungen der Zahl m in ein einfaches und ein dreifaches Quadrat reduciren (nur auf den Fall $\mu = 0$, also $m = 1$ passt die letztere Formel wieder nicht). Besonders bemerkenswerth ist der specielle Fall:

Jede Primzahl von der Form $3h + 1$ *ist stets und nur auf eine einzige Weise in ein einfaches und ein dreifaches Quadrat zerlegbar.*

Gehen wir nun zu den durch die zweite Form $(2, 1, 2)$ darstellbaren, nothwendig geraden Zahlen über; wir beschränken uns auf diejenigen von der Form $2m$, wo m wieder eine ungerade und durch 3 nicht theilbare Zahl bedeutet. Dann erkennen wir leicht, dass der Complex dieser Zahlen m mit dem eben behandelten vollständig identisch ist. Denn aus der Möglichkeit der Congruenz $z^2 \equiv -3 \pmod{m}$ folgt auch die der Congruenz $z^2 \equiv -3 \pmod{2m}$, und umgekehrt (§. 37), und ausserdem ist die Anzahl der Wurzeln wieder $= 2^{\mu}$. Ist ferner n' ein bestimmter Repräsentant einer solchen, und $n'^2 + 3 = 2ml$, so ist die Form $(2m, n', l)$ nothwendig von der zweiten Art (denn der mittlere Coefficient n' ist ungerade, folglich l gerade) und also gewiss der Form $(2, 1, 2)$ äquivalent; man kann daher (nach §. 62) sechs verschiedene Transformationen der letztern Form in die erstere finden, aus welchen folgende sechs Darstellungen

$$\pm (x, y), \pm (y, -x-y), \pm (x+y, -x)$$

entspringen, die alle zu derselben Wurzel n' gehören (die sechs zu der entgegengesetzten Wurzel $-n'$ gehörenden Darstellungen

entstehen aus diesen durch Vertauschung der ersten darstellenden Zahl mit der zweiten)*). Im Ganzen existiren daher

$$6 \cdot 2^{\mu} = 3 \cdot 2^{\mu+1}$$

verschiedene Darstellungen der Zahl $2m$ durch die Form (2, 1, 2), oder, was dasselbe ist, der Zahl m durch die Form $x^2 + xy + y^2$. Sieht man je vier zusammengehörige Darstellungen von der Form

$$(x, y), \quad (-x, -y), \quad (y, x), \quad (-y, -x)$$

als nicht wesentlich verschieden an, so ist die Anzahl der wesentlich verschiedenen Darstellungen nur noch

$$= 3 \cdot 2^{\mu-1}.$$

Für eine Primzahl p von der Form $3h + 1$ giebt es daher immer drei wesentlich verschiedene Darstellungen durch die Form $x^2 + xy + y^2$.

Beispiel: Ist $m = 13$, so sind $n = \pm 7$ die Wurzeln der Congruenz $z^2 \equiv -3 \pmod{26}$ und also auch der Congruenz $z^2 \equiv -3 \pmod{13}$. Wir bilden daher die beiden Formen (13, 7, 4) und (26, 7, 2). Sie gehen resp. durch die Substitutionen

$$\begin{pmatrix} -1, & -1 \\ +2, & +1 \end{pmatrix} \text{ und } \begin{pmatrix} 0, & +1 \\ -1, & -4 \end{pmatrix}$$

in die Formen (1, 0, 3) und (2, 1, 2) über. Die beiden inversen Substitutionen sind

$$\begin{pmatrix} +1, & +1 \\ -2, & -1 \end{pmatrix} \text{ und } \begin{pmatrix} -4, & -1 \\ +1, & 0 \end{pmatrix}$$

und folglich ist

$$13 = 1^2 + 3\,(-2)^2 = (-4)^2 + (-4) \cdot 1 + 1^2;$$

hieraus findet man leicht die beiden anderen Darstellungen

$$\begin{aligned} 13 &= 4^2 + 4 \cdot (-3) + (-3)^2 \\ &= 3^2 + 3 \cdot 1 + 1^2 \end{aligned}$$

---

*) Da von den Zahlen x, y, $x+y$ stets eine und nur eine gerade ist, so giebt es unter den sechs zu der Wurzel n' gehörenden Darstellungen der Zahl $2m$ immer zwei $\pm (x', y')$, in welchen y' gerade ist $= 2u$; setzt man ferner $x' + u = t$, so geht die Gleichung $x'x' + x'y' + y'y' = m$ über in $tt + 3uu = m$, d. h. man erhält eine Darstellung (t, u) der Zahl m durch die Form (1, 0, 3), und zwar gehört diese Darstellung zu derselben Wurzel n'. Hierin besteht der Zusammenhang zwischen den Darstellungen der Zahlen m und $2m$ resp. durch die Formen (1, 0, 3) und (2, 1, 2).

§. 71.

Als letztes Beispiel wählen wir die Determinante $D = -5$; es giebt *zwei* nicht äquivalente reducirte Formen

$$(1, 0, 5) \text{ und } (2, 1, 3),$$

beide sind ursprünglich und von der ersten Art. Wir suchen wieder das System aller ungeraden und durch 5 nicht theilbaren Zahlen m zu bestimmen, welche durch diese Formen darstellbar sind. Die dazu erforderliche Bedingung besteht darin, dass für jede in m aufgehende Primzahl p die Gleichung

$$\left(\frac{-5}{p}\right) = (-1)^{\frac{1}{2}(p-1)}\left(\frac{p}{5}\right) = +1$$

Statt finden muss; hieraus folgt (§. 52, II), dass jede solche Primzahl von einer der vier Formen

$$20h+1,\quad 20h+9,\quad 20h+3,\quad 20h+7$$

sein muss. Ist diese Bedingung erfüllt, und μ die Anzahl der verschiedenen Primzahlen p, so hat die Congruenz

$$z^2 \equiv -5 \pmod{m}$$

wieder 2^μ incongruente Wurzeln; ist n ein bestimmter Repräsentant einer solchen, und $n^2+5 = ml$, so ist die Form (m, n, l) nothwendig einer und nur einer der beiden obigen reducirten Formen äquivalent; es giebt dann jedesmal (nach §. 62) zwei Substitutionen, durch welche diese reducirte Form in (m, n, l) übergeht, also auch zwei zu der Wurzel n gehörige Darstellungen der Zahl m durch diese reducirte Form. Im Ganzen giebt es also

$$2 \cdot 2^\mu = 2^{\mu+1}$$

Darstellungen einer solchen Zahl durch die obigen reducirten Formen. Allein es bleibt noch zweifelhaft, durch welche der beiden reducirten Formen die zu einer bestimmten Wurzel n gehörigen beiden Darstellungen erfolgen; und eine ähnliche Frage wird jedesmal da auftreten, wo es mehrere nicht äquivalente Formen derselben Art giebt. In unserm Fall ist es nicht schwierig, diesen Zweifel zu heben.

Ist nämlich die Zahl m darstellbar durch die Form $(1, 0, 5)$, also z. B. $m = x^2 + 5y^2$, so folgt hieraus $m \equiv x^2 \pmod{5}$, d. h.

m ist quadratischer Rest von 5; ist dagegen die Zahl m darstellbar durch die zweite Form (2, 1, 3), also z. B. $m = 2x^2 + 2xy + 3y^2$, so ist $2m = (2x + y)^2 + 5y^2 \equiv (2x + y)^2 \pmod 5$, und, da 2 quadratischer Nichtrest von 5 ist, so ist m ebenfalls quadratischer Nichtrest von 5. Es tritt also hier die besonders einfache Erscheinung auf, dass alle Darstellungen einer Zahl entweder nur durch die Form (1, 0, 5) oder nur durch die Form (2, 1, 3) geschehen, je nachdem m quadratischer Rest oder Nichtrest von 5, d. h. je nachdem $m \equiv \pm 1$, oder $\equiv \pm 2 \pmod 5$ ist. Hieraus folgen die speciellen Sätze:

Jede Primzahl von einer der beiden Formen $20h + 1$, $20h + 9$ *ist auf vier Arten durch die Form* (1, 0, 5) *darstellbar (welche wesentlich nur eine einzige Zerlegung in ein einfaches und ein fünffaches Quadrat bilden); jede Primzahl von einer der beiden Formen* $20h + 3$, $20h + 7$ *ist auf vier Arten durch die Form* (2, 1, 3) *darstellbar.*

Beispiel 1: Ist $m = 29$, so sind $n = \pm 13$ die beiden Wurzeln der Congruenz $z^2 \equiv -5 \pmod{29}$; die hieraus gebildete Form (29, 13, 6) geht durch die Substitution

$$\begin{pmatrix} -1, & +1 \\ +2, & -3 \end{pmatrix}$$

in die reducirte Form (1, 0, 5) über; durch Umkehrung dieser Substitution erhält man die Zerlegung

$$29 = 3^2 + 5 \cdot 2^2.$$

Beispiel 2: Für $m = 27$ findet man $n = \pm 7$; die beiden entsprechenden Formen (27, 7, 2) und (27, −7, 2) gehen bezüglich durch die Substitutionen

$$\begin{pmatrix} 0, & +1 \\ -1, & -4 \end{pmatrix} \text{ und } \begin{pmatrix} 0, & 1 \\ -1, & 3 \end{pmatrix}$$

in die reducirte Form (2, 1, 3) über; durch Umkehrung derselben erhält man daher die vier Darstellungen

$$27 = 2(\mp 4)^2 + 2(\mp 4)(\pm 1) + 3(\pm 1)^2$$
$$27 = 2(\pm 3)^2 + 2(\pm 3)(\pm 1) + 3(\pm 1)^2$$

von denen die beiden ersteren zu der Wurzel $+7$, die beiden letzteren zu der Wurzel -7 gehören.

§. 72.

Wir wenden uns nun zu den Formen mit *positiver* Determinante D, um auch für sie die Hauptprobleme der Theorie der Aequivalenz zu lösen. Das zweite Problem (§. 59), aus *einer* Transformation einer Form in eine zweite *alle* Transformationen der erstern in die letztere zu finden, ist durch unsere frühere Untersuchung (§. 62) auf die Aufgabe zurückgeführt, alle ganzzahligen Auflösungen der Gleichung

$$t^2 - Du^2 = \sigma^2$$

zu finden. Dieselbe ist für positive Determinanten bei weitem schwieriger zu lösen, als für negative. Dasselbe gilt von dem ersten Hauptproblem: zu erkennen, ob zwei Formen von gleicher Determinante äquivalent sind oder nicht. Wir schlagen zur Lösung desselben einen ganz andern Weg ein, wie früher bei negativen Determinanten, einen Weg, der aber zugleich die Mittel an die Hand geben wird, auch die obige Gleichung vollständig aufzulösen.*)

Das Charakteristische dieser Methode besteht darin, dass wir auch *irrationale* Grössen in den Kreis unserer Betrachtungen ziehen. Ist nämlich (a, b, c) oder

$$ax^2 + 2bxy + cy^2$$

eine Form, deren Determinante $b^2 - ac = D$ positiv ist, so hat die entsprechende quadratische Gleichung

$$a + 2b\omega + c\omega^2 = 0$$

zwei reelle Wurzeln

$$\omega = \frac{-b \mp \sqrt{D}}{c} = \frac{a}{-b \pm \sqrt{D}},$$

die wir, je nachdem das obere oder untere Zeichen genommen wird, als die *erste* oder *zweite Wurzel der Form* (a, b, c) bezeichnen und von einander unterscheiden wollen, indem wir ein für alle Mal festsetzen, dass das Zeichen $\sqrt{D}$ stets die *positive* Quadratwurzel aus der Determinante bedeuten soll. Durch die Coefficienten der Form (a, b, c) ist also jede ihrer beiden Wurzeln vollständig, ohne Zweideutigkeit bestimmt. Aber umgekehrt ist auch jede Form (a, b, c) der Determinante D durch Angabe *einer* ihrer

*) *Lejeune Dirichlet: Vereinfachung der Theorie der binären quadratischen Formen von positiver Determinante* (Berliner Akad. 1854).

Wurzeln vollständig charakterisirt, in der Weise, dass zwei Formen (a, b, c) und (a', b', c') *derselben* Determinante D nothwendig identisch sind, sobald sie gleiche erste, oder gleiche zweite Wurzeln haben; denn aus der Gleichung

$$\frac{-b' \mp \sqrt{D}}{c'} = \frac{-b \mp \sqrt{D}}{c},$$

worin entweder die beiden oberen, oder die beiden unteren Zeichen zu nehmen sind, ergiebt sich in Folge der Irrationalität von $\sqrt{D}$ zunächst $c' = c$, und dann $b' = b$, also auch $a' = a$.

Im Folgenden nennen wir zwei Wurzeln ω, ω' zweier Formen resp. (a, b, c), (a', b', c') *gleichnamig*, wenn beide erste, oder beide zweite Wurzeln sind, *ungleichnamig* dagegen, wenn die eine die erste, die andere die zweite Wurzel ist. Wir können dann das eben erhaltene Resultat auch so aussprechen: *Wenn zwei Formen dieselbe (positive) Determinante besitzen, und wenn eine Wurzel der einen Form mit der gleichnamigen Wurzel der andern Form übereinstimmt, so sind beide Formen identisch.*

§. 73.

Wir wollen nun annehmen, es seien (a, b, c) und (a', b', c') zwei äquivalente Formen, und zwar wollen wir für einen Augenblick die uneigentliche Aequivalenz nicht ausschliessen, weil dadurch der Nerv der Betrachtung deutlicher hervortritt. Es sei $\left(\begin{smallmatrix}\alpha, \beta\\ \gamma, \delta\end{smallmatrix}\right)$ eine Substitution, durch welche (a, b, c) in (a', b', c') übergeht, also

$$\alpha\delta - \beta\gamma = \varepsilon = \pm 1.$$

Da durch diese Substitution

$$x = \alpha x' + \beta y',\ y = \gamma x' + \delta y'$$

identisch

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

wird, so leuchtet ein, dass vermöge der Formeln

$$\omega = \frac{\gamma + \delta\omega'}{\alpha + \beta\omega'},\quad \omega' = \frac{-\gamma + \alpha\omega}{\delta - \beta\omega}$$

aus einer Wurzel ω' der Form (a', b', c') eine Wurzel ω der Form (a, b, c) gefunden werden kann, und umgekehrt; denn die Wurzeln

dieser Formen sind ja die Werthe der Verhältnisse $y:x$ und $y':x'$, für welche die Formen verschwinden. Aber es fragt sich vor allen Dingen, ob zwei so verbundene Wurzeln ω und ω' gleichnamig sind, oder nicht. Da nun

$$\omega = \frac{-b \mp \sqrt{D}}{c}$$

ist, so folgt

$$\omega' = \frac{\gamma c - \alpha(-b \mp \sqrt{D})}{-\delta c + \beta(-b \mp \sqrt{D})} = \frac{b\alpha + c\gamma \pm \alpha\sqrt{D}}{-b\beta - c\delta \mp \beta\sqrt{D}};$$

machen wir den Nenner rational, indem wir den Bruch durch $-b\beta - c\delta \pm \beta\sqrt{D}$ erweitern und berücksichtigen, dass

$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b'$$
$$a\beta^2 + 2b\beta\delta + c\delta^2 = c'$$

ist, so ergiebt sich

$$\omega' = \frac{-b' \mp \varepsilon\sqrt{D}}{c'}.$$

Wir haben daher folgendes Resultat erhalten: *Wenn eine Form* (a, b, c) *durch eine Substitution* $\left(\begin{smallmatrix}\alpha, \beta\\ \gamma, \delta\end{smallmatrix}\right)$ *in eine äquivalente Form* (a', b', c') *übergeht, so ist je eine Wurzel* ω *der erstern mit je einer Wurzel* ω' *der letztern Form durch die Relation*

$$\omega = \frac{\gamma + \delta\omega'}{\alpha + \beta\omega'}, \quad \omega' = \frac{-\gamma + \alpha\omega}{\delta - \beta\omega}$$

verbunden; und zwar bilden ω, ω' *ein Paar gleichnamiger oder ungleichnamiger Wurzeln der beiden Formen, je nachdem die Substitution eine eigentliche oder uneigentliche ist.*

Wir schliessen von jetzt an uneigentliche Aequivalenz und uneigentliche Substitutionen gänzlich aus; es sind dann also stets zwei *gleichnamige* Wurzeln der beiden äquivalenten Formen in der angegebenen Weise mit einander verbunden. Dieser Satz lässt sich in folgender Weise umkehren:

Wenn zwei Formen (a, b, c), (a', b', c') *dieselbe Determinante haben, und wenn zwei gleichnamige Wurzeln* ω *und* ω' *derselben durch die Gleichung*

$$\omega = \frac{\gamma + \delta\omega'}{\alpha + \beta\omega'}$$

verbunden sind, in welcher die vier ganzen Zahlen α, β, γ, δ *der Gleichung*

$$\alpha\delta - \beta\gamma = 1$$

genügen, so sind die beiden Formen äquivalent, und zwar geht die erstere durch die Substitution $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ *in die letztere über.*

Denn durch diese Substitution geht (a, b, c) in eine äquivalente Form (a'', b'', c'') über, und bezeichnet man mit ω'' ihre mit ω gleichnamige Wurzel, so ist nach dem eben bewiesenen Satze

$$\omega = \frac{\gamma + \delta\omega''}{\alpha + \beta\omega''}, \text{ und folglich } \omega' = \omega'';$$

da ferner der Voraussetzung nach ω' mit ω, folglich auch mit ω'' gleichnamig ist, und da endlich (a', b', c') dieselbe Determinante wie (a, b, c), und folglich auch wie (a'', b'', c'') hat, so ist zufolge der Schlussbemerkung des vorigen Paragraphen (a', b', c') identisch mit (a'', b'', c''), d. h. (a, b, c) geht durch die obige Substitution in (a', b', c') über.

Von besonderer Wichtigkeit für das Folgende ist die Betrachtung zweier *benachbarten* Formen (a, b, a') und (a', b', a''), in welchen der Definition zufolge (§. 63) die Summe $b + b'$ durch a' theilbar, also $b + b' = -a'\delta$ ist, und von welchen die erstere in die letztere durch die Substitution $\left(\begin{smallmatrix}0, & 1\\ -1, & \delta\end{smallmatrix}\right)$ übergeht. Die gleichnamigen Wurzeln ω und ω' dieser beiden Formen hängen durch die Gleichungen

$$\omega = \delta - \frac{1}{\omega'}, \quad \omega' = \frac{1}{\delta - \omega}$$

zusammen.

§. 74.

Auch bei positiven Determinanten vergleicht man zwei Formen, deren Aequivalenz beurtheilt werden soll, nicht unmittelbar mit einander, sondern man transformirt jede von ihnen in eine sogenannte *reducirte**) Form; der Begriff einer solchen ist aber hier wesentlich verschieden von demjenigen, welcher früher (§. 64) für negative Determinanten aufgestellt ist.

Eine Form (a, b, c) von positiver Determinante D heisst eine reducirte Form, wenn, abgesehen vom Zeichen, ihre erste Wurzel

*) *Gauss: D. A.* art. 1 3.

$$\frac{-b-\sqrt{D}}{c} > 1,$$

ihre zweite Wurzel

$$\frac{-b+\sqrt{D}}{c} < 1$$

ist, und wenn ausserdem beide Wurzeln entgegengesetzte Zeichen haben.

Ziehen wir zunächst einige Folgerungen aus dieser Erklärung. Da die erste Wurzel numerisch grösser als die zweite, also auch die Summe der beiden Grössen b und $\sqrt{D}$ numerisch grösser als ihre Differenz sein soll, so muss, da $\sqrt{D}$ positiv ist, auch b positiv sein (nicht $= 0$); da ferner die beiden Wurzeln entgegengesetzte Zeichen haben, so gilt dasselbe auch von den beiden Grössen

$$-(b+\sqrt{D}) \text{ und } -b+\sqrt{D};$$

und da die erstere gewiss negativ ist, so muss die letztere positiv sein; es ist daher

$$0 < b < \sqrt{D}.$$

Bezeichnen wir ferner mit (c) wieder den absoluten Werth des Coefficienten c, so muss also im algebraischen Sinne (d. h. mit Rücksicht auf die Vorzeichen)

$$\frac{b+\sqrt{D}}{(c)} > 1 \text{ und } 0 < \frac{-b+\sqrt{D}}{(c)} < 1,$$

d. h. es muss

$$0 < \sqrt{D}-b < (c) < \sqrt{D}+b$$

sein; und umgekehrt leuchtet ein, dass jede Form (a, b, c), deren Coefficienten diesen letzteren Ungleichungen genügen, sicher eine reducirte Form ist, weil aus ihnen rückwärts die ursprünglichen Bedingungen sich ableiten lassen.

Aus der Definition ergeben sich noch weitere Folgerungen. Da $D = b^2 - ac$ und $b^2 < D$ ist, so müssen a und c entgegengesetzte Zeichen haben; da ferner die erste Wurzel und c ebenfalls entgegengesetzte Zeichen haben, so hat die erste Wurzel dasselbe Vorzeichen wie der erste Coefficient a der Form. Nun hat ferner die zweite Wurzel das entgegengesetzte Zeichen der ersten Wurzel, also dasselbe Vorzeichen wie der dritte Coefficient c der Form, was sich unmittelbar auch daraus ergiebt, dass $\sqrt{D}-b$ positiv ist.

Für den absoluten Werth des ersten Coefficienten a gelten dieselben Bedingungen, wie für den von c; denn da

$$D = b^2 + (a)(c),$$

also

$$(a) = \frac{(\sqrt{D}+b)(\sqrt{D}-b)}{(c)}$$

ist, so ergiebt sich aus den Bedingungen

$$\frac{\sqrt{D}+b}{(c)} > 1, \quad 0 < \frac{\sqrt{D}-b}{(c)} < 1,$$

dass

$$(a) > \sqrt{D}-b, \quad \text{und} \quad (a) < \sqrt{D}+b$$

ist*).

Für das Folgende ist noch der specielle Fall bemerkenswerth, in welchem

$$\sqrt{D}-(a) < b < \sqrt{D} \text{ und } (c) \geqq (a)$$

ist; aus diesen Bedingungen kann man nämlich stets schliessen, dass die Form (a, b, c) reducirt ist, obwohl die Umkehrung nicht gestattet ist. In der That, giebt man diesen Bedingungen die Form

$$0 < \sqrt{D}-b < (a) \leqq (c),$$

so ergiebt sich zunächst, dass die zweite Wurzel

$$\frac{-b+\sqrt{D}}{c}$$

numerisch < 1, ferner dass die erste Wurzel

$$\frac{-b-\sqrt{D}}{c} = \frac{a}{\sqrt{D}-b}$$

numerisch > 1 ist. Hieraus folgt weiter, wie oben, dass b positiv ist, weil $\sqrt{D}+b$ numerisch grösser als $\sqrt{D}-b$ ist; und folglich haben, da ausserdem $b < \sqrt{D}$ ist, beide Wurzeln entgegengesetzte Zeichen. Also ist die Form gewiss eine reducirte.

*) Dasselbe ergiebt sich unmittelbar daraus, dass die erste Wurzel einer Form (a, b, c) der reciproke Werth der zweiten Wurzel ihres *Gefährten* (c, b, a) ist; mithin sind entweder beide Formen reducirt, oder beide nicht reducirt.

§. 75.

Aus der Erklärung einer reducirten Form ergiebt sich ferner der folgende wichtige Satz*) (vergl. §. 67):

Für jede positive Determinante giebt es nur eine endliche Anzahl reducirter Formen.

Denn, bezeichnen wir mit λ die grösste ganze in $\sqrt{D}$ enthaltene Zahl, so dass $\lambda < \sqrt{D} < \lambda + 1$ und also λ mindestens $= 1$ ist, so kann der mittlere Coefficient b einer reducirten Form (a, b, c) nur die λ verschiedenen Werthe $1, 2 \ldots \lambda$ haben; für jeden dieser Werthe von b ist $D - b^2 = (a)(c)$ auf alle mögliche Arten in zwei Factoren zu zerlegen, welche zwischen $\lambda - b$ und $\lambda + 1 + b$ exclusive (oder zwischen $\lambda + 1 - b$ und $\lambda + b$ inclusive) liegen; je zwei solchen Factoren a und c hat man entgegengesetzte Zeichen zu geben, und man muss sie permutiren, wenn sie ungleich sind. Dann sind aber wirklich alle reducirten Formen gefunden, und es giebt deren offenbar nur eine endliche Anzahl.

Beispiel 1: Ist $D = 13$, so ist $\lambda = 3$; wir haben daher folgende Fälle und Zerlegungen:

$$b = 1; \quad 12 = 3 \cdot 4$$
$$b = 2; \quad 9 = 3 \cdot 3$$
$$b = 3; \quad 4 = 1 \cdot 4 = 2 \cdot 2$$

und diese liefern die folgenden 12 reducirten Formen:

$$(\pm 3, 1, \mp 4), (\pm 1, 3, \mp 4), (\pm 3, 2, \mp 3),$$
$$(\pm 4, 1, \mp 3), (\pm 4, 3, \mp 1), (\pm 2, 3, \mp 2).$$

Beispiel 2: Für $D = 19$ ist $\lambda = 4$; wir bilden daher folgende Tabelle:

$$b = 1; \quad 18 \text{ giebt keine Zerlegung};$$
$$b = 2; \quad 15 = 3 \cdot 5;$$
$$b = 3; \quad 10 = 2 \cdot 5;$$
$$b = 4; \quad 3 = 1 \cdot 3;$$

hieraus ergeben sich folgende 12 reducirte Formen:

$$(\pm 3, 2, \mp 5), (\pm 2, 3, \mp 5), (\pm 1, 4, \mp 3),$$
$$(\pm 5, 2, \mp 3), (\pm 5, 3, \mp 2), (\pm 3, 4, \mp 1).$$

*) *Gauss: D. A.* art. 185.

Beispiel 3: Für $D = 35$ ist $\lambda = 5$; also bilden wir die Tabelle

$b = 1$; 34 giebt keine Zerlegung;
$b = 2$; 31 „ „ „
$b = 3$; 26 „ „ „
$b = 4$; 19 „ „ „
$b = 5$; $10 = 1 \cdot 10 = 2 \cdot 5$;

wir erhalten daher 8 reducirte Formen:

$(\pm 1, 5, \mp 10)$, $(\pm 2, 5, \mp 5)$;
$(\pm 10, 5, \mp 1)$, $(\pm 5, 5, \mp 2)$.

Beispiel 4: Für $D = 79$ ist $\lambda = 8$; wir bilden daher folgende Tabelle:

$b = 1$; 78 giebt keine Zerlegung;
$b = 2$; 75 „ „ „
$b = 3$; $70 = 7 \cdot 10$;
$b = 4$; $63 = 7 \cdot 9$;
$b = 5$; $54 = 6 \cdot 9$;
$b = 6$; 43 giebt keine Zerlegung;
$b = 7$; $30 = 2 \cdot 15 = 3 \cdot 10 = 5 \cdot 6$;
$b = 8$; $15 = 1 \cdot 15 = 3 \cdot 5$;

wir erhalten daher 32 reducirte Formen:

$(\pm 7, 3, \mp 10)$, $(\pm 7, 4, \mp 9)$, $(\pm 6, 5, \mp 9)$, $(\pm 2, 7, \mp 15)$,
$(\pm 3, 7, \mp 10)$, $(\pm 5, 7, \mp 6)$, $(\pm 1, 8, \mp 15)$, $(\pm 3, 8, \mp 5)$,

und

$(\pm 10, 3, \mp 7)$, $(\pm 9, 4, \mp 7)$, $(\pm 9, 5, \mp 6)$, $(\pm 15, 7, \mp 2)$,
$(\pm 10, 7, \mp 3)$, $(\pm 6, 7, \mp 5)$, $(\pm 15, 8, \mp 1)$, $(\pm 5, 8, \mp 3)$.

§. 76.

Aehnlich wie bei negativen Determinanten (§. 64) beweisen wir auch die Richtigkeit des folgenden Satzes*):

Jede Form von positiver Determinante ist einer reducirten Form äquivalent.

Bezeichnen wir die gegebene Form von positiver Determinante

*) *Gauss: D. A.* art. 183.

D mit (a, b, a'), so suchen wir eine ihr nach rechts benachbarte Form (a', b', a'') so zu bestimmen, dass

$$\sqrt{D} - (a') < b' < \sqrt{D}$$

wird. Da zufolge der Erklärung einer benachbarten Form der mittlere Coefficient b' jeden Werth erhalten kann, welcher $\equiv -b \pmod{a'}$ ist, und keinen andern, so fragt sich nur, ob zwischen den Grenzen $\sqrt{D} - (a')$ und $\sqrt{D}$ stets ein solcher Werth existirt; dies ist offenbar der Fall, da die sämmtlichen zwischen diesen beiden Grenzen enthaltenen ganzen Zahlen

$$\lambda + 1 - (a'), \quad \lambda + 2 - (a') \ldots \lambda - 1, \quad \lambda$$

ein vollständiges Restsystem in Bezug auf den Modulus a' bilden; aus demselben Grunde ergiebt sich, dass nur eine einzige solche Zahl b' existirt. Nachdem $b' = -b - a'\delta$ bestimmt ist, geht die Form (a, b, a') durch die Substitution $\left(\begin{smallmatrix} 0, & 1 \\ -1, & \delta \end{smallmatrix}\right)$ in die benachbarte Form (a', b', a'') über, deren Coefficienten a', b' der obigen Bedingung Genüge leisten. Findet sich nun, dass zu gleicher Zeit $(a'') \geqq (a')$ wird, so ist nach dem am Schlusse des §. 74 besonders hervorgehobenen speciellen Fall die gefundene Form (a', b', a'') eine reducirte. Ist dagegen

$$(a') > (a''),$$

so verfahre man mit der gefundenen Form (a', b', a'') genau so wie mit der gegebenen Form, d. h. man bilde die ihr nach rechts benachbarte Form (a'', b'', a'''), in welcher

$$\sqrt{D} - (a'') < b'' < \sqrt{D}$$

ist, und welche gewiss eine reducirte ist, wenn $(a''') \geqq (a'')$ ist. Sollte aber wieder

$$(a'') > (a''')$$

sein, so setze man denselben Process in derselben Weise fort; da unter einer gegebenen positiven Zahl (a') nur eine endliche Anzahl von ganzen positiven Zahlen liegt, so muss man nach einer endlichen Anzahl von Transformationen durchaus zu einer Form $(a^{(n)}, b^{(n)}, a^{(n+1)})$, in welcher sowohl

$$\sqrt{D} - (a^{(n)}) < b^{(n)} < \sqrt{D}$$

als auch

$$(a^{(n+1)}) \geqq (a^{(n)})$$

ist, also zu einer reducirten Form gelangen, was zu beweisen war.

Es verdient bemerkt zu werden, dass bei diesem Process nicht gerade erst die letzte Form eine reducirte zu sein braucht, denn

es giebt reducirte Formen, in welchen die Bedingungen des besondern hier benutzten speciellen Falles nicht erfüllt sind. Von grösserer Wichtigkeit ist es aber, besonders darauf aufmerksam zu machen, dass durch den angegebenen Process auch jedes Mal eine Substitution gefunden wird, durch welche die gegebene Form in die reducirte Form übergeht, und zwar erhält man diese Substitution durch Composition der successiven Substitutionen, welche in dem Processe auftreten. Der Algorithmus selbst ist durchaus nicht beschwerlich (vergl. §. 64), wie folgende Beispiele zeigen.

Beispiel 1: Die Form (4, 6, 7) hat die Determinante $D = 8$; es ist also $\lambda = 2$. Unter den Zahlen

$$-4, -3, -2, -1, 0, 1, 2$$

ist $b' = 1 \equiv -6 \pmod 7$; dies giebt die benachbarte Form $(7, 1, -1)$, welche noch nicht reducirt ist. Da $(a'') = 1$ ist, so ist $b'' = \lambda = 2$, und folglich erhält man die benachbarte Form $(-1, 2, 4)$, welche wirklich reducirt ist. Durch die Substitution $\left(\begin{smallmatrix} 0, & +1 \\ -1, & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0, & 1 \\ -1, & 3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1, & +3 \\ +1, & -4 \end{smallmatrix}\right)$ geht die gegebene Form in die gefundene über.

Beispiel 2: Die Form (713, 60, 5) hat die Determinante $D = 35$; man findet nach der angegebenen Methode die nach rechts benachbarte Form (5, 5, −2), und zu dieser wieder die Form (−2, 5, 5), in welcher der letzte Coefficient in der That grösser ist als der erste. In diesem Beispiel ist aber auch schon die vorhergehende Form (5, 5, −2) reducirt. Die gegebene Form geht durch die Substitution $\left(\begin{smallmatrix} 0, & +1 \\ -1, & -13 \end{smallmatrix}\right)$ in (5, 5, −2) und durch die Substitution $\left(\begin{smallmatrix} 0, & +1 \\ -1, & -13 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0, & 1 \\ -1, & 5 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1, & +5 \\ 13, & -66 \end{smallmatrix}\right)$ in (−2, 5, 5) über.

Beispiel 3: Die Form (62, 95, 145), deren Determinante $D = 35$, geht durch die folgenden successiven Substitutionen

$$\left(\begin{smallmatrix} 0, & 1 \\ -1, & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0, & 1 \\ -1, & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0, & 1 \\ -1, & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0, & 1 \\ -1, & 4 \end{smallmatrix}\right)$$

successive in die Formen

$$(145, -95, 62), \quad (62, -29, 13), \quad (13, 3, -2), \quad (-2, 5, 5)$$

über, von denen erst die letzte reducirt ist; die Zusammensetzung dieser Substitutionen giebt die Substitution $\left(\begin{smallmatrix} -3, & +10 \\ +2, & -7 \end{smallmatrix}\right)$, durch welche (62, 95, 145) in (−2, 5, 5) übergeht.

§. 77.

Nachdem in den beiden vorhergehenden Paragraphen dargethan ist, dass jede Form von positiver Determinante einer reducirten Form äquivalent ist, und dass nur eine endliche Anzahl von reducirten Formen für jede gegebene Determinante existirt, so folgt hieraus unmittelbar:

Die Anzahl der Classen nicht äquivalenter Formen von positiver Determinante ist stets endlich.

Allein es bleibt noch die Hauptfrage zu beantworten, ob zwei nicht identische reducirte Formen derselben Determinante einander äquivalent sein können; denn erst dann haben wir (wie in §§. 65, 66 für negative Determinanten) die Mittel gewonnen, um über die Aequivalenz von zwei gegebenen Formen derselben positiven Determinante entscheiden zu können. Diese Untersuchung stösst bei positiven Determinanten auf bedeutende Schwierigkeiten, da in der That immer mehrere nicht identische und doch äquivalente reducirte Formen existiren.

Um einen sichern Boden für diese Untersuchung zu gewinnen, stellen wir zunächst die bestimmte Frage*):

Kann eine reducirte Form (a, b, a') *eine ihr nach rechts benachbarte Form* (a', b', a'') *haben, welche ebenfalls reducirt ist?*

Nehmen wir einmal an, dies sei möglich, und es sei $\left(\begin{smallmatrix} 0, & 1 \\ -1, & \delta \end{smallmatrix}\right)$ die Substitution, durch welche die reducirte Form (a, b, a') in die ebenfalls reducirte Form (a', b', a'') übergeht. Sind dann ω und ω' zwei gleichnamige Wurzeln der ersten und der zweiten Form, so hängen diese (nach §. 73) durch die Gleichungen

$$\omega = \delta - \frac{1}{\omega'}, \quad \omega' = \frac{1}{\delta - \omega}$$

mit einander zusammen. Wir wollen der Einfachheit halber festsetzen, dass ω und ω' die beiden *ersten* Wurzeln der beiden Formen bedeuten (obgleich dieselbe Relation auch zwischen den beiden zweiten Wurzeln Statt findet). Da in einer reducirten Form die beiden äusseren Coefficienten entgegengesetzte Zeichen haben, und die erste Wurzel stets das Zeichen des ersten Coefficienten besitzt, so haben die beiden *unechten* Brüche ω und ω' bezüglich die Vorzeichen von a und a', also *entgegengesetzte* Vorzeichen, da der erste

*) *Gauss: D. A.* art. 184.

Coefficient a' der zweiten Form zugleich der letzte Coefficient der ersten Form ist. Zufolge der obigen Relationen muss daher $\omega - \delta$ ein *echter* Bruch sein von gleichem Vorzeichen wie ω; es muss daher δ diejenige vollständig bestimmte ganze Zahl sein, welche dem absoluten Werth nach nächst kleiner als ω ist und dem Vorzeichen nach mit ω übereinstimmt. Wir schliessen hieraus, dass eine reducirte Form (a, b, a') höchstens eine einzige nach rechts benachbarte Form (a', b', a'') hat, welche ebenfalls reducirt ist.

Aber es existirt auch wirklich immer eine solche der reducirten Form (a, b, a') nach rechts benachbarte und reducirte Form (a', b', a''). Denn es sei ω die erste Wurzel der reducirten Form (a, b, a'), also ein unechter Bruch, dessen Vorzeichen mit dem von a übereinstimmt; so wähle man die ganze Zahl δ so, dass ihr absoluter Werth (δ) die grösste ganze in (ω) enthaltene ganze Zahl (also nie $= 0$) wird, und gebe δ das Vorzeichen von ω; dann geht die gegebene Form (a, b, a') durch die so bestimmte Substitution $\left(\begin{smallmatrix} 0; & 1 \\ -1; & \delta \end{smallmatrix}\right)$ in eine benachbarte Form (a', b', a'') über, deren erste Wurzel

$$\omega' = \frac{1}{\delta - \omega}$$

ein unechter Bruch ist, dessen Vorzeichen dem von ω und a entgegengesetzt ist und also mit dem von a' übereinstimmt. Bezeichnen wir nun mit ω_1 und ω'_1 die beiden zweiten Wurzeln, so besteht zwischen ihnen dieselbe Relation

$$\omega'_1 = \frac{1}{\delta - \omega_1};$$

da nun ω_1 ein echter Bruch ist, dessen Vorzeichen dem von ω, und also auch dem von δ entgegengesetzt, und da δ eine von Null verschiedene ganze Zahl ist, so folgt, dass $\delta - \omega_1$ ein unechter Bruch, und also ω'_1 ein echter Bruch ist, dessen Vorzeichen mit dem von δ, ω und a übereinstimmt, also dem von ω' und a' entgegengesetzt ist. Es ist also bewiesen, dass die beiden Wurzeln ω' und ω'_1 der neuen Form (a', b', a'') entgegengesetzte Zeichen haben, ferner dass die erste ω' ein unechter, die zweite ω'_1 ein echter Bruch ist; folglich ist diese Form in der That eine reducirte, was zu beweisen war.

Jede reducirte Form hat daher eine und nur eine nach rechts benachbarte Form, welche ebenfalls reducirt ist, und diese kann auf die angegebene Weise immer leicht gefunden werden.

Genau ebenso liesse sich nun auch beweisen, dass jede redu-

cirte Form eine und nur eine nach links benachbarte reducirte Form besitzt. Doch ist es bequemer, diesen Fall auf den eben behandelten durch die einleuchtende Bemerkung (§. 74 Anm.) zurückzuführen, dass die beiden Formen (a, b, a') und (a', b, a) gleichzeitig reducirte, oder gleichzeitig nicht reducirte Formen sind. Wenn nun die reducirte Form (a, b, a') eine nach links benachbarte und ebenfalls reducirte Form $('a, 'b, a)$ besitzt, so hat die reducirte Form (a', b, a) die nach rechts benachbarte Form $(a, 'b, 'a)$, welche ebenfalls reducirt ist; und umgekehrt, sobald die Form $(a, 'b, 'a)$ der reducirten Form (a', b, a) nach rechts benachbart und zugleich reducirt ist, so ist die Form $('a, 'b, a)$ ebenfalls reducirt und der Form (a, b, a') nach links benachbart. Da wir nun gesehen haben, dass eine reducirte Form (a', b, a) immer eine und nur eine nach rechts benachbarte reducirte Form $(a, 'b, 'a)$ hat, so folgt:

Jede reducirte Form (a, b, a') *besitzt stets eine und nur eine nach links benachbarte reducirte Form* $('a, 'b, a)$.

§. 78.

Aus den soeben bewiesenen Sätzen über die nach rechts und links benachbarten reducirten Formen ergiebt sich, dass man sämmtliche reducirte Formen einer positiven Determinante D in *Perioden**) eintheilen kann, die auf folgende Weise zu bilden sind. Man wähle irgend eine reducirte Form φ_0 und bilde die nach rechts und links fortgesetzte Reihe

$$\cdots\cdot \varphi_{-2}, \varphi_{-1}, \varphi_0, \varphi_1, \varphi_2 \cdots\cdot$$

der successiven nach rechts und nach links benachbarten reducirten Formen, welche durch das eine Glied φ_0 vollständig bestimmt sind. Da es nur eine endliche Anzahl von reducirten Formen der Determinante D giebt, und die ersten Coefficienten zweier auf einander folgenden Formen stets entgegengesetzte Zeichen haben, so muss einmal auf eine Form φ_μ dieser Reihe nach einer geraden Anzahl $2n$ von Gliedern eine mit φ_μ identische Form $\varphi_{\mu+2n}$ folgen; und da eine Form φ_μ oder $\varphi_{\mu+2n}$ nur eine

*) *Gauss: D. A.* art. 186.

einzige nach rechts, und nur eine einzige nach links benachbarte reducirte Form besitzt, so müssen auch die beiden Formen $\varphi_{\mu+1}$ und $\varphi_{\mu+1+2n}$, ebenso die beiden Formen $\varphi_{\mu-1}$ und $\varphi_{\mu-1+2n}$, und also auch allgemein je zwei Formen dieser Reihe identisch sein, deren Indices dieselbe Differenz $2n$ haben. In der ganzen Reihe sind daher höchstens $2n$ verschiedene Formen

$$\varphi_0,\ \varphi_1,\ \varphi_2 \ldots \varphi_{2n-2},\ \varphi_{2n-1};$$

und diese werden in der That alle von einander verschieden sein, wenn keine der Formen $\varphi_2,\ \varphi_4 \ldots \varphi_{2n-2}$ mit φ_0 identisch ist; denn wären φ_ν und $\varphi_{\nu+2n'}$ zwei identische Formen, so müsste auch $\varphi_{2n'}$ mit φ_0 identisch sein. Nehmen wir also an, dass $2n$ die Anzahl der wirklich verschiedenen Formen dieser Reihe ist, so besteht dieselbe aus einer nach beiden Seiten sich unendlich oft periodisch wiederholenden Folge dieser $2n$ Formen; je zwei Formen φ_μ und φ_ν, deren Indices eine durch $2n$ theilbare Differenz $\mu - \nu$ haben, sind identisch; und umgekehrt, sind die Formen φ_μ und φ_ν identisch, so ist $\mu \equiv \nu \pmod{2n}$.

Es kann nun sein, dass diese $2n$ Formen alle reducirten Formen der Determinante D erschöpfen; aber es ist auch möglich, dass ausser ihnen noch andere reducirte Formen derselben Determinante existiren. Im letztern Fall sei ψ_0 eine solche, in der obigen Periode nicht enthaltene reducirte Form, so entspricht ihr ebenso eine Periode von $2m$ unter einander verschiedenen Formen

$$\psi_0,\ \psi_1,\ \psi_2 \ldots \psi_{2m-2},\ \psi_{2m-1};$$

alle diese Formen der zweiten Periode werden auch von denen der ersten verschieden sein; denn besässen beide Perioden eine gemeinschaftliche Form, so wären beide Reihen vollständig identisch, da von dieser gemeinschaftlichen Form aus die Reihe nur auf eine einzige Weise nach rechts und links fortgesetzt werden kann.

In derselben Weise kann man fortfahren, bis endlich alle reducirten Formen in verschiedene Perioden eingetheilt sind; die Anzahl der Perioden ist nothwendig eine endliche; die Anzahl der Glieder kann in verschiedenen Perioden verschieden sein, jedenfalls ist sie stets gerade*).

*) Von besonderem Interesse sind noch folgende Bemerkungen (*Gauss: D. A.* artt. 187, 194). Wenn (a, b, c) eine reducirte Form ist, so gilt Dasselbe von ihrem Gefährten (c, b, a) (§. 74); sind die Perioden dieser beiden Formen entwickelt, und die beiden Formen selbst nach den Plätzen, welche sie in diesen Perioden einnehmen, mit φ_μ und ψ_ν bezeichnet, so leuchtet

Beispiel 1: Wir haben (§. 75) das System der reducirten Formen für die Determinante $D = 13$ aufgestellt; nehmen wir z. B. für φ_0 die Form $(3, 1, -4)$, so erhalten wir folgende Periode von zehn Formen

$$\varphi_0 = (3, 1, -4); \ \varphi_1 = (-4, 3, 1);$$
$$\varphi_2 = (1, 3, -4); \ \varphi_3 = (-4, 1, 3);$$
$$\varphi_4 = (3, 2, -3); \ \varphi_5 = (-3, 1, 4);$$
$$\varphi_6 = (4, 3, -1); \ \varphi_7 = (-1, 3, 4);$$
$$\varphi_8 = (4, 1, -3); \ \varphi_9 = (-3, 2, 3).$$

---

ein, dass auch $\varphi_{\mu+1}$ und $\psi_{\nu-1}$, allgemeiner je zwei Formen $\varphi_{\mu+h}$ und $\psi_{\nu-h}$ Gefährten sind, wo h jede beliebige ganze Zahl bedeutet. Hieraus geht hervor, dass beide Perioden aus gleich vielen Gliedern bestehen werden.

Es ist nun möglich, dass beide Perioden identisch sind, dass also ψ_ν selbst ein Glied in der Periode der Form φ_μ ist; und dann wird offenbar der Gefährte einer jeden Form dieser Periode ein Glied derselben Periode sein. Ist nun φ_r der Gefährte von φ_0, so ist; weil die äusseren Coefficienten einer reducirten Form entgegengesetzte Vorzeichen, und ausserdem die ersten Coefficienten der auf einander folgenden Formen abwechselnde Vorzeichen haben, nothwendig r ungerade $= 2m-1$; da nun φ_0 und φ_{2m-1} Gefährten sind, so gilt Dasselbe von φ_h und φ_{2m-1-h}, also auch von φ_m und φ_{m-1}, und ebenso, wenn $2n$ die Anzahl der Glieder der Periode bedeutet, von φ_{m+n} und $\varphi_{m-1-n} = \varphi_{m+n-1}$; bezeichnet man daher irgend eine der beiden Formen φ_m oder φ_{m+n} mit (A, B, C), so ist die ihr nach links benachbarte Form identisch mit (C, B, A), und folglich ist $2B \equiv 0 \pmod{A}$, d. h. φ_m und φ_{m+n} sind *ambige* Formen; und sie sind verschieden, weil m nicht $\equiv m+n \pmod{2n}$ ist.

Umgekehrt, ist in einer Periode eine ambige Form (A, B, C) enthalten, so ist ihr linker Nachbar ihr Gefährte (C, B, A), und folglich findet sich in derselben Periode noch eine zweite ambige Form. Ausser diesen beiden ambigen Formen φ_m und φ_{m+n} giebt es aber keine andere ambige Form in derselben Periode; denn, wenn φ_s eine ambige Form ist, so sind φ_{s-1} und φ_s, und folglich auch φ_{2s-1} und φ_0 Gefährten; mithin ist φ_{2s-1} identisch mit φ_{2m-1}, folglich $2s \equiv 2m \pmod{2n}$, also $s \equiv m$, oder $s \equiv m+n \pmod{2n}$.

Dieser Fall kann offenbar nur bei der Periode einer solchen Form eintreten (§§. 56, 58), welche ihrem Gefährten eigentlich und folglich sich selbst uneigentlich äquivalent ist, d. h. wenn die Form einer sogenannten *ambigen Classe* angehört. Dass umgekehrt jedes Mal, wenn diese Bedingung erfüllt ist, die Periode der Form auch ihren Gefährten und folglich zwei ambige Formen enthalten muss, ist eine unmittelbare Folge des weiter unten (§. 82) bewiesenen Hauptsatzes dieser ganzen Theorie. — Man vergleiche die Beispiele im Text.

Diese Rechnung geschieht am einfachsten auf folgende Art; um aus der reducirten Form (a, b, a') die ihr nach rechts benachbarte reducirte Form (a', b', a'') zu finden, braucht man nur ihren mittlern Coefficienten b' zu suchen, welcher durch die Bedingung $b' \equiv -b - a'\delta \pmod{a'}$ und die Nebenbedingungen

$$\lambda + 1 - (a') \leqq b' \leqq \lambda$$

stets vollständig bestimmt ist und durch den blossen Anblick der Form sogleich erkannt wird. In unserm Fall ist $\lambda = 3$; man findet daher den mittlern Coefficienten b' der Form φ_1 durch die Bedingungen

$$b' \equiv -1 \pmod{4}, \quad 0 \leqq b' \leqq 3,$$

nämlich $b' = 3$. Und nachdem so b' und $\delta = 1$ gefunden sind, ergiebt sich

$$a'' = \frac{b'^2 - D}{a'} = a + (b - b')\delta,$$

also in unserm Fall $a'' = 1$. In derselben Weise ist fortzufahren, bis die erste Form φ_0 sich reproducirt; in unserm Beispiel wird der mittlere Coefficient von φ_{10} dadurch bestimmt, dass er $\equiv -2 \pmod{3}$ sein, und ausserdem nicht ausserhalb der Grenzen 1 und 3 liegen muss, woraus folgt, dass er $= 1$ ist; also wird φ_{10} identisch mit φ_0.

Die so gefundenen zehn ursprünglichen Formen der ersten Art erschöpfen aber noch nicht alle reducirten Formen der Determinante 13; es bleiben noch zwei ursprüngliche Formen der zweiten Art übrig

$$\psi_0 = (2, 3, -2), \quad \psi_1 = (-2, 3, 2),$$

welche offenbar noch eine zweite Periode bilden.

Beispiel 2: Für $D = 19$ erhalten wir folgende zwei Perioden, jede von sechs Gliedern:

$$\varphi_0 = (3, 2, -5); \quad \varphi_1 = (-5, 3, 2)$$
$$\varphi_2 = (2, 3, -5); \quad \varphi_3 = (-5, 2, 3)$$
$$\varphi_4 = (3, 4, -1); \quad \varphi_5 = (-1, 4, 3)$$

und

$$\psi_0 = (-3, 2, 5); \quad \psi_1 = (5, 3, -2)$$
$$\psi_2 = (-2, 3, 5); \quad \psi_3 = (5, 2, -3)$$
$$\psi_4 = (-3, 4, 1); \quad \psi_5 = (1, 4, -3).$$

Beispiel 3: Für $D = 35$ erhält man folgende vier Perioden, jede von zwei Gliedern:

$$\varphi_0 = (1, 5, -10), \quad \varphi_1 = (-10, 5, 1)$$
$$\psi_0 = (10, 5, -1), \quad \psi_1 = (-1, 5, 10)$$
$$\chi_0 = (2, 5, -5), \quad \chi_1 = (-5, 5, 2)$$
$$\theta_0 = (5, 5, -2), \quad \theta_1 = (-2, 5, 5).$$

Beispiel 4: Die 32 reducirten Formen der Determinante $D = 79$ zerfallen in vier Perioden von je sechs Gliedern und zwei Perioden von je vier Gliedern; eine der sechsgliedrigen Perioden ist folgende:

$$\varphi_0 = (7, 3, -10); \quad \varphi_1 = (-10, 7, 3)$$
$$\varphi_2 = (3, 8, -5); \quad \varphi_3 = (-5, 7, 6)$$
$$\varphi_4 = (6, 5, -9); \quad \varphi_5 = (-9, 4, 7);$$

aus ihr entstehen die drei anderen durch Vertauschung der äusseren Coefficienten (womit die Vertauschung von rechts nach links in der Folge der Glieder verbunden ist), ferner durch Verwandlung der Vorzeichen der äusseren Coefficienten in die entgegengesetzten. Eine der beiden viergliedrigen Perioden ist

$$\psi_0 = (1, 8, -15); \quad \psi_1 = (-15, 7, 2)$$
$$\psi_2 = (2, 7, -15); \quad \psi_3 = (-15, 8, 1);$$

aus ihr entsteht die andere durch die Zeichenänderung der äusseren Coefficienten.

§. 79.

Die vorhergehenden Untersuchungen über die Perioden der reducirten Formen von positiver Determinante stehen in der engsten Beziehung zu der Entwicklung der Wurzeln dieser Formen in Kettenbrüche. Nehmen wir für die Anfangsform φ_0 einer Periode immer eine solche, deren erster Coefficient *positiv* ist, so ist auch ihre *erste* Wurzel ω_0 positiv. Wir bezeichnen mit ω_μ die *erste* Wurzel der Form φ_μ, mit δ_μ den vierten Coefficienten der Substitution

$$\begin{pmatrix} 0, & +1 \\ -1, & \delta_\mu \end{pmatrix},$$

durch welche φ_μ in die nach rechts benachbarte Form $\varphi_{\mu+1}$ übergeht, und endlich mit k_μ den absoluten Werth von δ_μ. Da (nach §. 77) der Coefficient δ_μ seinem Zeichen nach mit ω_μ übereinstimmt, und dem absoluten Werth nach die grösste in dem absoluten Werth von ω_μ enthaltene ganze Zahl ist, und da die Wurzeln $\omega_0, \omega_1, \omega_2 \cdots$ abwechselnd positiv und negativ sind, so ist $(-1)^\mu \omega_\mu$ stets positiv, und folglich

$$k_\mu = (-1)^\mu \delta_\mu;$$

zwischen den successiven Wurzeln $\omega_\mu, \omega_{\mu+1} \ldots$ bestehen aber folgende Relationen (§. 77):

$$\omega_\mu = \delta_\mu - \frac{1}{\omega_{\mu+1}}; \quad \omega_{\mu+1} = \delta_{\mu+1} - \frac{1}{\omega_{\mu+2}} \cdots$$

multiplicirt man diese Gleichungen der Reihe nach mit $\pm 1, \mp 1$ u. s. w. der Art, dass die linke Seite stets positiv wird, so erhält man

$$\pm \omega_\mu = k_\mu + \frac{1}{\mp \omega_{\mu+1}}; \quad \mp \omega_{\mu+1} = k_{\mu+1} + \frac{1}{\pm \omega_{\mu+2}} \cdots$$

und hieraus ergiebt sich für den positiven irrationalen unechten Bruch $(-1)^\mu \omega_\mu$ der folgende unendliche Kettenbruch (§. 23):

$$(-1)^\mu \omega_\mu = (k_\mu, k_{\mu+1}, k_{\mu+2} \ldots).$$

Offenbar ist dieser Kettenbruch periodisch; denn besteht die Periode der reducirten Formen φ aus $2n$ Gliedern, so ist $\delta_{\mu+2n} = \delta_\mu$ und also auch $k_{\mu+2n} = k_\mu$; es wiederholt sich daher die Reihe der Zahlen k immer nach höchstens $2n$ Gliedern von Neuem.

Beispiel 1: Nehmen wir $D = 13$, so haben wir, um die erste Wurzel ω_0 der Form $\varphi_0 = (3, 1, -4)$ in einen Kettenbruch zu entwickeln, ihre Periode aufzustellen (§. 78):

$$\begin{aligned} \varphi_0 &= (3, 1, -4); & \varphi_1 &= (-4, 3, 1) \\ \varphi_2 &= (1, 3, -4); & \varphi_3 &= (-4, 1, 3) \\ \varphi_4 &= (3, 2, -3); & \varphi_5 &= (-3, 1, 4) \\ \varphi_6 &= (4, 3, -1); & \varphi_7 &= (-1, 3, 4) \\ \varphi_8 &= (4, 1, -3); & \varphi_9 &= (-3, 2, 3); \end{aligned}$$

die successiven Werthe der Substitutionscoefficienten δ sind folgende:

$$\begin{aligned} &\delta_0 = +1, \quad \delta_1 = +6, \quad \delta_2 = +1, \quad \delta_3 = -1, \quad \delta_4 = +1, \\ &\delta_5 = -1, \quad \delta_6 = +6, \quad \delta_7 = -1, \quad \delta_8 = +1, \quad \delta_9 = -1; \end{aligned}$$

daraus ergeben sich die absoluten Werthe

$$k_0 = 1, \quad k_1 = 6, \quad k_2 = 1, \quad k_3 = 1, \quad k_4 = 1,$$
$$k_5 = 1, \quad k_6 = 6, \quad k_7 = 1, \quad k_8 = 1, \quad k_9 = 1.$$

Hier zeigt sich die eigenthümliche Erscheinung, dass die Period des Kettenbruchs nur aus fünf Gliedern besteht, während die Periode der Formen doppelt so viele Glieder enthält; wir werden später (§. 83) darauf zurückkommen. Die gesuchte Kettenbruch-Entwicklung ergiebt sich hieraus als die folgende:

$$\frac{1+\sqrt{13}}{4} = (1, 6, 1, 1, 1; 1, 6, 1, 1, 1; \ldots)$$

Ebenso liefern die beiden anderen reducirten Formen derselben Determinante $D = 13$, nämlich

$$\varphi_0 = (2, 3, -2), \quad \varphi_1 = (-2, 3, 2)$$

folgende Werthe

$$\delta_0 = +3, \ \delta_1 = -3,$$

also

$$k_0 = 3, \quad k_1 = 3$$

und folglich

$$\frac{3+\sqrt{13}}{2} = (3; 3; \ldots);$$

auch hier ist die Periode des Kettenbruchs nur halb so gross wie die der reducirten Formen.

Beispiel 2: Für $D = 19$ giebt die sechsgliedrige Formenperiode

$$\varphi_0 = (3, 2, -5); \quad \varphi_1 = (-5, 3, 2)$$
$$\varphi_2 = (2, 3, -5); \quad \varphi_3 = (-5, 2, 3)$$
$$\varphi_4 = (3, 4, -1); \quad \varphi_5 = (-1, 4, 3)$$

die Zahlen

$$\delta_0 = +1, \ \delta_1 = -3, \ \delta_2 = +1, \ \delta_3 = -2, \ \delta_4 = +8, \ \delta_5 = -2;$$
$$k_0 = 1, \quad k_1 = 3, \quad k_2 = 1, \quad k_3 = 2, \quad k_4 = 8, \quad k_5 = 2;$$

also

$$\frac{2+\sqrt{19}}{5} = (1, 3, 1, 2, 8, 2; \ldots)$$

Beispiel 3: Für $D = 79$ giebt die sechsgliedrige Periode

$$\varphi_0 = (7, 3, -10); \quad \varphi_1 = (-10, 7, 3)$$
$$\varphi_2 = (3, 8, -5); \quad \varphi_3 = (-5, 7, 6)$$
$$\varphi_4 = (6, 5, -9); \quad \varphi_5 = (-9, 4, 7)$$

die Zahlen

$$\delta_0 = +1, \ \delta_1 = -5, \ \delta_2 = +3, \ \delta_3 = -2, \ \delta_4 = +1, \ \delta_5 = -1;$$
$$k_0 = 1, \quad k_1 = 5, \quad k_2 = 3, \quad k_3 = 2, \quad k_4 = 1, \quad k_5 = 1;$$

also entsteht die Entwicklung

$$\frac{3 + \sqrt{79}}{10} = (1, 5, 3, 2, 1, 1; \ldots).$$

Ebenso liefert die viergliedrige Periode

$$\varphi_0 = (1, 8, -15); \quad \varphi_1 = (-15, 7, 2)$$
$$\varphi_2 = (2, 7, -15); \quad \varphi_3 = (-15, 8, 1)$$

die Zahlen

$$\delta_0 = +1, \ \delta_1 = -7, \ \delta_2 = +1, \ \delta_3 = -16$$
$$k_0 = 1, \ k_1 = 7, \ k_2 = 1, \ k_3 = 16;$$

also den Kettenbruch

$$\frac{8 + \sqrt{79}}{15} = (1, 7, 1, 16; \ldots).$$

Zu gleicher Zeit findet man natürlich auch die Entwicklung der Wurzeln der drei anderen Formen

$$-\frac{7 + \sqrt{79}}{2} = -(7, 1, 16, 1; \ldots)$$
$$\frac{7 + \sqrt{79}}{15} = (1, 16, 1, 7; \ldots)$$
$$-\frac{8 + \sqrt{79}}{1} = -(16, 1, 7, 1; \ldots)$$

durch einfache Verschiebung der Periode*).

---

*) Die Form $(1, 0, -D)$ ist der reducirten Form $\varphi_0 = (1, \lambda, \lambda^2 - D)$ äquivalent; die letzte Form der entsprechenden Periode ist offenbar $\varphi_{2n-1} = (\lambda^2 - D, \lambda, 1)$, und hieraus folgt eine Entwicklung von der Form

$$\frac{1}{\sqrt{D} - \lambda} = (k_0 \ldots k_{n-2}, k_{n-1}, k_{n-2} \ldots k_0, 2\lambda; \ldots)$$

und

$$\sqrt{D} = (\lambda; k_0 \ldots k_{n-2}, k_{n-1}, k_{n-2} \ldots k_0, 2\lambda; \ldots).$$

Eine ähnliche Entwicklung tritt jedes Mal auf, wenn in der Periode zwei ambige Formen vorkommen (§. 78).

§. 80.

Es bleibt nun noch die schwierigste Frage zu beantworten übrig, nämlich die, ob zwei reducirte Formen derselben Determinante, welche verschiedenen Perioden angehören, äquivalent sein können oder nicht. Dazu müssen wir eine Digression über die Theorie der Kettenbrüche machen, in welcher wir einige weniger bekannte Sätze über dieselben beweisen wollen.

Ein Kettenbruch $(a, b, c, d \ldots)$, dessen sämmtliche Elemente $a, b, c, d \ldots$ positive ganze Zahlen sind (mit Ausnahme des ersten a, für welches auch der Werth Null gestattet ist), soll im Folgenden ein *regelmässiger* heissen; der Werth eines solchen endlichen oder unendlichen Kettenbruchs ist bekanntlich stets positiv, und umgekehrt ist bekannt, dass jeder positive Werth stets und nur auf eine einzige Weise in einen regelmässigen Kettenbruch verwandelt werden kann. Sehr wichtig für unsere Zwecke ist nun die Umwandlung eines *unregelmässigen* unendlichen Kettenbruchs

$$(\alpha, \beta, \gamma \ldots \mu, \nu, p, q, r \ldots u, v \ldots),$$

dessen Elemente ganze Zahlen und zwar von einem bestimmten p ab sämmtlich *positive* ganze Zahlen sind, in einen regelmässigen. Es wird sich zeigen, *dass bei dieser Umwandlung alle Elemente $u, v \ldots$ von einem bestimmten, in endlicher Entfernung liegenden, Element u ab unverändert bleiben, und dass die Differenz zwischen der Anzahl der geänderten und der Anzahl der sie ersetzenden Elemente eine gerade oder ungerade Zahl ist, je nachdem der Werth des ganzen Kettenbruchs positiv oder negativ ist.*

Um dies zu beweisen, nehmen wir an, es sei ν das letzte nicht positive Element des Kettenbruchs, und wir setzen ausserdem zunächst voraus, dass ν nicht das erste Element des ganzen Kettenbruchs ist. Wir suchen nun die Unregelmässigkeit des Kettenbruchs von dieser äussersten Stelle ν zu entfernen und um mindestens eine Stelle weiter nach links zu drängen.

Hierzu brauchen wir offenbar nur den unendlichen Kettenbruch $(\mu, \nu, p, q \ldots)$ zu betrachten, den wir auch in endlicher Form (μ, ν, p') oder (μ, ν, p, q') oder (μ, ν, p, q, r') u. s. w. schreiben können, wenn wir die unendlichen regelmässigen Kettenbrüche

$(p, q, r, s \ldots)$, $(q, r, s \ldots)$, $(r, s \ldots)$ u. s. w.

zur Abkürzung mit p', q', r' u. s. w. bezeichnen. Wir haben nun folgende Fälle zu unterscheiden.

1. Ist $\nu = 0$, so ist

$$(\mu, 0, p') = \mu + p' = \mu + p + \frac{1}{q'}$$

oder also

$$(\mu, 0, p, q') = (\mu + p, q');$$

es ist also die Unregelmässigkeit von der Stelle $\nu = 0$ um mindestens eine Stelle nach links gedrängt, und zugleich ist an Stelle der abgeänderten drei Elemente $\mu, 0, p$ das einzige Element $\mu + p$ getreten.

2. Ist ν negativ $= -n$, und $n > 1$, so erhält man mit Benutzung der Identität

$$(g, -h) = (g - 1, 1, h - 1)$$

folgende successive Umformung:

$$(\mu, -n, p') = \left(\mu, -n + \frac{1}{p'}\right) = \left(\mu - 1, 1, n - 1 - \frac{1}{p'}\right)$$
$$= (\mu - 1, 1, n - 1, -p')$$

und hieraus durch nochmalige Anwendung derselben Identität

$$(\mu, -n, p, q') = (\mu - 1, 1, n - 2, 1, p' - 1)$$
$$= (\mu - 1, 1, n - 2, 1, p - 1, q').$$

An Stelle der drei abgeänderten Elemente $\mu, -n, p$ sind die fünf Elemente $\mu - 1, 1, n - 2, 1, p - 1$ getreten, und von diesen ist höchstens das erste negativ. Sollte ferner $n - 2$ oder $p - 1$, oder sollten beide Zahlen $= 0$ sein, so wird man durch einmalige oder zweimalige Anwendung der unter 1. aufgestellten Regel alle Elemente, mit Ausnahme des ersten, in positive verwandeln; auch dann wird der Unterschied zwischen der Anzahl der abgeänderten und der Anzahl der dieselben ersetzenden Elemente eine gerade Zahl bleiben, und die Unregelmässigkeit ist mindestens um eine Stelle nach links verschoben.

3. Ist $\nu = -$ [illegible] so ist die eben angegebene Regel nicht anwendbar; wenn gleichzeitig $p > 1$, so findet man

$$(\mu, -1, p, q') = (\mu - 2, 1, p - 2, q');$$

sollte $p = 2$ sein, so hat man wieder nach der unter 1. aufgestellten Regel zu verfahren. Ist aber $p = 1$, so hilft diese Formel Nichts; dann ist aber

$$(\mu, -1, 1, q') = \mu - 1 - q'$$

und folglich

$$(\mu, -1, 1, q, r, s') = (\mu - 2 - q, 1, r - 1, s');$$

und sollte $r = 1$ sein, so würde man wie in 1. verfahren.

Auf diese Weise ist in allen Fällen ohne Ausnahme die Unregelmässigkeit des Kettenbruchs von der Stelle ν um mindestens eine Stelle weiter nach links gedrängt, und zugleich ist der Unterschied zwischen der Anzahl der abgeänderten und der Anzahl der sie ersetzenden Elemente jedes Mal eine *gerade* Zahl. Durch successive Anwendung desselben Verfahrens wird man daher den ursprünglich gegebenen Kettenbruch

$$(\alpha, \beta, \gamma \ldots \mu, \nu, p, q, r \ldots t, u, v \ldots)$$

in einen andern

$$(\alpha', b, c \ldots k, l, u, v \ldots)$$

umformen können, in welchem alle auf das erste folgenden Elemente $b, c \ldots$ positive ganze Zahlen sind, welche von einer in endlicher Entfernung liegenden Stelle u an mit den Elementen des gegebenen Kettenbruchs übereinstimmen; und zwar wird der Unterschied zwischen der Anzahl der abgeänderten Elemente

$$\alpha, \beta, \gamma \ldots \mu, \nu, p, q, r \ldots t$$

und der Anzahl der sie ersetzenden Elemente

$$\alpha', b, c \ldots k, l$$

eine gerade Zahl sein, weil dasselbe bei jedem einzelnen Act der gesammten Umformung Statt findet.

Ist nun α' positiv oder $= 0$, so ist die Umformung vollendet, und der Werth des Kettenbruchs ist positiv; ist dagegen α' negativ $= -a$, so ist der Kettenbruch negativ, und zwar

$$= -(a - 1, 1, b - 1, c \ldots)$$

oder, wenn $b = 1$ sein sollte,

$$= -(a - 1, c + 1, d \ldots).$$

Bei diesem letzten Act ist die Anzahl der abgeänderten Elemente um eine Einheit kleiner oder grösser als die Anzahl der sie ersetzenden Elemente; und hiermit ist der letzte Punct unserer obigen Behauptung nachgewiesen.

§. 81.

Wir bedürfen zweitens für die Untersuchung der Aequivalenz zweier Formen noch des folgenden Satzes:

Sind $\alpha, \beta, \gamma, \delta$ *vier ganze Zahlen, welche der Bedingung*

$$\alpha\delta - \beta\gamma = 1$$

genügen, und deren erste α *von Null verschieden ist; findet ferner zwischen zwei Grössen* ω *und* Ω *die Relation*

$$\omega = \frac{\gamma + \delta\Omega}{\alpha + \beta\Omega}$$

Statt; so kann man stets

$$\omega = (\gamma', m, n \ldots r, \beta', \Omega)$$

setzen, wo die Anzahl der positiven ganzen Zahlen $m, n \ldots r$ *eine gerade ist,* γ' *und* β' *aber auch Null oder negative ganze Zahlen sein können.*

Um diesen Satz zu beweisen, können wir, ohne die Allgemeinheit zu beeinträchtigen, annehmen, dass die von Null verschiedene ganze Zahl α *positiv* ist; denn sollte α negativ sein, so verwandele man die Zeichen aller vier Zahlen $\alpha, \beta, \gamma, \delta$ in die entgegengesetzten, so bleibt die zwischen ihnen, und ebenso die zwischen ω und Ω bestehende Relation ungeändert. Ist nun zunächst $\alpha = 1$, also $\delta = \beta\gamma + 1$, so ist unmittelbar

$$\omega = \frac{\gamma + (\beta\gamma + 1)\Omega}{1 + \beta\Omega} = \gamma + \frac{\Omega}{1 + \beta\Omega} = (\gamma, \beta, \Omega),$$

also ist in diesem Fall unser Satz richtig. Ist aber $\alpha > 1$, so entwickle man den Bruch $\gamma : \alpha$ in den Kettenbruch $(\gamma', m, n \ldots r)$, dessen Elemente sämmtlich positive ganze Zahlen sind, mit Ausnahme des ersten γ', welches positiv, Null oder negativ sein wird, je nachdem γ positiv und grösser als α, oder positiv und kleiner als α, oder endlich negativ ist.

Wir können ferner voraussetzen, dass die Anzahl der positiven Elemente $m, n \ldots r$ gerade ist; denn da bei der gewöhnlichen Methode, einen Bruch $\gamma : \alpha$ in einen Kettenbruch zu verwandeln, das letzte Element r mindestens $= 2$ ist, so könnte man, wenn die Anzahl der Elemente $m, n \ldots r$ ungerade sein sollte, das letzte Element r in den Kettenbruch $r - 1 + \frac{1}{1}$ verwandeln und also statt

des obigen Kettenbruchs den folgenden $(\gamma', m, n \ldots r-1, 1)$ nehmen, in welchem die Anzahl der positiven Elemente $m, n \ldots r-1, 1$ nun gerade ist. Bildet man nun nach der früher (§. 23) angegebenen Methode die sogenannten Näherungsbrüche,

$$\frac{[\gamma']}{1}, \frac{[\gamma', m]}{[m]}, \frac{[\gamma', m, n]}{[m, n]} \ldots \frac{[\gamma', m, n \ldots q, r]}{[m, n \ldots q, r]},$$

so erkennt man leicht, dass ihre Nenner sämmtlich positiv sind. Damals haben wir auch bewiesen, dass diese Brüche irreductibel sind, und da der letzte der obigen Brüche dem in Folge der Relation $\alpha\delta - \beta\gamma = 1$ ebenfalls irreductibeln Bruche $\gamma : \alpha$ gleich, und α positiv ist, so muss

$$\alpha = [m, n \ldots q, r], \quad \gamma = [\gamma', m, n \ldots q, r]$$

sein, weil ein Bruch nur auf eine einzige Weise in die irreductibele Form mit positivem Nenner gebracht werden kann. Da ferner die Anzahl der Elemente $\gamma', m, n \ldots q, r$ ungerade ist, so folgt aus der damals aufgestellten Formel [§. 23, (9)], dass

$$[m, n \ldots q]\,[\gamma', m, n \ldots q, r] - [m, n \ldots q, r]\,[\gamma', m, n \ldots q] = -1$$

oder also

$$\alpha\,[\gamma', m, n \ldots q] - [m, n \ldots q]\,\gamma = 1$$

ist; vergleicht man dies mit der Relation $\alpha\delta - \beta\gamma = 1$, so ergiebt sich (ähnlich wie im §. 60), dass man

$$\delta = [\gamma', m, n \ldots q] + \gamma\beta'$$
$$\beta = [m, n \ldots q] + \alpha\beta'$$

d. h.

$$\delta = [\gamma', m, n \ldots q, r, \beta']$$
$$\beta = [m, n \ldots q, r, \beta']$$

also

$$\frac{\delta}{\beta} = (\gamma', m, n \ldots q, r, \beta')$$

setzen kann, wo β' eine ganze Zahl bedeutet*). Nach demselben Bildungsgesetz ist nun

$$\gamma + \delta\Omega = [\gamma', m, n \ldots r, \beta', \Omega]$$
$$\alpha + \beta\Omega = [m, n \ldots r, \beta', \Omega]$$

und folglich, wie zu beweisen war,

$$\omega = (\gamma', m, n \ldots r, \beta', \Omega).$$

*) Da die Brüche $\gamma : \alpha$, $\beta : \alpha$ resp. den Kettenbrüchen $(\gamma', m \ldots r)$, $(\beta', r \ldots m)$ gleich sind, so sind γ', β' die grössten in denselben enthaltenen ganzen Zahlen (im Sinne des §. 43).

§. 82.

Nachdem auch dieser zweite Punct aus der Theorie der Kettenbrüche behandelt ist, schreiten wir zur definitiven Entscheidung der Frage, ob zwei verschiedene Perioden von reducirten Formen einer positiven Determinante äquivalente Formen enthalten können. Es seien daher (a, b, c) und (A, B, C) zwei reducirte (eigentlich) äquivalente Formen; da alle Formen einer und derselben Periode einander stets äquivalent sind, so können wir annehmen, dass die ersten Coefficienten a, A, und folglich auch die ersten Wurzeln dieser beiden Formen *positiv* sind, weil im entgegengesetzten Fall die unmittelbar benachbarten Formen diese Eigenschaft besitzen würden. Bezeichnen wir (a, b, c) mit φ_0 und (A, B, C) mit Φ_0, und bilden wir für jede dieser beiden Formen (nach §. 78) die sie enthaltende Periode, so erhalten wir dadurch für die ersten Wurzeln ω_0, Ω_0 dieser beiden Formen die regelmässigen Kettenbrüche

$$\omega_0 = (k_0, k_1, k_2 \ldots),$$
$$\Omega_0 = (K_0, K_1, K_2 \ldots).$$

Ist nun $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ eine Substitution, durch welche φ_0 in Φ_0 übergeht, so besteht zwischen den ersten Wurzeln ω_0, Ω_0 die Relation

$$\omega_0 = \frac{\gamma + \delta\Omega_0}{\alpha + \beta\Omega_0},$$

und ausserdem ist

$$\alpha\delta - \beta\gamma = 1.$$

Da ferner α nicht $= 0$ sein kann, weil sonst $A = c$, also A negativ wäre, so kann man nach dem so eben bewiesenen Satze

$$\omega_0 = (\gamma', m, n \ldots r, \beta', \Omega_0)$$

und also auch

$$\omega_0 = (\gamma', m, n \ldots r, \beta', K_0, K_1, K_2 \ldots)$$

setzen, und in diesem unendlichen Kettenbruch, welcher wenigstens von der Stelle K_0 ab keine Unregelmässigkeit enthält, ist die Anzahl der Elemente $\gamma', m, n \ldots r, \beta'$ eine gerade $= 2g$. Ist β' positiv, so ist, da $\omega_0 > 1$ ist, auch γ' positiv, also der Bruch regelmässig. Ist aber $\beta' = 0$ oder negativ, so forme man den Kettenbruch nach den obigen Regeln (§. 80) in einen regelmässigen um; nimmt man μ hinreichend gross, so werden die Elemente $K_\mu, K_{\mu+1} \ldots$ bei

dieser Umformung ungeändert bleiben, und die Anzahl ν der Elemente, welche an die Stelle der vorhergehenden $(2g + \mu)$ Elemente

$$\gamma', m, n \ldots r, \beta', K_0 \ldots K_{\mu-1}$$

treten, wird $\equiv \mu \pmod 2$ sein (nach §. 80), da der Werth des ganzen Kettenbruchs *positiv* ist. Da nun ω_0 nur auf eine einzige Weise als ein regelmässiger Kettenbruch dargestellt werden kann, so müssen die Zahlen

$$K_\mu, K_{\mu+1}, K_{\mu+2} \ldots\ldots$$

resp. mit den Zahlen

$$k_\nu, k_{\nu+1}, k_{\nu+2}, \ldots\ldots$$

identisch sein. Ist daher $\mu + h$ ein Multiplum von der Anzahl der Formen, welche die Periode der Form Φ_0 bilden, und also eine gerade Zahl, so ist auch $\nu + h$ eine gerade Zahl $= 2m$, und die Zahlen

$$K_{\mu+h}, K_{\mu+h+1}, K_{\mu+h+2} \ldots$$

stimmen mit den Zahlen

$$K_0, K_1, K_2 \ldots,$$

und diese folglich mit den Zahlen

$$k_{2m}, k_{2m+1}, k_{2m+2} \ldots$$

überein. Hieraus folgt unmittelbar

$$\Omega_0 = (k_{2m}, k_{2m+1} \ldots) = \omega_{2m};$$

und da durch ihre erste Wurzel auch stets die Form vollständig charakterisirt ist (§. 72), so schliessen wir hieraus, dass die Form Φ_0 mit der Form φ_{2m} identisch sein muss, dass also Φ_0 sich in der aus φ_0 entwickelten Periode befinden muss. Wir haben so folgenden *Hauptsatz**) gewonnen:

Zwei äquivalente reducirte Formen von positiver Determinante gehören einer und derselben Periode an; zwei reducirte Formen können nicht äquivalent sein, wenn sie verschiedenen Perioden angehören.

Mit Hülfe dieses Satzes ergiebt sich nun eine Methode, um zu prüfen, ob zwei gegebene Formen von gleicher positiver Determinante äquivalent sind oder nicht. Man suche (nach §. 76) zu jeder der beiden Formen eine ihr äquivalente reducirte Form; je nachdem die so gefundenen reducirten Formen derselben oder verschiedenen Perioden angehören, sind die gegebenen Formen

*) *Gauss: D. A.* art. 193.

äquivalent, oder nicht äquivalent. Im erstern Fall ergiebt sich offenbar zugleich eine Substitution, durch welche die eine Form in die andere übergeht (vergl. §. 66).

Beispiel: Die beiden gegebenen Formen seien (713, 60, 5) und (62, 95, 145), welche dieselbe Determinante $D = 35$ haben. Die erste geht durch die Substitution $\left(\begin{smallmatrix} 0, & +1 \\ -1, & -13 \end{smallmatrix}\right)$ in die reducirte Form (5, 5, — 2), die zweite durch die Substitution $\left(\begin{smallmatrix} -3, & +10 \\ +2, & -7 \end{smallmatrix}\right)$ in die reducirte Form (— 2, 5, 5) über (§. 76). Diese beiden reducirten Formen gehören aber derselben zweigliedrigen Periode (5, 5, — 2), (— 2, 5, 5) an, und zwar geht die erstere durch die Substitution $\left(\begin{smallmatrix} 0, & 1 \\ -1, & 5 \end{smallmatrix}\right)$ in die letztere über. Mithin sind die beiden gegebenen Formen (713, 60, 5) und (62, 95, 145) äquivalent, und da $\left(\begin{smallmatrix} -7, & -10 \\ -2, & -3 \end{smallmatrix}\right)$ die inverse Substitution von $\left(\begin{smallmatrix} -3, & +10 \\ +2, & -7 \end{smallmatrix}\right)$ ist, so geht die erstere dieser beiden Formen durch die Substitution $\left(\begin{smallmatrix} 0, & +1 \\ -1, & -13 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0, & 1 \\ -1, & 5 \end{smallmatrix}\right)\left(\begin{smallmatrix} -7, & -10 \\ -2, & -3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -3, & -5 \\ +41, & +68 \end{smallmatrix}\right)$ in die letztere über.

§. 83.

Durch unsere letzten Untersuchungen ist das erste der beiden in §. 59 aufgestellten Hauptprobleme auch für Formen von *positiver* Determinante gelöst; das zweite haben wir in §. 62 auf die Auflösung der unbestimmten Gleichung

$$t^2 - Du^2 = \sigma^2$$

zurückgeführt, und es bleibt daher, um in der Theorie der Formen von positiver Determinante zu demselben Abschluss zu kommen, wie früher für negative Determinanten, nur noch übrig, diese Gleichung für jeden positiven (nicht quadratischen) Werth der Determinante D vollständig aufzulösen. *Fermat* hat diese Gleichung den Mathematikern zuerst vorgelegt, worauf ihre Lösung von dem Engländer *Pell* angegeben wurde; allein obwohl seine Methode die Lösung in jedem Fall wirklich giebt, so lag doch in ihr nicht der Nachweis, dass sie immer zum Ziele führen muss, und dass die Gleichung ausser der evidenten Auflösung $t = \pm\sigma$, $u = 0$ noch andere Auflösungen besitzt. Diese Lücke ist erst von *Lagrange**) ausgefüllt, und hierin besteht wohl eine der bedeutend-

*) *Solution d'un Problème d'Arithmétique*, Miscellanea Taurinensia, Tom. IV. (Œuvres de Lagrange, publ. par Serret, T. I. 1867. p. 669.) —

sten Leistungen des grossen Mathematikers auf dem Gebiete der Zahlentheorie, da die von ihm zu diesem Zweck eingeführten Principien in hohem Grade der Verallgemeinerung fähig und deshalb auch auf ähnliche höhere Probleme anwendbar sind *).

Wir schlagen hier einen ganz andern Weg ein, der sich den zunächst vorangehenden Untersuchungen unmittelbar anschliesst. Der Zusammenhang zwischen der obigen unbestimmten Gleichung und dem zweiten Hauptproblem in der Theorie der Aequivalenz war folgender. Ist (a, b, c) eine Form von der Determinante D und vom Theiler σ, und ist $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ irgend eine eigentliche Substitution, durch welche (a, b, c) in sich selbst übergeht so ist stets

$$\alpha = \frac{t - bu}{\sigma}, \quad \beta = -\frac{cu}{\sigma}, \quad \gamma = \frac{au}{\sigma}, \quad \delta = \frac{t + bu}{\sigma},$$

wo t, u zwei der Gleichung

$$t^2 - Du^2 = \sigma^2$$

genügende ganze Zahlen bedeuten; und umgekehrt, jeder Auflösung t, u der unbestimmten Gleichung entspricht durch die vorstehenden Formeln eine Substitution $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$, durch welche die Form (a, b, c) in sich selbst übergeht. Wir haben nun durch die letzten Untersuchungen, wie sich gleich zeigen wird, ein Mittel gewonnen, alle Transformationen $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ einer reducirten Form von positiver Determinante D in sich selbst direct zu finden, und folglich können wir hieraus auch alle Auflösungen t, u der unbestimmten Gleichung ableiten. Wir schicken der Ausführung dieser Untersuchung noch eine Bemerkung über die Perioden der reducirten Formen voraus.

Wir wissen, dass die Reihe der positiven Zahlen k, welche die Elemente des Kettenbruchs bilden, in den die erste Wurzel ω_0

Sur la solution des problèmes indéterminés du second degré, Mém. de l'Ac. de Berlin T. XXIII. (Œuvres de L. T. II. 1868. p. 375.) — *Additions aux Elémens d'Algèbre par L. Euler* §§. II, VIII. — Das Verdienst, die tiefe Bedeutung der Pell'schen Gleichung für die allgemeine Auflösung der unbestimmten Gleichungen zweiten Grades zuerst dargethan zu haben, gebührt *Euler*; man vergl.: *De solutione problematum Diophanteorum per numeros integros*, Comm. Petrop. VI. p. 175. *De resolutione formularum quadraticarum indeterminatarum per numeros integros*, Nov. Comm. Petrop. IX. p. 3. *De usu novi algorithmi in problemate Pelliano solvendo*, Nov. Comm. Petrop. XI. p. 28. *Nova subsidia pro resolutione formulae* $axx + 1 = yy$, Opusc. anal. I. p. 310. — Man vergleiche ferner *Gauss: D. A.* art. 197 — 202.

*) Siehe Supplement VIII.

einer reducirten Form φ_0 entwickelt wird, eine gerade Anzahl von Gliedern

$$k_0,\ k_1 \ldots k_{2n-1}$$

enthält, nach welchen dieselben Glieder periodisch wiederkehren; und zwar ist diese Anzahl $2n$ die der reducirten Formen, welche mit φ_0 in einer Periode enthalten sind. Wir haben aber oben (§. 79) an einzelnen Beispielen gesehen, dass die Zahlen k aus kleineren Perioden bestehen können; wir fanden z. B. aus der zehngliedrigen Formenperiode der Determinante $D = 13$ folgende Zahlen:

$$\delta_0 = +1,\ \delta_1 = -6,\ \delta_2 = +1,\ \delta_3 = -1,\ \delta_4 = +1;$$
$$\delta_5 = -1,\ \delta_6 = +6,\ \delta_7 = -1,\ \delta_8 = +1,\ \delta_9 = -1;$$

und also

$$k_0 = 1,\ k_1 = 6,\ k_2 = 1,\ k_3 = 1,\ k_4 = 1;$$

und hierauf wiederholt sich schon dieselbe Reihe

$$k_5 = 1,\ k_6 = 6,\ k_7 = 1,\ k_8 = 1,\ k_9 = 1.$$

Es ist nun wichtig zu untersuchen, wann dies eintreten kann. Es sei daher $2n$ die Gliederanzahl der Formenperiode und m die Gliederanzahl irgend einer Periode in der Reihe der Zahlen k. Dann ist, indem wir die früheren Bezeichnungen für die Formen und ihre ersten Wurzeln beibehalten, wenn m gerade ist,

$$\omega_m = (k_m, k_{m+1} \ldots) = (k_0, k_1 \ldots)$$

und folglich $\omega_m = \omega_0$, und also auch φ_m identisch mit φ_0 und daher nothwendig m ein Multiplum von $2n$; es existirt also jedenfalls keine kleinere Periode von gerader Gliederanzahl als die der ganzen Formenperiode entsprechende. Ist dagegen m ungerade, so ist $2m$ ebenfalls die Gliederanzahl einer Periode in der Reihe der Zahlen k, und folglich ist nach dem eben Bewiesenen $2m$ ein Multiplum von $2n$, also m mindestens $= n$; der Fall, dass die Periode der Zahlen k kürzer ist als die aus $2n$ Gliedern bestehende Periode der Formen, kann also nur dann eintreten, wenn n eine *ungerade* Zahl ist, indem dann, wie wir ja auch an dem obigen Beispiel sehen, die Periode der Zahlen k aus n Gliedern bestehen kann; es ist dann $\omega_n = -\omega_0$, und also $c_n = -c_0$, $b_n = b_0$, $a_n = -a_0$. Doch muss man sich hüten zu glauben, dass diese Erscheinung jedesmal wirklich eintreten *muss*, wenn n ungerade ist; denn wir haben nur gezeigt, dass sie in diesem Fall allein eintreten *kann*. Für $D = 19$ z. B. sind die beiden Formenperioden

sechsgliedrig (§. 79), also ist $n = 3$; aber die Perioden der Zahlen k sind nicht dreigliedrig, sondern sechsgliedrig *).

*) Die Erscheinung, dass die Kettenbruch-Entwicklung nur halb so lang ist, als die Periode der Form, wird, wie oben gezeigt ist, nur dann eintreten, wenn die Formen (a, b, c) und $(-a, b, -c)$ äquivalent sind, und man erkennt leicht (aus §. 82), dass sie dann auch stets eintreten muss. Führt man nun die Untersuchung über die Aequivalenz dieser beiden Formen genau ebenso durch wie in §. 62, so erhält man das Resultat: Die Coefficienten einer jeden Substitution $\left(\begin{smallmatrix}\lambda, & \mu\\ \nu, & \varrho\end{smallmatrix}\right)$, durch welche eine Form (a, b, c) von der Determinante D und vom Theiler σ in die Form $(-a, b, -c)$ übergeht, sind in den Formeln

$$\lambda = \frac{t - bu}{\sigma}, \quad \mu = \frac{cu}{\sigma}, \quad \nu = \frac{au}{\sigma}, \quad \varrho = -\frac{t + bu}{\sigma} \tag{I}$$

enthalten, wo t, u zwei ganze Zahlen bedeuten, welche der unbestimmten Gleichung

$$t^2 - Du^2 = -\sigma^2 \tag{II}$$

Genüge leisten; und umgekehrt, giebt es zwei solche ganze Zahlen t, u, so liefern jene Formeln (I) stets eine Substitution von der angegebenen Beschaffenheit. Die erwähnte Erscheinung wird daher stets und nur dann auftreten, wenn die Gleichung (II) *möglich* ist; tritt sie daher in der Periode irgend einer Form auf, so wird sie auch in allen Perioden derjenigen Formen auftreten, welche zu derselben *Ordnung* gehören (§. 61); ist ferner die Gleichung $t^2 - Du^2 = -1$ möglich, so wird sie bei allen Perioden dieser Determinante D auftreten. Dies ist z. B. stets der Fall, wenn $D = p^{2s+1}$ und p eine positive Primzahl $\equiv 1$ (mod. 4) ist; denn sind T, U die *kleinsten* positiven Zahlen, welche der Gleichung $T^2 - DU^2 = +1$ genügen (§. 84), so ist T ungerade, U gerade, und

$$\frac{T-1}{2} \cdot \frac{T+1}{2} = D\left(\frac{U}{2}\right)^2;$$

da die beiden Factoren linker Hand relative Primzahlen sind, so ist einer und nur einer von ihnen durch D theilbar; wäre nun $T - 1 = 2Df^2$, $T + 1 = 2g^2$, $U = 2fg$, so wäre $g^2 - Df^2 = +1$, und $f < U$, gegen die Voraussetzung; es muss daher $T - 1 = 2f^2$, $T + 1 = 2Dg^2$, $U = 2fg$, und also $f^2 - Dg^2 = -1$ sein, w. z. b. w. Zugleich leuchtet ein, dass $T + U\sqrt{D} = (f + g\sqrt{D})^2$ ist, was nur ein specieller Fall eines allgemeineren Satzes ist.

Besonders interessante Resultate erhält man, wenn man, falls die Gleichung (II) möglich ist, die Perioden von *ambigen* Formen betrachtet (§. 78). Um uns auf den einfachsten Fall zu beschränken, nehmen wir an, die Gleichung $t^2 - Du^2 = -1$ sei möglich; ist nun λ die grösste in $\sqrt{D}$ enthaltene ganze Zahl, also $\varphi_0 = (1, \lambda, \lambda^2 - D)$ eine reducirte und zugleich ambige Form, deren Periode $2n$ Glieder enthält (§. 79), so muss n ungerade $= 2m + 1$, und $\varphi_n = (-1, \lambda, D - \lambda^2)$, also $\varphi_{2m} = (D - \lambda^2, \lambda, -1)$ sein, und hieraus folgt leicht, dass $\varphi_m = (a, b, -a)$, $\varphi_{3m+1} = (-a, b, a)$, also $D = a^2 + b^2$ ist, wo a ungerade und relative Primzahl zu b ist, weil φ_0 eine ursprüngliche Form der ersten Art ist. Da wir vorhin gesehen haben, dass dieser

Um nun die unbestimmte Gleichung $t^2 - Du^2 = \sigma^2$ zu lösen, in welcher D eine beliebige nicht quadratische positive Zahl, und entweder $D \equiv 0 \pmod{\sigma^2}$, oder $4D \equiv \sigma^2 \pmod{4\sigma^2}$ ist, nehmen wir eine beliebige *reducirte* Form (a, b, c) von der Determinante D und vom Theiler σ. (Dass eine solche stets existirt, leuchtet aus §§. 61, 76 unmittelbar ein.) Wir nehmen ferner, was stets gestattet ist, *a positiv*, und folglich *c negativ* an; dann ist die erste Wurzel ω dieser Form positiv, und folglich

$$\omega = (k_0,\ k_1 \ldots k_{2hn-2},\ k_{2hn-1},\ \omega),$$

wo $2n$ die Gliederanzahl der Formenperiode, und h eine beliebige positive ganze Zahl ist. Setzt man nun

$$\frac{\gamma}{\alpha} = (k_0,\ k_1 \ldots k_{2hn-2});\quad \frac{\delta}{\beta} = (k_0,\ k_1 \ldots k_{2hn-1})$$

d. h. (nach §. 23)

$$\alpha = [k_1 \ldots k_{2hn-2}],\quad \beta = [k_1 \ldots k_{2hn-2},\ k_{2hn-1}],$$
$$\gamma = [k_0,\ k_1 \ldots k_{2hn-2}],\quad \delta = [k_0,\ k_1 \ldots k_{2hn-2},\ k_{2hn-1}],$$

so ist nach den schon öfter benutzten Sätzen $\alpha\delta - \beta\gamma = 1$ und

$$\alpha + \beta\omega = [k_1 \ldots k_{2hn-2},\ k_{2hn-1},\ \omega]$$
$$\gamma + \delta\omega = [k_0,\ k_1 \ldots k_{2hn-2},\ k_{2hn-1},\ \omega]$$

und folglich

$$\frac{\gamma + \delta\omega}{\alpha + \beta\omega} = (k_0,\ k_1 \ldots k_{2hn-2},\ k_{2hn-1},\ \omega) = \omega,$$

woraus unmittelbar folgt (§. 73), dass die Form (a, b, c) durch die Substitution $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ in sich selbst übergeht.

Setzt man daher für h der Reihe nach alle positiven ganzen Zahlen 1, 2, 3 ..., so erhält man durch die Zähler und Nenner der Näherungsbrüche vom Range $2hn - 1$ und $2hn$ jedesmal eine entsprechende Transformation $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ der Form (a, b, c) in sich selbst (wenn $n = 1$ ist und $h = 1$ genommen wird, hat man $\alpha = 1$, $\beta = k_1$, $\gamma = k_0$, $\delta = k_0 k_1 + 1$ zu setzen); die vier Coefficienten α, β, γ, δ sind immer *positiv*, und da ausserdem mit wachsendem h auch nothwendig die Zähler und Nenner der Näherungsbrüche

---

Fall stets eintritt, wenn D eine Primzahl $\equiv 1 \pmod 4$ ist, so liegt hierin ein neuer Beweis des Fermat'schen Satzes (§. 68), und zugleich eine directe Methode, die Zerlegung einer solchen Primzahl D in zwei Quadrate aus der Entwicklung von $\sqrt{D}$ in einen Kettenbruch abzuleiten (vergl. *Gauss*: *D. A.* art. 265; *Legendre: Théorie des Nombres* 3me éd. Tom. I. §. VII. (52)). Dies Resultat steht in der engsten Beziehung zu der biquadratischen Hülfsgleichung, welche bei der Theilung des Kreises in D gleiche Theile auftritt.

beständig wachsen, so entsprechen zwei verschiedenen Werthen von h auch zwei verschiedene Substitutionen $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$.

Umgekehrt wollen wir nun zeigen, dass man auf diese Weise *alle* die Transformationen $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ der Form (a, b, c) in sich selbst erhält, in denen die vier Coefficienten $\alpha, \beta, \gamma, \delta$ sämmtlich *positiv* sind. Denn es sei $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ eine solche Substitution, so ist (§. 73)

$$\alpha\delta - \beta\gamma = 1 \text{ und } \omega = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

also auch

$$\beta\omega^2 + (\alpha - \delta)\omega - \gamma = 0,$$

und zwar müssen dieser quadratischen Gleichung beide Wurzeln der Gleichung genügen. Da nun die eine zwischen 1 und $+\infty$, die andere zwischen -1 und 0 liegt, so muss die linke Seite dieser Gleichung für $\omega = 1$ negativ, für $\omega = -1$ positiv ausfallen; hieraus folgt, dass

$$\gamma + \delta > \alpha + \beta, \quad \beta + \delta > \alpha + \gamma$$

ist, wo die Ungleichheitszeichen die Gleichheit ausschliessen. Da wir beweisen wollen, dass $\gamma : \alpha$ und $\delta : \beta$ zwei auf einander folgende Näherungsbrüche eines regelmässigen Kettenbruchs $(k_0, k_1 \ldots)$ sind, so haben wir vor allem zu zeigen, dass $\gamma \geqq \alpha$ und $\delta > \gamma$ ist; dies ergiebt sich in der That aus den vorstehenden Ungleichungen. Wäre nämlich $\delta \leqq \gamma$, so würde aus der zweiten Ungleichung folgen, dass $\alpha < \beta$ und also auch $\alpha\delta < \beta\gamma$ sein müsste, während doch $\alpha\delta = \beta\gamma + 1$ ist; also ist gewiss $\delta > \gamma$. Wäre ferner $\gamma < \alpha$, also $\alpha = \gamma + \varrho$, wo ϱ eine positive ganze Zahl bedeutet, so würde aus der ersten Ungleichheit folgen, dass $\delta > \beta + \varrho$, also auch

$$\alpha\delta - \beta\gamma > (\beta + \gamma)\varrho + \varrho^2$$

wäre; dies ist aber wieder unmöglich, da die linke Seite $= 1$, die rechte aber mindestens $= 3$ ist, weil β, γ, ϱ positive ganze Zahlen bedeuten; also ist in der That $\gamma \geqq \alpha$.

Hieraus folgt nun weiter, dass man

$$\frac{\gamma}{\alpha} = (\gamma', m \ldots q, r)$$

setzen kann, wo die Elemente $\gamma', m \ldots q, r$ sämmtlich positiv sind, und zwar kann man es so einrichten, dass ihre Anzahl ungerade ist, weil man eventuell wieder r in $r - 1 + \frac{1}{1}$ auflösen kann. Nehmen wir ferner zunächst an, dass $\alpha > 1$ ist, so ist auch $\gamma > \alpha$ und γ nicht theilbar durch α, und folglich enthält der Kettenbruch

mindestens drei Elemente. Bilden wir daher den unmittelbar vorausgehenden Näherungsbruch

$$\frac{\varphi}{f} = (\gamma', m \ldots q),$$

so folgt aus $\alpha\varphi - f\gamma = 1$ und $\alpha\delta - \beta\gamma = 1$, dass man wieder $\beta = f + \alpha\beta'$, $\delta = \varphi + \gamma\beta'$ setzen kann, und hierin wird β' eine *positive* ganze Zahl sein. Wäre nämlich $\beta' = 0$, so wäre $\delta = \varphi$, und da φ gewiss $< \gamma$ ist, so wäre $\delta < \gamma$, während doch $\delta > \gamma$ ist; wäre ferner β' negativ, so wäre auch δ negativ, gegen unsere Voraussetzung, dass α, β, γ, δ positive ganze Zahlen sind. Es ist daher

$$\frac{\delta}{\beta'} = (\gamma', m \ldots q, r, \beta')$$

und folglich, ähnlich wie früher,

$$\omega = \frac{\gamma + \delta\omega}{\alpha + \beta\omega} = (\gamma', m \ldots q, r, \beta', \omega),$$

wo nun die Anzahl der positiven Elemente $\gamma', m \ldots q, r, \beta'$ gerade ist*). In dem bisher ausgeschlossenen Fall $\alpha = 1$ erhält man ein ganz ähnliches Resultat, denn dann ist

$$\omega = \frac{\gamma + (\beta\gamma + 1)\omega}{1 + \beta\omega} = (\gamma, \beta, \omega).$$

Wir erhalten daher für ω stets einen regelmässigen periodischen Kettenbruch

$$\omega = (\gamma', m \ldots q, r, \beta'; \gamma', m \ldots)$$

in welchem die Anzahl der Glieder $\gamma', m \ldots q, r, \beta'$ eine gerade ist. Da nun ein Werth ω nur auf eine einzige Weise in einen regelmässigen Kettenbruch entwickelt werden kann, so müssen die Zahlen $\gamma', m \ldots$ der Reihe nach mit den Zahlen $k_0, k_1 \ldots$ übereinstimmen; und da wir uns oben überzeugt haben, dass jede Periode der Zahlen k, deren Gliederzahl gerade ist, entweder mit der Reihe der den sämmtlichen $2n$ Formen entsprechenden Zahlen k identisch ist oder aus einer mehrmaligen Wiederholung dieser kleinsten Periode von gerader Gliederanzahl besteht, so ist also $r = k_{2hn-2}$, $\beta' = k_{2hn-1}$, wo h irgend eine positive ganze Zahl bezeichnet, und folglich

*) Dasselbe ergiebt sich auch unmittelbar daraus, dass die grössten in den Brüchen $\gamma : \alpha$, $\beta : \alpha$ enthaltenen ganzen Zahlen γ', β' zufolge der obigen Ungleichungen positiv sind (vergl. §. 81).

$$\frac{\gamma}{\alpha} = (k_0, k \ \ldots \ k_{2hn-2}), \quad \frac{\delta}{\beta} = (k_0, k_1 \ \ldots \ k_{2hn-2}, k_{2hn-1})$$

was zu beweisen war.

Nachdem wir gezeigt haben, wie wir alle aus vier *positiven* Coefficienten bestehenden Transformationen der reducirten Form (a, b, c) in sich selbst finden können, deren erster Coefficient a *positiv* ist, brauchen wir nur noch einen Blick auf die obigen Formeln

$$\alpha = \frac{t - bu}{\sigma}, \quad \beta = -\frac{cu}{\sigma}, \quad \gamma = \frac{au}{\sigma}, \quad \delta = \frac{t + bu}{\sigma}$$

zu werfen, um sogleich zu erkennen, dass die hieraus resultirenden Auflösungen t, u der unbestimmten Gleichung stets aus zwei *positiven* Zahlen t, u bestehen. Für u folgt dies aus der dritten Formel; da ferner, wie wir gesehen haben, $\delta > \gamma$ und $\gamma \geqq \alpha$, also $\delta > \alpha$ ist, so ergiebt sich, dass auch t positiv ist. Das Umgekehrte ist ebenfalls richtig; sind t, u zwei positive der unbestimmten Gleichung genügende Zahlen, so besteht die aus denselben abgeleitete Substitution $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ aus vier positiven Zahlen; denn da die Form (a, b, c) reducirt, also b positiv, und der Annahme nach a positiv, also c negativ ist, so sind zunächst β, γ, δ positiv; endlich ist $t^2 - b^2u^2 = \sigma^2 - acu^2$ positiv, folglich hat $t - bu$, also auch α, dasselbe Zeichen wie $t + bu$, nämlich das positive.

§. 84.

Wir können daher behaupten, dass alle aus zwei positiven Zahlen t, u bestehenden Auflösungen — und auf diese kommt es uns zunächst allein an — durch die Kettenbruchentwicklung der Wurzel ω der Form (a, b, c) gefunden werden, und zwar jede nur ein einziges Mal. Aus dem Anblick der unbestimmten Gleichung $t^2 - Du^2 = \sigma^2$ geht aber hervor, dass die zusammengehörigen positiven Werthe t, u gleichzeitig wachsen und gleichzeitig abnehmen; dasselbe folgt auch aus der Natur der Zähler und Nenner der Näherungsbrüche; u, und folglich auch t, wird gleichzeitig mit γ, also auch mit der von uns mit h bezeichneten Zahl wachsen; nehmen wir $h = 1$, so wird die entsprechende Auflösung, die wir mit (T, U) bezeichnen wollen, aus den kleinsten Zahlen bestehen,

d. h. T wird die kleinste aller Zahlen t, und gleichzeitig wird U die kleinste aller Zahlen u sein (die Auflösung $t = \sigma$, $u = 0$ gehört natürlich nicht zu den positiven Auflösungen). Diese kleinste Auflösung T, U findet man daher sehr leicht durch Entwicklung einer Periode von reducirten Formen.

Beispiel 1: Nimmt man für die Determinante $D = 79$ die reducirte Form $(7, 3, -10)$, welche natürlich von der ersten Art ist, so erhält man (§. 79)

$$k_0 = 1,\ k_1 = 5,\ k_2 = 3,\ k_3 = 2,\ k_4 = 1,\ k_5 = 1;$$

die successiven Näherungsbrüche sind folgende:

$$\frac{1}{1},\ \frac{6}{5},\ \frac{19}{16},\ \frac{44}{37},\ \frac{63}{53},\ \frac{107}{90};$$

aus den beiden letzten ergiebt sich daher die Substitution $\left(\begin{smallmatrix}53, & 90\\ 63, & 107\end{smallmatrix}\right)$; will man nur die kleinste Auflösung der Gleichung $t^2 - Du^2 = \sigma^2$, so braucht man nur die Nenner der Näherungsbrüche bis $\beta = 90$, oder die Zähler derselben bis $\gamma = 63$ zu bilden, so findet man durch die Formeln $\beta\sigma = -cu$ oder $\gamma\sigma = au$ die kleinste der Zahlen u, nämlich $U = 9$, und hieraus das zugehörige $T = V(\sigma^2 + DU^2) = 80$. Statt dessen findet man T auch durch die Formel $a\sigma + bU$ oder $\delta\sigma - bU$.

Nimmt man die reducirte Form $(1, 8, -15)$, so findet man folgende Zahlen (§. 79)

$$k_0 = 1,\ k_1 = 7,\ k_2 = 1,\ k_3 = 16;$$

also die Näherungsbrüche

$$\frac{1}{1},\ \frac{8}{7},\ \frac{9}{8},\ \frac{152}{135};$$

die beiden letzten liefern die Substitution $\left(\begin{smallmatrix}8, & 135\\ 9, & 152\end{smallmatrix}\right)$, und hieraus ergiebt sich wieder $U = 9$, $T = 80$, wie vorher.

Beispiel 2: Es sei $D = 13 \equiv 1 \pmod 4$; um die kleinste Auflösung der Gleichung $t^2 - 13u^2 = 4$ zu finden, nehmen wir die reducirte Form $(2, 3, -2)$, so ist (§. 79)

$$k_0 = 3,\ k_1 = 3;$$

die Näherungsbrüche sind also $\frac{3}{1}$ und $\frac{10}{3}$; dadurch erhalten wir die Substitution $\left(\begin{smallmatrix}1, & 3\\ 3, & 10\end{smallmatrix}\right)$ und hieraus $U = 3$, $T = 11$.

§. 85.

Nachdem wir gezeigt haben, wie die kleinste positive Auflösung (T, U) der unbestimmten Gleichung immer gefunden werden kann, gehen wir dazu über, alle anderen Auflösungen (t, u) auf diese eine zurückzuführen. Der Bequemlichkeit halber wollen wir, wenn t, u irgend zwei (positive oder negative) der Gleichung $t^2 - Du^2 = \sigma^2$ genügende Zahlen sind, und $\sqrt{D}$ stets positiv genommen wird, die Ausdrücke

$$\frac{t + u\sqrt{D}}{\sigma}, \quad \frac{t - u\sqrt{D}}{\sigma}$$

die zu dieser Auflösung (t, u) gehörigen Factoren nennen und als *ersten* und *zweiten Factor* von einander unterscheiden; das Product beider ist stets $= 1$; sie haben daher immer gleiche Zeichen, und zwar das positive oder negative, je nachdem t positiv oder negativ ist; haben ferner t und u gleiche Zeichen, so ist der erste Factor numerisch grösser als der zweite, folglich ist dann der erste numerisch > 1, der zweite numerisch < 1; das Gegentheil findet Statt, wenn t und u entgegengesetzte Zeichen haben; und wenn $u = 0$ ist, sind beide Factoren $= \pm 1$. Ist also z. B. (t, u) eine aus zwei positiven Zahlen bestehende Auflösung, so ist ihr erster Factor ein positiver unechter Bruch; und umgekehrt, ist der erste Factor ein positiver unechter Bruch, so sind beide Zahlen t, u positiv.

Sind (t', u') und (t'', u'') irgend zwei identische oder verschiedene Auflösungen, so kann man

$$\frac{t' + u'\sqrt{D}}{\sigma} \cdot \frac{t'' + u''\sqrt{D}}{\sigma} = \frac{t + u\sqrt{D}}{\sigma}$$

setzen, wo (t, u) wieder eine Auflösung bedeutet. Denn entwickelt man das Product links und trennt das Rationale vom Irrationalen, so findet man

$$t = \frac{t't'' + Du'u''}{\sigma}, \quad u = \frac{t'u'' + u't''}{\sigma};$$

da ferner aus der obigen Gleichung unmittelbar durch Verwandlung von $\sqrt{D}$ in $-\sqrt{D}$ oder auch durch den blossen Anblick der Ausdrücke für t, u die andere Gleichung

$$\frac{t'-u'\sqrt{D}}{\sigma}\cdot\frac{t''-u''\sqrt{D}}{\sigma}=\frac{t-u\sqrt{D}}{\sigma}$$

folgt, so ergiebt sich durch Multiplication beider

$$t^2-Du^2=\sigma^2;$$

es braucht daher nur noch gezeigt zu werden, dass u eine ganze Zahl ist, weil dann aus der vorstehenden Gleichung von selbst folgt, dass t^2, also auch t eine ganze Zahl ist. Geht nun σ^2 in D, folglich auch in t'^2, t''^2 auf, so sind t', t'' theilbar durch σ, und folglich ist u eine ganze Zahl; ist aber $4D\equiv\sigma^2 \pmod{4\sigma^2}$, so folgt $(2t')^2\equiv(\sigma u')^2 \pmod{4\sigma^2}$, hieraus $2t'\equiv\sigma u'$, und ebenso $2t''\equiv\sigma u'' \pmod{2\sigma}$, folglich $2(t'u''+u't'')\equiv 2\sigma u'u''\equiv 0 \pmod{2\sigma}$; mithin ist u auch jetzt eine ganze Zahl, w. z. b. w.

Dieser Satz lässt sich ohne Weiteres auf beliebig viele Auflösungen (t', u'), (t'', u''), (t''', u''') . . . ausdehnen: setzt man

$$\frac{t'+u'\sqrt{D}}{\sigma}\cdot\frac{t''+u''\sqrt{D}}{\sigma}\cdot\frac{t'''+u'''\sqrt{D}}{\sigma}\cdots=\frac{t+u\sqrt{D}}{\sigma},$$

so wird (t, u) stets wieder eine ganzzahlige Auflösung sein. Bestehen ferner alle jene Auflösungen aus zwei positiven Zahlen, so sind alle Factoren linker Hand positive unechte Brüche; dasselbe gilt also auch von dem ersten Factor der Auflösung (t, u), und folglich sind t, u zwei positive Zahlen.

Setzen wir alle die einzelnen Auflösungen (t', u'), (t'', u'') . . . identisch mit der kleinsten positiven Auflösung (T, U), so können wir

$$\left(\frac{T+U\sqrt{D}}{\sigma}\right)^n=\frac{t_n+u_n\sqrt{D}}{\sigma}$$

setzen, wo n eine beliebige positive ganze Zahl bedeutet, und es wird dann (t_n, u_n) jedesmal eine positive Auflösung werden; zugleich leuchtet ein, dass mit wachsendem Exponenten n der Werth der linker Hand stehenden Potenz eines unechten Bruchs, und folglich auch $t_n+u_n\sqrt{D}$ beständig wächst, so dass verschiedene Werthe von n auch verschiedene Auflösungen (t_n, u_n) liefern; und da die beiden Zahlen t_n, u_n entweder beide gleichzeitig wachsen, oder beide gleichzeitig abnehmen, so tritt offenbar das erstere oder letztere ein, je nachdem n wächst oder abnimmt.

Umgekehrt können wir zeigen, dass durch die vorstehende Formel in der That jede positive Auflösung (t, u) geliefert wird. Denn wäre der erste Factor einer solchen Auflösung keine genaue Potenz des ersten Factors der kleinsten Auflösung (T, U), so

müsste er, da beide positive unechte Brüche sind, zwischen zwei successiven Potenzen

$$\left(\frac{T+U\sqrt{D}}{\sigma}\right)^n \text{ und } \left(\frac{T+U\sqrt{D}}{\sigma}\right)^{n+1}$$

des letztern liegen, wo n mindestens $= 1$ ist. Dann wäre also

$$\frac{t_n+u_n\sqrt{D}}{\sigma} < \frac{t+u\sqrt{D}}{\sigma} < \frac{t_n+u_n\sqrt{D}}{\sigma}\cdot\frac{T+U\sqrt{D}}{\sigma},$$

und folglich, wenn man

$$\frac{t+u\sqrt{D}}{\sigma}\cdot\frac{t_n-u_n\sqrt{D}}{\sigma} = \frac{t'+u'\sqrt{D}}{\sigma}$$

setzt,

$$1 < \frac{t'+u'\sqrt{D}}{\sigma} < \frac{T+U\sqrt{D}}{\sigma};$$

es existirte daher eine positive Auflösung (t', u'), welche aus kleineren Zahlen t', u' bestände, als die kleinste Auflösung (T, U); was unmöglich ist.

Man findet daher alle aus zwei positiven Zahlen bestehenden Auflösungen durch die Formeln

$$\frac{t_n}{\sigma} = \frac{1}{\sigma^n}\left\{T^n + \frac{n(n-1)}{1.2}T^{n-2}U^2D + \cdots\right\}$$

$$\frac{u_n}{\sigma} = \frac{1}{\sigma^n}\left\{\frac{n}{1}T^{n-1}U + \frac{n(n-1)(n-2)}{1.2.3}T^{n-3}U^3D + \cdots\right\}$$

wenn man der Reihe nach für n alle positiven ganzen Zahlen setzt. Da nun ferner

$$\frac{t_n-u_n\sqrt{D}}{\sigma} = \left(\frac{T-U\sqrt{D}}{\sigma}\right)^n = \left(\frac{T+U\sqrt{D}}{\sigma}\right)^{-n}$$

ist, so ergiebt sich, dass durch die Formel

$$\frac{t_n+u_n\sqrt{D}}{\sigma} = \left(\frac{T+U\sqrt{D}}{\sigma}\right)^n$$

sämmtliche Auflösungen t_n, u_n gegeben sind, in welchen t_n positiv ist, wenn man für n alle ganzen positiven und negativen Zahlen setzt, indem $u_{-n} = -u_n$, $t_{-n} = t_n$ ist. Für $n = 0$ ergiebt sich ferner $t_0 = +\sigma$, $u_0 = 0$. Will man daher alle Auflösungen t, u ohne Ausnahme in eine Formel zusammendrängen, so braucht man nur

$$\frac{t+u\sqrt{D}}{\sigma} = \pm\left(\frac{T+U\sqrt{D}}{\sigma}\right)^n$$

zu setzen, und hierin jedes der beiden Vorzeichen mit jedem ganzzahligen Exponenten n zu combiniren. Dass auf diese Weise keine Auflösung übergangen, und jede nur einmal erzeugt wird, folgt unmittelbar daraus, dass unter den vier verschiedenen Auflösungen

$$(t, u), (t, -u), (-t, u), (-t, -u),$$

wenn u nicht $= 0$ ist, immer eine und nur eine aus zwei positiven Zahlen besteht.

Hiermit ist nun das zweite Hauptproblem der Lehre von der Aequivalenz auch für Formen von *positiver* Determinante vollständig gelöst. Wir sind durch die vollständige Auflösung der unbestimmten Gleichung $t^2 - Du^2 = \sigma^2$ in den Stand gesetzt, alle Transformationen einer solchen Form in sich selbst, und folglich auch alle Transformationen einer Form in eine äquivalente aus einer einzigen gegebenen solchen Transformation zu finden (§§. 61, 62); mithin ist auch die Aufgabe, alle eigentlichen Darstellungen einer gegebenen Zahl durch eine gegebene Form von positiver Determinante zu finden, als vollständig gelöst anzusehen (§. 60).