3.
Über eine Eigenschaft der quadratischen Formen von positiver Determinante.

(Von Herrn *G. Lejeune-Dirichlet.*)

(Vorgetragen in der Sitzung der physikalisch-mathematischen Klasse der Berliner Akademie am 16. Juli 1855.) *)

Da der neue Satz, welcher den Gegenstand dieser Vorlesung bildet, innig mit der Theorie der Gleichung

$$(1.)\qquad t^2-Du^2 = 1$$

zusammenhängt, so sind zunächst einige Bemerkungen über diese Gleichung zu machen, worin die gegebene positive ganze Zahl D keinem Quadrate gleich sein soll und von welcher hier nur die in positiven ganzen Zahlen t, u ausgedrückten Auflösungen zu berücksichtigen sind.

Sind T, U die kleinsten der Gleichung genügenden Werthe, so werden bekanntlich sämmtliche Auflösungen von der eben erwähnten Beschaffenheit durch die Formel

$$(T+U\sqrt{D})^n = t_n+u_n\sqrt{D}$$

erhalten, wenn man der ganzen Zahl n alle positiven Werthe beilegt. Unter diesen Auflösungen giebt es unendlich viele, in denen u_n durch eine beliebige (positive) Zahl S theilbar ist, und die Exponenten n, für die dieser Umstand statt findet, sind die aufeinander folgenden Vielfachen des kleinsten N derselben. Setzt man nämlich $D' = DS^2$, und bildet die neue Gleichung

$$t'^2-D'u'^2 = 1,$$

so erhellt, dafs jede Auflösung dieser letzteren, wenn $t=t'$, $u=Su'$ gesetzt wird, eine Auflösung von (1.) ergiebt, in welcher u durch S aufgeht, und umgekehrt, woraus das Behauptete und überdies folgt, dafs N durch die Gleichung

$$(T+U\sqrt{D})^N = T'+U'\sqrt{D'}$$

bestimmt wird, worin T', U' die kleinsten Werthe von t', u' bedeuten.

---

*) Es ist hier von den Zusätzen Gebrauch gemacht worden, welche der geehrte Herr Verfasser der von ihm in den Monatsberichten der Berliner Akademie (Juli 1855) eingerückten Notiz bei einer späteren Veröffentlichung derselben im *Liouville*schen Journal (Februar 1856) hinzugefügt hat.

Man kann, ohne T', U' zu kennen, den Exponenten N angeben, sobald für jeden der verschiedenen in S enthaltenen Primfactoren p der kleinste Werth ν, für den u_ν durch p aufgeht, und zugleich der Exponent δ der höchsten Potenz von p bekannt ist, durch welche u_ν theilbar ist. Es wird nämlich, wenn e eine beliebige durch p^ε (wo ε auch Null sein kann) und keine höhere Potenz von p theilbare Zahl bedeutet, unter der vorhin gemachten Voraussetzung $p^{\delta+\varepsilon}$ die höchste in $u_{\nu e}$ aufgehende Potenz von p.

Um dies zu beweisen, bezeichne man mit θ und η zwei ganze Zahlen, welche der Gleichung (1.) genügen, und überdies mit p^k (wo k von Null verschieden) die höchste in η enthaltene Potenz von p. Wenn man aus dieser Lösung durch die Formel

$$(\theta+\eta\sqrt{D})^m = t+u\sqrt{D}$$

eine neue herleitet, so hat man

$$u = \eta\left\{m\theta^{m-1}+\frac{m(m-1)(m-2)}{1.2.3}\theta^{m-3}\eta^2 D+\cdots\right\},$$

und, da θ nicht durch p theilbar ist, so erhellt, dafs die höchste in u aufgehende Potenz von p die $k$te sein wird, wenn m nicht durch p theilbar ist, dagegen die $k+1$ste, wenn $m=p$. Da nun die Erhebung zu irgend einer Potenz sich aus den beiden angeführten speciellen Fällen zusammensetzen läfst, so ergiebt sich hieraus das oben ausgesprochene Resultat.

Nach dem eben Bewiesenen besteht die nothwendige und hinreichende Bedingung dafür, dafs $u_{\nu e}$ durch p^α, wo α positiv, theilbar sei, darin, dafs e den Factor $p^{\alpha-\delta}$ haben mufs, wo der Exponent $\alpha-\delta$, wenn er negativ wird, durch Null zu ersetzen ist.

Unterscheidet man nun die verschiedenen in S enthaltenen Primfactoren p so wie die ihnen entsprechenden Werthe ν, δ durch Indices, und setzt

$$S = p_1^{\alpha_1} p_2^{\alpha_2} \ldots,$$

so ist nach dem Gesagten N das kleinste gemeinschaftliche Vielfache der Zahlen

$$\nu_1 p_1^{\alpha_1-\delta_1}, \quad \nu_2 p_2^{\alpha_2-\delta_2}, \quad \ldots$$

und man sieht sogleich, dafs wenn man ohne neue Primzahlen in S aufzunehmen, sämmtliche Exponenten α_1, α_2, ... über jede Grenze hinaus wachsen läfst, der Quotient $\frac{S}{N}$ bald einen festen von α_1, α_2, ... nicht mehr abhängigen Werth erreichen wird.

Aus der eben bewiesenen Eigenschaft ergiebt sich eine interessante Folgerung für die Theorie der quadratischen Formen von positiver Determinante. Fügt man zu den schon gemachten Voraussetzungen noch die hinzu, dafs D keinen quadratischen Faktor enthält, bezeichnet mit h die Anzahl der Klassen, in welche die zur Determinante D gehörigen Formen zerfallen, und nimmt h' in ähnlicher Bedeutung für die Determinante $D' = DS^2$, so hat man, wie in einer früheren Abhandlung (Rech. sur div. applic. sec. part.) bewiesen worden ist, die Gleichung

$$h' = h \frac{\log(T + U\sqrt{D})}{\log(T' + U'\sqrt{D'})} SR,$$

wo hinsichtlich des Factors R zu bemerken ist, dafs derselbe von den Primzahlen p_1, p_2, ..., nicht aber von den Exponenten α_1, α_2, ..., abhängt. Da man dieser Gleichung auch die Form

$$h' = h \frac{S}{N} R$$

geben kann, so folgt, dafs aus jeder positiven Determinante D unendlich viele andere DS^2 abgeleitet werden können, welchen allen dieselbe Klassenanzahl entspricht. Durch schickliche Wahl von D und den Primzahlen p_1, p_2, ... läfst sich bewirken, und zwar auf unendlich viele verschiedene Arten, dafs diese unveränderliche Anzahl der Klassen mit der der genera übereinstimmt, und so die Richtigkeit der von *Gaufs* ausgesprochenen Vermuthung beweisen, dafs die Reihe der positiven Determinanten, welche in jedem genus nur eine Klasse besitzen, nicht abbricht, was um so merkwürdiger ist, als die mit derselben Eigenschaft begabten negativen Determinanten nur in endlicher Anzahl zu sein scheinen (Disq. arith. art. 303 und 304). Nach einer sehr weit getriebenen Induction (sie erstreckt sich, wenn ich nicht irre, bis 10000), welche zuerst von *Euler* und später von *Gaufs* angestellt wurde, deren ersterer zu einer Zeit, wo die von *Lagrange* gegründete Theorie der quadratischen Formen noch nicht bestand, sich mit diesen Zahlen unter dem Namen der *numeri idonei* beschäftigte, d. h. der zur Auffindung grofser Primzahlen geeigneten Zahlen, würde die Anzahl der in Rede stehenden negativen Determinanten nicht mehr als 65 betragen, und die gröfste derselben würde, abgesehen vom Vorzeichen, den Werth 1848 haben.
