# SUR LA THÉORIE DES NOMBRES.

[Extrait d'une lettre adressée à M. Liouville.]

En voyant dans votre Journal l'élégante traduction que M. Terquem a bien voulu faire de mon *Mémoire sur la progression arithmétique**), j'ai eu l'idée d'étendre la même analyse aux formes quadratiques. En combinant cette analyse avec les considérations ingénieuses que M. Gauss développe dans les derniers numéros de sa cinquième section, on prouve non seulement que toute forme quadratique renferme une infinité de nombres premiers, mais encore qu'elle en contient qui soient d'une forme linéaire quelconque compatible avec la forme quadratique donnée.

Je me suis aussi beaucoup occupé dans ces derniers temps à étendre aux formes quadratiques à coefficients et indéterminées complexes, c'est-à-dire de la forme $t+u\sqrt{-1}$, les théorèmes qui ont lieu dans les cas ordinaires des entiers réels. Si l'on cherche en particulier à obtenir le nombre des formes quadratiques différentes qui existent dans cette hypothèse pour un déterminant donné, on arrive à ce résultat assez remarquable, que le nombre dont il s'agit dépend de la division de la lemniscate, de même que dans le cas des formes réelles et à déterminant positif, il se rattache à la section du cercle. Ce qui m'a surtout fait plaisir dans ce travail, c'est le parti qu'on y tire de considérations géométriques et particulièrement de la théorie des propriétés perspectives des figures. Au moyen de cet auxiliaire, la question qui d'abord, et considérée d'une manière purement analytique, paraît extrêmement compliquée, devient presque aussi simple que lorsqu'il s'agit de déterminants réels.

*) Tome IV du Journal de Liouville, page 393 [1]).

[1]) Bd. II dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

Les recherches dont je viens de vous indiquer l'objet, m'ont conduit à un théorème remarquable par sa simplicité et qui ne paraît pas sans importance pour la théorie des équations indéterminées des degrés supérieurs au second, matière encore très peu cultivée. Voici en quoi consiste ce théorème:

„Si l'équation:

$$s^n + a s^{n-1} + \cdots + g s + h = 0, \tag{1}$$

à coefficients entiers, n'a pas de diviseur rationnel, et si parmi ses racines:

$$\alpha, \beta, \ldots, \omega$$

il y en a au moins une qui soit réelle, je dis que l'équation indéterminée:

$$F(x, y, \ldots, z) = \varphi(\alpha)\varphi(\beta)\ldots\varphi(\omega) = 1, \tag{2}$$

où l'on a posé pour abréger:

$$\varphi(\alpha) = x + \alpha y + \cdots + \alpha^{n-1} z,$$

a toujours une infinité de solutions entières."

Pour établir ce théorème, il faut d'abord faire voir qu'il existe au moins un entier $m$ tel que l'équation:

$$F(x, y, \ldots, z) = m \tag{3}$$

ait une infinité de solutions. C'est à quoi l'on peut parvenir par différents moyens. Dans le cas du second degré, la chose, qui pour ce cas n'est pas nouvelle, résulte immédiatement des propriétés des fractions continues.

L'équation (3) ayant une infinité de solutions, il en existera deux telles que l'on ait:

$$F(x, y, \ldots, z) = m, \quad F(x', y', \ldots, z') = m,$$

et en même temps:

$$x \equiv x', \quad y \equiv y', \quad \ldots, \quad z \equiv z' \pmod{m}. \tag{4}$$

Cela posé, si nous considérons la fraction:

$$\frac{x' + \alpha y' + \cdots + \alpha^{n-1} z'}{x + \alpha y + \cdots + \alpha^{n-1} z},$$

on pourra évidemment, en multipliant par:

$$\varphi(\beta) \ \ldots \ \varphi(\omega),$$

lui donner la forme:

$$\frac{X + \alpha Y + \cdots + \alpha^{n-1} Z}{m},$$



où $X, Y, \ldots, Z$ sont des fonctions entières et à coefficients entiers de:

$$x, y, \ldots, z, \quad x', y', \ldots, z'.$$

Je dis maintenant que $X, Y, \ldots, Z$ sont des multiples de $m$. Pour le faire voir, admettons pour un instant que dans ces expressions:

$$x', \ y', \ \ldots, \ z'$$

soient changés en:

$$x, \ y, \ \ldots, \ z,$$

changement par lequel $X, Y, \ldots, Z$ resteront, en vertu des congruences (4), congrus à eux-mêmes. Par le changement dont il s'agit:

$$X + \alpha Y + \cdots + \alpha^{n-1} Z$$

doit devenir égal à $m$, ce qui ne peut arriver [l'équation (1) n'ayant pas de diviseurs rationnels] qu'autant que:

$$X, \ Y, \ \ldots, \ Z$$

deviennent respectivement:

$$m, \ 0, \ \ldots, \ 0.$$

Donc $X, Y, \ldots, Z$ sont divisibles par $m$, et la fraction considérée plus haut est:

$$\xi + \alpha\eta + \cdots + \alpha^{n-1}\zeta,$$

$\xi, \eta, \ldots, \zeta$ étant des entiers; d'où l'on conclut:

$$F(\xi, \eta, \ldots, \zeta) = 1,$$

solution qui en fournira une infinité d'autres.

Parmi les conséquences nombreuses qu'on peut tirer de ce théorème, il y en a une qui se présente pour ainsi dire d'elle-même; elle consiste en ce que les fonctions que LAGRANGE a d'abord considérées dans les *Mémoires de Berlin*, plus tard dans les *Additions à l'Algèbre* d'EULER, et qui se reproduisent par multiplication, si elles peuvent obtenir une certaine valeur, sont dès lors susceptibles de la même valeur pour une infinité de systèmes de valeurs des indéterminées $x, y, \ldots, z$, en supposant toutefois que l'équation algébrique d'où ces fonctions tirent leur origine satisfasse aux conditions ci-dessus énoncées.

# EINIGE RESULTATE VON UNTERSUCHUNGEN ÜBER EINE CLASSE HOMOGENER FUNCTIONEN DES DRITTEN UND DER HÖHEREN GRADE.

VON

G. LEJEUNE DIRICHLET.

Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1841, S. 280—285.

# EINIGE RESULTATE VON UNTERSUCHUNGEN ÜBER EINE CLASSE HOMOGENER FUNCTIONEN DES DRITTEN UND DER HÖHEREN GRADE.

[Mitgetheilt in der Sitzung der physikalisch-mathematischen Classe der Akademie der Wissenschaften am 11. October 1841.]

Die homogenen Functionen mit ganzzahligen Coefficienten, auf welche sich diese Untersuchungen beziehen, sind diejenigen besonderen Functionen jedes Grades, welche eine ihrem Grade gleiche Anzahl von unbestimmten ganzen Zahlen enthalten und zugleich in lineare Factoren mit irrationalen Coefficienten zerlegt werden können. Für den zweiten Grad fallen dieselben mit den so vielfach behandelten binären quadratischen Formen zusammen, und wie die Theorie dieser Formen einen der fruchtbarsten Theile der Arithmetik bildet, so kommen auch den analogen Ausdrücken von höherem Grade eine Menge der interessantesten Eigenschaften zu, deren Erforschung nicht nur der Theorie der Zahlen sondern auch anderen damit zusammenhängenden Disciplinen bedeutende Erweiterungen zu versprechen scheint. Von den zahlreichen Untersuchungen, zu welchen dieser Gegenstand Veranlassung giebt, betrifft die der Classe gemachte Mittheilung nur die Aufgabe:

„Alle Darstellungen einer gegebenen Zahl durch eine gegebene Function der genannten Art aufzufinden, oder sich doch zu überzeugen, dass die gegebene Zahl einer solchen Darstellung nicht fähig ist."

Um die Betrachtungen, auf welchen die Lösung der eben ausgesprochenen Frage beruht, in das gehörige Licht zu setzen, wird es zweckmässig sein, dieselben zunächst auf den zweiten Grad anzuwenden, obgleich die Aufgabe für diesen Fall längst durch andere Methoden ihre vollständige Erledigung gefunden hat.

Für diesen Fall verlangt die Aufgabe, dass man alle Auflösungen der unbestimmten Gleichung:

$$ax^2+2bxy+cy^2 = m \tag{1}$$

darstelle, in welcher:

$$b^2-ac = D$$

als positiv und keinem Quadrate gleich vorausgesetzt werden kann, da sonst die Frage gar keine Schwierigkeit darbietet. Die Methode, welche wir anzudeuten versuchen wollen, macht die Lösung dieses Problems von der Kenntniss irgend zweier Werthe abhängig, welche der bekanntlich immer möglichen Gleichung:

$$t^2-Du^2 = 1 \tag{2}$$

genügen. Sind:

$$T,\ U$$

zwei solche Werthe (die wir beide positiv voraussetzen können), und hätte man andererseits irgend eine Auflösung:

$$(X,\ Y)$$

der Gleichung (1), so würde man, nach einer von EULER gemachten Bemerkung, unzählige neue Auflösungen daraus ableiten können, welche durch die Formel:

$$ax+(b+\sqrt{D})y = \pm(aX+[b+\sqrt{D}]\,Y)(T+U\sqrt{D})^n \tag{3}$$

bestimmt werden, in welcher $n$ irgend eine positive oder negative ganze Zahl bezeichnet, und nach geschehener Entwickelung die rationalen Theile und die Coefficienten von $\sqrt{D}$ auf beiden Seiten besonders gleich zu setzen sind. Wie wichtig die von EULER gemachte Bemerkung auch sei, so begründet dieselbe doch noch keineswegs eine vollständige Zurückführung der Gleichung (1) auf die Gleichung (2), da dieselbe kein Mittel an die Hand giebt, eine erste Auflösung:

$$(X,\ Y)$$

zu finden, und andererseits, wie LAGRANGE gezeigt hat, der Ausdruck (3) nicht nothwendig alle Auflösungen der Gleichung (1) zu enthalten braucht, selbst wenn man für:

$$T,\ U$$

die kleinsten der Gleichung (2) genügenden Werthe wählt.

Um nun die oben verlangte vollständige Zurückführung zu bewerkstelligen, bemerke man, dass die in (3) enthaltenen Auflösungen eine Gruppe bilden,



welche dieselben Auflösungen zu enthalten fortfahren wird, wenn man statt der Auflösung $(X, Y)$ irgend eine der daraus ableitbaren einführt. Es folgt hieraus, dass die Gesammtheit aller Auflösungen der Gleichung (1) in Gruppen dieser Art vertheilt werden kann, und dass es zur vollständigen Lösung unserer Aufgabe nur darauf ankommen wird, aus jeder Gruppe eine Auflösung zu kennen, da alsdann die ganze Gruppe selbst durch (3) gegeben sein wird. Nun ist aber aus (3) klar, dass in jeder Gruppe der Ausdruck:

$$ax+(b+\sqrt{D})y$$

nothwendig einmal und nur einmal einen Werth annimmt, der zwischen die beiden Grenzen:

$$\sigma \quad \text{und} \quad \sigma(T+U\sqrt{D})$$

mit Ausschluss von einer derselben fällt, wenn $\sigma$ einen beliebigen positiven oder negativen Werth bezeichnet. Nimmt man z. B. $\sigma$ positiv, so giebt es also in jeder Gruppe eine und nur eine Auflösung von solcher Beschaffenheit, dass:

$$\sigma < ax+(b+\sqrt{D})y \leq \sigma(T+U\sqrt{D}). \tag{4}$$

Mit diesem Resultate ist nun die Frage sogleich erledigt, da man leicht durch eine endliche Anzahl von Versuchen alle den Ungleichheiten (4) genügenden Auflösungen der Gleichung (1) finden oder doch sich überzeugen kann, dass keine solche existirt. Man sieht die Möglichkeit hiervon sogleich, wenn man der Sache eine geometrische Einkleidung giebt. Als Gleichung einer auf rechtwinklige Coordinaten bezogenen Curve betrachtet, stellt (1) eine Hyperbel dar, von welcher nur ein endlicher Bogen den Bedingungen (4) genügt, so dass man also in der That leicht alle innerhalb dieses Bogens liegenden Punkte finden kann, deren Coordinaten ganze Zahlen sind. Jeder dieser Punkte bestimmt dann eine Gruppe von Auflösungen der Gleichung (1), und falls sich keiner findet, ist die Unmöglichkeit dieser Gleichung dargethan.

Wie man sieht, ist der Erfolg des eben beschriebenen Verfahrens von der Wahl der Auflösung $(T, U)$, welche dabei als Ausgangspunkt dient, ganz unabhängig. Die Rechnung wird jedoch am kürzesten, wenn diese Auflösung die in den kleinsten Zahlen ausgedrückte ist, aus welcher bekanntlich alle übrigen durch Potenziren erhalten werden können. Wählt man eine dieser abgeleiteten, so hat dies keinen anderen Uebelstand, als dass die Anzahl der Gruppen im Endresultat dadurch vergrössert wird.

Indem wir zum dritten Grade übergehen, werden wir, der Kürze wegen und um das Schreiben zu complicirter Ausdrücke zu vermeiden, nicht die allgemeinste Function der oben näher bezeichneten Art betrachten, sondern uns auf diejenige besondere dritten Grades beschränken, welche zu der allgemeinsten dieses Grades in ähnlicher Beziehung steht, wie sich für den zweiten Grad die sogenannte Hauptform:

$$x^2 - Dy^2$$

zu der allgemeinen Form:

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

derselben Determinante verhält. Ist:

$$s^3 + as^2 + bs + c = 0 \tag{5}$$

eine cubische Gleichung, deren Coefficienten ganze Zahlen sind, und welche durch keinen rationalen Factor theilbar ist, und bezeichnen:

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

die Wurzeln derselben, so ist der zu betrachtende Ausdruck:

$$F(x, y, z)$$

das Product von:

$$x + \alpha y + \alpha^2 z$$

und zwei ähnlichen aus $\beta$ und $\gamma$ gebildeten linearen Functionen. Die zu lösende Gleichung wird alsdann:

$$F(x, y, z) = m, \tag{6}$$

während die der obigen Gleichung (2) entsprechende mit der folgenden zusammenfällt:

$$F(t, u, v) = 1, \tag{7}$$

Was diese letztere betrifft, so lässt sich durch Betrachtungen, die hier nicht ausgeführt werden können, nachweisen, dass sie wie jene (2) immer auflösbar ist, und es wird nun zu zeigen sein, wie man aus einer oder zwei Auflösungen der Gleichung (7) alle Werthe $x$, $y$, $z$ ableiten kann, welche der Gleichung (6) genügen, oder wie man sich davon überzeugen kann, dass keine solche existiren. Hierbei treten nun zwei wesentlich verschiedene Fälle ein, je nachdem nämlich die Gleichung (5) nur eine oder drei reelle Wurzeln hat.

Im ersteren dieser Fälle, den wir allein hier ausführlich besprechen werden, hat die Gleichung (7) mit der Gleichung (2) die Eigenschaft gemein, dass alle



ihre Auflösungen aus einer Fundamental-Auflösung durch Potenziren abgeleitet werden können; allein es ist für unsern Zweck nicht erforderlich, diese einfachste Auflösung zu kennen, sondern das Verfahren bleibt bis auf die grössere Länge der Rechnung ganz dasselbe, wenn man von einer der abgeleiteten Auflösungen ausgeht. Ist nämlich:

$$(T, \quad U, \quad V)$$

eine solche*), und bezeichnet man andrerseits mit:

$$X, \quad Y, \quad Z$$

irgend welche ganze Zahlen, die der Gleichung (6) genügen, so lassen sich daraus unendlich viele neue ableiten, wenn man in der Gleichung:

$$x + \alpha y + \alpha^2 z = (X + \alpha Y + \alpha^2 Z)(T + \alpha U + \alpha^2 V)^n \tag{8}$$

nach geschehener Entwickelung die rationalen Theile, so wie die Coefficienten von $\alpha$ und $\alpha^2$ besonders gleich setzt. Die durch diese Formel mit einander verbundenen Auflösungen bilden offenbar wieder eine Gruppe, welche von der Wahl des Anfangsgliedes $(X, Y, Z)$ unabhängig ist, d. h. welche dieselbe bleibt, wenn man dieses mit irgend einem anderen Gliede derselben Gruppe vertauscht. Es folgt daraus, wie oben, dass sich die Gesammtheit aller Auflösungen der Gleichung (6) in solche Gruppen vertheilen lassen muss, und dass man sich im Besitze aller dieser Auflösungen befinden wird, sobald man aus jeder Gruppe ein Glied anzugeben im Stande ist. Nun ist aus (6) und (8) sogleich klar, wenn man unter $\alpha$ diejenige der Wurzeln der Gleichung (5) versteht, welche reell ist, dass:

$$x + \alpha y + \alpha^2 z$$

dasselbe Zeichen wie $m$ hat und in jeder Gruppe einmal und nur einmal einen Werth erhält, der zwischen den Grenzen:

$$\sigma \quad \text{und} \quad \sigma(T + \alpha U + \alpha^2 V)$$

mit beliebigem Ausschlusse von einer derselben liegt, wo die Grösse $\sigma$ ganz willkürlich und der einzigen Beschränkung unterworfen ist, ein dem Zeichen von $m$ gleiches Zeichen zu haben. Die Auffindung aller Auflösungen, welche diese doppelte Bedingung erfüllen und die Repräsentanten von eben so vielen Gruppen sind, lässt sich aber sogleich durch Versuche in endlicher Anzahl

*) Es versteht sich von selbst, dass die ganz illusorische Auflösung (1, 0, 0) ausgeschlossen werden muss.

bewerkstelligen, oder es lässt sich erkennen, dass keine solche und also überhaupt keine Auflösungen der Gleichung (6) existiren. In der That stellt die Gleichung (6), wenn man darin $x$, $y$, $z$ als rechtwinklige Coordinaten betrachtet, eine krumme Fläche von unendlicher Ausdehnung dar, welche in unserem Falle, wo nur eine der Wurzeln $\alpha$, $\beta$, $\gamma$ reell ist, eine Ebene und eine Gerade zu Asymptoten hat. Die oben erhaltenen Ungleichheitsbedingungen haben dann die geometrische Bedeutung, dass man nur das Stück der Fläche zu betrachten hat, welches zwischen den durch die Gleichungen:

$$x+\alpha y+\alpha^2 z=\sigma, \quad x+\alpha y+\alpha^2 z=\sigma(T+\alpha U+\alpha^2 V)$$

bestimmten Ebenen liegt, welche mit der vorher erwähnten Asymptoten-Ebene parallel sind. Dieses Stück aber hat, wie man leicht sieht, nur eine endliche Ausdehnung, so dass man also durch Versuche in beschränkter Anzahl immer wird entscheiden können, welche Punkte desselben ganzzahlige Coordinaten haben, wenn überhaupt Punkte dieser Art vorhanden sind.

Wir bemerken nur noch, dass in dem zweiten der früher unterschiedenen Fälle die Gleichung (7), wie in dem eben besprochenen, unendlich viele Auflösungen zulässt, die aber nicht alle aus einer durch Potenziren abgeleitet werden können. Es existiren vielmehr in diesem Falle zwei Grundauflösungen, welche durch Multiplication und Potenzirung alle übrigen erzeugen. Ohne diese zu kennen, wird es hinlänglich sein, von den derivirten zwei von solcher Beschaffenheit zu haben, dass nicht beide durch Potenzirung in eine und dieselbe dritte übergehen können, um daraus nach einem dem oben angegebenen ähnlichen Verfahren die Gesammtheit aller Auflösungen der Gleichung (6) ableiten zu können.

---

# VERALLGEMEINERUNG EINES SATZES AUS DER LEHRE VON DEN KETTENBRÜCHEN NEBST EINIGEN ANWENDUNGEN AUF DIE THEORIE DER ZAHLEN.

VON

G. LEJEUNE DIRICHLET.

Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1842, S. 93—95.

# VERALLGEMEINERUNG EINES SATZES AUS DER LEHRE VON DEN KETTENBRÜCHEN NEBST EINIGEN ANWENDUNGEN AUF DIE THEORIE DER ZAHLEN.

[Auszug aus einer in der Akademie der Wissenschaften am 14. April 1842 gelesenen Abhandlung.]

---

Ist $\alpha$ ein irrationaler Werth, so giebt es immer unendlich viele zusammengehörige ganze Zahlen $x$ und $y$, für welche der lineare Ausdruck $x-\alpha y$ numerisch kleiner als $\frac{1}{y}$ ist, wie dies aus der Theorie der Kettenbrüche längst bekannt ist. Die eben ausgesprochene Eigenschaft lässt sich wie folgt verallgemeinern:

„Sind $\alpha_1, \alpha_2, \ldots, \alpha_m$ gegebene positive oder negative Werthe von solcher Beschaffenheit, dass der lineare Ausdruck:

$$x_0+\alpha_1 x_1+\alpha_2 x_2+\cdots+\alpha_m x_m, \tag{1}$$

in welchem:

$$x_0,\ x_1,\ \ldots,\ x_m \tag{2}$$

unbestimmte positive oder negative ganze Zahlen bezeichnen, nur in dem Falle verschwinden kann, wenn $x_1 = x_2 = \cdots = x_m = 0$ und also auch $x_0 = 0$ ist, so giebt es immer unendlich viele Systeme (2), worin nicht:

$$x_1 = x_2 = \cdots = x_m = 0,$$

und für welche der Ausdruck (1) numerisch kleiner als $\frac{1}{s^m}$ ist, wo unter $s$ der grösste der Zahlenwerthe von $x_1, x_2, \ldots, x_m$ verstanden wird.“

Um diesen eben so einfachen als fruchtbaren Satz zu beweisen, wird es genügen nachzuweisen, dass ein System von der verlangten Beschaffenheit gefunden werden kann, für welches ausserdem der numerische Werth von (1) kleiner als eine vorher bestimmte Grösse $\delta$ ist. Um ein solches zu erhalten, nehme man eine positive ganze Zahl $n$, welche die Bedingung:

$$\frac{1}{(2n)^m} < \delta$$

erfüllt, und lege in dem Ausdrucke (1) jeder der Zahlen:

$$x_1,\ x_2,\ \ldots,\ x_m$$

alle in der Reihe:

$$-n,\ -(n-1),\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ n-1,\ n$$

enthaltenen Werthe bei. Bestimmt man nun für jede dieser $(2n+1)^m$ Verbindungen $x_0$ so, dass (1) einen nicht negativen unter der Einheit liegenden Werth erhält, so hat man $(2n+1)^m$ ächte Brüche, von denen nothwendig wenigstens zwei in *demselben* der durch die Werthe:

$$0,\ \frac{1}{(2n)^m},\ \frac{2}{(2n)^m},\ \ldots,\ \frac{(2n)^m-1}{(2n)^m},\ 1$$

begrenzten $(2n)^m$ Intervalle liegen müssen. Zieht man zwei Ausdrücke, denen solche Werthe entsprechen, von einander ab, so erhält man einen neuen Ausdruck von der Form (1), in welchem offenbar *erstens* die Zahlen $x_1, x_2, \ldots, x_m$ nicht alle zugleich verschwinden, *zweitens* keine dieser Zahlen, abgesehen vom Zeichen, $2n$ übertrifft, und dessen numerischer Werth endlich *drittens* kleiner als:

$$\frac{1}{(2n)^m} < \delta$$

und also auch kleiner als $\frac{1}{s^m}$ ist.

Hieraus folgt dann sogleich die Existenz von unendlich vielen Systemen (2), welche der Aussage des Satzes entsprechen. In der That, wie viele solcher Systeme man auch als schon bekannt voraussetzen möge, so wird es, da für keines derselben der Ausdruck (1) verschwindet, nach dem eben Gesagten möglich sein, ein neues von den gegebenen verschiedenes zu finden, indem man zu diesem Zwecke nur für $\delta$ den kleinsten Zahlenwerth des Ausdrucks (1) zu wählen braucht, welcher einem der schon bekannten Systeme entspricht.



Es giebt analoge Sätze für zwei oder mehr simultane Ausdrücke der Form (1), welche durch dieselben einfachen Betrachtungen erwiesen werden können, und von welchen der auf zwei bezügliche so lautet:

„Sind:

$$\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_m$$

und:

$$\beta_1,\ \beta_2,\ \ldots,\ \beta_m$$

(wo $m > 2$) zwei Reihen gegebener Werthe von solcher Beschaffenheit, dass die Summen:

(3) $$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_m x_m,$$

(4) $$\beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_m x_m,$$

nur in dem Falle gleichzeitig verschwinden können, wenn:

$$x_1 = x_2 = \cdots = x_m = 0$$

ist, so giebt es immer unendlich viele Systeme $x_1, x_2, \ldots, x_m$ nicht gleichzeitig verschwindender Zahlen, für welche (3) und (4) resp. numerisch kleiner sind als:

$$\frac{A}{s^a}$$

und:

$$\frac{B}{s^{m-2-a}},$$

in welchen Ausdrücken $A$ und $B$ bestimmte von:

$$\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_m,\quad \beta_1,\ \beta_2,\ \ldots,\ \beta_m$$

abhängende und $a$ eine beliebige zwischen 0 und $m-2$ liegende Constante bezeichnen.“

Ein für die Anwendungen auf die Zahlentheorie besonders wichtiger Fall ist der, wo die Exponenten $a$ und $m-2-a$ einander gleich genommen werden und die Ausdrücke in $\frac{A}{s^{\frac{m}{2}-1}}$ und $\frac{B}{s^{\frac{m}{2}-1}}$ übergehen.

Wir fügen noch hinzu, dass diese Sätze und ihre Beweise mit geringen Modificationen auf complexe Zahlen ausgedehnt werden können.

Vermittelst der eben erhaltenen Resultate lässt sich das Lemma, auf welchem die Verallgemeinerung der FERMATschen Gleichung $t^2 - Du^2 = 1$ beruht, ganz elementar beweisen*), und man sieht zugleich, dass das Lemma, so wie der

*) Comptes rendus des séances de l'Académie des sciences de Paris. Premier semestre 1840, p. 286.[1])

[1]) S. 622 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

darauf gegründete Satz noch richtig bleibt, wenn die algebraische Gleichung:

$$s^n + as^{n-1} + \cdots + gs + h = 0,$$

nur imaginäre Wurzeln hat, vorausgesetzt dass alsdann $n$ grösser als 2 sei. Die in Rede stehende Erweiterung fordert den Nachweis, dass es immer wenigstens *eine* ganze Zahl $m$ giebt, für welche die unbestimmte Gleichung:

$$F(x, y, z, \ldots) = m$$

unendlich viele Auflösungen zulässt, und dies folgt mit der grössten Leichtigkeit aus dem ersten oder dem erwähnten besonderen Falle des zweiten der obigen Sätze, je nachdem sich unter den Wurzeln der Gleichung wenigstens eine reelle befindet oder diese sämmtlich imaginär sind.

---

# ZUR THEORIE DER COMPLEXEN EINHEITEN.

VON

G. LEJEUNE DIRICHLET.

Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1846, S. 103—107.

# ZUR THEORIE DER COMPLEXEN EINHEITEN.[1])

[Mitgetheilt in der Sitzung der physikalisch-mathematischen Classe der Akademie der Wissenschaften am 30. März 1846.]

Es sei:

(1) $$F(\omega) = \omega^n + p_1\omega^{n-1} + p_2\omega^{n-2} + \cdots + p_n = 0$$

eine Gleichung von beliebigem Grade mit ganzen Coefficienten $p_1, p_2, \ldots, p_n$, die keinen rationalen Factor hat, und deren Wurzeln mit $\alpha, \beta, \ldots, \varrho$ bezeichnet werden sollen. Bildet man nun mit $n$ unbestimmten ganzen Zahlen $t, u, \ldots, z$ Ausdrücke von der Form:

$$\varphi(\alpha) = t + u\alpha + \cdots + z\alpha^{n-1}, \quad \varphi(\beta) = t + u\beta + \cdots + z\beta^{n-1}, \quad \ldots,$$

so wird das Product:

$$\varphi(\alpha)\varphi(\beta)\cdots\varphi(\varrho)$$

eine homogene Function mit ganzen Coefficienten von $t, u, \ldots, z$ sein, welche, wie LAGRANGE zuerst bemerkt hat, die merkwürdige Eigenschaft besitzt, sich durch Multiplication und folglich auch durch Potenzirung zu reproduciren. Für die Theorie der so gebildeten Functionen ist nun vor Allem die Beantwortung der Frage, für welche Systeme von Werthen $t, u, \ldots, z$ sie der Einheit gleich werden, d. h. die vollständige Auflösung der Gleichung:

(2) $$\varphi(\alpha)\varphi(\beta)\cdots\varphi(\varrho) = 1$$

von der grössten Wichtigkeit und als ein Fundamentalproblem dieser Theorie zu betrachten.

Nimmt man gewisse besondere Auflösungen dieser Gleichung aus, welche immer leicht gefunden werden können, und für welche die Factoren:

$$\varphi(\alpha), \varphi(\beta), \ldots, \varphi(\varrho)$$

Wurzeln der Einheit sind, so wird jede gegebene Auflösung, zu einer unbestimmten ganzen positiven oder negativen Potenz erhoben, unendlich viele neue Auflösungen erzeugen, und eben so einleuchtend ist es, dass man bei zwei oder mehr gegebenen Auflösungen unbestimmte Potenzen derselben durch Multiplication zu dem-

[1]) Die einleitenden Worte im Bericht über die Sitzung lauten: „Hr. Lejeune Dirichlet machte einige Mittheilungen über eine von ihm ausgeführte Untersuchung, welche die Theorie der complexen Einheiten zum Gegenstande hat und nächstens an einem andern Orte bekannt gemacht werden soll". K.

selben Zwecke verbinden kann. Für den speciellen Fall, wo $F(\omega) = \omega^2 - D$, geht unsere Gleichung in die bekannte PELLsche Gleichung über, deren sämmtliche Auflösungen aus einer Fundamentalauflösung durch Potenziren und Multipliciren mit $\pm 1$ erhalten werden. Es entsteht nun hier die Frage, ob für die allgemeine Gleichung eine ähnliche Eigenschaft stattfindet, und ob auch für diese solche Fundamentalauflösungen existiren, aus welchen durch Potenziren und Multipliciren sämmtliche Auflösungen gebildet werden können. Diese Frage findet ihre vollständige Erledigung in folgendem durch seine grosse Allgemeinheit merkwürdigen Satze:

„Bezeichnet $h$ die Gesammtanzahl der reellen und der Paare imaginärer conjugirter Wurzeln der Gleichung (1), so giebt es immer $h-1$ Fundamentalauflösungen von solcher Beschaffenheit, dass, wenn man dieselben potenzirt und in einander multiplicirt und dem so gebildeten allgemeinen Product der Reihe nach jede der vorher erwähnten besonderen Auflösungen als Factor zugesellt, alle Auflösungen von (2) und zwar jede nur einmal dargestellt werden."

Für die nächsten Grade nach dem zweiten liess sich dieser Satz ohne erhebliche Schwierigkeiten beweisen, und wir haben das auf den dritten Grad bezügliche Resultat in einer früheren Note*) schon vor mehreren Jahren ausgesprochen. Dem Beweise des Satzes in seiner ganzen Allgemeinheit, wie er sich auf dem Wege der Induction bald herausstellte, traten jedoch die grössten Schwierigkeiten entgegen, die erst nach vielen fruchtlosen Versuchen vollständig überwunden werden konnten. Fortgesetzte Beschäftigung mit diesem Gegenstande hat dann endlich den Beweis in solchem Grade vereinfacht, dass wir die Hauptmomente desselben mit wenigen Worten auf eine verständliche Weise zu bezeichnen im Stande sind.

Als der eigentliche Nerv dieses Beweises ist die Auffindung von $h-1$ von einander unabhängigen Auflösungen zu betrachten, unter welcher Benennung wir solche verstehen, die, zu beliebigen Potenzen erhoben und in einander multiplicirt, nie die evidente Auflösung $t = 1,\ u = 0,\ \ldots,\ z = 0$ ergeben, ausser wenn sämmtliche Potenzexponenten der Null gleich genommen werden. Sind nämlich $h-1$ solche Auflösungen bekannt, so lässt sich vermittelst der in der vorher angeführten Note entwickelten Methode die Gleichung:

$$\varphi(\alpha)\varphi(\beta)\cdots\varphi(\varrho) = r,$$

*) Monatsbericht für October 1841.[1])

[1]) S. 625 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.



in welcher $r$ eine gegebene ganze Zahl bezeichnet, immer vollständig auflösen oder doch zeigen, dass diese Gleichung keiner Auflösung fähig ist. Auf den besonderen Fall angewandt, wo $r = 1$, giebt dieses Verfahren die vollständige Auflösung der Gleichung (2) und nach einigen Umformungen des Resultats gerade in der Form, wie sie unser Satz ausspricht.

Was nun den Nachweis betrifft, dass immer $h-1$ von einander unabhängige Auflösungen existiren, so wird das dazu erforderliche Princip durch gewisse allgemeine Sätze an die Hand gegeben, die eine merkwürdige Verallgemeinerung der Eigenschaften der Kettenbrüche darbieten und der Akademie schon vor vier Jahren mitgetheilt worden sind*). Mit Hülfe dieser Sätze kann man immer eine Auflösung der Gleichung (2) finden, für welche der Zahlenwerth jedes der Ausdrücke $\varphi(\alpha), \varphi(\beta), \ldots, \varphi(\varrho)$, die reellen Wurzeln entsprechen, so wie jedes Product von je zweien, zu conjugirten imaginären Wurzeln gehörenden nach Belieben unter oder über der Einheit liegt, wenn man nur die zwei offenbar unmöglichen Combinationen ausschliesst, wo alle zugleich grösser oder alle zugleich kleiner als die Einheit sein sollen. Ist dieser Punkt erst erledigt, so lässt sich das über die unabhängigen Auflösungen Behauptete wie folgt zeigen.

Bezeichnet man für eine gegebene Auflösung mit:

$$a,\ b,\ \ldots,\ k$$

diejenigen der Ausdrücke $\varphi(\alpha), \varphi(\beta), \ldots, \varphi(\varrho)$, welche reell sind, so wie die Producte von je zwei zusammengehörigen imaginären, so hat man:

$$ab \cdots k = 1.$$

Sollen nun z. B. drei Auflösungen, für die wir $a, b, \ldots, k$ mit den Indices 1, 2, 3 versehen wollen, unabhängig von einander sein, so muss die Gleichung:

$$a_1^{m_1} a_2^{m_2} a_3^{m_3} = 1$$

nicht anders bestehen können, als wenn die ganzen Zahlen $m_1$, $m_2$, $m_3$ gleichzeitig verschwinden. Berücksichtigt man, dass diese Gleichung, wenn sie stattfindet, nicht aufhören wird, richtig zu sein, wenn man $a$ in $b$ oder $c$ verwandelt, und bezeichnet mit den grossen Buchstaben die Logarithmen der Zahlenwerthe der durch die entsprechenden kleinen ausgedrückten Grössen, so sieht man, dass die Bedingung für die Unabhängigkeit der drei Auflösungen darin besteht, dass die drei linearen Gleichungen:

*) Monatsbericht für April 1842.[1])

[1]) S. 633 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

$$A_1m_1+A_2m_2+A_3m_3=0,\quad B_1m_1+B_2m_2+B_3m_3=0,\quad C_1m_1+C_2m_2+C_3m_3=0$$

keine andere Auflösung in ganzen Zahlen zulassen dürfen als:

$$m_1=0,\quad m_2=0,\quad m_3=0.$$

Diese Bedingung wird aber offenbar erfüllt sein, wenn die sogenannte Determinante aus den neun Coefficienten oder nach der üblichen Bezeichnung der Ausdruck:

$$\Sigma\pm A_1B_2C_3$$

von Null verschieden ist, da alsdann die Gleichungen nur auf die angegebene Weise erfüllt werden können, selbst wenn man davon abstrahirt, dass $m_1$, $m_2$, $m_3$ ganz sein sollen.

Durch dieses Resultat, in Verbindung mit dem vorher erwähnten, ist nun ein Mittel gegeben, die Anzahl der unabhängigen Auflösungen allmählich zu vergrössern, bis sie gleich $h-1$ geworden ist. Um z. B. zu drei bekannten, für welche $\Sigma\pm A_1B_2C_3$ von Null verschieden ist, eine vierte hinzuzufügen, hat man nur $A_4$, $B_4$, $C_4$, $D_4$ so einzurichten, dass $\Sigma\pm A_1B_2C_3D_4$ ebenfalls nicht verschwinde. Nun ist aber bekanntlich:

$$\Sigma\pm A_1B_2C_3D_4 = D_4\Sigma\pm A_1B_2C_3+C_4F+B_4G+A_4H,$$

wo $F$, $G$, $H$ nichts die nun hinzukommende Auflösung Betreffendes enthalten. Giebt man jetzt $D_4$ dasselbe Zeichen, welches $\Sigma\pm A_1B_2C_3$ hat, und $C_4$, $B_4$, $A_4$ resp. die Zeichen von $F$, $G$, $H$, falls sie nicht verschwinden, so ist die zweite Seite und also auch die erste positiv, d. h. die neu hinzugekommene Auflösung bildet mit den drei schon vorhandenen ein System unabhängiger Auflösungen.

Wir bemerken zum Schlusse noch, dass die Untersuchungen, über welche wir so eben einige Andeutungen gegeben haben, mittelst derselben Principien einer viel grösseren Ausdehnung fähig sind, als denselben hier gegeben worden ist. Man kann, statt wie es hier geschehen ist, nur *eine* Gleichung zu Grunde zu legen, mehrere Gleichungen betrachten, und die Factoren der zu bildenden Function aus den einzelnen Combinationen der Wurzeln dieser Gleichungen zusammensetzen, so wie man auch andererseits statt der ganzen Zahlen, welche als Coefficienten oder als Variabeln der homogenen Function vorkommen, complexe Zahlen einer beliebigen Form einführen kann. Auf alle diese Erweiterungen bleiben dieselben Principien anwendbar, was das günstigste Zeugniss dafür ablegt, dass diese Principien dem wahren Wesen des Gegenstandes entnommen sind.