Ueber die Transformation

einer homogenen binaeren quadratischen Form

in

ein Aggregat von zwei Quadraten.

Untersuchungen über die Transformation der elliptischen Funktionen, insbesondere über die Theorie der Modulargleichungen, führten mich auf die zahlentheoretische Aufgabe, eine gegebene homogene binäre quadratische Form auf alle mögliche Weise durch ganzzahlige lineäre Substitutionen in ein Aggregat von zwei Quadraten zu transformiren.

Diese Aufgabe soll hier in einer Art behandelt werden, die für die Anwendung auf die genannte Theorie besonders fruchtreich ist; die Anwendung selbst wird einer spätern Gelegenheit vorbehalten.

I.

Die gegebene Form sei

$$ax^2 + 2bxx, + a, x,^2.$$

Sie soll durch eine ganzzahlige lineäre Substitution,

$$x = \alpha y + \beta, y,$$
$$x, = \alpha, y + \beta, y,,$$

transformirt werden in ein Aggregat zweier Quadrate:

$$cy^2 + c, y,^2.$$

Durch Einführung der Ausdrücke von x und x, in die Transformationsgleichung

$$ax^2 + 2bxx, + a, x,^2 = cy^2 + c, y,^2$$

ergeben sich sofort die 3 Gleichungen

$$a\alpha^2 + 2b\alpha\alpha, + a, \alpha,^2 = c$$
$$a\alpha\beta + b(\alpha\beta, + \alpha, \beta) + a, \alpha, \beta, = o$$
$$a\beta^2 + 2b\beta\beta, + a, \beta,^2 = c,.$$

Die erste und dritte dieser Gleichungen dienen dazu, die neuen Coëfficienten c, c, aus den gegebenen a, b, a, zu bestimmen; die zweite enthält die von den Substitutionscoëfficienten zu erfüllende Bedingung, damit die gegebene Form in ein Aggregat zweier Quadrate übergehe.

Die wesentliche Aufgabe ist daher, die diophantische Gleichung

$$a\alpha\beta + b(\alpha\beta, + \alpha, \beta) + a, \alpha, \beta, = o$$

aufzulösen. Der blosse Anblick dieser Gleichung führt sofort auf eine Beschränkung, die man den gegebenen ganzen Zahlen a, b, a,, und eine zweite, die man den Unbekannten α, β, $\alpha,$, $\beta,$, auflegen darf, ohne der Allgemeinheit, der Lösung wesentlich Eintrag zu thun.

Erstens. Haben die drei ganzen Zahlen a, b, a, einen allen dreien gemeinschaftlichen Faktor, so fällt dieser durch Division der ganzen Gleichung mit demselben weg, und es erhellt daraus, dass die Lösung der Aufgabe für alle „nicht ursprünglichen" Formen zusammenfällt mit derjenigen für die „ursprüngliche" Form (forma primitiva bei Gauss), aus welcher sie derivirt sind. Es ist also nur nöthig, die Aufgabe unter der Voraussetzung zu lösen, dass a, b, a, ohne einen allen dreien gemeinschaftlichen Factor seien, mithin die Form (a, b, a,) eine „ursprüngliche."

Zweitens. Ist $\begin{pmatrix}\alpha, & \beta\\ \alpha_{,}, & \beta_{,}\end{pmatrix}$ eine Lösung der Gleichung, so ist, wenn φ und ψ beliebige ganze Zahlen bezeichnen, auch $\begin{pmatrix}\alpha\varphi, & \beta\psi\\ \alpha_{,}\varphi, & \beta_{,}\psi\end{pmatrix}$ eine Lösung. Man hat daher nur nöthig diejenigen Lösungen aufzusuchen, in welchen α und $\alpha_{,}$ unter sich und ebenso β und $\beta_{,}$ unter sich relative Primzahlen sind, und kann aus jeder solchen Lösung unzählig viele andere ableiten, die diese Eigenschaft **nicht** haben.

II.

Nach dieser Einschränkung behandle ich nun die Aufgabe zuerst für den besonderen Fall, dass b = o ist.

Für diesen Fall geht die Bedingung, dass a, b, a, ohne einen allen dreien gemeinschaftlichen Factor seien, darin über, dass a und a, relative Primzahlen seien. Die von den Substitutionscoëfficienten zu erfüllende Gleichung lautet

$$a\alpha\beta + a_{,}\alpha_{,}\beta_{,} = o,$$

woraus folgt

$$\frac{\alpha\beta}{\alpha_{,}\beta_{,}} = -\frac{a_{,}}{a},$$

mithin, da α, β, $\alpha_{,}$, $\beta_{,}$ ganze Zahlen sein sollen:

$$\alpha\beta = a_{,}\Delta, \quad \alpha_{,}\beta_{,} = -a\Delta,$$

wo Δ eine beliebige ganze Zahl bezeichnet, die positiv oder negativ oder auch Null sein kann. Es kommt nun darauf an, $a_{,}\Delta$ und $-a\Delta$ so in zwei Factoren zu zerlegen, das α gegen $\alpha_{,}$ und β gegen $\beta_{,}$ relativ prim sei.
Dies ergiebt

$$\begin{aligned}\alpha &= a_{,}'\Phi \quad , \beta = a_{,}''\Psi\\ \alpha_{,} &= -a'\Psi \quad , \beta_{,} = a''\Phi.\end{aligned}$$

Hier bezeichnet Φ eine beliebige ganze Zahl ohne gemeinschaftlichen Factor mit $a'a_{,}''\Psi$, Ψ eine beliebige ganze Zahl ohne gemeinschaftlichen Factor mit $a_{,}'a''\Phi$; ferner ist durch $a = a'a''$ und $a_{,} = a_{,}'a_{,}''$ irgend ein Paar Zerlegungen von a und a, in das Product von zwei positiven oder negativen ganzen Zahlen angedeutet. Um alle möglichen Substitutionen $\begin{pmatrix}\alpha, & \beta\\ \alpha_{,}, & \beta_{,}\end{pmatrix}$ zu erhalten, wird man daher a und a, auf alle mögliche Art in zwei Factoren zerlegen müssen. Und nach der Anzahl dieser Zerlegungen werden sich die sämmtlichen Substitutionen in mm, Gruppen theilen, wenn m die Anzahl der verschiedenen Darstellungen von a als Product von zwei ganzzahligen Factoren, m, die von a, bezeichnet; hiebei sind die vier Darstellungen

$$a = a'a'' = a''a' = (-a')(-a'') = (-a'')(-a'),$$

welche aus der nämlichen Zerlegung von a in zwei Factoren entspringen, als vier gerechnet, wenn $a' \gtrless a''$, als 2, wenn $a' = a''$; ebenso bei $a_{,}$. Bezeichnet man die Anzahl der verschiedenen

Zerlegungen von a in zwei Factoren durch n, die von a, durch n,, so wird, wie leicht nachzuweisen ist, die Anzahl der verschiedenen Gruppen von Substitutionen entweder

4n.4n, oder (4n—2).4n, oder 4n.(4n,—2) oder (4n—2).(4n,—2),

je nachdem weder a noch a, eine Quadratzahl ist, oder a eine Quadratzahl ist, oder a, eine Quadratzahl ist, oder beide Quadratzahlen sind.

Bezeichnet man die Determinante der Substitutionscoëfficienten

$$\alpha\beta, - \alpha,\beta = \triangle,$$

so wird

$$\triangle = a,'a'' \Phi^2 + a'a,''\Psi^2.$$

Ferner erhält man

$$c = a\alpha^2 + a,\alpha,^2 = a,a,'\triangle \quad , \quad c, = a\beta^2 + a,\beta,^2 = a''a,''\triangle,$$

mithin die Transformationsgleichung

$$ax^2 + a,x,^2 = \triangle\,(a'a,'y^2 + a''a,''y,^2).$$

Fragt man nach der Anzahl der verschiedenen Gruppen von Transformationen der gegebenen Form, so ist dieselbe nicht gleich der vorher bestimmten Anzahl der verschiedenen Gruppen von Substitutionen $\begin{pmatrix} \alpha, & \beta \\ \alpha,, & \beta, \end{pmatrix}$. Vielmehr ist es leicht einzusehen, dass die 16 verschiedenen Gruppen von Substitutionen, welche durch die Zerlegungen a = a'a'' und a, = a,'a,'' entstehen und kurz angedeutet werden mögen durch

$$\begin{pmatrix} a,' & a,'' \\ a' & a'' \end{pmatrix} \quad \begin{pmatrix} a,' & a,'' \\ a'' & a' \end{pmatrix} \quad \begin{pmatrix} a,'' & a,' \\ a'' & a' \end{pmatrix} \quad \begin{pmatrix} a,'' & a,' \\ a' & a'' \end{pmatrix}$$

$$\begin{pmatrix} -a,' & -a,'' \\ a' & a'' \end{pmatrix} \quad \begin{pmatrix} -a,' & -a,'' \\ a'' & a' \end{pmatrix} \quad \begin{pmatrix} -a,'' & -a,' \\ a' & a'' \end{pmatrix} \quad \begin{pmatrix} -a,'' & -a,' \\ a'' & a' \end{pmatrix}$$

$$\begin{pmatrix} a,' & a,'' \\ -a' & -a'' \end{pmatrix} \quad \begin{pmatrix} a,' & a,'' \\ -a'' & -a' \end{pmatrix} \quad \begin{pmatrix} a,'' & a,' \\ -a' & -a'' \end{pmatrix} \quad \begin{pmatrix} a,'' & a,' \\ -a'' & -a' \end{pmatrix}$$

$$\begin{pmatrix} -a,' & -a,'' \\ -a' & -a'' \end{pmatrix} \quad \begin{pmatrix} -a,' & -a,'' \\ -a'' & -a' \end{pmatrix} \quad \begin{pmatrix} -a,'' & -a,' \\ -a' & -a'' \end{pmatrix} \quad \begin{pmatrix} -a,'' & -a,' \\ -a'' & -a' \end{pmatrix}$$

nur zwei verschiedene Gruppen von Werthen für $\triangle^2$ und auch nur zwei wirklich verschiedene Gruppen von Transformationen liefern, nämlich

$$\triangle^2 = (a,'a''\Phi^2 + a'a,''\Psi^2)^2 \quad , \quad ax^2 + a,x,^2 = \triangle\,(a'a,'y^2 + a''a,''y,^2)$$

und

$$\triangle^2 = (a,'a'\Phi^2 + a''a,''\Psi^2)^2 \quad , \quad ax^2 + a,x,^2 = \triangle\,(a''a,'y^2 + a'a,''y,^2).$$

Denn zwei Transformationen, die sich nur durch Vertauschung der Coëfficienten von y^2 und $y,^2$ unterscheiden, können nicht als wirklich verschieden betrachtet werden. Bedenkt man nun noch, dass beide Gruppen in „eine" zusammenfallen, wenn entweder a,' = a,'' oder a' = a'' oder beides zugleich ist, und dass das Erste nur vorkommen kann, wenn a, eine Quadratzahl ist, und auch dann nur für „eine" Zerlegung von a,, das Zweite nur, wenn a eine Quadratzahl ist, das Dritte nur, wenn beide Quadratzahlen sind, so ergiebt sich, wie man bald übersieht, das Resultat: „Je nachdem weder a noch a, eine Quadratzahl ist, oder a oder a, eine Quadratzahl ist, oder beide Quadratzahlen sind, ist die Anzahl der verschiedenen Gruppen von Transformationen entweder

2nn, oder 2(n—1)n, + n, oder 2n(n,—1) + n oder 2(n—1)(n,—1) + n—1 + n,—1 + 1

also entweder

nn, + n,n oder (n—1)n, + n,n oder nn, + (n,—1)n oder (n—1)n, + (n,—1) n + 1."

Betrachtet man den Ausdruck für die Substitutionsdeterminante $\triangle$, so lässt sich über die Werthe, welche $\triangle$ annehmen kann, Folgendes aussagen: „$\triangle$ durchläuft, wenn man alle möglichen Substitutionen aufstellt, alle ganzzahligen Werthe, die folgenden Bedingungen genügen:

1) Δ ist durch eine Form von der Determinante $-aa_,$ mit verschwindendem mittlern Coëfficienten in relativen Primzahlen darstellbar.

2) Δ hat mit $aa_,$ keine andern, als quadratische Faktoren von a und a, gemein."

Besonders zu bemerken ist, dass in dem vorliegenden Falle $b = o$ Δ stets auch den Werth ± 1 annehmen kann; man erhält denselben, wenn man setzt

$$a'a'' = a.(\pm 1) \quad , \quad a_,'a_,'' = (\pm 1).a, \quad , \quad \Phi = \pm 1, \ \Psi = o.$$

Für $\Delta = \pm 1$ wird die Form $ax^2 + a_,x_,^2$ in sich selbst transformirt. Die Anzahl der Substitutionen, welche ein und denselben Werth von Δ ergeben, ist gleich der Anzahl von Darstellungen der Zahl Δ durch die Form $a_,'a''\Phi^2 + a'a_,''\Psi^2$; letztere ist durch die Theorie der quadratischen Formen bestimmt.

Fasse ich jetzt die zur Transformation gehörenden Formeln noch einmal zusammen, so ist folgendes Resultat gewonnen:

„Bedeuten a und a, zwei beliebige relative Primzahlen, $a = a'a''$ und $a_, = a_,'a_,''$ irgend ein Paar Darstellungen derselben als Producte von zwei ganzen Zahlen, ferner Φ und Ψ zwei ganze Zahlen der Art, dass Φ relative Primzahl gegen $a'a_,''\Psi$ und Ψ relative Primzahl gegen $a_,'a''\Phi$ ist, so wird durch die Substitution

$$x = \alpha y + \beta y_, = \quad a_,'\Phi y + a_,''\Psi y_,$$
$$x_, = \alpha_, y + \beta_, y_, = -a'\Psi y + a''\Phi y_,$$

die Transformation

$$ax^2 + a_,x_,^2 = \Delta(a'a_,'y^2 + a''a_,''y_,^2)$$

bewirkt, wo

$$\Delta = \alpha\beta_, - \alpha_,\beta = a_,'a''\Phi^2 + a'a_,''\Psi^2.$$ "

Bezeichnet man $a'a_,' = A$, $a''a_,'' = A_,$ und bemerkt nun, dass $a.a_, = A.\,A_,$ ist, dass ferner a' der grösseste gemeinschaftliche Factor von a und A ist u. s. w., so lässt sich das gewonnene Resultat auch in folgender Form aussprechen, die weiter unten eine Parallele zwischen dem vorliegenden Falle $b = o$ und der Lösung der allgemeinen Aufgabe ergeben wird:

„Ist D eine beliebige ganze Zahl, $D = a.a_,$ eine Zerlegung derselben in das Product von zwei relativen Primzahlen, $D = A.A_,$ eine Zerlegung derselben in das Product von irgend zwei ganzen Zahlen, ist ferner

a' der grösseste gemeinschaftliche Factor von a und A,
a'' „ „ „ „ „ a und $A_,$,
$a_,'$ „ „ „ „ „ $a_,$ und A,
$a_,''$ „ „ „ „ „ $a_,$ und $A_,$,

so wird durch die Substitution

$$x = \alpha y + \beta y_, = \quad a_,'\Phi y + a_,''\Psi y_,$$
$$x_, = \alpha_, y + \beta_, y_, = -a'\Psi y + a''\Phi y_,$$

die Transformation

$$ax^2 + a_,x_,^2 = \Delta\,(Ay^2 + A_,y_,^2)$$

bewirkt, wo Φ, Ψ, Δ die oben angegebene Bedeutung haben."

Zum Schlusse dieser Behandlung des Falles $b = o$ hebe ich folgende Beispiele hervor:

1) Nimmt man $a'a'' = 1.a$, $a_,'a_,'' = 1.a_,$, so erhält man für diese Zerlegung folgende zwei Gruppen von Transformationen, welche zugleich, wenn a und a, absolute Primzahlen, die einzigen sind:

1. Gruppe
$$\begin{cases} x = \quad \Phi y + a_,\Psi y_, \\ x_, = -\Psi y + a\,\Phi y_, \\ \qquad ax^2 + a_,x_,^2 = \Delta\,(y^2 + aa_,y_,^2). \end{cases} \quad \Delta = a\Phi^2 + a_,\Psi^2$$

$$\text{2. Gruppe} \begin{cases} x = \Phi y + a_1 \Psi y, \\ x_1 = -a \Psi y + \Phi y, \end{cases} \Delta = \Phi^2 + a a_1 \Psi^2$$
$$a x^2 + a_1 x_1^2 = \Delta (a y^2 + a_1 y_1^2).$$

2) Ist $a = 1$, $a_1 =$ einer Primzahl p, so ist folgende die einzige Gruppe von Transformationen:

$$\begin{cases} x = \Phi y + p \Psi y, \\ x_1 = -\Psi y + \Phi y, \\ x^2 + p x_1^2 = \Delta (y^2 + p y_1^2). \end{cases}, \quad \Delta = \Phi^2 + p \Psi^2$$

Statt jeder der hier angegebenen Substitutionen sind nach dem Vorhergehenden noch sieben andere möglich.

III.

Ich gehe nun an die **allgemeine** Aufgabe, welche (vgl. No. I.) auf die Gleichung führte:

$$a\alpha\beta + b(\alpha\beta_1 + \alpha_1\beta) + a_1\alpha_1\beta_1 = 0.$$

Der blosse Anblick dieser Gleichung lehrt, dass höchstens einer der vier Substitutionscoëfficienten verschwinden kann; denn die Annahmen, $\alpha = \beta = 0$ oder $\alpha_1 = \beta_1 = 0$ oder $\alpha = \alpha_1 = 0$ oder $\beta = \beta_1 = 0$ sind ganz unstatthaft, die Annahmen $\alpha = \beta_1 = 0$ oder $\alpha_1 = \beta = 0$ aber erfüllen (ausser wenn $b = 0$) die Gleichung nicht, ohne dass noch ein dritter Coëfficient verschwindet. Schreibt man nun die Gleichung

$$(a\alpha + b\alpha_1)\beta + (b\alpha + a_1\alpha_1)\beta_1 = 0,$$
$$\text{oder } (a\beta + b\beta_1)\alpha + (b\beta + a_1\beta_1)\alpha_1 = 0,$$

so erhält man, der Reihe nach α, α_1, β, β_1 Null setzend und immer die Bedingung „α gegen α_1, β gegen β_1 relative Primzahl" bedenkend, sofort die vier Speciallösungen

$$\begin{Bmatrix} \alpha, & \beta \\ \alpha_1, & \beta_1 \end{Bmatrix} = \begin{Bmatrix} 0, & \frac{a_1}{\varphi_1} \\ \pm 1, & -\frac{b}{\varphi_1} \end{Bmatrix}, \begin{Bmatrix} \pm 1, & -\frac{b}{\varphi} \\ 0, & \frac{a}{\varphi} \end{Bmatrix}, \begin{Bmatrix} \frac{a_1}{\varphi_1}, & 0 \\ -\frac{b}{\varphi_1}, & \pm 1 \end{Bmatrix}, \begin{Bmatrix} -\frac{b}{\varphi}, & \pm 1 \\ \frac{a}{\varphi}, & 0 \end{Bmatrix},$$

worin φ den grössesten gemeinschaftlichen Factor von a und b, φ_1 den von b und a_1 bedeutet, so dass (mit Berücksichtigung von No. I.) φ und φ_1 relative Primzahlen sind. Bezeichnet man $a a_1 - b^2 = D$, so geben diese Lösungen die vier Transformationen

$$a x^2 + 2bxx_1 + a_1 x_1^2 = \frac{a_1}{\varphi_1}\left(\varphi_1 y^2 + \frac{D}{\varphi_1} y_1^2\right)$$
$$= \frac{a}{\varphi}\left(\varphi y^2 + \frac{D}{\varphi} y_1^2\right)$$
$$= \frac{a_1}{\varphi_1}\left(\frac{D}{\varphi_1} y^2 + \varphi_1 y_1^2\right)$$
$$= \frac{a}{\varphi}\left(\frac{D}{\varphi} y^2 + \varphi y_1^2\right)$$

Da zwei durch Vertauschung von y und y_1 in einander übergehende Formen nicht als wesentlich verschieden angesehen werden können, so repräsentiren übrigens diese vier Transformationen nur zwei verschiedene.

Die beiden angegebenen Formen der zu lösenden Gleichung führen auch sofort auf zwei vollständige Lösungen. Es folgt nämlich aus denselben:

$$1)\ \begin{matrix} a\alpha + b\alpha, = & d\beta, \\ b\alpha + a,\alpha, = -& d\beta \end{matrix} \quad \text{und} \quad 1')\ \begin{matrix} a\beta + b\beta, = -& d,\alpha, \\ b\beta + a,\beta, = & d,\alpha \end{matrix},$$

wo wegen der Bedingung „α gegen α,, β gegen β, relative Primzahl" d und d, ganze (nicht blos rationale) Zahlen sein müssen; denn wäre z. B. d ein Bruch, so würden, da α und α, mithin auch $a\alpha + b\alpha$, und $b\alpha + a,\alpha$, ganze Zahlen sind, β und β, den Nenner dieses Bruchs als gemeinschaftlichen Factor haben. Derselben Bedingung wegen ist d so zu bestimmen, dass es der grösseste gemeinschaftliche Factor von $a\alpha + b\alpha$, und $b\alpha + a,\alpha$, ist, d, so, dass es der grösseste gemeinschaftliche Factor von $a,\beta + b,\beta$, und $b,\beta + a,,\beta$, ist. Nun muss aber jeder gemeinschaftliche Factor von $a\alpha + b\alpha$, und $b\alpha + a,\alpha$, auch gemeinschaftlicher Factor von a, $(a\alpha + b\alpha,) - b(b\alpha + a,\alpha,)$ und $-b(a\alpha + b\alpha,) + a(b\alpha + a,\alpha,)$, d. h. von D.a und D.$\alpha$, sein (wo $D = aa, - b^2$), mithin, wegen „α gegen α, relative Primzahl", muss d ein Factor von D sein; ebenso sieht man es für d, ein. Löst man die beiden Gleichungen 1) nach α und α, auf, so folgt

$$\begin{aligned} D.\alpha &= (b\beta + a,,\beta,).d \\ D.\alpha, &= -(a\beta + b\beta,).d. \end{aligned}$$

Setzt man hierin für $b\beta + a,,\beta$, und $a\beta + b\beta$, aus den Gleichungen 1') ein d, α resp. — d, α,, so folgt

$$2)\ D = d.d,.$$

Diese Gleichung ist nothwendig, wenn die Gleichungen 1) und 1') gleichzeitig bestehen sollen; sie ist aber auch hinreichend, so dass, wenn $D = d.\,d$, ist, die Gleichungen 1') eine Folge der Gleichungen 1) sind und umgekehrt: kurz jedes Paar stellt dann dieselbe Gruppe von Lösungen dar. Mit Hülfe der Gleichungen 1) und 1') folgt weiter

$$3)\ \triangle = \alpha\beta, - \alpha,\beta = \frac{a\alpha^2 + 2b\alpha\alpha, + a,\alpha,^2 = a,\beta^2 + 2b,\beta\beta, + a,,\beta,^2.}{d \qquad\qquad d,}$$

$$c = a\alpha^2 + 2b\alpha\alpha, + a,\alpha,^2 = \triangle.d,\ c, = a,\beta^2 + 2b,\beta\beta, + a,,\beta,^2 = \triangle.d,.$$

$$4)\ ax^2 + 2bxx, + a,x,^2 = cy^2 + c,y,^2 = \triangle\,(dy^2 + d,y,^2).$$

Hiemit ist folgende Doppel-Lösung gewonnen:

„(1.) Man setze für α, α, alle möglichen Paare relativer Primzahlen (wobei negative Zahlen nicht auszuschliessen sind) und bestimme jedes Mal β und β, aus den Gleichungen 1), indem man d gleich dem grössesten gemeinschaftlichen Factor von $a\alpha + b\alpha$, und $b\alpha + a,\alpha$, setzt: so erhält man alle mit der in No. I. angegebenen Beschränkung behafteten Lösung $\binom{\alpha, \beta}{\alpha, \beta,}$ der vorgelegten Gleichung. — Ebenso, wenn man für β, β, alle möglichen Paare relativer Primzahlen setzt und α und α, aus den Gleichungen 1') bestimmt, wo d, = grössester gemeinschaftlicher Factor von $a,\beta + b,\beta$, und $b,\beta + a,,\beta$. — Die Gleichungen 2) 3) 4) geben in beiden Fällen die übrigen zur Transformation gehörigen Formeln."

Diese Lösung unterscheidet sich von der für den Fall b = o in No. II. gegebenen insofern, als dort sämmtliche vier Substitutionscoëfficienten gleichmässig von zwei beliebigen ganzen Zahlen Φ und Ψ abhängig gemacht sind, während hier das eine Paar durch das andere ausgedrückt ist. Doch ist es unschwer, wenn man hier b = o setzt, aus dieser Lösung die dort gegebene abzuleiten, worauf ich hier nicht eingehe. Durch die Formeln der Transformation wird man von selbst aufgefordert, die sämmtlichen Transformationen in Gruppen zu theilen nach den verschiedenen Zerlegungen d.d, von D in zwei Factoren; die Anzahl der Gruppen ist, da zwei Formen, in denen nur y und y, vertauscht sind, nicht als verschieden zu rechnen sind, gleich der Anzahl der verschiedenen Zerlegungen von D in zwei Factoren. Hierin herrscht die vollständigste Analogie mit dem Falle b = o, in welchem $D = a.a,$ wird. Denn in diesem Falle waren die Coëfficienten von $\triangle y^2$ und $\triangle y,^2$ resp. $a'a,'$ und $a''\,a,''$, welche in der That eine beliebige Zer-

egung von aa, in zwei Factoren darstellen; auch ist die in No. II. bestimmte Gruppenzahl der Transformationen nichts Anderes, als die Anzahl der verschiedenen Zerlegungen von aa, in zwei Factoren.

IV.

Auf eine neue Form der Auflösung führen die Formeln 3) für die Substitutionsdeterminante $\triangle$. Es sei m irgend eine durch die Form (a, b, a,) in relative Primzahlen darstellbare Zahl, r und r, die darstellenden Zahlen, also

$$m = ar^2 + 2brr, + a,r,^2.$$

Dann geht bekanntlich durch die Substitution (vgl. Dirichlets Vorlesungen über Zahlentheorie, herausgegeben von Dedekind)

$$\begin{aligned} \alpha &= r\psi + \varrho\psi, \\ \alpha, &= r,\psi + \varrho,\psi, \end{aligned}, \quad r\varrho, - r,\varrho = 1,$$

$a\alpha^2 + 2b\alpha\alpha, + a,\alpha,^2$ über in $m\psi^2 + 2n\psi\psi, + m,\psi,^2$, wo

$$n = ar\varrho + b(r\varrho, + r,\varrho) + a,r,\varrho, \quad , m, = \frac{n^2 + D}{m}$$

ist. Es wird

$$\begin{aligned} a\alpha + b\alpha, &= (ar + br,)\psi + (a\varrho + b\varrho,)\psi, \\ b\alpha + a,\alpha, &= (br + a,r,)\psi + (b\varrho + a,\varrho,)\psi, \end{aligned},$$

mithin

$$\begin{aligned} r(a\alpha + b\alpha,) + r,(b\alpha + a,\alpha,) &= m\psi + n\psi, \\ \varrho(a\alpha + b\alpha,) + \varrho,(b\alpha + a,\alpha,) &= n\psi + m,\psi, \end{aligned}.$$

Für $\psi, = o$, mithin $\psi = 1$ wird $\triangle = \frac{m}{d}$, und die beiden letzten Gleichungen werden

$$\begin{aligned} r(a\alpha + b\alpha,) + r,(b\alpha + a,\alpha,) &= m \\ \varrho(a\alpha + b\alpha,) + \varrho,(b\alpha + a,\alpha,) &= n \end{aligned},$$

woraus noch folgt

$$\begin{aligned} a\alpha + b\alpha, &= \varrho,m - r,n \\ ba + a,\alpha, &= -\varrho m + rn. \end{aligned}$$

Die beiden vorletzten Gleichungen zeigen, dass der grösseste gemeinschaftliche Factor von $a\alpha + b\alpha$, und $b\alpha + a,\alpha$, (d. h. d) auch gemeinschaftlicher Factor von m und n ist; die beiden letzten Gleichungen zeigen, dass der grösseste gemeinschaftliche Factor von m und n auch gemeinschaftlicher Factor von $a\alpha + b\alpha$, und $b\alpha + a,\alpha$, ist. In Summa: d ist der grösseste gemeinschaftliche Factor von m und n. Da

$$\frac{n^2 + D}{m} = m, = \text{ganze Zahl}$$

ist, so folgt hiemit auf eine zweite Art, dass d ein Factor von D ist. Und zwar ist nothwendig, wenn der grösseste gemeinschaftliche Factor von m und D gleich L.Q ist, wo L eine Zahl ohne quadratischen Factor, Q eine Quadratzahl bedeutet, entweder $d = L.\sqrt{(Q)}$ oder $d = L.Q$, so dass jedenfalls, wenn D keinen quadratischen Factor hat, $\triangle = \frac{m}{d}$ stets relative Primzahl gegen D. ist; wie für den Fall $b = o$ bereits in No. II. gefunden wurde.

Wir haben hiemit folgende Auflösung gewonnen, in der übrigens α, α, und β, β, mit einander vertauscht werden können:

„(2.) Es sei (m, n, m,) irgend eine der gegebenen Form (a, b, a,) eigentlich äquivalente Form, $\begin{pmatrix} r, & \varrho \\ r_{,}, & \varrho_{,} \end{pmatrix}$ irgend eine die letztere Form in die erstere transformirende Substitution, d der grösseste gemeinschaftliche Factor von m und n, $d, = \frac{aa, -b^2}{d} = \frac{D}{d}$; dann ist zu setzen

$$\triangle = \frac{m}{d}$$

$$\alpha = r\ ,\ \beta = \varrho\triangle - r\frac{n}{d},$$

$$\alpha, = r,,\ \beta, = \varrho,\triangle - r,\frac{n}{d},$$

Dadurch wird

$$ax^2 + 2bxx, + a,x,^2 = \triangle(dy^2 + d,y,^2).“$$

Zusatz I. Man erhält sämmtliche verschiedene Transformationen der Form (a, b, a,) in das Aggregat zweier ganzzahligen Quadrate, wenn man für m nach einander sämmtliche durch die Form a, b, a, darstellbare Zahlen, für n jedes Mal die sämmtlichen unter einander incongruenten kleinsten Wurzeln der Congruenz $n^2 + D \equiv o \pmod{m}$, für welche die Form (a, b, a,) der Form (m, n, m,) äquivalent ist (man kann hienach immer $n^2 \leqq \frac{m^2}{4}$ machen), für $\begin{pmatrix} r, & \varrho \\ r_{,}, & \varrho_{,} \end{pmatrix}$ endlich zu jedem m, n **eine** Substitution setzt.

Denn sind n und n' irgend zwei congruente Wurzeln der Congruenz $n^2 + D \equiv o \pmod{m}$, so ist $n' = n + m\nu$, wo ν eine ganze Zahl bedeutet. Der grösseste gemeinschaftliche Factor von m und n ist aber mit dem grössesten gemeinschaftlichen Factor von m und $n' = n + m\nu$ identisch; mithin hat d, also auch $\triangle, = \frac{m}{d}$ und $d, = \frac{D}{d}$, für zwei congruente Wurzeln denselben Werth; man erhält also für beide dasselbe Aggregat zweier Quadrate, obgleich die **Substitution** verschieden ist. Da r, ϱ, r,, ϱ, nur in den Substitutionscoëfficienten, nicht aber in dem Aggregat der Quadrate vorkommen, so ist dieses für alle verschiedenen Systeme $\begin{pmatrix} r, & \varrho \\ r_{,}, & \varrho_{,} \end{pmatrix}$ ebenfalls dasselbe.

Zusatz II. Da die Anzahl der durch die Form (a, b, a,) darstellbaren Zahlen ∞ ist, so ist hienach auch die Anzahl der verschiedenen Transformationen unendlich. Ein und dieselbe Transformation resultirt aber wieder aus unendlich vielen verschiedenen Substitutionen, da die unendlichen vielen in Bezug auf m congruenten n sämmtlich dasselbe Aggregrat zweier Quadrate ergeben.

Zusatz III. Die aus Auflösung (2.) sich ergebende Folgerung, dass irgend zwei äquivalente Formen genau dieselben Aggregate von zwei Quadraten ergeben, obgleich die zugehörigen Substitutionen verschieden sind, ist selbstverständlich, da man ja jede von zwei solchen Formen ganzzahlig in die andere und diese dann weiter in ein Aggregat zweier Quadrate transformiren kann. Ja man sieht sogar noch leicht ein, dass eine Form, welche eine andere enthält, sich in die sämmtlichen Aggregate von zwei Quadraten, welche der letztern entsprechen, transformiren lässt — jedoch nicht umgekehrt.

Zusatz IV. Setzt man erstens $m = a,$, $n = b$ und zweitens $m = a$, $n = b$, so erhält man die beiden aus den im Anfange von No. III. angegebenen vier Speciallösungen hervorgehenden Aggregate zweier Quadrate. In diesen Fällen wird $\triangle = +\frac{a,}{\varphi,}$ resp. $+\frac{a}{\varphi}$. Diese beiden Werthe ent-

sprechen dem Werthe + 1, welchen $\triangle$ im Falle $b = o$ annehmen kann; für $b = o$ wird $\varphi_, = a_,$, $\varphi = a$ mithin $\frac{a_,}{\varphi_,} = \frac{a}{\varphi} = 1$.

Zusatz V. Der Beweis, dass durch die in Auflösung (2.) angegebene Substitution wirklich die Transformation

$$ax^2 + 2bxx, + a,x,^2 = \triangle(dy^2 + d,y,^2), \text{ wo } \triangle = \frac{m}{d},\ d, = \frac{D}{d}$$

bewirkt wird, liegt zwar in der Ableitung dieser Auflösung aus Auflösung (1.), lässt sich jedoch nachträglich auch durch Rechnung führen. Durch die Substitution

$$\begin{matrix} x = \alpha y + \beta y, \\ x, = \alpha, y + \beta, y, \end{matrix} \text{ wird } \begin{matrix} ax^2 + 2bxx, + a,x,^2 \\ = (a\alpha^2 + 2ba\alpha, + a,\alpha,^2)y^2 \\ +2(a\alpha\beta + b(\alpha\beta, + \alpha,\beta) + a,\alpha,\beta,)yy, \\ + (\alpha\beta^2 + 2b\beta\beta, + \alpha,\beta,^2)y,^2. \end{matrix}$$

Nun ist

$$a\alpha^2 + 2ba\alpha, + a,\alpha,^2 = ar^2 + 2brr, + a,r,^2 = m. = \frac{m}{d}.d = \triangle.d!$$

$$a\alpha\beta + b(\alpha\beta, + \alpha,\beta) + a,\alpha,\beta, = ar\left(\varrho\triangle - r\frac{n}{d}\right) + br\left(\varrho,\triangle - r,\frac{n}{d}\right)$$

$$+ br,\left(\varrho\triangle - r\frac{n}{d}\right) + a,r,\left(\varrho,\triangle - r,\frac{n}{d}\right)$$

$$= (ar\varrho + b(r\varrho, + r,\varrho) + a,r,\varrho,)\triangle - (ar^2 + 2brr, + a,r,^2)\frac{n}{d}$$

$$= n\triangle - m.\frac{n}{d} = n.\frac{m}{d} - m.\frac{n}{d} = o!$$

$$a\beta^2 + 2b\beta\beta, + a,\beta,^2 = a\left(\varrho\triangle - r\frac{n}{d}\right)^2 + 2b\left(\varrho\triangle - r\frac{n}{d}\right)\left(\varrho,\triangle - r,\frac{n}{d}\right) + a,\left(\varrho,\triangle - r,\frac{n}{d}\right)^2$$

$$= (a\varrho^2 + 2b\varrho\varrho, + a,\varrho,^2)\triangle^2 - 2(ar\varrho + b(r\varrho, + r,\varrho) + a,r,\varrho,)\triangle.\frac{n}{d} + (ar^2 + 2brr, + a,r,^2)\frac{n^2}{d^2}$$

$$= m,\triangle^2 - 2n.\triangle.\frac{n}{d} + m.\frac{n^2}{d^2} = m,\triangle^2 - 2n\triangle.\frac{n}{d} + \triangle.\frac{n^2}{d}$$

$$= \triangle\left(m,\triangle - \frac{n^2}{d}\right) = \triangle.\frac{m,m - n^2}{d} = \triangle.\frac{D}{d}, \text{ weil } n^2 + D = mm, \text{ ist.}$$

V.

Gehen wir noch einmal zurück zu den Gleichungen 1) und 1'). Von diesen vier Gleichungen gilt nicht blos, dass jedes Paar eine Folge des andren ist, wenn $d.d, = D$, sondern es gilt allgemein, dass je zwei der vier Gleichungen entweder den beiden andern widersprechen, oder aus ihnen folgen, je nachdem $d.d,$ nicht $= D$ oder $d.d, = D$ ist. Dies erkennt man sofort, indem man die vier Gleichungen schreibt:

$$\begin{matrix} d,\alpha, + a\beta + b\beta, = o, \\ -d,\alpha + b\beta + a,\beta, = o, \\ -a\alpha - b\alpha, + d\beta, = o, \\ -b\alpha - a,\alpha, - d\beta = o. \end{matrix}$$

Sollen nicht sämmtliche vier Unbekannten verschwinden, so muss die Determinante verschwinden, d. h.

$$(d,d - aa, + b^2)^2 = o, \text{ mithin } d.d, = D$$

sein. Damit verschwinden aber zugleich sämmtliche Partialdeterminanten 3. Grades, dagegen nicht die 2. Grades, also je zwei Gleichungen sind eine Folge der beiden andren, die vier Unbekannten sind homogene lineäre Ausdrücke von zwei willkürlichen Grössen. Man kann daher allgemein setzen

$$\alpha = \alpha' X + \alpha'' X_, \quad , \quad \beta = \beta' X + \beta'' X_,$$
$$\alpha, = \alpha,' X + \alpha,'' X_, \quad , \quad \beta = \beta,' X + \beta,'' X_,$$

wo die acht Coëfficienten bestimmte, X und $X_,$ aber willkürliche Zahlen bedeuten; diese Form haben z. B. auch die Gleichungen 1) und 1') und man erhält sie überhaupt, wenn man die vier Unbekannten durch irgend zwei derselben ausdrückt. Es muss nun das Ziel sein, es dahin zu bringen, dass in dieser Form sowohl die acht Coëfficienten ganze Zahlen bedeuten, als auch X und $X_,$ nur ganzzahlige Werthe durchlaufen. Die acht Coëfficienten sind nun in der That ganze Zahlen, wenn man die vier Unbekannten durch irgend zwei derselben ausdrückt; X und $X_,$ aber werden dann Brüche mit constantem Nenner, der entweder d oder d, oder b oder a oder a, ist. Die Zähler dieser Brüche können nicht alle beliebigen ganzzahligen Werthe annehmen, sondern nur solche, dass α, $\alpha,$, β, $\beta,$ stets ganze Zahlen sind. Damit dies der Fall sei, haben diese Zähler stets zwei Congruenzen zu erfüllen, deren Modul d resp. d, resp. b resp. a resp. a, ist. Diese Congruenzen sind leicht aufzulösen, und es wird die gewünschte Form der Auflösung durch eine Kettenbruchentwickelung erreicht. Doch bei diesen Auflösungen bleibt immer die Schwierigkeit, es durch eine den willkürlichen Zahlen auferlegte Beschränkung zu erreichen, dass α gegen $\alpha,$, β gegen $\beta,$ relative Primzahl sei. Nur in den Fällen, wenn b entweder gegen a oder gegen a, oder gegen beide relative Primzahl ist, lässt sich dies leicht erreichen. In diesen Fällen gilt Folgendes:

(I.) Wenn b gegen a relative Primzahl ist, so sind folgendes zwei vollständige Lösungen der vorgelegten diophantischen Gleichung (die zugleich die Bedingung, dass α gegen $\alpha,$, β gegen $\beta,$ relative Primzahl sei, erfüllen):

$$\begin{aligned}
a &= \quad bd\beta, - b\beta,' &&= -(bb - a,a)\alpha, + d\alpha,' \\
a, &= -ad\beta, + a\beta,' &&= \quad \alpha, \\
\beta &= -(bb - a,a)\beta, - d,\beta,' &&= -bd,\alpha, - b\alpha,' \\
\beta, &= \quad \beta, &&= \quad ad,\alpha, + a\alpha,'
\end{aligned}$$

Hierin bezeichnet d.d, eine beliebige Zerlegung von D in zwei Factoren; ferner, wenn k die Anzahl der Glieder des in einen Kettenbruch verwandelten Bruches $\frac{b}{a}$ (die etwanigen Ganzen nicht mitgerechnet) bedeutet, sind für $(-1)^k b$ und $(-1)^k a$ resp. Zähler und Nenner des vorletzten Partialwerthes dieses Kettenbruchs zu setzen. $\beta,$ und $\beta,'$ resp $\alpha,$ und $\alpha,'$ können beliebige ganzzahlige Werthe annehmen, doch so, dass immer $d\beta,$ relative Primzahl gegen $\beta,'$ und $\beta,$ relative Primzahl gegen $d,\beta,'$, $d,\alpha,$ relative Primzahl gegen $\alpha,'$ und $\alpha,$ gegen $d\alpha,'$ ist. $\triangle = \alpha\beta, - \alpha,\beta$ ist für beide Lösungen eine quadratische Form von der Determinante $-D$, nämlich

$$\begin{aligned}
\triangle &= \{b - (bb - a,a)a\}d\beta,^2 - 2aD\beta,\beta,' + ad,\beta,'^2 \\
&= \{b - (bb - a,a)a\}d,\alpha,^2 + 2aD\alpha,\alpha,' + ad\alpha,'^2.\text{“}
\end{aligned}$$

(II.) „Wenn b gegen a, relative Primzahl ist, so sind folgendes zwei vollständige Lösungen

$$\begin{aligned}
\alpha &= \quad -a,d\beta - a,\beta' &&= \quad \alpha \\
\alpha, &= \quad b,d\beta + b\beta' &&= -(aa, - bb,)\alpha + d\alpha' \\
\beta &= \quad \beta &&= \quad a,d,\alpha - a,\alpha' \\
\beta &= -(aa, - bb,)\beta - d,\beta' &&= -b,d,\alpha + b\alpha',
\end{aligned}$$

wo d und d, die vorher angegebene Bedeutung haben, ferner, wenn k, die Anzahl der Glieder des in einen Kettenbruch verwandelten Bruches $\frac{a_,}{b_,}$ (die etwanigen Ganzen nicht mitgerechnet) bedeutet, für $(-1)^{k_,}a_,$ und $(-1)^{k_,}b_,$ resp. Zähler und Nenner des vorletzten Partialwerthes dieses Kettenbruchs zu setzen sind. β und β' resp. α und α' können beliebige ganzzahlige Werthe annehmen, doch so, dass immer β' relative Primzahl gegen $d\beta$, β gegen $d_,\beta'$, α' gegen $d_,\alpha$, α gegen $d\alpha'$ ist. $\triangle$ wird eine quadratische Form von der Determinante $-D$, nämlich

$$\triangle = \{(aa_, - bb_,)a_, - b_,\}d_,\beta^2 + 2a_,.D\beta\beta' + a_,d_,\beta'^2$$
$$= \{(aa_, - bb_,)a_, - b_,\}d_,\alpha^2 - 2a_,.D\alpha\alpha' + a_,d\alpha'^2.$$

(III.) „Wenn b sowohl gegen a als gegen a, relative Primzahl ist, so gelten (I.) und (II.) zugleich."

Bei diesen Lösungen ist die den willkürlichen Zahlen aufgelegte Beschränkung ganz analog der den Zahlen Φ und Ψ im Falle $b = o$ auferlegten. Die Transformationsformeln lauten immer

$$x = \alpha y + \beta y,$$
$$x, = \alpha, y + \beta, y,$$
$$ax^2 + 2bxx, + a,x,^2 = \triangle (dy^2 + d,y,^2).$$

Der Vorzug dieser Lösungen besteht darin, dass man, wenn a, b, a, numerisch gegeben sind, wirklich die Lösungen in Gruppen nach den verschiedenen Zerlegungen von D in zwei Factoren ordnen kann, während bei den Lösungen (1.) und (2.) d und d, für jedes Werthepaar der willkürlichen Zahlen einzeln als grösseste gemeinschaftliche Factoren bestimmt werden müssen.

Ich leite hier nur Lösung (I.) ab, da der Beweis für (II.) ganz analog ist. Aus den Gleichungen 1) in No. III. folgt

$$\frac{a\alpha + b\alpha,}{d} = \beta, \quad = \text{ganze Zahl},$$
$$\frac{b\alpha + a,\alpha,}{d} = -\beta = \text{ganze Zahl}.$$

Es ist die Aufgabe, wenn d einen bestimmten Factor von D bedeutet, diejenigen Werthepaare von α, α, anzugeben, für welche diese beiden Brüche ganze Zahlen werden, oder für welche die beiden Congruenzen erfüllt werden

$$a\alpha + b\alpha, \equiv o \pmod{d}$$
$$b\alpha + a,\alpha, \equiv o \pmod{d}.$$

Es ist aber leicht einzusehen, dass, wenn b relative Primzahl gegen a, die zweite Congruenz eine Folge der ersten ist. Wenn nämlich a und b relativ prim sind, so ist nothwendig a relative Primzahl gegen $aa, - b^2 = D$, also auch gegen jeden Factor d von D. Wenn nun

$$a\alpha + b\alpha, \equiv o \pmod{d},$$

so ist gewiss

$$ab\alpha + b^2\alpha, \equiv o \pmod{d},$$

d. h.

$$ab\alpha + (aa, - D)\alpha, \equiv o \pmod{d},$$

also, da $D\alpha, \equiv o \pmod{d}$ ist, auch

$$a(b\alpha + a,\alpha,) \equiv o \pmod{d}.$$

Da nun a relative Primzahl gegen d ist, so folgt hieraus

$$b\alpha + a,\alpha, \equiv o \pmod{d},$$

d. h. es ist, wie behauptet wurde, die zweite Congruenz erfüllt, wenn es die erste ist. Die Auflösung dieser Congruenz oder, was dasselbe ist, der diophantischen Gleichung $a\alpha + b\alpha, = d\beta$, ist aber

$$\alpha = \quad b.d\beta, - b\beta,'$$
$$\alpha, = -a\,d\beta, + a\beta,',$$

wo β, und $\beta_{,}'$ beliebige ganze Zahlen bedeuten, und $\mathfrak{b}$ und $\mathfrak{a}$ die Gleichung $a\mathfrak{b} - b\mathfrak{a} = 1$ erfüllen müssen. Es ist jedoch leicht einzusehen, dass die verschiedenen Werthepaare von $\mathfrak{b}$ und $\mathfrak{a}$ nichts wesentlich Verschiedenes geben, so dass die bei (I.) gegebene Definition von $\mathfrak{b}$ und $\mathfrak{a}$ statthaft ist. Es wird noch

$$\beta = -\frac{b\alpha + a_{,}\alpha_{,}}{d} = -(b\mathfrak{b} - a_{,}\mathfrak{a})\beta, + \frac{b^2 - aa_{,}}{d}\beta_{,}' = -(b\mathfrak{b} - a_{,}\mathfrak{a})\beta, - d_{,}\beta_{,}'.$$

Jeder gemeinschaftliche Factor von α und $\alpha_{,}$ ist auch gemeinschaftlicher Factor von $a\alpha + b\alpha_{,} = d\beta$, und $\mathfrak{a}\alpha + \mathfrak{b}\alpha_{,} = \beta_{,}'$, und umgekehrt; jeder gemeinschaftliche Factor von β und $\beta_{,}$ ist auch gemeinschaftlicher Factor von $\beta_{,}$ und $d_{,}\beta_{,}'$, und umgekehrt. Soll daher α gegen $\alpha_{,}$, β gegen $\beta_{,}$ relative Primzahl sein, so ist es nothwendig und hinreichend, dass $d\beta$, relative Primzahl gegen $\beta_{,}'$, β, gegen $d_{,}\beta_{,}'$ sei. — Endlich wird

$$\Delta = \frac{a\alpha^2 + 2b\alpha\alpha_{,} + a_{,}\alpha_{,}^2}{d} = (a\mathfrak{b}^2 - 2b\mathfrak{b}\mathfrak{a} + a_{,}\mathfrak{a}^2)d\beta_{,}^2 - 2aD\beta_{,}\beta_{,}' + ad_{,}\beta_{,}'^2$$
$$= \{b - (b\mathfrak{b} - a_{,}\mathfrak{a})\mathfrak{a}\}d\beta_{,}^2 - 2aD\beta_{,}\beta_{,}' + ad_{,}\beta_{,}'^2,$$

da $a\mathfrak{b} - b\mathfrak{a} = 1$ ist. Die Determiniante dieser quadratischen Form ist $\mathfrak{a}^2D^2 - ad_{,}d\{a\mathfrak{b}^2 - 2b\mathfrak{b}\mathfrak{a} + a_{,}\mathfrak{a}^2\}$ $= -D(a\mathfrak{b} - b\mathfrak{a})^2 = -D$. w, z. b. w. Die Transformationsformel $ax^2 + 2bxx_{,} + a_{,}x_{,}^2 = \Delta(dy^2 + d_{,}y_{,}^2)$ ist früher aus den Gleichungen 1) abgeleitet und gilt daher auch hier vermöge der Ableitung der Lösung (I.) aus denselben Gleichungen. Doch kann man sich auch a posteriori durch Rechnung davon überzeugen.

VI.

Es seien $\begin{pmatrix}\alpha, & \beta\\ \alpha_{,}, & \beta_{,}\end{pmatrix}$ und $\begin{pmatrix}\mathcal{A}, & B\\ \mathcal{A}_{,}, & B_{,}\end{pmatrix}$ irgend zwei Lösungen der vorgelegten Aufgabe, und zwar gehöre die erste Lösung zu der Zerlegung $D = d.d_{,}$, die letztere zu der Zerlegung $D = \mathfrak{D}.\mathfrak{D}_{,}$. Dann folgt mittelst der Gleichungen 1):

$$\begin{array}{l|l} a\alpha + b\alpha_{,} = \beta_{,}d & b\alpha + a_{,}\alpha_{,} = -\beta d \\ a\mathcal{A} + b\mathcal{A}_{,} = B_{,}\mathfrak{D} & b\mathcal{A} + a_{,}\mathcal{A}_{,} = -B\mathfrak{D} \\ \hline (\alpha\mathcal{A}_{,} - \alpha_{,}\mathcal{A})a = d\beta_{,}\mathcal{A}_{,} - \mathfrak{D}\alpha_{,}B_{,} & (\alpha\mathcal{A}_{,} - \alpha_{,}\mathcal{A})b = -d\beta\mathcal{A}_{,} + \mathfrak{D}\alpha_{,}B. \\ (\alpha\mathcal{A}_{,} - \alpha_{,}\mathcal{A})b = -d\beta_{,}\mathcal{A} + \mathfrak{D}\alpha B_{,} & (\alpha\mathcal{A}_{,} - \alpha_{,}\mathcal{A})a_{,} = d\beta\mathcal{A} - \mathfrak{D}\alpha B. \end{array}$$

Durch Gleichsetzung der beiden Werthe für b folgt

$$d(\beta\mathcal{A}_{,} - \beta_{,}\mathcal{A}) + \mathfrak{D}(\alpha B_{,} - \alpha_{,}B) = 0,$$

oder

$$\frac{\alpha B_{,} - \alpha_{,}B}{\beta\mathcal{A}_{,} - \beta_{,}\mathcal{A}} = -\frac{d}{\mathfrak{D}} = -\frac{\mathfrak{D}_{,}}{d_{,}} = -\sqrt{\left(\frac{d}{d_{,}}.\frac{\mathfrak{D}_{,}}{\mathfrak{D}}\right)}$$

Ferner folgt:

$$D = aa_{,} - b^2 = \frac{\begin{vmatrix} d\beta_{,}\mathcal{A}_{,} - \mathfrak{D}B_{,}\alpha, & , & -d\beta\mathcal{A}_{,} + \mathfrak{D}B\alpha_{,} \\ -d\beta_{,}\mathcal{A} + \mathfrak{D}B_{,}\alpha & , & d\beta\mathcal{A} - \mathfrak{D}B\alpha \end{vmatrix}}{(\alpha\mathcal{A}_{,} - \alpha_{,}\mathcal{A})^2} = d\mathfrak{D}.\frac{\beta B_{,} - \beta_{,}B}{\alpha A_{,} - \alpha_{,}\mathcal{A}}.$$

Oder, da $D = d.d_{,} = \mathfrak{D}.\mathfrak{D}_{,} = \sqrt{(d.d_{,}.\mathfrak{D}.\mathfrak{D}_{,})}$ ist:

$$\frac{\alpha\mathcal{A}_{,} - \alpha_{,}\mathcal{A}}{\beta B_{,} - \beta_{,}B} = \frac{d}{D_{,}} = \frac{D}{d_{,}} = \sqrt{\left(\frac{d}{d_{,}}.\frac{\mathfrak{D}}{\mathfrak{D}_{,}}\right)}$$

Es lässt sich zeigen, dass die beiden so erhaltenen Gleichungen

$$5)\quad \begin{cases} \dfrac{\alpha B_{,} - \alpha_{,}B}{d} + \dfrac{\beta\mathcal{A}_{,} - \beta_{,}\mathcal{A}}{\mathfrak{D}} = \dfrac{\alpha B_{,} - \alpha_{,}B}{\mathfrak{D}_{,}} + \dfrac{\beta\mathcal{A}_{,} - \beta_{,}\mathcal{A}}{d_{,}} = \dfrac{\alpha B_{,} - \alpha_{,}B}{\sqrt{(d\mathfrak{D}_{,})}} + \dfrac{\beta\mathcal{A}_{,} - \beta_{,}\mathcal{A}}{\sqrt{(d_{,}\mathfrak{D}\cdot)}} = 0, \\ \dfrac{\alpha\mathcal{A}_{,} - \alpha_{,}\mathcal{A}}{d} - \dfrac{\beta B_{,} - \beta_{,}B}{\mathfrak{D}_{,}} = \dfrac{\alpha\mathcal{A}_{,} - \alpha_{,}\mathcal{A}}{\mathfrak{D}} - \dfrac{\beta B_{,} - \beta_{,}B}{d_{,}} = \dfrac{\alpha\mathcal{A}_{,} - \alpha_{,}\mathcal{A}}{\sqrt{(d\mathfrak{D})}} - \dfrac{\beta B_{,} - \beta_{,}B}{\sqrt{(d_{,}\mathfrak{D}_{,})}} = 0, \end{cases}$$

nicht bloss nothwendig, sondern auch hinreichend sind, damit $\begin{pmatrix} \mathcal{A}, & B \\ \mathcal{A}_{,}, & B_{,} \end{pmatrix}$ eine Lösung sei, wenn $\begin{pmatrix} \alpha, & \beta \\ \alpha_{,}, & \beta_{,} \end{pmatrix}$ eine Lösung ist. Schreibt man nämlich die beiden Gleichungen in der Form

$$\mathfrak{D}(\alpha B_{,} - \alpha_{,} B) = -\,\mathrm{d}(\beta \mathcal{A}_{,} - \beta_{,} \mathcal{A}),$$
$$\mathfrak{D}(\beta B_{,} - \beta_{,} B) = \quad \mathrm{d}_{,}(\alpha \mathcal{A}_{,} - \alpha_{,} \mathcal{A}),$$

und löst dieselben nach B und $B_{,}$ auf, so erhält man

$$-\,\mathfrak{D}(\alpha\beta_{,} - \alpha_{,}\beta).B_{,} = \mathrm{d}(\beta \mathcal{A}_{,} - \beta_{,} \mathcal{A})\,\beta_{,} + \mathrm{d}_{,}(\alpha \mathcal{A}_{,} - \alpha_{,} \mathcal{A}).\alpha_{,},$$
$$-\,\mathfrak{D}(\alpha\beta_{,} - \alpha_{,}\beta).B = \mathrm{d}(\beta \mathcal{A}_{,} - \beta_{,} \mathcal{A}).\beta + \mathrm{d}_{,}(\alpha \mathcal{A}_{,} - \alpha_{,} \mathcal{A}).\alpha.$$

Da aber $\begin{pmatrix} \alpha, & \beta \\ \alpha_{,}, & \beta_{,} \end{pmatrix}$ eine Lösung sein soll, so ist identisch

$$\beta_{,} = \frac{\mathrm{a}\alpha + \mathrm{b}\alpha_{,}}{\mathrm{d}}, \quad \alpha_{,} = -\,\frac{\alpha\beta + \mathrm{b}\beta_{,}}{\mathrm{d}_{,}}, \quad \beta = -\,\frac{\mathrm{b}\alpha + \mathrm{a}_{,}\alpha_{,}}{\mathrm{d}}, \quad \alpha = \frac{\mathrm{b}\beta + \mathrm{a}_{,}\beta_{,}}{\mathrm{d}_{,}}.$$

Mithin wird

$$\begin{aligned} -\,\mathfrak{D}(\alpha\beta_{,} - \alpha_{,}\beta).B_{,} &= (\beta \mathcal{A}_{,} - \beta_{,} \mathcal{A})(\mathrm{a}\alpha + \mathrm{b}\alpha_{,}) - (\alpha \mathcal{A}_{,} - \alpha_{,} \mathcal{A})(\mathrm{a}\beta + \mathrm{b}\beta_{,}) \\ &= -\,(\alpha\beta_{,} - \alpha_{,}\beta)(\mathrm{a}\mathcal{A} + \mathrm{b}\mathcal{A}_{,}) \\ -\,\mathfrak{D}(\alpha\beta_{,} - \alpha_{,}\beta).B &= -\,(\beta \mathcal{A}_{,} - \beta_{,} \mathcal{A})(\mathrm{b}\alpha + \mathrm{a}_{,}\alpha_{,}) + (\alpha \mathcal{A}_{,} - \alpha_{,} \mathcal{A})(\mathrm{b}\beta + \mathrm{a}_{,}\beta_{,}) \\ &= \quad (\alpha\beta_{,} - \alpha_{,}\beta)(\mathrm{b}\mathcal{A} + \mathrm{a}_{,}\mathcal{A}_{,}), \end{aligned}$$

d. h.

$$B_{,} = \frac{\mathrm{a}\mathcal{A} + \mathrm{b}\mathcal{A}_{,}}{\mathfrak{D}}, \quad B = -\,\frac{\mathrm{b}\mathcal{A} + \mathrm{a}_{,}\mathcal{A}_{,}}{\mathfrak{D}}.$$

Mithin ist, wie behauptet wurde, $\begin{pmatrix} \mathcal{A}, & B \\ \mathcal{A}_{,}, & B_{,} \end{pmatrix}$ auch eine Lösung, wenn $\begin{pmatrix} \alpha, & \beta \\ \alpha_{,}, & \beta_{,} \end{pmatrix}$ eine Lösung ist und $\mathcal{A}$, B, $\mathcal{A}_{,}$, $B_{,}$, aus den Gleichungen 5) so bestimmt werden, dass $\mathcal{A}$ gegen $\mathcal{A}_{,}$, B gegen B relative Primzahl ist. Es sei übrigens bemerkt, dass die Gleichungen 5) sich auch in folgende elegantere Form bringen lassen:

$$\frac{(\alpha \mathcal{A}_{,} - \alpha_{,} \mathcal{A})(\alpha B_{,} - \alpha_{,} B)}{\mathrm{d}} + \frac{(\beta \mathcal{A}_{,} - \beta_{,} \mathcal{A})(\beta B_{,} - \beta_{,} B)}{\mathrm{d}_{,}} = 0,$$

$$5') \quad \frac{(\mathcal{A}\alpha_{,} - \mathcal{A}_{,}\alpha)(\mathcal{A}\beta_{,} - \mathcal{A}_{,}\beta)}{\mathfrak{D}} + \frac{(B\alpha_{,} - B_{,}\alpha)(B\beta_{,} - B_{,}\beta)}{\mathfrak{D}_{,}} = 0.$$

Es werde für den Augenblick der grösseste gemeinschaftliche Factor irgend zweier ganzen Zahlen p und q durch [p, q] bezeichnet. Bezeichnet man dann ferner

$$\frac{\mathfrak{D}}{[\mathfrak{D}, \mathrm{d}]} = \frac{\mathrm{d}_{,}}{[\mathrm{d}_{,}, \mathfrak{D}_{,}]} = \mathrm{d}_{,}', \quad \frac{\mathfrak{D}}{[\mathfrak{D}, \mathrm{d}_{,}]} = \frac{\mathrm{d}}{[\mathrm{d}, \mathfrak{D}_{,}]} = \mathrm{d}',$$

$$\frac{\mathfrak{D}_{,}}{[\mathfrak{D}_{,}, \mathrm{d}]} = \frac{\mathrm{d}_{,}}{[\mathrm{d}_{,}, \mathfrak{D}]} = \mathrm{d}_{,}'', \quad \frac{\mathfrak{D}_{,}}{[\mathfrak{D}_{,}, \mathrm{d}_{,}]} = \frac{\mathrm{d}}{[\mathrm{d}, \mathfrak{D}]} = \mathrm{d}'',$$

so folgt aus den Gleichungen 5):

$$6) \quad \begin{aligned} -\,(\beta \mathcal{A}_{,} - \beta_{,} \mathcal{A}) &= \mathrm{d}_{,}' \Phi, & -\,(\beta B_{,} - \beta_{,} B) &= \mathrm{d}_{,}'' \Psi, \\ \alpha \mathcal{A}_{,} - \alpha_{,} \mathcal{A} &= -\,\mathrm{d}' \Psi, & \alpha B_{,} - \alpha_{,} B &= \mathrm{d}'' \Phi, \end{aligned}$$

wo Φ und Ψ ganze Zahlen bedeuten. Endlich folgt noch

$$\begin{aligned} 7) \quad (\alpha\beta_{,} - \alpha_{,}\beta)(\mathcal{A}B_{,} - \mathcal{A}_{,}B) &= (\alpha \mathcal{A}_{,} - \alpha_{,} \mathcal{A})(\beta B_{,} - \beta_{,} B) - (\alpha B_{,} - \alpha_{,} B)(\beta \mathcal{A}_{,} - \beta_{,} \mathcal{A}) \\ &= \mathrm{d}_{,}' \mathrm{d}'' \Phi^2 + \mathrm{d}_{,}'' \mathrm{d}' \Psi^2. \end{aligned}$$

Bedenkt man nun noch, dass aus

$$\mathrm{x} = \alpha \mathrm{y} + \beta \mathrm{y}_{,} = \mathcal{A} Y + B Y_{,}$$
$$\mathrm{x}_{,} = \alpha_{,} \mathrm{y} + \beta_{,} \mathrm{y}_{,} = \mathcal{A}_{,} Y + B_{,} Y_{,}$$

folgt

$$8\begin{cases}(\alpha\beta_{,}-\alpha_{,}\beta)y = -(\beta\mathcal{A}_{,}-\beta_{,}\mathcal{A})Y-(\beta B_{,}-\beta_{,}B)Y_{,} = \quad d_{,}'\Phi Y + d_{,}''\Psi Y,\\ (\alpha\beta_{,}-\alpha_{,}\beta)y_{,} = \quad (\alpha\mathcal{A}_{,}-\alpha_{,}\mathcal{A})Y+(\alpha B_{,}-\alpha_{,}B)Y_{,} = -d'\Psi Y + d''\Phi Y_{,},\end{cases}$$

so kann die Analogie mit den Formeln für den Fall b = o, wie sie sich in No. I. finden, nicht verborgen bleiben. Ganz vollständig wird dieselbe allerdings erst, wenn man auch dort **irgend** zwei Lösungen mit einander in Verbindung setzt und a', a'', $a_{,}'$, $a_{,}''$ etwas anders definirt, als es dort geschehen ist. Die Definition dieser Zahlen in der zweiten Fassung der Lösung war dort folgende

$$a_{,}' = [a_{,}, A] \quad , \quad a' = [a, A]$$
$$a_{,}'' = [a_{,}, A_{,}] \quad , \quad a'' = [a, A_{,}]$$

Da $a.a_{,} = A.A_{,} = D$, so kann man aber a', a'', $a_{,}'$, $a_{,}''$ auch so definiren:

$$a_{,}' = \frac{A}{[A, a]} = \frac{a_{,}}{[a_{,}, A_{,}]} \quad , \quad a' = \frac{A}{[A, a_{,}]} = \frac{a}{[a, A_{,}]}$$
$$a_{,}'' = \frac{A_{,}}{[A_{,}, a]} = \frac{a_{,}}{[a_{,}, A]} \quad , \quad a'' = \frac{A_{,}}{[A_{,}, a_{,}]} = \frac{a}{[a, A]}$$

Diese Definition ist vollständig conform derjenigen von $d_{,}$, d'', $d_{,}'$, $d_{,}''$. In den Fällen übrigens, dass entweder $[d, d_{,}] = 1$ oder $[\mathfrak{D}, \mathfrak{D}_{,}] = 1$ oder auch $[d, d_{,}] = [\mathfrak{D}, \mathfrak{D}_{,}] = 1$ ist, hat man

$$\begin{matrix}[\mathfrak{D}, d].[\mathfrak{D}, d_{,}] = \mathfrak{D}\\ [\mathfrak{D}_{,}, d].[\mathfrak{D}_{,}, d_{,}] = \mathfrak{D}_{,}\end{matrix} \text{ resp. } \begin{matrix}[d, \mathfrak{D}].[d, \mathfrak{D}_{,}] = d\\ [d_{,}, \mathfrak{D}].[d_{,}, \mathfrak{D}_{,}] = d_{,}\end{matrix} \text{ resp. Beides,}$$

und es wird

$$d_{,}' = [d_{,}, \mathfrak{D}] \quad , \quad d_{,} = [d, \mathfrak{D}]$$
$$d_{,}'' = [d_{,}, \mathfrak{D}_{,}] \quad , \quad d'' = [d, \mathfrak{D}_{,}]$$

In diesen Fällen ist auch $d'd''d_{,}'d_{,}'' = d.d_{,} = \mathfrak{D}.\mathfrak{D}_{,} = D$, gerade wie im Falle b = o $a'a''a_{,}'a_{,}'' = a.a_{,} = A.A_{,} = D$ war.

VII.

Aus den von mir gegebenen Lösungen und Formeln ergeben sich unmittelbar einige zahlentheoretische Folgerungen, die ich hiemit anschliesse.

Folgerung I. Ist D irgend eine ganze Zahl und sind durch irgend eine Form von der Determinante — D zwei verschiedene Potenzen, m^{π} und $m^{\pi + \Pi}$, einer und derselben ganzen Zahl m ohne gemeinschaftlichen Factor mit D in relativen Primzahlen darstellbar, so ist mindestens **eine** Potenz von m zwischen m^{Π} und $m^{2\pi + \Pi}$ durch die Form (1, 0, D) in relativen Primzahlen darstellbar.

Beweis. Sind m^{π} und $m^{\pi + \Pi}$ durch die Form (a, b, $a_{,}$) von der Determinante — D in relativen Primzahlen darstellbar, so kann man zufolge Auflösung (2.), da nach Voraussetzung m relative Primzahl gegen D also auch gegen n ist, setzen.

$$\alpha\beta_{,} - \alpha_{,}\beta = m^{\pi} \quad , \quad \mathcal{A}B_{,} - \mathcal{A}_{,}B = m^{\pi + \Pi}.$$

Hier entspricht m^{π} resp. $m^{\pi + \Pi}$ dem m in Auflösung (2.), d und $\mathfrak{D}$ sind gleich 1, mithin $d_{,} = \mathfrak{D}_{,} = D$. Danach folgt aus No. VI.

$$d_{,}' = 1, \; d' = 1, \; d_{,}'' = D, \; d'' = 1,$$

und weiter mit Hülfe von Form 7):

$$(\alpha\beta_{,} - \alpha_{,}\beta)(\mathcal{A}B_{,} - \mathcal{A}_{,}B) = m^{2\pi + \Pi} = \Phi^2 + D\Psi^2.$$

Mit Rücksicht darauf, dass α gegen $\alpha_,$, β gegen $\beta_,$, A gegen $A_,$, B gegen $B_,$ relative Primzahl ist, folgt aber aus den Gleichungen 6), dass jeder gemeinschaftliche Factor von Φ und Ψ auch gemeinschaftlicher Factor von $\alpha\beta_, - \alpha_,\beta$ und $AB_, - A_,B$ sein muss (jedoch nicht umgekehrt.) Daher kann der grösseste gemeinschaftliche Factor von Φ und Ψ höchstens m^{π} sein, und es bleibt immer noch eine Potenz von m, deren Exponent $\leqq 2\pi + \Pi$ und $\geqq \Pi$ ist, durch die Form (1, 0, D) in relativen Primzahlen darstellbar.

Anmerkung. Auf andere Weise lässt sich Folgerung I. folgendermaassen beweisen: Sind m^{π} und $m^{\pi+\Pi}$ durch (a, b, a,) in relativen Primzahlen darstellbar, so ist (a, b, a,) transformirbar in die äquivalente Form $\left(m\pi, n, \frac{n^2 + D}{m^{\pi}}\right)$. Durch diese ist, weil sie eben der Form (a, b, a,) äquivalent ist, $m^{\pi+\Pi}$ in relativen Primzahlen darstellbar, also

$$m^{\pi+\Pi} = m^{\pi}\psi^2 + 2n\psi\psi_, + \frac{n^2 + D}{m^{\pi}}\psi_,^2$$

$$= \frac{1}{m^{\pi}}\left[\left(m^{\pi}\psi + n\psi_,\right)^2 + D\psi_,^2\right]$$

$$= \frac{1}{m^{\pi}}\left[\psi'^2 + D\psi_,^2\right],$$

mithin $m^{2\pi+\Pi} = \psi'^2 + D\psi_,^2$.

Da ψ und $\psi_,$ relative Primzahlen sind, so ist der grösseste gemeinschaftliche Factor von $\psi_,$ und ψ' gleich dem grössesten gemeinschaftlichen Factor von $\psi_,$ und m^{π}, mithin höchstens m^{π}, womit der Beweis geliefert ist.

Folgerung II. Ist D eine positive ganze Zahl von der Form $8n - 1$, so ist (ausser der stets durch die Form (1, o, D) darstellbaren Potenz 2^0) immer wenigstens **eine** Potenz von zwei durch die Form (1, o, D) in relativen Primzahlen darstellbar. Und zwar ist der Exponent der niedrigsten durch die Form (1, o, D) in relativen Primzahlen darstellbaren Potenz von 2 stets $\leqq 2H - 1$, wo H die Classenanzahl der Formen von der Determinante $-D$ bedeutet. — Das hier von 2 Gesagte gilt von jeder Potenz von 2, z. B. 4, 8, 16.

Beweis. Ist D eine positive ganze Zahl von der Form $8n - 1$, so ist (vgl. u. A. Dirichlet's Vorlesungen über Zahlentheorie) jede Potenz von 2 durch wenigstens **eine** Formenclasse von der Determinante $-D$ in relativen Primzahlen darstellbar. Nun wird entweder wenigstens eine, oder es wird keine der H Potenzen $2, 2^2, \ldots\ldots 2^H$ durch die Form (1, o, D) dargestellt. Im ersteren Falle ist der Beweis geliefert. Im zweiten Falle muss wenigstens eine der $H - 1$ mit der Form (1, o, D) nicht äquivalenten Formenclassen zwei der Potenzen $2, 2^2 \ldots\ldots 2^H$ darstellen, und der ungünstigste Fall ist der, dass diese beiden Potenzen die beiden höchsten, 2^{H-1} und 2^H, sind; in diesem Falle ist (vgl. Folgerung I.) $\pi = H - 1$, $\pi + \Pi = H$, mithin $2\pi + \Pi = 2H - 1$, q. d. e. — Aus dem ersten Satze des Beweises folgt nunmehr unmittelbar, dass diese Gleichung auch für jede Potenz von 2 gilt.

Folgerung III. Ist D eine durch die ungerade Primzahl p nicht theilbare ganze Zahl und zugleich $-D$ quadratischer Rest von p, so ist (ausser p^0) immer wenigstens **eine** Potenz von p durch die Form (1, o, D) in relativen Primzahlen darstellbar. Und zwar ist der Exponent der niedrigsten durch die Form (1, 0, D) in relativen Primzahlen darstellbaren Potenz

von p stets $\leqq 2H-1$, wo H die Classenanzahl der Formen von der Determinante $-D$ bedeutet. — Dasselbe, als von p, gilt von jeder Potenz von p.

Beweis geschieht entsprechend wie der von Folgerung II., mit Hülfe des Satzes, dass, wenn p eine ungerade Primzahl ist, jede Zahl, die quadratischer Rest zu p ist, auch quadratischer Rest zu p^{ν} ist (wo ν irgend eine positive ganze Zahl bedeutet), und dass daher jede Potenz von p durch wenigstens **eine** Formenclasse von der Determinante $-D$ darstellbar ist, wenn $-D$ quadratischer Rest von p.

Folgerung IV. Bedeutet D irgend eine ganze Zahl, m eine ganze Zahl ohne gemeinschaftlichen Factor mit D, und ist die Potenz m^{Π} durch die Form (1, o, D), die Potenz m^{π}, wo $\pi \leqq \Pi$, durch **irgend** eine Form von der Determinante $-D$ in relativen Primzahlen darstellbar, so ist durch die letztere Form auch wenigstens eine der Potenzen von m zwischen $m^{\Pi-\pi}$ und $m^{\Pi+\pi}$ (diese Grenzen mit eingeschlossen) in relativen Primzahlen darstellbar.

Beweis. Es sei (a, b, a,) die m^{π} in relativen Primzahlen darstellende Form; dann sind nach Auflösung (2.) immer Lösungen $\begin{pmatrix}\alpha, & \beta\\ \alpha_{,}, & \beta_{,}\end{pmatrix}$ zu finden von der Art, dass $\alpha\beta_{,} - \alpha_{,}\beta = m^{\pi}$ ist; für eine solche Lösung ist $d = 1$, $d_{,} = D$. Ferner ist nach Voraussetzung

$$m^{\Pi} = \Phi_{,}^{2} + D\Psi_{,}^{2},$$

wo $\Phi_{,}$ und Ψ relative Primzahlen. Ich benutze nun die Formeln 5) 6) 7) in No. VI. Dort ist bewiesen, dass $\begin{pmatrix}\mathcal{A}, & B\\ \mathcal{A}_{,}, & B_{,}\end{pmatrix}$ eine Lösung ist, wenn $\begin{pmatrix}\alpha, & \beta\\ \alpha_{,}, & \beta_{,}\end{pmatrix}$ eine Lösung ist und $\mathcal{A}$, B, $\mathcal{A}_{,}$, $B_{,}$ aus den Formeln 5) bestimmt werden. Da aber die Formeln 6) aus den Formeln 5) folgen und umgekehrt, so gilt dasselbe von den Formeln 6). Ich setze nun in den Formeln 6):

$$d = 1,\ d_{,} = D,\ \mathfrak{D} = 1,\ \mathfrak{D}_{,} = D,\ \Phi = \Phi_{,}F,\ \Psi = \Psi_{,}F.$$

Dann wird, da hier $[d, d_{,}] = [\mathfrak{D}, \mathfrak{D}_{,}] = 1$ ist,

$$d_{,}' = [D, 1] = 1 \quad , \quad d_{,}'' = [D, D] = D$$
$$d' = [1, 1] = 1 \quad , \quad d'' = [1, D] = 1,$$

mithin werden die Formeln 6):

$$-(\beta\mathcal{A}_{,} - \beta_{,}\mathcal{A}) = \Phi_{,}F \qquad -(\beta B_{,} - \beta_{,}B) = D\Psi_{,}F$$
$$\alpha\mathcal{A}_{,} - \alpha_{,}\mathcal{A} = -\Psi_{,}F \quad , \qquad \alpha B_{,} - \alpha_{,}B = \Phi_{,}F.$$

Hierin wähle ich für F die kleinste ganze Zahl, welche bewirkt, dass für $\mathcal{A}$, B, $\mathcal{A}_{,}$, $B_{,}$ aus diesen Gleichungen sich ganzzahlige Werthe ergeben; danach ist F nothwendig ein Factor von $\alpha\beta_{,} - \alpha_{,}\beta$. Es wird dann von selbst auch $\mathcal{A}$ gegen $\mathcal{A}_{,}$, B gegen $B_{,}$ relative Primzahl. Denn jeder gemeinschaftliche Factor $\mathcal{A}$ und $\mathcal{A}_{,}$ muss auch gemeinschaftlicher Factor von $\alpha\mathcal{A}_{,} - \alpha_{,}\mathcal{A}$ und $\beta\mathcal{A}_{,} - \beta_{,}\mathcal{A}$ sein, also, da $\Phi_{,}$ gegen $\Psi_{,}$ relative Primzahl ist, Factor von F; F wird aber durch die Division mit $\alpha\beta_{,} - \alpha_{,}\beta$ fortgeschafft. Jeder gemeinschaftliche Factor von B und $B_{,}$ muss auch gemeinschaftlicher Factor von $\beta B_{,} - \beta_{,}B$ und $\alpha B_{,} - \alpha_{,}B$ d. h. von $D\Psi_{,}F$ und $\Phi_{,}F$ sein; nun muss D gegen $\Phi_{,}$ relative Primzahl sein, weil sonst m^{Π}, also auch m einen gemeinschaftlichen Factor mit D hätte, was gegen die Voraussetzung wäre; also auch $D\Psi_{,}$ gegen $\Phi_{,}$ relative Primzahl und jeder gemeinschaftliche Factor von $\beta B_{,} - \beta_{,}B$ und $\alpha B_{,} - \alpha_{,}B$ mithin Factor von F; F wird aber durch die Division mit $\alpha\beta_{,} - \alpha_{,}\beta$ aufgehoben.

Zufolge Formel 7) wird nun

$$(\alpha\beta_{,} - \alpha_{,}\beta)(\mathcal{A}B_{,} - \mathcal{A}_{,}B) = (\Phi_{,}^{2} + D\Psi_{,}^{2})\ F^{2} = m^{\Pi}.F^{2}.$$

Es ist aber

$$\alpha\beta_{,} - \alpha_{,}\beta = m^{\pi}, \quad AB_{,} - A_{,}B = aA^2 + 2bAA_{,} + a_{,}A_{,}^2,$$

also

$$aA^2 + 2bAA_{,} + a_{,}A^2 = m^{\Pi - \pi} \cdot F^2.$$

Nun ist F, als Factor von $\alpha\beta_{,} - \alpha_{,}\beta$, mindestens 1 und höchstens m^{π}, womit der Beweis geliefert ist.

So wie Folgerung II. und III. mit Hülfe von Folgerung I. folgten, lassen sich aus IV. noch zwei ähnliche Folgerungen ableiten. Doch ich übergehe dieselben, da ihre Aufstellung und ihr Beweis nicht die geringste Schwierigkeit bieten, und schliesse diese Arbeit mit der Bemerkung, dass insbesondere die Folgerungen II. und III. es sind, welche eine interessante Anwendung auf die Transformation der elliptischen Functionen und besonders die Aufstellung der Modulargleichungen in der irrationalen Form, wie sie von Jacobi für den 3. und 5. Grad in § 30 der Fundamenta nova etc. und von Prof. Schrœter in seiner Inaugural-Dissertation (De aequationibus modularibus, Königsberg 1854) für alle Primzahl-Grade bis zum 31. incl. angegeben ist, zulassen. Es würde über die Grenzen des dieser Abhandlung gewährten Raumes hinausgehen, wenn ich über diese Anwendung selbst, welche auf einer Umformung der durch Multiplikation zweier Θ Functionen mit verschiedenen Moduln entstehenden unendlichen Doppelreihen beruht, auch nur eine oberflächliche Andeutung noch hinzufügen wollte.

E. Hübner.