8.

Untersuchungen über die cubischen Formen mit zwei Variabeln.

(Von Herrn Stud. *Gotth. Eisenstein* zu Berlin.)

Erste Abtheilung.

§. 1.

Jeder Ausdruck von der Form

$$1. \quad ax^3+3bx^2y+3cxy^2+dy^3 = (a, b, c, d) = f,$$

in welchem a, b, c, d gegebene, x, y unbestimmte ganze Zahlen vorstellen, heifst eine ***cubische Form.***

Bezeichnet man die Coëfficientenverbindungen

$$2. \quad b^2-ac, \quad bc-ad, \quad c^2-bd$$

respective durch

$$A, \qquad B, \qquad C,$$

so heifst die quadratische Form

$$3. \quad Ax^2+Bxy+Cy^2 = F$$

die ***determinirende Form*** der cubischen Form f. Endlich nenne ich die Determinante der quadratischen Form $2F$, nämlich

$$4. \quad B^2-4AC = D\ ^*),$$

die ***Determinante*** der cubischen Form f. Diese Determinante kann auf folgende Art in die Coëfficienten der cubischen Form ausgedrückt werden:

$$5. \quad D = (bc-ad)^2-4(b^2-ac)(c^2-bd)$$
$$= a^2d^2-3b^2c^2+4ac^3+4db^3-6abcd.$$

Die Determinante D ist genau diejenige Verbindung, von deren Vorzeichen es abhängt, ob die Gleichung

$$ax^3+3bx^2+3cx+d = 0$$

nur eine oder drei reelle Wurzeln hat.

Wird ω der gröfste gemeinschaftliche Theiler von a, b, c, d genannt, ω_1 der von $a, 3b, 3c, d$ und Ω der von $A, B, C,$ so ist ω^2, wie man aus den Gleichungen (2.) sieht, immer ein Theiler von Ω, während Ω^2 und

*) Nach *Gaufs* ist D die Determinante der Form $2F = 2Ax^2+2Bxy+2Cy^2$.

ω^4 wiederum Theiler von D sind. So oft also D keinen biquadratischen Theiler hat, können auch a, b, c, d keinen gemeinschaftlichen Theiler haben.

§. 2.

Wendet man auf die cubische Form

$$f = ax^3 + 3bx^2y + 3cxy^2 + dy^3$$

die Substitution

$$6. \quad x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y' \quad \begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$$

an, und ordnet das Resultat nach den neuen Variabeln x' und y', so erhält man die neue cubische Form

$$f' = a'x'^3 + 3b'x'^2y' + 3c'x'y'^2 + d'y'^3,$$

deren Coëfficienten a', b', c', d' auf folgende Art durch die alten Coëfficienten a, b, c, d ausgedrückt werden können:

$$7. \quad \begin{cases} a' = a\alpha^3 + 3b\alpha^2\gamma + 3c\alpha\gamma^2 + d\gamma^3, \\ b' = a\alpha^2\beta + b(\alpha^2\delta + 2\alpha\beta\gamma) + c(2\alpha\gamma\delta + \beta\gamma^2) + d\gamma^2\delta, \\ c' = a\alpha\beta^2 + b(\beta^2\gamma + 2\alpha\beta\delta) + c(2\beta\gamma\delta + \alpha\delta^2) + d\gamma\delta^2, \\ d' = a\beta^3 + 3b\beta^2\delta + 3c\beta\delta^2 + d\delta^3. \end{cases}$$

Die Form f' heifst unter der Form f enthalten, weil jede durch f' darstellbare Zahl auch durch f darstellbar ist; aber nicht umgekehrt.

Die Transformation $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$ heifst eine eigentliche oder uneigentliche Transformation, je nachdem $\alpha\delta - \beta\gamma$, welches durch ε bezeichnet sein mag, positiv oder negativ ist.

Die Gleichungen (6.),

$$\alpha x' + \beta y' = x \quad \text{und} \quad \gamma x' + \delta y' = y,$$

nach x und y aufgelöset, geben

$$x' = \frac{\delta x - \beta y}{\varepsilon}, \qquad y' = \frac{-\gamma x + \delta y}{\varepsilon}.$$

Ist daher

$$7. \quad \alpha\delta - \beta\gamma = \varepsilon = \pm 1,$$

so hat man zugleich eine Transformation von f' in f, nämlich die folgende:

$$\begin{pmatrix} \delta, -\beta \\ -\beta, \alpha \end{pmatrix}.$$

In diesem Falle enthalten also die beiden Formen f und f' einander gegenseitig und heifsen aequivalente cubische Formen; und zwar wird ihre Aequivalenz eine eigentliche oder uneigentliche genannt, je nachdem

$$\alpha\delta - \beta\gamma = +1, \quad \text{oder} \quad \alpha\delta - \beta\gamma = -1 \text{ ist.}$$

Es ist nun leicht, foldende Sätze zu beweisen:

„Wenn die Form f die Form f', und f' die f'' enthält, so enthält auch die f die f''."

„Wenn f und f', so wie f' und f'' aequivalente Formen sind, so sind auch f und f'' aequivalent" u. s. w.

Diese Sätze und ihre Beweise sind durchaus analog den entsprechenden für die quadratischen Formen; ich halte mich deshalb nicht bei denselben auf, da es mir nur besonders darauf ankomut, das den cubischen Formen Eigenthümliche und Characteristische hervorzuheben.

„Sind f und f' aequivalent, welches ich so bezeichne:

$$f \sim f',$$

so sind sowohl die ω als die ω_1 für beide dieselben." Dies ergiebt sich aus dem blofsen Anblick der Gleichungen (7.) und der ihnen entsprechenden beim Übergange von f' zu f.

Eine cubische Form bildet mit der Gesammtheit aller ihr aequivalenter cubischer Formen eine ***Classe*** cubischer Formen.

Für jede Classe aequivalenter cubischer Formen haben ω und ω_1 einen ganz bestimmten Werth.

§. 3.

Lehrsatz. „Enthält eine cubische Form f eine zweite f', und geht sie durch die Transformation $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ in f' über, so enthält auch die determinirende Form F der cubischen Form f, die determinirende Form F' der Form f', und zwar geht F durch die Transformation

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

in F' über; und sind die beiden cubischen Formen aequivalent, so sind es auch die determinirenden Formen; und zwar gehen die letzteren durch dieselbe Transformation in einander über; wie die ersteren."

Beweis. Wenn man die Coëfficienten der determinirenden Form F', nämlich

$$b'^2 - a'c', \quad b'c' - a'd', \quad c'^2 - b'd'$$

vermittels der Gleichungen (7.) in die Coëfficienten der cubischen Form f, nämlich a, b, c, d ausdrückt, so findet man, nach den nöthigen Reductionen,

$$b'^2 - a'c' = \varepsilon^2[(b^2 - ac)\alpha^2 + (bc - ad)\alpha\gamma + (c^2 - bd)\gamma^2],$$
$$b'c' - a'd' = \varepsilon^2[2(b^2 - ac)\alpha\beta + (bc - ad)(\alpha\delta + \beta\gamma) + 2(c^2 - bd)\gamma\delta],$$
$$c'^2 - b'd' = \varepsilon^2[(b^2 - ac)\beta^2 + (bc - ad)\beta\delta + (c^2 - bd)\delta^2].$$

Diese Gleichungen lassen sich, wenn A', B', C' die Coëfficienten von F vorstellen, folgendermaafsen schreiben:

$$9. \quad \begin{cases} A' = A(\alpha\varepsilon)^2 + B\alpha\varepsilon.\gamma\varepsilon + C(\gamma\varepsilon)^2, \\ B' = 2A\alpha\varepsilon.\beta\varepsilon + B(\alpha\varepsilon.\delta\varepsilon + \beta\varepsilon.\gamma\varepsilon) + 2C\gamma\varepsilon.\delta\varepsilon, \\ C' = A(\beta\varepsilon)^2 + B\beta\varepsilon.\delta\varepsilon + C(\delta\varepsilon)^2. \end{cases}$$

Dieselben Gleichungen findet man aber merkwürdigerweise ebenfalls, wenn man auf die Form

$$F = Ax^2 + Bxy + Cy^3$$

die Substitution

$$10. \quad x = \alpha\varepsilon.x' + \beta\varepsilon.y', \quad y = \gamma\varepsilon.x' + \delta\varepsilon.y', \quad \text{d. h.} \quad \begin{pmatrix} \alpha\varepsilon, & \beta\varepsilon \\ \gamma\varepsilon, & \delta\varepsilon \end{pmatrix}$$

anwendet und die Coëfficienten der neuen quadratischen Form durch A', B', C' bezeichnet. Also geht in der That die Form F durch die Substitution

$$\begin{pmatrix} \alpha\varepsilon, & \beta\varepsilon \\ \gamma\varepsilon, & \delta\varepsilon \end{pmatrix}$$

in die Form F' über. Ist nun speciell $\varepsilon = 1$, sind also f und f' eigentlich aequivalent, so sind auch F und F' aequivalent und gehen durch die Substitution

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

in einander über. Ist hingegen $\varepsilon = -1$, so hat man die Transformation $\begin{pmatrix} -\alpha, & -\beta \\ -\gamma, & -\delta \end{pmatrix}$ beim Übergange von F zu F'; und diese kann durch die andere $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ ersetzt werden: folglich sind F und F' mit f und f' zugleich uneigentlich aequivalent.

Bezeichnet man die Determinanten von f und f', nämlich die Verbindungen

$$a^2d^2 - 3b^2c^2 + 4ac^3 + 4db^3 - 6abcd \quad \text{und}$$
$$a'^2d'^2 - 3b'^2c'^2 + 4a'c'^3 + 4d'b'^3 - 6a'b'c'd'$$

durch D und D', so hat man, wie sich aus dem obigen Beweise mit ergiebt, die höchst einfache Relation

$$11. \quad D' = (\alpha\delta - \beta\gamma)^6.D,$$

mithin für den Fall der Aequivalenz:

$$D' = D.$$

„*Also haben aequivalente cubische Formen aequivalente determinirende Formen und dieselbe Determinante.*"

Der eben bewiesene Satz kann als ein Fundamentalsatz für die Theorie der cubischen Formen angesehen werden, denn er begründet eine höchst einfache Eintheilung und Classificirung sämmtlicher cubischen Formen. In der

That: da alle Formen derselben Classe dieselbe Determinante haben, so zerfallen alle möglichen cubischen Formen, die zu einer gegebenen Determinante D gehören, in eine bestimmte Anzahl K von Classen, die auch Null sein könnte, wenn es etwa gar keine cubischen Formen mit der Determinante D geben sollte. Betrachtet man nun wiederum die sämmtlichen zur Determinante $D = B^2 - 4AC$ gehörigen quadratischen Formen

$$Ax^2 + Bxy + Cy^2,$$

so constituiren diese ebenfalls eine Anzahl h von Classen

$$\Gamma_1, \quad \Gamma_2, \quad \Gamma_3, \quad \ldots \ldots \quad \Gamma_h,$$

welche nach *Dirichlet's* genialen Untersuchungen für eine negative Determinante von der Anzahl der Quadratreste für den Modul D abhängt, die unter einer gewissen Grenze liegen, und für eine positive Determinante von dem Exponenten der aus der Kreistheilung sich ergebenden Auflösung der *Pell*schen Gleichung. Da aber die determinirenden Formen aller aequivalenten cubischen Formen in dieselbe Classe gehören, während umgekehrt nicht alle cubischen Formen mit aequivalenten determinirenden Formen aequivalent sein müssen, so wird man für jede der obigen Classen quadratischer Formen Γ_n eine zugehörige Anzahl k_n (die auch Null sein kann) von Classen zugehöriger cubischer Formen haben, deren determinirende Formen alle zu der Classe Γ_n gehören, und es ist dann

$$k_1 + k_2 + \ldots\ldots + k_n = K.$$

Man erhält also auf diesem Wege eine merkwürdige Doppel-Eintheilung sämmtlicher Classen cubischer Formen, indem man zuerst jedesmal alle diejenigen zusammenfafst, deren determinirende Formen aequivalent sind, und dann auf's Neue jedesmal alle zu derselben Determinante gehörenden zu einer höhern Ordnung vereinigt.

§. 4.

In der Theorie der quadratischen Formen wird gezeigt, dafs, wenn zwei Formen aequivalent sind, es gewöhnlich einige, zuweilen unendlich viele Transformationen giebt, durch welche die beiden Formen in einander übergehen können. Dieser Umstand kann bei den cubischen Formen nie eintreten, sondern wenn zwei cubische Formen aequivalent sind, so kann man nur durch *eine einzige Transformation* von der einen zur andern gelangen.

Es seien

$$f = ax^3 + 3bx^2y + 3cxy^2 + dy^3 = (a, b, c, d) \text{ und}$$
$$f' = a'x'^3 + 3b'x'^2y' + 3c'x'y'^2 + dy'^3 = (a', b', c', d')$$

zwei aequivalente cubische Formen, und

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

eine Transformation von f in f'. Um nun den Satz in aller Strenge zu erweisen, dafs nämlich keine zweite von der Transformation $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ verschiedene Transformation von f in f' existirt, mufs man mehrere Fälle unterscheiden.

Es sei zuerst die Determinante D der beiden cubischen Formen eine positive Zahl. Da in diesem Falle die cubische Gleichung

$$L = ax^3 + 3bx^2 + 3cx + d = 0,$$

so wie die andere

$$L' = a'x^3 + 3b'x^2 + 3c'x + d' = 0,$$

eine reelle und zwei imaginäre Wurzeln hat, so sei die reelle Wurzel $\frac{p}{p'}$ und die beiden imaginären $\begin{smallmatrix}q+ri, & q-ri\\ b'+ri, & q'-r'i\end{smallmatrix}$.

Nachdem man diese Wurzeln gefunden, kann man die Formen f und f' in lineare Factoren zerlegen, und setzen:

$$\left.\begin{aligned} f &= a[x-py][x-(q+ri)y][x-(q-ri)y]\\ f' &= a'[x'-p'y'][x'-(q'+r'i)y'][x'-(q'-r'i)y']\end{aligned}\right\} \quad i = \sqrt{-1}.$$

Wendet man nun in der That auf f die Substitution $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ an, so kommt

$$a[(\alpha-\gamma p)x' + (\beta-\delta p)y'][(\alpha-\gamma q-\gamma ri)x' + (\beta-\delta q-\delta ri)y'] \times[(\alpha-\gamma q+\gamma ri)x' + (\beta-\delta q-\delta ri)y'].$$

Dieser Ausdruck mufs also $= f'$ sein. Umgekehrt: setzt man den gefundenen Ausdruck

$$= f' = a'[x'-p'y'][x'-(q'+r'i)y'][x'-(q'-r'i)y'],$$

so hat man eine Gleichung, welche in Verbindung mit der Gleichung

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

nach α, β, γ, δ als Unbekannten aufgelöset, alle Transformationen von f in f', wenn es deren mehrere geben sollte, liefern mufs.

Es läfst sich nun zeigen, dafs sich aus diesen Gleichungen höchstens zwei Systeme für α, β, γ, δ bestimmen lassen.

In der That: da man nur den reellen Factor mit dem reellen und die imaginären unter einander vergleichen kann, so darf man nur setzen:

1. $$a' = a(\alpha-\gamma p)(\alpha-\gamma q-\gamma ri)(\alpha-\gamma q+\gamma ri),$$
2. $$\frac{\beta-\delta p}{\alpha-\gamma p} = -\frac{a'}{a}p',$$

3. $\frac{\beta-\delta q-\delta r i}{\alpha-\gamma q-\gamma r i} = -\frac{a'}{a}(q'\pm r' i)$, d. h. entweder $= -\frac{a'}{a}(q'+r' i)$

oder $= -\frac{a'}{a}(q'-r' i)$,

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

Die Gleichung (3.), mit irgend einem der beiden Vorzeichen von r' genommen, repräsentirt jedesmal zwei Gleichungen, da man den reellen Theil mit dem reellen, den imaginären mit dem imaginären vergleichen mufs. Auf diese Weise erhält man aus den beiden Gleichungen (2.) und (3.) drei lineare Gleichungen zur Bestimmung der Werthe von

$$\frac{\alpha}{\beta},\ \frac{\gamma}{\beta},\ \frac{\delta}{\beta};$$

also jedesmal, sowohl für $+r'$ als $-r'$, ein einziges System dieser Werthe. Es sei eins dieser beiden Systeme

$$\lambda,\ \nu,\ \varrho,$$

so erhält man aus der Gleichung $\alpha\delta-\beta\gamma = 1$:

$$\frac{\alpha}{\beta}\cdot\frac{\delta}{\beta}-\frac{\gamma}{\beta} = \frac{1}{\beta^2},\quad \text{also}\quad \beta^2 = \frac{1}{\lambda\varrho-\nu}.$$

Von den beiden Werthen β und $-\beta$, die dieser Gleichung genügen, darf man nur den einen nehmen; denn da man aus jedem dieser beiden Werthe die Werthe von α, γ, δ vollständig bestimmt, nämlich aus dem Werthe β, $\alpha = \lambda\beta$, $\gamma = \nu\beta$, $\delta = \varrho\beta$, und aus dem negativen $-\beta$, $\alpha = -\lambda\beta$, $\gamma = -\nu\beta$, $\delta = -\varrho\beta$, so müfste es, sollten beide Werthe der Quadratwurzel zulässig sein, möglich sein, zugleich durch zwei Substitutionen von der Form

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}\quad\begin{pmatrix}-\alpha, & -\beta\\ -\gamma, & -\delta\end{pmatrix}$$

von einer cubischen Form zu einer ihr aequivalenten überzugehen. Da die Unmöglichkeit dieses Letzteren sich aus dem blofsen Anblick der Gleichungen (7.) ergiebt (§. 1.), so folgt, dafs zu jedem der beiden entgegengesetzten Werthe von r höchstens *ein* System α, β, γ, δ gehört, also dafs im Ganzen höchstens zwei solcher Systeme existiren können.

Ich habe im Vorhergehenden bewiesen, dafs eine cubische Form mit positiver Determinante nie mehr als zwei Transformationen in eine ihr aequivalente zuläfst. Um nun zu zeigen, dafs nie zwei, sondern immer nur eine Transformation existirt, beweise ich, dafs aus der Annahme zweier Transformationen zwischen zwei aequivalenten Formen sich zwei Formen finden lassen, die durch ***drei*** verschiedene Transformationen in einander übergehen;

was dem Bewiesenen widerstreitet. Angenommen also, es gingen die Formen f und f' durch die beiden verschiedenen Transformationen

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = t_1, \qquad \begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix} = t_2$$

in einander über. Man bilde die reciproke Transformation von t_1, nämlich

$$t_3 = \begin{pmatrix}\delta, & -\beta\\ -\gamma, & \alpha\end{pmatrix},$$

durch welche f' in f übergeht, und verbinde sie mit t_2, so erhält man die neue Transformation

$$\tau_1 = \begin{pmatrix}\alpha'\delta - \beta'\gamma, & -\alpha'\beta + \beta'\alpha\\ \gamma'\delta - \delta'\beta, & -\gamma'\beta + \delta'\alpha\end{pmatrix},$$

durch welche f in f, d. h. f in sich selbst übergeht. Auf der andern Seite bilde man die reciproke Transformation von t_2 und verbinde sie mit t_1, so erhält man wiederum eine Transformation

$$\tau_2 = \begin{pmatrix}\alpha\delta' - \beta\gamma', & -\alpha\beta' + \beta\alpha'\\ \gamma\delta' - \delta\gamma', & -\gamma\beta' + \delta\alpha'\end{pmatrix},$$

durch welche f in sich selbst übergeht. Da sich zu diesen beiden Transformationen τ_1 und τ_2 noch die evidente

$$\tau_3 = \begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}$$

gesellt, so würde man also ***drei verschiedene*** *) Transformationen haben, durch welche f in sich selbst übergehen könnte; was dem Bewiesenen widerstreitet.

Zweitens sei D negativ. Bezeichnen wir die determinirenden quadratischen Formen der beiden cubischen Formen f und f' durch F und F', so mufs jede Transformation, durch welche f in f' übergeht, auch F in F' übergehen lassen. Untersuchen wir nun, auf wie viele Arten die beiden quadratischen Formen F und F', oder, was dasselbe ist, die beiden quadratischen Formen

$$(2A, B, 2C) \quad \text{und} \quad (2A', B', 2C')$$

(nach der Bezeichnung von ***Gaufs***) in einander übergehen können, so finden wir, dafs, mit Ausnahme weniger specieller Fälle, in welchen 4 oder 6 Transformationen stattfinden, und die wir der Kürze halber gegenwärtig bei Seite lassen wollen, die beiden quadratischen Formen nur durch zwei, und zwar durch zwei entgegengesetzte Transformationen ***(Gaufs Disq. Art. 179.)***

$$\tau = \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}, \qquad \tau' = \begin{pmatrix}-\alpha, & -\beta\\ -\gamma, & -\delta\end{pmatrix}$$

*) Dafs sie alle drei verschieden sein müssen, läfst sich sehr leicht indirect nachweisen.

in einander übergehen. Bemerken wir nun, dafs zwei aequivalente cubische Formen nie durch zwei entgegengesetzte Transformationen zugleich in einander übergehen können, weil die Form f durch die Transformation τ' in $-f'$ übergeht, sobald sie durch die Transformation τ in f' verwandelt wird, so findet sich unser Satz auch für diesen Fall erwiesen.

§. 5.

Lehrsatz. Der vierfache Cubus des ersten Coëfficienten der determinirenden quadratischen Form einer zur Determinante D gehörigen cubischen Form ist immer durch die quadratische Grundform

$$U^2 - DV^2$$

darstellbar."

Die cubische Form sei $f = ax^3 + 3bx^2y + 3cxy^2 + dy^3$; alsdann ist der erste Coëfficient ihrer determinirenden quadratischen Form $b^2 - ac = A$, und die Determinante

$$D = a^2d^2 - 3b^2c^2 + 4ac^3 + 4db^3 - 6abcd;$$

also hat man die identische Gleichung

$$1. \quad (3abc - 2b^3 - a^2d)^2 - Da^2 = 4A^3,$$

von deren Richtigkeit man sich durch die Entwickelung überzeugt. In dieser Formel liegt aber der Beweis des Lehrsatzes.

Es sei nun A' eine beliebige, durch die Form

$$Ax^2 + Bxy + Cy^2 = F$$

darstellbare Zahl; dann kann man F in eine zweite quadratische Form transformiren, deren erster Coëfficient $= A'$ ist. Dieselbe sei daher

$$A'x'^2 + B'x'y' + C'y'^2 = F'.$$

Wendet man nun die nämliche Transformation, durch welche man F' aus F erhielt, auf die cubische Form f an, so erhält man eine zweite cubische Form f', und es wird nach dem in §. 3. Bewiesenen F' die determinirende quadratische Form von der cubischen Form f' sein. Da nun A' der erste Coëfficient von F', und D die Determinante von f' ist, so folgt aus dem obigen Lehrsatze, dafs $4A'^3$ durch die quadratische Grundform $U^2 - DV^2$ darstellbar sein wird. Man hat demnach folgenden allgemeinen Satz.

Lehrsatz. „Wenn eine Zahl N durch die determinirende Form einer cubischen Form mit der Determinante D darstellbar ist, so ist ihr vierfacher Cubus $4N^3$ durch die quadratische Grundform

$$U^2 - DV^2$$

darstellbar."

Auf ganz ähnliche Weise läfst sich auch der folgende Satz beweisen:

Lehrsatz. „Wenn eine Zahl durch die determinirende Form $Ax^2+Bxy+Cy^2=F$ einer cubischen Form $f=(a, b, c, d)$ mit der Determinante D darstellbar ist, so ist ihr *Quadrat* durch die entgegengesetzte Form $Ax^2-Bxy+Cy^2$ darstellbar."

Denn wenn A' irgend eine durch die Form F darstellbare Zahl bezeichnet, so läfst sich die Form F in eine aequivalente Form F' transformiren, deren erster Coëfficient der Zahl A' gleich ist; es sei $F'=A'x'^2+B'x'y'+C'y'^2$. Durch die nämliche Transformation erhält man aber nach §. 3. aus f die neue cubische Form

$$f'=a'x'^3+3b'x'^2y'+3c'x'y'^2+d'y'^3,$$

deren determinirende Form die Form F' ist. Man hat nun nach §. 1. die nachstehenden Gleichungen:

$$A'=b'^2-a'c', \quad B'=b'c'-a'd', \quad C'=c'^2-b'd',$$

und aus diesen ergeben sich unmittelbar auf rein algebraischem Wege die folgenden drei:

$$2. \quad A'^2=A'b'^2-B'a'b'+C'a'^2,$$
$$3. \quad A'C'=A'c'^2-B'b'c'+C'c'^2,$$
$$4. \quad C'^2=A'd'^2-B'd'c'+C'c'^2.$$

Aus der Gleichung (2.) ersieht man aber, dafs A'^2 durch die Form

$$A'x^2-B'xy+C'y^2$$

repräsentirt werden kann. Da nun diese Form der Form

$$Ax^2-Bxy+Cy^2$$

aequivalent ist, so mufs A'^2 ebenfalls durch diese letztere Form darstellbar sein; was zu beweisen war.

§. 6.

Mit Hülfe der vorhergehenden Sätze wird es uns möglich sein, einen merkwürdigen Zusammenhang nachzuweisen, der zwischen der Theorie der *cubischen Formen* und der Theorie der *Zusammensetzung* oder *Multiplication* der quadratischen Formen stattfindet. Da jedoch diese Untersuchung in ihrer ganzen Allgemeinheit, d. h. für jede beliebige Determinante, ein näheres Eingehen in die Natur dieser letzteren Theorie erfordert, welche, so viel ich weifs, seit ihrer Entdeckung durch den berühmten Verfasser der „Disquisitiones" noch durch Niemand weiter ausgebildet worden ist, so sei es uns erlaubt, den Gegenstand für's Erste in einem speciellen Falle zu behandeln.

Wir nehmen den Fall, in welchem die Determinante von der Form $D = -4p$ und p eine positive Primzahl von der Form $4n+3$ ist, welche, als Determinante einer quadratischen Form angesehen, zu denen gehört, die *Gaufs* regelmäfsige nennt.

Ich stelle mir jetzt die Aufgabe: alle quadratischen Formen zu finden, welche determinirende Formen zu cubischen Formen mit der Determinante $-4p$ sein können; und da jede quadratische Form, die diese Eigenschaft besitzt, sie mit allen ihr aequivalenten theilt (§. 3.), so wird es genügen, alle nicht aequivalenten quadratischen Formen dieser Gattung aufzusuchen. Es sei

$$1. \quad ax^3+3bx^2y+3cxy^2+dy^3 = f$$

eine cubische Form, deren determinirende quadratische Form

$$2. \quad Ax^2+Bxy+Cy^2 = F$$

und deren Determinante $= B^2-4AC = -4p$ ist. Alsdann mufs zuerst B eine gerade Zahl sein, weil sonst die Gleichung $B^2-4AC = -4p$ nicht existiren kann. Es ist also $B = 2\mathrm{B}$, so dafs

$$3. \quad \mathrm{B}^2-AC = -p$$

ist. Hierauf ist $-p$ die Determinante der quadratischen Formen

$$4. \quad (A, \mathrm{B}, C) = F;$$

nach der Bezeichnung von *Gaufs*.

Nach dem Lehrsatze des vorigen Paragraphen ist nun der vierfache Cubus jeder durch F darstellbaren Zahl durch die Form x^2+4py^2 darstellbar: also wird der einfache Cubus jeder durch F darstellbaren Zahl durch die Form x^2+py^2, mithin allgemein durch alle Formen der zur Determinante $-p$ gehörigen Hauptclasse darstellbar sein; oder, noch allgemeiner: es werden die Cuben aller Zahlen, welche sich durch diejenige Classe darstellen lassen, welche die Form F enthält, durch die Hauptclasse darstellbar sein.

Unter der für die Primzahl p gemachten Annahme werden sich alle zur Determinante $-p$ gehörigen Classen quadratischer Formen durch successives Zusammensetzen aus einer derselben bilden lassen. Nennen wir $h = 2\lambda+1$ die Anzahl dieser Classen, welche wir durch K bezeichnen und durch Indices von einander unterscheiden wollen, so lassen sich dieselben immer in folgende Ordnung bringen:

$$5. \quad K_{-\lambda}, \; K_{-(\lambda-1)}, \; \ldots \; K_{-1}, \; K_0, \; K_1, \; \ldots \; K_{\lambda-1}, \; K_\lambda;$$

welche Reihe als in sich zurückkehrend zu betrachten ist, so dafs auf K_λ wieder $K_{-\lambda}$ folgt, und wo jede Classe aus der vorhergehenden und der Classe K_1 zusammengesetzt ist, K_0 die Hauptclasse vorstellt und entgegengesetzten

Classen entgegengesetzte Indices entsprechen. Nun hat Hr. Professor ***Lejeune Dirichlet***, der Verfasser des Beweises über die arithmetische Progression, durch eine neue Anwendung seines herrlichen Princips gezeigt, dafs jede dieser Classen unendlich viele Primzahlen repräsentirt: wir können uns dieselben daher sämmtlich durch solche Formen repräsentirt vorstellen, deren erste Coëfficienten Primzahlen sind.

Es sei $(A, B, C) \sim F_\mu$ und q, der erste Coëfficient von F_μ, eine ungerade Primzahl. Da nun q^3 durch die Classe K_0 darstellbar sein soll, so mufs der Index μ der Bedingung

$$6. \quad 3\mu \equiv 0 \pmod{h}$$

genügen. Andere Formen also, als diejenigen, welche diese Bedingung erfüllen, können für den in Rede stehenden Fall nicht determinirende Formen zu cubischen Formen bilden.

Auf der andern Seite werde ich zeigen, dafs allen quadratischen Classen, welche die Bedingung (6.) erfüllen, in der That cubische Classen entsprechen; und zwar jeder derselben nur eine einzige.

Es sei also F_μ eine quadratische Form, deren Index der Congruenz (6.) genügt, oder, was dasselbe ist, welche durch ihre Triplication die Hauptclasse hervorbringt, so dafs man

$$7. \quad q^3 = U^2 + p.V^2$$

setzen kann; wo U und V relative Primzahlen sind.

Dieses vorausgesetzt, betrachten wir die cubische Form

$$8. \quad Vx^3 + 3bx^2y + 3\frac{b^2-q}{V}xy^2 + \frac{b^3-3qb+2U}{V^2}y^3,$$

in welcher b eine noch vorläufig unbestimmt gelassene ganze Zahl vorstellt. Diese cubische Form genügt den Bedingungen, dafs der erste Coëfficient ihrer determinirenden quadratischen Form $= b^2 - V.\frac{b^2-q}{V} = q$ und dafs ihre Determinante $= 4\frac{U^2-q^3}{V^2} = -4p$ ist. Suchen wir jetzt b so zu bestimmen, dafs ihre beiden letzten Coëfficienten ganze Zahlen werden. Zu dem Ende mufs den beiden Congruenzen

$$9. \quad b^2 - q \equiv 0 \pmod{V},$$

$$10. \quad b^3 - 3qb + 2U \equiv 0 \pmod{V^2}$$

genügt werden.

Wenn wir den Ausdruck $b^3 - 3qb + 2U$ durch $\varphi(b)$ bezeichnen, so ist der Differenzialquotient $\frac{d\varphi(b)}{db} = 3(b^2 - q)$; was für die Auflösung der beiden

Congruenzen von Wichtigkeit ist. Ferner bemerke ich, dafs wegen der Gleichung (7.) q^3, also auch q zu V^2, mithin auch zu jedem in V enthaltenen Theiler quadratischer Rest sein wird. Beschäftigen wir uns nun mit der Auflösung der beiden Congruenzen.

I. Es sei l die höchste in V aufgehende Potenz einer ungeraden Primzahl. Dann genügen, wie bekannt, der Cougruenz $b^2 \equiv q \pmod{l}$ zwei nach dem Modul l incongruente, dem Zeichen nach entgegengesetzte Werthe von b, die wir durch $\pm z$ bezeichnen. Bilden wir nun die Reihe der Zahlen

$$11. \quad z,\ z+l,\ z+2l,\ \ldots\ z+(l-1)l,$$

so befindet sich unter denselben eine einzige, welche zugleich der Congruenz $b^2 \equiv q \pmod{l^2}$ genügt. Wird dieselbe mit ζ bezeichnet, so ist auch $\zeta^3 \equiv q\zeta \pmod{l^2}$, also $\varphi(\zeta) \equiv 2(U - q\zeta) \pmod{l^2}$. Nun folgt aus (7.) $q^3 \equiv U^2 \pmod{l^2}$, also ist $U^2 - q^2\zeta^2 \equiv 0 \pmod{l^2}$, d. h. $(U - q\zeta)(U + q\zeta)$ durch l^2 theilbar. Da nun diese beiden Factoren keinen in l enthaltenen gemeinschaftlichen Theiler haben können, weil derselbe sonst in ihrer Differenz $2U$, also in U und V zugleich aufgehen würde, so wird nothwendig einer der beiden Ausdrücke $U \mp q\zeta$ durch l^2 theilbar sein, während der andere zu l relative Primzahl ist. Das Zeichen von ζ kann demnach auf eine und nur auf eine Art so bestimmt werden, dafs $\varphi(\zeta) \equiv 0 \pmod{l^2}$. Der Werth $b = \zeta$ genügt dann den beiden Congruenzen

$$12. \quad b^2 - q \equiv 0 \pmod{l} \quad \text{und} \quad 13. \quad b^3 - 3qb + 2U \equiv 0 \pmod{l^2}.$$

Ich behaupte aber, dafs auch jeder Werth von der Form $\zeta + kl$, also jeder in der Reihe (11.) enthaltene Werth, wenn man das Zeichen von z schicklich wählt, diesen beiden Congruenzen genügen wird. In der That setze man $\zeta + kl$ in den Ausdruck $\varphi(b)$ statt b, so erhält man

$$\varphi(\zeta + kl) \equiv \varphi(\zeta) + kl\frac{d\varphi(\zeta)}{d\zeta} \pmod{l^2},$$

welches durch l^2 theilbar sein wird, weil $\varphi(\zeta)$ durch l^2 und $\frac{d\varphi(\zeta)}{d\zeta} = 3(\zeta^2 - q)$ durch l theilbar ist.

Als Resultat dieser Untersuchung ergiebt sich also, dafs für jede höchste in V enthaltene Potenz l einer ungeraden Primzahl immer eine und nur eine einzige ganze Zahl z existirt, die so beschaffen ist, dafs sie, mit allen ihr nach dem Modul l congruenten statt b gesetzt, die sämmtlichen Auflösungen der beiden Congruenzen (12. und 13.) giebt.

II. Es sei für den Fall, dafs V eine gerade Zahl ist, $2^\vartheta = l$ die höchste in V enthaltene Potenz von 2. Alsdann läfst sich durch ganz ähnliche Betrachtungen zeigen, dafs auch für diesen Werth von l den Congruenzen (12. u. 13.) ein einziger Werth von b mit allen ihm nach dem Modul l congruenten genügt. Wenn $\vartheta = 1$ oder $= 2$, also $l = 2$ oder $= 4$ ist, so sieht man sogleich, dafs dieser Werth $b = 1$ ist. Es sei $\vartheta \geqq 3$: alsdann existiren vier nach dem Modul l incongruente Werthe von b, die der Congruenz $b^2 \equiv q \pmod{l}$ genügen; und wenn man einen derselben z nennt, so lassen sie sich auf folgende Art gruppiren:

14. $\quad +z, \quad -z, \quad z+2^{\vartheta-1}, \quad -z+2^{\vartheta-1}$ (*Gaufs* Disq. 103).

Von diesen 4 Werthen genügen aber nur zwei $\pm z$ zugleich der Congruenz $b^2 \equiv q \pmod{l^2}$. Es sei also $z^2 \equiv q \pmod{l^2}$; alsdann folgt wie oben

$$\varphi(z) \equiv 2(U - qz) \pmod{l^2},$$

und da wegen (7.) $q^3 \equiv U^2 \pmod{l^2}$, also $U^2 - q^2 z^2 \equiv 0 \pmod{l^2}$ ist, und die beiden Factoren $U \mp qz$ höchstens den gemeinschaftlichen Theiler 2 haben können, so wird sich das Zeichen von z immer auf eine und nur auf eine Art so bestimmen lassen, dafs $U - qz$ durch $\frac{1}{2}l^2$, also $\varphi(z)$ durch l^2 theilbar ist. Es bleibt noch zu zeigen, dafs der Werth $b = z + 2^{\vartheta-1}$ der Congruenz (13.) nicht genügen kann. Diese Annahme würde auf die Congruenz

$$\varphi(z) + 2^{\vartheta-1}.3(z^2 - q) + 2^{2\vartheta-2}.z \equiv 0 \pmod{2^{2\vartheta}}$$

führen, welche nicht stattfinden kann, da q, also z, eine ungerade Zahl ist.

III. Stellt man sich nun V auf die Form

15. $\quad V = l.l'.l''....$

gebracht vor, wo l, l', l'' etc. Potenzen verschiedener Primzahlen sind, mit Einschlufs der 2, so lassen sich die Congruenzen (12. und 13.) nach jedem der Moduln l, l', l'', ... auflösen, und geben jedesmal eine einzige Lösung. Bezeichnen wir diese Lösungen nach den verschiedenen Moduln der Reihe nach, resp. durch z, z', z'' etc., und suchen dann eine Zahl, welche zugleich $\equiv z \pmod{l}$, $\equiv z' \pmod{l'}$, $\equiv z'' \pmod{l''}$ etc. ist, so wird dieselbe, statt b gesetzt, nothwendig den beiden Congruenzen (9. u. 10.) zugleich genügen; und alle anderen Zahlen, welche die nämliche Eigenschaft haben, werden ihr nach dem Modul V congruent sein.

Da nun ferner alle nach dem Modul V congruenten Werthe von b, in die cubische Form (8.) gesetzt, lauter aequivalente Formen hervorbringen, die durch Substitutionen von der folgenden Art:

16. $\quad x = x' + ky', \quad y = 0.x' + y',$

für welche

$$1.1-k.0 = 1'$$

ist, in einander übergehen, so werden wir auf diesem Wege immer zu einer, aber auch nur zu einer einzigen Classe cubischer Formen gelangen, welche allen Bedingungen genügt.

Zweitens läfst sich nachweisen, dafs es unmöglich ist, auf anderem Wege eine zweite Classe cubischer Formen zu entdecken, die dieselben Eigenschaften besitzt. Denn man stelle sich irgend eine cubische Form

$$ax^3+3bx^2y+3cxy^2+dy^3 = f$$

vor, deren determinirende quadratische Form zum ersten Coëfficienten q hat und deren Determinante $=-4p$ ist. Alsdann läfst sich f durch Zerlegung in lineare Factoren auf die Form

$$17.\quad f = \frac{1}{a^2}\left\{ax+[b-\sqrt[3]{(E+a\sqrt{-p})}-\sqrt[3]{(E-a\sqrt{-p})}]y\right\}$$
$$\times\left\{ax+[b-\varrho\sqrt[3]{(E+a\sqrt{-p})}-\varrho^2\sqrt[3]{(E-a\sqrt{-p})}]y\right\}$$
$$\times\left\{ax+[b-\varrho^2\sqrt[3]{(E+a\sqrt{-p})}-\varrho\sqrt[3]{(E-a\sqrt{-p})}]y\right\}$$

bringen, wo E eine ganze Zahl ist, die mit a keinen gemeinschaftlichen Theiler hat, $\varrho=\frac{1}{2}(-1+\sqrt{-3})$ und

$$18.\quad E^2+pa^2 = q^3$$

ist. Da nun die unbestimmte Gleichung $U^2+pV^2=q^3$ nur auf eine einzige Art in relativen Primzahlen lösbar ist, so mufs $E=U$ und $a=V$ sein. Bemerkt man dies und multiplicirt die drei Factoren in (17.) wirklich in einander, so wird man wieder zu der cubischen Form (8.) geführt, von welcher wir oben ausgegangen waren.

Aus allem diesen ergiebt sich nun Folgendes.

„Wenn p eine Primzahl von der Form $4n+3$ ist und $-p$ zu den regelmäfsigen Determinanten gehört, so entspricht jeder Classe quadratischer Formen mit der Determinante $-p$, welche durch ihre Triplication die Hauptclasse hervorbringt, eine Classe cubischer Formen mit der Determinante $-4p$, während den übrigen quadratischen Classen keine cubischen Classen mit derselben Determinante entsprechen."

Mit diesem eleganten Satze schliefse ich diese erste Abtheilung, in welcher ich nur die Elemente eines ganz neuen Feldes der Zahlenlehre aufstellen wollte. Sollte ich mir schmeicheln dürfen, dafs dieser erste Versuch

eines Anfängers sich des Beifalls der Mathematiker erfreuen könnte, so würde ich mit Vergnügen die begonnene Arbeit fortsetzen; zumal da ich gerade die interessantesten Resultate zurückhalten mufste, auf welche die vollständige Theorie der Vertheilung der cubischen Classen auf die quadratischen führt, und die auf eine merkwürdige Weise von der Betrachtung derjenigen Formen abhängen, welche ganz allgemein, nicht blofs die Haupt- oder Grundform, sondern eine beliebige gegebene primitive quadratische Form durch ihre Triplication erzeugen.

Berlin im December 1843.

(Die Fortsetzung folgt.)