Zur Theorie der zerlegbaren Formen, insbesondere der kubischen.*)

Von

Arnold Meyer †.

Im folgenden soll der Versuch gemacht werden, die wesentlichsten Grundlagen zu einer Behandlung der in lineare Faktoren zerlegbaren homogenen Funktionen zu liefern. Zwar hat schon Herr Hermite in einigen Abhandlungen (Crelle's Journal Bd. 40 und 47) die Reduktion dieser Formen auf eine endliche Anzahl gezeigt, dadurch, dass er die Quadrate der reellen Linearfaktoren und die Produkte aus je zwei konjugierten in eine Summe vereinigte und dann auf die so entstandene quadratische Form die von ihm für solche Formen entwickelte Reduktionsmethode anwandte. Im folgenden soll ein anderer, wie mir scheint, genuinerer Weg eingeschlagen werden. Zunächst wird gezeigt werden, dass sich jede zerlegbare Form als Norm eines linearen Ausdrucks mit komplexen, aus Wurzeln einer irreduktibeln Gleichung gebildeten Koeffizienten darstellen lässt. Der so erhaltene Ausdruck wird dann mit Hülfe der von Herrn Kummer aufgestellten Theorie der idealen Primfaktoren untersucht und seine Reduktion auf eine bestimmte Normalform teils mit Hülfe dieser Theorie, teils durch Anwendung linearer Substitutionen bewerkstelligt. Dabei ergiebt sich nicht nur die

*) Die nachfolgende, aus den Akten der Fachlehrer-Abteilung des eidg. Polytechnikums stammende und von Herrn Prof. Hurwitz, dem gegenwärtigen Vorstande dieser Abteilung, mir zur Veröffentlichung übergebene Abhandlung ist Arnold Meyer's Habilitationsschrift, durch welche er sich Ostern 1870 die venia legendi am eidg. Polytechnikum erwarb. Obwohl sie durch die neueren Arbeiten auf dem Gebiete der Idealtheorie vielfach überholt ist, bietet sie doch des Interessanten und Eigenartigen so viel, dass ihr Abdruck auch heute noch gerechtfertigt erscheinen wird. **F. Rudio.**

Endlichkeit der Klassenanzahl, sondern auch der enge Zusammenhang, der zwischen derselben und der Klassenanzahl der idealen komplexen Zahlen stattfindet. Zum Schlusse wird dann noch gezeigt, in welcher Beziehung die komplexen Einheiten zu den Transformationen der Formen in sich selbst stehen.

Der Einfachheit wegen beschränke ich mich hier auf eine specielle Gattung kubischer Formen, wende aber dabei möglichst Methoden an, deren allgemeine Anwendbarkeit auf Formen beliebiger Grade sofort einleuchtet. Bei der Entwicklung der hiebei in Anwendung kommenden speciellen Theorie aus Kubikwurzeln gebildeter komplexer Zahlen mache ich nach dem Vorgange von Herrn Selling (Ueber die idealen Primfaktoren der komplexen Zahlen, welche aus Wurzeln einer beliebigen irreduktibeln Gleichung rational gebildet sind, in Schlömilch's Zeitschrift X. Jahrg. 1865) von der Theorie der imaginären Kongruenzwurzeln Gebrauch, wie sie von Gauss (im Nachlass) angedeutet, von Galois und Serret ausgeführt worden ist.

I.

§ 1. Zerlegung in Linearfaktoren.

Es sei $f(x_1, x_2, \ldots\ldots x_n)$

eine ganze homogene, in lineare Faktoren zerlegbare Funktion (Form) m^{ten} Grades von n Unbestimmten

$$x_1, x_2, \ldots\ldots x_n$$

und mit reellen ganzen Zahlen zu Koeffizienten.

Durch eine lineare Transformation lässt sich immer bewirken, dass der Koeffizient von x_1^m, wenn er es nicht schon sein sollte, von 0 verschieden wird; es sei also derselbe $= a$. Alsdann kann die Form in folgender Weise (vgl. Hermite, Journal v. Liouville Bd. 64) zerlegt werden:

$$f = a\, \overset{1}{u}\, \overset{2}{u} \ldots\ldots \overset{m}{u},$$

wo

$$\begin{aligned}
\overset{1}{u} &= x_1 + \overset{1}{u}_2 x_2 + \cdots\cdots + \overset{1}{u}_n x_n \\
\overset{2}{u} &= x_1 + \overset{2}{u}_2 x_2 + \cdots\cdots + \overset{2}{u}_n x_n \\
&\vdots \\
\overset{m}{u} &= x_1 + \overset{m}{u}_2 x_2 + \cdots\cdots + \overset{m}{u}_n x_n.
\end{aligned}$$

Setzen wir nun

$$x_3 = 0,\ x_4 = 0, \ldots\ldots x_n = 0,$$

so können wir die binäre Form m^{ten} Grades

$$f(x_1, x_2, 0, \ldots\ldots 0) = \varphi(x_1, x_2)$$

in lineare Faktoren zerlegen. Es sei

$$\varphi(x_1, x_2) = a(x_1 + \omega_1 x_2)(x_1 + \omega_2 x_2) \ldots\ldots (x_1 + \omega_m x_2);$$

somit

$$\overset{1}{u}_2 = \omega_1, \overset{2}{u}_2 = \omega_2, \ldots\ldots \overset{m}{u}_2 = \omega_m,$$

wo

$$\omega_1, \omega_2 \ldots\ldots \omega_m$$

die Wurzeln sind der Gleichung:

$$\varphi(x, -1) = 0.$$

Um nun

$$\overset{1}{u}_3, \overset{2}{u}_3, \ldots\ldots \overset{m}{u}_3$$

zu bestimmen, setze man

$$x_4 = 0,\ x_5 = 0, \ldots\ldots x_n = 0$$

und vergleiche die Koeffizienten von $x_1^k x_2^l x_3$ $(k = 0,1 \ldots m-1)$ in der Gleichung

$$f(x_1, x_2, x_3, 0, \ldots\ldots 0)$$

$$= a(x_1 + \omega_1 x_2 + \overset{1}{u}_3 x_3)(x_1 + \omega_2 x_2 + \overset{2}{u}_3 x_3) \ldots\ldots (x_1 + \omega_m x_2 + \overset{m}{u}_3 x_3),$$

so sieht man, dass die Produkte aus a in folgende Aggregate ganze Zahlen sind:

$$\overset{1}{u}_3 \qquad + \overset{2}{u}_3 \qquad \ldots\ldots + \overset{m}{u}_3$$

$$\overset{1}{u}_3(\omega_2 + \omega_3 + \cdots\cdots \omega_m) + \overset{2}{u}_3(\omega_1 + \omega_3 + \cdots \omega_m) + \cdots\cdots + \overset{m}{u}_3\ (\omega_1 + \omega_2 + \cdots + \omega_{m-1})$$

$$\text{(A)}\quad \overset{1}{u}_3(\omega_2\omega_3 + \cdots + \omega_{m-1}\omega_m) + \overset{2}{u}_3(\omega_1\omega_3 + \cdots + \omega_{m-1}\omega_m) + \cdots + \overset{m}{u}_3\ (\omega_1\omega_2 + \cdots + \omega_{m-2}\omega_{m-1})$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\overset{1}{u}_3 \cdot \omega_2\omega_3 \ldots\ldots\ldots \omega_m + \overset{2}{u}_3 \cdot \omega_1\omega_3 \ldots\ldots \omega_m + \ldots + \overset{m}{u}_3\ \omega_1\omega_2 \ldots\ldots \omega_{m-1}$$

Die Determinante Δ dieses Systems verschwindet, so oft zwei von den Wurzeln $\omega_1, \omega_2 \ldots \omega_m$ einander gleich werden; sie ist also durch das Produkt aller Wurzeldifferenzen teilbar, ausserdem

ist sie vom Grade $\frac{m(m-1)}{2}$ und hat als Anfangsglied

$$1 \cdot \omega_1 \cdot \omega_1\,\omega_2 \cdot \omega_1\,\omega_2\,\omega_3 \ldots\ldots \omega_1\,\omega_2 \ldots \omega_{m-1} = \omega_1^{m-1}\,\omega_2^{m-2} \ldots\ldots \omega_{m-2}^2 \cdot \omega_{m-1};$$

sie ist somit identisch mit dem Produkte aller Wurzeldifferenzen:

$$\Delta = (\omega_1 - \omega_2)\,(\omega_1 - \omega_3) \ldots\ldots (\omega_{m-1} - \omega_m)$$

$$= (-1)^{\frac{m(m-1)}{2}} \begin{vmatrix} 1 & , & 1 & , \ldots\ldots & 1 \\ \omega_1 & , & \omega_2 & , \ldots\ldots & \omega_m \\ \omega_1^2 & , & \omega_2^2 & , \ldots\ldots & \omega_m^2 \\ \cdot & & \cdot & & \cdot \\ \omega_1^{m-1} & , & \omega_2^{m-1} & , \ldots\ldots & \omega_m^{m-1} \end{vmatrix}$$

Wird nun vorerst angenommen, die Gleichung $\varphi(x, -1) = 0$ habe keine gleichen Wurzeln, die Diskriminante Δ^2 derselben sei also von null verschieden, so lassen sich die Koeffizienten

$$\overset{1}{u}_3, \quad \overset{2}{u}_3, \ldots\ldots \overset{m}{u}_3$$

aus obigen Gleichungen bestimmen als ganze Funktionen der Wurzeln $\omega_1, \omega_2 \ldots \omega_m$ mit Koeffizienten, welche Brüche sind mit dem gemeinsamen Nenner $a\,\Delta^2$.

Vertauscht man im System (A) die Indices der Wurzeln ω in beliebiger Weise und zugleich die obern Indices von u_3 in derselben Weise, so bleibt das System (abgesehen von der Aufeinanderfolge der Summanden) völlig ungeändert, und es ist somit $\overset{k}{u}_3$ eine symmetrische Funktion der $m-1$ Wurzeln

$$\omega_1, \quad \omega_2 \ldots\ldots \omega_{k-1}, \quad \omega_{k+1} \ldots\ldots \omega_m$$

und daher als ganze rationale Funktion von ω_k darstellbar und zwar als dieselbe, welche $\overset{1}{u}_3$ von ω_1 ist. Man kann also setzen:

$$\overset{k}{u}_3 = \overset{3}{a}_0 + \overset{3}{a}_1\,\omega_k + \ldots\ldots + \overset{3}{a}_{m-1}\,\omega_k^{m-1}.$$

Ganz in derselben Weise stellen sich auch $\overset{k}{u}_4 \ldots \overset{k}{u}_m$ dar, so dass der Ausdruck für $\overset{k}{u}$ wird:

$$\overset{k}{u} = x_1 + \omega_k\,x_2 + (\overset{3}{a}_0 + \overset{3}{a}_1\,\omega_k + \ldots\ldots\ldots + \overset{3}{a}_{m-1}\,\omega_k^{m-1})\,x_3 + \ldots$$

$$\ldots\ldots + (\overset{n}{a}_0 + \overset{n}{a}_1\,\omega_k + \ldots\ldots\ldots + \overset{n}{a}_{m-1}\,\omega_k^{m-1})\,x_n,$$

wo die Koeffizienten a rationale Brüche sind, in deren Nenner keine andern Primfaktoren vorkommen als solche, welche in a und Δ^2 enthalten sind.

In den obigen Ausdrücken kommen die Unbestimmten nur in folgenden m Verbindungen vor:

$$\begin{aligned}
&x_1 + \overset{3}{a}_0 x_3 + \overset{4}{a}_0 x_4 + \cdots\cdots + \overset{n}{a}_0 x_n \\
&x_2 + \overset{3}{a}_1 x_3 + \overset{4}{a}_1 x_4 + \cdots\cdots + \overset{n}{a}_1 x_n \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
&\overset{3}{a}_{m-1} x_3 + \overset{4}{a}_{m-1} x_4 + \cdots\cdots + \overset{n}{a}_{m-1} x_n ;
\end{aligned}$$

setzt man diese Ausdrücke neuen Variabeln $y_1, y_2, \ldots . y_m$ gleich, so wird

$$\overset{k}{u} = y_1 + \omega_k y_2 + \overset{3}{\omega}_k y_3 + \cdots\cdots + \omega_k^{m-1} y_m ,$$

und es lassen sich daher diejenigen Formen, deren Grad m kleiner ist als die Anzahl n der Unbestimmten, immer auf solche reduzieren, wo $n = m$. Da ferner die Formen, für welche $n < m$, aus denjenigen, in welchen $n = m$ ist, hervorgehen, wenn $n - m$ der Unbestimmten gleich null gesetzt werden, so genügt es anzunehmen, es sei der Grad der Gleichung gleich der Anzahl der Unbestimmten.

§ 2. Der Fall, wo $\Delta = 0$.

Es bleibt noch der Fall zu untersuchen, wo die Gleichung $\varphi(x, -1) = 0$ gleiche Wurzeln hat.

In diesem Falle kann man, anstatt Glieder in $x_1^{m-p} x_2^p$ zu betrachten, an Stelle von x_2 irgend eine andere Unbestimmte x_k wählen, für welche die Koeffizienten $\overset{r}{u}_k$ alle von einander verschieden sind. Giebt es kein solches x_k, ist aber kein Linearfaktor $\overset{r}{u}$ mit einem andern identisch, so ist es doch stets möglich, durch eine lineare Transformation zu bewirken, dass die Gleichung $\varphi(x, -1) = 0$ ungleiche Wurzeln hat.

In der That: wird $\overset{r}{u}$ durch die Substitution

$$\begin{aligned}
x_1 &= y_1 + \beta\ y_2 + \gamma\ y_3 + \cdots\cdots + \lambda\ y_n \\
x_2 &= \quad \beta'\ y_2 + \gamma'\ y_3 + \cdots\cdots + \lambda'\ y_n \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
x_n &= \quad \beta^{(n-1)} y_2 + \gamma^{(n-1)} y_3 + \cdots\cdots + \lambda^{(n-1)} y_n
\end{aligned}$$

transformiert und geht es dabei über in

$$\overset{r}{u}' = y_1 + \overset{r}{u}_2' \, y_2 + \cdots\cdots\cdots + \overset{r}{u}_n' \, y^n,$$

so ist

$$\overset{1}{u}_2' = \beta + \overset{1}{u}_2 \, \beta' + \overset{1}{u}_3 \, \beta'' + \cdots\cdots + \overset{1}{u}_n \, \beta^{(n-1)}$$

$$\overset{2}{u}_2' = \beta + \overset{2}{u}_2 \, \beta' + \overset{2}{u}_3 \, \beta'' + \cdots\cdots + \overset{2}{u}_n \, \beta^{(n-1)}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\overset{m}{u}_2' = \beta + \overset{m}{u}_2 \, \beta' + \overset{m}{u}_3 \, \beta'' + \cdots\cdots + \overset{m}{u}_n \, \beta^{(n-1)}.$$

Die ganzen Zahlen $\beta', \beta'' \ldots . \beta^{(n-1)}$ lassen sich unter obiger Voraussetzung immer so wählen, dass die Grössen $\overset{1}{u}_2', \overset{2}{u}_2', \ldots \overset{m}{u}_2'$ alle von einander verschieden sind.

Seien vorerst die mn Grössen $\overset{r}{u}_k$ alle reell und sei μ der kleinste absolute Wert von denjenigen Differenzen

$$\overset{r}{u}_k - \overset{s}{u}_k, \; (r \gtrless s),$$

welche nicht null sind, M der grösste. Da es sich hier um rein algebraische Grössen handelt, so kann das Minimum, ohne genau null zu werden, nicht unter eine bestimmte endliche Grösse hinabsinken, noch das Maximum eine bestimmte endliche Grösse übersteigen.

Man nehme nun eine ganze positive Zahl h an, die den beiden Bedingungen

$$h > M, \; h\mu > 1 + \frac{1}{h^2 - 1} \left(= \frac{h^2}{h^2 - 1} \right)$$

genüge, und setze

$$\beta' = 1, \beta'' = h^2, \beta''' = h^4, \ldots\ldots \beta^{(n-1)} = h^{2n-4};$$

dann behaupte ich, dass obiger Forderung genügt sei. Wäre nämlich

$$\overset{r}{u}_2' = \overset{s}{u}_2',$$

so müsste sein

$$0 = \overset{r}{u}_2 - \overset{s}{u}_2 + h^2 \, (\overset{r}{u}_3 - \overset{s}{u}_3) + \cdots\cdots + h^{2n-4} \, (\overset{r}{u}_n - \overset{s}{u}_n).$$

Nun ist das Glied

$$h^{2k-4} \, (\overset{r}{u}_k - \overset{s}{u}_k)$$

entweder genau null, oder es liegt dem absoluten Werte nach zwischen

$$h^{2k-4}\,\mu \text{ und } h^{2k-4}\,M,$$

d. h. zwischen

$$h^{2k-5}\,\frac{h^2}{h^2-1} = \frac{h^{2k-3}}{h^2-1} \text{ und } h^{2k-3}.$$

Wären nun etwa die Differenzen

$$\overset{r}{u}_n - \overset{s}{u}_n,\ \overset{r}{u}_{n-1} - \overset{s}{u}_{n-1},\ \ldots\ldots\ \overset{r}{u}_{k+1} - \overset{s}{u}_{k+1}$$

alle gleich null, dagegen $\overset{r}{u}_k - \overset{s}{u}_k$ von null verschieden, so wird die Summe aller vorhergehenden Glieder

$$\overset{r}{u}_2 - \overset{s}{u}_2 + h^2\,(\overset{r}{u}_3 - \overset{s}{u}_3) + \cdots\cdots + h^{2k-6}\,(\overset{r}{u}_{k-1} - \overset{s}{u}_{k-1})$$

numerisch kleiner als

$$h + h^3 + h^5 + \cdots\cdots + h^{2k-5} = h\,\frac{h^{2k-4}-1}{h^2-1} < \frac{h^{2k-3}}{h^2-1}$$

und könnte sich somit gegen den Wert von $h^{2k-4}\,(\overset{r}{u}_k - \overset{s}{u}_k)$, der numerisch grösser ist als $\frac{h^{2k-3}}{h^2-1}$, nicht aufheben; obige Summe kann daher nur zu null werden, wenn alle Differenzen null sind, d. h. $\overset{r}{u}$ mit $\overset{s}{u}$ identisch ist.

Sind die Grössen $\overset{r}{u}_k$, $\overset{s}{u}_k$ nicht alle reell, so kann man die imaginären und reellen Teile gesondert betrachten und nimmt für h die grössere der hiebei in Anwendung kommenden Zahlen h.

Sind dabei einige der Reihen $\overset{r}{u}$ in den reellen Teilen identisch, so nehme man nur eine von ihnen; sie müssen dann in ihren imaginären Teilen alle verschieden sein und die betreffenden u'_2 werden sich in ihren reellen Teilen nicht, wol aber in ihren imaginären unterscheiden, und ähnlich ist zu verfahren, wenn einige Reihen in den imaginären Teilen koincidieren sollten.

§ 3. Zerlegung der Form für den Fall $\Delta = 0$.

Nach dieser Transformation kann die Gleichung $\varphi\,(x, -1) = 0$ nur dann noch gleiche Wurzeln haben, wenn die betreffenden Linearfaktoren vollständig gleich sind. In diesem Falle aber lässt sich die Form in ein Produkt von zerlegbaren Formen mit rationalen Koeffizienten zerfällen.

Um dies nachzuweisen, will ich zuvörderst zeigen, dass das Produkt der gemeinschaftlichen Linearfaktoren zweier zerlegbarer

Formen sich als zerlegbare Form mit rationalen Koeffizienten darstellen lässt.

Es seien

$$f(x_1, x_2 \ldots\ldots x_n) \text{ und } F(x_1, x_2 \ldots\ldots x_n)$$

zwei zerlegbare Formen resp. von den Graden m und p, welche den zerlegbaren Faktor

$$\varphi(x_1, x_2 \ldots\ldots x_n)$$

vom Grade q gemein haben sollen, und es sei

$$f(x_1, x_2, \ldots\ldots x_n) = \varphi(x_1, x_2 \ldots\ldots x_n) \cdot \psi(x_1, x_2 \ldots\ldots x_n)$$
$$F(x_1, x_2, \ldots\ldots x_n) = \varphi(x_1, x_2 \ldots\ldots x_n) \cdot \Psi(x_1, x_2 \ldots\ldots x_n).$$

Die Koeffizienten von x_1^m und x_1^p resp. können wiederum als von null verschieden und einander gleich angenommen werden.

Haben nun die Gleichungen

$$f(x, -1, 0, 0 \ldots\ldots 0) = f_1(x) = 0$$
$$\text{und } F(x, -1, 0, \ldots\ldots 0) = F_1(x) = 0$$

einen gemeinschaftlichen Faktor von höherm Grade als dem q^{ten}, so sind die Formen f und F zuerst auf ähnliche Weise wie oben durch eine gemeinsame Substitution in solche zu transformieren, für welche diese Gleichungen nur q gemeinschaftliche Wurzeln haben. Ist dies erreicht, so suche man nach der gewöhnlichen Methode den grössten gemeinschaftlichen Divisor von $f_1(x)$ und $F_1(x)$. Dieser wird sein

$$\varphi_1(x) = \varphi(x, -1_1\ 0, \ldots\ldots 0);$$

dadurch sind die Koeffizienten der binären Form $\varphi(x_1, x_2, 0 \ldots\ldots 0)$ bestimmt, und man kann weiter so verfahren:

Man bestimme durch Division

$$\psi_1(x) = \frac{f_1(x)}{\varphi_1(x)},$$

so wird sein

$$f(x_1, x_2, 0, \ldots\ldots 0) = \varphi(x_1, x_2, 0, \ldots\ldots 0)\, \psi(x_1, x_2, 0, \ldots\ldots 0);$$

nun füge man in φ und ψ Glieder der Form

$$x_1^k x_2^l x_3, \quad (\text{wo } k + l = q - 1 \text{ in } \varphi, \text{ und } = m - q - 1 \text{ in } \psi \text{ ist})$$

mit unbestimmten Koeffizienten hinzu, so erhält man ebensoviel lineare Gleichungen, um dieselben zu bestimmen; dann berechne

man in derselben Weise die Glieder in $x_1^k x_2^l x_3$ u. s. w., so ergiebt sich zuletzt

$$\varphi(x_1, x_2, x_3, 0, \ldots\ldots 0) \text{ und } \psi(x_1, x_2, x_3, 0, \ldots\ldots 0).$$

Auf dieselbe Weise fortfahrend, gelangt man successive zur Kenntnis der Glieder, welche ausser x_1, x_2, x_3 auch x_4, hierauf derer, welche noch x_5 enthalten u. s. f. Man sieht also, dass die gemeinsamen Faktoren von f und F ein Produkt bilden, welches selbst eine zerlegbare Form mit rationalen Koeffizienten ist.

Sei nun U das Produkt aus Faktoren von f, welche α mal, V derer, welche β mal vorkommen, u. s. w.; also

$$f = U^\alpha V^\beta W^\gamma \ldots\ldots$$
$$\text{und } \alpha > \beta > \gamma > \ldots\ldots;$$

dann ist

$$\frac{\partial f}{\partial x_1} = U^{\alpha-1} V^{\beta-1} W^{\gamma-1} \ldots \left\{ \alpha \frac{\partial U}{\partial x_1} VW \ldots + \beta U \frac{\partial V}{\partial x_1} W \ldots + \ldots \right\}$$

und es ist

$$f_1 = U^{\alpha-1} V^{\beta-1} W^{\gamma-1} \ldots\ldots$$

der grösste gemeinschaftliche Faktor von f und $\frac{\partial f}{\partial x_1}$; also eine zerlegbare Funktion mit rationalen Koeffizienten. Hieraus bestimmt sich in derselben Weise

$$f_2 = U^{\alpha-2} V^{\beta-2} W^{\gamma-2} \ldots\ldots;$$

fährt man so fort, so erhält man zuletzt U allein, hierauf successive $V, W, \ldots\ldots$ Die Untersuchung reduziert sich daher auf die Betrachtung jeder der Formen $U, V, W, \ldots\ldots$ für sich.

Ist die Gleichung $\varphi(x, -1) = 0$ reduktibel, ohne gleiche Wurzeln zu haben, so sei $\psi(x)$ ein irreduktibler Faktor p^{ten} Grades derselben und $\omega_1, \omega_2, \ldots\ldots \omega_p$ seine Wurzeln. Alsdann ist das Produkt der Faktoren

$$\overset{1}{u}\,\overset{2}{u}\,\overset{3}{u} \ldots\ldots \overset{p}{u}$$

eine symmetrische Funktion von $\omega_1, \omega_2, \ldots\ldots \omega_p$; also eine zerlegbare Form mit rationalen Koeffizienten. Die Form f reduziert sich daher auch in diesem Falle auf ein Produkt von zerlegbaren Formen, entsprechend den irreduktibeln Faktoren von $\varphi(x, -1) = 0$.

Endlich kann an Stelle der Gleichung $\varphi(x, -1) = 0$ eine solche gesetzt werden, in welcher der Koeffizient der höchsten Potenz die

Einheit ist, wenn an Stelle der Wurzel ω die Wurzel $a\,\omega$ eingeführt wird, und es können die Koeffizienten von $x_1, x_2, \ldots\ldots x_n$ in $\overset{1}{u}, \overset{2}{u}, \ldots\ldots \overset{n}{u}$ als ganze komplexe Zahlen angenommen werden, wenn nachher die Funktion durch eine entsprechende ganze Zahl, welche gemeinschaftlicher Teiler ihrer Koeffizienten sein wird, wieder dividiert wird.

§ 4.

Nach allem diesen rechtfertigt es sich, der Diskussion folgende Form der zerlegbaren Formen zu Grunde zu legen:

„Es sei

$$\omega^n + p_1\,\omega^{n-1} + \cdots\cdots + p_n = 0$$

eine Gleichung, in welcher der Koeffizient der höchsten Potenz $= 1$ und die übrigen Koeffizienten reelle ganze Zahlen sind, und welche sich nicht in Faktoren derselben Art zerlegen lasse (also irreduktibel sei);

$$\omega_1, \omega_2, \ldots\ldots \omega_n$$

seien ihre Wurzeln und

$$\overset{k}{u} = \overset{k}{u}_1 x_1 + \overset{k}{u}_2 x_2 + \cdots\cdots + \overset{k}{u}_n x_n$$

eine lineare homogene Funktion von n Unbestimmten

$$x_1, x_2, \ldots\ldots x_n,$$

deren Koeffizienten

$$\overset{k}{u}_1, \overset{k}{u}_2, \ldots\ldots \overset{k}{u}_n$$

ganze ganzzahlige Funktionen der Wurzeln ω_k seien, also von der Form

$$\overset{k}{u}_r = \overset{r}{a}_0 + \overset{r}{a}_1\,\omega_k + \overset{r}{a}_2\,\omega_k^2 + \cdots\cdots + \overset{r}{a}_{n-1}\,\omega_k^{n-1},$$

wo die Koeffizienten a reelle ganze Zahlen sind.

Alsdann ist das Produkt

$$\overset{1}{u}\,\overset{2}{u} \ldots\ldots \overset{n}{u}$$

eine homogene ganze ganzzahlige Funktion n^{ten} Grades von $x_1, x_2 \ldots\ldots x_n$. Die Koeffizienten können noch einen allen gemeinschaftlichen Zahlfaktor haben; der grösste sei m, so ist endlich

$$f(x_1, x_2, \ldots\ldots x_n) = \frac{1}{m}\,\overset{1}{u}\,\overset{2}{u} \ldots\ldots \overset{n}{u}$$

die den weitern Betrachtungen zu Grunde zu legende Form."

Im folgenden soll nun für ω die reelle Kubikwurzel aus einer positiven ganzen Zahl D angenommen werden und ausserdem (was nur eine scheinbare Beschränkung ist) soll D durch keine dritte Potenz einer Primzahl teilbar sein, also keinen kubischen Faktor enthalten. Es ist also vor allem die Theorie der aus solchen Wurzeln gebildeten komplexen Zahlen zu entwickeln.

II.

§ 5. Einleitendes.

Es seien ω die reelle, ω', ω'' die konjugiert-imaginären Wurzeln der Gleichung

$$\omega^3 = D$$

und D eine ganze, positive, durch keine Kubikzahl teilbare Zahl. Der Ausdruck

$$\varphi(\omega) = a + b\,\omega + c\,\omega^2$$

heisst eine komplexe ganze Zahl in ω, wenn a, b, c ganze Zahlen sind. Im folgenden soll der Kürze wegen unter einer komplexen Zahl, wo nicht ausdrücklich das Gegenteil erwähnt wird, immer eine ganze komplexe Zahl verstanden sein. Das Produkt der drei konjugierten Faktoren

$$(a + b\,\omega + c\,\omega^2)\,(a + b\,\omega' + c\,\omega'^2)\,(a + b\,\omega'' + c\,\omega''^2)$$
$$= a^3 + D\,b^3 + D^2\,c^3 - 3\,D\,a\,b\,c$$

heisst die Norm jedes derselben und soll mit $N(a + b\,\omega + c\,\omega^2)$ bezeichnet werden. Ist es der Einheit gleich, so heisst $\varphi(\omega)$ eine komplexe Einheit.

Es sind nun zunächst die Bedingungen aufzustellen, unter welchen eine solche Norm durch eine reelle Primzahl teilbar ist. Dies geschieht mit Hülfe von Kongruenzen in Bezug auf diese Primzahlen als Moduln und zwar ist zu diesem Zwecke zuerst die Kongruenz

$$z^3 \equiv D$$

zu behandeln. Hierbei verhalten sich aber die verschiedenen reellen Primzahlen wesentlich verschieden; ich werde sie in fünf Kategorien sondern, und zwar sollen p, q, r Primzahlen bedeuten,

welche nicht in D aufgehen, die Primzahlen s und t dagegen sollen in D enthalten sein und zwar die ersteren einfach, die letztern im Quadrat. Ferner sollen mit p diejenigen Primzahlen der Form $6n+1$ bezeichnet werden, für welche D kubischer Rest, mit q diejenigen, für welche D kubischer Nichtrest ist; die Primzahlen r endlich sind die von der Form $6n-1$. Was die Zahlen 2 und 3 anbetrifft, so sind dieselben besonders zu untersuchen.

Da im folgenden von imaginären Kongruenzwurzeln Gebrauch gemacht wird, so mag noch nachstehender Satz über dieselben besonders hervorgehoben werden:

„Sei $$f(x) \equiv 0 \pmod{m}$$

eine irreduktible Kongruenz n^{ten} Grades nach dem Primzahlmodulus m, und i eine ihrer Wurzeln, so lässt sich jede ganze ganzzahlige Funktion $\varphi(i)$ von i auf die Form bringen:

$$a_0 + a_1 i + a_2 i^2 + \cdots\cdots + a_{n-1} i^{n-1}.$$

Ein Produkt aus solchen Funktionen $\varphi, \varphi', \varphi'', \ldots\ldots$ ist nicht anders durch m teilbar, als wenn eine dieser Funktionen, z. B. φ es ist, d. h. es müssen die Koeffizienten $a_0, a_1, a_2 \ldots\ldots a_{n-1}$ alle durch m teilbar sein."

Ist m eine Primzahl der Form $6n+1$, so hat die Kongruenz

$$x^3 \equiv 1 \pmod{m}$$

die drei reellen Wurzeln

$$1, \quad \frac{-1+\sqrt{-3}}{2}, \quad \frac{-1-\sqrt{-3}}{2}$$

wo $\sqrt{-3}$ irgend eine ungerade Zahl bedeutet, deren Quadrat $\equiv -3 \pmod{m}$. Ist also z irgend eine Wurzel der Kongruenz

$$z^3 \equiv D \pmod{m},$$

so sind die übrigen

$$\frac{-1 \pm \sqrt{-3}}{2} z$$

und es sind die drei Wurzeln reell oder imaginär, je nachdem m zu den Primzahlen p oder q gehört. Ebenso hat die Kongruenz

$$\xi_\mu^3 \equiv D \pmod{p^\mu}$$

drei reelle, nach dem Modul p inkongruente Wurzeln.

Die Kongruenz

$$\eta_{\mu}^{3} \equiv D \pmod{r^{\mu}}$$

dagegen hat nur eine reelle Wurzel η_{μ}; die beiden andern sind

$$\eta_{\mu}\,\tau \text{ und } \eta_{\mu}\,\tau^{2},$$

wenn $\tau = \frac{-1+\sqrt{-3}}{2}$ eine Wurzel der irreduktibeln Kongruenz

$$\tau^{2} + \tau + 1 \equiv 0 \pmod{r}$$

bezeichnet.

§ 6. Teilbarkeit der Norm durch eine reelle Primzahl.

Mit Hülfe dieser Sätze entscheidet sich nun die Teilbarkeit von $N(a + b\,\omega + c\,\omega^{2}) = N\varphi(\omega)$ durch eine reelle Primzahl in folgender Weise:

Bezeichnet man mit z_{μ}, z'_{μ}, z''_{μ} die reellen oder imaginären Kongruenzwurzeln von

$$z^{3} \equiv D \pmod{m^{\mu}},$$

wo m eine der Primzahlen p, q, r bedeutet, so ist

$$N(a+b\omega+c\omega^{2}) \equiv (a+bz_{\mu}+cz_{\mu}^{2})(a+bz'_{\mu}+cz'^{2}_{\mu})(a+bz''_{\mu}+cz''^{2}_{\mu}) \pmod{m^{\mu}};$$

denn wie bei der Reduktion ganzer Funktionen von ω, ω', ω'' die Gleichungen in Anwendung kommen:

$$\omega + \omega' + \omega'' = 0, \quad \omega'\,\omega'' + \omega''\,\omega + \omega\,\omega' = 0, \quad \omega\,\omega'\,\omega'' = D,$$

so kommen bei der Reduktion von ganzen Funktionen der Kongruenzwurzeln z_{μ}, z'_{μ}, z''_{μ} in Anwendung die Kongruenzen

$$z_{\mu} + z'_{\mu} + z''_{\mu} \equiv 0, \quad z'_{\mu}z''_{\mu} + z''_{\mu}z_{\mu} + z_{\mu}z'_{\mu} \equiv 0, \quad z_{\mu}z'_{\mu}z''_{\mu} \equiv D \pmod{m^{\mu}}.$$

Hieraus aber ergiebt sich sofort, wenn mit ξ, η wie oben die resp. den p, r entsprechenden Kongruenzwurzeln bezeichnet werden:

1. Damit $N\varphi(\omega)$

durch p^{μ} teilbar sei, nicht aber durch $p^{\mu+1}$, muss das Produkt

$$\varphi(\xi_{\mu}) \cdot \varphi(\xi'_{\mu}) \cdot \varphi(\xi''_{\mu})$$

durch p^{μ}, das Produkt aber

$$\varphi(\xi_{\mu+1}) \cdot \varphi(\xi'_{\mu+1}) \cdot \varphi(\xi''_{\mu+1})$$

nicht durch $p^{\mu+1}$ teilbar sein.

2. Damit

$$N\varphi(\omega) = N(a + b\omega + c\omega^2)$$

durch q teilbar sei, muss jeder der Koeffizienten a, b, c durch q teilbar sein, weil $z^3 \equiv D \pmod{q}$ eine irreduktible Gleichung ist. Die Norm ist dann aber durch q^3 teilbar. Und allgemein: damit $N(a + b\omega + c\omega^2)$ durch $q^{3\mu}$, aber durch keine höhere Potenz von q teilbar sei, müssen a, b, c durch q^μ, aber nicht alle durch $q^{\mu+1}$ teilbar sein.

3. Damit $N\varphi(\omega)$

durch r^μ teilbar sei, nicht aber durch $r^{\mu+1}$, muss das Produkt

$$\varphi(\eta_\mu) \cdot \varphi(\tau\eta_\mu) \cdot \varphi(\tau^2\eta_\mu)$$

durch r^μ, dagegen das Produkt

$$\varphi(\eta_{\mu+1}) \cdot \varphi(\tau\eta_{\mu+1}) \cdot \varphi(\tau^2\eta_{\mu+1})$$

nicht durch $r^{\mu+1}$ teilbar sein. Die Bedingung, dass

$$\varphi(\tau\eta_\mu) = a + b\tau\eta_\mu + c\tau^2\eta_\mu^2 \equiv a + b\tau\eta_\mu + c(1+\tau)\eta_\mu^2$$

durch r^μ teilbar sei, zerfällt aber in die beiden folgenden:

$$a - c\eta_\mu^2 \equiv 0, \quad b - c\eta_\mu \equiv 0 \pmod{r^\mu},$$

und es ist dann zugleich auch

$$\varphi(\tau^2\eta_\mu) = a + b\tau^2\eta_\mu + c\tau\eta_\mu \equiv 0 \pmod{r^\mu}.$$

4. Für die Zahlen s und t ergeben sich die Bedingungen leicht durch direkte Betrachtung der Norm

$$N\varphi(\omega) + a^3 + Db^3 + D^2c^3 - 3Dabc;$$

nämlich es ist $N\varphi(\omega) + N(a + b\omega + c\omega^2)$

durch s teilbar, wenn a durch s teilbar ist,
durch s^2 teilbar, wenn a, b durch s teilbar sind,
durch s^3 teilbar, wenn a, b, c durch s teilbar sind,

und allgemein

durch $s^{3\mu+\nu}$ teilbar, wenn a, b, c durch s^μ und
$N\left(\frac{a}{s^\mu} + \frac{b}{s^\mu}\omega + \frac{c}{s^\mu}\omega^2\right)$ durch s^ν teilbar ist.

5. Was die Primzahlen t anbetrifft, so kann $N(a + b\omega + c\omega^2)$ niemals bloss durch t teilbar sein; ferner ist $N(a + b\omega + c\omega^2)$

durch t^2 teilbar, wenn a durch t teilbar ist,
durch t^3 teilbar, wenn a, b durch t teilbar sind,

durch t^4 teilbar, wenn a durch t^2, b durch t teilbar ist,
durch t^5 teilbar, wenn a durch t^2, b, c durch t teilbar sind, etc.;
allgemein: damit $N(a+b\omega+c\omega^2)$ durch $t^{3\mu+\nu}$ teilbar sei für $\mu>0$, müssen a, b, c durch $t^{\mu-1}$ und $N\left(\frac{a+b\omega+c\omega^2}{t^{\mu-1}}\right)$ durch $t^{3+\nu}$ teilbar sein.

6. Die Zahl 2 schliesst sich in ihrem Verhalten für ein gerades D den Zahlen s und t an, für ein ungerades den Zahlen r; denn in letzterem Fall hat die Kongruenz

$$z^3 \equiv D \pmod 2$$

die reelle Wurzel 1, die übrigen sind Wurzeln der irreduktibeln Kongruenz

$$\tau^2+\tau+1 \equiv 0 \pmod 2.$$

Die Zahl 3 endlich verhält sich wie die Zahlen s oder t, jenachdem D durch 3 oder durch 3^2 teilbar ist.

Ist D weder $\equiv 0$, mod 3, noch $D^2 \equiv 1$, mod 9, so findet man leicht die Bedingungen:

Es ist $N(a+b\omega+c\omega^2)$
$\equiv 0 \pmod 3$, wenn $a+Db+c \equiv 0 \pmod 3$,
$\equiv 0 \pmod{3^2}$, wenn $a \equiv Db \equiv c \pmod 3$,
$\equiv 0 \pmod{3^3}$, wenn $a \equiv b \equiv c \equiv 0 \pmod 3$.

Ist $D^2 \equiv 1 \pmod 9$, so lassen sich keine so einfachen Bedingungen mehr aufstellen; indess ist für das Folgende die Betrachtung dieses Falles überflüssig.

§ 7. Definition der idealen Primfaktoren.

Auf obiges gestützt ergiebt sich nun folgende Definition der idealen Primfaktoren der komplexen Zahl $\varphi(\omega) = a+b\omega+c\omega^2$.

1. Die Primzahlen p sind als aus drei komplexen Primfaktoren bestehend zu betrachten; sie ordnen sich den Kongruenzwurzeln ξ, ξ', ξ'' zu, indem man sagt:

$\varphi(\omega)$ enthält den zur Kongruenzwurzel ξ gehörenden Primfaktor von p und zwar genau μ mal,
wenn $\varphi(\xi_\mu)$ durch p^μ, aber $\varphi(\xi_{\mu+1})$ nicht durch $p^{\mu+1}$ teilbar ist und ganz ebenso sind

$$\varphi(\xi'_\mu) \equiv 0 \pmod{p^\mu}, \quad \varphi(\xi''_\mu) \equiv 0 \pmod{p^\mu}$$

die Bedingungen, dass $\varphi(\omega)$ die resp. zu ξ' und ξ'' gehörenden Primfaktoren von p je μ mal enthalte.

Was nun die konjugierten Faktoren $a + b\omega' + c\omega'^2$ und $a + b\omega'' + c\omega''^2$ anbetrifft, so ist hierüber Folgendes zu bemerken:

Sind π, π', π'' die drei Primfaktoren von p, und enthält

$\varphi(\omega)$ den Faktor $\pi^\alpha \pi'^\beta \pi''^\gamma$, so nehme ich an, es enthalte
$\varphi(\omega')$ den Faktor $\pi'^\alpha \pi''^\beta \pi^\gamma$ und
$\varphi(\omega'')$ den Faktor $\pi''^\alpha \pi^\beta \pi'^\gamma$.

Diese Zuordnung ist aber eine willkürliche, indem man ebenso gut sagen könnte, es enthalte

$\varphi(\omega')$ den Faktor $\pi''^\alpha \pi^\beta \pi'^\gamma$,
$\varphi(\omega'')$ den Faktor $\pi'^\alpha \pi''^\beta \pi^\gamma$.

Für gegenwärtige Zwecke ist es aber gleichgültig, welche der beiden Anordnungen gewählt werde, da $\varphi(\omega')$ und $\varphi(\omega'')$ immer symmetrisch auftreten werden.

2. Da $N\varphi(\omega)$ nicht anders durch die Primzahl q teilbar sein kann, als wenn $\varphi(\omega)$ es ist, so ist q auch in der komplexen Theorie eine Primzahl.

3. Die Primzahl r besteht wieder aus drei Primfaktoren $\varrho, \varrho', \varrho''$, und zwar enthält $\varphi(\omega)$ den zur reellen Kongruenzwurzel η gehörenden Primfaktor von r genau μ mal, wenn

$\varphi(\eta_\mu) \equiv 0 \pmod{r^\mu}$ ist, aber $\varphi(\eta_{\mu+1})$ nicht $\equiv 0 \pmod{r^{\mu+1}}$.

Ferner enthält $\varphi(\omega)$ jeden der zu den imaginären Kongruenzwurzeln gehörenden Primfaktoren ϱ', ϱ'' genau μ mal, wenn zugleich

$$a - c\eta_\mu^2 \equiv 0, \quad b - c\eta_\mu \equiv 0 \pmod{p^\mu},$$

aber nicht zugleich

$$a - c\eta_{\mu+1}^2 \equiv 0, \quad b - c\eta_{\mu+1} \equiv 0 \pmod{p^{\mu+1}}$$

ist, oder kürzer, wenn

$\varphi(\tau\eta_\mu) \equiv 0 \pmod{p^\mu}$, aber $\varphi(\tau\eta_{\mu+1})$ nicht $\equiv 0 \pmod{p^{\mu+1}}$.

Ferner soll hier wiederum angenommen werden, wenn

$\varphi(\omega)$ den Faktor $\varrho^\alpha(\varrho'\varrho'')^\beta$ enthält, so enthalte
$\varphi(\omega')$ den Faktor $\varrho'^\alpha(\varrho''\varrho)^\beta$ und
$\varphi(\omega'')$ den Faktor $\varrho''^\alpha(\varrho\varrho')^\beta$.

4. Von idealen Primfaktoren der Zahlen s und t, sowie der Zahl 3 sehe ich ab, da die Einführung solcher für das folgende keinen Vorteil gewährt. Wenn daher im folgenden von idealen Zahlen die Rede ist, so sind damit immer solche gemeint, deren Normen zu $3D$ prim sind.

§ 8. Eigenschaften der idealen Primfaktoren.

Es ist nun zu beweisen, dass die so definierten idealen Primfaktoren wirklich den Charakter von Primfaktoren besitzen. Dies geschieht durch folgende Sätze:

1. Wenn keine der Zahlen $\varphi(\omega)$, $\psi(\omega)$ den komplexen Primfaktor ω enthält, so enthält ihn auch das entwickelte Produkt nicht.

a) Enthalten die beiden Zahlen den zu ξ gehörenden Primfaktor von p nicht, so ist von den reellen Zahlen $\varphi(\xi)$ und $\psi(\xi)$ der Voraussetzung nach keine durch p teilbar, also auch ihr Produkt nicht, noch der ihm kongruente Ausdruck, welchen man erhält, wenn man an Stelle von $\xi^3 D$ setzt. Dieser Ausdruck aber entsteht auch, wenn man im entwickelten Produkt $\varphi(\omega).\psi(\omega)$ die Gleichungswurzel ω durch die Kongruenzwurzel ξ ersetzt; folglich enthält dieses Produkt den zu ξ gehörenden Primfaktor von p nicht.

b) Soll

$$N(\varphi(\omega).\psi(\omega)) = N\varphi(\omega).N\psi(\omega)$$

durch q teilbar sein, so muss einer der Faktoren es sein; dies kann aber nur geschehen, wenn entweder $\varphi(\omega)$ oder $\psi(\omega)$ durch q teilbar ist; folglich etc.

c) Enthält keine der Zahlen $\varphi(\omega)$, $\psi(\omega)$ den zu η gehörenden Primfaktor von r, so ist weder $\varphi(\eta)$, noch $\psi(\eta)$ durch r teilbar und der Satz ergiebt sich wie für die Zahlen p.

Enthalten die Zahlen $\varphi(\omega)$, $\psi(\omega)$ die zu den imaginären Kongruenzwurzeln gehörenden Primfaktoren von r nicht, so ist weder $\varphi(\tau\eta) = a - c\eta^2 + \tau(b\eta - c\eta^2)$, noch $\psi(\tau\eta) = a' - c'\eta^2 + \tau(b'\eta - c'\eta^2)$ durch r teilbar, also auch das Produkt nicht, da sonst wegen der Irreduktibilität der Kongruenz

$$\tau^2 + \tau + 1 \equiv 0 \pmod{r}$$

einer der Faktoren es sein müsste.

2. Wenn $\varphi(\omega)$ einen Primfaktor ω genau μ mal, $\psi(\omega)$ genau ν mal enthält, so enthält ihn das entwickelte Produkt $f(\omega)$ genau $\mu + \nu$ mal.

a) Der Voraussetzung nach ist

$$\varphi(\xi_\mu) \equiv 0 \pmod{p^\mu}, \quad \varphi(\xi_{\mu+1}) \text{ nicht} \equiv 0 \pmod{p^{\mu+1}}$$

also auch $\varphi(\xi_{\mu+\nu}) \equiv 0 \pmod{p^\mu}$, $\varphi(\xi_{\mu+\nu+1})$ nicht $\equiv 0 \pmod{p^{\mu+1}}$,

ebenso $\psi(\xi_{\mu+\nu}) \equiv 0 \pmod{p^\nu}$, $\psi(\xi_{\mu+\nu+1})$ nicht $\equiv 0 \pmod{p^{\nu+1}}$;

also ist

$$f(\xi_{\mu+\nu}) \equiv \varphi(\xi_{\mu+\nu}) \cdot \psi(\xi_{\mu+\nu}) \equiv 0 \pmod{p^{\mu+\nu}};$$

$$f(\xi_{\mu+\nu+1}) \equiv \varphi(\xi_{\mu+\nu+1}) \cdot \psi(\xi_{\mu+\nu+1}) \text{ nicht} \equiv 0 \pmod{p^{\mu+\nu+1}}.$$

b) Ist $\varphi(\omega)$ durch q^μ, $\psi(\omega)$ durch q^ν teilbar, so ist $f(\omega) = \varphi(\omega) \cdot \psi(\omega)$ durch $q^{\mu+\nu}$ teilbar, aber nicht durch $q^{\mu+\nu+1}$, da weder

$$\frac{\varphi(\omega)}{q^\mu} = \left(\frac{a}{q^\mu} + \frac{b}{q^\mu}\omega + \frac{c}{q^\mu}\omega^2\right), \text{ noch } \frac{\psi(\omega)}{q^\nu} = \left(\frac{a'}{q^\nu} + \frac{b'}{q^\nu}\omega + \frac{c'}{q^\nu}\omega^2\right)$$

durch q teilbar sind.

c) Für den zur reellen Kongruenzwurzel gehörenden Primfaktor von r folgt der Beweis wie oben für die Primzahl p, wenn ξ durch η, für die beiden andern, wenn ξ durch $\eta\tau$ ersetzt wird.

3. Wenn

$$\varphi(\omega) = a + b\omega + c\omega^2$$

alle Primfaktoren von p oder r enthält, jeden mindestens μ mal, so ist es resp. durch p^μ oder r^μ teilbar.

Denn der Voraussetzung nach gelten für p und r resp. die Kongruenzen

$$\begin{aligned} &a + b\xi_\mu + c\xi_\mu^2 \equiv 0 \pmod{p^\mu}; && a + b\eta_\mu + c\eta_\mu^2 \equiv 0 \pmod{r^\mu}, \\ &a + b\xi'_\mu + c\xi'^2_\mu \equiv 0, && a + b\tau\eta_\mu + c\tau^2\eta_\mu^2 \equiv 0, \\ &a + b\xi''_\mu + c\xi''^2_\mu \equiv 0, && a + b\tau^2\eta_\mu + c\tau\eta_\mu^2 \equiv 0; \end{aligned}$$

die Determinanten dieser linearen Systeme aber sind resp. nicht durch p oder r teilbar, da ihre Quadrate $\equiv -27D^2$ sind, resp. nach den Moduln p oder r. Es müssen somit a, b, c resp. durch p^μ, r^μ teilbar sein.

4. Wenn $\varphi(\omega)$

die Primfaktoren von p resp. μ, μ', μ'' mal enthält, so ist $N\varphi(\omega)$ durch $p^{\mu+\mu'+\mu''} = p^{\lambda}$

teilbar; denn der Voraussetzung nach ist

$$\varphi(\xi_{\mu}) \equiv \varphi(\xi_{\lambda}) \equiv 0 \pmod{p^{\mu}},$$
$$\varphi(\xi'_{\mu'}) \equiv \varphi(\xi'_{\lambda}) \equiv 0 \pmod{p^{\mu'}},$$
$$\varphi(\xi''_{\mu''}) \equiv \varphi(\xi''_{\lambda}) \equiv 0 \pmod{p^{\mu''}};$$

somit

$$\varphi(\xi_{\lambda}) \cdot \varphi(\xi'_{\lambda}) \cdot \varphi(\xi''_{\lambda}) \equiv N\varphi(\omega) \equiv 0 \pmod{p^{\lambda}}.$$

Ebenso, wenn $\varphi(\omega)$ den zur reellen Kongruenzwurzel gehörenden Primfaktor von r μ mal, die beiden andern μ' mal enthält, ist

$$N\varphi(\omega) \equiv 0 \pmod{r^{\cdot \mu + 2\mu'}}.$$

Da nun die Norm jeder komplexen ganzen Zahl eine reelle ganze Zahl von endlicher Grösse ist und die oben aufgestellten Kongruenzen das Vorkommen jedes Primfaktors von p, q, r in unzweideutiger Weise bestimmen, so folgt der Satz:

5. Jede gegebene komplexe ganze Zahl enthält nur eine endliche Anzahl unveränderlich bestimmter Primfaktoren.

6. Ist $\varphi(\omega)$ eine wirkliche komplexe Zahl, deren Norm zu $3D$ prim ist und enthält die wirkliche komplexe Zahl $\psi(\omega)$ alle Primfaktoren von $\varphi(\omega)$ und jeden mindestens ebenso oft, so ist $\psi(\omega)$ durch $\varphi(\omega)$ teilbar, d. h. der Quotient $\frac{\psi(\omega)}{\varphi(\omega)}$ ist eine wirkliche komplexe Zahl.

Denn $\psi(\omega)\,\varphi(\omega')\,\varphi(\omega'')$

enthält alle Primfaktoren von p, r, welche in

$$N\varphi(\omega) = \varphi(\omega)\,\varphi(\omega')\,\varphi(\omega'')$$

enthalten sind, mindestens ebenso oft, ist daher nach 3. einzeln durch die in $N\varphi(\omega)$ enthaltenen Primzahlpotenzen teilbar, also der Quotient

$$\frac{\psi(\omega)\,\varphi(\omega')\,\varphi(\omega'')}{N\varphi(\omega)} = \frac{\psi(\omega)}{\varphi(\omega)}$$

eine ganze Zahl.

Wenn im weitern von der Teilbarkeit einer wirklichen oder idealen komplexen Zahl durch eine andere gesprochen wird, so soll darunter verstanden sein, es enthalte der Dividend alle idealen Primfaktoren des Divisors (welcher zu 3 D prim anzunehmen ist) und jeden mindestens ebenso oft wie dieser.

7. Sind $\varphi(\omega)$ und $\psi(\omega)$ beide prim zu 3 D (d. h. ihre Normen) und enthalten sie jeden idealen Primfaktor von p, q, r gleich oft, so ist, der Quotient

$$\frac{\psi(\omega)}{\varphi(\omega)}$$

eine komplexe Einheit.

§ 9. Multiplikatoren; Endlichkeit der Klassenanzahl.

Es soll nun zunächst nachgewiesen werden, dass man immer eine komplexe Zahl $a + b\omega + c\omega^2$ finden kann, welche alle idealen Primfaktoren einer idealen Zahl $J(\omega)$ mindestens ebenso oft enthält, wie diese letztere und für welche der Quotient

$$\frac{N(a + b\omega + c\omega^2)}{NJ(\omega)}$$

unter einer bestimmten endlichen Grenze liegt.

Es enthalte $J(\omega)$ den zu ξ gehörenden Primfaktor von p μ mal, den zu ξ' gehörenden μ' mal und den zu ξ'' gehörenden μ'' mal; ebenso die Primfaktoren von p, resp. μ_1, μ_1', μ_1'' mal u. s. w.; die Primzahl q λ mal, q_1 λ_1 mal etc.; die zu η, $\eta\tau$ gehörenden Primfaktoren von r resp. ν, ν' mal etc.; dann müssen die Koeffizienten a, b, c folgenden Systemen von Kongruenzen genügen:

$$a + b\xi_\mu + c\xi_\mu^2 \equiv 0 \pmod{p^\mu}; \quad a + b\overset{(1)}{\xi}_{\mu_1} + c\overset{(1)}{\xi}{}^2_{\mu_1} \equiv (0 \bmod p_1^{\mu_1});$$

$$a + b\xi'_{\mu'} + c\xi'^2_{\mu'} \equiv 0 \pmod{p^{\mu'}}; \quad a + b\overset{(1)}{\xi}{}'_{\mu_1'} + c\overset{(1)}{\xi}{}'^2_{\mu_1'} \equiv 0 \pmod{p_1^{\mu_1'}};$$

$$a + b\xi''_{\mu''} + c\xi''^2_{\mu''} \equiv 0 \pmod{p^{\mu''}}; \quad a + b\overset{(1)}{\xi}{}''_{\mu_1''} + c\overset{(1)}{\xi}{}''^2_{\mu_1''} \equiv 0 \pmod{p_1^{\mu_1''}}$$

etc.

$$a \equiv 0 \pmod{q^{\lambda}}, \quad a \equiv 0 \pmod{q_1^{\lambda_1}},$$
$$b \equiv 0 \qquad\qquad b \equiv 0$$
$$c \equiv 0 \qquad\qquad c \equiv 0$$
$$\text{etc.}$$

$$a + b\eta_{\nu} + c\eta_{\nu}^{2} \equiv 0 \pmod{r^{\nu}}; \quad a + b\overset{(1)}{\eta}_{\nu_1} + c\overset{(1)2}{\eta}_{\nu_1} \equiv 0 \pmod{r_1^{\nu}};$$
$$\left.\begin{aligned} a - c\eta_{\nu'}^{2} &\equiv 0 \\ b - c\eta_{\nu'} &\equiv 0 \end{aligned}\right\} \pmod{r^{\nu'}}; \qquad \left.\begin{aligned} a - c\overset{(2)2}{\eta}_{\nu_1'} &\equiv 0 \\ b - c\overset{(1)}{\eta}_{\nu_1'} &\equiv 0 \end{aligned}\right\} \pmod{r_1^{\nu_1'}};$$
$$\text{etc.}$$

Diese Kongruenzen lassen sich zusammenziehen. Man bestimme

$$\xi \equiv \xi_{\mu} \pmod{p^{\mu}}; \quad \xi' \equiv \xi'_{\mu'} \pmod{p^{\mu'}}; \quad \xi'' \equiv \xi''_{\mu''} \pmod{p^{\mu''}};$$
$$\equiv \overset{(1)}{\xi}_{\mu_1} \pmod{p^{\mu_1}}; \quad \equiv \overset{(1)}{\xi}'_{\mu_1'} \pmod{p^{\mu_1'}}; \quad \equiv \overset{(1)}{\xi}''_{\mu_1''} \pmod{p_1^{\mu_1''}};$$
$$\text{etc.} \qquad\qquad \text{etc.} \qquad\qquad \text{etc.}$$

$$\eta \equiv \eta_{\nu} \pmod{r^{\nu}}; \qquad \eta' \equiv \eta'_{\nu'} \pmod{r^{\nu'}};$$
$$\equiv \eta_{\nu_1} \pmod{r_1^{\nu_1}}; \qquad \equiv \overset{(1)}{\eta}'_{\nu_1'} \pmod{r_1^{\nu_1'}};$$
$$\text{etc.} \qquad\qquad \text{etc.},$$

so hat man die Kongruenzen

$$a + b\xi + c\xi^{2} \equiv 0 \pmod{p^{\mu} p_1^{\mu_1} \ldots .}; \quad a \equiv 0,$$
$$a + b\xi' + c\xi'^{2} \equiv 0 \pmod{p^{\mu'} p_1^{\mu_1'} \ldots .}; \quad b \equiv 0 \pmod{q^{\lambda} q_1^{\lambda_1} \ldots .}$$
$$a + b\xi'' + c\xi''^{2} \equiv 0 \pmod{p^{\mu''} p_1^{\mu_1''} \ldots .}; \quad c \equiv 0,$$

$$a + b\eta + c\eta^{2} \equiv 0 \pmod{r^{\nu} r_1^{\nu_1} \ldots .}$$
$$\left.\begin{aligned} a - c\eta'^{2} &\equiv 0 \\ b - c\eta' &\equiv 0 \end{aligned}\right\} \pmod{r^{\nu'} r_1^{\nu_1'} \ldots .}$$

Die Norm der Zahl $J(\omega)$ ist

$$NJ(\omega) = p^{\mu+\mu'+\mu''} p_1^{\mu_1+\mu_1'+\mu_1''} \ldots q^{3\lambda} q_1^{3\lambda_1} \ldots r^{\nu+2\nu'} r_1^{\nu_1+2\nu_1'} \ldots .$$

und genau ebenso gross ist die Anzahl der verschiedenen Restenkombinationen für sämtliche Moduln. Bestimmt man nun die ganze Zahl k so, dass

$$k^3 < NJ(\omega) < (k+1)^3,$$

und giebt den Koeffizienten a, b, c unabhängig von einander die $k+1$ Werte

$$0, 1, 2, \ldots . k,$$

so erhält man $(k+1)^3$ Kombinationen, unter welchen daher vermöge der obigen Ungleichheiten notwendig gleiche vorkommen müssen. Die Differenzen

$$a = a_1 - a_2, \quad b = b_1 - b_2, \quad c = c_1 - c_2$$

der Zahlen a_1, b_1, c_1 und a_2, b_2, c_2, welche solche identische Kombinationen liefern, geben offenbar eine Lösung jener Kongruenzen. Die gefundenen Werte a, b, c aber liegen innerhalb der Grenzen $-k$ und $+k$ und es ist daher der absolute Wert von $N(a+b\omega+c\omega^2)$

$$< k^3 [1 + D + D^2 + 3D]$$

und somit

$$\frac{N(a+b\omega+c\omega^2)}{NJ(\omega)} < 1 + 4D + D^2.$$

Nennt man nun jede ideale Zahl, deren Produkt mit der idealen Zahl $J(\omega)$ eine wirkliche komplexe Zahl ist, einen Multiplikator von $J(\omega)$, so ist

$$M(\omega) = \frac{a+b\omega+c\omega^2}{J(\omega)}$$

ein solcher Multiplikator, dessen Norm

$$NM(\omega) < 1 + 4D + D^2.$$

Da nun die Anzahl idealer Zahlen, deren Norm unter eine bestimmte Grenze fällt, endlich ist, so folgt:

„Es giebt stets eine endliche bestimmte Anzahl von Multiplikatoren".

Ideale Zahlen, welche, mit demselben Multiplikator zusammengesetzt, wirkliche komplexe Zahlen geben, heissen äquivalent und gehören in dieselbe Klasse; die Anzahl der Klassen ist daher gleich

der Anzahl der Multiplikatoren und obiger Satz gleichbedeutend mit dem folgenden:

„Die Klassenanzahl der idealen komplexen Zahlen ist endlich".

In Bezug auf die weiter hieraus fliessenden Sätze mag auf die Abhandlungen von Herrn Prof. Kummer verwiesen werden.

Ich bemerke nur noch, dass man von den Multiplikatoren immer voraussetzen darf, dass ihre Normen zu $3D$ prim seien und dass sie keine wirkliche komplexe Zahl als Faktor enthalten. Denn die Zahlen a, b, c, sind nur nach dem Modul $NJ(\omega)$ bestimmt, welcher der Voraussetzung nach zu $3D$ prim ist, und man kann sie daher immer durch andere ihnen mod $NJ(\omega)$ resp. kongruente ersetzen, welche die Eigenschaft haben, dass sie keiner der Bedingungen Genüge leisten, welche erforderlich sind, wenn $N(a+b\omega+c\omega^2)$ eine in $3D$ aufgehende Primzahl enthalten soll.

§ 10. Komplexe Einheiten.

Nach dem Satze von Dirichlet (Monatsberichte der Berliner Akademie, März 1846) giebt es für die im Vorliegenden betrachteten komplexen Zahlen eine Einheit $E(\omega)$, von welcher alle übrigen Potenzen mit ganzen positiven oder negativen Exponenten sind.

Für das Folgende ist es aber notwendig, noch eine besondere Art gebrochener Einheiten in Betracht zu ziehen. Es bezeichne Θ^2 den grössten in D enthaltenen quadratischen Faktor, also Θ das Produkt sämtlicher Primzahlen t; ferner sei θ irgend ein Divisor von Θ, $g(\omega)=a+b\omega+c\omega^2$ eine komplexe Zahl, deren Norm $=\theta^3$ ist. Alsdann müssen, wie früher bewiesen, a, b durch θ teilbar, $\frac{a}{\theta}$ aber prim zu Θ sein. Enthielte nämlich $\frac{a}{\theta}$ noch die Primzahl t, so müsste $Ng(\omega)$ durch t^4 oder durch t^2 teilbar sein, je nachdem t in θ aufgeht oder nicht. c soll zu θ prim angenommen werden, denn sonst liesse sich der Bruch

$$\frac{g(\omega)}{\theta},$$

um den es sich hier handelt, reduzieren. Brüche dieser Form will ich der Kürze wegen hier als gebrochene Einheiten bezeichnen, da

$$N\left(\frac{g(\omega)}{\theta}\right)=1$$

ist, während unter „Einheit" schlechtweg immer eine ganze komplexe Zahl zu verstehen ist, deren Norm $= 1$.

Von diesen gebrochenen Einheiten gelten nun folgende Sätze:

1. Damit die n^{te} Potenz von $\frac{g(\omega)}{\theta}$ eine ganze Zahl sei, ist notwendig und hinreichend, dass n ein Vielfaches von θ sei.

Sei

$$g(\omega) = \theta(a' + b'\omega) + c\omega^2,$$

so ist

$$g(\omega)^n = \sum_{k=0}^{n} \frac{n(n-1)\ldots(n-k+1)}{1.\,2\ldots k}(a' + b'\omega)^{n-k}\,\theta^{n-k}\,c^k\,\omega^{2k}.$$

Da nun $\omega^3 = D$ durch θ^2 teilbar ist, so werden alle Glieder, für welche das Doppelte der grössten in $\frac{2k}{3}$ enthaltenen ganzen Zahl $\geqq k$ durch θ^n teilbar sein. Dies ist aber der Fall für alle ganzen Werte von k mit Ausnahme von $k = 1$, also ist

$$\begin{aligned} g(\omega)^n &\equiv n(a' + b'\omega)^{n-1} \cdot c\omega^2 \cdot \theta^{n-1} \pmod{\theta^n}, \\ &\equiv n\,a'^{n-1} c\omega^2 \theta^{n-1}. \end{aligned}$$

Nun sind der Voraussetzung nach a' und c beide prim zu θ; folglich kann $g(\omega)^n$ nicht anders durch θ^n teilbar sein, als wenn n es ist. w. z. b w.

Es mag noch ausdrücklich hervorgehoben werden, dass nach gehöriger Reduktion im Nenner des Produkts zweier Brucheinheiten $\frac{g(\omega)}{\theta}$ und $\frac{g'(\omega)}{\theta'}$ nur erste Potenzen der Primzahlen t vorkommen können; denn käme etwa t^2 vor, so wäre die Norm des Zählers durch t^6 teilbar und daher (nach § 6) die Koeffizienten desselben durch t, gegen die Voraussetzung.

2. Wesentlich verschieden sollen alle diejenigen Lösungen

$$g(\omega) = x + \omega y + \omega^2 z$$

der Gleichung

$$Ng(\omega) = \theta^3$$

heissen, welche sich nicht durch Multiplikation mit Einheiten auseinander ableiten lassen. Die Anzahl dieser wesentlich verschiedenen Lösungen ist beschränkt. Hievon kann man sich leicht in folgender

Weise überzeugen (vgl. Dirichlet, Monatsberichte der Berliner Akademie, Okt. 1841).

Angenommen, es sei $E > 1$ (wäre dies nicht der Fall, so gälte dies doch von E^{-1}); dann lässt sich durch Multiplikation mit einer passenden Potenz von E immer bewirken, dass

$$1 < x + \omega y + \omega^2 z < E,$$

somit $$\frac{\theta^3}{E} < (x + \omega' y + \omega'^2 z)(x + \omega'' y + \omega''^2 z) < \theta^3,$$

oder $$\frac{\theta^3}{E} < x^2 + \omega^2 y^2 + \omega^4 z^2 - \omega^3 yz - \omega^2 xz - \omega xy < \theta^3,$$

oder auch

$$\frac{4\theta^3}{E} < (2x - \omega y - \omega^2 z)^2 + 3\omega^2 (y - \omega z)^2 < 4\theta^3.$$

Denkt man sich nun x, y, z als Koordinaten in einem rechtwinkligen Achsensystem, so bilden die Punkte, für welche x, y, z ganze Werte haben, ein parallelopipedisch (kubisch) angeordnetes System und die obigen Bedingungen sagen aus, dass nur solche Punkte in Betracht kommen, welche innerhalb des Raumes liegen, welcher von den parallelen Ebenen

$$1 = x + \omega y + \omega^2 z, \quad E = x + \omega y + \omega^2 z$$

und den Mantelflächen der beiden elliptischen Cylinder begrenzt ist

$$\frac{4\theta^3}{E} = (2x - \omega y - \omega^2 z)^2 + 3\omega^2 (y - \omega z)^2,$$
$$4\theta^3 = (2x - \omega y - \omega^2 z)^2 + 3\omega^2 (y - \omega z)^2.$$

Die Achsen dieser Cylinder sind parallel der Geraden

$$\begin{matrix} 2x - \omega y - \omega^2 z = 0 \\ y - \omega z = 0 \end{matrix} \quad \text{oder} \quad \begin{matrix} x = \omega^2 z \\ y = \omega z \end{matrix}$$

und diese Gerade liegt nicht in der jenen Ebenen parallelen Ebene

$$x + \omega y + \omega^2 z = 0,$$

somit ist jener Raum ein begrenzter und die Anzahl der Punkte innerhalb desselben eine endliche.

3. Alle gebrochnen Einheiten $\frac{g(\omega)}{\theta}$ mit demselben Nenner lassen sich als Potenzen mit ganzen Exponenten von einer derselben darstellen. Seien

$$\frac{g(\omega)}{\theta} \quad \text{und} \quad \frac{g'(\omega)}{\theta}$$

zwei solche Einheiten, so sind, wie bewiesen,

$$\left(\frac{g(\omega)}{\theta}\right)^{\theta} \text{ und } \left(\frac{g'(\omega)}{\theta}\right)^{\theta}$$

ganze Einheiten, also resp. gleich E^{λ} und E^{μ}; somit, da es sich hier um reelle Zahlen handelt,

$$\frac{g'(\omega)}{\theta} = \left(\frac{g(\omega)}{\theta}\right)^{\frac{\mu'}{\lambda'}},$$

wo $\frac{\mu'}{\lambda'} = \frac{\mu}{\lambda}$ und μ' prim zu λ'. Nun bestimme man die ganzen Zahlen α, β so, dass $\alpha\,\lambda' + \beta\,\mu' = 1$ sei, und setze

$$\frac{G(\omega)}{\theta} = \left(\frac{g(\omega)}{\theta}\right)^{\alpha}\left(\frac{g'(\omega)}{\theta}\right)^{\beta},$$

so ist

$$\frac{g(\omega)}{\theta} = \left(\frac{G(\omega)}{\theta}\right)^{\lambda'} \text{ und } \frac{g'(\omega)}{\theta} = \left(\frac{G(\omega)}{\theta}\right)^{\mu'}.$$

Sollte ein dritter Bruch $\frac{g''(\omega)}{\theta}$ noch keine ganze Potenz von $\frac{G(\omega)}{\theta}$ sein, so leite man aus beiden auf dieselbe Weise einen neuen ab, von welchem $\frac{g''(\omega)}{\theta}$ sowol als $\frac{G(\omega)}{\theta}$ ganze Potenzen sind, u. s. w.; da die Anzahl der wesentlich verschiedenen Brüche $\frac{g(\omega)}{\theta}$ endlich ist, so wird man auch nach einer endlichen Anzahl von Operationen zum Ziele gelangen.

4. Hat man nun zwei Brüche $\frac{G(\omega)}{\theta}$ und $\frac{G'(\omega)}{\theta'}$ mit verschiedenen Nennern θ und θ', von denen alle andern Brüche mit resp. denselben Nennern ganze Potenzen seien, so lässt sich aus denselben auf analoge Weise eine gebrochene Einheit $\frac{G_1(\omega)}{\theta_1}$ ableiten, in welcher der Nenner θ_1 das kleinste Vielfache von θ, θ' ist und von welcher $\frac{G(\omega)}{\theta}$ und $\frac{G'(\omega)}{\theta'}$ ganze Potenzen sind. Sei nämlich

$$\left(\frac{G(\omega)}{\theta}\right)^{\theta} = E^{\lambda}, \left(\frac{G'(\omega)}{\theta'}\right)^{\theta'} = E^{\mu},$$

so sind λ und μ resp. prim zu θ und θ . Sei ferner ϑ der grösste gemeinschaftliche Teiler von θ, θ'; ν der von λ, μ, so setze man

$$\frac{\theta'\lambda}{\vartheta\nu} = \lambda', \quad \frac{\theta\,\mu}{\vartheta\nu} = \mu';$$

dann sind λ', μ' relativ prim und man kann also die ganzen Zahlen α, β immer so bestimmen, dass

$$\lambda' \alpha + \mu' \beta = 1.$$

Nimmt man nun

$$\frac{G_1(\omega)}{\theta_1} = \left(\frac{G(\omega)}{\theta}\right)^{\alpha} \left(\frac{G'(\omega)}{\theta'}\right)^{\beta},$$

so wird

$$\frac{G(\omega)}{\theta} = \left(\frac{G_1(\omega)}{\theta_1}\right)^{\lambda'}; \quad \frac{G'(\omega)}{\theta'} = \left(\frac{G_1(\omega)}{\theta_1}\right)^{\mu'};$$

ausserdem kann

$$\left(\frac{G_1(\omega)}{\theta_1}\right)^{n} = E^{\left(\frac{\lambda}{\theta}\alpha + \frac{\mu}{\theta'}\beta\right)n} = E^{\frac{\vartheta\nu}{\theta\theta'}n},$$

da ν prim ist zu $\theta\,\theta'$, nicht anders eine Einheit sein, als wenn n ein Multiplum ist von $\frac{\theta\,\theta'}{\vartheta} = \theta_1$ und es ist somit der Bruch $\frac{G_1(\omega)}{\theta_1}$ (nach 2) irreduktibel.

5. Auf diese Weise verfahrend wird man offenbar zu einer gebrochenen Einheit gelangen können, von welcher alle wesentlich verschiedenen Brüche $\frac{g(\omega)}{\theta}$ ganze Potenzen sind. Sei $\frac{G(\omega)}{\Theta_1}$ eine solche Einheit, so ist Θ_1, das kleinste gemeinschaftliche Multiplum aller in den Brüchen $\frac{g(\omega)}{\theta}$ vorkommenden Nenner. Es sind auch alle $\varphi(\Theta_1)$ verschiedenen Potenzen $\left(\frac{G(\omega)}{\Theta_1}\right)^{n}$, in welchen der Exponent n prim ist zu Θ_1, Einheiten von der Art, dass jeder der Brüche $\frac{g(\omega)}{\theta}$, abgesehen von (ganzen) Einheiten, sich als ganze Potenz derselben darstellen lässt. Sei

$$\left(\frac{G(\omega)}{\Theta_1}\right)^{\Theta_1} = E^{k},$$

wo k prim zu Θ_1, so lässt sich an Stelle von $\frac{G(\omega)}{\Theta_1}$ noch eine andere Einheit $\frac{H(\omega)}{\Theta_1}$ setzen, welche dieselben Eigenschaften hat wie jene, für welche aber

$$\left(\frac{H(\omega)}{\Theta_1}\right)^{\Theta_1} = E.$$

Denn macht man

$$\Theta_1\,\alpha + k\beta = 1 \quad \text{und} \quad \frac{H(\omega)}{\Theta_1} = \left(\frac{G(\omega)}{\Theta_1}\right)^{\beta} E^{a},$$

so wird

$$\frac{G(\omega)}{\Theta_1} = \left(\frac{H(\omega)}{\Theta_1}\right)^{k},$$

$$E = \left(\frac{H(\omega)}{\Theta_1}\right)^{\Theta_1},$$

und es sind somit alle hier betrachteten Einheiten, ganze und gebrochene, ganze Potenzen von $\frac{H(\omega)}{\Theta_1}$.

III.

§ 11. Allgemeines.

Nach diesen Vorbereitungen gehe ich zum eigentlichen Gegenstande der vorliegenden Abhandlung über. Ich betrachte also die Form

$$f(x_1, x_2, x_3) = \frac{1}{m} N(u_1 x_1 + u_2 x_2 + u_3 x_3)$$

wo

$$u_1 = a_1 + b_1\,\omega + c_1\,\omega^2$$

$$u_2 = a_2 + b_2\,\omega + c_2\,\omega^2$$

$$u_3 = a_3 + b_3\,\omega + c_3\,\omega^2.$$

Die Koeffizienten in u_1, u_2, u_3 sind gewöhnliche ganze Zahlen; m ist grösster gemeinschaftlicher Teiler der Koeffizienten von

$$x_1^3, x_2^3, x_3^3,\ 3x_1^2 x_2,\ 3x_1^2 x_3, \ldots,\ 3x_1 x_2 x_3.$$

Diejenigen Formen, für welche der grösste gemeinschaftliche Teiler der Koeffizienten von

$$x_1^3,\ x_2^3,\ x_3^3,\ x_1^2 x_2, \ldots,\ x_1 x_2 x_3$$

$= 3m$ ist, und welche den uneigentlich primitiven in der Theorie der binären quadratischen Formen entsprechen, sollen im folgenden von der Untersuchung ausgeschlossen werden.

Der Vollständigkeit wegen füge ich noch den expliciten Ausdruck von $f(x_1, x_2, x_3)$ bei:

$$mf(x_1, x_2, x_3) =$$

$$(a_1^3 + Db_1^3 + D^2c_1^3 - 3Da_1b_1c_1)x_1^3$$

$$+ (a_2^3 + Db_2^3 + D^2c_2^3 - 3Da_2b_2c_2)x_2^3$$

$$+ (a_3^3 + Db_3^3 + D^2c_3^3 - 3Da_3b_3c_3)x_3^3$$

$$+ 3[a_1^2a_2 + Db_1^2b_2 + D^2c_1^2c_2 - D(b_1c_1a_2 + c_1a_1b_2 + a_1b_1c_2)]x_1^2x_2$$

$$+ 3[a_1^2a_3 + Db_1^2b_3 + D^2c_1^2c_3 - D(b_1c_1a_3 + c_1a_1b_3 + a_1b_1c_3)]x_1^2x_3$$

$$+ 3[a_2^2a_1 + Db_2^2b_1 + D^2c_2^2c_1 - D(b_2c_2a_1 + c_2a_2b_1 + a_2b_2c_1)]x_2^2x_1$$

$$+ 3[a_2^2a_3 + Db_2^2b_3 + D^2c_2^2c_3 - D(b_2c_2a_3 + c_2a_2b_3 + a_2b_2c_3)]x_2^2x_3$$

$$+ 3[a_3^2a_1 + Db_3^2b_1 + D^2c_3^2c_1 - D(b_3c_3a_1 + c_3a_3b_1 + a_3b_3c_1)]x_3^2x_1$$

$$+ 3[a_3^2a_2 + Db_3^2b_2 + D^2c_3^2c_2 - D(b_3c_3a_2 + c_3a_3b_2 + a_3b_3c_2)]x_3^2x_2$$

$$+ 3[2(a_1a_2a_3 + Db_1b_2b_3 + D^2c_1c_2c_3) - D(a_1b_2c_3 + a_1b_3c_2 + a_2b_1c_3$$

$$+ a_2b_3c_1 + a_3b_1c_2 + a_3b_2c_1)]x_1x_2x_3.$$

Wird die Form durch eine lineare Substitution

$$x_1 = \alpha y_1 + \beta y_2 + \gamma y_3$$

$$x_2 = \alpha' y_1 + \beta' y_2 + \gamma' y_3$$

$$x_3 = \alpha'' y_1 + \beta'' y_2 + \gamma'' y_3$$

der Determinante 1 in die Form

$$f(y_1, y_2, y_2) = \frac{1}{m} N(v_1 y_1 + v_2 y_2 + v_3 y_3)$$

transformiert, so bestehen, wenn

$$v_1 = a_1' + b_1'\omega + c_1'\omega^2$$

$$v_2 = a_2' + b_2'\omega + c_2'\omega^2$$

$$v_3 = a_3' + b_3'\omega + c_3'\omega^2$$

gesetzt wird, die Gleichungen

$$v_1 = u_1\alpha + u_2\alpha' + u_3\alpha''$$
$$v_2 = u_1\beta + u_2\beta' + u_3\beta''$$
$$v_3 = u_1\gamma' + u_2\gamma' + u_3\gamma''$$

$a_1' = a_1\alpha + a_2\alpha' + a_3\alpha''$; $b_1' = b_1\alpha + b_2\alpha' + b_3\alpha''$; $c_1' = c_1\alpha + c_2\alpha' + c_3\alpha''$

$a_2' = a_1\beta + a_2\beta' + a_3\beta''$; $b_2' = b_1\beta + b_2\beta' + b_3\beta''$; $c_2' = c_1\beta + c_2\beta' + c_3\beta''$

$a_3' = a_1\gamma + a_2\gamma' + a_3\gamma''$; $b_3' = b_1\gamma + b_2\gamma' + b_3\gamma''$; $c_3' = c_1\gamma + c_2\gamma' + c_3\gamma''$

und es ist daher die Determinante

$$\Delta' = \begin{vmatrix} a_1', & b_1', & c_1' \\ a_2', & b_2', & c_2' \\ a_3', & b_3', & c_3' \end{vmatrix}$$

das Produkt der Determinanten

$$\Delta = \begin{vmatrix} a_1, & b_1, & c_1 \\ a_2, & b_2, & c_2 \\ a_3, & b_3, & c_3 \end{vmatrix} \text{ und } \Sigma = \begin{vmatrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{vmatrix} = 1,$$

also

$$\Delta' = \Delta.$$

Ausserdem ist

$$\begin{vmatrix} u_1, & u_2, & u_3 \\ u_1', & u_2', & u_3' \\ u_1'', & u_2'', & u_3'' \end{vmatrix} = \begin{vmatrix} a_1, & b_1, & c_1 \\ a_2, & b_2, & c_2 \\ a_3, & b_3, & c_3 \end{vmatrix} \begin{vmatrix} 1, & 1, & 1 \\ \omega, & \omega', & \omega'' \\ \omega^2, & \omega'^2, & \omega''^2 \end{vmatrix} = \Delta\Omega,$$

wo

$$\Omega^2 = -27D^2.$$

Die Invariante S (nach der Bezeichnung von Herrn Aronhold) ist $= \left(\frac{3}{2}\right)^2 \left(\frac{D\Delta}{m}\right)^4$, die Invariante $T = \left(\frac{3}{2}\right)^3 \left(\frac{D\Delta}{m}\right)^6$,

also

$$T^2 = S^3$$

und daher die Resultante $R = T^2 - S^3 = 0$.

Der Koeffizient von $3x_1\,x_2\,x_3$ ist gerade oder ungerade, je nachdem $D\Delta$ gerade oder ungerade ist, und es ist dann immer resp. $\frac{1}{4}\,S$ oder $4\,S$ eine ganze Zahl, also m Divisor resp. von $\frac{3D\Delta}{2}$ oder von $3D\Delta$.

Die neun Koeffizienten a_1, b_1 c_1 etc. in u_1, u_2, u_3 können ohne einen allen gemeinschaftlichen Teiler angenommen werden; dann haben auch die neun Koeffizienten a_1', b_1' etc. in v_1, v_2, v_3 keinen solchen gemeinschaftlichen Teiler, insofern, wie im folgenden überall, nur von Substitutionen mit reellen ganzzahligen Koeffizienten und der Determinante 1 die Rede ist.

Ebenso leuchtet ein, dass ein gemeinschaftlicher komplexer (wirklicher oder idealer) Divisor von u_1, u_2, u_3 auch ein solcher von v_1, v_2, v_3 ist, und umgekehrt.

Die Determinante Δ endlich soll, wie erlaubt ist, positiv angenommen werden.

§ 12. Fundamentalsatz.

Vorerst soll nun folgender Satz bewiesen werden:

„Bedeutet Θ das Produkt derjenigen Primzahlen, welche in D quadratisch vorkommen, so kann die Zahl m immer auf die Form

$$\theta^3 \,.\, n$$

gebracht werden, wo θ ein Divisor von Θ ist und n prim zu $3D$; und es kann n so in das Produkt $n_1\,n_1'\,n_1''$ von konjugierten (wirklichen oder idealen) Faktoren zerlegt werden, dass u_1, u_2, u_3 alle n_1 als Faktor enthalten."

Ich betrachte zuerst die Zahl 3.

Sei m durch 3^μ und durch keine höhere Potenz von 3 teilbar, so lässt sich $N(u_1\,x_1 + u_2\,x_2 + u_3\,x_3)$ durch eine lineare Substitution immer so transformieren, dass der Koeffizient $N\,u_1$ von x_1^3 genau durch 3^μ teilbar ist. Ist dies erreicht, so setze man

$$u_1'\,u_1'' = v$$

und schreibe

$$f = \frac{1}{m}\,N(u_1\,x_1 + u_2\,x_2 + u_3\,x_3)$$

in der Form

$$f = \frac{1}{m\,N(u_1)^2}\; N(u_1\,x_1 + u_2\,x_2 + u_3\,x_3);$$

dann ist $m\,N(u_1)^2$ genau durch $3^{3\mu}$ teilbar, $u_1\,v$, $u_2\,v$, $u_3\,v$ durch 3^{μ} und zwar $u_1\,v = N(u_1)$ durch keine höhere Potenz von 3.

Dass $u_2\,v$ wirklich durch 3^{μ} teilbar ist, ergiebt sich z. B. auf folgende Weise:

Sei

$$u_1\,v = a$$
$$u_2\,v = a' + b'\omega + c'\omega^2$$
$$u_3\,v = a'' + b''\omega + c''\omega^2.$$

Nun ist

$$u_2 u_1' u_1'' + u_1 u_2' u_1'' + u_1 u_2' u_2''$$

durch $3^{\mu+1}$ teilbar als Koeffizient von $x_1^2 x_2$ in $N(u_1x_1 + u_2x_2 + u_3x_3)$, oder da

$$u_2 u_1' u_1'' = u_2 v = a' + b'\omega + c'\omega^2 \qquad \text{ist,}$$

$$(a' + b'\omega + c'\omega^2) + (a' + b'\omega' + c'\omega'^2) + (a' + b'\omega'' + c'\omega''^2) = 3a'$$

durch $3^{\mu+1}$, also a' durch 3^{μ} teilbar.

Es ist aber auch

$$N(u_2 v) = a'^3 + D b'^3 + D^2 c'^3 - 3D a' b' c'$$

und der Koeffizient von $3x_1 x_2^2$:

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

durch $3^{3\mu}$ teilbar, oder da a und a' durch 3^{μ} teilbar sind und zwar a nicht durch $3^{\mu+1}$:

$$b'\,c' \equiv 0 \pmod{3^{2\mu}},$$

$$D b'^3 + D^2 c'^3 \equiv 0 \pmod{3^{3\mu}},$$

woraus, wenn D nicht durch 3^2 teilbar ist, leicht folgt, dass sowohl b' als c' durch 3^{μ} teilbar sein muss, und in derselben Weise wird gezeigt, dass a'', b'', c'' durch 3^{μ} teilbar sind.

Ist D durch 3^2 teilbar, so muss zwar b' auch noch durch 3^{μ}, c' aber braucht nur durch $3^{\mu-1}$ teilbar zu sein. Hebt man nun im

Nenner von f resp. den Faktor $3^{3\mu-3}$ oder $3^{3\mu}$, aus den Koeffizienten des linearen Ausdrucks

$$u_1 v x_1 + u_2 v x_2 + u_3 v x_3$$

den Faktor $3^{\mu-1}$ oder 3^{μ} weg, so bleibt im Nenner eine Zahl, welche den Faktor 3 in der dritten Potenz oder gar nicht enthält, je nachdem D durch 3^2 teilbar ist oder nicht.

Für die Zahlen s und t beweist sich der Satz in ähnlicher Weise. Ist m genau durch $s^\mu t^\nu$ teilbar, so kann $u_1 v$ ebenfalls so vorausgesetzt werden; dann sind aber

$$N(u_1 v), \quad N(u_2 v), \quad N(u_3 v)$$

durch $s^{3\mu} t^{3\nu}$ teilbar, also die Koeffizienten von $u_1 v$, $u_2 v$, $u_3 v$ durch $s^\mu t^{\nu-1}$. Nach Weghebung dieses Faktors und der entsprechenden $s'^{\mu'} t'^{\nu'-1}, \ldots$ bleibt also noch eine Zahl m von der Form

$$m = \theta^3 . n,$$

wo θ ein Teiler ist von Θ, und die Zahl n prim zu $3D$. Ausserdem erhellt leicht aus den (§ 6) aufgestellten Bedingungen der Teilbarkeit der Norm komplexer Zahlen durch Primzahlen t, dass θ^3 das grösste aus solchen Primzahlen gebildete Produkt ist, welches zugleich in $N(u_1)$, $N(u_2)$, $N(u_3)$ aufgeht.

Hienach kann n bloss noch Primzahlen p und r enthalten, da sich die Primzahlen q sofort wegheben lassen; auch können u_1, u_2, u_3 nicht sämtlich alle drei Primfaktoren einer Primzahl p oder r enthalten, ansonst sie durch diese Primzahlen teilbar wären.

Beweis für die Primzahlen p.

Es seien also z. B. π^α, $\pi'^{\alpha'}$ die höchsten Potenzen der Primfaktoren π, π' von p, welche zugleich in u_1, u_2, u_3 enthalten sind, während π'' nicht zugleich in allen dreien vorkomme. Ersetzt man nun in u_1, u_2, u_3 die Wurzel ω successive durch die Kongruenzwurzeln ξ_a, $\xi'_{a'}$, ξ'', so gehen sie in reelle ganze Zahlen über und die Linearfunktion werde resp.

$$p^{\alpha}\ (A_1 x_1 + A_2 x_2 + A_3 x_3)$$
$$p^{\alpha'}\ (A_1' x_1 + A_2' x_2 + A_3' x_3)$$
$$A_1'' x_1 + A_2'' x_2 + A_3'' x_3,$$

wo nun der Voraussetzung nach die drei Koeffizienten derselben in Klammern stehenden Linearfunktion niemals alle drei durch p teilbar sind.

Giebt man nun jeder der drei Zahlen x_1, x_2, x_3 die Werte

$$0,\ 1,\ 2,\ \ldots .\ p-1,$$

so wird jeder der obigen (in Klammern stehenden) Ausdrücke für p^2 Kombinationen $\equiv 0 \pmod{p}$; also giebt es höchstens $3p^2$ Kombinationen, für welche mindestens einer derselben $\equiv 0 \pmod{p_1}$ ist. Im Ganzen giebt es aber p^3 Kombinationen, also mindestens

$$p^3 - 3p^2 = p^2(p-3)$$

Kombinationen, für welche keiner der Ausdrücke $\equiv 0 \pmod{p_1}$ wird.

Nun ist $p > 3$; also kann man für x_1, x_2, x_3 immer Wertsysteme finden, für welche $N(u_1 x_1 + u_2 x_2 + u_3 x_3)$ durch keine höhere Potenz als die $(\alpha+\alpha')^{\text{te}}$ teilbar ist. Der Voraussetzung nach sind aber alle diese Normen durch m teilbar; somit ist der Exponent k der in m enthaltenen Potenz p^k von p immer $\leqq (\alpha+\alpha')$, und es lässt sich daher k immer so in zwei Zahlen $k = \mu + \mu'$ zerlegen, dass

$$\mu \leqq \alpha,\quad \mu' \leqq \alpha'$$

und also u_1, u_2, u_3 alle sowohl π^{μ} als $\pi'^{\mu'}$ als Faktor enthalten.

Beweis für die Primzahlen r und die Zahl 2.

Für die Primzahlen r lässt sich der Beweis ganz in ähnlicher Weise führen; er erstreckt sich dann aber nicht auf die Zahl 2, welche, wenn D ungerade ist, zu dieser Klasse von Primzahlen gehört. Folgende Betrachtung hingegen, welche sich auch auf die Primzahlen p anwenden lässt, hat auch für die Zahl 2 Gültigkeit.

Es zerfalle r in die drei Primfaktoren ϱ, ϱ', ϱ'', von denen ϱ der reellen Wurzel der Kongruenz $\eta^3 \equiv D \pmod{r}$ zugehöre. Angenommen nun, m sei durch r^{ν} teilbar, so wäre die Zerlegung

von r^ν in drei Faktoren, von denen jeder die Koeffizienten eines der drei Faktoren von $N(u_1 x_1 + u_2 x_2 + u_3 x_3)$ misst, dann unmöglich, wenn u_1, u_2, u_3 weder alle den Faktor ϱ^ν, noch alle den Faktor $(\varrho' \varrho'')^{\frac{\nu}{2}}$ enthielten. Da nun Nu_1, Nu_2, Nu_3 alle durch r^ν, aber u_1, u_2, u_3 nicht alle durch r teilbar sind, so muss eine der Zahlen u, z. B. u_1 entweder von der Form sein

$$\varrho^{\alpha_1} \cdot k \qquad \text{oder} \qquad (\varrho' \varrho'')^{\beta_1} \cdot k,$$

wo α_1 oder $2\beta_1 \geqq \nu$

und k keinen Primfaktor von r enthält. Es sei also erstlich

$$u_1 = \varrho^{\alpha_1} \cdot k_1$$
$$u_2 = \varrho^{\alpha_2} \cdot (\varrho' \varrho'')^{\beta_2} \cdot k_2$$
$$u_3 = \varrho^{\alpha_3} (\varrho' \varrho'')^{\beta_3} k_3,$$

wo die k_1, k_2, k_3 keine Primfaktoren von r enthalten sollen und eine der Zahlen α_2, α_3, z. B. α_2, $< \nu$, sei.

Nun ist der Voraussetzung nach der Koeffizient

$$u_1 u_1' u_2'' + u_1 u_2' u_1'' + u_2 u_1' u_1''$$

von $x_1^2 x_2$ durch r^ν teilbar. Derselbe hat die Form

$$\varrho^{\alpha_2} (\varrho' \varrho'')^{\alpha_1 + \beta_2} \cdot K + \varrho'^{\alpha_2} (\varrho \varrho'')^{\alpha_1 + \beta_2} K' + \varrho''^{\alpha_2} (\varrho \varrho')^{\alpha_1 + \beta_2} K'',$$

wo K, K', K'' keine Primfaktoren von r enthalten. Wegen $\alpha_2 < \nu$ ist derselbe aber weder durch ϱ^ν, noch durch ϱ'^ν, noch durch ϱ''^ν, somit auch nicht durch r^ν teilbar; contra hyp.

Würde zweitens angenommen, es sei

$$u_1 = (\varrho' \varrho'')^{\beta_1} \cdot k_1 \qquad 2\beta_1 \geqq \nu$$
$$u_2 = \varrho^{\alpha_2} \cdot (\varrho' \varrho'')^{\beta_2} \cdot k_2 \qquad 2\beta_2 < \nu$$
$$u_3 = \varrho^{\alpha_3} \cdot (\varrho' \varrho'')^{\beta_3} \cdot k_3 \qquad 2\beta_2 + \alpha_2 \geqq \nu,$$

wo k_1, k_2, k_3 wiederum von Primfaktoren von r frei sind, so würde der Koeffizient

$$u_1 u_2' u_2'' + u_2 u_1' u_2'' + u_2 u_2' u_1''$$

von $x_1 x_2^2$ die Form annehmen

$$\varrho^{2\beta_2} (\varrho' \varrho'')^{\alpha_2 + \beta_1 + \beta_2} K + \varrho'^{2\beta_2} (\varrho \varrho'')^{\alpha_2 + \beta_1 + \beta_2} K' + \varrho''^{2\beta_2} (\varrho' \varrho)^{\alpha_2 + \beta_1 + \beta_2} K'';$$

somit wäre er wegen $2\beta_2 < \nu$ und $2(\beta_2 + \beta_1) + \alpha_2 \geqq 2\nu$ weder durch ϱ^ν, noch durch ϱ'^ν, noch durch ϱ''^ν, also auch nicht durch r^ν teilbar.

§ 13. Reduktion.

Nach dem Vorhergehenden lässt sich jede Form des vorliegenden Systems in folgender Weise ausdrücken:

$$f = \frac{1}{\theta^3} N\left(\frac{u_1 x_1 + u_2 x_2 + u_3 x_3}{n_1}\right);$$

u_1, u_2, u_3 sind wirkliche ganze komplexe Zahlen in ω, deren grösster gemeinschaftlicher idealer Teiler die Zahl n_1 ist, derjenige ihrer Normen aber das Produkt $\theta^3 . N(n_1)$, wo $N(n_1)$ prim ist zu $3D$.

Es sei nun

$$1, M_1, M_2, \ldots\ldots M_{h-1}$$

ein System von idealen Multiplikatoren, deren Normen zu $3D$ prim seien, und welche keine wirkliche komplexe Zahl als Faktor enthalten sollen. Ist M_k derjenige Multiplikator des obigen Systems, welcher die Zahl n_1 zu einer wirklichen macht, so setze man

$$M_k . n_1 = m_k$$

und

$$f = \frac{1}{\theta^3} N\left(\frac{u_1 N(M_k) . x_1 + u_2 N(M_k) . x_2 + u_3 N(M_k) . x_3}{m_k . M_k' M_k''}\right);$$

hier sind $u_1 N(M_k)$, $u_2 N(M_k)$, $u_3 N(M_k)$

wirkliche komplexe Zahlen, welche durch die wirkliche komplexe Zahl m_k teilbar sind. Setzt man also die Quotienten

$$\frac{u_1 N(M_k)}{m_k} = v_1, \frac{u_2 N(M_k)}{m_k} = v_2, \frac{u_3 N(M_k)}{m_k} = v_3,$$

so sind v_1, v_2, v_3 wiederum wirkliche komplexe Zahlen, welche sämtlich durch $M_k' M_k''$ teilbar sind, und es wird

$$f = \frac{1}{\theta^3} N\left(\frac{v_1 x_1 + v_2 x_2 + v_3 x_3}{M_k' M_k''}\right) = \frac{1}{\theta^3 N(M_k)^2} N(v_1 x_1 + v_2 x_2 + v_3 x_3).$$

An Stelle unendlich vieler Zahlen m ist also die endliche Anzahl von Zahlen getreten, welche Produkte sind aus dritten Potenzen der Divisoren von Θ in die h Zahlen

$$1, N(M_1)^2, N(M_2)^2, \ldots . N(M_{h-1})^2.$$

Da nun für jedes Formensystem der Ausdruck $\frac{\Delta}{m}$ einen gegebenen unveränderlichen (ganzen oder gebrochenen) Wert δ hat, so muss auch

$$\Delta = N(M_p)^2 \cdot \theta^3 \cdot \delta$$

sein für die Form f.

Die Normen von v_1, v_2, v_3 sind alle durch θ^3 teilbar und daher, wenn wieder

$$v_1 = a_1 + b_1 \omega + c_1 \omega^2$$

$$v_2 = a_2 + b_2 \omega + c_2 \omega^2$$

$$v_3 = a_3 + b_3 \omega + c_3 \omega^2$$

gesetzt wird, alle Zahlen a und b durch θ, somit Δ durch θ^2 teilbar. Ferner ist (§ 11) $N(M_k)^2 \theta^3$ Divisor von $3D\Delta$, also weil $N(M_k)$ prim ist zu $3D$, Δ teilbar durch $N(M_k)^2$; folglich auch durch $N(M_k)^2 \cdot \theta^2$ und daher $\theta\delta$ eine ganze Zahl.

Die weitere Reduktion geschieht mit Hülfe linearer Transformationen. Wendet man auf die Form f die Substitution

$$\alpha, \quad \beta, \quad \gamma$$

$$\alpha', \quad \beta', \quad \gamma'$$

$$\alpha'', \quad \beta'', \quad \gamma''$$

an, so kann man γ, γ', γ'' immer so wählen, dass c_3 der grösste gemeinschaftliche Teiler von c_1, c_2, c_3 wird. Hierauf kann man durch Anwendung einer Substitution der Form

$$1, \quad 0, \quad 0$$

$$0, \quad 1, \quad 0$$

$$\alpha'', \quad \beta'', \quad 1$$

die Zahlen α'', β'' so nehmen, dass $c_1 = 0$, $c_2 = 0$ wird.

Durch eine weitere Substitution der Form

$$\alpha, \quad \beta, \quad 0$$

$$\alpha', \quad \beta', \quad 0$$

$$0, \quad 0, \quad 1$$

ist es noch möglich $b_1 = 0$ zu machen, so dass das System der Koeffizienten jetzt lautet

$$\begin{matrix} a_1 & 0 & 0 \\ a_2 & b_2 & 0 \\ a_3 & b_3 & c_3 \end{matrix}$$

Endlich wird man noch durch eine Substitution

$$\begin{matrix} 1, & \beta, & \gamma \\ 0, & 1, & \gamma' \\ 0, & 0, & 1 \end{matrix}$$

bewirken, dass die Bedingungen erfüllt sind

$$0 \leqq a_2 < a_1 ; \qquad 0 \leqq b_3 < b_2$$
$$0 \leqq a_3 < a_1 .$$

Hiebei können a_1, b_2, c_3 als positiv vorausgesetzt werden; denn da $\Delta = a_1 b_2 c_3$ der Annahme nach positiv ist, so müssten zwei von diesen Zahlen, z. B. b_2, c_3, negativ, die dritte a_1 positiv sein; dann würden aber durch die Substitution

$$\begin{matrix} 1, & 0, & 0 \\ 0, & -1, & 0 \\ 0, & 0, & -1 \end{matrix}$$

sofort die Zeichen von b_2 und c_3 umgekehrt.

Es ist also nunmehr jede Form des Systems auf eine ihr äquivalente, von folgender Gestalt reduziert:

$$f = \frac{1}{\theta^3} N\left(\frac{u_1 x_1 + u_2 x_2 + u_3 x_3}{M_k' M_k''}\right),$$

wo

$$u_1 = a_1$$
$$u_2 = a_2 + b_2 \omega$$
$$u_3 = a_3 + b_3 \omega + c_3 \omega^2.$$

Die Koeffizienten a, b, c sind den Bedingungen unterworfen

$$a_1 b_2 c_3 = \theta^3 . N(M_k)^2 . \delta$$
$$0 \leqq a_2 < a_1 ; \qquad 0 \leqq b_3 < b_2$$
$$0 \leqq a_3 < a_1 ; \qquad 0 < c_3 ;$$

ausserdem müssen u_1, u_2, u_3 durch $M_k' . M_k''$ und a_1, a_2, a_3, b_2, b_3 durch θ teilbar sein, c_3 aber prim sein zu θ.

Da nun 1) die Anzahl h der Multiplikatoren M und diejenige der Divisoren θ von Θ endlich ist, 2) die ganzen Zahlen a_1, a_2, a_3, b_2, b_3, c_3 den eben genannten Bedingungen genügen müssen, so ergiebt sich, dass die Anzahl der reduzierten Formen, also jedenfalls auch die Anzahl nicht äquivalenter Formen des Systems endlich ist.

§ 14. Bedingungen der Teilbarkeit.

Ich untersuche jetzt die Bedingungen der Teilbarkeit von u_1, u_2, u_3 durch die ideale Zahl $M_k' . M_k''$ und lasse dabei der Symmetrie wegen die Bedingung fallen, dass M_k keine wirkliche komplexe Zahl als Faktor enthalten dürfe; nur die Primzahlen q betrachte ich als weggehoben und setze also der frühern Bezeichnungsweise gemäss:

$$M_k = \pi\pi^{\mu}\ \pi\pi'^{\mu'}\ \pi\pi''^{\mu''} \ldots . \varrho^{\lambda}\ (\varrho'\ \varrho'')^{\nu} \ldots .$$
$$M_k' = \pi\pi'^{\mu}\ \pi\pi''^{\mu'}\ \pi\pi^{\mu''} \ldots . \varrho'^{\lambda}\ (\varrho''\ \varrho)^{\nu} \ldots .$$
$$M_k'' = \pi\pi''^{\mu}\ \pi\pi^{\mu'}\ \pi\pi'^{\mu''} \ldots . \varrho''^{\lambda}(\varrho\ \varrho')^{\nu} \ldots .;$$

also ist

$$M_k' M_k'' = \pi\pi^{\mu'+\mu''}\ \pi\pi'^{\mu''+\mu}\ \pi\pi''^{\mu+\mu'} \ldots . \varrho^{2\nu}\,(\varrho'\,\varrho'')^{\lambda+\nu} \ldots .$$

und es muss demnach folgendes System von Kongruenzen erfüllt sein

$$a_1 \equiv 0,\ a_2 + b_2\xi \equiv 0,\ a_3 + b_3\xi + c_3\xi^2 \equiv 0 \pmod{p^{\mu'+\mu''}},$$
$$a_1 \equiv 0,\ a_2 + b_2\xi' \equiv 0,\ a_3 + b_3\xi' + c_3\xi'^2 \equiv 0 \pmod{p^{\mu''+\mu}},$$
$$a_1 \equiv 0,\ a_2 + b_2\xi'' \equiv 0,\ a_3 + b_3\xi'' + c_3\xi''^2 \equiv 0 \pmod{p^{\mu+\mu'}}$$

etc.

$$a_1 \equiv 0,\ a_2 + b_2\eta \equiv 0,\ a_3 + b_3\eta + c_3\eta^2 \equiv 0 \pmod{r^{2\nu}},$$
$$a_1 \equiv 0,\quad a_2 \equiv 0,\quad a_3 - c_3\eta^2 \equiv 0 \pmod{r^{\lambda+\nu}}$$
$$b_2 \equiv 0,\quad b_3 - c_3\eta \equiv 0$$

etc.,

wo der Einfachheit wegen die jedesmaligen Indices von ξ, η etc. weggelassen sind. Bedeuten α, β, γ die Zahlen $\mu' + \mu''$, $\mu + \mu''$, $\mu' + \mu$ der Grösse nach geordnet, so dass

$$\alpha > \beta > \gamma,$$

und ist ebenso ε die grössere, ϑ die kleinere der Zahlen $\lambda+\nu$, 2ν, so ersieht man leicht aus obigen Kongruenzen, dass

a_1 durch $p^{\alpha}\, r^{\varepsilon}$

a_2 und b_2 durch $p^{\beta} r^{\lambda+\nu}$

a_3, b_3, c_3 durch $p^{\lambda}\, r^{\vartheta}$

teilbar sind. Setzt man daher

$$A_1 = p^{\alpha}\, p_1^{\alpha_1} \ldots . \; r^{\varepsilon}\, r_1^{\varepsilon_1} \ldots .$$

$$B_2 = p^{\beta}\, p_1^{\beta_1} \ldots . \; r^{\lambda+\nu}\, r_1^{\lambda_1+\nu_1} \ldots$$

$$C_3 = p^{\gamma}\, p_1^{\gamma_1} \ldots . \; r^{\vartheta}\, r_1^{\vartheta_1} \ldots .,$$

so kann man schreiben, wenn man noch die Teilbarkeit durch θ berücksichtigt:

$$u_1 = \theta A_1 \,.\, \mathfrak{a}_1$$

$$u_2 = \theta B_2 \,.\, (\mathfrak{a}_2 + \mathfrak{b}_2\, \omega)$$

$$u_3 = C_3\, (\theta\, \mathfrak{a}_2 + \theta\, \mathfrak{b}_3\, \omega + \mathfrak{c}_3\, \omega^2)$$

Erwägt man, dass

$$\alpha + \beta + \gamma = 2\,(\mu + \mu' + \mu'')$$

$$\varepsilon + \vartheta = \lambda + 3\,\nu,$$

so sieht man, dass

$$A_1\, B_2\, C_3 = N\,(M_k)^2$$

$$\mathfrak{a}_1\, \mathfrak{b}_2\, \mathfrak{c}_3 = \theta\, \delta.$$

Setzt man noch

$$\frac{A_1}{B_2} = \mathfrak{A},\ \frac{A_1}{C_3} = \mathfrak{B},\ \frac{B_2}{C_3} = \mathfrak{C},$$

so sind $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ ganze Zahlen, und man hat die Bedingungen:

$$0 \leqq \mathfrak{a}_2 < \mathfrak{A}\,\mathfrak{a}_1\,; \qquad 0 \leqq \mathfrak{b}_3 < \mathfrak{C}\,\mathfrak{b}_2.$$

$$0 \leqq \mathfrak{a}_3 < \mathfrak{B}\,\mathfrak{a}_1$$

Sind $\mathfrak{a}_1$, $\mathfrak{b}_2$, $\mathfrak{c}_3$ der Gleichung $\mathfrak{a}_1\,\mathfrak{b}_2\,\mathfrak{c}_3 = \theta\,\delta$ gemäss angenommen, so haben $\mathfrak{a}_2$, $\mathfrak{a}_3$, $\mathfrak{b}_3$ noch Kongruenzen zu genügen, welche sie resp. nach den Moduln $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ bestimmen.

Es wäre nun noch die Anzahl der reduzierten Formen eines Systems zu bestimmen, das einem gegebenen Werte von δ entspricht. Zu diesem Zwecke sind für θ alle diejenigen Divisoren von Θ anzunehmen, für welche $\theta\,\delta$ eine ganze Zahl wird; hierauf ist jeder Wert von $\theta\,\delta$ auf alle möglichen Weisen so in drei Faktoren $\mathfrak{a}_1$, $\mathfrak{b}_2$, $\mathfrak{c}_3$ zu zerlegen, dass $\mathfrak{c}_3$ prim wird zu θ. Für jede solche Zerlegung hat man dann $\mathfrak{a}_1^2\,\mathfrak{b}_2$ Kombinationen von $\mathfrak{a}_1$ Werten $\mathfrak{a}_2$, mit $\mathfrak{a}_1$ Werten $\mathfrak{a}_3$ und $\mathfrak{b}_2$ Werten $\mathfrak{b}_3$. Von diesen $\mathfrak{a}_1^2\,\mathfrak{b}_2$ Kombinationen sind aber alle diejenigen auszuschliessen, für welche u_1, u_2, u_3 einen grössern gemeinschaftlichen idealen Teiler als $M_k'\,M_k''$ haben und für welche der grösste gemeinschaftliche Teiler von $\frac{N(u_1)}{\theta^3}$, $\frac{N(u_2)}{\theta^3}$, $\frac{N(u_3)}{\theta^3}$ nicht prim ist zu $3\,D$.

Diese Bestimmung ist indes, wenn auch nicht schwierig, so doch weitläufig; ich muss sie daher für jetzt übergehen und erwähne nur noch den speciellen Fall (welcher etwa demjenigen bei den quadratischen Formen entspricht, wo die Determinante keinen quadratischen Faktor enthält), wo $\delta = \frac{1}{\Theta}$ ist, und also, da $\theta\,\delta$ eine ganze Zahl sein muss, θ nur den Wert Θ haben kann; dann

ist $\qquad \mathfrak{a}_1\,\mathfrak{b}_2\,\mathfrak{c}_3 = 1,$

somit einzeln $\qquad \mathfrak{a}_1 = 1,\ \mathfrak{b}_2 = 1,\ \mathfrak{c}_3 = 1.$

Die Zahlen $\mathfrak{a}_2$, $\mathfrak{a}_3$, $\mathfrak{b}_3$ sind jetzt durch die angeführten Kongruenzen unzweideutig bestimmt und es entspricht daher jedem Multiplikator M nur eine reduzierte Form und es ist in diesem Fall die Anzahl der reduzierten Formen genau gleich der Klassenanzahl der komplexen Zahlen.

§ 15. Lemmata.

Es bleibt nun noch zu untersuchen, ob in einem System reduzierter Formen auch noch äquivalente sich finden können, und zu zeigen, wie, wenn dies der Fall ist, dasselbe auf ein System nicht äquivalenter Formen weiter zu reduzieren ist. Ich will dabei annehmen, es seien aus dem Multiplikator die reellen Primzahlen, die er etwa enthält, weggehoben. Alsdann ist, wie leicht zu sehen, $A_1 = N(M_k)$.

Zuerst schicke ich einige Sätze voraus:

1) Wenn zwei reduzierte Formen

$$f = \frac{1}{\theta^3} N\left(\frac{u_1 x_1 + u_2 x_2 + u_3 x_3}{M_k' M_k''}\right), \quad \varphi = \frac{1}{\theta'^3} N\left(\frac{v_1 x_1 + v_2 x_2 + v_3 x_3}{M_i' M_i''}\right)$$

in ihrer entwickelten Form (§ 11) identisch sind, so sind auch einzeln θ und θ', M_k und M_k', $u_1 x_1 + u_2 x_2 + u_3 x_3$ und $v_1 x_1 + v_2 x_2 + v_3 x_3$ identisch.

In der That, es sei

$$u_1 = \theta \,.\, N(M_k) \,.\, \mathfrak{a}_1, \quad v_1 = \theta' \,.\, N(M_i)\, \mathfrak{a}_1',$$

so ist der Voraussetzung nach

$$\frac{1}{\theta^3} N\left(\frac{u_1}{M_k' M_k''}\right) = \frac{1}{\theta'^3} N\left(\frac{v_1}{M_i' M_i''}\right),$$

oder
$$\mathfrak{a}_1^3 N(M_k) = \mathfrak{a}_1'^3 N(M_i),$$

also
$$\mathfrak{a}_1^2 \theta' u_1 = \mathfrak{a}_1'^2 \theta v_1 ;$$

und

$$\mathfrak{a}_1^6 \theta'^3 N(u_1 x_1 + u_2 x_2 + u_3 x_3) = \mathfrak{a}_1'^6 \theta^3 N(v_1 x_1 + v_2 x_2 + v_3 x_3),$$

oder

$$N(\mathfrak{a}_1^2 \theta' u_1 x_1 + \cdots) = N(\mathfrak{a}_1'^2 \theta v_1 x_1 + \cdots).$$

Wenn aber die Normen zweier reelle Linearfaktoren und die Koeffizienten einer und derselben Unbestimmten (hier von x_1) einander gleich sind, so müssen, wie sich dies z. B. schon aus der Methode der Zerlegung in Linearfaktoren ergiebt, diese Linearfunktionen vollständig identisch sein, d. h. es ist

$$\mathfrak{a}_1^2 \theta' \,.\, (u_1 x_1 + u_2 x_2 + u_3 x_3) = \mathfrak{a}_1'^2 \theta (v_1 x_1 + v_2 x_2 + v_3 x_3).$$

Nun sind resp. $M_k' M_k''$ und $M_i' M_i''$ die grössten gemeinschaftlichen idealen Teiler von u_1, u_2, u_3, und v_1, v_2 v_3; somit

$$\mathfrak{a}_1^2 \theta' \,.\, M_k' M_k'' = \mathfrak{a}_1'^2 \theta \,.\, M_i' M_i''$$

und hieraus wegen

$$\alpha) \qquad \mathfrak{a}_1^3 N(M_k) = \mathfrak{a}_1'^3 N(M_i)$$

$$\mathfrak{a}_1 \theta \,.\, M_k = \mathfrak{a}_1' \theta' \,.\, M_i.$$

Es gehören also M_k und M_i zu derselben Klasse, daher

$$M_k = M_i$$

$$\mathfrak{a}_1 \theta = \mathfrak{a}_1' \theta',$$

woraus mit Rücksicht auf Gleichung α) folgt

$$\mathfrak{a}_1 = \mathfrak{a}_1', \qquad \theta = \theta' \qquad \text{w. z. b. w.}$$

2) Ein reduzierter Linearfaktor

$$a_1 x_1 + (a_2 + b_2 \omega) x_2 + (a_3 + b_3 \omega + c_3 \omega^2) x_3$$

kann nicht durch lineare Transformation in einen andern, davon verschiedenen, ebenfalls reduzierten

$$a_1' x_1 + (a_2' + b_2' \omega) x_2 + (a_3' + b_3' \omega + c_3' \omega^2) x_3$$

verwandelt werden.

Denn ginge der erste in den zweiten über durch die Substitution

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'', \end{matrix}$$

so müssten die Gleichungen erfüllt sein:

$$a_1' = a_1 \alpha + a_2 \alpha' + a_3 \alpha'', \quad 0 = b_2 \alpha' + b_3 \alpha'', \quad 0 = c_3 \alpha''$$

$$a_2' = a_1 \beta + a_2 \beta' + a_3 \beta'', \quad b_2' = b_2 \beta' + b_3 \beta'', \quad 0 = c_3 \beta''$$

$$a_3' = a_1 \gamma + a_2 \gamma' + a_3 \gamma'', \quad b_3' = b_2 \gamma' + b_3 \gamma'', \quad c_3' = c_3 \gamma'',$$

woraus folgt, da b_2, c_3 nicht null sind:

$$\alpha'' = 0, \quad \beta'' = 0, \quad \alpha' = 0$$

$$\alpha\beta'\gamma'' = 1,$$

somit, weil diese Koeffizienten alle positiv sind,

$$a_1' = a_1, \quad b_2' = b_2 \quad c_3' = c_3$$

$$\alpha = 1, \quad \beta' = 1, \quad \gamma'' = 1.$$

Endlich folgt aus den Bedingungsgleichungen:

$$0 \leqq a_2 < a_1 \qquad 0 \leqq a_2' < a_1'$$

$$0 \leqq a_3 < a_1 \qquad 0 \leqq a_3' < a_1'$$

$$0 \leqq b_3 < b_2 \qquad 0 \leqq b_3' < b_2'$$

leicht noch

$$\beta = 0, \quad \gamma = 0, \quad \gamma' = 0;$$

d. h. die Substitution ist die identische

$$1, \ 0, \ 0$$

$$0, \ 1, \ 0$$

$$0, \ 0, \ 1$$

w. z. b. w.

3) Wird hingegen der reduzierte Linearfaktor

$$\overset{(0)}{u} = u_1 x_1 + u_2 x_2 + u_3 x_3$$

mit der Fundamentaleinheit E multipliziert, hierauf durch lineare Transformationen wieder reduziert, so wird man im Allgemeinen einen von $\overset{(0)}{u}$ verschiedenen reduzierten Ausdruck $\overset{(1)}{u}$ erhalten. Wendet man dasselbe Verfahren auf $\overset{(1)}{u}$ an, so erhalte man $\overset{(2)}{u}$ u. s. w. Durch wiederholte Anwendung desselben wird man also eine Reihe von reduzierten Linearfaktoren

$$\overset{(0)}{u}, \quad \overset{(1)}{u}, \quad \overset{(2)}{u}, \ldots\ldots$$

erhalten. Anstatt $\overset{(k)}{u}$ aus $\overset{(k-1)}{u}$ abzuleiten, indem man letzteres mit E multipliziert und reduziert, kann man auch direkt $\overset{(0)}{u}$ mit E^k multiplizieren und dann reduzieren. Beide Resultate müssen identisch sein, da das Endresultat dasselbe ist, ob man einen Linearfaktor

$u_1 x_1 + u_2 x_2 + u_3 x_3$ zuerst mit einer Einheit multipliziere und dann durch eine lineare Substitution transformiere, oder ob man umgekehrt zuerst (mit derselben Substitution) transformiere und dann mit der Einheit multipliziere. Obige Reihe von reduzierten Formen wird daher auch erhalten, indem man die Faktoren

$$\overset{(0)}{u}, \quad E\overset{(0)}{u}, \quad E^2\overset{(0)}{u}, \ldots .$$

reduziert, und es kann dieselbe auch rückwärts fortgesetzt werden:

$$\ldots . \overset{(-2)}{u}, \overset{(-1)}{u}, \overset{(0)}{u}, \overset{(1)}{u}, \overset{(2)}{u}, \ldots .$$

Ich behaupte nun, dass diese Reihe aus einer endlichen Anzahl verschiedener, aber periodisch wiederkehrender Glieder bestehen müsse. In der That: durch Multiplikation des Linearfaktors mit einer Einheit e bleibt die Determinante Δ des Koeffizientensystems unverändert; denn es ist

$$\begin{vmatrix} u_1, & u_2, & u_3 \\ u_1', & u_2', & u_3' \\ u_1'', & u_2'', & u_3'' \end{vmatrix} = \Delta\Omega$$

und

$$\Delta'\Omega = \begin{vmatrix} eu_1, & eu_2, & eu_3 \\ e'u_1', & e'u_2', & e'u_3' \\ e''u_1'', & e''u_2'', & e''u_3'' \end{vmatrix} = N(e) \cdot \Delta\Omega = \Delta\Omega,$$

also

$$\Delta' = \Delta.$$

Dasselbe gilt von einer Transformation durch eine lineare Substitution der Determinante 1. Derselben Determinante Δ entspricht aber nur eine endliche Anzahl reduzierter Linearfaktoren; folglich müssen gewisse derselben wiederkehren (und zwar unendlich oft). Seien $\overset{(r)}{u}$, $\overset{(s)}{u}$ zwei gleiche Glieder obiger Reihe und

$$\overset{(r)}{u}, \overset{(r+1)}{u}, \ldots \ldots \overset{(s-1)}{u}$$

alle von einander verschieden. Nun leitet sich $\overset{(s+k)}{u}$ aus $\overset{(s)}{u}$ durch Multiplikation von $\overset{(s)}{u}$ mit E^k und nachherige Reduktion ab; auf

dieselbe Weise kann $\overset{(r+k)}{u}$ aus $\overset{(r)}{u}$ abgeleitet werden, und da der Voraussetzung nach $\overset{(r)}{u}$ und $\overset{(s)}{u}$ identisch sind, so müssen es auch $\overset{(r+k)}{u}$ und $\overset{(s+k)}{u}$ sein. Setzt man speziell $k = -r$ und $s - r = \lambda$, so findet sich $\overset{(0)}{u}$ identisch mit $\overset{(s-r)}{u}$ oder $\overset{(\lambda)}{u}$, und man hat dann eine Periode von λ Gliedern

$$\overset{(0)}{u},\ \overset{(1)}{u},\ \overset{(2)}{u},\ \ldots\ldots\ \overset{(\lambda-1)}{u},$$

welche entstehen durch Reduktion von

$$\overset{(0)}{u},\ E\overset{(0)}{u},\ E^2\overset{(0)}{u},\ \ldots\ldots E^{\lambda-1}\overset{(0)}{u},$$

und zwar sind, wie leicht zu sehen, die Glieder derselben alle von einander verschieden, und die notwendige und hinreichende Bedingung, dass irgend zwei Glieder $\overset{(r)}{u}$ und $\overset{(s)}{u}$ der Reihe

$$\ldots\ \overset{(-2)}{u},\ \overset{(-1)}{u},\ \overset{(0)}{u},\ \overset{(1)}{u},\ \overset{(2)}{u},\ \ldots\ldots$$

identisch seien, ist

$$r \equiv s \pmod{\lambda}.$$

§ 16. Entscheidung der Aequivalenz.

Es seien nun

$$f = \frac{1}{\theta^3}\, N\left(\frac{u_1 x_1 + u_2 x_2 + u_3 x_3}{M'_k\, M''_k}\right) \text{ und } \varphi = \frac{1}{\theta'^3}\, N\left(\frac{v_1 x_1 + v_2 x_2 + v_3 x_3}{M'_i\, M''_i}\right)$$

zwei reduzierte Formen. Es soll entschieden werden, ob sie äquivalent seien oder nicht. Angenommen, sie seien es und es gehe φ in f über durch die Substitution

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma''. \end{matrix}$$

Dabei gehe $v_1 x_1 + v_2 x_2 + v_3 x_3$ über in $w_1 x_1 + w_2 x_2 + w_3 x_3$, wo demnach

$$w_1 = v_1\alpha + v_2\alpha' + v_3\alpha''$$

$$w_2 = v_1\beta + v_2\beta' + v_3\beta''$$

$$w_3 = v_1\gamma + v_2\gamma' + v_3\gamma''$$

ist. Dann haben w_1, w_2, w_3, wenn von Primfaktoren von $3D$ abgesehen wird, wieder den grössten gemeinschaftlichen idealen Teiler $M_i' M_i''$, und es ist

$\frac{1}{\theta'^3} N\left(\frac{w_1x_1 + w_2x_2 + w_3x_3}{M_i' M''}\right)$ identisch mit $\frac{1}{\theta^3} N\left(\frac{u_1x_1 + u_2x_2 + u_3x_3}{M_k' M_k''}\right)$.

Aus dieser Identität folgt

$$\frac{w_1}{u_1} = \frac{w_2}{u_2} = \frac{w_3}{u_3}.$$

Wird dieser Quotient mit k bezeichnet und

$$k_1 = k\,\frac{M_k' M_k''}{M_i' M_i''}$$

gesetzt, so kommt

$$\frac{w_1x_1 + w_2x_2 + w_3x_3}{M_i' M_i''} = k_1\,\frac{u_1x_1 + u_2x_2 + u_3x_3}{M_k' M_k''}.$$

Da nun $M_i' M_i''$ ein idealer Teiler ist von w_1, w_2, w_3, so enthält der Ausdruck links nur ganze ideale Zahlen zu Koeffizienten; dasselbe muss daher mit dem Ausdruck rechts der Fall sein. Auch hier müssen sich die idealen Primfaktoren des Nenners gegen die des Zählers fortheben. Da nun u_1, u_2, u_3 den grössten gemeinschaftlichen idealen Teiler $M_k' M_k''$ haben, so müssen sich alle idealen Primfaktoren des Nenners von k_1 gegen die des Zählers fortheben. Schreibt man die Gleichung aber

$$\frac{1}{k_1} \cdot \frac{w_1x_1 + w_2x_2 + w_3x_3}{M_i' M_i''} = \frac{u_1x_1 + u_2x_2 + u_3x_3}{M_k' M_k''},$$

so sieht man, dass auch die idealen Primfaktoren des Zählers von k, sich gegen die des Nenners fortheben müssen. Macht man nun durch Multiplikation mit einem passenden idealen Faktor in Zähler und Nenner den Zähler zu einer wirklichen complexen Zahl z. B.

$$k_1 = \frac{w_1}{u_1} \cdot \frac{N(M_k)}{M_k M_i' M_i''} = \frac{g(\omega)}{\theta_1 \cdot i(\omega)},$$

wo θ_1 das Produkt der in u_1 enthaltenen Primzahlen t bedeutet, insofern sie sich gegen solche im Zähler nicht wegheben, so ist $i(\omega)$ eine ideale Zahl, die mit $M_k \,.\, M_i' \, M_i''$ in dieselbe Klasse gehört, also auch $i(\omega) M_i$ mit M_k. Nun ist

$$\theta'^3 = \theta^3 N(k_1) = \frac{\theta^3}{\theta_1^3} \, N\left(\frac{g(\omega)}{i(\omega)}\right),$$

oder

$$N \frac{g(\omega)}{i(\omega)} = \frac{\theta'^3 \, \theta_1^3}{\theta^3} = \theta''^3,$$

wo θ'' eine ganze Zahl ist. Die Zahl k_1 stellt sich also heraus als das Produkt von $\frac{1}{\theta_1}$ in einen Bruch $\frac{g(\omega)}{i(\omega)}$. Der Zähler $g(\omega)$ dieses Bruchs ist eine wirkliche komplexe Zahl und hat zur Norm das Produkt aus der dritten Potenz eines Divisors von Θ in einen Faktor, welcher zu $3D$ prim ist; der Nenner $i(\omega)$ ist das Produkt aller idealen in $g(\omega)$ enthaltenen Primfaktoren.

Aus allen Brüchen $\frac{g(\omega)}{i(\omega)}$ von der eben erwähnten Eigenschaft, für welche $i(\omega)$ in dieselbe Klasse komplexer Zahlen gehört, wähle man je einen. Die Anzahl der so erhaltenen Brüche[1]) ist also höchstens gleich der Anzahl h der Multiplikatoren.

Giebt es nun unter diesen Brüchen keinen, für welchen $i(\omega) \,.\, M_i$ mit M_k in dieselbe Klasse gehört, so können offenbar die vorgelegten Formen nicht äquivalent sein. Existiert aber ein solcher Bruch $\frac{g(\omega)}{i(\omega)}$, so multipliziere man mit demselben den Ausdruck

$$\frac{u_1 x_1 + u_2 x_2 + u_3 x_3}{M_k' \, M_k''}.$$

Schreibt man das Produkt in der Form

$$\frac{g(\omega) \,.\, N(M_i) \, (u_1 x_1 + u_2 x_2 + u_3 x_3)}{i(\omega) \, M_i \,.\, M_k' M_k'' \,.\, M_i' M_i''},$$

so sind die Koeffizienten von x_1, x_2, x_3 im Zähler wirkliche komplexe Zahlen, welche durch die wirkliche komplexe Zahl

[1]) Dieselben lassen sich als Potenzen eines derselben darstellen und ihre Anzahl ist ein Divisor von h.

$i(\omega) M_i \,.\, M_k' M_k''$ teilbar sind. Hebt man diese weg und bringt den Zähler durch lineare Transformationen in die reduzierte Form

$$\omega_1 x_1 + \omega_2 x_2 + \omega_3 x_3,$$

so erhält man den Ausdruck

$$\frac{\omega_1 x_1 + \omega_2 x_2 + \omega_3 x_3}{M_i' M_i''},$$

und die Untersuchung ist darauf zurückgeführt, zu entscheiden, ob zwei reduzierte Formen mit demselben idealen Nenner $M_i' M_i''$ äquivalent sein können.

Die Frage, ob

$$\frac{1}{\theta^3} N\left(\frac{u_1 x_1 + u_2 x_2 + u_3 x_3}{M_k' M_k''}\right) \text{ mit } \frac{1}{\theta'^3} N\left(\frac{v_1 x_1 + v_2 x_2 + v_3 x_3}{M_k' M_k''}\right)$$

identisch sein könne, kann wieder behandelt werden wie vorhin; nur gehört jetzt die ideale Zahl $i(w)$ zur Hauptklasse, d. h. sie ist eine wirkliche komplexe Zahl und daher $g(\omega)$ teilbar durch $i(\omega)$. Nennt man den Quotienten $g'(\omega)$, so ist nun $g'(\omega)$ eine komplexe Zahl, deren Norm die dritte Potenz eines Divisors θ von Θ ist. Alle Zahlen $\frac{g'(\omega)}{\theta}$ können nach § 10 als ganze Potenzen einer einzigen $\frac{H(\omega)}{\Theta_1}$ dargestellt werden, und zwar stellen die ersten $(\Theta_1 - 1)$ Potenzen der letztern alle Zahlen $\frac{g'(\omega)}{\theta}$ dar, welche nicht durch Multiplikation mit einer Einheit aus einander abgeleitet werden können und nur solche. Mit diesen $\Theta_1 - 1$ ersten Potenzen multipliziere man den Ausdruck $\frac{u_1 x_1 + u_2 x_2 + u_3 x_3}{\theta}$, wobei gemeinschaftliche Faktoren t im Nenner und den Koeffizienten des Zählers wegzulassen sind, und reduziere den erhaltenen Linearfaktor. Von jedem der so erhaltenen Linearfaktoren bilde man endlich noch die durch Multiplikation mit Einheiten abgeleitete Periode, so muss sich unter den so erhaltenen Formen auch die Form φ befinden, ansonst φ und f nicht äquivalent sein können. Denn durch das angegebene Verfahren sind alle reduzierten Formen gebildet worden, welche der Form f äquivalent sind.

Hieraus ergiebt sich folgende Konstruktion eines Systems nicht äquivalenter Formen:

Man nehme irgend eine reduzierte Form, multipliziere den Ausdruck

$$\frac{u_1 x_1 + u_2 x_2 + u_3 x_3}{\theta \,.\, M_k' \, M_k''},$$

dessen Norm die Form vorstellt, mit jedem der oben definierten Brüche

$$\frac{1}{\theta'} \cdot \frac{g(\omega)}{i(\omega)} \quad \left(\text{wo } \theta'^3 = N\left(\frac{g(\omega)}{i(\omega)}\right)\right)$$

und reduziere; jeden der erhaltenen reduzierten Linearfaktoren multipliziere man mit den ersten $\Theta_1 - 1$ Potenzen von $\frac{H(\omega)}{\Theta_1}$ und reduziere wieder; endlich bilde man von allen so erhaltenen reduzierten Linearfunktionen $u_1 x_1 + u_2 x_2 + u_3 x_3$, soweit dieselben nicht identisch sind, die Periode. Die Normen aller so erhaltenen Ausdrücke $\frac{u_1 x_1 + u_2 x_2 + u_3 x_3}{\theta \,.\, M_k' \, M_k''}$ sind äquivalente Formen.

Hierauf nehme man von den übrig gebliebenen reduzierten Formen je eine und leite aus ihr in derselben Weise alle äquivalenten ab, u. s. w., bis alle Formen des Systems erschöpft sind.

Nimmt man nun von allen auf diese Weise aus einer Form abgeleiteten nur eine, beliebige heraus, so bildet der Komplex der so gewählten ein System nicht äquivalenter Formen, wie es zu gegebenen Werten von D und δ gehört.

Für den speziellen Fall, wo D keinen quadratischen Teiler hat, also $\Theta = 1$ ist, fallen die Zahlen $\frac{g(\omega)}{i(\omega)}$ und $\frac{H(\omega)}{\Theta_1}$ weg; zwei Formen sind dann immer nicht äquivalent, wenn sie verschiedenen Multiplikatoren zugehören. Was die Gliederzahl λ einer Periode anbetrifft, so kann dieselbe für nicht äquivalente Formen verschieden sein.

§ 17. Transformation der Formen in sich selbst [1]).

Mit Hülfe der vorangegangenen Entwickelungen ergeben sich nun die Transformationen einer beliebigen Form F in eine ihr äquivalente Φ auf folgende Weise:

---

[1]) Vgl. Dirichlet, Zahlentheorie § 60.

Sind F und Φ irgend zwei äquivalente Formen, und man kennt eine Transformation Σ von F in Φ und alle Transformationen S von Φ in sich selbst, so stellt, wie leicht ersichtlich, $\Sigma S \Sigma^{-1}$ irgend eine Transformation von F in sich selbst dar; man braucht deshalb nur die Transformationen der reduzierten Formen in sich selbst zu kennen.

Sei also

$$f = N\left(\frac{u_1 x_1 + u_2 x_2 + u_3 x_3}{\theta \,.\, M_k' M_k''}\right)$$

eine reduzierte Form, die durch die Substitution S in sich selbst übergehe, so dass, wenn $w_1 x_1 + w_2 x_2 + w_3 x_3$ den transformierten Ausdruck $u_1 x_1 + u_2 x_2 + u_3 x_3$ bedeutet,

$$N\left(\frac{w_1 x_1 + w_2 x_2 + w_3 x_3}{\theta \,.\, M_k' M_k''}\right)$$

identisch ist mit f; also

$N(w_1 x_1 + w_2 x_2 + w_3 x_3)$ identisch mit $N(u_1 x_1 + u_2 x_2 + u_3 x_3)$.

Bezeichnet man das Verhältnis

$$\frac{w_1}{u_1} = \frac{w_2}{u_2} = \frac{w_3}{u_3}$$

mit k, so wird

$$w_1 x_1 + w_2 x_2 + w_3 x_3 = k\ (u_1 x_1 + u_2 x_2 + u_3 x_3),$$

$$N(k) = 1,$$

und man findet ganz in derselben Weise wie früher, dass k eine gebrochene Einheit $\frac{g(\omega)}{\theta_1}$ ist; und zwar muss der Nenner θ_1 ein Divisor von θ sein, denn enthielte er eine dieses nicht teilende Primzahl t, so ginge diese nicht in den Koeffizienten der Produkte

$$u_1 g(\omega),\quad u_2 g(\omega),\quad u_3 g(\omega)$$

auf, wie man sofort sieht, wenn man beachtet, dass in

$$g(\omega) = a + b\omega + c\omega^2,$$

a und b durch t teilbar sind, c nicht, und dass in u_1, u_2, u_3 wenigstens einer der Koeffizienten a_1, a_2, a_3 nicht durch t teilbar

ist; somit wäre der Nenner θ für beide Formen nicht derselbe. Es lassen sich aber alle solchen Brüche $\frac{g(\omega)}{\theta}$ als ganze Potenzen eines derselben

$$\frac{g(\omega)}{\theta} = \left(\frac{H(\omega)}{\Theta_1}\right) \cdot \frac{\Theta_1}{\theta}$$

darstellen. Man multipliziere daher $u_1 x_1 + u_2 x_2 + u_3 x_3$ mit $\frac{g(\omega)}{\theta}$ und reduziere. Ist der so erhaltene Ausdruck mit $u_1 x_1 + u_2 x_2 + u_3 x_3$ wieder identisch, so giebt die bei der Reduktion angewandte Substitution eine Transformation in sich selbst; ist er von $u_1 x_1 + u_2 x_2 + u_3 x_3$ verschieden, so multipliziere man wieder mit $\frac{g(\omega)}{\theta}$ und reduziere, und so fahre man fort, bis man auf einen mit $u_1 x_1 + u_2 x_2 + u_3 x_3$ identischen Ausdruck gelangt, was nach höchstens $\theta\lambda$ Wiederholungen geschehen muss. Die Zusammensetzung der dabei angewandten Substitutionen liefert eine Transformation in sich selbst und zwar die Fundamentaltransformation, aus deren Wiederholung alle übrigen hervorgehen.

Ich führe hier noch die Litteratur der bis jetzt behandelten Beispiele von zerlegbaren Formen an:

1) Die klassische Theorie der binären quadratischen Formen.
2) Die binären quadratischen Formen mit komplexen Koeffizienten und Unbestimmten, als specielles Beispiel zerlegbarer biquadratischer Formen (Dirichlet, Crelle's Journal Bd. 24; Smith, Proceed. of the R. Society 1864).
3) Eisenstein, Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln etc. (Crelle's Journ. Bd. 28).
4) Abhandlungen von Eisenstein (Cr. J. Bd. 27) und Arndt über binäre kubische Formen.
5) Hermite, Extraits de lettres à M. Jacobi (Cr. J. Bd. 40).
   „ Sur la théorie des formes quadratiques (Cr. J. Bd. 47).

Obwohl ich in vorstehender Arbeit bemüht gewesen bin, die Sache so zu behandeln, dass die unmittelbare Anwendbarkeit der Methode auf die allgemeinen zerlegbaren Formen, nachdem zuvor die allgemeine Theorie der komplexen Zahlen aufgestellt worden ist (worüber auf die oben angeführte Abhandlung von Herrn Selling verwiesen werden mag), unmittelbar einleuchtet, so sind doch der Natur des hier untersuchten speciellen Falles nach einige wesentliche Punkte ausgefallen. So die Theorie der ambigen Formen, weil hier von keiner Vertauschbarkeit der drei Faktoren die Rede sein konnte; ferner ist auch nur eine Fundamentaleinheit und demzufolge auch nur eine Fundamentalsubstitution für Transformationen in sich selbst aufgetreten. Erwähnen muss ich auch noch, dass schon im Jahr 1859 von Herrn Prof. Kummer in seiner bewundernswürdigen Abhandlung über die allgemeinen Reziprozitätsgesetze (§ 6) eine Arbeit von Herrn Kronecker über diesen Gegenstand angekündigt wurde, die aber meines Wissens bis jetzt leider nicht erschienen ist.

Soll ich noch angeben, welchen Teil der Abhandlung ich als neu, wenigstens meines Wissens noch nirgends publiziert, jedenfalls aber als ganz selbständige Arbeit betrachte, so ist es, nebst einigen Entwicklungen in Abschnitt I und II, hauptsächlich Abschnitt III; indessen lege ich eher Gewicht auf die dargelegte Behandlungsweise als auf die gewonnenen Resultate.

Endlich möge der Drang der Umstände häufige Unebenheiten in Darstellung und Ausdruck einigermassen entschuldigen.

Zürich, 2. April 1870.