Zur Theorie der positiven quadratischen Formen *).

(Von Herrn *Hermann Minkowski* in Bonn.)

Eine wesentlich positive quadratische Form von n Variabeln, mit reellen Coefficienten und nichtverschwindender Determinante, kann — wie eine Darstellung der Form als Summe der Quadrate von n unabhängigen reellen linearen Formen leicht erkennen lässt — nur bei einer endlichen Anzahl ganzzahliger linearer Transformationen ungeändert bleiben. Jede einzelne von diesen Transformationen muss daher eine endliche Ordnung besitzen, d. h. nach einer endlichen Reihe von Wiederholungen zur identischen Transformation führen, und kann deshalb, nach § 1 meines Aufsatzes *Ueber den arithmetischen Begriff der Aequivalenz*, niemals der identischen Transformation modulo 4 congruent sein, wenn sie nicht mit derselben übereinstimmt.

Das Gleiche gilt nun in Bezug auf eine jede ungerade Primzahl als Modul; und aus diesem Umstande ergeben sich einige Aufschlüsse über die gesammte Anzahl der in Rede stehenden Transformationen, eine Anzahl, von welcher zuerst Herr *Camille Jordan* bewiesen hat, dass sie eine nur von der Zahl n abhängende Grenze nicht überschreiten kann **).

§ 1.

Eine lineare Transformation

$$(A.) \qquad x_h = a_{h1}y_1 + a_{h2}y_2 + \cdots + a_{hn}y_n \qquad (h = 1, 2, \ldots n)$$

von endlicher Ordnung ist dadurch charakterisirt, dass die mit einem Parameter r gebildete Determinante

*) Der nachfolgende Aufsatz wurde in Verbindung mit dem Aufsatze *Ueber den arithmetischen Begriff der Aequivalenz* (dieses Journal, Bd. 100, S. 449) vom Verfasser im März 1887 der philosophischen Facultät zu Bonn als Habilitationsschrift vorgelegt.

**) Journal de l'École polytechnique, cah. 48, p. 133.

$$(\Delta) \qquad |r\delta_{hk} - a_{hk}| \qquad \left(\begin{smallmatrix} h,\ k = 1, 2, \ldots n \\ \delta_{hh} = 1,\ \delta_{hk} = 0,\ h \gtrless k \end{smallmatrix}\right)$$

nur für Einheitswurzeln verschwindet, und zwar für einen mehrfachen, etwa m-fachen Nullwerth zusammen mit allen ihren $(m-1)^{\text{ten}}$ Unterdeterminanten *).

Bei ganzzahligen Coefficienten a_{hk} liefert daher eine Zerlegung in irreductible Factoren für Δ einen Ausdruck:

$$(1.) \qquad (r-1)^m f_{\nu'}(r) f_{\nu''}(r) \ldots \qquad (m \gtrless 0,\ \nu > 1),$$

wenn mit $f_\nu(r)$ für eine ganze Zahl $\nu > 1$ diejenige ganze Function $\varphi(\nu)^{\text{ten}}$ Grades bezeichnet wird, welche für die primitiven ν^{ten} Einheitswurzeln verschwindet und als Coefficient des höchsten Gliedes die Zahl 1 hat. Der Grad von (1.) ist:

$$n = m + \varphi(\nu') + \varphi(\nu'') + \cdots.$$

Soll die Transformation $(A.)$ in Bezug auf irgend eine ungerade Primzahl p der identischen Transformation congruent sein, so muss sie mit derselben zusammenfallen.

Denn ist

$$a_{hk} \equiv \delta_{hk} \pmod{p} \qquad (h, k = 1, 2, \ldots n),$$

und setzt man für r eine ganze Zahl

$$c \equiv 1 + p \pmod{p^2},$$

so geht Δ durch p^n auf. Damit aber der Ausdruck (1.) durch p^n theilbar werde, ist nothwendig, dass in Δ kein $f_\nu(r)\,(\nu > 1)$ auftrete, dass also $\Delta = (r-1)^n$ sei. Denn $(c-1)^m$ enthält zwar genau p^m, irgend ein $f_\nu(c)$ aber, wenn $\nu > 1$ ist, niemals die Potenz $p^{\varphi(\nu)}$.

Letzteres sieht man in folgender Weise ein. Ist eine Zahl ν ein Vielfaches von $p^\varkappa$, aber nicht mehr von $p^{\varkappa+1}$, so findet man:

$$c^\nu \equiv 1 + \nu p \pmod{p^{\varkappa+2}};$$

also enthält $c^\nu - 1$ dieselbe Potenz von p wie $p\nu$. Ein $f_\nu(r)$ hat den Ausdruck:

$$\frac{(r^\nu - 1)(r^{\frac{\nu}{\alpha\beta}} - 1)(r^{\frac{\nu}{\alpha\gamma}} - 1)\ldots}{(r^{\frac{\nu}{\alpha}} - 1)(r^{\frac{\nu}{\beta}} - 1)(r^{\frac{\nu}{\gamma}} - 1)\ldots},$$

wenn $\alpha, \beta, \gamma, \ldots$ die verschiedenen Primzahlen aus ν sind; also geht in $f_\nu(c)$ dieselbe Potenz von p auf wie in

$$\frac{p\nu \cdot p^{\frac{\nu}{\alpha\beta}} \cdot p^{\frac{\nu}{\alpha\gamma}} \cdots}{p^{\frac{\nu}{\alpha}} \cdot p^{\frac{\nu}{\beta}} \cdot p^{\frac{\nu}{\gamma}} \cdots}.$$

*) *Hermite,* dieses Journal, Bd. 47, S. 312; *C. Jordan,* dieses Journal, Bd. 84. S. 112.

Diese Zahl ist 1, wenn ν sich aus mehreren ungleichen Primzahlen zusammensetzt, dagegen, wenn ν Potenz einer einzigen Primzahl ist, gleich dieser Primzahl. Die höchste in $f_\nu(c)$ enthaltene Potenz von p ist demnach p^1 oder p^0, je nachdem ν eine Potenz von p ist oder nicht. Im ersteren Falle ist aber, $\nu > 1$ vorausgesetzt, $\varphi(\nu)$ mindestens gleich $p-1 \geqq 2$, im letzteren mindestens gleich 1.

Hat man nun $\Delta = (r-1)^n$, so müssen, damit $(A.)$ eine endliche Ordnung besitze, auch alle $(n-1)^{\text{ten}}$ Unterdeterminanten, also die Coefficienten von Δ für $r = 1$ verschwinden, d. h. $(A.)$ ist die identische Transformation.

§ 2.

Es bezeichne f irgend eine positive quadratische Form mit n Variabeln, reellen Coefficienten und nichtverschwindender Determinante, und es sei $t(f)$ die Anzahl der verschiedenen ganzzahligen Transformationen, durch welche diese Form in sich selbst übergeht.

Sollten in f die Coefficienten nicht sämmtlich in rationalen Verhältnissen zu einander stehen, so kann man immer leicht eine beliebig wenig von f verschiedene positive Form herstellen, in welcher solches der Fall ist, und welche dabei genau dieselben ganzzahligen Transformationen in sich zulässt wie f. Letzteres thun ferner alle Formen, welche in den Verhältnissen ihrer Coefficienten mit f ganz übereinstimmen. Im Folgenden können wir deshalb voraussetzen, die Coefficienten von f seien ganze Zahlen ohne gemeinsamen Theiler.

Die $t(f)$ Transformationen bilden eine Gruppe, und an anderer Stelle werde ich nachweisen, dass man, ausgehend von positiven quadratischen Formen, wenn auch nicht zu allen möglichen endlichen Gruppen ganzzahliger linearer Transformationen, so doch im Besondern zu allen denjenigen gelangen kann, welche nicht in umfassenderen Gruppen als Untergruppen enthalten sind.

Die in Rede stehende Gruppe ist *einstufig isomorph* zur Gruppe der Reste ihrer Transformationen in Bezug auf irgend eine ungerade Primzahl p. Denn lieferten zwei ihrer Transformationen, etwa A und B, gleiche Reste modulo p, so würde die Transformation $A^{-1}.B$, welche, als Angehörige der Gruppe, ebenfalls von endlicher Ordnung wäre, der identischen Transformation modulo p congruent, aber von ihr verschieden sein, was nach § 1 nicht angeht.

Die Gruppe der $t(f)$ Transformationenreste ist offenbar eine Untergruppe der Gruppe sämmtlicher incongruenter Transformationenreste modulo p von einer Determinante $\equiv \pm 1 (\mathrm{mod.}\, p)$, und ihre Ordnung, die Zahl $t(f)$, daher ein Divisor der Ordnung der letzteren Gruppe, d. i. der Zahl

$$(1.) \qquad 2(p^n-1)p^{n-1}(p^{n-1}-1)p^{n-2}\ldots(p^2-1)p \text{ *).}$$

Jene Gruppe ist aber ebenso schon eine Untergruppe der Gruppe aller derjenigen Transformationenreste modulo p, welche die Form f modulo p ungeändert lassen. Die Ordnung dieser Gruppe hat für alle ungeraden Primzahlen p, welche nicht in der Determinante D der Form f aufgehen, also jedenfalls für *sämmtliche* Primzahlen über einer gewissen Grenze l, den folgenden Ausdruck **), wenn n gerade ist:

$$(2.) \qquad p^{\frac{1}{4}n(n-2)}.2(p^2-1)(p^4-1)\ldots(p^{n-2}-1)(p^{\frac{n}{2}}-\varepsilon),$$

wo $\varepsilon = \left(\frac{(-1)^{\frac{n}{2}}D}{p}\right)$ eine Einheit bedeutet; wenn n ungerade ist:

$$(3.) \qquad p^{\frac{1}{4}(n-1)^2}.2(p^2-1)(p^4-1)\ldots(p^{n-1}-1).$$

Als Divisor *sämmtlicher* Zahlen (2.) oder (3.) für ungerade Primzahlen $p > l$, ist die Zahl $t(f)$ auch ein Divisor des *grössten gemeinschaftlichen Divisors* aller dieser Zahlen.

Um ein Resultat zu erhalten, das von der speciellen Form f unabhängig ist, denken wir uns in (2.) den Factor $p^{\frac{n}{2}}-\varepsilon$ durch sein Vielfaches $\frac{1}{2}(p^n-1)$ ersetzt; ferner möge l mindestens gleich $n+1$ sein. Dann ist jener grösste gemeinsame Divisor dargestellt durch:

$$\overline{n}| \;=\; \prod_q q^{\left[\frac{n}{q-1}\right]+\left[\frac{n}{q(q-1)}\right]+\left[\frac{n}{q^2(q-1)}\right]+\cdots} \qquad (q=2,\ 3,\ 5,\ 7,\ 11,\ \ldots),$$

wenn unter der Bezeichnung $[a]$ die grösste in a enthaltene ganze Zahl verstanden wird, und wenn q die Reihe der Primzahlen soweit durchläuft, bis das Product von selbst abbricht, d. i. bis zur grössten Primzahl, welche noch $\leqq n+1$ ist.

Man hat, um dieses einzusehen, für eine jede Primzahl q eine Zahl (2.) bez. (3.) aufzusuchen, welche eine möglichst niedrige Potenz von q enthält. Man gelangt zu einer solchen, indem man die Primzahl p in folgender

*) *Galois,* Journal de *Liouville,* t. XI, 1846, p. 410.

**) Vgl. *Untersuchungen über quadratische Formen,* Acta Mathematica, Bd. 7, S. 218.

Weise wählt: wenn $q > n+1$ ist, als primitive Wurzel in Bezug auf q; wenn $q \leqq n+1$ und ungerade ist, als primitive Wurzel für den Modul q^2; wenn $q = 2$ ist, als Zahl der Form $\equiv \mp 1+4 \pmod 8$. Die Existenz von Primzahlen p dieser Formen über der Grenze l ist eine Folge des bekannten Theorems über die arithmetischen Progressionen.

Im ersten der drei unterschiedenen Fälle ist dann die in Betracht kommende Zahl (2.) oder (3.) durch q überhaupt nicht theilbar; im zweiten geht q in $p^\nu - 1$ nur auf, wenn ν ein Vielfaches von $q-1$ ist, und zwar dann in derselben Potenz wie in $q.\frac{\nu}{q-1}$, mithin in der Zahl (2.) bez. (3.) in derselben Potenz wie in $q^{\left[\frac{n}{q-1}\right]}.1.2...\left[\frac{n}{q-1}\right]$; im dritten enthält $p^{2\nu}-1$ dieselbe Potenz von 2 wie 8ν, also die Zahl (2.) bez. (3.) dieselbe wie $2^{n+\left[\frac{n}{2}\right]}.1.2...\left[\frac{n}{2}\right]$.

Die Identität der hier auftretenden Primzahlpotenzen mit denjenigen aus $\overline{n}|$ ergiebt sich durch Anwendung der bekannten Relation:

$$1.2...n = n! = \prod_q q^{\left[\frac{n}{q}\right]+\left[\frac{n}{q^2}\right]+\left[\frac{n}{q^3}\right]+\cdots} \qquad (q = 2, 3, 5, 7, \ldots),$$

und man erhält damit in der That den Satz:

Die Anzahl der ganzzahligen Transformationen einer positiven quadratischen Form mit n Variabeln (und von nichtverschwindender Determinante) in sich selbst ist ein Divisor der Zahl $\overline{n}|$.

Als grösster gemeinsamer Divisor aller Zahlen (1.) würde sich $2^{\left[\frac{n}{2}\right]}.\overline{n}|$ ergeben haben.

Die Zahl $\overline{n}|$ selbst ist ein Divisor von $(2n)!$; denn in ihrem Ausdrucke verkleinert man keinen der Exponenten, wenn man in denselben anstatt $q-1$ überall $\frac{1}{2}q$ schreibt.

Als specielle Fälle seien die folgenden erwähnt: die Form

$$\mathfrak{D}_n = x_1^2+x_2^2+\cdots+x_n^2$$

geht durch $2^n.n!$, die Form

$$\mathfrak{D}_n = (\Sigma x_h)^2+\Sigma x_h^2 \text{ *)} \qquad (h = 1, 2, \ldots n)$$

von der Determinante $n+1$ durch $2.(n+1)!$ ganzzahlige Transformationen in sich selbst über.

*) Die Form $\mathfrak{D}_n$ ist von den Herren *Korkine* und *Zolotareff* eingehender untersucht worden, vgl. Mathematische Annalen, Bd. 6 und Bd. 11.

Die Zahl $\overline{n}|$ ist ferner das *kleinste* gemeinsame Vielfache aller möglichen Anzahlen $t(f)$.

Denn zunächst enthält die der Form $\mathfrak{Q}_n$ angehörige Zahl $t(\mathfrak{Q}_n)$ dieselbe Potenz von 2 wie $\overline{n}|$. Ist ferner q eine der ungeraden Primzahlen $\leqq n+1$, und bildet man eine Form f als Summe von $\left[\frac{n}{q-1}\right]$ Formen $\mathfrak{D}_{q-1}$ und der Form $\mathfrak{Q}_{\left(n-(q-1)\left[\frac{n}{q-1}\right]\right)} = \mathfrak{Q}$ mit fortlaufend nummerirten Variabeln, so ist für diese Form f die Zahl

$$t(f) = (2.q!)^{\left[\frac{n}{q-1}\right]}.\left[\frac{n}{q-1}\right]!\,t(\mathfrak{Q})$$

durch dieselbe Potenz von q theilbar wie $\overline{n}|$.

Man hat im Einzelnen $\overline{2}| = 24$, $\overline{3}| = 48$, $\overline{4}| = 5760$, etc. und allgemein:

$$\overline{2n+1}| = 2.\overline{2n}|, \quad \overline{2n}| = 2b_n.\overline{2n-1}|, \quad \overline{n}| = 2^n.b_1b_2\ldots b_{\left[\frac{n}{2}\right]},$$

wenn unter b_n eine Zahl verstanden wird, welche alle und nur solche Primzahlen q enthält, für welche $2n$ durch $q-1$ aufgeht, und jede derselben in einer Potenz $q^{\varkappa+1}$, falls sie in n in der Potenz $q^{\varkappa}(\varkappa \geqq 0)$ auftritt.

Bedeutet B_n die n^{te} *Bernoulli*sche Zahl, so stellt b_n den Nenner von $\frac{1}{n}B_n$ vor *).

Die Bestimmung der ganzzahligen Transformationen einer positiven Form $f = \sum_1^n a_{hk}x_hx_k$ in sich selbst geschieht durch Vermittelung der äquivalenten reducirten Formen.

Nach der Definition von Herrn *Hermite* **) gelten in einer positiven Klasse f diejenigen Formen als *reducirt,* welche das kleinste System

$$a_{11}, \quad a_{22}, \quad \ldots \quad a_{nn}$$

(d. i. kurz ausgedrückt den kleinsten Werth von

$$a_{11}g^{n-1}+a_{22}g^{n-2}+\cdots+a_{nn}$$

bei hinreichend grossem positivem g) ergeben.

Den Sätzen, welche ich dieses Journal, Bd. 99 mitgetheilt habe, schliessen sich die folgenden für den Fall von sechs Variabeln an.

---

*) Vgl. *Lipschitz,* dieses Journal, Bd. 96, S. 4.

**) Dieses Journal, Bd. 40, S. 302.

Eine Form f mit sechs Variabeln ist immer und nur dann positiv und reducirt, wenn sie allen Ungleichungen

$$f(m_1, m_2, \ldots m_6) \geqq a_{hh} \qquad (h = 1, 2, \ldots 6)$$

genügt, für welche die Zahlen m in folgender Tabelle enthalten sind:

m_h	$\pm m_{h'}$	$\pm m_{h''}$	$\pm m_{h'''}$	$\pm m_{h\text{IV}}$	$\pm m_{h\text{V}}$
1	1				
1	1	1			
1	1	1	1		
1	1	1	1	1	
1	1	1	1	2	
1	1	1	1	1	1
1	1	1	1	1	2
1	1	1	1	2	2
1	1	1	1	2	3

(die nicht aufgeführten Grössen m sind gleich Null zu setzen), und ferner den Ungleichungen:

$$a_{11} \leqq a_{22} \leqq \cdots \leqq a_{66}.$$

Nur für die reducirten und die aus denselben durch Permutation der Variabeln hervorgehenden Formen nehmen die Verbindungen

$$a_{11}+a_{22}+\cdots+a_{66}, \quad \ldots, \quad a_{11}a_{22}\ldots a_{66}$$

ihre kleinsten Werthe an.

Die *Hermite*schen reducirten Formen mit sieben Variabeln lassen sich nicht mehr durch eine Reihe einzelner linearer Ungleichungen vollständig charakterisiren.

Berlin, den 15. Februar 1887.

Berichtigung.

Dieses Journal Bd. C, S. 451, Z. 1 v. u. ist zu lesen:

$$\varepsilon s_k = \Sigma_h a_{hk} s_h \qquad (h, k = \nu, \ldots n),$$

und in den darauf folgenden Zeilen ist S durch diejenige Substitution zu ersetzen, welche aus S^{-1} durch Vertauschung der Horizontal- mit den Verticalreihen hervorgeht.
