# BIBLIOGRAPHIC RECORD TARGET



**Storage Number:** _____

AAT3434
UL FMT B RT a BL m T/C DT 07/15/88 R/DT 08/01/90 CC STAT mm E/L 1
010: : |a 11005950
035/1: : |a (RLIN)MIUG84-B57996
035/2: : |a (CaOTULAS)160191853
040: : |c MiU |d MiU
050/1:0 : |a QA3 |b .M6
100:1 : |a Minkowski, H. |q (Hermann), |d 1864-1909.
245:00: |a Gesammelte abhandlungen von Hermann Minkowski, |c unter mitwirkung von Andreas Speiser und Hermann Weyl hrsg. von David Hilbert.
260: : |a Leipzig, |a Berlin, |b B. G. Teubner, |c 1911.
300/1: : |a 2 v. |b fronts. (ports.) diagrs. (1 fold.) |c 27 cm.
500/1: : |a "Hermann Minkowski. Gedächtnisrede, gehalten in der öffentlichen sitzung der K. Gesellschaft der wissenschaften zu Göttingen am 1. mai, 1909, von David Hilbert": v. 1, p. [v]-xxxi.
650/1: 0: |a Mathematics.
650/2: 0: |a Geometry.

Verlag B. G. Teubner, Leipzig. Blechinger & Leykauf, Wien, hof. & ep.

H. Minkowski

# GESAMMELTE ABHANDLUNGEN

VON

# HERMANN MINKOWSKI

UNTER MITWIRKUNG VON

**ANDREAS SPEISER** UND **HERMANN WEYL**

HERAUSGEGEBEN VON

**DAVID HILBERT**

ERSTER BAND

MIT EINEM BILDNIS HERMANN MINKOWSKIS
UND 6 FIGUREN IM TEXT

LEIPZIG UND BERLIN
DRUCK UND VERLAG VON B. G. TEUBNER
1911

# INHALT DES ERSTEN BANDES.

Seite

Gedächtnisrede auf H. Minkowski, von D. Hilbert . . . . . V

**Zur Theorie der quadratischen Formen.**

I. Grundlagen für eine Theorie der quadratischen Formen mit ganzzahligen Koeffizienten. . . . . 3
(In französischer Sprache unter dem Titel: Mémoire sur la théorie des formes quadratiques, in den Mémoires présentés par divers savants à l'Académie des Sciences de l'Institut national de France, Tome XXIX, No. 2; 1884.)

II. Sur la réduction des formes quadratiques positives quaternaires 145
(Comptes rendus de l'Académie des Sciences, Paris, t. 96, pp. 1205—1210; 1883.)

III. Über positive quadratische Formen . . . . . 149
(Crelles Journal für die reine und angewandte Mathematik, Bd. 99, S. 1—9; 1886.)

IV. Untersuchungen über quadratische Formen. Bestimmung der Anzahl verschiedener Formen, welche ein gegebenes Genus enthält . . . . . 157
(Inauguraldissertation, Königsberg 1885; Acta Mathematica, Bd. 7, S. 201—258; 1885.)

V. Über den arithmetischen Begriff der Äquivalenz und über die endlichen Gruppen linearer ganzzahliger Substitutionen. . . . 203
(Crelles Journal für die reine und angewandte Mathematik, Bd. 100, S. 449—458; 1887.)

VI. Zur Theorie der positiven quadratischen Formen . . . . . 212
(Crelles Journal für die reine und angewandte Mathematik, Bd. 101, S. 196—202; 1887.)

VII. Über die Bedingungen, unter welchen zwei quadratische Formen mit rationalen Koeffizienten ineinander rational transformiert werden können (Auszug aus einem von Herrn H. Minkowski in Bonn an Herrn Adolf Hurwitz gerichteten Brief). . . . . 219
(Crelles Journal für die reine und angewandte Mathematik, Bd. 106, S. 5—26; 1890.)

**Zur Geometrie der Zahlen.**

VIII. Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen. . . . . 243
(Crelles Journal für die reine und angewandte Mathematik, Bd. 107, S. 278—297; 1891.)

Seite

IX. Théorèmes arithmétiques (Extrait d'une lettre de M. H. Minkowski à M. Hermite) . . . . . 261
(Comptes rendus de l'Académie des Sciences, Paris, t. 112, pp. 209—212; 1891.)

X. Über Geometrie der Zahlen (Bericht über einen Vortrag zu Halle) . 264
(Verhandlungen der 64. Naturforscher- und Ärzteversammlung zu Halle, 1891, S. 13, und Jahresbericht der Deutschen Mathematiker-Vereinigung, Bd. 1, S. 64—65; 1892.)

XI. Extrait d'une lettre adressée à M. Hermite. . . . . 266
(Bulletin des Sciences mathématiques, 2e série, t. XVII, pp. 24—29; 1893.)

XII. Über Eigenschaften von ganzen Zahlen, die durch räumliche Anschauung erschlossen sind . . . . . 271
(Mathematical Papers read at the international Mathematical Congress held in connection with the world's Columbian Exposition Chicago, 1893, pp. 201—207; ferner unter dem Titel: Sur les propriétés des nombres entiers qui sont dérivées de l'intuition de l'espace, von L. Laugel ins Französische übersetzt, in Nouvelles Annales de Mathématiques, 3e série, t. XV, pp. 393—403; 1896.)

XIII. Zur Theorie der Kettenbrüche . . . . . 278
(Von L. Laugel ins Französische übersetzt unter dem Titel: Généralisation de la théorie des fractions continues, in Annales de l'École Normale supérieure, 3e série, t. XIII, pp. 41—60; 1896.)

XIV. Ein Kriterium für die algebraischen Zahlen . . . . . 293
(Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen, mathematisch-physikalische Klasse, 1899, S. 64—88.)

XV. Zur Theorie der Einheiten in den algebraischen Zahlkörpern 316
(Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen, mathematisch-physikalische Klasse, 1900, S. 90—93.)

XVI. Über die Annäherung an eine reelle Größe durch rationale Zahlen . . . . . 320
(Mathematische Annalen, Bd. 54, S. 91—124; 1901.)

XVII. Quelques nouveaux théorèmes sur l'approximation des quantités à l'aide de nombres rationnels . . . . . 353
(Bulletin des Sciences mathématiques, 2e série, t. XXV, pp. 72—76; 1901.)

XVIII. Über periodische Approximationen algebraischer Zahlen. . . 357
(Acta Mathematica, Bd. 26, S. 333—351; 1902.)

# Hermann Minkowski.

Gedächtnisrede, gehalten in der öffentlichen Sitzung der K. Gesellschaft der Wissenschaften zu Göttingen am 1. Mai 1909

von

**David Hilbert.**

(Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen. 1909.)

Einen schweren unermeßlichen Verlust haben zu Beginn des Jahres 1909 unsere Gesellschaft, unsere Universität, die Wissenschaft und wir alle persönlich erlitten: durch ein hartes Geschick wurde uns jäh entrissen unser Kollege und Freund Hermann Minkowski im Vollbesitz seiner Lebenskraft, aus der Mitte freudigsten Wirkens, von der Höhe seines wissenschaftlichen Schaffens.

Seinem Andenken widmen wir diese Stunde.

Hermann Minkowski wurde am 22. Juni 1864 zu Alexoten in Rußland geboren, kam als Knabe nach Deutschland und trat Oktober 1872 im Alter von $8\frac{1}{4}$ Jahren in die Septima des Altstädtischen Gymnasiums zu Königsberg i. Pr. ein. Da er von sehr rascher Auffassung war und ein vortreffliches Gedächtnis hatte, wurde er auf mehreren Klassen in kürzerer als der vorgeschriebenen Zeit versetzt und verließ das Gymnasium schon März 1880 — noch als Fünfzehnjähriger — mit dem Zeugnis der Reife.

Ostern 1880 begann Minkowski seine Universitätsstudien. Insgesamt hat er 5 Semester in Königsberg, vornehmlich bei Weber und Voigt, und 3 Semester in Berlin studiert, wo er die Vorlesungen von Kummer, Kronecker, Weierstraß, Helmholtz und Kirchhoff hörte.

Seine Befähigung zur Mathematik zeigte sich früh; fiel ihm doch im ersten Semester bereits für die Lösung einer mathematischen Aufgabe eine Geldprämie zu, auf die er freilich zugunsten eines armen Mitschülers verzichtete, so daß sein frühzeitiger Erfolg zu Hause gar nicht bekannt wurde — eine kleine Begebenheit, die zugleich die Bescheidenheit und Herzensgüte kennzeichnet, wie er sie sein ganzes Leben hindurch allen Menschen gegenüber, die ihm näher kamen, betätigt hat.

Sehr bald begann Minkowski tiefgehende und gründliche mathematische Studien. Ostern 1881 hatte die Pariser Akademie das Problem der Zerlegung der ganzen Zahlen in eine Summe von fünf Quadraten als Preisthema gestellt. Dieses Thema griff der siebzehnjährige Student mit aller

Energie an und löste die gestellte Aufgabe aufs glänzendste, indem er weit über das Preisthema hinaus die allgemeine Theorie der quadratischen Formen, insbesondere ihre Einteilung in Ordnungen und Geschlechter — zunächst sogar für beliebigen Trägheitsindex — entwickelte*). Es ist erstaunlich, welch sichere Herrschaft Minkowski schon damals über die algebraischen Methoden, insbesondere die Elementarteilertheorie, sowie über die transzendenten Hilfsmittel wie die Dirichletschen Reihen und die Gaußschen Summen besaß, — Kenntnisse, die noch heute lange nicht allgemeines Eigentum der Mathematiker geworden sind, die aber freilich zur erfolgreichen Inangriffnahme des Pariser Preisthemas eine notwendige Voraussetzung bildeten. Hören wir, wie Minkowski selbst in dem Begleitschreiben zu seiner der Pariser Akademie eingereichten Arbeit sich ausspricht**): „Durch die von der Académie des Sciences gestellte Aufgabe angeregt", so schreibt der jugendliche Student, „unternahm ich eine genauere Untersuchung der allgemeinen quadratischen Formen mit ganzzahligen Koeffizienten. Ich ging dabei von dem natürlichen Gedanken aus, daß die Zerlegung einer Zahl in eine Summe von fünf Quadraten in ähnlicher Weise von den quadratischen Formen mit vier Variablen abhängen würde, wie bekanntlich die Zerlegung einer Zahl in eine Summe von drei Quadraten von den quadratischen Formen mit zwei Variablen abhängt. Diese Untersuchung hat mir in der Tat die gewünschten Resultate über die Zerlegung einer Zahl in eine Summe von fünf Quadraten geliefert. Indessen erscheinen diese Resultate bei der großen Allgemeinheit der von mir gefundenen Sätze nicht überall als das eigentliche Hauptziel der vorliegenden Arbeit; sie stellen vielmehr nur ein Beispiel für die gewonnenen umfangreichen Theorien dar. Wenn daher viele der nachfolgenden Betrachtungen nicht immer unmittelbar auf das Thema der Preisfrage hinweisen, so wage ich dennoch zu hoffen, daß die Akademie nicht der Ansicht sein werde, ich würde mehr gegeben haben, wenn ich weniger gegeben hätte." Mit dem Motto: „Rien n'est beau que le vrai, le vrai seul est aimable" reichte der noch nicht Achtzehnjährige am 30. Mai 1882 die Arbeit der Pariser Akademie ein. Obwohl dieselbe, entgegen den Bestimmungen der Akademie, in deutscher Sprache abgefaßt war, so erkannte die Akademie dennoch unter ausdrücklicher Betonung des exzeptionellen Falles auf Zuerteilung des vollen Preises, da — wie es im Kommissionsbericht heißt — eine Arbeit von solcher Bedeutung nicht wegen einer Irregularität der Form von der

*) „Mémoire sur la théorie des formes quadratiques à coefficients entiers." Mémoires présentés par divers savants à l'Académie des Sciences de l'Institut national de France, T. XXIX. No. 2 (1884). Unter dem Titel „Grundlagen für eine Theorie der quadratischen Formen mit ganzzahligen Koeffizienten", diese Ges. Abhandlungen, Bd. I, S. 3—144. **) Vgl. diese Ges. Abhandlungen, Bd. I, S. 4.

Bewerbung auszuschließen sei, und erteilte ihm im April 1883 den Grand Prix des Sciences Mathématiques.

Als die Zuerkennung des Akademiepreises an Minkowski in Paris bekannt wurde, richtete die dortige chauvinistische Presse gegen ihn die unbegründetsten Angriffe und Verdächtigungen. Die französischen Akademiker C. Jordan und J. Bertrand stellten sich sofort rückhaltlos auf die Seite Minkowskis. „Travaillez, je vous prie, à devenir un géomètre éminent.“ In dieser Mahnung des großen französischen Mathematikers C. Jordan an den jungen deutschen Studenten gipfelte die bei diesem Anlaß zwischen C. Jordan und Minkowski geführte Korrespondenz, — eine Mahnung, die Minkowski treulich beherzigt hat; begann doch nun für ihn eine arbeitsfrohe und publikationsreiche Zeit.

Gauß hat in seinen Disquisitiones arithmeticae die Theorie der binären quadratischen Formen mit ganzzahligen Koeffizienten und damit zugleich den wesentlichen Inhalt der heutigen Theorie der quadratischen Zahlkörper geschaffen. Nach zwei verschiedenen Richtungen hin war die Verallgemeinerung der Gaußschen Theorie möglich: einmal als Theorie der quadratischen Formen mit beliebig vielen Variablen und dann als Theorie der zerlegbaren Formen höherer Ordnung, d. h. als Theorie der Zahlkörper von beliebigem Grade. Durch das Pariser Preisthema war Minkowski zunächst auf die erstere Verallgemeinerung der Gaußschen Theorie hingewiesen: in der Tat sehen wir Minkowski in den folgenden Jahren ausschließlich seine ganze Arbeitskraft dem Studium der *Theorie der quadratischen Formen* und der aufs engste damit zusammenhängenden Fragen widmen. Die Gaußsche Theorie der quadratischen Formen hatte eine wesentliche Ergänzung durch Dirichlet erfahren, indem es diesem gelungen war, auf Grund einer ihm eigentümlichen transzendenten Methode für die Anzahl der Klassen binärer quadratischer Formen mit gegebener Determinante geschlossene Ausdrücke aufzustellen. Es lag nahe, diese Methode nach jenen beiden oben gekennzeichneten Richtungen hin zu verallgemeinern. Nach letzterer Richtung hin, nämlich für die Theorie der algebraischen Zahlkörper, war jene Verallgemeinerung der Dirichletschen Methode bereits von Kummer und in allgemeinster Weise von Dedekind vorgenommen worden; in ersterer Richtung aber, nämlich für das Problem der quadratischen Formen von beliebig vielen Variablen, lagen nur einige Vorarbeiten von St. Smith, jenem schon bejahrten englischen Zahlentheoretiker, vor, welcher auch bei der Bewerbung um den Pariser Preis Minkowskis Konkurrent gewesen war. Minkowski führte nun die Bestimmung der Anzahl der in einem Geschlecht enthaltenen Klassen quadratischer Formen von beliebig vielen Variablen — denn darauf spitzt sich das in Frage kommende Problem zu — nach der von Dirichlet für binäre

quadratische Formen angewandten transzendenten Methode durch. Die hierbei gefundenen Resultate bilden den wesentlichen Inhalt der Inaugural-Dissertation*), auf Grund deren Minkowski am 30. Juli 1885 von der philosophischen Fakultät in Königsberg zum Doktor promoviert wurde.

Wie glücklich die Ideen des jugendlichen Minkowski auch auf anderem als rein zahlentheoretischem Gebiete waren, ersehen wir aus der bei dieser Gelegenheit von ihm aufgestellten These, die so lautete: „Es ist nicht wahrscheinlich, daß eine jede positive Form sich als eine Summe von Formenquadraten darstellen läßt.“ Es fiel mir als Opponent die Aufgabe zu, bei der öffentlichen Promotion diese These anzugreifen. Die Disputation schloß mit meiner Erklärung, ich sei durch seine Ausführungen überzeugt, daß es wohl schon im ternären Gebiete solch merkwürdige Formen geben möchte, die so eigensinnig seien, positiv zu bleiben, ohne sich doch eine Darstellung als Summe von Formenquadraten gefallen zu lassen. Die Minkowskische These war für mich später die Veranlassung, die Untersuchung der Frage aufzunehmen und für die in der These ausgesprochene Vermutung den strengen Nachweis zu erbringen. Es stellte sich außerdem späterhin heraus, daß das Problem der Darstellung definiter Formen durch Formenquadrate auch bei der Frage nach der Möglichkeit geometrischer Konstruktionen mittels gewisser elementarer Hilfsmittel eine interessante Rolle spielt und andererseits mit gewissen tieferen Problemen über die Darstellbarkeit algebraischer Zahlen als Summen von Quadraten zusammenhängt. Auch von anderer Seite ist seitdem das Problem aufgenommen worden und hat zu interessanten speziellen Ergebnissen geführt.

Angeregt durch eine von Kronecker gestellte Forderung, die eine schärfere Fassung des arithmetischen Begriffs der Äquivalenz von Formen betraf, gelangte Minkowski zu der interessanten Frage nach dem Verhalten linearer ganzzahliger Substitutionen von beliebiger Variablenzahl im Sinne der Kongruenz nach einem beliebigen Modul**). Minkowski gewann dabei den anwendungsreichen Satz, daß eine homogene lineare ganzzahlige Substitution mit $n$ Variablen von einer endlichen Ordnung, die nach einem ganzzahligen Modul $\geqq 3$ der identischen Substitution kongruent ausfällt, selbst notwendig die identische Substitution ist. Mit Hilfe dieses Satzes

---

*) Untersuchungen über quadratische Formen. I. Bestimmung der Anzahl verschiedener Formen, welche ein gegebenes Genus enthält. Acta Mathematica, Bd. 7 (1885), S. 201—258. Diese Ges. Abhandlungen, Bd. I, S. 157—202.

**) Ueber den arithmetischen Begriff der Aequivalenz und über die endlichen Gruppen linearer ganzzahliger Substitutionen. Crelles Journal, Bd. 100 (1887), S. 449—458. Diese Ges. Abhandlungen, Bd. I, S. 203—211. Zur Theorie der positiven quadratischen Formen. Crelles Journal, Bd. 101 (1887), S. 196—202. Diese Ges. Abhandlungen, Bd. I, S. 212—218.

gelingt es Minkowski unter anderem zu zeigen, daß die Ordnung jeder endlichen Gruppe von homogenen linearen ganzzahligen Substitutionen mit $n$ Variablen stets ein Divisor der Zahl

$$2^n(2^n-1)(2^n-2)\ldots(2^n-2^{n-1})$$

ist, und desgleichen stellt er eine nur von $n$ abhängige Zahl auf, in welcher notwendig allemal die Anzahl der ganzzahligen Substitutionen aufgehen muß, die eine definite quadratische Form mit $n$ Variablen in sich selbst überführen. Die beiden Abhandlungen, welche diese Resultate entwickeln, reichte er der philosophischen Fakultät in Bonn als Habilitationsschrift ein; April 1887 erteilte ihm diese die venia legendi für Mathematik.

Noch eine Arbeit Minkowskis sei hier genannt, die ich der Jugendepoche seines mathematischen Schaffens zuzähle, da sie ebenfalls ausschließlich das Gebiet der quadratischen Formen betrifft; es ist diejenige*), in welcher Minkowski die Bedingungen dafür aufstellt, daß eine quadratische Form mit rationalen Zahlenkoeffizienten sich vermöge einer linearen Substitution mit rationalen Zahlenkoeffizienten in eine andere ebensolche quadratische Form oder in ein rationales Vielfaches einer solchen Form transformieren läßt. Als äußerer Anlaß dazu diente ihm eine von Hurwitz und mir gemeinsam verfaßte Arbeit über ternäre diophantische Gleichungen vom Geschlechte Null. Die Untersuchung von Hurwitz und mir hatte ergeben, daß jede ternäre diophantische Gleichung vom Geschlechte Null durch eine rationale eindeutig umkehrbare Transformation in eine quadratische Gleichung übergeführt werden kann; die weiter entstehenden Fragen, insbesondere die Frage nach den Kriterien dafür, daß eine quadratische diophantische Gleichung bei beliebiger Variablenzahl durch rationale Zahlen lösbar ist, finden durch Minkowski ihre vollständige Erledigung; doch gestaltet sich noch darüber hinaus die Bearbeitung des Problems durch Minkowski zu einer vollständigen Invariantentheorie der quadratischen Formen im zahlentheoretischen Sinne.

Nunmehr beginnt für Minkowskis mathematische Produktion die reichste und bedeutendste Epoche; seine bisher auf das spezielle Gebiet der quadratischen Formen gerichteten Untersuchungen erhalten mehr und mehr den großen Zug ins Allgemeine und gipfeln schließlich in der Schaffung und dem Ausbau der Lehre, für die er selbst den treffenden Namen „*Geometrie der Zahlen*“ geprägt hat und die er in dem großartig angelegten Werke gleichen Titels dargestellt hat.

Das Problem, aus den unendlich vielen Formen einer Klasse durch

*) Ueber die Bedingungen, unter welchen zwei quadratische Formen mit rationalen Coefficienten in einander rational transformiert werden können. Crelles Journal, Bd. 106 (1890), S. 5—26. Diese Ges. Abhandlungen, Bd. I, S. 219—239.

bestimmte Ungleichheitsbedingungen eine einzige auszusondern, d. h. das Problem der Reduktion der quadratischen Formen, hatte Minkowski schon wiederholt beschäftigt. Vor allem ergriffen ihn die berühmten Briefe, die 1850 Ch. Hermite über diesen Gegenstand an Jacobi gerichtet hatte, und insbesondere der dort von Hermite aufgestellte Satz, daß die kleinste von Null verschiedene Größe, die durch eine positive quadratische Form von $n$ Variablen mit der Determinante 1 mittels ganzer Zahlen darstellbar ist, niemals einen gewissen, nur von der Zahl $n$ abhängigen Betrag übersteigt. Durch die Beschäftigung mit diesem Satze wurde Minkowski zu Betrachtungen veranlaßt, auf die wir ein wenig näher eingehen müssen.

Wir denken uns nach Minkowski dasjenige würfelförmig angeordnete, den ganzen Raum erfüllende Punktsystem, welches entsteht, wenn man den rechtwinkligen Koordinaten $x, y, z$ alle ganzzahligen Werte erteilt. Minkowski nannte ein solches Punktsystem ein Zahlengitter. Bedeutet nun $F(x, y, z)$ eine homogene positive quadratische Form von $x, y, z$ mit der Determinante 1, so stellt die Gleichung $F(x, y, z) = c$ für irgendeinen positiven Wert der Konstanten $c$ ein bestimmtes Ellipsoid mit dem Nullpunkt als Mittelpunkt dar. Wir denken uns nun um jeden Punkt des Zahlengitters als Mittelpunkt ein diesem Ellipsoid kongruentes und ähnlich gelegenes Ellipsoid konstruiert: ist dann der Wert der Konstanten $c$ genügend klein, so werden diese Ellipsoide offenbar sämtlich völlig voneinander getrennt liegen. Der größte Wert von $c$, bei welchem dies noch der Fall ist und die Ellipsoide demnach einander nur in einzelnen Punkten berühren, sei $\frac{1}{4} M$. Da bei dieser Raumerfüllung auf je einen Würfel mit der Kantenlänge 1 je eines der Ellipsoide kommt, so folgt leicht, daß der Inhalt des Ellipsoides $F(x, y, z) = \frac{1}{4} M$ notwendig kleiner als der Inhalt jenes Würfels ausfällt, d. h. es ist gewiß

$$\frac{4\pi}{3} \sqrt{\left(\frac{M}{4}\right)^3} < 1.$$

Andererseits ist leicht zu erkennen, daß das Ellipsoid $F(x, y, z) = M$ gewiß außer dem Nullpunkt keinen Punkt des Zahlengitters in seinem Innern enthält; liegen doch auf seiner Oberfläche gerade noch diejenigen Gitterpunkte, die die Mittelpunkte der das Ellipsoid $F(x, y, z) = \frac{1}{4} M$ berührenden Ellipsoide sind, d. h. $M$ ist der kleinste von Null verschiedene, durch ganze Zahlen darstellbare Wert der quadratischen Form, und jene Ungleichung liefert für dieses Minimum die obere Schranke

$$M < \sqrt[3]{\frac{6^2}{\pi^2}}.$$

Dieser Beweis eines tiefliegenden zahlentheoretischen Satzes ohne rechnerische Hilfsmittel wesentlich auf Grund einer geometrisch anschau-

lichen Betrachtung ist eine Perle Minkowskischer Erfindungskunst. Bei der Verallgemeinerung auf Formen mit $n$ Variablen führt der Minkowskische Beweis auf eine natürlichere und weit kleinere obere Schranke für jenes Minimum $M$, als sie bis dahin Hermite gefunden hatte. Noch wichtiger aber als dies war es, daß der wesentliche Gedanke des Minkowskischen Schlußverfahrens nur die Eigenschaft des Ellipsoides, daß dasselbe eine konvexe Figur ist und einen Mittelpunkt besitzt, benutzte und daher auf beliebige konvexe Figuren mit Mittelpunkt übertragen werden konnte. Dieser Umstand führte Minkowski zum ersten Male zu der Erkenntnis, daß überhaupt der *Begriff des konvexen Körpers* ein fundamentaler Begriff in unserer Wissenschaft ist und zu deren fruchtbarsten Forschungsmitteln gehört.

Ein konvexer (nirgends konkaver) Körper ist nach Minkowski als ein solcher Körper definiert, der die Eigenschaft hat, daß, wenn man zwei seiner Punkte ins Auge faßt, auch die ganze geradlinige Strecke zwischen denselben zu dem Körper gehört.

Die Bedeutung des Begriffs des konvexen Körpers für die Grundlagen der Geometrie beruht in dem engen Zusammenhange, der, wie Minkowski erkannte, zwischen diesem Begriff und dem fundamentalen Satze Euklids besteht, wonach im Dreiecke die Summe zweier Seiten stets größer als die dritte Seite ist. Dieser Satz Euklids, welcher ja lediglich von elementaren, aus den Axiomen unmittelbar entnommenen Begriffen handelt, folgt bei Euklid aus dem Axiom von der Kongruenz zweier Dreiecke. Lassen wir nun alle Axiome der gewöhnlichen Euklidischen Geometrie bestehen mit Ausnahme des Axioms von der Dreieckskongruenz, indem wir vielmehr dieses durch das andere, weniger aussagende Axiom, daß in jedem Dreieck die Summe zweier Seiten größer als die dritte sein soll, ersetzen, so gelangen wir zu einer Geometrie, welche keine andere ist als diejenige, die Minkowski aufgestellt und zur Grundlage seiner geometrischen Untersuchungen gemacht hat. Diese *Minkowskische Geometrie* ist dann im wesentlichen durch folgende Festsetzungen charakterisiert:

1. Zwei Strecken heißen dann einander gleich, wenn man sie durch Parallelverschiebung des Raumes ineinander überführen kann.

2. Die Punkte, die von einem festen Punkte $O$ gleichen Abstand haben, werden durch eine gewisse konvexe geschlossene Fläche des gewöhnlichen Euklidischen Raumes mit $O$ als Mittelpunkt repräsentiert, so daß an Stelle der konzentrischen Kugeln der gewöhnlichen Euklidischen Geometrie ein System ineinander geschachtelter, durch Ähnlichkeitstransformation erzeugter konvexer Flächen tritt.

Insofern in der Minkowskischen Geometrie das Parallelenaxiom gilt, dagegen an Stelle des Axioms von der Dreieckskongruenz der gewöhn-

lichen Euklidischen Geometrie jenes weniger aussagende Axiom tritt, daß im Dreieck die Summe zweier Seiten die dritte übertrifft, ist die Minkowskische Geometrie eine der gewöhnlichen Euklidischen Geometrie nächststehende Geometrie, ebenso wie die Bolyai-Lobatschefskysche Geometrie, zu der sie ein Gegenstück bildet. Wie die Bolyai-Lobatschefskysche Geometrie in verschiedenen mathematischen Disziplinen, besonders in der Theorie der analytischen Funktionen mit linearen Transformationen in sich, die fruchtbarste Anwendung findet, so zeigt sich die Minkowskische Geometrie besonders für die Zahlentheorie von hervorragender Bedeutung.

Übertragen wir die eben angestellten geometrischen Überlegungen ins Analytische. In gewöhnlichen rechtwinkligen Koordinaten $x_1, \ldots, x_n$ des $n$-dimensionalen Raumes kann die Oberfläche eines konvexen Körpers in der Gestalt

$$f(x_1, \ldots, x_n) = 1$$

dargestellt werden, so daß $f$ eine positive homogene (nicht notwendig rationale) Funktion ersten Grades bedeutet, deren wesentlichste Eigenschaft die ist, die durch die Funktionalungleichung

$$f(x_1 + y_1, \ldots, x_n + y_n) \leqq f(x_1, \ldots, x_n) + f(y_1, \ldots, y_n)$$

zum Ausdruck gebracht wird. Die Minkowskische Entfernung zwischen zwei Punkten $x_1, \ldots, x_n$ und $y_1, \ldots, y_n$ wird dann allgemein durch den Ausdruck

$$f(x_1 - y_1, \ldots, x_n - y_n)$$

definiert. Die ursprünglich zugrunde gelegte Fläche $f$

$$f(x_1, \ldots, x_n) = 1$$

heißt Eichfläche; sie ist das Minkowskische Analogon der Kugel im gewöhnlichen Euklidischen Raume.

Das Ausgangsbeispiel des Ellipsoides erhält man, wenn man hier für $f$ die Funktion $\sqrt{F}$ nimmt, wo $F$ die oben (S. X) erwähnte quadratische Form bedeutet.

Nun werde als Eichkörper ein konvexer Körper mit Mittelpunkt, d. h. ein solcher konvexer Körper genommen, der einen Punkt im Innern aufweist, in welchem alle hindurchgehenden Sehnen des Körpers halbiert werden. Dann gilt für die so definierte Minkowskische Entfernung der Satz, daß für die kleinste Entfernung zwischen zwei Gitterpunkten, d. h. für $M$, eine obere Schranke existiert, die allein vom Volumen des Eichkörpers abhängt; und zwar schließt man leicht, daß ein konvexer Körper mit einem Mittelpunkte in einem Punkte des Zahlengitters und vom Volumen $2^n$ immer noch mindestens zwei weitere Punkte des Zahlengitters, sei es im Innern, sei es auf der Begrenzung, enthalten muß.

Dieser Satz ist einer der anwendungsreichsten der Arithmetik; aus ihm leitet Minkowski seinen bekannten Determinantensatz ab, demzufolge

man in irgend $n$ ganzen homogenen linearen Formen von $n$ Variablen mit beliebigen reellen Koeffizienten und der Determinante 1 immer den Variablen solche ganzzahligen Werte, die nicht sämtlich Null sind, erteilen kann, daß dabei alle Formen absolute Beträge $\leqq 1$ erlangen; ferner die das Wesen der algebraischen Zahl tief berührende Tatsache, daß die Diskriminante eines algebraischen Zahlkörpers stets von $\pm 1$ verschieden ist, d. h. daß es für einen algebraischen Zahlkörper stets wenigstens eine durch das Quadrat eines Primideals teilbare Primzahl, eine sogenannte Verzweigungszahl, gibt, analog wie in der Theorie der algebraischen Funktionen bekanntlich gezeigt wird, daß eine algebraische Funktion stets Verzweigungspunkte besitzen muß.

Aber der obige Satz vom Volumen des Eichkörpers, den ich einen der anwendungsreichsten der Arithmetik nannte, bildet doch nur das Anfangsglied einer Reihe weiterer auf geometrischer Anschauung fußender Schlußweisen von weittragender Bedeutung. So gelangt Minkowski durch eine sehr sinnreiche geometrische Überlegung, bei der der zugrunde gelegte konvexe Körper sukzessive nach bestimmten Vorschriften dilatiert wird, zu einer Erweiterung des ursprünglichen Satzes, die so lautet: Ist das Volumen des Eichkörpers gleich $2^n$, so ist nicht nur, wie oben behauptet, die kleinste Minkowskische Entfernung $\leqq 1$, sondern sogar das Produkt der $n$ kleinsten Entfernungen, in $n$ unabhängigen Richtungen genommen, fällt stets $\leqq 1$ aus. Die Endlichkeit der Klassenanzahl der positiven quadratischen Formen von $n$ Variablen mit gegebener Determinante ist unter anderm eine leichte Folge dieses allgemeinen Satzes.

Wie oben ausgeführt wurde, hat Minkowski für das Minimum einer quadratischen Form $F$ von $n$ Variablen mit der Determinante 1 mittels seiner geometrischen Methode eine obere, nur von $n$ abhängige Schranke aufgestellt. Das genaue Minimum, d. h. der kleinste von Null verschiedene Wert, den $F$ für ganzzahlige Variablen erlangt, ist notwendig noch eine Funktion der Koeffizienten der Form $F$; lassen wir diese beliebig variieren, so jedoch, daß die Determinante beständig 1 bleibt, so können wir nach dem Maximum $k_n$ der Minima aller dieser Formen fragen; dasselbe wird eine nur von $n$ abhängige Zahl sein, welche jene obere Schranke ebenfalls nicht übersteigen kann. Durch völlig andere Hilfsmittel, aber ebenfalls ausgehend von einer geometrischen Betrachtung, bei der nunmehr der Begriff des Strahlenkörpers an Stelle des konvexen Körpers die wesentlichste Rolle spielt — Strahlenkörper ist ein Körper mit einem gewissen Punkte im Innern, der alle Strecken zwischen diesem Punkte und einem beliebigen Punkte des Körpers ganz enthält, so daß ein Strahlenkörper von einem gewissen Punkte aus diejenige Eigenschaft aufweist, welche bei einem konvexen Körper für jeden seiner Punkte erfüllt ist — gelangt

Minkowski für jenes Maximum $k_n$ des Minimums der quadratischen Form $F$ auch zu einer unteren Schranke. Ein überraschendes und für die Genauigkeit der Minkowskischen Methode zeugendes Resultat ist es, daß diese untere Schranke und die früher gefundene obere Schranke asymptotisch für $n = \infty$ ineinander fließen, so daß Minkowski die Limesgleichung

$$\lim_{n=\infty} \frac{\log k_n}{\log n} = 1$$

aussprechen konnte.

Ch. Hermite, damals der Senior der französischen Mathematiker, hatte von Anbeginn die zahlentheoretischen Arbeiten Minkowskis mit höchstem Interesse und lebhaftester Freude verfolgt. Es ist rührend, wie rückhaltlos er die Vorzüge der Minkowskischen Methode gegenüber seinen eigenen Entwicklungen anerkennt, als Minkowski ihm die eben besprochenen Resultate mitteilt. „Au premier coup d'œil j'ai reconnu", so schreibt Ch. Hermite in einem der an Minkowski gerichteten Briefe, „que vous avez été bien au delà de mes recherches en nous ouvrant dans le domaine arithmétique des voies toutes nouvelles." Und in einem zwei Jahre späteren Briefe vom November 1892 heißt es: „Je me sens rempli d'étonnement et de plaisir devant vos principes et vos résultats, ils m'ouvrent comme un monde arithmétique entièrement nouveau, où les questions fondamentales de notre science sont traitées avec un éclatant succès auquel tous les géomètres rendront hommage. Vous voulez bien, Monsieur, — et je vous en suis sincèrement reconnaissant — rapporter à mes anciennes recherches le point de départ de vos beaux travaux, mais vous les avez tant dépassées qu'elles ne gardent plus d'autre mérite que d'avoir ouvert la voie dans laquelle vous êtes entré."

Hiernach nimmt es nicht Wunder, daß Hermites Begeisterung für die zahlentheoretischen Methoden Minkowskis keine Grenzen kannte, als die erste Lieferung seiner Geometrie der Zahlen 1896 erschien. „Je crois voir la terre promise", so schreibt Hermite an Laugel, von dem er sich eine Übersetzung des Minkowskischen Buches zu seinem persönlichen Gebrauch anfertigen ließ. Und in der Tat, welche Fülle der verschiedenartigsten und tiefliegendsten arithmetischen Wahrheiten werden in diesem Hauptwerke Minkowskis durch das geometrische Band gehalten und verknüpft! Die Theorie der Einheiten in den algebraischen Zahlkörpern, Sätze über die Ordnung einer endlichen Gruppe von homogenen linearen ganzzahligen Substitutionen und über die Zahl der Transformationen einer positiven quadratischen Form in sich, der Beweis für die Endlichkeit der Klassenanzahl von positiven quadratischen Formen mit gegebener Determinante, die Annäherung an beliebig viele reelle Größen durch rationale Zahlen mit den gleichen Nennern, die Theorie der Linearformen mit

ganzen komplexen Koeffizienten, Sätze über Minima von Potenzsummen linearer Formen, die Theorie der Kettenbrüche usw. bilden, von den schon vorhin aufgeführten Gegenständen abgesehen, die Themata des Minkowskischen Buches über die Geometrie der Zahlen.

Minkowski legte besonderen Wert auf die Darstellung, die er in seinem Buche der Theorie der gewöhnlichen Kettenbrüche hat zuteil werden lassen; er war der Meinung, daß durch seine geometrische Veranschaulichung erst das wahre Wesen des Kettenbruches enthüllt werde. In einer späteren Arbeit*) gelangt er, ebenfalls geleitet durch ein geometrisches Verfahren, welches in der sukzessiven Konstruktion von Parallelogrammen besteht, zu einer neuen Art von Kettenbruchentwicklung für eine beliebige reelle Zahl $\alpha$. Diese Minkowskische Kettenbruchentwicklung ist so beschaffen, daß die dabei auftretenden Näherungsbrüche $\frac{x}{y}$ auch ohne Vermittlung des Kettenbruches direkt durch die Ungleichung

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{2}\frac{1}{y^2}$$

charakterisiert werden können; sie stellt demnach das bis dahin vermißte Analogon in der Größentheorie dar zu der in der Funktionentheorie üblichen Kettenbruchentwicklung, bei der ja ebenfalls die sämtlichen Näherungsbrüche, die der Kettenbruch einer Potenzreihe liefert, auch ohne den Kettenbruch unmittelbar definierbar sind.

Die Schlußlieferung von Minkowskis Geometrie der Zahlen ist nicht mehr erschienen, doch hat Minkowski den Stoff, den er für diese Lieferung plante, im wesentlichen in seinen späteren Abhandlungen zur Darstellung gebracht**).

Wenn wir uns diesen zuwenden, so haben wir vor allem eines Problems zu gedenken, dem Minkowski schon früh sein lebhaftes Interesse schenkte und auf welches er dann die in der ersten Lieferung seines Buches entwickelten Methoden mit sehr bemerkenswertem Erfolge anwandte***). Nach Lagrange fällt bekanntlich die Entwicklung einer reellen Zahl in einen Kettenbruch immer dann und nur dann periodisch aus, wenn die Zahl Wurzel einer quadratischen Gleichung mit rationalen Koeffizienten ist. Insofern dieser Satz ein notwendiges und hinreichendes

*) Ueber die Annäherung an eine reelle Größe durch rationale Zahlen. Mathematische Annalen, Bd. 54 (1901), S. 91—124. Diese Ges. Abhandlungen, B. I, S. 320—352.

**) Die posthum veröffentlichte „zweite Lieferung der Geometrie der Zahlen" (Leipzig 1910) entspricht nicht der ursprünglich von Minkowski geplanten Schlußlieferung, sondern bringt vielmehr nur das fünfte Kapitel der ersten Lieferung zum Abschluß.

***) Ein Kriterium für die algebraischen Zahlen. Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen, mathematisch-physikalische Klasse, 1899, S. 64—88. Diese Ges. Abhandlungen, Bd. I, S. 293—315.

Kriterium für die quadratische Irrationalität enthält, lag es nahe, einen entsprechenden Satz für die algebraische Irrationalität beliebigen Grades $n$ aufzustellen; doch waren alle bis dahin in dieser Richtung liegenden Versuche — ich erinnere an den Jacobischen Kettenbruchalgorithmus zur Entwicklung der kubischen Irrationalität, dessen Periodizität noch bis heute nicht festgestellt ist — vergeblich geblieben. Es gelang Minkowski zum ersten Male auf Grund sehr tiefliegender arithmetischer Sätze, zu deren Beweis seine geometrischen Methoden herangezogen werden, das gewünschte Kriterium für die algebraischen Zahlen beliebigen Grades $n$ zu gewinnen. Der Minkowskische Algorithmus ist nicht ganz einfach; er besteht zunächst in einer Vorschrift, wie man aus der beliebig vorgelegten Zahl $\alpha$ in eindeutig bestimmter Weise eine Kette von gewissen linearen Substitutionen von $n$ Variablen bestimmt und alsdann aus diesen gewisse lineare Formen ableitet: die Zahl $\alpha$ ist dann algebraisch vom Grade $n$, wenn die Kette niemals abbricht und zugleich alle jene unendlich vielen Formen aus einer endlichen Anzahl unter ihnen durch Multiplikation mit Faktoren entstehen.

In einer weiteren Untersuchung über die periodische Approximation algebraischer Zahlen*) beantwortet dann Minkowski insbesondere die Frage nach denjenigen algebraischen Zahlen $\alpha$, für welche jene Substitutionen periodischen Charakter aufweisen, denen also in diesem Sinne genau die von Lagrange für die quadratische Irrationalität entdeckte Eigenschaft zukommt. Minkowski fand, daß die verlangte Periodizität außer für die quadratische Irrationalität nur noch in fünf ganz bestimmten Fällen stattfindet: nämlich im Falle $n = 3$, $\alpha$ komplex; ferner $n = 3$, $\alpha$ reell, während die zu $\alpha$ konjugierten Zahlen komplex sind; im Falle $n = 4$, wenn $\alpha$ nebst allen konjugierten Zahlen komplex ist, und endlich in je einem speziellen Fall bei $n = 4$ und $n = 6$.

Hatte Minkowski das ganze von ihm erschlossene Gebiet Geometrie der Zahlen genannt, weil er zu den Methoden, aus denen seine arithmetischen Sätze fließen, durch räumliche Anschauung geführt worden war, so blieb er auch bei der weiteren Erforschung dieses Gebietes stets dem Bestreben treu, durch engen Anschluß an die geometrischen Vorstellungen und Bilder die Fruchtbarkeit seiner Methoden zu zeigen; er wird nicht müde, durch originelle Modifikationen seine ursprünglichen Überlegungen zu vertiefen, die gefundenen arithmetischen Sätze zu vervollkommnen und neue zu ersinnen.

So gelangt Minkowski**) zu einer gitterförmigen Bedeckung der Ebene

*) Ueber periodische Approximationen algebraischer Zahlen. Acta Mathematica, Bd. 26 (1902), S. 333—351. Diese Ges. Abhandlungen, Bd. I, S. 357—371.

**) Ueber die Annäherung an eine reelle Größe durch rationale Zahlen. Mathematische Annalen, Bd. 54 (1901), S. 108 ff. Diese Ges. Abhandlungen, Bd. I, S. 336 ff.

mit Parallelogrammen, bei der die ganze Ebene vollständig und andererseits keine Partie der Ebene mehr als zweifach überdeckt wird; diese Tatsache führt ihn unmittelbar zu einem Satze von Tschebyscheff über nichthomogene lineare diophantische Ungleichungen und zwar in einer allgemeineren und vollkommeneren Form, als derselbe von Tschebyscheff aufgestellt worden war.

Ferner wirft Minkowski die Frage auf*), unendlich viele untereinander kongruente und parallel orientierte Körper derart anzuordnen, daß sie, ohne einander zu durchdringen, sich so dicht als überhaupt möglich zusammenschließen, während ihre Schwerpunkte ein parallelepipedisches Punktsystem bilden. Wählt man für die Körper Kugeln, so zeigt sich dann, daß im Raume von drei Dimensionen zwar die bekannte tetraëdrale Anordnung von Kugeln die dichteste ist, daß aber in Räumen von höheren Dimensionen die dieser entsprechende tetraëdrale Anordnung keineswegs die dichteste Kugellagerung liefert. Das Problem der dichtesten Lagerung von Kugeln im $n$-dimensionalen Raum läuft auf die Bestimmung des Maximums $k_n$ hinaus und hängt zusammen mit der Frage nach der Reduktion der positiven quadratischen Formen; diesem Problem wendet sich Minkowski in seiner zahlentheoretischen Abhandlung über den Diskontinuitätsbereich für arithmetische Äquivalenz**) noch einmal zu, es in vollendeter Form lösend, gleichsam als offensichtliches Wahrzeichen für die Leichtigkeit und Überlegenheit seiner gegenwärtigen mehr geometrischen Methoden im Vergleich zu dem Standpunkt seiner Jugendarbeiten.

Die Beweise der allgemeinen Sätze: der reduzierte Raum für die positiven quadratischen Formen von $n$ Variablen ist eine konvexe Pyramide mit der Spitze im Nullpunkt, die von einer endlichen Anzahl durch diesen Punkt laufender Ebenen begrenzt wird; und: im Gebiet der positiv-definiten Formen grenzt der reduzierte Raum nur an eine endliche Anzahl von äquivalenten Räumen an; ferner die Berechnung des Volumens des reduzierten Raumes für alle Formen, deren Determinante eine gegebene Grenze nicht übersteigt, sowie die Anwendung hiervon auf die Bestimmung des asymptotischen Wertes der Klassenanzahl positiver quadratischer Formen sind die Glanzpunkte dieser letzten und inhaltreichsten zahlentheoretischen Abhandlung Minkowskis.

Von der Bedeutung der Zahlentheorie, wie sie in den Werken ihrer Heroen Fermat, Euler, Lagrange, Legendre, Gauß, Hermite, Dirichlet, Kummer, Jacobi und in deren begeisterten Aussprüchen sich wider-

*) Dichteste gitterförmige Lagerung kongruenter Körper. Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen, mathematisch-physikalische Klasse, 1904, S. 311—355. Diese Ges. Abhandlungen, Bd. II, S. 3—42.

**) Diskontinuitätsbereich für arithmetische Äquivalenz. Crelles Journal, Bd. 129 (1905), S. 220—274. Diese Ges. Abhandlungen, Bd. II, S. 53—100.

spiegelt, war Minkowski aufs tiefste durchdrungen; ihre Reize empfand er jederzeit aufs lebhafteste: war doch, was man an der Zahlentheorie rühmt, die Einfachheit ihrer Grundlagen, die Genauigkeit ihrer Begriffe und die Reinheit ihrer Wahrheiten ganz und gar zu seinem Wesen passend und seiner innersten Neigung am meisten zusagend. Wenn es zutrifft, daß nur ein enger Kreis von Mathematikern der Pflege der Zahlentheorie sich hingibt und so viele „von den eigenartigen, durch die Zahlentheorie ausgelösten Stimmungen kaum einen Hauch verspüren“: den Grund hierfür erblickt er darin, daß die Schöpfungen eines Gauß und der andern Großen zu erhaben sind. Und um in dieser gewaltigen Musik, wie er die Zahlentheorie nennt, für diejenigen, die nicht nur erbaut, sondern auch ergötzt sein wollen, die einschmeichelnden Melodien herauszuheben und so zu ihrem Genusse mehr anzulocken, dazu veröffentlichte er die Vorlesung, die er Winter 1903/04 in Göttingen gehalten hat, und in welcher er in leicht faßlicher Weise ohne die Voraussetzung besonderer Vorkenntnisse die wichtigsten Grundsätze der Geometrie der Zahlen und die einfachsten Anwendungen auf die Theorie der quadratischen Formen, auf die Zahlkörper und vor allem auf die Annäherung reeller und komplexer Größen durch rationale Zahlen auseinandersetzt. Das so entstandene Buch „*Diophantische Approximationen*“*) kann vorzüglich zur Einführung in die von Minkowski geschaffenen Methoden dienen.

Minkowski ist es zu danken, daß nach Hermites Tode die Führerrolle in der Zahlentheorie wieder in deutsche Hände zurückfiel und, wenn man überhaupt bei einer solchen Wissenschaft, wie es die Arithmetik ist, die Beteiligung der Nationen an den Fortschritten und Errungenschaften abwägen will: wesentlich durch Minkowskis Wirken ist es gekommen, daß heute im Reiche der Zahlen die bedingungslose und unbestrittene deutsche Vorherrschaft statthat.

Die Überzeugung von der tiefen Bedeutung des Begriffes eines konvexen Körpers, dessen Verwendung in der Zahlentheorie so erfolgreich gewesen war, hatte sich bei Minkowski immer mehr befestigt, und dieser Begriff bildet denn auch das Bindeglied zwischen denjenigen Arbeiten Minkowskis, die wesentlich zahlentheoretische Ziele im Auge haben, und seinen rein geometrischen Untersuchungen.

Das ursprüngliche Ziel, das Minkowski bei seinen rein geometrischen Untersuchungen im Auge hatte, war, die Begriffe Länge und Oberfläche mittels des Begriffes Volumen, „dieses elementarsten Begriffes der Analysis des Unendlichen“, zu erfassen**). In der Tat gelingt ihm diese Reduktion

*) Diophantische Approximationen. Eine Einführung in die Zahlentheorie. Leipzig 1907.

**) Volumen und Oberfläche. Mathematische Annalen, Bd. 57 (1903), S. 447—495. Diese Ges. Abhandlungen, Bd. II, S. 230—276.

durch ein einfaches Grenzverfahren. Ist etwa eine Kurve im Raume gegeben, so denkt sich Minkowski um jeden ihrer Punkte eine Kugel mit dem Radius $r$ abgegrenzt. Das Volumen des so insgesamt in der Umgebung der Kurve abgegrenzten Bereiches nach Division durch den Inhalt des Kreises vom Radius $r$ strebt in der Grenze für verschwindende Werte von $r$ im allgemeinen einer Größe zu, die nunmehr als die Länge der Kurve eingeführt wird. Ähnlich kann der Begriff des Inhaltes einer Fläche eingeführt werden, und insbesondere die so entstehende Definition der Oberfläche ist es, durch die Minkowski zu einer wichtigen Verallgemeinerung des Begriffes der Oberfläche gelangt, indem er nämlich an Stelle von Kugeln beliebige einander ähnliche und ähnlich gelegene konvexe Körper verwendet — genau im Sinne der vorhin bei Besprechung der zahlentheoretischen Abhandlungen geschilderten Minkowskischen Geometrie.

Durch den Ausbau des Gedankens, die Kugel durch einen beliebigen Eichkörper zu ersetzen, gelangt Minkowski zu demjenigen Begriffe, der das Fundament seiner ganzen Theorie bildet, zu dem *Begriffe des gemischten Volumens* von irgend drei konvexen Körpern. Das gemischte Volumen von drei konvexen Körpern $K_1$, $K_2$, $K_3$ ist eine ganz bestimmte eindeutig aus denselben durch ein dreifaches Integral darzustellende Zahl $V_{123}$, die in das gewöhnliche Volumen eines Körpers übergeht, wenn man jene drei Körper miteinander identifiziert, die in die gewöhnliche Oberfläche eines Körpers übergeht, wenn man zwei von jenen drei Körpern miteinander identifiziert und den dritten gleich der Kugel mit dem Radius 1 nimmt und die endlich mit der totalen mittleren Krümmung der Oberfläche eines Körpers übereinstimmt, wenn man für zwei von jenen drei Körpern die Kugel mit dem Radius 1 wählt. So erscheint der Begriff des gemischten Volumens als der einfachste übergeordnete Begriff, der die Begriffe Volumen, Oberfläche, totale mittlere Krümmung als Spezialfälle enthält, und diese letzteren Begriffe sind damit in viel engeren Zusammenhang miteinander gebracht; steht doch deshalb auch von vornherein zu erwarten, daß wir auf diesem Standpunkte über das Verhältnis zwischen jenen Begriffen einen weit tieferen und allgemeineren Aufschluß erhalten, als bisher möglich war. Das Hauptergebnis, welches in dieser Hinsicht die Minkowskische Theorie liefert, gipfelt in der Ungleichung

$$V_{123}^2 \geqq V_{122}\, V_{133},$$

einer Ungleichung, die lediglich quadratischen Charakter trägt, während beispielsweise der bekannte Satz, daß die Kugel unter allen Körpern gleicher Oberfläche das größte Volumen besitzt, für Volumen $V$ und Oberfläche $O$ eines beliebigen Körpers durch die kubische Ungleichung

$$36\pi\, V^2 \geqq O^3$$

ausgedrückt wird. Diese kubische Ungleichung aber und somit insbesondere jener Satz über das Maximum des Kugelvolumens erscheint bei Minkowski als spezieller Ausfluß der genannten inhaltreicheren und einfacheren quadratischen Ungleichung; zugleich treten neben jenen Satz vom Maximum des Kugelvolumens eine ganze Reihe gleich wichtiger Sätze über die Kugel. Über das gemischte Volumen stellt Minkowski den allgemeinen Satz auf, daß, wenn man aus drei Körpern vom Volumen 1 das gemischte Volumen bildet, dieses stets $\geqq 1$ ist und nur dann gleich 1 wird, wenn die drei Körper miteinander identisch sind oder durch Translation miteinander zur Deckung gebracht werden können — ein Satz, der ebenfalls die in Rede stehende Maximaleigenschaft der Kugel als spezielle Folge mit enthält.

Zur analytischen Durchführung dieser Gedanken bedient sich Minkowski im wesentlichen der Methode der Ebenenkoordinaten. Die letzteren erscheinen in der Tat als das naturgemäße Hilfsmittel zur Darstellung der Minkowskischen Theorie; ist doch das Mischvolumen nichts Anderes als eine zweimalige Bildung der ersten Variation des gewöhnlichen Volumens, falls man dieses durch Ebenenkoordinaten ausdrückt.

Des weiteren beschäftigt sich Minkowski mit dem einfachen und elementaren Begriffe des konvexen Polyeders und weiß diesem vielbehandelten Gegenstande neue und fruchtbare Seiten abzugewinnen. Sein grundlegender Satz sagt aus, daß ein konvexes Polyeder stets durch die Richtungen der Normalen und die Inhalte seiner Seitenflächen bis auf eine Translation eindeutig bestimmt wird. Aus diesem Satze leitet Minkowski durch Grenzübergang das merkwürdige Theorem ab, wonach es immer eine und nur eine geschlossene konvexe Fläche gibt, für die die Gaußsche Krümmung als stetige Funktion der Richtungskosinusse ihrer Normalen vorgeschrieben ist. Indem hierbei Minkowski die Krümmung — unmittelbar an die ursprüngliche Betrachtungsweise von Gauß anschließend — durch eine Integralforderung definiert, vermeidet er es, die Existenz der zweiten Ableitungen der die Fläche definierenden Funktion vorauszusetzen, und erreicht eben dadurch jene größtmögliche Einfachheit und Allgemeinheit in der Fassung und Entwicklung des Theorems.

Das Minkowskische Problem der Bestimmung der geschlossenen konvexen Flächen mit vorgeschriebener Gaußscher Krümmung ist wesentlich identisch mit dem Problem der Integration einer gewissen *partiellen Differentialgleichung vom Monge-Ampèreschen Typus*; so kommt es, daß die ursprünglich rein geometrische, auf dem Begriff des konvexen Körpers beruhende Methode Minkowskis zugleich für die Theorie der Integration gewisser nichtlinearer partieller Differentialgleichungen bis dahin unbekannte Fragestellungen und aussichtsreiche Angriffspunkte liefert.

Endlich werde noch eines kleinen Vortrages*) von Minkowski Erwähnung getan, den er vor seiner Übersiedelung nach Göttingen in der hiesigen mathematischen Gesellschaft gehalten hat und der bisher nur in einer russischen Übersetzung publiziert worden ist; derselbe enthält einen Satz von elementarem Charakter, wonach die Körper, deren Breite konstant d. h. in jeder Richtung genommen die nämliche ist, und andererseits die Körper konstanten Umfanges miteinander identisch sind; dabei ist unter Umfang der Umfang des Querschnittes des in irgendeiner Richtung dem Körper umschriebenen Zylinders zu verstehen.

Sein Interesse für die physikalische Wissenschaft hat Minkowski frühzeitig bekundet. Schon in den ersten Jahren seiner Privatdozentenzeit in Bonn beschäftigte er sich mit theoretischen Untersuchungen über *Hydrodynamik*. Helmholtz legte 1888 in der Akademie der Wissenschaften zu Berlin eine Arbeit**) von Minkowski über das Problem der kräftefreien Bewegung eines beliebigen starren Körpers in einer reibungslosen inkompressiblen Flüssigkeit vor. Um die Bewegung des Körpers völlig zu kennzeichnen, ist die Bestimmung von sechs unbekannten Funktionen der Zeit erforderlich. Das wichtigste Resultat von Minkowski besteht nun in der Reduktion des ursprünglich durch das Hamiltonsche Prinzip gelieferten Variationsproblems auf ein Variationsproblem, welches nur zwei unbekannte Funktionen der Zeit enthält.

Die Ferienzeiten während der Bonner Jahre verlebte Minkowski in der Regel in Königsberg, dem Wohnorte seiner Familie, wo er dann mit Hurwitz und mir fast täglich zusammenkam, meist auf Spaziergängen in der Königsberger Umgebung. Einmal, Weihnachten 1890, blieb Minkowski in Bonn; auf mein Zureden nach Königsberg zu kommen, stellte er sich in einem launigen Briefe als einen physikalisch völlig Durchseuchten hin, der erst eine zehntägige Quarantäne durchmachen müßte, ehe Hurwitz und ich ihn in Königsberg als mathematisch rein zu unseren Spaziergängen zulassen würden. „Ich habe mich", so fährt Minkowski in seinem Briefe fort, „ganz der Magie, wollte sagen der Physik ergeben. Ich habe meine praktischen Übungen im physikalischen Institut, zu Hause studiere ich Thomson, Helmholtz und Konsorten; ja von Ende nächster Woche an arbeite ich sogar an einigen Tagen der Woche in blauem Kittel in einem Institut zur Herstellung physikalischer Instrumente, also ein Praktikus schändlichster Sorte." Von Heinrich Hertz in Bonn fühlte sich Minkowski

*) Ueber die Körper konstanter Breite. Moskau, Mathematische Sammlung (Matematičeskij Sbornik), Bd. 25 (1906), S. 505—508. Diese Ges. Abhandlungen, Bd. II, S. 277—279.

**) Ueber die Bewegung eines festen Körpers in einer Flüssigkeit. Sitzungsberichte der Berliner Akademie, 1888, S. 1095—1110. Diese Ges. Abhandlungen, Bd. II, S. 283—297.

stark angezogen; er äußerte, daß er, wenn Hertz am Leben geblieben wäre, sich schon damals mehr der Physik zugewandt hätte.

August 1892 war Minkowski zum außerordentlichen Professor in der philosophischen Fakultät zu Bonn ernannt worden. April 1894 ermöglichte auf Minkowskis und meinen dringenden Wunsch der damalige Ministerialrat Althoff, der Scharfblickende, in dem Minkowski sehr frühzeitig einen Gönner und Bewunderer gefunden hatte, die Versetzung Minkowskis nach Königsberg, und ein Jahr später wurde Minkowski dann in Königsberg mein Nachfolger im dortigen Ordinariat für Mathematik. Aus diesem Amte schied er Oktober 1896, um einem Rufe als Professor für Mathematik an das Eidgenössische Polytechnikum in Zürich zu folgen. Dort verheiratete er sich im Jahre 1897 mit Auguste Adler aus Straßburg i. E. In Zürich blieb er bis zum Herbst 1902. Da war es wiederum Althoff, der Minkowski auf den für seine Wirksamkeit angemessensten Boden verpflanzte; mit einer Kühnheit, wie sie vielleicht in der Geschichte der Verwaltung der Preußischen Universitäten beispiellos dasteht, schuf Althoff aus nichts hier in Göttingen eine neue ordentliche Professur, und dieser Tat Althoffs danken wir es, daß seit Herbst 1902 Minkowski der unsrige gewesen ist. Bereits Oktober 1901 hatte ihn unsere Gesellschaft zu ihrem korrespondierenden Mitgliede in der mathematisch-physikalischen Klasse gewählt.

Als Frucht der vielseitigen theoretisch-physikalischen Studien, die Minkowski auch in Zürich betrieben hatte und in Göttingen fortsetzte, ist der Enzyklopädieartikel über *Kapillarität**) anzusehen, in welchem er in wahrhaft musterhafter Weise in aller Kürze, dem beschränkten Raum entsprechend, die sämtlichen theoretischen Gesichtspunkte dieses Kapitels der Physik auseinandersetzt und die schwierigen mathematischen Grundlagen, insbesondere soweit sie die Variationsrechnung betreffen, in origineller, zum Teil ganz neuer Form entwickelt.

Aber am nachhaltigsten fesselten Minkowski die modernen elektrodynamischen Theorien, die er mehrere Semester hindurch mit mir gemeinsam betrieb, insbesondere in Vorträgen, zu denen das von ihm und mir geleitete Seminar Anlaß bot. Die letzten Schöpfungen Minkowskis entsprangen diesen Studien, denen er mit großem Eifer oblag; hatte er doch für die nächsten Semester Vorlesungen und Seminar über Elektronentheorie geplant.

H. A. Lorentz hat zuerst erkannt, daß die Grundgleichungen der Elektrodynamik für den reinen Äther die Eigenschaft der Invarianz gegenüber denjenigen gleichzeitigen Transformationen der Raumkoordinaten $x, y, z$ und

*) Enzyklopädie der mathematischen Wissenschaften, Bd. V 1, Heft 4, S. 558—613. Diese Ges. Abhandlungen, Bd. II, S. 298—351.

des Zeitparameters $t$ besitzen, die — falls man die Lichtgeschwindigkeit gleich 1 nimmt — den Ausdruck $x^2 + y^2 + z^2 - t^2$ in sich überführen. Im Zusammenhang mit dieser rein mathematischen Tatsache und in der Absicht, davon Rechenschaft zu geben, daß eine relative Bewegung der Erde gegen den Lichtäther nicht wahrgenommen wird, war jener scharfsinnige Forscher in kühnem Gedankenfluge zu der Einsicht gelangt, daß der Begriff des starren Körpers in dem bisherigen Sinne nicht aufrecht zu erhalten sei, sondern in der Weise modifiziert werden müsse, daß Elektrizität und Materie, sofern sie eine Bewegung von der Geschwindigkeit $v$ besitzen, in Richtung dieser Bewegung eine Verkürzung ihrer Ausdehnung erfahren und zwar im Verhältnis $1 : \sqrt{1 - v^2}$. Daß eine weitere Konsequenz dieser Idee eine neuartige Auffassung des Zeitbegriffes ist, und insbesondere alle den Lorentz-Transformationen entsprechenden Bezugsysteme zur Einführung eines Zeitparameters gleichberechtigt sind, dies erkannt zu haben, ist das Verdienst des Physikers Einstein.

Die Ideenbildungen von Lorentz und Einstein, die man unter dem Namen des Relativitätsprinzipes zusammenfaßt, waren es, die Minkowski die Anregung zu seinen wichtigen und auch in weiteren Kreisen bekannt gewordenen *elektrodynamischen Untersuchungen* gaben. Minkowski*) legte sofort jener mathematischen Tatsache der Invarianz der elektrodynamischen Grundgleichungen gegenüber den Lorentz-Transformationen die allgemeinste und weitgehendste Bedeutung bei, indem er diese Invarianz als eine Eigenschaft auffaßte, die überhaupt allen Naturgesetzen zukomme, ja daß sie nichts Anderes als eine schon in den Begriffen Raum und Zeit selbst enthaltene und diese beiden Begriffe gegenseitig verkettende und miteinander verschmelzende Eigenschaft sei. Auch dem Nicht-Naturforscher ist die Tatsache geläufig, daß die Naturgesetze von der Orientierung im Raume sowie von der Zeit unabhängig sind, und ferner lehrt die gewöhnliche Mechanik, daß, wenn ein System sich bewegt, stets auch diejenige Bewegung statthaben kann, bei welcher die Geschwindigkeitsvektoren sämtlicher materieller Punkte je um einen konstanten Vektor vermehrt sind: darüber hinaus behauptet nun nach Minkowski das Relativitätsprinzip — oder, wie es Minkowski später nennt, das *Weltpostulat* —, daß die Naturgesetze in einem noch viel höheren Sinne von Raum und Zeit unabhängig, nämlich invariant gegenüber allen Lorentz-Transformationen sind. Indem nun durch die Lorentz-Transformationen gewisse Abänderungen des Zeitparameters zugelassen werden, die nicht bloß auf eine veränderte Wahl des Zeitanfanges hinauslaufen, fällt konsequenterweise überhaupt der Be-

*) Die Grundgleichungen für die elektromagnetischen Vorgänge in bewegten Körpern. Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen, mathematisch-physikalische Klasse, 1908, S. 53—111. Diese Ges. Abhandlungen, Bd. II, S. 352—404.

griff der Gleichzeitigkeit zweier Ereignisse als an sich existierend. Nur weil wir gewohnt sind, ein bestimmtes Bezugsystem für Raum und Zeit stark approximativ eindeutig zu wählen, halten wir den Begriff der Gleichzeitigkeit für einen absoluten — ungefähr wie Wesen, gebannt an eine enge Umgebung eines Punktes auf einer Kugeloberfläche, darauf verfallen könnten, die Kugel sei ein geometrisches Gebilde, an welchem ein Durchmesser an sich ausgezeichnet ist. Tatsächlich ist die Sachlage die, daß stets zwei Ereignisse, die an zwei Orten zu zwei verschiedenen Zeiten stattfinden, als gleichzeitig aufgefaßt werden können, sobald die Zeitdifferenz kleiner als die Entfernung beider Orte, d. h. diejenige Zeit ausfällt, die das Licht braucht, um von dem einen Orte zu dem andern zu gelangen. Ähnlich verhält es sich mit drei Ereignissen zu drei verschiedenen Zeiten, die ebenfalls als gleichzeitig stattfindend aufgefaßt werden können, sobald gewisse Ungleichheiten zwischen den Raum- und Zeitparametern erfüllt sind. Erst durch vier Ereignisse ist im allgemeinen das Bezugsystem von Raum und Zeit eindeutig festgelegt. — „Von Stund an sollen Raum für sich und Zeit für sich völlig zu Schatten herabsinken, und nur noch eine Art Union der beiden soll Selbständigkeit bewahren." So bekannte sich Minkowski eingangs des eindrucksvollen Vortrages*), den er auf der vorjährigen Naturforscherversammlung zu Köln vor einer zahlreichen, ihm mit größter Aufmerksamkeit folgenden Zuhörerschaft, bestehend aus Mathematikern, Physikern und Philosophen, gehalten hat.

Um die in Rede stehende Invarianz der Naturgesetze richtig zu verstehen, ersetze man sowohl die Raum- und Zeitparameter $x, y, z, t$, wie auch diejenigen Größen, die in den die Naturgesetze ausdrückenden Gleichungen als Funktionen von $x, y, z, t$ auftreten, durch die entsprechend linear transformierten Größen: dann müssen die erhaltenen Gleichungen die nämliche Form für die neuen Größen in den neuen Veränderlichen aufweisen. Beispielsweise sind im Falle der elektrodynamischen Grundgleichungen die mit der Dichte multiplizierten Geschwindigkeitskomponenten $u, v, w$ zusammen mit der Dichte $\varrho$ als vier Größen anzusehen, die in gleicher Weise mit den Variablen $x, y, z, t$ transformiert werden; die Vektorenpaare dagegen, der elektrische und der magnetische Vektor einerseits und die elektrische und magnetische Erregung andererseits, sind als je sechs Größen anzusehen, die wie die sechs zweireihigen Determinanten einer Matrix zweier Raumzeitpunkte, d. h. etwa wie die Plückerschen Linienkoordinaten sich transformieren. Da demnach bei diesen Transformationen eine Vermischung von Geschwindigkeiten und Dichte und

*) Raum und Zeit. Physikalische Zeitschrift, 10. Jahrgang, Nr. 3 (1909), S. 104—111; Jahresberichte der Deutschen Mathematiker-Vereinigung, Bd. 18 (1909), S. 75—88. Diese Ges. Abhandlungen, Bd. II, S. 431—444.

ebenso von elektrischen und magnetischen Vektoren stattfindet, so ist absolut genommen eine Festlegung von Geschwindigkeit und Dichte der Substanz, sowie der elektrischen und magnetischen Vektoren nicht möglich; diese Begriffe hängen vielmehr ebenfalls wesentlich von der Wahl des Bezugsystems für $x, y, z, t$ ab.

Minkowski wendet nun das eben gekennzeichnete und von ihm mathematisch präzisierte Weltpostulat — und darin erblicke ich seine bedeutsamste positive Leistung auf diesem Gebiete — dazu an, um die elektrodynamischen Grundgleichungen für bewegte Materie, deren definitive Form unter den Physikern außerordentlich strittig war, herzuleiten. Dazu sind nur drei sehr einfache Grundannahmen nötig: nämlich

1) die Annahme, daß die Geschwindigkeit der Materie stets und an allen Orten kleiner als 1 d. h. als die Lichtgeschwindigkeit ist;

2) das Axiom, daß, wenn an einer einzelnen Stelle die Materie in einem Momente ruht — die Umgebung mag in irgendwelcher Bewegung begriffen sein — dann für jenen „Raumzeitpunkt" zwischen den magnetischen und elektrischen Vektoren und deren Ableitungen nach $x, y, z, t$ genau die nämlichen Beziehungen statthaben, die zu gelten hätten, falls alle Materie ruhte;

3) die Annahme der von niemand bestrittenen elektrodynamischen Grundgleichungen für ruhende Materie.

Die elektrodynamischen Grundgleichungen, die Minkowski auf diesem Wege erhält*), lassen, was Durchsichtigkeit und Einheitlichkeit betrifft, nichts zu wünschen übrig; sie stimmen mit den bisherigen Beobachtungen überein, weichen indes in mannigfaltiger Weise von den bis dahin gebrauchten, von Lorentz und Cohn aufgestellten Gleichungen ab, indem diese keineswegs das Weltpostulat genau erfüllen. Die *Minkowskischen elektrodynamischen Grundgleichungen* sind eine notwendige Folgerung des Weltpostulates — sie sind von derselben Gewißheit wie dieses.

Immer mehr und mehr befestigte sich Minkowski in der Überzeugung von der allgemeinen Gültigkeit und der eminenten Fruchtbarkeit und Tragweite seines Weltpostulats und — die wunderbaren, vielverheißenden Ideen von M. Planck über die Dynamik bewegter Systeme bestärkten ihn darin — von der Notwendigkeit einer Reform der gesamten Physik nach Maßgabe dieses Postulats.

Was die Mechanik betrifft, so gelangte Minkowski durch Einführung

*) Mit der Ausarbeitung einer Ableitung dieser Gleichungen auf Grund der Vorstellungen der Elektronentheorie war Minkowski in den letzten Wochen seines Lebens beschäftigt. Unter Benutzung der nachgelassenen Papiere ist eine solche Herleitung in Minkowskis Sinne von Herrn M. Born (Mathematische Annalen, Bd. 68 (1910), S. 526—551; diese Ges. Abhandlungen, Bd. II, S. 405—430) durchgeführt worden.

des Begriffs der Eigenzeit eines materiellen Punktes zu einem gewissen System modifizierter Newtonscher Bewegungsgleichungen, bestehend aus vier Gleichungen, von denen die drei ersten in die gewöhnlichen Newtonschen Gleichungen übergehen, wenn man die Lichtgeschwindigkeit $c$ unendlich werden läßt, während die vierte eine Folge der drei ersten ist und den Satz von der Erhaltung der Energie ausspricht. In dieser dem Weltpostulat gemäß reformierten Mechanik fallen die Disharmonien zwischen der Newtonschen Mechanik und der modernen Elektrodynamik von selbst weg. Aber die Minkowskische Untersuchung führt darüber hinaus zu der prinzipiell interessanten Tatsache, daß auf Grund des Weltpostulates die vollständigen Bewegungsgesetze allein aus dem Satz von der Erhaltung der Energie ableitbar sind.

Ferner zeigte Minkowski, wie das Newtonsche Gravitationsgesetz zu modifizieren sei, damit es dem Weltpostulat genügt. Das *Minkowskische Gravitationsgesetz* verknüpft mit der *Minkowskischen Mechanik* ist nicht weniger geeignet, die astronomischen Beobachtungen zu erklären als das Newtonsche Gravitationsgesetz verknüpft mit der Newtonschen Mechanik. Dabei bedeutet die Minkowskische Formulierung eine Fortpflanzung der Gravitation mit Lichtgeschwindigkeit — was unserer heutigen Anschauungsweise über Fernwirkung weit besser entspricht als die alte Newtonsche Momentanwirkung.

Als Beleg dafür, wie die Minkowskische Betrachtungsweise, die sich stets in der vierdimensionalen Raum-Zeitmannigfaltigkeit $x, y, z, t$ — Welt genannt — bewegt, erst imstande ist, die innere Einfachheit und den wahren Kern der Naturgesetze zu enthüllen, sei nur noch auf den wunderbar durchsichtigen, von Minkowski angegebenen Ausdruck für die so äußerst komplizierte ponderomotorische Wirkung zweier bewegter elektrischer Teilchen hingewiesen.

Damit ist die Würdigung der hauptsächlichsten Ergebnisse der Publikationen Minkowskis beendigt; aber die wissenschaftliche Wirksamkeit seiner Person ist durch die zur Veröffentlichung gelangten Schriften keineswegs erschöpft. Nach welchen Richtungen weiterhin und in welchem Sinne sich diese Wirksamkeit Minkowskis vornehmlich erstreckte, bedarf noch einer kurzen Darlegung, da erst dann die volle Bedeutung Minkowskis für die Entwicklung der Mathematik der Gegenwart sich erkennen läßt.

Zunächst gedenke ich der Stellungnahme Minkowskis gegenüber derjenigen mathematischen Disziplin, welche heute eine hervorragende Rolle in unserer Wissenschaft einnimmt und ihren gewaltigen Einfluß auf alle Gebiete der Mathematik ausströmt, nämlich der Mengentheorie. Diese von Georg Cantor zuerst in fruchtbarer Weise in Angriff genommene und

durch kühne Ideen zu gewaltiger Höhe geführte Lehre wurde damals von dem im Gebiet der Zahlentheorie maßgebenden Mathematiker Kronecker aufs entschiedenste bekämpft. Obwohl Minkowski in Berlin bei Kronecker studiert hatte und sich dem mächtigen Einfluß, den dieser in der Zahlentheorie ausübte, willig hingab: die Vorurteile, von denen Kronecker befangen war, durchschaute er frühzeitig; er war der erste Mathematiker unserer Generation — und ich habe ihn darin nach Kräften unterstützt —, der die hohe Bedeutung der Cantorschen Theorie erkannte und zur Geltung zu bringen suchte. „Die spätere Geschichte", so führt Minkowski in einem in Königsberg gehaltenen Vortrag über das Aktual-Unendliche in der Natur aus, „wird Cantor als einen der tiefsinnigsten Mathematiker dieser Zeit bezeichnen; es ist sehr zu bedauern, daß eine nicht auf sachlichen Gründen allein beruhende Opposition, die von einem sehr angesehenen Mathematiker" — gemeint ist eben Kronecker — „ausging, Cantor die Freude an seinen wissenschaftlichen Forschungen trüben konnte." Minkowski verehrte in Cantor den originellsten zeitgenössischen Mathematiker zu einer Zeit, als in damals maßgebenden mathematischen Kreisen der Name Cantor geradezu verpönt war und man in Cantors transfiniten Zahlen lediglich schädliche Hirngespinste erblickte. Minkowski äußerte wohl, daß Cantors Name noch genannt werden würde, wenn man die heute — weil sie modisch sind — im Vordergrunde stehenden Mathematiker längst vergessen hat. Der Umstand, daß ein Mann wie Minkowski, der das exakte Schließen in der Mathematik gewissermaßen verkörperte und dessen Sinn für echte Zahlentheorie über allem Zweifel war, so urteilte, ist der Verbreitung der Cantorschen Theorie, „dieser ursprünglichen Schöpfung genialer Intuition und spezifischen mathematischen Denkens", wie sie mit Recht kürzlich ein jüngerer Mathematiker genannt hat, sehr zustatten gekommen.

Minkowski hat stets danach gestrebt, nicht nur über die Methoden der reinen Mathematik die Herrschaft zu erlangen, sondern auch den wesentlichen Inhalt aller derjenigen Wissensgebiete sich anzueignen, in denen die Mathematik als Hilfswissenschaft eine entscheidende Rolle zu spielen berufen ist. Wie tief er dann in solche Wissensgebiete, die seinem eigentlichen Arbeitsfelde fern lagen, eindrang und wie kritisch auch hier sein Blick war, zeigen die mannigfachen Vorträge, die er bei verschiedenen Anlässen, namentlich in unserer mathematischen Gesellschaft, gehalten hat, sowie seine Universitätsvorlesungen. Zumal in Göttingen hat Minkowski außer den üblichen Vorlesungen eine große Anzahl von Spezialvorlesungen über die verschiedensten Gegenstände gehalten, z. B. über Linien- und Kugelgeometrie, Analysis situs, automorphe Funktionen, Invariantentheorie, Wärmestrahlung und Wahrscheinlichkeitsrechnung. Diese

Vorlesungen waren stets klar durchdacht und fein geformt; ihr Ziel war, die Ergebnisse neuester Forschung kritisch zu sichten, auf die einfachste Form zu bringen und alsdann in Verbindung mit den alten Sätzen der Theorie einheitlich zur Darstellung zu bringen. Wie sehr es ihm dabei gelang, auch den schwerfälligeren Zuhörern die Wege zu ebnen und die reiferen ganz für sich zu gewinnen, beweist der steigende Zuspruch, dessen sich diese Vorlesungen in Göttingen erfreuten. Besonders verstand er es, in höheren Vorlesungen junge Mathematiker zu eigenen Forschungen anzuregen. Unter den Dissertationen, die seiner Anregung zu verdanken sind, seien nur die von L. Kollros, Un algorithme pour l'approximation simultanée de deux grandeurs (1905), und E. Swift, Über die Form und Stabilität gewisser Flüssigkeitstropfen (1907), genannt, deren wertvolle Resultate in weiteren Fachkreisen bekannt geworden sind.

Daß Minkowski auch Nichtfachleuten durch die Heranziehung treffender Gleichnisse und anschaulicher Bilder über schwierige mathematische Gegenstände vorzutragen und in ihnen eine Vorstellung von der Größe und Erhabenheit unserer Wissenschaft zu erwecken wußte, zeigt am besten die Rede, die er in der Festsitzung der Göttinger mathematischen Gesellschaft zur hundertjährigen Wiederkehr des Geburtstages von Dirichlet gehalten hat*). Die begeisterten und klaren Ausführungen, die dort Minkowski über den Charakter der Zahlentheorie, ihre Bedeutung und ihre Stellung zu anderen Disziplinen machte, beruhen auf einer tiefen Erfassung des Wesens der Zahlentheorie und sind das Beste, was je über diese wunderbarste Schöpfung menschlichen Geistes gesagt worden ist. Hierfür sei das Zeugnis desjenigen Mathematikers angerufen, der als Schüler von Dirichlet ein kompetentes Urteil hat, und den wir heute im In- und Auslande als den Senior der Mathematiker, als den einzigen lebenden Heros aus der größten Epoche der Zahlentheorie verehren dürfen. „Ich habe Ihren Vortrag", so schrieb Richard Dedekind an Minkowski, „mit größtem Genuß fünfmal und noch viel öfter durchgelesen und bin besonders von der großen historischen Auffassung ergriffen, mit der Ihr Vortrag die tiefsten Gedanken unserer Wissenschaft deutlich erfaßt und in ihrer Entwicklung verfolgt".

Trotz seiner milden Denkart war Minkowski im Grunde kritisch, er erkannte leicht die Schwächen einer Beweisführung oder einer Ideenbildung und legte im allgemeinen auch an die Arbeiten anderer einen strengen Maßstab an. Er unterschied scharf zwischen oberflächlichen und soliden Mathematikern. Von einer guten mathematischen Arbeit ver-

*) P. G. Lejeune Dirichlet und seine Bedeutung für die heutige Mathematik. Jahresbericht der Deutschen Mathematiker-Vereinigung, Bd. 14 (1905), S. 149—163. Diese Ges. Abhandlungen, Bd. II, S. 447—461.

langte er, daß in ihr eine klar gestellte und des Interesses werte Frage gelöst werde.

So sehr er von echter Bescheidenheit war und mit seiner Person gern im Hintergrunde blieb, war er doch von der innersten Überzeugung getragen, daß vieles von dem, was er schuf, die Arbeiten anderer zeitgenössischer Autoren überleben und einst zur allgemeinen Anerkennung gelangen würde. Den von ihm gefundenen Satz von der Lösbarkeit linearer Ungleichungen mit der Determinante 1, seinen Beweis für die Existenz von Verzweigungszahlen im Zahlkörper oder die Reduktion der kubischen Ungleichung, die die vorhin genannte Maximaleigenschaft der Kugel ausdrückt, auf eine quadratische Ungleichung stellte er wohl innerlich selbst den besten Leistungen der mathematischen Klassiker auf dem Gebiet der Zahlentheorie und Geometrie gleichwertig an die Seite.

Man müsse fleißig sein, das Leben sei ja so kurz, äußerte er wohl. Und in der Tat, die Wissenschaft begleitete ihn überall, sie war ihm zu jeder Zeit interessant und ermüdete ihn an keinem Ort, sei es auf einem Ausflug, in der Sommerfrische oder in der Bildergalerie, in dem Eisenbahncoupé oder auf dem Großstadtpflaster.

Noch in den letzten Nächten, die er zu Hause zubrachte, beschäftigte ihn die Formung der Worte in seinem Kölner Vortrage, und er überlegte, welche Wendung dem naiven Sprachgefühl besser entspräche. Das war charakteristisch für ihn: er strebte zuerst nach Einfachheit und Klarheit des Gedankens — Dirichlet und Hermite waren darin seine Vorbilder —, dann bemühte er sich, dem Gedanken auch eine vollkommene Darstellung zu geben. Er war von großer Genauigkeit und einer ins kleinste Detail gehenden Eigenheit, was die Wahl der Bezeichnungen und der Buchstaben betraf, eine Genauigkeit, die — freilich wie bei Minkowski gepaart mit einem aufs Große gerichteten Blick — dem rechten Forscher stets eigen ist, und die wir heute bedauerlicherweise seltener werden sehen. Auch sonst, wenn er im kleineren Kreise über einen wissenschaftlichen Gegenstand sprach, legte er auf die Form und den Ausdruck Wert, und besonders in unserer mathematischen Gesellschaft verfehlte er selten, seinem Vortrage einige wohl überlegte, die Zuhörer anregende Bemerkungen vorauszuschicken.

Frei von aller vorgefaßten Meinung und von aller Einseitigkeit zeigte er auch für die entferntesten Anwendungen der Mathematik Interesse — immer der Meinung, daß diese auch der reinen Wissenschaft schließlich zum Vorteil dienen würden. So nahm er auch an den Sitzungen der Göttinger Vereinigung für angewandte Mathematik und Physik aufs regste teil.

Er besaß eine scharfe Beobachtungsgabe auch für Dinge, die nicht

seine Wissenschaft betrafen. Wie er denn überhaupt für alles, was Menschen bewegt — von der Politik bis zum Theater — Verständnis, nicht selten Eifer und Lebhaftigkeit bekundete. Dem Fernerstehenden schien es mitunter bei dem im allgemeinen ruhigen Temperament Minkowskis, als schenke er einer Sache wenig Interesse: oft fiel gerade dann von Minkowskis Seite eine Bemerkung, die den Kern der Sache traf, oder er hatte gar ein Zitat aus Faust bereit, den er vollständig auswendig konnte. Noch in der letzten arbeitsreichsten Zeit seines Lebens liebte er es, seinen Kindern Gedichte von Goethe und Schiller auswendig vorzutragen — mit der Begeisterung, die ihm aus seiner Jugendzeit frisch geblieben war.

Für seine Person war er äußerst einfach und anspruchslos, mehr bedacht auf das Wohlergehen seiner Angehörigen als auf sein eigenes.

Er war von unentwegtem Optimismus, stets überzeugt, daß das Gute und Richtige zum schließlichen Siege gelangen würde. Für junge heranwachsende Mathematiker hatte er viel persönliches Interesse und sah sie häufig bei sich im Hause; er sprach sich bisweilen überschwenglich über die Kenntnisse und den Fleiß einzelner unter ihnen aus und setzte große Hoffnungen auf ihre Zukunft.

Seit meiner ersten Studienzeit war mir Minkowski der beste und zuverlässigste Freund, der an mir hing mit der ganzen ihm eigenen Tiefe und Treue. Unsere Wissenschaft, die uns das liebste war, hatte uns zusammengeführt; sie erschien uns wie ein blühender Garten; in diesem Garten gibt es geebnete Wege, auf denen man mühelos genießt, indem man sich umschaut, zumal an der Seite eines Gleichempfindenden. Gern suchten wir aber auch verborgene Pfade auf und entdeckten manche neue, uns schön dünkende Aussicht, und wenn der eine dem andern sie zeigte und wir sie gemeinsam bewunderten, war unsere Freude vollkommen.

Sein stiller Sinn stand nicht nach äußeren Zeichen der Anerkennung; doch empfand er eine lebhafte Genugtuung, wenn mir eine solche zuteil wurde. Allem, was mich betraf, brachte er sein stets gleichbleibendes Interesse und seine herzlichste Teilnahme entgegen. Zumal die kleine Stadt hier erleichterte unsern Verkehr: ein Telephonruf zur Vermittlung einer Verabredung oder ein paar Schritte über die Straße und ein Steinchen an die klirrende Scheibe des kleinen Eckfensters seiner Arbeitsstube — und er war da, zu jeder mathematischen oder nichtmathematischen Unternehmung bereit.

Noch auf der Krankenbahre liegend — todeswund — galten seine Gedanken dem Bedauern, daß er in der nächsten Stunde des Seminars, in der ich meine Lösung des Waringschen Problems vortragen wollte, nicht zugegen sein könne. Seinem Andenken darum habe ich meine die Lösung

enthaltende Abhandlung gewidmet, die erste, von deren Inhalt er keine Kenntnis mehr genommen hat und über deren Korrekturbogen sein sicheres Auge nicht geglitten ist.

Er war mir ein Geschenk des Himmels, wie es nur selten jemand zuteil wird, und ich muß dankbar sein, daß ich es so lange besaß.

Jeder, der ihm näher stand, empfand die Harmonie seiner Persönlichkeit und den Zauber seiner Genialität; sein Wesen war wie der Klang einer Glocke, so hell in dem Glück bei der Arbeit und der Heiterkeit seines Gemütes, so voll in der Beständigkeit und Zuverlässigkeit, so rein in seinem idealen Streben und seiner Lebensauffassung.

Wie er gelebt hat, so starb er — als Philosoph. Wenige Stunden noch vor seinem Tode traf er die Anordnungen über die Korrektur seiner im Druck befindlichen Arbeit und überlegte, ob es sich empfehlen würde, seine unfertigen Manuskripte zu verwerten. Er sprach sein Bedauern über sein Schicksal aus, da er doch noch vieles hätte machen können; seiner letzten elektrodynamischen Arbeit aber würde es vielleicht zugute kommen, daß er zur Seite trete — man werde sie mehr lesen und mehr anerkennen. Zum Abschiednehmen verlangte er nach den Seinigen und nach mir.

Mehr als sechs Jahre hindurch haben wir, seine nächsten mathematischen Kollegen, jeden Donnerstag pünktlich drei Uhr mit ihm zusammen den mathematischen Spaziergang auf den Hainberg gemacht — auch den letzten Donnerstag vor seinem Tode, wo er uns mit besonderer Lebhaftigkeit von den neuen Fortschritten seiner elektrodynamischen Untersuchungen erzählte: den Donnerstag darauf — wiederum um drei Uhr — gaben wir ihm das letzte Geleit. Dienstag, den 12. Januar, mittags, war er einer Blinddarmentzündung erlegen; bei dem bösartigen Charakter, mit dem die Krankheit auftrat, hatte auch die Sonntag Nacht ausgeführte Operation nicht mehr helfen können.

Jäh hat ihn der Tod von unserer Seite gerissen. Was uns aber der Tod nicht nehmen kann, das ist sein edles Bild in unserem Herzen und das Bewußtsein, daß sein Geist in uns fortwirkt.

# ZUR THEORIE
# DER QUADRATISCHEN FORMEN

# I.

# Grundlagen für eine Theorie der quadratischen Formen mit ganzzahligen Koeffizienten.

(Mémoires présentés par divers savants à l'Académie des Sciences de l'Institut national de France, Tome XXIX, No. 2. 1884.)

(Vorbemerkung des Herausgebers. Diese Abhandlung ist von Minkowski im Mai 1882 der Pariser Académie des Sciences als Preisschrift, und zwar in Gestalt eines in deutscher Sprache verfaßten Manuskriptes, eingereicht worden (vgl. Comptes Rendus, Bd. 96 (1883), pp. 879–883). In den Mémoires des Savants étrangers ist sie, von Minkowski selbst ins Französische übertragen, unter dem Titel „Mémoire sur la théorie des formes quadratiques à coefficients entiers" erschienen. Die vorliegende deutsche Ausgabe folgt überall dort, wo der gedruckte französische Text als unmittelbare Übersetzung des ursprünglichen deutschen Manuskriptes gelten kann, dem letzteren; an den zahlreichen Stellen, an denen beide voneinander abweichen, ist der französische Text als maßgebend angesehen und ins Deutsche rückübersetzt worden. Ein Verzeichnis der hauptsächlichsten dieser Stellen befindet sich am Schlusse der Abhandlung. Von dem Herausgeber herrührende Zusätze und Anmerkungen sind durch doppelte eckige Klammern [[ ]] kenntlich gemacht.)

**[[Begleitschreiben an die Académie des Sciences.]]**

J'ai l'honneur de soumettre au jugement de l'Académie mon Mémoire ci-joint, intitulé: «*Fondements pour une théorie des formes quadratiques à coefficients numériques*» comme ouvrage de concours au *Grand Prix des sciences mathématiques*, proposé pour la solution de la question: «Théorie de la décomposition des nombres entiers en une somme de cinq carrés.»

Tout en espérant avoir réussi à résoudre la question proposée, et à la généraliser en même temps, je dois demander l'indulgence de l'Académie en plus d'un rapport.

Arrivé il y a peu de jours seulement à ce point d'ample développement de ces attrayantes théories, j'ai dû y interrompre mon ouvrage, voyant qu'il ne me restait pour le faire arriver au terme du 1$^{er}$ juin, que juste le temps de le mettre au net. C'est pourquoi avant tout il m'a été impossible d'en faire une traduction en français, ce qui, du reste

à l'état actuel de mes connaissances dans cette langue, je n'aurais su faire que d'une façon assez imparfaite.

Cette insuffisance de temps m'a empêché d'épuiser tout le matériel que j'ai trouvé pour cette question intéressante, ainsi que de donner à la rédaction tous ces soins que j'aurais voulu y porter, pour rendre mon ouvrage aussi en fait de forme, plus digne du noble forum, au jugement duquel j'ose le soumettre.

Je prie l'Académie de bien vouloir excuser ces faiblesses et de daigner examiner mon ouvrage tel que je suis forcé à le présenter.

L'auteur
du mémoire portant l'épigraphe: «Rien n'est beau que le vrai, le vrai seul est aimable.»

(Koenigsberg), le 29 mai 1882.

---

Durch die von der Académie des Sciences gestellte Aufgabe „Théorie de la décomposition des nombres entiers en une somme de cinq carrés" angeregt, unternahm ich eine genauere Untersuchung der allgemeinen quadratischen Formen mit ganzzahligen Koeffizienten. Ich ging dabei von dem natürlichen Gedanken aus, daß die Zerlegung einer Zahl in eine Summe von fünf Quadraten in ähnlicher Weise von den quadratischen Formen mit vier Variablen abhängen würde, wie bekanntlich die Zerlegung einer Zahl in eine Summe von drei Quadraten von den quadratischen Formen mit zwei Variablen abhängt. Diese Untersuchung hat mir in der Tat die gewünschten Resultate über die Zerlegung einer Zahl in eine Summe von fünf Quadraten geliefert. Indessen erscheinen diese Resultate bei der großen Allgemeinheit der von mir gefundenen Sätze nicht überall als das eigentliche Hauptziel der vorliegenden Arbeit; sie stellen vielmehr nur ein Beispiel für die gewonnenen umfangreichen Theorien dar. Wenn daher viele der nachfolgenden Betrachtungen nicht immer unmittelbar auf das Thema der Preisfrage hinweisen, so wage ich dennoch zu hoffen, daß die Akademie nicht der Ansicht sein werde, ich würde mehr gegeben haben, wenn ich weniger gegeben hätte.

Ich teile kurz die bemerkenswertesten Sätze dieser Arbeit mit. — Es sei

$$f = \sum_{i,k=1}^{n} a_{ik} x_i x_k$$

eine quadratische Form mit ganzzahligen Koeffizienten $a_{ik}$ und von einer nicht-verschwindenden Determinante $\Delta$, welche sich durch eine reelle Transformation in eine Summe von $n - I$ positiven und $I$ negativen Qua-

draten transformieren lasse. Die Zahl $I$ heißt der Index der Form $f$. Das System

$$A = \begin{pmatrix} a_{11}, & a_{12}, \ldots, & a_{1n} \\ a_{21}, & a_{22}, \ldots, & a_{2n} \\ \cdot & \cdot \quad \cdot \quad \cdot & \cdot \\ a_{n1}, & a_{n2}, \ldots, & a_{nn} \end{pmatrix}$$

nennen wir das quadratische System der Form $f$. Der größte Teiler aller $h$-reihigen Unterdeterminanten des Systemes $A$ sei $d_{h-1}$, der größte Teiler aller doppelt genommenen unsymmetrischen und einfach genommenen symmetrischen $h$-reihigen Determinanten von $A$ sei gleich $\sigma_h d_{h-1}$. $\sigma_h$ ist gleich 1 oder gleich 2 ($\sigma_n = 1$, $d_{n-1} = (-1)^I \cdot \Delta$). Ist

$$g = \sum_{i,k=1}^{n} b_{ik} y_i y_k$$

eine zweite quadratische Form, welche durch eine ganzzahlige Substitution von der Determinante 1 aus $f$ hervorgeht, so heißt $g$ der Form $f$ äquivalent, und es gelten, wenn der Form $g$ die Zahlen $c_{h-1}$ und $\varrho_h$ [[in derselben Weise wie $d_{h-1}$ und $\sigma_h$ der Form $f$]] angehören, die Beziehungen

$$\sigma_h = \varrho_h, \quad d_{h-1} = c_{h-1}.$$

Wir betrachten hauptsächlich Formen $f$, für welche der größte Teiler der Koeffizienten $a_{ik}$, nämlich $d_0$, gleich 1 ist, sogenannte primitive Formen. Für eine primitive Form setzen wir

$$\begin{aligned} d_1 &= o_1, \\ d_2 &= o_1^{\,2} o_2, \\ &\cdot \quad \cdot \quad \cdot \quad \cdot, \\ d_{n-1} &= o_1^{\,n-1} o_2^{\,n-2} \cdots o_{n-1}. \end{aligned}$$

Die Zahlen $o_h$ und $\sigma_h$ nennen wir die Invarianten der (primitiven) Form $f$. Alle Formen $f$, für welche die $2(n-1)+1$ Zahlen

$$\begin{pmatrix} \sigma_1, & \sigma_2, \ldots, & \sigma_{n-1} \\ o_1, & o_2, \ldots, & o_{n-1} \end{pmatrix}, I$$

gleiche Werte haben, fassen wir in eine Ordnung zusammen. Zwei äquivalente Formen gehören derselben Ordnung an.

Die Existenz einer Ordnung ist (wenn wir $\sigma_0 = 1$, $o_0 = 0$; $\sigma_n = 1$, $o_n = 0$ setzen) an die folgenden Hauptbedingungen gebunden:

I. Die Größen $o_h$ sind ganze Zahlen.

II. Die Zahlen $\sigma_h$ und $\sigma_{h-1} \cdot o_h \cdot \sigma_{h+1}$ sind nicht gleichzeitig durch 2 teilbar ($\sigma_h$ ist relativ prim zu $\sigma_{h-1} \cdot o_h \cdot \sigma_{h+1}$).

III. Die Größen $\frac{\sigma_{h-1}\, o_h}{\sigma_{h+1}}$ und $\frac{\sigma_{h+1}\, o_h}{\sigma_{h-1}}$ sind ganze Zahlen.

Außer diesen Hauptbedingungen besteht im Falle, daß nicht sämtliche $n-1$ Zahlen $\sigma_{h-1}\, o_h\, \sigma_{h+1}$ Quadratzahlen sind, die einzige Nebenbedingung:

Wenn $n \equiv 0 \pmod 2$ und

$$\sigma_1 = 2,\ \sigma_2 = 1, \ldots,\ \sigma_{n-2} = 1,\ \sigma_{n-1} = 2$$

wird, so ist, wenn wir die in den Zahlen $o_h$ aufgehenden Potenzen von 2 gleich $2^{\omega_h}$ setzen,

$$\prod_{j=1}^{\frac{n}{2}} \frac{o_{2j-1}}{2^{\omega_{2j-1}}} \equiv (-1)^{I+\frac{n}{2}} \pmod 4.$$

Im Falle, daß die sämtlichen $n-1$ Zahlen $\sigma_{h-1}\, o_h\, \sigma_{h+1}$ Quadrate sind, treten noch mehrere einfache Nebenbedingungen hinzu. Alle Ordnungen, welche mit den von uns aufgestellten Bedingungen verträglich sind, enthalten wirklich Formenklassen.

Zum Beweise dieser Sätze in betreff der Formenordnungen führen wir den folgenden, sehr fruchtbaren und leicht auf Formen von beliebig hohem Grade auszudehnenden Begriff ein: Eine quadratische Form

$$R = \sum_{i,k=1}^{n} R_{ik}\, x_i\, x_k$$

heißt ein Rest einer Formenklasse $f$ in bezug auf einen Modul $N$, wenn sich in dieser Formenklasse eine Form

$$\Phi = \sum_{i,k=1}^{n} A_{ik}\, x_i\, x_k$$

vorfindet, für welche die sämtlichen Kongruenzen

$$A_{ik} \equiv R_{ik} \pmod N$$

statthaben. — Wir können den Rest $R$ der Formenklasse $f$ so wählen, daß er nach dem Modul $N$ in eine Summe von mehreren Einzelformen mit einer oder zwei Variablen zerfällt, und wir nennen einen Rest $R$, für welchen die Anzahl dieser Einzelformen den größtmöglichen Wert erhält und in welchem die $n$ Variablen in bestimmter Weise geordnet sind, einen Hauptrest der Klasse $f$. Ein Hauptrest $R$ einer Klasse $f$ hängt, wie wir zeigen, nur von den Resten seiner $n$ mittleren*) Koeffizienten ab.

Wir bezeichnen die aus den ersten $h$ Reihen einer Form $f$ gebildeten symmetrischen Unterdeterminanten durch $\sigma_h\, d_{h-1}\, f_h$. Wir können in jeder Formenklasse $f$ eine Form $\varphi$ bestimmen, für welche die Zahlen $\varphi_h$ zu den Zahlen $2\, o_1\, o_2 \ldots o_{n-1} \cdot \varphi_{h-1}\, \varphi_{h+1}$ relativ prim ausfallen. Eine derartige Form heißt eine charakteristische Form der Klasse $f$. Die aus den ersten

*) [[Die $R_{ii}$ werden als mittlere, die $R_{ik}\,(i \neq k)$ als seitliche Koeffizienten einer quadratischen Form $R = \Sigma R_{ik}\, x_i\, x_k$ bezeichnet.]]

$h$ [[Horizontal- und Vertikal-]] Reihen des quadratischen Systems von $\varphi$ gebildete Form $\{\varphi_h\}$ von $h$ Variablen möge den Index $I_h$ besitzen. Die aus den $n+1$ Zahlen

$$I_0 = 0;\quad I_1,\ I_2, \ldots,\ I_{n-1};\quad I_n = I$$

entstehenden Einheiten $\varepsilon_h = (-1)^{I_h}$ stellen die Vorzeichen der Zahlen $\varphi_h$ vor, und es sind mithin die Größen $\varepsilon_h \varphi_h$ positiv.

Zwei Formenklassen $f$ und $g$, welche irgendeinen gleichen Formenrest für einen Modul $N$ besitzen, enthalten lauter gleiche Formenreste für den Modul $N$. Wir nennen zwei derartige Formenklassen kongruent für den Modul $N$. Alle Formenklassen, welche für einen jeden Modul $N$ kongruent sind und welche einen gleichen Index $I$ besitzen, fassen wir in ein Formengenus zusammen. Äquivalente Formen gehören demselben Genus an.

Zwei Formenklassen, welche in einem und demselben Genus enthalten sind, besitzen dieselbe Ordnung.

Für alle charakteristischen Formen $\varphi$ der verschiedenen, in einem Genus $G$ enthaltenen Formenklassen $f$ besitzen,

$\mathfrak{C})$

I. wenn $\sigma_{h-1}\, o_h\, \sigma_{h+1} \equiv 0 \pmod p$ ist und $p$ eine ungerade Primzahl bedeutet, die Einheiten

$$\left(\frac{\varphi_h}{p}\right),$$

II. wenn $\sigma_{h-1}\, o_h\, \sigma_{h+1} \equiv 0 \pmod 4$ ist, die drei Einheiten

$$(-1)^{\frac{\varphi_h - 1}{2}},\quad \left(\frac{\varphi_{h-1}}{\varepsilon_h \varphi_h}\right)\cdot(-1)^{\frac{I_h(I_h-1)}{1\cdot 2}},\quad \left(\frac{\varphi_{h+1}}{\varepsilon_h \varphi_h}\right)\cdot(-1)^{\frac{I_h(I_h+1)}{1\cdot 2}};$$

III. wenn $\sigma_{h-1}\, o_h\, \sigma_{h+1} \equiv 0 \pmod 8$ ist, die Einheiten

$$\left(\frac{2}{\varphi_h}\right)$$

die nämlichen Werte.

Umgekehrt gehören zwei Formen $f$ wirklich stets einem und demselben Genus an, sobald für die charakteristischen Formen $\varphi$ dieser Formenklassen die vorstehenden Einheiten die nämlichen Werte besitzen.

Zwischen den Einheiten $\mathfrak{C})$, die wir die Charaktere des Genus $G$ nennen, bestehen alle diejenigen Bedingungen, welche sich aus den Kongruenzen

k) $$-\sigma_{h-1}\, o_h\, \sigma_{h+1}\cdot \varphi_{h-1}\, \varphi_{h+1} \equiv X_h^{\,2} \pmod{\sigma_h^{\,2}\, \varphi_h}$$

erschließen lassen, also insbesondere die Bedingungen

$$\left\{\left(\frac{\varphi_{h-1}}{\varepsilon_h \varphi_h}\right)\cdot(-1)^{\frac{I_h(I_h-1)}{2}}\right\}\cdot\left\{\left(\frac{\varphi_{h+1}}{\varepsilon_h \varphi_h}\right)\cdot(-1)^{\frac{I_h(I_h+1)}{2}}\right\}$$

$$= \left(\frac{\sigma_{h-1}\, 2^{\omega_h}\, \sigma_{h+1}}{\varphi_h}\right)\cdot(-1)^{\frac{\varphi_h-1}{2}\cdot\frac{e_h+1}{2}}\cdot\left(\frac{\varphi_h}{e_h}\right)$$

$$[o_h = 2^{\omega_h}\cdot e_h,\ e_h \equiv 1 \pmod 2]$$

und

$$\prod_{h=1}^{n-1}\left(\frac{\sigma_{h-1}2^{\omega_h}\sigma_{h+1}}{\varphi_h}\right)\cdot(-1)^{\sum_{h=1}^{n-1}\frac{\varphi_h-1}{2}\cdot\frac{e_h+1}{2}}\prod_{h=1}^{n-1}\left(\frac{\varphi_h}{e_h}\right)$$

$$=(-1)^{\left[\frac{I}{2}\right]}\cdot(-1)^{\frac{\varphi_0-1}{2}\cdot\frac{\varphi_1-1}{2}+\frac{\varphi_1-1}{2}\cdot\frac{\varphi_2-1}{2}+\cdots+\frac{\varphi_{n-1}-1}{2}\cdot\frac{\varphi_n-1}{2}}$$

Wenn die Charaktere eines Genus $G$ allen Bedingungen genügen, welche sich aus den Kongruenzen k) ergeben, so besitzt das Genus $G$ wirklich Formen. (Insbesondere folgt aus diesem Umstand die bis jetzt noch nicht bewiesene Tatsache, daß die definiten positiven Formen von der Determinante 1 und einer Variablenzahl größer oder gleich 8 mehr als eine Formenklasse enthalten.)

Es sei $f$ eine primitive Form. Wir bezeichnen die $(n-1)$-reihigen Minoren der Determinante $\Delta$ in bekannter Weise durch

$$\frac{\partial\Delta}{\partial a_{ik}}=A_{ik},$$

und wir setzen

$$A_{ik}=(-1)^I d_{n-2}\cdot a'_{n-i+1,\,n-k+1}.$$

Die Form

$$f'=\sum_{i,k=1}^{n}a'_{ik}x'_ix'_k$$

nennen wir dann die der Form $f$ adjungierte Form.

Ist eine Form $f'$ einer Form $f$ adjungiert, so ist auch der Form $f'$ die Form $f$ adjungiert.

Besitzt die Form $f$ eine Ordnung

$$\begin{pmatrix}\sigma_1, & \sigma_2, & \ldots, & \sigma_{n-1}\\ o_1, & o_2, & \ldots, & o_{n-1}\end{pmatrix},\ I,$$

so besitzt ihre adjungierte Form $f'$ eine Ordnung

$$\begin{pmatrix}\sigma_1', & \sigma_2', & \ldots, & \sigma'_{n-1}\\ o_1', & o_2', & \ldots, & o'_{n-1}\end{pmatrix},\ I',$$

für welche

$$\sigma_h'=\sigma_{n-h},\quad o_h'=o_{n-h};\quad I'=I$$

wird. — Der charakteristischen Form $\varphi'$ der Klasse $f'$ ist eine charakteristische Form $\varphi$ der Klasse $f$ adjungiert, für welche die Beziehungen

$$\varphi_h'=\varphi_{n-h}\cdot(-1)^I\quad\text{und}\quad I_h'+I_{n-h}=I$$

bestehen. Infolge dieser Beziehungen können die Charaktere und demgemäß die Genera adjungierter Formen sofort auseinander hergeleitet werden.

Die Beweise der soeben entwickelten Sätze bilden den Inhalt des ersten Teiles der vorliegenden Arbeit, in welchem alle quadratischen

Formen $f$ von nicht-verschwindender Determinante ohne Beschränkung behandelt sind.

In dem zweiten Teile dieser Arbeit betrachte ich die Darstellung von Formen mit niedrigerer Variablenzahl durch Formen mit höherer Variablenzahl und insbesondere die Darstellung von ganzen Zahlen durch Formen. Ich verallgemeinere und erweitere die von Gauß über Darstellungen von Zahlen und binären Formen durch ternäre Formen gegebenen Sätze und betrachte im weiteren Verlaufe der Untersuchung besonders definite positive Formen. Zuletzt wende ich mich zu einer Bestimmung des Maßes einiger besonders ausgezeichneter definiter Genera und gewinne dadurch die verlangten Sätze über die Darstellung einer Zahl durch eine Summe von fünf Quadraten. Schließlich füge ich noch ohne Beweis ein sehr allgemeines Theorem in betreff des Maßes eines definiten positiven Genus von $n$ Variablen hinzu, aus welchem sich sämtliche von Eisenstein in diesem Gebiete aufgestellten Sätze als spezielle Fälle ergeben. — Infolge der Nähe des von der Akademie gegebenen Termines mußte ich mich in dem zweiten Teile an manchen Stellen mit kurzen Andeutungen begnügen, und es sind dadurch einige Mängel in der Redaktion desselben veranlaßt, welche ich zu entschuldigen bitte.

# Erster Teil.

## Über die Reste quadratischer Formen.

### Kap. I. Klassen quadratischer Formen. — Index, Invarianten und Ordnung einer Form.

Wir betrachten quadratische Formen $f = \sum_{i,k=1}^{n} a_{ik} x_i x_k = \{a_{ik}\}$, welche ganzzahlige Koeffizienten und eine nicht-verschwindende Determinante besitzen.

Die Anwendung einer beliebigen ganzzahligen Substitution

$$S: \qquad x_i = \sum_{l} s_i^l y_l \qquad (i, l = 1, 2, \ldots, n)$$

auf die quadratische Form $f$ führt zu einer neuen Form

$$g = \overline{S} f S = \sum_{l,m=1}^{n} b_{lm} y_l y_m .^{*})$$

Die Form $g$ heißt in der Form $f$ *enthalten.*

*) Wir bezeichnen mit $\overline{S}$ dasjenige System, das sich aus $S$ durch Vertauschung der Horizontal- und Vertikalreihen ableitet.

*Wir beschäftigen uns insbesondere mit Substitutionen S, deren Determinante* $= 1$ *ist.* In diesem Falle kann die Form $g$ durch eine zweite ganzzahlige Substitution von der Determinante 1 in $f$ zurückgeführt werden. Für $|S| = 1$ ist daher sowohl $g$ in $f$ als $f$ in $g$ enthalten. Mit Rücksicht auf diese ihre gegenseitige Beziehung nennen wir alsdann $f$ und $g$ *äquivalent.* Um die Äquivalenz zweier Formen auszudrücken, bedienen wir uns mitunter des Zeichens $\sim$ $(f \sim g)$. Es besteht der Fundamentalsatz:

A. *Wenn zwei Formen einer dritten äquivalent sind, so sind sie untereinander äquivalent.*

Denn ist

$$g_1 = \overline{S}_1 f S_1, \quad g_2 = \overline{S}_2 f S_2,$$

so haben wir

$$g_1 = (\overline{S_2^{-1} S_1}) \cdot g_2 \cdot (S_2^{-1} S_1) \sim g_2 .$$

Die Gesamtheit aller einer bestimmten Form $f$ äquivalenten Formen nennen wir eine *Formenklasse.* Infolge des Satzes A. sind zwei Formen, welche derselben Klasse angehören, untereinander äquivalent, während zwei Formen aus verschiedenen Klassen nicht äquivalent sind. Wir werden eine gegebene Form selten als besonderes, durch seine $\frac{n(n+1)}{2}$ Koeffizienten bestimmtes Individuum betrachten; meistens wird sie uns nur als ein *Repräsentant* der ihr entsprechenden Formenklasse gelten.

Eine jede Form $f$ von nicht-verschwindender Determinante kann, wie man weiß, durch eine lineare Transformation mit reellen (keineswegs immer ganzzahligen) Koeffizienten in eine Summe von $n$ zum Teil positiven, zum Teil negativen Quadraten übergeführt werden. Es mögen bei irgendeiner solchen Transformation $I = I(f)$ Quadrate das negative und $n - I$ Quadrate das positive Vorzeichen erhalten; alsdann ist nach einem bekannten Satze die Zahl $I$ für die Form $f$ charakteristisch, und es wird eine jede Darstellung von $f$ durch eine Summe von $n$ positiven oder negativen Quadraten die Gestalt

$$f = -\sum_{h=1}^{I} \mathsf{X}_h^2 + \sum_{h=1}^{n-I} \Xi_h^2$$

erhalten. Wir gewinnen hieraus leicht für die algebraische Äquivalenz zweier Formen $f$ und $g$ die Bedingung

$$I(f) = I(g).$$

Die Zahl $I(f)$ heißt der *Index* der Form $f$.

Die Form $g = \{b_{lm}\}$ sei in der Form $f = \{a_{ik}\}$ vermittels einer Substitution $S = \{s_i^l\}$ enthalten. Wir bezeichnen die Subdeterminanten $h^{\text{ten}}$ Grades

$$\begin{vmatrix} a_{i_1 k_1}, a_{i_1 k_2}, \ldots, a_{i_1 k_h} \\ a_{i_2 k_1}, a_{i_2 k_2}, \ldots, a_{i_2 k_h} \\ \cdots\cdots\cdots \\ a_{i_h k_1}, a_{i_h k_2}, \ldots, a_{i_h k_h} \end{vmatrix}, \quad \begin{vmatrix} b_{l_1 m_1}, b_{l_1 m_2}, \ldots, b_{l_1 m_h} \\ b_{l_2 m_1}, b_{l_2 m_2}, \ldots, b_{l_2 m_h} \\ \cdots\cdots\cdots \\ b_{l_h m_1}, b_{l_h m_2}, \ldots, b_{l_h m_h} \end{vmatrix}, \quad \begin{vmatrix} s_{i_1}^{l_1}, s_{i_1}^{l_2}, \ldots, s_{i_1}^{l_h} \\ s_{i_2}^{l_1}, s_{i_2}^{l_2}, \ldots, s_{i_2}^{l_h} \\ \cdots\cdots\cdots \\ s_{i_h}^{l_1}, s_{i_h}^{l_2}, \ldots, s_{i_h}^{l_h} \end{vmatrix}$$

durch

$$A\binom{i_1, i_2, \ldots, i_h}{k_1, k_2, \ldots, k_h}, \quad B\binom{l_1, l_2, \ldots, l_h}{m_1, m_2, \ldots, m_h}, \quad S^{\binom{l_1, l_2, \ldots, l_h}{i_1, i_2, \ldots, i_h}},$$

oder, wofern die besondere Wahl der $h$ Horizontal- und Vertikalreihen unter den gegebenen $n$ Horizontal- und Vertikalreihen gleichgültig ist, durch

$$A_h, \quad B_h, \quad S_h \text{ oder } S_h^0.$$

Wir gebrauchen für die symmetrischen $A_h$ und $B_h$ die Buchstaben $F_h$ und $G_h$ und für die unsymmetrischen $A_h$ und $B_h$ die Buchstaben $P_h$ und $Q_h$.

Nach einem bekannten Determinantensatze ist

$$B\binom{l_1, l_2, \ldots, l_h}{m_1, m_2, \ldots, m_h} = \frac{\sum_{i,k}^{1,n} A\binom{i_1, i_2, \ldots, i_h}{k_1, k_2, \ldots, k_h} S^{\binom{l_1, l_2, \ldots, l_h}{i_1, i_2, \ldots, i_h}} S^{\binom{m_1, m_2, \ldots, m_h}{k_1, k_2, \ldots, k_h}}}{(1 \cdot 2 \cdots h) \cdot (1 \cdot 2 \cdots h)}.$$

In der Entwicklung eines $G_h$ sehen wir die $F_h$ mit einem Faktor $S_h^2$, die $P_h$ mit einem Faktor $2 S_h S_h^0$ behaftet; in der Entwicklung eines $Q_h$ weisen sowohl die $F_h$ als die $P_h$ einen Faktor $S_h S_h^0$ auf:

$$G_h = \sum F_h S_h^2 \quad + \sum P_h \, 2 S_h S_h^0,$$
$$Q_h = \sum F_h S_h S_h^0 + \sum P_h \, S_h S_h^0.$$

Wir schließen aus dieser Bemerkung, daß der größte Divisor der $F_h$, $P_h$ in dem größten Divisor der $G_h$, $Q_h$ und der größte Divisor der $F_h$, $2 P_h$ in dem größten Divisor der $G_h$, $2 Q_h$ aufgeht.

Den größten positiven Divisor der $F_h$, $P_h$ setzen wir gleich $d_{h-1}$ und den größten positiven Divisor der $F_h$, $2 P_h$ gleich $\sigma_h d_{h-1}$. Die Zahl $\sigma_h$ stellt uns dann den größten Divisor der Größen $\frac{F_h}{d_{h-1}}$, $2 \frac{P_h}{d_{h-1}}$ vor. Da der größte Teiler der $\frac{F_h}{d_{h-1}}$, $\frac{P_h}{d_{h-1}}$ die Einheit ist, so nimmt $\sigma_h$ den Wert 1 an, wenn von den Zahlen $\frac{F_h}{d_{h-1}}$ wenigstens eine ungerade ist, und $\sigma_h$ wird gleich 2, wenn alle $\frac{F_h}{d_{h-1}}$ gerade ausfallen. Die Zahl $d_{n-1}$ ist dem absoluten Wert der Determinante $|a_{ik}|$ gleich, und es wird daher

$$|a_{ik}| = (-1)^I \cdot d_{n-1};$$

ferner ist $\sigma_n = 1$.

Enthält nicht nur die Form $f$ die Form $g$, sondern auch die Form $g$ die Form $f$, sind also $f$ und $g$ äquivalent, so geht einerseits der größte positive Divisor $d_{h-1}(f)$ der $F_h$, $P_h$ in dem größten positiven Divisor $d_{h-1}(g)$ der $G_h$, $Q_h$ und der größte positive Divisor $\sigma_h(f)\,d_{h-1}(f)$ der $F_h$, $2\,P_h$ in dem größten positiven Divisor $\sigma_h(g)\,d_{h-1}(g)$ der $G_h$, $2\,Q_h$ auf; andererseits geht auch $d_{h-1}(g)$ in $d_{h-1}(f)$ und $\sigma_h(g)\,d_{h-1}(g)$ in $\sigma_h(f)\,d_{h-1}(f)$ auf. Für äquivalente Formen $f$ und $g$ bestehen demnach die Beziehungen

$$\sigma_h(f) = \sigma_h(g); \quad d_{h-1}(f) = d_{h-1}(g). \tag{1}$$

Wir nennen eine Form $f = \{a_{ik}\}$ *primitiv in bezug auf einen Modul* $N$, sobald die Koeffizienten $a_{ik}$ einen größten gemeinsamen Teiler besitzen, welcher zu $N$ relativ prim ist. Eine beliebige Form ist nach dieser Definition primitiv in bezug auf einen Modul $N$, sobald sie primitiv in bezug auf alle in $N$ enthaltenen Primfaktoren ist.

In dem Folgenden werden wir fast ausschließlich Formen $f$ betrachten, für welche der größte Teiler der $a_{ik}$, nämlich $d_0$, gleich 1 wird und die wir kurz *primitive* Formen heißen. Eine nicht-primitive Form $f = \{a_{ik}\}$ ist dem Produkt aus der Zahl $d_0$ und der primitiven Form $\frac{f}{d_0} = \left\{\frac{a_{ik}}{d_0}\right\}$ gleich.

Jeder primitiven Form $f$ entsprechen $2(n-1)$ Zahlen

$$\sigma_1, \sigma_2, \ldots, \sigma_{n-2}, \sigma_{n-1},$$
$$d_1, d_2, \ldots, d_{n-2}, d_{n-1}.$$

Wir führen ferner $n-1$ Größen $o_h$ durch die Gleichungen

$$\begin{aligned} d_1 &= o_1, \\ d_2 &= o_1^2 o_2, \\ &\cdots\cdots\cdots \\ d_{n-1} &= o_1^{n-1} o_2^{n-2} \ldots o_{n-1}, \end{aligned} \qquad o_h = \frac{d_h\, d_{h-2}}{d_{h-1}^2}$$

ein.

Gemäß den Formeln (1) sind alle $o_h$ und $\sigma_h$ *Invarianten* der Klasse $f$. Wir unterscheiden die $o_h$ und $\sigma_h$ als Invarianten $o(f)$ und Invarianten $\sigma(f)$.

Alle Formenklassen, welche die Größen $\sigma_h$, $o_h$ gemein haben und für welche der Index $I(f)$ denselben Wert $I$ annimmt, fassen wir in eine *Ordnung*

$$\begin{pmatrix} \sigma_1, \sigma_2, \ldots, \sigma_{n-2}, \sigma_{n-1} \\ o_1, o_2, \ldots, o_{n-2}, o_{n-1} \end{pmatrix}, \quad I$$

zusammen.

Unsere nächste Aufgabe wird in der Aufsuchung der für die Existenz einer Ordnung erforderlichen Bedingungen bestehen.

## Kap. II. Formenreste. — Die Invarianten $o(f)$ sind ganze Zahlen.

Bei allen Fragen, in welchen es sich weniger um die numerischen Werte der Unterdeterminanten einer Form $f = \{a_{ik}\}$ als um die Teilbarkeit dieser Unterdeterminanten durch gegebene Zahlen $N$ handelt, kommen für uns offenbar nur die Reste der $\frac{n(n+1)}{2}$ Koeffizienten $a_{ik}$ nach den Moduln $N$ in Betracht, und wir können daher diese Koeffizienten durch beliebige, ihnen nach den Moduln $N$ kongruente Zahlen ersetzen.

Eine Form $R = \{R_{ik}\}$ heißt *ein Rest der Formenklasse $f$ in bezug auf den Modul $N$*, sobald in dieser Klasse eine Form $\Phi = \{A_{ik}\}$ anzutreffen ist, für welche sämtliche Kongruenzen

$$A_{ik} \equiv R_{ik} \pmod{N}$$

erfüllt sind. Wir gebrauchen alsdann die Bezeichnung

$$\Phi \equiv \{R_{ik}\} \pmod{N}.$$

Wir werden für eine jede Formenklasse eine Reihe besonders ausgezeichneter Formenreste bestimmen, zu denen man gelangt, wenn man auf eine beliebige Form der betreffenden Klasse Substitutionen von der folgenden Art ausübt:

$$S^{\pm 1}_{(i,k)}: \qquad x_i = x_i',\ x_k = \pm x_i' + x_k', \qquad x_h = x_h'\ (h \neq i, k)$$

und

$$P_{(l,m)}: \qquad x_l = x_m',\ x_m = -x_l', \qquad x_h = x_h'\ (h \neq l, m)$$

und

$$x_i = x_i' + \sum_{(k>i)} s_k x_k', \qquad x_h = x_h'\ (h \neq i).$$

Zunächst verschafft uns die Betrachtung der so gewonnenen Klassenreste den Satz:

B. *Für eine jede Ordnung, welche wirklich Formen enthält, werden die Invarianten $o_h$ ganze Zahlen.*

Wir können diesen Satz auch in der folgenden veränderten Weise aussprechen:

C. Ist die quadratische Form $f = \{a_{ik}\}$ in bezug auf eine Primzahl $q$ primitiv und sind die höchsten, in den Zahlen $d_1, d_2, \ldots, d_{n-1}$ der Form $f$ aufgehenden Potenzen von $q$ resp. $q^{\partial_1}, q^{\partial_2}, \ldots, q^{\partial_{n-1}}$, so fallen die Größen $\omega_h = (\partial_h - \partial_{h-1}) - (\partial_{h-1} - \partial_{h-2})$ nicht negativ aus.

Die $\omega_h$ sind mit den $\partial_h$ durch die Gleichungen

$$\partial_h = h\omega_1 + (h-1)\omega_2 + \cdots + \omega_h$$

verbunden. Die Potenzen $q^{\omega_h}$ sind offenbar diejenigen Potenzen von $q$, welche in den Größen $o_h = \frac{d_h}{d_{h-1}} : \frac{d_{h-1}}{d_{h-2}}$ aufgehen; sobald also keine der

Zahlen $\omega_h$ negativ ist, müssen die $o_h$ sämtlich ganze Zahlen sein. Die erste von 0 verschiedene der Zahlen $\omega_h$ ist gewiß positiv, da sie gleich der ersten von 0 verschiedenen Zahl $\partial_h$ ist. — Wir werden die Gültigkeit des Satzes C. für Formen von $n$ Variablen aus der Annahme der Gültigkeit desselben für Formen von weniger als $n$ Variablen herleiten. Hierdurch ist dann zugleich seine Allgemeingültigkeit dargetan; denn da dieser Satz für $n = 1$ gewiß richtig ist — in diesem Fall existiert überhaupt kein $o_h$ —, wird er sofort auch für $n = 2, 3, \ldots, n$ erwiesen sein.

Für den Beweis des Satzes C. genügt die Einführung besonderer Formenreste für Moduln, welche Potenzen der Primzahl $q$ sind. Nur müssen wir den Fall einer ungeraden Primzahlpotenz $q^t = p^t$ von dem Falle einer Potenz $q^t = 2^t$ sondern.*)

I. Wir beginnen mit dem Falle einer ungeraden Primzahl $q = p$.

1. Jede in bezug auf $p$ primitive Form $f = \sum_{i,k=1}^{n} a_{ik} x_i x_k$ von $n$ Variablen ist einer Form

$$f_{(1)} \equiv \begin{pmatrix} \alpha, & 0, & \ldots, & 0 \\ 0, & p^{\omega_1} a_{11}^{(1)}, & \ldots, & p^{\omega_1} a_{1,n-1}^{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ 0, & p^{\omega_1} a_{n-1,1}^{(1)}, & \ldots, & p^{\omega_1} a_{n-1,n-1}^{(1)} \end{pmatrix} \pmod{p^t},$$

$$f_{(1)} \equiv \alpha \xi^2 + p^{\omega_1} \sum_{i,k=1}^{n-1} a_{ik}^{(1)} x_i^{(1)} x_k^{(1)} \pmod{p^t}$$

äquivalent, deren erster Koeffizient $\alpha$ zu $p$ relativ prim ist, während $f^{(1)} = \sum_{i,k=1}^{n-1} a_{ik}^{(1)} x_i^{(1)} x_k^{(1)}$ eine in bezug auf $p$ primitive Form von $n-1$ Variablen darstellt.

Beweis: Wenn $f$ in bezug auf $p$ primitiv ist, so sind die Zahlen $a_{ii}$, $2a_{ik}$ gewiß nicht alle durch $p$ teilbar. Ebenso können auch die Zahlen $a_{ii}$, $a_{ii} \pm 2a_{ik} + a_{kk}$ nicht alle durch $p$ teilbar sein; denn sie haben offenbar denselben größten gemeinsamen Teiler wie die $a_{ii}$, $2a_{ik}$. Sollten also die Koeffizienten $a_{ii}$ der Form $f$ sämtlich durch $p$ teilbar sein, so würde eine der Zahlen $a_{ii} \pm 2a_{ik} + a_{kk}$ zu $p$ relativ prim sein, und wir dürften auf $f$ nur eine Substitution $S_{(i,k)}^{\pm 1}$ anwenden, um in der veränderten Form die zu $p$ prime Zahl $a_{ii} \pm 2a_{ik} + a_{kk}$ als einen mittleren Koeffizienten zu erzielen. Wir können demnach von $f$ voraussetzen, daß es einen durch $p$ nicht teilbaren Koeffizienten $a_{ii}$ besitzt. Durch Ausübung

*) Wir bezeichnen stets durch $q$ eine beliebige und durch $p$ eine ungerade Primzahl.

einer Substitution $P_{(1,t)}$ verwandelt sich $f$ alsdann in einen Repräsentanten

$$\hat{f}_{(1)} \equiv \begin{pmatrix} \alpha, & E_1, & \ldots, & E_{n-1} \\ E_1, & c_{11}, & \ldots, & c_{1,n-1} \\ \cdot & \cdot & \cdot & \cdot \\ E_{n-1}, & c_{n-1,1}, & \ldots, & c_{n-1,n-1} \end{pmatrix} \pmod{p^t},$$

in welchem $\alpha$ zu $p$ prim ist. Auf $\hat{f}_{(1)}$ wenden wir die Substitution

$$S^{(1)} = \begin{pmatrix} 1, & K_1, & K_2, & \ldots, & K_{n-1} \\ & 1, & 0, & \ldots, & 0 \\ & & \cdot & \cdot & \cdot \\ & & & & 1 \end{pmatrix}$$

an. Eine solche Substitution läßt $\alpha$ ungeändert, während sie $E_h$ in

$$E_h + \alpha K_h$$

verwandelt. Bestimmen wir daher die $K_h$ aus den gewiß lösbaren Kongruenzen

$$E_h + \alpha K_h \equiv 0 \pmod{p^t},$$

so geht die Form $\hat{f}_{(1)}$ durch die Substitution $S^{(1)}$ in eine Form

$$f_{(1)} \equiv \begin{pmatrix} \alpha, & 0, & \ldots, & 0 \\ 0, & r_{11}^{(1)}, & \ldots, & r_{1,n-1}^{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ 0, & r_{n-1,1}^{(1)}, & \ldots, & r_{n-1,n-1}^{(1)} \end{pmatrix} \pmod{p^t}$$

über. Ist $t > \omega_1$, so wird $p^{\omega_1}$ die größte Potenz von $p$ sein, welche in allen $r_{ik}^{(1)}$ enthalten ist, und wenn wir $r_{ik}^{(1)} = p^{\omega_1} a_{ik}^{(1)}$ setzen, so haben wir die angegebene Gestalt von $f_{(1)}$ erlangt.

2. Der Form $f(\sim f_{(1)})$ teilten wir $n-1$ Zahlen $d_1, d_2, \ldots, d_{n-1}$ zu; $n-2$ Zahlen $d_1^{(1)}, d_2^{(1)}, \ldots, d_{n-2}^{(1)}$ von ähnlicher Bedeutung gehören der Form $f^{(1)} = \{a_{ik}^{(1)}\}$ an. Es bezeichnet $d_{h-1}^{(1)}$ für $f^{(1)}$ den größten gemeinsamen Teiler aller $A_h^{(1)}$. Es seien die höchsten in $d_1^{(1)}, d_2^{(1)}, \ldots, d_{n-2}^{(1)}$ aufgehenden Potenzen von $p$ resp. $p^{\partial_1^{(1)}}, p^{\partial_2^{(1)}}, \ldots, p^{\partial_{n-2}^{(1)}}$. Für die Form $f_{(1)}$ gelten die Kongruenzen

$$A_{(1)^h} \equiv \alpha \cdot p^{(h-1)\omega_1} A_{h-1}^{(1)}, \quad p^{h\omega_1} A_h^{(1)}, \quad 0 \pmod{p^t}.$$

Wir wollen den Modul $p^t$ größer gewählt denken als die größte der Zahlen $p^{\partial_1}, p^{\partial_2}, \ldots, p^{\partial_{n-1}}$. Dann muß die höchste Potenz von $p$, welche in allen $A_{(1)^h}$ aufgeht, d. i. die Potenz $p^{\partial_{h-1}}$, zugleich die höchste Potenz von $p$ sein, welche in allen $\alpha \cdot p^{(h-1)\omega_1} A_{h-1}^{(1)}, p^{h\omega_1} A_h^{(1)}$ aufgeht. Die höchste Potenz von $p$, welche in den $\alpha \cdot p^{(h-1)\omega_1} A_{h-1}^{(1)}$ aufgeht, ist offenbar $p^{(h-1)\omega_1 + \partial_{h-2}^{(1)}}$; die höchste Potenz von $p$, welche in den $p^{h\omega_1} A_h^{(1)}$ aufgeht,

ist $p^{h\omega_1+\partial_{h-1}^{(1)}}$. Demnach wird $\partial_{h-1}$ mit der kleineren der Zahlen

$$(h-1)\omega_1+\partial_{h-2}^{(1)},\quad h\omega_1+\partial_{h-1}^{(1)}$$

übereinstimmen müssen.

Setzen wir jetzt die Gültigkeit unseres Satzes C. für die Form $f^{(1)}$ von $n-1$ Variablen voraus. Dann werden die durch die Gleichungen

$$\partial_h^{(1)}=h\omega_1^{(1)}+(h-1)\omega_2^{(1)}+\cdots+\omega_h^{(1)}$$

bestimmten Größen $\omega_h^{(1)}$ positiv oder gleich Null ausfallen, und es wird

$$\partial_{h-2}^{(1)}\leqq\partial_{h-1}^{(1)},$$

woraus sich wegen $\omega_1\geqq 0$

$$(h-1)\omega_1+\partial_{h-2}^{(1)}\leqq h\omega_1+\partial_{h-1}^{(1)}$$

ergibt. Von diesen beiden Zahlen ist also jedenfalls die erste nicht größer als die zweite, und wir erhalten folglich

$$\partial_{h-1}=(h-1)\omega_1+\partial_{h-2}^{(1)},$$

oder, wenn wir

$$\omega_{h-1}^{(1)}=\omega_h\quad(h>1)$$

setzen und die Gleichungen ausführlicher schreiben:

$$\partial_h=h\omega_1+(h-1)\omega_2+\cdots+\omega_h,\quad \omega_h\geqq 0.$$

II. Wenn die Primzahl $q=2$ ist, unterscheiden wir die Fälle $\sigma_1=1$ und $\sigma_1=2$.

$\sigma_1=1$. — 1. Jede in bezug auf 2 primitive Form $f=\sum_{i,k=1}^{n}a_{ik}x_ix_k$, welche eine Invariante $\sigma_1=1$ besitzt, ist einer Form

$$f_{(1)}\equiv\begin{pmatrix}\alpha, & 0, & \ldots, & 0\\ 0, & 2^{\omega_1}a_{11}^{(1)}, & \ldots, & 2^{\omega_1}a_{1,n-1}^{(1)}\\ \cdot & \cdot & \cdot & \cdot\\ 0, & 2^{\omega_1}a_{n-1,1}^{(1)}, & \ldots, & 2^{\omega_1}a_{n-1,n-1}^{(1)}\end{pmatrix}\pmod{2^t},$$

$$f_{(1)}\equiv\alpha\xi^2+2^{\omega_1}\sum_{i,k=1}^{n-1}a_{ik}^{(1)}x_i^{(1)}x_k^{(1)}\pmod{2^t}$$

äquivalent, in welcher der erste Koeffizient $\alpha$ ungerade ist, während $f^{(1)}=\sum_{i,k=1}^{n-1}a_{ik}^{(1)}x_i^{(1)}x_k^{(1)}$ eine in bezug auf 2 primitive Form vorstellt, welche im Falle $\omega_1=0$ eine erste Invariante $\sigma$ gleich 1 besitzt.

Beweis: Es befinden sich, wenn $\sigma_1=1$ ist, unter den Koeffizienten $a_{ii}$ ungerade Größen. Außerdem muß es im Falle $\omega_1=0$ eine ungerade Determinante $a_{kk}a_{hh}-a_{kh}^2$ geben. Denn wären alle diese Determinanten gerade, so würden die Kongruenzen

$$a_{kk}a_{hh} \equiv a_{kh}^2 \pmod 2$$

und

$$a_{kh}^2 a_{k_0h_0}^2 \equiv a_{kk}a_{hh}a_{k_0k_0}a_{h_0h_0} \equiv a_{kh_0}^2 a_{k_0h}^2 \pmod 2$$

gelten, und folglich wären auch alle Determinanten $a_{kh}a_{k_0h_0} - a_{kh_0}a_{k_0h}$ gerade, so daß die höchste Potenz von 2, welche in allen diesen Determinanten enthalten ist, nämlich $2^{\omega_1}$, nicht gleich 1 sein könnte. Wir können im Falle $\omega_1 = 0$ ferner voraussetzen, daß die Form $f$ für denselben Index $i$ sowohl ein ungerades $a_{ii}$ als auch eine ungerade Determinante $a_{ii}a_{hh} - a_{ih}^2$ besitzt. Denn wären in $f$ die Indizes $i$ der ungeraden $a_{ii}$ alle von den Indizes $k, h$ der ungeraden Zahlen $a_{kk}a_{hh} - a_{kh}^2$ verschieden, so hätte man gleichzeitig

$$\begin{gathered} a_{ii} \equiv 1, \quad a_{kk}a_{hh} - a_{kh}^2 \equiv 1; \\ a_{ii}a_{kk} - a_{ik}^2 \equiv 0, \quad a_{ii}a_{hh} - a_{ih}^2 \equiv 0, \quad a_{kk} \equiv 0, \quad a_{hh} \equiv 0, \end{gathered} \pmod 2,$$

d. h.

$$\begin{pmatrix} a_{ii}, & a_{ik}, & a_{ih} \\ a_{ki}, & a_{kk}, & a_{kh} \\ a_{hi}, & a_{hk}, & a_{hh} \end{pmatrix} \equiv \begin{pmatrix} 1, & 0, & 0 \\ 0, & 0, & 1 \\ 0, & 1, & 0 \end{pmatrix} \pmod 2.$$

Durch Ausübung einer Substitution $S_{(i,k)}^{\pm 1}$ auf $f$ erhielte man eine Form, in welcher die Zahlen $a_{ii}$ und $a_{ii}a_{hh} - a_{ih}^2$ bzw. durch die Zahlen

$$a_{ii} \pm 2a_{ik} + a_{kk}$$

und

$$(a_{ii}a_{hh} - a_{ih}^2) \pm 2(a_{ik}a_{hh} - a_{ih}a_{kh}) + (a_{kk}a_{hh} - a_{kh}^2)$$

ersetzt erscheinen, welche beide ungerade sind. Vermittels einer Substitution $P_{(1,i)}$ können wir jetzt $f$ in eine Form

$$\widehat{f}_{(1)} \equiv \begin{pmatrix} \alpha, & E_1, & \dots, & E_{n-1} \\ E_1, & c_{11}, & \dots, & c_{1,n-1} \\ \dots & \dots & \dots & \dots \\ E_{n-1}, & c_{n-1,1}, & \dots, & c_{n-1,n-1} \end{pmatrix} \pmod{2^t}$$

transformieren, in welcher $\alpha$ und im Falle $\omega_1 = 0$ auch eine der Größen $\alpha c_{ii} - E_i^2$ ungerade ist. Diese Form $\widehat{f}_{(1)}$ geht durch eine Substitution

$$S^{(1)} = \begin{pmatrix} 1, & K_1, & K_2, & \dots, & K_{n-1} \\ & 1, & 0, & \dots, & 0 \\ & & \dots & \dots & \dots \\ & & & & 1 \end{pmatrix},$$

in welcher die $K_h$ den Kongruenzen

$$E_h + \alpha K_h \equiv 0 \pmod{2^t}$$

genügen, in eine Form

$$f_{(1)} \equiv \begin{pmatrix} \alpha, & 0, & \ldots, & 0 \\ 0, & 2^{\omega_1} a_{11}^{(1)}, & \ldots, & 2^{\omega_1} a_{1,n-1}^{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ 0, & 2^{\omega_1} a_{n-1,1}^{(1)}, & \ldots, & 2^{\omega_1} a_{n-1,n-1}^{(1)} \end{pmatrix} \pmod{2^t}$$

über, in welcher $f^{(1)} = \{a_{ik}^{(1)}\}$ in bezug auf 2 primitiv ist. Hierin fällt, wenn $\omega_1 = 0$ ist, eine der Größen $\alpha 2^{\omega_1} a_{ii}^{(1)} \equiv a_{ii}^{(1)} \pmod 2$ ungerade aus, und folglich wird in diesem Falle die Form $f^{(1)}$ eine erste Invariante $\sigma$ gleich 1 besitzen.

2. An die Form $f_{(1)}$ können wir sofort dieselben Schlüsse anknüpfen wie in Absatz I, 2. dieses Kapitels, und wir gelangen, indem wir der Form $f^{(1)}$ $n-2$ Zahlen $\omega_h^{(1)}$ zuerteilen und den Modul $2^t$ größer als die größte der Zahlen $2^{\partial_1}, 2^{\partial_2}, \ldots, 2^{\partial_{n-1}}$ wählen, in derselben Weise zum gewünschten Ziele:

$$\omega_{h-1}^{(1)} = \omega_h \quad (h>1), \quad \partial_h = h\omega_1 + (h-1)\omega_2 + \cdots + \omega_h, \quad \omega_h \geqq 0.$$

$\sigma_1 = 2$. — 1. Jede in bezug auf 2 primitive Form $f = \sum_{i,k=1}^{n} a_{ik} x_i x_k$, welche eine Invariante $\sigma_1 = 2$ besitzt, ist einer Form

$$f_{(2)} \equiv \begin{pmatrix} 2\alpha, & \mathfrak{A}, & 0, & \ldots, & 0 \\ \mathfrak{A}, & 2\tilde{\alpha}, & 0, & \ldots, & 0 \\ 0, & 0, & 2^{\omega_2} a_{11}^{(2)}, & \ldots, & 2^{\omega_2} a_{1,n-2}^{(2)} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & 2^{\omega_2} a_{n-2,1}^{(2)}, & \ldots, & 2^{\omega_2} a_{n-2,n-2}^{(2)} \end{pmatrix} \pmod{2^t},$$

$$f_{(2)} \equiv 2(\alpha\xi^2 + \mathfrak{A}\xi\tilde{\xi} + \tilde{\alpha}\tilde{\xi}^2) + 2^{\omega_2} \sum_{i,k=1}^{n-2} a_{ik}^{(2)} x_i^{(2)} x_k^{(2)} \pmod{2^t}$$

äquivalent, in welcher die Zahl $\mathfrak{A}$ einen willkürlich gewählten ungeraden Wert hat*), $\alpha$ ungerade und $f^{(2)} = \sum_{i,k=1}^{n-2} a_{ik}^{(2)} x_i^{(2)} x_k^{(2)}$ eine in bezug auf 2 primitive Form ist.

Beweis: Wegen $\sigma_1 = 2$ müssen alle $a_{ii}$ gerade ausfallen, während mindestens eines der $a_{ik}$ $(i \neq k)$ ungerade wird. Wir können annehmen, daß gleichzeitig $a_{ik} \equiv 1 \pmod 2$ und $a_{ii} \equiv 2 \pmod 4$ gilt. Sind nämlich für ein ungerades $a_{ik}$ gleichzeitig $a_{ii}$ und $a_{kk}$ durch 4 teilbar, so genügt es, auf $f$ eine Substitution $S_{(i,k)}^{\pm 1}$ anzuwenden, um zu erzielen, daß der Koeffizient $a_{ii}$ durch die Zahl $a_{ii} \pm 2a_{ik} + a_{kk} \equiv 2 \pmod 4$ ersetzt wird.

*) Wir bezeichnen mit $\mathfrak{A}$ stets ungerade Zahlen, welche willkürlich gewählt werden dürfen.

Durch eine geeignete Umstellung der Variablen mittels der Substitutionen $P_{(1,i)}$, $P_{(2,k)}$ können wir daher der Form $f$ die Gestalt verleihen

$$\hat{f}_{(2)} \equiv \begin{pmatrix} 2\alpha, & A, & E_1, & \ldots, & E_{n-2} \\ A, & 2a, & \tilde{E}_1, & \ldots, & \tilde{E}_{n-2} \\ E_1, & \tilde{E}_1, & c_{11}, & \ldots, & c_{1,n-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ E_{n-2}, & \tilde{E}_{n-2}, & c_{n-2,1}, & \ldots, & c_{n-2,n-2} \end{pmatrix} \pmod{2^t},$$

in welcher $\alpha$ und $A$ ungerade sind. Auf dieses $\hat{f}_{(2)}$ wenden wir eine Substitution

$$S^{(2)} = \begin{pmatrix} 1, & M, & K_1, & K_2, & \ldots, & K_{n-2} \\ & 1, & \tilde{K}_1, & \tilde{K}_2, & \ldots, & \tilde{K}_{n-2} \\ & & 1, & 0, & \ldots, & 0 \\ & & & \cdot & \cdot & \cdot \\ & & & & & 1 \end{pmatrix}$$

an. Eine solche Substitution läßt $2\alpha$ ungeändert, während dieselbe

$$A \quad \text{in} \quad A + 2\alpha M$$

und

$$E_h \quad \text{in} \quad E_h + 2\alpha K_h + A\tilde{K}_h,$$

$$\tilde{E}_h \quad \text{in} \quad (\tilde{E}_h + AK_h + 2a\tilde{K}_h) + M(E_h + 2\alpha K_h + A\tilde{K}_h)$$

verwandelt. Bezeichnet $\mathfrak{A}$ eine beliebige ungerade Größe, so hat die Kongruenz

$$2\alpha M \equiv \mathfrak{A} - A \pmod{2^t}$$

stets Lösungen, und ebenso sind wegen

$$4\alpha a - A^2 \equiv 1 \pmod 2$$

die Kongruenzen

$$\begin{aligned} E_h + 2\alpha K_h + A\tilde{K}_h &\equiv 0 \\ \tilde{E}_h + AK_h + 2a\tilde{K}_h &\equiv 0 \end{aligned} \pmod{2^t}$$

auflösbar; sie ergeben

$$K_h \equiv \frac{A\tilde{E}_h - 2\alpha E_h}{4\alpha a - A^2}, \quad \tilde{K}_h \equiv \frac{AE_h - 2\alpha\tilde{E}_h}{4\alpha a - A^2} \pmod{2^t}.$$

Mit Hilfe der so bestimmten Werte der $M$, $K_h$, $\tilde{K}_h$ geht daher die Form $\hat{f}_{(2)}$ in eine Form $f_{(2)}$ von der gewünschten Art über. In dieser Form $f_{(2)}$ müssen wegen $\sigma_1 = 2$ die sämtlichen $2^{\omega_2} a_{ii}^{(2)}$ gerade sein. Folglich sind im Falle $\omega_2 = 0$ auch alle $a_{ii}^{(2)}$ gerade, und die Form $f^{(2)} = \{a_{ik}^{(2)}\}$ wird in diesem Falle eine erste Invariante $\sigma$ gleich 2 besitzen.

2. Die höchste Potenz von 2, welche allen $A_{(2)^h}$ der Form $f_{(2)}\,(\sim f)$ gemeinsam ist, d. h. die höchste in $d_{h-1}$ aufgehende Potenz von 2, sei wieder $2^{\partial_h - 1}$, die höchste in den $A_h^{(2)}$ der Form $f^{(2)}$ aufgehende Potenz

von 2 sei $2^{\partial_{h-1}^{(2)}}$. Wir bemerken, daß die Potenz $2^{\partial_1}$, welche unter anderem in $4\alpha\tilde{\alpha} - \mathfrak{A}^2$ aufgehen muß, offenbar gleich 1 ist und daß infolgedessen $\partial_1 = 0$ wird. Wir haben für die Größen $A_{(2)^h}$ die Kongruenzen

$$A_{(2)^h} \equiv (4\alpha\tilde{\alpha} - \mathfrak{A}^2)2^{(h-2)\omega_2}A_{h-2}^{(2)}, \quad \begin{matrix} 2\alpha \cdot 2^{(h-1)\omega_2}A_{h-1}^{(2)}, \\ \mathfrak{A} \cdot 2^{(h-1)\omega_2}A_{h-1}^{(2)}, \\ 2\tilde{\alpha} \cdot 2^{(h-1)\omega_2}A_{h-1}^{(2)}, \end{matrix} \quad 2^{h\omega_2}A_h^{(2)}, \quad 0 \pmod{2^t}.$$

Wählen wir nun $t$ größer als die größte der Zahlen $\partial_1, \partial_2, \ldots, \partial_{n-1}$, so wird die höchste in allen $A_{(2)^h}$ aufgehende Potenz von 2, nämlich $2^{\partial_h - 1}$, zugleich die höchste Potenz von 2 sein, welche allen auf der rechten Seite der vorstehenden Kongruenzen befindlichen Größen gemeinsam ist. Es ist aber die höchste in allen

$$(4\alpha\tilde{\alpha} - \mathfrak{A}^2)2^{(h-2)\omega_2}A_{h-2}^{(2)},$$

in allen

$$2\alpha \cdot 2^{(h-1)\omega_2}A_{h-1}^{(2)}, \quad \mathfrak{A} \cdot 2^{(h-1)\omega_2}A_{h-1}^{(2)}, \quad 2\tilde{\alpha} \cdot 2^{(h-1)\omega_2}A_{h-1}^{(2)},$$

in allen

$$2^{h\omega_2}A_h^{(2)}$$

aufgehende Potenz von 2 resp.

$$2^{(h-2)\omega_2 + \partial_{h-3}^{(2)}}, \quad 2^{(h-1)\omega_2 + \partial_{h-2}^{(2)}}, \quad 2^{h\omega_2 + \partial_{h-1}^{(2)}}.$$

Sonach wird $\partial_{h-1}$ mit der kleinsten der drei Zahlen

$$(h-2)\omega_2 + \partial_{h-3}^{(2)}, \quad (h-1)\omega_2 + \partial_{h-2}^{(2)}, \quad h\omega_2 + \partial_{h-1}^{(2)}$$

übereinstimmen müssen.

Nehmen wir jetzt an, für die Form $f^{(2)} = \{a_{ik}^{(2)}\}$ von $n-2$ Variablen wäre der Satz C. richtig, so werden die Größen $\omega_h^{(2)}$, welche durch die Gleichungen

$$\partial_h^{(2)} = h\omega_1^{(2)} + (h-1)\omega_2^{(2)} + \cdots + \omega_h^{(2)}$$

bestimmt sind, nicht negativ ausfallen, und es müssen demnach die Ungleichungen

$$\partial_{h-3}^{(2)} \leqq \partial_{h-2}^{(2)} \leqq \partial_{h-1}^{(2)}$$

statthaben. Umsomehr gelten dann wegen $\omega_2 \geqq 0$ die weiteren Ungleichungen

$$(h-2)\omega_2 + \partial_{h-3}^{(2)} \leqq (h-1)\omega_2 + \partial_{h-2}^{(2)} \leqq h\omega_2 + \partial_{h-1}^{(2)}.$$

Mithin wird $\partial_{h-1}$, welches der kleinsten der vorstehenden drei Zahlen gleich werden soll, gleich $(h-2)\omega_2 + \partial_{h-3}^{(2)}$ werden, und wir erhalten in diesem letzten Fall, indem wir

$$\omega_1 = \partial_1 = 0 \qquad \text{und} \qquad \omega_{h-2}^{(2)} = \omega_h \qquad (h > 2)$$

setzen, gleichfalls

$$\partial_h = h\omega_1 + (h-1)\omega_2 + \cdots + \omega_h, \quad \omega_h \geqq 0.$$

---

Wir führen jetzt einige Bezeichnungen ein, welche für die folgenden Untersuchungen wichtig sind. Wir setzen für eine jede Primzahl $q$ ($q = p$ oder $= 2$)

$$v_1 = \omega_1,\ v_2 = \omega_1 + \omega_2,\ \ldots,\ v_{n-1} = \omega_1 + \omega_2 + \cdots + \omega_{n-1},$$

woraus sich sofort

$$\partial_1 = v_1,\ \partial_2 = v_1 + v_2,\ \ldots,\ \partial_{n-1} = v_1 + v_2 + \cdots + v_{n-1}$$

ergibt. Die Potenzen $q^{v_h}$ sind diejenigen Potenzen von $q$, welche in den Größen $\frac{d_h}{d_{h-1}}$ aufgehen. Ferner nehmen wir an, von den $n-1$ Zahlen $\omega_h$ seien im ganzen $\lambda - 1\,(1 \leqq \lambda \leqq n)$ von Null verschieden, nämlich die Größen

$$(\vartheta_0 = 0) \qquad \omega_{\vartheta_1},\ \omega_{\vartheta_2},\ \ldots,\ \omega_{\vartheta_{\lambda-2}},\ \omega_{\vartheta_{\lambda-1}}, \qquad (\vartheta_\lambda = n)$$

und wir bestimmen $\lambda$ Zahlen $\varkappa_k$ durch die Gleichungen

$$\vartheta_1 = \varkappa_1,\ \vartheta_2 = \varkappa_1 + \varkappa_2,\ \ldots,\ n = \vartheta_\lambda = \varkappa_1 + \varkappa_2 + \cdots + \varkappa_\lambda,\ (\varkappa_k = \vartheta_k - \vartheta_{k-1}).$$

So oft der besondere Wert der Primzahl $q$ hervorgehoben werden soll, werden wir den sämtlichen Größen $\omega, v, \partial, \lambda$ die Zahl $q$ in Klammern beifügen.

## Kap. III. **Hauptformenreste und Hauptrepräsentanten für einen Modul $N$.**

I. Der Modul $N$ möge ein Produkt von $c_0$ zueinander relativ primen Zahlen $N_1, N_2, \ldots, N_{c_0}$ sein. Wir beweisen den folgenden Satz:

Wenn in der Klasse $f$ sich $c_0$ Formen $R_c = \overline{S}_c f S_c\,(c = 1, 2, \ldots, c_0)$ vorfinden, welche die Reste

$$R_c \equiv \{r_{ik}^{(c)}\} \pmod{N_c} \qquad (c = 1, 2, \ldots, c_0)$$

besitzen, so können wir einen Repräsentanten

$$R = \overline{S} f S \equiv \{r_{ik}\} \pmod{N}$$

dieser Klasse angeben, welcher den Kongruenzen

$$r_{ik} \equiv r_{ik}^{(c)} \pmod{N_c} \qquad (c = 1, 2, \ldots, c_0)$$

genügt.

Beweis: $S_c$ läßt sich als Substitution von der Determinante 1 bekanntlich in eine gewisse Anzahl Teilsubstitutionen von der Art

$$x_i = x_i' + M_c x_k',\quad x_k = x_k',\quad x_h = x_h' \quad (h \neq i, k)$$

zerlegen. Führen wir in diesen Teilsubstitutionen anstatt der $M_c$ beliebige andere Zahlen $M_c^*$ ein, welche gleichzeitig den Kongruenzen

$$M_c^* \equiv M_c \pmod{N_c} \qquad \text{und} \qquad M_c^* \equiv 0 \left(\mathrm{mod}\ \frac{N}{N_c}\right)$$

genügen, und setzen die so veränderten Teilsubstitutionen in genau derselben Weise, wie sie durch Zerlegung von $S_c$ entstanden sind, zu einer neuen Substitution $S_c^*$ zusammen, so wird offenbar

$$S_c^* \equiv S_c \pmod{N_c}, \qquad S_c^* \equiv \begin{pmatrix} 1, 0, \ldots, 0 \\ 0, 1, \ldots, 0 \\ \cdots\cdots\cdots \\ 0, 0, \ldots, 1 \end{pmatrix} \left(\mathrm{mod}\ \frac{N}{N_c}\right).$$

Es folgt also

$$R_c^* = \overline{S_c^*} f S_c^* \equiv R_c \pmod{N_c}, \qquad R_c^* \equiv f \left(\mathrm{mod}\ \frac{N}{N_c}\right),$$

und für die Form

$$R = \overline{S_1^* S_2^* \ldots S_{c_0}^*} \cdot f \cdot S_1^* S_2^* \ldots S_{c_0}^*$$

haben wir in der Tat

$$R \equiv \overline{S_c^*} f S_c^* \equiv R_c \pmod{N_c}.$$

Dieser Satz zeigt uns die Möglichkeit, vermittels der Formenreste nach den Teilmoduln $N_1, N_2, \ldots, N_{c_0}$ einen Formenrest nach dem zusammengesetzten Modul $N$ zu finden. Insbesondere können die $N_c$ die verschiedenen in $N$ enthaltenen Primzahlpotenzen bedeuten; wir kommen daher mit der Bestimmung ausgezeichneter Formenreste für Primzahlpotenzen $q^t$ als Moduln aus. Es genügt auch völlig, wenn wir nur Moduln $q^t$ oberhalb gewisser Grenzen betrachten; denn es ist ein jeder Formenrest für einen Modul $N$ zugleich Formenrest für alle in $N$ aufgehenden Moduln $N_0$; insbesondere wird daher ein jeder Formenrest für einen Modul $q^t$ auch Formenrest für alle Moduln $q^{t_0}$ sein, welche kleiner als $q^t$ sind.

Durch eine wiederholte Anwendung der in Kap. II gewonnenen Sätze erkennen wir, daß eine jede Formenklasse für jeden Modul $q^t$ Reste besitzt, welche sich als Summen von Formen mit einer oder mit zwei Variablen darstellen.

II. ($q = p$.) *Aus der Klasse äquivalenter Formen, welcher die zu $p$ primitive Form $f$ angehört, kann ein Repräsentant*

$$\varphi \equiv \begin{pmatrix} \alpha_1, & & & & \\ & p^{\omega_1}\alpha_2, & & & \\ & & p^{\omega_1+\omega_2}\alpha_3, & & \\ & & & \cdots, & \\ & & & & p^{\omega_1+\omega_2+\cdots+\omega_{n-1}}\alpha_n \end{pmatrix} \pmod{p^t}$$

*ausgewählt werden, in welchem die $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ sämtlich zu $p$ relativ prime Zahlen sind.*

Wir beweisen diesen Satz, welcher für $n = 1$ selbstverständlich ist, vermittels eines Schlusses von $n-1$ auf $n$. Angenommen dieser Satz sei für Formen mit $n-1$ Variablen bereits bewiesen, so können wir die Form $p^{\omega_1} f^{(1)}$ des Repräsentanten

$$f_{(1)} \equiv \alpha\xi^2 + p^{\omega_1} f^{(1)} \pmod{p^t}$$

durch eine gewisse Substitution in eine andere überführen, deren Rest nach dem Modul $p^t$ aus lauter eingliedrigen Einzelformen besteht. Durch

dieselbe Substitution geht dann $f_{(1)}$ in eine Form von der Gestalt $\varphi$ über, womit unser Satz bewiesen ist.

Mit Benutzung der am Ende von Kap. II eingeführten Bezeichnungen können wir für $\varphi$ schreiben

$$\varphi \equiv \varphi_{(1)} + \varphi_{(2)} + \cdots + \varphi_{(\lambda)} \equiv \sum_{k=1}^{\lambda} \varphi_{(k)} \pmod{p^t},$$

$$\varphi_{(k)} \equiv p^{v_{\vartheta_k - 1}} \sum_{s=1}^{x_k} \alpha_s^{(k)} \xi_s^{(k)} \xi_s^{(k)} \pmod{p^t}, \qquad (\alpha_s^{(k)} = \alpha_{\vartheta_{k-1}+s})$$

$$0 < v_{\vartheta_1} < v_{\vartheta_2} < \cdots < v_{\vartheta_{\lambda-1}}.$$

($q = 2$.) 1. Es sei $f$ eine in bezug auf 2 primitive Form, und es mögen die $\varkappa_1 - 1$ ersten Zahlen $\omega_h$ dieser Form gleich Null sein ($\omega_1 = 0$, $\omega_2 = 0, \ldots, \omega_{\varkappa_1 - 1} = 0$), während die $\varkappa_1^{\text{te}}$ Zahl $\omega_{\varkappa_1}$ ($1 \leqq \varkappa_1 \leqq n$) die erste der Zahlen $\omega_h$ sei, welche nicht verschwindet. Wenn dann die Invariante $\sigma_1$ von $f$ gleich 2 ist, muß $\varkappa_1 \equiv 0 \pmod 2$ sein. Wir können, falls $\sigma_1 = 1$ ist, statt $f$ einen Repräsentanten

$$f_{(\varkappa_1)} \equiv \begin{pmatrix} \alpha_1^{(1)}, & & & & & \\ & \alpha_2^{(1)}, & & & & \\ & & \ldots, & & & \\ & & & \alpha_{\varkappa_1}^{(1)}, & & \\ & & & & 2^{\omega_{\varkappa_1}} a_{11}^{(\varkappa_1)}, \ldots, & 2^{\omega_{\varkappa_1}} a_{1,n-\varkappa_1}^{(\varkappa_1)} \\ & & & & \ldots\ldots\ldots & \\ & & & & 2^{\omega_{\varkappa_1}} a_{n-\varkappa_1,1}^{(\varkappa_1)}, \ldots, & 2^{\omega_{\varkappa_1}} a_{n-\varkappa_1,n-\varkappa_1}^{(\varkappa_1)} \end{pmatrix} \pmod{2^t}$$

einführen, in welchem die Zahlen $\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_{\varkappa_1}^{(1)}$ ungerade sind und $f^{(\varkappa_1)} = \sum_{i,k=1}^{n-\varkappa_1} a_{ik}^{(\varkappa_1)} x_i^{(\varkappa_1)} x_k^{(\varkappa_1)}$ eine in bezug auf 2 primitive Form vorstellt; falls aber $\sigma_1 = 2$ ist, einen Repräsentanten

$$f_{(\varkappa_1)} \equiv \begin{pmatrix} 2\alpha_1^{(1)}, \mathfrak{A}_1^{(1)} & & & & & \\ \mathfrak{A}_1^{(1)}, 2\tilde{\alpha}_1^{(1)}, & & & & & \\ & 2\alpha_2^{(1)}, \mathfrak{A}_2^{(1)} & & & & \\ & \mathfrak{A}_2^{(1)}, 2\tilde{\alpha}_2^{(1)}, & & & & \\ & & \ldots, & & & \\ & & & 2\alpha_{\frac{\varkappa_1}{2}}^{(1)}, \mathfrak{A}_{\frac{\varkappa_1}{2}}^{(1)} & & \\ & & & \mathfrak{A}_{\frac{\varkappa_1}{2}}^{(1)}, 2\tilde{\alpha}_{\frac{\varkappa_1}{2}}^{(1)}, & & \\ & & & & 2^{\omega_{\varkappa_1}} a_{11}^{(\varkappa_1)}, \ldots, & 2^{\omega_{\varkappa_1}} a_{1,n-\varkappa_1}^{(\varkappa_1)} \\ & & & & \ldots\ldots\ldots & \\ & & & & 2^{\omega_{\varkappa_1}} a_{n-\varkappa_1,1}^{(\varkappa_1)}, \ldots, & 2^{\omega_{\varkappa_1}} a_{n-\varkappa_1,n-\varkappa_1}^{(\varkappa_1)} \end{pmatrix} \pmod{2^t},$$

in welchem die Zahlen $\mathfrak{A}_1^{(1)}, \mathfrak{A}_2^{(1)}, \ldots, \mathfrak{A}_{\frac{\varkappa_1}{2}}^{(1)}$ beliebige ungerade Werte haben, die Zahlen $\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_{\frac{\varkappa_1}{2}}^{(1)}$ ungerade sind und die Form $f^{(\varkappa_1)} = \sum_{i,k=1}^{n-\varkappa_1} a_{ik}^{(\varkappa_1)} x_i^{(\varkappa_1)} x_k^{(\varkappa_1)}$ in bezug auf 2 primitiv ist.

Beweis. Wir hatten in Kap. II für $f$ im Falle $\sigma_1 = 1$ zunächst einen Repräsentanten

$$f_{(1)} \equiv \alpha \xi^2 + 2^{\omega_1} f^{(1)} \pmod{2^t} \qquad [\alpha \equiv 1 \pmod 2]$$

gewonnen, in welchem $f^{(1)} = \{a_{ik}^{(1)}\}$ eine in bezug auf 2 primitive Form vorstellte, die, falls $\omega_1 = 0$ war, eine erste Invariante $\sigma$ gleich 1 besaß, und im Falle $\sigma_1 = 2$ einen Repräsentanten

$$f_{(2)} \equiv 2(\alpha \xi^2 + \mathfrak{A} \xi \tilde{\xi} + \tilde{\alpha} \tilde{\xi}^2) + 2^{\omega_2} f^{(2)} \pmod{2^t},$$
$$[\alpha \equiv 1,\ \mathfrak{A} \equiv 1 \pmod 2],$$

in welchem $f^{(2)} = \{a_{ik}^{(2)}\}$ eine in bezug auf 2 primitive Form vorstellte, die, falls $\omega_2 = 0$ war, eine erste Invariante $\sigma$ gleich 2 besaß.

Im Falle $\varkappa_1 \leqq \sigma_1$ haben diese Repräsentanten die Gestalt, welche unser Satz verlangt. Wenn $\varkappa_1 > \sigma_1$ wird und mithin $\omega_{\sigma_1} = 0$ ist, besitzt die Form $f^{(\sigma_1)} = \{a_{ik}^{(\sigma_1)}\}$ ebenso wie $f$ eine erste Invariante $\sigma$ gleich $\sigma_1$. Nun ergibt sich aus den in Kap. II bewiesenen Gleichungen $\omega_{h-\sigma_1}^{(\sigma_1)} = \omega_h (h > \sigma_1)$ infolge unserer Annahme über die Größen $\omega_h$ sofort

$$\omega_1^{(\sigma_1)} = 0,\ \omega_2^{(\sigma_1)} = 0,\ \ldots,\ \omega_{\varkappa_1-\sigma_1-1}^{(\sigma_1)} = 0,\ \omega_{\varkappa_1-\sigma_1}^{(\sigma_1)} = \omega_{\varkappa_1} > 0.$$

Folglich wird für die Form $f^{(\sigma_1)}$ schon die $(\varkappa_1 - \sigma_1)^{\text{te}}$ der Zahlen $\omega_h^{(\sigma_1)}$ größer als Null ausfallen. Machen wir also die Annahme, unser Satz wäre bereits bewiesen, sobald die erste von 0 verschiedene Zahl $\omega$ sich unter den $\varkappa_1 - \sigma_1$ ersten dieser Zahlen befindet, so werden wir $2^{\omega_{\sigma_1}} f^{(\sigma_1)}$ durch gewisse Substitutionen in eine Form überführen können, welche die in dem Satze geforderte Gestalt besitzt, und wenn $\sigma_1(f^{(\sigma_1)}) = \sigma_1(f) = 2$ ist, wird $\varkappa_1 - \sigma_1 = \varkappa_1 - 2 \equiv 0 \pmod 2$ sein. Dieselben Substitutionen transformieren alsdann die Form $f_{(\sigma_1)}$ in Formen von der Gestalt $f_{(\varkappa_1)}$, und im Falle $\sigma_1 = 2$ wird $\varkappa_1 \equiv 0 \pmod 2$ sein. Hierdurch ist unser Satz für den Fall bewiesen, daß eine der $\varkappa_1$ ersten Zahlen $\omega$ nicht verschwindet.

In derselben Weise, in welcher der Form $f$ die $n-1$ Zahlen $\omega_h$ entsprechen, gehören zur Form $f^{(\varkappa_1)}$ gewisse $n - \varkappa_1 - 1$ Größen $\omega_h^{(\varkappa_1)}$; durch eine wiederholte Anwendung der Relationen

$$\omega_{h-\sigma_1}^{(\sigma_1)} = \omega_h \qquad (h > \sigma_1)$$

finden wir leicht

$$\omega_h = \omega_{h-\varkappa_1}^{(\varkappa_1)} \qquad (h > \varkappa_1).$$

2. *Eine in bezug auf 2 primitive Form $f$ kann in einen Repräsentanten*

$$\varphi \equiv \varphi_{(1)} + \varphi_{(2)} + \cdots + \varphi_{(\lambda)} \equiv \sum_{k=1}^{\lambda} \varphi_{(k)} \pmod{2^t}$$

*transformiert werden, in welchem die Formen* $\varphi_{(k)}$ *Reste von der Gestalt*

$$(\mathrm{R_I}) \qquad \varphi_{(k)} \equiv 2^{v_{\vartheta_k - 1}} \sum_{s=1}^{\varkappa_k} \alpha_s^{(k)} \xi_s^{(k)} \xi_s^{(k)} \pmod{2^t}$$

*oder im Falle* $\varkappa_k \equiv 0 \pmod 2$ *auch von der Gestalt*

$$(\mathrm{R_{II}}) \quad \varphi_{(k)} \equiv 2^{v_{\vartheta_{k-1}+1}} \sum_{s=1}^{\frac{1}{2}\varkappa_k} (\alpha_s^{(k)} \xi_s^{(k)} \xi_s^{(k)} + \mathfrak{A}_s^{(k)} \xi_s^{(k)} \tilde{\xi}_s^{(k)} + \tilde{\alpha}_s^{(k)} \tilde{\xi}_s^{(k)} \tilde{\xi}_s^{(k)}) \pmod{2^t}$$

*besitzen.*

$$0 < v_{\vartheta_1} < v_{\vartheta_2} < \cdots < v_{\vartheta_{\lambda-1}}.$$

Für ein $\lambda = 1$ erhellt die Richtigkeit dieses Satzes schon aus den in 1. gewonnenen Resultaten. Infolge der Relationen $\omega_h = \omega_{h-\varkappa_1}^{(\varkappa_1)}$ $(h > \varkappa_1)$ erkennen wir, daß, wenn $\lambda - 1$ von den $n - 1$ zur Form $f_{(\varkappa_1)}$ gehörigen Zahlen $\omega_h$ nicht verschwinden, alsdann von den $n - \varkappa_1 - 1$ zur Form $f^{(\varkappa_1)}$ gehörigen Zahlen $\omega_h^{(\varkappa_1)}$ nur $\lambda - 2$ größer als Null ausfallen. Machen wir daher die Annahme, unser Satz wäre richtig für alle Formen, welche nur $\lambda - 2$ von 0 verschiedene Zahlen $\omega$ besitzen, so wird die Form $2^{\omega_{\varkappa_1}} f^{(\varkappa_1)}$ für den Modul $2^t$ durch eine gewisse Substitution auf eine Gestalt gebracht werden können, wie sie unser Satz verlangt. Durch die nämliche Substitution geht dann die Form $f_{(\varkappa_1)}$ wirklich in eine Form von der Gestalt $\varphi$ über.

III. Jeder Formenrest einer Klasse $f$, welcher die Gestalt $\varphi \pmod{q^t}$ hat, soll ein *Hauptformenrest* [[oder Hauptrest]] dieser Klasse für den Modul $q^t$ heißen, während jede Form der Klasse $f$, welche einen Hauptrest für den Modul $q^t$ liefert, ein *Hauptrepräsentant* dieser Klasse für den Modul $q^t$ genannt werden möge.

In einem Hauptrest für einen Modul $q^t$ sind entweder die seitlichen Koeffizienten alle $\equiv 0 \pmod{q^t}$ oder können im Falle $q = 2$ zum Teil (mit einer leichten Einschränkung) nach dem Modul $q^t$ willkürlich gewählt werden. Jedenfalls kann man es in zwei verschiedenen Hauptresten für einen Modul $q^t$ stets ohne Mühe erreichen, daß diese Koeffizienten modulo $q^t$ dieselben Werte annehmen, und auf diese Weise wird ein Hauptrest für einen Modul $q^t$ nur von den Resten seiner $n$ mittleren Koeffizienten abhängen.

Eine Form $\varphi$ soll ein Hauptrepräsentant für einen zusammengesetzten Modul $N$ und ihr Rest soll ein Hauptrest für den Modul $N$ heißen, sobald $\varphi$ einen Hauptrepräsentanten für alle in $N$ aufgehenden Primzahlpotenzen vorstellt.

## Kap. IV. **Bedingungen für die Existenz einer Ordnung $O$.**

Mit Hilfe der Hauptformenreste für Moduln $2^t$ können wir jetzt Bedingungen finden, an welche die Existenz einer Ordnung

$$\begin{pmatrix} \sigma_1, & \sigma_2, & \ldots, & \sigma_{n-1} \\ o_1, & o_2, & \ldots, & o_{n-1} \end{pmatrix}, \qquad I$$

gebunden ist.

I. Es sei $f$ eine in bezug auf 2 primitive Form.

1. Wir gehen zunächst von den in Kap. III aufgestellten Repräsentanten

$$f_{(\varkappa_1)} \equiv \Phi_{(1)} + 2^{\omega_{\varkappa_1}} f^{(\varkappa_1)} \pmod{2^t}$$

aus, in denen $\Phi_{(1)}$ und $f^{(\varkappa_1)}$ in bezug auf 2 primitive Formen bezeichnen. Die $\varkappa_1 - 1$ Zahlen $\sigma$ der Form $\Phi_{(1)}$ setzen wir gleich $\varrho_1^{(1)}, \varrho_2^{(1)}, \ldots, \varrho_{\varkappa_1-1}^{(1)}$ und die $n - \varkappa_1 - 1$ Zahlen $\sigma$ der Form $f^{(\varkappa_1)}$ gleich $\sigma_1^{(\varkappa_1)}, \sigma_2^{(\varkappa_1)}, \ldots, \sigma_{n-\varkappa_1-1}^{(\varkappa_1)}$. Ferner bezeichnen wir die $h$-reihigen Unterdeterminanten der Formen $f_{(\varkappa_1)}, f^{(\varkappa_1)}, \Phi_{(1)}$ durch $F_{(h;\varkappa_1)}$ oder $P_{(h;\varkappa_1)}$, $F_h^{(\varkappa_1)}$ oder $P_h^{(\varkappa_1)}$, $D_h^{(1)}$ oder $M_h^{(1)}$, indem wir einen Buchstaben $F, D$ anwenden, sobald die betreffende Unterdeterminante symmetrisch ist, dagegen einen Buchstaben $P, M$, sobald dieselbe unsymmetrisch ausfällt. Die aus den ersten $\varkappa_1$ Reihen von $f_{(\varkappa_1)}$ gebildete symmetrische Determinante möge gleich $|\Phi_{(1)}|$ sein.

Für die Invarianten $\sigma$ der Form $f_{(\varkappa_1)}$ $(\sim f)$ erhalten wir die folgenden Sätze.

*Es ist*

$$\sigma_h = \varrho_h^{(1)} \quad (h < \varkappa_1).$$

In der Tat zeigen die Kongruenzen

$$\begin{matrix} F_{(h;\varkappa_1)} \equiv D_h^{(1)}, & 0 \\ P_{(h;\varkappa_1)} \equiv M_h^{(1)}, & 0 \end{matrix} \pmod 2 \quad [h < \varkappa_1],$$

daß einerseits die höchsten Potenzen von 2, welche in allen Zahlen $F_{(h;\varkappa_1)}$, $P_{(h;\varkappa_1)}$ und in allen $D_h^{(1)}$, $M_h^{(1)}$ aufgehen, und andererseits die größten Potenzen, welche in allen $F_{(h;\varkappa_1)}$, $2P_{(h;\varkappa_1)}$ und in allen $D_h^{(1)}$, $2M_h^{(1)}$ aufgehen, nach dem Modul 2 kongruent sind. Da nun die höchste in den Größen $F_{(h;\varkappa_1)}$, $P_{(h;\varkappa_1)}$ $(h < \varkappa_1)$ aufgehende Potenz von 2, nämlich $2^{\partial_{h-1}}$, infolge unserer Annahme über die Zahlen $\omega_h$ $(h < \varkappa_1)$ gleich 1 ist, so wird die höchste in allen $D_h^{(1)}$, $M_h^{(1)}$ aufgehende Potenz von 2 ebenfalls gleich 1 sein müssen, und die höchsten Potenzen von 2, welche in den $F_{(h;\varkappa_1)}$, $2P_{(h;\varkappa_1)}$ und in den $D_h^{(1)}$, $2M_h^{(1)}$ aufgehen, werden die Werte $\sigma_h$ und $\varrho_h^{(1)}$ haben. Jetzt müssen die Größen $\sigma_h$ und $\varrho_h^{(1)}$, da sie nach dem Modul 2 kongruent und zugleich $\leqq 2$ sind, identisch sein, und es ergibt sich demnach in der Tat $\sigma_h = \varrho_h^{(1)}$ für $h < \varkappa_1$.

*Es ist*

$$\sigma_h = 1 \quad (h = \varkappa_1).$$

Die Größe $\sigma_{\varkappa_1}$ muß in der Zahl $|\Phi_{(1)}|$ aufgehen; diese ist aber offenbar ungerade, mithin ist $\sigma_{\varkappa_1}=1$.

*Es ist*

$$\sigma_h=\sigma_{h-\varkappa_1}^{(\varkappa_1)} \quad (h>\varkappa_1).$$

Für die Determinanten $F_{(h;\varkappa_1)}$ und $P_{(h;\varkappa_1)}$ $(h>\varkappa_1)$ bestehen die Kongruenzen

$$F_{(h;\varkappa_1)}\equiv|\Phi_{(1)}|\,2^{(h-\varkappa_1)\omega_{\varkappa_1}}F_{h-\varkappa_1}^{(\varkappa_1)},\quad 2^{(h-h_0)\omega_{\varkappa_1}}D_{h_0}^{(1)}F_{h-h_0}^{(\varkappa_1)},\quad 0 \pmod{2^t},$$

$$P_{(h;\varkappa_1)}\equiv|\Phi_{(1)}|\,2^{(h-\varkappa_1)\omega_{\varkappa_1}}P_{h-\varkappa_1}^{(\varkappa_1)},\quad \begin{cases} 2^{(h-h_0)\omega_{\varkappa_1}}D_{h_0}^{(1)}P_{h-h_0}^{(\varkappa_1)},\\ 2^{(h-h_0)\omega_{\varkappa_1}}M_{h_0}^{(1)}F_{h-h_0}^{(\varkappa_1)},\\ 2^{(h-h_0)\omega_{\varkappa_1}}M_{h_0}^{(1)}P_{h-h_0}^{(\varkappa_1)}, \end{cases} \quad 0 \pmod{2^t}$$

$$(h_0=0,\ 1,\ \ldots,\ \varkappa_1-1;\ D_0^{(1)}=1,\ M_0^{(1)}=0).$$

Machen wir jetzt die Annahme $t>\partial_{h-1}+1$, so wird eine jede Größenreihe, welche nach dem Modul $2^t$ mit der Größenreihe $F_{(h;\varkappa_1)}$, $2P_{(h;\varkappa_1)}$ übereinstimmt, durch eben dieselbe Potenz $\sigma_h 2^{\partial_h-1}$ und durch keine höhere Potenz von 2 teilbar sein wie die Größenreihe $F_{(h;\varkappa_1)}$, $2P_{(h;\varkappa_1)}$. Nun ist die höchste Potenz von 2, welche den Zahlen

$$|\Phi_{(1)}|\,2^{(h-\varkappa_1)\omega_{\varkappa_1}}F_{h-\varkappa_1}^{(\varkappa_1)},\quad 2\,|\Phi_{(1)}|\,2^{(h-\varkappa_1)\omega_{\varkappa_1}}P_{h-\varkappa_1}^{(\varkappa_1)}$$

gemeinsam ist, gleich

$$\sigma_{h-\varkappa_1}^{(\varkappa_1)}\cdot 2^{(h-\varkappa_1)\omega_{\varkappa_1}+\partial_{h-\varkappa_1}^{(\varkappa_1)}-1},$$

während in den Zahlen

$$2^{(h-h_0)\omega_{\varkappa_1}}D_{h_0}^{(1)}F_{h-h_0}^{(\varkappa_1)},\quad \begin{matrix} 2\cdot 2^{(h-h_0)\omega_{\varkappa_1}}D_{h_0}^{(1)}P_{h-h_0}^{(\varkappa_1)},\\ 2\cdot 2^{(h-h_0)\omega_{\varkappa_1}}M_{h_0}^{(1)}F_{h-h_0}^{(\varkappa_1)},\\ 2\cdot 2^{(h-h_0)\omega_{\varkappa_1}}M_{h_0}^{(1)}P_{h-h_0}^{(\varkappa_1)}, \end{matrix}$$

eine Potenz

$$\geqq 2^{(h-h_0)\omega_{\varkappa_1}+\partial_{h-h_0}^{(\varkappa_1)}-1}\geqq 2^{\omega_{\varkappa_1}}\cdot 2^{(h-\varkappa_1)\omega_{\varkappa_1}+\partial_{h-\varkappa_1}^{(\varkappa_1)}-1}$$
$$\geqq \sigma_{h-\varkappa_1}^{(\varkappa_1)}\cdot 2^{(h-\varkappa_1)\omega_{\varkappa_1}+\partial_{h-\varkappa_1}^{(\varkappa_1)}-1}$$

aufgeht.

Wir bekommen daher für ein $h>\varkappa_1$ die Beziehung

$$\sigma_{h-\varkappa_1}^{(\varkappa_1)}\cdot 2^{(h-\varkappa_1)\omega_{\varkappa_1}+\partial_{h-\varkappa_1}^{(\varkappa_1)}-1}=\sigma_h\cdot 2^{\partial_h-1}.$$

Aus der oben gewonnenen Gleichung $\omega_{h-\varkappa_1}^{(\varkappa_1)}=\omega_h$ $(h>\varkappa_1)$ folgt aber ohne Schwierigkeit

$$2^{(h-\varkappa_1)\omega_{\varkappa_1}+\partial_{h-\varkappa_1}^{(\varkappa_1)}-1}=2^{\partial_h-1},$$

und wir gelangen sonach wirklich zu dem Resultat $\sigma_h=\sigma_{h-\varkappa_1}^{(\varkappa_1)}$ $(h>\varkappa_1)$.

2. Sei jetzt

$$\varphi \equiv \Phi_{(1)} + 2^{\omega_{\vartheta_1}}\{\Phi_{(2)} + 2^{\omega_{\vartheta_2}}[\Phi_{(3)} + \cdots + 2^{\omega_{\vartheta_{\lambda-1}}}(\Phi_{(\lambda)})\cdot\cdot]\} \pmod{2^t}$$

ein Hauptrepräsentant der Klasse $f$ nach dem Modul $2^t$. Wir wollen die Invarianten $\sigma$ der Formen $\Phi_{(k)}$ durch

$$\varrho_1^{(k)},\ \varrho_2^{(k)},\ \ldots,\ \varrho_{\varkappa_k-2}^{(k)},\ \varrho_{\varkappa_k-1}^{(k)}$$

bezeichnen.

D. *Die Invarianten $\sigma_h$ können vermittels der Relationen*

$$\sigma_{\vartheta_{k-1}+h} = \varrho_h^{(k)} \quad (h = 1,\ 2,\ \ldots,\ \varkappa_k - 1)$$

*und*

$$\sigma_{\vartheta_k} = 1$$

*durch die Invarianten $\varrho_h^{(k)}$ ausgedrückt werden.*

Beweis: In 1. erhielten wir die Gleichungen

$$\sigma_h = \varrho_h^{(1)}\ (h < \varkappa_1),\quad \sigma_{\vartheta_1} = 1,\quad \sigma_h = \sigma_{h-\varkappa_1}^{(\varkappa_1)}\quad (h > \varkappa_1);$$

dieselben rechtfertigen im Falle $\lambda = 1$ den Satz D. vollständig, während sie uns in den Fällen $\lambda > 1$ eine Gelegenheit zur Anwendung eines Schlusses von $\lambda - 1$ auf $\lambda$ verschaffen. Wie wir in Kap. III gesehen haben, gehört der Form $f^{(\varkappa_1)}$ in derselben Weise die Zahl $\lambda - 1$ zu, wie der Form $f$ die Zahl $\lambda$ entspricht, und es ist sofort klar, daß der Hauptrepräsentant $\varphi \pmod{2^t}$ der Klasse $f$ einen Hauptrepräsentanten

$$2^{\omega_{\varkappa_1}}\varphi^{(\varkappa_1)} \equiv 2^{\omega_{\varkappa_1}}\{\Phi_{(2)} + 2^{\omega_{\vartheta_2}}[\Phi_{(3)} + \cdots + 2^{\omega_{\vartheta_{\lambda-1}}}(\Phi_{(\lambda)})\cdot\cdot]\} \pmod{2^t}$$

für die Form $2^{\omega_{\varkappa_1}}f^{(\varkappa_1)}$ mit sich führt. Machen wir nun die Annahme, der Satz sei richtig für Formen mit $\lambda - 2$ von Null verschiedenen Zahlen $\omega$, so erhalten wir

$$\sigma_{\vartheta_{k-1}-\varkappa_1+h}^{(\varkappa_1)} = \varrho_h^{(k)}\ \ (k > 1;\ h = 1, \ldots,\ \varkappa_k - 1)$$

und

$$\sigma_{\vartheta_k-\varkappa_1}^{(\varkappa_1)} = 1\ \ (k > 1),$$

woraus auf der Stelle die Gleichungen

$$\sigma_{\vartheta_{k-1}+h} = \varrho_h^{(k)}\ \ (k > 1;\ h = 1, \ldots,\ \varkappa_k - 1)$$

und

$$\sigma_{\vartheta_k} = 1\ (k > 1)$$

hervorgehen; dieselben beweisen zusammen mit den Gleichungen

$$\sigma_h = \varrho_h^{(1)}\ (h = 1, \ldots,\ \varkappa_1 - 1)\quad \text{und}\quad \sigma_{\vartheta_1} = 1$$

den Satz D. für die Form $f$, welche $\lambda - 1$ von Null verschiedene Zahlen $\omega$ besitzt.

3. Je nachdem $\Phi_{(k)}$ einen Rest von der Gestalt

$$(\mathrm{R_I}) \qquad \Phi_{(k)} \equiv \begin{pmatrix} \alpha_1^{(k)}, & & & \\ & \alpha_2^{(k)}, & & \\ & & \dots, & \\ & & & \alpha_{\varkappa_k}^{(k)} \end{pmatrix} \pmod{2^{t-v_{\vartheta_{k-1}}}}$$

oder von der Gestalt

$$(\mathrm{R_{II}}) \quad \Phi_{(k)} \equiv \begin{pmatrix} 2\alpha_1^{(k)}, \ \mathfrak{A}_1^{(k)}, & & & & \\ \mathfrak{A}_1^{(k)}, \ 2\tilde{\alpha}_1^{(k)}, & & & & \\ & 2\alpha_2^{(k)}, \ \mathfrak{A}_2^{(k)}, & & & \\ & \mathfrak{A}_2^{(k)}, \ 2\tilde{\alpha}_2^{(k)}, & & & \\ & & \dots, & & \\ & & & 2\alpha_{\frac{1}{2}\varkappa_k}^{(k)}, \ \mathfrak{A}_{\frac{1}{2}\varkappa_k}^{(k)}, & \\ & & & \mathfrak{A}_{\frac{1}{2}\varkappa_k}^{(k)}, \ 2\tilde{\alpha}_{\frac{1}{2}\varkappa_k}^{(k)} \end{pmatrix} \pmod{2^{t-v_{\vartheta_{k-1}}}}$$

läßt, erhalten die Größen $\varrho_h^{(k)}$, wie wir uns leicht überzeugen, die Werte

$$(\mathrm{R_I}) \qquad \varrho_1^{(k)} = 1, \ \varrho_2^{(k)} = 1, \dots, \ \varrho_{\varkappa_k - 2}^{(k)} = 1, \ \varrho_{\varkappa_k - 1}^{(k)} = 1 \quad (\varrho_h^{(k)} = 1)$$

oder die Werte

$$(\mathrm{R_{II}}) \qquad \varrho_1^{(k)} = 2, \ \varrho_2^{(k)} = 1, \dots, \ \varrho_{\varkappa_k - 2}^{(k)} = 1, \ \varrho_{\varkappa_k - 1}^{(k)} = 2 \cdot \begin{pmatrix} \varrho_{2i-1}^{(k)} = 2 \\ \varrho_{2i}^{(k)} = 1 \end{pmatrix}$$

Der Fall eines Restes $(\mathrm{R_{II}})$ kann nur bei geradem $\varkappa_k$ eintreten. Nehmen wir an, von den $\lambda$ Größen $\varkappa_k$ seien im ganzen $\lambda_0$ gerade, nämlich die folgenden

$$\varkappa_{\tau_1}, \ \varkappa_{\tau_2}, \dots, \ \varkappa_{\tau_{\lambda_0}}.$$

Dann werden alle $\lambda - \lambda_0$ Formen $\Phi_{(k)}$, für welche der Index $k$ keiner der Zahlen $\tau_1, \tau_2, \dots, \tau_{\lambda_0}$ gleich ist, gewiß Reste von der Gestalt $(\mathrm{R_I})$ besitzen.

Für die in bezug auf 2 primitive Form $f$ mögen die $\lambda_f$ Formen

$$\Phi_{(\tau_{\pi_1})}, \ \Phi_{(\tau_{\pi_2})}, \dots, \ \Phi_{(\tau_{\pi_{\lambda_f}})}$$

Reste von der Art $(\mathrm{R_{II}})$ lassen, während alle $\lambda - \lambda_f$ übrigen Formen $\Phi_{(k)}$ Reste von der Art $(\mathrm{R_I})$ besitzen mögen. Wir können dann sagen, der Form $f$ gehöre die Kombination

$$[\pi_1, \ \pi_2, \dots, \ \pi_{\lambda_f}]$$

an, und es ist sofort einleuchtend, daß durch diese Kombination von Zahlen $\pi$ aus der Reihe der Zahlen $1, 2, \dots, \lambda_0$ die $n-1$ Invarianten $\sigma$ der Form $f$ vollständig bestimmt sind. Wir erschließen daraus leicht den Satz:

E. Wenn die $n-1$ Invarianten $o_h$ und der Index $I$ gegeben sind, so führen höchstens

$$2^{\lambda_0}\left(\leqq 2^{\left[\frac{n}{2}\right]}\right)^{*)}$$

von den sämtlichen $2^{n-1}$ verschiedenen Kombinationen

$$(\sigma_1, \sigma_2, \ldots, \sigma_{n-2}, \sigma_{n-1}); \quad \sigma_h = 1, 2,$$

welche sich überhaupt bilden lassen, zu wirklich existierenden Ordnungen

$$O: \begin{pmatrix} \sigma_1, & \sigma_2, \ldots, & \sigma_{n-1} \\ o_1, & o_2, \ldots, & o_{n-1} \end{pmatrix}, \ I.$$

In der Tat ist die Anzahl aller überhaupt zulässigen Kombinationen $(\sigma_h)$ höchstens so groß wie die Anzahl sämtlicher angebbaren Kombinationen

$$[\pi_1, \pi_2, \ldots, \pi_{\lambda_f}].$$

Diese letztere Anzahl ist aber offenbar gleich

$$\sum_{\lambda_f=1}^{\lambda_0} \frac{\lambda_0(\lambda_0-1)\cdots(\lambda_0-\lambda_f+1)}{1\cdot 2\cdots\lambda_f} = 2^{\lambda_0}.$$

Hieraus geht das Behauptete sofort hervor.

Wie wir später (im Kap. XI) nachweisen werden, ist die Anzahl derjenigen Kombinationen $(\sigma_h)$, welche, mit den $n-1$ Größen $o_h$ und der Zahl $I$ verbunden, zu wirklich existierenden Ordnungen führen, in der Tat mit nur wenigen Ausnahmen gleich $2^{\lambda_0}$.

Eine dieser Ausnahmen kann eintreten, wenn $\lambda = \lambda_0$ ist. Alsdann sind sämtliche Zahlen $\varkappa_1, \varkappa_2, \ldots, \varkappa_\lambda$ und mithin auch ihre Summe $\varkappa_1 + \varkappa_2 + \cdots + \varkappa_\lambda = n$ gerade, und es fragt sich, ob die Kombination $[1, 2, \ldots, \lambda]$ eine wirklich bestehende Ordnung zu liefern vermag. Für diese Kombination müßte

$$\sigma_1 = 2, \ \sigma_2 = 1, \ \ldots, \ \sigma_{n-2} = 1, \ \sigma_{n-1} = 2$$

sein, und es müßten sämtliche Reste $\Phi_{(k)}$ die Gestalt $(R_{II})$ erhalten. Für die Determinanten $|\Phi_{(k)}|$ dieser Formen werden daher die Kongruenzen gelten

$$|\Phi_{(k)}| \equiv (-1)^{\frac{\varkappa_k}{2}} \pmod 4,$$

aus welchen sich sofort

$$|\Phi_{(1)}|\,|\Phi_{(2)}|\cdots|\Phi_{(\lambda)}| \equiv (-1)^{\frac{\varkappa_1+\varkappa_2+\cdots+\varkappa_\lambda}{2}} \equiv (-1)^{\frac{n}{2}} \pmod 4$$

*) Es ist $n \geqq \varkappa_{\tau_1} + \varkappa_{\tau_2} + \cdots + \varkappa_{\tau_{\lambda_0}}$, und wir haben $\varkappa_{\tau_\pi} > 0$, $\varkappa_{\tau_\pi} \equiv 0 \pmod 2$, also $\varkappa_{\tau_\pi} \geqq 2$. Demnach kommt $n \geqq 2\lambda_0$ oder $\lambda_0 \leqq \left[\frac{n}{2}\right]$.

ergibt. Nun ist die Determinante der Form $\varphi$, wie man leicht erkennt,

$$(-1)^I \cdot d_{n-1} \equiv |\Phi_{(1)}|\,|\Phi_{(2)}|\cdots|\Phi_{(\lambda)}| \cdot 2^{\partial_{n-1}} \pmod{2^{2+\partial_{n-1}}}$$
$$[t > 1 + \partial_{n-1}].$$

Wir erhalten hieraus die Kongruenz

$$(-1)^I \cdot \frac{d_{n-1}}{2^{\partial_{n-1}}} \equiv (-1)^{\frac{n}{2}} \pmod 4.$$

Beachten wir jetzt die Beziehungen

$$\frac{d_{n-1}}{2^{\partial_{n-1}}} = \left[\frac{o_1}{2^{\omega_1}}\right]^{n-1}\left[\frac{o_2}{2^{\omega_2}}\right]^{n-2}\cdots\left[\frac{o_{n-1}}{2^{\omega_{n-1}}}\right], \quad \left[\frac{o_h}{2^{\omega_h}}\right]^2 \equiv 1 \pmod 4,$$
$$n \equiv 0 \pmod 2,$$

so gelangen wir zu der Bedingung

$$\prod_{h=1}^{\frac{n}{2}} \frac{o_{2h-1}}{2^{\omega_{2h-1}}} \equiv (-1)^{I+\frac{n}{2}} \pmod 4.$$

Dieselbe liefert den folgenden Ausnahmefall:

Sobald $\lambda = \lambda_0$ $[n \equiv 0 \pmod 2]$ und

$$\prod_{h=1}^{\frac{n}{2}} \frac{o_{2h-1}}{2^{\omega_{2h-1}}} \equiv -(-1)^{I+\frac{n}{2}} \pmod 4$$

wird, führen höchstens $2^{\lambda_0-1}$ Kombinationen der $\sigma_h$ zu wirklich existierenden Ordnungen, da in diesem Falle die Kombination

$$\sigma_1 = 2,\ \sigma_2 = 1,\ \ldots,\ \sigma_{n-2} = 1,\ \sigma_{n-1} = 2$$

unmöglich ist.

II. Den gewonnenen Resultaten wollen wir jetzt einen Ausdruck geben, welcher uns ohne weiteres in den Stand setzt, zu entscheiden, ob irgendeine Ordnung $O$ Formen enthalten kann.

*Eine Ordnung*

$$\begin{pmatrix}\sigma_0 = 1;\ \sigma_1, \sigma_2, \ldots, \sigma_{n-2}, \sigma_{n-1};\ \sigma_n = 1\\ o_0 = 0;\ o_1, o_2, \ldots, o_{n-2}, o_{n-1};\ o_n = 0\end{pmatrix}, \quad I$$

*ist nur dann möglich, wenn die ganzen Zahlen $\sigma_h$, $o_h$ und $I$ den folgenden Gesetzen gehorchen:*

*1) Die Zahlen $\sigma_h$ und $\sigma_{h-1}o_h\sigma_{h+1}$ sind nicht beide zugleich durch 2 teilbar ($\sigma_h$ relativ prim zu $\sigma_{h-1}o_h\sigma_{h+1}$).*

*2) Die Größen $\frac{\sigma_{h-1}o_h}{\sigma_{h+1}}$ und $\frac{\sigma_{h+1}o_h}{\sigma_{h-1}}$ sind ganze Zahlen.*

*3) Wenn* $n \equiv 0 \pmod 2$ *und* $\sigma_1 = 2,\ \sigma_2 = 1,\ \ldots,\ \sigma_{n-2} = 1,\ \sigma_{n-1} = 2$ *ist, so wird*

$$\prod_{h=1}^{\frac{n}{2}} \frac{o_{2h-1}}{2^{\omega_{2h-1}}} \equiv (-1)^{I+\frac{n}{2}} \pmod 4.$$

Damit diese Gesetze ohne Ausnahme auch für $h = 1$ und $h = n-1$ gelten, haben wir den $2(n-1)$ Invarianten $o_h$ und $\sigma_h$ noch je zwei weitere Invarianten $o_0 = 0,\ o_n = 0$ und $\sigma_0 = 1,\ \sigma_n = 1$ hinzugefügt.

Der Satz 1) zerfällt in zwei Teile:

$\alpha$) Wenn $o_h \equiv 0 \pmod 2$ ist, so wird $\sigma_h = 1$, und wenn $\sigma_h = 2$ ist, so wird $o_h \equiv 1 \pmod 2$.

Es ergibt sich dieses aus der Relation $\sigma_{\vartheta_k} = 1$; denn sobald $o_h \equiv 0 \pmod 2$ ist, muß $h$ mit einer der Zahlen $\vartheta_k$ übereinstimmen, und sobald $\sigma_h = 2$ ist, muß $h$ von den Zahlen $\vartheta_k$ verschieden und folglich $o_h \equiv 1 \pmod 2$ sein.

$\beta$) Wenn $\sigma_h = 2$ ist, so wird $\sigma_{h-1} = 1,\ \sigma_{h+1} = 1$.

Dies erkennt man sofort aus dem Satze D. und den Werten, welche die Größen $\varrho_h^{(k)}$ annehmen können.

Den Satz 2) können wir auch folgendermaßen aussprechen:

Es ist $\sigma_{h-1} o_h \equiv \sigma_{h-1} o_h \sigma_{h+1} \equiv o_h \sigma_{h+1} \pmod 2$;

oder:

Wenn $\sigma_{h-1} \neq \sigma_{h+1}$, also $\sigma_{h-1}\sigma_{h+1} = 2$ ist, so muß $o_h \equiv 0 \pmod 2$ sein;

oder:

Wenn $\sigma_{h-1} o_h \sigma_{h+1}$ durch 2 und nicht durch 4 teilbar ist, so wird $\sigma_{h-1} = 1,\ \sigma_{h+1} = 1$.

Die Werte der $\varrho_h^{(k)}$ zeigen, daß stets $\sigma_{h-1} = \sigma_{h+1}$ ist, sobald $h$ keiner der Zahlen $\vartheta_k$ gleich ist; es kann demnach nur dann $\sigma_{h-1} \neq \sigma_{h+1}$ sein, wenn $h$ mit einer der Zahlen $\vartheta_k$ übereinstimmt, also $o_h \equiv 0 \pmod 2$ ist.

Aus den Gesetzen 1) und 2) läßt sich der Satz E. von neuem herleiten.

## Kap. V. **Sätze über Hauptreste. — Grundformen für einen Modul $N$.**

Die Hauptreste einer primitiven Formenklasse $f$ besitzen eine Reihe interessanter Eigenschaften, von denen wir einige in dem Folgenden mitteilen wollen.

I. Wir setzen die höchste in dem Produkt $\sigma_{n-1} o_1 o_2 \ldots o_{n-1}$ aufgehende Potenz einer Primzahl $q$ gleich $q^{G(q)}$; für ein ungerades $q = p$ wird diese Potenz offenbar gleich $p^{v_{n-1}(p)}$, dagegen für $q = 2$ gleich $\sigma_{n-1} \cdot 2^{v_{n-1}(2)}$. Je nachdem eine Zahl $q^t \leqq q^{G(q)}$ oder $> q^{G(q)}$ ist, treten in den Hauptresten von $f$ für den Modul $q^t$ mittlere Koeffizienten auf, welche

durch den Modul $q^t$ teilbar sind, oder es ist keiner dieser Koeffizienten durch $q^t$ teilbar. Aus diesem Grunde beschränken wir uns auf die Untersuchung von Moduln $N$, deren Primfaktoren $q^t (t > 0)$ die Potenzen $q^{G(q)}$ überschreiten.

Es möge die Form $\varphi$ einen Hauptrepräsentanten der primitiven Klasse $f$ in bezug auf einen derartigen Modul $N$ bedeuten. Wir bezeichnen die aus den ersten $h (= 1, 2, \ldots, n)$ Horizontal- und Vertikalreihen der Form $\varphi$ gebildeten symmetrischen Unterdeterminanten durch $\sigma_h d_{h-1} \varphi_h$, und wir setzen noch $\varphi_0 = 1$. Die Zahl $\varphi_n$ ist gleich $(-1)^I$.

Die sämtlichen $n + 1$ Größen $\varphi_h (h = 0; 1, 2, \ldots, n)$ sind offenbar ganze Zahlen, und wir behaupten:

1. Die $n + 1$ Zahlen

$$\varphi_0; \varphi_1, \varphi_2, \cdots, \varphi_{n-1}, \varphi_n$$

fallen sämtlich zu $N$ relativ prim aus.

Zunächst möge $N$ aus einer einzigen Primzahlpotenz $q^t (> q^{G(q)})$ bestehen. Ein Blick auf die Hauptrepräsentanten $\varphi$ zeigt uns, daß die Determinanten $\sigma_h d_{h-1} \varphi_h$ sich für ein $q^t = p^t$ als Produkte aus den Potenzen $p^{\partial_{h-1}(p)}$ und aus zu $p$ primen Zahlen darstellen, während sie für ein $q^t = 2^t$ gleich Produkten aus den Potenzen $\sigma_h \cdot 2^{\partial_{h-1}(2)}$ und aus ungeraden Zahlen werden. Hieraus schließen wir, daß die $\varphi_h$ in der Tat zu der Primzahl $q$ relativ prim sind. Falls $N$ sich aber aus mehreren Primzahlpotenzen $q^t (> q^{G(q)})$ zusammensetzt, so ist der Hauptrepräsentant $\varphi$ für den Modul $N$ zugleich Hauptrepräsentant für jeden dieser Moduln $q^t$. Nach dem soeben Gesagten sind daher die Größen $\varphi_h$ zu jeder der Primzahlen $q$ prim, und sie werden demnach auch zu der Zahl $N$ relativ prim sein.

Die $n$ mittleren Koeffizienten einer beliebigen quadratischen Form können stets durch die $\frac{n(n-1)}{2}$ seitlichen Koeffizienten dieser Form und durch die aus den ersten $h (= 1, 2, \ldots, n)$ Reihen dieser Form gebildeten symmetrischen Unterdeterminanten ausgedrückt werden. Beachten wir die besonderen Werte, welche die $\frac{n(n-1)}{2}$ seitlichen Koeffizienten in einem Hauptrest für den Modul $N$ besitzen, so gelangen wir zu dem folgenden Satze:

2. Wenn die Form $\varphi$ einen Hauptrepräsentanten der Klasse $f$ für den Modul $N$ vorstellt, so kann vermittels der $n + 1$ zur Form $\varphi$ gehörigen Zahlen $\varphi_h (h = 0; 1, 2, \ldots, n)$ ein Hauptrest der Klasse $f$ für den Modul $N$ gefunden werden.

Ist $N$ beispielsweise ungerade, so liefert ein Hauptrepräsentant $\varphi$ (mod $N$) uns den Hauptrest

$$\varphi \equiv \begin{pmatrix} \frac{\sigma_1 \varphi_1}{\sigma_0 \varphi_0}, & & & & \\ & o_1 \cdot \frac{\sigma_2 \varphi_2}{\sigma_1 \varphi_1}, & & & \\ & & o_1 o_2 \cdot \frac{\sigma_3 \varphi_3}{\sigma_2 \varphi_2}, & & \\ & & & \cdots, & \\ & & & & o_1 o_2 \ldots o_{n-1} \cdot \frac{\sigma_n \varphi_n}{\sigma_{n-1} \varphi_{n-1}} \end{pmatrix} \pmod{N}.$$

Ein wenig umständlicher gestaltet sich der Ausdruck des Hauptrestes (mod $N$) durch die Größen $\varphi_h$, wenn der Modul $N$ gerade ist und nicht alle Invarianten $\sigma_h$ der Form $\varphi$ gleich 1 werden. Wenn $N = 2^t$ ist, müssen wir, um vermittels der Zahlen $\varphi_h$ eines Hauptrepräsentanten einen Hauptrest zu finden, so viele willkürliche ungerade Zahlen $\mathfrak{A}$ einführen, als es Invarianten $\sigma_h$ gibt, welche gleich 2 ausfallen.

---

Wir nennen eine Form $\psi\,(\sim f)$ eine *Grundform* der Klasse $f$ für einen Modul $N$, sobald die aus den ersten $h$ Horizontal- und Vertikalreihen der Form $\psi$ gebildeten symmetrischen Determinanten Werte $\sigma_h d_{h-1} \psi_h$ erhalten, in welchen die Zahlen $\psi_h$ zu $N$ relativ prim sind.

Es ist leicht einzusehen, daß die Klasse $f$ für einen jeden Modul $N$ Grundformen enthält; denn treten in dem Modul $N$ die Primzahlen $q_1, q_2, \ldots, q_{c_0}$ auf, so bildet nach dem Satz 1. offenbar jeder Hauptrepräsentant in bezug auf einen Modul $N^* = q_1^{t_1} q_2^{t_2} \ldots q_{c_0}^{t_{c_0}} [t_c > G(q_c), c = 1, 2, \ldots, c_0]$ eine Grundform für den Modul $N$.

Wir haben die folgenden Sätze: Eine Grundform für einen Modul $N$ ist Grundform für alle in $N$ enthaltenen Faktoren; und umgekehrt: Eine Form, welche für gewisse Primzahlen $q$ eine Grundform ist, stellt auch für jeden Modul $N$, der nur durch diese Primzahlen $q$ teilbar ist, eine Grundform vor.

Mit Hilfe von Betrachtungen, welche denen in Kap. II angestellten analog sind, kann man den Satz beweisen:

3. Jede Grundform $\psi$ für einen Modul $N$ kann vermittels einer Substitution

$$S = \begin{pmatrix} 1, & s_1^2, & s_1^3, & \ldots, & s_1^n \\ & 1, & s_2^3, & \ldots, & s_2^n \\ & & 1, & \ldots, & s_3^n \\ & & & \cdots & \cdots \\ & & & & 1 \end{pmatrix}$$

in einen Hauptrepräsentanten $\varphi$ für einen jeden Modul $N_0$, der keine anderen Primzahlen enthält als der Modul $N$, übergeführt werden.

Man sieht, daß die Substitution $S$ die Werte der $n+1$ Größen $\psi_h$

ungeändert läßt, so daß für die Form $\varphi = \bar{S}\psi S$ die Relationen $\varphi_h = \psi_h$ gelten. Da nun einerseits nach 2. aus den Größen $\varphi_h$ eines Hauptrepräsentanten $\varphi \pmod{N_0}$ sofort ein Hauptrest der Klasse $f$ für den Modul $N_0$ gefunden werden kann und andererseits die Zahlen $\psi_h$ der Grundform $\psi \pmod{N}$ mit den Zahlen $\varphi_h$ übereinstimmen, so können wir auch unmittelbar von der Grundform $\psi$ ohne Zuhilfenahme der Form $\varphi$ zu Hauptresten der Klasse $f$ für den Modul $N_0$ gelangen, und wir erhalten den Satz:

4. Eine jede Grundform $\psi \pmod{N}$ führt unmittelbar zu Hauptresten in bezug auf jeden Modul $N_0$, welcher keine anderen Primzahlen enthält als der Modul $N$.

Insbesondere schließen wir hieraus:

F. Eine jede Grundform $\psi$ für eine Primzahl $q$ liefert Hauptreste für alle Moduln $q^t$.

Die Bestimmung einer Grundform $\psi$ für eine Primzahl $q$ kann sehr leicht geschehen. Denn es besteht der folgende Satz, in welchem $\bar{\lambda}(q) - 1$ die Zahl der durch $q$ teilbaren Größen $\sigma_{h-1} o_h \sigma_{h+1} (h = 1, 2, \ldots, n-1)$ bezeichnet:

Eine jede primitive Form $f$ kann durch höchstens $n - \bar{\lambda}(q)$ Substitutionen von der Art

$$S_{(i,k)}^{\pm 1}: \qquad x_i = x_i', \; x_k = \pm x_i' + x_k'; \qquad x_h = x_h' (h \neq i, k)$$

und durch höchstens $n - 1$ Substitutionen von der Art

$$P_{(l,m)}: \qquad x_l = x_m', \; x_m = -x_l'; \qquad x_h = x_h' (h \neq l, m)$$

in eine Grundform $\psi$ für die Primzahl $q$ transformiert werden.

Die Substitutionen $P_{(l,m)}$ sind offenbar sehr einfach auszuführen, da sie im Grunde nur eine Vertauschung zweier Reihen der quadratischen Koeffizientensysteme bedeuten.

II. Wenn für eine primitive Form $f$ die Zahl $\sigma_{h-1} o_h \sigma_{h+1}$ durch eine Primzahl $q$ teilbar ist, so gibt es unter den $h$-reihigen symmetrischen Determinanten $D_h(f)$ der Form $f$ solche, für welche die Zahl $\dfrac{D_h(f)}{\sigma_h d_{h-1}} = \Delta_h(f)$ zu $q$ relativ prim wird.

Beweis: Es sei zunächst $q = p$. Ein Hauptrepräsentant $\varphi \pmod{p^t > p^{G(p)}}$ der Klasse $f$ läßt einen Rest

$$\varphi \equiv \begin{Bmatrix} \alpha_1, \\ \cdots, \\ p^{\omega_1+\omega_2+\cdots+\omega_{h-1}}\alpha_h, \\ p^{\omega_1+\omega_2+\cdots+\omega_h}\alpha_{h+1}, \\ \cdots, \\ p^{\omega_1+\omega_2+\cdots+\omega_{n-1}}\alpha_n \end{Bmatrix} \pmod{p^t}.$$

Aus demselben ersehen wir, daß die höchste Potenz von $p$, welche in der Determinante

$$\varphi\begin{pmatrix}1, 2, \ldots, h\\ 1, 2, \ldots, h\end{pmatrix} = \sigma_h d_{h-1}\varphi_h$$

aufgeht, gleich $p^{\partial_h - 1}$ ist, während die höchste, in allen übrigen $h$-reihigen Determinanten

$$\varphi\begin{pmatrix}i_1, i_2, \ldots, i_h\\ k_1, k_2, \ldots, k_h\end{pmatrix}$$

der Form $\varphi$ enthaltene Potenz von $p$ gleich $p^{\partial_h - 1 + \omega_h}$ wird.

Geht $\varphi$ in die Form $f$ durch die Substitution

$$\xi_i = \sum_{k=1}^{n} u_i^k x_k$$

über, so bekommen wir für die symmetrischen $h$-reihigen Unterdeterminanten der Form $f$ die Gleichungen

$$D(l_1, l_2, \ldots, l_h) = \frac{\sum_{(i,k)}^{1,n} \varphi\begin{pmatrix}i_1, i_2, \ldots, i_h\\ k_1, k_2, \ldots, k_h\end{pmatrix} U\begin{pmatrix}l_1, l_2, \ldots, l_h\\ i_1, i_2, \ldots, i_h\end{pmatrix} U\begin{pmatrix}l_1, l_2, \ldots, l_h\\ k_1, k_2, \ldots, k_h\end{pmatrix}}{(1 \cdot 2 \cdots h) \cdot (1 \cdot 2 \cdots h)}.$$

Dieselben liefern infolge der soeben gemachten Bemerkung die Kongruenz

$$\begin{aligned} D(l_1, l_2, \ldots, l_h) &= \sigma_h d_{h-1} \Delta(l_1, l_2, \ldots, l_h) \\ &\equiv \sigma_h d_{h-1}\varphi_h \cdot \left(U\begin{pmatrix}l_1, l_2, \ldots, l_h\\ 1, 2, \ldots, h\end{pmatrix}\right)^2 \pmod{p^{\partial_h - 1 + \omega_h}} \end{aligned}$$

oder

$$(2) \qquad \Delta(l_1, l_2, \ldots, l_h) \equiv \varphi_h \cdot \left(U\begin{pmatrix}l_1, l_2, \ldots, l_h\\ 1, 2, \ldots, h\end{pmatrix}\right)^2 \pmod{p^{\omega_h(p)}}.$$

Die Zahlen $U\begin{pmatrix}l_1, l_2, \ldots, l_h\\ 1, 2, \ldots, h\end{pmatrix}$ können keinen gemeinsamen, von 1 verschiedenen Teiler besitzen; denn ein solcher Teiler müßte zugleich die Determinante $|u_i^k|$ teilen, und diese könnte mithin nicht gleich 1 sein. Es müssen sich demnach unter den Zahlen $U\begin{pmatrix}l_1, l_2, \ldots, l_h\\ 1, 2, \ldots, h\end{pmatrix}$ solche befinden, welche zu $p$ prim ausfallen. Wenn nun die Größe $\sigma_{h-1}\sigma_h\sigma_{h+1}$ durch $p$ teilbar ist, so wird offenbar $\omega_h(p) \geqq 1$, und es entspricht alsdann infolge der Kongruenz (2) einer jeden durch $p$ nicht teilbaren Zahl $U\begin{pmatrix}l_1, l_2, \ldots, l_h\\ 1, 2, \ldots, h\end{pmatrix}$ eine durch $p$ nicht teilbare Zahl $\Delta(l_1, l_2, \ldots, l_h)$. Hieraus erhellt die Richtigkeit unseres Satzes für den Fall $q = p$.

Wenn $q = 2$ ist, so gelangen wir durch Betrachtung eines Hauptrepräsentanten $\varphi \pmod{2^t > 2^{G(2)}}$ in ähnlicher Weise zu einer Kongruenz

$$(3) \qquad \Delta(l_1, l_2, \ldots, l_h) \equiv \varphi_h \cdot X_h^2 \pmod{\sigma_{h-1} 2^{\omega_h(2)} \sigma_{h+1}},$$

und diese Kongruenz zeigt uns, daß unter den Größen $\Delta(l_1, l_2, \ldots, l_h)$ sich ungerade befinden müssen, sobald $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod 2$ wird. — Dieses letzte Resultat erhalten wir einfacher, wenn wir beachten, daß einerseits $\sigma_h$ gleich 2 sein müßte, sobald alle $\Delta(l_1, l_2, \ldots, l_h)$ gerade werden, während andererseits nach Kap. IV, Absatz II zu einem $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod 2$ stets ein $\sigma_h$ gleich 1 gehört.

Aus jeder Grundform $\psi$ in bezug auf eine Primzahl $q$ können wir nach dem Satz F. für einen jeden Modul $q^t$ Hauptrepräsentanten $\varphi$ herleiten, deren Zahlen $\varphi_h$ den Zahlen $\psi_h$ gleich werden. Infolge dieses Umstandes dürfen wir die Kongruenzen (2) und (3) durch die Kongruenzen

$$\frac{D_h(f)}{\sigma_h d_{h-1}} = \Delta_h(f) \equiv \psi_h \cdot X_h^2 \pmod{p^{\omega_h(p)}} \tag{4}$$

und

$$\frac{D_h(f)}{\sigma_h d_{h-1}} = \Delta_h(f) \equiv \psi_h \cdot X_h^2 \pmod{\sigma_{h-1} 2^{\omega_h(2)} \sigma_{h+1}} \tag{5}$$

ersetzen, welche resp. für eine Grundform $\psi \pmod p$ und $\psi \pmod 2$ gelten werden.

Für eine Grundform $\psi$ in bezug auf den Modul $2 \prod_{h=1}^{n-1} o_h$ müssen offenbar sämtliche Kongruenzen (4) und (5) zu gleicher Zeit statthaben, und wir bekommen daher für eine Grundform $\psi \left(\text{mod } 2 \prod_{h=1}^{n-1} o_h\right)$ die Beziehungen

$$\frac{D_h(f)}{\sigma_h d_{h-1}} = \Delta_h(f) \equiv \psi_h \cdot X_h^2 \pmod{\sigma_{h-1} o_h \sigma_{h+1}};$$

dieselben liefern uns für irgend zwei beliebige Zahlen $\Delta_h'(f)$ und $\Delta_h''(f)$ eine Kongruenz

$$\Delta_h'(f) \cdot \Delta_h''(f) \equiv [\Delta_h'''(f)]^2 \pmod{\sigma_{h-1} o_h \sigma_{h+1}}.$$

## Kap. VI. **Formengruppen für einen Modul $N$. — Charaktere.**

I. Zwei *Formen* $\varphi = \{\alpha_{ik}\}$ und $\psi = \{\beta_{ik}\}$ heißen *kongruent* nach einem Modul $N$, wenn sie den sämtlichen Kongruenzen $\alpha_{ik} \equiv \beta_{ik} \pmod N$ genügen, d. h. wenn sie für den Modul $N$ den nämlichen Rest ergeben. Gleicherweise nennen wir zwei *Formenklassen* $f$ und $g$ für einen Modul $N$ *kongruent*, wenn sie irgend zwei nach diesem Modul $N$ kongruente Repräsentanten enthalten. Wir drücken die Kongruenz zweier Formen $\varphi$ und $\psi$ durch das Zeichen $\equiv [\varphi \equiv \psi \pmod N]$ und die Kongruenz zweier Klassen $f$ und $g$ durch das Zeichen $\simeq [f \simeq g \pmod N]$ aus.

Wir beweisen den Satz:

Wenn für irgend zwei Repräsentanten $\varphi$ und $\psi$ zweier Klassen $f$ und $g$ eine Kongruenz

$$\varphi \equiv \psi \pmod{N}$$

besteht, so kann zu jeder Form $f_0$ der einen eine Form $g_0$ der anderen Klasse bestimmt werden, welche ihr nach dem Modul $N$ kongruent ist.

Denn wenden wir irgendeine Substitution $S$ gleichzeitig auf beide Formen $\varphi$ und $\psi$ an, so gehen dieselben in zwei Formen $\varphi_0 (\sim \varphi)$ und $\psi_0 (\sim \psi)$ über, welche ebenso wie $\varphi$ und $\psi$ einer Kongruenz

$$\varphi_0 \equiv \psi_0 \pmod{N}$$

genügen. Nun können wir $S$ so wählen, daß $\varphi_0 = f_0$ wird. Dann wird das betreffende $\psi_0$ der Klasse $g$ gleich $g_0 \equiv f_0 \pmod{N}$ werden.

Nach diesem Satze enthalten zwei Formenklassen, welche für einen Modul $N$ kongruent sind, lauter gleiche Formenreste für den Modul $N$. Daraus folgt:

G. Sind zwei Formenklassen $g_,$ und $g_{,,}$ einer dritten Formenklasse $f$ nach dem Modul $N$ kongruent, so sind sie auch untereinander nach dem Modul $N$ kongruent.

Denn ist $g_, \simeq f \pmod{N}$ und $g_{,,} \simeq f \pmod{N}$, so stimmen sowohl die Reste der Klasse $g_,$ für den Modul $N$ als auch die Reste der Klasse $g_{,,}$ für den Modul $N$ völlig mit den Resten der Klasse $f$ für den Modul $N$ überein. Es werden demnach auch die Reste der beiden Klassen $g_,$ und $g_{,,}$ für den Modul $N$ einander gleich sein, d. h. es wird wirklich $g_, \simeq g_{,,} \pmod{N}$ werden.

Der Satz G. zeigt uns die Möglichkeit einer Einteilung aller Formen in eine endliche Anzahl von *Gruppen* in bezug auf einen Modul $N$, indem wir zwei Formenklassen in dieselbe oder in verschiedene Gruppen (mod $N$) aufnehmen, je nachdem sie in bezug auf $N$ kongruent sind oder nicht. Es werden alsdann sämtliche Klassen einer und derselben Gruppe modulo $N$ untereinander kongruent sein, während zwei Klassen aus verschiedenen Gruppen modulo $N$ inkongruent sein werden.

Es leuchtet ein, daß die Anzahl aller verschiedenen Gruppen für einen Modul $N$, zu welchen wir durch diese Einteilung gelangen, notwendig eine endliche ist. Denn es gibt gewiß nicht mehr als $N^{\frac{n(n+1)}{2}}$ verschiedene Gruppen für den Modul $N$, da doch eine jede quadratische Form $f = \{a_{ik}\}$ nach dem Modul $N$ mindestens einer der $N^{\frac{n(n+1)}{2}}$ Formen $\{R_{ik}\}$ $(R_{ik} = 1, 2, \ldots, N)$ kongruent sein muß.

II. Wenn der Modul $N$ ein Produkt aus $c_0$ zueinander relativ primen Zahlen $N_1, N_2, \ldots, N_{c_0}$ ist, so erfordert das Bestehen einer Kongruenz

$$f \simeq g \pmod{N}$$

das gleichzeitige Bestehen der $c_0$ einzelnen Kongruenzen

$$f \simeq g \pmod{N_c} \qquad (c = 1, 2, \ldots, c_0),$$

und umgekehrt findet die erstere Kongruenz wirklich statt, sobald die $c_0$ letzteren Kongruenzen sämtlich erfüllt sind.

In der Tat ist jeder Rest der Formenklassen $f$ und $g$ in bezug auf den Modul $N$ zugleich Rest dieser Formenklasse für die sämtlichen Moduln $N_c$. Ist also $f \simeq g \pmod{N}$, so wird auch $f \simeq g \pmod{N_c}$ sein.

Falls umgekehrt die $c_0$ Kongruenzen

$$f \simeq g \pmod{N_c} \qquad (c = 1, 2, \ldots, c_0)$$

alle erfüllt sind, so können wir zunächst in der Klasse $f$ gewiß $c_0$ Formen $\varphi_c$ und in der Klasse $g$ ebenfalls $c_0$ Formen $\psi_c$ angeben derart, daß die $c_0$ Kongruenzen

$$\varphi_c \equiv \psi_c \pmod{N_c} \qquad (c = 1, 2, \ldots, c_0)$$

statthaben. Darauf können wir nach Kap. III, Absatz I in den Klassen $f$ und $g$ je eine Form $\varphi$ und $\psi$ angeben, welche den Kongruenzen

$$\varphi \equiv \varphi_c \pmod{N_c}, \quad \psi \equiv \psi_c \pmod{N_c} \qquad (c = 1, 2, \ldots, c_0)$$

genügen. Die Koeffizienten dieser beiden letzten Formen $\varphi$ und $\psi$ sind nun in bezug auf die sämtlichen zueinander primen Moduln $N_c$, also auch in bezug auf den Modul $N = N_1 N_2 \ldots N_{c_0}$ kongruent; mithin wird

$$\varphi \equiv \psi \pmod{N},$$

und hieraus ergibt sich auf der Stelle

$$f \simeq g \pmod{N}.$$

Wählen wir für die Zahlen $N_c$ die verschiedenen in $N$ enthaltenen Primzahlpotenzen $q^t$, so zeigt sich, daß die Untersuchung von Gruppen für einen beliebigen Modul $N$ auf die Untersuchung von Gruppen in bezug auf Primzahlpotenzen $q^t$ hinausläuft.

III. Wir wollen die notwendigen und hinreichenden Bedingungen für die Kongruenz zweier Formenklassen nach einem Modul $N$ auffinden. Nach Aufstellung dieser Bedingungen werden wir dazu übergehen, zu prüfen, ob es verschiedene Formenklassen von demselben Index $I$ gibt, welche nach allen überhaupt möglichen Moduln kongruent sind, und aus diesen nach jedem Modul kongruenten Formenklassen werden wir die *Genera* von Formen bilden.

Nehmen wir an, die Klassen $f$ und $g$ seien nach dem Modul $N$ kongruent, und setzen wir ferner, der größeren Einfachheit halber, voraus, daß $f$ und $g$ in bezug auf $N$ primitiv sind und daß die Faktoren $q^t$ $(t > 0)$ von $N$ für ein $q = p$ die Potenzen $p^{\nu_n - 1(p)}$ und für ein $q = 2$ die Potenzen $\frac{4}{\sigma_{n-1}} 2^{\nu_n - 1(2)}$, welche den Formen $f$ und $g$ entsprechen, übersteigen.

1. Nach den soeben bewiesenen Sätzen besitzen die Formenklassen $f$ und $g$ für einen jeden der in $N$ aufgehenden Moduln $q^t$ vollständig dieselben Reste und folglich auch dieselben Hauptreste. Aus der Gestalt dieser Hauptreste für die Moduln $q^t (> q^{G(q)})$ können wir aber die Werte der Zahlen

$$q^{\omega_1},\ q^{\omega_2},\ \ldots,\ q^{\omega_{n-1}}$$

und, wenn $q = 2$ ist, auch die Werte der Zahlen

$$\sigma_1,\ \sigma_2,\ \ldots,\ \sigma_{n-1},$$

welche zu den beiden Klassen $f$ und $g$ gehören, unmittelbar ablesen. Folglich müssen die Formen $f$ und $g$ für alle in $N$ aufgehenden Primzahlen $q$ dieselben Größen $q^{\omega_h}$ und, falls $q = 2$ ist, auch dieselben Größen $\sigma_h$ darbieten.

2. Es seien $\Delta(f)$ und $\Delta(g)$ die Determinanten der Formen $f$ und $g$. Für $\Delta(g) = |b_{ik}|$ besteht die Beziehung

$$\Delta(g) = \sum_{i=1}^{n} b_{ii} \frac{\partial \Delta(g)}{\partial b_{ii}} + 2 \sum_{i<k}^{1,n} b_{ik} \frac{\partial \Delta(g)}{\partial b_{ik}}.$$

Hierin ist die größte Potenz einer Primzahl $q$, welche in allen $\frac{\partial \Delta(g)}{\partial b_{ii}}$, $2\frac{\partial \Delta(g)}{\partial b_{ik}}$ aufgeht, für ein $q = p$ gleich $p^{\partial_{n-2}(p)}$ und für ein $q = 2$ gleich $\sigma_{n-1} \cdot 2^{\partial_{n-2}(2)}$. Verändern wir also die Koeffizienten der Form $g$ um Vielfache der Größe $q^t$, so wird die Determinante von $g$ sich um Vielfache der Größe $p^{t+\partial_{n-2}(p)}$ oder der Größe $\sigma_{n-1} \cdot 2^{t+\partial_{n-2}(2)}$ ändern, je nachdem $q = p$ oder $q = 2$ ist. Erinnern wir uns, daß es zu $f$ äquivalente Formen $f_0$ gibt, für welche $f_0 \equiv g \pmod N$ ist, so schließen wir daraus im Falle $q = p$ die Kongruenz

$$\Delta(f) \equiv \Delta(g) \pmod{p^{t+\partial_{n-2}(p)}}$$

und im Falle $q = 2$ die Kongruenz

$$\Delta(f) \equiv \Delta(g) \pmod{\sigma_{n-1} \cdot 2^{t+\partial_{n-2}(2)}}.$$

3. Man kann gewisse als Funktionen der Koeffizienten der Formen $f$ und $g$ ausdrückbare Einheiten angeben, welche für $f$ und für $g$ dieselben Werte annehmen.

Wir bezeichnen durch $\sigma_h d_{h-1} \Delta_h(f)$ die symmetrischen $h$-reihigen Unterdeterminanten, welche sich aus dem quadratischen System der Form $f$ bilden lassen, und durch $\sigma_h d_{h-1}(f_h)$ alle aus $h$ Reihen einer beliebigen Form der Klasse $f$ bestehenden Unterdeterminanten. Die Reste der Zahlen $\sigma_h d_{h-1}(f_h)$ für einen Modul $N$ sind offenbar durch die Reste der Formenklasse $f$ für den Modul $N$ schon völlig bestimmt. Wenn also zwei Formenklassen $f$ und $g$ für den Modul $N$ gleiche Reste lassen, so nehmen auch die Zahlen $\sigma_h d_{h-1}(f_h)$ und $\sigma_h d_{h-1}(g_h)$ für den Modul $N$

kongruente Werte an. Daher sind die Eigenschaften der Kongruenzen

$$\sigma_h d_{h-1}(f_h) \equiv \sigma_h d_{h-1} m_h \pmod{N}$$

für die Gruppe, welcher die Form $f$ für den Modul $N$ angehört, charakteristisch.

Wir sprechen den Satz aus:

Wenn die Kongruenz $(f_h) \equiv m_h \pmod{N_0}$ $[1 \leqq h \leqq n-1]$ für ein bestimmtes $m_h$ Lösungen besitzt, so sind auch alle weiteren Kongruenzen $(f_h) \equiv m_h Z^2 \pmod{N_0}$ lösbar, in welchen $Z$ eine beliebige zu $N_0$ relativ prime Größe bedeutet.

Denn besitzt die Kongruenz $(f_h) \equiv m_h \pmod{N_0}$ Lösungen, so muß es in der Klasse $f$ eine Form $\Phi$ geben, welche eine $h$-reihige symmetrische Determinante $\sigma_h d_{h-1} \Delta_h(\Phi) \equiv \sigma_h d_{h-1} m_h \pmod{\sigma_h d_{h-1} N_0}$ aufweist. Da die Zahl $h \geqq 1$ und $\leqq n-1$ ist, können wir annehmen, daß in dieser Determinante Glieder aus einer gewissen, etwa der $i^{\text{ten}}$ Reihe des Systems $\Phi$, dagegen keine Glieder einer gewissen andern, etwa der $k^{\text{ten}}$ Reihe dieses Systems erscheinen. Weil die Zahl $Z$ zu $N_0$ relativ prim sein soll, können wir eine Zahl $Z_0$ bestimmen, welche der Kongruenz

$$Z Z_0 \equiv 1 \pmod{N_0^2}$$

oder einer Gleichung

$$Z Z_0 - z N_0 z_0 N_0 = 1$$

genügt. Durch die Substitution

$$x_i = Z x_i' + z N_0 x_k', \quad x_k = z_0 N_0 x_i' + Z_0 x_k'$$

$$\left[x_i \equiv Z x_i', \quad x_k \equiv \frac{1}{Z} x_k' \pmod{N_0}\right]$$

von der Determinante 1 geht dann die Form $\Phi$ in eine Form $\Phi_0$ über, in welcher an die Stelle der Determinante $\sigma_h d_{h-1} \Delta_h(\Phi)$ offenbar eine Determinante

$$\sigma_h d_{h-1} \Delta_h(\Phi_0) \equiv \sigma_h d_{h-1} \Delta_h(\Phi) Z^2 \equiv \sigma_h d_{h-1} m_h Z^2 \pmod{\sigma_h d_{h-1} N_0}$$

getreten ist. Die Zahl $\Delta_h(\Phi_0)$ ist gleichfalls eine der Zahlen $(f_h)$, und es besitzt sonach die Kongruenz $(f_h) \equiv m_h Z^2 \pmod{N_0}$ in der Tat Lösungen.

Aus dem vorstehenden Satz ersehen wir, daß bei einer Untersuchung der Kongruenzen $(f_h) \equiv m_h \pmod{N_0}$ vor allem der quadratische Charakter der Zahl $m_h$ in Betracht kommen wird. Nehmen wir beispielsweise an, der Modul $N_0$ sei eine Potenz einer Primzahl $p$ $(N_0 = p^{t_0})$ und die Kongruenz $(f_h) \equiv m_h \pmod{p^{t_0}}$ nicht für alle zu $p$ primen Zahlen $m_h$ lösbar. Dann ist diese Kongruenz entweder nur für alle solche zu $p$ primen $m_h$ lösbar, welche quadratische Reste von $p$ sind, oder nur für alle solche zu $p$ primen $m_h$, welche quadratische Nichtreste von $p$ sind. Wenn wir den

Formen $f$ im ersten Fall einen Charakter $\left(\frac{(f_h)}{p}\right) = +1$ zuteilen, dagegen im zweiten Fall einen Charakter $\left(\frac{(f_h)}{p}\right) = -1$, so kann die Einheit $\left(\frac{(f_h)}{p}\right)$, welche der Form $f$ entspricht, dazu dienen, die Gruppe, welcher die Klasse $f$ für den Modul $p^{t_0+\delta_{h-1}(p)}$ angehört, von anderen Gruppen nach diesem Modul zu trennen.

*Wenn wir zeigen sollen, daß die Größen $(f_h)$ einer Klasse $f$ gewisse gegebene Charaktere besitzen, so genügt es, die beiden folgenden Punkte festzustellen:*

*1. daß die Zahlen $\Delta_h(\varphi)$ einer bestimmten Form $\varphi$ der Klasse $f$ wirklich die gegebenen Charaktere besitzen;*

*2. daß, wenn die Zahlen $\Delta_h(\Phi)$ einer beliebigen Form $\Phi$ der Klasse $f$ diese Charaktere besitzen, alsdann auch die Zahlen $\Delta_h(F)$ aller aus $\Phi$ vermittels Substitutionen*

$$S^{\pm 1}_{(i,k)}: \qquad x_i = x_i', \quad x_k = \pm x_i' + x_k'$$

*hervorgehenden Formen $F$ dieselben Charaktere besitzen.*

Sind diese beiden Punkte festgestellt, so müssen die sämtlichen $(f_h)$ der Klasse $f$ wirklich die gegebenen Charaktere besitzen. Man sieht dieses auf der Stelle ein, indem man von dem bekannten Satze Gebrauch macht, daß eine jede ganzzahlige Substitution von der Determinante 1 sich in eine Reihe von Substitutionen $S^{\pm 1}_{(i,k)}$ zerlegen läßt. — Diesen allgemeinen Weg zur Entscheidung über die Existenz von Charakteren schlagen wir etzt in einigen Beispielen ein.

Blicken wir zunächst auf die Hauptrepräsentanten $\varphi$ für einen Modul $q^t$ zurück, so machen wir die folgenden Beobachtungen:

$(q = p)$. Wenn $o_h \equiv 0 \pmod p$ ist, so werden alle Zahlen $\Delta_h(\varphi)$ eines Hauptrepräsentanten $\varphi \pmod{p^t > p^{\nu_{n-1}(p)}}$ mit Ausnahme einer einzigen kongruent Null $(\mathrm{mod}\, p)$, und dieses eine zu $p$ prime $\Delta_h(\varphi)$ besitzt selbstverständlich einen bestimmten Charakter $\left(\frac{\Delta_h(\varphi)}{p}\right)$.

$(q = 2)$. Wenn $\sigma_{h-1} o_h \sigma_{h+1} \equiv 4 \pmod 8$ ist, so sind die $\Delta_h(\varphi)$ eines Hauptrepräsentanten $\varphi \pmod{2^t > \sigma_{n-1} \cdot 2^{\nu_{n-1}(2)}}$ zum Teil $\equiv 0 \pmod 4$, zum Teil $\equiv \delta\,(= \pm 1) \pmod 4$. Wenn $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod 8$ ist, so werden alle $\Delta_h(\varphi)$ eines Hauptrepräsentanten $\varphi \pmod{2^t > \sigma_{n-1} \cdot 2^{\nu_{n-1}(2)}}$ mit Ausnahme eines einzigen $\equiv 0 \pmod 4$, und dieses eine ist ungerade. Im Falle $\sigma_{h-1} o_h \sigma_{h+1} \equiv 4 \pmod 8$ besitzen also die ungeraden $\Delta_h(\varphi)$ einen Charakter $(-1)^{\frac{\Delta_h(\varphi)-1}{2}}$ und im Falle $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod 8$ zwei Charaktere $(-1)^{\frac{\Delta_h(\varphi)-1}{2}}$ und $\left(\frac{2}{\Delta_h(\varphi)}\right)$, während die geraden $\Delta_h(\varphi)$ in diesen beiden Fällen $\equiv 0 \pmod 4$ sind.

Diese Bemerkungen, welche sich unmittelbar aus der Gestalt der Hauptrepräsentanten $\varphi$ ergeben, lassen vermuten, daß einer Formenklasse $f$ im Falle $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod p$ ein Charakter $\left(\frac{(f_h)}{p}\right)$, im Falle $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod 4$ ein Charakter $(-1)^{\frac{(f_h)-1}{2}}$ und im Falle $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod 8$ ein Charakter $\left(\frac{2}{(f_h)}\right)$ angehört. Wir bestätigen diese Vermutung, indem wir den Satz beweisen:

Ist $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod p$ oder $\equiv 0 \pmod 4$ oder $\equiv 0 \pmod 8$, so besitzen die Größen $\Delta_h(F)$ einer Form $F$, welche aus einer anderen Form $\Phi (\sim f)$ vermittels einer Substitution $S_{(i,k)}^{\pm 1}$ hervorgeht, dieselben quadratischen Charaktere in bezug auf die Moduln $p$ oder 4 oder 8 wie die Zahlen $\Delta_h(\Phi)$.

Beweis: Die $h$-reihigen symmetrischen Unterdeterminanten der Form $F$,

$$\sigma_h d_{h-1} F_h = D_F \begin{pmatrix} k_0, & k_1, & \ldots, & k_{h-1} \\ k_0, & k_1, & \ldots, & k_{h-1} \end{pmatrix},$$

werden gleich den Größen

$$\sigma_h d_{h-1} \Phi_h = D_\Phi \begin{pmatrix} k_0, & k_1, & \ldots, & k_{h-1} \\ k_0, & k_1, & \ldots, & k_{h-1} \end{pmatrix}, \tag{6}$$

sobald sich unter den Zahlen $k_0, k_1, \ldots, k_{h-1}$ entweder sowohl $i$ als $k$ oder weder $i$ noch $k$ befinden; dagegen werden diese Determinanten gleich den Größen

$$D_\Phi \begin{pmatrix} i, & k_1, \ldots, & k_{h-1} \\ i, & k_1, \ldots, & k_{h-1} \end{pmatrix} \pm 2 D_\Phi \begin{pmatrix} i, & k_1, \ldots, & k_{h-1} \\ k, & k_1, \ldots, & k_{h-1} \end{pmatrix} + D_\Phi \begin{pmatrix} k, & k_1, \ldots, & k_{h-1} \\ k, & k_1, \ldots, & k_{h-1} \end{pmatrix} \tag{7}$$
$$= \sigma_h d_{h-1} \left( \Phi_h' \pm \frac{2}{\sigma_h} \Phi_h'^{,''} + \Phi_h'' \right),$$

sobald $k_0 = i$ wird. Es ist klar, daß unser Satz für diejenigen Zahlen $F_h$ statthat, welche aus den ersteren Größen $D_F$ entspringen, da sie mit gewissen der Zahlen $\Phi_h$ übereinstimmen. Die Zahlen $F_h$ dagegen, welche aus den letzteren Größen $D_F$ entspringen, gewinnen mit Hilfe des bekannten Determinantensatzes

$$D_\Phi \begin{pmatrix} i, & k_1, \ldots, & k_{h-1} \\ i, & k_1, \ldots, & k_{h-1} \end{pmatrix} D_\Phi \begin{pmatrix} k, & k_1, \ldots, & k_{h-1} \\ k, & k_1, \ldots, & k_{h-1} \end{pmatrix} - \left[ D_\Phi \begin{pmatrix} i, & k_1, \ldots, & k_{h-1} \\ k, & k_1, \ldots, & k_{h-1} \end{pmatrix} \right]^2$$
$$= D_\Phi \begin{pmatrix} k_1, \ldots, & k_{h-1} \\ k_1, \ldots, & k_{h-1} \end{pmatrix} D_\Phi \begin{pmatrix} i, & k, & k_1, \ldots, & k_{h-1} \\ i, & k, & k_1, \ldots, & k_{h-1} \end{pmatrix}$$

oder

$$\sigma_h^2 \Phi_h' \Phi_h'' - (\Phi_h'^{,''})^2 = \sigma_{h-1} o_h \sigma_{h+1} \cdot \Phi_{h-1} \Phi_{h+1}, \tag{8}$$

die Gestalt

$$F_h = \Phi_h' \left(1 \pm \frac{\Phi_h',''}{\sigma_h \Phi_h'}\right)^2 + \frac{\sigma_{h-1} o_h \sigma_{h+1} \cdot \Phi_{h-1}\Phi_{h+1}}{\sigma_h^2 \Phi_h'},$$

$$F_h = \Phi_h'' \left(1 \pm \frac{\Phi_h',''}{\sigma_h \Phi_h''}\right)^2 + \frac{\sigma_{h-1} o_h \sigma_{h+1} \cdot \Phi_{h-1}\Phi_{h+1}}{\sigma_h^2 \Phi_h''}.$$

Ist jetzt zunächst $o_h \equiv 0 \pmod p$, so sind die Zahlen $\Phi_h'$ und $\Phi_h''$ entweder beide $\equiv 0 \pmod p$, oder es wird wenigstens eine derselben relativ prim zu $p$. Im ersteren Falle wird infolge der Kongruenz

$$\sigma_h^2 \Phi_h' \Phi_h'' - (\Phi_h','')^2 \equiv 0 \pmod{o_h}$$

auch $\Phi_h','' \equiv 0 \pmod p$, und der Ausdruck $F_h = \Phi_h' \pm \frac{2}{\sigma_h} \Phi_h','' + \Phi_h''$ ist also gleichfalls $\equiv 0 \pmod p$; im letzteren Falle ist entweder

$$\frac{\sigma_{h-1} o_h \sigma_{h+1} \Phi_{h-1}\Phi_{h+1}}{\sigma_h^2 \Phi_h'} \quad \text{oder} \quad \frac{\sigma_{h-1} o_h \sigma_{h+1} \Phi_{h-1}\Phi_{h+1}}{\sigma_h^2 \Phi_h''}$$

durch $p$ teilbar, und $F_h$ erhält daher einen Wert

$$\equiv \Phi_h' \left(1 \pm \frac{\Phi_h',''}{\sigma_h \Phi_h'}\right)^2 \quad \text{oder} \quad \equiv \Phi_h'' \left(1 \pm \frac{\Phi_h',''}{\sigma_h \Phi_h''}\right)^2 \pmod p.$$

In beiden Fällen besitzt offenbar $F_h$ keinen andern quadratischen Charakter in bezug auf $p$ als die Zahlen $\Phi_h$.

Sobald $\sigma_{h-1} o_h \sigma_{h+1} \equiv 4 \pmod 8$ oder $\equiv 0 \pmod 8$ wird, ist die Zahl $\sigma_h$ immer gleich 1. Wird hier eine der Zahlen $\Phi_h'$, $\Phi_h''$ ungerade, so ist das betreffende $F_h$ nach dem Modul 4 oder 8 entweder

$$\equiv \Phi_h' \left(1 \pm \frac{\Phi_h',''}{\Phi_h'}\right)^2 \quad \text{oder} \quad \equiv \Phi_h'' \left(1 \pm \frac{\Phi_h',''}{\Phi_h''}\right)^2;$$

wenn dagegen $\Phi_h'$ sowohl als $\Phi_h''$ kongruent Null (mod 4) wird, so ist wegen $\Phi_h' \Phi_h'' - (\Phi_h','')^2 \equiv 0 \pmod{\sigma_{h-1} o_h \sigma_{h+1}}$ $\Phi_h',''$ gerade, und der Ausdruck $F_h = \Phi_h' \pm 2\Phi_h','' + \Phi_h''$ erhält gleichfalls einen Wert $\equiv 0 \pmod 4$. Demnach besitzen die $F_h$ immer dieselben quadratischen Charaktere für den Modul 4 oder 8 wie die $\Phi_h$.

Aus dem Satze II (Kap. V) ersehen wir noch, daß die Charaktere, welche wir soeben betrachtet haben, leicht aus einer jeden vorgelegten Form $f$ erschlossen werden können, ohne daß es nötig wäre, $f$ einer linearen Transformation zu unterwerfen. Denn sobald $o_h \equiv 0 \pmod p$ ist, gibt es unter den Größen $\Delta_h(f)$, welche ja selbst Zahlen $(f_h)$ sind, solche, die zu $p$ relativ prim werden und für die demnach $\left(\frac{\Delta_h(f)}{p}\right) = \left(\frac{(f_h)}{p}\right)$ ist; und ähnlich gibt es in den Fällen $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod 4$ oder $\equiv 0 \pmod 8$ unter den Größen $\Delta_h(f)$ immer ungerade, für welche also resp.

$$(-1)^{\frac{\Delta_h(f)-1}{2}} = (-1)^{\frac{(f_h)-1}{2}} \quad \text{und} \quad \left(\frac{2}{\Delta_h(f)}\right) = \left(\frac{2}{(f_h)}\right)$$

wird.

Eine zweite Methode zur Herleitung der Charaktere

$$\left(\frac{(f_h)}{p}\right), \quad (-1)^{\frac{(f_h)-1}{2}}, \quad \left(\frac{2}{(f_h)}\right)$$

ergibt sich unmittelbar aus den Formeln (2) und (3) des Kap. V.

Außer den Charakteren, die wir bisher gefunden haben, gibt es noch eine Reihe weiterer Charaktere, deren Existenz *mit Benutzung des quadratischen Reziprozitätsgesetzes* durch ein analoges Verfahren nachgewiesen werden kann. Wir behalten uns vor, die hierauf bezüglichen Bemerkungen bei einer anderen Gelegenheit ausführlicher darzulegen.

Jetzt wenden wir uns dazu, den Fall $h = 1$ der Kongruenzen $(f_h) \equiv m_h \pmod{N_0}$ zu diskutieren.

## Kap. VII. Über die Anzahl der Lösungen der Kongruenzen

$$f = \sum_{i,k=1}^{n} a_{ik} x_i x_k \equiv m \pmod{N}.$$

I. Wir bezeichnen die Anzahl sämtlicher für den Modul $N$ inkongruenten Lösungssysteme $(X_i)$ der Kongruenz

$$f = \sum_{i,k=1}^{n} a_{ik} X_i X_k \equiv m \pmod{N}$$

durch $f\{m; N\}$.

Gehören die Formen $f$ und $g$ zu derselben Gruppe nach einem Modul $N$, so wird

$$f\{m; N\} = g\{m; N\}. \tag{9}$$

Denn es möge die Form $f$ durch die Substitution $x_i = \sum_{k=1}^{n} s_k^i y_k$ in eine äquivalente Form $f_0 \equiv g \pmod{N}$ übergehen. Wir gewinnen dann aus einem jeden Systeme $(Y_k) \pmod{N}$, für welches $g(Y_k) \equiv f_0(Y_k) \equiv m \pmod{N}$ wird, ein bestimmtes System $X_i \equiv \sum_{k=1}^{n} s_i^k Y_k \pmod{N}$, für welches $f(X_i) \equiv m \pmod{N}$ wird, und aus zwei modulo $N$ verschiedenen Systemen $(Y_k)$ gewinnen wir wegen $|s_i^k| = 1$ stets zwei modulo $N$ verschiedene Systeme $(X_i)$. Folglich wird $f\{m; N\} \geqq g\{m; N\}$ sein. Aber auf dieselbe Weise schließt man $f\{m; N\} \leqq g\{m; N\}$, woraus sich die zu beweisende Gleichung ergibt.

Die verschiedenen Zahlen $f\{m; N\}$, welche einer bestimmten Form $f$ angehören, hängen einesteils von der Ordnung, andernteils von den Charakteren dieser Form ab. Um dies zu zeigen, tun wir gut, anstelle der

Größen $f\{m; N\}$, welche im allgemeinen ziemlich kompliziert ausfallen, Verbindungen derselben einzuführen, welche sich in einer einfacheren und übersichtlicheren Weise ausdrücken lassen. Zu solchen Verbindungen gelangen wir durch Hinzuziehung von Einheitswurzeln.

Es möge die Größe

$$e^{\frac{2\pi i}{N}} = \cos\frac{2\pi}{N} + i\sin\frac{2\pi}{N},$$

welche eine primitive $N^{\text{te}}$ Einheitswurzel vorstellt, gleich $r_N$ gesetzt werden. Wir wollen die Summen

$$(10)\qquad f\{1; N\}\, r_N^{1\cdot h} + f\{2; N\}\, r_N^{2\cdot h} + \cdots + f\{N; N\}\, r_N^{N\cdot h} = \sum_{m=1}^{N} f\{m; N\}\, r_N^{m\,h} = f(h; N)$$

betrachten, in welchen $h$ eine ganze Zahl bedeutet.

Infolge der Gleichung $r_N^N = 1$ nehmen diese Summen $f(h; N)$ für zwei nach dem Modul $N$ kongruente Zahlen $h$ gleiche Werte an. Erteilen wir der Größe $h$ die $N$ für den Modul $N$ inkongruenten Werte $1, 2, \ldots, N$, so entstehen im ganzen $N$ Größen

$$f(1; N),\quad f(2; N),\ \ldots,\ f(N; N),$$

durch welche sich umgekehrt die Zahlen $f\{m; N\}$ ausdrücken lassen. Wir bekommen

$$(11)\qquad f\{m; N\} = \frac{1}{N}\cdot\sum_{h=1}^{N} f(h; N)\, r_N^{-h\,m}.$$

Die Gleichungen (10) und (11) zeigen, daß die Untersuchung der Größen $f\{m; N\}$ vollständig auf eine Untersuchung der Größen $f(h; N)$ hinauskommt.

Für zwei nach dem Modul $N$ kongruente Formen $f$ und $g$ liefert die Gleichung (9) die Relationen $f(h; N) = g(h; N)$. Beachten wir, daß eine jede Form $g$, welche der Kongruenz $g \equiv f \pmod N$ genügt, einen Rest der Klasse $f$ in bezug auf den Modul $N$ vorstellt, so können wir den Satz aussprechen:

H. Ist $\varphi$ ein beliebiger Rest der Klasse $f$, so gelten die Gleichungen

$$f(h; N) = \varphi(h; N) \quad \text{und} \quad f\{m; N\} = \varphi\{m; N\}.$$

Es hat die Identität

$$(12)\qquad \sum_{m=1}^{N} f\{m; N\}\, r_N^{m\,h} = \sum_{\xi_i}^{1,N} r_N^{h\,f(\xi_i)}$$

statt, sobald in der zweiten Summe jede der Variablen $\xi_i$ ein vollständiges Restsystem nach dem Modul $N$ durchläuft. — Denn erteilen wir einer

jeden Größe $\xi_i$ die sämtlichen $N$ Werte $\equiv 1, 2, \ldots, N \pmod N$, so nimmt $f(\xi_i)$ je $f\{1; N\}$-mal einen Wert $\equiv 1 \pmod N$, je $f\{2; N\}$-mal einen Wert $\equiv 2 \pmod N$, usf., je $f\{N; N\}$-mal einen Wert $\equiv N \pmod N$ an. In der Summe $\sum_{\xi_i}^{1,N} r_N^{hf(\xi_i)}$ wird demnach je $f\{1; N\}$-mal ein Glied $r_N^{1\cdot h}$, je $f\{2; N\}$-mal ein Glied $r_N^{2\cdot h}$, usf., je $f\{N; N\}$-mal ein Glied $r_N^{N\cdot h}$ auftreten, und daraus ergibt sich die Gleichung (12).

Die Identität (12) liefert, mit der Gleichung (10) verbunden, eine neue Definition der Größen $f(h; N)$, nämlich

$$f(h; N) = \sum_{\xi_i}^{1,N} r_N^{hf(\xi_i)}.\text{*)}$$

Aus dieser Gleichung fließt leicht der folgende Hauptsatz, durch welchen die Bestimmung dieser Größen außerordentlich erleichtert wird:

J. *Wenn die quadratische Form $f$ nach dem Modul $N$ in eine Summe von quadratischen Formen $f_s$* [[*mit getrennten Variablen*]] *zerfällt:*

$$f(\xi_i) \equiv \sum_{s=1}^{s_0} f_s(\xi_k^{(s)}) \pmod N,$$

*so wird*

$$f(h; N) = \prod_{s=1}^{s_0} f_s(h; N).$$

Denn bezeichnen wir die Variablen der einzelnen Formen $f_s$ mit $\xi_k^{(s)}$, so erhalten wir die Relationen

$$f_s(h; N) = \sum_{\xi_k^{(s)}}^{1,N} r_N^{hf_s(\xi_k^{(s)})} \qquad (s = 1, 2, \ldots, s_0),$$

deren Multiplikation unmittelbar

$$\sum_{\xi_k^{(s)}}^{1,N} r_N^{h\sum_{s=1}^{s_0} f_s(\xi_k^{(s)})} = \sum_{\xi_i}^{1,N} r_N^{hf(\xi_i)} = f(h; N)$$

ergibt.

II. Die Größen $f(h; N)$ sind infolge der Beziehung $r_N^N = 1$ unabhängig von den besonderen Restsystemen, welche von den einzelnen Variablen $\xi_i$ durchlaufen werden. Wir schließen aus diesem Umstande die Sätze:

1) Wenn $N_0$ ein Teiler von $N$ ist, so gilt

$$f(h; N_0) = \left(\frac{N}{N_0}\right)^{-n} \cdot f\left(h\frac{N}{N_0}; N\right). \tag{13}$$

*) Die Summen $f(h; N)$ sind von Herrn Weber im Band 74 des Crelleschen Journals behandelt worden.

Bekanntlich setzt sich ein jedes vollständige Restsystem für den Modul $N$ aus $\frac{N}{N_0}$ vollständigen Restsystemen für den Modul $N_0$ zusammen. Es ist daher

$$\sum_{\xi_i}^{1,N} r_N^{h\frac{N}{N_0}f(\xi_i)} = \left(\frac{N}{N_0}\right)^n \cdot \sum_{\xi_i}^{1,N_0} r_{N_0}^{hf(\xi_i)},$$

und hieraus geht sofort die Gleichung (13) hervor. Wenn insbesondere $N$ eine Primzahlpotenz $q^t$ ist, so folgt für $t \geqq t_0$

$$f(h; q^{t_0}) = q^{-n(t-t_0)} \cdot f(hq^{t-t_0}; q^t).$$

2) Es ist

$$f(hZ^2; N) = f(h; N),$$

sobald $Z$ eine zu $N$ relativ prime Zahl bedeutet.

Wegen $f(Zx_i) = Z^2 f(x_i)$ ist die Größe $f(hZ^2; N)$ gleich der Summe

$$\sum_{x_i}^{1,N} r_N^{hf(Zx_i)}.$$

Setzen wir nun $Zx_i \equiv \xi_i \pmod N$, so werden offenbar die Zahlen $\xi_i$ zugleich mit den Zahlen $x_i$ vollständige Restsysteme nach dem Modul $N$ durchlaufen. Also wird diese Summe gleich $f(h; N)$ sein.

3) Wenn die Zahl $N$ ein Produkt aus $c_0$ zueinander relativ primen Zahlen $N_c$ ist, so wird

$$f(h; N) = \prod_{c=1}^{c_0} f\left(h\frac{N}{N_c}; N_c\right).$$

Beweis: Wir wollen die Zahlen $\frac{N}{N_c} = L_c$ setzen. Jede dieser Zahlen $L_c$ ist offenbar zu der entsprechenden Zahl $N_c$ relativ prim, während sie durch alle übrigen Größen $N_{c^*}\,(c^* \neq c)$ teilbar ist. Wenn wir in dem Ausdrucke

$$\xi \equiv L_1\xi^{(1)} + L_2\xi^{(2)} + \cdots + L_{c_0}\xi^{(c_0)} \pmod N$$

die Größen $\xi^{(c)}$ vollständige Restsysteme nach den Moduln $N_c$ durchlaufen lassen, so erhalten wir $N$ Zahlen, welche ein vollständiges Restsystem für den Modul $N$ bilden. Denn es können nicht zwei von diesen $N$ Zahlen nach dem Modul $N$ kongruent sein, da aus einer jeden Kongruenz

$$\sum L_c\xi^{(c)} \equiv \sum L_c\xi_0^{(c)} \pmod N$$

auf der Stelle

$$L_c\xi^{(c)} \equiv L_c\xi_0^{(c)} \pmod{N_c}$$

oder, weil die Zahlen $L_c$ zu den Größen $N_c$ relativ prim sind,

$$\xi^{(c)} \equiv \xi_0^{(c)} \pmod{N_c}$$

folgen würde. Wir dürfen demnach für die Größe $f(h; N)$ schreiben

$$f(h; N) = \sum_{\xi_i^{(c)}}^{1,N_c} r_N^{h \cdot f\left(\sum_{c=1}^{c_0} L_c \xi_i^{(c)}\right)}.$$

Durch Multiplikation der beiden Kongruenzen

$$\xi_i \equiv \sum_{c=1}^{c_0} L_c \xi_i^{(c)} \pmod N \quad \text{und} \quad \xi_k \equiv \sum_{c=1}^{c_0} L_c \xi_k^{(c)} \pmod N$$

erhalten wir, da das Produkt $L_c L_{c^*}$ für zwei ungleiche Indizes $c$ und $c^*$ gleich $N \cdot \frac{N}{N_c N_{c^*}} \equiv 0 \pmod N$ wird,

$$\xi_i \xi_k \equiv \sum_{c=1}^{c_0} L_c^2 \xi_i^{(c)} \xi_k^{(c)} \pmod N,$$

also

$$f\left(\sum_{c=1}^{c_0} L_c \xi_i^{(c)}\right) \equiv \sum_{c=1}^{c_0} L_c^2 f(\xi_i^{(c)}) \pmod N.$$

Demnach bekommen wir für $f(h; N)$ die Gleichung

$$f(h; N) = \sum_{\xi_i^{(c)}}^{1, N_c} r_N^{h \sum_{c=1}^{c_0} L_c^2 f(\xi_i^{(c)})} = \prod_{c=1}^{c_0} \left( \sum_{\xi_i^{(c)}}^{1, N_c} r_N^{h L_c^2 f(\xi_i^{(c)})} \right).$$

Die Einzelglieder des Produkts in dieser Formel sind jetzt wegen $r_N^{L_c} = r_{N_c}$ gleich $f(hL_c; N_c)$, und wir gewinnen wirklich die Identität, welche wir beweisen wollten.

Wählen wir für die Zahlen $N_c$ die verschiedenen in $N$ enthaltenen Primzahlpotenzen $q^t$, so können mit Hilfe des soeben bewiesenen Satzes die Größen $f(h; N)$ auf Größen $f(h; q^t)$ zurückgeführt werden. Es erhellt hieraus sofort, daß wir uns weiterhin auf die Betrachtung von Größen $f(h; q^t)$ für Primzahlpotenzmoduln $q^t$ beschränken dürfen. Wir brauchen ferner nur solche Moduln zu untersuchen, welche gewisse Grenzen $q^{G(q)}$ überschreiten. Denn es lassen sich mit Hilfe des Satzes 1) die Größen $f(h; q^{t_0})$ für Moduln $q^{t_0} < q^t$ stets durch Größen $f(h; q^t)$ ausdrücken.

III. Um die Größen $f(h; q^t)$ für einen Primzahlmodul $q^t$ zu finden, gehen wir von einem Hauptrest $\varphi$ der Klasse $f$ für den Modul $q^t$ aus. Die diesem Reste $\varphi$ angehörigen Größen $\varphi(h; q^t)$ sind nach dem Satz H. den Größen $f(h; q^t)$ gleich.

($q = p$). Wenn nun zunächst $q^t = p^t$ ist, so zerfällt der Hauptrest $\varphi \pmod{p^t}$ in eine Summe von Einzelformen von der Art

$$F \equiv p^M \alpha \xi^2 \pmod{p^t}, \qquad [\alpha \text{ relativ prim zu } p]$$

und die Größen $\varphi(h; p^t)$ können mit Hilfe des Satzes J. durch die Größen

$$F(h; p^t) = \sum_{\xi=1}^{p^t} e^{\frac{2\pi i p^M h \alpha \xi^2}{p^t}} = \sum_{\xi=1}^{p^t} e^{\frac{2\pi i \tau \xi^2}{p^t}} = (\tau; p^t) \qquad [\tau = p^M h \alpha]$$

dargestellt werden.

$(q = 2)$. Wenn hingegen $q^t = 2^t$ ist, so zerfällt der Hauptrest $\varphi \pmod{2^t}$ in eine Summe von Einzelformen von der Art

$$F \equiv 2^M \alpha \xi^2 \pmod{2^t} \qquad [\alpha \text{ relativ prim zu } 2]$$

oder von der Art

$$F_0 \equiv 2^M (\alpha \xi^2 + \mathfrak{A} \xi \tilde{\xi} + \tilde{\alpha} \tilde{\xi}^2) \pmod{2^t} \qquad [\mathfrak{A} \equiv 1 \pmod 2],$$

und die Größen $\varphi(h; 2^t)$ lassen sich mit Hilfe des Satzes J. durch die Größen

$$F(h; 2^t) = \sum_{\xi=1}^{2^t} e^{\frac{2\pi i 2^M h \alpha \xi^2}{2^t}} = \sum_{\xi=1}^{2^t} e^{\frac{2\pi i \tau \xi^2}{2^t}} = (\tau; 2^t) \qquad [\tau = 2^M h \alpha]$$

und durch Größen

$$F_0(h; 2^t) = \sum_{\xi, \tilde{\xi}=1}^{2^t} e^{\frac{2\pi i h 2^M}{2^t} (\alpha \xi^2 + \mathfrak{A} \xi \tilde{\xi} + \tilde{\alpha} \tilde{\xi}^2)}$$

darstellen.

## Kap. VIII. **Bestimmung der Größen $f(h; q^t)$ in den einfachsten Fällen.**

I. Vermittels der soeben aufgestellten Sätze können die allgemeinen Größen $f(h; q^t)$ stets auf die drei Summen

$$(\tau; p^t), \quad (\tau; 2^t), \quad F_0(h; 2^t)$$

zurückgeführt werden. Wir wollen jetzt der Reihe nach die Werte dieser Summen aufsuchen.

$(q = p)$. Wenn $\tau$ relativ prim zu $p$ ist, so beweist man leicht die Beziehung

$$(\tau; p) = \left(\frac{\tau}{p}\right) (1; p).$$

Um $(1; p)$ zu erhalten, betrachten wir einen Rest

$$\Phi \equiv x_1 x_2 \equiv \begin{pmatrix} 0, & 1 \\ 1, & 0 \end{pmatrix} \pmod p,$$

für welchen

$$\Phi(1; p) = \sum_{x_1=1}^{p} \sum_{x_2=1}^{p} e^{\frac{2\pi i x_1 x_2}{p}} = p$$

ist. Die Form $\Phi$ besitzt nach unseren Sätzen einen Hauptrepräsentanten

$$\Phi_0 \equiv \begin{pmatrix} a, & 0 \\ 0, & a_0 \end{pmatrix} \equiv a x^2 + a_0 x_0^2 \pmod p,$$

in welchem $a$ und $a_0$ zu $p$ relativ prim sind. Die Determinante dieses Repräsentanten $\Phi_0$ wird mit der Determinante von $\Phi$ nach dem Modul $p$ übereinstimmen müssen; wir erhalten daher

$$aa_0 \equiv -1 \pmod{p},$$

und es ist für die Form $\Phi_0$

$$\Phi_0(1;p) = \sum_{x=1}^{p} e^{\frac{2\pi i a x^2}{p}} \cdot \sum_{x_0=1}^{p} e^{\frac{2\pi i a_0 x_0^2}{p}} = \left(\frac{aa_0}{p}\right)(1;p)^2 = (-1)^{\frac{p-1}{2}}(1;p)^2.$$

Da nun wegen $\Phi \simeq \Phi_0 \pmod{p}$ die Größen $\Phi(1;p)$ und $\Phi_0(1;p)$ identisch sein müssen, so bekommen wir die Gleichung

$$(1;p)^2 = (-1)^{\frac{p-1}{2}} p,$$

und wir können mithin

$$(1;p) = i^{\left(\frac{p-1}{2}\right)^2} p^{\frac{1}{2}} \delta_p$$

setzen, wo die Größe $\delta_p$ eine nur von $p$ abhängige Einheit bezeichnet. Bekanntlich ist diese Einheit stets gleich $+1$.

Vermittels der Größe $(1;p)$ kann man leicht die allgemeine Summe $(\tau;p^t)$ ausdrücken, und wenn man $\tau = p^T\tau_0$ ($\tau_0$ relativ prim zu $p$) setzt, erhält man die Gleichungen

$(14_0)$ für $t-T \leqq 0$: $\quad (\tau;p^t) = p^t,$

$(14_1)$ für $t-T > 0$: $\quad (\tau;p^t) = \left(\frac{\tau_0}{p}\right)^{t-T} p^{\frac{t+T}{2}} i^{\frac{1}{4}(p^{t-T}-1)^2} \delta_p^{t-T}.$

($q=2$). Für die Summe $(\tau;2^t)$ gelten, wenn man $\tau = 2^T\tau_0 [\tau_0 \equiv 1 \pmod 2]$ setzt, die Formeln

$(15_0)$ für $t-T < 1$: $\quad (\tau;2^t) = 2^t,$

$(15_1)$ für $t-T = 1$: $\quad (\tau;2^t) = 0,$

$(15_2)$ für $t-T > 1$: $\quad (\tau;2^t) = \left(1 + i(-1)^{\frac{\tau_0-1}{2}}\right)\left(\frac{2}{\tau_0}\right)^{t-T} 2^{\frac{t+T}{2}}.$*)

---

Mit Hilfe der Summen $(\tau;2^t)$ können wir jetzt den Wert der Summe

$$\Sigma = \sum_{\xi,\tilde{\xi}=1}^{2^t} e^{\frac{2\pi i\tau}{2^t}(\alpha\xi^2 + \mathfrak{A}\xi\tilde{\xi} + \tilde{\alpha}\tilde{\xi}^2)} \qquad [\mathfrak{A} \equiv 1 \pmod 2]$$

bestimmen. Wir wollen die Größe $4\alpha\tilde{\alpha} - \mathfrak{A}^2$ durch $D$ bezeichnen.

Es möge zunächst $\tau$ ungerade und $t \geqq 1$ sein. Für einen Rest von der Art

$$\Phi \equiv \xi_0^2 + 2\tau(\alpha\xi^2 + \mathfrak{A}\xi\tilde{\xi} + \tilde{\alpha}\tilde{\xi}^2) \equiv \begin{pmatrix} 1, & 0, & 0 \\ 0, & 2\tau\alpha, & \tau\mathfrak{A} \\ 0, & \tau\mathfrak{A}, & 2\tau\tilde{\alpha} \end{pmatrix} \pmod{2^{t+1}}$$

---

*) Gauß, Summatio quarundam serierum singularium. Gesammelte Werke, Bd. II.

wird

$$\Phi(1; 2^{t+1}) = 4 \sum_{\xi_0=1}^{2^{t+1}} e^{\frac{2\pi i \xi_0^2}{2^{t+1}}} \cdot \sum_{\xi, \bar{\xi}=1}^{2^t} e^{\frac{2\pi i \tau}{2^t}(\alpha \xi^2 + \mathfrak{A} \xi \bar{\xi} + \bar{\alpha} \bar{\xi}^2)} = 4 \cdot (1; 2^{t+1}) \Sigma.$$

Die Summe $(1; 2^{t+1})$ erhält nach der Gleichung $(15_2)$, da $t+1$ nach unserer Annahme größer als 1 ist, den Wert $(1+i)2^{\frac{t+1}{2}}$, und wir bekommen daher

$$\Phi(1; 2^{t+1}) = 2^{\frac{t+5}{2}}(1+i)\Sigma.$$

Die Form $\Phi$ besitzt, da ihre Determinante ungerade ist und ihre beiden Invarianten $\sigma$ gleich 1 sind, für den Modul $2^{t+1}$ einen Hauptrepräsentanten von der Art

$$\Phi_0 \equiv \begin{pmatrix} a_1, 0, 0 \\ 0, a_2, 0 \\ 0, 0, a_3 \end{pmatrix} \equiv a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 \pmod{2^{t+1}},$$

in welchem die Größen $a_1$, $a_2$, $a_3$ ungerade sind. Da die Determinante der Form $\Phi_0$ der Determinante von $\Phi$ für den Modul $2^{t+1}$ kongruent wird, so besteht die Kongruenz

$$a_1 a_2 a_3 \equiv D \cdot \tau^2 \pmod{2^{t+1}},$$

aus welcher

$$a_1 a_2 a_3 \equiv -1 \pmod 4$$

folgt.

Es müssen demnach von den Größen $a_1$, $a_2$, $a_3$ entweder eine oder drei $\equiv -1 \pmod 4$ sein; wir erkennen leicht, daß der erste oder der zweite Fall eintritt, je nachdem die Einheit

$$\delta = (-1)^{\frac{a_2-1}{2}\cdot\frac{a_3-1}{2} + \frac{a_3-1}{2}\cdot\frac{a_1-1}{2} + \frac{a_1-1}{2}\cdot\frac{a_2-1}{2}}$$

gleich $+1$ oder gleich $-1$ ist. Um zu entscheiden, welchen Wert diese Einheit annimmt, beachten wir, daß die Kongruenzen $\Phi \equiv 1 \pmod 4$ und $\Phi_0 \equiv 1 \pmod 4$ wegen $\Phi \simeq \Phi_0 \pmod{2^{t+1} \geqq 4}$ gleich viel Lösungen zulassen müssen. Nun finden wir die Anzahl der Lösungen der Kongruenz $\Phi \equiv 1 \pmod 4$ gleich $2^4\left[1 + \frac{1}{2}\left(\frac{2}{D}\right)\right]$ und die Anzahl der Lösungen von $\Phi_0 \equiv 1 \pmod 4$ gleich $2^4\left(1 + \frac{1}{2}\delta\right)$; es wird daher die Beziehung

$$\delta = \left(\frac{2}{D}\right)$$

bestehen. Für den Formenrest $\Phi_0$ ergibt sich

$$\Phi_0(1; 2^{t+1}) = (a_1; 2^{t+1}) \cdot (a_2; 2^{t+1}) \cdot (a_3; 2^{t+1}).$$

Mit Hilfe der Formel $(15_2)$ schließen wir hieraus, da $t+1 > 1$ ist,

$$\Phi_0(1;2^{t+1}) = \left[1+i(-1)^{\frac{a_1-1}{2}}\right]\left[1+i(-1)^{\frac{a_2-1}{2}}\right]\left[1+i(-1)^{\frac{a_3-1}{2}}\right]\cdot \cdot\left(\frac{2}{a_1a_2a_3}\right)^{t+1}2^{\frac{3t+3}{2}}.$$

Aus der Kongruenz $D\cdot\tau^2 \equiv a_1a_2a_3 \pmod{2^{t+1}\geqq 4}$ gewinnen wir die Gleichung

$$\left(\frac{2}{a_1a_2a_3}\right)^{t+1} = \left(\frac{2}{D}\right)^{t+1};$$

ferner finden wir

$$\left[1+i(-1)^{\frac{a_1-1}{2}}\right]\left[1+i(-1)^{\frac{a_2-1}{2}}\right]\left[1+i(-1)^{\frac{a_3-1}{2}}\right] = 2(1+i)\delta = 2(1+i)\left(\frac{2}{D}\right)$$

Also wird

$$\Phi_0(1;2^{t+1}) = \left(\frac{2}{D}\right)^t(1+i)2^{\frac{3t+5}{2}}.$$

Da nun wegen $\Phi \overset{\sim}{\sim} \Phi_0 \pmod{2^{t+1}}$ die Größen $\Phi(1;2^{t+1})$ und $\Phi_0(1;2^{t+1}$ einander gleich sind, so erhalten wir

$$\Sigma = \left(\frac{2}{D}\right)^t 2^t.$$

Wenn die Größe $\tau$ durch eine Potenz von 2 teilbar ist, so können wir $\tau$ in der Form $\tau = 2^T\tau_0\,[\tau_0 \equiv 1 \pmod 2]$ darstellen, und wir bekommen alsdann die beiden Formeln

$(16_0)$ für $t-T \leqq 0$: $\quad \Sigma = 2^{2t}$,

$(16_1)$ für $t-T > 0$: $\quad \Sigma = \left(\frac{2}{D}\right)^{t-T}2^{t+T}$.

II. Wir benutzen jetzt die gefundenen Summen zur Bestimmung von Größen $\varphi(h;q^t)$ für einige besonders einfache Reste $\varphi \pmod{q^t}$. Wir stellen die Zahl $h$ in der Form $h = q^{\bar{h}}h_0$ ($h_0$ relativ prim zu $q$) dar.

($q = p$). Die Größen $F(h;p^t)$ eines Restes $F \equiv p^M\alpha\xi^2 \pmod{p^t}$ [$\alpha$ relativ prim zu $p$] sind durch die Gleichungen

$$F(h;p^t) = (hp^M\alpha;p^t)$$

gegeben. Es ergeben sich die Formeln

für $\bar{h} \geqq t-M$: $\quad F(h;p^t) = p^t$,

für $\bar{h} < t-M$: $\quad F(h;p^t) = \left(\frac{h_0\alpha}{p}\right)^{t-M-\bar{h}} p^{\frac{t+M+\bar{h}}{2}} i^{\frac{1}{4}(p^{t-M-\bar{h}}-1)^2}\delta_p^{\,t-M-\bar{h}}$.

Die Größen $\varphi(h;p^t)$, welche einem Rest

$$\varphi \equiv p^M(\alpha_1\xi_1^{\,2}+\alpha_2\xi_2^{\,2}+\cdots+\alpha_\varkappa\xi_\varkappa^{\,2}) \equiv \sum_{i=1}^{\varkappa} p^M\alpha_i\xi_i^{\,2} \equiv \sum_{i=1}^{\varkappa} F_i \pmod{p^t}$$

angehören, genügen den Relationen

$$\varphi(h;p^t) = \prod_{i=1}^{\varkappa} F_i(h;p^t).$$

Setzen wir das Produkt $\prod_{i=1}^{\varkappa}\alpha_i \equiv (\varphi) \pmod{p^{t-M}}$, so gewinnen wir die Formeln

für $\bar{h} \geqq t-M$: $\qquad \varphi(h;p^t) = p^{\varkappa t}$,

für $\bar{h} < t-M$:

$$\varphi(h;p^t) = \left(\frac{(\varphi)}{p}\right)^{t-M-\bar{h}} p^{\frac{\varkappa(t+M+\bar{h})}{2}} \left(\frac{h_0}{p}\right)^{\varkappa(t-M-\bar{h})} i^{\frac{\varkappa}{4}(p^{t-M-\bar{h}}-1)^2} \delta_p^{\varkappa(t-M-\bar{h})}.$$

Aus denselben ersehen wir, daß die Größen $\varphi(h;p^t)$ sich in zwei Faktoren zerlegen lassen, von denen der erste eine Einheit vorstellt, während der zweite dem absoluten Werte nach mit $\varphi(h;p^t)$ übereinstimmt und allein von den Größen $h$, $p^t$; $\varkappa$, $M$ abhängt. Bezeichnen wir diesen zweiten Faktor durch $\overset{0}{\varphi}(h;p^t)$, so erhalten wir die Formeln

für $\bar{h} \geqq t-M$: $\qquad \varphi(h;p^t) = \overset{0}{\varphi}(h;p^t)$,

für $\bar{h} < t-M$: $\qquad \varphi(h;p^t) = \left(\frac{(\varphi)}{p}\right)^{t-M-\bar{h}} \cdot \overset{0}{\varphi}(h;p^t)$.

($q=2$). Die Größen $F(h;2^t)$ eines Restes $F \equiv 2^M\alpha\xi^2 \pmod{2^t}$ [$\alpha$ relativ prim zu 2] haben die Werte

$$F(h;2^t) = (h2^M\alpha;2^t),$$

und es ergeben sich die drei Formeln

für $\bar{h} > t-1-M$: $\qquad F(h;2^t) = 2^t$,

für $\bar{h} = t-1-M$: $\qquad F(h;2^t) = 0$,

für $\bar{h} < t-1-M$: $\quad F(h;2^t) = \left[1+i(-1)^{\frac{h_0\alpha-1}{2}}\right]\left(\frac{2}{h_0\alpha}\right)^{t-M-\bar{h}} 2^{\frac{t+M+\bar{h}}{2}}$.

Die Größen $\varphi(h;2^t)$ eines Restes

$$\varphi \equiv 2^M(\alpha_1\xi_1^2 + \alpha_2\xi_2^2 + \cdots + \alpha_\varkappa\xi_\varkappa^2) \equiv \sum_{i=1}^{\varkappa} 2^M\alpha_i\xi_i^2 \equiv \sum_{i=1}^{\varkappa} F_i \pmod{2^t}$$

genügen den Gleichungen

$$\varphi(h;2^t) = \prod_{i=1}^{\varkappa} F_i(h;2^t).$$

Setzen wir das Produkt $\prod_{i=1}^{\varkappa}\alpha_i \equiv (\varphi) \pmod{2^{t-M}}$, so folgen die Relationen

$$(17)\begin{cases} \text{für } \bar{h} > t-1-M: & \varphi(h;2^t) = 2^{\varkappa t}, \\ \text{für } \bar{h} = t-1-M: & \varphi(h;2^t) = 0, \\ \text{für } \bar{h} < t-1-M: & \\ \varphi(h;2^t) = \prod_{i=1}^{\varkappa}\left[1+i(-1)^{\frac{h_0\alpha_i-1}{2}}\right] \cdot \left(\frac{2}{(\varphi)}\right)^{t-M-\bar{h}} \left(\frac{2}{h_0}\right)^{\varkappa(t-M-\bar{h})} 2^{\frac{\varkappa(t+M+\bar{h})}{2}}. \end{cases}$$

Die Größen $\Phi(h; 2^t)$ eines Restes

$$\Phi \equiv 2^M\Big(\sum_1^{l_1}\alpha_i^{(1)}\xi_i^{(1)}\xi_i^{(1)} + 2\sum_1^{l_2}\alpha_i^{(2)}\xi_i^{(2)}\xi_i^{(2)} + \cdots + 2^{m-1}\sum_1^{l_m}\alpha_i^{(m)}\xi_i^{(m)}\xi_i^{(m)}\Big)$$

$$\equiv \sum_{s=1}^{m}\Big(2^{M+s-1}\sum_{i=1}^{l_s}\alpha_i^{(s)}\xi_i^{(s)}\xi_i^{(s)}\Big) \equiv \sum_{s=1}^{m}\varphi_s \pmod{2^t}$$

$$[l_s > 0,\ l_1 + l_2 + \cdots + l_m = l]$$

sind gleich

$$\Phi(h; 2^t) = \prod_{s=1}^{m}\varphi_s(h; 2^t).$$

Aus den Beziehungen (17) schließen wir für die einzelnen Reste $\varphi_s$ die Gleichungen

$(18_0)$ für $\bar{h} > t - s - M$: $\quad \varphi_s(h; 2^t) = 2^{l_s t}$,

$(18_1)$ für $\bar{h} = t - s - M$: $\quad \varphi_s(h; 2^t) = 0$,

$(18_2)$ für $\bar{h} < t - s - M$:

$$\varphi_s(h; 2^t) = \prod_{i=1}^{l_s}\Big[1 + i(-1)^{\frac{h_0\alpha_i^{(s)}-1}{2}}\Big]\cdot\Big(\frac{2}{(\varphi_s)}\Big)^{t-M-s-1-\bar{h}} 2^{l_s\frac{t+M+s-1+\bar{h}}{2}}\Big(\frac{2}{\bar{h}_0}\Big)^{l_s(t-M-s-1-\bar{h})}.$$

Wenn $\bar{h} \geqq t - M$ ist, so haben für die sämtlichen Größen $\varphi_s(h; 2^t)$ die Relationen $(18_0)$ statt. In diesem Falle findet sich daher

$(19_0)$ für $\bar{h} \geqq t - M$: $\quad \Phi(h; 2^t) = 2^{lt}$.

Befriedigt die Zahl $\bar{h}$ die Ungleichung $t - M > \bar{h} \geqq t - m - M$, so können wir eine Zahl $m_0$ aus der Reihe $1, 2, \ldots, m$ angeben, für welche $\bar{h} = t - m_0 - M$ ist. Dann tritt für die Größe $\varphi_{m_0}(h; 2^t)$ des Restes $\varphi_{m_0}$, welcher dieser Zahl $m_0$ entspricht, die Gleichung $(18_1)$ in Kraft, und es verschwindet daher diese Größe $\varphi_{m_0}(h; 2^t)$. Demnach wird auch $\Phi(h; 2^t)$ gleich Null, und wir bekommen

$(19_1)$ für $t - M > \bar{h} \geqq t - m - M$: $\quad \Phi(h; 2^t) = 0$.

Fällt die Zahl $\bar{h}$ kleiner als $t - m - M$ aus, so gelten für die sämtlichen Größen $\varphi_s(h; 2^t)$ die Gleichungen $(18_2)$; es ergibt sich, wenn wir $\prod_{s=1}^{m}(\varphi_s) \equiv (\Phi) \pmod{2^{t-M-m+1}}$ setzen,

$(19_2)$ für $t - m - M > \bar{h}$:

$$\Phi(h; 2^t) = \prod_{s=1}^{m}\prod_{i=1}^{l_s}\Big[1 + i(-1)^{\frac{h_0\alpha_i^{(s)}-1}{2}}\Big]\cdot\left\{\Big(\frac{2}{(\varphi_{m-1})}\Big)\Big(\frac{2}{(\varphi_{m-3})}\Big)\cdots\Big(\frac{2}{\left(\varphi_{m+1-2\left[\frac{m}{2}\right]}\right)}\Big)\right\}\cdot$$

$$\cdot\Big(\frac{2}{(\Phi)}\Big)^{t-M-m-1-\bar{h}} 2^{\sum_{s=1}^{m}l_s\frac{t+M+s-1+\bar{h}}{2}}\Big(\frac{2}{\bar{h}_0}\Big)^{\sum_{s=1}^{m}l_s(t-M-s-1-\bar{h})}.$$

Das in dieser letzten Formel auftretende Produkt

$$\prod\left[1+i(-1)^{\frac{l_0\alpha_i^{(s)}-1}{2}}\right]$$

besitzt die Gestalt

$$\Pi=\prod_{k=1}^{l}\left[1+i(-1)^{\frac{\delta_k-1}{2}}\right].$$

Wir wollen jetzt nachsehen, von welchen Argumenten ein derartiges Produkt eigentlich abhängt. — Nehmen wir an, von den Größen $(-1)^{\frac{\delta_k-1}{2}}$ seien im ganzen $l_0$ gleich $-1$ und $l-l_0$ gleich $+1$, so erhält $\Pi$ den Wert

$$\Pi=(1+i)^{l-l_0}(1-i)^{l_0}$$

oder wegen der Beziehung $(1-i)=-i(1+i)$ den Wert

$$\Pi=(-1)^{l_0}i^{l_0}(1+i)^{l}.$$

Nun ist

$$i^{l_0}=i^{2\left[\frac{l_0}{2}\right]}i^{l_0-2\left[\frac{l_0}{2}\right]}=(-1)^{\left[\frac{l_0}{2}\right]}i^{l_0-2\left[\frac{l_0}{2}\right]},$$

und die Größe $i^{l_0-2\left[\frac{l_0}{2}\right]}$ wird offenbar gleich 1 oder gleich $i$, je nachdem $l_0$ gerade oder ungerade ist. Wir können daher schreiben

$$i^{l_0-2\left[\frac{l_0}{2}\right]}=\frac{1+(-1)^{l_0}}{2}+\frac{1-(-1)^{l_0}}{2}i=i^{l_0^2},$$

und wir bekommen die Gleichung

$$\Pi=(-1)^{\left[\frac{l_0}{2}\right]}\left[\frac{1+(-1)^{l_0}}{2}-\frac{1-(-1)^{l_0}}{2}i\right](1+i)^{l}.$$

Dieselbe zeigt uns, daß einerseits das Produkt $\Pi$ durch die Zahl $l$ und die beiden Einheiten $(-1)^{l_0}$ und $(-1)^{\left[\frac{l_0}{2}\right]}$ vollständig bestimmt ist, während andererseits aus dem Werte von $\Pi$ die Werte der Größen $l$, $(-1)^{l_0}$, $(-1)^{\left[\frac{l_0}{2}\right]}$ erschlossen werden können.

Die Einheiten $(-1)^{l_0}$, $(-1)^{\left[\frac{l_0}{2}\right]}$ lassen sich in der folgenden Weise durch die Einheiten $(-1)^{\frac{\delta_k-1}{2}}$ ausdrücken:

$$(-1)^{l_0}=(-1)^{\sum_{k=1}^{l}\frac{\delta_k-1}{2}},\quad (-1)^{\left[\frac{l_0}{2}\right]}=(-1)^{\sum_{k'<k''}^{1,l}\frac{\delta_{k'}-1}{2}\cdot\frac{\delta_{k''}-1}{2}}.$$

Denn da erstens $\frac{\delta_k-1}{2}$ gerade oder ungerade wird, je nachdem $(-1)^{\frac{\delta_k-1}{2}}$ gleich $+1$ oder gleich $-1$ ist, so erscheinen in der Summe $\sum\frac{\delta_k-1}{2}$,

welche sich über alle Zahlen $\frac{\delta_k - 1}{2}$ erstreckt, im ganzen $l - l_0$ gerade und $l_0$ ungerade Glieder; die Summe ist daher $\equiv l_0 \pmod 2$. — Zweitens wird die Größe $\frac{\delta_{k'} - 1}{2} \cdot \frac{\delta_{k''} - 1}{2}$ ungerade oder gerade, je nachdem die Zahlen $(-1)^{\frac{\delta_{k'} - 1}{2}}$ und $(-1)^{\frac{\delta_{k''} - 1}{2}}$ alle beide gleich $-1$ sind oder das Gegenteil stattfindet. Bilden wir daher die Summe $\sum \frac{\delta_{k'} - 1}{2} \cdot \frac{\delta_{k''} - 1}{2}$ über alle möglichen Kombinationen zweier verschiedener Indizes $k'$ und $k''$, so treten in dieser Summe genau soviel ungerade Glieder auf, als Verbindungen von je zwei Größen $(-1)^{\frac{\delta_{k'} - 1}{2}} = -1$ und $(-1)^{\frac{\delta_{k''} - 1}{2}} = -1$ existieren. Unter den $l_0$ Zahlen $(-1)^{\frac{\delta_k - 1}{2}}$, welche gleich $-1$ sind, gibt es nun offenbar im ganzen $\frac{l_0 (l_0 - 1)}{2}$ $\left\{\equiv \left[\frac{l_0}{2}\right] \pmod 2\right\}$ derartige Verbindungen, und es wird demnach

$$\sum_{k' < k''}^{1, l} \frac{\delta_{k'} - 1}{2} \cdot \frac{\delta_{k''} - 1}{2} \equiv \left[\frac{l_0}{2}\right] \pmod 2.$$

Anstatt der Formel $(19_2)$ erhalten wir jetzt für $t - m - M > \bar{h}$:

$$(19_3) \quad \left\{ \begin{aligned} \Phi(h; 2^t) = {} & \left[\frac{1 + (-1)^{\frac{(\Phi) - 1}{2}}}{2} - \frac{1 - (-1)^{\frac{(\Phi) - 1}{2}}}{2} i\right] (-1)^{\frac{(\Phi) - 1}{2} \cdot \frac{h_0 - 1}{2}} \cdot \\ & \cdot \left(\frac{2}{(\Phi)}\right)^{t - M - m - 1 - \bar{h}} \left(\frac{2}{(\varphi_{m-1})}\right) \left(\frac{2}{(\varphi_{m-3})}\right) \cdots \left(\frac{2}{\left(\varphi_{m+1-2\left[\frac{m}{2}\right]}\right)}\right) \cdot \\ & \cdot (-1)^{\frac{1}{2} \cdot \sum_{(i', s') \neq (i'', s'')} \frac{\alpha_{i'}^{s'} - 1}{2} \cdot \frac{\alpha_{i''}^{s''} - 1}{2}} (1 + i)^l 2^{\sum_{s=1}^{m} l_s \frac{t + M + s - 1 + \bar{h}}{2}} (-i)^{l \left(\frac{h_0 - 1}{2}\right)^2} \cdot \\ & \cdot \left(\frac{2}{h_0}\right)^{\sum_{s=1}^{m} l_s (t - M - s - 1 - \bar{h})} . \end{aligned} \right.$$

Wir sehen, daß alle nicht-verschwindenden Größen $\Phi(h; 2^t)$ sich in zwei Faktoren zerlegen lassen, von denen der erste eine Potenz von $i = \sqrt{-1}$ ist, während der zweite dem absoluten Werte nach mit $\Phi(h; 2^t)$ übereinstimmt und allein von den Größen $h$, $2^t$; $m$, $l_s$, $M$ abhängt. Setzen wir diesen zweiten Faktor gleich $\overset{0}{\Phi}(h; 2^t)$, so gewinnen wir die Formeln

$(20_0)$ für $\bar{h} \geqq t - M$: $\quad \Phi(h; 2^t) = \overset{0}{\Phi}(h; 2^t)$,

$(20_1)$ für $t - M > \bar{h} \geqq t - m - M$: $\quad \Phi(h; 2^t) = 0$,

$(20_2)$ für $t - m - M > \bar{h}$:

$$\Phi(h;2^t) = \overset{0}{\Phi}(h;2^t)\left[\frac{1+(-1)^{\frac{(\Phi)-1}{2}}}{2} - \frac{1-(-1)^{\frac{(\Phi)-1}{2}}}{2}i\right]\cdot$$

$$\cdot(-1)^{\frac{(\Phi)-1}{2}\cdot\frac{h_0-1}{2}}\left(\frac{2}{(\Phi)}\right)^{t-M-m-1-\bar{h}}\left(\frac{2}{(\varphi_{m-1})}\right)\left(\frac{2}{(\varphi_{m-3})}\right)\cdots\left(\frac{2}{\left(\varphi_{m+1-2\left[\frac{m}{2}\right]}\right)}\right)$$

$$\cdot(-1)^{\frac{1}{2}\cdot\sum_{(i',s')\neq(i'',s'')}\frac{\alpha_{i'}^{s'}-1}{2}\cdot\frac{\alpha_{i''}^{s''}-1}{2}}.$$

Von Bedeutung für die Folge ist die Bemerkung, daß sowohl im Falle $l=1$ als im Falle $l=2$, $(-1)^{\frac{(\Phi)-1}{2}} = -1$ die Einheit

$$(-1)^{\frac{1}{2}\sum\frac{\alpha_{i'}^{s'}-1}{2}\cdot\frac{\alpha_{i''}^{s''}-1}{2}}$$

gleich $+1$ gesetzt werden muß.

---

Für die Größen $\Phi(h;2^t)$ eines Restes

$$\Phi \equiv 2^M(\alpha\xi^2 + \mathfrak{A}\xi\tilde{\xi} + \tilde{\alpha}\tilde{\xi}^2) \pmod{2^t}$$

gelten, wenn wir $4\alpha\tilde{\alpha} - \mathfrak{A}^2 \equiv (\Phi) \pmod{2^{2+t-M}}$ setzen, die Formeln

für $\bar{h} \geqq t-M$: $\quad \Phi(h;2^t) = 2^{2t} = \overset{0}{\Phi}(h;2^t)$,

für $\bar{h} < t-M$:

$$\Phi(h;2^t) = \left(\frac{2}{(\Phi)}\right)^{t-M-\bar{h}} 2^{t+M+\bar{h}} = \overset{0}{\Phi}(h;2^t)\cdot\left(\frac{2}{(\Phi)}\right)^{t-M-\bar{h}},$$

worin die Größen $\overset{0}{\Phi}(h;2^t)$ allein von den Zahlen $h$, $2^t$; $M$ abhängen.

## Kap. IX. **Charaktere der Hauptrepräsentanten und der Grundformen.**

Wir werden jetzt nachweisen, daß die Größen $f(h;q^t)$ einer allgemeinen Form $f$ ebenso wie die Größen $\varphi(h;q^t)$ der besonderen Reste $\varphi$, welche wir soeben betrachtet haben, in zwei Faktoren von wesentlich verschiedener Art zerfallen. Der eine dieser Faktoren, den man durch $\overset{0}{f}(h;q^t)$ bezeichnen kann, hängt, wenn $q=p$ ist, allein von den Zahlen $p^{\omega_k}$, und wenn $q=2$ ist, allein von den Zahlen $2^{\omega_k}$ und $\sigma_k$ ab, während der zweite sich im Falle $q=p$ mittels einer, im Falle $q=2$ mittels einer oder zweier Einheiten $C$ darstellen läßt. — Diese Einheiten $C$ werden sich dann umgekehrt durch Größen $f(h;q^t)$ und $\overset{0}{f}(h;q^t)$ ausdrücken lassen. Da aber sowohl die Größen $f(h;q^t)$ als die Größen $\overset{0}{f}(h;q^t)$ für alle in bezug auf den Modul $q^t$ kongruenten Formenklassen $f$ gleiche Werte erhalten, so werden auch die Einheiten $C$ für alle nach

dem Modul $q^t$ kongruenten Formenklassen $f$ die gleichen Werte annehmen, d. h. diese Einheiten werden Charaktere der Formen $f$ vorstellen.

Die Charaktere $C$, zu welchen wir auf diese Weise gelangen, werden sich zunächst als Funktionen der Koeffizienten eines Hauptrestes $\varphi \pmod{q^t}$ darstellen. Nun haben wir aber in Kap. V gesehen, erstens, daß wir die Koeffizienten eines Hauptrestes $\varphi$ durch die $n+1$ Zahlen $\varphi_h$ eines zum Hauptreste $\varphi$ gehörigen Hauptrepräsentanten ausdrücken können, und zweitens, daß sich eine jede Grundform $\psi \pmod{q}$ einer Klasse $f$ in einen Hauptrepräsentanten $\varphi \pmod{q^t}$ transformieren läßt, dessen Zahlen $\varphi_h$ den Zahlen $\psi_h$ gleich sind. Wir können demnach auch die Einheiten $C$ durch die Zahlen $\varphi_h$ eines Hauptrepräsentanten $\varphi$ ausdrücken, und wir werden alsdann die Werte dieser Einheiten unmittelbar aus einer jeden beliebigen Grundform $\psi \pmod{q}$ herleiten können.

I. Es möge zunächst $q = p$ sein, und es sei $f$ eine in bezug auf $p$ primitive Form. Jeder Hauptrest $\varphi$ der Klasse $f$ für einen Modul $p^t$ $(> p^{v_{n-1}(p)})$ besitzt dann die Gestalt

$$\varphi \equiv \varphi_1 + \varphi_2 + \cdots + \varphi_\lambda = \sum_{i=1}^{\lambda} \varphi_i \pmod{p^t},$$

$$\varphi_i \equiv p^{v_{\vartheta_i - 1}} \sum_{s=1}^{\varkappa_i} \alpha_s^{(i)} \xi_s^{(i)} \xi_s^{(i)} \pmod{p^t}.$$

Wir finden daher nach Satz J. in Kap. VII die Größen $\varphi(h; p^t) = f(h; p^t)$ durch die Gleichungen

$$\varphi(h; p^t) = \prod_{i=1}^{\lambda} \varphi_i(h; p^t). \tag{21}$$

Die $\lambda + 1$ Zahlen

$$M_0 = 0;\ M_1 = v_{\vartheta_1},\ M_2 = v_{\vartheta_2},\ \ldots,\ M_{\lambda-1} = v_{\vartheta_{\lambda-1}};\ M_\lambda = t$$

befriedigen die Ungleichungen

$$M_0 < M_1 < M_2 < \cdots < M_{\lambda-1} < M_\lambda. \tag{22}$$

Denn für ein $i < \lambda$ ist immer $M_i - M_{i-1} = v_{\vartheta_i} - v_{\vartheta_{i-1}} = \omega_{\vartheta_i} \geqq 1$, während wir für $i = \lambda$ gemäß unserer Annahme über $t$ die Beziehung $M_\lambda - M_{\lambda-1} = t - v_{n-1} > 0$ bekommen.

Wir wollen die $\lambda + 1$ Zahlen

$$\bar{h}_0 = t - M_0 = t;\ \bar{h}_1 = t - M_1;\ \bar{h}_2 = t - M_2,\ \ldots,\ \bar{h}_{\lambda-1} = t - M_{\lambda-1};$$
$$\bar{h}_\lambda = t - M_\lambda = 0$$

einführen. Aus den Ungleichungen (22) ergeben sich sofort die Ungleichungen

$$\bar{h}_0 > \bar{h}_1 > \bar{h}_2 > \cdots > \bar{h}_{\lambda-1} > \bar{h}_\lambda. \tag{23}$$

Wenn wir die Zahl $h$ in der Form $h = p^{\bar{h}} \cdot h_0$ ($h_0$ relativ prim zu $p$) darstellen, so gelten für die Größen $\varphi_k(h; p^t)$ nach Kap. VIII, Absatz II, die Relationen

$(24_0)$ für $\bar{h} \geqq \bar{h}_{k-1}$: $\varphi_k(h; p^t) = \overset{0}{\varphi}_k(h; p^t)$,

$(24_1)$ für $\bar{h} < \bar{h}_{k-1}$: $\varphi_k(h; p^t) = \overset{0}{\varphi}_k(h; p^t) \cdot \left(\frac{(\varphi_k)}{p}\right)^{\bar{h}_{k-1} - \bar{h}}$,

in welchen die Faktoren $\overset{0}{\varphi}_k(h; p^t)$ nicht-verschwindende und allein von den Zahlen $h, p^t; \omega(p)$ abhängige Zahlen bedeuten.

Aus der Gleichung (21) und den Formeln (24) erkennen wir, daß die Größen $\varphi(h; p^t)$ außer von den Zahlen $h, p^t; \omega(p)$ nur von den Einheiten $\left(\frac{(\varphi_k)}{p}\right)$ abhängen können. Wir wollen diese Einheiten umgekehrt durch die Größen $\varphi(h; p^t)$ und $\overset{0}{\varphi}_k(h; p^t)$ ausdrücken.

Wenn wir der Zahl $h$ die Werte $1, 2, \ldots, p^t$ erteilen, so durchläuft der Exponent $\bar{h}$ das Intervall $t, t-1, \ldots, 0$. Beachten wir, daß $\bar{h}_0 = t$ und $\bar{h}_\lambda = 0$ ist, so leuchtet ein, daß dieses Intervall mit dem Intervalle

$$\bar{h}_0, \bar{h}_1, \bar{h}_2, \ldots, \bar{h}_{\lambda-1}, \bar{h}_\lambda$$

übereinstimmt. Falls wir von der Größe $\bar{h} = t$ absehen, für welche offenbar $h = p^{\bar{h}} \cdot \bar{h}_0 \equiv 0 \pmod{p^t}$ und $\varphi(h; p^t) = p^{n\,t}$ ist, wird daher eine jede der Zahlen $\bar{h}\,(= t-1, \ldots, 0)$ einer und nur einer Ungleichung

$$(25) \qquad \bar{h}_{i-1} > \bar{h} \geqq \bar{h}_i$$

genügen. Wir wollen die Zahlen $\bar{h}$, welche der Ungleichung (25) genügen, durch $\bar{h}^{(i)}$ und die diesen Zahlen $\bar{h}^{(i)}$ zugehörigen Zahlen $h$ durch $h^{(i)}$ bezeichnen; die Zahlen $h$, deren $\bar{h}$ gleich $\bar{h}_i$ ist, mögen $h_i$ heißen.

Infolge (23) erfüllt jede Zahl $\bar{h}^{(i)}$ die Ungleichungen

$(26_0)$ $\qquad \bar{h}^{(i)} \geqq \bar{h}_i \quad > \bar{h}_{i+1} > \cdots > \bar{h}_{\lambda-1} > \bar{h}_\lambda,$

$(26_1)$ $\qquad \bar{h}^{(i)} < \bar{h}_{i-1} < \bar{h}_{i-2} < \cdots < \bar{h}_1 \quad < \bar{h}_0.$

Folglich gehorchen alle Größen $\varphi_k(h^{(i)}; p^t)$, deren Index $k$ einer der Zahlen $i+1, i+2, \ldots, \lambda$ gleich ist, den Gesetzen $(24_0)$ und alle Größen $\varphi_k(h^{(i)}; p^t)$, deren Index $k$ einer der Zahlen $1, 2, \ldots, i$ gleich ist, den Gesetzen $(24_1)$. Für den Quotienten

$$\frac{\varphi_k(h^{(i)}; p^t)}{\varphi_k(h_{i-1}; p^t)} : \frac{\overset{0}{\varphi}_k(h^{(i)}; p^t)}{\overset{0}{\varphi}_k(h_{i-1}; p^t)} = \{h^{(i)}\}_k$$

gewinnen wir demnach die Formeln

$$\{h^{(i)}\}_k = 1 \qquad \text{für } k = i+1, i+2, \ldots, \lambda$$

und

$$\{h^{(i)}\}_k = \left(\frac{(\varphi_k)}{p}\right)^{\bar{h}_{i-1} - \bar{h}^{(i)}} \qquad \text{für } k = 1, 2, \ldots, i.$$

Setzen wir die Einheit

$$\left(\frac{\prod_{k=1}^{i}(\varphi_k)}{p}\right) = \Theta_i,$$

so ergibt sich für das Produkt $\prod_{k=1}^{\lambda} \varphi_k(h^{(i)}; p^t) = \varphi(h^{(i)}; p^t)$:

$$\varphi(h^{(i)}; p^t) = \Theta_i^{\bar{h}_{i-1} - \bar{h}^{(i)}} \cdot \varphi(h_{i-1}; p^t) \cdot \prod_{k=1}^{\lambda} \frac{\overset{0}{\varphi}_k(h^{(i)}; p^t)}{\overset{0}{\varphi}_k(h_{i-1}; p^t)}. \tag{27}$$

Nehmen wir jetzt an, es seien schon alle diejenigen Größen $\varphi(p^{\bar{h}} \cdot h_0; p^t)$ bekannt, deren $\bar{h}$ die Ungleichung $\bar{h} \geqq \bar{h}_{i-1}$ befriedigt. Um alsdann zu einer Kenntnis aller Größen $\varphi(p^{\bar{h}} \cdot h_0; p^t)$ zu gelangen, deren $\bar{h} \geqq \bar{h}_i$ ist, brauchen wir nur noch diejenigen Größen $\varphi(p^{\bar{h}} \cdot h_0; p^t)$ aufzusuchen, für welche $\bar{h}_{i-1} > \bar{h} \geqq \bar{h}_i$ ist, das sind die Größen $\varphi(h^{(i)}; p^t)$. Aus der vorstehenden Gleichung (27) ist nun einerseits klar, daß wir zur Bestimmung dieser Größen höchstens der Einheiten $\Theta_i^{\bar{h}_{i-1} - \bar{h}^{(i)}}$ bedürfen, während andererseits diese Einheiten sich durch Größen $\varphi(h; p^t)$ und $\overset{0}{\varphi}_k(h; p^t)$ ausdrücken lassen. Unter den Einheiten $\Theta_i^{\bar{h}_{i-1} - \bar{h}^{(i)}}$ befindet sich, da die Differenz $\bar{h}_{i-1} - \bar{h}^{(i)}$ die Werte

$$1, 2, \ldots, \bar{h}_{i-1} - \bar{h}_i \geqq 1$$

durchläuft, die Einheit $\Theta_i$ selber. Wenden wir dieses Resultat der Reihe nach für die Werte $i = 1, 2, \ldots, \lambda$ an, so erhalten wir den Satz:

Die Größen $\varphi(h; p^t)$ $[t > v_{n-1}(p)]$ hängen außer von den Zahlen $p^{\omega(p)}$ von den $\lambda_p + 1$ Einheiten

$$\Theta_i = \left(\frac{\prod_{k=1}^{i}(\varphi_k)}{p}\right) \quad (i = 0, 1, 2, \ldots, \lambda_p), \ [\Theta_0 = 1]$$

ab, und umgekehrt können die $\lambda_p + 1$ Einheiten durch Größen $\varphi(h; p^t)$ und durch die Zahlen $p^{\omega(p)}$ ausgedrückt werden.

Sowohl die Einheiten $\Theta_i$ als die Einheiten $\left(\frac{(\varphi_i)}{p}\right) = \frac{\Theta_i}{\Theta_{i-1}}$ sind also Charaktere der Form $f$.

Wir drücken jetzt die Charaktere $\Theta_i$ durch die $n+1$ Zahlen $\varphi_h$ eines Hauptrepräsentanten aus, welcher den Rest $\varphi$ liefert. Zunächst erkennen wir, daß die beiden Charaktere $\Theta_0$ und $\Theta_\lambda$ nur von der Ordnung der Form $f$ abhängen. Denn es ist

$$\Theta_0 = 1 = 1 \cdot \left(\frac{\varphi_0}{p}\right),$$

und für $\Theta_\lambda$ erhält man mit Hilfe der Kongruenz

$$\prod_{k=1}^{\lambda}(\varphi_k) \equiv (-1)^I \cdot \frac{d_{n-1}}{p^{\partial_{n-1}}} \pmod{p^{t-v_{n-1}}}, \qquad [t > v_{n-1}]$$

die aus Kap. VI (S. 40) folgt, die Beziehung

$$\Theta_\lambda = \left(\frac{(-1)^I \frac{d_{n-1}}{p^{\partial_{n-1}}}}{p}\right) = \left(\frac{\frac{d_{n-1}}{p^{\partial_{n-1}}}}{p}\right) \cdot \left(\frac{\varphi_n}{p}\right).$$

Die übrigen Charaktere $\Theta_i$ lassen sich mit Hilfe der Kongruenzen

$$\prod_{k=1}^{i}(\varphi_k) \equiv \varphi_{\vartheta_i} \frac{d_{\vartheta_i - 1}}{p^{\partial_{\vartheta_i - 1}}} \pmod{p^{\bar{h}_{i-1}}}$$

durch die Einheiten

$$C_i(p) = \left(\frac{\varphi_{\vartheta_i}}{p}\right)$$

ausdrücken. Diese Charaktere $C(p)$ sind mit den in Kap. VI gefundenen Charakteren $\left(\frac{\varphi_h}{p}\right)$ identisch.

Die Anzahl derjenigen Charaktere $C(p)$, welche nicht schon von vornherein durch die Ordnung der Form $\varphi$ gegeben sind, beträgt $\lambda_p - 1$. Nun ist für alle Primzahlen $p$, welche in dem Produkte $\prod_{k=1}^{n-1} o_k$ nicht aufgehen, $\lambda_p = 1$. Folglich werden nur diejenigen Primzahlen $p$, welche in diesem Produkt enthalten sind, besondere Charaktere $C(p)$ liefern. Auf diesem Umstande beruht es vornehmlich, daß die Anzahl aller unabhängigen Charaktere, welche einer gegebenen Formenklasse $f$ angehören, einen endlichen Wert besitzt.

II. Es möge jetzt $q = 2$ sein, und es stelle $f$ eine in bezug auf 2 primitive Form vor. Wir betrachten irgend einen Hauptrepräsentanten $\varphi$ der Klasse $f$ für einen Modul $2^t > \frac{4}{\sigma_{n-1}} \cdot 2^{v_{n-1}(2)}$. Sobald irgendeine Invariante $\sigma_T$ der Form $f$ den Wert 1 erhält, verschwinden von den Koeffizienten $R_{ik}$ $(i < k)$ des Restes $\varphi$ alle diejenigen modulo $2^t$, für welche $i \leqq T$ und $k > T$ ist. Wenn $\sigma_T = 1$ ist, zerfällt demgemäß der Rest $\varphi$ für den Modul $2^t$ in zwei Einzelreste $\Phi$ und $\Phi_0$, von denen der eine, $\Phi$, die $T$ ersten Reihen des Restes $\varphi$ und der andere die $n - T$ letzten Reihen dieses Restes enthält. Wir überzeugen uns ferner, daß der Rest $\Phi$ zu 2 primitiv wird, während die höchste, in allen Koeffizienten des Restes $\Phi_0$ aufgehende Potenz von 2 den Wert $2^{v_T}$ annimmt, sowie daß die Invarianten $\sigma$ des Restes $\Phi$ gleich $\sigma_1, \sigma_2, \ldots, \sigma_{T-1}$ und die Invarianten $\sigma$ des Restes $\Phi_0$ gleich $\sigma_{T+1}, \sigma_{T+2}, \ldots, \sigma_{n-1}$ werden. Wiederholen wir diese Bemerkungen für mehrere Invarianten $\sigma_T = 1$, so gelangen wir ohne Schwierigkeit zu dem folgenden Satze:

K. Wenn wir von den $n-1$ Invarianten $\sigma$ der Form $f$ beliebige $L-1$ auswählen, welche den Wert 1 haben, etwa

$$(T_0=0) \qquad \sigma_{T_1}=1,\ \sigma_{T_2}=1,\ \ldots,\ \sigma_{T_{L-2}}=1,\ \sigma_{T_{L-1}}=1, \qquad (T_L=n)$$

und die Zahlen $T_i - T_{i-1} = K_i$ setzen, so können wir aus den $K_1$ ersten Reihen von $\varphi$ einen Rest $\Phi_1$, aus den $K_2$ folgenden Reihen einen Rest $\Phi_2$, usw., aus den $K_L$ letzten Reihen von $\varphi$ eine Form $\Phi_L$ bilden, und der Rest $\varphi$ zerfällt für den Modul $2^t$ in $L$ Einzelreste

$$\varphi \equiv \Phi_1 + \Phi_2 + \cdots + \Phi_L \pmod{2^t}.$$

Die Reste $\Phi_i$ erscheinen als Produkte aus einem Faktor $2^{\varrho_{T_{i-1}}}$ und einer zu 2 primitiven Form. Bezeichnen wir die $K_i - 1$ Invarianten $\sigma$ dieser zu 2 primitiven Form durch $\mathsf{P}_k^{(i)}$ und die $K_i - 1$ Invarianten $\omega(2)$ dieser Form durch $\Omega_k^{(i)}$, so bestehen die Relationen

$$\mathsf{P}_k^{(i)} = \sigma_{T_{i-1}+k}, \quad \Omega_k^{(i)} = \omega_{T_{i-1}+k}. \qquad (k=1, 2, \ldots, K_i-1)$$

Einige besondere Fälle dieser Zerlegungen von $\varphi$ in Formen $\Phi_i$ haben wir schon im Früheren untersucht.

So bekommen wir erstens die Zerlegung von $\varphi$ in lauter Formen

$$F \equiv 2^M \alpha \xi^2 \pmod{2^t}$$

von einer Variablen oder Formen

$$F_0 \equiv 2^M(\alpha\xi^2 + \mathfrak{A}\xi\tilde{\xi} + \tilde{\alpha}\tilde{\xi}^2) \pmod{2^t}$$

von zwei Variablen, indem wir für die Größen $T_i$ ohne Ausnahme alle diejenigen Zahlen aus der Reihe $1, 2, \ldots, n-1$ wählen, denen eine Invariante $\sigma_T = 1$ entspricht.

Zweitens entsteht die in den Kapiteln III und IV betrachtete Zerlegung von $\varphi$ in $\lambda$ Formen $\varphi_i$, indem wir die Zahlen $T_i$ gleich den $\lambda - 1$ Zahlen $\vartheta_i$ annehmen, welche zu den $\lambda - 1$ nicht-verschwindenden Zahlen $\omega_{\vartheta_i}$ gehören.

Eine dritte Zerlegung des Restes $\varphi$, welche gleichfalls durch das angegebene Verfahren gefunden werden kann, wird uns jetzt zur Bestimmung der Größen $\varphi(h; 2^t)$ dienen.

Es mögen von den $n-1$ Größen $\sigma_{i-1} 2^{\omega_i} \sigma_{i+1}$ im ganzen $\mu - 1$ $(1 \leqq \mu \leqq n)$ durch 4 teilbar sein, nämlich die folgenden

$$(\eta_0=0) \qquad \sigma_{\eta_1-1} 2^{\omega_{\eta_1}} \sigma_{\eta_1+1},\ \ldots,\ \sigma_{\eta_{\mu-1}-1} 2^{\omega_{\eta_{\mu-1}}} \sigma_{\eta_{\mu-1}+1}, \qquad (\eta_\mu = n)$$

während alle übrigen $n - \mu$ dieser Zahlen entweder gleich 1 oder gleich 2 sein mögen. Nach Kap. IV, Absatz II bestehen alsdann die Relationen

$$\sigma_{\eta_1}=1,\ \sigma_{\eta_2}=1,\ \ldots,\ \sigma_{\eta_{\mu-2}}=1,\ \sigma_{\eta_{\mu-1}}=1.$$

Wir können demnach die Zahlen $T_i$ gleich den $\mu - 1$ Zahlen $\eta_1, \eta_2, \ldots,$

$\eta_{\mu-2}$, $\eta_{\mu-1}$ annehmen, und wir gewinnen dann eine Zerlegung von $\varphi$ in $\mu$ Formen

$$\varphi \equiv \Phi_1 + \Phi_2 + \cdots + \Phi_\mu \equiv \sum_{i=1}^{\mu} \Phi_i \pmod{2^t}.$$

Die Größen $\varphi(h; 2^t) = f(h; 2^t)$ werden sich dann aus den Gleichungen

$$\varphi(h; 2^t) = \prod_{i=1}^{\mu} \Phi_i(h; 2^t)$$

bestimmen.

Nach dem Satze K. müssen die Zahlen

$$\mathsf{P}_{k-1}^{(i)} 2^{\Omega_k^{(i)}} \mathsf{P}_{k+1}^{(i)} \qquad (k = 1, 2, \ldots, \eta_i - \eta_{i-1} - 1)$$

mit den Zahlen

$$\sigma_{\eta_{i-1}+k-1} 2^{\omega_{\eta_{i-1}+k}} \sigma_{\eta_{i-1}+k+1}$$

übereinstimmen. Da nun diese letzteren Zahlen unserer Annahme gemäß sämtlich kleiner als 4 sein sollen, so folgt, daß auch die Zahlen $\mathsf{P}_{k-1}^{(i)} 2^{\Omega_k^{(i)}} \mathsf{P}_{k+1}^{(i)}$ sämtlich gleich 1 oder gleich 2 sein werden. Wir überzeugen uns nun leicht mit Hilfe der in Kap. IV, Absatz II aufgestellten Sätze, daß dieses dann und nur dann eintrifft, wenn die Reste $\Phi_i$ von der Gestalt

$$(28_1) \qquad \Phi_i \equiv 2^{v_{\eta_{i-1}}} \sum_{s=1}^{m_i} \left( 2^{s-1} \sum_{r=1}^{l_s} \alpha_r^{(s)} \xi_r^{(s)} \xi_r^{(s)} \right) \pmod{2^t}$$

$$[l_s \geqq 1,\ m_i \geqq 1]$$

oder von der Gestalt

$$(28_2) \qquad \Phi_i \equiv 2^{v_{\eta_{i-1}+1}} (\alpha \xi^2 + \mathfrak{A} \xi \tilde{\xi} + \tilde{\alpha} \tilde{\xi}^2) \pmod{2^t}$$

sind.

Wir wollen jeder Form $\Phi_i$, je nachdem sie von der Gestalt $(28_1)$ oder von der Gestalt $(28_2)$ ist, eine Zahl $\tau_i$ gleich 1 oder gleich 2 zuteilen. Wir haben die Beziehungen

$$\tau_i = \mathsf{P}_1^{(i)} = \mathsf{P}_{\eta_i - \eta_{i-1}-1}^{(i)}$$

oder

$$\tau_i = \sigma_{\eta_{i-1}+1} = \sigma_{\eta_i - 1}.$$

Wir führen $\mu + 1$ Zahlen $M_i$ vermittels der Gleichungen

$$2^{M_0} = \tau_1 = \sigma_1, \quad 2^{M_1} = \tau_2 \cdot 2^{v_{\eta_1}}, \quad 2^{M_2} = \tau_3 \cdot 2^{v_{\eta_2}}, \quad \ldots,$$
$$2^{M_{\mu-1}} = \tau_\mu \cdot 2^{v_{\eta_{\mu-1}}}, \quad 2^{M_\mu} = 2^t,$$

und $\mu$ Zahlen $\tilde{M}_i$ vermittels der Gleichungen

$$2^{\tilde{M}_0} = \frac{4}{\tau_1} \cdot 2^{v_{\eta_1}-1}, \quad 2^{\tilde{M}_1} = \frac{4}{\tau_2} \cdot 2^{v_{\eta_2}-1}, \quad 2^{\tilde{M}_2} = \frac{4}{\tau_3} \cdot 2^{v_{\eta_3}-1}, \quad \ldots,$$
$$2^{\tilde{M}_{\mu-1}} = \frac{4}{\tau_\mu} \cdot 2^{v_{\eta_\mu}-1}$$

ein. Die Potenzen $2^{M_i-1}$ werden, wenn $\tau_i = 1$ ist, gleich $2^{v_{\eta_i}-1}$, und wenn $\tau_i = 2$ ist, gleich $2^{v_{\eta_i-1}+1}$; die Potenzen $2^{\tilde{M}_i-1}$ sind, wenn $\tau_i = 1$ ist, gleich $2^{2+v_{\eta_i-1}} = 2^{1+m_i+M_i-1}$, dagegen wenn $\tau_i = 2$ ist, gleich

$$2^{1+v_{\eta_i}-1} = 2^{M_i-1}.$$

Folglich hat man stets $\tilde{M}_{i-1} \geqq M_{i-1}$. Ferner erhält man wegen

$\sigma_{\eta_i-1}\, 2^{\omega_{\eta_i}}\, \sigma_{\eta_i+1} \geqq 4$ und $2^t > \frac{4}{\sigma_{n-1}} \cdot 2^{v_{n-1}}$ für $i < \mu$:

$$2^{M_i - \tilde{M}_{i-1}} = \frac{\tau_i \tau_{i+1} \cdot 2^{v_{\eta_i} - v_{\eta_i}-1}}{4} = \frac{\sigma_{\eta_i-1} \cdot 2^{\omega_{\eta_i}} \cdot \sigma_{\eta_i+1}}{4} \geqq 1$$

und

$$2^{M_\mu - \tilde{M}_{\mu-1}} = \frac{2^t}{\frac{4}{\sigma_{n-1}} \cdot 2^{v_{n-1}}} > 1,$$

so daß man die Ungleichungen findet

$$(29) \qquad M_0 \leqq \tilde{M}_0 \leqq M_1 \leqq \tilde{M}_1 \leqq \cdots \leqq M_{\mu-1} \leqq \tilde{M}_{\mu-1} < M_\mu = t.$$

Wir bezeichnen die Zahlen $t - M_i$ durch $\bar{h}_i$ und die Zahlen $t - \tilde{M}_i$ durch $\tilde{h}_i$. Aus (29) folgen sofort die Ungleichungen

$$(30) \qquad \bar{h}_0 \geqq \tilde{h}_0 \geqq \bar{h}_1 \geqq \tilde{h}_1 \geqq \cdots \geqq \bar{h}_{\mu-1} \geqq \tilde{h}_{\mu-1} > \bar{h}_\mu = 0,$$

und es gelten die Relationen

für $\tau_i = 1$: $\qquad \bar{h}_{i-1} = \tilde{h}_{i-1} + 1 + m_i,$

für $\tau_i = 2$: $\qquad \bar{h}_{i-1} = \tilde{h}_{i-1},$

und

$$(31) \qquad 2^{\tilde{h}_i - 1 - \bar{h}_i} = \frac{\sigma_{\eta_i-1} \cdot 2^{\omega_{\eta_i}} \cdot \sigma_{\eta_i+1}}{4} \geqq 1 \quad (i < \mu);$$

$$\tilde{h}_{\mu-1} - \bar{h}_\mu > 0.$$

Wir wollen für einen jeden Rest $\Phi_i$ von der Gestalt $(28_1)$

$$\Phi_i \equiv 2^{M_i-1} \sum_{s=1}^{m_i} \left( 2^{s-1} \sum_{r=1}^{l_s} \alpha_r^{(s)}\, \xi_r^{(s)}\, \xi_r^{(s)} \right) \equiv \sum_{s=1}^{m_i} \varphi_s^{(i)} \pmod{2^t}$$

eine Einheit

$$\mathfrak{l}_i = \left(\frac{2}{\left(\varphi_{m_i-1}^{(i)}\right)}\right)\left(\frac{2}{\left(\varphi_{m_i-3}^{(i)}\right)}\right) \cdots \left(\frac{2}{\left(\varphi_{m_i+1-2\left[\frac{m_i}{2}\right]}^{(i)}\right)}\right) \cdot$$

$$\cdot \left(\frac{2}{\prod_{k=1}^{i-1}(\Phi_k)}\right)^{m_i+1-2\left[\frac{m_i+1}{2}\right]} \cdot (-1)^{\frac{1}{2}\sum_{(r',s') \neq (r'',s'')} \frac{\alpha_{r'}^{s'}-1}{2} \cdot \frac{\alpha_{r''}^{s''}-1}{2}}$$

und für einen jeden Rest $\Phi_i$ von der Gestalt $(28_2)$

$$\Phi_i \equiv 2^{M_i-1}(\alpha\xi^2 + \mathfrak{A}\xi\tilde{\xi} + \tilde{\alpha}\tilde{\xi}^2) \pmod{2^t}$$

eine Einheit

$$\mathfrak{l}_i = 1$$

bilden.

Für die Größen $\Phi_k(h; 2^t)$ $[h = 2^{\bar{h}}h_0,\ h_0 \equiv 1 \pmod 2]$ ergeben sich jetzt die Formeln

$(32_0)$ für $\bar{h} \geqq \bar{h}_{k-1}$: $\quad \Phi_k(h; 2^t) = \overset{0}{\Phi}_k(h; 2^t)$,

$(32_1)$ für $\bar{h} \leqq \tilde{h}_{k-1}$: $\quad \Phi_k(h; 2^t) = \overset{0}{\Phi}_k(h; 2^t) \cdot \mathfrak{l}_k \cdot \left(\frac{2}{\prod_{i=1}^{k-1}(\Phi_i)}\right)^{\bar{h}_{k-1}-\tilde{h}_{k-1}} \cdot$

$$\cdot (-i)^{\tau_k^2\left(\frac{(\Phi_k)-1}{2}\right)^2} (-1)^{\tau_k \cdot \frac{(\Phi_k)-1}{2} \cdot \frac{h_0-1}{2}} \left(\frac{2}{(\Phi_k)}\right)^{\tilde{h}_{k-1}-\bar{h}},$$

$(32_2)$ und für $\tau_k = 1$, $\bar{h}_{k-1} > \bar{h} > \tilde{h}_{k-1}$: $\quad \Phi_k(h; 2^t) = 0$,

in welchen die Faktoren $\overset{0}{\Phi}_k(h; 2^t)$ nicht-verschwindende und allein von den Zahlen $h, 2^t$; $\sigma, \omega(2)$ abhängige Größen bedeuten.

Wir wollen die Zahlen $\bar{h}$, welche der Ungleichung

$$\tilde{h}_{k-1} \geqq \bar{h} \geqq \bar{h}_k$$

genügen, durch $\bar{h}^{(k)}$ bezeichnen. Eine jede Zahl $\bar{h}^{(k)}$ befriedigt infolge (30) außerdem die Ungleichungen

$(33_1)$ $\qquad \bar{h}^{(k)} \geqq \bar{h}_k \geqq \bar{h}_{k+1} \geqq \cdots \geqq \bar{h}_{\mu-1} \geqq \bar{h}_\mu$,

$(33_2)$ $\qquad \bar{h}^{(k)} \leqq \tilde{h}_{k-1} \leqq \tilde{h}_{k-2} \leqq \cdots \leqq \tilde{h}_1 \leqq \tilde{h}_0$.

Demzufolge gehorchen alle Größen $\Phi_i(2^{\bar{h}^{(k)}}h_0; 2^t)$, deren Index $i$ einer der Zahlen $k+1, k+2, \ldots, \mu$ gleich ist, den Gesetzen $(32_0)$ und alle Größen $\Phi_i(2^{\bar{h}^{(k)}}h_0; 2^t)$, deren Index $i$ einer der Zahlen $1, 2, \ldots, k$ gleich ist, den Gesetzen $(32_1)$. Wir bekommen demnach für den Quotienten

$$\frac{\Phi_i(2^{\bar{h}^{(k)}}h_0; 2^t)}{\Phi_i(2^{\bar{h}_{k-1}}h_0; 2^t)} : \frac{\overset{0}{\Phi}_i(2^{\bar{h}^{(k)}}h_0; 2^t)}{\overset{0}{\Phi}_i(2^{\bar{h}_{k-1}}h_0; 2^t)} = \{h^{(k)}\}_i$$

die Gleichungen

$$\{h^{(k)}\}_i = 1 \qquad (\text{für } i = k+1, k+2, \ldots, \mu),$$

$$\{h^{(k)}\}_i = \left(\frac{2}{(\Phi_i)}\right)^{\bar{h}_{k-1}-\bar{h}^{(k)}} \qquad (\text{für } i = 1, 2, \ldots, k-1)$$

und für $i = k$:

$$\{h^{(k)}\}_k = \mathfrak{l}_k \cdot \left(\frac{2}{\prod_{i=1}^{k-1}(\Phi_i)}\right)^{\bar{h}_{k-1}-\tilde{h}_{k-1}} \cdot (-i)^{\tau_k^2\left(\frac{(\Phi_k)-1}{2}\right)^2} \cdot$$

$$\cdot (-1)^{\tau_k \frac{(\Phi_k)-1}{2} \cdot \frac{h_0-1}{2}} \left(\frac{2}{(\Phi_k)}\right)^{\tilde{h}_{k-1}-\bar{h}^{(k)}}.$$

Für das Produkt $\prod_{i=1}^{\mu} \Phi_i(2^{\bar{h}^{(k)}}h_0; 2^t) = \varphi(2^{\bar{h}^{(k)}}h_0; 2^t)$ ergibt sich jetzt

$$\varphi(2^{\bar{h}(k)}h_0;\,2^t) = \mathsf{l}_k \cdot (-i)^{\tau_k^2\left(\frac{(\Phi_k)-1}{2}\right)^2} (-1)^{\tau_k\frac{(\Phi_k)-1}{2}\cdot\frac{h_0-1}{2}} \cdot \left(\frac{2}{\prod_{i=1}^{k}(\Phi_i)}\right)^{\tilde{h}_{k-1}-\bar{h}(k)} \cdot \varphi(2^{\bar{h}_{k-1}}h_0;\,2^t) \prod_{i=1}^{\mu}\frac{\overset{0}{\Phi}_i(2^{\bar{h}(k)}h_0;\,2^t)}{\overset{0}{\Phi}_i(2^{\bar{h}_{k-1}}h_0;\,2^t)},$$

woraus wir insbesondere die Beziehungen

$$(34_1)\quad \varphi(2^{\tilde{h}_{k-1}}h_0;\,2^t) = \mathsf{l}_k \cdot (-i)^{\tau_k^2\left(\frac{(\Phi_k)-1}{2}\right)^2} (-1)^{\tau_k\frac{(\Phi_k)-1}{2}\cdot\frac{h_0-1}{2}} \cdot \varphi(2^{\bar{h}_{k-1}}h_0;\,2^t) \prod_{i=1}^{\mu}\frac{\overset{0}{\Phi}_i(2^{\tilde{h}_{k-1}}h_0;\,2^t)}{\overset{0}{\Phi}_i(2^{\bar{h}_{k-1}}h_0;\,2^t)}$$

und

$$(34_2)\quad \varphi(2^{\bar{h}(k)}h_0;\,2^t) = \left(\frac{2}{\prod_{i=1}^{k}(\Phi_i)}\right)^{\tilde{h}_{k-1}-\bar{h}(k)} \varphi(2^{\tilde{h}_{k-1}}h_0;\,2^t) \prod_{i=1}^{\mu}\frac{\overset{0}{\Phi}_i(2^{\bar{h}(k)}h_0;\,2^t)}{\overset{0}{\Phi}_i(2^{\tilde{h}_{k-1}}h_0;\,2^t)}$$

gewinnen.

Wir nehmen jetzt an, es seien schon alle diejenigen Größen $\varphi(2^{\bar{h}}h_0;\,2^t)$ bekannt, deren $\bar{h} \geqq \bar{h}_{k-1}$ ist. Um alsdann zu einer Kenntnis aller Größen $\varphi(2^{\bar{h}}h_0;\,2^t)$ zu gelangen, deren $\bar{h}$ die Ungleichung $\bar{h} \geqq \bar{h}_k$ befriedigt, brauchen wir nur die sämtlichen Größen $\varphi(2^{\bar{h}}h_0;\,2^t)$ zu untersuchen, für welche $\tilde{h}_{k-1} \geqq \bar{h} \geqq \bar{h}_k$ gilt, das sind die Größen $\varphi(2^{\bar{h}(k)}h_0;\,2^t)$. Denn ist $\tau_k = 1$, so wird $\bar{h}_{k-1} = \tilde{h}_{k-1} + 1 + m_k$, und die sämtlichen Zahlen $\bar{h}$, welche $\geqq \bar{h}_k$ sind, genügen entweder der Ungleichung $\bar{h} \geqq \bar{h}_{k-1}$ oder der Ungleichung $\bar{h}_{k-1} > \bar{h} > \tilde{h}_{k-1}$ oder der Ungleichung $\tilde{h}_{k-1} \geqq \bar{h} \geqq \bar{h}_k$. Ist aber $\bar{h} \geqq \bar{h}_{k-1}$, so ist die Größe $\varphi(2^{\bar{h}}h_0;\,2^t)$ schon bekannt, und erfüllt $\bar{h}$ die Ungleichung $\bar{h}_{k-1} > \bar{h} > \tilde{h}_{k-1}$, so wird $\Phi_k(2^{\bar{h}}h_0;\,2^t) = 0$, also auch $\varphi(2^{\bar{h}}h_0;\,2^t) = 0$. Es sind mithin in der Tat nur diejenigen Größen $\varphi(2^{\bar{h}}h_0;\,2^t)$ zu betrachten, für welche $\tilde{h}_{k-1} \geqq \bar{h} \geqq \bar{h}_k$ ist. Wenn hingegen $\tau_k = 2$ ist, so wird $\bar{h}_{k-1} = \tilde{h}_{k-1}$, und die Zahlen $\bar{h}$, welche $\geqq \bar{h}_k$ sind, genügen entweder der Ungleichung $\bar{h} \geqq \bar{h}_{k-1}$, in welchem Falle die Größen $\varphi(2^{\bar{h}}h_0;\,2^t)$ als bekannt anzusehen sind, oder sie genügen der Ungleichung $\tilde{h}_{k-1} \geqq \bar{h} \geqq \bar{h}_k$.

Mit Hilfe der Gleichungen $(34_1)$ und $(34_2)$ ziehen wir jetzt den folgenden Schluß:

L. Wenn alle Größen $\varphi(2^{\bar{h}}h_0;\,2^t)$, deren $\bar{h} \geqq \bar{h}_{k-1}$ ist, gegeben sind, so bedürfen wir zur Bestimmung der sämtlichen Größen $\varphi(2^{\bar{h}(k)}h_0;\,2^t)$ höchstens der Einheiten $\mathsf{l}_k$, $(-1)^{\frac{(\Phi_k)-1}{2}}$, $\left(\frac{2}{\prod_{i=1}^{k}(\Phi_i)}\right)^{\tilde{h}_{k-1}-\bar{h}(k)}$, und umgekehrt können diese Einheiten stets durch Größen $\varphi(2^{\bar{h}}h_0;\,2^t)$ und $\overset{0}{\Phi}_i(2^{\bar{h}}h_0;\,2^t)$ $(\bar{h} \geqq \bar{h}_k)$ ausgedrückt werden.

Die Größe $\tilde{h}_{k-1} - \bar{h}^{(k)}$ erhält, da die Zahlen $\bar{h}^{(k)}$ der Ungleichung $\tilde{h}_{k-1} \geqq \bar{h}^{(k)} \geqq \bar{h}_k$ genügen sollen, die Werte

$$0,\ 1,\ 2,\ \ldots,\ \tilde{h}_{k-1} - \bar{h}_k.$$

Unter den Einheiten $\left(\frac{2}{\prod_{i=1}^{k}(\Phi_i)}\right)^{\tilde{h}_{k-1}-\bar{h}^{(k)}}$ wird daher die Einheit $\left(\frac{2}{\prod_{i=1}^{k}(\Phi_i)}\right)$ selber auftreten, sobald $\tilde{h}_{k-1} - \bar{h}_k \geqq 1$ ist.

Wir wollen annehmen, von den Zahlen $\sigma_{i-1} 2^{\omega_i} \sigma_{i+1}$ $(i = 1, 2, \ldots, n-2, n-1)$ seien im ganzen $\nu - 1$ $(1 \leqq \nu \leqq n)$ größer oder gleich 8, nämlich die folgenden:

$$(\xi_0 = 0) \qquad \sigma_{\xi_1 - 1} 2^{\omega_{\xi_1}} \sigma_{\xi_1 + 1},\ \ldots,\ \sigma_{\xi_{\nu-1}-1} 2^{\omega_{\xi_{\nu-1}}} \sigma_{\xi_{\nu-1}+1}, \qquad (\xi_\nu = n),$$

wo

$$(K_0 = 0) \qquad \xi_1 = \eta_{K_1},\ \ldots,\ \xi_{\nu-1} = \eta_{K_{\nu-1}} \qquad (K_\nu = \mu)$$

ist, während alle übrigen $n - \nu$ Zahlen $\sigma_{i-1} 2^{\omega_i} \sigma_{i+1}$ höchstens gleich 4 sein mögen. Es sind dann infolge der Gleichungen (31) von den $\mu$ Zahlen $\tilde{h}_{k-1} - \bar{h}_k$ $(k = 1, 2, \ldots, \mu)$ die $\nu$ folgenden

$$\tilde{h}_{K_1 - 1} - \bar{h}_{K_1},\ \tilde{h}_{K_2 - 1} - \bar{h}_{K_2},\ \ldots,\ \tilde{h}_{K_{\nu-1}-1} - \bar{h}_{K_{\nu-1}} \quad \text{und} \quad \tilde{h}_{K_\nu - 1} - \bar{h}_{K_\nu}$$

größer oder gleich 1, während die übrigen $\mu - \nu$ dieser Zahlen verschwinden.

Wenden wir das Resultat L. der Reihe nach für die Werte $k = 1, 2, \ldots, \mu$ an und beachten wir einerseits, daß alle Größen $\varphi(2^{\bar{k}} h_0; 2^t)$, deren $\bar{h} \geqq \bar{h}_0$ ist, gleich $2^{nt}$ werden, und andererseits, daß ein jedes $\bar{h} \geqq \bar{h}_\mu$, d. i. $\geqq 0$ ist, so gewinnen wir den Satz:

Die Größen $\varphi(h; 2^t)$ $\left(2^t > \frac{4}{\sigma_{n-1}} 2^{\nu_n - 1^{(2)}}\right)$ hängen von den Zahlen $\sigma$, $2^{\omega^{(2)}}$ und den $2(\mu + 1) + (\nu + 1)$ Einheiten

$$\mathsf{H}_k = (-1)^{\frac{-1 + \prod_{i=1}^{k}(\Phi_i)}{2}} \qquad (k = 0, 1, 2, \ldots, \mu) \quad [\mathsf{H}_0 = 1],$$

$$\mathsf{Z}_k = \left(\frac{2}{\prod_{i=1}^{K_k}(\Phi_i)}\right) \qquad (k = 0, 1, 2, \ldots, \nu) \quad [\mathsf{Z}_0 = 1],$$

und

$$\mathsf{E}_k = \prod_{i=1}^{k} \left\{ \left(\frac{2}{\prod_{j=1}^{i-1}(\Phi_j)}\right)^{\tilde{h}_{i-2} - \bar{h}_{i-1}} \cdot \mathsf{I}_i \cdot (-1)^{\frac{-1 + \prod_{j=1}^{i-1}(\Phi_j)}{2} \cdot \frac{1 + \prod_{j=1}^{i}(\Phi_j)}{2}} \right\}$$

$$(k = 0, 1, 2, \ldots, \mu) \quad [\mathsf{E}_0 = 1]$$

ab, und umgekehrt können diese sämtlichen Einheiten durch die Zahlen $\sigma$, $2^{\omega(2)}$ und durch Größen $\varphi(h; 2^t)$ ausgedrückt werden.

Die Einheiten $\mathsf{E}_k$, $\mathsf{H}_k$, $\mathsf{Z}_k$ sind also ebenso wie die Einheiten $\mathsf{I}_k$, $(-1)^{\frac{(\Phi_k)-1}{2}}$ Charaktere der Form $f$.

Die Anzahl der Reste $\Phi_k$, denen ein $\tau_k = 2$ entspricht, ist gleich der Anzahl aller derjenigen Invarianten $\sigma$ der Form $f$, welche gleich 2 werden. Die Charaktere $(-1)^{\frac{(\Phi_k)-1}{2}}$, welche einer Form $\Phi_k$ von der Gestalt $(28_2)$ angehören, sind gleich $-1$, und die Charaktere $\mathsf{I}_k$, welche einer Form $\Phi_k$ von der Gestalt $(28_2)$ entsprechen, gleich $+1$. Ferner erkennen wir aus der am Schlusse von Kap. VIII gemachten Bemerkung, daß die Einheit $\mathsf{I}_k$ den Wert $+1$ erhalten muß, so oft der Rest $\Phi_k$ die Gestalt

$$\Phi_k \equiv 2^M \alpha \xi^2 \pmod{2^t}$$

oder die Gestalt

$$\Phi_k \equiv 2^M(\alpha\xi^2 + \alpha_0\xi_0^2) \pmod{2^t}; \quad (-1)^{\frac{\alpha\alpha_0-1}{2}} = (-1)^{\frac{(\Phi_k)-1}{2}} = -1$$

besitzt.

Wir drücken jetzt die Charaktere $\mathsf{E}_k$, $\mathsf{H}_k$, $\mathsf{Z}_k$ durch die $n+1$ Zahlen $\varphi_h$ eines Hauptrepräsentanten $\varphi \pmod{2^t}$ aus.

Die in Kap. VI (S. 40) aufgestellte Kongruenz ergibt unmittelbar

$$\prod_{i=1}^{\mu}(\Phi_i) \equiv (-1)^I \cdot \frac{d_{n-1}}{2^{\partial_n - 1}} \left( \mod 4 \cdot \frac{2^t}{\frac{4}{\sigma_{n-1}} 2^{v_n - 1}} \right);$$

auf einem ähnlichen Wege gelangen wir zu den Beziehungen

$$\prod_{i=1}^{k}(\Phi_i) \equiv \frac{d_{\eta_k - 1}}{2^{\partial_{\eta_k} - 1}} \cdot \varphi_{\eta_k} \pmod{2^{2+\tilde{h}_k - 1}}.$$

Also wird

$$\mathsf{H}_0 = (-1)^{\frac{\varphi_0 - 1}{2}}, \quad \mathsf{H}_\mu = \left( \frac{-1}{\frac{d_{n-1}}{2^{\partial_n - 1}}} \right) (-1)^{\frac{\varphi_n - 1}{2}},$$

$$\mathsf{Z}_0 = \left(\frac{2}{\varphi_0}\right), \qquad \mathsf{Z}_\nu = \left( \frac{2}{\frac{d_{n-1}}{2^{\partial_n - 1}}} \right) \left(\frac{2}{\varphi_n}\right),$$

und ebenso kann man die übrigen Charaktere $\mathsf{H}_k$, $\mathsf{Z}_k$ durch die Einheiten

$$C_k(4) = (-1)^{\frac{\varphi_{\eta_k} - 1}{2}}$$

und

$$C_k(8) = \left(\frac{2}{\varphi_{\zeta_k}}\right)$$

ausdrücken. Diese Charaktere $C(4)$ und $C(8)$ sind mit den in Kap. VI

betrachteten Charakteren $(-1)^{\frac{\varphi_h-1}{2}}$ und $\left(\frac{2}{\varphi_h}\right)$ identisch. Die Charaktere $\mathsf{E}_k$ lassen sich als Produkte von zwei Faktoren darstellen, von denen der eine [falls $o_h = 2^{\omega_h} \cdot e_h$, $e_h \equiv 1 \pmod 2$ gesetzt wird] gleich

$$\mathfrak{C}_k(4) = \prod_{i=1}^{\eta_k-1} \left(\frac{\sigma_{i-1} 2^{\omega_i} \sigma_{i+1}}{\varphi_i}\right) (-1)^{\sum_{i=1}^{\eta_k-1} \frac{\varphi_i-1}{2} \cdot \frac{e_i+1}{2}} \cdot$$

$$\cdot (-1)^{\frac{\varphi_0-1}{2} \cdot \frac{\varphi_1-1}{2} + \frac{\varphi_1-1}{2} \cdot \frac{\varphi_2-1}{2} + \cdots + \frac{\varphi_{\eta_k-2}-1}{2} \cdot \frac{\varphi_{\eta_k-1}-1}{2} + \frac{\varphi_{\eta_k-1}-1}{2} \cdot \frac{\varphi_{\eta_k}-1}{2}}$$

ist, während der andere allein von der Ordnung der Form $f$ und dem Charakter

$$C_k(4) = (-1)^{\frac{\varphi_{\eta_k}-1}{2}}$$

abhängt. Bei einer Aufzählung sämtlicher Charaktere für den Modul $2^t$ können wir daher die Charaktere $\mathsf{E}_k$ durch die Charaktere $\mathfrak{C}_k(4)$ ersetzen.

## Kap. X. [[**Bedingungen für die Gültigkeit der Kongruenz $f \cong g \pmod{q^t}$.**]]

Wir haben gesehen, daß die Kongruenz zweier Klassen $f$ und $g$ nach einem Modul $q^t$, der die höchsten in den Größen $\frac{4}{\sigma_{n-1}} o_1 o_2 \ldots o_{n-1}$ der beiden Formen $f$ und $g$ aufgehenden Potenzen von $q$ übersteigt, von den folgenden Bedingungen abhängt:

I. Die Klassen $f$ und $g$ besitzen, wenn $q = p$, dieselben Größen $p^{\omega_h}$ und, wenn $q = 2$, dieselben Größen $2^{\omega_h}$, $\sigma_h$.

II. Die Determinanten der Klassen $f$ und $g$ sind, wenn $q = p$ ist, nach dem Modul $p^{t+\partial_{n-2}(p)}$, und wenn $q = 2$ ist, nach dem Modul $\sigma_{n-1} \cdot 2^{t+\partial_{n-2}(2)}$ einander kongruent.

III. Die Hauptreste der Klassen $f$ und $g$ besitzen, wenn $q = p$, dieselben Charaktere $\Theta(p)$ und, wenn $q = 2$, dieselben Charaktere $\mathsf{E}(4)$, $\mathsf{H}(4)$, $\mathsf{Z}(8)$; oder (was auf dasselbe hinauskommt):

Die Größen $f(h; q^t)$ und $g(h; q^t)$ sind identisch.

Diese Bedingungen sind aber auch hinreichend dafür, daß die Klassen $f$ und $g$ nach dem Modul $q^t$ kongruent sind; denn es gilt der Satz:

M. Genügen zwei Klassen $f$ und $g$ den Bedingungen I, II, III, so kann man jede Form der einen in äquivalente Formen transformieren, welche nach dem Modul $q^t$ einem beliebigen Repräsentanten $g$ der andern kongruent sind.

Man kann sich zweier verschiedener Methoden bedienen, um diesen Satz zu beweisen, indem man ihn entweder durch einen Schluß von

$n_0 (< n)$ auf $n$ bestätigt oder indem man Substitutionen bestimmt, welche einen Hauptrest $\varphi$ der Klasse $f$ in einen Hauptrest $\psi$ der Klasse $g$ überführen. — Da die Zeit drängt, muß ich darauf verzichten, diese Methoden hier zu entwickeln.*)

## Kap. XI. Genera von Formen. — Bedingungen für die Existenz eines Genus.

Die Zahl der Charaktere, welche zu einer gegebenen Form $f$ gehören und nicht von vornherein durch die Ordnung

$$O\colon \quad \begin{pmatrix} \sigma_h \\ o_h \end{pmatrix}, \quad I$$

dieser Form bestimmt sind, ist stets endlich. Denn wir sahen, daß allein die in dem Produkt $2 \cdot \frac{2}{\sigma_{n-1}} o_1 o_2 \ldots o_{n-1} = \Pi(f)$ enthaltenen Primzahlen derartige Charaktere liefern können.

Wir fassen alle diejenigen Formenklassen, welche dieselbe Ordnung und dieselben Charaktere wie eine gegebene Form besitzen, in ein *Genus* von Formen zusammen.

Der Satz M. in Kap. X zeigt uns, daß die Klassen eines und desselben Genus in bezug auf jeden Modul $p^t > p^{\nu_{n-1}(p)}$ und in bezug auf jeden Modul $2^t > \frac{4}{\sigma_{n-1}} 2^{\nu_{n-1}(2)}$ kongruent sind, woraus wir mit Hilfe des Satzes II in Kap. VI schließen, daß *zwei Klassen desselben Genus in bezug auf jeden beliebigen Modul kongruent sind.*

Umgekehrt ist klar, daß zwei Klassen $f$ und $g$ von gleichem Index $I$, welche verschiedenen Genera angehören, nicht in bezug auf jeden Modul $N$ kongruent sein können. Denn wenn die Invarianten oder die Charaktere der Klassen $f$ und $g$ nicht die gleichen sind, so kann, wie man leicht erkennt, nicht gleichzeitig $f \simeq g \pmod{\Pi(f)}$ und $f \simeq g \pmod{\Pi(g)}$ sein.

Man kann die sämtlichen Charaktere einer Klasse $f$ mit Hilfe eines Hauptrestes dieser Klasse für den Modul $\Pi$ herleiten. Folglich werden zwei Klassen derselben Ordnung $O$ die gleichen Charaktere besitzen, sobald sie in bezug auf den Modul $\Pi$ einander kongruent sind. Also kann man ein Genus von Formen auch in der folgenden Weise definieren:

Ein Genus $f$ besteht aus allen denjenigen Klassen, welche der Ordnung $f$ angehören und in bezug auf den Modul $\Pi(f)$ der Klasse $f$ kongruent sind.

I. Um zu entscheiden, ob zwei Klassen derselben Ordnung $O$ in demselben Genus enthalten sind, kann man sich der Grundformen dieser Klassen für den Modul $\Pi$ bedienen. — Wir behaupten:

*) Siehe die Note [[am Schlusse dieser Abhandlung, S. 136—143]].

Jede primitive Formenklasse $f$ der Ordnung $O$ besitzt für den Modul $\Pi$ Grundformen $\varphi$, in welchen die Zahlen $\varphi_h$ zu den Zahlen $\varphi_{h-1} \cdot \varphi_{h+1}$ relativ prim sind.

In der Tat: wir bemerken zunächst, daß eine Form $f_{h+1} = \{r_{ik}^{(h+1)}\}$ $(i, k = 1, 2, \ldots, h+1)$ von $h+1$ Variablen und von einer Ordnung

$$\begin{pmatrix} \sigma_1, & \sigma_2, & \ldots, & \sigma_{h-1}, & \sigma_h \\ o_1, & o_2, & \ldots, & o_{h-1}, & \sigma_{h+1}\varphi_{h+1} \cdot o_h \end{pmatrix}$$

stets in eine äquivalente Form $\{r_{ik}^{(h)}\}$ $(i, k = 1, 2, \ldots, h+1)$ transformiert werden kann, in welcher die Teilform $f_h = \{r_{ik}^{(h)}\}$ $(i, k = 1, 2, \ldots, h)$ von $h$ Variablen eine Ordnung

$$\begin{pmatrix} \sigma_1, & \sigma_2, & \ldots, & \sigma_{h-2}, & \sigma_{h-1} \\ o_1, & o_2, & \ldots, & o_{h-2}, & \sigma_h\varphi_h \cdot o_{h-1} \end{pmatrix}$$

mit einer zu der Zahl $\Pi \cdot \varphi_{h+1}$ relativ primen Zahl $\varphi_h$ besitzt. Um eine Form von der gewünschten Beschaffenheit zu erhalten, brauchen wir nämlich nur eine Grundform der Klasse $f_{h+1}$ in bezug auf den Modul $\Pi \cdot \varphi_{h+1}$ zu bestimmen.

Wenden wir diese Bemerkung für $h = n-1, n-2, \ldots, 1$ an, indem wir von der Form $f = f_n = \{r_{ik}^{(n)}\}$ $(i, k = 1, 2, \ldots, n)$ ausgehen, so gewinnen wir einen Repräsentanten $\varphi = \{r_{ik}^{(1)}\}$ $(i, k = 1, 2, \ldots, n)$, in welchem die Teilformen $\{r_{ik}^{(1)}\}$ $(i, k = 1, 2, \ldots, h)$ eine Ordnung

$$\begin{pmatrix} \sigma_1, & \sigma_2, & \ldots, & \sigma_{h-2}, & \sigma_{h-1} \\ o_1, & o_2, & \ldots, & o_{h-2}, & \sigma_h\varphi_h \cdot o_{h-1} \end{pmatrix}$$

besitzen, während die Zahlen $\varphi_h$ zu den Zahlen $\Pi \cdot \varphi_{h+1}$ relativ prim sind. Dieser Repräsentant $\varphi$ gibt uns also eine Grundform für den Modul $\Pi$ mit Zahlen $\varphi_h$, welche zu den Zahlen $\varphi_{h-1} \cdot \varphi_{h+1}$ relativ prim sind. Eine solche Form $\varphi$ nennen wir eine *charakteristische Form* der Klasse $f$.

Es möge irgendeine charakteristische Form $\varphi$ der Klasse $f$ vorliegen. Wir wollen die Formen von $h$ Variablen, welche aus den $h$ ersten Reihen des Systems von $\varphi$ gebildet sind, durch $\{\varphi_h\}$ bezeichnen. Es mögen die Indizes dieser Formen $\{\varphi_h\}$ $(h = 1, 2, \ldots, n)$ gleich $I_h$ sein. Dann ist $I_n = I$, und wir setzen noch $I_0 = 0$. Wir schreiben $(-1)^{I_h} = \varepsilon_h$. Die $n+1$ Einheiten $\varepsilon_h$ stellen die Vorzeichen der Größen $\varphi_h$ vor, und es werden daher die Größen $\varepsilon_h\varphi_h$ sämtlich positiv.

Für die Formen $\{\varphi_h\}$ erhalten wir nach einem bekannten Satz die Zerlegungen

$$\{\varphi_h\} = \frac{Z_1^{\,2}}{\varphi_0\varphi_1} + \frac{Z_2^{\,2}}{\varphi_1\varphi_2} + \cdots + \frac{Z_h^{\,2}}{\varphi_{h-1}\varphi_h}.$$

Führen wir jetzt $n$ Einheiten $\delta_1, \delta_2, \ldots, \delta_n$ vermittels der Beziehungen $\delta_h = \varepsilon_h\varepsilon_{h-1}$, $\varepsilon_h = \delta_1\delta_2 \ldots \delta_h$ ein, so müssen von den $h$ ersten Einheiten

$\delta_1, \delta_2, \ldots, \delta_h$ im ganzen $I_h$ gleich $-1$ und $h - I_h$ gleich $+1$ sein, und wir bekommen insbesondere

$$(-1)^{\sum_{i<k}^{1,h} \frac{\delta_i - 1}{2} \cdot \frac{\delta_k - 1}{2}} = (-1)^{\frac{I_h (I_h - 1)}{2}} = (-1)^{\left[\frac{I_h}{2}\right]}.$$

Wenn wir diese Einheit durch die Größen $\varepsilon_i$ ausdrücken, so ergibt sich

$$(-1)^{\frac{I_h (I_h - 1)}{2}} = (-1)^{\sum_{i=1}^{h-1} \frac{\varepsilon_i - 1}{2}} \cdot$$
$$\cdot (-1)^{\frac{\varepsilon_0 - 1}{2} \cdot \frac{\varepsilon_1 - 1}{2} + \frac{\varepsilon_1 - 1}{2} \cdot \frac{\varepsilon_2 - 1}{2} + \cdots + \frac{\varepsilon_{h-2} - 1}{2} \cdot \frac{\varepsilon_{h-1} - 1}{2} + \frac{\varepsilon_{h-1} - 1}{2} \cdot \frac{\varepsilon_h - 1}{2}}.$$

Aus der in Kap. VI (S. 43) aufgestellten Gleichung (8) gewinnen wir eine Kongruenz

$$(35) \qquad -\sigma_{h-1} 2^{\omega_h} \sigma_{h+1} e_h \varphi_{h-1} \varphi_{h+1} \equiv X_h^2 \pmod{\sigma_h^2 \varphi_h},$$

in welcher die Zahl $X_h$ zu $\sigma_h^2 \varphi_h$ relativ prim ausfällt, da nach unserer Voraussetzung über die Form $\varphi$ die Zahl $-\sigma_{h-1} o_h \sigma_{h+1} \varphi_{h-1} \varphi_{h+1}$ zu $\sigma_h^2 \varphi_h$ relativ prim ist. Aus dieser Kongruenz folgt auf der Stelle die Gleichung

$$\left(\frac{\varphi_{h-1} \varphi_{h+1}}{\varepsilon_h \varphi_h}\right) = \left(\frac{-\sigma_{h-1} 2^{\omega_h} \sigma_{h+1}}{\varepsilon_h \varphi_h}\right) \cdot \left(\frac{e_h}{\varepsilon_h \varphi_h}\right),$$

welche wegen

$$\left(\frac{-1}{\varepsilon_h \varphi_h}\right) = (-1)^{\frac{\varepsilon_h - 1}{2} + \frac{\varphi_h - 1}{2}}, \quad \left(\frac{\sigma_{h-1} 2^{\omega_h} \sigma_{h+1}}{\varepsilon_h \varphi_h}\right) = \left(\frac{\sigma_{h-1} 2^{\omega_h} \sigma_{h+1}}{\varphi_h}\right),$$

$$\left(\frac{e_h}{\varepsilon_h \varphi_h}\right) = (-1)^{\frac{e_h - 1}{2} \cdot \frac{\varphi_h - 1}{2}} \left(\frac{\varphi_h}{e_h}\right)$$

die Form annimmt

$$(36) \quad \left(\frac{\varphi_{h-1}}{\varepsilon_h \varphi_h}\right) \cdot \left(\frac{\varphi_{h+1}}{\varepsilon_h \varphi_h}\right) = (-1)^{\frac{\varepsilon_h - 1}{2}} \left(\frac{\sigma_{h-1} 2^{\omega_h} \sigma_{h+1}}{\varphi_h}\right) \cdot (-1)^{\frac{e_h + 1}{2} \cdot \frac{\varphi_h - 1}{2}} \left(\frac{\varphi_h}{e_h}\right).$$

Wir gewinnen demnach die $n + 1$ Formeln

$$\left(\frac{\varphi_1}{\varepsilon_0 \varphi_0}\right) = 1,$$

$$\left(\frac{\varphi_0}{\varepsilon_1 \varphi_1}\right) \cdot \left(\frac{\varphi_2}{\varepsilon_1 \varphi_1}\right) = (-1)^{\frac{\varepsilon_1 - 1}{2}} \left(\frac{\sigma_0 2^{\omega_1} \sigma_2}{\varphi_1}\right) (-1)^{\frac{e_1 + 1}{2} \cdot \frac{\varphi_1 - 1}{2}} \left(\frac{\varphi_1}{e_1}\right),$$

$$\left(\frac{\varphi_1}{\varepsilon_2 \varphi_2}\right) \cdot \left(\frac{\varphi_3}{\varepsilon_2 \varphi_2}\right) = (-1)^{\frac{\varepsilon_2 - 1}{2}} \left(\frac{\sigma_1 2^{\omega_2} \sigma_3}{\varphi_2}\right) (-1)^{\frac{e_2 + 1}{2} \cdot \frac{\varphi_2 - 1}{2}} \left(\frac{\varphi_2}{e_2}\right),$$

. . . . . .

$$\left(\frac{\varphi_{n-3}}{\varepsilon_{n-2} \varphi_{n-2}}\right) \cdot \left(\frac{\varphi_{n-1}}{\varepsilon_{n-2} \varphi_{n-2}}\right) = (-1)^{\frac{\varepsilon_{n-2} - 1}{2}} \left(\frac{\sigma_{n-3} 2^{\omega_{n-2}} \sigma_{n-1}}{\varphi_{n-2}}\right) (-1)^{\frac{e_{n-2} + 1}{2} \cdot \frac{\varphi_{n-2} - 1}{2}} \left(\frac{\varphi_{n-2}}{e_{n-2}}\right),$$

$$\left(\frac{\varphi_{n-2}}{\varepsilon_{n-1} \varphi_{n-1}}\right) \cdot \left(\frac{\varphi_n}{\varepsilon_{n-1} \varphi_{n-1}}\right) = (-1)^{\frac{\varepsilon_{n-1} - 1}{2}} \left(\frac{\sigma_{n-2} 2^{\omega_{n-1}} \sigma_n}{\varphi_{n-1}}\right) (-1)^{\frac{e_{n-1} + 1}{2} \cdot \frac{\varphi_{n-1} - 1}{2}} \left(\frac{\varphi_{n-1}}{e_{n-1}}\right),$$

$$\left(\frac{\varphi_{n-1}}{\varepsilon_n \varphi_n}\right) = 1.$$

Wir multiplizieren jetzt diese $n+1$ Gleichungen miteinander und benutzen dabei das Reziprozitätsgesetz, welches sich für zwei ungerade, zueinander relativ prime Zahlen $U$ und $V$, deren Vorzeichen gleich $u$ und $v$ sind, in der Formel

$$\left(\frac{V}{u\,U}\right)\cdot\left(\frac{U}{v\,V}\right)=(-1)^{\frac{u-1}{2}\cdot\frac{v-1}{2}+\frac{U-1}{2}\cdot\frac{V-1}{2}}$$

ausspricht. Dadurch erhalten wir die Relation

$$(37)\quad\begin{cases}(-1)^{\left[\frac{I}{2}\right]}=(-1)^{\sum_{h=1}^{n-1}\frac{\varepsilon_h-1}{2}}\cdot(-1)^{\frac{\varepsilon_0-1}{2}\cdot\frac{\varepsilon_1-1}{2}+\frac{\varepsilon_1-2}{2}\cdot\frac{\varepsilon_2-1}{2}+\cdots+\frac{\varepsilon_{n-2}-1}{2}\cdot\frac{\varepsilon_{n-1}-1}{2}+\frac{\varepsilon_{n-1}-1}{2}\cdot\frac{\varepsilon_n-1}{2}}\\ \qquad=\prod_{h=1}^{n-1}\left(\frac{\sigma_{h-1}2^{\omega_h}\sigma_{h+1}}{\varphi_h}\right)\cdot\prod_{h=1}^{n-1}\left(\frac{\varphi_h}{e_h}\right)\cdot(-1)^{\sum_{h=1}^{n-1}\frac{e_h+1}{2}\cdot\frac{\varphi_h-1}{2}}\cdot\\ \qquad\qquad(-1)^{\frac{\varphi_0-1}{2}\cdot\frac{\varphi_1-1}{2}+\frac{\varphi_1-1}{2}\cdot\frac{\varphi_2-1}{2}+\cdots+\frac{\varphi_{n-2}-1}{2}\cdot\frac{\varphi_{n-1}-1}{2}+\frac{\varphi_{n-1}-1}{2}\cdot\frac{\varphi_n-1}{2}}.\end{cases}$$

Bilden wir das Produkt aus den ersten $\eta_k$ oder aus den ersten $\eta_k+1$ der obigen Gleichungen, so erkennen wir, daß der Charakter $\mathfrak{C}_k(4)$ mit Hilfe der Charaktere $C(p)$, $C(4)$, $C(8)$ und der Einheit

$$D_k^-=\left(\frac{\varphi_{\eta_k}-1}{\varepsilon_{\eta_k}\varphi_{\eta_k}}\right)(-1)^{\frac{I_{\eta_k}(I_{\eta_k}-1)}{2}}$$

oder der Einheit

$$D_k^+=\left(\frac{\varphi_{\eta_k}+1}{\varepsilon_{\eta_k}\varphi_{\eta_k}}\right)(-1)^{\frac{I_{\eta_k}(I_{\eta_k}+1)}{2}}$$

dargestellt werden kann. Infolgedessen können wir statt der Charaktere $\mathfrak{C}_k$ die Charaktere $D_k^-$ oder $D_k^+$ einführen.

Zwischen den beiden Charakteren $D_k^-$ und $D_k^+$ besteht zufolge der Gleichung (36) die Relation

$$(38)\qquad D_k^-\cdot D_k^+=\left(\frac{\sigma_{\eta_k-1}\cdot 2^{\omega_{\eta_k}}\cdot\sigma_{\eta_k+1}}{\varphi_{\eta_k}}\right)(-1)^{\frac{e_{\eta_k}+1}{2}\cdot\frac{\varphi_{\eta_k}-1}{2}}\left(\frac{\varphi_{\eta_k}}{e_{\eta_k}}\right).$$

Wir können jetzt den Satz aussprechen:

*Eine charakteristische Form $\varphi$ der primitiven Formenklasse $f$ besitzt:*

I. *wenn* $\sigma_{h-1}o_h\sigma_{h+1}\equiv 0\pmod p$ *ist, einen Charakter*

$$\left(\frac{\varphi_h}{p}\right),$$

II. *wenn* $\sigma_{h-1}o_h\sigma_{h+1}\equiv 0\pmod 4$ *ist, drei Charaktere*

$$(-1)^{\frac{\varphi_h-1}{2}},\quad\left(\frac{\varphi_{h-1}}{\varepsilon_h\varphi_h}\right)(-1)^{\frac{I_h(I_h-1)}{2}},\quad\left(\frac{\varphi_{h+1}}{\varepsilon_h\varphi_h}\right)(-1)^{\frac{I_h(I_h+1)}{2}},$$

III. *wenn* $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod 8$ *ist, einen Charakter*

$$\left(\frac{2}{\varphi_h}\right).$$

Diese Charaktere sind an die folgenden Bedingungen gebunden:

1. Es sind

$$\left(\frac{\varphi_0}{p}\right) = 1, \quad \left(\frac{\varphi_n}{p}\right) = (-1)^{\frac{p-1}{2} \cdot I}; \quad (-1)^{\frac{\varphi_0 - 1}{2}} = 1, \quad (-1)^{\frac{\varphi_n - 1}{2}} = (-1)^I;$$

$$\left(\frac{2}{\varphi_0}\right) = 1, \quad \left(\frac{2}{\varphi_n}\right) = 1;$$

$$\left(\frac{\varphi_1}{\varepsilon_0 \varphi_0}\right)(-1)^{\frac{I_0(I_0+1)}{2}} = 1, \quad \left(\frac{\varphi_{n-1}}{\varepsilon_n \varphi_n}\right)(-1)^{\frac{I_n(I_n-1)}{2}} = (-1)^{\left[\frac{I}{2}\right]}.$$

2. Wenn $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod 4$ ist, so wird

$$\left[\left(\frac{\varphi_{h-1}}{\varepsilon_h \varphi_h}\right)(-1)^{\frac{I_h(I_h-1)}{2}}\right]\left[\left(\frac{\varphi_{h+1}}{\varepsilon_h \varphi_h}\right)(-1)^{\frac{I_h(I_h+1)}{2}}\right] = \left(\frac{\sigma_{h-1} 2^{\omega_h} \sigma_{h+1}}{\varphi_h}\right)(-1)^{\frac{e_h+1}{2} \cdot \frac{\varphi_h - 1}{2}} \left(\frac{\varphi_h}{e_h}\right).$$

3. Wenn $\sigma_h = 2$ ist, in welchem Falle

$$\sigma_{h-2} o_{h-1} \sigma_h \equiv 0 \equiv \sigma_h o_{h+1} \sigma_{h+2} \pmod 4 \quad \text{und} \quad o_h \equiv 1 \pmod 2$$

wird, so hat zwischen den Charakteren

$$(-1)^{\frac{\varphi_{h-1} - 1}{2}} \quad \text{und} \quad (-1)^{\frac{\varphi_{h+1} - 1}{2}}$$

die Beziehung statt:

$$(-1)^{\frac{\varphi_{h-1} - 1}{2}} \cdot (-1)^{\frac{\varphi_{h+1} - 1}{2}} = (-1)^{\frac{e_h + 1}{2}}.$$

4. Wenn $\sigma_{h-2} o_{h-1} \sigma_h \equiv 0 \equiv \sigma_h o_{h+1} \sigma_{h+2} \pmod 4$ und $o_h \equiv 1 \pmod 2$ ist und zwischen den Charakteren $(-1)^{\frac{\varphi_{h-1} - 1}{2}}$ und $(-1)^{\frac{\varphi_{h+1} - 1}{2}}$ die Gleichung

$$(-1)^{\frac{\varphi_{h-1} - 1}{2}} \cdot (-1)^{\frac{\varphi_{h+1} - 1}{2}} = (-1)^{\frac{e_h + 1}{2}}$$

statthat, so wird

$$\left[\left(\frac{\varphi_h}{\varepsilon_{h-1} \varphi_{h-1}}\right)(-1)^{\frac{I_{h-1}(I_{h-1}+1)}{2}}\right]\left[\left(\frac{\varphi_h}{\varepsilon_{h+1} \varphi_{h+1}}\right)(-1)^{\frac{I_{h+1}(I_{h+1}-1)}{2}}\right] = \left(\frac{\varphi_h}{e_h}\right).$$

5. Wenn $\sigma_{h_1 - 1} o_{h_1} \sigma_{h_1 + 1} \equiv 0 \pmod 4$, $\sigma_{h_{11} - 1} o_{h_{11}} \sigma_{h_{11} + 1} \equiv 0 \pmod 4$ und $h_1 - h_{11} = \pm 1$ ist, so wird

$$\left[\left(\frac{\varphi_{h_1}}{\varepsilon_{h_{11}} \varphi_{h_{11}}}\right)(-1)^{\frac{I_{h_{11}}[I_{h_{11}} + (h_1 - h_{11})]}{2}}\right]\left[\left(\frac{\varphi_{h_{11}}}{\varepsilon_{h_1} \varphi_{h_1}}\right)(-1)^{\frac{I_{h_1}[I_{h_1} + (h_{11} - h_1)]}{2}}\right] = (-1)^{\frac{\varphi_{h_1} - 1}{2} \cdot \frac{\varphi_{h_{11}} - 1}{2}}.$$

Die Bedingungen 1. ergeben sich aus den Beziehungen $\varphi_0 = 1$, $\varphi_n = (-1)^I$; die Bedingung 2. stimmt mit der Gleichung (38) überein;

die Bedingung 3. entspringt aus der Kongruenz (35), welche für ein $\sigma_h = 2$ die Relation

$$-e_h \varphi_{h-1} \varphi_{h+1} \equiv 1 \pmod 4$$

liefert; die Bedingung 4. schließen wir aus der Gleichung

$$\left[\left(\frac{\varphi_h}{\varepsilon_{h-1}\varphi_{h-1}}\right)(-1)^{\frac{I_{h-1}(I_{h-1}+1)}{2}}\right]\left[\left(\frac{\varphi_h}{\varepsilon_{h+1}\varphi_{h+1}}\right)(-1)^{\frac{I_{h+1}(I_{h+1}-1)}{2}}\right]$$
$$= \left(\frac{\sigma_{h-1}2^{\omega_h}\sigma_{h+1}}{\varphi_h}\right)(-1)^{\frac{e_h\varphi_{h-1}\varphi_{h+1}+1}{2}\cdot\frac{\varphi_h-1}{2}}\left(\frac{\varphi_h}{e_h}\right),$$

welche eine unmittelbare Folge von (36) ist; die Bedingung 5. ist eine Identität. — Drücken wir die Charaktere $D_k$ durch die Charaktere $\mathfrak{C}_k(4)$ aus, so werden sämtliche Bedingungen 2., 4., 5. zu Identitäten, und es bleiben allein die Bedingungen 3. und die Bedingung (37) zu erfüllen.

II. Zu jeder Kombination von Charakteren I., II., III., welche allen Bedingungen 1., 2., 3., 4., 5. genügt, gehört ein Genus der Ordnung $O$, welches wirklich primitive Formen enthält.

Beweis: Es möge irgendeine Kombination der Charaktere I., II., III. oder der Charaktere $C(p)$, $C(4)$, $C(8)$, $\mathfrak{C}(4)$ gegeben sein, welche keiner der aufgestellten Bedingungen widerspricht. Alsdann können wir leicht $n-1$ Zahlen $\overline{\varphi}_h$ finden, welche zu den Zahlen $2o_h$ relativ prim sind und für welche die Einheiten $C_p(\overline{\varphi})$, $C_4(\overline{\varphi})$, $C_8(\overline{\varphi})$, $\mathfrak{C}_4(\overline{\varphi})$ gleich den gegebenen Größen $C(p)$, $C(4)$, $C(8)$, $\mathfrak{C}(4)$ ausfallen. Da die Einheiten $C_p(\overline{\varphi})$, $C_4(\overline{\varphi})$, $C_8(\overline{\varphi})$, $\mathfrak{C}_4(\overline{\varphi})$ nur von den Resten der Zahlen $\overline{\varphi}_h$ in bezug auf die Moduln $8o_h$ abhängen, so erhellt, daß für irgendein System von Zahlen $\varphi_h$, welches den Kongruenzen

$$\varphi_h \equiv \overline{\varphi}_h \pmod{8o_h} \qquad (h = 1, 2, \ldots, n-2, n-1)$$

genügt, gewiß auch die Einheiten $C_p(\varphi)$, $C_4(\varphi)$, $C_8(\varphi)$, $\mathfrak{C}_4(\varphi)$ gleich den gegebenen Einheiten $C(p)$, $C(4)$, $C(8)$, $\mathfrak{C}(4)$ sein werden.

Wir wählen nun $n$ Einheiten $\delta_1, \delta_2, \ldots, \delta_n$, von welchen $I$ gleich $-1$ und $n-I$ gleich $+1$ sein mögen, und setzen $\delta_1\delta_2\ldots\delta_h = \varepsilon_h$. Aus dem bekannten Satz, daß eine jede arithmetische Progression $zS+s$ ($s$ relativ prim zu $S$, $z = -\infty \ldots, -2, -1, 0, 1, 2, \ldots +\infty$) sowohl unendlich viele positive als unendlich viele negative Primzahlen enthält, erkennen wir (mit Hinzuziehung eines einfachen Schlusses von $h-1$ auf $h$), daß wir die Zahlen $\varphi_h \equiv \overline{\varphi}_h \pmod{8o_h}$ ($h = 1, 2, \ldots, n-2, n-1$) derart bestimmen können, daß die Größen $\varepsilon_h\varphi_h$ positive Primzahlen werden, daß die Zahlen $\varphi_h$ zu den Zahlen $2o_1o_2\ldots o_{n-2}o_{n-1}\cdot\varphi_{h-1}$ relativ prim ausfallen und daß $n-1$ Kongruenzen der Form

$$[\varphi_0 = 1] \qquad -\sigma_{h-1}o_h\sigma_{h+1}\varphi_{h-1}\varphi_{h+1} \equiv X_h^2 \pmod{\sigma_h^2\varphi_h} \qquad [\varphi_n = (-1)^I]$$

statthaben.*) Nachdem wir $n-1$ derartige Zahlen $\varphi_h$ gefunden haben, suchen wir $n-1$ Zahlen $y_1, y_2, \ldots, y_{n-1}$ auf, welche den Kongruenzen

$$[y_0 = 0] \qquad -\frac{1}{o_h}\frac{\sigma_{h+1}\varphi_{h+1}}{\sigma_{h-1}\varphi_{h-1}} \equiv y_h^2 \pmod{\sigma_h\varphi_h} \quad (h = 1, 2, \ldots, n-1)$$

genügen, und wir setzen die ganzen Zahlen

$$\frac{\sigma_{h+1}\varphi_{h+1} + \sigma_{h-1}\varphi_{h-1}o_h y_h^2}{\sigma_h\varphi_h} = t_h$$

und

$$o_1 o_2 \cdots o_h \cdot y_h = \mathsf{Y}_h, \quad o_1 o_2 \cdots o_h \cdot t_h = \mathsf{T}_h.$$

Die Form

$$\varphi = \begin{pmatrix} \mathsf{T}_0, & \mathsf{Y}_1 & & & & & \\ \mathsf{Y}_1, & \mathsf{T}_1, & \mathsf{Y}_2 & & & & \\ & \mathsf{Y}_2, & \mathsf{T}_2, & \mathsf{Y}_3 & & & \\ & & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & & \mathsf{Y}_{n-2}, & \mathsf{T}_{n-2}, & \mathsf{Y}_{n-1} \\ & & & & & \mathsf{Y}_{n-1}, & \mathsf{T}_{n-1} \end{pmatrix}$$

bildet jetzt, wie man sich leicht überzeugt, eine charakteristische Form für ein Genus $G$, welches die gegebenen Charaktere besitzt. — Die aus den ersten $h$ Reihen von $\varphi$ gebildeten symmetrischen Unterdeterminanten werden gleich den Zahlen $\sigma_h d_{h-1}\varphi_h$.

Das soeben entwickelte Verfahren dient, wie zum Beweise der Existenz eines Formengenus $G$, so auch zum Nachweise der Existenz einer beliebigen Ordnung. Um ein Beispiel zu geben, zeigen wir, daß es primitive Formen mit 8 Variablen von der Determinante 1 gibt, welche der Ordnung

$$\begin{pmatrix} \sigma_h \\ o_h \end{pmatrix} = \begin{pmatrix} 2, & 1, & 2, & 1, & 2, & 1, & 2 \\ 1, & 1, & 1, & 1, & 1, & 1, & 1 \end{pmatrix}, \quad I = 0$$

angehören.

Man erkennt, daß die $8 - 1 = 7$ Zahlen

$$\varphi_1 = 1, \ \varphi_2 = 3, \ \varphi_3 = 5, \ \varphi_4 = 13, \ \varphi_5 = 5, \ \varphi_6 = 3, \ \varphi_7 = 1$$

den Kongruenzen (36) genügen, und man erhält die Form

$$\varphi^{(8)} = \begin{pmatrix} 2, & 1 & & & & & & \\ 1, & 2, & 1 & & & & & \\ & 1, & 4, & 3 & & & & \\ & & 3, & 4, & 5 & & & \\ & & & 5, & 20, & 3 & & \\ & & & & 3, & 12, & 1 & \\ & & & & & 1, & 4, & 1 \\ & & & & & & 1, & 2 \end{pmatrix} \sim \begin{pmatrix} 2, & 1 & & & & & & \\ 1, & 2, & 1, & 0, & -1 & & & \\ & 1, & 2, & 1, & 0 & & & \\ & 0, & 1, & 2, & 1 & & & \\ & -1, & 0, & 1, & 2, & 1 & & \\ & & & & 1, & 2, & 1 & \\ & & & & & 1, & 2, & 1 \\ & & & & & & 1, & 2 \end{pmatrix}.$$

*) Siehe Dirichlet, Vorlesungen über Zahlentheorie, herausgeg. von Dedekind, 1880, S. 328. [[4. Auflage (1894), S. 328]].

Da diese Form einer anderen Ordnung angehört wie die Form $\varphi^{(0)} = \sum_{h=1}^{8} x_h^2$, so kann sie dieser Form $\varphi^{(0)}$ nicht äquivalent sein, und wir sehen somit, daß die Formen von 8 Variablen und der Determinante 1 mindestens zwei Formenklassen liefern. Entsprechend liefern die Formen von $n\left(=8\left[\frac{n}{8}\right]+n_0,\ n_0<8\right)$ Variablen und der Determinante 1 mindestens $\left[\frac{n}{8}\right]+1$ Formenklassen. Denn es sind die $\left[\frac{n}{8}\right]+1$ Formen

$$\varphi_{(m)} = \varphi^{(8)}(x_1, \ldots, x_8) + \varphi^{(8)}(x_9, \ldots, x_{16}) + \cdots + \varphi^{(8)}(x_{8m-7}, \ldots, x_{8m}) + \sum_{h=8m+1}^{n} x_h^2$$

$$\left(m = 0, 1, 2, \ldots, \left[\frac{n}{8}\right]\right)$$

sämtlich von der Determinante 1, und es können nicht zwei von diesen Formen einander äquivalent sein, da die Anzahl der Darstellungen der Zahl 1 durch eine dieser Formen $\varphi_{(m)}$ gleich $2(n-8m)$ ist und mithin für keine zwei dieser Formen denselben Wert erhält.

III. Die Anzahl der sämtlichen Kombinationen der Charaktere I., II., III., welche mit den aufgestellten Bedingungen verträglich sind, möge durch $g$ bezeichnet werden. Wir wollen die Anzahl der Größen $\sigma_{h-1}o_h\sigma_{h+1}$ $(h = 1, 2, \ldots, n-2, n-1)$, welche durch eine ungerade Primzahl $p$ oder durch die Zahl 4 oder durch die Zahl 8 teilbar sind, von neuem gleich $\lambda_p - 1$, gleich $\mu - 1$, gleich $\nu - 1$ setzen; die Anzahl der Fälle, in welchen zwei aufeinanderfolgende Zahlen $\sigma_{h-1}o_h\sigma_{h+1}$ $(h=0, 1, 2, \ldots, n-1, n)$ gleichzeitig durch 4 teilbar sind, sei gleich $\mu_{,}$, und die Anzahl der Fälle, in welchen $\sigma_h = 1$, $\sigma_{h-2}o_{h-1}\sigma_h \equiv 0 \equiv \sigma_h o_{h+1}\sigma_{h+2} \pmod 4$, $o_h \equiv 1 \pmod 2$ $(h = 1, 2, \ldots, n-1)$ ist, sei gleich $\mu_{,,}$; ferner möge $\mu - \mu_0$ die Anzahl aller Invarianten $\sigma_h (h = 1, 2, \ldots, n-1)$ bedeuten, welche gleich 2 sind.

Die Zahl $g$, welche zugleich die Anzahl der sämtlichen wirklich vorhandenen Genera von der Ordnung

$$O: \begin{pmatrix} \sigma_1, & \sigma_2, & \ldots, & \sigma_{n-2}, & \sigma_{n-1} \\ o_1, & o_2, & \ldots, & o_{n-2}, & o_{n-1} \end{pmatrix}, \quad I$$

ergibt, erhält den Ausdruck

$$g = g_0[1 + \{\mu_0 - \mu_{,,}\} + \square(\mu_0 - \mu_{,} - \mu_{,,})],$$

in welchem die Größen $g_0$, $\{\mu_0 - \mu_{,,}\}$, $\square(\mu_0 - \mu_{,} - \mu_{,,})$ die nachstehende Bedeutung haben:

Es ist

$$g_0 = 2^{\sum_{(p)}(\lambda_p - 1) + 2(\mu_0 - 1) + (\nu - 1)} \left(\frac{1}{2}\right)^{\mu_{,}} \left(\frac{3}{4}\right)^{\mu_{,,}},$$

worin die Summe $\sum_{(p)}(\lambda_p - 1)$ über alle Größen $\lambda_p$ zu erstrecken ist, welche einer in dem Produkt $\prod_{h=1}^{n-1} o_h$ aufgehenden ungeraden Primzahl $p$ entsprechen.

Es ist

$$\{\mu_0 - \mu_{,,}\} = 0,$$

sobald $\mu_0 - \mu_{,,} > 0$ ist, und

$$\{\mu_0 - \mu_{,,}\} = (-1)^{\frac{n}{2} - I + \mu_{,,}} \cdot \left( \frac{-1}{\prod_{h=1}^{\frac{n}{2}} \frac{o_{2h-1}}{2^{\omega_{2h-1}}}} \right) \cdot \frac{1}{3^{\mu_{,,}}}, \quad [n \equiv 0 \pmod 2]$$

sobald $\mu_0 - \mu_{,,} = 0$, d. h. $\mu_{,} = 0$, $n = 2\mu$ ist.

Es wird

$$\square(\mu_0 - \mu_{,} - \mu_{,,}) = 0,$$

wenn $\mu_0 - \mu_{,} - \mu_{,,} > 0$ ist oder wenn irgendeine der Zahlen $\sigma_{h-1} o_h \sigma_{h+1}$ $(h = 1, 2, \ldots, n-1)$ kein Quadrat ist, dagegen wird

$$\square(\mu_0 - \mu_{,} - \mu_{,,}) = \delta(n - 2I) \cdot \frac{1}{3^{\mu_{,,}} 2^{\left[\frac{\mu_{,}-1}{2}\right]}}$$

$$\left\{ \begin{array}{c|c|c|c|c|c|c|c|l} n - 2I \equiv & 1 & 3 & 5 & 7 & 0 & 2 & 4 & 6 \pmod 8 \\ \delta(n-2I) = & 1 & -1 & -1 & 1 & 1 & 0 & -1 & 0 \end{array} \right\},$$

wenn $\mu_0 - \mu_{,} - \mu_{,,} = 0$ ist und die sämtlichen Zahlen $\sigma_{h-1} o_h \sigma_{h+1}$ Quadrate sind.

Offenbar besitzt nach dem Satze II. eine Ordnung $O$ stets primitive Formen, wenn nicht $g = 0$ ist. Man erkennt leicht, daß nur in den folgenden Fällen $g = 0$ werden kann:

$(\square = 0)$ wenn

$$\mu_0 = 0;\ \mu_{,} = 0,\ \mu_{,,} = 0, \quad (-1)^{\frac{n}{2} - I} \prod_{h=1}^{\frac{n}{2}} \frac{o_{2h-1}}{2^{\omega_{2h-1}}} \equiv -1 \pmod 4$$

ist;

$(\delta = -1)$ wenn alle Zahlen $\sigma_{h-1} o_h \sigma_{h+1}$ Quadratzahlen sind und entweder

$$\mu_0 = 0;\ \mu_{,} = 0,\ \mu_{,,} = 0, \qquad n - 2I \equiv 4 \pmod 8$$

oder

$$\mu_0 = 1;\ \mu_{,} = 1,\ \mu_{,,} = 0, \qquad n - 2I \equiv 3, 5 \pmod 8$$

oder

$$\mu_0 = 1;\ \mu_{,} = 0,\ \mu_{,,} = 1, \qquad n - 2I \equiv 4 \pmod 8$$

oder

$$\mu_0 = 2;\ \mu_{,} = 2,\ \mu_{,,} = 0, \qquad n - 2I \equiv 4 \pmod 8$$

ist.

## Kap. XII. Adjungierte Formen. — Reziprozität zwischen den Ordnungen $\begin{pmatrix}\sigma_1, \sigma_2, \cdots, \sigma_{n-2}, \sigma_{n-1}\\ o_1, o_2, \cdots, o_{n-2}, o_{n-1}\end{pmatrix}$, $I$ und $\begin{pmatrix}\sigma_{n-1}, \sigma_{n-2}, \cdots, \sigma_2, \sigma_1\\ o_{n-1}, o_{n-2}, \cdots, o_2, o_1\end{pmatrix}$, $I$.

Es sei $f=\sum_{i,k=1}^{n} a_{ik}x_i x_k$ eine primitive quadratische Form von der Determinante $\Delta(f)$. Der größte gemeinsame Teiler aller $(n-1)$-reihigen Unterdeterminanten $\frac{\partial\Delta(f)}{\partial a_{ik}}$ ist gleich $d_{n-2}$. Setzen wir also

$$\frac{1}{d_{n-2}}\cdot\frac{\partial\Delta(f)}{\partial a_{ik}}=\varepsilon\cdot a'_{n-i+1,n-k+1},$$

wo $\varepsilon=(-1)^{I(f)}$ ist, so wird die Form

$$f'=\sum_{i,k=1}^{n} a'_{ik}x'_i x'_k$$

ebenso wie die Form $f$ primitiv sein. Diese Form $f'$ soll der Form $f$ *adjungiert* heißen, und wir schreiben $f\asymp f'$.

N. Wenn die Form $f$ einer Form $g=\sum_{l,m=1}^{n} b_{lm}y_l y_m$ äquivalent ist, so ist die zu $f$ adjungierte Form $f'$ der zu $g$ adjungierten Form $g'=\sum_{l,m=1}^{n} b'_{lm}y'_l y'_m$ äquivalent.

Denn nehmen wir an, die Form $f$ gehe in $g$ durch eine Substitution

$$S:\quad x_i=\sum_{l=1}^{n} s_i^l y_l$$

über, so wird

$$B\begin{pmatrix}l_1, l_2, \ldots, l_{n-1}\\ m_1, m_2, \ldots, m_{n-1}\end{pmatrix}$$
$$=\sum A\begin{pmatrix}i_1, i_2, \ldots, i_{n-1}\\ k_1, k_2, \ldots, k_{n-1}\end{pmatrix} S^{(l_1, l_2, \ldots, l_{n-1})}_{(i_1, i_2, \ldots, i_{n-1})} S^{(m_1, m_2, \ldots, m_{n-1})}_{(k_1, k_2, \ldots, k_{n-1})}.$$

Die Unterdeterminanten $S^{(l_1, l_2, \ldots, l_{n-1})}_{(i_1, i_2, \ldots, i_{n-1})}$ stimmen dem absoluten Werte nach mit den Zahlen $\frac{\partial|S|}{\partial s_i^l}=s'^{n-l+1}_{n-i+1}$ überein, und wir erkennen leicht, daß die vorstehende Gleichung sich schreiben läßt

$$(-1)^I d_{n-2}b'_{lm}=\sum_{i,k=1}^{n}(-1)^I d_{n-2}a'_{ik}s'^{l}_{i}s'^{m}_{k}.$$

Demnach wird die Form $f'$ in $g'$ durch die Substitution

$$S': \quad x_i' = \sum_{l=1}^{n} s_i'^{l} y_l'$$

transformiert. Man findet noch $|S'| = |S|^{n-1}$. Wenn also $|S| = 1$ und $f \sim g$ ist, so wird $|S'| = 1$ und $f' \sim g'$.

Die Substitution $S'$ möge der Substitution $S$ *adjungiert* heißen ($S \asymp S'$).

Wenn $f$ vermittelst einer linearen Substitution in eine Summe von $n$ Quadraten

$$f = -\sum_{h=1}^{I(f)} \mathsf{X}_h^2 + \sum_{h=1}^{n-I(f)} \Xi_h^2$$

transformiert wird, so läßt sich die Form $f'$ in der Gestalt

$$f' = -\sum_{h=1}^{I(f)} \mathsf{X}_h'^2 + \sum_{h=1}^{n-I(f)} \Xi_h'^2$$

schreiben. Es gilt also die Beziehung

$$I(f) = I(f') = I.$$

Wir bezeichnen die $n-1$ Invarianten $\sigma$, $o$, $d$ der Form $f'$ durch $\sigma_h'$, $o_h'$, $d_h'$ $(h = 1, 2, \cdots, n-2, n-1)$.

Man beweist leicht den folgenden Satz:

*Wenn $f'$ der Form $f$ adjungiert ist, wird auch $f$ der Form $f'$ adjungiert sein.*

Denn ist $f'' = \sum_{i,k=1}^{n} a_{ik}'' x_i'' x_k''$ die zu $f'$ adjungierte Form, so gelten nach einem bekannten Determinantensatz die Gleichungen

$$(\varepsilon d_{n-2})^{n-1} \cdot \varepsilon d_{n-2}' a_{ik}'' = (\varepsilon d_{n-2})^{n-1} \cdot \frac{\partial \Delta(f')}{\partial a_{n-i+1,n-k+1}'} = (\varepsilon d_{n-1})^{n-2} \cdot a_{ik},$$

in denen $\varepsilon = (-1)^I$ ist. Demnach ist der Quotient $\frac{a_{ik}''}{a_{ik}}$ immer positiv und für alle Werte von $i$ und $k$ derselbe. Da aber die Größen $a_{ik}''$ ebenso wie die $a_{ik}$ ganze Zahlen ohne einen gemeinsamen Teiler $> 1$ sind, so muß $\frac{a_{ik}''}{a_{ik}} = 1$, d. i. $f'' = f$ werden.

Man kann die Ordnung der Form $f'$ aus der Ordnung der Form $f$ herleiten. Wenn wir die symmetrischen $h$-reihigen Unterdeterminanten der Form $f$ und der Form $f'$ durch $F_h$ und durch $F_h'$ bezeichnen, die unsymmetrischen aber durch $P_h$ und durch $P_h'$, so bestehen nach einem bekannten Satz zwischen den $F_h$, $P_h$, $F_h'$, $P_h'$ die Relationen

$$(\varepsilon d_{n-2})^h F_h' = (\varepsilon d_{n-1})^{h-1} F_{n-h}, \quad (\varepsilon d_{n-2})^h P_h' = (\varepsilon d_{n-1})^{h-1} P_{n-h}.$$

Infolgedessen muß erstens der größte positive Teiler aller Zahlen $(\varepsilon d_{n-2})^h F_h'$,

$(\varepsilon d_{n-2})^h P_h'$ mit dem größten positiven Teiler der Zahlen $(\varepsilon d_{n-1})^{h-1} F_{n-h}$, $(\varepsilon d_{n-1})^{h-1} P_{n-h}$ übereinstimmen; zweitens wird der größte positive Teiler der Zahlen $(\varepsilon d_{n-2})^h F_h'$, $(\varepsilon d_{n-2})^h 2 P_h'$ dem größten positiven Teiler der Zahlen $(\varepsilon d_{n-1})^{h-1} F_{n-h}$, $(\varepsilon d_{n-1})^{h-1} 2 P_{n-h}$ gleich sein müssen. Wir bekommen demnach die Gleichungen

$$d_{n-2}^h d_{h-1}' = d_{n-1}^{h-1} d_{n-h-1},$$
$$\sigma_h' d_{n-2}^h d_{h-1}' = \sigma_{n-h} d_{n-1}^{h-1} d_{n-h-1}.$$

Die Division der zweiten Gleichung durch die erste gibt zunächst

$$\sigma_h' = \sigma_{n-h},$$

d. i.

$$\sigma_1' = \sigma_{n-1},\ \sigma_2' = \sigma_{n-2},\ \ldots,\ \sigma_{n-2}' = \sigma_2,\ \sigma_{n-1}' = \sigma_1. \tag{39}$$

Dann führt die Kombination der drei Gleichungen

$$d_{n-2}^{h+1} d_h' = d_{n-1}^h d_{n-h-2}, \tag{40$_1$}$$
$$d_{n-2}^h d_{h-1}' = d_{n-1}^{h-1} d_{n-h-1}, \tag{40$_2$}$$
$$d_{n-2}^{h-1} d_{h-2}' = d_{n-1}^{h-2} d_{n-h} \tag{40$_3$}$$

zu

$$\frac{d_h' \cdot d_{h-2}'}{(d_{h-1}')^2} = \frac{d_{n-h} \cdot d_{n-h-2}}{d_{n-h-1}^2}, \quad o_h' = o_{n-h},$$

d. i.

$$o_1' = o_{n-1},\ o_2' = o_{n-2},\ \ldots,\ o_{n-2}' = o_2,\ o_{n-1}' = o_1. \tag{41}$$

Die Form $f'$ gehört daher einer Ordnung

$$O': \begin{pmatrix} \sigma_{n-1}, & \sigma_{n-2}, & \ldots, & \sigma_2, & \sigma_1 \\ o_{n-1}, & o_{n-2}, & \ldots, & o_2, & o_1 \end{pmatrix}, \quad I$$

an.

Unter Benutzung des Satzes N. können wir jetzt das Resultat aussprechen:

Jeder Klasse $f$ der Ordnung $\begin{pmatrix} \sigma_h \\ o_h \end{pmatrix}$, $I$ ist eine bestimmte Klasse $f'$ der Ordnung $\begin{pmatrix} \sigma_{n-h} \\ o_{n-h} \end{pmatrix}$, $I$ adjungiert.

Wenn $\varphi$ eine Grundform der Klasse $f$ für den Modul $N$ bedeutet, so stellt die der Form $\varphi$ adjungierte Form $\varphi'$ eine Grundform der Klasse $f'$ für den Modul $N$ vor. Denn offenbar sind die $n+1$ Zahlen $\varphi_h'$ der Form $\varphi'$ mit den $n+1$ Zahlen $\varphi_h$ der Form $\varphi$ durch die Gleichungen

$$\varphi_h' = (-1)^I \varphi_{n-h},$$

d. i.

$$\varphi_1' = (-1)^I \varphi_{n-1},\ \varphi_2' = (-1)^I \varphi_{n-2},\ \ldots,\ \varphi_{n-2}' = (-1)^I \varphi_2,\ \varphi_{n-1}' = (-1)^I \varphi_1$$

verbunden.

Demnach sind die Charaktere der Klasse $f'$ aus denen der Klasse $f$ ableitbar. Wir schließen hieraus den Satz:

Gehören die beiden Formen $f$ und $g$ einem und demselben Genus an, so sind auch die ihnen adjungierten Formen $f'$ und $g'$ in einem und demselben Genus enthalten.

Infolgedessen werden zwei *Genera* allemal dann *adjungiert* heißen, wenn eine Form des einen Genus einer Form des andern adjungiert ist.

## Zweiter Teil.

## Über die Darstellung ganzer Zahlen durch quadratische Formen.

### Kap. XIII. **Hilfssatz.**

Es sei ein System von $n \cdot \nu$ ganzen Zahlen $u_k^h$ $(0 \leqq k < n,\ 0 \leqq h < \nu)$

$$(u) = \begin{pmatrix} u_0^0, & u_1^0, & \ldots, & u_{n-1}^0 \\ u_0^1, & u_1^1, & \ldots, & u_{n-1}^1 \\ \cdot & \cdot & \cdot & \cdot \\ u_0^{\nu-1}, & u_1^{\nu-1}, & \ldots, & u_{n-1}^{\nu-1} \end{pmatrix} \qquad (\nu < n)$$

gegeben. Falls die sämtlichen $\nu$-reihigen Unterdeterminanten

$$u \begin{pmatrix} 0, & 1, & \ldots, & \nu-1 \\ k_0, & k_1, & \ldots, & k_{\nu-1} \end{pmatrix} \qquad (k = 0,\ 1, \ldots, n-1),$$

welche sich aus diesem Systeme bilden lassen, keinen gemeinsamen Teiler $> 1$ besitzen, so können wir $n(n-\nu)$ ganze Zahlen $u_k^h$ $(0 \leqq k < n,\ \nu \leqq h < n)$ so finden, daß die $n$-reihige Determinante

$$|u_k^h| \qquad (k, h = 0,\ 1, \ldots, n-1)$$

den Wert 1 erhält.*)

Beweis. — Dieser Satz ist evident, wenn $\nu = 0$ ist; denn in diesem Fall kann man $u_k^h = 1$ $(k = h)$, $u_k^h = 0$ $(k \neq h)$ nehmen.

Ist $\nu > 0$, so wird der größte gemeinsame Teiler der $n$ Zahlen $u_0^0$, $u_1^0, \ldots, u_{n-1}^0$ in dem größten gemeinsamen Teiler der Determinanten

$$u \begin{pmatrix} 0, & 1, & \ldots, & \nu-1 \\ k_0, & k_1, & \ldots, & k_{\nu-1} \end{pmatrix}$$

enthalten und folglich gleich 1 sein.

1. Wir beweisen zunächst, daß, wenn der größte gemeinsame Teiler der $n$ ganzen Zahlen $u_0^0$, $u_1^0, \ldots, u_{n-1}^0$ gleich der Einheit ist, stets eine Substitution

*) Gauß, Disquisitiones arithmeticae, art. 279.

$$S: \quad v_i = \sum_k s_i^k u_k \qquad (i, k = 0, 1, \ldots, n-1)$$

von der Determinante 1 gefunden werden kann, welche den $n$ Gleichungen

$$\sum_k s_0^k u_k^0 = 1, \quad \sum_k s_1^k u_k^0 = 0, \ldots, \quad \sum_k s_{n-1}^k u_k^0 = 0$$

genügt, d. h. welche die $n$ Zahlen $u_k = u_k^0$ durch die $n$ Größen $v_0 = 1$, $v_1 = 0, \ldots, v_{n-1} = 0$ ersetzt.

In der Tat, falls von den $n$ Zahlen $u_0^0, u_1^0, \ldots, u_{n-1}^0$ nur eine einzige, etwa $u_i^0$, von Null verschieden ist, so stellt diese Zahl offenbar zugleich den größten Teiler der sämtlichen $n$ Zahlen $u_k^0$ vor, und es wird demnach $u_i^0 = \pm 1$, $\sum_{h=0}^{n-1} (u_h^0)^2 = 1$ sein. Ist dann $i = 0$, so kann man als Substitution $S$ die folgende wählen:

$$v_0 = \pm u_0, \quad v_{i_0} = \pm u_{i_0}; \quad v_h = u_h \ (h \neq 0, i_0),$$

in der $i_0$ irgend einen von 0 verschiedenen Index bedeutet; wenn aber $i > 0$ ist, statt dessen die folgende:

$$v_0 = \pm u_i, \quad v_i = \pm u_0; \quad v_h = u_h \ (h \neq 0, i).$$

Falls aber unter den $n$ Zahlen $u_0^0, u_1^0, \ldots, u_{n-1}^0$ mindestens zwei, etwa $u_i^0, u_k^0$ von Null verschieden sind, so wird $\sum_{h=0}^{n-1} (u_h^0)^2 > 1$, und wenn $(u_i^0)^2 \geqq (u_k^0)^2$ ist, können wir eine Einheit $\pm 1$ so bestimmen, daß $(u_i^0)^2 > (u_i^0 \pm u_k^0)^2$ ausfällt. Durch Ausübung der Substitution

$$(s): \quad U_i^0 = u_i^0 \pm u_k^0, \quad U_k^0 = u_k^0; \quad U_h^0 = u_h^0 (h \neq i, k)$$

von der Determinante 1 erhalten wir dann $n$ Zahlen $U_0^0, U_1^0, \ldots, U_{n-1}^0$ ohne gemeinsamen Teiler, für welche die Ungleichung

$$\sum_{h=0}^{n-1} (u_h^0)^2 > \sum_{h=0}^{n-1} (U_h^0)^2$$

statthat.

Nehmen wir an, daß der Punkt 1. unseres Satzes bereits für alle Systeme $U_0^0, U_1^0, \ldots, U_{n-1}^0$ ohne gemeinsamen Teiler, für welche die Größe $\sum_{h=0}^{n-1} (U_h^0)^2$ kleiner als $\sum_{h=0}^{n-1} (u_h^0)^2$ ist, bewiesen sei, so können wir eine Substitution $(\tau)$ von der Determinante 1 finden, welche die Zahlen $U_0^0, U_1^0, \ldots, U_{n-1}^0$ durch die Zahlen $1, 0, \ldots, 0$ ersetzt, und die zusammengesetzte Substitution $S = (\tau) \cdot (s)$ ergibt alsdann das gleiche Resultat für die Zahlen $u_0^0, u_1^0, \ldots, u_{n-1}^0$.

2. Bilden wir das Produkt des Systemes

$$u = \begin{pmatrix} u_0^0, & u_1^0, & \ldots, & u_{n-1}^0 \\ u_0^1, & u_1^1, & \ldots, & u_{n-1}^1 \\ \ldots & \ldots & \ldots & \ldots \\ u_0^{n-1}, & u_1^{n-1}, & \ldots, & u_{n-1}^{n-1} \end{pmatrix},$$

in welchem die Zahlen $u_k^h (\nu \leqq h < n)$ vorläufig unbestimmte Größen sein mögen, und des Systemes

$$S = \begin{pmatrix} s_0^0, & s_1^0, & \ldots, & s_{n-1}^0 \\ s_0^1, & s_1^1, & \ldots, & s_{n-1}^1 \\ \ldots & \ldots & \ldots & \ldots \\ s_0^{n-1}, & s_1^{n-1}, & \ldots, & s_{n-1}^{n-1} \end{pmatrix},$$

so ergibt sich ein System von der Gestalt

$$v = u \cdot S = \begin{pmatrix} 1, & 0, & \ldots, & 0 \\ v_0^1, & v_1^1, & \ldots, & v_{n-1}^1 \\ \ldots & \ldots & \ldots & \ldots \\ v_0^{n-1}, & v_1^{n-1}, & \ldots, & v_{n-1}^{n-1} \end{pmatrix},$$

in welchem die Größen $v_k^h (1 \leqq h < \nu)$ allein von den $s_i^k$ und den gegebenen Zahlen $u_k^h$ abhängen, während die Größen $v_k^h (\nu \leqq h < n)$ sich durch die $s_i^k$ und die gesuchten Zahlen $u_k^h$ ausdrücken.

Aus dem Umstande, daß die Determinante $|s_i^k|$ gleich 1 ist, erkennen wir, daß der größte gemeinsame Teiler der sämtlichen $(\nu-1)$-reihigen Unterdeterminanten

$$v \begin{pmatrix} 1, \ldots, \nu-1 \\ k_1, \ldots, k_{\nu-1} \end{pmatrix} \qquad (k = 1, \ldots, n-1)$$

des Systems

$$(v) = \begin{pmatrix} v_1^1, & \ldots, & v_{n-1}^1 \\ \ldots & \ldots & \ldots \\ v_1^{\nu-1}, & \ldots, & v_{n-1}^{\nu-1} \end{pmatrix}$$

dem größten gemeinsamen Teiler der sämtlichen Unterdeterminanten

$$u \begin{pmatrix} 0, 1, \ldots, \nu-1 \\ k_0, k_1, \ldots, k_{\nu-1} \end{pmatrix},$$

d. i. der Einheit gleich sein wird. Nehmen wir also unsern Satz für den Fall $n-1$, $\nu-1$ schon als bewiesen an, so können wir solche ganze Zahlen $v_1^h, \ldots, v_{n-1}^h (\nu \leqq h < n)$ bestimmen, daß die Determinante

$$|v_k^h| \qquad (k, h = 1, \ldots, n-1)$$

den Wert 1 erhält. Setzen wir alsdann noch für die Zahlen $v_0^h (\nu \leqq h < n)$ beliebige ganze Zahlen ein, so besitzt das zusammengesetzte System $v \cdot S^{-1}$

offenbar die Determinante 1 und lauter ganzzahlige Koeffizienten, und seine $\nu$ ersten Reihen stimmen mit den $\nu$ Reihen des Systems $(u)$ überein. Demnach liefert uns dieses System $v \cdot S^{-1} = u$ sofort $n(n-\nu)$ ganze Zahlen $u_k^h (\nu \leqq h < n)$, für welche

$$|u_k^h| = 1 \qquad (k, h = 0, 1, \ldots, n-1)$$

wird, und hierdurch ist unser Satz für den Fall $n, \nu$ bewiesen. Da er gewiß für den Fall $n - \nu, 0$ statthat, ergibt sich also seine Gültigkeit für die Fälle

$$n-\nu+1,\ 1;\ n-\nu+2,\ 2; \ldots;\ n,\ \nu.$$

## Kap. XIV. Darstellung einer Form von $\nu$ Variablen durch eine Form von $n$ Variablen. — Äquivalente Darstellungen und Darstellungsgruppen.

I. Wir sagen, eine Form

$$\varphi = \sum_{i,k=1}^{\nu} \alpha_{ik} \xi_i \xi_k$$

von $\nu$ Variablen sei *darstellbar* durch eine Form

$$f = \sum_{i,k=1}^{n} a_{ik} x_i x_k$$

von $n$ Variablen $(n > \nu)$, wenn die Form $f$ vermittels einer Substitution

$$(r): \quad x_i = \sum_{k=1}^{\nu} r_i^k \xi_k \qquad (i = 1, 2, \ldots, n),$$

in welcher die Größen $r_i^k$ ganze Zahlen sind, in $\varphi$ übergeht.

Für die Koeffizienten $\alpha_{lm}$ ergeben sich die Gleichungen

$$\alpha_{lm} = \sum_{i,k=1}^{n} a_{ik} r_i^l r_k^m.$$

Aus denselben erhellt, daß der größte Teiler $d_0$ der sämtlichen Koeffizienten $a_{ik}$ in dem größten Teiler der sämtlichen Koeffizienten $\alpha_{lm}$ enthalten ist und daß die Substitution $(r)$, welche die Form $\varphi$ durch $f$ darstellt, auch zur Darstellung der Form $\frac{\varphi}{d_0} = \left\{\frac{\alpha_{ik}}{d_0}\right\}$ durch die primitive Form $\frac{f}{d_0} = \left\{\frac{a_{ik}}{d_0}\right\}$ dienen kann. Infolge dieses Umstandes dürfen wir uns auf die Untersuchung der Fälle, in denen die Form $f$ primitiv ist, beschränken.

Im Folgenden betrachten wir insbesondere Darstellungen $(r)$, für welche der größte gemeinsame Teiler der $\nu$-reihigen Unterdeterminanten

des Systems

$$\begin{pmatrix} r_1^1, & r_2^1, & \ldots, & r_n^1 \\ r_1^2, & r_2^2, & \ldots, & r_n^2 \\ \cdot & \cdot & \cdot & \cdot \\ r_1^\nu, & r_2^\nu, & \ldots, & r_n^\nu \end{pmatrix} \qquad (\nu < n)$$

gleich 1 ist, und welche wir *eigentliche Darstellungen* nennen.

Wenn die Darstellung $(r)$ eine eigentliche ist, so können wir nach unserm Hilfssatz $n(n-\nu)$ Zahlen $r_i^k (k > \nu)$ finden derart, daß die Determinante

$$|r_i^k| \qquad (i, k = 1, 2, \ldots, n)$$

den Wert 1 erhält. Die Form $f$ geht alsdann durch die Substitution

$$R: \quad x_i = \sum_{k=1}^{n} r_i^k \xi_k \qquad (i = 1, 2, \ldots, n)$$

in eine äquivalente Form $\Phi$ über, in welcher die aus den ersten $\nu$ Horizontal- und Vertikalreihen gebildete Form mit $\varphi$ identisch ist.

Wenn umgekehrt in der Klasse $f$ ein Repräsentant $\Phi$ vorhanden ist, in welchem die aus den ersten $\nu$ Reihen gebildete Form gleich $\varphi$ wird, so ergibt jede Substitution, vermittelst deren $f$ in $\Phi$ übergeht, eine eigentliche Darstellung von $\varphi$ durch $f$.

Wir gewinnen aus dieser Bemerkung, in welcher die Form $f$ nur als Repräsentant ihrer Klasse erscheint, den Satz:

Durch zwei äquivalente Formen $f$ und $g$ können ebendieselben Formen $\varphi$ eigentlich dargestellt werden.

Ferner ist es leicht den folgenden Satz zu beweisen:

O. Wenn die Form $\varphi = \sum_{i,k=1}^{\nu} \alpha_{ik} \xi_i \xi_k$ durch die Form $f$ eigentlich dargestellt werden kann, so ist auch jede der Form $\varphi$ äquivalente Form $\psi = \sum_{i,k=1}^{\nu} \beta_{ik} \eta_i \eta_k$ durch $f$ eigentlich darstellbar.

In der Tat: es möge $\varphi$ durch die Substitution

$$(\tau): \quad \xi_i = \sum_{k=1}^{\nu} \tau_i^k \eta_k \qquad (i = 1, 2, \ldots, \nu)$$

von der Determinante 1 in die Form $\psi$ übergehen. Wenn wir auf $f$ zuerst die Substitution $(r)$ und darauf die Substitution $(\tau)$ anwenden, so erhalten wir zuerst die Form $\varphi$ und dann die Form $\psi$. Zu derselben Form $\psi$ müssen wir nun offenbar gelangen, indem wir auf $f$ unmittelbar die zusammengesetzte Substitution $(r)\cdot(\tau)$, d. i. die Substitution

$$(s): \quad x_i = \sum_{k=1}^{\nu} \left( \sum_{h=1}^{\nu} r_i^h \tau_h^k \right) \eta_k \qquad (i = 1, 2, \ldots, n)$$

anwenden. Hiernach ist die Form $\psi$ durch $f$ vermittels der Substitution

$$(s): \quad x_i = \sum_{k=1}^{\nu} s_i^k \eta_k \qquad (i = 1, 2, \ldots, n)$$

darstellbar, in welcher

$$s_i^k = \sum_{h=1}^{\nu} r_i^h \tau_h^k \qquad \begin{pmatrix} k = 1, 2, \ldots, \nu \\ i = 1, 2, \ldots, n \end{pmatrix} \tag{42}$$

ist.

Nach einem bekannten Satz gelten die Beziehungen

$$|s_i^k| = |r_i^h| \cdot |\tau_h^k|, \qquad \begin{pmatrix} i = i_1, i_2, \ldots, i_\nu \\ k, h = 1, 2, \ldots, \nu \end{pmatrix}$$

d. i.

$$s \begin{pmatrix} 1, 2, \ldots, \nu \\ i_1, i_2, \ldots, i_\nu \end{pmatrix} = r \begin{pmatrix} 1, 2, \ldots, \nu \\ i_1, i_2, \ldots, i_\nu \end{pmatrix}.$$

Diese Beziehungen zeigen uns, daß der größte Teiler der sämtlichen aus $\nu$ Reihen der Substitution $(s)$ gebildeten Unterdeterminanten gleich dem größten Teiler der sämtlichen aus $\nu$ Reihen der Substitution $(r)$ gebildeten Unterdeterminanten ist. Folglich ist die Darstellung $(s)$ eine eigentliche, sobald $(r)$ eine eigentliche Darstellung ist.

Wir wollen die Darstellung $(s) = (r) \cdot (\tau)$ der Form $\psi$ der Darstellung $(r)$ der Form $\varphi$ *äquivalent* nennen und schreiben $(r_\varphi) \sim (s_\psi)$.

Unter den $\nu$-reihigen Determinanten der Substitution $(r)$ gibt es mindestens eine von Null verschiedene; es sei etwa

$$r \begin{pmatrix} 1, 2, \ldots, \nu \\ i_1, i_2, \ldots, i_\nu \end{pmatrix} \neq 0.$$

Wählen wir unter den Gleichungen (42) diejenigen $\nu$ aus, welche den Werten $i = i_1, i_2 \ldots, i_\nu$ und $k = k$ entsprechen und lösen sie nach den Koeffizienten $\tau_h^k$ auf, so erhalten wir

$$\tau_h^k = \sum_i \frac{1}{r \begin{pmatrix} 1, 2, \ldots, \nu \\ i_1, i_2, \ldots, i_\nu \end{pmatrix}} \cdot \frac{\partial r \begin{pmatrix} 1, 2, \ldots, \nu \\ i_1, i_2, \ldots, i_\nu \end{pmatrix}}{\partial r_i^h} \cdot s_i^k. \qquad (i = i_1, i_2, \ldots, i_\nu) \tag{43}$$

Also können die Koeffizienten $\tau_h^k$ vermittels der Größen $r_i^h$ und $s_i^k$ ausgedrückt werden. Daraus schließen wir, daß zwei verschiedene Transformationen $(\tau)$ von $\varphi$ in $\psi$ niemals dieselbe einer gegebenen Darstellung $(r_\varphi)$ äquivalente Darstellung $(s_\psi)$ liefern können.

II. Wenn zwei Formen $\varphi$ und $\psi$ durch $f$ vermittels zweier Substitutionen $(r)$ und $(s)$ dargestellt sind, welche die Bedingungen

$$r \begin{pmatrix} 1, 2, \ldots, \nu \\ i_1, i_2, \ldots, i_\nu \end{pmatrix} = s \begin{pmatrix} 1, 2, \ldots, \nu \\ i_1, i_2, \ldots, i_\nu \end{pmatrix} \qquad (i = 1, 2, \ldots, n) \tag{44}$$

erfüllen, so ist stets $\varphi \sim \psi$ und $(r_\varphi) \sim (s_\psi)$.

In der Tat: sind die Zahlen $r_i^k (k > \nu)$ so gewählt, daß die Substitution

$$R: \quad x_i = \sum_{k=1}^{n} r_i^k \xi_k \qquad (i = 1, 2, \ldots, n)$$

die Determinante 1 besitzt, und setzen wir $s_i^k = r_i^k (k > \nu)$, so zeigen die Gleichungen (44) unmittelbar, daß die Substitution

$$S: \quad x_i = \sum_{k=1}^{n} s_i^k \eta_k \qquad (i = 1, 2, \ldots, n)$$

gleichfalls von der Determinante 1 ist. Die beiden Formen $\overline{R} \cdot f \cdot R = \Phi$ und $\overline{S} \cdot f \cdot S = \Psi$ können wir schreiben

$$\Phi = \sum_{i,k=1}^{n} \alpha_{ik} \xi_i \xi_k \quad \text{und} \quad \Psi = \sum_{i,k=1}^{n} \beta_{ik} \eta_i \eta_k;$$

dann wird

$$\varphi = \sum_{i,k=1}^{\nu} \alpha_{ik} \xi_i \xi_k \quad \text{und} \quad \psi = \sum_{i,k=1}^{\nu} \beta_{ik} \eta_i \eta_k.$$

Offenbar gilt

$$\Psi = \overline{R^{-1} S} \cdot \Phi \cdot R^{-1} S.$$

Man erkennt also, daß sich vermittels der Substitution

$$R^{-1}S: \quad \xi_i = \sum_{k=1}^{n} \tau_i^k \eta_k, \qquad (i = 1, 2, \ldots, n)$$

in der

$$\tau_i^k = \sum_{h=1}^{n} \frac{\partial |R|}{\partial r_h^i} \cdot s_h^k \qquad (i, k = 1, 2, \ldots, n)$$

ist, die Form $\Phi$ in $\Psi$ verwandelt.

Wie man leicht einsieht, lassen sich die Zahlen $\frac{\partial |R|}{\partial r_h^i} (i > \nu)$ mit Hilfe der Größen $r \begin{pmatrix} 1, 2, \ldots, \nu \\ i_1, i_2, \ldots, i_\nu \end{pmatrix}$ und mittels Zahlen $r_{h_0}^k (k > \nu)$ ausdrücken. Folglich gilt

$$\frac{\partial |R|}{\partial r_h^i} = \frac{\partial |S|}{\partial s_h^i} \qquad (i > \nu),$$

also

$$\tau_i^k = \begin{matrix} 1 \, (i = k) \\ 0 \, (i \neq k) \end{matrix} \qquad (i > \nu),$$

und die Substitution $R^{-1}S$ nimmt die Form an

$$R^{-1}S: \quad \xi_i = \sum_{k=1}^{n} \tau_i^k \eta_k \quad (i \leqq \nu), \qquad \xi_i = \eta_i \quad (i > \nu).$$

Wir finden sonach

$$\beta_{lm} = \sum_{i,k=1}^{\nu} \alpha_{ik} \tau_i^l \tau_k^m, \qquad (l, m = 1, 2, \ldots, \nu)$$

und die Form $\varphi$ geht vermittels der Substitution

$$(\tau): \quad \xi_i = \sum_{k=1}^{\nu} \tau_i^k \eta_k \qquad (i = 1, 2, \ldots \nu)$$

in $\psi$ über. Die Determinante dieser Substitution ist gleich der Determinante der Substitution $R^{-1}S$, d. i. gleich der Einheit. Mithin ist die Form $\varphi$ der Form $\psi$ äquivalent.

Setzen wir die Systeme $R$ und $R^{-1}S$ zusammen, so müssen wir zu dem System $S$ gelangen. Daraus ergeben sich die Gleichungen

$$s_i^k = \sum_{h=1}^{\nu} r_i^h \tau_h^k, \quad (k = 1, 2, \ldots, \nu; \; i = 1, 2, \ldots, n)$$

aus denen ersichtlich ist, daß die Darstellung $(s_\psi)$ der Darstellung $(r_\varphi)$ äquivalent ist.

III. Mit Hilfe des Satzes II. können wir leicht den folgenden Satz beweisen:

P. Ist $\varphi \sim \psi'$, $\varphi \sim \psi''$ und $(r_\varphi) \sim (s_{\psi'})$, $(r_\varphi) \sim (s_{\psi''})$, so ist $(s_{\psi'}) \sim (s_{\psi''})$.

Wir fassen die sämtlichen Darstellungen einer Form $\varphi$, welche einer gegebenen Darstellung dieser Form äquivalent sind, in eine *Gruppe von Darstellungen* der Form $\varphi$ zusammen. Aus dem Satze P. folgt alsdann, daß zwei Darstellungen $(r_\varphi)$ derselben Gruppe stets äquivalent, zwei Darstellungen $(r_\varphi)$ aus verschiedenen Gruppen nicht äquivalent sind.

Aus den Gleichungen (42) und (43) erkennen wir, daß die Anzahl aller verschiedenen Darstellungen $(r)$ einer Form $\varphi$, welche in einer Gruppe von Darstellungen dieser Form auftreten [d. i. die Dichtigkeit einer derartigen Gruppe $(r_\varphi)$] gleich der Anzahl der sämtlichen verschiedenen Transformationen (von der Determinante 1) der Form $\varphi$ in sich selbst ist. Daraus schließen wir leicht, daß die Darstellungsgruppen zweier äquivalenter Formen gleiche Dichtigkeit besitzen.

Wir nennen zwei *Gruppen* von Darstellungen $(r_\varphi)$ und $(s_\psi)$ *äquivalent*, wenn irgendeine Darstellung der einen Gruppe irgendeiner Darstellung der andern äquivalent ist. Der Satz P. zeigt dann, daß zwei beliebige Darstellungen nur dann äquivalent sind, wenn sie äquivalenten Gruppen von Darstellungen angehören. Hiernach bilden die sämtlichen Darstellungen $(s_\psi)$, welche einer gegebenen Darstellung $(r_\varphi)$ äquivalent sind, eine Gruppe von Darstellungen der Form $\psi$.

## Kap. XV. **Adjungierte Darstellungen und adjungierte Darstellungsgruppen.**

I. Es möge eine primitive Form $f$ von $n$ Variablen mit Hilfe einer Substitution

$$R: \quad x_i = \sum_{k=1}^{n} r_i^k \xi_k \qquad (i = 1, 2, \ldots, n)$$

von der Determinante 1 in eine äquivalente Form $\Phi = \{\alpha_{ik}\}$ $(i, k = 1, 2, \ldots, n)$ übergehen, und es möge $\varphi$ die Form $\sum_{i,k=1}^{\nu} \alpha_{ik} \xi_i \xi_k$ von $\nu$ Variablen bezeichnen. Es sei $f'$ die adjungierte Form von $f$,

$$R': \quad x_i' = \sum_{k=1}^{n} r_i'^k \xi_k' \qquad (i = 1, 2, \ldots, n)$$

die adjungierte Substitution von $R$ und $\Phi' = \{\alpha_{ik}'\}$ $(i, k = 1, 2, \ldots, n)$ die adjungierte Form von $\Phi$. In Kap. XII haben wir gesehen, daß die Form $f'$ mit Hilfe der Substitution $R'$ in $\Phi'$ übergeht. Wir setzen die Form $\sum_{i,k=1}^{n-\nu} \alpha_{ik}' \xi_i' \xi_k'$ von $n - \nu = \nu'$ Variablen gleich $\varphi'$. Ist die Determinante der Form $\varphi$ gleich $\sigma_\nu d_{\nu-1} \cdot (\varphi)$ und die Determinante von $\varphi'$ gleich $\sigma_{\nu'}' d_{\nu'-1}' \cdot (\varphi')$, so gilt die Beziehung

$$(\varphi) = (\varphi') \cdot (-1)^{I(f)}.$$

Wir wollen sagen, die Darstellung

$$(r'): \quad x_i' = \sum_{k=1}^{\nu'} r_i'^k \xi_k' \qquad (i = 1, 2, \ldots, n)$$

der Form $\varphi'$ durch die Form $f'$ sei der Darstellung

$$(r): \quad x_i = \sum_{k=1}^{\nu} r_i^k \xi_k \qquad (i = 1, 2, \ldots, n)$$

der Form $\varphi$ durch die Form $f$ *adjungiert*, und wollen uns des Zeichens $(r_\varphi) \asymp (r_{\varphi'}')$ bedienen. — Aus der Reziprozität zwischen den Formen $f$ und $f'$ erhellt, daß, wenn die Darstellung $(r_{\varphi'}')$ der Darstellung $(r_\varphi)$ adjungiert ist, umgekehrt die Darstellung $(r_\varphi)$ der Darstellung $(r_{\varphi'}')$ adjungiert ist.

Da die Systeme $R$ und $R'$ adjungiert sind, bestehen für die Darstellungen $(r)$ und $(r')$ die sämtlichen Gleichungen

$$(45) \qquad r \begin{pmatrix} 1, & 2, & \ldots, & \nu \\ i_1, & i_2, & \ldots, & i_\nu \end{pmatrix} = r' \begin{pmatrix} 1, & 2, & \ldots, & \nu' \\ i_1', & i_2', & \ldots, & i_{\nu'}' \end{pmatrix},$$

in denen die Indizes $i$ und $i'$ so gewählt sein sollen, daß die $n$ Zahlen $i_h$; $n+1-i_{h'}'$ abgesehen von der Reihenfolge den $n$ Zahlen $1, 2, \ldots, n$ gleich sind und die Permutation

$$(i_1, i_2, \ldots, i_\nu, n+1-i_{\nu'}', \ldots, n+1-i_2', n+1-i_1')$$

aus $(1, 2, \ldots, n)$ vermittels einer geraden Anzahl von Transpositionen hervorgeht.

II. Umgekehrt sind die beiden Darstellungen $(r_\varphi)$ und $(r_{\varphi'}')$ stets adjungiert, sobald sie die sämtlichen Bedingungen (45) erfüllen.

In der Tat: seien die Zahlen $\varrho_i'^k$ $(k > \nu')$ so gewählt, daß die Substitution

$$(\varrho'): \quad x_i' = \sum_{k=1}^{\nu'} r_i'^k \xi_k' + \sum_{k=\nu'+1}^{n} \varrho_i'^k \xi_k' \qquad (i = 1, 2, \ldots, n)$$

die Determinante 1 besitzt, und sei

$$(\varrho): \quad x_i = \sum_{k=1}^{\nu} \varrho_i^k \xi_k + \sum_{k=\nu+1}^{n} R_i^k \xi_k \qquad (i = 1, 2, \ldots, n)$$

die adjungierte Substitution von $(\varrho')$. Es wird dann

$$\varrho \begin{pmatrix} 1, & 2, & \ldots, & \nu \\ i_1, & i_2, & \ldots, & i_\nu \end{pmatrix} = r' \begin{pmatrix} 1, & 2, & \ldots, & \nu' \\ i_1', & i_2', & \ldots, & i_{\nu'}' \end{pmatrix},$$

woraus sich wegen der Gleichungen (45)

$$r \begin{pmatrix} 1, & 2, & \ldots, & \nu \\ i_1, & i_2, & \ldots, & i_\nu \end{pmatrix} = \varrho \begin{pmatrix} 1, & 2, & \ldots, & \nu \\ i_1, & i_2, & \ldots, & i_\nu \end{pmatrix}$$

ergibt. Wir erkennen nunmehr, daß die Substitution

$$R: \quad x_i = \sum_{k=1}^{\nu} r_i^k \xi_k + \sum_{k=\nu+1}^{n} R_i^k \xi_k \qquad (i = 1, 2, \ldots, n)$$

die Determinante 1 besitzt und daß die adjungierte Substitution von $R$ die Form erhält:

$$R': \quad x_i' = \sum_{k=1}^{\nu'} r_i'^k \xi_k' + \sum_{k=\nu'+1}^{n} R_i'^k \xi_k' \qquad (i = 1, 2, \ldots, n).$$

Also ist die Darstellung $(r')$ in der Tat der Darstellung $(r)$ adjungiert.

III. Wir können jetzt den folgenden Satz beweisen:

Ist $(r_\varphi) \sim (s_\psi)$ $(\varphi \sim \psi)$ und $(r_\varphi) \prec (r_{\varphi'}')$, $(s_\psi) \prec (s_{\psi'}')$, so ist stets $(r_{\varphi'}') \sim (s_{\psi'}')$ $(\varphi' \sim \psi')$ und $(r_\varphi) \prec (s_{\psi'}')$, $(s_\psi) \prec (r_{\varphi'}')$.

In der Tat ergibt die Voraussetzung

$$r \begin{pmatrix} 1, & 2, & \ldots, & \nu \\ i_1, & i_2, & \ldots, & i_\nu \end{pmatrix} = s \begin{pmatrix} 1, & 2, & \ldots, & \nu \\ i_1, & i_2, & \ldots, & i_\nu \end{pmatrix} = r' \begin{pmatrix} 1, & 2, & \ldots, & \nu' \\ i_1', & i_2', & \ldots, & i_{\nu'}' \end{pmatrix} = s' \begin{pmatrix} 1, & 2, & \ldots, & \nu' \\ i_1', & i_2', & \ldots, & i_{\nu'}' \end{pmatrix},$$

woraus unmittelbar die Richtigkeit der aufgestellten Behauptung folgt.

Dieser Satz zeigt, daß zwei äquivalenten Darstellungen stets dieselben adjungierten Darstellungen zukommen.

Wir nennen zwei *Gruppen* von Darstellungen $(r)$, $(r')$ *adjungiert*, sobald irgendeine Darstellung der einen Gruppe irgendeiner Darstellung der andern adjungiert ist. Aus dem vorstehenden Satz schließen wir, daß, wenn zwei Gruppen von Darstellungen adjungiert sind, jede Darstellung der einen Gruppe jeder Darstellung der andern adjungiert ist.

Den sämtlichen äquivalenten Darstellungsgruppen, welche zu Formen einer bestimmten Klasse $\varphi$ von $\nu$ Variablen gehören, sind äquivalente Darstellungsgruppen einer bestimmten Klasse $\varphi'$ von $\nu'$ Variablen adjungiert. Die beiden Klassen $\varphi$ und $\varphi'$ besitzen hiernach eine gewisse Reziprozität in bezug auf die Formen $f$ und $f'$, und man kann sehr bemerkenswerte Relationen zwischen den Indizes, den Ordnungen und den Genera dieser beiden Klassen aufstellen. Wir leiten an dieser Stelle nur die Relation zwischen den Indizes her.

Q. Bezeichnen wir durch $J$ den Index von $\varphi$, durch $J'$ den Index von $\varphi'$ und durch $I$ den Index von $f$ und $f'$, so hat die Gleichung statt

$$J + J' = I. \qquad (J \leqq I,\ J' \leqq I)$$

Denn setzen wir die aus den ersten $h(= 1, 2, \ldots, n)$ Horizontal- und Vertikalreihen von $\Phi$ resp. $\Phi'$ gebildeten Unterdeterminanten gleich $\sigma_h d_{h-1} \Delta_h$ resp. $\sigma'_h d'_{h-1} \Delta'_h$, so ist die Zahl $J$ resp. $J'$ gleich der Anzahl der sämtlichen negativen Größen aus der Reihe $\frac{\Delta_h}{\Delta_{h-1}} (h = 1, 2, \ldots, \nu;\ \Delta_0 = 1)$ resp. aus der Reihe $\frac{\Delta'_h}{\Delta'_{h-1}}$ $(h = 1, 2, \ldots, \nu';\ \Delta'_0 = 1)$, während die Zahl $I$ gleich der Anzahl der negativen Größen aus der Reihe $\frac{\Delta_h}{\Delta_{h-1}}$ $(h = 1, 2, \ldots, n)$ oder aus der Reihe $\frac{\Delta'_h}{\Delta'_{h-1}}$ $(h = 1, 2, \ldots, n)$ wird. Nun haben wir nach Kap. XII die Relationen $\Delta_h = (-1)^I \cdot \Delta'_{n-h}$ $(h = 0, 1, 2, \ldots, n)$; dieselben führen mit Leichtigkeit zu dem angegebenen Resultate.

Von besonderem Interesse ist der Fall, in welchem die Form $\varphi$ eine Ordnung

$$\begin{pmatrix} \sigma_1, & \sigma_2, & \ldots, & \sigma_{\nu-2}, & \sigma_{\nu-1} \\ o_1, & o_2, & \ldots, & o_{\nu-2}, & \sigma_\nu o_{\nu-1} \cdot m \end{pmatrix}, \quad J$$

und die Form $\varphi'$ eine Ordnung

$$\begin{pmatrix} \sigma_1', & \sigma_2', & \ldots, & \sigma'_{\nu'-2}, & \sigma'_{\nu'-1} \\ o_1', & o_2', & \ldots, & o'_{\nu'-2}, & \sigma'_{\nu'} o'_{\nu'-1} \cdot m \end{pmatrix}, \quad J'$$

besitzt.

## Kap. XVI. **Darstellung von ganzen Zahlen durch Formen mit $n$ Variablen.**

Wir wollen weiterhin insbesondere den Fall betrachten, in welchem eine der Zahlen $\nu$, $\nu'$ gleich 1 ist. Es sei $\nu = 1$, $\nu' = n-1$.

Wenn die Form $f$ mit Hilfe der Substitution

$$(t): \quad x_i = t_i \xi \qquad (i = 1, 2, \ldots, n)$$

in eine (einvariablige) Form $b\xi^2$ übergeht, so wird die Zahl $b$ durch $f$ vermittels der Zahlen

$$(t): \quad x_i = t_i$$

dargestellt, und umgekehrt ist die Form $b\xi^2$ stets durch $f$ darstellbar, sobald die Zahl $b$ durch $f$ dargestellt werden kann.

Wir nennen die Darstellung $x_i = t_i$ der Zahl $b$ durch die Form $f$ eigentlich, wenn die Darstellung von $b\xi^2$ durch $f$ eigentlich ist, d. h. wenn der größte gemeinsame Teiler $\tau$ der $n$ Zahlen $t_i$ gleich 1 ist.

So oft der Teiler $\tau$ größer als 1 ist, muß $b$ den Faktor $\tau^2 > 1$ enthalten, und die Darstellung $x_i = t_i$ der Zahl $b$ durch $f$ liefert die eigentliche Darstellung $x_i = \frac{t_i}{\tau}$ der Zahl $\frac{b}{\tau^2}$ durch $f$. Wir gelangen infolgedessen zu allen überhaupt möglichen Darstellungen einer Zahl $b$ durch eine Form $f$, indem wir die sämtlichen quadratischen Divisoren $\tau^2$ von $b$ aufsuchen und alle eigentlichen Darstellungen der Zahlen $\frac{b}{\tau^2}$ durch die Form $f$ bestimmen.

Wir setzen die Form $f$ als primitiv voraus. Zwei eigentliche Darstellungen $(t)$ und $(t^0)$ einer Form $b\xi^2$ oder einer Zahl $b$ durch die Form $f$ werden nach unseren Definitionen nur dann äquivalent sein, wenn die sämtlichen Gleichungen $t_i = t_i^0$ $(i = 1, 2, \ldots, n)$ statthaben, d. h. wenn sie identisch sind. Infolgedessen sprechen sich die in Kap. XV aufgestellten Sätze für den Fall $\nu = 1$ folgendermaßen aus*):

I. Zu jeder eigentlichen Darstellung $(t)$ einer Zahl $b$ durch die Form $f$ sind eigentliche Darstellungen $(r')$ gewisser Formen $\varphi'$ von $n-1$ Variablen und der Determinante $(-1)^I d'_{n-2} \cdot b$ durch die Form $f'$ adjungiert.

I'. Zu jeder eigentlichen Darstellung $(r')$ einer Form $\varphi'$ von $n-1$ Variablen und der Determinante $(-1)^I d'_{n-2} \cdot b$ durch die Form $f'$ ist eine einzige eigentliche Darstellung $(t)$ der Zahl $b$ durch die Form $f$ adjungiert.

II. Zu zwei äquivalenten Darstellungen $(r')$ und $(s')$ zweier äquivalenter Formen $\varphi'$ und $\psi'$ von $n-1$ Variablen und der Determinante $(-1)^I d'_{n-2} \cdot b$ durch die Form $f'$ ist eine und dieselbe Darstellung $(t)$ der Zahl $b$ durch die Form $f$ adjungiert.

*) Siehe Gauß, Disquisitiones arithmeticae, art. 280.

II′. Wenn zu einer und derselben Darstellung $(t)$ der Zahl $b$ durch die Form $f$ zwei Darstellungen $(r')$ und $(s')$ zweier Formen $\varphi'$ und $\psi'$ mit $n-1$ Variablen und von der Determinante $(-1)^I d'_{n-2} \cdot b$ durch die Form $f'$ adjungiert sind, so sind die Formen $\varphi'$ und $\psi'$ und die Darstellungen $(r')$ und $(s')$ äquivalent.

Um die sämtlichen eigentlichen Darstellungen einer Zahl $b$ durch eine primitive Form $f$ zu bestimmen, können wir jetzt in folgender Weise verfahren: wir wählen aus einer jeden Formenklasse mit $n-1$ Variablen und von der Determinante $(-1)^I d'_{n-2} \cdot b$ einen Repräsentanten $\varphi'$ aus, suchen die sämtlichen nicht-äquivalenten Gruppen von eigentlichen Darstellungen dieser Formen $\varphi'$ durch die Form $f'$ auf und bestimmen zu jeder dieser nicht-äquivalenten Gruppen die einzige adjungierte eigentliche Darstellung der Zahl $b$ durch die Form $f$. Auf diese Weise wird man zu den sämtlichen überhaupt möglichen eigentlichen Darstellungen der Zahl $b$ durch die Form $f$ gelangen und zwar zu einer jeden dieser Darstellungen nur ein einziges Mal.

## Kap. XVII. **Darstellungen von Formen mit $n-1$ Variablen durch Formen mit $n$ Variablen.**

Wir wenden uns jetzt zu einer näheren Untersuchung der eigentlichen Darstellungen einer Form mit $n-1$ Variablen durch eine primitive Form mit $n$ Variablen.

I. Es möge eine Form $\varphi' = \sum_{i,k=1}^{n-1} b'_{ik}\, \xi'_i\, \xi'_k$ von der Determinante $(-1)^I d'_{n-2} \cdot b$ durch eine primitive Form $f' = \sum_{i,k=1}^{n} a'_{ik}\, x'_i\, x'_k$ vermittels einer Substitution

$$(\vartheta'): \quad x'_i = \sum_{k=1}^{n-1} \vartheta'^{k}_{i}\, \xi'_k \qquad (i = 1, 2, \ldots, n)$$

[[eigentlich]] dargestellt werden.

Bestimmen wir $n$ Zahlen $t'_i$, so daß die Substitution

$$(t'): \quad x'_i = \sum_{k=1}^{n-1} \vartheta'^{k}_{i}\, \xi'_k + t'_i\, \xi' \qquad (i = 1, 2, \ldots, n)$$

die Determinante 1 besitzt, so wird die Form $\overline{(t')} \cdot f' \cdot (t') = B'$ der Form $f'$ äquivalent sein und sich schreiben lassen

$$B' = \sum_{i,k=1}^{n-1} b'_{ik}\, \xi'_i\, \xi'_k + 2 \sum_{i=1}^{n-1} b'_i\, \xi'_i\, \xi' + b'\, \xi'^2.$$

Wir bezeichnen durch $f = \sum_{i,k=1}^{n} a_{ik} x_i x_k$ die zu $f'$ adjungierte Form, durch

$$(t): \quad x_i = t_i \xi + \sum_{k=1}^{n-1} \vartheta_i^k \xi_k \qquad (i = 1, 2, \ldots, n)$$

die adjungierte Substitution von $(t')$ und durch

$$B = b\xi^2 + 2\sum_{i=1}^{n-1} b_i \xi \xi_i + \sum_{i,k=1}^{n-1} b_{ik} \xi_i \xi_k$$

die zu $B'$ adjungierte Form. Die $n$ Zahlen $t_i$ drücken sich dabei durch die gegebenen Koeffizienten $\vartheta_i'^k$ aus. Es gelten die Beziehungen

$$(46) \qquad \sum_{i=1}^{n} t_i' t_{n-i+1} = 1, \quad \sum_{h=1}^{n-1} \vartheta'^{\,n-h}_{n-i+1} \vartheta_k^h + t'_{n-i+1} t_k = \begin{matrix} 1 & (i = k) \\ 0 & (i \neq k) \end{matrix},$$

und wir bekommen $B = \overline{(t)} \cdot f \cdot (t)$, d. i.

$$b_{lm} = \sum_{i,k=1}^{n} a_{ik} \vartheta_i^l \vartheta_k^m$$

und

$$(47) \qquad b = \sum_{i,k=1}^{n} a_{ik} t_i t_k, \quad b_h = \sum_{i,k=1}^{n} a_{ik} t_i \vartheta_k^h.$$

Mit Benutzung der Summen

$$T_i = \sum_{h=1}^{n} a_{ih} t_h = a_{i1} t_1 + a_{i2} t_2 + \cdots + a_{in} t_n = \frac{1}{2} \frac{\partial b}{\partial t_i}$$

können wir die Formeln (47) auch schreiben

$$(48) \qquad b = \sum_{i=1}^{n} T_i t_i, \quad b_h = \sum_{i=1}^{n} T_i \vartheta_i^h.$$

Wir setzen $|b'_{ik}| = |\varphi'|$, $|b_{ik}| = |\varphi|$ und

$$\frac{\partial |\varphi'|}{\partial b'_{ik}} = (-1)^I \cdot d'_{n-3} \cdot c_{n-i,\,n-k}, \quad \frac{\partial |\varphi|}{\partial b_{ik}} = (-1)^I \cdot d_{n-3} \cdot c'_{n-i,\,n-k}.$$

Da die Formen $f$ und $f'$ adjungiert sind, gelten nach einem bekannten Determinantensatze die Gleichungen

$$\{(-1)^I \cdot d'_{n-2} b\} \{(-1)^I \cdot d'_{n-2} b_{ik}\} - \{(-1)^I \cdot d'_{n-2} b_i\} \{(-1)^I \cdot d'_{n-2} b_k\} = (-1)^I \cdot d'_{n-1} \cdot \{(-1)^I \cdot d'_{n-3} \cdot c_{ik}\}$$

oder

$$(49) \qquad -o_1 c_{ik} = b_i b_k - b b_{ik},$$

aus denen wir die Kongruenzen gewinnen

$$(50) \qquad -o_1 c_{ik} \equiv b_i b_k \pmod{b}$$

oder

$$-o_1 \cdot \Big(\sum_{i,k=1}^{n-1} c_{ik}\xi_i\xi_k\Big) \equiv \Big(\sum_{i=1}^{n-1} b_i\xi_i\Big)^2 \pmod{b}.$$

Jede Darstellung $(\vartheta')$ der Form $\varphi'$ durch die Form $f'$ liefert auf solche Weise bestimmte Lösungen $(b_1, b_2, \ldots, b_{n-1})$ der $\frac{n(n-1)}{2}$ Kongruenzen (50). Wir sagen, die Darstellung $(\vartheta')$ *gehöre* zu diesen Lösungen $(b_h)$ $(h = 1, 2, \ldots, n-1)$*).

II. Wenn wir den $n$ Zahlen $t_1', t_2', \ldots, t_n'$ alle möglichen Werte erteilen, welche die Bedingung $\sum_{i=1}^{n} t_i' t_{n-i+1} = 1$ erfüllen, so erhalten wir alle Lösungen $(b_h)$ der Kongruenzen (50), zu welchen die gegebene Darstellung $(\vartheta')$ der Form $\varphi'$ gehört. Es besteht nun der Satz:

Alle Lösungen $(b_1, b_2, \ldots, b_{n-1})$ der Kongruenzen (50), zu welchen die nämliche Darstellung $(\vartheta')$ der Form $\varphi'$ gehört, sind nach dem Modul $b$ kongruent.

In der Tat, die Summen

$$\sum_{h=1}^{n-1} \vartheta'^{\,n-h}_{n-i+1} \cdot b_h = \vartheta'^{\,n-1}_{n-i+1} \cdot b_1 + \vartheta'^{\,n-2}_{n-i+1} \cdot b_2 + \cdots + \vartheta'^{\,1}_{n-i+1} \cdot b_{n-1}$$

nehmen mit Hilfe der Formeln (48) und (46) die Werte an

$$\sum_{h=1}^{n-1}\Big(\vartheta'^{\,n-h}_{n-i+1} \cdot \sum_{k=1}^{n} \vartheta^h_k T_k\Big) = \sum_{k=1}^{n}\Big(T_k \sum_{h=1}^{n-1} \vartheta^h_k \vartheta'^{\,n-h}_{n-i+1}\Big) = -t'_{n-i+1}\sum_{k=1}^{n} T_k t_k + T_i.$$

Es kommt also

$$(51) \qquad \sum_{h=1}^{n-1} \vartheta'^{\,n-h}_{n-i+1} \cdot b_h - \sum_{k=1}^{n} a_{ik} t_k = -b\,t'_{n-i+1} \equiv 0 \pmod{b}.$$
$$(i = 1, 2, \ldots, n)$$

Fassen wir irgendwelche $n-1$ von diesen $n$ Gleichungen zusammen, etwa alle diejenigen, welche einem Index $i \neq g$ entsprechen, so können wir dieselben nach den $n-1$ Größen $b_h$ auflösen, und es ergibt sich

$$t_g b_h - \sum_{(i)}\Big(\frac{\partial t_g}{\partial \vartheta'^{\,n-h}_{n-i+1}} \cdot \sum_{k=1}^{n} a_{ik} t_k\Big) = b \cdot \vartheta_g^{\,h} \equiv 0 \pmod{b} \qquad (i \neq g).$$

*) Siehe Gauß, Disquisitiones arithmeticae, art. 282.

Es ist klar, daß die Größen $t_k$, $\frac{\partial t_g}{\partial \vartheta_{n-i+1}'^{n-h}}$ vermittels der Koeffizienten $\vartheta_i'^k$ der Darstellung $(\vartheta')$ ausgedrückt werden können; es sind daher auch die Reste der Zahlen

$$t_1 b_h,\ t_2 b_h,\ \ldots,\ t_n b_h$$

nach dem Modul $b$ durch diese Zahlen $\vartheta_i'^k$ vollständig bestimmt. Da die Darstellung $(\vartheta')$ eine eigentliche ist, können die $n$ Zahlen $t_1, t_2, \ldots, t_n$ keinen gemeinsamen Teiler größer als 1 besitzen, und es müssen sich daher unter diesen $n$ Zahlen solche befinden, die zu einem beliebigen Primfaktor $q$ von $b$ relativ prim sind. Infolge dieses Umstandes sind auch die Reste der $n-1$ Zahlen $b_h$ für jede in $b$ aufgehende Primzahlpotenz $q^t$ und mithin für den Modul $b$ selbst eindeutig durch die Koeffizienten $\vartheta_i'^k$ bestimmt, und hieraus geht unmittelbar das Behauptete hervor.

Setzen wir jetzt voraus, man könne $n$ Zahlen $t_i'$ $\left(\sum_{i=1}^{n} t_i' t_{n-i+1} = 1\right)$ so finden, daß die Darstellung $(\vartheta')$ zu der Wurzel $(b_h)$ der Kongruenzen (50) gehört, und es möge $(\tilde{b}_h)$ eine andere, nach dem Modul $b$ der Wurzel $(b_h)$ kongruente Wurzel dieser Kongruenzen sein. Alsdann kann man $n$ Zahlen $\tilde{t}_i'$ $\left(\sum_{i=1}^{n} \tilde{t}_i' t_{n-i+1} = 1\right)$ derart finden, daß die Darstellung $(\vartheta')$ zu dieser Wurzel $(\tilde{b}_h)$ gehört.

In der Tat, es möge $\tilde{b}_h = b_h + b e_h$ sein. Für die Zahlen $\tilde{t}_i'$ müssen die Beziehungen

$$\sum_{h=1}^{n-1} \vartheta_{n-i+1}'^{n-h} \cdot \tilde{b}_h - \sum_{k=1}^{n} a_{ik} t_k = -b \cdot \tilde{t}_{n-i+1}' \tag{51}$$

statthaben. Die Differenz der Gleichungen (51) und ($\tilde{51}$) ergibt sogleich

$$\tilde{t}_i' = t_i' - \sum_{h=1}^{n-1} \vartheta_i'^{n-h} e_h. \tag{52}$$

Daraus geht hervor, daß die Bestimmung der Zahlen $\tilde{t}_i'$ jedenfalls nur auf eine einzige Weise möglich sein kann. Führen wir nun für die Zahlen $\tilde{t}_i'$ die Ausdrücke (52) ein, so ist die Gleichung ($\tilde{51}$) wirklich erfüllt. Multiplizieren wir dann diese Gleichung mit $t_i$ und bilden die Summe über alle Werte $i = 1, 2, \ldots, n$, so bekommen wir

$$b \cdot \sum_{i=1}^{n} \tilde{t}_{n-i+1}' t_i = \sum_{i,k=1}^{n} a_{ik} t_i t_k,$$

d. i.

$$\sum_{i=1}^{n} \tilde{t}'_{n-i+1} t_i = 1.$$

Die Darstellung $(\vartheta')$ gehört also in der Tat zu der Wurzel $(\tilde{b}_h)$ der Kongruenzen (50).

Ist insbesondere $e_h = 0$, $\tilde{b}_h = b_h (h = 1, 2, \ldots, n-1)$, so wird $\tilde{t}'_i = t'_i (i = 1, 2, \ldots, n)$. Man sieht demnach, daß es nicht zwei verschiedene Substitutionen $(t')$ geben kann, welche dieselben Koeffizienten $\vartheta_i'^k$ besitzen und die Form $f'$ durch dieselbe Form $B'$ ersetzen.

III. Zu den eben bewiesenen Sätzen gelangen wir auch auf folgendem Wege*):

Es seien $\tilde{t}_1', \tilde{t}_2', \ldots, \tilde{t}_n'$ irgendwelche Zahlen, welche ebenso wie die Zahlen $t_1', t_2', \ldots, t_n'$ der Gleichung

$$\sum_{i=1}^{n} \tilde{t}'_i \cdot t_{n-i+1} = 1$$

genügen, und es möge die Form $f'$ durch die Substitution

$$(\tilde{t}'): \quad x_i' = \sum_{k=1}^{n-1} \vartheta_i'^k \tilde{\xi}'_k + \tilde{t}_i' \tilde{\xi}' \qquad (i = 1, 2, \ldots, n)$$

in eine Form

$$\tilde{B}' = \sum_{i,k=1}^{n-1} b'_{ik} \tilde{\xi}_i' \tilde{\xi}_k' + 2 \sum_{i=1}^{n-1} \tilde{b}_i' \tilde{\xi}_i' \tilde{\xi} + \tilde{b}' \tilde{\xi}'^2$$

übergehen. Der Substitution $(\tilde{t}')$ sei die Substitution

$$(\tilde{t}): \quad x_i = t_i \tilde{\xi} + \sum_{k=1}^{n-1} \tilde{\vartheta}_i^k \tilde{\xi}_k \qquad (i = 1, 2, \ldots, n)$$

und der Form $\tilde{B}'$ die Form

$$\tilde{B} = b \tilde{\xi}^2 + 2 \sum_{i=1}^{n-1} \tilde{b}_i \tilde{\xi} \tilde{\xi}_i + \sum_{i,k=1}^{n-1} \tilde{b}_{ik} \tilde{\xi}_i \tilde{\xi}_k$$

adjungiert. Wie man aus Kap. XIV (II) ersieht, geht alsdann die Form $B$ mit Hilfe der Substitution

$$(t)^{-1} \cdot (\tilde{t}): \quad \xi = \tilde{\xi} + \sum_{h=1}^{n-1} e_h \cdot \tilde{\xi}_h, \qquad \xi_h = \tilde{\xi}_h \quad (h = 1, 2, \ldots, n-1),$$

in welcher

$$e_h = \sum_{i=1}^{n} t'_{n-i+1} \tilde{\vartheta}_i^h$$

*) Siehe Gauß, Disquisitiones arithmeticae, art. 282.

ist, in die Form $\tilde{B}$ über. Wir bekommen daher

$$\tilde{b}_h = b_h + be_h, \qquad \tilde{b}_h \equiv b_h \pmod{b},$$

und die beiden Lösungen $(b_h)$ und $(\tilde{b}_h)$ der Kongruenzen (50) sind in der Tat kongruent modulo $b$.

Die Substitution $(t')^{-1}\cdot(\tilde{t}')$, welche die Form $B'$ in $\tilde{B}'$ verwandelt, läßt sich jetzt schreiben

$$(t')^{-1}\cdot(\tilde{t}'): \quad \xi_h' = \tilde{\xi}_h' - e_{n-h}\cdot\tilde{\xi}' \quad (h = 1, 2, \ldots, n-1), \qquad \xi' = \tilde{\xi}'.$$

Durch Zusammensetzung der beiden Systeme $(t')$ und $(t')^{-1}(\tilde{t}')$ müssen wir zu dem System $(\tilde{t}')$ gelangen. Auf diese Weise erhalten wir von neuem die Bedingungen (52). Führen wir aber für die Zahlen $\tilde{t}_i'$ die Werte (52) ein, so ist die Substitution $(\tilde{t}')$ in der Tat von der Determinante 1 und verwandelt die Form $f'$ in eine Form $\tilde{B}'$, deren adjungierte Form $\tilde{B}$ anstelle der Koeffizienten $b_h$ die Zahlen $\tilde{b}_h$ aufweist.

IV. Man kann leicht die folgende Relation beweisen, welche später Anwendung finden wird:

$$(53) \qquad \prod_{h=1}^{n-1} o_h^2 = -(n-2)\,bb'\cdot\prod_{h=1}^{n-1} o_h + o_1 o_1'\cdot\sum_{i,k=1}^{n-1} c_{ik}c'_{n-i,n-k}.$$

In der Tat hat man

$$|\varphi| = \sum_{k=1}^{n-1} b_{ik}\frac{\partial|\varphi|}{\partial b_{ik}},$$

d. i.

$$(54) \qquad o_1 o_2 \ldots o_{n-2} b' = \sum_{k=1}^{n-1} b_{ik}\cdot c'_{n-i,n-k}.$$

Die Determinante der Form $B$ läßt sich schreiben

$$(-1)^I\cdot d_{n-1} = b\cdot|\varphi| - \sum_{i,k=1}^{n-1} b_i b_k \frac{\partial|\varphi|}{\partial b_{ik}};$$

daraus ergibt sich

$$\prod_{h=1}^{n-1} o_h^2 = bb'\cdot\prod_{h=1}^{n-1} o_h - o_1'\cdot\sum_{i,k=1}^{n-1} b_i b_k\cdot c'_{n-i,n-k}.$$

Führen wir hierin statt der Zahlen $b_i b_k$ die Zahlen $-o_1 c_{ik} + bb_{ik}$ ein und benutzen die Beziehung (54), so bekommen wir sofort die behauptete Gleichung.

V. Es ist klar, daß es überhaupt keine eigentlichen Darstellungen der Form $\varphi' = \{b_{ik}'\}$ von der Determinante $(-1)^I\cdot d'_{n-2}\cdot b$ durch die Form $f'$ geben kann, sobald nicht die Größen $c_{n-i,n-k} = (-1)^I\cdot\frac{1}{d'_{n-3}}\cdot\frac{\partial|\varphi'|}{\partial b'_{ik}}$ ganze Zahlen werden. Sind aber diese sämtlichen Größen ganze Zahlen,

so wird eine jede eigentliche Darstellung $(\mathfrak{S}')$ der Form $\varphi'$ durch $f'$ zu einer einzigen Lösung $(b_h) \pmod b$ der Kongruenzen

$$-o_1 c_{ik} \equiv b_i b_k \pmod b$$

gehören, und wir werden sonach alle möglichen eigentlichen Darstellungen $(\mathfrak{S}')$ der Form $\varphi'$ durch $f'$ bekommen, indem wir die sämtlichen modulo $b$ inkongruenten Systeme

$$(b_1, b_2, \ldots, b_{n-1})$$

aufsuchen, welche diese Kongruenzen erfüllen, und für jedes dieser Systeme die sämtlichen eigentlichen Darstellungen $(\mathfrak{S}')$ bestimmen, welche zu demselben gehören.

Für ein bestimmtes gegebenes System $(b_h) \pmod b$ kann dies auf folgende Weise geschehen:

Wir bezeichnen die ganzen Zahlen

$$\frac{o_1 c_{ik} + b_i b_k}{b}$$

durch $b_{ik}$ und untersuchen die Form

$$B = b\xi^2 + 2\sum_{i=1}^{n-1} b_i \xi \xi_i + \sum_{i,k=1}^{n-1} b_{ik} \xi_i \xi_k.$$

Diese Form geht mit Hilfe der Substitution

$$\xi = \eta - \sum_{h=1}^{n-1} \frac{b_h}{b} \eta_h, \quad \xi_h = \eta_h \qquad (h = 1, 2, \ldots, n-1)$$

in eine Form

$$B_0 = b\eta^2 + \sum_{i,k=1}^{n-1} \frac{o_1 c_{ik}}{b} \eta_i \eta_k$$

über. Wir ersehen hieraus, daß die Determinante von $B$ gleich $(-1)^I \cdot d_{n-1}$ ist. Ferner gilt $\frac{\partial |B|}{\partial b_{n-i,\, n-k}} = (-1)^I \cdot d_{n-2} \cdot b'_{ik}$, und wir setzen

$$\frac{\partial |B|}{\partial b} = (-1)^I \cdot d_{n-2} \cdot b' \qquad \text{und} \qquad \frac{\partial |B|}{\partial b_{n-i}} = (-1)^I \cdot d_{n-2} \cdot b'_i.$$

Aus den vorhergehenden Sätzen leuchtet ein, daß wenn die Form $B$ der Form $f$ nicht äquivalent ist, keine eigentlichen, zu der Wurzel $(b_h)$ der Kongruenzen (50) gehörenden Darstellungen der Form $\varphi'$ durch $f'$ existieren. Sobald aber $B \sim f$ ist, so wird auch die zu $B$ adjungierte Form $B'$ der Form $f'$ äquivalent sein und sich schreiben lassen

$$B' = \sum_{i,k=1}^{n-1} b'_{ik} \xi'_i \xi'_k + 2\sum_{i=1}^{n-1} b'_i \xi'_i \xi' + b' \xi'^2.$$

Eine jede Substitution

$$(t'): \quad x_i' = \sum_{k=1}^{n-1} \vartheta_i'^k \xi_k' + t_i' \xi' \qquad (i = 1, 2, \ldots, n)$$

von der Determinante 1, mit deren Hilfe die Form $f'$ in $B'$ übergeht, liefert dann eine eigentliche Darstellung

$$(\vartheta'): \quad x_i' = \sum_{k=1}^{n-1} \vartheta_i'^k \xi_k' \qquad (i = 1, 2, \ldots, n)$$

von $\varphi'$ durch $f'$, und wir gelangen, indem wir sämtliche verschiedenen Substitutionen $(t')$ von der Determinante 1 bilden, durch welche $f'$ in $B'$ transformiert wird, zu allen überhaupt möglichen Darstellungen $(\vartheta'_{\varphi'})$, welche zu der Wurzel $(b_h)$ gehören, und zwar zu einer jeden dieser Darstellungen ein einziges Mal. Denn wir haben gesehen, daß zwei verschiedene Transformationen $(t')$ niemals die gleichen Koeffizienten $\vartheta_i'^k$ darbieten können.

## Kap. XVIII. Index, Ordnung und Genus der durch eine Form von $n$ Variablen darstellbaren Formen von $n-1$ Variablen.

Es sei eine primitive Form $f = \sum_{i,k=1}^{n} a_{ik} x_i x_k$ von einem Index $I$, einer Ordnung $O: \binom{\sigma_h}{o_h}$ und einem Genus $G$ gegeben, und es möge die Zahl $b$ vermittels eines Systems

$$(t): \quad x_i = t_i$$

durch $f$ dargestellt sein.

Da die Koeffizienten $a_{ii}$, $2a_{ik}$ sämtlich durch $\sigma_1$ teilbar sind, wird die Zahl $b$ den Faktor $\sigma_1$ enthalten. Es bedeute $\delta$ das Vorzeichen der Zahl $b$ und $m$ den absoluten Wert von $\frac{b}{\sigma_1}$. Dann wird $b = \delta \cdot \sigma_1 m$. Wir betrachten insbesondere Zahlen $b$, für welche die Größe $m$ zu der Determinante $\Delta$ von $f$ relativ prim ist.

Wir nennen den größten gemeinsamen Teiler $T$ der $n$ Zahlen $T_i = \sum_{k=1}^{n} a_{ik} t_k$ den *Teiler der Darstellung* $(t)$, und sagen, eine Darstellung $(t)$ sei *primär*, wenn ihr Teiler $T$ gleich 1 ist. Eine primäre Darstellung ist stets eigentlich; denn der größte gemeinsame Teiler $\tau$ der $n$ Zahlen $t_k$ geht in allen Summen $T_i$ und folglich auch in der Zahl $T$ auf. Ist daher $T = 1$, so wird auch der Teiler $\tau$ der Einheit gleich sein. — Aus den Gleichungen (48) erhellt, daß der Teiler $T$ der Darstellung $(t)$ in den sämtlichen Zahlen $b, b_1, b_2, \ldots, b_{n-1}$ aufgehen wird. Andererseits erkennen

wir aus den Gleichungen (51), daß der größte Teiler der Zahlen $b, b_h$ in den sämtlichen Zahlen $T_i$ aufgeht. Es stimmt demnach der Teiler $T$ der Darstellung $(t)$ mit dem größten Teiler der Zahlen $b, b_h$ überein. Die Kongruenzen $b \equiv 0$, $b_h \equiv 0 \pmod{T}$ ergeben unmittelbar $\Delta \equiv 0 \pmod{T}$. Folglich wird, falls die Zahl $m$ zu $\Delta$ relativ prim sein soll, der Teiler $T$ in $\sigma_1$ aufgehen, und eine [[eigentliche]] Darstellung $(t)$ der Zahl $b$ wird stets primär sein, außer in dem Falle, daß $\sigma_1 = 2$, $m \equiv 1 \pmod{2}$ ist und die Zahlen $T_i$ alle gerade ausfallen.

Der Darstellung $(t)$ der Zahl $b$ durch die Form $f$ ist eine Darstellung $(\vartheta')$ einer Form $\varphi' = \sum_{i,k=1}^{n-1} b'_{ik}\xi'_i\xi'_k$ von der Determinante $(-1)^I d'_{n-2} \cdot b$ durch die Form $f' = \sum_{i,k=1}^{n} a'_{ik}x'_i x'_k$ adjungiert. Wir wollen die Beziehungen untersuchen, welche zwischen den Indizes, den Ordnungen und den Genera der Form $\varphi'$ und der Form $f'$ bestehen.

*Index der Form $\varphi'$.*

Nach dem Satze Q. (Kap. XV) muß der Index der Form $\varphi'$ gleich $I$ oder $I-1$ sein, je nachdem die Zahl $b$ positiv ($\delta = 1$) oder negativ ($\delta = -1$) ist. Da der Index einer Form von $n-1$ Variablen stets zwischen den Grenzen 0 und $n-1$ eingeschlossen ist, wird die Form $\varphi'$ niemals durch die Form $f'$ darstellbar sein, wenn $I = 0$ und $b < 0$ oder $I = n$ und $b > 0$ ist.

*Ordnung der Form $\varphi'$.*

Es sei der größte gemeinsame Teiler der sämtlichen Koeffizienten $b'_{ik}$ der Form $\varphi'$ gleich $e'$, und es seien $e_1', e_2', \ldots, e'_{n-2}$ die Invarianten $o$ und $\tau_1', \tau_2', \ldots, \tau'_{n-2}$ die Invarianten $\sigma$ der primitiven Form $\frac{\varphi'}{e'}$. Es gilt alsdann die Beziehung

$$\sigma_1 d'_{n-2} m = e'^{n-1} \cdot e_1'^{n-2} e_2'^{n-3} \ldots e'_{n-2}. \tag{55}$$

Wir bezeichnen durch $q^{\varepsilon'}$, $q^{\varepsilon_h'}$ die höchsten Potenzen einer Primzahl $q$, welche in den Größen $e'$, $e_h'$ aufgehen. Wir wollen jetzt die Zahlen $\varepsilon'$, $\varepsilon_h'$ durch die Zahlen $\omega_h'$ ausdrücken.

1. Es bedeute zunächst $q$ eine in $m$ aufgehende Primzahl. Wäre die Größe $e'$ oder eine der $n-3$ ersten Invarianten $e_1', e_2', \ldots, e'_{n-3}$ durch diese Primzahl $q$ teilbar, so müßten die sämtlichen ganzen Zahlen $c_{ik} = (-1)^I \cdot \frac{1}{d'_{n-3}} \cdot \frac{\partial |\varphi'|}{\partial b'_{n-i,\,n-k}}$ gleichfalls durch $q$ teilbar sein, und die Gleichung (53) gäbe $\prod_{h=1}^{n-1} o_h$ oder $\Delta \equiv 0 \pmod{q}$, was gegen unsere Voraus-

setzung streitet, daß die Zahl $m$ zu $\Delta$ relativ prim ist. Wir finden sonach für jede in $m$ aufgehende Primzahl $\varepsilon' = 0$; $\varepsilon_1' = 0$, $\varepsilon_2' = 0$, ..., $\varepsilon_{n-3}' = 0$. Wegen (55) wird dann die Größe $q^{\varepsilon'_{n-2}}$ der größten Potenz von $q$ gleich sein, welche in $\sigma_1 m$ oder in $b$ aufgeht. Indem wir dieses Resultat für die sämtlichen in $m$ enthaltenen Primzahlen $q$ anwenden, erkennen wir, daß die Invariante $e'_{n-2}$ durch $m$ teilbar sein muß.

2. Es bedeute jetzt $q$ eine ungerade Primzahl $p$, welche nicht in $m$ aufgeht. Da die Zahl $b$ alsdann zu $p$ relativ prim ist, so können wir die Zahlen $(b_1, b_2, \ldots, b_{n-1})$, zu welchen die Darstellung $(\vartheta')$ gehört, so wählen, daß sie neben den Kongruenzen (50) für den Modul $b$ noch den weiteren Kongruenzen

$$b_1 \equiv 0,\ b_2 \equiv 0,\ \ldots,\ b_{n-1} \equiv 0 \pmod{p^t}$$

für irgend einen Modul $p^t (> p^{v_{n-1}(p)})$ genügen. Es wird alsdann

$$o_1 c_{ik} \equiv b b_{ik} \pmod{p^t},$$

und die Form $B$ besitzt für den Modul $p^t$ einen Rest

$$B \equiv \begin{pmatrix} b, & 0 & , \ldots, & 0 \\ 0, & \frac{o_1 c_{11}}{b} & , \ldots, & \frac{o_1 c_{1,n-1}}{b} \\ \cdot & \cdot & \cdot & \cdot \\ 0, & \frac{o_1 c_{n-1,1}}{b} & , \ldots, & \frac{o_1 c_{n-1,n-1}}{b} \end{pmatrix} \pmod{p^t}.$$

Schlüsse, welche denen von Kap. III ganz analog sind, zeigen jetzt, daß die Form $\sum_{i,k=1}^{n-1} c_{ik} \xi_i \xi_k$ primitiv in bezug auf $p$ sein muß und daß die höchsten in den Invarianten $o$ dieser Form aufgehenden Potenzen von $p$ bzw. gleich $p^{\omega'_{n-2}}, p^{\omega'_{n-3}}, \ldots, p^{\omega'_1}$ sind. Andererseits müssen diese Potenzen gleich $p^{\varepsilon'_{n-2}}, p^{\varepsilon'_{n-3}}, \ldots, p^{\varepsilon'_1}$ sein; denn die Form $\{c_{ik}\}$ ist ein Multiplum der zu $\frac{\varphi'}{e'}$ adjungierten Form. Wir gewinnen also die Beziehungen

$$\varepsilon_1' = \omega_1',\ \varepsilon_2' = \omega_2',\ \ldots,\ \varepsilon'_{n-2} = \omega'_{n-2}.$$

Indem wir jetzt diese Werte der Zahlen $\varepsilon_h'$ in die Formel (55) einführen, finden wir noch $\varepsilon' = 0$. Die Form $\varphi'$ muß also in bezug auf $p$ primitiv sein.

3. Es möge endlich die Primzahl $q$ gleich 2 sein. Gemäß unserer Annahme, daß die Zahl $m$ zu $\Delta$ relativ prim sei, werden wir die beiden Fälle $m \equiv 1 \pmod 2$ und $m \equiv 0$, $\Delta \equiv 1 \pmod 2$ zu untersuchen haben.

I. Wir betrachten zunächst den Fall $m \equiv 1 \pmod 2$.

($\sigma_1 = 1$). Ist in diesem Falle $\sigma_1 = 1$, so wird die Zahl $b$ ungerade sein, und wir können infolgedessen die Zahlen $(b_1, b_2, \ldots, b_{n-1})$, zu welchen die Darstellung $(\vartheta')$ gehört, so wählen, daß sie neben den Kongruenzen (50) nach dem Modul $b$ noch den Kongruenzen

$$b_1 \equiv 0,\ b_2 \equiv 0,\ \ldots,\ b_{n-1} \equiv 0 \pmod{2^t}$$

für irgend einen Modul $2^t (> \sigma_{n-1} \cdot 2^{v_{n-1}(2)})$ genügen. Alsdann wird

$$o_1 c_{ik} \equiv b b_{ik} \pmod{2^t}$$

und folglich

$$B \equiv \begin{pmatrix} b, & 0 & , \ldots, & 0 \\ 0, & \frac{o_1 c_{11}}{b} & , \ldots, & \frac{o_1 c_{1,n-1}}{b} \\ \cdot & \cdot & \cdot & \cdot \\ 0, & \frac{o_1 c_{n-1,1}}{b} & , \ldots, & \frac{o_1 c_{n-1,n-1}}{b} \end{pmatrix} \pmod{2^t}.$$

Aus diesem Rest von $B$ ersehen wir, daß die Form $\sum_{i,k=1}^{n-1} c_{ik}\xi_i\xi_k$ zu 2 primitiv ausfällt, daß die Zahlen $\varepsilon'$, $\varepsilon_h'$ durch die Gleichungen

$$\varepsilon' = 0,\ \varepsilon_1' = \omega_1',\ \varepsilon_2' = \omega_2',\ \ldots,\ \varepsilon_{n-2}' = \omega_{n-2}' \tag{56}$$

gegeben sind und daß die Potenzen $\sigma_{n-h}' \cdot 2^{\partial_{h-1}}$ mit den kleineren der Potenzen

$$\tau_{n-h}' \cdot 2^{\partial_{h-1}}, \qquad \tau_{n-h-1}' \cdot 2^{\partial_h}$$

übereinstimmen oder, was auf dasselbe hinauskommt, daß die Invarianten $\sigma_{n-h}'$ mit den kleineren der je zwei Zahlen

$$\tau_{n-h}' \quad \text{und} \quad \tau_{n-h-1}' \cdot 2^{\omega_1+\omega_2+\cdots+\omega_h}$$

übereinstimmen.

Wir wollen nun annehmen, daß die $\varkappa_1 - 1$ $(1 \leqq \varkappa_1 \leqq n)$ ersten der Größen $\omega_h$, nämlich $\omega_1, \omega_2, \ldots, \omega_{\varkappa_1-1}$ gleich Null seien, während die $\varkappa_1^{\text{te}}$ dieser Zahlen, $\omega_{\varkappa_1}$, von Null verschieden sei. Alsdann ist nach Kap. IV $\sigma_1 = 1$, $\sigma_2 = 1, \ldots, \sigma_{\varkappa_1-1} = 1$; $\sigma_{\varkappa_1} = 1$. Die Größe $\tau_{n-h-1}' \cdot 2^{\omega_1+\omega_2+\cdots+\omega_h}$ wird für $h < \varkappa_1$ gleich $\tau_{n-h-1}'$ und für $h \geqq \varkappa_1$ größer oder gleich $2\tau_{n-h-1}' \geqq \tau_{n-h}'$. Für $h \geqq \varkappa_1$ ist daher immer $\sigma_{n-h}' = \tau_{n-h}'$.

Die Relationen (56) ergeben

$$\varepsilon_{n-\varkappa_1}' \geqq 1,\ \varepsilon_{n-\varkappa_1+1}' = 0,\ \varepsilon_{n-\varkappa_1+2}' = 0,\ \ldots,\ \varepsilon_{n-2}' = 0.$$

Die $\varkappa_1 - 2$ letzten Invarianten $\tau_h'$ können infolgedessen nach den in Kap. IV gegebenen Sätzen nur die Werte

$$\tau_{n-\varkappa_1+1}' = 1,\ \tau_{n-\varkappa_1+2}' = 1,\ \ldots,\ \tau_{n-2}' = 1 \tag{$57_1$}$$

oder die Werte

$$\tau_{n-\varkappa_1+1}' = 2,\ \tau_{n-\varkappa_1+2}' = 1,\ \ldots,\ \tau_{n-2}' = 2 \tag{$57_2$}$$

annehmen.

Der letztere Fall $(57_2)$ ist an die Bedingungen $\varkappa_1 - 1 \equiv 0 \pmod 2$ und $\varkappa_1 - 1 > 0$ gebunden. Wenn also $\varkappa_1 \equiv 0 \pmod 2$ und auch wenn $\varkappa_1 = 1$ wird, erhalten wir stets $\tau_h' = \sigma_h'$ $(h = 1, 2, \ldots, n-2)$. Ist dagegen $\varkappa_1 \equiv 1 \pmod 2$ und $\varkappa_1 > 1$, so sind die Fälle $(57_1)$ und $(57_2)$ alle beide möglich.

Der zweite dieser Fälle tritt offenbar nur dann ein, wenn die Invariante $\tau'_{n-2}$ gleich 2 ist, d. h. wenn die Zahlen

$$c_{ii} = \frac{1}{o_1}(b b_{ii} - b_i^2) \equiv b_{ii} - b_i \pmod 2$$

alle kongruent 0 (mod 2) sind, oder, was auf das nämliche hinauskommt, wenn die $n-1$ Kongruenzen

$$b_i \equiv b_{ii} \pmod 2 \qquad [b \equiv 1 \pmod 2] \tag{58}$$

gelten.

Wir können voraussetzen, daß der Rest $f \pmod 2$ von der in Kap. III angegebenen Gestalt $f_{(\varkappa_1)}$ ist. Geht dann $f$ durch die Substitution

$$(t): \quad x_i = t_i \xi + \sum_{k=1}^{n-1} \vartheta_i^{\,k} \xi_k \qquad (i = 1, 2, \ldots, n)$$

in $B$ über, so wird

$$b_i \equiv t_1 \vartheta_1^{\,i} + t_2 \vartheta_2^{\,i} + \cdots + t_{\varkappa_1} \vartheta_{\varkappa_1}^{\,i}, \; b_{ii} \equiv \vartheta_1^{\,i} + \vartheta_2^{\,i} + \cdots + \vartheta_{\varkappa_1}^{\,i} \pmod 2,$$

und der Fall $(57_2)$ ist durch die Bedingungen

$$(t_1 - 1)\vartheta_1^{\,i} + (t_2 - 1)\vartheta_2^{\,i} + \cdots + (t_{\varkappa_1} - 1)\vartheta_{\varkappa_1}^{\,i} \equiv 0 \pmod 2 \quad (i = 1, 2, \ldots, n-1) \tag{59}$$

gekennzeichnet. Zu diesen Kongruenzen können wir noch die Kongruenz

$$(t_1 - 1)t_1 + (t_2 - 1)t_2 + \cdots + (t_{\varkappa_1} - 1)t_{\varkappa_1} \equiv 0 \pmod 2, \tag{60}$$

die wegen $t_h(t_h - 1) \equiv 0 \pmod 2$ evident ist, hinzufügen. Da die Determinante der Substitution $(t)$ ungerade $(= 1)$ ist, können die $\varkappa_1$-reihigen Unterdeterminanten des Systems

$$|t_h, \vartheta_h^{\,1}, \vartheta_h^{\,2}, \ldots, \vartheta_h^{\,n-1}| \qquad (h = 1, 2, \ldots, \varkappa_1)$$

nicht sämtlich gerade sein. Demnach gibt es unter den $n$ Kongruenzen (59), (60) $\varkappa_1$, deren Determinante ungerade ist. Lösen wir dann diese $\varkappa_1$ Kongruenzen nach den $\varkappa_1$ Größen $t_1 - 1, t_2 - 1, \ldots, t_{\varkappa_1} - 1$ auf, so bekommen wir

$$t_1 - 1 \equiv 0, \; t_2 - 1 \equiv 0, \; \ldots, \; t_{\varkappa_1} - 1 \equiv 0 \pmod 2.$$

Man erkennt also, daß die Kongruenzen (58) die einzige Lösung

$$t_1 \equiv 1, \; t_2 \equiv 1, \; \ldots, \; t_{\varkappa_1} \equiv 1 \pmod 2$$

zulassen.

$(\sigma_1 = 2.)$ Es sei jetzt $\sigma_1 = 2$ und mithin $b = \delta \cdot \sigma_1 m \equiv 2 \pmod 4$. Die $n-1$ Zahlen $(b_1, b_2, \ldots, b_{n-1})$ sind dann entweder alle gerade, oder es befinden sich unter ihnen auch ungerade Größen. Im ersteren Falle wird $T_i = \sum_{k=1}^{n} a_{ik} t_k \equiv 0 \pmod 2$ $(i = 1, 2, \ldots, n)$, und folglich ist die gegebene Darstellung $(t)$ der Zahl $b$ nur im zweiten Falle primär.

Wir wollen annehmen, von den Größen $\omega_h$ seien die $\varkappa_1 - 1 \; (1 \leqq \varkappa_1 \leqq n)$ ersten, nämlich $\omega_1, \omega_2, \ldots, \omega_{\varkappa_1 - 1}$, gleich Null, während die $\varkappa_1^{\text{te}}$ dieser

Zahlen, $\omega_{\varkappa_1}$, von Null verschieden sein möge, und wir wollen annehmen, daß der Rest $f \pmod 4$ von der in Kap. III angegebenen Gestalt $f_{(\varkappa_1)}$ sei. Dann gelten die Kongruenzen

$$T_1 \equiv t_2,\ T_2 \equiv t_1,\ T_3 \equiv t_4,\ T_4 \equiv t_3,\ \ldots,\ T_{\varkappa_1-1} \equiv t_{\varkappa_1},\ T_{\varkappa_1} \equiv t_{\varkappa_1-1};$$
$$T_h \equiv 0 \pmod 2 \quad (h > \varkappa_1),$$

und es werden die Zahlen $T_i$ nur dann sämtlich gerade ausfallen, wenn

$$t_1 \equiv 0,\ t_2 \equiv 0,\ \ldots,\ t_{\varkappa_1} \equiv 0 \pmod 2$$

wird. Diese Kongruenzen bilden demnach die notwendige und hinreichende Bedingung dafür, daß die $n-1$ Zahlen $b_h$ sämtlich durch 2 teilbar werden. Diese Kongruenzen sind jedoch mit der Annahme $b \equiv 2 \pmod 4$ nur in dem Falle verträglich, daß $2^{\omega_{\varkappa_1}}\sigma_{\varkappa_1+1} = 2$ und also $2^{\omega_{\varkappa_1}} = 2$, $\sigma_{\varkappa_1+1} = 1$ wird. In der Tat, ist $2^{\omega_{\varkappa_1}}\sigma_{\varkappa_1+1} \equiv 0 \pmod 4$, so sieht man leicht, daß in dem Rest $f \equiv \Phi_{(1)} + 2^{\omega_{\varkappa_1}} f^{(\varkappa_1)} \pmod 4$ alle Koeffizienten $2^{\omega_{\varkappa_1}} a_{ii}^{(\varkappa_1)}$, $2^{\omega_{\varkappa_1}} 2 a_{ik}^{(\varkappa_1)}$ kongruent Null $\pmod 4$ werden. Infolgedessen ist eine jede Zahl $b$, welche durch $f$ vermittels gerader Zahlen $t_1, t_2, \ldots, t_{\varkappa_1}$ dargestellt wird, durch 4 teilbar.

Wenn von den $n-1$ Zahlen $b_1, b_2, \ldots, b_{n-1}$ einige ungerade ausfallen, so werden sich auch unter den Zahlen $c_{ii} = \frac{1}{o_1}(-b_i^2 + b b_{ii})$ ungerade Größen befinden. Die Form $\Phi = \sum_{i,k=1}^{n-1} c_{ik}\xi_i\xi_k$ wird daher in bezug auf 2 primitiv ausfallen und sich in einen Repräsentanten

$$\tilde{\Phi} = \begin{pmatrix} c^*, & c_1^*, & \ldots, & c_{n-2}^* \\ c_1^*, & c_{11}^*, & \ldots, & c_{1,n-2}^* \\ \cdot & \cdot & \cdot & \cdot \\ c_{n-2}^*, & c_{n-2,1}^*, & \ldots, & c_{n-2,n-2}^* \end{pmatrix}$$

verwandeln lassen, in welchem $c^* \equiv 1 \pmod 2$ ist und die Koeffizienten $c_1^*, \ldots, c_{n-2}^*$ kongruent Null nach einem Modul $2^t (> \sigma_{n-1} \cdot 2^{v_{n-1}(2)})$ sind. Bedeutet $M$ den größten Teiler der sämtlichen Koeffizienten von $\Phi$, so wird die Form $\frac{\delta \cdot \Phi}{M}$ der Form $\frac{\varphi'}{e'}$ adjungiert sein. Wir wollen durch $\frac{\tilde{\varphi}'}{e'}$ die zu $\frac{\delta \cdot \tilde{\Phi}}{M}$ adjungierte Form bezeichnen. Dann ist die Form $\tilde{\varphi}'$ der Form $\varphi'$ äquivalent. Anstatt der vorliegenden Darstellung $(\vartheta')$ der Form $\varphi'$ durch $f'$ können wir jetzt irgendeine äquivalente Darstellung $(\tilde{\vartheta}')$ der Form $\tilde{\varphi}'$ durch $f'$ betrachten. Für diese Darstellung $(\tilde{\vartheta}')$ möge anstelle der Form $B$ eine Form

$$\tilde{B} = b\tilde{\xi}^2 + 2\sum_{i=0}^{n-2} \tilde{b}_i \tilde{\xi}\tilde{\xi}_i + \sum_{i,k=0}^{n-2} \tilde{b}_{ik}\tilde{\xi}_i\tilde{\xi}_k$$

treten.

Wir erhalten die Gleichungen

$$-o_1 c^* = \tilde{b}_0^{\,2} - b\cdot\tilde{b}_{00},\quad -o_1 c_i^* = \tilde{b}_0\tilde{b}_i - b\cdot\tilde{b}_{0i},\quad -o_1 c_{ik}^* = \tilde{b}_i\tilde{b}_k - b\cdot\tilde{b}_{ik}.$$

Da wir $b\equiv 0 \pmod 2$ und $c^*\equiv 1$, $c_i^*\equiv 0 \pmod 2$ vorausgesetzt haben, ergeben sich die Kongruenzen

$$\tilde{b}_0\equiv 1;\ \tilde{b}_1\equiv 0,\ \ldots,\ \tilde{b}_{n-2}\equiv 0 \pmod 2.$$

Die Darstellung $(\tilde{\vartheta}')$ bestimmt nur die Reste der Zahlen $\tilde{b}_i$ nach dem Modul $b$ $[\equiv 2 \pmod 4]$. Wir können daher die Zahlen so wählen, daß sie den Kongruenzen

$$\tilde{b}_1\equiv c_1^*,\ \ldots,\ \tilde{b}_{n-2}\equiv c_{n-2}^* \pmod{2^{t+1}}$$

genügen. Alsdann werden wegen $\tilde{b}_0\tilde{b}_i - b\cdot\tilde{b}_{0i} = -o_1 c_i^*$ die Kongruenzen $\tilde{b}_{0i}\equiv 0 \pmod{2^t}$ und wegen $\tilde{b}_i\tilde{b}_k - b\cdot\tilde{b}_{ik} = -o_1 c_{ik}^*$ die Kongruenzen $c_{ii}^*\equiv 0$, $2c_{ik}^*\equiv 0 \pmod 4$ statthaben, und die Form $\tilde{B}$ wird für den Modul $2^t$ einen Rest

$$\tilde{B}\equiv \begin{Vmatrix} b, & b_0 & & \\ b_0, & b_{00} & & \\ & \frac{o_1 c_{11}^*}{b}, & \ldots, & \frac{o_1 c_{1,n-2}^*}{b} \\ & \ldots & \ldots & \ldots \\ & \frac{o_1 c_{n-2,1}^*}{b}, & \ldots, & \frac{o_1 c_{n-2,n-2}^*}{b} \end{Vmatrix} \pmod{2^t}$$

liefern, in welchem $b\equiv 0$, $b_0\equiv 1$, $b_{00}\equiv 0$, $\frac{o_1 c_{ii}^*}{b}\equiv 0 \pmod 2$ ist.

Dieser Rest von $\tilde{B}$ zeigt, daß die höchste in allen Koeffizienten $c_{ik}^*$ der Form $\sum_{i,k=1}^{n-2} c_{ik}^*\xi_i\xi_k$ aufgehende Potenz von 2 gleich $2^{\omega_{n-2}'+1}$ ist, sowie daß für die in bezug auf 2 primitive Form $\left\{\frac{c_{ik}^*}{2^{\omega_{n-2}'+1}}\right\}$ die Invarianten $2^{\omega(2)}$ gleich $2^{\omega_{n-3}'}, \ldots, 2^{\omega_1'}$ und die Invarianten $\sigma$ gleich $\sigma_{n-3}', \ldots, \sigma_1'$ sind. Indem wir dieses Resultat auf den Rest der Form $\tilde{\Phi} \pmod{2^t}$ anwenden, erkennen wir, daß die Invarianten $2^{\omega(2)}$ dieser Form gleich $\sigma_1\cdot 2^{\omega_{n-2}'}, 2^{\omega_{n-3}'}, \ldots, 2^{\omega_1'}$ und die Invarianten $\sigma$ dieser Form gleich $\sigma_{n-2}'$, $\sigma_{n-3}', \ldots, \sigma_1'$ sind. Andererseits ist offenbar, daß die Invarianten $2^{\omega(2)}$ der Form $\tilde{\Phi}$ mit den Zahlen $2^{\varepsilon_{n-2}'}, 2^{\varepsilon_{n-3}'}, \ldots, 2^{\varepsilon_1'}$ und die Invarianten $\sigma$ dieser Form mit den Größen $\tau_{n-2}', \tau_{n-3}', \ldots, \tau_1'$ übereinstimmen. Folglich wird

$$\varepsilon_1' = \omega_1',\ \varepsilon_2' = \omega_2',\ \ldots,\ \varepsilon_{n-3}' = \omega_{n-3}',\ 2^{\varepsilon_{n-2}'} = \sigma_1\cdot 2^{\omega_{n-2}'},$$
$$\tau_1' = \sigma_1',\ \tau_2' = \sigma_2',\ \ldots,\ \tau_{n-3}' = \sigma_{n-3}',\ \tau_{n-2}' = \sigma'_{-2} = 1.$$

Führen wir diese Werte der Zahlen $\varepsilon_h'$ in die Relation (55) ein, so finden wir noch $\varepsilon' = 0$.

II. Wir betrachten endlich den Fall, in welchem $m \equiv 0 \pmod 2$ und $\Delta \equiv 1 \pmod 2$ ist. Es sei $2^v$ die höchste in $m$ aufgehende Potenz von 2. Wir sahen in 1., daß die Zahlen $\varepsilon'$, $\varepsilon_h'$ durch die Gleichungen

$$\varepsilon' = 0,\ \varepsilon_1' = 0,\ \varepsilon_2' = 0,\ \ldots,\ \varepsilon_{n-3}' = 0,\ 2^{\varepsilon_{n-2}'} = \sigma_1 \cdot 2^v$$

gegeben sind.

Wir haben sonach nur noch die Invarianten $\tau_h'$ zu bestimmen. Die letzte dieser Invarianten, $\tau_{n-2}'$, wird, da $2^{\varepsilon_{n-2}'} \geqq 2$ ist, stets gleich 1. Die übrigen $n-3$ Invarianten $\tau_h'$ müssen nach den in Kap. IV gegebenen Sätzen entweder die Werte

$$\tau_1' = 1,\ \tau_2' = 1,\ \ldots,\ \tau_{n-3}' = 1$$

oder die Werte

$$\tau_1' = 2,\ \tau_2' = 1,\ \ldots,\ \tau_{n-3}' = 2$$

erhalten. Der letztere dieser beiden Fälle ist an die Bedingung $n - 2 \equiv 0 \pmod 2$, also $n \equiv 0 \pmod 2$ gebunden. Außerdem muß, wie wir leicht einsehen, eine jede Invariante $\tau_h'$ die entsprechende Invariante $\sigma_h'$ als Faktor enthalten. Wir gewinnen daher das folgende Resultat: Wenn $n \equiv 1 \pmod 2$ wird, in welchem Falle stets $\sigma_1' = 1$, $\sigma_2' = 1, \ldots, \sigma_{n-2}' = 1$, $\sigma_{n-1}' = 1$ ist, so haben wir $\tau_1' = 1$, $\tau_2' = 1$, $\ldots$, $\tau_{n-3}' = 1$, $\tau_{n-2}' = 1$; wenn dagegen $n \equiv 0 \pmod 2$ ist, so wird, falls $\sigma_1' = 1$, $\sigma_2' = 1$, $\ldots$, $\sigma_{n-2}' = 1$, $\sigma_{n-1}' = 1$ ist, entweder $\tau_1' = 1$, $\tau_2' = 1, \ldots, \tau_{n-3}' = 1$, $\tau_{n-2}' = 1$ oder $\tau_1' = 2$, $\tau_2' = 1$, $\ldots$, $\tau_{n-3}' = 2$, $\tau_{n-2}' = 1$, und falls $\sigma_1' = 2$, $\sigma_1' = 1$, $\ldots$, $\sigma_{n-2}' = 1$, $\sigma_{n-1}' = 2$ wird, haben wir stets $\tau_1' = 2$, $\tau_2' = 1$, $\ldots$, $\tau_{n-3}' = 2$, $\tau_{n-2}' = 1$.

---

Wir können die Sätze, zu denen wir gelangt sind, in der folgenden Weise zusammenfassen:

Wenn eine primäre Darstellung $(t)$ einer Zahl $b = \delta \cdot \sigma_1 m$ ($m$ relativ prim zu $\Delta$) durch die Form $f$ einer Darstellung $(\vartheta')$ einer Form $\varphi'$ von $n-1$ Variablen und der Determinante $(-1)^I \cdot d_{n-2}' b$ durch die Form $f'$ adjungiert ist, so fällt $\varphi'$ primitiv aus und gehört zu einer Ordnung

$$\begin{pmatrix} \tau_h' \\ e_h' \end{pmatrix} \ (h = 1, 2, \ldots, n-2), \quad J' = I - \frac{1-\delta}{2},$$

deren Invarianten $e_h'$ den Gleichungen

$$e_1' = o_1',\ e_2' = o_2',\ \ldots,\ e_{n-3}' = o_{n-3}',\ e_{n-2}' = o_{n-2}' \cdot \sigma_1 m$$

genügen und deren Invarianten $\tau_h'$ entweder die Gleichungen

(I) $$\tau_1' = \sigma_1',\ \tau_2' = \sigma_2',\ \ldots,\ \tau_{n-3}' = \sigma_{n-3}',\ \tau_{n-2}' = \sigma_{n-2}'$$

oder auch, falls $\sigma_1 = 1$, $m \equiv \varkappa_1 \equiv 1 \pmod 2$, $\varkappa_1 > 1$ ist, die Gleichungen

$$\text{(II)}\qquad \begin{cases} \tau_1' = \sigma_1', \quad \tau_2' = \sigma_2', \ \ldots, \ \tau'_{n-\varkappa_1} = \sigma'_{n-\varkappa_1}, \\ \tau'_{n-\varkappa_1+1} = 2, \ \tau'_{n-\varkappa_1+2} = 1, \ \ldots, \ \tau'_{n-3} = 1, \ \tau'_{n-2} = 2, \\ \sigma'_{n-\varkappa_1+1} = 1, \ \sigma'_{n-\varkappa_1+2} = 1, \ \ldots, \ \sigma'_{n-3} = 1, \ \sigma'_{n-2} = 1, \end{cases}$$

oder, falls $\varkappa_1 = n$, $\sigma_1 = 1$, $m \equiv \varkappa_1 \equiv 0 \pmod 2$, $\varkappa_1 > 2$ ist, die Gleichungen

$$\text{(II)}\qquad \begin{cases} \tau_1' = 2, \ \tau_2' = 1, \ \ldots, \ \tau'_{n-3} = 2, \ \tau'_{n-2} = 1, \\ \sigma_1' = 1, \ \sigma_2' = 1, \ \ldots, \ \sigma'_{n-3} = 1, \ \sigma'_{n-2} = 1 \end{cases}$$

erfüllen.

Wir wollen die Ordnung der Form $\varphi'$, je nachdem die Gleichungen (I) oder (II) statthaben, durch $O_I'(b)$ oder durch $O_{II}'(b)$ bezeichnen.

Sei jetzt $\varphi$ die der Form $\varphi'$ adjungierte Form. Aus dem obigen Satz erhellt, daß $\varphi$ gleich $\sum_{i,k=1}^{n-1} c_{ik}\xi_i\xi_k$ oder gleich $-\sum_{i,k=1}^{n-1} c_{ik}\xi_i\xi_k$ sein wird, je nachdem die Zahl $b$ positiv oder negativ ist. Wir können daher $\varphi = \delta \cdot \sum_{i,k=1}^{n-1} c_{ik}\xi_i\xi_k$ setzen, und die Form $\varphi$ wird primitiv sein und der Ordnung

$$\begin{pmatrix} \tau'_{n-2}, & \tau'_{n-3}, & \ldots, & \tau_1' \\ e'_{n-2}, & e'_{n-3}, & \ldots, & e_1' \end{pmatrix}, \quad J' \qquad [e'_{n-2} = o'_{n-2} \cdot \sigma_1 m]$$

angehören.

Wir wählen die Form $\varphi'$ in ihrer Klasse so aus, daß $\varphi$ einen Hauptrest für den Modul $b$ vorstellt. Dann wird

$$\delta \cdot \varphi = \begin{pmatrix} c^*, & c_1^*, & c_2^*, & \ldots, & c_{n-2}^* \\ c_1^*, & c_{11}^*, & c_{12}^*, & \ldots, & c_{1,n-2}^* \\ c_2^*, & c_{21}^*, & c_{22}^*, & \ldots, & c_{2,n-2}^* \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ c_{n-2}^*, & c_{n-2,1}^*, & c_{n-2,2}^*, & \ldots, & c_{n-2,n-2}^* \end{pmatrix} \equiv \begin{pmatrix} c^*, & 0, & 0, & \ldots, & 0 \\ 0, & 0, & 0, & \ldots, & 0 \\ 0, & 0, & 0, & \ldots, & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0, & 0, & 0, & \ldots, & 0 \end{pmatrix} \pmod b,$$

wo $c^*$ zu $b$ relativ prim ist, und den $\frac{n(n-1)}{2}$ Kongruenzen

$$\text{(61)}\quad -o_1 c^* \equiv \tilde{b}_0^{\,2} \pmod b, \quad -o_1 c_i^* \equiv \tilde{b}_0 \tilde{b}_i \pmod b, \quad -o_1 c_{ik}^* \equiv \tilde{b}_i \tilde{b}_k \pmod b$$
$$(i, k = 1, 2, \ldots, n-2)$$

kann nicht anders genügt werden, als wenn man

$$\text{(62)}\qquad -o_1 c^* \equiv \tilde{b}_0^{\,2} \pmod b$$

und

$$\tilde{b}_1 \equiv 0, \ \tilde{b}_2 \equiv 0, \ \ldots, \ \tilde{b}_{n-2} \equiv 0 \pmod b$$

hat. Es wird daher die Anzahl der sämtlichen inkongruenten Systeme $(\tilde{b}_0, \tilde{b}_1, \ldots, \tilde{b}_{n-2}) \pmod b$, welche den $\frac{n(n-1)}{2}$ Kongruenzen (61) genügen,

mit der Anzahl der inkongruenten Lösungen $\tilde{b}_0 \pmod{b}$ der einzigen Kongruenz (62) übereinstimmen. Diese letztere Anzahl ist, sobald die Kongruenz (62) überhaupt keine Lösungen besitzt, gleich Null, dagegen wenn die Kongruenz (62) lösbar ist und wenn in der Zahl $b$ im ganzen $\mu$ ungerade Primzahlen $p$ aufgehen, gleich $2^{\mu}$, falls $b \equiv 1 \pmod 2$ oder $b \equiv 2 \pmod 4$ ist, oder gleich $2^{\mu+1}$, wenn $b \equiv 4 \pmod 8$ ist, oder gleich $2^{\mu+2}$, falls $b \equiv 0 \pmod 8$ ist.

*Genus der Form $\varphi'$.*

Wir wollen jetzt zeigen, daß die Form $\varphi'$ nur einem einzigen Genus $G_I'(b)$ oder $G_{II}'(b)$ der Ordnung $O_I'(b)$ resp. $O_{II}'(b)$ angehören kann und daß die Charaktere dieses Genus völlig durch die Charaktere des Genus $G'$ der Form $f'$ bestimmt sind.

Vergleichen wir zu diesem Zweck die Charaktere der Form $\varphi'$ und der Form $B'$ in bezug auf einen Modul $q^t$ miteinander. Der Einfachheit halber denken wir uns die Form $\varphi'$ als eine Grundform für den Modul $q$ gewählt. Bezeichnen wir die aus den $h$ ersten Reihen der Form $B'$ und der Form $\varphi'$ gebildeten symmetrischen Unterdeterminanten durch $\sigma_h' d_{h-1}' B_h'$ und durch $\tau_h' d_{h-1}' \varphi_h'$, so bestehen die Beziehungen $\sigma_h' B_h' = \tau_h' \varphi_h'$ $(h \leqq n-2)$ und $(-1)^I \cdot B_{n-1}' = \frac{b}{\sigma_1} = \delta \cdot m$. Die Größe $(-1)^I \cdot \tau_{n-2}' \varphi_{n-2}'$ stimmt mit dem Koeffizienten $c^*$ der Form $\delta \cdot \varphi$ überein, so daß wir die Kongruenz (62) auch

$$-(-1)^I \cdot o_1 \tau_{n-2}' \varphi_{n-2}' \equiv \tilde{b}_0^2 \pmod{\sigma_1 b} \tag{63}$$

schreiben können.

1. Bedeutet zunächst $q$ eine ungerade Primzahl $p$, welche nicht in $b$ und nicht in $\Delta$ aufgeht, so besitzt weder die Form $\varphi'$ noch die Form $B'$ einen Charakter $C_p$.

2. Zweitens sei $q$ eine ungerade Primzahl $p$, welche in $b$ aufgeht und mithin zu $\Delta$ relativ prim ist. Alsdann besitzt die Form $B'$ keine Charaktere $C_p$, während die Form $\varphi'$ den einzigen Charakter $\left(\frac{\varphi_{n-2}'}{p}\right)$ liefert, welcher wegen der Kongruenz (63) den Wert $\left(\frac{-(-1)^I \cdot o_1 \tau_{n-2}'}{p}\right)$ erhält.

3. Wenn drittens $q$ eine ungerade Primzahl $p$ ist, welche in $\Delta$ aufgeht und mithin zu $b$ relativ prim ausfällt, so stellt die Form $B'$ eine Grundform für den Modul $p$ vor, sobald wir für $\varphi'$ eine Grundform für diesen Modul genommen haben. Es besitzt die Form $\varphi'$ einen Charakter $\left(\frac{\varphi_h'}{p}\right)$, wenn die Invariante $e_h'$ durch $p$ teilbar ist, und die Form $B'$ einen Charakter $\left(\frac{B_h'}{p}\right)$, wenn die Invariante $o_h'$ durch $p$ teilbar ist. Nun ist

offenbar ein jedes $e_h'$ $(h \leqq n-2)$ dann und nur dann durch $p$ teilbar, wenn das zugehörige $o_h'$ durch $p$ teilbar wird. Demnach zieht ein jeder Charakter $\left(\frac{B_h'}{p}\right)$ einen bestimmten Charakter $\left(\frac{\varphi_h'}{p}\right)$ nach sich, und es sind diese beiden Charaktere wegen $\sigma_h' B_h' = \tau_h' \varphi_h'$ gegenseitig durcheinander bestimmt. Es muß ferner, wenn $o_{n-1}' \equiv 0 \pmod p$ wird, der Charakter $\left(\frac{B_{n-1}'}{p}\right)$ gleich $\left(\frac{(-1)^I \cdot \frac{b}{\sigma_1}}{p}\right)$ sein.

4. Endlich untersuchen wir die Charaktere für einen Modul $q^t = 2^t$.

I. Es möge zuerst $m \equiv 1 \pmod 2$ sein. Gehört dann die Form $\varphi'$ zu der Ordnung $O_I'(b)$, gelten sonach die Beziehungen $\sigma_h' = \tau_h'$ $(h \leqq n-2)$, so stimmen die Zahlen $\varphi_h'$ mit den entsprechenden Größen $B_h'$ überein, und es werden die Größen $\tau_{h-1}' e_h' \tau_{h+1}'$ $(h \leqq n-2)$ nur dann den Faktor 4 oder 8 enthalten, wenn die entsprechenden Größen $\sigma_{h-1}' o_h' \sigma_{h+1}'$ $(h \leqq n-2)$ durch 4 oder durch 8 teilbar sind. Infolgedessen wird jeder Charakter $C_4$, $C_8$, $\mathfrak{C}_4$ der Form $\varphi'$ gleich einem bestimmten Charakter $C_4$, $C_8$, $\mathfrak{C}_4$ der Form $B'$ sein. Außerdem wird, wie wir leicht bemerken, wenn $\sigma_{n-2}' o_{n-1}' \equiv 0 \pmod 4$ ist, der Charakter $(-1)^{\frac{B_{n-1}'-1}{2}}$ gleich $(-1)^{\frac{(-1)^I \cdot \frac{b}{\sigma_1}-1}{2}}$, und wenn $\sigma_{n-2}' o_{n-1}' \equiv 0 \pmod 8$ ist, der Charakter $\left(\frac{2}{B_{n-1}'}\right)$ gleich $\left(\frac{2}{\frac{b}{\sigma_1}}\right)$. Ferner liefert, falls $\sigma_1 = 2$ ist, die Kongruenz (63) die Bedingung $-(-1)^I \cdot o_1 \varphi_{n-2}' \equiv 1 \pmod 4$ oder

$$(-1)^{\frac{\varphi_{n-2}'-1}{2}} = (-1)^{\frac{-(-1)^I o_1 - 1}{2}}.$$

Wenn die Form $\varphi'$ der Ordnung $O_{II}'(b)$ angehört, so können wir ähnlich schließen, oder wir können auch auf die folgende Art vorgehen: Im Falle einer Ordnung $O_{II}'(b)$ ist jedenfalls $\sigma_1 = 1$ und $b = \delta \cdot \sigma_1 m \equiv 1 \pmod 2$. Infolgedessen können wir in diesem Falle die Zahlen $b_1$, $b_2$, $\ldots$, $b_{n-1}$ sämtlich kongruent Null $(\mathrm{mod}\ 2^{\omega_1' + \omega_2' + \cdots + \omega_{n-1}'} = 2^{\nu_n'-1})$ annehmen. Alsdann werden wegen der Gleichungen

$$-b\,b' = \sum_{i=1}^{n-1} b_{n-i} b_i' - \prod_{h=1}^{n-1} o_h, \quad -b b_k' = \sum_{i=1}^{n-1} b_{n-i} b_{ik}'$$

auch die Zahlen $b'$, $b_1'$, $b_2'$, $\ldots$, $b_{n-1}'$ durch $2^{\nu_n'-1}$ teilbar sein. Daraus erhellt, daß für jede ganze Zahl $z'$ die Kongruenz $B' \equiv z' \pmod{2^{\nu_n'-1}}$ genau $2^{\nu_n'-1}$ mal soviel Lösungen besitzen wird als die Kongruenz $\varphi' \equiv z' \pmod{2^{\nu_n'-1}}$. Nun können nach Kap. IX, wie wir wissen, die Charaktere der Form $B'$ und die der Form $\varphi'$ für die Moduln $2^t$ aus den Anzahlen

der Lösungen der verschiedenen Kongruenzen $B' \equiv z' \pmod{2^{v'_n-1}}$ und $\varphi' \equiv z' \pmod{2^{v'_n-1}}$ hergeleitet werden. Es sind daher in dem vorliegenden Falle wirklich die Charaktere der beiden Formen $\varphi'$ und $B'$ für die Moduln $2^t$ gegenseitig durcheinander gegeben.

II. Es möge endlich $m \equiv 0$, $\Delta \equiv 1 \pmod 2$ sein. Die Form $\varphi'$ besitzt dann, falls $\sigma_1 b \equiv 0 \pmod 4$ ist, einen Charakter $(-1)^{\frac{\varphi'_{n-2}-1}{2}}$, welcher infolge der Kongruenz (63) den Wert $(-1)^{\frac{-(-1)^I o_1 - 1}{2}}$ besitzt, und falls $\sigma_1 b \equiv 0 \pmod 8$ ist, einen Charakter $\left(\frac{2}{\varphi'_{n-2}}\right)$, welcher wegen (63) gleich $\left(\frac{2}{o_1}\right)$ ist. Alle übrigen Charaktere der Form $\varphi'$ für die Moduln $2^t$ können durch diese Einheiten $(-1)^{\frac{\varphi'_{n-2}-1}{2}}$ und $\left(\frac{2}{\varphi'_{n-2}}\right)$ und durch Charaktere $C_p$ ausgedrückt werden.

## Kap. XIX. Über den Inbegriff der Darstellungen einer ganzen Zahl durch die verschiedenen Formen eines Genus $G$.

Bekanntlich gibt es nur eine endliche Anzahl von Formenklassen, welche dieselbe Determinante $\Delta$ und denselben Index $I$ aufweisen. Da nun die Formen, welche einem und demselben Genus angehören, gewiß dieselbe Determinante und denselben Index besitzen, so wird infolgedessen auch ein jedes Genus nur eine endliche Anzahl verschiedener Klassen besitzen.

Es sei ein bestimmtes Genus $G$ von Formen gegeben; wir greifen aus jeder seiner Klassen irgendeinen Repräsentanten heraus. Wenn das Genus $G$ sich im ganzen aus $g$ verschiedenen Formenklassen zusammensetzt, bekommen wir auf diese Weise $g$ untereinander nicht-äquivalente Formen $f_1, f_2, \ldots, f_g$, und es ist klar, daß eine jede Form des Genus $G$ einer und nur einer dieser $g$ Formen äquivalent ist. Daher wird das System dieser $g$ Formen $f_1, f_2, \ldots, f_g$ ein *vollständiges Formensystem* für das Genus $G$ genannt. Man erkennt leicht, daß die den Formen $f_1, f_2, \ldots, f_g$ adjungierten Formen $f_1', f_2', \ldots, f_g'$ ein vollständiges Formensystem für das dem Genus $G$ adjungierte Genus $G'$ bilden.

Bezeichnen wir durch $\sigma_1 \varphi_1$ irgendeine durch Formen $f$ des Genus $G$ darstellbare ganze Zahl, für welche $\varphi_1$ zu $\Delta$ relativ prim ausfällt. Eine jede andere Zahl $b$, welche ebenfalls durch Formen $f$ des Genus $G$ darstellbar ist, muß alsdann einer bestimmten Kongruenz von der Form $b \equiv \sigma_1 \varphi_1 Z^2 \pmod{\sigma_0 o_1 \sigma_2}$ Genüge leisten. Es liege eine solche Zahl $b = \delta \cdot \sigma_1 m$ vor, für welche $m$ zu $\Delta$ relativ prim ist, und wir wollen die Gesamtheit der primären Darstellungen dieser Zahl $b$ durch die ver-

schiedenen Formen $f$ eines vollständigen Formensystems des Genus $G$ betrachten.

Erinnern wir uns, daß wir in Kap. XVIII für jede Zahl $b = \delta \cdot \sigma_1 m$ ($m$ relativ prim zu $\Delta$) ein bestimmtes Genus $G'_I(b)$, und falls $\sigma_1 = 1$, $m \equiv \varkappa_1 \equiv 1 \pmod 2$, $\varkappa_1 > 1$ oder $\sigma_1 = 1$, $m \equiv \varkappa_1 \equiv 0 \pmod 2$, $\varkappa_1 > 2$ ist, außerdem ein bestimmtes Genus $G'_{II}(b)$ definiert haben. Wir verschaffen uns jetzt ein vollständiges System von Formen $\varphi'$ für das Genus $G'_I(b)$ und, falls das Genus $G'_{II}(b)$ zulässig ist, auch für das Genus $G'_{II}(b)$. Alsdann wird jeder primären Darstellung der Zahl $b$ durch eine der Formen $f$ eine einzige Gruppe von Darstellungen einer einzigen dieser Formen $\varphi'$ durch eine der Formen $f'$ adjungiert sein. Wir erhalten mithin sämtliche möglichen primären Darstellungen der Zahl $b$ durch die $f$, indem wir für jede der Formen $\varphi'$ die sämtlichen nicht-äquivalenten Gruppen von Darstellungen durch die Formen $f'$ aufsuchen. Für eine bestimmte Form $\varphi' = \{b'_{ik}\}$ kann dies auf folgende Weise geschehen:

Wir denken uns der Einfachheit halber $\varphi'$ so angenommen, daß die ihr adjungierte Form $\varphi = \delta \cdot \{c_{ik}\}$ einen Hauptrest für den Modul $b$ vorstellt, und bezeichnen durch $(-1)^I \cdot \delta \tau'_{n-2} \varphi'_{n-2}$ den ersten Koeffizienten dieser Form $\varphi$. Infolge der besonderen Wahl des Genus $G'_I(b)$ oder zutreffendenfalls des Genus $G'_{II}(b)$ ist gewiß die Kongruenz

$$-(-1)^I \cdot o_1 \tau'_{n-2} \varphi'_{n-2} \equiv \tilde{b}_0^{\,2} \pmod{\sigma_1 b}$$

auflösbar, und wir schließen hieraus mittels der in Kap. XVIII gegebenen Sätze sofort, daß auch die $\frac{n(n-1)}{2}$ Kongruenzen

$$-o_1 c_{ik} \equiv b_i b_k \pmod b \tag{50}$$

lösbar sein werden. Es sei N die Anzahl der sämtlichen inkongruenten Lösungen $(b_1, b_2 \ldots, b_{n-1}) \pmod b$ dieser Kongruenzen. Enthält der Modul $b$ genau $\mu$ verschiedene ungerade Primzahlen, so ist die Zahl N, wie wir sahen, gleich $2^\mu$, wenn $b \equiv 1 \pmod 2$ oder $b \equiv 2 \pmod 4$ ist, gleich $2^{\mu+1}$, wenn $b \equiv 4 \pmod 8$ ist, und gleich $2^{\mu+2}$, wenn $b \equiv 0 \pmod 8$ ist. Eine jede Gruppe von eigentlichen Darstellungen der Form $\varphi'$ durch eine der Formen $f'_1, f'_2, \ldots, f'_g$ muß jetzt zu einem und nur zu einem dieser N inkongruenten Lösungssysteme $(b_1, b_2, \ldots, b_{n-1}) \pmod b$ der Kongruenzen (50) gehören. Um die Darstellungen von $\varphi'$ zu finden, welche zu einer bestimmten dieser N Wurzeln $(b_1, b_2, \ldots, b_{n-1})$ gehören, können wir folgendermaßen vorgehen:

Wir setzen

$$\frac{o_1 c_{ik} + b_i b_k}{b} = b_{ik}$$

und

$$B = b\xi^2 + 2\sum_{i=1}^{n-1} b_i \xi \xi_i + \sum_{i,k=1}^{n-1} b_{ik} \xi_i \xi_k.$$

Da wir gezeigt haben, daß der Index, die Invarianten und die Charaktere des Genus $G'$ auf eindeutig bestimmte Weise durch den Index, die Invarianten und die Charaktere des Genus $G'_I(b)$ oder des Genus $G'_{II}(b)$ dargestellt werden können, muß jetzt das Genus der Form $B$ mit dem gegebenen Genus $G$ identisch sein. Daher besitzt die der Form $B$ adjungierte Form die Gestalt

$$B' = \sum_{i,k=1}^{n-1} b'_{ik}\xi'_i\xi'_k + 2\sum_{i=1}^{n-1} b'_i\xi'_i\xi' + b'\xi'^2$$

und gehört dem Genus $G'$ an. Diese Form $B'$ wird daher einer und nur einer der $g$ Formen $f'_1, f'_2, \ldots, f'_g$ äquivalent sein, die wir mit $f'$ bezeichnen wollen. Es gibt dann keine Darstellung von $\varphi'$ durch eine der übrigen $g-1$ von $f'$ verschiedenen Formen $f'_k$, welche zu der Wurzel $(b_h)$ gehört. Dagegen sind wohl Darstellungen von $\varphi'$ durch die Form $f'$ vorhanden, welche zu der Wurzel $(b_h)$ gehören, und es liefert eine jede Substitution

$$(t'): \quad x'_i = \sum_{k=1}^{n-1} \vartheta'^{k}_{i}\xi'_k + t'_i\xi' \qquad (i = 1, 2, \ldots, n)$$

von der Determinante 1, welche die Form $f'$ in $B'$ verwandelt, eine derartige Darstellung

$$(\vartheta'): \quad x'_i = \sum_{k=1}^{n-1} \vartheta'^{k}_{i}\xi'_k \qquad (i = 1, 2, \ldots, n)$$

der Form $\varphi'$ durch $f'$. Ferner ist aus Kap. XVII bekannt, daß zwei verschiedene Transformationen $(t')$ von $f'$ in $B'$ stets zu zwei verschiedenen Darstellungen von $\varphi'$ durch $f'$ führen. Infolgedessen ist die Anzahl der sämtlichen verschiedenen Darstellungen von $\varphi'$ durch $f'$, welche zu der gegebenen Wurzel $(b_h)$ gehören, gleich der Anzahl der verschiedenen Substitutionen von der Determinante 1, welche die Form $f'$ in $B'$, oder, was auf dasselbe hinauskommt, welche die Form $f'$ in sich überführen.

Diese sämtlichen Darstellungen lassen sich dann in eine gewisse Anzahl $R$ nicht-äquivalenter Darstellungsgruppen verteilen. Eine jede dieser $R$ Gruppen enthält genau soviel verschiedene Darstellungen $(\vartheta')$, als man verschiedene Substitutionen von der Determinante 1 bilden kann, durch welche die Form $\varphi'$ in sich selbst übergeht. Den $R$ verschiedenen Gruppen von Darstellungen der Form $\varphi'$ durch $f'$ sind endlich $R$ verschiedene Darstellungen der Zahl $b$ durch die Form $f$ adjungiert, welche alle zu der Wurzel $(b_1, b_2, \ldots, b_{n-1})$ gehören.

## Kap. XX. Maß eines positiven Genus. — Maß der Darstellungen einer ganzen Zahl durch die Formen eines positiven Genus.

Wir wollen jetzt unsere weiteren Untersuchungen auf den Fall $I = 0$, d. i. auf den Fall positiver Formen $f$ und $f'$ beschränken. Die Anzahl der ganzzahligen Substitutionen von der Determinante 1, vermittels deren eine positive Form $f$ in sich selbst übergeführt werden kann, ist, wie man weiß, stets eine endliche. Wir bezeichnen diese Zahl durch $t(f)$. Die Größe $t(f)$ nimmt, wie man weiß, für alle Formen $f$ derselben Klasse den gleichen Wert an. Ferner erkennt man leicht, daß für zwei adjungierte Formen $f$ und $f'$ die Größen $t(f)$ und $t(f')$ gleich sind. In der Tat, wird die Form $f$ durch eine Substitution $S$ in sich selbst transformiert, so geht die Form $f'$ nach den in Kap. XII aufgestellten Sätzen durch die adjungierte Substitution $S'$ in sich selbst über.

Die Größe $\frac{1}{t(f)}$ heißt das *Maß* der Klasse $f$*). Bedeuten $f_1, f_2, \ldots, f_g$ verschiedene Formenklassen, so wird die Summe der Maße

$$\frac{1}{t(f_h)} \; (h = 1, 2, \ldots, g)$$

der einzelnen Formen $f_h$ das Maß des Klassensystems $f_1, f_2, \ldots, f_g$ genannt. Zum Beispiel ist das Maß eines Genus $G$ die Summe der Maße aller in diesem Genus enthaltenen Klassen und das Maß einer Ordnung $O$ die Summe der Maße aller in dieser Ordnung enthaltenen Klassen. Hiernach ist das Maß einer Ordnung $O$ gleich der Summe der Maße der sämtlichen in dieser Ordnung enthaltenen Genera $G$.

Durch eine positive Form $f$ können nur positive Zahlen $b$ dargestellt werden, und durch eine positive Form $f'$ können nur positive Formen $\varphi'$ dargestellt werden.

Wenn eine Zahl $b$ vermittels eines Systems $x_i = t_i$ durch eine Form $f$ dargestellt wird, so wird die Größe $\frac{1}{t(f)}$ als das *Maß* dieser Darstellung bezeichnet. Wenn mehrere Darstellungen $(t)$ einer oder mehrerer Zahlen $b$ durch eine oder mehrere Formen $f$ vorliegen, so wird die Summe der Maße aller dieser einzelnen Darstellungen $(t)$ das Maß des ganzen vorliegenden Systems von Darstellungen genannt. Hat man beispielsweise $R$ verschiedene Darstellungen derselben Zahl $b$ durch dieselbe Form $f$, so wird $\frac{R}{t(f)}$ das Maß dieser Darstellungen sein.

Wir betrachten jetzt wieder den Inbegriff der sämtlichen primären Darstellungen einer Zahl $b = \delta \cdot \sigma_1 m [\equiv \sigma_1 \varphi_1 Z^2 \pmod{\sigma_0 o_1 \sigma_2}$, $m$ relativ prim zu $\Delta]$ durch ein vollständiges System von Formen $f_1, f_2, \ldots, f_g$ eines

*) Eisenstein, Crelles Journal, Bd. 35. [[Math. Abhandlungen, S. 180.]]

Genus $G$. Aber wir wollen jetzt die Zahl $b$ und das Genus $G$ als positiv voraussetzen ($\delta = 1$, $I = 0$). Es sei wiederum $\varphi'$ irgend eine Form aus dem Genus $G'_I(b)$ oder auch, falls $\sigma_1 = 1$, $m \equiv \varkappa_1 \equiv 1 \pmod 2$, $\varkappa_1 > 1$ oder $\sigma_1 = 1$, $m \equiv \varkappa_1 \equiv 0 \pmod 2$, $\varkappa_1 > 2$ ist, aus dem Genus $G'_{II}(b)$, und es bedeute $\varphi = \{c_{ik}\}$ die zu $\varphi'$ adjungierte Form. Aus jeder Lösung der $\frac{n(n-1)}{2}$ Kongruenzen

$$-\sigma_1 c_{ik} \equiv b_i b_k \pmod b \tag{50}$$

entspringen (nach Kap. XIX) $R = \frac{t(f')}{t(\varphi')}$ verschiedene Darstellungen der Zahl $b$ durch eine bestimmte Form $f$ aus der Reihe der $g$ Formen $f_1, f_2, \ldots, f_g$. Für das Maß $M_0$ dieser $R$ Darstellungen erhält man daher

$$M_0 = \frac{t(f')}{t(\varphi')} \cdot \frac{1}{t(f)} = \frac{1}{t(\varphi')}.$$

Die Größe $M_0$ ist also gleich dem Maße der Form $\varphi'$ und fällt demnach unabhängig von der besonderen Form $f$ aus. Infolgedessen liefert jede der verschiedenen Wurzeln $(b_1, b_2, \ldots, b_{n-1})$ der Kongruenzen (50) ein gleiches Maß von Darstellungen der Zahl $b$ durch die Formen des Genus $G$. Es ist dieses eben derjenige Umstand, durch welchen die Einführung des Maßbegriffes der Formen und Darstellungen eine so hohe Bedeutung gewinnt. Das Maß aller Darstellungen von $b$, welche zu den $\mathsf{N}$ verschiedenen Wurzeln der Kongruenzen (50) gehören, wird nun offenbar gleich $\frac{\mathsf{N}}{t(\varphi')}$, d. i. gleich dem $\mathsf{N}$-fachen Maße der Form $\varphi'$. Demgemäß wird dann das Maß aller derjenigen Darstellungen von $b$, welche aus den verschiedenen Klassen $\varphi'$ des Genus $G'_I(b)$ oder zutreffendenfalls des Genus $G'_{II}(b)$ entspringen, gleich dem $\mathsf{N}$-fachen Maße aller Formenklassen des Genus $G'_I(b)$, resp. des Genus $G'_{II}(b)$, d. i. gleich dem $\mathsf{N}$-fachen Maße des Genus $G'_I(b)$, resp. des Genus $G'_{II}(b)$. Wir gewinnen dadurch den folgenden Satz:

Das Maß aller primären Darstellungen einer Zahl $b = \sigma_1 m$ ($m$ relativ prim zu $\Delta$) durch die verschiedenen Formen $f$ des Genus $G$ ist im allgemeinen gleich dem $\mathsf{N}$-fachen Maß des Genus $G'_I(b)$ und im besonderen, wenn $\sigma_1 = 1$, $m \equiv \varkappa_1 \pmod 2$, $\varkappa_1 > 2$ wird, gleich dem $\mathsf{N}$-fachen Maß der beiden Genera $G'_I(b)$ und $G'_{II}(b)$.

## Kap. XXI. Über die Anzahl der Darstellungen einer ganzen Zahl durch eine Summe von fünf Quadraten.

Die Anwendung des zuletzt gewonnenen Resultates auf den Fall $n = 5$, $\Delta = 1$ verschafft uns einige interessante Sätze über die Darstellung von ganzen Zahlen durch eine Summe von fünf Quadraten.

Bekanntlich bilden die positiven Formen mit fünf Variablen von der Determinante 1 eine einzige Formenklasse, welche durch die Form

$$f = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2$$

repräsentiert werden kann. Diese Form $f$ gehört dem einzigen Geschlecht $G$ der Ordnung

$$O: \begin{pmatrix} \sigma_1 = 1, & \sigma_2 = 1, & \sigma_3 = 1, & \sigma_4 = 1 \\ o_1 = 1, & o_2 = 1, & o_3 = 1, & o_4 = 1 \end{pmatrix}, \quad I = 0$$

an, und sie repräsentiert zugleich, da alle Formen dieses Genus die Determinante 1 besitzen müssen, die einzige Klasse dieses Genus.

Der Form $f$ ist die Form

$$f' = x_1'^2 + x_2'^2 + x_3'^2 + x_4'^2 + x_5'^2$$

adjungiert, welche mit $f$ identisch ist. Das Maß der Klassen $f$ und $f'$ oder des Genus $G$ ist, wie man ohne weiteres erkennt, gleich

$$\frac{1}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 2^4} = \frac{1}{2^7 \cdot 3 \cdot 5} = \frac{1}{1920} = \frac{1}{M_5}.$$

Bezeichnen wir für einen Augenblick die Anzahl der sämtlichen Systeme $x_i$ ohne gemeinsamen Teiler, welche einer Gleichung $f(x_i) = m$ genügen, mit $(m)_5$, so ist das Maß der eigentlichen Darstellungen einer Zahl $m$ durch eine Form des Genus $G$ gleich $\frac{(m)_5}{M_5}$. Da $\Delta = 1$ ist, so wird eine jede beliebige Zahl $m$ zu $\Delta$ relativ prim, und es können die Größen $\frac{(m)_5}{M_5}$ nach dem in Kap. XX bewiesenen Satze durch das Maß des einen Genus $G_I'(m)$ oder der beiden Genera $G_I'(m)$ und $G_{II}'(m)$ von Formen mit vier Variablen ausgedrückt werden. Wir haben infolgedessen, um zu einer Kenntnis der Größen $(m)_5$ zu gelangen, nur die Maße dieser Genera aufzusuchen.

Die Form $f$ ist ein Hauptrepräsentant für den Modul 2; es ist $\sigma_1 = 1$ und $\varkappa_1 = 5 \equiv 1 \pmod 2$. Wir müssen demnach für eine Zahl $m$ die Darstellungen $x_i = t_i$, in welchen die fünf Zahlen $t_i$ nicht alle ungerade sind, und die Darstellungen $x_i = t_i$, in welchen $t_1 \equiv t_2 \equiv t_3 \equiv t_4 \equiv t_5 \equiv 1 \pmod 2$ ist, voneinander unterscheiden. Die Darstellungen $(t)$ der ersten Art sind mit Darstellungen von primitiven Formen $\varphi'$ des Genus

$$G_I'(m): \begin{pmatrix} \tau_1' = 1, & \tau_2' = 1, & \tau_3' = 1 \\ e_1' = 1, & e_2' = 1, & e_3' = m \end{pmatrix}, \quad J' = 0; \quad -\varphi_3' \equiv X^2 \pmod m$$

adjungiert, während die Darstellungen $(t)$ der zweiten Art mit Darstellungen primitiver Formen $\varphi'$ des Genus

$$G_{II}'(m): \begin{pmatrix} \tau_1' = 2, & \tau_2' = 1, & \tau_3' = 2 \\ e_1' = 1, & e_2' = 1, & e_3' = m \end{pmatrix}, \quad J' = 0; \quad -2\varphi_3' \equiv X^2 \pmod m$$

adjungiert sind. Bezeichnet N die Anzahl der Lösungen der Kongruenz

$X^2 \equiv 1 \pmod{m}$, so ist infolgedessen die Anzahl $(m)_5^1$ der Darstellungen erster Art gleich dem $M_5 \cdot \mathsf{N}$-fachen Maße des Genus $G_I'(m)$ und die Anzahl $(m)_5^2$ der Darstellungen zweiter Art gleich dem $M_5 \cdot \mathsf{N}$-fachen Maße des Genus $G_{II}'(m)$.

Wie man leicht erkennt, gibt es für eine Zahl $m$ nur dann Darstellungen $(t)$ der zweiten Art, wenn $m \equiv 5 \pmod 8$ ist. Denn die Kongruenzen $t_i \equiv 1 \pmod 2$ $(i = 1, 2, 3, 4, 5)$ ergeben unmittelbar $t_i^2 \equiv 1 \pmod 8$ und $m = \sum_{i=1}^{5} t_i^2 \equiv 5 \pmod 8$. — Die in Kap. XI aufgestellten Bedingungen für die Existenz eines Genus lassen erkennen, daß das Genus $G_I'(m)$ für jede Zahl $m$ und das Genus $G_{II}'(m)$ nur für ein $m \equiv 5 \pmod 8$ Formen enthält. Es wird demnach eine jede Zahl $m$ als eine Summe von fünf beliebigen Quadraten darstellbar sein, während nur die Zahlen $m \equiv 5 \pmod 8$ sich als eine Summe von fünf ungeraden Quadraten darstellen lassen.

---

Alle Darstellungen einer Zahl $m$ durch eine Summe von fünf Quadraten, bei welchen die fünf einzelnen Quadrate abgesehen von ihrer Reihenfolge und den Vorzeichen ihrer Wurzeln $x_i$ miteinander übereinstimmen, fassen wir als eine einzige *Zerfällung* der Zahl $m$ in eine Summe von fünf Quadraten zusammen. Bezeichnen wir die Anzahl der Zerfällungen einer Zahl $m$ in eine Summe von fünf Quadraten durch $D_5$, die Anzahl der sämtlichen Darstellungen von $m$ durch eine Summe

$$n_1 x_1^2 + n_2 x_2^2 + \cdots + n_\nu x_\nu^2 \quad (n_1 + n_2 + \cdots + n_\nu \leqq 5)$$

durch $R(n_1, n_2, \ldots, n_\nu)$, so gilt die Relation

$$\begin{aligned} D_5 = {} & \tfrac{1}{3840} R(1,1,1,1,1) + \tfrac{1}{192} R(1,1,1,2) + \tfrac{1}{768} R(1,1,1,1) \\ & + \tfrac{1}{48} R(1,1,3) + \tfrac{1}{64} R(1,2,2) + \tfrac{1}{64} R(1,1,2) + \tfrac{1}{128} R(1,1,1) \\ & + \tfrac{1}{16} R(1,4) + \tfrac{5}{48} R(2,3) + \tfrac{1}{24} R(1,3) + \tfrac{1}{64} R(2,2) + \tfrac{3}{64} R(1,2) \\ & + \tfrac{5}{128} R(1,1) - \tfrac{1}{40} R(5) + \tfrac{1}{16} R(4) + \tfrac{1}{64} R(2) + \tfrac{35}{256} R(1). \end{aligned}$$

## Kap. XXII. **Über die Bestimmung des Maßes einiger positiver Genera.**

Unter Anwendung der von Dirichlet*) gegebenen Prinzipien können wir das Maß eines beliebigen Genus $G$ positiver Formen bestimmen. Ich wollte zeigen, worauf sich allgemein diese Bestimmung gründet; wegen der Kürze der Zeit muß ich mich jedoch darauf beschränken, in dem

*) Dirichlet, Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres, Crelles Journal, Bd. 19 und 21. [[Werke, Bd. I.]]

Folgenden nur die Maße einiger spezieller Genera mit drei und vier Variablen zu betrachten.

I. Wir gehen dabei aus von Summen der Form

$$S = \sum_{x_i} \frac{1}{\{f(x_i)\}^{\frac{n}{2}(1+\varrho)}}, \qquad (n \geqq 2)$$

in welchen $f(x_i)$ eine beliebige positive Form von einer Determinante $\Delta > 0$ und $\varrho$ eine beliebige positive Größe bedeutet, und in welchen die Variablen $x_1, x_2, \ldots, x_n$ Systeme von $n$ ganzen, nicht sämtlich verschwindenden Zahlen durchlaufen sollen.

1. Es sei $N$ eine ganze positive Zahl und $\alpha_1, \alpha_2, \ldots, \alpha_n$ irgendwelche $n$ Reste für diesen Modul $N$. Wir wollen zunächst für die Größen $x_1, x_2, \ldots, x_n$ alle Systeme von ganzen Zahlen einsetzen, welche nach dem Modul $N$ die Reste $\alpha_1, \alpha_2, \ldots, \alpha_n$ lassen, das sind alle Systeme von der Gestalt

$$(x) \qquad x_i = Nv_i + \alpha_i, \qquad (v_i = -\infty, \cdots, -1, 0, 1, \cdots, +\infty)$$

(wobei das System $x_1 = 0, x_2 = 0, \ldots, x_n = 0$, falls es gleichfalls von der Form $Nv_i + \alpha_i$ $(i = 1, 2, \ldots, n)$ ist, stets ausgeschlossen wird). Da die Form $f$ positiv ist, so nimmt für jedes einzelne dieser Wertesysteme $(x)$ der Ausdruck $\{f(x_1, x_2, \ldots, x_n)\}^{\frac{n}{2}}$ einen positiven und von Null verschiedenen Wert an. Wir wollen die Anzahl aller derjenigen unter diesen Systemen, für welche die Größe $\{f(x_i)\}^{\frac{n}{2}}$ nicht größer ausfällt als eine positive Größe $t$, durch $\tau$ bezeichnen. Anstelle der Ungleichung

$$\left(\sum_{i,k=1}^{n} a_{ik} x_i x_k\right)^{\frac{n}{2}} \leqq t$$

können wir schreiben

$$\sum_{i,k=1}^{n} a_{ik} \frac{x_i}{t^{\frac{1}{n}}} \frac{x_k}{t^{\frac{1}{n}}} \leqq 1,$$

oder, indem wir

$$\xi_i = \frac{x_i}{Nt^{\frac{1}{n}}} = \frac{1}{t^{\frac{1}{n}}} v_i + \frac{\alpha_i}{Nt^{\frac{1}{n}}}; \qquad a_{ik} N^2 = A_{ik}$$

setzen, auch

$$\sum_{i,k=1}^{n} A_{ik} \xi_i \xi_k \leqq 1.$$

Der Grenzwert des Verhältnisses $\frac{\tau}{t}$ für ein unendlich wachsendes $t$ wird nach einem bekannten Satze von Dirichlet gleich dem $n$-fachen Integral

$$J = \int\int \cdots \int d\xi_1 d\xi_2 \cdots d\xi_n,$$

in welchem die Variablen $\xi_i$ alle diejenigen Wertsysteme zu durchlaufen haben, für welche die Ungleichung

$$\sum_{i,k=1}^{n} A_{ik}\xi_i\xi_k \leqq 1$$

erfüllt ist. Dieses Integral erhält nach Dirichlet den Wert

$$J = \frac{1}{|A_{ik}|^{\frac{1}{2}}} \cdot \frac{\left\{\Gamma\left(\frac{1}{2}\right)\right\}^n}{\Gamma\left(1+\frac{n}{2}\right)},$$

in welchem $|A_{ik}|$ die aus den $n^2$ Größen $A_{ik}$ gebildete Determinante bedeutet. Diese Determinante ist wegen $A_{ik} = a_{ik}N^2$ gleich $|a_{ik}|N^{2n} = \Delta \cdot N^{2n}$. Ferner wird bekanntlich die Größe $\Gamma\left(\frac{1}{2}\right) = \pi^{\frac{1}{2}}$, während $\Gamma\left(1+\frac{n}{2}\right)$, je nachdem $n$ gerade oder ungerade ist, den Wert

$$1 \cdot 2 \cdot 3 \cdots \frac{n}{2} = \frac{n}{2} \cdot \frac{n-2}{2} \cdots \frac{4}{2} \cdot \frac{2}{2}$$

oder den Wert

$$\frac{1}{2} \cdot \frac{3}{2} \cdot \frac{5}{2} \cdots \frac{n}{2}\Gamma\left(\frac{1}{2}\right) = \pi^{\frac{1}{2}} \cdot \frac{n}{2} \cdot \frac{n-2}{2} \cdots \frac{3}{2} \cdot \frac{1}{2}$$

annimmt. Wir können mithin

$$\frac{\left\{\Gamma\left(\frac{1}{2}\right)\right\}^n}{\Gamma\left(1+\frac{n}{2}\right)} = \pi^{\left[\frac{n}{2}\right]} : \prod_{h=0}^{\left[\frac{n-1}{2}\right]} \left(\frac{n-2h}{2}\right) = e_n$$

setzen, und wir bekommen

$$J = e_n \cdot \frac{\Delta^{-\frac{1}{2}}}{N^n}.$$

Der Grenzwert des Quotienten $\frac{\tau}{t}$ für ein unendlich abnehmendes $\frac{1}{t^{\frac{1}{n}}}$ ist hiernach endlich.

Infolge dieses Umstandes konvergiert nach einem weiteren Satze von Dirichlet die unendliche Reihe

$$S = \sum \frac{1}{[f(x_i)]^{\frac{n}{2}(1+\varrho)}} \qquad \begin{pmatrix} x_i = Nv_i + \alpha_i,\ v_i = -\infty, \cdots, -1, 0, 1, \cdots, +\infty \\ (x_1, x_2, \ldots, x_n) \neq (0, 0, \ldots, 0) \end{pmatrix}$$

für ein jedes positive $\varrho$, und es wird der Grenzwert von $\varrho \cdot S$ für ein positives unendlich abnehmendes $\varrho$ gleich

$$\lim_{\varrho = 0} (\varrho \cdot S) = J = e_n \cdot \frac{\Delta^{-\frac{1}{2}}}{N^n}.$$

Ist der Modul $N$ gleich 1, so haben die Variablen $x_i$ alle möglichen Systeme von ganzen Zahlen mit Ausnahme des einen $x_1 = 0, x_2 = 0, \ldots, x_n = 0$

zu durchlaufen, und der Limes von $\varrho \cdot S$ nimmt seinen größten Wert $e_n : \sqrt{\Delta}$ an.

2. Wir wollen jetzt annehmen, daß der größte gemeinsame Teiler der $n$ Zahlen $\alpha_i$ zu $N$ relativ prim wird, und wir wollen den $n$ Größen $v_i$ nur solche ganzzahligen Werte erteilen, für welche die $n$ Zahlen $x_i = Nv_i + \alpha_i$ ohne gemeinsamen Teiler ausfallen. Anstatt der Summe $S$ erhalten wir dann eine kleinere Summe $S_0$.

Bezeichnen wir die verschiedenen in $N$ aufgehenden Primzahlen durch $q_1, q_2, \ldots, q_M$ und setzen wir

$$S_n = \sum_{z=1}^{\infty} \frac{1}{z^n} = \frac{1}{1^n} + \frac{1}{2^n} + \frac{1}{3^n} + \cdots,$$

$$\varphi_n(N) = N^n \left(1 - \frac{1}{q_1^n}\right)\left(1 - \frac{1}{q_2^n}\right) \cdots \left(1 - \frac{1}{q_M^n}\right) = N^n (N)_n,$$

so wird der Grenzwert von $\varrho \cdot S_0$ für unendlich abnehmendes $\varrho$ gleich

$$\lim_{\varrho = 0} (\varrho \cdot S_0) = \frac{e_n}{S_n} \cdot \frac{\Delta^{-\frac{1}{2}}}{\varphi_n(N)}.$$

Wir bemerken, daß wir den hier auftretenden Ausdruck $\varphi_n(N)$ in ähnlicher Weise definieren können wie die speziellere Funktion

$$\varphi_1(N) = N\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) \cdots \left(1 - \frac{1}{q_M}\right).$$

Denn wir haben den Satz:

Lassen wir jede der $n$ Zahlen $\alpha_i$ die sämtlichen $N$ Werte $1, 2, \ldots, N$ durchlaufen, so gibt es unter den $N^n$ sich dabei ergebenden Systemen $\varphi_n(N)$ Systeme, für welche der größte Teiler der $n$ Größen $\alpha_1, \alpha_2, \ldots, \alpha_n$ zu $N$ relativ prim wird.

Man kann leicht die folgenden Relationen beweisen, in denen die Größe $m$ alle ganzen positiven und zu $N$ relativ primen Zahlen durchlaufen soll:

$$1 = \lim_{\varrho = 0} (\varrho S_{1+\varrho}) = \frac{N}{\varphi_1(N)} \lim_{\varrho = 0} \left(\varrho \sum_m \frac{1}{m^{1+\varrho}}\right); \quad S_n = \frac{N^n}{\varphi_n(N)} \cdot \sum_m \frac{1}{m^n} \quad (n > 1).$$

3. Wir leiten jetzt eine Umformung her, welche für die weiteren Untersuchungen wichtig ist. Wir wollen mit $m$ oder $m_0$ alle positiven und zu $N$ relativ primen ganzen Zahlen und mit $q', q'', \ldots, q^{(\mu)}$ die verschiedenen in einer Zahl $m$ aufgehenden Primzahlen bezeichnen. Es seien $\psi(m)$ und $\Psi(m)$ zwei Funktionen, welche den Bedingungen

$$\psi(m \cdot m_0) = \psi(m) \cdot \psi(m_0); \quad \Psi(m \cdot m_0) = \Psi(m) \cdot \Psi(m_0),$$

$$\psi(1) = 1, \; -1 \leqq \psi(q) \leqq 1; \quad \Psi(1) = 1, \; \Psi(q) = \pm \frac{1}{q^{1+\varrho}}$$

genügen.

Die über alle verschiedenen Zahlen $m$ ausgedehnte Summe

$$\sum = \sum_m \left\{ \prod_{k=1}^{\mu} (1 + \psi(q^{(k)})) \cdot \Psi(m) \right\}$$

ist für jedes positive $\varrho$ konvergent.

Indem wir die Zahlen $m$ in ihre verschiedenen Primzahlpotenzen $q^t$ zerlegen, erkennen wir, daß die Summe $\sum$ gleich dem über sämtliche in $N$ nicht aufgehenden Primzahlen $q$ ausgedehnten Produkt

$$\prod_q [1 + (1 + \psi(q))\Psi(q) + (1 + \psi(q))\Psi(q^2) + (1 + \psi(q))\Psi(q^3) + \cdots]$$

wird. Die Einzelglieder dieses Produktes sind wegen $\Psi(q^t) = [\Psi(q)]^t$ gleich

$$1 + \frac{(1 + \psi(q))\Psi(q)}{1 - \Psi(q)} = \frac{1 - [\psi(q) \cdot \Psi(q)]^2}{[1 - \Psi(q)]\,[1 - \psi(q) \cdot \Psi(q)]},$$

sodaß wir

$$\sum = \frac{\prod \frac{1}{1 - \Psi(q)} \cdot \prod \frac{1}{1 - \psi(q)\Psi(q)}}{\prod \frac{1}{1 - [\psi(q)\Psi(q)]^2}}$$

bekommen. Nun gilt, wenn man $\Phi = \Psi$ oder $= \psi \cdot \Psi$ oder $= \psi^2 \cdot \Psi^2$ nimmt, stets

$$\prod_q \frac{1}{1 - \Phi(q)} = \sum_m \Phi(m),$$

und hieraus geht sofort die Identität

$$\sum = \frac{\sum_m \Psi(m) \cdot \sum_m \psi(m)\Psi(m)}{\sum_m (\psi(m)\Psi(m))^2} \tag{64}$$

hervor.

II. ($n = 2$.) Bekanntlich haben zwei positive binäre Formen $f$, welche demselben Genus angehören, stets dasselbe Maß $\frac{1}{t(f)} \left( = \frac{1}{2} \text{ oder } = \frac{1}{4} \text{ oder } = \frac{1}{6} \right)$. Infolgedessen ist das Maß eines Genus $f$ von Formen mit zwei Variablen gleich der mit der Konstanten $\frac{1}{t(f)}$ multiplizierten Klassenanzahl dieses Genus und kann daher mit Hilfe der von Dirichlet aufgestellten Formeln bestimmt werden. So findet sich z. B., wenn $N$ irgendeine Zahl kongruent 1 (mod 4) ist und $P_1, P_2, \ldots, P_\nu$ die verschiedenen in $N$ aufgehenden Primzahlen sind, das Maß eines beliebigen Genus

$$\begin{pmatrix} \sigma_1 = 1 \\ o_1 = N \end{pmatrix}, \quad \left(\frac{\varphi}{P_k}\right) \qquad (k = 1, 2, \ldots, \nu)$$

gleich

$$\frac{1}{2^\nu} \sqrt{N} \cdot h(N),$$

wo

$$h(N) = \frac{1}{\pi} \sum_{m}' \left(\frac{-N}{m}\right) \frac{1}{m} \qquad (m \text{ rel. pr. zu } 2N)$$

ist $[h(N) > 0]$.

$(n = 3)$. Wir betrachten jetzt eine Ordnung

$$O\colon \begin{pmatrix} \sigma, & \sigma' \\ o, & o' \end{pmatrix}$$

von primitiven Formen mit drei Variablen. Dieser Ordnung wird die Ordnung

$$O'\colon \begin{pmatrix} \sigma', & \sigma \\ o', & o \end{pmatrix}$$

adjungiert sein.

Wir beschäftigen uns insbesondere mit dem Fall, in welchem die Invarianten $o$ und $o'$ alle beide ungerade sind. In diesem Falle wird $\sigma = 1$, $\sigma' = 1$; $o \equiv 1$, $o' \equiv 1 \pmod 2$. Wir bezeichnen die Primzahlen, welche in $o$ aufgehen, durch $t_1, t_2, \ldots, t_\vartheta$, die Primzahlen, welche in $o'$ aufgehen, durch $t_1', t_2', \ldots, t_{\vartheta'}'$, die Primzahlen, welche in $o$, aber nicht in $o'$ aufgehen, durch $p_1, p_2, \ldots, p_\delta$, die Primzahlen, welche in $o'$, aber nicht in $o$ aufgehen, durch $p_1', p_2', \ldots, p_{\delta'}'$, endlich die Primzahlen, welche sowohl in $o$ als in $o'$ aufgehen, durch $r_1 = r_1', r_2 = r_2', \ldots, r_\tau = r_{\tau'}' (\tau = \tau')$. Die Zahlen $t$ bestehen aus den Zahlen $p$ und den Zahlen $r$, die Zahlen $t'$ aus den Zahlen $p'$ und den Zahlen $r'$; mithin ist $\vartheta = \delta + \tau$, $\vartheta' = \delta' + \tau'$.

1. Es möge $\Phi$ eine in der Ordnung $O$ auftretende Grundform für den Modul $2oo'$ und $\Phi'$ ihre in der Ordnung $O'$ auftretende adjungierte Form sein. Setzen wir den ersten Koeffizienten von $\Phi$ gleich $\varphi$ und den ersten Koeffizienten von $\Phi'$ gleich $\varphi'$, so besitzen die Formen $\Phi$ und $\Phi'$ die $\vartheta + \vartheta'$ Charaktere

$$C(\varphi)\colon \left(\frac{\varphi}{p_1}\right), \left(\frac{\varphi}{p_2}\right), \ldots, \left(\frac{\varphi}{p_\delta}\right); \quad \left(\frac{\varphi}{r_1}\right), \left(\frac{\varphi}{r_2}\right), \ldots, \left(\frac{\varphi}{r_\tau}\right),$$

$$C'(\varphi')\colon \left(\frac{\varphi'}{p_1'}\right), \left(\frac{\varphi'}{p_2'}\right), \ldots, \left(\frac{\varphi'}{p_{\delta'}'}\right); \quad \left(\frac{\varphi'}{r_1'}\right), \left(\frac{\varphi'}{r_2'}\right), \ldots, \left(\frac{\varphi'}{r_{\tau'}'}\right),$$

welche der Gleichung

$$\left(\frac{\varphi}{o}\right) \cdot \left(\frac{\varphi'}{o'}\right) = (-1)^{\frac{\varphi-1}{2} \cdot \frac{\varphi'-1}{2} + \frac{o+1}{2} \cdot \frac{\varphi-1}{2} + \frac{o'+1}{2} \cdot \frac{\varphi'-1}{2}}$$

oder

$$(-1)^{\frac{o'\varphi+1}{2} \cdot \frac{o\varphi'+1}{2}} = (-1)^{\frac{o+1}{2} \cdot \frac{o'+1}{2}} \left(\frac{\varphi}{o}\right) \cdot \left(\frac{\varphi'}{o'}\right) = \mathsf{T}$$

genügen.

Wenn die Form $\Phi$ Hauptrepräsentant für einen Modul $N$ ist, so läßt sie sich schreiben

$$\Phi \equiv \begin{pmatrix} \varphi, & 0, & 0 \\ 0, & \frac{o\varphi'}{\varphi}, & 0 \\ 0, & 0, & \frac{oo'}{\varphi'} \end{pmatrix} \pmod N.$$

Indem wir $N = t$ oder $N = p'$ annehmen, erkennen wir hieraus leicht, daß die Anzahl der Lösungen der Kongruenz

$$\Phi(\xi_1, \xi_2, \xi_3) \equiv 0 \pmod t \quad \text{resp.} \quad \Phi(\xi_1, \xi_2, \xi_3) \equiv 0 \pmod{p'}$$

gleich

$$t^2 \quad \text{resp.} \quad p'^2 + \left(\frac{-o\varphi'}{p'}\right) p'(p'-1)$$

ist. Dementsprechend wird die Anzahl der nach einem Modul $t$ oder $p'$ inkongruenten Systeme $(\xi_1, \xi_2, \xi_3)$, für welche die Form $\Phi(\xi_1, \xi_2, \xi_3)$ zu $t$ resp. $p'$ relativ prim ausfällt, gleich

$$t^3\left(1 - \frac{1}{t}\right) \quad \text{resp.} \quad p'^3\left(1 - \frac{1}{p'}\right)\left[1 - \left(\frac{-o\varphi'}{p'}\right)\frac{1}{p'}\right].$$

Ist der Modul $N$ gleich 4, so hat die Anzahl der Lösungen $(\xi_1, \xi_2, \xi_3)$ (mod 4) der Kongruenz

$$\Phi(\xi_1, \xi_2, \xi_3) \equiv o' \pmod 4$$

den Wert $2^3(2-1)$ oder $2^3(2+1)$, je nachdem die Einheit

$$\mathsf{T} = (-1)^{\frac{o\varphi'+1}{2}\cdot\frac{o'\varphi+1}{2}}$$

gleich 1 oder gleich $-1$ ist. Unter diesen $2^3(2-\mathsf{T})$ Lösungen der Kongruenz $\Phi(\xi_i) \equiv o' \pmod 4$ befinden sich, wie man leicht erkennt, jedenfalls nicht die Systeme $\xi_1 \equiv 1$, $\xi_2 \equiv 1$, $\xi_3 \equiv 1 \pmod 2$. Denn für diese Systeme wird stets

$$\Phi(\xi_i) \equiv \varphi + \frac{o\varphi'}{\varphi} + \frac{oo'}{\varphi'} \equiv -o' \pmod 4.$$

2. Wir gehen jetzt zur Bestimmung des Maßes $M$ eines Genus

$$G: \begin{pmatrix} 1, & 1 \\ o, & o' \end{pmatrix}, \; C(\varphi), \; C'(\varphi')$$

über, in welchem die Charaktere $C(\varphi)$, $C'(\varphi')$ gegebene Werte (1 oder $-1$) besitzen. Wir bilden zunächst ein vollständiges Formensystem $\Phi_1, \Phi_2, \ldots, \Phi_K$ für das Genus $G$.

Eine zu $2oo'$ relativ prime, positive Zahl $m$, welche $\equiv o' \pmod 4$ ist, kann offenbar nur dann durch die Formen $\Phi$ dargestellt werden, wenn die Einheiten $C(m)$ gleich den gegebenen Charakteren $C(\varphi)$ sind. Sobald aber die sämtlichen Gleichungen $C(m) = C(\varphi)$ statthaben, wird, wenn wir annehmen, daß die Zahl $m$ die $\mu$ ungeraden Primzahlen $q_1, q_2, \ldots, q_\mu$ enthält, das Maß der eigentlichen Darstellungen von $m$ durch die Formen $\Phi$

gleich dem $2^{\mu}$-fachen Maße des Genus

$$\chi' : \left(\frac{1}{o'm}\right), \left(\frac{\chi'}{t'}\right) = \left(\frac{\varphi'}{t'}\right), \left(\frac{\chi'}{q}\right) = \left(\frac{-o}{q}\right),$$

d. i. gleich

$$\frac{1}{2^{\vartheta'}} \sqrt{o'm} \cdot h(o'm)$$

sein.

Wir bilden jetzt die Summe

$$\sum\nolimits_{\varrho} = \sum_{k=1}^{K} \left( \sum \frac{\{t(\Phi_k)\}^{-1}}{\{\Phi_k(\xi_1, \xi_2, \xi_3)\}^{\frac{3}{2}(1+\varrho)}} \right),$$

in welcher die Größen $\xi_1, \xi_2, \xi_3$ alle verschiedenen Systeme von ganzen Zahlen ohne gemeinsamen Teiler durchlaufen sollen, für welche $\Phi_k(\xi_1, \xi_2, \xi_3)$ zu $2oo'$ relativ prim und $\equiv o' \pmod 4$ ausfällt. Diese Systeme $\xi_1, \xi_2, \xi_3$ sind, wie sich aus dem in 1. über die Kongruenzen $\Phi \equiv 0 \pmod t$ oder $\pmod{p'}$ und $\Phi \equiv o' \pmod 4$ Bemerkten ergibt, in

$$\frac{1}{2}\left(1 - \frac{\mathsf{T}}{2}\right)(4oo')^3 (2oo')_1 \cdot \prod_{p'} \left[1 - \left(\frac{-o\varphi'}{p'}\right)\frac{1}{p'}\right]$$

arithmetischen Reihen

$$\xi_1 = 4oo' V_1 + \Xi_1, \quad \xi_2 = 4oo' V_2 + \Xi_2, \quad \xi_3 = 4oo' V_3 + \Xi_3$$

enthalten. Der Grenzwert von $\varrho \cdot \sum_{\varrho}$ für ein unendlich abnehmendes $\varrho$ wird infolgedessen gleich

$$L = \frac{\frac{1}{2}\left(1 - \frac{\mathsf{T}}{2}\right)(4oo')^3 \cdot (2oo')_1 \cdot \prod_{p'} \left[1 - \left(\frac{-o\varphi'}{p'}\right)\frac{1}{p'}\right] \cdot e_3 \cdot M}{\sqrt{o^2 o'}\,(4oo')^3 (2oo')_3 \cdot S_3}.$$

Jetzt können wir die Summe $\sum_{\varrho}$ nach den numerischen Werten der Zahlen $\Phi_k(\xi_1, \xi_2, \xi_3)$ ordnen, und wir bekommen dadurch einen Ausdruck

$$\sum\nolimits_{\varrho} = \sum \frac{\{m\}}{m^{\frac{3}{2}(1+\varrho)}}, \qquad \begin{pmatrix} m \text{ rel. pr. zu } 2oo'; \\ o'm \equiv 1 \pmod 4 \end{pmatrix}$$

in welchem die Funktionen $\{m\}$ die Maße der Darstellungen der Zahlen $m$ durch die sämtlichen Formen $\Phi$ bedeuten werden. Mithin können wir schreiben

$$\sum\nolimits_{\varrho} = \frac{1}{2^{\vartheta'}} \cdot \sum \frac{\sqrt{o'm} \cdot h(o'm)}{m^{\frac{3}{2}(1+\varrho)}} \qquad \begin{pmatrix} C(m) = C(\varphi) \\ o'm \equiv 1 \pmod 4 \end{pmatrix}$$

und

$$L = \lim_{\varrho = 0}\left(\varrho \sum\nolimits_{\varrho}\right) = \frac{1}{2^{\vartheta'}} \cdot \lim\left(\varrho \sum \frac{\sqrt{o'm} \cdot h(o'm)}{m^{\frac{3}{2}(1+\varrho)}}\right) \cdot \qquad \begin{pmatrix} C(m) = C(\varphi) \\ o'm \equiv 1 \pmod 4 \end{pmatrix}$$

Ein Vergleich der beiden für den Grenzwert $L$ gewonnenen Ausdrücke ergibt die Formel

$$\frac{\left(1-\frac{\mathsf{T}}{2}\right)(2oo')_1\cdot\prod_{p'}\left[1-\left(\frac{-o\varphi'}{p'}\right)\frac{1}{p'}\right]\cdot\prod_{p}\left[1-\left(\frac{-o'\varphi}{p}\right)\frac{1}{p}\right]\cdot M\cdot e_3}{2oo'\cdot(2oo')_3\cdot S_3}=$$

$$\frac{1}{2^{\vartheta'}}\cdot\lim\left(\varrho\sum\frac{\sqrt{m}\,h(o'm)\prod_{p}\left[1-\left(\frac{-o'm}{p}\right)\frac{1}{p}\right]}{m^{\frac{3}{2}(1+\varrho)}}\right)=$$

$$\frac{1}{2^{\vartheta'}}\cdot\lim\left(\varrho\sum\frac{\sqrt{m}\,h(o^2o'm)}{m^{\frac{3}{2}(1+\varrho)}}\right)\cdot$$

$$[o^2o'm\equiv 1\pmod 4;\quad C(m)=C(\varphi)]$$

Dieselbe verwandelt sich, indem wir

$$M=\frac{oo'}{2^{\vartheta+\vartheta'}}\cdot\prod_{p'}\left[1+\left(\frac{-o\varphi'}{p'}\right)\frac{1}{p'}\right]\cdot\prod_{p}\left[1+\left(\frac{-o'\varphi}{p}\right)\frac{1}{p}\right]\cdot$$

$$\cdot\prod_{r=r'}\left(1-\frac{1}{rr'}\right)\cdot\left(1+\frac{\mathsf{T}}{2}\right)\cdot M_0$$

setzen, in

$$(65)\quad\frac{(2oo')_1\cdot(2oo')_2\cdot e_3 M_0}{2^{\vartheta}\cdot(2oo')_3\cdot 2S_3}=\lim\left(\varrho\sum\frac{\sqrt{m}\,h(o^2o'm)}{m^{\frac{3}{2}(1+\varrho)}}\right)\cdot\begin{pmatrix}o^2o'm\equiv 1\pmod 4\\ C(m)=C(\varphi)\end{pmatrix}$$

Beachten wir nun, daß das Maß des Genus

$$G:\quad\begin{pmatrix}1, & 1\\ o, & o'\end{pmatrix},\ C(\varphi),\ C'(\varphi')$$

mit dem Maße des Genus

$$G':\quad\begin{pmatrix}1, & 1\\ o', & o\end{pmatrix},\ C'(\varphi'),\ C(\varphi)$$

übereinstimmt, so können wir sofort eine zweite Gleichung hinschreiben:

$$(65')\quad\frac{(2oo')_1\cdot(2oo')_2\cdot e_3 M_0}{2^{\vartheta'}\cdot(2oo')_3\cdot 2S_3}=\lim\left(\varrho\sum\frac{\sqrt{m'}\,h(o'^2om')}{m'^{\frac{3}{2}(1+\varrho)}}\right)\cdot\begin{pmatrix}o'^2om'\equiv 1\pmod 4\\ C'(m')=C'(\varphi')\end{pmatrix}$$

Wir ersehen jetzt aus der Gleichung (65), daß die Größe $M_0$ von den speziellen Charakteren $C'(\varphi')$ unabhängig ist, und aus der Gleichung (65'), daß die Größe $M_0$ von den speziellen Charakteren $C(\varphi)$ unabhängig ist. Die Größe $M_0$ kann daher nur von den beiden Invarianten $o$ und $o'$ abhängen.

3. Um den Wert von $M_0$ zu finden, können wir auf folgende Weise verfahren:

Bilden wir die Summe der Gleichungen (65) für die sämtlichen Genera der Ordnung $O$, welche die nämlichen Charaktere $C'(\varphi')$ besitzen, so ergibt sich die Gleichung

$$\frac{(2oo')_1\cdot(2oo')_2\cdot e_3 M_0}{(2oo')_3\cdot 2S_3}=\lim\left(\varrho\sum\frac{\sqrt{m}\,h(o^2o'm)}{m^{\frac{3}{2}(1+\varrho)}}\right)=\{o^2o'\},\ \begin{pmatrix}o^2o'm\equiv 1\,(\mathrm{mod}\,4)\\ m\text{ rel. pr. zu }o^2o'\end{pmatrix}$$

worin die Summation jetzt über alle zu $2o^2o'$ relativ primen Zahlen $m$, welche $\equiv o^2o' \pmod 4$ sind, auszudehnen ist. Ebenso erhalten wir aus der Gleichung (65′) die Relation

$$\frac{(2oo')_1 \cdot (2oo')_2 \cdot e_3 M_0}{(2oo')_3 \cdot 2S_3} = \lim\left(\varrho \sum \frac{\sqrt{m'}\, h(o'^2 o m')}{m'^{\frac{3}{2}(1+\varrho)}}\right) = \{o'^2 o\}, \quad \begin{pmatrix} o'^2 o m' \equiv 1 \pmod 4 \\ m' \text{ rel. pr. zu } o'^2 o \end{pmatrix}$$

worin die Summation über alle zu $2o'^2o$ relativ primen Zahlen $m'$, welche $\equiv o'^2 o \pmod 4$ sind, auszudehnen ist. Es ergibt sich demnach die Gleichung

$$\{o^2 o'\} = \{o'^2 o\}.$$

In dem Falle, daß eine der Invarianten $o, o'$ gleich 1 ist, gewinnen wir daraus insbesondere die Formel

$$\{D^2\} = \{D\}, \qquad [D \equiv 1 \pmod 2]$$

mit deren Hilfe wir dann noch

$$\{o^2 o'\} = \{o^4 o'^2\} = \{o^2 o'^2\} = \{oo'\}, \quad \{o'^2 o\} = \{o'^4 o^2\} = \{o'^2 o^2\} = \{o'o\};$$
$$\{o^2 o'\} = \{o'^2 o\} = \{oo'\}$$

bekommen.

Wir wollen jetzt die Größe

$$\{D\} = \lim\left(\varrho \sum_R \frac{\sqrt{R}\, h(DR)}{R^{\frac{3}{2}(1+\varrho)}}\right) \quad \begin{pmatrix} DR \equiv 1 \pmod 4 \\ R \text{ rel. pr. zu } 2D \end{pmatrix}$$

bestimmen. Es möge $r$ eine in der Größe $D$ nicht aufgehende ungerade Primzahl bedeuten. Wir zerlegen dann $\{D\}$, indem wir die Zahlen $R$ nach der höchsten in ihnen enthaltenen Potenz von $r$ ordnen, in eine Summe von Grenzwerten

$$\{D\} = \sum_{s=0}^{\infty} \{D; s\},$$

$$\{D; s\} = \lim\left(\varrho \sum_{R_0} \frac{\sqrt{R_0 r^s}\, h(D R_0 r^s)}{(R_0 r^s)^{\frac{3}{2}(1+\varrho)}}\right) = \frac{1}{r^s} \lim\left(\varrho \sum_{R_0} \frac{\sqrt{R_0}\, h(D R_0 r^s)}{R_0^{\frac{3}{2}(1+\varrho)}}\right).$$
$$[Dr^s R_0 \equiv 1 \pmod 4; \; R_0 \text{ rel. pr. zu } Dr]$$

Die hier auftretenden einzelnen Grenzwerte

$$\lim\left(\varrho \sum_{R_0} \frac{\sqrt{R_0}\, h(Dr^s R_0)}{R_0^{\frac{3}{2}(1+\varrho)}}\right)$$

sind, wenn $s > 0$ ist, gleich $\{Dr^s\} = \{Dr\}$. Ist aber $s = 0$, so können wir die Summe

$$\{D; 0\} = \lim\left(\varrho \sum_{R_0} \frac{\sqrt{R_0}\, h(D R_0)}{R_0^{\frac{3}{2}(1+\varrho)}}\right) \quad \begin{pmatrix} DR_0 \equiv 1 \pmod 4 \\ R_0 \text{ rel. pr. zu } Dr \end{pmatrix}$$

in zwei Partialsummen $L_+$ und $L_-$ zerlegen, indem wir alle diejenigen Glieder von $\{D; 0\}$, für welche $R_0$ quadratischer Rest von $r$ ist, in eine

Summe $L_+$ und alle diejenigen Glieder von $\{D; 0\}$, für welche $R_0$ quadratischer Nichtrest von $r$ ist, in eine Summe $L_-$ zusammenfassen. Jeder der beiden Grenzwerte $L_\varepsilon (\varepsilon = +1, -1)$ läßt sich schreiben

$$L_\varepsilon = \frac{1}{1 - \left(\frac{-D}{r}\right)\frac{\varepsilon}{r}} \lim \left( \varrho \sum_{R_0} \frac{\sqrt{R_0}\, h(DR_0)\left[1 - \left(\frac{-DR_0}{r}\right)\frac{1}{r}\right]}{R_0^{\frac{3}{2}(1+\varrho)}} \right)$$

$$= \frac{1}{1 - \left(\frac{-D}{r}\right)\frac{\varepsilon}{r}} \lim \left( \varrho \sum \frac{\sqrt{R_0}\, h(Dr^2 R_0)}{R_0^{\frac{3}{2}(1+\varrho)}} \right); \qquad \left[\left(\frac{R_0}{r}\right) = \varepsilon\right]$$

$$L_\varepsilon = \frac{1}{2} \cdot \frac{\{Dr^2\}}{1 - \left(\frac{-D}{r}\right)\frac{\varepsilon}{r}},$$

so daß sich

$$\{D; 0\} = L_+ + L_- = \frac{\{Dr\}}{1 - \frac{1}{r^2}}$$

ergibt. Demnach finden wir

$$\{D\} = \{Dr\}\left(\frac{1}{1 - \frac{1}{r^2}} + \frac{1}{r} + \frac{1}{r^2} + \cdots\right) = \{Dr\}\,\frac{1 - \frac{1}{r^3}}{\left(1 - \frac{1}{r}\right)\left(1 - \frac{1}{r^2}\right)},$$

d. i.

$$\text{für } s \geqq 1: \quad \{Dr^s\} = \{Dr\} = \{D\} \cdot \frac{(r)_1 \cdot (r)_2}{(r)_3}.$$

Durch eine wiederholte Anwendung dieser Formel gewinnen wir die Gleichung

(66) $$\{D\} = \{1\} \cdot \frac{(D)_1 \cdot (D)_2}{(D)_3}.$$

Die Relation

$$\frac{(2oo')_1 \cdot (2oo')_2\, e_3\, M_0}{(2oo')_3 \cdot 2S_3} = \{oo'\}$$

nimmt jetzt die Form an

$$M_0 = \frac{14}{3e_3} S_3 \cdot \{1\}.$$

Die Größe $M_0$ ist mithin eine Konstante; wir bestimmen dieselbe aus dem Maß des Genus $\begin{pmatrix} 1, & 1 \\ 1, & 1 \end{pmatrix}$. Bekanntlich ist dieses Maß gleich $\frac{1}{24}$, und es wird folglich $M_0 = \frac{1}{12}$.

Dieser Wert von $M_0$ kann auch direkt mit Hilfe der Formel (66) hergeleitet werden. In der Tat, nehmen wir an, daß die Größe $D$ die sämtlichen ungeraden Primzahlen enthält, die unterhalb einer Größe $\Omega$ liegen, so werden die Grenzwerte der Ausdrücke $\frac{\{D\}}{(D)_1}$, $(D)_2$, $(D)_3$ für $\Omega = \infty$ bzw. gleich $\frac{2}{3\pi} \cdot \frac{1}{4}$, $\frac{1}{(2)_2 \cdot S_2}$, $\frac{1}{(2)_3 \cdot S_3}$. Wir finden also $\{1\} = \frac{S_2}{7\pi \cdot S_3}$ und folglich $M_0 = \frac{2S_2}{3\pi \cdot e_3} = \frac{1}{12}$.

Wir gelangen auf diese Weise zu dem folgenden Resultate:
Das Maß eines Genus

$$\begin{pmatrix} 1, & 1 \\ o, & o' \end{pmatrix},\ C(\varphi),\ C'(\varphi') \qquad [o, o' \equiv 1 \pmod 2]$$

ist gleich

$$M = \frac{o\,o'}{12} \cdot \left[1 + \frac{1}{2}(-1)^{\frac{o+1}{2}\cdot\frac{o'+1}{2}} \left(\frac{\varphi}{o}\right)\left(\frac{\varphi'}{o'}\right)\right] \cdot \frac{1}{2^{\vartheta+\vartheta'}} \cdot \prod_{p} \left[1 + \left(\frac{-o'\varphi}{p}\right)\frac{1}{p}\right] \cdot$$

$$\cdot \prod_{p'} \left[1 + \left(\frac{-o\varphi'}{p'}\right)\frac{1}{p'}\right] \cdot \prod_{r=r'} \left(1 - \frac{1}{rr'}\right) \cdot$$

Dieser Satz ist bereits von Eisenstein in Band 35 von Crelles Journal angegeben worden.

Insbesondere schließen wir hieraus für das Maß eines Genus

$$\varphi' \colon \begin{pmatrix} 1, & 1 \\ 1, & m \end{pmatrix},\ \left(\frac{\varphi}{q}\right),$$

wenn die Zahl $m$ ungerade ist und im ganzen $\mu$ Primzahlen $q$ enthält, die Gleichung

$$M = \frac{m}{12}\left[1 + \frac{1}{2}(-1)^{\frac{m+1}{2}}\left(\frac{\varphi}{m}\right)\right] \cdot \frac{1}{2^{\mu}} \prod_{q} \left[1 + \left(\frac{-\varphi}{q}\right)\frac{1}{q}\right] \cdot$$

Mit Hilfe ähnlicher Betrachtungen können wir auch das Maß eines beliebigen Genus von Formen mit drei Variablen bestimmen.

Wir erwähnen hier nur noch den besonderen Fall, daß das Maß eines Genus

$$\varphi' \colon \begin{pmatrix} 2, & 1 \\ 1, & 2m \end{pmatrix},\ \left(\frac{\varphi}{q}\right),\ (-1)^{\frac{\varphi-1}{2}} = -1 \qquad [m \equiv 1 \pmod 2]$$

gleich

$$\frac{m}{48}\left[1 + (-1)^{\frac{m+1}{2}}\left(\frac{\varphi}{m}\right)\right] \frac{1}{2^{\mu}} \prod_{q} \left[1 + \left(\frac{-\varphi}{q}\right)\frac{1}{q}\right]$$

ist.

III. ($n = 4$). Wir werden die Ordnungen

$$O_I'(d) \colon \begin{pmatrix} 1, & 1, & 1 \\ 1, & 1, & d \end{pmatrix}$$

untersuchen, welche eine so wichtige Rolle in der Theorie der Darstellung ganzer Zahlen durch eine Summe von fünf Quadraten spielen. — Es möge $2^v$ die höchste in $d$ aufgehende Potenz von 2 sein. Setzen wir $d = 2^v \cdot d_0$ [$d_0 \equiv 1 \pmod 2$] und bezeichnen wir mit $p_1, p_2, \ldots, p_\vartheta$ die in $d_0$ enthaltenen ungeraden Primzahlen, mit $\Phi'$ eine Grundform der Ordnung $O_I'(d)$ für den Modul $2d$, so besitzt die Form $\Phi'$, wenn $\varphi_1$ den

ersten Koeffizienten ihrer adjungierten Form $\Phi$ bedeutet, je nach den Fällen $v < 2$, $v = 2$, $v > 2$, die $\vartheta_0 = \vartheta$, $\vartheta + 1$, $\vartheta + 2$ Charaktere

$$C(\varphi_1) \quad \begin{cases} \left(\frac{\varphi_1}{p_1}\right), \left(\frac{\varphi_1}{p_2}\right), \ldots, \left(\frac{\varphi_1}{p_\vartheta}\right), & (v < 2) \\ \left(\frac{\varphi_1}{p_1}\right), \left(\frac{\varphi_1}{p_2}\right), \ldots, \left(\frac{\varphi_1}{p_\vartheta}\right), (-1)^{\frac{\varphi_1 - 1}{2}}, & (v = 2) \\ \left(\frac{\varphi_1}{p_1}\right), \left(\frac{\varphi_1}{p_2}\right), \ldots, \left(\frac{\varphi_1}{p_\vartheta}\right), (-1)^{\frac{\varphi_1 - 1}{2}}, \left(\frac{2}{\varphi_1}\right). & (v > 2) \end{cases}$$

Folglich besteht die Ordnung $O_I'(d)$ aus $g = 2^{\vartheta_0}$ verschiedenen Genera $G_1'$, $G_2', \ldots, G_g'$. Wir bezeichnen die Maße dieser Genera durch $M_1'$, $M_2'$, $\ldots, M_g'$.

Ist $p$ eine der $\vartheta$ Primzahlen $p_1, p_2, \ldots, p_\vartheta$, so besitzt die Kongruenz $\Phi(\xi_i) \equiv 0 \pmod p$ $p^3$ Lösungen $(\xi_i) \pmod p$ und die Kongruenz $\Phi(\xi_i) \equiv 0 \pmod 2$ im ganzen $2^3$ Lösungen $(\xi_i) \pmod 2$. Infolgedessen wird die Anzahl der inkongruenten Wertsysteme $(\xi_i) \pmod p$ oder $\pmod 2$, für welche die Form $\Phi(\xi_i)$ zu einer der Primzahlen $p$ oder zu der Zahl 2 relativ prim wird, gleich $p^4 - p^3 = p^4\left(1 - \frac{1}{p}\right)$ oder gleich $2^4 - 2^3 = 2^4\left(1 - \frac{1}{2}\right)$, und die Anzahl der nach dem Modul $2d$ inkongruenten Wertsysteme $(\xi_i)$, für welche $\Phi(\xi_i)$ einen zu $2d$ relativ primen Wert annimmt, ist gleich $(2d)^4 \cdot (2d)_1$.

Bedeutet jetzt $\mathsf{P}(\varphi_1)$ irgendein Produkt der Charaktere $C(\varphi_1)$, so muß die Funktion $\mathsf{P}(m)$ ($m$ relativ prim zu $2d$) den Bedingungen

$$\mathsf{P}(m) \cdot \mathsf{P}(m_0) = \mathsf{P}(m \cdot m_0), \quad \mathsf{P}(m) \cdot \mathsf{P}(m) = 1$$

genügen. Bestimmen wir jetzt ein vollständiges Formensystem $\Phi_1, \Phi_2, \ldots, \Phi_K$ für die der Ordnung $O_I'$ adjungierte Ordnung $O_I$ und bilden wir die Summe

$$\sum\nolimits_\varrho = \sum_{k=1}^{K} \left( \sum \frac{\mathsf{P}_k(\varphi_1) \cdot \{t(\Phi_k)\}^{-1}}{\{\Phi_k(\xi_1, \xi_2, \xi_3, \xi_4)\}^{\frac{4}{2}(1+\varrho)}} \right)$$

über alle möglichen ganzzahligen Wertsysteme $\xi_1, \xi_2, \xi_3, \xi_4$ ohne gemeinsamen Teiler, für welche der Ausdruck $\Phi_k(\xi_i)$ zu $2d$ relativ prim ausfällt, so wird dieselbe für jedes positive $\varrho$ konvergieren, und der Grenzwert von $\varrho \cdot \sum_\varrho$ wird für unendlich abnehmendes $\varrho$ gleich

$$L = \left( \sum_{i=1}^{g} \mathsf{P}^{(i)}(\varphi_1) M_i' \right) \cdot \frac{(2d)_1 \cdot e_4}{(2d)_4 \cdot S_4 \sqrt{d^3}}$$

werden.

Wir ordnen jetzt die Summe $\sum_\varrho$ nach den numerischen Werten der Zahlen $\Phi_k(\xi_1, \xi_2, \xi_3, \xi_4)$. Das Maß der Darstellungen einer zu $2d$ relativ primen Zahl $m$, in welcher $\mu$ ungerade Primzahlen $q_1, q_2, \ldots, q_\mu$ auf-

gehen, durch die Formen $\Phi_k$ ist gleich dem $2^{\mu}$-fachen Maße des Genus

$$\chi' : \quad \begin{pmatrix} 1, & 1 \\ 1, & m \end{pmatrix}, \ \left(\frac{\chi}{q}\right) = \left(\frac{-d}{q}\right),$$

d. i. gleich

$$\frac{m}{12}\left[1 - \frac{1}{2}(-1)^{\frac{m-1}{2}\cdot\frac{d_0-1}{2}}\left(\frac{m}{d_0}\right)\left(\frac{2^{\nu}}{m}\right)\right]\cdot\prod_{q}\left[1 + \left(\frac{d}{q}\right)\frac{1}{q}\right].$$

Infolgedessen können wir für die Summe $\sum_{\varrho}$ schreiben

$$\sum\nolimits_{\varrho} = \frac{1}{12}\sum_{m}\left\{\left[1 - \frac{1}{2}(-1)^{\frac{m-1}{2}\cdot\frac{d_0-1}{2}}\left(\frac{m}{d_0}\right)\left(\frac{2^{\nu}}{m}\right)\right]\cdot\prod_{q}\left[1 + \left(\frac{d}{q}\right)\frac{1}{q}\right]\cdot\frac{m\,\mathsf{P}(m)}{m^{2(1+\varrho)}}\right\}$$

$$= \frac{1}{12}\,\mathsf{T}_{\varrho} - \frac{1}{24}\,\overset{0}{\mathsf{T}}_{\varrho},$$

wo

$$\mathsf{T}_{\varrho} = \sum_{m}\prod\left[1 + \left(\frac{d}{q}\right)\frac{1}{q}\right]\frac{m\mathsf{P}(m)}{m^{2(1+\varrho)}}, \quad \overset{0}{\mathsf{T}}_{\varrho} = \sum_{m}\prod\left[1 + \left(\frac{d}{q}\right)\frac{1}{q}\right]\left(\frac{d}{m}\right)\frac{m\,\mathsf{P}(m)}{m^{2(1+\varrho)}}$$

ist.

Die Summen $\mathsf{T}_{\varrho}$ und $\overset{0}{\mathsf{T}}_{\varrho}$ können wir mit Hilfe der in I. gegebenen Formel (64) umformen. Da die Größe $\mathsf{P}(m)$ dem absoluten Werte nach gleich 1 ist, ergibt sich

$$\mathsf{T}_{\varrho} = \frac{\sum\frac{m\,\mathsf{P}(m)}{m^{2(1+\varrho)}}\cdot\sum\left(\frac{d}{m}\right)\frac{\mathsf{P}(m)}{m^{2(1+\varrho)}}}{\sum\frac{1}{m^{4(1+\varrho)}}}, \quad \overset{0}{\mathsf{T}}_{\varrho} = \frac{\sum\left(\frac{d}{m}\right)\frac{m\,\mathsf{P}(m)}{m^{2(1+\varrho)}}\cdot\sum\frac{\mathsf{P}(m)}{m^{2(1+\varrho)}}}{\sum\frac{1}{m^{4(1+\varrho)}}}.$$

Es wird also

$$L = \lim_{\varrho=0}\left(\varrho\sum\nolimits_{\varrho}\right) = \frac{1}{12}\lim_{\varrho=0}(\varrho\,\mathsf{T}_{\varrho}) - \frac{1}{24}\lim_{\varrho=0}\left(\varrho\,\overset{0}{\mathsf{T}}_{\varrho}\right)$$

und

$$\lim_{\varrho=0}(\varrho\,\mathsf{T}_{\varrho}) = \frac{1}{(2d)_4\cdot S_4}\cdot\sum\left(\frac{d}{m}\right)\frac{\mathsf{P}(m)}{m^2}\cdot\frac{1}{2}\lim_{\varrho=0}\left(\varrho\sum\frac{\mathsf{P}(m)}{m^{1+\varrho}}\right),$$

$$\lim_{\varrho=0}\left(\varrho\,\overset{0}{\mathsf{T}}_{\varrho}\right) = \frac{1}{(2d)_4\cdot S_4}\cdot\sum\frac{\mathsf{P}(m)}{m^2}\cdot\frac{1}{2}\lim_{\varrho=0}\left(\varrho\sum\frac{\mathsf{P}(m)\left(\frac{d}{m}\right)}{m^{1+\varrho}}\right).$$

Für die Größe $\mathsf{P}(m)$ wählen wir der Reihe nach die $2^{\vartheta_0}$ Glieder des über alle $\vartheta_0$ Größen $C(m)$ ausgedehnten Produktes

$$\Pi = \prod(1 + C(m)) = 1 + \cdots.$$

Durch jedesmalige Vergleichung der beiden Ausdrücke des Grenzwertes $L$ erhalten wir dann $2^{\vartheta_0}$ lineare Relationen zwischen den $2^{\vartheta_0}$ Größen $M_i'$, vermittels deren diese Größen eindeutig bestimmt werden können. Denn die Determinante dieser $2^{\vartheta_0}$ Gleichungen ist, wie man leicht erkennt, dem absoluten Werte nach gleich $2^{\vartheta_0\cdot 2^{\vartheta_0-1}}$.

Die beiden Grenzwerte

$$l = \lim_{\varrho=0}\left(\varrho \sum \frac{\mathsf{P}(m)}{m^{1+\varrho}}\right), \quad l_0 = \lim_{\varrho=0}\left(\varrho \sum \frac{\mathsf{P}(m)\left(\frac{d}{m}\right)}{m^{1+\varrho}}\right)$$

sind bereits von Dirichlet angegeben worden. In den Fällen $v = 0$, $d_0 \equiv -1 \pmod 4$ und $v = 1$ ist der Grenzwert $l_0$ gleich Null, während der Grenzwert $l$ gleich $(2d)_1$ oder gleich 0 ist, je nachdem $\mathsf{P}(m)$ mit dem Gliede 1 des Produktes $\Pi$ übereinstimmt oder nicht übereinstimmt. In diesen Fällen $v = 0$, $d_0 \equiv -1 \pmod 4$ und $v = 1$ erhalten wir daher

$$M_i' = \frac{1}{24 e_4}\sqrt{d^3} \cdot \frac{1}{2^{\vartheta_0}} \sum \left(\frac{d}{m}\right)\frac{1}{m^2}.$$

Wenn dagegen $v = 0$, $d_0 \equiv 1 \pmod 4$ oder $v \geqq 2$ wird, so erscheint die Größe

$$\left(\frac{d}{m}\right) = \left(\frac{m}{d_0}\right) \cdot \left(\frac{2^v}{m}\right)(-1)^{\frac{m-1}{2}\cdot\frac{d_0-1}{2}}$$

selbst unter den Gliedern des Produktes $\Pi$; es findet sich infolgedessen der Grenzwert $l_0$ gleich $(2d)_1$ oder gleich 0, je nachdem $\mathsf{P}(m) = \left(\frac{d}{m}\right)$ ist oder nicht; ähnlich wird der Grenzwert $l$ gleich $(2d)_1$ oder gleich 0, je nachdem $\mathsf{P}(m)$ mit 1 übereinstimmt oder nicht übereinstimmt. Wir bekommen demnach für die Fälle $v = 0$, $d_0 \equiv 1 \pmod 4$ oder $v \geqq 2$ die Formeln

$$M_i' = \frac{1}{24 e_4}\left[1 - \frac{1}{2}(-1)^{\frac{\varphi_1-1}{2}\cdot\frac{d_0-1}{2}}\left(\frac{\varphi_1}{d_0}\right)\left(\frac{2^v}{\varphi_1}\right)\right]\sqrt{d^3} \cdot \frac{1}{2^{\vartheta_0}} \sum \left(\frac{d}{m}\right)\frac{1}{m^2}.$$

Mit Hilfe dieser Gleichungen für die Größen $M_i'$ können wir insbesondere das Maß des in Kap. XXI betrachteten Genus $G_I'(d)$ finden. Wir bekommen so den folgenden Satz:

Die Anzahl der eigentlichen Darstellungen einer ganzen Zahl $d$ durch eine Summe von fünf Quadraten, welche nicht sämtlich ungerade sind, ist, wenn $d \equiv 3 \pmod 4$ oder $\equiv 2 \pmod 4$ ist, gleich

$$1920 \cdot \frac{1}{12\pi^2}\sqrt{d^3} \cdot \sum \left(\frac{d}{m}\right)\frac{1}{m^2},$$

dagegen, wenn $d \equiv 1 \pmod 4$ oder $\equiv 0 \pmod 4$ ist, gleich

$$\frac{1}{2} \cdot 1920 \cdot \frac{1}{12\pi^2}\sqrt{d^3} \cdot \sum \left(\frac{d}{m}\right)\frac{1}{m^2}.$$

Wir können diese beiden Formeln in eine einzige zusammenfassen und erhalten dann den folgenden Satz:

*Die Anzahl der eigentlichen Darstellungen einer ganzen Zahl $d$ durch eine Summe von fünf nicht lauter ungeraden Quadraten beträgt*

$$\frac{40}{\pi^2}\left(3 - (-1)^{\left[\frac{d}{2}\right]}\right)\sqrt{d^3} \cdot \sum \left(\frac{d}{m}\right)\frac{1}{m^2}. \qquad (m \text{ rel. pr. zu } 2d)$$

Ähnlich können wir die Maße der Genera einer Ordnung

$$O'_{II}(d): \quad \begin{pmatrix} 2, & 1, & 2 \\ 1, & 1, & d \end{pmatrix}$$

bestimmen. Die Formeln für das Maß des in Kap. XXI betrachteten Genus $G'_{II}(d)$ ergeben dann den folgenden Satz:

*Eine Zahl* $d \equiv 5 \pmod 8$ *besitzt*

$$\frac{32}{\pi^2}\sqrt{d^3}\cdot\sum\left(\frac{d}{m}\right)\frac{1}{m^2} \qquad (m \text{ rel. pr. zu } 2d)$$

*eigentliche Darstellungen durch eine Summe von fünf ungeraden Quadraten.* Eine Zahl $d$, welche nicht kongruent 5 (mod 8) ist, läßt sich nicht durch eine Summe von fünf ungeraden Quadraten darstellen.

Die in diesen Formeln auftretenden Summen $\frac{1}{\pi^2}\sqrt{d^3}\cdot\sum\left(\frac{d}{m}\right)\frac{1}{m^2}$ sind spezielle Fälle der Summen

$$\sum\nolimits_s = \frac{\sqrt{d^{2s-1}}}{\pi^s}\sum_m\left(\frac{(-1)^s\cdot d}{m}\right)\frac{1}{m^s}. \quad (d>0;\ m \text{ rel. pr. zu } 2d)$$

Indem wir, je nachdem $s = 2s_0$ oder $s = 2s_0 - 1$ ist, von den bekannten Werten der Reihe $\sum_{k=1}^{\infty}\frac{\cos 2\pi kz}{k^{2s_0}}$ oder der Reihe $\sum_{k=1}^{\infty}\frac{\sin 2\pi kz}{k^{2s_0-1}}$ Gebrauch machen, können wir für diese Summen analoge Ausdrücke finden, wie sie Dirichlet für den Fall $s = 1$ aufgestellt hat.

## Kap. XXIII. **Maß eines beliebigen Genus einer Ordnung** $\begin{pmatrix} 1 \\ o_h \end{pmatrix}$ **[$o_h \equiv 1 \pmod 2$].**

Die Untersuchung über die Maße positiver Genera habe ich soweit gefördert, daß ich in kurzer Zeit das Maß eines jeden beliebigen Genus angeben zu können hoffe. Um einen Begriff von den Resultaten zu geben, welche ich auf diesem interessanten Gebiet erhalten habe, will ich das Maß eines Genus $G$:

$$(o_0 = 0) \qquad \begin{pmatrix} 1, & 1, & \ldots, & 1, & 1 \\ o_1, & o_2, & \ldots, & o_{n-2}, & o_{n-1} \end{pmatrix} \qquad (o_n = 0)$$

$$C(\varphi_1),\ C(\varphi_2),\ \ldots,\ C(\varphi_{n-2}),\ C(\varphi_{n-1})$$

mitteilen, für welches die Invarianten $o_h$ sämtlich ungerade sind.

Sind $u', u'', \ldots; v', v'', \ldots$ irgend zwei Reihen ganzer Zahlen, so wollen wir durch das Symbol $NP(\overset{+}{u}', \overset{+}{u}'', \ldots; \overset{-}{v}', \overset{-}{v}'', \ldots)$ alle Primzahlen bezeichnen, welche in den sämtlichen Primzahlen $u', u'', \ldots$ enthalten sind

und welche gleichzeitig zu den sämtlichen Zahlen $v', v'', \ldots$ relativ prim ausfallen.

Es sei $\tau_h$ die Anzahl der verschiedenen Zahlen $NP(\overset{+}{o}_h)$. Die Anzahl aller der Ordnung $\binom{1}{o_h}$ angehörigen verschiedenen Genera wird dann gleich $g = 2^{\sum_{h=1}^{n-1}\tau_h}$ sein.

Wir wollen mit $k$ die sämtlichen Zahlen der Reihe $1, 2, \ldots, \left[\frac{n-1}{2}\right]$ bezeichnen und mit $i$ alle Zahlen, für welche $k \leqq i \leqq n-k$ ist. Von den Zahlen $o_{i-k}$ und $o_{i+k}$ ist dann mindestens eine von Null verschieden, und es sind die Größen

$$r_i^{(k)} = o_i^k \cdot \prod_{h=1}^{k-1} (o_{i-h} \cdot o_{i+h})^{k-h}$$

gleichfalls von Null verschieden. — Wir wollen die Zahlen $NP(\overset{+}{o}_{i-k}, \overset{+}{o}_{i+k}; \overset{-}{r}_i^{(k)})$ durch $\omega_i^{(k)}$ bezeichnen, ferner, wenn $k < i < n-k$ ist, die Zahlen $NP(\overset{+}{o}_{i-k} \cdot \overset{+}{o}_{i+k}; \overset{-}{r}_i^{(k)})$, wenn aber $i - k = 0$ oder $i + k = n$ ist, die Zahlen $NP(\overset{+}{o}_{i-k}, \overset{+}{o}_{i+k}; \overset{-}{r}_i^{(k)})$ durch $\vartheta_i^{(k)}$ bezeichnen. Die Zahlen $NP\left(\prod_{h=1}^{2k} \overset{+}{o}_h\right)$ mögen $p_0^{(k)}$ und die Zahlen $NP\left(\prod_{h=1}^{2k} \overset{+}{o}_{n-h}\right)$ mögen $p_n^{(k)}$ heißen. Bilden wir das Produkt

$$\prod \frac{\left(1 - \frac{1}{(p_0^{(k)})^{2k}}\right)\left(1 - \frac{1}{(p_n^{(k)})^{2k}}\right)}{\left(1 - \frac{1}{(\omega_i^{(k)})^{2k}}\right)\left(1 - \frac{1}{(\vartheta_i^{(k)})^{2k}}\right)}$$

über alle möglichen Primzahlen

$$\omega_i^{(k)},\ \vartheta_i^{(k)},\ p_0^{(k)},\ p_n^{(k)}, \qquad (k \leqq i \leqq n-k)$$

welche einem bestimmten $k$ entsprechen, so wird dasselbe, wie man leicht erkennt, ein vollständiges Quadrat, und wir können es durch $\Pi_k^2$ bezeichnen $(\Pi_k > 0)$. Das Produkt

$$\prod \left[1 + \left(\frac{(-1)^k \cdot r_i^{(k)} \cdot \varphi_{i-k} \cdot \varphi_{i+k}}{\omega_i^{(k)}}\right) \frac{1}{(\omega_i^{(k)})^k}\right],$$

welches über alle Primzahlen $\omega_i^{(k)}$ ausgedehnt sei, die einem bestimmten $k$ entsprechen, möge gleich $D_k$ gesetzt werden. Ferner schreiben wir

$$\prod_{k=1}^{\left[\frac{n-1}{2}\right]} \Pi_k = \Pi, \qquad \prod_{k=1}^{\left[\frac{n-1}{2}\right]} D_k = D$$

und

$$\prod_{h=1}^{n-1} o_h^{h(n-h)} = \Delta.$$

Endlich führen wir die beiden Einheiten ein

$$\delta_0 = \prod_{h=1}^{n-1}\left(\frac{\varphi_h}{o_h}\right)\cdot(-1)^{\left[\frac{n}{4}\right]+\sum_{t'<t''}^{1,n-1}\frac{\left(\prod_{h=1}^{t'}o_h\right)-1}{2}\cdot\frac{\left(\prod_{h=1}^{t''}o_h\right)-1}{2}}\cdot(-1)^{\left[\frac{n}{2}\right]\left(\left[\frac{n}{2}\right]+\sum_{t=1}^{n-1}\frac{\left(\prod_{h=1}^{t}o_h\right)-1}{2}\right)},$$

$$\delta_n = \prod_{h=1}^{n-1}\left(\frac{\varphi_{n-h}}{o_{n-h}}\right)\cdot(-1)^{\left[\frac{n}{4}\right]+\sum_{t'<t''}^{1,n-1}\frac{\left(\prod_{h=1}^{t'}o_{n-h}\right)-1}{2}\cdot\frac{\left(\prod_{h=1}^{t''}o_{n-h}\right)-1}{2}}\cdot(-1)^{\left[\frac{n}{2}\right]\left(\left[\frac{n}{2}\right]+\sum_{t=1}^{n-1}\frac{\left(\prod_{h=1}^{t}o_{n-h}\right)-1}{2}\right)}$$

Wenn $n \equiv 1 \pmod 2$ oder $n \equiv 0 \pmod 2$, $\Delta \equiv (-1)^{\frac{n}{2}} \pmod 4$ ist, findet man $\delta_0 = \delta_n$, und wir setzen

$$\delta = \frac{\delta_0 + \delta_n}{2},$$

dagegen, wenn $n \equiv 0 \pmod 2$, $\Delta \equiv -(-1)^{\frac{n}{2}} \pmod 4$ ist,

$$\delta = 0.$$

Alsdann gelten für das Maß $M$ des Genus $G$ die beiden Formeln:

für $n \equiv 1 \pmod 2$: $\quad M = \frac{\varepsilon_n}{g}\cdot\Pi\cdot D\cdot\Delta^{\frac{1}{2}}\left(1+\frac{\delta}{2^{\frac{n-1}{2}}}\right)$

und für $n \equiv 0 \pmod 2$:

$$M = \frac{\varepsilon_n}{g}\cdot\Pi\cdot D\cdot\Delta^{\frac{1}{2}}\left(1+\frac{\delta}{2^{\frac{n}{2}-1}}\right)\cdot\pi^{-\frac{n}{2}}\sum\left(\frac{(-1)^{\frac{n}{2}}\Delta}{m}\right)\frac{1}{m^{\frac{n}{2}}},$$

worin die Größen $\varepsilon_n$ gewisse rationale Konstante bedeuten, welche nur von der Zahl $n$ abhängen. —

Um diese Formeln für den Fall $n$ zu bestätigen, falls sie für den Fall $n-1$ bereits bewiesen sind, können wir, wenn $n \equiv 0 \pmod 2$ ist, genau auf dieselbe Art verfahren, wie Dirichlet zur Bestimmung des Maßes eines Genus mit zwei Variablen getan hat, und, wenn $n \equiv 1 \pmod 2$ ist, genau auf dieselbe Art, wie wir soeben zur Aufstellung des Maßes eines Genus mit drei Variablen verfahren sind.

## Note über die Kongruenzen $f \cong g \pmod{q^t}$.

In dieser Note wollen wir einen Beweis des Satzes M., Kap. X, geben. Wir bezeichnen durch $q^{\vartheta_{k-1}(f)}$ die höchste Potenz einer Primzahl $q$,

welche in den sämtlichen $k$-reihigen Unterdeterminanten einer Form $f$ aufgeht, und wir setzen $q^{\partial_k - \partial_{k-1}} = q^{v_k}$, $q^{v_k - v_{k-1}} = q^{\omega_k}$.

I. $[q = p \equiv 1 \pmod 2.]$ — *Zwei Klassen $f$ und $g$ von Formen mit $n$ Variablen sind in bezug auf einen Modul $p^t (> p^{v_{n-1}(f)}, > p^{v_{n-1}(g)})$ kongruent, wenn die Relationen*

$$f\{m; p^t\} = g\{m; p^t\} \qquad [m \equiv 1, 2, \ldots, p^t \pmod{p^t}] \tag{67}$$

*statthaben und wenn die Determinanten $\Delta(f)$ und $\Delta(g)$ nach dem kleineren der beiden Moduln $p^{t+\partial_{n-2}(f)}$, $p^{t+\partial_{n-2}(g)}$ kongruent sind.*

Beweis. Wir können voraussetzen, daß die eine der beiden Formen $f$ und $g$ in bezug auf $p$ primitiv ist. Denn ist $f = p^\partial \cdot f_0$, $g = p^\partial \cdot g_0$ $(\partial > 0,\ \partial \leqq t)$, so gilt $f(h; p^t) = f_0(h \cdot p^\partial; p^t) = p^{n\partial} \cdot f_0(h; p^{t-\partial})$ und $g(h; p^t) = p^{n\partial} \cdot g_0(h; p^{t-\partial})$*); die Beziehungen (67) ergeben also

$$f_0(h; p^{t-\partial}) = g_0(h; p^{t-\partial});$$

andererseits liefert die Kongruenz $f_0 \simeq g_0 \pmod{p^{t-\partial}}$ sofort $f \simeq g \pmod{p^t}$.

Ist die Form $f$ primitiv in bezug auf $p$, so wird die Kongruenz $f(x_i) \equiv \alpha \pmod{p^t}$ für gewisse zu $p$ relativ prime Zahlen $\alpha$ lösbar sein. Für diese selben Zahlen $\alpha$ hat dann die Kongruenz $g(y_i) \equiv \alpha \pmod{p^t}$ gleichfalls Lösungen; denn wir haben $g\{\alpha; p^t\} = f\{\alpha; p^t\}$ vorausgesetzt. Folglich muß die Form $g$ ebenso wie $f$ in bezug auf $p$ primitiv sein. — Da die Zahlen $\alpha$ zu $p$ relativ prim sind, können die $x_i$ in einer Kongruenz $f(x_i) \equiv \alpha \pmod{p^t}$ nicht sämtlich durch $p$ teilbar sein. Es ist demnach möglich, $n$ Zahlen $\xi_i \equiv x_i \pmod{p^t}$ zu bestimmen, deren größter gemeinsamer Teiler gleich 1 ist. Alsdann kann man eine Substitution

$$S = \begin{pmatrix} \xi_1, \ldots, \ldots, \ldots \\ \xi_2, \ldots, \ldots, \ldots \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \xi_n, \ldots, \ldots, \ldots \end{pmatrix}$$

von der Determinante 1 finden, welche die Form $f$ in eine Form $\widehat{f}_{(1)}$ überführt, deren erster Koeffizient kongruent $\alpha \pmod{p^t}$ wird. Nach Kap. II läßt sich diese Form $\widehat{f}_{(1)}$ noch in einen Repräsentanten von der Gestalt

$$f_{(1)} \equiv \alpha \xi^2 + F^{(1)} \pmod{p^t}$$

transformieren. Für die Form $f_{(1)}$ gelten die Beziehungen

$$\partial_{k-1}(F^{(1)}) = \partial_k(f), \quad (k \geqq 1); \qquad \Delta(F^{(1)}) \equiv \frac{\Delta(f)}{\alpha} \pmod{p^{t+\partial_{n-2}(f)}}$$

und

$$F^{(1)}(h; p^t) = \frac{f(h; p^t)}{(\alpha h; p^t)}, \qquad (\alpha h; p^t) \neq 0.$$

*) Siehe Kapitel VII.

Die nämlichen Schlüsse finden auf die Form $g$ Anwendung. Wir erhalten für diese Form einen Repräsentanten

$$g_{(1)} \equiv \alpha\xi^2 + G^{(1)} \pmod{p^t},$$

für welchen

$$\partial_{k-1}(G^{(1)}) = \partial_k(g), \quad (k \geqq 1); \qquad \Delta(G^{(1)}) = \frac{\Delta(g)}{\alpha} \pmod{p^{t+\partial_{n-2}(g)}}$$

und

$$G^{(1)}(h; p^t) = \frac{g(h; p^t)}{(\alpha h; p^t)}$$

ist.

Setzen wir jetzt voraus, unser Satz sei bereits für Formen mit $n-1$ Variablen als richtig erkannt, so wird

$$F^{(1)} \simeq G^{(1)} \pmod{p^t}$$

und folglich $f_{(1)} \simeq g_{(1)} \pmod{p^t}$. Damit wird unser Satz also auch für Formen mit $n$ Variablen bewiesen sein.

II. ($q = 2$.) *Zwei Klassen $f$ und $g$ von Formen mit $n$ Variablen sind in bezug auf einen Modul $2^t (> 2^{\vartheta_{n-1}(f)}, > 2^{\vartheta_{n-1}(g)})$ kongruent, wenn die Relationen*

$$f\{m; 2^t\} = g\{m; 2^t\} \quad [m \equiv 1, 2, \ldots, 2^t \pmod{2^t}]$$

*und die Kongruenzen*

$$2^{\omega_k(f)} \equiv 2^{\omega_k(g)} \pmod 2 \qquad (k = 0, 1, \ldots, n-1) \tag{68}$$

*statthaben und wenn die Determinanten $\Delta(f)$ und $\Delta(g)$ nach dem kleineren der beiden Moduln $\sigma_{n-1}(f) \cdot 2^{t+\partial_{n-2}(f)}$, $\sigma_{n-1}(g) \cdot 2^{t+\partial_{n-2}(g)}$ kongruent sind.*

Beweis. Es genügt, den Fall zu betrachten, daß die eine, $f$, der beiden Formen primitiv in bezug auf 2 ist.

1. Es sei zunächst $\sigma_1(f) = 1$. Dann können wir ungerade Zahlen $\alpha$ finden, für welche $f\{\alpha; 2^t\} > 0$ ist, und für dieselben Zahlen $\alpha$ wird dann $g\{\alpha; 2^t\} > 0$ sein. Infolgedessen ist die Form $g$ primitiv in bezug auf 2, und es gilt $\sigma_1(g) = 1$.

Sobald für eine ungerade Zahl $\alpha$ die Kongruenzen

$$f(\xi_i) \equiv \alpha \pmod{2^t}, \qquad g(\eta_i) \equiv \alpha \pmod{2^t}$$

lösbar sind, können wir $f$ und $g$ in zwei Repräsentanten

$$f_{(1)} \equiv \alpha\xi^2 + F^{(1)} \equiv \alpha\xi^2 + 2^{\omega_1(f)} \cdot f^{(1)} \pmod{2^t},$$
$$g_{(1)} \equiv \alpha\xi^2 + G^{(1)} \equiv \alpha\xi^2 + 2^{\omega_1(g)} \cdot g^{(1)} \pmod{2^t}$$

transformieren, in denen $f^{(1)}$ und $g^{(1)}$ primitive Formen in bezug auf 2 vorstellen.

Wenn eine der beiden Zahlen $\omega_1(f)$, $\omega_1(g)$ gleich Null ist, so verschwindet die andere gleichfalls; denn es ist $2^{\omega_1(f)} \equiv 2^{\omega_1(g)} \pmod 2$. In dem Falle, daß $2^{\omega_1(f)} = 2^{\omega_1(g)} = 1$ ist, kann man stets voraussetzen, daß die ungerade Zahl $\alpha$ und die Systeme $\xi_i \pmod{2^t}$ und $\eta_i \pmod{2^t}$ so gewählt

sind, daß die Formen $f^{(1)}$ und $g^{(1)}$ alle beide eine erste Invariante $\sigma$ gleich 1 besitzen.

In der Tat, die Form $f$ möge von der in Kap. III aufgestellten Gestalt $f_{(\varkappa_1)}$ sein, und es möge

$$S \equiv \begin{pmatrix} \xi_1, & \vartheta_1^{\,1}, & \ldots, & \vartheta_1^{\,n-1} \\ \xi_2, & \vartheta_2^{\,1}, & \ldots, & \vartheta_2^{\,n-1} \\ \cdot & \cdot & \cdot & \cdot \\ \xi_n, & \vartheta_n^{\,1}, & \ldots, & \vartheta_n^{\,n-1} \end{pmatrix} \pmod{2^t}$$

diejenige Substitution bedeuten, welche $f$ in $f_{(1)}$ verwandelt. Ist $\omega_1(f) = 0$, so wird $\varkappa_1(f) > 1$. Damit die erste Invariante $\sigma$ der Form $f^{(1)}$ gleich 2 wird, müssen die Kongruenzen

$$\xi_1 + \xi_2 + \cdots + \xi_{\varkappa_1} \equiv 1, \qquad \xi_1 \vartheta_1^{\,i} + \xi_2 \vartheta_2^{\,i} + \cdots + \xi_{\varkappa_1} \vartheta_{\varkappa_1}^{i} \equiv 0,$$
$$\vartheta_1^{\,i} + \vartheta_2^{\,i} + \cdots + \vartheta_{\varkappa_1}^{i} \equiv 0 \pmod 2$$

gelten. Wie man leicht erkennt, können diese Kongruenzen nur in dem Falle bestehen, daß

$$\varkappa_1 \equiv 1 \pmod 2; \qquad \xi_1 \equiv \xi_2 \equiv \cdots \equiv \xi_{\varkappa_1} \equiv 1 \pmod 2$$

ist. Fällt also $\varkappa_1 \equiv 0 \pmod 2$ aus, so wird stets $\sigma_1(f^{(1)}) = 1$. Ist aber $\varkappa_1 \equiv 1 \pmod 2$ und $\varkappa_1 > 1$, so finden sich unter den $2^{nt-1}$ Systemen $\xi_i \pmod{2^t}$, welche die Kongruenz $f(\xi_i) \equiv 1 \pmod 2$ erfüllen, $2^{nt-1}\left(1 - \frac{1}{2^{\varkappa_1 - 1}}\right)$ Systeme $\xi_i \pmod{2^t}$, denen eine Form $f^{(1)}$ mit einer Invariante $\sigma_1(f^{(1)}) = 1$ entspricht, und $2^{nt-1} \cdot \frac{1}{2^{\varkappa_1 - 1}}$ Systeme $\xi_i \pmod{2^t}$, denen eine Form $f^{(1)}$ mit einer Invariante $\sigma_1(f^{(1)}) = 2$ entspricht.

Die Kongruenzen (68) ergeben die Beziehung $\varkappa_1(f) = \varkappa_1(g) = \varkappa_1$, und wir gelangen für die Form $g$ zu Resultaten, welche denen für die Form $f$ erhaltenen ganz analog sind. Im Falle $\varkappa_1 \equiv 0 \pmod 2$ findet sich demnach unsere Annahme verwirklicht. Prüfen wir jetzt den Fall, daß $\varkappa_1 \equiv 1 \pmod 2$ und $\varkappa_1 > 1$ ist. Wenn keine der Zahlen $\alpha$, die man mit Hilfe von Systemen $\xi_i \pmod{2^t}$, für welche $\sigma_1(f^{(1)}) = 1$ wird, erhält, mit Hilfe von Systemen $\eta_i \pmod{2^t}$ erhalten werden könnte, für welche $\sigma_1(g^{(1)}) = 1$ ist, so würde man aus den Gleichungen $f\{\alpha; 2^t\} = g\{\alpha; 2^t\}$ schließen, daß mindestens $2^{nt-1}\left(1 - \frac{1}{2^{\varkappa_1 - 1}}\right)$ Systeme $\eta_i \pmod{2^t}$ Formen $g^{(1)}$ mit einer Invariante $\sigma_1(g^{(1)}) = 2$ liefern müßten. Aber das kann nicht sein, da wegen $\varkappa_1 > 1$ und $\equiv 1 \pmod 2$ stets $2^{nt-1} \frac{1}{2^{\varkappa_1 - 1}} < 2^{nt-1}\left(1 - \frac{1}{2^{\varkappa_1 - 1}}\right)$ ist. Infolgedessen gibt es in der Tat Zahlen $\alpha$ und Systeme $\xi_i \pmod{2^t}$ und $\eta_i \pmod{2^t}$, für welche man $\sigma_1(f^{(1)}) = 1$ und $\sigma_1(g^{(1)}) = 1$ bekommt.

Nach Kap. II gelten jetzt die folgenden Relationen:

$$\omega_{k-1}(F^{(1)}) = \omega_k(f), \qquad \sigma_{k-1}(F^{(1)}) = \sigma_k(f),$$
$$\Delta(F^{(1)}) \equiv \frac{\Delta(f)}{\alpha} \pmod{\sigma_{n-1}(f) \cdot 2^{t+\partial_{n-2}(f)}};$$
$$\omega_{k-1}(G^{(1)}) = \omega_k(g), \qquad \sigma_{k-1}(G^{(1)}) = \sigma_k(g),$$
$$\Delta(G^{(1)}) \equiv \frac{\Delta(g)}{\alpha} \pmod{\sigma_{n-1}(g) \cdot 2^{t+\partial_{n-2}(g)}},$$

und wir finden die Formeln

$$F^{(1)}(h;\, 2^t) = \frac{f(h;\, 2^t)}{(\alpha h;\, 2^t)}, \qquad G^{(1)}(h;\, 2^t) = \frac{g(h;\, 2^t)}{(\alpha h;\, 2^t)}, \quad (\alpha h;\, 2^t) \neq 0$$

in denen $h$ irgendeine Zahl bedeutet, die inkongruent $2^{t-1} \pmod{2^t}$ ist, und die Formeln

$$F^{(1)}(h;\, 2^t) = 0, \qquad G^{(1)}(h;\, 2^t) = 0, \qquad (\varkappa_1 = 1)$$
$$F^{(1)}(h;\, 2^t) = 2^{nt}, \qquad G^{(1)}(h;\, 2^t) = 2^{nt}, \qquad (\varkappa_1 > 1)$$

wenn $h \equiv 2^{t-1} \pmod{2^t}$ ist. Nehmen wir also an, unser Satz sei bereits für Formen mit $n-1$ Variablen bewiesen, so erhalten wir $F^{(1)} \simeq G^{(1)} \pmod{2^t}$ und daraus $f_{(1)} \simeq g_{(1)} \pmod{2^t}$.

2. Es möge jetzt $\sigma_1(f) = 2$ sein. Da $f$ in bezug auf 2 primitiv ist, wird die Zahl $2^{\omega_0(f)}$ gleich 1, und die Kongruenz $2^{\omega_0(f)} \equiv 2^{\omega_0(g)} \pmod 2$ ergibt $2^{\omega_0(g)} = 1$. Also ist die Form $g$ gleichfalls primitiv in bezug auf 2. Wir finden $\sigma_1(g) = 2$; denn wäre $\sigma_1(g) = 1$, so erhielten wir $g(2^{t-1};\, 2^t) = 0$, während $f(2^{t-1};\, 2^t)$ gleich $2^{nt}$ wäre. Die Kongruenzen (68) ergeben die Beziehung $\varkappa_1(f) = \varkappa_1(g)$, welche uns sofort zeigt, daß $f \simeq g \pmod 2$ ist. Es sei also $t > 1$.

Sobald für eine Zahl $2\alpha \equiv 2 \pmod 4$ die Kongruenz $f(\xi_i) \equiv 2\alpha \pmod{2^t}$ lösbar ist, können wir $f$ vermittels einer Substitution

$$S \equiv \begin{pmatrix} \xi_1, & \vartheta_1^{\,1}, & \ldots, & \vartheta_1^{\,n-1} \\ \xi_2, & \vartheta_2^{\,1}, & \ldots, & \vartheta_2^{\,n-1} \\ \cdot & \cdot & \cdot & \cdot \\ \xi_n, & \vartheta_n^{\,1}, & \ldots, & \vartheta_n^{\,n-1} \end{pmatrix} \pmod{2^t}$$

von der Determinante 1 in eine Form

$$\widehat{f}_{(2)} \equiv \begin{pmatrix} 2\alpha, & E_1, & \ldots, & E_{n-1} \\ E_1, & \ldots, & \ldots, & \ldots \\ \cdot & \cdot & \cdot & \cdot \\ E_{n-1}, & \ldots, & \ldots, & \ldots \end{pmatrix} \pmod{2^t}$$

transformieren. Wir nennen das System $\xi_i \pmod{2^t}$ primär, wenn unter den Zahlen $E_1, \ldots, E_{n-1}$ ungerade vorkommen. Allemal, wenn das System $\xi_i$ primär ausfällt, läßt sich die Form $\widehat{f}_{(2)}$ in einen Repräsentanten von der Gestalt

$$f_{(2)} \equiv 2(\alpha\xi^2 + \mathfrak{A}\xi\tilde{\xi} + \tilde{\alpha}\tilde{\xi}^2) + 2^{\omega_2(f)} \cdot f^{(2)} \equiv \chi + F^{(2)} \pmod{2^t}$$

verwandeln, in dem $\mathfrak{A} \equiv 1 \pmod 2$ ist.

Wir wollen jetzt voraussetzen, die Form $f$ sei von der in Kap. III betrachteten Gestalt $f_{(\varkappa_1)}$. Damit die Zahlen $E_1, \ldots, E_{n-1}$ sämtlich gerade sind, müssen dann die Kongruenzen

$$\xi_1 \vartheta_2^{\,i} + \xi_2 \vartheta_1^{\,i} + \cdots + \xi_{\varkappa_1 - 1} \vartheta_{\varkappa_1}^{\,i} + \xi_{\varkappa_1} \vartheta_{\varkappa_1 - 1}^{\,i} \equiv 0 \pmod 2$$

gelten, deren einzige Lösung

$$[\varkappa_1 \equiv 0 \pmod 2], \qquad \xi_1 \equiv \xi_2 \equiv \cdots \equiv \xi_{\varkappa_1} \equiv 0 \pmod 2$$

ist. Aber diese Kongruenzen sind nur dann mit der Kongruenz $2\alpha \equiv 2 \pmod 4$ verträglich, wenn $\sigma_{\varkappa_1+1}(f) \cdot 2^{\omega_{\varkappa_1}(f)} = 2$ ist. Also werden, falls $\sigma_{\varkappa_1+1}(f) \cdot 2^{\omega_{\varkappa_1}(f)} > 2$ ist, die sämtlichen Systeme $\xi_i$, für welche $f(\xi_i) \equiv 2 \pmod 4$ ausfällt, primär sein. Sobald hingegen $\sigma_{\varkappa_1+1}(f) \cdot 2^{\omega_{\varkappa_1}(f)} = 2$ ist, finden wir unter den $2^{nt-1}$ Systemen $\xi_i \pmod{2^t}$, für welche $f(\xi_i) \equiv 2 \pmod 4$ ist, $2^{nt-1}\left(1 - \frac{1}{2^{\varkappa_1}}\right)$ primäre Systeme und $2^{nt-1} \cdot \frac{1}{2^{\varkappa_1}}$ nichtprimäre Systeme. Dieselben Schlüsse finden auf die Form $g$ Anwendung.

Indem wir für den Fall $\sigma_{\varkappa_1+1}(f) \cdot 2^{\omega_{\varkappa_1}(f)} = 2$ bemerken, daß die Zahl $2^{nt-1} \cdot \frac{1}{2^{\varkappa_1}} < 2^{nt-1}\left(1 - \frac{1}{2^{\varkappa_1}}\right)$ ist, schließen wir wie in 1., daß wir die Zahl $2\alpha$ so wählen können, daß einerseits die Kongruenz $f(\xi_i) \equiv 2\alpha \pmod{2^t}$ eine primäre Lösung $\xi_i$ und andererseits die Kongruenz $g(\eta_i) \equiv 2\alpha \pmod{2^t}$ eine primäre Lösung $\eta_i$ besitzt. Ist dies geschehen, so liefert die Form $f$ einen Repräsentanten von der Form $f_{(2)}$, und die Form $g$ kann in eine Form von der Gestalt

$$g_{(2)} \equiv 2(\alpha\xi^2 + A\xi\tilde{\xi} + a\tilde{\xi}^2) + 2^{\omega_2(g)} \cdot g^{(2)} \pmod{2^t}$$

verwandelt werden, in der $A \equiv 1 \pmod 2$ ist.

Wir können jetzt voraussetzen, daß $a \equiv \tilde{\alpha} \pmod 2$ ist. In der Tat, es sei zunächst $\sigma_1(f^{(2)}) \cdot 2^{\omega_2(f)} \geqq 4$. Alsdann wird die Anzahl der Lösungen der Kongruenz $f_{(2)} \equiv 2 \pmod 4$ gleich $2^{2n-1}\left[1 - \frac{1}{2} \cdot \left(\frac{2}{4\alpha\tilde{\alpha} - \mathfrak{A}^2}\right)\right]$. Die Kongruenz $2^{\omega_2(f)} \equiv 2^{\omega_2(g)} \pmod 2$ ergibt $2^{\omega_2(g)} \geqq 2$, und es gilt $\sigma_1(g^{(2)}) \cdot 2^{\omega_2(g)} \geqq 4$. Denn wäre $\sigma_1(g^{(2)}) \cdot 2^{\omega_2(g)} = 2$, so bekämen wir $2^{\omega_2(g)} = 2$, $\sigma_1(g^{(2)}) = 1$, und die Kongruenz $g_{(2)} \equiv 2 \pmod 4$ hätte $2^{2n-1}$ Lösungen, so daß $g_{(2)}\{2;4\} \neq f_{(2)}\{2;4\}$ wäre. Ist jetzt $\sigma_1(g^{(2)}) \cdot 2^{\omega_2(g)} \geqq 4$, so liefert die Beziehung $f_{(2)}\{2;4\} = g_{(2)}\{2;4\}$ sofort $\left(\frac{2}{4\alpha\tilde{\alpha} - \mathfrak{A}^2}\right) = \left(\frac{2}{4\alpha a - A^2}\right)$, d. i. $\tilde{\alpha} \equiv a \pmod 2$.

Gilt aber $\sigma_1(f^{(2)}) \cdot 2^{\omega_2(f)} = \sigma_1(g^{(2)}) \cdot 2^{\omega_2(g)} = 2$ und $a \equiv \tilde{\alpha} + 1 \pmod 2$, so können wir die Form $2^{\omega_2(g)} \cdot g^{(2)}$ zunächst derart transformieren, daß einer ihrer mittleren Koeffizienten, $r_{ii}^{(2)}$, kongruent 2 (mod 4) wird. Durch Anwendung einer Substitution

$$\tilde{\xi} = \tilde{\xi}', \qquad x_i^{(2)} = \tilde{\xi}' + x_i'^{(2)}$$

gelangen wir dann zu einer Form, in welcher der Koeffizient $a$ durch

einen Koeffizienten $a_0 \equiv a + 1 \equiv \tilde{\alpha} \pmod 2$ ersetzt ist, und diese Form kann wiederum in eine Form von der Gestalt $g_{(2)}$ verwandelt werden, in der der Koeffizient $a_0$ der nämliche ist.

Demnach ist es stets möglich, anzunehmen, daß

$$a \equiv \tilde{\alpha} \pmod 2,$$

d. i.

$$4\alpha\tilde{\alpha} - \mathfrak{A}^2 \equiv 4\alpha a - A^2 \pmod 8$$

gilt. Infolge dieses Umstandes können wir eine Zahl $Z$ finden, welche der Kongruenz

$$4\alpha\tilde{\alpha} - \mathfrak{A}^2 \equiv (4\alpha a - A^2)Z^2 \pmod{2^{t+1}}$$

genügt, und $g_{(2)}$ geht vermittels einer Substitution

$$\xi \equiv Z \cdot \tilde{\xi}', \qquad x_i^{(2)} \equiv \frac{1}{Z} \cdot x_i'^{(2)} \pmod{2^t}$$

von der Determinante 1 in eine Form über, welche dieselbe Gestalt besitzt, in der aber der Rest

$$\begin{pmatrix} 2\alpha, & A \\ A, & 2a \end{pmatrix} \pmod{2^t}$$

durch den Rest

$$\begin{pmatrix} 2\alpha, & AZ \\ AZ, & 2aZ^2 \end{pmatrix} \pmod{2^t}$$

ersetzt ist. Dieser letztere Rest verwandelt sich noch durch eine Substitution

$$S_0 \equiv \begin{pmatrix} 1, & \frac{\mathfrak{A} - AZ}{2\alpha} \\ 0, & 1 \end{pmatrix} \pmod{2^t}$$

in einen Rest

$$\equiv \begin{pmatrix} 2\alpha, & \mathfrak{A} \\ \mathfrak{A}, & 2\tilde{\alpha} \end{pmatrix} \equiv \chi \pmod{2^t}.$$

Für die Form $g_{(2)}$ erhalten wir demnach eine Kongruenz von der Gestalt

$$g_{(2)} \simeq \chi + G^{(2)} \pmod{2^t}.$$

Wir haben jetzt die folgenden Beziehungen:

$$\omega_{k-2}(F^{(2)}) = \omega_k(f), \qquad \sigma_{k-2}(F^{(2)}) = \sigma_k(f),$$

$$\Delta(F^{(2)}) \equiv \frac{\Delta(f)}{4\alpha\tilde{\alpha} - \mathfrak{A}^2} \pmod{\sigma_{n-1}(f) \cdot 2^{t+\partial_{n-2}(f)}};$$

$$\omega_{k-2}(G^{(2)}) = \omega_k(g), \qquad \sigma_{k-2}(G^{(2)}) = \sigma_k(g),$$

$$\Delta(G^{(2)}) \equiv \frac{\Delta(g)}{4\alpha\tilde{\alpha} - \mathfrak{A}^2} \pmod{\sigma_{n-1}(g) \cdot 2^{t+\partial_{n-2}(g)}}$$

und

$$F^{(2)}(h; 2^t) = \frac{f(h; 2^t)}{\chi(h; 2^t)}, \qquad G^{(2)}(h; 2^t) = \frac{g(h; 2^t)}{\chi(h; 2^t)}. \quad [\chi(h; 2^t) \neq 0]$$

Nehmen wir an, unser Satz sei bereits für Formen mit einer kleineren Anzahl von Variablen als $n$ bewiesen, so finden wir $F^{(2)} \simeq G^{(2)} \pmod{2^t}$ und daraus auch $f_{(2)} \simeq g_{(2)} \pmod{2^t}$.

# Inhaltsverzeichnis.


| Kapitel | | Seite |
|---|---|---|
| | Begleitschreiben an die Académie des Sciences | 3 |
| | Inhaltsübersicht | 4 |
| | **Erster Teil.** | |
| | **Über die Reste quadratischer Formen.** | |
| I. | Klassen quadratischer Formen. — Index, Invarianten und Ordnung einer Form | 9 |
| II. | Formenreste. — Die Invarianten $o(f)$ sind ganze Zahlen | 13 |
| III. | Hauptformenreste und Hauptrepräsentanten für einen Modul $N$ | 21 |
| IV. | Bedingungen für die Existenz einer Ordnung $O$ | 26 |
| V. | Sätze über Hauptreste. — Grundformen für einen Modul $N$ | 32 |
| VI. | Formengruppen für einen Modul $N$. — Charaktere | 37 |
| VII. | Über die Anzahl der Lösungen der Kongruenzen $f = \sum_1^n a_{ik} x_i x_k \equiv m \pmod N$ | 45 |
| VIII. | Bestimmung der Größen $f(h; q^t)$ in den einfachsten Fällen | 50 |
| IX. | Charaktere der Hauptrepräsentanten und der Grundformen | 58 |
| X. | Bedingungen für die Gültigkeit der Kongruenz $f \simeq g \pmod{q^t}$ | 70 |
| XI. | Genera von Formen. — Bedingungen für die Existenz eines Genus | 71 |
| XII. | Adjungierte Formen. — Reziprozität zwischen den Ordnungen $\begin{pmatrix} \sigma_1, \sigma_2, \ldots, \sigma_{n-2}, \sigma_{n-1} \\ o_1, o_2, \ldots, o_{n-2}, o_{n-1} \end{pmatrix}, I$ und $\begin{pmatrix} \sigma_{n-1}, \sigma_{n-2}, \ldots, \sigma_2, \sigma_1 \\ o_{n-1}, o_{n-2}, \ldots, o_2, o_1 \end{pmatrix}, I$ | 80 |
| | **Zweiter Teil.** | |
| | **Über die Darstellung ganzer Zahlen durch quadratische Formen.** | |
| XIII. | Hilfssatz | 83 |
| XIV. | Darstellung einer Form von $v$ Variablen durch eine Form von $n$ Variablen ($v < n$). — Äquivalente Darstellungen und Darstellungsgruppen | 86 |
| XV. | Adjungierte Darstellungen und adjungierte Darstellungsgruppen | 91 |
| XVI. | Darstellung von ganzen Zahlen durch Formen mit $n$ Variablen | 94 |
| XVII. | Darstellungen von Formen mit $n-1$ Variablen durch Formen mit $n$ Variablen | 95 |
| XVIII. | Index, Ordnung und Genus der durch eine Form von $n$ Variablen darstellbaren Formen von $n-1$ Variablen | 102 |
| XIX. | Über den Inbegriff der Darstellungen einer ganzen Zahl durch die verschiedenen Formen eines Genus $G$ | 113 |
| XX. | Maß eines positiven Genus. — Maß der Darstellungen einer ganzen Zahl durch die Formen eines positiven Genus | 116 |
| XXI. | Über die Anzahl der Darstellungen einer ganzen Zahl durch eine Summe von fünf Quadraten | 117 |
| XXII. | Über die Bestimmung des Maßes einiger positiver Genera | 119 |
| XXIII. | Maß eines beliebigen Genus einer Ordnung $\begin{pmatrix} 1 \\ o_h \end{pmatrix} [o_h \equiv 1 \pmod 2]$ | 134 |
| | Note über die Kongruenzen $f \simeq g \pmod{q^t}$ | 136 |

## Verzeichnis der hauptsächlichsten vom Herausgeber übersetzten Stellen.*)

Das *Begleitschreiben* (S. 3—4) und die *Inhaltsübersicht* (S. 4—9) finden sich, diese in deutscher, jenes in französischer Sprache, nur im deutschen Manuskript, während sie in den Mémoires des Savants étrangers nicht mit zum Abdruck gelangt sind.

### Erster Teil.

Überschrift (S. 9, Z. 21).
Kap. I. S. 9, Fußnote. S. 10, Z. 1; Z. 6; Z. 34. S. 12, Z. 28—29.
Kap. II. S. 13, Z. 16—22. S. 14, Z. 2—3; Z. 28—30; Fußnote. S. 15, Z. 1; Z. 21; Z. 32—33. S. 16, Z. 20—29; Z. 31—S. 17, Z. 28. S. 18, Z. 5—6; Z. 15—16; Z. 28—31. S. 19, Z. 19—20; Z. 30—33. S. 20, Z. 3.
Kap. III. S. 24, Z. 8; Z. 13; Z. 16; Z. 36. S. 25, Z. 25—28.
Kap. IV. S. 26, Z. 1; Z. 22—28; Z. 32—34. S. 27, Z. 5—6.
Kap. V. S. 33; Z. 9. S. 34, Z. 9—11; Z. 26—27. S. 35, Z. 17—18.
Kap. VI. S. 37, Z. 25—31. S. 39, Z. 8; Z. 28—S. 40, Z. 33. S. 41, Z. 5. S. 42, Z. 16—17. S. 43, Z. 22. S. 45, Z. 1; Z. 9—10.
Kap. VII. S. 45, Z. 17—18; Z. 24—28. S. 47, Fußnote. S. 48, Z. 11; Z. 15.
Kap. VIII. S. 50, Z. 12—13; Z. 19—20. S. 51, Z. 10—13; Z. 16—17. S. 53, Z. 20. S. 58, Z. 8—10.
Kap. IX. S. 58, Z. 17—23. S. 62, Z. 13—14. S. 65, Z. 5—10. S. 69, Z. 18; Z. 25.
Kap. X. S. 70, Z. 11—S. 71, Z. 4.
Kap. XI. S. 71, Z. 5—36. S. 72, Z. 12—14; Z. 22—23; Z. 27—28. S. 74, Z. 21. S. 77, Fußnote.
Kap. XII. S. 81, Z. 3—4; Z. 11; Z. 13—15. S. 82, Z. 23—24.

### Zweiter Teil.

Überschrift (S. 83, Z. 9—10).
Kap. XIII. S. 83, Z. 24—S. 84, Z. 5; Z. 9—13; Z. 18; Z. 24—30. S. 86, Z. 7—8.
Kap. XIV, S. 86, Z. 24—27. S. 88, Z. 13—14; Z. 17—27. S. 89, Z. 1—S. 90, Z. 2; Z. 5—7; Z. 13—14.
Kap. XV. S. 91, Z. 8—10; Z. 25—S. 93, Z. 2; Z. 6—7.
Kap. XVI. S. 94, Z. 26—27.
Kap. XVII. S. 95, Z. 29—S. 96, Z. 9. S. 98, Z. 2; Z. 13—22; Z. 26—S. 99, Z. 8. S. 100, Z. 5—6; Z. 9—10; Z. 17—23. S. 102, Z. 10—12.
Kap. XVIII. S. 102, Z. 20—22; Z. 28—30. S. 103, Z. 4—14. S. 104, Z. 20; Z. 23—25; Z. 33. S. 106, Z. 8; Z. 18—24; Z. 32—33. S. 107, Z. 10; Z. 27—29. S. 108, Z. 6. S. 109, Z. 4. S. 110, Z. 28. S. 112; Z. 18—19; Z. 22.
Kap. XIX. S. 114, Z. 3—6; Z. 25—27. S. 115, Z. 18—22.
Kap. XX. S. 116, Z. 23—25.
Kap. XXI. S. 118, Z. 26—29; Z. 37.
Kap. XXII. S. 119, Z. 30. S. 120, Z. 15—16. S. 123, Z. 18—19. S. 124, Z. 20—21. S. 125, Z. 31. S. 129, Z. 23—28. S. 130, Z. 25. S. 131, Z. 6. S. 133, Z. 1—3; Z. 19—21; Z. 29. S. 134, Z. 3—4; Z. 15.
Kap. XXIII. S. 134, Z. 22; Z. 27—S. 135, Z. 5. S. 136, Z. 14—20.

Die *Note über die Kongruenzen* $f \equiv g \pmod{q^t}$ (S. 136—142) und das *Inhaltsverzeichnis* (S. 143) fehlen im deutschen Manuskript vollständig.

---

*) Vgl. die Vorbemerkung auf Seite 3. — S. bedeutet „Seite", Z. „Zeile". Bei der Abzählung der Zeilen sind die Symbole für Ordnungen und Unterdeterminanten

$$\begin{pmatrix}\sigma_1, \sigma_2, \cdots, \sigma_{n-1}\\ o_1, o_2, \ldots, o_{n-1}\end{pmatrix}, I, \quad \text{bzw.} \quad A\begin{pmatrix}i_1, i_2, \ldots, i_h\\ k_1, k_2, \ldots, k_h\end{pmatrix}, \quad S\begin{pmatrix}l_1, l_2, \ldots, l_h\\ i_1, i_2, \ldots, i_h\end{pmatrix}$$

einzeilig, die als Zahlsysteme geschriebenen quadratischen Formen oder Substitutionen hingegen mit der Anzahl ihrer Druckzeilen in Ansatz gebracht.

II.

# Sur la réduction des formes quadratiques positives quaternaires.*)

(Comptes rendus de l'Académie des Sciences, Paris 1883, t. 96, pp. 1205—1210).
(Note de M. Minkowski, présentée par M. Jordan.)

M. Charve a publié, aux Comptes rendus de 1881, une Note sur la réduction des formes quadratiques positives quaternaires. Je prends la liberté d'ajouter sur cet objet les observations suivantes, auxquelles je suis parvenu en étudiant les beaux Mémoires de M. Hermite dans le Journal de Crelle t. 40, 41 et 47. (Oeuvres, t. I, p. 94, p. 100, p. 164, p. 193, p. 200, p. 234.)

Les recherches sur la réduction des formes quadratiques positives s'appuient sur le théorème suivant:

I. *Une forme quadratique positive* $f = \sum_{h,k=1}^{n} a_{hk} x_h x_k$ *à déterminant* $D$ *n'obtient que pour un nombre fini de systèmes numeriques* $(x_h)$ *une valeur qui ne surpasse pas une quantité positive donnée* $E$.

*Démonstration.* En appliquant à $f$ la substitution au déterminant 1,

$$x_h = y_h, \quad x_k = y_k + \frac{\frac{\partial D}{\partial a_{hk}}}{\frac{\partial D}{\partial a_{hh}}} y_h \qquad (k \neq h),$$

$f$ sera transformée en

$$g = \frac{D}{\frac{\partial D}{\partial a_{hh}}} y_h^2 + g_h \qquad (y_h = x_h),$$

où $g_h$ représente une forme positive aux $n-1$ variables $y_k\,(k \neq h)$. Par conséquent, si la valeur de $f$ ne doit pas être plus grande que la quantité $E$, nous obtenons un système d'inégalités

$$E \geqq f = g \geqq \frac{D}{\frac{\partial D}{\partial a_{h\,h}}} x_h^2,$$

auquel ne peut satisfaire qu'un nombre fini de nombres entiers $x_h$.

*) Der Text dieser Arbeit, wie er hier veröffentlicht wird, folgt einem Manuskript, das von Minkowski angefertigt wurde, nachdem die Arbeit bereits in den Comptes rendus erschienen war, und das weit korrekter ist, als die dort zum Abdruck gelangte ältere Fassung. (Anm. d. Herausg.)

Nous arrangeons toutes les formes positives en un certain ordre. Nous disons qu'une forme positive $g = \sum_{h,k=1}^{n} b_{hk} x_h x_k$ est *placée à côté* d'une forme $f = \sum_{h,k=1}^{n} a_{hk} x_h x_k$, si les coefficients $b_{hh}$ sont égaux aux coefficients $a_{hh}$, par contre *au-dessus* (ou *au-dessous*) de la forme $f$, si les coefficients $b_{hh}$ et $a_{hh}$ ne sont pas tous d'accord, et si le premier coefficient $b_{hh}$, qui n'est pas égal au coefficient correspondant $a_{hh}$, est plus grand (ou plus petit) que $a_{hh}$.

A l'aide du théorème I on peut facilement démontrer: 1° que, parmi toutes les formes qui résultent d'une forme donnée $f$ à l'aide des substitutions numériques au déterminant 1 et qui donnent la classe $f$, apparaissent certaines formes $\varphi$ qui sont placées au-dessous de toutes les autres formes de cette classe; 2° que le nombre de ces formes $\varphi$ est ordinairement égal à 1, et que ce n'est qu'exceptionnellement qu'il devient plus grand que 1; 3° que ces formes $\varphi$ peuvent toujours être trouvées par un procédé fini.

Les formes $\varphi = \sum_{h,k=1}^{n} \alpha_{hk} \xi_h \xi_k$ sont ce que M. Hermite appelle des formes *réduites*. Les formes réduites $\varphi$ de la même classe ont sûrement les mêmes coefficients $\alpha_{hh}$.

II. *Pour $n = 2, 3, 4$, une forme $\varphi$ est réduite, et elle ne l'est que si elle satisfait aux inégalités*

$$\alpha_{11} \leqq \alpha_{22} \leqq \cdots \leqq \alpha_{nn} \tag{I}$$

*et à toutes les inégalités*

$$\varphi(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) \geqq \alpha_{hh}, \tag{II}$$

*dans lesquelles $\varepsilon_h$ signifie une unité, et où les autres $\varepsilon_k$ $(k \neq h)$ ont ou les valeurs 0, ou $+1$, ou $-1$.*

*Démonstration.* A) Les conditions (I) et (II) sont sûrement *nécessaires* pour que $\varphi$ soit une forme réduite; car si l'on avait $\alpha_{hh} > \alpha_{kk}$ pour $h < k$, $\varphi$ serait transformée par la substitution

$$S_I: \qquad \xi_h = \eta_k, \quad \xi_k = \eta_h; \quad \xi_l = \eta_l \qquad (h < k, \; l \neq h, k)$$

et si l'on avait $\varphi(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) < \alpha_{hh}$ $(\varepsilon_h = \pm 1, \varepsilon_k = 0, \pm 1)$, par la substitution

$$S_{II}: \qquad \xi_h = \varepsilon_h \eta_h, \quad \xi_k = \eta_k + \varepsilon_k \eta_h \qquad (k \neq h)$$

en une forme qui serait placée au-dessous de $\varphi$; par conséquent, $\varphi$ ne pourrait pas être réduite. Des inégalités (II) résultent spécialement les conditions $\alpha_{hh} \pm 2\alpha_{hk} + \alpha_{kk} \geqq \alpha_{hh}$, c'est-à-dire

$$\alpha_{kk} \geqq \pm 2\alpha_{hk}. \tag{$\alpha$}$$

B) Les conditions (I) et (II) sont aussi *suffisantes* pour que $\varphi$ soit réduite. Pour le démontrer, nous observons:

1° Que des inégalités (II) résultent toutes les autres inégalités

$$\text{(m)} \qquad \varphi(m_1, m_2, \ldots, m_n) \geqq \alpha_{hh} \qquad (m_h > 0),$$

dans lesquelles $m_h$ signifie un nombre quelconque différent de zéro, et les autres $m_k$ des nombres entiers tout à fait à volonté.

Nous désignons par $\varepsilon_k$ le nombre 0, ou $+1$, ou $-1$, selon que $m_k$ est égal à zéro, ou positif, ou négatif. Les quantités $\varepsilon_k m_k = \mu_k$ représentent les valeurs absolues des nombres $m_k$. Si les $n$ quantités $m_k$, à l'exception du seul nombre $m_h$, sont égales à zéro, $\varphi(m_k)$ devient évidemment égal à $\alpha_{hh} m_h^2 \geqq \alpha_{hh}$ et l'inégalité (m) aura lieu. Mais si des nombres $m_k$, au moins deux, sont différents de zéro, nous déterminons un indice $t$ de la manière suivante. Nous cherchons les nombres $m_\tau$, dont la valeur absolue est la plus petite sans être nulle, et nous posons, si parmi ces nombres $m_\tau$ se trouve aussi le nombre $m_h$, l'indice $t = h$, mais si ce n'est pas le cas, $t$ égal à l'un quelconque des nombres $\tau$. Si nous écrivons alors $s_k = \varepsilon_k \mu_t (k \neq t)$ et $s_t = 0$, les nombres $s_k$ ne seront pas tous égaux à zéro, et nous obtenons l'identité:

$$\varphi(m_1, m_2, \ldots, m_n) = \varphi(m_k - s_k + s_k) = \varphi(m_k - s_k) + \sum_{i,k=1}^{n} \alpha_{ik}(m_i s_k + m_k s_i - s_i s_k)$$

$$= \varphi(m_k - s_k) + 2 m_t^2 \sum_{k \neq t} \alpha_{kt} \varepsilon_k \varepsilon_t + \sum_{i,k \neq t} \alpha_{ik}(m_i s_k + m_k s_i - s_i s_k),$$

qui, à cause de la relation

$$2 \sum_{k \neq t} \alpha_{kt} \varepsilon_k \varepsilon_t = [\varphi(\varepsilon_k) - \alpha_{tt}] - \sum_{i,k \neq t} \alpha_{ik} \varepsilon_i \varepsilon_k,$$

prend la forme

$$\varphi(m_k) = \varphi(m_k - s_k) + m_t^2 [\varphi(\varepsilon_k) - \alpha_{tt}] + 2 \mu_t \sum_{i \neq t} \varepsilon_i (\mu_i - \mu_t) \sum_{k \neq t} \alpha_{ik} \varepsilon_k.$$

Ici, par suite des inégalités (II) et ($\alpha$), ni la quantité $[\varphi(\varepsilon_k) - \alpha_{tt}]$, ni les quantités

$$\sum_{k \neq t} \alpha_{ik} \varepsilon_i \varepsilon_k \left( = \underset{n=2}{\alpha_{ii} \varepsilon_i^2}, \ \alpha_{ii} \varepsilon_i^2 + \underset{n=3}{\alpha_{ik} \varepsilon_i \varepsilon_k}, \ \alpha_{ii} \varepsilon_i^2 + \underset{n=4}{\alpha_{ik} \varepsilon_i \varepsilon_k} + \alpha_{ik'} \varepsilon_i \varepsilon_{k'} \right)$$

ne sont négatives; par conséquent, nous obtenons l'inégalité

$$\varphi(m_k) \geqq \varphi(m_k - s_k),$$

pendant qu'on a en même temps

$$m_h - s_h > 0 \quad \text{et} \quad \sum m_k^2 > \sum (m_k - s_k)^2.$$

Si nous mettons maintenant $\sum m_k^2 = M$, et si nous supposons que le point 1° du théorème B) soit déjà prouvé pour tous les systèmes $(m_1, m_2, \ldots, m_n)$, $m_h > 0$, pour lesquels $\sum m_k^2$ devient plus petit que $M$,

il ressort évidemment $\varphi(m_k - s_k) \geqq \alpha_{hh}$ et $\varphi(m_k) \geqq \alpha_{hh}$. Sans doute l'inégalité (m) a lieu pour les systèmes $(m_k)$, pour lesquels on a $\sum m_k^2 \leqq 1$, $m_h > 0$, c'est-à-dire pour le seul système $m_h = 1$, $m_k = 0$ $(k \neq h)$. Ainsi, le point 1° est parfaitement démontré.

2° Admettons que pour la forme $\varphi$ les inégalités (I) et (II) soient satisfaites et, par conséquent, aussi toutes les inégalités (m). Alors $\varphi$ est, en effet, réduite.

*Démonstration.* Supposons d'abord que $\varphi$ puisse être transformée par une substitution numérique $\xi_h = \sum_{k=1}^{n} r_h^k \eta_k$ à déterminant 1 en une forme $\psi = \sum_{h,k=1}^{n} \beta_{hk} \eta_h \eta_k$ qui soit placée au-dessous de $\varphi$.

Soit $\beta_{ii}$ le premier des coefficients $\beta_{11}, \beta_{22}, \ldots, \beta_{nn}$ de la forme $\psi$ qui n'est pas égal au coefficient correspondant de la forme $\varphi$. On aura $\beta_{kk} = \alpha_{kk}$ $(k < i)$ et $\beta_{ii} = \varphi(r_1^i, r_2^i, \ldots, r_n^i) < \alpha_{ii}$.

Soit $r_l^i$ la dernière des quantités $r_1^i, r_2^i, \ldots, r_n^i$ qui est différente de zéro. On aura $\beta_{ii} = \varphi(\ldots, r_l^i, \ldots) \geqq \alpha_{ll}$. Soit $\alpha_{tt}$ $(t \geqq l)$ la dernière des quantités $\alpha_{11}, \alpha_{22}, \ldots, \alpha_{nn}$, qui a encore la valeur $\alpha_{ll}$ tandis que $\alpha_{hh}$ devient $> \alpha_{ll}$, si l'indice $h$ est $> t$. Des relations $\alpha_{ii} > \beta_{ii}$, $\beta_{ii} \geqq \alpha_{ll} = \alpha_{tt}$ et des inégalités (I) on conclut que le nombre $t$ est $< i$; donc pour $k \leqq t$ on aura $\beta_{kk} = \alpha_{kk} \leqq \alpha_{tt}$. Par conséquent, toutes les quantités $r_h^k$, pour lesquelles on a $k \leqq t$ et $h > t$, seront égales à zéro, puisque chacune de ces quantités, si elle différait de zéro, fournirait l'inégalité $\alpha_{kk} \geqq \alpha_{hh}$, tandis que l'on a $\alpha_{kk} \leqq \alpha_{tt}$, $\alpha_{hh} > \alpha_{tt}$. Dans le déterminant $|r_h^k|$ s'évanouissent donc toutes les $(t+1)(n-t)$ quantités

$$r_h^k \quad (k = 1, 2, \ldots, t;\ i;\quad h = t+1, \ldots, n)$$

qui sont les termes d'un système de $n - t$ séries horizontales et de $t+1$ séries verticales. Ce déterminant doit donc être égal à zéro, et l'on rencontre une contradiction.

De ce qui précède on déduit, à l'aide du théorème I, que l'on peut déterminer pour chaque forme positive $f$ toutes les formes réduites de sa classe à l'aide d'un nombre fini de substitutions de la forme $S_I$ ou $S_{II}$. (Toute classe $f$, pour laquelle aucune des inégalités (I) et (II) ne se change en une équation, a une *seule* forme réduite.)

Dans le cas $n = 4$, j'ai trouvé pour la limitation des coefficients des formes réduites des identités symétriques analogues à celles que Gauss a établies pour les formes ternaires (Gauss, Oeuvres complètes, t. II). Je reviendrai sur ces identités dans une autre occasion.

III.

# Über positive quadratische Formen.

(Crelles Journal für die reine und angewandte Mathematik, Bd. 99, S. 1—9.)

Meine Abhandlung „Sur la théorie des formes quadratiques à coefficients entiers“*) schließt mit der Bestimmung des Maßes für einige Genera von positiven quadratischen Formen. Das *Maß* eines Genus ist eine Größe, welche erhalten wird, indem man sämtliche Klassen des Genus abzählt und dabei die einzelnen Klassen in entsprechenden Verhältnissen rechnet, als sie verschiedene Formen besitzen. Ich hatte mich seinerzeit auf die Betrachtung spezieller Genera beschränkt. Mittlerweile bin ich zu einfachen Ergebnissen für das Maß eines beliebigen Genus gelangt. Die schließlichen Formeln sind zu einem Teile bereits von H. J. Stephen Smith veröffentlicht worden**). Das Resultat gewinnt aber außerordentlich an Klarheit und erlangt eine weitergehende Bedeutung, indem man jene Definition des Genus zugrunde legt, von welcher ich in der erwähnten Arbeit ausgegangen bin, und zu welcher auch Herr Poincaré geführt worden ist***).

Ich setze Formen von fester Variablenzahl $n$ und von nichtverschwindender Determinante voraus. Dann definiere ich:

A. Das *Genus* einer Form $f = \sum_1^n a_{ik} x_i x_k$ wird gebildet von allen den Formen $g$, welche denselben Trägheitsindex wie $f$ besitzen und welche mit $f$ für jeden beliebigen Modul $N$ kongruent sind.

Dabei heißt eine Form $g$ *kongruent* mit $f$ in bezug auf einen Modul $N$, wenn es möglich ist, aus $f$ mit Hilfe einer linearen Substitution von einer Determinante $\equiv 1 \pmod N$ eine Form herzuleiten, in welcher sämtliche Koeffizienten für den Modul $N$ dieselben Reste lassen wie die entsprechenden Koeffizienten von $g$.

Die Definition A. stellt an die Formen $g$ nur scheinbar unendlich viele Anforderungen. In Wirklichkeit gilt der Satz:

---

*) Mémoires présentés à l'Académie des Sciences T. XXIX. Nr. 2. Unter dem Titel „Grundlagen für eine Theorie der quadratischen Formen mit ganzzahligen Koeffizienten“, diese Ges. Abhandlungen, Bd. I, S. 3—144.

**) Proceedings of the Royal Society of London. 1868. (Collected Papers, vol. I, p. 510.)

***) Comptes rendus de l'Académie des Sciences à Paris. 1882. I.

B. Eine Form $g$ gehört dann und nur dann dem Genus einer Form $f$ an, wenn sie denselben Index $I$ und dieselbe Determinante $\Delta$ wie $f$ besitzt und dazu mit $f$ für den Modul $2\Delta$ kongruent ist.

Immer dann, wenn diese Bedingungen erfüllt sind, wird es zugleich (nach Sätzen von Smith) möglich sein, die Form $f$ in die Form $g$ mittels solcher linearer Substitutionen von der Determinante 1 überzuführen, in denen die Koeffizienten rationale Zahlen mit einem zu $2\Delta$ relativ primen Generalnenner sind.

Das Genus einer Form $f = \{a_{ik}\}$ ist eindeutig bestimmt, sobald man sein *vollständiges System von Invarianten* kennt. Dieses System umfaßt die folgenden Größen:

1. Den Index $I$ der Form $f$.

2. Die größten positiven Teiler der sämtlichen Unterdeterminanten von 1, 2, ..., $n$ Reihen des Systems $|a_{ik}|$. Diese Teiler mögen der Reihe nach mit $d_0, d_1, \ldots, d_{n-1}$ bezeichnet werden, so daß sich insbesondere

$$\Delta = (-1)^I \cdot d_{n-1}$$

ergibt.

3. $n-1$ Größen $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$, welche die Werte 1 oder 2 haben. Und zwar ist ein $\sigma_h$ gleich 1, wenn unter den symmetrischen $h$-reihigen Minoren von $|a_{ik}|$ sich solche vorfinden, die, vom Teiler $d_{h-1}$ befreit, ungerade ausfallen; gleich 2, wenn das Entgegengesetzte eintritt.

4. Eine Reihe von Einheiten $\pm 1$, die Charaktere der Form $f$.

In Art. IV und Art. XI meiner am Anfange zitierten Arbeit [[diese Ges. Abhandlungen, Bd. I, S. 31—32 und S. 75—76]] sind alle Bedingungen zusammengestellt, denen die Invarianten eines (wirklich existierenden) Genus zu genügen haben. Insbesondere müssen die $n$ Gleichungen

$$d_0 = o_0,\ d_1 = o_0^2 o_1,\ \ldots,\ d_{n-1} = o_0^n o_1^{n-1} \ldots o_{n-1}$$

stets zu $n$ *ganzen* Zahlen $o_0, o_1, \ldots, o_{n-1}$ führen.

Ich will hier nur von *positiven* Formen sprechen, also $I = 0$ voraussetzen. Jede positive Form $f$ läßt eine endliche Anzahl von Transformationen von der Determinante 1 in sich zu. Diese Anzahl mag $t(f)$ genannt sein. Die Größe $t(f)$ ist konstant für alle Formen der Klasse $f$; ihr reziproker Wert stellt das Maß der Klasse $f$ vor.

Das Maß $M$ eines positiven Genus $f$ $(= \{a_{ik}\})$ ist nun definiert durch eine Summe:

$$\sum \frac{1}{t(\varphi)},$$

erstreckt über sämtliche verschiedenen Formenklassen $\varphi$, welche das betrachtete Genus aufweist*).

*) Eisenstein, Crelles Journal, Bd. 35. (Mathem. Abhandlungen, S. 177.)

Mit $f(N)$ will ich bezeichnen, wie viele für einen Modul $N$ inkongruente Substitutionen von einer Determinante $\equiv 1 \pmod N$ man bilden kann, die, auf $f = \{a_{ik}\}$ angewandt, die sämtlichen Reste $a_{ik} \pmod N$ ungeändert lassen. Gemäß der Definition A. wird die Zahl $f(N)$ eine Invariante des Genus $f$ vorstellen. Den reziproken Wert dieser Zahl wird man passend als das *Maß* des Genus $f$ *für den Modul* $N$ bezeichnen können.

*Diese speziellen Maße* $\frac{1}{f(N)}$ *finde ich als die wesentlichen Faktoren des Maßes* $M$.

In betreff der Zahlen $f(N)$ gelten folgende Sätze:

1. Wenn $N$ sich aus mehreren Primzahlpotenzen zusammensetzt, $N = \prod q^t$, so ist $f(N) = \prod f(q^t)$.

Für Potenzen einer festen Primzahl $q$ findet man:

2. Für alle Potenzen $q^t$, welche die höchste in

$$2 \cdot \prod_{h=0}^{n-1} o_h$$

enthaltene Potenz von $q$ überschreiten, fällt die Größe

$$\frac{f(q^t)}{q^{\frac{n(n-1)}{2}t}}$$

konstant aus. Man setze diese Größe gleich

$$q^U \cdot f\{q\},$$

wo $q^U$ die höchste in $\prod_{h=0}^{n-1} \left(o_h^{\frac{(n-h)(n-h+1)}{2}-1}\right)$ enthaltene Potenz von $q$ sei. Alsdann wird $f\{q\}$ im wesentlichen nur von quadratischen Charakteren des Genus $f$ abhängen. (Ferner wird für das zu $f$ adjungierte Genus

$$F = \sum_1^n \frac{\partial \Delta}{\partial a_{ik}} x_i x_k$$

die Gleichung $F\{q\} = f\{q\}$ gelten.) Die Größe $f\{q\}$ bildet so den hauptsächlichen Faktor aller Größen $f(q^t)$.

*Wenn nun*

$$D = \prod_{h=1}^{n-1} o_h^{h(n-h)},$$

*so erhalte ich für das Maß des Genus* $f$ *einfach:*

$$M = c \cdot \sqrt{D} \frac{1}{f\{2\}} \cdot \frac{1}{f\{3\}} \cdot \frac{1}{f\{5\}} \cdots \frac{1}{f\{q\}} \cdots, \tag{1}$$

wo $c$ die Konstante

$$2\,\frac{\Gamma\left(\frac{1}{2}\right)\cdot\Gamma\left(\frac{2}{2}\right)\cdots\Gamma\left(\frac{n}{2}\right)}{\left\{\Gamma\left(\frac{1}{2}\right)\right\}^{\frac{n(n+1)}{2}}} \qquad \left(\Gamma\left(\tfrac{1}{2}\right)=\sqrt{\pi},\ \text{usw.}\right)$$

bedeutet, und wo das Produkt der Reihe nach über alle Primzahlen $q = 2, 3, 5, 7, \ldots$ auszudehnen ist.

Als Beispiel betrachte man ein positives Genus von (eigentlich) primitiven binären Formen von einer Determinante $\Delta \equiv 1 \pmod 4$. Man hat hier $n = 2$, $\sigma_1 = 1$, $o_1 = D = \Delta$. Für jede ungerade Primzahl $q$, die nicht in $\Delta$ aufgeht, ergibt sich

$$f\{q\} = 1 - \left(\frac{-\Delta}{q}\right)\frac{1}{q};$$

dagegen für jede Primzahl $q$ aus $2\Delta$:

$$f\{q\} = 2.$$

Bedeutet also $\mu$ die Anzahl aller (ungeraden) Primzahlen von $\Delta$, so kommt

$$M = \frac{1}{2^{\mu}}\cdot\frac{\sqrt{\Delta}}{\pi}\sum\left(\frac{-\Delta}{m}\right)\frac{1}{m},$$

wo $m$ alle positiven und zu $2\Delta$ relativ primen Zahlen zu durchlaufen hat. Ist $\Delta > 1$, so besitzt jede Klasse unseres Genus das Maß $\frac{1}{2}$. Die Größe $M$ wird dann gleich der halben Klassenanzahl des betrachteten Genus. Man gewinnt so ein Resultat, welches mit den Dirichletschen Formeln übereinstimmt.

Ohne mich bei weiteren Beispielen aufzuhalten, will ich nur zeigen, daß der Ausdruck (1) stets einen endlichen Wert besitzt.

Für jede ungerade Primzahl $q$, die nicht in $D$ aufgeht, findet man, wenn $n$ gerade:

$$f\{q\} = \left(1-\frac{1}{q^2}\right)\left(1-\frac{1}{q^4}\right)\cdots\left(1-\frac{1}{q^{n-2}}\right)\cdot\left\{1-\left(\frac{(-1)^{\frac{n}{2}}D}{q}\right)\frac{1}{q^{\frac{n}{2}}}\right\},$$

und wenn $n$ ungerade:

$$f\{q\} = \left(1-\frac{1}{q^2}\right)\left(1-\frac{1}{q^4}\right)\cdots\left(1-\frac{1}{q^{n-1}}\right)\cdot$$

Für jede solche Primzahl fällt also die Größe

$$\frac{\left(1-\frac{1}{q^2}\right)\left(1-\frac{1}{q^4}\right)\cdots\left(1-\frac{1}{q^{2\left[\frac{n-1}{2}\right]}}\right)}{f\{q\}} = E_q$$

besonders einfach aus. Nun kann man leicht in (1) diese Größe als allgemeines Produktglied einführen. Man braucht nur mit der Identität

$$1 = S_2 S_4 \ldots S_{2\left[\frac{n-1}{2}\right]}\cdot\prod_q\left(1-\frac{1}{q^2}\right)\left(1-\frac{1}{q^4}\right)\cdots\left(1-\frac{1}{q^{2\left[\frac{n-1}{2}\right]}}\right)$$

zu multiplizieren, wo $S_{2k}$ die Summe $1 + \frac{1}{2^{2k}} + \frac{1}{3^{2k}} + \cdots$ bezeichnet, deren Wert in bekannter Weise durch die $k^{\text{te}}$ Bernoullische Zahl, $B_k$, ausgedrückt ist. Setzt man, wenn $n$ gerade:

$$\mathfrak{c} = \left(\frac{1}{2}\right)^{\frac{n-4}{2}} \cdot B_1 B_2 \cdots B_{\frac{n-2}{2}},$$

und wenn $n$ ungerade:

$$\mathfrak{c} = \left(\frac{1}{2}\right)^{\frac{n-3}{2}} \cdot B_1 B_2 \cdots B_{\frac{n-1}{2}} \cdot \frac{1}{1 \cdot 2 \cdots \frac{n-1}{2}},$$

läßt man ferner $\partial$ die sämtlichen Primzahlen von $2D$ durchlaufen, so kommt, wenn $n \equiv 0 \pmod 2$:

$$M = \mathfrak{c} \cdot \frac{\sqrt{D}}{\pi^{\frac{n}{2}}} \cdot \prod_{\partial} E_{\partial} \cdot \sum \left(\frac{(-1)^{\frac{n}{2}} D}{m}\right) \frac{1}{m^{\frac{n}{2}}}, \tag{2}$$

(wo die Summation alle positiven und zu $2D$ relativ primen Zahlen $m$ betrifft), und wenn $n \equiv 1 \pmod 2$, so kommt:

$$M = \mathfrak{c} \cdot \sqrt{D} \cdot \prod_{\partial} E_{\partial}. \tag{2}$$

Diese Ausdrücke sind denen ähnlich, welche Smith angegeben hat, und man kann wohl aus der erwähnten Note von Smith die Werte der Größen $E_{\partial}$ für ungerade Primzahlen $\partial$, sowie in einigen speziellen Fällen auch für die Primzahl $\partial = 2$ entnehmen. Doch tritt dort nicht die hier entwickelte einfache Bedeutung dieser Größen zutage, und diese gerade ist es, welche erkennen läßt, daß ähnliche Verhältnisse auch für allgemeinere Formen bestehen. Vor allem fällt auf, daß der Ausdruck (1) nichts enthält, was an *positive* quadratische Formen gebunden ist. In der Tat besitzt dieser Ausdruck auch für alle indefiniten Genera (von nicht zerlegbaren Formen) einen endlichen Wert. Indem man nach der Bedeutung dieses Wertes forscht, gelangt man zu einer interessanten Erklärung des Maßbegriffes für indefinite Formen.

---

Ich will noch einige Sätze in betreff der Reduktion der positiven Formen mit beliebigen reellen Koeffizienten hinzufügen. Ist diese es ja, welche die Mittel gibt, um in jedem einzelnen Falle die Klassen eines Genus zu sondern und deren Maß zu berechnen. Ich wende (in etwas veränderter Form) diejenige Reduktionsmethode an, welche Herr Hermite im 40. Bande des Crelleschen Journals S. 302 (Oeuvres, T. I, p. 149) aufgestellt hat.

„In einer gegebenen Klasse von positiven quadratischen Formen sollen diejenigen Formen

$$f = \sum_1^n a_{ik} x_i x_k$$

*reduzierte* heißen, welche vor allen anderen Formen den kleinsten Wert der Verbindung

$$R = a_{11} + \delta \cdot a_{22} + \delta^2 \cdot a_{33} + \cdots + \delta^{n-1} \cdot a_{nn}$$

ergeben, wo $\delta$ eine positive unendlich kleine Größe bezeichnet."

Gemäß dieser Definition werden alle reduzierten Formen einer Klasse in den $n$ Koeffizienten

$$(a_{11}, a_{22}, \ldots, a_{nn})$$

übereinstimmen. Der Koeffizient $a_{11}$ insbesondere wird das *Minimum* der Klasse $f$ vorstellen.

Die charakteristischen Bedingungen solcher reduzierten Formen rühren für $n = 2$ von Lagrange und für $n = 3$ von Seeber her. Für den Fall $n = 4$ habe ich einen diesbezüglichen Satz in den Comptes rendus vom April 1883 [[diese Ges. Abhandlungen, Bd. I, S. 145—148]] mitgeteilt. (Der Beweis ist dort, namentlich am Schluß, durch eine Menge Druckfehler sehr entstellt.) Ein weiterer Satz existiert nun für den Fall $n = 5$. Ich fasse das Resultat für alle vier Fälle $n = 2, 3, 4, 5$ zusammen.

„In diesen Fällen ist eine Form

$$f = \sum_1^n a_{ik} x_i x_k$$

immer und nur dann eine positive und reduzierte Form, wenn sie einer Reihe von Ungleichungen

$$\text{(I)} \qquad f(m_1, m_2, \ldots, m_n) \geqq a_{ii} \qquad (i = 1, 2, \ldots, n)$$

genügt, wo die $m_h$, je nach den vier Fällen, den folgenden Tabellen gemäß zu wählen sind:

$n = 2$,

| $m_i$ | $\pm m_{i'}$ |
|---|---|
| 1 | 1 |

$n = 3$,

| $m_i$ | $\pm m_{i'}$ | $\pm m_{i''}$ |
|---|---|---|
| 1 | 1 | 0 |
| | 1 | 1 |

$n = 4$,

| $m_i$ | $\pm m_{i'}$ | $\pm m_{i''}$ | $\pm m_{i'''}$ |
|---|---|---|---|
| 1 | 1 | 0 | 0 |
| | 1 | 1 | 0 |
| | 1 | 1 | 1 |

$n = 5$,

| $m_i$ | $\pm m_{i'}$ | $\pm m_{i''}$ | $\pm m_{i'''}$ | $\pm m_{i^{\mathrm{IV}}}$ |
|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 0 |
| | 1 | 1 | 0 | 0 |
| | 1 | 1 | 1 | 0 |
| | 1 | 1 | 1 | 1 |
| | 1 | 1 | 1 | 2 |

und wenn ferner

(II) $$a_{11} \leqq a_{22} \leqq \cdots \leqq a_{nn}$$

ist."

In allen diesen Fällen wird also eine Hermitesche reduzierte Form durch eine endliche Anzahl einzelner linearer Ungleichungen definiert.

Genügt eine Form allen Bedingungen (I), so ist sie entweder selbst reduziert oder läßt sich doch durch eine oder mehrere Substitutionen von der Art

$$x_i = y_k, \quad x_k = -y_i$$

in eine reduzierte Form überführen. Jedenfalls stimmen ihre $n$ Hauptkoeffizienten, abgesehen von der Reihenfolge, mit den $n$ Koeffizienten $a_{ii}$ einer ihr äquivalenten reduzierten Form überein. Nun erkennt man leicht, daß den Bedingungen (I) alle solchen Formen genügen müssen, welche in ihrer Klasse den kleinsten Wert der Verbindung

$$\mathfrak{R}_1 = a_{11} + a_{22} + \cdots + a_{nn}$$

oder der Verbindung

$$\mathfrak{R}_n = a_{11}\, a_{22} \ldots a_{nn}$$

oder gewisser ähnlicher Verbindungen $\mathfrak{R}$ ergeben.

In den Fällen $n = 2, 3, 4, 5$ liefern sonach die Hermiteschen reduzierten Formen einer Klasse für jede einzelne der Größen $a_{11}+a_{22}+\cdots+a_{nn}$, $a_{11}a_{22} + a_{11}a_{33} + \cdots$, $a_{11}a_{22}\ldots a_{nn}$, ... den kleinsten Wert, welchen diese Größe für Formen der betrachteten Klasse überhaupt annehmen kann. Umgekehrt, wenn eine Form von $n$ $(= 2, 3, 4, 5)$ Variablen für *irgendeine* der Verbindungen $\mathfrak{R}$ einen kleinsten Wert ergibt, so geht diese Form bei geeigneter Permutation ihrer Koeffizientenreihen in eine Hermitesche reduzierte Form über; sie liefert also auch für alle anderen Verbindungen $\mathfrak{R}$ einen kleinsten Wert.

Diese Sätze, welche für $n = 2$ und $n = 3$ interessante Eigenschaften ebener und räumlicher Gitter ausdrücken, scheinen um so bemerkenswerter, als sie nicht mehr für größere Werte des $n$ gelten.

Im allgemeinen ist eine reduzierte Form um so eigentümlicher, in je mehr von den Ungleichungen (I) und (II) das Gleichheitszeichen statthat. Es gibt nun positive reduzierte Formen $f$, für welche $\frac{n(n+1)}{2} - 1$ linear unabhängige von den Ungleichungen (I) und (II) in Gleichungen übergehen, durch die dann die Verhältnisse der $\frac{n(n+1)}{2}$ Größen $a_{ik}$ vollständig und zwar in rationaler Weise bestimmt sind. Solche reduzierten Formen mögen *Grenzformen* heißen. Unter allen Grenzformen, denen dieselben Verhältnisse der Koeffizienten zukommen, wird es offenbar *eine* geben, deren Koeffizienten ganze Zahlen ohne einen gemeinsamen Teiler sind. Diese heiße eine *primitive* Grenzform.

„Da die Anzahl der Ungleichungen (I) und (II) eine beschränkte ist, so existiert (für $n = 2, 3, 4, 5$) immer nur eine beschränkte Anzahl von primitiven Grenzformen."

Um dieselben wirklich darzustellen, will ich mit $(a)_\nu$ diejenige quadratische Form von $\nu$ Variablen bezeichnen, deren $\nu$ Hauptkoeffizienten sämtlich gleich $a$, und deren übrige Koeffizienten sämtlich gleich 1 sind. Die Determinante dieser Form ist $(a-1)^{\nu-1} \cdot (a-1+\nu)$. Ich finde dann folgende primitive Grenzformen:

Wenn $n = 2$ ist, die Form $\varphi = (2)_2 = 2(x_1^2 + x_1 x_2 + x_2^2)$ und deren Nebenreduzierte $2(x_1^2 - x_1 x_2 + x_2^2)$.

Wenn $n = 3$ ist, die Form $\varphi = (2)_3$ und die Nebenreduzierten dieser Form.

Wenn $n = 4$ ist, die Form $\varphi = (2)_4$ und deren Nebenreduzierten; ferner die Form $\psi$, welche durch die Substitution

$$x_h = y_h + y_4, \quad x_4 = 2y_4 \qquad (h = 1, 2, 3)$$

in

$$(2)_1 + (2)_1 + (2)_1 + (2)_1 = 2(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$

übergeht, und die Nebenreduzierten dieser Form $\psi$.

Wenn $n = 5$ ist, die Form $\varphi = (2)_5$ und deren Nebenreduzierten; weiter die Form $\psi$, welche durch die Substitution

$$x_h = y_h + y_5, \quad x_5 = -y_4 + y_5 \qquad (h = 1, 2, 3, 4)$$

in $(2)_1 + (2)_1 + (2)_3$ übergeht, und deren Nebenreduzierten; endlich die Form $\chi$, welche durch

$$x_h = y_h + (-1)^h y_5, \quad x_5 = 2y_5 \qquad (h = 1, 2, 3, 4)$$

in $(4)_5$ übergeht, und die Nebenreduzierten von $\chi$.

Ohne Mühe wird man erkennen, daß die Klassen dieser Grenzformen identisch sind mit den *„formes extrêmes"*, welche die Herren Korkine und Zolotareff in ihren interessanten Aufsätzen im 6. und 11. Bande der Mathematischen Annalen eingeführt haben. Es sind darunter positive Formen verstanden, welche die Eigenschaft besitzen, daß ihr Minimum abnimmt, so oft den Koeffizienten unendlich kleine Variationen beigelegt werden, welche die Determinante der Form nicht vergrößern. Die nahe Beziehung zu diesen „Formen mit größtem Minimum" ist für die Reduktionsmethode von Herrn Hermite charakteristisch.

Wiesbaden, den 31. Januar 1885.

IV.

# Untersuchungen über quadratische Formen.

## Bestimmung der Anzahl verschiedener Formen, welche ein gegebenes Genus enthält.

(Inauguraldissertation (Königsberg 1885); Acta Mathematica, Band 7, S. 201—258.)

Dem Andenken meines teuren Vaters.

In meiner Arbeit «*Sur la théorie des formes quadratiques à coefficients entiers*»*) habe ich den Begriff des Genus lediglich aus dem Begriffe der Formenkongruenz hergeleitet. Ein solches Verfahren erwies sich bereits dort als äußerst vorteilhaft. Seine Berechtigung wird vielleicht noch schärfer durch die folgenden Entwicklungen hervortreten. Ich werde mich hier mit jenen Zahlen beschäftigen, welche im Falle allgemeiner Genera dieselbe Rolle spielen, wie im Falle binärer Genera die Klassenanzahlen. Gewisse Sätze über Formenkongruenzen werden zunächst erraten lassen, in welcher Gestalt sich die Ausdrücke jener Zahlen darbieten müssen. Unter Anwendung Dirichletscher Prinzipien soll alsdann gezeigt werden, daß die erratenen Formeln in Wirklichkeit richtig sind.

## Einleitung.

### 1. Ein Genus und seine Formenanzahl.

Unter den *Resten* einer quadratischen Form $f = \sum_1^n a_{ik} x_i x_k$ in bezug auf einen Modul $N$ verstehen wir alle diejenigen Formen, welche aus $f$ hervorgehen, indem die Koeffizienten $a_{ik}$ in beliebiger Weise um Vielfache des Moduls $N$ geändert werden.

---

*) Mémoires présentés par divers savants à l'Académie des Sciences de l'Institut de France. Tome XXIX, N°. 2 (1884). Ich zitiere diese Arbeit im folgenden kurz mit *F. Q.* — Den auf *F. Q.* bezüglichen Zitaten fügen wir stets in [[ ]] den entsprechenden Hinweis auf die hier (Bd. I, S. 3—144) veröffentlichte deutsche Ausgabe hinzu. (Anm. d. Herausg.)

Wir nennen zwei Formen $f$ und $g$ (von derselben Variablenzahl $n$) *kongruent* in bezug auf einen Modul $N$, $f \cong g \pmod N$, wenn es lineare Substitutionen von einer Determinante $\equiv 1 \pmod N$ gibt, durch welche die Reste der einen Form für den Modul $N$ in Reste der anderen Form für den Modul $N$ übergehen.

Wir betrachten ausschließlich Formen von nichtverschwindender Determinante.

Es kann der Fall eintreten, daß zwei Formen $f$ und $g$ *für einen jeden beliebigen Modul* kongruent sind. Solches findet offenbar immer statt, wenn $f$ und $g$ derselben Klasse äquivalenter Formen angehören, d. i. durch ganzzahlige Substitutionen von der Determinante 1 ineinander übergehen. Es ereignet sich überhaupt dann und nur dann, wenn $f$ und $g$ dieselbe Determinante $\Delta$ besitzen und in bezug auf den Modul $2\Delta$ kongruent sind.

Immer und nur dann, wenn die Formen $f$ und $g$ diesen Bedingungen genügen und dazu einen gleichen Trägheitsindex liefern, wird es möglich sein, die eine dieser Formen in die andere durch solche linearen Substitutionen von der Determinante 1 überzuführen, in welchen die Koeffizienten rationale Zahlen mit einem zu $2\Delta$ relativ primen Generalnenner sind.*)

Alle Formen, welche denselben Trägheitsindex $I$ haben wie eine gegebene Form, und welche mit dieser Form für einen jeden beliebigen Modul kongruent sind, fassen wir in ein *Genus* zusammen. Da die Formen eines Genus eine feste Determinante besitzen, so können sie, nach bekannten Sätzen, nur in eine endliche Anzahl verschiedener Formenklassen zerfallen.

Es ist aber im allgemeinen nicht sowohl die Anzahl dieser *Klassen*, welche sich durch einfache Formeln ausdrücken läßt, als vielmehr die Anzahl der in einem Genus enthaltenen *Formen*. Zwar ist die letztere Anzahl stets eine unendliche, denn schon jede einzelne Formenklasse besitzt unendlich viel Formen. Doch zeigt es sich bald, daß für ein jedes Genus eine gewisse, positiv unendliche Größe $\Omega$ existiert, welche nur von den einfachsten Invarianten des Genus abhängt, und zu welcher alle die Formenanzahlen der einzelnen Klassen des Genus in endlichen Verhältnissen stehen. Dieses $\Omega$ bestimmt dann auch den Grad, in welchem die Formenanzahl des gesamten Genus unendlich wird. Fällt die Formenanzahl in einer oder in mehreren Klassen des Genus gleich $M \cdot \Omega$ aus, so bezeichnen wir die positive endliche Größe $M$ als das *Maß* der betreffenden Klassen.

---

*) Henry I. Stephen Smith, Philosophical Transactions, CLVII, 1867 (On the Orders and Genera of Ternary Quadratic Forms, art. 12) und: Proceedings of the Royal Society of London, XVI, 1868 (On the Orders and Genera of Quadratic Forms containing more than three Indeterminates, p. 202). (Collected Papers, vol. I, p. 480 und p. 516.)

Am einfachsten gestaltet sich der Begriff des Maßes für definite Formen, also in den Fällen $I = 0$ und $I = n$, mit welchen wir uns später hauptsächlich beschäftigen werden. Man weiß, daß eine definite quadratische Form $f$ immer nur eine endliche Anzahl von Transformationen von der Determinante 1 in sich zuläßt. Sei $t(f)$ diese Anzahl. Nennen wir ferner $\Omega_0$ die Anzahl aller möglichen linearen ganzzahligen Substitutionen $S$ von $n$ Reihen und von der Determinante 1. Würden wir alle diese $S$ auf die Form $f$ anwenden, so müßten wir zu einer jeden Form der Klasse $f$ gelangen, und zwar zu einer jeden genau $t(f)$-mal. Die Anzahl der verschiedenen Formen der Klasse $f$ wird daher $\frac{1}{t(f)} \cdot \Omega_0$ betragen. Wählen wir demnach, was in der Tat geschehen soll, im Falle definiter Formen die erwähnte Größe $\Omega = \Omega_0$, so können wir als das Maß einer definiten Klasse $f$ die Größe $\frac{1}{t(f)}$ erklären. Das Maß für die Formenanzahl eines definiten Genus wird dann $\sum \frac{1}{t(f)}$ sein, wo die Summe über alle verschiedenen Klassen $f$ des Genus zu erstrecken ist.

In solchen speziellen Fällen, wo die Größe $t(f)$ konstant ausfällt für alle Formen eines Genus, ergibt die vorstehende Summe einfach den $t(f)^{\text{ten}}$ Teil der Klassenanzahl des Genus. Derartige Fälle sind Regel bei binären Formen. Man hat da gewöhnlich $t(f) = 2$. Nur für die Klassen $f = d(x^2 + y^2)$ wird $t(f) = 4$, und für die Klassen $f = 2d(x^2 + xy + y^2)$ wird $t(f) = 6$.

Ich bemerke noch beiläufig, daß die Größe $\Omega_0$ sich mit der $(n^2-1)^{\text{ten}}$ Potenz der Anzahl $\omega$ aller möglichen ganzen Zahlen von $-\infty$ bis $+\infty$ vergleichen läßt. Es gilt nämlich in gewissem Sinne die Beziehung:

$$\Omega_0 = \frac{\omega^{n^2-1}}{S_2 S_3 \dots S_n},$$

wo

$$S_k = 1 + \frac{1}{2^k} + \frac{1}{3^k} + \frac{1}{4^k} + \cdots. \qquad (k = 2, 3, \dots, n)$$

Eine Deutung des Maßbegriffes für indefinite Formen soll den Gegenstand einer späteren Arbeit bilden. Ich erwähne nur, daß als Maß einer primitiven binären Form $ax^2 + 2bxy + cy^2$ von einer negativen, nicht quadratischen Determinante $ac - b^2 = -D < 0$ am passendsten der Ausdruck $\frac{\pi}{\log\left(\frac{T + U\sqrt{D}}{\sigma}\right)}$ festgesetzt wird, wo $\sigma (= 1, 2)$ den größten Teiler der Koeffizienten $a$, $2b$, $c$ bedeutet, und wo $T$ und $U$ die zwei kleinsten positiven Zahlen sind, welche der Gleichung $T^2 - DU^2 = \sigma^2$ Genüge leisten.

## 2. Das vollständige System von Invarianten eines Genus.

Um ein Genus eindeutig zu charakterisieren, bedarf es nicht durchaus der Kenntnis einer seiner Formen. Es genügt bereits, wenn man imstande ist, sein *vollständiges System von Invarianten* anzugeben. Wir verstehen unter dieser Bezeichnung eine Reihe von Größen, welche sich als arithmetische Funktionen einer repräsentierenden Form $f$ des Genus darstellen lassen, und welche die doppelte Eigenschaft haben, einmal: ungeändert zu bleiben, so oft die Form $f$ durch eine andere Form *desselben* Genus ersetzt wird, dann aber: in ihrer Gesamtheit sich stets zu ändern, sobald für $f$ irgendeine Form eines *anderen* Genus genommen wird.

Ein vollständiges System von Invarianten eines Genus $f$ umfaßt die folgenden Größen:

1. den Trägheitsindex $I$ der Form $f$. Derselbe sagt aus, wie viele Quadrate mit dem Vorzeichen Minus auftreten, sobald $f$ durch irgendeine reelle Substitution in eine Summe von $n$, zum Teil positiven, zum Teil negativen Quadraten transformiert wird;

2. die $n$ Invarianten $d_0$; $o_1, o_2, \ldots, o_{n-1}$, und die $n-1$ Invarianten $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ der Form $f$.

Die Invariante $d_0$ stellt den positiven größten gemeinsamen Teiler der Koeffizienten $a_{ik}$ von $f$ vor.

Zu den Invarianten $o_h$ gelangt man in folgender Weise. Man bezeichne mit $d_1, d_2, \ldots, d_{n-1}$ die positiven größten gemeinsamen Teiler aller 2-, 3-, ..., $n$-reihigen Unterdeterminanten von $|a_{ik}|$, so daß insbesondere $\Delta = (-1)^I \cdot d_{n-1}$ kommt. Aus den Zahlen $d_h$ entstehen die Invarianten $o_h$ vermittels der Gleichungen:

$$\frac{d_1}{d_0^{\,2}} = o_1, \quad \frac{d_2}{d_0^{\,3}} = o_1^{\,2} o_2, \quad \ldots, \quad \frac{d_{n-1}}{d_0^{\,n}} = o_1^{\,n-1} o_2^{\,n-2} \ldots o_{n-1},$$

oder

$$o_h = \frac{d_h d_{h-2}}{d_{h-1}^2}.$$

Die Invarianten $\sigma$ sind Größen von den Werten 1 oder 2. Man hat $\sigma_h = 1$, wenn unter den symmetrischen $h$-reihigen Minoren von $f$ sich solche vorfinden, die, von dem Faktor $d_{h-1}$ befreit, ungerade ausfallen; dagegen $\sigma_h = 2$, wenn diese Minoren alle durch $2 d_{h-1}$ aufgehen.

Die Größen $o_h$ sind stets ganze Zahlen, und die Größen $\sigma_h$ müssen den folgenden Bedingungen genügen:

I. Die Zahlen $\sigma_{h-1} o_h \sigma_{h+1}$ und $\sigma_h$ dürfen nicht zugleich durch 2 teilbar sein.

II. Die Quotienten $\frac{\sigma_{h-1} o_h}{\sigma_{h+1}}$ und $\frac{o_h \sigma_{h+1}}{\sigma_{h-1}}$ müssen ganz sein.

Wir führen noch die Invarianten ein: $\sigma_0 = 1$, $\sigma_n = 1$ und $o_0 = 0$, $o_n = 0$.

3. die *Charaktere* der Form $f$. Dieses sind eine Reihe von Einheiten $\pm 1$, welche in Gestalt Legendrescher Symbole auftreten. Um sie möglichst einfach darzustellen, trifft man am besten folgende Voraussetzung über die repräsentierende Form $f$: Die aus den ersten $h(=1, 2, \ldots, n-1)$ Reihen von $f$ gebildeten symmetrischen Minoren sollen Werte $\sigma_h d_{h-1} \varphi_h$ ergeben von solcher Art, daß ein jedes $\varphi_h$ relativ prim zu $2 o_1 o_2 \ldots o_{n-1}$ und zu $\varphi_{h-1}$ und $\varphi_{h+1}$ ausfällt. Dabei hat man sich noch $\varphi_0 = 1$ und $\varphi_n = (-1)^I$ zu denken. Nach *F. Q.*, p. 83 [[S. 72]], lassen sich in jeder Klasse des Genus Formen $f$ von dieser Eigentümlichkeit finden; man nennt sie *charakteristische Formen.*

Es sei allgemein $\varepsilon_h$ das Vorzeichen von $\varphi_h$; ferner mag $I_h$ angeben, wie viele von den Einheiten $\frac{\varepsilon_1}{\varepsilon_0}, \frac{\varepsilon_2}{\varepsilon_1}, \ldots, \frac{\varepsilon_h}{\varepsilon_{h-1}}$ negativ ausfallen, so daß insbesondere $I_0 = 0$ und $I_n = I$ zu nehmen ist. Für eine charakteristische Form $f$ erweisen sich folgende Einheiten $C$ als Charaktere:

1) wenn $\sigma_{h-1} o_h \sigma_{h+1}$ durch eine ungerade Primzahl $p$ teilbar ist, die Einheit

$$\left(\frac{\varphi_h}{p}\right);$$

2) wenn $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod 4$ ist, die Einheiten

$$(-1)^{\frac{\varphi_h - 1}{2}}, \quad \left(\frac{\varphi_{h-1}}{\varepsilon_h \varphi_h}\right)(-1)^{\frac{I_h(I_h-1)}{2}}, \quad \left(\frac{\varphi_{h+1}}{\varepsilon_h \varphi_h}\right)(-1)^{\frac{I_h(I_h+1)}{2}};$$

3) wenn $\sigma_{h-1} o_h \sigma_{h+1} \equiv 0 \pmod 8$ ist, die Einheit

$$\left(\frac{2}{\varphi_h}\right).$$

Diese Einheiten $C$ bilden zusammen mit den Größen $I$, $d_0$, $o_h$, $\sigma_h$ wirklich ein vollständiges System von Invarianten für das betrachtete Genus, so daß kein zweites Genus da sein kann, welches zu eben diesen Invarianten führt.

Die Einheiten $C$ müssen alle Bedingungen erfüllen, welche sich für sie aus den quadratischen Kongruenzen

$$(1) \qquad -\sigma_{h-1} o_h \sigma_{h+1} \varphi_{h-1} \varphi_{h+1} \equiv X_h^2 \pmod{\sigma_h^2 \varphi_h}$$

erschließen lassen. Man findet diese Bedingungen in *F. Q.*, pp. 87—88 [[S. 75—76]] zusammengestellt.

Es gilt der Satz:

(A) Wenn die Invarianten $I$, $d_0$, $o$, $\sigma$ und die Charaktere $C$ in beliebiger Weise festgesetzt werden, doch so, daß sie den Bedingungen I., II. genügen, ferner allen Bedingungen, welche aus den Kongruenzen (1) folgen, so existiert wirklich ein Genus, welches zu diesen Invarianten und Charakteren Veranlassung gibt.

Ein Beweis dieses Satzes ist *F. Q.*, pp. 89—90 [[S. 76—77]], mit Hilfe des bekannten Theorems über die arithmetischen Progressionen geführt. Ich habe dort diesen Hilfssatz $(n-1)$-mal hintereinander angewandt zur sukzessiven Auffindung von $n-1$ Zahlen $\varphi_1, \varphi_2, \ldots, \varphi_{n-1}$ für eine charakteristische Form des gewünschten Genus. Man überzeugt sich aber leicht, daß es immer genügt, ein einziges Mal von diesem Satze Gebrauch zu machen, nämlich um allein $\varphi_{n-1}$ als Primzahl zu bestimmen; und man sieht dann ferner, daß in den Fällen $n \geqq 3$ dieser Hilfssatz sich ganz entbehren läßt, wenn nur der Satz (A) bereits für $n = 2$ bewiesen ist.

Alle Formengenera, welche dieselben Werte der Größen $I$, $d_0$, $o_h$, $\sigma_h$ besitzen, werden in eine *Ordnung*

$$d_0, \quad \begin{pmatrix} \sigma_1, & \sigma_2, & \ldots, & \sigma_{n-1} \\ o_1, & o_2, & \ldots, & o_{n-1} \end{pmatrix}, \quad I$$

zusammengefaßt.

Wir beschäftigen uns meist mit Formen $f$, deren $d_0$ gleich 1 ist, und die man *primitive* Formen nennt. Im Falle die Größe $d_0$ einer Form $f$ relativ prim zu einer Zahl $N$ ist, heißt diese Form primitiv in bezug auf $N$.

## Erster Teil.

### 3. Die Anzahl der Reste eines Genus in bezug auf einen Modul $N$.

Wir wollen zunächst untersuchen, wieviel verschiedene Formenreste ein gegebenes Genus in bezug auf einen gegebenen Modul $N$ liefert. In der Anzahl dieser Formenreste finden wir einen Divisor der Formenanzahl des Genus, und wir werden so alle wesentlichen Faktoren kennen lernen, aus welchen sich die Ausdrücke für die Formenanzahl zusammensetzen.

Das Genus möge durch eine beliebige seiner Formen, $f$, repräsentiert werden. Es ist dann klar, daß wir die Reste des Genus nach dem Modul $N$ nur unter denjenigen Formen suchen dürfen, welche $\simeq f \pmod N$ sind. Man gelangt zu diesen Formen, indem man auf $f$ ein vollständiges System von lauter inkongruenten Substitutionen $T$ von einer Determinante $\equiv 1 \pmod N$ anwendet. Ein solches System wird leicht bestimmt. Man braucht beispielsweise nur von den $N^{n^2}$ inkongruenten Substitutionen

$$x_i \equiv \sum_k t_i^k y_k \pmod N, \quad t_i^k = 1, 2, \ldots, N \qquad (i, k = 1, 2, \ldots, n)$$

alle diejenigen fortzulassen, in welchen die Determinante nicht $\equiv 1 \pmod N$ ausfällt.

In dem Systeme der $T$ mögen sich im ganzen $\mathfrak{N}$ Substitutionen finden lassen, — etwa die folgenden: $T_1, T_2, \ldots, T_{\mathfrak{N}}$ —, durch welche $f$ in $\mathfrak{N}$ verschiedene Reste: $g_1, g_2, \ldots, g_{\mathfrak{N}} \pmod N$ übergehe. Das gegebene

Genus enthält dann sicher nicht mehr als diese $\mathfrak{N}$ Reste. Wir behaupten aber, daß diese Reste wirklich alle dem gegebenen Genus, ja schon der (ganz beliebigen) Klasse $f$ eigen sind.

In der Tat, zu jeder Substitution

$$T = \begin{vmatrix} x_1, & \cdots\cdots \\ x_2, & \cdots\cdots \\ \cdots & \cdots\cdots \\ x_n, & \cdots\cdots \end{vmatrix} \equiv 1 \pmod{N}$$

läßt sich immer eine nach dem Modul $N$ kongruente Substitution $S$ von einer Determinante 1 bestimmen. Im Falle $n = 1$ leuchtet dieses unmittelbar ein. Wenn $n > 1$ ist, so bedienen wir uns zum Beweise eines Schlusses von $n - 1$ auf $n$. Offenbar muß der größte Teiler der $n$ Zahlen $x_i$ zu $N$ relativ prim sein. Man kann daher $n$ Zahlen $\xi_i \equiv x_i \pmod{N}$ finden, deren größter Teiler gleich 1 ist. Alsdann läßt sich bekanntlich eine Substitution

$$S_0 = \begin{vmatrix} \xi_1, & \cdots\cdots \\ \xi_2, & \cdots\cdots \\ \cdots & \cdots\cdots \\ \xi_n, & \cdots\cdots \end{vmatrix}$$

von der Determinante 1 bilden (*F. Q.*, p. 98 [[S. 83]]). Das Produkt $S_0^{-1} \cdot T$ gewinnt jetzt die Form

$$U \equiv \begin{vmatrix} 1, & U_1, & \ldots, & U_{n-1} \\ 0, & u_1^1, & \ldots, & u_1^{n-1} \\ \cdot & \cdot & \cdot & \cdot \\ 0, & u_{n-1}^1, & \ldots, & u_{n-1}^{n-1} \end{vmatrix} \equiv 1 \pmod{N}.$$

Ist unser Lemma bereits für den Fall $n - 1$ erwiesen, so können wir anstelle der $u_i^k$ solche kongruente Zahlen einführen, daß $|u_i^k|$ in 1 übergeht. Ferner setzen wir anstelle der ersten Vertikalreihe von $U$ einfach die Zahlen 1, 0, ..., 0. Auf diese Weise wird $U$ in eine kongruente Substitution $V$ von der Determinante 1 übergehen, und das Produkt $S_0 \cdot V = S$ erscheint als eine mit $T$ kongruente Substitution von der Determinante 1.

Wir können so zu allen Substitutionen $T_1, T_2, \ldots, T_{\mathfrak{N}}$ kongruente Substitutionen $S_1, S_2, \ldots, S_{\mathfrak{N}}$ von der Determinante 1 bilden. Durch diese muß sich $f$ in äquivalente Formen mit den Resten $g_1, g_2, \ldots, g_{\mathfrak{N}}$ verwandeln, was zu beweisen war.

Es ist nun leicht plausibel zu machen, daß die Formenanzahl der Klasse $f$ ein Vielfaches der Zahl $\mathfrak{N}$ wird. Man denke sich zu dem Behufe in der Klasse $f$ alle verschiedenen Formen gekennzeichnet, welche

nach dem Modul $N$ den Rest $f$ lassen, und für jede dieser Formen je eine Substitution $S$ notiert, durch welche dieselbe aus $f$ entsteht. Durch Anwendung aller $S \cdot S_1$, $S \cdot S_2$, ..., $S \cdot S_{\mathfrak{N}}$ müssen dann aus $f$ die sämtlichen Formen der Klasse $f$ hervorgehen, und zwar eine jede ein einziges Mal. Die Zahl $\mathfrak{N}$ teilt somit wirklich in gewissem Sinne die (unendliche) Formenanzahl der Klasse $f$, und da diese Klasse eine beliebige ist, auch die Formenanzahl des gesamten Genus, wie am Anfange ausgesprochen war.

Um einen Ausdruck für die Zahl $\mathfrak{N}$ zu gewinnen, verfährt man folgendermaßen. Es sei $\psi_n(N)$ die Anzahl der Individuen eines vollständigen Systemes von inkongruenten Substitutionen $T$ von einer Determinante $\equiv 1 \pmod N$. Alle diejenigen $T$, welche auf den Rest $f \pmod N$ ohne Wirkung bleiben, nenne man $\mathsf{T}$, und es sei $f(N)$ die Anzahl der verschiedenen $\mathsf{T}$. Die Substitutionen $\mathsf{T} \cdot T_1$, $\mathsf{T} \cdot T_2$, ..., $\mathsf{T} \cdot T_{\mathfrak{N}}$ müssen das gesamte System der $T$ erschöpfen, und man erhält so:

$$\mathfrak{N} = \frac{\psi_n(N)}{f(N)}.$$

In welcher Weise die Größe $\psi_n(N)$ gefunden wird, ist bekannt*). Damit ein $T \equiv 1 \pmod N$ ausfalle, ist zunächst erforderlich, daß die $n$ Zahlen $x_1$, $x_2$, ..., $x_n$ der ersten Vertikalreihe ohne gemeinsamen Teiler mit $N$ gewählt seien. Eine solche Wahl kann auf $N^n \cdot (N)_n$ Arten geschehen, wenn $(N)_n$ das über alle verschiedenen Primzahlen $q$ von $N$ ausgedehnte Produkt $\prod\left(1 - \frac{1}{q^n}\right)$ bedeutet. Man sieht leicht, daß zu jedem, ohne Teiler mit $N$ gewählten Systeme $x_i$ mindestens ein $T$ gehört. Alle möglichen $T$ mit der ersten Vertikalreihe $x_i$ folgen dann durch Zusammensetzung dieses einen mit den verschiedenen Substitutionen $U \equiv 1 \pmod N$. In $U$ unterliegen die $n-1$ Zahlen $U_i$ gar keiner Beschränkung. Es lassen sich also im ganzen $N^{n-1} \cdot \psi_{n-1}(N)$ inkongruente $U$ bilden, und man erlangt die Beziehung:

$$\psi_n(N) = N^{2n-1} \cdot (N)_n \cdot \psi_{n-1}(N).$$

Da nun $\psi_1(N) = 1$ ist, so entsteht

$$\psi_n(N) = N^{n^2-1} \cdot (N)_2 \cdot (N)_3 \cdots (N)_n.$$

Es handelt sich also wesentlich um die Bestimmung der Größen $f(N)$. Dabei genügt es, den Fall zu untersuchen, wo $N$ eine Primzahlpotenz $q^t$ ist.

Denn setzt $N$ sich aus mehreren Primzahlpotenzen $q^t$ zusammen, $N = \prod q^t$, so hat man $f(N) = \prod f(q^t)$.

*) Jordan, Traité des substitutions, 120—124.

So oft nämlich eine Substitution $\mathsf{T} \equiv 1 \pmod N$ ist, ergibt sich dieselbe auch $\equiv 1$ nach jedem der Moduln $q^t$, und ändert sie den Rest $f \pmod N$ nicht, so ändert sie auch keinen der Reste $f \pmod{q^t}$. Liegt andererseits für einen jeden Modul $q^t$ ein $\mathsf{T}_q$ vor, von einer Determinante $\equiv 1 \pmod{q^t}$, welches auf $f \pmod{q^t}$ ohne Wirkung bleibt, so wird die Substitution $\mathsf{T} \pmod N$, welche allen Kongruenzen

$$\mathsf{T} \equiv \mathsf{T}_q \pmod{q^t}$$

genügt, $\equiv 1 \pmod N$ ausfallen, und den Rest $f \pmod N$ nicht ändern. So geht die behauptete Relation hervor.

## 4. Hilfssätze zur Bestimmung der Zahlen $f(q^t)$.

Wir brauchen in betreff der Größen $f(q^t)$ nur den Fall zu betrachten, wo $f$ primitiv in bezug auf $q$ ist, also die Koeffizienten $a_{ik}$ von $f$ nicht sämtlich den Teiler $q$ haben. Denn sei etwa $f = q^d \cdot g$ und $d > 0$. So lange man $d \geqq t > 0$ hat, bleibt der Rest $f \pmod{q^t}$ bei jeder Substitution ungeändert, und man erhält $f(q^t) = \psi_n(q^t)$. Wenn aber $d < t$ ist, so gilt die Relation

$$f(q^t) = q^{(n^2-1)d} \cdot g(q^{t-d}). \tag{2}$$

In der Tat, eine jede Substitution $\mathsf{T} \equiv 1 \pmod{q^t}$, welche auf $f \pmod{q^t}$ ohne Wirkung ist, ändert auch $g \pmod{q^{t-d}}$ nicht; und ebenso wird ein jedes $\mathfrak{T} \equiv 1 \pmod{q^{t-d}}$, welches auf $g \pmod{q^{t-d}}$ ohne Wirkung bleibt, auch $f \pmod{q^t}$ nicht ändern. Aus einem jeden $\mathfrak{T}$ lassen sich aber $q^{(n^2-1)d}$, nach dem Modul $q^t$ verschiedene Substitutionen $\mathsf{T}$ herleiten. Denn in einem $\mathfrak{T}$ ist immer mindestens ein Koeffizient $c$ da, für welchen $\frac{\partial \mathfrak{T}}{\partial c}$ zu $q$ relativ prim ausfällt. Wir können nun, um eine Substitution $\mathsf{T}$ zu gewinnen, erst jeden der $n^2 - 1$ übrigen Koeffizientenreste $\pmod{q^{t-d}}$ von $\mathfrak{T}$ durch $q^d$ verschiedene Reste $\pmod{q^t}$ ersetzen. Der Rest von $c$ für den Modul $q^t$ folgt hernach eindeutig aus der Bedingung, daß die veränderte Substitution eine Determinante $\equiv 1 \pmod{q^t}$ ergebe.

Insofern es uns um Faktoren für die Formenanzahl eines Genus zu tun ist, reicht die Betrachtung solcher Moduln $q^t$ aus, welche gewisse Grenzen $q^{\sigma(q)}$ überschreiten. Denn ist $t \geqq t - d > 0$, so beweist man leicht, daß die Zahl $\psi_n(q^{t-d}) : f(q^{t-d})$ einen Divisor der Zahl $\mathfrak{N} = \frac{\psi_n(q^t)}{f(q^t)}$ vorstellt. Beachtet man die oben gegebenen Werte von $\psi_n(q^t)$, so läuft dieses darauf hinaus, daß die Zahl $f(q^t)$ in der Zahl $q^{(n^2-1)d} \cdot f(q^{t-d})\,[t-d>0]$ aufgeht.

Für eine mit $q$ primitive Form $f$ machen wir von folgenden Bezeichnungen Gebrauch. Die höchsten in den Invarianten $o_1, o_2, \ldots, o_{n-1}$ ent-

haltenen Potenzen von $q$ sollen die Exponenten besitzen: $\omega_1, \omega_2, \ldots, \omega_{n-1}$, und es sei allgemein

$$v_h = \omega_1 + \omega_2 + \cdots + \omega_h, \quad \partial_h = h\omega_1 + (h-1)\omega_2 + \cdots + \omega_h.$$

Ferner nehmen wir an, von den $n-1$ nicht negativen Zahlen $\omega_h$ seien im ganzen $\lambda - 1$ größer als Null, nämlich die folgenden:

$$(\vartheta_0 = 0) \qquad \omega_{\vartheta_1}, \ \omega_{\vartheta_2}, \ \ldots, \ \omega_{\vartheta_{\lambda-1}} \qquad (\vartheta_\lambda = n)$$

und wir bilden die Gleichungen

$$\vartheta_1 = \varkappa_1, \quad \vartheta_2 = \varkappa_1 + \varkappa_2, \ \ldots, \ \vartheta_h = \varkappa_1 + \varkappa_2 + \cdots + \varkappa_\lambda,$$

d. i.

$$\varkappa_k = \vartheta_k - \vartheta_{k-1}.$$

Der Quotient aus der Determinante $\Delta$ von $f$ und der Potenz $q^{\partial_{n-1}}$ mag für einen Moment $\Delta_0$ heißen. Wir werden weiterhin voraussetzen, daß unsere Moduln $q^t$, wenn $q$ einer ungeraden Primzahl $p$ gleich ist, die Potenz $p^G = p^{v_n-1}$, und wenn $q = 2$ ist, die Potenz $2^G = 2^{1+v_n-1}$ überschreiten. Die Folge davon wird sein, daß ein jeder Rest $f \pmod{q^t}$ uns, wenn $q = p$ ist, den Wert der Einheit $\left(\frac{\Delta_0}{p}\right)$, und wenn $q = 2$ ist, den Wert der Einheit $(-1)^{\frac{\Delta_0-1}{2}}$, sowie im Falle $\sigma_{n-1} = 2$ auch den Wert der Einheit $\left(\frac{2}{\Delta_0}\right)$ liefert. Denn es gilt der Satz:

Genügt eine Form $g$ schon der Kongruenz

$$g \simeq f \pmod{q^{G+1}}$$

und soll noch $g \simeq f \pmod{q^t}$ sein, so ist notwendig und hinreichend, daß, wenn $q = p$, die Beziehung

$$\Delta(g) \equiv \Delta(f) \pmod{p^{t+\partial_{n-2}}},$$

und wenn $q = 2$, die Beziehung

$$\Delta(g) \equiv \Delta(f) \pmod{\sigma_{n-1} \cdot 2^{t+\partial_{n-2}}}$$

bestehe.

Ich erwähne noch einige, zum Teil bekannte Sätze über Kongruenzen, welche bald ihre Anwendung finden werden.

(B) Ist eine Form $f$ und eine Zahl $\alpha$ prim in bezug auf eine ungerade Primzahl $p$, und hat die Kongruenz

$$f(\xi_i) \equiv \alpha \pmod{p}$$

$A \cdot p^{n-1}$ Lösungen, so besitzt die Kongruenz

$$(3) \qquad f(\xi_i) \equiv \alpha \pmod{p^t} \qquad (t > 1)$$

$A \cdot p^{(n-1)t}$ Lösungen.

Denn genügt ein System $\xi_i$ der Kongruenz

$$(4) \qquad f(\xi_i) \equiv \alpha \pmod{p^{t-1}},$$

und setzt man $x_i \equiv \xi_i + p^{t-1}u_i \pmod{p^t}$, so kommt, da $t > 1$ sein soll,

$$f(x_i) \equiv f(\xi_i) + p^{t-1} \cdot \sum u_i \frac{\partial f}{\partial \xi_i} \pmod{p^t}.$$

Nun können die Zahlen $\frac{\partial f}{\partial \xi_i}$ nicht sämtlich durch $p$ teilbar sein, da man $\frac{1}{2}\sum \xi_i \frac{\partial f}{\partial \xi_i} \equiv \alpha \pmod{p}$ hat. Also ergibt die Kongruenz

$$\frac{\alpha - f(\xi_i)}{p^{t-1}} \equiv \sum u_i \frac{\partial f}{\partial \xi_i} \pmod{p}$$

$p^{n-1}$ Lösungen $u_i \pmod{p}$, und eine jede Lösung von (4) liefert $p^{n-1}$ Lösungen von (3), woraus unmittelbar unser Satz folgt.

Jetzt sei $f = \sum a_{ik} x_i x_k$ eine in bezug auf 2 primitive Form, und $\alpha$ eine ungerade Zahl. Wir unterscheiden zwei Fälle, je nachdem die Invariante $\sigma_1$ von $f$ den Wert 1 oder 2 hat, die Zahlen $a_{ii}$ also zum Teil ungerade oder sämtlich gerade ausfallen.

(C) Ist $\sigma_1 = 1$, und besitzt die Kongruenz

$$f(\xi_i) \equiv \alpha \pmod{8}$$

$A \cdot 2^{3(n-1)}$ Lösungen, so liefert die Kongruenz

$$f(\xi_i) \equiv \alpha \pmod{2^t} \qquad (t > 3) \tag{3}$$

$A \cdot 2^{(n-1)t}$ Lösungen.

In der Tat, es genügen der Kongruenz

$$f(\xi_i) \equiv \alpha \pmod{2^{t-1}} \tag{4}$$

zusammen mit einem Systeme $\xi_i \pmod{2^{t-1}}$ immer alle die $2^n$ Systeme $x_i \pmod{2^{t-1}}$, für welche $x_i \equiv \xi_i \pmod{2^{t-2}}$ ist. Denn jedes dieser Systeme läßt sich in die Form $x_i \equiv \xi_i + 2^{t-2}\delta_i \pmod{2^{t-1}}$ setzen, wo die $n$ Größen $\delta_i$ entweder 0 oder 1 bedeuten; man hat also wirklich:

$$f(x_i) \equiv f(\xi_i) + 2^{t-1} \cdot \sum \delta_i \frac{1}{2} \frac{\partial f}{\partial \xi_i} \equiv \alpha \pmod{2^{t-1}}.$$

Bildet man nun mit Hilfe einer Lösung $\xi_i \pmod{2^{t-2}}$ von (4) ein System $x_i \equiv \xi_i + 2^{t-2} u_i \pmod{2^{t-1}}$, so kommt

$$f(x_i) \equiv f(\xi_i) + 2^{t-1} \cdot \sum u_i \frac{1}{2} \frac{\partial f}{\partial \xi_i} \pmod{2^t},$$

und die Kongruenz

$$\frac{\alpha - f(\xi_i)}{2^{t-1}} \equiv \sum u_i \frac{1}{2} \frac{\partial f}{\partial \xi_i} \pmod{2}$$

ergibt $2^{n-1}$ Lösungen $u_i \pmod{2}$. So führt eine jede Lösung $\xi_i \pmod{2^{t-2}}$ von (4) zu $2^{n-1}$ Lösungen $\xi_i \pmod{2^{t-1}}$ von (3), woraus die Richtigkeit unserer Behauptung erhellt.

Es ist auch klar, daß unser Satz gültig bleibt, wenn wir alle solchen Lösungen $\xi_i$ ausschließen, die zugleich gewissen gegebenen linearen Kongruenzen nach dem Modul 2 genügen.

(D) Ist zweitens $\sigma_1 = 2$, und hat die Kongruenz

$$f(\xi_i) \equiv 2\alpha \pmod{4}$$

$2A \cdot 2^{2(n-1)}$ Lösungen, in welchen die $n$ Zahlen $\frac{1}{2}\frac{\partial f}{\partial \xi_i}$ nicht sämtlich gerade sind, so liefert die Kongruenz

$$f(\xi_i) \equiv 2\alpha \pmod{2^t} \qquad (t>2) \tag{3}$$

$2A \cdot 2^{(n-1)t}$ Lösungen, bei welchen die $n$ Zahlen $\frac{1}{2}\frac{\partial f}{\partial \xi_i}$ nicht sämtlich gerade sind.

Denn setzt man $\frac{1}{2}f = \varphi$, so gruppieren sich je $2^n$ Lösungen $\xi_i \pmod{2^t}$ von (3) zu je einer Lösung $\xi_i \pmod{2^{t-1}}$ von $\varphi(\xi_i) \equiv \alpha \pmod{2^{t-1}}$. Unser Satz geht so in einen analogen Satz in betreff des Ausdruckes $\varphi$ über, welcher dann ähnlich bewiesen wird wie der Satz (B).

Wir schreiten nun zur Bestimmung der Größen $f(q^t)$*). Dabei werden wir uns hauptsächlich auf diejenigen Resultate stützen, welche in der Note zu meiner am Anfange zitierten Arbeit enthalten sind (*F. Q.*, pp. 169—178 [[S. 136—143]]).

## 5. Der Fall einer ungeraden Primzahl.

Wir betrachten zunächst den einfacheren Fall, wo $q$ gleich einer ungeraden Primzahl $p$ ist. Die Form $f$ sei primitiv in bezug auf $p$. Der Modul $p^t$ möge die Potenz $p^{\nu_{n-1}}$ überschreiten.

Da wir $f$ durch jeden nach dem Modul $p^t$ kongruenten Rest ersetzen dürfen, so können wir annehmen (*F. Q.*, p. 7 [[S. 14]]), $f$ habe den Typus

$$f \equiv \alpha\xi^2 + F \pmod{p^t},$$

wo $\alpha$ zu $p$ prim ist und $F$ einen Rest von $n-1$ Variablen vorstellt. Die Koeffizienten von $F$ müssen den Faktor $p^{\omega_1}$ enthalten, und setzen wir

$$F \equiv p^{\omega_1} f^{(1)} \pmod{p^t},$$

so fällt der Rest $f^{(1)}$ primitiv in bezug auf $p$ aus, und die $n-2$ Invarianten $p^{\omega_h^{(1)}}$, welche diesem Reste angehören, erfüllen die Gleichungen:

$$\omega_{h-1}^{(1)} = \omega_h. \qquad (h = 2, 3, \ldots, n-1)$$

Wir denken uns die $f(p^t)$ verschiedenen Substitutionen T von einer Determinante $\equiv 1 \pmod{p^t}$ aufgestellt, welche den Rest $f \pmod{p^t}$ in sich selbst überführen. In jeder dieser Substitutionen muß die erste Vertikalreihe aus $n$ Zahlen $\xi_i \pmod{p^t}$ bestehen, welche

$$f(\xi_i) \equiv \alpha \pmod{p^t}$$

ergeben. Der vorstehenden Kongruenz mögen $A \cdot p^{(n-1)t}$ verschiedene Systeme $\xi_i \pmod{p^t}$ Genüge leisten. Die Betrachtungen aus *F. Q.*, p. 170

*) In einem ausgezeichneten Falle, nämlich für die Form $f = x_1^2 + x_2^2 + \cdots + x_n^2$, sind die Zahlen $f(q)$ von Herrn Jordan gegeben (Traité des substitutions, 201—214, Ordre du groupe orthogonal).

[[S. 137]], lassen erkennen, daß jedem dieser Systeme $\xi_i$ wirklich Substitutionen T zukommen, welche den Rest $f$ in sich selbst transformieren.

Es fragt sich, wie viele verschiedene T können aus einem bestimmten Systeme $\xi_i$ hervorgehen. Ist $T_0$ eine erste dieser Substitutionen, so wird jedes überhaupt vorhandene T mit der ersten Vertikalreihe $\xi_i$ in ganz bestimmter Weise zusammengesetzt sein als Produkt aus $T_0$ und aus zwei Substitutionen $U$ und $\mathfrak{T}$ von der Form

$$U \equiv \begin{vmatrix} 1, & U_1, & \ldots, & U_{n-1} \\ 0, & 1, & \ldots, & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & \ldots, & 1 \end{vmatrix}, \quad \mathfrak{T} \equiv \begin{vmatrix} 1, & 0, & \ldots, & 0 \\ 0, & t_1^1, & \ldots, & t_1^{n-1} \\ \cdot & \cdot & \cdot & \cdot \\ 0, & t_{n-1}^1, & \ldots, & t_{n-1}^{n-1} \end{vmatrix} \pmod{p^t}.$$

Soll nun T den Rest $f$ in sich selbst überführen, so ist nötig, daß auch $U \cdot \mathfrak{T}$ diesen Rest in sich selbst transformiere. Hierzu wieder ist erforderlich, daß die Relationen $U_h \equiv 0 \pmod{p^t}$ gelten, und daß die Substitution $\mathfrak{T}$ auf den Rest $F \pmod{p^t}$ ohne Wirkung bleibe. Die Anzahl der verschiedenen T mit der ersten Vertikalreihe $\xi_i$, welche $f \pmod{p^t}$ nicht ändern, wird daher gleich der Anzahl der verschiedenen $\mathfrak{T}$ sein, welche auf $F \pmod{p^t}$ ohne Wirkung sind, also gleich $F(p^t)$. Zieht man noch die Formel (2) in Betracht, so kommt schließlich

$$f(p^t) = p^{(n-1)t+\omega_1[(n-1)^2-1]} \cdot A \cdot f^{(1)}(p^{t-\omega_1}).$$

Wir setzen nun allgemein:

$$f(p^t) = p^{\frac{n(n-1)}{2}t+\sum_{h=1}^{n-1}\omega_h\left(\frac{(n-h)(n-h+1)}{2}-1\right)} \cdot f\{p\}. \qquad \left(t > \sum_{h=1}^{n-1}\omega_h\right)$$

Für den Rest $f^{(1)}$ bilden wir eine entsprechende Größe $f^{(1)}\{p\}$. *Die vorstehende Relation verwandelt sich alsdann in:*

$$f\{p\} = A \cdot f^{(1)}\{p\}, \tag{5}$$

und diese Formel bleibt auch für $n = 1$ gültig, falls nur für eine Form $F$ von Null Variablen $F\{p\} = \frac{1}{2}$ genommen wird.

Es handelt sich jetzt um die Bestimmung der Größe $A$. Nach dem Satze (B) muß $A \cdot p^{n-1}$ die Anzahl aller Lösungen von $f(\xi_i) \equiv \alpha \pmod{p}$ ausdrücken. Bedeutet $\varkappa$ den Index der ersten von den Zahlen $\omega_1, \omega_2, \ldots, \omega_{n-1}, \omega_n\ (= -\infty)$, welche nicht verschwindet, so können wir $f$ von dem Typus voraussetzen:

$$\left.\begin{aligned} f &\equiv \Phi + p^{\omega_\varkappa} \cdot f^{(\varkappa)} \\ \Phi &\equiv \alpha_1 \xi_1^{\,2} + \alpha_2 \xi_2^{\,2} + \cdots + \alpha_\varkappa \xi_\varkappa^{\,2} \end{aligned}\right\} \pmod{p^t}, \qquad (\alpha_1 = \alpha)$$

wo ein jedes $\alpha_1, \alpha_2, \ldots, \alpha_\varkappa$ und ebenso der Rest $f^{(\varkappa)}$ primitiv in bezug auf $p$ ist (*F. Q.*, p. 19 [[S. 22]]). Wir erhalten dann $f \equiv \Phi \pmod{p}$, und

$A \cdot p^{\varkappa-1}$ muß die Anzahl der Lösungen von $\Phi \equiv \alpha \pmod p$ geben. Nun läßt sich diese letztere Anzahl nach bekannten Sätzen herleiten.*) Man gelangt so zu folgenden Beziehungen:

1. wenn $\varkappa \equiv 0 \pmod 2$,

$$A = \left(1 - \theta \cdot p^{-\frac{\varkappa}{2}}\right), \quad \theta = \left(\frac{(-1)^{\frac{\varkappa}{2}} \cdot \alpha_1 \alpha_2 \ldots \alpha_\varkappa}{p}\right);$$

2. wenn $\varkappa \equiv 1 \pmod 2$,

$$A = \left(1 + \theta^1 \cdot p^{-\frac{\varkappa-1}{2}}\right), \quad \theta^1 = \left(\frac{(-1)^{\frac{\varkappa-1}{2}} \cdot \alpha_2 \alpha_3 \ldots \alpha_\varkappa}{p}\right).$$

Im Falle $\varkappa = 1$ hat man sich $\theta^1 = 1$ zu denken.

Wir können weiter die Größe $f\{p\}$ auf $f^{(\varkappa)}\{p\}$ zurückführen. Man findet:

$$f\{p\} = \mathfrak{A} \cdot f^{(\varkappa)}\{p\},$$

wenn $\mathfrak{A}$ den folgenden Ausdruck bedeutet: im Falle $\varkappa \equiv 0 \pmod 2$,

$$\mathfrak{A} = 2\left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p^4}\right) \cdots \left(1 - \frac{1}{p^{\varkappa-2}}\right) \cdot \left(1 - \frac{\theta}{p^{\frac{\varkappa}{2}}}\right);$$

und im Falle $\varkappa \equiv 1 \pmod 2$,

$$\mathfrak{A} = 2\left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p^4}\right) \cdots \left(1 - \frac{1}{p^{\varkappa-1}}\right).$$

Für ein $\varkappa = 1$ stimmt diese Gleichung unmittelbar mit (5) überein, während sie für ein $\varkappa > 1$ leicht aus (5) mit Hilfe eines Schlusses von $\varkappa - 1$ auf $\varkappa$ hervorgeht. Man braucht nur zu beachten, daß dem Reste $f^{(1)}$ in derselben Weise die Zahl $\varkappa - 1$ angehört wie dem Reste $f$ die Zahl $\varkappa$.

Für alle ungeraden Primzahlen $p$, welche nicht in der Determinante $\Delta$ der Form $f$ aufgehen, wird $\varkappa = n$, also $\alpha_1 \alpha_2 \ldots \alpha_\varkappa \equiv \Delta \pmod p$, während $f^{(\varkappa)}$ sich als ein Rest von Null Variablen erweist. Für alle diese Primzahlen $p$ kommt daher:

1. wenn $n \equiv 0 \pmod 2$,

$$f(p^t) = p^{\frac{n(n-1)}{2}t} \cdot \left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p^4}\right) \cdots \left(1 - \frac{1}{p^{n-2}}\right) \cdot \left\{1 - \left(\frac{(-1)^{\frac{n}{2}}\Delta}{p}\right)\frac{1}{p^{\frac{n}{2}}}\right\};$$

2. wenn $n \equiv 1 \pmod 2$,

$$f(p^t) = p^{\frac{n(n-1)}{2}t} \cdot \left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p^4}\right) \cdots \left(1 - \frac{1}{p^{n-1}}\right) \cdot$$

---

*) Lebesgue, Recherches sur les nombres, § 5 (Journal de Liouville, T. 2, pp. 266—275). — C. Jordan, Comptes rendus, 1866, I, pp. 687—690; Traité des substitutions, 197—200; Journal de Liouville, 2me série, T. 17, p. 372. — *F. Q.* artt. VII—VIII [[S. 45—58]].

Um die Größen $f\{p\}$ vollständig darzustellen, wollen wir endlich $f$ als *Hauptrest* für den Modul $p^t$ voraussetzen. Falls die Bezeichnungen aus **4.** gelten, so heißt dieses, $f$ soll den Typus haben:

$$f \equiv \{\Phi_1 + p^{\omega\vartheta_1}[\Phi_2 + p^{\omega\vartheta_2}[\Phi_3 + \cdots + p^{\omega\vartheta_{\lambda-1}}(\Phi_\lambda)..]]\} \pmod{p^t},$$

$$\Phi_k \equiv \alpha_1^{(k)}\xi_1^{(k)}\xi_1^{(k)} + \cdots + \alpha_{\varkappa_k}^{(k)}\xi_{\varkappa_k}^{(k)}\xi_{\varkappa_k}^{(k)} \pmod{p^{t-v_{\vartheta_k-1}}},$$

wo die $\alpha_h^{(k)}$ sämtlich zu $p$ prim sind (*F. Q.*, p. 19 [[S. 22]]).

*Für einen Hauptrest $f$ wird die Größe $f\{p\}$ gleich einem Produkte aus der Potenz $2^{\lambda-1}$ und aus $\lambda$ Faktoren $\mathfrak{A}_k$, welche den $\lambda$ einzelnen Resten $\Phi_k$ entsprechen und folgende Bedeutung haben:*

$$\mathfrak{A}_k = \left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p^4}\right)\cdots\left(1 - \frac{1}{p^{2\left[\frac{\varkappa_k}{2}\right]}}\right)\cdot \mathfrak{a}_k,$$

*wo $\left[\frac{\varkappa_k}{2}\right]$ die größte in $\frac{\varkappa_k}{2}$ enthaltene ganze Zahl vorstellt, und $\mathfrak{a}_k = 1$ ist im Falle $\varkappa_k \equiv 1 \pmod 2$, dagegen:*

$$\mathfrak{a}_k = \left(1 + \theta_k \cdot p^{-\frac{\varkappa_k}{2}}\right)^{-1}, \quad \theta_k = \left(\frac{(-1)^{\frac{\varkappa_k}{2}}\cdot \Delta(\Phi_k)}{p}\right),$$

*wenn $\varkappa_k \equiv 0 \pmod 2$ ist.*

Die Richtigkeit dieser Formeln ergibt sich sofort mit Hilfe eines Schlusses von $\lambda - 1$ auf $\lambda$. Man bemerkt nämlich, daß dem Reste $f^{(\varkappa)}(\varkappa = \varkappa_1)$ in derselben Weise die Zahl $\lambda - 1$ zukommt wie dem Reste $f$ die Zahl $\lambda$.

## 6. Der Fall der Primzahl 2.

Wir behandeln jetzt den Fall $q = 2$, welcher auf etwas umständlicherem Wege zu gleich einfachen Resultaten führt. Die Form $f$ sei primitiv in bezug auf 2. Wir machen für dieselbe von den in **4.** angegebenen Bezeichnungen Gebrauch. Der Modul $2^t$ sei größer als die Potenz $2^{1+v_{n-1}}$; man hat dann immer $t \geqq 2$, und wenn $v_{n-1} > 0$, auch $t \geqq 3$.

Wir werden die Größen $f(2^t)$ finden, indem wir $f$ als *Hauptrest* für den Modul $2^t$ annehmen, also für $f$ den Typus zulassen:

$$f \equiv \{\Phi_1 + 2^{\omega\vartheta_1}[\Phi_2 + \cdots + 2^{\omega\vartheta_{\lambda-1}}(\Phi_\lambda)..]\} \pmod{2^t},$$

wo die einzelnen $\Phi_k$ Reste vorstellen, die in bezug auf 2 primitiv sind, und entweder dem Typus

$$(\mathrm{R_I}) \qquad \Phi_k \equiv \begin{pmatrix} \alpha_1^{(k)}, & & & \\ & \alpha_2^{(k)}, & & \\ & & \cdots & \\ & & & \alpha_{\varkappa_k}^{(k)} \end{pmatrix} \pmod{2^{t-v_{\vartheta_k-1}}}$$

oder, wenn $\varkappa_k$ gerade ist, auch dem Typus

$$(\mathrm{R_{II}}) \qquad \Phi_k \equiv \begin{pmatrix} 2\alpha_1^{(k)}, & A_1^{(k)}, & & & & \\ A_1^{(k)}, & 2\tilde{\alpha}_1^{(k)}, & & & & \\ & & \cdots & & & \\ & & \cdots & & & \\ & & & 2\alpha_{\frac{\varkappa_k}{2}}^{(k)}, & A_{\frac{\varkappa_k}{2}}^{(k)} \\ & & & A_{\frac{\varkappa_k}{2}}^{(k)}, & 2\tilde{\alpha}_{\frac{\varkappa_k}{2}}^{(k)} \end{pmatrix} \pmod{2^{t-v_{\vartheta_k-1}}}$$

angehören (*F. Q.*, p. 23 [[S. 25]]). Dabei bedeuten die $\alpha_h^{(k)}$, ebenso wie die $A_h^{(k)}$, lauter ungerade Größen.

Wir geben jedem Reste $\Phi_k$ vom Typus $(\mathrm{R_I})$ eine Zahl $\tau_k = 1$ und jedem Reste $\Phi_k$ vom Typus $(\mathrm{R_{II}})$ eine Zahl $\tau_k = 2$. Die $\varkappa_k - 1$ Invarianten $\sigma$ eines Restes $\Phi_k$ nennen wir $\varrho_1^{(k)}, \varrho_2^{(k)}, \ldots, \varrho_{\varkappa_k-1}^{(k)}$. Es gelten dann folgende Beziehungen (*F. Q.*, art. IV [[S. 28—29]]): wenn $\tau_k = 1$:

$$\varrho_h^{(k)} = 1;$$

wenn $\tau_k = 2$:

$$\varrho_{2h_0-1}^{(k)} = 2, \quad \varrho_{2h_0}^{(k)} = 1;$$

ferner:

$$\sigma_{\vartheta_{k-1}+h} = \varrho_h^{(k)}, \qquad (h = 1, 2, \ldots, \varkappa_k - 1)$$

und:

$$\sigma_{\vartheta_k} = 1,$$

so daß die Zahlen $\tau_k$ durch die Invarianten $\sigma_h$ bestimmt sind. In der Tat erhält man insbesondere:

$$\tau_k = \sigma_{\vartheta_{k-1}+1} = \sigma_{\vartheta_k-1}.$$

Ein Ausdruck von der Gestalt $\frac{1}{\tau}\Phi$ mag, je nachdem $\tau = 1$ oder $\tau = 2$ ist, kurz mit (I) oder mit (II) bezeichnet werden. Wir schicken zunächst einige Bemerkungen über die Kongruenzen

$$(\mathrm{I}) \equiv m \pmod 4 \quad \text{und} \quad (\mathrm{II}) \equiv m \pmod 2$$

voraus.

I. Für einen Ausdruck

$$\Psi \equiv \alpha_1 \xi_1^2 + \alpha_2 \xi_2^2 + \cdots + \alpha_\varkappa \xi_\varkappa^2 \pmod 4$$

mögen $\Psi_0, \Psi_1, \Psi_2, \Psi_3$ die Anzahlen der Lösungen von

$$\Psi \equiv 0, 1, 2, 3 \pmod 4$$

vorstellen. Diese 4 Anzahlen können leicht nach *F. Q.*, art. VIII [[S. 50 bis 58]], gefunden werden. Man setze nämlich

$$\begin{aligned} 4\Psi_0 &= \psi_0 + \psi_1 + \psi_2 + \psi_3, \\ 4\Psi_1 &= \psi_0 - i\psi_1 - \psi_2 + i\psi_3, \\ 4\Psi_2 &= \psi_0 - \psi_1 + \psi_2 - \psi_3, \\ 4\Psi_3 &= \psi_0 + i\psi_1 - \psi_2 - i\psi_3, \end{aligned}$$

wo $i = \sqrt{-1}$, und bilde die Einheiten:

$$(6_I)\qquad \varepsilon = (-1)^{\left[\frac{\varkappa}{2}\right]} \cdot (-1)^{\sum_{k=1}^{\varkappa} \frac{\alpha_k - 1}{2}},$$

$$\delta = (-1)^{\left[\frac{\varkappa}{4}\right]} \cdot (-1)^{\left[\frac{\varkappa}{2}\right]\left(\left[\frac{\varkappa}{2}\right] + \sum_{k=1}^{\varkappa} \frac{\alpha_k - 1}{2}\right)} \cdot (-1)^{\sum_{k'<k''}^{1,\varkappa} \frac{\alpha_{k'}-1}{2} \cdot \frac{\alpha_{k''}-1}{2}}.$$

Alsdann geben die Formeln *F. Q.*, p. 62 und p. 64 [[S. 55 und S. 57]]:

$$\psi_0 = 2^{2\varkappa}, \quad \psi_2 = 0$$

und

$$\psi_h = \left(\frac{1+\varepsilon}{2} - \frac{1-\varepsilon}{2} i\right) \varepsilon^{\frac{h-1}{2}} \cdot \delta \cdot (-i)^{\varkappa^2 \left(\frac{h-1}{2}\right)^2} \cdot \left(\frac{1+i}{\sqrt{2}}\right)^{\varkappa - 2\left[\frac{\varkappa}{2}\right]} \cdot 2^{\frac{3\varkappa}{2}}. \quad (h = 1, 3)$$

Wir unterscheiden die folgenden Fälle:

1. $\varkappa \equiv 0 \pmod 2$.

A) $\varepsilon = 1$; $\psi_1 = \delta \cdot 2^{\frac{3\varkappa}{2}}$, $\psi_3 = \delta \cdot 2^{\frac{3\varkappa}{2}}$.

$$4\Psi_0 = 2^{2\varkappa} + \delta \cdot 2^{\frac{3\varkappa}{2}+1},$$
$$4\Psi_2 = 2^{2\varkappa} - \delta \cdot 2^{\frac{3\varkappa}{2}+1},$$
$$4\Psi_1 = 4\Psi_3 = 2^{2\varkappa}.$$

B) $\varepsilon = -1$; $\psi_1 = -i\delta \cdot 2^{\frac{3\varkappa}{2}}$, $\psi_3 = i\delta \cdot 2^{\frac{3\varkappa}{2}}$.

$$4\Psi_0 = 4\Psi_2 = 2^{2\varkappa},$$
$$4\Psi_1 = 2^{2\varkappa} - \delta \cdot 2^{\frac{3\varkappa}{2}+1},$$
$$4\Psi_3 = 2^{2\varkappa} + \delta \cdot 2^{\frac{3\varkappa}{2}+1}.$$

2. $\varkappa \equiv 1 \pmod 2$.

A) $\varepsilon = 1$; $\psi_1 = \delta \cdot \frac{1+i}{\sqrt{2}} \cdot 2^{\frac{3\varkappa}{2}}$, $\psi_3 = \delta \cdot \frac{1-i}{\sqrt{2}} \cdot 2^{\frac{3\varkappa}{2}}$.

$$4\Psi_0 = 4\Psi_1 = 2^{2\varkappa} + \delta \cdot 2^{\frac{3\varkappa+1}{2}},$$
$$4\Psi_2 = 4\Psi_3 = 2^{2\varkappa} - \delta \cdot 2^{\frac{3\varkappa+1}{2}}$$

B) $\varepsilon = -1$; $\psi_1 = \delta \cdot \frac{1-i}{\sqrt{2}} \cdot 2^{\frac{3\varkappa}{2}}$, $\psi_3 = \delta \cdot \frac{1+i}{\sqrt{2}} \cdot 2^{\frac{3\varkappa}{2}}$.

$$4\Psi_0 = 4\Psi_3 = 2^{2\varkappa} + \delta \cdot 2^{\frac{3\varkappa+1}{2}},$$
$$4\Psi_2 = 4\Psi_1 = 2^{2\varkappa} - \delta \cdot 2^{\frac{3\varkappa+1}{2}}.$$

In betreff der Einheiten $\varepsilon$ und $\delta$ erwähnen wir noch einige Punkte.

1. Der Rest $l \equiv \alpha_1 + \alpha_2 + \cdots + \alpha_\varkappa \pmod 4$ ist durch die Einheit $\varepsilon$ bestimmt.

Da nämlich immer $\alpha_k \equiv 1 \pmod 2$ ist, so kommt zunächst

$$l \equiv \varkappa \pmod 2, \quad (-1)^l = (-1)^\varkappa.$$

Sind ferner von den Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_\varkappa$ im ganzen $\varkappa_0$ kongruent $-1 \pmod 4$ und $\varkappa - \varkappa_0$ kongruent $1 \pmod 4$, so folgt einerseits:

$$\varepsilon = (-1)^{\left[\frac{\varkappa}{2}\right] - \varkappa_0},$$

andererseits:

$$l \equiv (\varkappa - \varkappa_0) - \varkappa_0 \equiv \varkappa - 2\varkappa_0 \pmod 4,$$

mithin:

$$(-1)^{\left[\frac{l}{2}\right]} = (-1)^{\left[\frac{\varkappa}{2}\right] - \varkappa_0} = \varepsilon.$$

Im speziellen findet man, wenn $\varkappa \equiv 1 \pmod 2$:

$$l \equiv \varepsilon \pmod 4.$$

2. Ersetzt man $\Psi$ durch $-\Psi$, also $\alpha_k \pmod 4$ durch $-\alpha_k \pmod 4$, so mögen an die Stelle von $\varepsilon$ und $\delta$ die Einheiten $\varepsilon^-$ und $\delta^-$ treten. Man erhält unmittelbar:

$$\varepsilon^- = \varepsilon \cdot (-1)^\varkappa, \quad \delta^- = \delta \cdot \varepsilon^{\varkappa - 1},$$

also

1) $\varkappa \equiv 0 \pmod 2$: $\varepsilon^- = \varepsilon$, $\quad \delta^- = \delta \cdot \varepsilon$;

2) $\varkappa \equiv 1 \pmod 2$: $\varepsilon^- = -\varepsilon$, $\quad \delta^- = \delta$.

Dasselbe Resultat erschließt man auch leicht aus der aufgestellten Tabelle, indem man die Beziehungen $\Psi_{-h} = (-\Psi)_h$ beachtet.

3. Wir wollen

$$\Psi^1 \equiv \alpha_2 \xi_2^{\,2} + \cdots + \alpha_\varkappa \xi_\varkappa^{\,2} \pmod 4$$

setzen und die Einheiten $\varepsilon$ und $\delta$, welche zu $\Psi^1$ gehören, mit $\varepsilon^1$ und $\delta^1$ bezeichnen.

Mit Hilfe der Relationen

$$\left[\frac{\varkappa}{2}\right] - \left[\frac{\varkappa - 1}{2}\right] \equiv \varkappa - 1, \quad \left[\frac{\varkappa}{4}\right] - \left[\frac{\varkappa - 1}{4}\right] \equiv (\varkappa - 1)\left[\frac{\varkappa - 1}{2}\right] \pmod 2$$

findet man:

$$\varepsilon = (-1)^{\varkappa - 1} \cdot (-1)^{\frac{\alpha - 1}{2}} \cdot \varepsilon^1, \quad \delta = (-1)^{\varkappa \cdot \frac{\alpha - 1}{2}} \cdot \varepsilon^{(\varkappa - 1) + \frac{\alpha - 1}{2}} \cdot \delta^1, \quad (\alpha = \alpha_1)$$

also

1. $\varkappa \equiv 0 \pmod 2$;

   A) $\varepsilon = 1$: $\quad \delta = \delta^1$, $\quad \alpha \equiv -\varepsilon^1 \pmod 4$;

   B) $\varepsilon = -1$: $\quad \delta = -(-1)^{\frac{\alpha - 1}{2}} \cdot \delta^1$, $\quad \alpha \equiv \varepsilon^1 \pmod 4$.

2. $\varkappa \equiv 1 \pmod 2$;

   A) $\alpha \equiv -\varepsilon \pmod 4$: $\quad \varepsilon^1 = -1$, $\quad \delta = -\varepsilon \cdot \delta^1$;

   B) $\alpha \equiv \varepsilon \pmod 4$: $\quad \varepsilon^1 = 1$, $\quad \delta = \delta^1$.

II. Jetzt liege ein Ausdruck vor:

$$\mathsf{X} \equiv (\alpha_1 \xi_1^2 + A_1 \xi_1 \tilde{\xi}_1 + \tilde{\alpha}_1 \tilde{\xi}_1^2) + \cdots + \left(\alpha_{\frac{\varkappa}{2}} \xi_{\frac{\varkappa}{2}}^2 + A_{\frac{\varkappa}{2}} \xi_{\frac{\varkappa}{2}} \tilde{\xi}_{\frac{\varkappa}{2}} + \tilde{\alpha}_{\frac{\varkappa}{2}} \tilde{\xi}_{\frac{\varkappa}{2}}^2\right) \pmod 2,$$

und es bedeute $\mathsf{X}_0$ und $\mathsf{X}_1$ die Anzahl der Lösungen von

$$\mathsf{X} \equiv 0 \quad \text{und} \quad \mathsf{X} \equiv 1 \pmod 2.$$

Setzt man

$$2\mathsf{X}_0 = \chi_0 + \chi_1, \quad 2\mathsf{X}_1 = \chi_0 - \chi_1,$$

ferner:

$$(6_{\text{II}}) \qquad \theta = \left(\frac{2}{4\alpha_1 \tilde{\alpha}_1 - A_1^2}\right) \cdot \cdot \left(\frac{2}{4\alpha_{\frac{\varkappa}{2}} \tilde{\alpha}_{\frac{\varkappa}{2}} - A_{\frac{\varkappa}{2}}^2}\right),$$

so kommt nach *F. Q.*, p. 65 [[S. 58]]:

$$\chi_0 = 2^{\varkappa}, \quad \chi_1 = \theta \cdot 2^{\frac{\varkappa}{2}},$$

also:

$$2\mathsf{X}_0 = 2^{\varkappa} + \theta \cdot 2^{\frac{\varkappa}{2}}, \quad 2\mathsf{X}_1 = 2^{\varkappa} - \theta \cdot 2^{\frac{\varkappa}{2}}.$$

Nach diesen Vorbereitungen wollen wir versuchen, eine Formel aufzustellen, mit deren Hilfe die Größen $f(2^t)$ für Reste von $n(>1)$ Variablen auf entsprechende Größen für Reste von weniger als $n$ Variablen zurückgeführt werden können. Für Reste $f$ von einer Variablen hat man einfach $f(2^t) = 1$.

Da wir $f$ als Hauptrest für den Modul $2^t$ voraussetzen, so gilt jedenfalls eine Kongruenz

$$f \equiv \Phi_1 + 2^{\omega_{\varkappa_1}} f^{(\varkappa_1)} \pmod{2^t}, \qquad (\omega_{\varkappa_1} \geqq 1)$$

wo $\Phi_1$ einen Rest vom Typus ($\text{R}_{\text{I}}$) oder ($\text{R}_{\text{II}}$) bedeutet. Wir unterscheiden zwei Fälle, je nachdem die Invariante $\tau_1 = \sigma_1$ den Wert 1 oder 2 erhält.

$(\sigma_1 = 1)$.

Ist zunächst $\sigma_1 = 1$, so läßt $f$ sich zugleich in der Form schreiben:

$$f \equiv \alpha \xi^2 + 2^{\omega_1} f^{(1)} \pmod{2^t},$$

wo $\alpha$ ungerade ist und $f^{(1)}$ einen in bezug auf 2 primitiven Rest vorstellt, welcher im Falle $\omega_1 = 0\,(\varkappa_1 > 1)$ eine erste Invariante $\sigma$ gleich 1 ergibt. Überhaupt folgen die Invarianten $\sigma_h^{(1)}$ und $2^{\omega_h^{(1)}}$ von $f^{(1)}$ aus den Gleichungen:

$$\sigma_{h-1}^{(1)} = \sigma_h, \quad \omega_{h-1}^{(1)} = \omega_h. \qquad (h = 2, 3, \ldots, n-1)$$

Die Anzahl $f(2^t)$ der inkongruenten Substitutionen $\mathsf{T}$ von einer Determinante $\equiv 1 \pmod{2^t}$, welche den Rest $f$ in sich selbst überführen, drückt sich in ähnlicher Weise aus wie oben die Zahl $f(p^t)$. In der Tat, die erste Vertikalreihe einer Substitution $\mathsf{T}$ muß immer von $n$ Zahlen $\xi_i \pmod{2^t}$ gebildet sein, welche

$$(3) \qquad f(\xi_i) \equiv \alpha \pmod{2^t}$$

liefern. Dazu tritt in den Fällen, wo $\varkappa_1 > 1$ ist, noch die Bedingung, daß nicht zu gleicher Zeit die sämtlichen Kongruenzen

$$\xi_1 \equiv 1,\ \xi_2 \equiv 1,\ \ldots,\ \xi_{\varkappa_1} \equiv 1 \pmod 2 \tag{7}$$

bestehen dürfen (*F. Q.*, p. 172 und 128 [[S. 139 und 106]]). Wir bezeichnen mit $A \cdot 2^{(n-1)t}$, je nachdem $\varkappa_1 = 1$ oder $> 1$ ist, entweder die Anzahl aller möglichen Lösungen $\xi_i$ von (3) oder nur die Anzahl aller derjenigen Lösungen $\xi_i$, welche nicht zugleich die Kongruenzen (7) erfüllen.

Die Betrachtungen in *F. Q.*, p. 172 [[S. 139]], zeigen, daß wirklich jedem dieser Systeme $\xi_i$ Substitutionen $\mathsf{T}$ entsprechen, welche den Rest $f$ in sich selbst transformieren. Ebenso wie in **5.** schließt man dann, daß jedes solche System $\xi_i$ zu genau soviel verschiedenen $\mathsf{T}$ Veranlassung gibt, als verschiedene Substitutionen von einer Determinante $\equiv 1 \pmod{2^t}$ existieren, welche auf den Rest $2^{\omega_1} f^{(1)}$ ohne Wirkung sind. So gewinnt man die Beziehung:

$$f(2^t) = 2^{(n-1)t + \omega_1[(n-1)^2-1]} \cdot A \cdot f^{(1)}(2^{t-\omega_1}).$$

In betreff der Größe $A$ unterscheiden wir die Fälle $\varkappa_1 = 1$ und $\varkappa_1 > 1$.

1. Ist zunächst $\varkappa_1 = 1$, so gibt unsere Annahme über $t$ (wenn $n > 1$) jedenfalls $t \geqq 3$. Nach dem Satze **4.** (C) muß daher $A \cdot 2^{3(n-1)}$ die Anzahl der Lösungen von $f(\xi_i) \equiv \alpha \pmod 8$ ausdrücken.

Indem man in $f$ alle Glieder fortläßt, welche durch 8 teilbar sind, erlangt $f$ entweder den Typus:

$$f \equiv \alpha\xi^2 \pmod 8. \tag{8}$$

In diesem Falle hat man $f \equiv \alpha \pmod 8$, sobald $\xi \equiv 1 \pmod 2$ ist. Die Anzahl der Lösungen von $f \equiv \alpha \pmod 8$ beträgt demnach $4 \cdot 2^{3(n-1)}$ und man findet:

$$A = 4.$$

Oder $f$ gehört einem der beiden Typen an:

$$\left.\begin{aligned} f &\equiv \alpha\xi^2 + 4(\mathrm{I}) \\ f &\equiv \alpha\xi^2 + 4(\mathrm{II}) + 4(\mathrm{I}) \end{aligned}\right\} \pmod 8. \tag{9}$$

In dem Ausdrucke 4(I) erscheint mindestens ein Glied $4\mathfrak{a}\mathfrak{x}^2 \equiv 4\mathfrak{x} \pmod 8$. Durch Änderung des Restes von $\mathfrak{x} \pmod 2$ können wir aus jeder Lösung von $f \equiv \alpha \pmod 8$ eine solche von $f \equiv \alpha + 4 \pmod 8$ herleiten, und umgekehrt. Diese zwei Kongruenzen besitzen also gleich viel, nämlich $2 \cdot 2^{3(n-1)}$ Lösungen, und man erhält:

$$A = 2.$$

Oder $f$ gehört dem Typus an:

$$f \equiv \alpha\xi^2 + 4(\mathrm{II}) \pmod 8. \tag{10}$$

In diesem Falle hat $f \equiv \alpha \pmod 8$ stets $\xi \equiv 1 \pmod 2$ und $(\mathrm{II}) \equiv 0 \pmod 2$ zur Folge. Bildet man für den Rest (II) von $\varkappa_2 = \varkappa$ Variablen,

nach der Formel $(6_{II})$, eine Einheit $\theta$, so ergibt sich die Anzahl der Lösungen von $(II) \equiv 0 \pmod 2$ gleich $2^{\varkappa-1}\left(1+\theta\cdot 2^{\frac{-\varkappa}{2}}\right)$, und man bekommt

$$A = 2\left(1+\frac{\theta}{2^{\frac{\varkappa}{2}}}\right).$$

Oder $f$ gehört dem Typus an:

$$f \equiv \alpha\xi^2 + 2(I) \pmod 8. \tag{11}$$

Dann ist $f \equiv \alpha \pmod 8$ identisch mit $\xi \equiv 1 \pmod 2$ und $(I) \equiv 0 \pmod 4$. Gehören zu dem Reste (I) von $\varkappa_2 = \varkappa$ Variablen, gemäß der Formel $(6_I)$, zwei Einheiten $\varepsilon$ und $\delta$, so liefert die obige Tabelle:

1) $\varkappa \equiv 0 \pmod 2$,

$$\varepsilon = 1: \qquad A = \left(1+\frac{\delta}{2^{\frac{\varkappa}{2}-1}}\right);$$

$$\varepsilon = -1: \qquad A = 1.$$

2) $\varkappa \equiv 1 \pmod 2$,

$$A = \left(1+\frac{\delta}{2^{\frac{\varkappa-1}{2}}}\right).$$

Oder $f$ gehört endlich dem Typus an:

$$f \equiv \alpha\xi^2 + 2(I) + 4(I)_1 \pmod 8. \tag{12}$$

In diesem Falle enthält $2(I)$ mindestens ein Glied $2\mathfrak{a}\mathfrak{x}^2 \equiv 2\mathfrak{x} \pmod 4$, mit dessen Hilfe die Lösungen von $f \equiv 1$ und $f \equiv 3 \pmod 4$ einander eindeutig zugeordnet werden können; und ebenso erscheint in $4(I)_1$ mindestens ein Glied $4\mathfrak{a}\mathfrak{x}^2 \equiv 4\mathfrak{x} \pmod 8$, infolge dessen die Kongruenzen $f \equiv \alpha$ und $f \equiv \alpha + 4 \pmod 8$ gleich viel Lösungen zulassen. So findet man leicht:

$$A = 1.$$

2. Jetzt sei $\varkappa_1 > 1$. Wir teilen für einen Moment die Systeme $\xi_i$, welche $f(\xi_i) \equiv 1 \pmod 2$ ergeben, in Systeme erster oder zweiter Art ein, je nachdem sie den Bedingungen (7) entgegen sind oder mit denselben harmonieren. Irgendein System $\xi_i \pmod 4$ erster Art möge die Kongruenz

$$f(\xi_i) \equiv \alpha \pmod 4 \tag{13}$$

erfüllen. Da ein solches System zugleich einen bestimmten Wert des Restes $f(\xi_i) \pmod 8$ ergibt, so wird es nur einer der beiden Kongruenzen $f(\xi_i) \equiv \alpha \pmod 8$ und $f(\xi_i) \equiv \alpha + 4 \pmod 8$ Genüge leisten. Ist nun von den Zahlen $\xi_1, \xi_2, \ldots, \xi_{\varkappa_1}$ etwa $\xi_k$ die erste, welche nicht ungerade ausfällt, und ändern wir den Rest $\xi_k \pmod 4$ in $\xi_k + 2 \pmod 4$, so geht aus dem Systeme $\xi_i \pmod 4$ ein anderes System erster Art hervor, welches offenbar der anderen von diesen beiden Kongruenzen genügen muß. So erhellt, daß diese zwei Kongruenzen gleich viel Lösungen erster Art zulassen.

Beachtet man jetzt die Definition der Größe $A$ und den Satz **4.** (C), so folgt, daß in allen Fällen die Anzahl der Lösungen erster Art von (13) durch $A \cdot 2^{2(n-1)}$ ausgedrückt ist. Man gelangt zu dieser Anzahl, indem man die Anzahl aller möglichen Lösungen dieser Kongruenz um die Anzahl ihrer Lösungen zweiter Art vermindert.

Wir unterscheiden die Fälle $\varkappa_1 \equiv 0 \pmod 2$ und $\varkappa_1 \equiv 1 \pmod 2$, schreiben aber der Einfachheit halber $\varkappa$ für $\varkappa_1$.

$1^0$. Zunächst sei $\varkappa \equiv 0 \pmod 2$. In diesem Falle treten überhaupt keine Lösungen zweiter Art auf, da die Kongruenzen (7) stets $f(\xi_i) \equiv \varkappa \pmod 2$ nach sich ziehen.

Entweder ist nun $f$ von dem Typus:

$$f \equiv (\mathrm{I}) \pmod 4. \tag{14}$$

Lassen wir dieselben Bezeichnungen wie oben für $\Psi$ gelten, so liefert die aufgestellte Tabelle:

$$\varepsilon = 1: \qquad A = 1; \qquad [\delta = \delta^1, (-1)^{\frac{\alpha-1}{2}} = -\varepsilon^1]$$

$$\varepsilon = -1: \qquad A = \left(1 + \frac{\delta^1}{2^{\frac{\varkappa}{2}-1}}\right). \qquad [\delta = -(-1)^{\frac{\alpha-1}{2}} \cdot \delta^1, \ (-1)^{\frac{\alpha-1}{2}} = \varepsilon^1]$$

Oder $f$ ist von dem Typus:

$$f \equiv (\mathrm{I}) + 2(\mathrm{I})_1 \pmod 4. \tag{15}$$

Alsdann erscheint in $2(\mathrm{I})_1$ ein Glied $2\mathfrak{a}\mathfrak{x}^2 \equiv 2\mathfrak{x} \pmod 4$, welches bewirkt, daß $f \equiv 1$ und $f \equiv 3 \pmod 4$ gleich viel Lösungen zulassen. Demnach kommt einfach:

$$A = 1.$$

$2^0$. Endlich sei $\varkappa \equiv 1 \pmod 2$. Wir unterscheiden dieselben zwei Fälle.

Entweder ist $f$ von dem Typus:

$$f \equiv (\mathrm{I}) \pmod 4. \tag{14}$$

Identifizieren wir den Rest (I) mit dem obigen Ausdrucke $\Psi$, so entsteht für Systeme $\xi_i$ zweiter Art:

$$f(\xi_i) \equiv \alpha_1 + \alpha_2 + \cdots + \alpha_\varkappa \equiv \varepsilon \pmod 4.$$

Diese Systeme gehen also nur den Fall an, wo $\alpha \equiv \varepsilon \pmod 4$ ist. Mithin kommt:

$$\alpha \equiv -\varepsilon \pmod 4: \qquad A = \left(1 - \frac{\delta}{2^{\frac{\varkappa-1}{2}}}\right); \qquad [\varepsilon^1 = -1, \ \delta = -\varepsilon \cdot \delta^1]$$

$$\alpha \equiv \varepsilon \pmod 4: \qquad A = \left(1 + \frac{\delta}{2^{\frac{\varkappa-1}{2}}} - \frac{1}{2^{\varkappa-2}}\right) = \left(1 - \frac{\delta}{2^{\frac{\varkappa-1}{2}}}\right)\left(1 + \frac{\delta^1}{2^{\frac{\varkappa-3}{2}}}\right) \cdot$$

$$[\varepsilon^1 = 1, \ \delta = \delta^1]$$

Oder $f$ ist vom Typus:

$$f \equiv (\mathrm{I}) + 2(\mathrm{I})_1 \pmod 4. \tag{15}$$

Alsdann bewirkt ein jedes Glied $2\alpha\mathfrak{x}^2 \equiv 2\mathfrak{x} \pmod 4$ aus $2(\mathrm{I})_1$, daß $f \equiv 1$ und $f \equiv 3 \pmod 4$ sowohl gleich viel Lösungen erster, wie gleichviel Lösungen zweiter Art besitzen, und man findet:

$$A = \left(1 - \frac{1}{2^{\varkappa-1}}\right)\cdot$$

$$\underline{(\sigma_1 = 2).}$$

Wenn $\sigma_1 = 2$ ist, so läßt $f$ sich zugleich in der Form schreiben:

$$f \equiv 2(\alpha\xi^2 + \mathsf{A}\xi\tilde{\xi} + \tilde{\alpha}\tilde{\xi}^2) + 2^{\omega_2} f^{(2)} \pmod{2^t},$$

wo $\alpha$ und $\mathsf{A}$ ungerade sind, und $f^{(2)}$ einen in bezug auf 2 primitiven Rest bedeutet. Die Invarianten $\sigma_h^{(2)}$ und $2^{\omega_h^{(2)}}$ von $f^{(2)}$ bestimmen sich aus den Gleichungen:

$$\sigma^{(2)}_{h-2} = \sigma_h, \qquad \omega^{(2)}_{h-2} = \omega_h. \qquad (h = 3, 4, \ldots, n-1)$$

Wir betrachten die $f(2^t)$ Substitutionen $\mathsf{T}$ von einer Determinante $\equiv 1 \pmod{2^t}$, welche den Rest $f$ in sich selbst verwandeln. In jeder dieser Substitutionen muß die erste Vertikalreihe von $n$ Zahlen $\xi_i \pmod{2^t}$ gebildet werden, welche

$$f(\xi_i) \equiv 2\alpha \pmod{2^t} \tag{3}$$

ergeben. Ferner dürfen diese Zahlen nicht zugleich alle Bedingungen

$$\xi_1 \equiv 0,\ \xi_2 \equiv 0,\ \ldots,\ \xi_{\varkappa_1} \equiv 0 \pmod 2 \tag{7}$$

erfüllen (*F. Q.*, p. 175 und 129 [[S. 141 und 107]]). Wir bezeichnen mit $2A \cdot 2^{(n-1)t}$ die Anzahl aller Systeme $\xi_i \pmod{2^t}$, welche der Kongruenz (3), aber nicht sämtlichen Kongruenzen (7) genügen.

Jedes dieser Systeme $\xi_i$ tritt wirklich in mindestens einer von den Substitutionen $\mathsf{T}$ als erste Vertikalreihe auf (*F. Q.*, pp. 175—177 [[S. 141—142]]), also etwa in einem $\mathsf{T}_0$. Es fragt sich, für wieviel verschiedene $\mathsf{T}$ ein solches System $\xi_i$ die erste Vertikalreihe bildet; offenbar für alle diejenigen $\mathsf{T}$, welche zusammengesetzt sind aus $\mathsf{T}_0$ und aus einer Substitution $T$ mit der ersten Vertikalreihe $1, 0, \ldots, 0$. Man hat also zu ermitteln, wie viele Substitutionen vom Typus

$$T \equiv \begin{vmatrix} 1, & U & , \ldots\ldots \\ 0, & \eta_0 & , \ldots\ldots \\ 0, & \eta_1 & , \ldots\ldots \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot \\ 0, & \eta_{n-2}, & \ldots\ldots \end{vmatrix} \equiv 1 \pmod{2^t}$$

den Rest $f$ in sich selbst transformieren.

Setzen wir

$$f^{(1)} \equiv (4\alpha\tilde{\alpha} - \mathsf{A}^2)\eta_0^2 + 2^{\omega_2+1}\cdot\alpha\cdot f^{(2)}(\eta_1, \ldots, \eta_{n-2}) \pmod{2^{t+1}},$$

so entsteht zunächst die Bedingung

$$f^{(1)}(\eta_0, \eta_1, \ldots, \eta_{n-2}) \equiv (4\alpha\tilde{\alpha} - \mathsf{A}^2) \pmod{2^{t+1}}.$$

Dieser Kongruenz mögen $\frac{1}{2}A^{(1)} \cdot 2^{(n-2)t}$ verschiedene Systeme $\eta_i \pmod{2^t}$ Genüge leisten. Durch Überlegungen, wie sie in *F. Q.*, pp. 176—177 [[S. 141—142]], angestellt sind, überzeugt man sich, daß wirklich jedem dieser Systeme $\eta_i$ Substitutionen $T$ zukommen, welche den Rest $f$ in sich selbst transformieren; es fragt sich wieviele.

Die Gesamtheit aller solcher $T$ wird hervorgehen, indem man eine beliebige unter ihnen, etwa $T_0$, mit allen Substitutionen

$$\mathfrak{T} \equiv \begin{vmatrix} 1, & U, & V_1, & \ldots, & V_{n-2} \\ 0, & 1, & \tilde{V}_1, & \ldots, & \tilde{V}_{n-2} \\ 0, & 0, & t_1^1, & \ldots, & t_1^{n-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & t_{n-2}^1, & \ldots, & t_{n-2}^{n-2} \end{vmatrix} \equiv 1 \pmod{2^t}$$

zusammensetzt, welche $f \pmod{2^t}$ in sich selbst überführen. Für $\mathfrak{T}$ findet man $2U \equiv 0$, $V_h \equiv 0$, $\tilde{V}_h \equiv 0 \pmod{2^t}$; und man erkennt, daß die Anzahl der verschiedenen $\mathfrak{T}$ durch $2F(2^t)$ ausgedrückt ist, falls $F$ den Rest $2^{\omega_2}f^{(2)}$ bedeutet. So ergibt sich die Beziehung

$$f(2^t) = 2^{(n-1)t+(n-2)t+1+\omega_2[(n-2)^2-1]} \cdot A \cdot A^{(1)} \cdot f^{(2)}(2^{t-\omega_2}).$$

Nun hat man zugleich

$$f^{(1)}(2^{t+1}) = 2^{(n-2)(t+1)+(\omega_2+1)[(n-2)^2-1]} \cdot A^{(1)} \cdot f^{(2)}(2^{t-\omega_2});$$

also kommt endlich:

$$f(2^t) = 2^{(n-1)t-n(n-3)} \cdot A \cdot f^{(1)}(2^{t+1}).$$

Um die Größe $A$ zu finden, beachte man, daß das System der $\varkappa_1$ Kongruenzen (7) sich als identisch mit dem Systeme $\frac{1}{2}\frac{\partial f}{\partial \xi_i} \equiv 0 \pmod 2$ $(i = 1, 2, \ldots, n)$ erweist. Nach **4.** (D) muß infolgedessen $A \cdot 2^{n-1}$ die Anzahl aller Lösungen von

$$\frac{1}{2}f(\xi_i) \equiv 1 \pmod 2 \tag{13}$$

vorstellen, bei welchen die $n$ Zahlen $\frac{1}{2}\frac{\partial f}{\partial \xi_i}$ nicht sämtlich gerade sind. Wir wollen für $\varkappa_1$ einfach $\varkappa$ setzen.

Entweder ist $\frac{1}{2}f$ vom Typus:

$$\frac{1}{2}f \equiv (\mathrm{II}) \pmod 2. \tag{14}$$

In diesem Falle liefern die Kongruenzen (7) stets $f \equiv 0 \pmod 4$; sie sind also nicht mit (13) verträglich. Gehört zu (II) wie oben eine Einheit $\theta$, so kommt demnach:

$$A = \left(1 - \frac{\theta}{2^{\frac{\varkappa}{2}}}\right).$$

Oder $\frac{1}{2} f$ ist vom Typus:

[15] $$\frac{1}{2} f \equiv (\mathrm{II}) + (\mathrm{I}) \pmod 2.$$

Dann erscheint in (I) ein Glied $\mathfrak{a}\mathfrak{x}^2 \equiv \mathfrak{x} \pmod 2$, welches zur Folge hat, daß $\frac{1}{2} f \equiv 0$ und $\frac{1}{2} f \equiv 1 \pmod 2$ gleich viel Lösungen zulassen, man betrachte diese Kongruenzen für sich oder zusammen mit den Kongruenzen (7). Man erhält also:

$$A = \left(1 - \frac{1}{2^{\varkappa}}\right).$$

Die Größe $A^{(1)}$ bestimmt sich mit Hilfe der Formeln aus $(\sigma_1 = 1)$ Im Falle [14] findet man, wenn $\varkappa = 2$: $A^{(1)} = 4$, und wenn $\varkappa > 2$:

$$A^{(1)} = 2\left(1 + \frac{\theta^1}{2^{\frac{\varkappa}{2}-1}}\right), \quad \text{wobei} \quad \theta = \left(\frac{2}{4\alpha\tilde{\alpha} - \mathsf{A}^2}\right) \cdot \theta^1;$$

im Falle [15] wird immer $A^{(1)} = 2$.

---

Wir setzen jetzt allgemein:

$$f(2^t) = 2^{\frac{n(n-1)}{2}t + \sum_{h=1}^{n-1} \omega_h \left(\frac{(n-h)(n-h+1)}{2} - 1\right)} \cdot \prod_{h=1}^{n-1} \sigma_h \cdot f\{2\}. \quad \left(t > 1 + \sum_{h=1}^{n-1} \omega_h\right)$$

*Unsere Rekursionsformeln gehen dann in*

$$f\{2\} = A \cdot f^{(1)}\{2\}$$

*über,* und auf Grund der gefundenen Werte von $A$ können wir den vollständigen Ausdruck der Größe $f\{2\}$ hinschreiben.

Es bedeute, wie bisher, $f$ einen aus $\lambda$ Gliedern bestehenden Hauptrest, wo $\lambda$ gleich ist der um 1 vermehrten Anzahl aller durch 2 teilbaren Größen $2^{\omega_h}$ $(h = 1, \ldots, n-1)$. Ferner bezeichne $\mu - 1$ die Anzahl aller Größen aus der Reihe $\sigma_{h-1} 2^{\omega_h} \sigma_{h+1}$ $(h = 1, \ldots, n-1)$, welche den Faktor 4 enthalten, und $\nu - 1$ die Anzahl aller Größen dieser Reihe welche durch 8 aufgehen.

*Die Größe $f\{2\}$ ist dann gleich einem Produkte aus der Potenz* $\frac{2^{(2\mu-1)+(\nu-1)}}{\Pi\sigma_h}$ *und aus $\lambda$ Faktoren $\mathfrak{A}_k$, welche den $\lambda$ einzelnen Resten $\Phi_k$ entsprechen und folgendermaßen bestimmt werden:*

(I). *So oft $\Phi_k$ ein Rest vom Typus* $(\mathrm{R_I})$ *ist, nehme man:*

$$\mathfrak{A}_k = \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{2^4}\right) \cdots \left(1 - \frac{1}{2^{2\left[\frac{\varkappa_k - 1}{2}\right]}}\right) \cdot \mathfrak{a}_k,$$

*und setze* $\mathfrak{a}_k = 1$, *falls die Zahlen* $\tau_{k-1} \cdot 2^{\omega_{\vartheta_k - 1}}$ *und* $2^{\omega_{\vartheta_k}} \cdot \tau_{k+1}$ *nicht beide durch* 4 *teilbar sind; andernfalls aber bilde man für* $\Phi_k$, *gemäß den Formeln* $(6_{\mathrm{I}})$, *zwei Einheiten* $\varepsilon_k$ *und* $\delta_k$, *und setze:*

1) *wenn* $\varkappa_k \equiv 0 \pmod 2$,

*je nachdem* $\varepsilon_k = 1$ *oder* $= -1$ *ist,*

$$\mathfrak{a}_k = \left(1 + \delta_k \cdot 2^{-\frac{\varkappa_k}{2}+1}\right)^{-1} \quad \text{oder} \quad = 1;$$

2) *wenn* $\varkappa_k \equiv 1 \pmod 2$,

$$\mathfrak{a}_k = \left(1 + \delta_k \cdot 2^{-\frac{\varkappa_k - 1}{2}}\right)^{-1}.$$

(II). *So oft* $\Phi_k$ *ein Rest vom Typus* $(\mathrm{R}_{\mathrm{II}})$ *ist, nehme man:*

$$\mathfrak{A}_k = \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{2^4}\right) \cdots \left(1 - \frac{1}{2^{\varkappa_k}}\right) \cdot \mathfrak{a}_k,$$

*und setze* $\mathfrak{a}_k = 1$, *falls die Zahlen* $\tau_{k-1} \cdot 2^{\omega_{\vartheta_k - 1}}$ *und* $2^{\omega_{\vartheta_k}} \cdot \tau_{k+1}$ *nicht beide durch* 4 *teilbar sind; andernfalls aber bilde man für* $\Phi_k$, *gemäß der Formel* $(6_{\mathrm{II}})$, *eine Einheit* $\theta_k$, *und setze:*

$$\mathfrak{a}_k = \left(1 + \theta_k \cdot 2^{-\frac{\varkappa_k}{2}}\right)^{-1}.$$

Die Richtigkeit dieser Ausdrücke ergibt sich mit Hilfe eines Schlusses von $n-1$ auf $n$.

Wir erwähnen noch folgende Relation. Bedeutet $M - 1$ die Anzahl aller durch 4 teilbaren Größen $\tau_k \cdot 2^{\omega_{\vartheta_k}} \cdot \tau_{k+1}$, so hat man

$$2^{\mu - 1} = 2^{M-1} \cdot \frac{\sigma_1 \sigma_2 \cdots \sigma_{n-1}}{\tau_1 \tau_2 \cdots \tau_\lambda}.$$

Die Kongruenzen $f(\xi_i) \equiv m \pmod{2^t}$ sind sehr eingehend von Herrn C. Jordan in der Abhandlung *Sur la forme canonique des congruences du second degré et le nombre de leurs solutions**) untersucht worden. Die über diesen Gegenstand hier angestellten Betrachtungen sind indes wesentlich anderer Art. Die am Anfange gegebenen Werte der Zahlen $\Psi_h$ und $\chi_h$ wird man auch aus Art. 8 des *Mémoire sur la représentation des nombres par des sommes de cinq carrés***) von H. Smith ableiten können.

## 7. Die Größen $f\{q\}$ in ihrer Abhängigkeit von den Charakteren $C$.

Die Einheiten, welche in den Größen $f\{q\}$ auftreten, sind offenbar Invarianten der Form $f$. Sie müssen sich daher mit Hilfe der besonderen Charaktere $C$ ausdrücken lassen, die wir in **2.** aufgezählt haben.

Um dieses darzutun, setzen wir $f$, wie in **2.**, als charakteristische Form

---

*) Journal de Liouville, Deuxième Série, T. XVII, 1872, pp. 368—402.

**) Mémoires présentés à l'Académie des Sciences de Paris, T. XXIX, No. 1. (Collected Papers, vol. II, p. 623.)

ihres Genus voraus. Die aus den ersten $h$ Reihen von $f$ gebildeten symmetrischen Minoren mögen also Werte $\sigma_h d_{h-1}\varphi_h$ von solcher Art liefern, daß ein jedes $\varphi_h$ relativ prim zu $2o_1o_2\ldots o_{n-1}$ und zu $\varphi_{h-1}\cdot\varphi_{h+1}$ ausfällt. Ferner sei $f$ primitiv.

Bedeutet $q$ zunächst irgendeine ungerade Primzahl, die nicht in $\Delta$ aufgeht, so hängt $f\{q\}$, außer von der Zahl $n$, nur in dem Falle eines geraden $n$, noch von einer Einheit $\theta$ ab. Man findet dieselbe gleich

$$\left(\frac{(-1)^{\frac{n}{2}}\Delta}{q}\right)=\left(\frac{(-1)^{\frac{n}{2}-1}o_1o_3\ldots o_{n-3}o_{n-1}}{q}\right).$$

Ist weiter $q=p$ irgendeine ungerade Primzahl aus $\Delta$, so sind, laut Voraussetzung, sämtliche Zahlen $\varphi_h$ zu $p$ prim. Wir besitzen also in $f$ eine *Grundform* für den Modul $p$ (*F. Q.*, pp. 35—36 [[S. 34—35]]). Die Klasse $f$ liefert infolgedessen für einen jeden Modul $p^t$ unter anderen Resten auch folgenden Hauptrest:

$$\varphi\equiv\left\{\begin{array}{cccc}\frac{\sigma_1\varphi_1}{\sigma_0\varphi_0}, & & & \\ & o_1\cdot\frac{\sigma_2\varphi_2}{\sigma_1\varphi_1}, & & \\ & & \ldots & \\ & & & o_1o_2\ldots o_{n-1}\cdot\frac{\sigma_n\varphi_n}{\sigma_{n-1}\varphi_{n-1}}\end{array}\right\}\pmod{p^t}.$$

In dem Ausdrucke von $f\{p\}=\varphi\{p\}$ gehört zu jeder von den $\lambda$ Zahlen $\varkappa_k$, welche gerade ausfällt, eine Einheit $\theta$. Setzt man $\vartheta_{k-1}=r$ $\vartheta_k=s$, und ist also $s-r=\varkappa_k\equiv 0\pmod 2$, so nimmt eine solche Einheit den Wert an:

$$\left(\frac{(-1)^{\frac{s-r}{2}}o_{r+1}o_{r+3}\ldots o_{s-3}o_{s-1}\cdot\sigma_r\varphi_r\sigma_s\varphi_s}{p}\right).$$

Endlich sei $q=2$. Nach Voraussetzung sind alle Zahlen $\varphi_h$ ungerade, und $f$ stellt eine *Grundform* für den Modul 2 vor. Man gewinnt daher, nach *F. Q.*, pp. 34—36 [[S. 33—35]] einen Hauptrest

$$\varphi\equiv\{\Phi_1+2^{\omega\vartheta_1}[\Phi_2+\cdots+2^{\omega\vartheta_{\lambda-1}}(\Phi_\lambda)\cdot\cdot]\}\pmod{2^t}$$

der Klasse $f$, indem man die Einzelreste $\Phi_k$ in folgender Weise auswählt. Zur Abkürzung sei $\vartheta_{k-1}=r$, $\vartheta_k=s$; dann nehme man, wenn $\tau_k=1$:

$$\left.\begin{array}{c}\frac{2^{\sigma_r}\cdot\Phi_k}{o_1o_2\ldots o_r}\equiv\psi_1+o_{r+1}\psi_2+\cdots+o_{r+1}o_{r+2}\ldots o_{s-1}\psi_{s-r}\\ \psi_i\equiv\frac{\varphi_{r+i}}{\varphi_{r+i-1}}\xi_i^2\end{array}\right\}\pmod{2^{t-\sigma_r}},$$

und wenn $\tau_k=2$, also jedenfalls $s-r\equiv 0\pmod 2$:

$$\left.\begin{aligned} \frac{2^{v_r}}{o_1 o_2 \dots o_r} \cdot \Phi_k &\equiv \psi_1 + o_{r+1} o_{r+2} \psi_2 + \dots + o_{r+1} o_{r+2} \dots o_{s-2} \psi_{\frac{s-r}{2}} \\ \psi_i &\equiv \frac{2\varphi_{r+2i-1}}{\varphi_{r+2i-2}} \xi_i^2 + 2 A_i \xi_i \eta_i + \frac{o_{r+2i-1} \varphi_{r+2i} - A_i^2 \varphi_{r+2i-2}}{2\varphi_{r+2i-1}} \eta_i^2 \end{aligned}\right\} (\mathrm{mod}\, 2^{t-v_r}),$$

wo die $A_i$ irgendwelche ungerade Zahlen bedeuten sollen.

So oft nun $\tau_k = 1$ ist und die Zahlen $\sigma_{r-1} 2^{v_r}$ und $2^{v_s} \sigma_{s+1}$ beide durch 4 teilbar sind, kommen für den Ausdruck $f\{2\}$ zwei aus den Koeffizienten von $\Phi_k$ gebildete Einheiten $\varepsilon$ und $\delta$ in Betracht. Indem man wiederholt die für ungerade $a$ und $\alpha$ geltende Kongruenz

$$\frac{a\alpha - 1}{2} \equiv \frac{a-1}{2} + \frac{\alpha - 1}{2} \pmod 2$$

anwendet, ergibt sich $\varepsilon$ als eine Potenz von $-1$ mit dem Exponenten:

$$\frac{\varphi_r - 1}{2} + \frac{\varphi_s - 1}{2} + \sum \frac{o_{s-2u+1} + 1}{2}, \quad \left(u = 1, 2, \dots, \left[\frac{s-r}{2}\right]\right)$$

während $\delta$ aus zwei Potenzen von $-1$ zusammengesetzt erscheint, von denen die eine den Exponenten:

$$\frac{\varphi_r - 1}{2} \cdot \frac{\varphi_{r+1} - 1}{2} + \frac{\varphi_{r+1} - 1}{2} \cdot \frac{\varphi_{r+2} - 1}{2} + \dots + \frac{\varphi_{s-1} - 1}{2} \cdot \frac{\varphi_s - 1}{2} + \sum_{h=r+1}^{s-1} \frac{\varphi_h - 1}{2} \cdot \frac{o_h + 1}{2}$$

und die andere den Exponenten:

$$\frac{\varphi_r + (-1)^{s-r}}{2} \cdot \left(\frac{\varphi_s - 1}{2} + \sum \frac{o_{s-2u+1} + 1}{2}\right) + \frac{\varphi_s - 1}{2} \cdot \sum \frac{o_{s-2v} + 1}{2} + \sum \frac{o_{s-2u+1} + 1}{2} \cdot \frac{o_{s-2v} + 1}{2} \quad \left(u, v, \mathfrak{u}, \mathfrak{v} = 1, 2, \dots, \left[\frac{s-r}{2}\right], \ \mathfrak{u} \leqq \mathfrak{v}\right)$$

erhält.

Die erste Potenz aus $\delta$ findet man mit Hilfe der Formeln aus *F. Q.*, p. 85 [[S. 73]] gleich

$$\left\{\left(\frac{\varphi_{r+1}}{e_r \varphi_r}\right)(-1)^{\frac{I_r(I_r+1)}{2}}\right\}\left\{\left(\frac{\varphi_{s-1}}{e_s \varphi_s}\right)(-1)^{\frac{I_s(I_s-1)}{2}}\right\} \cdot \prod_{h=r+1}^{s-1} \left(\frac{\varphi_h}{o_h}\right),$$

während die zweite, ebenso wie die Einheit $\varepsilon$ sich unmittelbar durch die Charaktere $(-1)^{\frac{\varphi_r - 1}{2}}$ und $(-1)^{\frac{\varphi_s - 1}{2}}$ ausdrückt.

Es verdient beachtet zu werden, daß in $f\{2\}$ die Einheiten $\varepsilon$ und $\delta$ nur in der Verbindung $\frac{\delta + \delta^-}{2}$ auftreten, wo $\delta^- = \delta \cdot \varepsilon^{\varkappa_k - 1}$ die zu $-\Phi_k$ gehörige Einheit $\delta$ bedeutet.

So oft ferner $\tau_k = 2$ ist, und die Zahlen $\sigma_{r-1} 2^{v_r}$ und $2^{v_s} \sigma_{s+1}$ beide

durch 4 teilbar sind, begegnet man in $f\{2\}$ einer aus den Koeffizienten von $\Phi_k$ gebildeten Einheit

$$\theta = \left(\frac{2}{o_{r+1}\, o_{r+3} \cdots o_{s-3}\, o_{s-1}\, \varphi_r\, \varphi_s}\right).$$

Wir bemerken schließlich, daß die mit $f = \sum a_{ik} x_i x_k$ adjungierte Form $f' = \frac{(-1)^I}{d_{n-2}} \cdot \sum \frac{\partial \Delta}{\partial a_{n-i+1,\, n-k+1}} x_i' x_k'$ lauter Größen $f'\{q\}$ liefert, welche mit den Größen $f\{q\}$ identisch sind. Es erhellt dieses leicht aus dem Umstande, daß die Invarianten $o_h'$, $\sigma_h'$ und die Zahlen $\varphi_h'$ der Form $f'$ die Gleichungen erfüllen:

$$o_h' = o_{n-h}, \quad \sigma_h' = \sigma_{n-h}, \quad \varphi_h' = (-1)^I \cdot \varphi_{n-h}.$$

## 8. Ausdruck für die Formenanzahl eines Genus.

Irgendein primitives Genus $f$ sei definiert durch seine Invarianten $I$, $o_h$, $\sigma_h$, $C$, welche allen für die Existenz des Genus notwendigen Bedingungen genügen mögen. Wir bilden nach den in **5.**, **6.** und **7.** angegebenen Regeln die verschiedenen Größen $f\{q\}$, welche zu unserem Genus gehören. Wir setzen ferner

$$\mathfrak{D} = \prod_{h=1}^{n-1} o_h^{h(n-h)}$$

und

$$c_n = 2\, \frac{\Gamma\left(\frac{1}{2}\right) \cdot \Gamma\left(\frac{2}{2}\right) \cdots \Gamma\left(\frac{n}{2}\right)}{\left\{\Gamma\left(\frac{1}{2}\right)\right\}^{\frac{n(n+1)}{2}}},$$

wo $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$, $\Gamma(1) = 1$, $\Gamma(u+1) = u\Gamma(u)$.

Wir wollen von dem Falle absehen, wo $n = 2$ und $(-1)^I o_1 = \Delta$ eine negative Quadratzahl ist, das Genus also lauter zerlegbare Formen enthält.

Schließt man diesen Fall aus, so besitzt das über alle möglichen Primzahlen $q = 2, 3, 5, \ldots$ erstreckte Produkt

$$M = c_n \cdot \frac{\sqrt{\mathfrak{D}}}{\sigma_1 \sigma_2 \cdots \sigma_{n-1}} \cdot \frac{1}{f\{2\}} \cdot \frac{1}{f\{3\}} \cdot \frac{1}{f\{5\}} \cdots \frac{1}{f\{q\}} \cdots \tag{16}$$

stets einen endlichen Wert.

Um dieses nachzuweisen, wollen wir in $M$ die Größe

$$\frac{\left(1-\frac{1}{q^2}\right)\left(1-\frac{1}{q^4}\right)\cdots\left(1-\frac{1}{q^{2\left[\frac{n-1}{2}\right]}}\right)}{f\{q\}} = E_q$$

als allgemeines Glied einführen. Solches kann leicht geschehen, indem man mit der Identität

$$1 = S_2 S_4 \dots S_{2\left[\frac{n-1}{2}\right]} \cdot \prod_q \left(1 - \frac{1}{q^2}\right)\left(1 - \frac{1}{q^4}\right) \cdots \left(1 - \frac{1}{q^{2\left[\frac{n-1}{2}\right]}}\right)$$

multipliziert, wo $S_{2k}$ die Summe $\sum_{z=1}^{\infty} \frac{1}{z^{2k}}$ bedeutet. Man weiß, daß diese Summe den Wert $\frac{1}{2} B_k \cdot \frac{(2\pi)^{2k}}{(2k)!}$ hat, falls unter $B_k$ die $k^{\text{te}}$ Bernoullische Zahl verstanden wird.

Für jede nicht in $2\Delta$ enthaltene Primzahl $p$ kommt, wenn $n \equiv 1 \pmod 2$:

$$E_p = 1,$$

und wenn $n \equiv 0 \pmod 2$:

$$E_p = \left\{1 - \left(\frac{(-1)^{\frac{n}{2}}\Delta}{p}\right) p^{-\frac{n}{2}}\right\}^{-1}. \qquad \left(\frac{\Delta}{p}\right) = \left(\frac{(-1)^I \cdot \mathfrak{D}}{p}\right)$$

Sind also die nicht in $\Delta$ aufgehenden, ungeraden Primzahlen, ihrer Größe nach geordnet: $p$, $p'$, $p''$ usw., so wird das unendliche Produkt:

$$E_p E_{p'} E_{p''} \dots,$$

je nachdem $n \equiv 1 \pmod 2$ oder $n \equiv 0 \pmod 2$, gleich 1 oder gleich der Summe:

$$\sum \left(\frac{(-1)^{\frac{n}{2}}\Delta}{m}\right) \frac{1}{m^{\frac{n}{2}}},$$

wo $m$ alle positiven und zu $2\Delta$ relativ primen ganzen Zahlen durchläuft. Zur Bezeichnung dieser Dirichletschen Summe mag das Symbol

$$D_{\frac{n}{2}}\left[(-1)^{\frac{n}{2}}\Delta\right]$$

dienen.

Man setze nun:

$$c_n \cdot S_2 S_4 \dots S_{2\left[\frac{n-1}{2}\right]} = \mathfrak{c}_n,$$

d. i., wenn $n \equiv 1 \pmod 2$:

$$\mathfrak{c}_n = \left(\frac{1}{2}\right)^{\frac{n-3}{2}} \cdot B_1 B_2 \dots B_{\frac{n-1}{2}} \cdot \frac{1}{1 \cdot 2 \cdots \frac{n-1}{2}},$$

und wenn $n \equiv 0 \pmod 2$:

$$\mathfrak{c}_n = \left(\frac{1}{2}\right)^{\frac{n-4}{2}} \cdot B_1 B_2 \dots B_{\frac{n-2}{2}} \cdot \frac{1}{\pi^{\frac{n}{2}}},$$

und lasse ferner $\delta$ alle Primzahlen aus $2\mathfrak{D}$ durchlaufen. Dann können wir endlich schreiben, wenn $n \equiv 1 \pmod 2$:

$$(17) \qquad M = \mathfrak{c}_n \cdot \frac{\sqrt{\mathfrak{D}}}{\sigma_1 \sigma_2 \cdots \sigma_{n-1}} \cdot \prod_{\partial} E_{\partial},$$

und wenn $n \equiv 0 \pmod 2$:

$$(17) \qquad M = \mathfrak{c}_n \cdot \frac{\sqrt{\mathfrak{D}}}{\sigma_1 \sigma_2 \cdots \sigma_{n-1}} \cdot \prod_{\partial} E_{\partial} \cdot D_{\frac{n}{2}}\left[(-1)^{\frac{n}{2}-I} \cdot \mathfrak{D}\right].$$

Diese Ausdrücke zeigen in der Tat, daß $M$ einen endlichen und positiven Wert annimmt.

Für ein Genus von binären zerlegbaren Formen gewinnt man ein ähnliches konvergentes Produkt $M$, indem man $\frac{1-\frac{1}{q}}{f\{q\}}$ an die Stelle von $\frac{1}{f\{q\}}$ treten läßt.

Wir behaupten nun:

*Die Formenanzahl unseres Genus besitzt den Ausdruck:*

$$M \cdot \Omega,$$

*wo $M$ das angegebene Produkt und $\Omega$ eine positive unendliche Größe bedeutet, die nur von $n$ und $I$ und von der Anzahl der Darstellungen der Zahl 0 durch die Formen des Genus abhängt.*

*In den Fällen eines definiten Genus ($I = 0$ oder $I = n$) ist insbesondere dieses $\Omega$ gleich der Anzahl aller ganzzahligen $n$-reihigen Substitutionen von der Determinante 1, und mithin $M$ gleich der über alle Klassen $Cl$ des Genus erstreckten Summe $\sum \frac{1}{t(Cl)}$.*

Wir werden uns begnügen, das vorstehende Resultat für die Fälle definiter (und zwar positiver) Genera zu erweisen. Dabei werden wir von den Dirichletschen Methoden*) Gebrauch machen, und in den Fällen $n > 2$ einen Schluß von $n-1$ auf $n$ zu Hilfe nehmen.

## Zweiter Teil.

### 9. Das Maß eines positiven Genus dargestellt durch einen gewissen Grenzwert.

Ein positives Genus $G$ von $n$ ($\geqq 2$) Variablen sei definiert durch seine Ordnung $O$:

$$d_0, \qquad \begin{pmatrix} \sigma_1, & \sigma_2, & \cdots, & \sigma_{n-2}, & \sigma_{n-1} \\ o_1, & o_2, & \cdots, & o_{n-2}, & o_{n-1} \end{pmatrix}, \qquad I = 0$$

und seine Charaktere $C$. Wir setzen voraus, daß dieselben den für die Existenz des Genus notwendigen Bedingungen genügen. $d_0$ sei gleich 1, das Genus also primitiv.

*) Dirchlet, Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres. (Crelles Journal, Bd. 19, und Werke, Bd. I.)

Es sei $\Delta$ die Determinante des Genus, und $R$ eine beliebige zu $2\Delta$ relativ prime ganze Zahl. Durch die Kenntnis der Invarianten $O$ und $C$ sind wir befähigt, die Reste unseres Genus für einen jeden beliebigen Modul hinzuschreiben. Insbesondere können wir also irgendeinen Hauptrest $\varphi$ in bezug auf den Modul $\sigma_1 \cdot 8\Delta R$ angeben. Der erste Koeffizient von $\varphi$ heiße $\sigma_1 \alpha$. Die Zahl $\alpha$ ist dann sicher relativ prim zu $8\Delta R$.

Wir richten unser Augenmerk auf den quadratischen Charakter von $\alpha$ in bezug auf den Modul $8\Delta R$. Enthält $\Delta$ im ganzen $\mathfrak{d}$ ungerade Primzahlen $\partial$, und $R$ im ganzen $\mathfrak{r}$ ungerade Primzahlen $r$, so wird dieser Charakter durch die Gesamtheit der folgenden $2 + \mathfrak{d} + \mathfrak{r}$ Symbole definiert:

$$C(\alpha) \qquad (-1)^{\frac{\alpha-1}{2}}, \quad \left(\frac{2}{\alpha}\right), \quad \left(\frac{\alpha}{\partial}\right), \quad \left(\frac{\alpha}{r}\right).$$

Diese Symbole können zum Teil Charaktere des Genus vorstellen, zum Teil können sie bei anderer Wahl des Restes $\varphi$ andere Werte erlangen.*)

*) Man überzeugt sich leicht, daß in dieser Beziehung die nachstehenden Sätze gelten:

Eine jede Einheit $\left(\frac{\alpha}{r}\right)$ kann sowohl gleich $+1$ wie gleich $-1$ ausfallen.

Eine Einheit $\left(\frac{\alpha}{\partial}\right)$ hat einen festen Wert, wenn $o_1 \equiv 0 \pmod{\partial}$, also $\varphi$ von dem Typus $\sigma_1 \alpha \xi^2 \pmod{\partial}$ ist. Sonst kann dieselbe beide Werte $\pm 1$ annehmen.

Was die Einheiten $(-1)^{\frac{\alpha-1}{2}}$ und $\left(\frac{2}{\alpha}\right)$ anlangt, so unterliegen dieselben keiner Beschränkung, wenn $\sigma_1 = 2$ ist. Ebenso im allgemeinen, wenn $\sigma_1 = 1$ ist; nur bestehen hier die folgenden Ausnahmefälle:

1. Ist $\varphi \equiv \alpha \xi^2 \pmod 8$, so sind beide Einheiten $(-1)^{\frac{\alpha-1}{2}}$ und $\left(\frac{2}{\alpha}\right)$ Charaktere.

2. Ist $\varphi \equiv \alpha \xi^2 \pmod 4$, oder $\varphi \equiv \alpha \xi^2 + \beta \eta^2 \pmod 4$ und $\alpha \equiv \beta \pmod 4$, oder $\varphi \equiv \alpha \xi^2 + \beta \eta^2 + \gamma \zeta^2 \pmod 4$ und $\alpha \equiv \beta \equiv \gamma \pmod 4$, so hat die Einheit $(-1)^{\frac{\alpha-1}{2}}$ einen festen Wert.

3. Ist $\varphi \equiv \alpha \xi^2 + 2\beta \eta^2 \pmod 8$ und setzt man $(-1)^{\frac{\alpha\beta+1}{2}} = \varepsilon$, so können $(-1)^{\frac{\alpha-1}{2}}$ und $\left(\frac{2}{\alpha}\right)$ sich nur mit $\varphi$ so ändern, daß $\varepsilon^{\frac{\alpha-1}{2}} \cdot \left(\frac{2}{\alpha}\right)$ fest bleibt.

4. Wenn $\varphi \equiv \alpha \xi^2 + 2(\beta \eta^2 + \gamma \zeta^2) \pmod 8$, so sind für die Einheiten $(-1)^{\frac{\alpha-1}{2}}$ und $\left(\frac{2}{\alpha}\right)$ nur drei von den vier Systemen $\pm 1, \pm 1$ zulässig. Ist nämlich $\beta \equiv -\gamma \pmod 4$, so kann der Fall nicht eintreten, daß $(-1)^{\frac{\alpha-1}{2}}$ ungeändert bleibt, während $\left(\frac{2}{\alpha}\right)$ in $-\left(\frac{2}{\alpha}\right)$ übergeht, und hat man $\beta \equiv \gamma \equiv \theta \cdot \alpha \pmod 4$, $\theta = \pm 1$, so ist der Fall ausgeschlossen, daß $(-1)^{\frac{\alpha-1}{2}}$ ins Gegenteil umschlägt, während $\left(\frac{2}{\alpha}\right)$ sich in $\theta \cdot \left(\frac{2}{\alpha}\right)$ verwandelt.

Wie in **6.** bezeichnen wir mit $\varkappa$ den Index der ersten von den $n$ Zahlen $o_1, o_2, \ldots, o_{n-1}, o_n\ (=0)$, welche gerade ausfällt.

Wir denken uns in jeder überhaupt existierenden Klasse des Genus je eine Form ausgesucht, welche nach dem Modul $\sigma_1 \cdot 8\Delta R$ den Rest $\varphi$ läßt. Eine beliebige der so gewonnenen Formen sei $f$.

Wir bestimmen für die Variablen von $f$ alle Systeme $\xi_1, \xi_2, \ldots, \xi_n$, welche dem Ausdrucke $f(\xi_i)$ einen Wert $\sigma_1 m$ erteilen, wo $m$ prim zu $8\Delta R$ ist und den Gleichungen

$$C(m) = C(\alpha)$$

genügt, welche aber dabei, falls $\varkappa > 1$ ist, nicht die Bedingungen

$$\xi_1 \equiv \xi_2 \equiv \cdots \equiv \xi_\varkappa \equiv \sigma_1 \pmod 2 \tag{7}$$

erfüllen. Über alle diese Wertsysteme $\xi_i\ (\neq 0, 0, \ldots, 0)$ erstrecken wir alsdann die Summe

$$\Xi = \varrho \sum \frac{1}{\left\{\frac{1}{\sigma_1} f(\xi_i)\right\}^{\frac{n}{2}(1+\varrho)}},$$

und wir wollen den Grenzwert ermitteln, welchen diese Summe für ein positives, unendlich abnehmendes $\varrho$ erreicht.

Die definierten Wertsysteme $\xi_i$ werden in einer gewissen Anzahl $\mathsf{A}$ von arithmetischen Progressionen

$$\xi_1 = 8\Delta R \cdot X_1 + v_1, \quad \xi_2 = 8\Delta R \cdot X_2 + v_2, \quad \ldots, \quad \xi_n = 8\Delta R \cdot X_n + v_n$$

enthalten sein. Man bezeichne mit $2^{3(n-1)} \cdot A_2$, wenn $\varkappa > 1$, die Anzahl aller derjenigen Lösungen $\xi_i \pmod 8$ von

$$\frac{1}{\sigma_1} \varphi(\xi_i) \equiv \alpha \pmod 8,$$

welche nicht zugleich den Bedingungen (7) genügen, und wenn $\varkappa = 1$, die Anzahl aller möglichen Lösungen dieser Kongruenz; ferner mit $2^{n-1} \cdot A_p$ die Anzahl aller Lösungen von

$$\varphi(\xi_i) \equiv \sigma_1 \alpha \pmod p,$$

wenn $p$ eine der ungeraden Primzahlen aus $\Delta R$ bedeutet. In den Ausdrücken von $A_2$ und $A_p$ erscheint $\alpha$, wie wir wissen, nur in den Einheiten $C(\alpha)$. Dieser Umstand läßt erkennen, daß die Anzahl $\mathsf{A}$ den Wert hat:

$$\mathsf{A} = (8\Delta R)^n \cdot \frac{1}{2} \prod_q \left\{\frac{1}{2}\left(1 - \frac{1}{q}\right) A_q\right\}, \qquad (q = 2, \mathfrak{d}, \mathfrak{r})$$

wo $q$ die $1 + \mathfrak{d} + \mathfrak{r}$ Primzahlen von $8\Delta R$ durchläuft.

Setzt man für die $\xi_i$ zunächst nur alle diejenigen Systeme, welche in einer der $\mathsf{A}$ Progressionen vorkommen, so ergibt sich der Grenzwert der entstehenden Summe für ein $\varrho = +0$, nach *F. Q.*, p. 148 [[S. 121]], gleich

$$e_n \cdot \frac{(8\Delta R)^{-n}}{\sqrt{\frac{\Delta}{\sigma_1^{\,n}}}},$$

wo

$$e_n = \frac{\left\{\Gamma\left(\frac{1}{2}\right)\right\}^n}{\Gamma\left(1+\frac{n}{2}\right)} = \pi^{\left[\frac{n}{2}\right]} \cdot \frac{2^{\left[\frac{n+1}{2}\right]}}{n(n-2)\cdots\left(n-2\left[\frac{n-1}{2}\right]\right)}.$$

Für die ganze Summe $\Xi$ wird daher

$$\lim_{\varrho=0}(\Xi) = e_n \cdot \frac{(8\Delta R)_1}{2^{2+\mathfrak{d}+\mathfrak{r}}} \cdot \frac{\sigma_1^{\frac{n}{2}}}{\sqrt{\Delta}} \cdot \prod_q A_q, \qquad (q=2,\ \mathfrak{d},\ \mathfrak{r})$$

wo $(8\Delta R)_1$ das über alle Primzahlen $q$ von $8\Delta R$ erstreckte Produkt $\prod\left(1-\frac{1}{q}\right)$ bedeutet.

Eine Summe $X$, von ähnlicher Beschaffenheit wie $\Xi$, mag jetzt nur alle solchen Systeme $\xi_i = x_i$ umfassen, in welchen die $n$ Zahlen $\xi_1, \xi_2, \ldots, \xi_n$ keinen gemeinschaftlichen Teiler haben. Offenbar entstehen alle möglichen Systeme $\xi_i$, wenn wir diese besonderen Systeme $x_i$ mit allen positiven und zu $8\Delta R$ relativ primen Zahlen $z$ multiplizieren. Man findet daher

$$\Xi = X \cdot \sum \frac{1}{z^{n(1+\varrho)}},$$

und in der Grenze für $\varrho = 0$:

$$\operatorname{Lim}\left(\frac{\Xi}{X}\right) = \sum \frac{1}{z^n}.$$

Die hier auftretende Summe hat bekanntlich den Wert:

$$(8\Delta R)_n \cdot S_n,$$

wenn $S_n$ die Summe $1 + \frac{1}{2^n} + \frac{1}{3^n} + \cdots$ und $(8\Delta R)_n$ das über alle Primzahlen $q$ von $8\Delta R$ erstreckte Produkt $\prod\left(1-\frac{1}{q^n}\right)$ ausdrückt.

Wir bemerken noch, daß die Summe $X$ sich in $t(f)$ untereinander identische Summen $X_0$ zerlegen läßt. Dabei ist unter $t(f)$, wie in **1.**, die Anzahl aller Substitutionen von der Determinante 1 verstanden, welche die Form $f$ in sich selbst transformieren. (Solche Summen $X_0$ haben dann auch in Fällen indefiniter Formen einen Sinn.)

Wir bilden endlich die Doppelsumme:

$$S = \varrho \cdot \sum \frac{1}{t(f)} \cdot \sum \frac{1}{\left\{\frac{f(x_i)}{\sigma_1}\right\}^{\frac{n}{2}(1+\varrho)}},$$

erstreckt, einmal: über alle die inäquivalenten Formen $f\,(\equiv \varphi, \bmod \sigma_1 \cdot 8\Delta R)$, die wir oben als Repräsentanten der einzelnen Klassen des Genus auf-

gestellt hatten; und dann, für jede dieser Formen $f$: über alle solchen Systeme $x_1, x_2, \ldots, x_n$ ohne gemeinsamen Teiler, welche einer Kongruenz

$$\frac{f(x_i)}{\sigma_1} \equiv \alpha z^2 \pmod{8\Delta R}$$

genügen, wo $z$ zu $8\Delta R$ relativ prim ist, und welche dabei, falls $\varkappa > 1$, nicht alle Bedingungen

$$x_1 \equiv x_2 \equiv \cdots \equiv x_\varkappa \equiv \sigma_1 \pmod 2 \tag{7}$$

erfüllen.

Der Grenzwert $l$ der früheren Summe $X$ hatte sich als unabhängig von der speziellen Form $f$ erwiesen. Infolgedessen muß der Grenzwert $L$ dieser Doppelsumme gleich $l \asymp \sum \frac{1}{t(f)}$ sein. Durch die hier erscheinende einfache Summe ist aber das Maß $M$ unseres Genus dargestellt; man erhält demnach:

$$L = e_n \cdot \frac{(8\Delta R)_1}{2^{2+\mathfrak{d}+\mathfrak{r}}} \cdot \frac{1}{(8\Delta R)_n \cdot S_n} \cdot \frac{\sigma_1^{\frac{n}{2}}}{\sqrt{\Delta}} \cdot \prod_q A_q \cdot M. \qquad (q = 2, \mathfrak{d}, r)$$

Wir werden jetzt für $L$ einen zweiten Ausdruck ableiten, und durch Vergleichung der beiden Ausdrücke werden wir dann die in 8. aufgestellten Formeln als richtig erkennen.

## 10. Bestimmung desselben Grenzwertes auf anderem Wege.

Wir haben soeben den Grenzwert $L$ gefunden, indem wir uns die Summe $S$ erst nach den einzelnen Formen $f$, und dann nach der numerischen Größe der Zahlen $\frac{f(x_i)}{\sigma_1}$ geordnet dachten. Nun handelt es sich in $S$ um lauter positive Glieder; wir müssen daher zu demselben Grenzwert $L$ gelangen, wenn wir die Summe $S$ direkt nach der Größe der Zahlen $\frac{1}{\sigma_1} f(x_i) = m$ anordnen. Durch ein solches Arrangement entsteht für $S$ zunächst ein Ausdruck von der Gestalt:

$$\varrho \sum \frac{M(m)}{m^{\frac{n}{2}(1+\varrho)}},$$

wo die Summation alle positiven Zahlen $m$ betrifft, die zu $8\Delta R$ relativ prim sind und den Gleichungen $C(m) = C(\alpha)$ genügen.

Für jede dieser Zahlen $m$ hat die Größe $M(m)$ folgende Bedeutung. Es bezeichne $m(f)$, wie oft eine bestimmte Form $f$ die Zahl $\sigma_1 m$ mit Hilfe von Systemen $x_i$ darzustellen vermag, welche keinen gemeinsamen Teiler $> 1$ haben, und außerdem, falls $\varkappa > 1$, nicht alle Bedingungen (7) erfüllen. Dann ist:

$$M(m) = \sum \frac{m(f)}{t(f)},$$

wo die Summe sich über alle die Formen $f$ erstreckt. Die Größe $M(m)$ bildet also, wie wir uns nach *F. Q.*, p. 142 [[S. 116]] ausdrücken, das Maß für alle die definierten Darstellungen $x_i$ der Zahl $\sigma_1 m$ durch die verschiedenen Formen $f$ des Genus $G$.

Treten in der Zahl $m$ im ganzen $\mu$ ungerade Primzahlen $p_1, p_2, \ldots, p_\mu$ auf, so erscheint, nach *F. Q.*, p. 143 [[S. 117]], dieses Maß $M(m)$ als das $2^\mu$-fache von dem Maße eines bestimmten positiven Genus $G(m)$ von Formen mit $n-1$ Variablen, welches enge mit dem Genus $G$ zusammenhängt. Von den Sätzen, welche diesen Zusammenhang feststellen, wollen wir hier soviel anführen, als für die Bestimmung der Größe $M(m)$ von Wichtigkeit ist (vgl. *F. Q.*, art. XVIII [[S. 102—113]]).

1. Es sei zunächst $n = 2$, in welchem Falle $\Delta$ und $o_1$ identisch sind. Je nach der Beschaffenheit der Zahl $m$ bieten sich zwei Möglichkeiten dar.

Entweder ist für die Zahl $m$ die quadratische Kongruenz

$$-\Delta \equiv z^2 \pmod{\sigma_1 m}$$

nicht lösbar. In diesem Falle existiert auch das Genus $G(m)$ nicht, und man hat sein Maß gleich 0 zu setzen.

Oder diese Kongruenz ist lösbar und besitzt $2^\mu$ Lösungen $z \pmod{\sigma_1 m}$. Alsdann wird das Genus $G(m)$ von der einen Form $g = \xi^2$ gebildet und liefert das Maß 1.

In beiden Fällen kann man schreiben:

$$M(m) = \left\{1 + \left(\frac{-\Delta R^2}{p_1}\right)\right\}\left\{1 + \left(\frac{-\Delta R^2}{p_2}\right)\right\}\cdots\left\{1 + \left(\frac{-\Delta R^2}{p_\mu}\right)\right\}.$$

Der zweite Fall ereignet sich beispielsweise, wenn man für $\sigma_1 m$ den ersten Koeffizienten einer der Formen $f$ wählt, was man tun darf. Denn nach Voraussetzung ist ein solcher Koeffizient $\equiv \sigma_1 \alpha \pmod{\sigma_1 \cdot 8\Delta R}$. Man hat dann jedenfalls $\left(\frac{-\Delta}{m}\right) = 1$, worin eine Bedingung für die Einheiten $C(m) = C(\alpha)$ liegt.

2. Ist $n > 2$, so erkennt man zunächst, daß die Invarianten von $G(m)$ durch die Zahl $m\,[C(m) = C(\alpha)]$ und die Invarianten von $G$ stets in solcher Weise ausgedrückt sind, daß das Genus $G(m)$ wirklich existiert. Wir haben bereits bemerkt, daß dieses Genus sich als positiv erweist. Man findet es auch primitiv. Seine Invarianten $o$ und $\sigma$ erlangen die Werte:

$$\begin{pmatrix} \sigma_2, & \sigma_3, & \ldots, & \sigma_{n-1} \\ \sigma_1 m \cdot o_2, & o_3, & \ldots, & o_{n-1} \end{pmatrix}.$$

Es sei $\Delta^1 = \prod_{h=2}^{n-1} o_h^{n-h}$ und $\mathfrak{D}^1 = \prod_{h=2}^{n-1} o_h^{(h-1)(n-h)}$. Ferner fallen seine Cha-

raktere derart aus, daß für jede seiner Formen $g = \sum_1^{n-1} c_{ik}\xi_i\xi_k$ die $\frac{n(n-1)}{2}$ Kongruenzen:

$$-\sigma_1 c_{ik} \equiv z_i z_k \pmod{\sigma_1 m} \tag{18}$$

je $2^\mu$ Lösungen zulassen.

Wir nehmen nun an, die Formeln aus 8. seien bereits für den Fall $n-1$ erwiesen, und wir wollen dieselben benutzen, um das Maß von $G(m)$ aufzustellen. Wir bilden zu dem Behufe für irgendeine Form $g$ dieses Genus alle Größen $g\{q\}$, und wir schreiben:

$$\frac{\left(1-\frac{1}{q^2}\right)\left(1-\frac{1}{q^4}\right)\cdots\left(1-\frac{1}{q^{2\left[\frac{n}{2}\right]-2}}\right)}{g\{q\}} = E_q^{\,1}.$$

Für das Maß von $G(m)$ erhalten wir dann einen Ausdruck:

$$\mathfrak{c}_{n-1}\cdot\frac{\sqrt{\mathfrak{D}^1}\cdot\sigma_1^{\frac{n-2}{2}}\,m^{\frac{n-2}{2}}}{\sigma_2\sigma_3\cdots\sigma_{n-1}}\cdot E_2^{\,1}E_3^{\,1}E_5^{\,1}\cdots E_q^{\,1}\cdots,$$

wo $\mathfrak{c}_{n-1}$ eine Konstante bedeutet; und die Größe $M(m)$ ergibt sich gleich diesem Ausdrucke, multipliziert mit $2^\mu$. Es sind jetzt die Größen $E_q^{\,1}$ zu ermitteln.

1) Ist zunächst $q$ irgendeine ungerade Primzahl, die weder in $\Delta R$, noch in $m$ aufgeht, so kommt nach 8., wenn $n \equiv 0 \pmod 2$:

$$E_q^{\,1} = 1,$$

und wenn $n \equiv 1 \pmod 2$:

$$E_q^{\,1} = \left[1-\left(\frac{(-1)^{\frac{n-1}{2}}\sigma_1 m\Delta^1}{q}\right)\frac{1}{q^{\frac{n-1}{2}}}\right]^{-1}.$$

In dem letzteren Falle hat man zugleich: $\left(\frac{\Delta^1}{q}\right) = \left(\frac{\Delta R^2}{q}\right)$. Bildet man das Produkt $\prod E_q^{\,1}$ über alle nicht in $2\Delta Rm$ aufgehenden Primzahlen $q$ in ihrer natürlichen Reihenfolge, so kann man für dasselbe, je nachdem $n \equiv 0 \pmod 2$ oder $n \equiv 1 \pmod 2$ ist, entweder 1 oder die Summe $D_{\frac{n-1}{2}}\left[(-1)^{\frac{n-1}{2}}\sigma_1 m\Delta R^2\right]$ setzen.

2) Ist weiter $q = p$ eine der $\mu$ ungeraden Primzahlen aus $m$, und $p^d$ die höchste Potenz dieser Primzahl, welche $m$ teilt, so besitzt das Genus $G(m)$ Reste vom Typus:

$$g \equiv c\xi^2 + p^d(c_1\xi_1^{\,2} + \cdots + c_{n-2}\xi_{n-2}^{\,2}) \pmod{p^t}, \qquad (t > d)$$

wo die Größen $c, c_1, \ldots, c_{n-2}$ sämtlich zu $p$ prim sind. Aus den Kongruenzen (18) erschließt man das Bestehen einer Kongruenz:

$$-o_1 c \equiv z^2 \pmod{p^d};$$

man findet ferner:

$$cc_1 \ldots c_{n-2} \equiv \left(\frac{\sigma_1 m}{p^d}\right)^{n-2} \cdot \Delta^1 \pmod{p^{t-d}}.$$

Im Falle eines $n \equiv 0 \pmod 2$, wo zugleich $\left(\frac{o_1 \Delta^1}{p}\right) = \left(\frac{\Delta}{p}\right)$, kommt also

$$\left(\frac{c_1 \ldots c_{n-2}}{p}\right) = \left(\frac{-\Delta}{p}\right).$$

Die Formeln aus **5.** und **8.** geben in diesem Falle:

$$E_p^{\,1} = \frac{1}{2}\left[1 + \left(\frac{(-1)^{\frac{n-2}{2}} c_1 \ldots c_{n-2}}{p}\right) \frac{1}{p^{\frac{n-2}{2}}}\right] = \frac{1}{2}\left\{1 + \left(\frac{(-1)^{\frac{n}{2}} \Delta R^2}{p}\right) \frac{1}{p^{\frac{n-2}{2}}}\right\},$$

dagegen, wenn $n \equiv 1 \pmod 2$:

$$E_p^{\,1} = \frac{1}{2}.$$

3) Ist endlich $q$ eine der Primzahlen aus $8\Delta R$, so besitzt das gegebene Genus $G$ für einen jeden Modul $q^t$ Hauptreste $f_1$ mit einem ersten Koeffizienten $\sigma_1 m$. Aus diesen Hauptresten entspringen, nach den Sätzen aus *F. Q.*, art. XVIII [[S. 102—113]], in einfacher Weise Hauptreste des Genus $G(m)$.

Bedeutet $q$ zunächst eine der ungeraden Primzahlen $e$, $r$, so hat ein $f_1$ den Typus:

$$f_1 \equiv \sigma_1 m \xi^2 + \frac{o_1 f^{(1)}}{\sigma_1 m} \pmod{q^t}.$$

Der hier auftretende Rest $f^{(1)} \pmod{q^{t-\omega_1}}$ bildet dann einen Rest des Genus $G(m)$.

Ist $q = 2$, so müssen die Fälle $\sigma_1 = 1$ und $\sigma_1 = 2$ unterschieden werden.

Im ersteren Falle hat ein $f_1$ den Typus:

$$f_1 \equiv m\xi^2 + \frac{o_1 f^{(1)}}{m} \pmod{2^t},$$

wo $f^{(1)}$ einen in bezug auf 2 primitiven Rest vorstellt, welcher im Falle $o_1 \equiv 1 \pmod 2$ eine erste Invariante $\sigma$ gleich 1 liefert. In diesem $f^{(1)} \pmod{2^{t-\omega_1}}$ finden wir einen Rest von $G(m)$.

Im zweiten Falle ($\sigma_1 = 2$) hat $f_1$ den Typus:

$$f_1 \equiv 2(m\xi^2 + A\xi\tilde{\xi} + \tilde{m}\tilde{\xi}^2) + \frac{o_1 o_2 f^{(2)}}{m} \pmod{2^t},$$

wo $A$ ungerade und $f^{(2)}$ primitiv in bezug auf 2 ist, und man gewinnt in

$$f^{(1)} \equiv \frac{(4m\tilde{m} - A^2)}{o_1}\eta^2 + 2o_2 f^{(2)} \pmod{2^{t+1}}$$

einen Rest des Genus $G(m)$.

In allen Fällen ergibt sich nun, nach **5.** und **6.**, wenn $t$ groß genug gewählt ist, die Beziehung:

$$f\{q\} = A_q \cdot f^{(1)}\{q\},$$

wobei $A_q$ mit der in **9.** auf diese Weise bezeichneten Größe identisch ist. Für die Ausdrücke $E_q$ und $E_q^1$ folgt hieraus, wenn $n \equiv 0 \pmod 2$ und $> 2$, die Gleichung:

$$E_q^1 = A_q E_q,$$

und wenn $n \equiv 1 \pmod 2$:

$$E_q^1 = \frac{A_q E_q}{1 - \frac{1}{q^{n-1}}}.$$

Im Falle $n = 2$ findet man in ähnlicher Weise: $f\{q\} = A_q$, also, da hier $E_q = \frac{1}{f\{q\}}$ ist: $A_q E_q = 1$.

Fassen wir alles Vorhergehende zusammen, so können wir die Größe $M(m)$, wenn $n > 2$ ist, in folgender Form schreiben:

$$\mathfrak{c}_{n-1} \cdot \frac{\sqrt{\mathfrak{D}^1} \cdot \sigma_1^{\frac{n-2}{2}} m^{\frac{n-2}{2}}}{\sigma_2 \sigma_3 \dots \sigma_{n-1}} \cdot \prod_q A_q E_q \cdot (m), \qquad (q = 2, \partial, r)$$

wobei im Falle eines geraden $n$:

$$(m) = \prod_p \left\{ 1 + \left( \frac{(-1)^{\frac{n}{2}} \Delta R^2}{p} \right) \frac{1}{p^{\frac{n-2}{2}}} \right\}, \quad (p = p_1, p_2, \dots, p_\mu)$$

und im Falle eines ungeraden $n$:

$$(m) = \frac{1}{(8\Delta R)_{n-1}} \cdot D_{\frac{n-1}{2}}\left[ (-1)^{\frac{n-1}{2}} \sigma_1 m \Delta R^2 \right].$$

Dieser Ausdruck bleibt nun auch für $n = 2$ gültig, wenn $\mathfrak{c}_1 = 1$ genommen wird.

Wir vergleichen jetzt den früher gefundenen Ausdruck von $L$ mit dem Grenzwerte $\operatorname{Lim}\left( \varrho \sum \frac{M(m)}{m^{\frac{n}{2}(1+\varrho)}} \right)$. Dadurch erhalten wir eine Beziehung für das Maß $M$ des gegebenen Genus. In dieselbe setzen wir

$$M = \mathfrak{c}_n \cdot \frac{\sqrt{\mathfrak{D}}}{\sigma_1 \sigma_2 \dots \sigma_{n-1}} \cdot \prod_q E_q \cdot D_R \cdot M_0, \qquad (q = 2, \partial, r)$$

wo $D_R = 1$ sei für ein ungerades $n$, und gleich $D_{\frac{n}{2}}\left[ (-1)^{\frac{n}{2}} \Delta R^2 \right]$ für ein gerades $n$, und wo $\mathfrak{D} = \Delta \cdot \mathfrak{D}^1$ und

$$\mathfrak{c}_n = 2\frac{\mathfrak{c}_1}{e_2} \; (n = 2); \quad = \frac{\mathfrak{c}_{n-1}}{e_n} \cdot \frac{2}{n} \; (n \equiv 0, \bmod 2;\ n > 2);$$

$$= \frac{\mathfrak{c}_{n-1}}{e_n} \cdot \frac{2}{n} \cdot S_{n-1} \; (n \equiv 1, \bmod 2)$$

die Größen aus 8. bedeuten sollen. Die Größe $M_0$ erweist sich dann als unabhängig von der Zahl $R$, und es wird $M_0 = 1$ sein müssen, damit die in 8. für $M$ aufgestellten Ausdrücke in Wirklichkeit gelten.

Schreibt man noch $\frac{2}{n}\varrho$ für $\varrho$, so lauten die Endformeln: wenn $n = 2$,

$$(19)\quad 2 \cdot \frac{(8\Delta R)_1}{2^{2+\mathfrak{b}+\mathfrak{r}}} \cdot \frac{D_1[-\Delta R^2]}{(8\Delta R)_2 \cdot S_2} \cdot M_0 = \operatorname{Lim} \varrho \sum \frac{1}{m^{1+\varrho}} \prod_p \left[1 + \left(\frac{-\Delta R^2}{p}\right)\right];$$

wenn $n \equiv 0 \pmod 2$ und $> 2$,

$$(20)\quad \frac{(8\Delta R)_1}{2^{2+\mathfrak{b}+\mathfrak{r}}} \cdot \frac{D_{\frac{n}{2}}\left[(-1)^{\frac{n}{2}}\Delta R^2\right]}{(8\Delta R)_n \cdot S_n} \cdot M_0$$

$$= \operatorname{Lim}\left\{ \varrho \sum \frac{1}{m^{1+\varrho}} \prod_p \left[ 1 + \left(\frac{(-1)^{\frac{n}{2}}\Delta R^2}{p}\right) \frac{1}{p^{\frac{n-2}{2}}} \right] \right\};$$

wenn $n \equiv 1 \pmod 2$,

$$(21)\quad \frac{(8\Delta R)_1}{2^{2+\mathfrak{b}+\mathfrak{r}}} \cdot \frac{(8\Delta R)_{n-1} \cdot S_{n-1}}{(8\Delta R)_n \cdot S_n} \cdot M_0$$

$$= \operatorname{Lim}\left\{ \varrho \sum \frac{1}{m^{1+\varrho}} D_{\frac{n-1}{2}}\left[(-1)^{\frac{n-1}{2}} \sigma_1 m \Delta R^2\right] \right\}.$$

Dabei durchläuft $m$, wie erinnert werden mag, alle positiven und zu $8\Delta R$ relativ primen ganzen Zahlen, für welche die $2 + \mathfrak{b} + \mathfrak{r}$ Einheiten

$$C(m) \qquad (-1)^{\frac{m-1}{2}},\ \left(\frac{2}{m}\right),\ \left(\frac{m}{\partial}\right),\ \left(\frac{m}{r}\right)$$

gewisse feste Werte annehmen, die für ein $n = 2$ jedenfalls der Bedingung $\left(\frac{-\Delta R^2}{m}\right) = 1$ genügen.

Diese Zahlen $m$ bilden offenbar die Individuen von $(8\Delta R)^n \cdot \frac{(8\Delta R)_1}{2^{2+\mathfrak{b}+\mathfrak{r}}}$ arithmetischen Progressionen $8\Delta R \cdot U + m_0$, $(U = 0, 1, \ldots, \infty)$ von der Differenz $8\Delta R$. Infolgedessen muß nach Dirichlet die Gleichung bestehen:

$$(22)\quad \frac{(8\Delta R)_1}{2^{2+\mathfrak{b}+\mathfrak{r}}} = \operatorname{Lim}\left(\varrho \sum \frac{1}{m^{1+\varrho}}\right).$$

Von derselben werden wir sofort Gebrauch machen, um in allen Fällen das Resultat $M_0 = 1$ abzuleiten.

## 11. Beweis, daß $M_0 = 1$ ist.

Wir schicken die folgende Betrachtung voraus:

Es sei eine ganze positive oder negative Zahl $N$ teilbar durch alle ungeraden Primzahlen, die unter einer gewissen Grenze $G + 1$ liegen;

ferner soll $p$ die sämtlichen Primzahlen irgendeiner zu $2N$ relativ primen Zahl $m$ durchlaufen; endlich sei $\nu > 1$ und $\gamma = \frac{1}{(\nu-1)G^{\nu-1}}$; dann gelten die Ungleichungen:

$$1-\gamma < D_\nu[N] < 1+\gamma; \quad 1 < (2N)_\nu \cdot S_\nu < 1+\gamma;$$
$$1-\gamma < \prod\left[1+\left(\frac{N}{p}\right)\frac{1}{p^\nu}\right] = \Pi_\nu < 1+\gamma.$$

In der Tat, man erhält zunächst

$$D_\nu[N] = \sum\left(\frac{N}{m}\right)\frac{1}{m^\nu},$$

wo die Summation sich auf alle zu $2N$ relativ primen und positiven Zahlen $m$ bezieht. Die kleinste dieser Zahlen $m$, welche von 1 verschieden ist, besitzt mindestens den Wert $G+1$. Die vorstehende Summe liegt daher zwischen den beiden Größen:

$$1 \pm \left(\frac{1}{(G+1)^\nu} + \frac{1}{(G+2)^\nu} + \cdots\right).$$

Da nun

$$\frac{1}{(G+k)^\nu} < \int_{G+k-1}^{G+k} \frac{dx}{x^\nu},$$

so folgt um so mehr:

$$1 - \int_G^\infty \frac{dx}{x^\nu} < D_\nu[N] < 1 + \int_G^\infty \frac{dx}{x^\nu}.$$

In derselben Weise ergeben sich die Ungleichungen für die Größe $(2N)_\nu \cdot S_\nu$, welche den Wert der über alle Zahlen $m$ erstreckten Summe $\sum\frac{1}{m^\nu}$ ausdrückt.

Was endlich das Produkt $\Pi_\nu$ anlangt, so kommt zunächst

$$\Pi_\nu \leqq \prod(1+p^{-\nu}) < 1 + [(G+1)^{-\nu} + (G+2)^{-\nu} + \cdots] < 1+\gamma,$$

und dann

$$\Pi_\nu \geqq \prod(1-p^{-\nu}) > \frac{1}{1+[(G+1)^{-\nu}+(G+2)^{-\nu}+\cdots]} > \frac{1}{1+\gamma} > 1-\gamma.$$

Auf Grund der vorstehenden Ungleichungen können wir jetzt in allen Fällen, wo $n > 4$ ist, die Beziehung $M_0 = 1$ nachweisen.

Wir wählen einfach die Zahl $R$ derart, daß in $\Delta R$ sämtliche ungeraden Primzahlen auftreten, die kleiner als eine Zahl $G+1$ sind. Unsere Ungleichungen liefern uns dann, wenn $n$ ungerade und $> 3$ ist, für alle Größen:

$$D_{\frac{n-1}{2}}\left[(-1)^{\frac{n-1}{2}}\sigma_1 m \Delta R^2\right], \quad (8\Delta R)_n \cdot S_n, \quad \frac{1}{(8\Delta R)_{n-1}\cdot S_{n-1}},$$

und wenn $n$ gerade und $> 4$ ist, für alle Größen:

$$\Pi\left[1+\left(\frac{(-1)^{\frac{n}{2}}\Delta R^2}{p}\right)\frac{1}{p^{\frac{n-2}{2}}}\right],\quad (8\Delta R)_n\cdot S_n,\quad \frac{1}{D_{\frac{n}{2}}\left[(-1)^{\frac{n}{2}}\Delta R^2\right]}$$

einmal obere und dann untere Grenzen. Indem wir erst diese oberen und dann diese unteren Grenzen einsetzen und jedesmal die hervorgehende Ungleichung durch die Gleichung (22) dividieren, bekommen wir, wenn $n \equiv 1 \pmod 2$ und $> 3$:

$$\frac{1-\gamma_{\frac{n-3}{2}}}{1+\gamma_{n-2}} < M_0 < \left(1+\gamma_{\frac{n-3}{2}}\right)(1+\gamma_{n-1}),$$

und wenn $n \equiv 0 \pmod 2$ und $> 4$:

$$\frac{1-\gamma_{\frac{n-4}{2}}}{1+\gamma_{\frac{n-2}{2}}} < M_0 < \frac{\left(1+\gamma_{\frac{n-4}{2}}\right)(1+\gamma_{n-1})}{1-\gamma_{\frac{n-2}{2}}},$$

wobei $\gamma_h$ für $\frac{1}{hG^h}$ gesetzt ist. Lassen wir jetzt die Zahl $G$ ins Unendliche wachsen, so folgt in der Tat: $M_0 = 1$.

Es bleibt uns noch übrig, die Fälle $n = 2, 3, 4$ zu untersuchen.

Ist $n = 2$, so nehme man $R = 1$ und betrachte zu gleicher Zeit alle die Grenzwerte $L(m)$, welche die rechte Seite der Gleichung (19) darstellt, wenn man den $2 + \mathfrak{d}$ Einheiten $C(m)$ alle die Wertsysteme beilegt, die der Bedingung $\left(\frac{-\Delta}{m}\right) = 1$ genügen. Man bilde aus diesen $2^{1+\mathfrak{d}}$ Grenzwerten ebensoviele lineare Kombinationen: $\sum c(m)\,L(m) = L_c$; $c(m)$ bedeute hier ein beliebiges Glied des über alle Einheiten $C(m)$ erstreckten Produktes $\Pi[1 + C(m)]$; von je zwei Einheiten $c(m)$, die ein Produkt gleich $\left(\frac{-\Delta}{m}\right)$ geben, soll aber immer nur eine beibehalten werden. Aus den Summen $L_c$ folgen umgekehrt die Größen $L(m)$ mit Hilfe der Gleichungen $2^{1+\mathfrak{d}}\cdot L(m) = \sum_c c(m)\cdot L_c$. Die Grenzwerte $L_c$ sind von Dirichlet angegeben. Unter ihnen ist nur einer von Null verschieden, nämlich derjenige, welcher zu $c = 1 = \left(\frac{-\Delta}{m}\right)$ gehört; dieser besitzt einen Ausdruck, aus welchem sofort $M_0 = 1$ hervorgeht.

In den Fällen $n = 3$ und $n = 4$ gebe ich für die Relation $M_0 = 1$ einen Beweis, welcher sich auf die Sätze aus der Anmerkung zu **9.** stützt. Übrigens ließe sich für diese Fälle noch dieselbe Methode verwerten, welche in den Fällen $n > 4$ angewandt wurde. Für $n = 3$ sehe man auch: Smith, *On the Orders and Genera of Ternary Quadratic Forms*, artt. 13

—21 (Phil. Trans. CLVII, 1867; Collected Papers, vol. I) und: *F. Q.*, pp. 156—159 [[S. 127—129]]; für $n = 4$: *F. Q.*, pp. 162—163 [[S. 131—133]], und: Smith, *Sur la représentation des nombres par une somme de cinq carrés* (Mém. prés. T. XXIX; Collected Papers, vol. II).

Ist $n = 3$, so konstatiere man zunächst, daß dem speziellen Genus $G$ von der Ordnung

$$\begin{pmatrix} 1, & 1 \\ 1, & 1 \end{pmatrix}, \qquad (\Delta = 1)$$

welches die Formen von der Determinante 1 enthält, ein $M_0 = 1$, d. i. ein $M = \frac{1}{24}$ zukommt. Bekanntlich bilden alle Formen von $G$ eine einzige Klasse, welche durch $f = x_1^2 + x_2^2 + x_3^2$ repräsentiert wird*), und dieses $f$ läßt in der Tat genau 24 Transformationen von der Determinante 1 in sich selbst zu. Die Anwendung der Gleichung (21) auf $G$ liefert:

$$(23) \qquad \frac{(2R)_1}{2^{2+\mathfrak{r}}} \cdot \frac{(2R)_2 \cdot S_2}{(2R)_3 \cdot S_3} = \operatorname{Lim}\left\{\varrho \sum \frac{1}{m^{1+\varrho}} D_1[-mR^2]\right\},$$

wo $m$ alle positiven und zu $2R$ relativ primen Zahlen mit festen Einheiten:

$$(-1)^{\frac{m-1}{2}}, \quad \left(\frac{2}{m}\right), \quad \left(\frac{m}{r_1}\right), \quad \left(\frac{m}{r_2}\right), \quad \ldots, \quad \left(\frac{m}{r_{\mathfrak{r}}}\right)$$

zu durchlaufen hat. Dabei ist nach **9.** Anm. die Einheit $(-1)^{\frac{m-1}{2}}$ stets gleich $+1$ zu nehmen, während die übrigen Einheiten ganz nach Belieben gewählt werden dürfen.

Die vorstehende Formel benutzen wir, um für ein beliebiges ternäres Genus $G$ von einer Ordnung

$$\begin{pmatrix} \sigma_1, & \sigma_2 \\ o_1, & o_2 \end{pmatrix} \qquad (\Delta = o_1^2 o_2)$$

die Relation $M_0 = 1$ abzuleiten. Nach (21) genügt die Größe $M_0$ eines solchen Genus jedenfalls einer Gleichung

$$(24) \qquad \frac{(2\Delta)_1}{2^{2+\mathfrak{b}}} \cdot \frac{(2\Delta)_2 \cdot S_2}{(2\Delta)_3 \cdot S_3} \cdot M_0 = \operatorname{Lim}\left\{\varrho \sum \frac{1}{m^{1+\varrho}} D_1[-\sigma_1 \Delta m]\right\} = \{m\},$$

wo $m$ alle positiven und zu $2\Delta$ relativ primen Zahlen mit bestimmten festen Einheiten

$$C(m) \qquad (-1)^{\frac{m-1}{2}}, \quad \left(\frac{2}{m}\right), \quad \left(\frac{m}{\partial_1}\right), \quad \left(\frac{m}{\partial_2}\right), \quad \ldots, \quad \left(\frac{m}{\partial_{\mathfrak{b}}}\right)$$

durchläuft.

Wir betrachten zuerst den Fall, wo $\sigma_1 o_2$ und $\sigma_2 o_1$ beide vollständige Quadrate sind.

Das Genus $G$ werde durch eine charakteristische Form $f$ repräsen-

*) Vgl. z. B. Dirichlet in Crelles Journal, Bd. 40, S. 228. (Werke, Bd. II, S. 92.)

tiert. Der erste Koeffizient von $f$ heiße $\sigma_1\varphi_1$, und es sei $\sigma_2\varphi_2$ der erste Koeffizient der zu $f$ adjungierten Form. Die Zahlen $\varphi_1$ und $\varphi_2$ sind dann prim zueinander, und es gelten zwei Kongruenzen

$$-o_1\sigma_2\varphi_2 \equiv X_1^2 \pmod{\sigma_1^2\varphi_1}$$
$$-o_2\sigma_1\varphi_1 \equiv X_2^2 \pmod{\sigma_2^2\varphi_2}.$$

Dieselben geben

$$-\left(\frac{-\varphi_2}{\varphi_1}\right)\cdot\left(\frac{-\varphi_1}{\varphi_2}\right) = (-1)^{\frac{\varphi_1+1}{2}\cdot\frac{\varphi_2+1}{2}} = -1,$$

also

$$\varphi_1 \equiv 1, \quad \varphi_2 \equiv 1 \pmod 4,$$

was nur mit $\sigma_1 = 1$, $\sigma_2 = 1$ verträglich ist. Denn hätte man etwa $\sigma_2 = 2$, so würde die zweite Kongruenz zugleich $-\varphi_1 \equiv 1 \pmod 4$ liefern. Nach **7.** besitzt nun unser Genus den Hauptrest $\varphi_1\xi_1^2 + \frac{o_1\varphi_2}{\varphi_1}\xi_2^2 + \frac{o_1 o_2}{\varphi_2}\xi_3^2 \pmod 4$. Derselbe zeigt, daß in (24) die Einheit $(-1)^{\frac{m-1}{2}}$ allein gleich $+1$ genommen werden darf. Setzt man $\sigma_1\Delta = 2^{2h}\cdot R^2$ $(R \equiv 1, \bmod 2)$, so kann daher der Grenzwert $\{m\}$ nach der Formel (23) bestimmt werden, und man findet $M_0 = 1$.

Zweitens sei eine der Zahlen $\sigma_1 o_2$ und $\sigma_2 o_1$ kein vollständiges Quadrat.

Das Maß des Genus $G$ stimmt, wie wir wissen, mit dem Maße des adjungierten Genus von der Ordnung

$$\begin{pmatrix}\sigma_2, & \sigma_1\\ o_2, & o_1\end{pmatrix}$$

überein; ebenso liefern diese beiden Genera gleiche Größen $f\{q\}$; sie müssen also auch dasselbe $M_0$ ergeben. Wir brauchen daher nur eines dieser Genera zu untersuchen und können annehmen, es sei $\sigma_1 o_2$, also auch $\sigma_1\Delta$ kein vollständiges Quadrat.

Aus $\sigma_1\Delta$ gehe durch Division mit einer möglichst hohen Potenz von 4 die Zahl $d$ hervor. Wir betrachten irgendein Genus $\varphi_1$ der Ordnung

$$\begin{pmatrix}1, & 1\\ 1, & d\end{pmatrix},$$

denken uns aber im Falle $d \equiv 1 \pmod 4$ (was dann sicher gestattet ist), die Charaktere $\left(\frac{\varphi_2}{\partial}\right)$ dieses Genus so ausgesucht, daß die Einheit $\delta = (-1)^{\frac{d+1}{2}}\cdot\left(\frac{\varphi_2}{d}\right) = (-1)^{\frac{\varphi_1 d+1}{2}\cdot\frac{\varphi_2+1}{2}}$ gleich $+1$ wird. Die zu $\varphi_1$ gehörige Größe $M_0$ läßt sich ebenfalls durch einen der Grenzwerte $\{m\}$ darstellen; und zwar ist hier, nach den Sätzen aus **9.** Anm., ein jeder der $2^{2+b}$ Grenzwerte $\{m\}$ in gleicher Weise verwendbar. Alle die Grenzwerte $\{m\}$ müssen demnach untereinander gleich sein.

Bilden wir jetzt die Formel (24) für das zu $\varphi_1$ adjungierte Genus $\varphi_2$ der Ordnung

$$\begin{pmatrix} 1, & 1 \\ d, & 1 \end{pmatrix},$$

so ergeben sich die Grenzwerte $\{m\}$ gleich gewissen Grenzwerten

$$\operatorname{Lim}\left\{\varrho \sum \frac{1}{m^{1+\varrho}} D_1[-d^2 m]\right\},$$

wo $m$ wie vorher Reihen von positiven Zahlen mit festen Charakteren $C(m) = \pm 1$ zu durchlaufen hat. Hier ist für die Einheit $(-1)^{\frac{m-1}{2}}$, nach **9.** Anm., stets der Wert $+1$ zulässig. Wenn man $d = R$, resp. $= 2R$ setzt, kann man also für den vorstehenden Grenzwert die Formel (23) benutzen, und man gelangt zu $M_0 = 1$.

Ist endlich $n = 4$, so haben wir einen Grenzwert

$$\operatorname{Lim}\left[\varrho \sum \frac{1}{m^{1+\varrho}} \prod_p \left\{1 + \left(\frac{-\Delta}{p}\right)\frac{1}{p}\right\}\right] = \{m\}$$

zu ermitteln, wo $m$ alle positiven und zu $2\Delta$ relativ primen Zahlen mit festen Einheiten

$$C(m) \qquad (-1)^{\frac{m-1}{2}}, \ \left(\frac{2}{m}\right), \ \left(\frac{m}{\partial_1}\right), \ \left(\frac{m}{\partial_2}\right), \ \ldots, \ \left(\frac{m}{\partial_\mathfrak{b}}\right)$$

durchläuft. Wir bilden aus $\Delta$ durch Division mit einer möglichst hohen Potenz von 4 eine Zahl $\Delta_0$. Die Größe $M_0$ für irgendein Genus der Ordnung

$$\begin{pmatrix} 1, & 1, & 1 \\ 1, & 1, & \Delta_0 \end{pmatrix}$$

hängt dann gleichfalls von irgendeinem Grenzwerte $\{m\}$ ab. Für ein solches Genus unterliegen aber, nach den Sätzen aus **9.** Anm., die Einheiten $C(m)$ durchaus keiner Beschränkung. Alle die $2^{2+\mathfrak{b}}$ Grenzwerte $\{m\}$ müssen also untereinander gleich sein, und wir können sie gleich dem $2^{2+\mathfrak{b}\,\text{ten}}$ Teile ihrer Summe setzen. Diese Summe wird durch einen ähnlichen Grenzwert gebildet, wo $m$ alle möglichen positiven und zu $2\Delta$ relativ primen Zahlen durchläuft. Dieser letzte Grenzwert gestattet nach *F. Q.*, p. 150 und 162 [[S. 123 und 132]] eine Transformation in:

$$\operatorname{Lim}\left(\varrho \sum \frac{1}{m^{1+\varrho}} \cdot \frac{\sum \left(\frac{\Delta}{m}\right) m^{-2-\varrho}}{\sum m^{-4-2\varrho}}\right) = (2\Delta)_1 \cdot \frac{D_2(\Delta)}{(2\Delta)_4 \cdot S_4},$$

welche dann unmittelbar zu $M_0 = 1$ führt.

---

Von den verschiedenen Darstellungen, deren das Maß eines Genus fähig ist, erscheint als die natürlichste die hier gegebene mit Hilfe eines unendlichen Produktes, in welchem einer jeden Primzahl ein bestimmter

Faktor entspricht*). Ihre Bedeutung reicht über das spezielle Gebiet der quadratischen Formen hinaus: es zeigt diese Darstellung, daß zur Lösung arithmetischer Probleme über Formenanzahlen ein Studium jener wichtigen Gruppenbildungen erforderlich ist, auf welche Herr Camille Jordan in Nr. 302 des *Traité des Substitutions* aufmerksam gemacht hat.

Ausdrücke für das Maß eines positiven Genus quadratischer Formen von $n$ Variablen sind zuerst von Henry J. Stephen Smith in der Note *On the Orders and Genera of Quadratic Forms containing more than three Indeterminates* (Roy. Soc. Proc. XVI, 1868, pp. 197—208; Collected Papers, vol. I, pp. 510—523) mitgeteilt. Die Formeln von Smith sind ähnlich unseren Formeln (17) in 8., erschöpfen aber nicht alle Fälle; sie geben im wesentlichen die Werte der von uns $E_q$ genannten Faktoren für ungerade Primzahlen $q$, doch für die Primzahl 2 nur in den weniger verwickelten Fällen, wo das Genus eine ungerade Determinante besitzt.

In einem folgenden Aufsatze beabsichtige ich verschiedene Anwendungen der hier gefundenen Resultate auseinanderzusetzen.

## Vita.

Natus sum Hermann Minkowski in Russiae oppido Alexoten die XXII. mensis junii anni 1864. Anno 1872 in civitatem Borussorum susceptus, gymnasium Palaeopolitanum Regimonti adii. Vere anni 1880 maturitatis testimonium adeptus, per quinque semestria Regimonti, per tria Berolini studiis mathematicis incubui. Docuerunt me viri illustrissimi: de Helmholtz, Hurwitz, Lindemann, Kirchhoff, Kronecker, Kummer, Runge, Voigt, Weber, Weierstraß, quibus omnibus optime de me meritis gratias ago maximas.

## Thesen.

I. Es ist nicht wahrscheinlich, daß eine jede positive Form sich als eine Summe von Formenquadraten darstellen läßt.

II. Es hat seine Bedenken, in mathematischen Untersuchungen sich auf räumliche Anschauung zu berufen.

---

Öffentliche Verteidigung der Dissertation und der Thesen: am 30. Juli 1885.
Opponenten: Herr Dr. David Hilbert,
Herr Emil Wiechert, stud. math.

---

*) Ich habe auf diese Darstellung im 99. Bande des Journals für die reine und angewandte Mathematik hingewiesen. Diese Ges. Abhandlungen S. 150—153.

V.

# Über den arithmetischen Begriff der Äquivalenz und über die endlichen Gruppen linearer ganzzahliger Substitutionen.

(Crelles Journal für die reine und angewandte Mathematik, Band 100, S. 449—458).

Herr Kronecker stellt in § 24 (S. 107) seiner *Festschrift zu Herrn Kummers Doktor-Jubiläum**) an eine rationelle Fassung des arithmetischen Begriffs der Äquivalenz von Formen die Forderungen, daß auf Grund einer solchen die verschiedenen Formenklassen gleich dicht werden, und die Anzahl der Klassen möglichst klein ausfalle, und entwickelt in §§ 1 und 2 der Abhandlung: *Über bilineare Formen mit vier Variabeln***), wie diesen Forderungen für definite quadratische Formen mit zwei Variablen genügt werden kann. Dabei erscheint der Umstand von wesentlicher Bedeutung, daß diese Formen, abgesehen von der identischen und der negativen identischen Transformation, keine eigentlichen Transformationen in sich zulassen können, welche modulo 2 der identischen Transformation kongruent sind.

Im folgenden will ich zeigen, in welcher Weise die Kroneckerschen Forderungen für alle diejenigen homogenen ganzen Formen irgendeiner Variablenzahl zu erfüllen sind, welche nur eine endliche Zahl von linearen ganzzahligen Transformationen in sich zulassen, also beispielsweise für alle wesentlich positiven (oder wesentlich negativen) quadratischen Formen von nichtverschwindender Determinante.

## § 1.

*Es gibt keine homogene lineare ganze ganzzahlige Substitution mit n Variablen von einer endlichen Ordnung, welche modulo 4 der identischen Substitution kongruent wäre, diese selbst ausgenommen.*

Denn es sei

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

*) Crelles Journal, Bd. 92. (Werke, Bd. II, S. 370.)

**) Abhandlungen der Berliner Akademie, 1883. (Werke, Bd. II, S. 429.)

eine solche Substitution, es mögen also die Kongruenzen gelten:

$$a_{hh} \equiv 1, \quad a_{hk} \equiv 0 \pmod 4 \qquad (h \neq k).$$

Damit $A$ eine endliche Ordnung besitze, ist notwendig und hinreichend, daß die Elementarteiler der mit einem Parameter $r$ gebildeten charakteristischen Determinante

$$\Delta = (-1)^n . |a_{hk} - r\delta_{hk}| \quad \begin{pmatrix} h, k = 1, 2, \ldots, n, \\ \delta_{hh} = 1, \ \delta_{hk} = 0, \ h \neq k \end{pmatrix}$$

nur für Wurzeln der Einheit verschwinden und sämtlich linear seien*).

Bedeutet $f_\nu(r)$, für irgendeine ganze Zahl $\nu > 1$, diejenige irreduktible ganze Funktion $\varphi(\nu)^{\text{ten}}$ Grades, welche für die primitiven $\nu^{\text{ten}}$ Einheitswurzeln Null wird, und deren höchster Koeffizient gleich 1 ist, so wird also die Determinante $\Delta$ jedenfalls einen Ausdruck erhalten

$$(1) \qquad (r-1)^m f_{\nu_1}(r) f_{\nu_2}(r) \ldots f_{\nu_g}(r), \qquad (m \geqq 0, \ \nu > 1)$$

wo die ganzen Zahlen $m$, $\nu$ der Bedingung genügen werden

$$(2) \qquad n = m + \varphi(\nu_1) + \varphi(\nu_2) + \cdots + \varphi(\nu_g) \geqq m + g.$$

Man setze nun für $r$ irgendeine ganze Zahl

$$c \equiv 1 + 4 \pmod 8$$

ein. Dann muß die Determinante $\Delta$ durch $2^{2n}$ aufgehen, weil jeder ihrer Koeffizienten durch 4 teilbar wird.

Untersuchen wir die höchste Potenz von 2, welche in (1) erscheint. Geht in einer Zahl $\nu$ die Potenz $2^\varkappa$, aber nicht mehr $2^{\varkappa+1}$ auf, so folgt

$$c^\nu \equiv c^{2^\varkappa} \equiv 1 + 2^{\varkappa+2} \pmod{2^{\varkappa+3}};$$

also wird $c^\nu - 1$ genau die Potenz $2^{\varkappa+2}$ aus $4\nu$ enthalten. Nun hat ein $f_\nu(r)$ bekanntlich 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 $\nu$ vorstellen; also enthält $f_\nu(c)$ dieselbe Potenz von 2 wie

$$\frac{4\nu \cdot 4\frac{\nu}{\alpha\beta} \cdot 4\frac{\nu}{\alpha\gamma} \cdots}{4\frac{\nu}{\alpha} \cdot 4\frac{\nu}{\beta} \cdot 4\frac{\nu}{\gamma} \cdots}.$$

Die letztere Zahl ist gleich 1, wenn die Zahl $\nu$ sich aus mehreren verschiedenen Primzahlen zusammensetzt, dagegen, wenn $\nu$ Potenz einer einzigen Primzahl ist, gleich dieser Primzahl, also entweder ungerade oder

*) Hermite, Crelles Journal, Bd. 47, S. 312 (Oeuvres, T. I, p. 199); C. Jordan, Crelles Journal, Bd. 84, S. 112.

gleich 2. Irgendein $f_\nu(c)$ ist also höchstens durch 2, das ganze Produkt (1) für $r = c$ also höchstens durch die Potenz $2^{2m+g}$ teilbar, die wegen (2) stets $< 2^{2n}$ ausfällt, außer im Falle $m = n$, wo dann überhaupt kein Faktor $f_\nu(r)$ in $\Delta$ auftritt.

Demnach verschwinden die Elementarteiler von $\Delta$ nur für $r = 1$, und da sie sämtlich linear sein sollen, so müssen in $\Delta$ für $r = 1$ selbst die Koeffizienten verschwinden, d. h. $A$ ist die identische Substitution, w. z. b. w.

Ein Quotient aus zwei verschiedenen, modulo 4 kongruenten ganzzahligen Substitutionen von endlicher Ordnung ist eine ganzzahlige Substitution von unendlicher Ordnung.

## § 2.

Zwei ganzzahlige Substitutionen $A$ und $S^{-1}AS$ sollen im folgenden nur dann als *ähnlich* bezeichnet werden, wenn die transformierende Substitution $S$ ganzzahlig und von einer Determinante $\pm 1$ ist.

Ist $A$ modulo 2 der identischen Substitution kongruent, so gilt dasselbe von jeder ähnlichen Substitution.

Hat für eine Substitution $A$ die charakteristische Determinante $\Delta$ einen Ausdruck

$$(r-1)^m(r+1)^{n-m},$$

dann gibt es ähnliche Substitutionen, in welchen:

$$a_{hk} = 0 \quad (h < k), \qquad a_{hh} = 1 \quad (h \leqq m), \qquad a_{hh} = -1 \quad (h > m).$$

Denn ist $A$ nicht selbst eine solche Substitution, so sei in $A$ $\nu$ der kleinste Wert von $h$, für welchen diese Gleichungen nicht mehr statthaben. Dann bildet die Determinante

$$|r\delta_{hk} - a_{hk}| \qquad (h, k = \nu, \ldots, n)$$

einen Divisor von $\Delta$ und verschwindet, wenn $\nu \leqq m$, noch für $r = \varepsilon = 1$, wenn $\nu > m$, für $r = \varepsilon = -1$. Man kann daher $n - \nu + 1$ ganze Zahlen $s_\nu, \ldots s_n$ ohne gemeinsamen Teiler bestimmen, so daß

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

wird, und ferner eine Substitution $S$ mit einer Determinante $\pm 1$, so daß man in $S^{-1}$

$$x_h = y_h \quad (h < \nu), \qquad x_\nu = \sum_{h=\nu}^{n} s_h y_h$$

hat.*) Dann finden sich in der Substitution $S^{-1}AS$ die obigen Gleichungen auch für $h = \nu$ erfüllt, und es ist evident, wie man weiter zu schließen hat.

*) Diese Stelle ist nach einer von Minkowski selbst herrührenden Berichtigung (Crelles Journal, Bd. 101, S. 202) korrigiert. (Anm. des Herausg.)

§ 3.

*Es gibt, außer den Substitutionen, welche einer Substitution*

$$x_h = \varepsilon_h y_h; \quad \varepsilon_h = +1, \quad -1 \qquad (h = 1, 2, \ldots, n)$$

*ähnlich sind, keine ganzzahlige Substitution von einer endlichen Ordnung, welche modulo 2 der identischen Substitution kongruent wäre.*

Denn es bedeute $A$ eine solche Substitution, es sei also

$$a_{hh} \equiv 1, \quad a_{hk} \equiv 0 \pmod 2 \qquad (h \neq k).$$

Dann ist $A \cdot A$, wie man sich leicht überzeugt, der identischen Substitution modulo 4 kongruent, muß also, nach § 1, mit dieser übereinstimmen. Die Elementarteiler der charakteristischen Determinante von $A$ können daher nur für $r = 1$ oder $r = -1$ verschwinden, und diese Determinante hat einen Ausdruck

$$(r-1)^m (r+1)^{n-m}.$$

Nach § 2 kann man daher eine Substitution $A^*$ bestimmen, welche $A$ ähnlich ist und in welcher

$$a^*_{hk} = 0 \quad (h < k), \qquad a^*_{hh} = 1 \quad (h \leqq m), \qquad a^*_{hh} = -1 \quad (h > m)$$

ist. Damit die Elementarteiler von $A^*$ linear ausfallen, muß noch

$$a^*_{hk} = 0 \quad (m \geqq h > k), \qquad a^*_{hk} = 0 \quad (h > k > m)$$

sein, so daß man in $A^*$ hat:

$$x_h = y_h \quad (h \leqq m), \qquad x_h = \sum 2 p_{hk} y_k - y_h \quad (h > m,\ k = 1, \ldots, m).$$

Dann findet man $A^* = P^{-1} \mathfrak{A} P$, wenn $P$ die Substitution

$$x_h = y_h \quad (h \leqq m), \qquad x_h = -\sum p_{hk} y_k + y_h \quad (h > m,\ k = 1, \ldots, m)$$

und $\mathfrak{A}$ die Substitution

$$x_h = y_h \quad (h = 1, \ldots, m), \qquad x_h = -y_h \quad (h = m+1, \ldots, n)$$

bedeutet, womit unser Satz bewiesen ist.

Ist $0 < m < n$, so zerlegt sich jede quadratische Form, welche durch $\mathfrak{A}$ in sich selbst transformiert wird, in $f_1 + f_2$, wo $f_1$ nur von $x_1, \ldots, x_m$ und $f_2$ nur von $x_{m+1}, \ldots, x_n$ abhängt.

Um zu erkennen, inwieweit die gefundene Darstellung von $A$ willkürlich bleibt, untersuchen wir eine Gleichung:

$$S^{-1} \mathfrak{A} S = \mathfrak{A}, \quad |S| = \pm 1.$$

Man denke sich $S$ und $\mathfrak{A}$ als bilineare Formen mit zwei Reihen von $n$ Variablen, teile jede Reihe in $m$ und $n - m$ Variablen ein, und zerlege entsprechend $S$ in vier Teile und $\mathfrak{A}$ in $\mathfrak{A}_1 - \mathfrak{A}_2$, dann ergibt sich

$$(S_{11} + S_{12} + S_{21} + S_{22})(\mathfrak{A}_1 - \mathfrak{A}_2) = (\mathfrak{A}_1 - \mathfrak{A}_2)(S_{11} + S_{12} + S_{21} + S_{22}),$$

$$S_{11} - S_{12} + S_{21} - S_{22} = S_{11} + S_{12} - S_{21} - S_{22},$$

also

$$S_{12} = 0, \quad S_{21} = 0 \quad \text{und} \quad S = S_{11} + S_{22}, \quad |S_{11}| = \pm 1, \quad |S_{22}| = \pm 1.$$

§ 4.

Es bedeute wieder $A$ eine, modulo 2 der identischen kongruente Substitution, und es werde gesetzt: $a_{hh} \equiv \varepsilon_h \pmod 4$, $\varepsilon_h = \pm 1$. Dann sind in $\varepsilon A$, wenn $\varepsilon$ die Substitution

$$x_h = \varepsilon_h y_h \qquad (h = 1, 2, \ldots, n)$$

vorstellt, alle ungeraden Koeffizienten $\equiv 1 \pmod 4$. Hat ferner letzteres für irgend zwei Substitutionen statt, welche modulo 2 der identischen Substitution kongruent sind, so findet es sich auch im Produkte derselben erfüllt.

*Jede ganzzahlige Substitution*

$$A: \qquad x_h = \sum a_{hk} y_k \qquad (h, k = 1, 2, \ldots, n)$$

*von einer Determinante* 1, *welche den Kongruenzen*

$$a_{hh} \equiv 1 \pmod 4, \quad a_{hk} \equiv 0 \pmod 2 \qquad (h \neq k)$$

*genügt, läßt sich als Produkt von lauter Substitutionen* $S_{hk}^{\pm 1}$ *von der Form:* $x_1 = y_1, \ldots, x_{h-1} = y_{h-1}, x_h = y_h \pm 2y_k, x_{h+1} = y_{h+1}, \ldots, x_n = y_n$ $(h \neq k)$ *darstellen.*

Man kann beim Beweise dieses Satzes sich einer Methode bedienen, ähnlich derjenigen, welche Herr Kronecker für die Zerlegung beliebiger ganzzahliger Substitutionen in elementare aufgestellt hat*).

Es genügt, zu zeigen, daß $A$ durch wiederholtes Zusammensetzen mit Substitutionen $S_{hk}^{\mp 1}$ auf die identische Substitution reduziert werden kann. Sei in $A$ $x_h$ die erste Variable, welche nicht einfach in $y_h$ übergehe, dann ergibt die Determinante von $A$:

$$1 \equiv 0 \ (\text{modd } a_{hh}, a_{h,h+1}, \ldots, a_{hn}),$$

also $a_{hh} = 1$, sobald alle Zahlen $a_{h,h+1}, \ldots, a_{hn}$ verschwinden.

Sei aber noch eine dieser Zahlen, z. B. $a_{hk} (h < k)$, von Null verschieden, und bedeute $\pm 1$ die positive oder negative Einheit, je nachdem $a_{hh}$ und $a_{hk}$ gleiches oder verschiedenes Zeichen haben. Der absolute Wert der ungeraden Zahl $a_{hh}$ ist verschieden von dem absoluten Werte der geraden Zahl $a_{hk}$; ist er kleiner als letzterer, so finden sich die Zahlen $a_{hh}$ und $a_{hk}$ in $AS_{hk}^{\mp 1}$ durch $a_{hh}$, $a_{hk} \mp 2a_{hh}$, ist er größer, in $AS_{kh}^{\mp 1}$ durch $a_{hh} \mp 2a_{hk}$, $a_{hk}$, also jedesmal durch zwei Zahlen ersetzt, von denen eine unverändert, die andere dem absoluten Werte nach kleiner ist. So können $a_{hh}, a_{h,h+1}, \ldots, a_{hn}$ allmählich auf $1, 0, \ldots, 0$ reduziert werden.

Ist alsdann eine der Zahlen $a_{h1}, \ldots, a_{h,h-1}$, etwa $a_{hk} (h > k)$, von Null verschieden und $\pm 1$ ihr Vorzeichen, so erscheint diese Zahl in $AS_{hk}^{\mp 1}$

*) Monatsberichte der Berliner Akademie, 1866, S. 608 ff., oder Crelles Journal, Bd. 68, S. 282 ff. (Werke, Bd. I, S. 158 ff.)

durch $a_{hk} \mp 2$ ersetzt, also, absolut genommen, verkleinert. Alle diese Zahlen können daher zum Verschwinden gebracht werden.

In der auf solche Weise reduzierten Substitution erfährt auch die $h^{te}$ Variable keine Änderung, und damit ist, unter Zuhilfenahme eines Schlusses von $h$ auf $h+1$, unser Satz verifiziert.

## § 5.

1. Es sei $G$ irgendeine endliche Gruppe von homogenen linearen ganzen ganzzahligen Substitutionen mit $n$ Variablen. In derselben bilden diejenigen Substitutionen, welche modulo 2 der identischen Substitution kongruent sind, eine ausgezeichnete Untergruppe, welche $\mathfrak{G}$ heißen möge.

*Die Ordnung von $\mathfrak{G}$ ist eine Potenz $2^{\mathfrak{n}}$, $0 \leqq \mathfrak{n} \leqq n$. Die Gruppe $\mathfrak{G}$ ist ähnlich einer Untergruppe der Gruppe der $2^n$ Substitutionen*

$$\mathfrak{J}: \qquad x_h = \pm y_h . \qquad (h = 1, 2, \ldots, n)$$

Eine jede Substitution $\mathfrak{S}$ von $\mathfrak{G}$ genügt nämlich nach § 3 der Gleichung $\mathfrak{S}\mathfrak{S} = \mathfrak{E}$, wenn $\mathfrak{E}$ die identische Substitution bedeutet.

Findet man nun in $\mathfrak{G}$ außer $\mathfrak{E}$ (und eventuell $-\mathfrak{E}$) noch eine Substitution $\mathfrak{A}$, so kann man, nach § 3, $\mathfrak{G}$ derart transformiert voraussetzen, daß $\mathfrak{A}$ einen Ausdruck hat

$$x_h = y_h \quad (h = 1, \ldots, m), \qquad x_h = -y_h \quad (h = m+1, \ldots, n).$$

Erscheint dann in $\mathfrak{G}$ außer der Gruppe $\{\mathfrak{E}, -\mathfrak{E}, \mathfrak{A}\}$ noch ein $\mathfrak{B}$, so ist auch $\mathfrak{B}\mathfrak{A} \cdot \mathfrak{B}\mathfrak{A} = \mathfrak{E}$, also $\mathfrak{B}^{-1}\mathfrak{A}\mathfrak{B} = \mathfrak{A}$. Nach § 3 muß daher $\mathfrak{B}$ sich in $\mathfrak{B}_1 + \mathfrak{B}_2$ zerlegen, wo $\mathfrak{B}_1$ und $\mathfrak{B}_2$ Substitutionen mit $m$ und $n-m$ Variablen sind. Dieselben sind ebenso wie $\mathfrak{B}$ von einer endlichen Ordnung und modulo 2 von der Ordnung Eins, können daher, nach § 3, durch Transformation mit Substitutionen $S_1$ und $S_2$ von einer Determinante $\pm 1$ in einen, $\mathfrak{J}$ analogen Typus übergeführt werden. Durch Transformation mit $S_1 + S_2$ erlangt dann auch $\mathfrak{B}$ den Typus $\mathfrak{J}$, während $\mathfrak{A}$ sowie $\mathfrak{E}$ ungeändert bleiben.

Enthält jetzt $\mathfrak{G}$ außer der Gruppe $\{\mathfrak{E}, -\mathfrak{E}, \mathfrak{A}, \mathfrak{B}\}$ noch ein $\mathfrak{C}$, so ist $\mathfrak{C}^{-1}\mathfrak{A}\mathfrak{C} = \mathfrak{A}$, $\mathfrak{C}^{-1}\mathfrak{B}\mathfrak{C} = \mathfrak{B}$ usw. Sollte endlich $\mathfrak{G}$, auf irgendeine Weise transformiert, alle Substitutionen $\mathfrak{J}$ enthalten, so würden damit sicher die Substitutionen von $\mathfrak{G}$ erschöpft sein. Denn ein jedes $\mathfrak{S}$ müßte dann, wegen $\mathfrak{S}^{-1}\mathfrak{J}\mathfrak{S} = \mathfrak{J}$, sich auf alle möglichen Arten in $\mathfrak{S}_1 + \mathfrak{S}_2$ zerlegen lassen.

Die Substitutionen von $G$ verteilen sich in Reihen $\mathfrak{G}, A\mathfrak{G}, \ldots$ von je $2^{\mathfrak{n}}$ Substitutionen, welche untereinander modulo 2 kongruent sind.

*Die Gruppe $G$ ist $2^{\mathfrak{n}}$-stufig isomorph zur Gruppe $G_R$ der Reste ihrer Substitutionen nach dem Modul 2.* Letztere Gruppe bildet offenbar eine Untergruppe der Gruppe sämtlicher inkongruenter Substitutionenreste

modulo 2 von einer Determinante $\equiv 1 \pmod 2$; ihre Ordnung ist daher ein Divisor der Ordnung dieser Gruppe, d. i. der Zahl:

$$N = (2^n - 1)(2^n - 2) \cdots (2^n - 2^{n-1}).$$

Also:

*Die Ordnung jeder endlichen Gruppe von homogenen linearen ganzen ganzzahligen Substitutionen mit n Variablen ist ein Divisor der Zahl* $2^n N$.

Ein eingehenderes Studium der endlichen Gruppen ganzzahliger Substitutionen, welches ich mir für einen folgenden Aufsatz vorbehalte, führt zu fundamentalen Beziehungen zwischen der Theorie der aus Wurzeln der Einheit gebildeten komplexen Zahlen und der Theorie der Reduktion der wesentlich positiven quadratischen Formen.

2. Sei jetzt $f$ eine homogene ganze Form mit $n$ Variablen, welche nur eine endliche Anzahl von linearen ganzzahligen Transformationen in sich zulasse; und sei $t(f)$ diese Anzahl.

Die $t(f)$ Transformationen werden eine endliche Gruppe bilden; also ist $t(f)$ ein Divisor von $2^n N$, also $t(f) \leq 2^n N$. Sie sind sämtlich von einer Determinante $\pm 1$; man findet unter ihnen außer der identischen Transformation keine, welche der identischen modulo 4 kongruent wäre, dagegen noch irgend $2^{\mathfrak{n}} - 1$ Transformationen $(0 \leq \mathfrak{n} \leq n)$, welche der identischen modulo 2 kongruent sind.

Die letzteren Transformationen können im Falle $n = 2$ nur sein: 1. wenn $f$ von gerader Dimension ist, die negative identische Transformation, 2. Transformationen, welche der Transformation

$$x_1 = y_1, \quad x_2 = -y_2$$

ähnlich, also von einer Determinante $-1$ sind.

## § 6.

Es bedeute allgemein

$S_a$ eine (homogene lineare ganze) ganzzahlige Substitution von einer Determinante $\pm 1$,

$S_e$ eine ebensolche Substitution von einer Determinante 1,

$S_u$ eine ebensolche Substitution von einer Determinante 1, welche modulo 2 der identischen Substitution kongruent ist,

$S_e$, wenn $n = 2$ ist, eine Substitution $S_u = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$, in welcher entweder

$$\alpha - 1 \equiv \beta \equiv \gamma \equiv \delta - 1 \equiv 0 \pmod 4,$$

oder

$$\alpha + \delta \equiv -2 \pmod 8$$

und dabei nicht

$$\alpha + 1 \equiv \beta \equiv \gamma \equiv \delta + 1 \equiv 0 \pmod 4$$

ist,

wenn $n > 2$ ist, eine ganzzahlige Substitution von einer Determinante 1, welche der identischen Substitution modulo 4 kongruent ist.

Die $S_a$, die $S_e$, die $S_u$, alle $S_v$ bilden Gruppen. Von solchen vier Gruppen ist jede folgende eine ausgezeichnete Untergruppe jeder vorhergehenden. Im Falle $n = 2$ entsteht die Gruppe der $S_u$ aus der Gruppe der $S_v$ durch Hinzunahme der Substitution

$$x_1 = -y_1, \quad x_2 = -y_2 .$$

Zwei binäre Formen gerader Dimension, welche durch ein $S_u$ ineinander übergehen, lassen sich daher auch durch ein $S_v$ ineinander überführen.

Zwei homogene ganze Formen heißen *äquivalent*, wenn sie durch ein $S_a$, *eigentlich äquivalent*, wenn sie durch ein $S_e$ ineinander transformiert werden können.

Zwei Formen sollen *vollständig**) äquivalent heißen, wenn sie durch ein $S_v$ ineinander transformiert werden können.

Wir wollen uns auf Formen beschränken, welche nur eine endliche Anzahl von linearen ganzzahligen Transformationen in sich zulassen. Jede solche Form ist *sich selbst* nur vermittels der identischen Transformation vollständig äquivalent. Daher enthält eine Klasse vollständig äquivalenter Formen ebensoviel verschiedene Formen, als verschiedene Substitutionen $S_v$ existieren. Der Begriff der vollständigen Äquivalenz führt also, der Kroneckerschen Forderung entsprechend, zu einer für alle Klassen konstanten, nur von der Variablenzahl $n$ abhängenden Dichtigkeit.

Geht eine Form $f$ durch $t(f)$ Transformationen in sich selbst über, so wird die Klasse der mit $f$ äquivalenten Formen, je nachdem $n = 2$ oder $> 2$ ist, sich in $\frac{2^2 N}{t(f)}$ oder in $\frac{2^{n^2} N}{t(f)}$ verschiedene Klassen von untereinander vollständig äquivalenten Formen auflösen. $N$ bedeutet hier die Zahl aus § 5. Da $t(f)$ stets in $2^n N$ aufgeht, so werden in den Fällen $n \geqq 3$ die Klassenanzahlen den Faktor $2^{n^2-n}$ enthalten.

Auf Grund der Untersuchungen von Herrn Camille Jordan über die Zusammensetzung der linearen Gruppe (*Traité des Substitutions*, 127—140) läßt sich ferner nachweisen, daß man nicht durch eine von der hier gegebenen abweichende Fassung des Begriffs der vollständigen Äquivalenz zu kleineren Klassenanzahlen, d. i. zu einer größeren konstanten Dichtigkeit in den Klassen gelangen kann, wenn man nur folgendes voraussetzt: Die Gesamtheit der Substitutionen, welche vollständige Äquivalenz hervorrufen, soll eine *ausgezeichnete* Untergruppe der Gruppe derjenigen Substitutionen sein, welche Äquivalenz hervorrufen; oder (was dasselbe ist):

*) Kronecker, Über bilineare Formen mit vier Variabeln, S. 9. (Werke, Bd. II, S. 434.)

Zwei vollständig äquivalente Formen sollen, irgendeiner äquivalenz-erzeugenden Transformation zu gleicher Zeit unterworfen, vollständig äquivalent bleiben.

Wollte man indes von dieser Voraussetzung absehen, so könnte man in den Fällen $n \geqq 3$ dem Begriffe der vollständigen Äquivalenz z. B. die Gruppe derjenigen Substitutionen von der Determinante 1 zugrunde legen, in welchen

$$a_{hh} \equiv 1 \pmod 4, \quad a_{hk} \equiv 0 \pmod 4 \ (h < k), \quad a_{hk} \equiv 0 \pmod 2 \ (h > k)$$

ist; dann würden sich Klassen von einem $2^{\frac{n^2-n}{2}}$-mal so großen Formeninhalte ergeben.

Königsberg i. Pr., 1886.

VI.

# Zur Theorie der positiven quadratischen Formen.*)

(Crelles Journal für die reine und angewandte Mathematik, Band 101, S. 196—202).

Eine wesentlich positive quadratische Form von $n$ Variablen, mit reellen Koeffizienten 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 *Über den arithmetischen Begriff der Äquivalenz*, niemals der identischen Transformation modulo 4 kongruent 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 gesamte 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

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

von endlicher Ordnung ist dadurch charakterisiert, daß die mit einem Parameter $r$ gebildete Determinante

$$\Delta = |r\delta_{hk} - a_{hk}| \qquad \begin{pmatrix} h, k = 1, 2, \ldots, n \\ \delta_{hh} = 1, \ \delta_{hk} = 0, \ h \neq k \end{pmatrix}$$

nur für Einheitswurzeln verschwindet, und zwar für einen mehrfachen,

*) Der nachfolgende Aufsatz wurde in Verbindung mit dem Aufsatze *Über den arithmetischen Begriff der Äquivalenz* (Crelles Journal, Bd. 100, S. 449—458; diese Ges. Abhandlungen, Bd. I, S. 201—211) vom Verfasser im März 1887 der philosophischen Fakultät zu Bonn als Habilitationsschrift vorgelegt.

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

etwa $m$-fachen Nullwert zusammen mit allen ihren $(m-1)^{\text{ten}}$ Unterdeterminanten*).

Bei ganzzahligen Koeffizienten $a_{hk}$ liefert daher eine Zerlegung in irreduktible Faktoren für $\Delta$ einen Ausdruck:

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

wenn mit $f_\nu(r)$ für eine ganze Zahl $\nu > 1$ diejenige ganze Funktion $\varphi(\nu)^{\text{ten}}$ Grades bezeichnet wird, welche für die primitiven $\nu^{\text{ten}}$ Einheitswurzeln verschwindet und als Koeffizient 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 irgendeine ungerade Primzahl $p$ der identischen Transformation kongruent 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 $\Delta$ durch $p^n$ auf. Damit aber der Ausdruck (1) durch $p^n$ teilbar werde, ist notwendig, daß in $\Delta$ kein $f_\nu(r)\,(\nu > 1)$ auftrete, daß also $\Delta = (r-1)^n$ sei. Denn $(c-1)^m$ enthält zwar genau $p^m$, irgendein $f_\nu(c)$ aber, wenn $\nu > 1$ ist, niemals die Potenz $p^{\varphi(\nu)}$.

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

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

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

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

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

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

Diese Zahl ist 1, wenn $\nu$ sich aus mehreren ungleichen Primzahlen zusammensetzt, dagegen, wenn $\nu$ Potenz einer einzigen Primzahl ist, gleich

*) Hermite, Crelles Journal, Bd. 47, S. 312 (Oeuvres, T. I, p. 199); C. Jordan, Crelles Journal, Bd. 84, S. 112.

dieser Primzahl. Die höchste in $f_\nu(c)$ enthaltene Potenz von $p$ ist demnach $p^1$ oder $p^0$, je nachdem $\nu$ 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 Koeffizienten von $\Delta$ für $r = 1$ verschwinden, d. h. $A$ ist die identische Transformation.

## § 2.

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

Sollten in $f$ die Koeffizienten nicht sämtlich in rationalen Verhältnissen zueinander 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 tun ferner alle Formen, welche in den Verhältnissen ihrer Koeffizienten mit $f$ ganz übereinstimmen. Im folgenden können wir deshalb voraussetzen, die Koeffizienten von $f$ seien ganze Zahlen ohne gemeinsamen Teiler.

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 irgendeine ungerade Primzahl $p$. Denn lieferten zwei ihrer Transformationen, etwa $A$ und $B$, gleiche Reste modulo $p$, so würde die Transformation $A^{-1} \cdot B$, welche, als Angehörige der Gruppe, ebenfalls von endlicher Ordnung wäre, der identischen Transformation modulo $p$ kongruent, aber von ihr verschieden sein, was nach § 1 nicht angeht.

Die Gruppe der $t(f)$ Transformationenreste ist offenbar eine Untergruppe der Gruppe sämtlicher inkongruenter Transformationenreste modulo $p$ von einer Determinante $\equiv \pm 1 \pmod p$, und ihre Ordnung, die Zahl $t(f)$, daher ein Divisor der Ordnung der letzteren Gruppe, d. i. der Zahl

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

*) Galois, Journal de Liouville, T. XI, 1846, p. 410. (Oeuvres, p. 27.)

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 *sämtliche* Primzahlen über einer gewissen Grenze $l$, den folgenden Ausdruck*), wenn $n$ gerade ist:

$$(3) \qquad p^{\frac{1}{4}n(n-2)} \cdot 2(p^2-1)(p^4-1)\dots(p^{n-2}-1)\left(p^{\frac{n}{2}}-\varepsilon\right),$$

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

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

Als Divisor *sämtlicher* Zahlen (3) oder (4) 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 speziellen Form $f$ unabhängig ist, denken wir uns in (3) den Faktor $p^{\frac{n}{2}} - \varepsilon$ 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:

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

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 Produkt 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 (3) bzw. (4) aufzusuchen, welche eine möglichst niedrige Potenz von $q$ enthält. Man gelangt zu einer solchen, indem man die Primzahl $p$ in folgender 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 (3) oder (4) durch $q$ überhaupt nicht teilbar; im zweiten

*) Vgl. *Untersuchungen über quadratische Formen*, Acta Mathematica, Bd. 7, S. 218. Diese Ges. Abhandlungen, Bd. I, S. 170.

geht $q$ in $p^\nu - 1$ nur auf, wenn $\nu$ ein Vielfaches von $q-1$ ist, und zwar dann in derselben Potenz wie in $q \cdot \frac{\nu}{q-1}$, mithin in der Zahl (3) bzw. (4) in derselben Potenz wie in $q^{\left[\frac{n}{q-1}\right]} \cdot 1 \cdot 2 \cdots \left[\frac{n}{q-1}\right]$; im dritten enthält $p^{2\nu} - 1$ dieselbe Potenz von 2 wie $8\nu$, also die Zahl (3) bzw. (4) dieselbe wie $2^{n+\left[\frac{n}{2}\right]} \cdot 1 \cdot 2 \cdots \left[\frac{n}{2}\right]$.

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

$$1 \cdot 2 \cdots n = n! = \prod_q q^{\left[\frac{n}{q}\right] + \left[\frac{n}{q^2}\right] + \left[\frac{n}{q^3}\right] + \cdots}, \qquad (q = 2, 3, 5, 7, \ldots)$$

und man erhält damit in der Tat den Satz:

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

Als größter gemeinsamer Divisor aller Zahlen (2) würde sich $2^{\left[\frac{n}{2}\right]} \cdot \overline{n}|$ 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 spezielle Fälle seien die folgenden erwähnt: die Form

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

geht durch $2^n \cdot n!$, die Form

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

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

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 numerierten

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

Variablen, so ist für diese Form $f$ die Zahl

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

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

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

$$\overline{2n+1} = 2 \cdot \overline{2n}, \quad \overline{2n} = 2b_n \cdot \overline{2n-1}, \quad \overline{n} = 2^n \cdot b_1 b_2 \ldots b_{\left[\frac{n}{2}\right]},$$

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.

Bezeichnet $B_n$ die $n^{\text{te}}$ Bernoullische Zahl, so stellt $b_n$ den Nenner von $\frac{1}{n} B_n$ vor*).

Die Bestimmung der ganzzahligen Transformationen einer positiven Form $f = \sum_1^n a_{hk} x_h x_k$ in sich selbst geschieht durch Vermittlung der äquivalenten reduzierten Formen.

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

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

(d. i. kurz ausgedrückt den kleinsten Wert von

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

bei hinreichend großem positivem $g$) ergeben.

Den Sätzen, welche ich in Crelles Journal, Bd. 99 [[diese Ges. Abhandlungen, Bd. I, S. 153—156]] mitgeteilt habe, schließen sich die folgenden für den Fall von sechs Variablen an.

Eine Form $f$ mit sechs Variablen ist immer und nur dann positiv und reduziert, 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:

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

**) Crelles Journal, Bd. 40, S. 302. (Oeuvres, T. I, p. 149.)

| $m_h$ | $\pm m_{h'}$ | $\pm m_{h''}$ | $\pm m_{h'''}$ | $\pm m_{h^{\mathrm{IV}}}$ | $\pm m_{h^{\mathrm{V}}}$ |
|---|---|---|---|---|---|
| 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 reduzierten und die aus denselben durch Permutation der Variablen hervorgehenden Formen nehmen die Verbindungen

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

ihre kleinsten Werte an.

Die Hermiteschen reduzierten Formen mit sieben Variablen lassen sich nicht mehr durch eine Reihe einzelner linearer Ungleichungen vollständig charakterisieren.

Berlin, den 15. Februar 1887.

VII.

# Über die Bedingungen, unter welchen zwei quadratische Formen mit rationalen Koeffizienten ineinander rational transformiert werden können.

(Auszug aus einem von Herrn H. Minkowski in Bonn an Herrn Adolf Hurwitz gerichteten Briefe.)

(Crelles Journal für die reine und angewandte Mathematik, Band 106, S. 5—26.)

Bei unserem letzten Zusammensein interessierten Sie und Herr Hilbert sich für die Frage, unter welchen Umständen zwei diophantische Gleichungen zweiten Grades sich rational ineinander transformieren lassen*). In den folgenden Zeilen will ich eine Entscheidung dieser Frage zu geben versuchen.

Es liege irgendeine quadratische Form mit rationalen Koeffizienten vor, $f$. Die Anzahl ihrer Variablen heiße $n$, und bei dieser Variablenzahl habe die Form eine nichtverschwindende Determinante; als Aggregat von $n$ Quadraten reeller linearer Formen dargestellt, möge $f$ im ganzen $I$ Quadrate mit negativem, und also $n - I$ mit positivem Vorzeichen aufweisen. Unterwirft man die Form einer beliebigen linearen Transformation mit rationalen Koeffizienten und von nichtverschwindender Determinante, so bleibt dabei zunächst außer den Zahlen $n$ und $I$, da die Determinante

*) Bei der Untersuchung der ternären diophantischen Gleichungen vom Geschlechte Null wurden Herr Hilbert und ich auf diese Frage geführt. Wenn zwei diophantische Gleichungen durch rationale eindeutig umkehrbare Transformationen ineinander übergeführt werden können, so lassen sich offenbar die Lösungen einer jeden dieser Gleichungen aus den Lösungen der anderen ableiten; beide Gleichungen repräsentieren also im wesentlichen dieselbe Aufgabe. Wir rechnen deshalb alle diophantischen Gleichungen, welche aus einer durch die genannten Transformationen hervorgehen, in eine Klasse. Unsere Untersuchung, welche demnächst in den Acta mathematica erscheinen wird, [[Acta mathematica Bd. 14, S. 217—224]] ergab nun, daß in jeder Klasse ternärer diophantischer Gleichungen vom Geschlechte Null auch quadratische Gleichungen enthalten sind. Die sich hier anknüpfende Frage nach den Invarianten einer solchen Klasse findet daher durch die allgemeinen Sätze, welche Herr Minkowski aufstellt und beweist, ihre Erledigung. A. Hurwitz.

der Form sich um das Quadrat der rationalen Transformationsdeterminante vervielfacht, die Gesamtheit aller der Primzahlen ungeändert, welche in der Determinante der Form in ungeraden Potenzen aufgehen. Das Produkt aller dieser Primzahlen, mit dem Vorzeichen $(-1)^I$ der Determinante genommen, heiße $A$; sind Primzahlen der bezeichneten Art nicht vorhanden, so werde $A = (-1)^I$ gesetzt.

Weiter werde ich nun zeigen, daß, wenn $p$ eine ganz beliebige Primzahl bedeutet, immer aus den Resten der Form $f$ für genügend hohe Potenzen von $p$ als Moduln in gewisser Weise eine im allgemeinen nicht schon durch $A$ allein bestimmte Größe sich herstellen läßt — ich werde sie $C_p$ nennen —, welche ihrer Bildung nach nur der Werte 1 oder $-1$ fähig ist, und welche den Wert, den sie für $f$ hat, bei keiner rationalen umkehrbaren Transformation von $f$ verändert (vgl. unten Gleichung (1) und (2)). Für alle diejenigen ungeraden Primzahlen, welche weder in der Determinante noch in dem Generalnenner der Koeffizienten von $f$ wirklich vorkommen (d. h. in nichtverschwindenden Potenzen), findet sich diese Einheit von vornherein gleich $+1$, so daß sie überhaupt nur für eine endliche Anzahl von Primzahlen $-1$ sein kann. Diese Bemerkung vorweggenommen, besteht für die Gesamtheit der Einheiten $C_p$ von vornherein eine Beziehung zu den Werten $n$, $I$ und $A$, nämlich ihr Produkt, also $C_2 C_3 C_5 C_7 C_{11} \ldots$, erweist sich, wenn $j$ die Anzahl der verschiedenen Primzahlen von der Form $4l+3$ aus $A$ bedeutet, gleich 1 oder $-1$, je nachdem die Zahl $n - 2I - 2j$ modulo 8 den Rest 0, 1, 6, 7 oder 2, 3, 4, 5 läßt. Auf diese Beziehung gründe ich eben den Nachweis für die invariante Natur der Einheiten $C_p$: ich mache zuerst klar, daß jedesmal bei einer Transformation höchstens diejenigen Einheiten $C_p$ sich ändern könnten, welche den in der Determinante und dem Generalnenner der Transformation vorkommenden Primzahlen entsprechen, und dann nehme ich zu Hilfe, daß eine jede rationale umkehrbare Transformation aus solchen besonderen zusammengesetzt werden kann, in deren Determinante und Generalnenner höchstens eine einzige Primzahl aufgeht. Da nun das Produkt aller Einheiten $C_p$ invariant sein soll und deshalb sich nicht eine allein ändern kann, so bleiben bei derartigen Teiltransformationen und also auch bei jeder Transformation die Einheiten $C_p$ ausnahmslos ungeändert.

Im Falle $n = 2$ gelten außerdem noch folgende Beziehungen der Einheiten $C_p$ zu dem von quadratischen Teilern befreiten Kern der Determinante: Sowie eine Primzahl $p$ in $A$ nicht vorkommt und $-A$ quadratischer Rest von $p$ bzw., im Falle $p = 2$, von 8 ist, ist immer $C_p = 1$. — Im Falle $n = 1$ sind durch die Zahl $A$ bereits sämtliche Einheiten $C_p$ bestimmt: Für die in $A$ nicht aufgehenden Primzahlen ist immer $C_p = 1$,

für die in $A$ aufgehenden gleich 1 oder $-1$, je nachdem $\frac{A}{p}$ quadratischer Rest oder Nichtrest von $p$ ist bzw., im Falle $p = 2$, die Form $8l \pm 1$ oder $8l \pm 3$ hat.

Nach dem, was über die Einheiten $C_p$ bereits gesagt ist, müssen auch alle solchen ungeraden Primzahlen sich nach jeder rationalen Transformation von $f$ beständig in der Determinante oder dem Generalnenner der transformierten Form wiederfinden, welche zwar der Zahl $A$ nicht angehören, aber ein $C_p = -1$ ergeben; ist B das Produkt aller *dieser* Primzahlen, so wird daher, wenn die transformierte Form ganzzahlige Koeffizienten erhalten sollte, ihre Determinante den Faktor $A\mathsf{BB}$ haben müssen.

Durch eine Reihe von sehr einfachen ganzzahligen Transformationen mit der Determinante 1 und von solchen rationalen Transformationen, welche jede darin bestehen, daß sie eine einzelne Variable rational vervielfachen, gelingt es nun stets, wie ich zeigen werde, die vorgelegte Form in eine Form mit ganzzahligen Koeffizienten und genau von der Determinante $A\mathsf{BB}$ überzuführen. Dabei erweisen sich dann diejenigen arithmetischen Funktionen dieser Form, welche, wie man sich ausdrückt, ihr *Geschlecht* definieren, im allgemeinen als eindeutig durch $I$, $A$ und die Einheiten $C_p$ bestimmt. Nur, wenn zwischen $n$, $A$ und dem Werte der Einheit $C_2$ eine gewisse Beziehung statthat, könnte noch die erhaltene Form zwei verschiedenen Geschlechtern von der Determinante $A\mathsf{BB}$ angehören; dann ist von diesen nur eines ungerade Zahlen darzustellen fähig, und sollte man nicht gerade zu einer Form dieses ungeraden Geschlechts gekommen sein, so kann man zu der erhaltenen Form stets solche äquivalente Formen finden, welche sich in Formen dieses Geschlechts in der einfachen Weise überführen lassen, daß man eine gewisse ihrer Variablen mit 2, eine gewisse andere mit $\frac{1}{2}$ multipliziert. Nun hat zuerst Henry John Stephen Smith*) ausgesprochen, daß irgend zwei Formen *eines* Geschlechts immer durch rationale Transformationen von der Determinante 1 und mit einem, zu einer beliebig vorgeschriebenen Zahl relativ primen Generalnenner ineinander übergeführt werden können, eine Eigenschaft, welche sie umgekehrt auch als zu demselben Geschlecht gehörig charakterisiert. Smith hat diesen fundamentalen Satz der Lehre von den quadratischen Formen in der Abhandlung „*On the Orders and Genera of Ternary Quadratic Forms*“ art. 12**) für ternäre Formen bewiesen, und auf Grund derselben Prinzipien und unter Zuhilfenahme gewisser Resultate aus meiner Arbeit „*Sur la théorie des formes quadratiques à coefficients*

*) Proceedings of the Royal Society of London, XVI. 1868. p. 202. (Collected Papers, vol. I, p. 516.)

**) Philosophical Transactions, CLVII. 1867. (Collected Papers, vol. I, p. 480.)

*entiers*"*) kann der Beweis für Formen mit beliebiger Variablenzahl geführt werden. Demnach wird es immer möglich sein, unsere Form $f$ in eine bestimmte Form eines, durch die Einheiten $C_p$ (und durch $n$ und $I$) völlig bestimmten Geschlechts von der Determinante $A\mathsf{BB}$ rational zu transformieren.

Nun bezeichne $B$ das Produkt aller überhaupt vorhandenen ungeraden Primzahlen, für welche $C_p = -1$ ist; dann sind aus dem Werte von $B$ die Werte sämtlicher Einheiten $C_p$ ersichtlich — der Wert von $C_2$ bei Benutzung der Relation für das Produkt aller $C_p$ —, und man wird den Satz aussprechen dürfen:

Theorem I. *Zwei rationale quadratische Formen mit n Variablen und nichtverschwindenden Determinanten können dann und nur dann rational ineinander transformiert werden, wenn sie gleiche Invarianten I, A und B haben.*

Die vorher definierte Zahl $\mathsf{B}$ ist offenbar der Quotient aus $B$ und dem größten Divisor von $A$ und $B$.

Der Trägheitsindex $I$ ist eine Zahl zwischen 0 bis $n$. $A$ hat das Vorzeichen $(-1)^I$, $B$ ist positiv; vom Vorzeichen abgesehen, sind $A$ und $B$ Produkte von lauter verschiedenen Primzahlen bzw. 1; $B$ ist ungerade, in $A$ kann unter Umständen die Primzahl 2 eingehen. — Im Falle $n = 2$ enthält $B$ niemals eine ungerade Primzahl, welche in $A$ nicht vorkommt und von welcher $-A$ quadratischer Rest ist, weil für jede solche Primzahl hier $C_p = 1$ ist, und wenn $-A \equiv 1 \pmod 8$ ist, ist immer $C_2 = 1$ und muß infolgedessen die Anzahl der in $B$ vorkommenden Primzahlen mit der alsdann offenbar ganzzahligen Größe $\frac{1}{2}(1 - I - j)$ zugleich gerade oder ungerade ausfallen; dabei soll $j$ wieder die Anzahl der Primzahlen von der Form $4l + 3$ aus $A$ vorstellen. — Im Falle $n = 1$ ist $B$ das Produkt aller derjenigen ungeraden Primzahlen $p$ aus $A$, für welche $\frac{A}{p}$ quadratischer Nichtrest von $p$ ist.

*Zu jedem mit den vorstehenden Bedingungen verträglichen Systeme von Zahlen n, I, A, B gibt es wirklich ein oder zwei Geschlechter ganzzahliger Formen von der zugehörigen Determinante* $A\mathsf{BB}$, und können Repräsentanten dieser Geschlechter nach pp. 89—90 meiner vorher zitierten Arbeit [[diese Ges. Abhandlungen, Bd. I, S. 76—77]] aufgestellt werden.

Sie sehen hiernach, daß bei gegebener Variablenzahl und gegebenem Trägheitsindex stets unendlich viele verschiedene Typen von quadratischen Formen, die nicht rational ineinander zu transformieren sind, existieren, und daß von $n = 3$ an die unendliche Anzahl dieser Typen in gewissem

*) Mémoires présentés à l'Académie des Sciences de l'Institut de France, XXIX. Nr. 2. 1884. Diese Ges. Abhandlungen, Bd. I, S. 3—144.

Sinne durch eine Potenz von 2 ausgedrückt werden kann, deren Exponent die um 1 verminderte doppelte Anzahl aller natürlichen Primzahlen ist.

Man kann die Invarianten $n$, $I$, $A$, $B$ einer *zerfallenden* quadratischen Form, d. h. einer solchen, welche als Summe zweier Formen mit verschiedenen Variablen erscheint, stets durch die entsprechenden Invarianten ihrer Teile und umgekehrt die eines Teiles durch die der Form und des anderen Teiles darstellen. Nämlich die Zahlen $n$ der Teile und ebenso die Zahlen $I$ der Teile geben summiert die entsprechende Zahl der Summe; die Invariante $A$ der Summe ist, von ihrem Vorzeichen $(-1)^I$ abgesehen, das Produkt aller der Primzahlen, welche nur in einer der Zahlen $A$ der zwei Teile vorkommen, und endlich ist (vgl. unten Gleichung (3)) die Zahl $B$ der Summe das Produkt aller der Primzahlen von der Form $4l+1$, welche nur in einer der Zahlen $B$ der Teile vorkommen, und aller der Primzahlen von der Form $4l+3$, welche entweder in beiden $A$ und in beiden oder in keinem der $B$ der Teile, oder in einem der $B$ und zugleich in einem oder in keinem der $A$ der Teile vorkommen.

Hält man dieses Resultat mit dem Umstande zusammen, daß von $n=3$ an die Invarianten $A$ und $B$ völlig unabhängig voneinander sind, so ist insbesondere zu schließen, *daß man zu jeder Form $f$ mit mehr als drei Variablen nach Belieben eine Form $g$ mit drei Variablen weniger annehmen kann, welche nur, als Aggregat von soviel Quadraten reeller linearer Formen dargestellt, als sie Variablen besitzt, weder mehr positive noch mehr negative Quadrate enthalten darf als $f$ in einer entsprechenden Darstellung, und daß dann jedesmal ein Typus von rationalen Formen $\chi$ mit drei Variablen existiert, so daß $f$ rational in $g+\chi$ transformiert werden kann.* Beispielsweise kann $g=\sum \pm x_h^2 (h=1,2,\ldots,n-3)$ genommen werden, wenn darin nicht mehr als $I$ Koeffizienten $-1$ und nicht mehr als $n-I$ gleich 1 sind, wobei $n$ und $I$ sich auf $f$ beziehen. —

Bei der von Ihnen angeregten Frage nun handelt es sich nicht darum, ob zwei quadratische Formen sich direkt rational ineinander transformieren lassen, sondern ob vielleicht eine solche Transformation dadurch möglich gemacht werden kann, daß man die Formen noch mit geeigneten Faktoren versieht. Es ist also noch zu untersuchen, in welchen Punkten die Zahlen $n$, $I$, $A$, $B$ der verschiedenen rationalen Multipla einer und derselben Form $f$ alle miteinander übereinstimmen und in welchen nicht.

Je nachdem der Faktor, mit welchem man eine Form $f$ multipliziert, positiv oder negativ ist, ändert sich ihr Index $I$ nicht, oder er geht in $n-I$ über; in jedem Falle bleibt der absolute Wert von $n-2I$ unverändert; ich bemerke, daß $n-2I$ die Differenz zwischen der Anzahl der Quadrate mit positivem und der mit negativem Vorzeichen in einer Darstellung von $f$ als Aggregat von $n$ Quadraten reeller linearer Formen ist. Wenn $n$

gerade und $I = \frac{n}{2}$ ist, so behält der Index selbst in jedem Falle seinen Wert.

Wir können uns hier auf Hinzufügung solcher rationaler Faktoren $M$ zu $f$ beschränken, die, vom Vorzeichen abgesehen, Produkte von lauter verschiedenen Primzahlen sind, indem wir uns jeden rationalen quadratischen Faktor mit den Variablen der Form verschmolzen denken können. Die Determinante von $f$ nimmt in $Mf$ den Faktor $M^n$ an. Wenn $n$ gerade ist, so bleibt also ihr von quadratischen Teilern entblößter Kern $A$ ungeändert; ist $n$ ungerade, so gibt es unter allen diesen Vielfachen $Mf$ ein einziges, dessen Determinantenkern 1 ist, nämlich die Form $Af$, und es wird dann die dieser Form zukommende Zahl $B$ als Invariante der diophantischen Gleichung $f = 0$ zu betrachten sein.

Um die hinsichtlich der Einheiten $C_p$ obwaltenden Verhältnisse klarzulegen, möge mit $\delta(p)$ oder $\delta$ die Zahl 0 bzw. 1 bezeichnet werden, je nachdem die gerade betrachtete Primzahl $p$ in der Zahl $A$ von $f$ nicht vorkommt bzw. darin vorkommt. Unter $c_p$ soll dann die positive oder negative Einheit verstanden werden, je nachdem die, $p$ nicht mehr enthaltende Zahl $(-1)^{\left[\frac{n}{2}\right]+(n-1)\delta} \cdot p^{-\delta} A$ quadratischer Rest oder Nichtrest von $p$ ist bzw., falls $p = 2$ ist, die Form $8l \pm 1$ oder $8l \pm 3$ hat; endlich soll $c$ ohne Index diejenige Einheit vorstellen, welcher die ungerade Zahl $(-1)^{\left[\frac{n}{2}\right]} 2^{-\delta(2)} A$ modulo 4 kongruent ist; $\left[\frac{n}{2}\right]$ bedeutet hier immer die größte in $\frac{n}{2}$ enthaltene ganze Zahl. Wenn $n$ gerade ist, so sind für alle Formen $Mf$ die Zahlen $\delta$ dieselben. Aus den später für die Einheiten $C_p$ aufzustellenden Gleichungen (vgl. unten (1) und (2)) wird nun unmittelbar zu schließen sein:

*Von der Einheit $C_p$ einer Form $f$ unterscheidet sich die entsprechende Einheit einer Form $Mf$, wenn $M = p$ ist, um den Faktor $c_p$; wenn $M$ zu $p$ relativ prim ist, um den Faktor $\left(\frac{M}{p^\delta}\right)$ oder $\left(\frac{c^{n-1} 2^\delta}{M}\right)$, je nachdem $p$ ungerade oder 2 ist.* Die Klammern bedeuten das Legendre-Jacobische Symbol, und zwar setze ich dasselbe hier für den Fall negativer Zahlen im Zähler wie im Nenner durch die Gleichung $\left(\frac{Z}{N}\right) = -\left(\frac{Z}{-N}\right)$ definiert voraus, so daß insbesondere für alle ungeraden Zahlen $N$, für positive sowohl wie für negative, das Symbol $\left(\frac{-1}{N}\right) = (-1)^{\frac{N-1}{2}}$ ist. Hieraus folgt nun:

1) Wenn $n$ gerade ist, so hat eine Einheit $C_p$ dann und nur dann für alle Formen $Mf$ gleichen Wert, wenn $p$ in $A$ nicht vorkommt ($\delta = 0$) und $(-1)^{\frac{n}{2}} A$ quadratischer Rest von $p$ bzw., wenn $p = 2$, von 8 ist ($c_p = 1$

bzw. $c = 1$ und $c_2 = 1$). Bezeichnet also $\mathsf{B}_1$ das Produkt aller derjenigen von den hier in Betracht kommenden Primzahlen, für welche $C_p = -1$ ist, so stellt dieses $\mathsf{B}_1$, ebenso wie $A$, hier eine Invariante der Gleichung $f = 0$ vor. $\mathsf{B}_1$ ist, von einem eventuellen Faktor 2 abgesehen, ein Divisor der früher definierten Zahl $\mathsf{B}$; multipliziert man $f$ mit allen außerdem noch in $\mathsf{B}$ vorkommenden ungeraden Primzahlen (d. h. für die $\delta = 0$, $c_p = -1$, $C_p = -1$ ist) und noch mit der Primzahl 2, falls $(-1)^{\frac{n}{2}} A \equiv 5 \pmod 8$ (d. i. $\delta(2) = 0$, $c = 1$, $c_2 = -1$) und $C_2 = -1$ ist, so entsteht eine Form, die $\mathsf{B}_2 f$ heißen möge, welche unter den Vielfachen $Mf$ die Eigenschaft besitzt, für möglichst wenige von den in $A$ nicht vorkommenden ungeraden Primzahlen, nämlich nur für diejenigen aus $\mathsf{B}_1$, ein $C_p = -1$ zu ergeben, und auch, wenn $(-1)^{\frac{n}{2}} A \equiv 1 \pmod 4$ ist, insofern dies überhaupt angeht, nicht ein $C_2 = -1$ zu liefern.

Da die Zahlen $A$ und $\mathsf{B}_1$ Produkte von lauter verschiedenen Primzahlen sind, so sind die Werte dieser beiden Zahlen aus dem Werte der einen Zahl $D = A\mathsf{B}_1\mathsf{B}_1$ zu entnehmen, welche, da $\mathsf{B}_1$ zu $A$ relativ prim ist, keine Primzahl in einer höheren als der zweiten Potenz enthalten wird. Der Wert dieser Zahl $D$ ist außer durch das Verhältnis, in welchem die einzelnen Primzahlen von $\mathsf{B}_1$ zu $A$ stehen sollen, durch die bereits oben erwähnten, für die Einheiten $C_p$ von vornherein gegebenen Beziehungen in der Weise beschränkt, daß, wenn $(-1)^{\frac{n}{2}} A = 1$ (d. h. $A = \pm 1$ und $\frac{1}{2}(n - 2I)$ gerade) ist, die Anzahl der in $\mathsf{B}_1$ auftretenden Primzahlen zugleich mit der Zahl $\frac{1}{4}(n - 2I)$ gerade oder ungerade sein muß, und daß im Falle $n = 2$ immer $\mathsf{B}_1 = 1$ ist.

2) Wenn $n$ ungerade ist, so möge der Buchstabe $D$ zur Bezeichnung der Invariante $B$ der Form $Af$ verwandt werden; diese findet sich dann, durch die Invarianten von $f$ ausgedrückt, gleich $A_1\mathsf{B}$, wenn $A_1$ das Produkt aller derjenigen ungeraden Primzahlen aus $A$ bedeutet, für welche $C_p = -c_p$ ist. Im Falle $n = 1$ ist immer $D = 1$.

Theorem II. *Wenn zwei Formen mit n Variablen und mit nichtverschwindenden Determinanten in den absoluten Werten ihrer Zahlen $n - 2I$ und in ihren Invarianten D übereinstimmen, so kann jede von ihnen rational in ein rationales Vielfaches der anderen transformiert werden.*

Ich beweise diesen Satz, indem ich ihn auf den Satz I zurückführe:

1) Ist $n$ gerade, so multipliziere man jede der beiden Formen mit ihrer Zahl $\mathsf{B}_2$, und falls die Indizes der Formen nicht gleich sind (also sich zu $n$ ergänzen und beziehungsweise unter und über $\frac{1}{2}n$ liegen), noch eine der Formen mit $-1$. Man hat dann zwei Formen, $\varphi$, $\psi$, welche gleichen Index und dasselbe $A$ besitzen, und für alle in ihrer Zahl $A$ nicht

aufgehenden ungeraden Primzahlen gleiche Einheiten $C_p$ liefern, und überdies, wenn $(-1)^{\frac{n}{2}} A \equiv 1 \pmod 4$ (d. h. $\delta(2) = 0$, $c = 1$) ist, auch dasselbe $C_2$ ergeben; und es kommt darauf an, eine der Formen, etwa $\psi$, noch mit einem solchen positiven Faktor zu multiplizieren, daß eine Form entsteht, welche mit der anderen Form $\varphi$ in *allen* Einheiten $C_p$ übereinstimmt. Ist nun $M$ irgendeine zu $2D$ relativ prime, positive ganze Zahl, welche den Bedingungen genügt, daß für jede in $A$ aufgehende ungerade Primzahl $p$ $\left(\frac{M}{p}\right) = 1$ oder $= -1$ ist, je nachdem die Charaktere $C_p$ für $\varphi$ und $\psi$ gleich oder verschieden sind, und daß, wenn *nicht* $(-1)^{\frac{n}{2}} A \equiv 1 \pmod 4$ ist, das Symbol $\left(\frac{c 2^{\delta(2)}}{M}\right) = 1$ oder $= -1$ ist, je nachdem $\varphi$ und $\psi$ gleiche oder verschiedene Charaktere $C_2$ haben, so kann bei $M\psi$ und $\varphi$ ein Zweifel über die Gleichheit der Einheiten $C_p$ nur noch hinsichtlich der in $M$ aufgehenden Primzahlen möglich sein. Die genannten Bedingungen für $M$ sind aber derart, daß man ihnen durch eine *Primzahl* gerecht werden kann, in welchem Falle es sich nur noch um den einen Charakter $C_M$ handeln wird; und dieser wird dann für $M\psi$ und $\varphi$ deshalb nicht verschieden sein können, weil er sich für beide Formen in gleicher Weise durch das Produkt der übrigen Charaktere $C_p$ ausdrücken läßt.

2) Ist $n$ ungerade, so multipliziere man jede der vorgelegten Formen mit ihrer Zahl $A$, und man erhält so zwei Formen, für die alle Bedingungen dafür erfüllt sind, daß sie sich rational ineinander transformieren lassen.

Es mögen noch einige spezielle Folgerungen aus den Sätzen I und II Erwähnung finden.

Eine rationale Form kann dann und nur dann in irgendwelche *negative*, rationale Multipla von sich selbst rational transformiert werden, wenn ihre Variablenzahl $n$ gerade und ihr Trägheitsindex gleich $\frac{1}{2}n$ ist.

*Eine Form $f$ ist dann und nur dann in $-f$ rational zu transformieren, wenn ihre Variablenzahl $n$ gerade, ihr Trägheitsindex gleich $\frac{1}{2}n$ ist und ihre Determinante keine Primzahl von der Form $4l + 3$ in ungerader Potenz enthält.*

Durch welche quadratische Formen mit $n$ Variablen können von Null verschiedene, rationale Quadratzahlen dargestellt werden? Ist durch irgendeine Form eine von Null verschiedene Zahl $N$ darstellbar, so läßt die Form sich stets so rational transformieren, daß sie die Zahl $N$ als ersten Koeffizienten erhält, und dann geht sie bei dem ersten Schritte der gewöhnlichen Methode, eine quadratische Form in Einzelformen mit einer Variable zu zerlegen, über in $Nx^2 +$ einer Form, welche die Variable $x$ nicht mehr enthält. Es handelt sich also hier um die Kriterien für solche Formen mit $n$ Variablen, welche sich rational transformieren lassen in

das Quadrat einer Variable + einer Form mit $n-1$ Variablen, und man findet:

*Von Null verschiedene rationale Quadratzahlen sind darstellbar durch jede nicht wesentlich negative Form mit* 4 *oder mehr Variablen; durch jede nicht wesentlich negative Form mit drei Variablen, deren Invarianten A und B auch bei Formen mit zwei Variablen vorkommen können* (die hierfür zu erfüllenden Bedingungen s. oben)*; durch jede nicht wesentlich negative Form mit zwei Variablen, deren Invarianten A und B auch bei einer Form mit einer Variable vorkommen können.*

Wann kann durch eine rationale Form $f$ die Zahl Null rational dargestellt werden (natürlich, ohne daß alle Variablen verschwindende Werte erhalten)? Es sei $f$ irgendwie in eine Summe von $n$ Formen mit einer Variablen transformiert, und in einer Lösung von $f=0$ etwa die Variable einer dieser Formen, welche $Nx^2$ heißen möge, von Null verschieden und $=x_1$. Die Form $f$ besteht dann aus $Nx^2$ und einer Form mit $n-1$ Variablen; durch letztere wird, während durch $f$ die Zahl Null dargestellt wird, die Zahl $-Nx_1^2$ dargestellt, und diese Form läßt sich daher nach dem vorher Bemerkten rational transformieren in eine Form $-Ny^2+$ einer Form mit $n-2$ Variablen. Da nun $N(x^2-y^2)$ stets in $x^2-y^2$ rational zu transformieren ist, so muß also $f$ in $x^2-y^2+$ einer Form mit $n-2$ Variablen zu transformieren sein, wenn $f=0$ lösbar sein soll; so ergibt sich:

*Die Zahl Null ist rational darstellbar*
*durch jede indefinite Form mit fünf oder mehr Variablen,*
*durch jede indefinite Form mit vier Variablen, deren Invariante D nur erste (keine zweiten) Potenzen von Primzahlen enthält,*
*durch jede indefinite Form mit drei Variablen, deren Invariante D gleich* 1 *ist,*
*durch jede (indefinite) Form mit zwei Variablen, deren Invariante* $D=-1$ *ist.*

Betreffs der über die Gleichung $ax^2+by^2+cz^2=0$ existierenden Literatur sei auf die Vorlesungen über Zahlentheorie von Dirichlet, herausgegeben von Dedekind, III. Aufl. Suppl. X [[IV. Aufl. Suppl. X, S. 418 ff.]] verwiesen. Kriterien für die Darstellbarkeit der Zahl Null durch beliebige ternäre Formen sind von H. J. St. Smith*) ohne Beweis publiziert: dieselben sind dann später von Herrn A. Meyer**) begründet worden. Ferner hat Herr Meyer***) die notwendigen und hinreichenden Bedingungen für

*) Proceedings of the Royal Society of London, XIII, p. 110. (Collected Papers, vol. I, p. 410.)

**) Crelles Journal für Mathematik, Bd. 98, S. 177.

***) Mathematische Mitteilungen, Vierteljahrsschrift der naturforschenden Gesellschaft in Zürich, XXIX. S. 209.

die Auflösbarkeit der Gleichung $ax^2+by^2+cz^2+du^2=0$, doch in einer umständlicheren Fassung als der hier gegebenen, aufgestellt und bewiesen, daß durch eine jede indefinite Form mit mehr als vier Variablen die Zahl Null rational darstellbar ist. — Endlich ist zu erwähnen, daß Eisenstein*) die Frage behandelt hat, welche ternären Formen sich rational in ein Multiplum von $x^2+y^2+z^2$ transformieren lassen.

Ich werde nun zunächst das Bildungsgesetz der Einheiten $C_p$ ableiten.

---

Jeder rationalen quadratischen Form $f(x_1, x_2, \ldots, x_n)$ mit gebrochenen Koeffizienten kann in ganz bestimmter Weise eine aus ihr durch eine rationale Transformation abzuleitende Form mit ganzen Koeffizienten zugeordnet werden, nämlich, wenn $\mathsf{N}$ den Generalnenner der Koeffizienten von $f$ bedeutet, die Form $\mathsf{N}\mathsf{N}f$, in welche $f$ durch die Substitution $x_h=\mathsf{N}y_h$ $(h=1, 2, \ldots, n)$ übergeht. Wir können uns deshalb auf die Betrachtung ganzzahliger Formen beschränken, und brauchen mit denselben auch nur solche Transformationen vorzunehmen, durch welche wir wieder auf ganzzahlige Formen kommen.

Es ist klar, daß wir solche Funktionen einer quadratischen Form, welche für alle rationalen umkehrbaren Transformationen der Form invariant sein sollen, nur unter den, das Geschlecht der Form definierenden Größen zu suchen haben; Größen nämlich, die nicht einmal für alle Formen eines Geschlechts gleichwertig sind, erleiden immer schon bei gewissen rationalen Transformationen von der Determinante 1 Änderungen.

Die Invarianten des Geschlechts einer quadratischen Form sind ihre *Ordnung* und ihre *Charaktere*. (Die nun zunächst folgenden Bemerkungen sind meinem Aufsatze „Sur la théorie des formes quadratiques“ entnommen, den ich weiterhin kurz mit *F. Q.* zitieren will.)**) Heißt die Form $f=\sum_1^n a_{hk}x_hx_k (a_{hk}=a_{kh})$, und sind alle Koeffizienten ganze Zahlen und die Determinante $|a_{hk}|=\Delta$ von Null verschieden, so rechnet man zu den Bestimmungsstücken der Ordnung der Form ihre Zahl $n$, ihren Trägheitsindex $I$, ihre Determinante $\Delta$, ferner die größten gemeinsamen Teiler aller einreihigen, aller zweireihigen usw. bis aller $(n-1)$-reihigen Unterdeterminanten von $|a_{hk}|$ — diese Teiler mögen der Reihe nach $d_0, d_1, \ldots, d_{n-2}$ heißen, endlich diejenigen größten gemeinsamen Teiler, welche an die Stelle dieser Teiler treten, wenn von den betreffenden Unterdeterminanten die unsymmetrischen mit dem Faktor 2 multipliziert genommen werden

---

*) Journal de Liouville. XVII. 1852. S. 473.

**) In [[ ]] fügen wir diesen Zitaten den entsprechenden Hinweis auf die in diesen Gesammelten Abhandlungen, Bd. I, S. 3—144, veröffentlichte deutsche Ausgabe hinzu. (Anm. d. Herausg.)

— diese letzteren Teiler bezeichne ich mit $\sigma_1 d_0$, $\sigma_2 d_1$, ..., $\sigma_{n-1} d_{n-2}$, so daß eine jede Zahl $\sigma_h$ gleich 1 oder gleich 2 ist; ich setze noch $\Delta = (-1)^l d_{n-1}$ und $\sigma_0 = 1$, $\sigma_n = 1$. Die durch die Gleichungen

$$d_h = d_0^{h+1} o_1^h o_2^{h-1} \ldots o_h \qquad (h = 1, 2, \ldots, n-1)$$

bestimmten $n-1$ Größen $o_h$ erweisen sich immer als ganze Zahlen (*F. Q.*, p. 6 [[S. 13]]), und ferner sind die Zahlen $\sigma_h$ immer so beschaffen, daß ein Produkt $\sigma_{h-1} o_h \sigma_{h+1}$ ungerade ist, sowie $\sigma_h = 2$ ist, und durch 4 teilbar, sowie $\sigma_{h-1} = 2$ oder $\sigma_{h+1} = 2$ ist (*F. Q.*, p. 31 [[S. 31]]).

Die Charaktere sind Größen, die in Gestalt Legendrescher Symbole auftreten, also Einheiten $\pm 1$; ihre Werte können, wie ich *F. Q.* artt. VII-IX [[S. 45—70]] gezeigt habe, ausnahmslos erschlossen werden aus den Werten der verschiedenen Summen*)

$$f(\alpha, N) = \sum e^{\frac{2\pi i \alpha f(x_1, x_2, \ldots, x_n)}{N}} \qquad \begin{pmatrix} x_h = 1, 2, \ldots, N \\ h = 1, 2, \ldots, n \end{pmatrix},$$

in welchen $N$ und $\alpha$ zueinander relativ prime ganze Zahlen bedeuten und die Variablen Restsysteme modulo $N$ zu durchlaufen haben; $e$ ist hier die Basis der natürlichen Logarithmen, $\pi$ die Ludolphsche Zahl, $i = \sqrt{-1}$. Die Werte solcher Summen $f(\alpha, N)$ hängen offenbar nur von den Resten von $f$ in bezug auf die Moduln $N$ ab.

Indem man die Betrachtungen, welche *F. Q.*, p. 60 beziehungsweise p. 65 [[S. 54 und 58]] abgebrochen sind, fortführt, gelangt man in betreff dieser Summen insbesondere zu folgendem wichtigen Resultate:

*Zu jeder Primzahl $p$ gehört eine gewisse Einheit $C_p$ von solcher Art, daß für jede Potenz $p^t$, welche nicht niedriger als die in $\frac{4\Delta}{\sigma_{n-1} d_{n-2}}$ aufgehende Potenz von $p$ ist, und jede beliebige zu $p$ relativ prime Zahl $\alpha$, wenn noch $p^\partial$ die höchste in $\Delta$ enthaltene Potenz von $p$ bedeutet und die Einheiten $c_p$ und $c$ in der bereits oben festgesetzten Beziehung zur Determinante stehen, die Gleichung gilt: wenn $p$ ungerade ist,*

$$(1) \qquad f(\alpha, p^t) = \left(\frac{\alpha}{p^{\partial+nt}}\right) C_p c_p{}^t i^{\left(\frac{p^{\partial+nt}-1}{2}\right)^2} p^{\frac{\partial+nt}{2}};$$

*wenn $p = 2$ ist,*

$$(2) \qquad f(\alpha, 2^t) = \left(\frac{c^{n-1} 2^{\partial+nt}}{\alpha}\right) C_2 c_2{}^t (-i)^{\left(\frac{\alpha^n c-1}{2}\right)^2} \left(\frac{1+i}{\sqrt{2}}\right)^{n-2\left[\frac{n}{2}\right]} 2^{\frac{\partial+nt+n}{2}}.$$

Die erste Klammer auf der rechten Seite ist jedesmal ein Legendresches Symbol. Ich bemerke noch, daß $\sigma_{n-1} d_{n-2}$ den größten gemeinsamen Teiler der sämtlichen Zahlen $\frac{\partial\Delta}{\partial a_{hh}}$ und $2\frac{\partial\Delta}{\partial a_{hk}}$ $(h \neq k)$ vorstellt.

---

*) Diese Summen bilden auch den Gegenstand des Aufsatzes von Herrn H. Weber: Ueber die mehrfachen Gaußschen Summen, Crelles Journal, Bd. 74, S. 214—256.

Da für solche ungerade Primzahlen, welche in der Determinante $\Delta$ nicht vorkommen, der Exponent $t$ in (1) bereits gleich Null genommen werden darf, so ist für alle diese Primzahlen offenbar $C_p = 1$. Überhaupt haben wir hier diejenigen Einheiten vor uns, von welchen oben die Rede gewesen ist, wenn wir nur noch festsetzen, daß unter den Einheiten $C_p$ einer Form $f$ mit einem Generalnenner $\mathsf{N} > 1$ die entsprechenden Einheiten der ganzzahligen Form $\mathsf{N}\mathsf{N}f$ verstanden werden sollen.

Daß eine jede der vorstehend definierten Einheiten $C_p$ ungeändert bleibt bei allen solchen rationalen umkehrbaren Transformationen von $f$, bei welchen Determinante und Generalnenner zu der betreffenden Primzahl $p$ relativ prim sind, und welche aus $f$ wieder ganzzahlige Formen hervorgehen lassen, ist ohne weiteres ersichtlich. Denn da durch solche Transformationen aus zwei, für einen Modul $p^t$ inkongruenten Systemen der Variablen von $f$ immer wieder inkongruente Systeme der neuen Variablen, und also aus vollständigen Restsystemen in bezug auf einen Modul $p^t$ wieder solche Systeme entstehen, so erfahren dabei die Summen $f(\alpha, p^t)$ keine Veränderung, nnd da offenbar auch die Potenz $p^\vartheta$ sich nicht ändert, so behält auch die Einheit $C_p$ ihren Wert bei.

Sehen wir nun zu, wie diese Einheiten $C_p$ zu berechnen sind. Zerfällt eine Form $f$, in bezug auf einen Modul $p^t$ betrachtet, in die Summe zweier Formen, $f'$, $f''$, mit verschiedenen Variablen, so ist jede ihr zugehörige Summe $f(\alpha, p^t)$ das Produkt der analogen Summen für $f'$ und $f''$, und so folgt aus (1) für ein ungerades $p$:

$$C_p = (-1)^{\frac{p^{\vartheta'}-1}{2}\frac{p^{\vartheta''}-1}{2}} C_p' C_p'', \tag{3}$$

und aus (2) für $p = 2$:

$$C_2 = (-1)^{n'n''\frac{c-1}{2}+\frac{c'-1}{2}\frac{c''-1}{2}} C_2' C_2''; \tag{4}$$

die gestrichelten Buchstaben sind auf die Formen $f'$ und $f''$ zu beziehen.

Nun kann man jede Form $f$, wenn von ihren Zahlen $o_1, o_2, \ldots, o_{n-1}$ im ganzen $\lambda - 1$ durch eine Primzahl $p$ teilbar sind, durch höchstens $n - \lambda$ Substitutionen, welche darin bestehen, daß sie eine Variable um eine zweite vermehren, und höchstens $n - 1$ Substitutionen, welche darin bestehen, daß sie zwei Variablen miteinander permutieren und gleichzeitig eine derselben mit $-1$ multiplizieren, in eine solche Form $\varphi$ transformieren, in welcher die aus den ersten $h = 1, 2, \ldots, n-1$ Horizontal- und Vertikalreihen der Determinante gebildeten Unterdeterminanten möglichst niedrige Potenzen von $p$ als Faktoren haben, d. h. Werte $\sigma_h d_{h-1} \varphi_h$ besitzen, in denen die Zahlen $\varphi_h$ zu $p$ relativ prim sind (*F. Q.*, p. 36 [[S. 35]]); es werde noch $\varphi_0 = 1$, $\varphi_n = (-1)^I$ gesetzt. Eine derartige Form $\varphi$ nenne ich eine *Grundform* in bezug auf $p$, und eine Grundform kann weiter für

jeden Modul $p^t$ mit Hilfe von solchen Substitutionen, in deren Determinante alle Glieder links von der Diagonale Null und alle Glieder in der Diagonale 1 sind und welche daher die Werte der Zahlen $\sigma_h d_{h-1} \varphi_h$ $(h = 1, 2, \ldots, n)$ sämtlich ungeändert lassen, in sogenannte *Hauptreste* umgewandelt, d. h. dergestalt transformiert werden, daß sie modulo $p^t$ in eine Summe von Formen mit einer Variable oder, wenn $p = 2$ ist, in Formen mit einer Variable und Formen zweiter Art mit zwei Variablen zerfällt. Bringt man dann die Formeln (3) und (4) in Anwendung und benutzt zugleich die bereits oben auseinandergesetzten und nun aus (1) und (2) fast unmittelbar zu entnehmenden Relationen, welche die Einheiten $C_p$ zweier Formen verbinden, die rationale Vielfache voneinander sind, so wird man in letzter Instanz auf die Einheiten $C_p$ der Form $xx$ geführt, die sich sämtlich gleich 1 erweisen (vgl. Gauß, Summatio quarumdam serierum singularium, Werke, Bd. II), und auf Einheiten $C_2$ für Formen $\alpha xx + \beta xy + \gamma yy$ mit ganzen $\alpha$, $\beta$, $\gamma$ und ungeraden $\beta$, die ebenfalls gleich 1 sind (*F. Q.*, pp. 57—59 [[S. 51—53]]).

Die Exponenten der in den Zahlen $d_0$, $o_1$, $o_2$, …, $o_{n-1}$ der Form $f$ aufgehenden Potenzen von $p$ mögen $v_0$, $\omega_1$, $\omega_2$, …, $\omega_{n-1}$ heißen, und es werde noch gesetzt $v_0 + \omega_1 + \omega_2 + \cdots + \omega_h = v_h$ $(h = 1, 2, \ldots, n-1)$; ferner mögen mit $D_h$ $(h = 1, 2, \ldots, n)$ diejenigen, zu $p$ relativ primen Zahlen bezeichnet werden, die sich ergeben, wenn die Zahlen $\sigma_h d_{h-1} \varphi_h$ einer mit $f$ äquivalenten Grundform $\varphi$ in bezug auf $p$ von ihren Potenzen von $p$ befreit werden. Die aus einer solchen Grundform entstehenden Hauptreste lauten dann, wenn $p$ ungerade ist (*F. Q.*, p. 34 [[S. 34]]):

$$(5) \qquad p^{v_0} D_1 x_1^2 + p^{v_1} \frac{D_2}{D_1} x_2^2 + \cdots + p^{v_{n-1}} \frac{D_n}{D_{n-1}} x_n^2 \pmod{p^t},$$

und man findet auf dem soeben angegebenen Wege:

$$C_p = \left(\frac{-1}{p^{\sum v_h v_k}}\right)\left(\frac{D_n}{p^{v_{n-1}}}\right) \prod \left(\frac{D_h}{p^{\omega_h}}\right). \qquad \begin{pmatrix} h = 1, 2, \ldots, n-1 \\ k = 0, 1, \ldots, h-1 \end{pmatrix}$$

Wenn $p = 2$ ist, so können die aus einer Grundform entspringenden Hauptreste so geschrieben werden:

$$(6) \qquad \sum_{(\sigma_h = 1,\ \sigma_{h-1} = 1)} \Big\{ 2^{v_h - 1} \frac{D_h}{D_{h-1}} x_h^2$$

$$\text{bzw. } 2^{v_h - 1 + 1} \Big( \frac{D_h}{D_{h-1}} x_h^2 + u_h x_h x_{h+1} + \frac{D_{h+1} + u_h^2 D_{h-1}}{4 D_h} x_{h+1}^2 \Big) \Big\} \pmod{2^t},$$
$$(\sigma_h = 2;\ \sigma_{h-1} = 1,\ \sigma_{h+1} = 1)$$

worin die binären Formen *denjenigen* Größen $\sigma_h$ entsprechen, welche gleich 2 sind (und welche immer die Relationen $\sigma_{h-1} = 1$, $\sigma_{h+1} = 1$ und $-D_{h-1} \equiv D_{h+1} \pmod 4$ im Gefolge haben), und wobei die $u_h$ in diesen binären Formen beliebige ungerade Zahlen bedeuten; man erhält dann:

$$C_2 = (-1)^{\left[\frac{n}{4}\right]+\left[\frac{n}{2}\right]\left(\left[\frac{n}{2}\right]+\frac{D_n-1}{2}\right)}(-1)^{\sum \frac{D_h-1}{2}\frac{D_{h+1}+1}{2}}\left(\frac{\sigma_{n-1}2^{v_{n-1}}}{D_n}\right)\prod\left(\frac{\sigma_{h-1}2^{\omega_h}\sigma_{h+1}}{D_h}\right).$$
$$(h = 1, 2, \ldots, n-1)$$

Für die Gesamtheit dieser Einheiten $C_p$ besteht eine Beziehung zur Determinante von $f$, die sich folgendermaßen herleiten läßt. Man kann zu $f$ immer solche äquivalente Formen $\varphi$ finden, welche sowohl für die Primzahl 2 wie für alle in der Determinante von $f$ aufgehenden ungeraden Primzahlen Grundformen sind und in welchen außerdem je zwei aufeinanderfolgende der Zahlen $\varphi_1, \varphi_2, \ldots, \varphi_{n-1}$ zueinander relativ prim sind (*F. Q.*, p. 83 [[S. 72]]). Für solche Formen $\varphi$ führen die quadratischen Kongruenzen:

$$-\sigma_{h-1}o_h\sigma_{h+1}\varphi_{h-1}\varphi_{h+1} \equiv X_h^2 \pmod{\sigma_h^2\varphi_h}, \qquad (h = 1, 2, \ldots, n-1)$$

welche leicht aus einem bekannten Determinantensatze zu erschließen sind, zu Gleichungen:

$$\left(\frac{-\sigma_{h-1}o_h\sigma_{h+1}\varphi_{h-1}\varphi_{h+1}}{\varepsilon_h\varphi_h}\right) = 1; \qquad (h = 1, 2, \ldots, n-1)$$

die $\varepsilon_h$ sollen hier die Vorzeichen der Größen $\varphi_h$ vorstellen; und das Produkt dieser $n-1$ Gleichungen kann durch wiederholte Anwendung des quadratischen Reziprozitätsgesetzes, wenn man noch zu Hilfe nimmt, daß der Trägheitsindex $I$ mit der Anzahl der Zahlen $-1$ in der Reihe $\varepsilon_1, \frac{\varepsilon_2}{\varepsilon_1}, \frac{\varepsilon_3}{\varepsilon_2}, \ldots, \frac{(-1)^I}{\varepsilon_{n-1}}$ identisch ist, und wenn man mit $j$ die Anzahl der in der Determinante von $f$ in ungeraden Potenzen aufgehenden Primzahlen von der Form $4l+3$ bezeichnet, in die Relation umgewandelt werden:

$$(7) \qquad \prod C_p = (-1)^{\left[\frac{n-2I-2j}{4}\right]+\left[\frac{n-2I-2j}{2}\right]},$$

wo das Produkt über die Primzahl 2 und alle in der Determinante von $f$ vorkommenden ungeraden Primzahlen zu erstrecken ist und noch über beliebig viele weitere Primzahlen ausgedehnt werden kann; die eckige Klammer bedeutet das Symbol für größte ganze Zahlen.

Diese Relation verhilft uns nun zu dem noch fehlenden Nachweise, daß eine Einheit $C_p$ auch bei allen solchen rationalen umkehrbaren Transformationen von $f$ in andere ganzzahlige Formen ungeändert bleibt, bei welchen nicht sowohl Determinante wie Generalnenner zu $p$ relativ prim sind. Eine jede solche Transformation läßt sich nämlich, worauf ich sofort noch näher eingehen werde, darstellen als Produkt aus einer ersten Transformation, in deren Determinante und Generalnenner die Primzahl $p$ ausschließlich eingeht, und aus einer zweiten Transformation, in welcher Determinante und Generalnenner zu $p$ relativ prim sind. Führt die ganze Transformation die Form $f$ wieder in eine ganzzahlige Form über, so

muß solches auch die erste Teiltransformation tun, weil die zweite nicht imstande sein würde, einen durch die erste in $f$ hineingebrachten Generalnenner wieder herauszuschaffen. Die erste Teiltransformation ändert $C_p$ nicht, weil sie nach dem bereits Bewiesenen nur diese Einheit allein ändern könnte, nun aber infolge von (7) eine einzelne solche Einheit sich nicht ändern kann; die zweite ist auf $C_p$ sicher ebenfalls ohne Einfluß, also gilt dasselbe von der ganzen Transformation.

Von der Gleichung für das Produkt aller Einheiten $C_p$ läßt sich noch eine interessante Anwendung machen. Stellt man eine positive Zahl $N$, in ihre verschiedenen Primzahlpotenzen zerlegt, in der Form $N = \prod p^t$ dar, so ist nach *F. Q.*, p. 52 [[S. 48]]:

$$f(\alpha, N) = \prod f\left(\alpha \frac{N}{p^t}, p^t\right).$$

Bringt man diese Relation mit den Gleichungen (1), (2) und (7) in Verbindung, so folgt:

*Für jeden positiven Modul $N$, welcher durch $\frac{4\Delta}{\sigma_{n-1} d_{n-2}}$ teilbar ist, und für beliebige zu ihm relativ prime Zahlen $\alpha$ ist:*

$$\sum_{\substack{x_h = 1, 2, \ldots, N \\ h = 1, 2, \ldots, n}} e^{\frac{2\pi i \alpha f(x_1, x_2, \ldots, x_n)}{N}}$$
$$= \left(\frac{(-1)^{\left[\frac{n}{2}\right]} \Delta N^n}{\alpha}\right) i^{-n^2 \left(\frac{\alpha-1}{2}\right)^2 + \left[\frac{n-2I}{2}\right]} \left(\frac{1+i}{\sqrt{2}}\right)^{n-2\left[\frac{n}{2}\right]} \sqrt{(-1)^I \Delta (2N)^n}.$$

Die erste Klammer auf der rechten Seite bedeutet das Legendresche Symbol. Bemerkenswert ist namentlich, daß diese Summe nur von der Determinante $\Delta$ und dem Reste von $I$ (mod 4) abhängt, im übrigen aber von den Charakteren der Form $f$ völlig unabhängig ist.

---

Wegen des soeben herangezogenen Hilfssatzes über die Zerlegung beliebiger rationaler Transformationen in solche, deren Determinante und Generalnenner nur durch *eine* Primzahl aufgehen, kann auf die Aufsätze von Smith *„On systems of linear indeterminate equations and congruences“**) und von Frobenius über die *„Theorie der linearen Formen mit ganzen Koeffizienten“***) verwiesen werden; doch sind vielleicht auch die folgenden Bemerkungen über jenen Satz nicht uninteressant. Es genügt offenbar, wenn man die in Rede stehenden Zerlegungen für ganz-

---

*) Philosophical Transactions, vol. 151. 1861. (Collected Papers, vol. I, p. 367.)

**) Crelles Journal, Bd. 86.

zahlige Transformationen auszuführen imstande ist, da man einen etwa vorhandenen Generalnenner jederzeit in angemessener Weise in Faktoren zerlegen und diese dann unter die Teiltransformationen verteilen kann. Jede ganzzahlige Transformation läßt sich nun immer (und zwar auf unendlich viele Arten) darstellen als Produkt aus einer solchen ganzzahligen Transformation, für welche alle Elemente, die in ihrer Determinante rechts von der Diagonale stehen, Null sind und die ich deshalb für einen Moment eine rechts reduzierte Transformation nennen will, und einer ganzzahligen Transformation von der Determinante 1; dieses erhellt aus dem Umstande, daß man eine jede ganzzahlige Determinante auf die in Frage kommende Gestalt in der Weise bringen kann, daß man in ihr wiederholt Vertikalreihen zueinander addiert oder voneinander subtrahiert. Das Produkt zweier rechts reduzierter Transformationen:

$$|p_h^k| \quad (p_h^k = 0,\ h < k) \quad \text{und} \quad |q_h^k| \quad (q_h^k = 0,\ h < k) \qquad (h, k = 1, 2, \ldots, n)$$

ist nun immer wieder eine rechts reduzierte Transformation:

$$|r_h^k| \quad (r_h^k = 0,\ h < k), \qquad (h, k = 1, 2, \ldots, n)$$

und zwar ist für diese:

$$r_h^h = p_h^h q_h^h, \quad r_h^{h-d} = \sum p_h^{h-\delta}\, q_{h-\delta}^{h-d}. \quad \begin{pmatrix} h = 1, 2, \ldots, n \\ d = 1, 2, \ldots, h-1 \\ \delta = 0, 1, \ldots, d \end{pmatrix}$$

Umgekehrt ersieht man aus diesen Gleichungen, daß jede rechts reduzierte Transformation in zwei andere zerlegt werden kann, sowie für die Zahlen $r_h^h$ ihrer Diagonalreihe eine Zerlegung in Zahlenpaare $p_h^h$, $q_h^h$ von solcher Art vorliegt, daß ein jedes $p_h^h$ zu $q_1^1, q_2^2, \ldots, q_{h-1}^{h-1}$ relativ prim ist; denn alsdann kann man der Reihe nach für $d = 1, 2, \ldots, h-1$ alle Größen $p_h^{h-d}$, $q_h^{h-d}$ als ganze Zahlen finden, indem man immer zuerst $p_h^{h-d}$ der Kongruenz

$$p_h^{h-d} \equiv \frac{r_h^{h-d} - \sum_{\delta=1}^{d-1} p_h^{h-\delta}\, q_{h-\delta}^{h-d}}{q_{h-d}^{h-d}} \pmod{p_h^h} \qquad (h = d+1, d+2, \ldots, n)$$

gemäß wählt und hernach

$$q_h^{h-d} = \frac{r_h^{h-d} - \sum_{\delta=1}^{d} p_h^{h-\delta}\, q_{h-\delta}^{h-d}}{p_h^h} \qquad (h = d+1, d+2, \ldots, n)$$

setzt. Beispielsweise kann man für die Zahlen $p_h^h$ die höchsten in den Zahlen $r_h^h$ überhaupt aufgehenden Potenzen irgendeiner Primzahl $p$ nehmen, wodurch man auf die für uns wichtige Zerlegung kommt.

---

Mit dem Nachweis der invarianten Natur der Einheiten $C_p$ ist zugleich die Existenz der oben vermittels dieser Einheiten definierten Zahl $B$ sichergestellt, und es erübrigt nur noch zu zeigen, daß in der Tat mit den Zahlen $n$, $I$, $A$, $B$ das System derjenigen Funktionen einer quadratischen Form, welche bei allen rationalen umkehrbaren Transformationen der Form ungeändert bleiben, vollständig erschöpft ist.

Zu dem Ende gehe ich wieder von irgendeiner ganzzahligen quadratischen Form $f$ aus, und ich suche dieselbe rational in eine ganzzahlige Form mit möglichst kleiner Determinante zu transformieren. Es fragt sich, kann dabei ein bestimmter Primfaktor $p$ der Determinante in Wegfall kommen oder nicht.

Es sei zunächst $p$ eine ungerade Primzahl. Man bestimme irgendeine mit $f$ äquivalente Grundform in bezug auf $p$; aus einer solchen folgt für einen jeden Modul $p^t$ ein Hauptrest von dem unter (5) angegebenen Typus; es werde eine solche Potenz $p^t$ gewählt, welche die zu $f$ gehörige Potenz $p^{\nu_n - 1}$ überschreitet. Sowie dann in dem betreffenden Hauptreste (5) einer der Exponenten $v_{h-1}$ sich $\geqq 2$ erweisen sollte, kann derselbe um 2 verringert werden, dadurch daß man die zugehörige Variable dem $p^{\text{ten}}$ Teile einer neuen Variable gleich setzt, bei welcher Operation alle Koeffizienten des Hauptrestes ganze Zahlen bleiben werden. Indem man diese Reduktion so oft als angänglich wiederholt und am Schlusse nötigenfalls noch eine Umstellung der Variablen vornimmt, kommt man zu einer Form mit einem Reste:

$$\alpha_1 \xi_1^{\,2} + \cdots + \alpha_{n-m} \xi_{n-m}^{\,2} + p(\alpha_{n-m+1} \xi_{n-m+1}^{\,2} + \cdots + \alpha_n \xi_n^{\,2}) \pmod{p^2},$$

worin alle $\alpha_h$ zu $p$ relativ prim sind. Die Determinante dieser Form enthält genau die Potenz $p^m$ als Faktor, und $m$ ist eine Zahl zwischen 0 und $n$. Ob $m$ gerade oder ungerade ausfällt, wird davon abhängen, ob die Primzahl $p$ in der Zahl $A$ von $f$ nicht enthalten war ($\delta = 0$) oder in ihr vorkam ($\delta = 1$). Die Einheit $C_p$ erhält hier den Ausdruck

$$\left(\frac{(-1)^{\left[\frac{m}{2}\right]} \alpha_{n-m+1} \cdots \alpha_n}{p}\right). \tag{8}$$

*Im Falle $n = 2$ ist daher, sowie $p$ in $A$ nicht vorkommt und $-A$ quadratischer Rest von $p$ ist, immer $C_p = 1$* (nämlich sowohl für $m = 2$ wie für $m = 0$).

Die erhaltene Form kann nun unter Umständen so transformiert werden, daß an die Stelle von $m$ eine kleinere Zahl tritt. Hat man nämlich eine binäre Form

$$\begin{pmatrix} p\alpha & 0 \\ 0 & p\beta \end{pmatrix} \pmod{p^2}$$

(ich bezeichne hier die Form durch das quadratische Schema ihrer Koeffizienten), in welcher $\alpha$ und $\beta$ zu $p$ relativ prim sind, und ist $-\alpha\beta$ quadratischer Rest von $p$, so kann man eine Zahl $\eta$ finden, so daß $\alpha+\beta\eta^2$ durch $p$, aber nicht durch $p^2$ aufgeht, und jene Form verwandelt sich durch die Substitution $\begin{vmatrix} 1 & 0 \\ \eta & 1 \end{vmatrix} \cdot \begin{vmatrix} 1 & 0 \\ 0 & p \end{vmatrix}$ in eine andere Form, deren Determinante genau die Potenz $p^4$ enthält, von der sich aber der quadratische Faktor $p^2$ ablöst, den man durch die Substitution $\begin{vmatrix} p^{-1} & 0 \\ 0 & p^{-1} \end{vmatrix}$ beseitigen kann; es resultiert dann eine Form, deren Determinante überhaupt nicht durch $p$ aufgeht und welche wieder eine Grundform in bezug auf $p$ ist.

Ist aber in jener binären Form $-\alpha\beta$ quadratischer Nichtrest von $p$, so fällt $\alpha+\beta\eta^2 \pmod p$ für alle $\frac{p-1}{2}$ modulo $p$ inkongruenten und von Null verschiedenen Quadrate $\eta^2$ von Null und von $\alpha$ verschieden aus, und muß deshalb für mindestens eines dieser $\eta$ einen anderen quadratischen Charakter in bezug auf $p$ liefern als $\alpha$. Durch die mit dem betreffenden $\eta$ gebildete Substitution $\begin{vmatrix} 1 & 0 \\ \eta & 1 \end{vmatrix}$ wird dann aus $\begin{pmatrix} p\alpha & 0 \\ 0 & p\beta \end{pmatrix} \pmod{p^2}$ eine Grundform in bezug auf $p$, die sich in einen analogen Hauptrest überführen läßt, in welchem aber die anstelle von $\alpha$ tretende Zahl einen anderen quadratischen Charakter in bezug auf $p$ hat als $\alpha$. Aus dieser letzten Bemerkung ersieht man, daß, wenn die Zahl $m$ oben $\geqq 3$ ist, man es immer so einrichten kann, daß unter den letzten $m$ Zahlen $\alpha_h$ sich zwei solche befinden, deren negativ genommenes Produkt quadratischer Rest von $p$ ist, und welche also zu der vorher beschriebenen Reduktion Gelegenheit bieten. Ob dann, wenn $m$ gerade und bereits auf 2 gebracht ist, jene Operation noch einmal anwendbar erscheint, ob also die Primzahl $p$ durch rationale Transformation aus der Determinante ganz herausgeschafft werden kann oder aber die Determinante immer durch $p^2$ teilbar bleiben muß, wird davon abhängen, ob $C_p = 1$ ist oder $= -1$. Man sieht demnach, daß, je nachdem die Determinante von $f$ eine gerade Potenz von $p$ enthält und $C_p = 1$ ist, oder sie eine ungerade Potenz von $p$ enthält, oder eine gerade und $C_p = -1$ ist, man von $f$ zu einer Form $g$ gelangen kann, deren Determinante überhaupt nicht durch $p$ aufgeht, oder den Faktor $p$ enthält, oder den Faktor $p^2$. Für diese Form $g$ existieren dann außer $c_p$ und $C_p$ keine weiteren quadratischen Charaktere in bezug auf die Primzahl $p$. Denn alle derartigen Charaktere müßten sich, wie bereits oben bemerkt wurde, aus den Werten der dieser Form zugehörigen Gaußschen Summen $g(\alpha, p^t)$ erschließen lassen; für diese gilt hier aber bereits von $t = 1$ an (in dem ersten der drei unterschiedenen Fälle sogar von $t = 0$ an) die Formel (1).

Mit der so gewonnenen Form können nun entsprechend den weiteren in ihrer Determinante etwa enthaltenen ungeraden Primzahlen analoge Operationen vorgenommen werden, und Potenzen dieser Primzahlen nach Möglichkeit aus der Determinante entfernt werden. (Bis man dabei zur Betrachtung einer bestimmten Primzahl $p$ gekommen ist, hat man lauter Substitutionen angewandt, deren Determinanten zu dieser Primzahl relativ prim sind, und sind deshalb die auf diese Primzahl bezüglichen Potenzen $p^{\varrho_h - 1}\,(h = 1, 2, \ldots, n)$ von $f$ völlig unberührt geblieben.)

Jetzt betrachte ich das Verhältnis der vorgelegten Form $f$ zur Primzahl 2. Es werde zu $f$ oder zu einer der späteren Formen eine äquivalente Grundform in bezug auf 2 aufgesucht; aus einer solchen entspringt für jeden Modul $2^t$ ein Hauptrest von dem unter (6) angegebenen Typus, welcher aus Formen mit einer Variable und aus binären Formen $2^\varrho \cdot \begin{pmatrix} 2\alpha & \beta \\ \beta & 2\gamma \end{pmatrix}$ mit ungeraden $\beta$ und $\alpha$ zusammengesetzt erscheint. Eine jede dieser binären Formen geht durch die Substitution $\begin{vmatrix} 1 & 0 \\ 0 & 2 \end{vmatrix}$ in eine Grundform in bezug auf 2 über, deren zugehörige Hauptreste sich noch weiter in je zwei Formen mit einer Variable auflösen. Man kann so zu einer Grundform in bezug auf 2 gelangen, welche in bezug auf Moduln $2^t$ Hauptreste ergibt, die in lauter Formen mit einer Variable zerfallen, und von diesen Hauptresten kommt man, ähnlich wie bei ungeraden Primzahlen, zu Formen mit Resten:

$$\alpha_1 \xi_1^{\,2} + \cdots + \alpha_{n-m} \xi_{n-m}^{\,2} + 2(\alpha_{n-m+1} \xi_{n-m+1}^{\,2} + \cdots + \alpha_n \xi_n^{\,2}) \pmod{16},$$

worin alle $\alpha_h$ ungerade sind. Hier erhält die Einheit $C_2$ den Ausdruck

$$(9) \qquad (-1)^{\left[\frac{n}{4}\right] + \left[\frac{n}{2}\right]\left(\left[\frac{n}{2}\right] + \sum \frac{\alpha_h - 1}{2}\right) + \sum \frac{\alpha_h - 1}{2} \frac{\alpha_k - 1}{2}} \left(\frac{2}{\alpha_{n-m+1} \cdots \alpha_n}\right) \cdot \begin{pmatrix} h = 1, 2, \ldots, n \\ k = 1, 2, \ldots, h-1 \end{pmatrix}$$

Um eine möglichst kleine Zahl $m$ zu erzielen, bemerke ich zunächst, daß eine binäre Form $\begin{pmatrix} 2\alpha & 0 \\ 0 & 2\beta \end{pmatrix} \pmod 8$, in welcher $\alpha$ und $\beta$ ungerade und $\alpha \equiv \beta \pmod 4$ ist, durch die Substitution $\begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} \cdot \begin{vmatrix} 1 & 0 \\ 0 & 2 \end{vmatrix}$ in eine Form mit dem quadratischen Faktor 4 übergeht; entfernt man diesen durch die Substitution $\begin{vmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{vmatrix}$, so bleibt eine Grundform in bezug auf 2 mit ungerader Determinante übrig, die gleichfalls zu zerfallenden Haupt-

resten, aber mit ungeraden Koeffizienten in der Diagonale Veranlassung gibt. Diese Reduktion ist immer möglich, wenn $m \geqq 3$ ist, weil dann unter den $m$ letzten Zahlen $\alpha_h$ sich immer mindestens zwei modulo 4 kongruente finden müssen. Ist man so in den Fällen $n \geqq 3$ und, wenn $m$ gerade ist, bis zu einem $m = 2$ gelangt, und ist diese Reduktion dann zunächst nicht weiter möglich, so kann man aus dem Hauptreste, den man gerade vor sich hat, gewiß einen Teilrest $\begin{pmatrix} \alpha & 0 \\ 0 & 2\beta \end{pmatrix}$ (mod 16) mit ungeraden Zahlen $\alpha$ und $\beta$ herausnehmen, und ein solcher geht durch die Substitution $\begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix}$ in eine Grundform über, welche Hauptreste ergibt, die anstelle der Zahl $\beta$ ungerade Zahlen von anderem quadratischen Charakter in bezug auf 4 als $\beta$ enthalten, wodurch die beschriebene Reduktion noch einmal anwendbar wird. So kann man in den Fällen $n \geqq 3$ von $f$ stets zu einer Form $g$ gelangen, deren Determinante entweder ungerade ist oder den Faktor 2 höchstens einmal enthält, und zwar zu einer solchen Form, welche auch ungerade Zahlen darstellt.

Im Falle $n = 2$ würde die hier benutzte Methode zur Verringerung der Zahl $m$ ihren Dienst bei einem Reste $\begin{pmatrix} 2\alpha & 0 \\ 0 & 2\beta \end{pmatrix}$ (mod 16) versagen, für welchen $-\alpha\beta \equiv 1 \pmod 4$ ist. Ist dann $-\alpha\beta \equiv 1 \pmod 8$, so kann man eine Zahl $\eta$ finden, so daß $\alpha + \beta\eta^2$ durch 8, aber nicht durch 16 aufgeht, und dieser Rest geht durch die Substitution $\begin{vmatrix} 1 & 0 \\ \eta & 1 \end{vmatrix} \cdot \begin{vmatrix} 1 & 0 \\ 0 & 8 \end{vmatrix}$ in einen Rest über, von welchem sich der quadratische Faktor 16 rational abtrennen läßt, so daß eine Form $g$ übrig bleibt, die in einen Hauptrest mit einer Zahl $m = 0$ überzuführen ist. *In diesem Falle, also wenn* $-A \equiv 1 \pmod 8$, *ist daher immer* $C_2 = 1$.

Hat man aber $-A \equiv 5 \pmod 8$, so sind die Fälle $m = 0$ und $m = 2$ wesentlich verschieden, und der erste ist mit $C_2 = 1$, der zweite mit $C_2 = -1$ verbunden. Auch der im zweiten Falle sich ergebende Rest $\begin{pmatrix} 2\alpha & 0 \\ 0 & 2\beta \end{pmatrix}$ (mod 16), $-\alpha\beta \equiv 5 \pmod 8$ kann in eine Form $g$ mit ungerader Determinante transformiert werden, nämlich durch die Substitution $\begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} \cdot \begin{vmatrix} 1 & 0 \\ 0 & 2 \end{vmatrix}$ und nachherige Abtrennung des Faktors 4; diese Form ist dann aber notwendig von der zweiten Art (sie stellt nur gerade Zahlen dar).

Die Formen $g$, auf welche man so in jedem Falle kommt, deren Determinanten nicht durch 4 aufgehen, besitzen außer den Einheiten $c$, $c_2$

und $C_2$ keine weiteren Charaktere in bezug auf die Primzahl 2, wie aus dem Umstande zu entnehmen ist, daß für sie die Gaußschen Summen $g(\alpha, 2^t)$, soweit dieselben für ein $t > 0$ sich noch nicht der Formel (2) anpassen, einfach Null sind.

Fassen wir alle diese Resultate zusammen, so ist in der Tat gezeigt, daß jede vorgelegte Form $f$ rational in eine Form eines durch ihre Zahlen $A$ und $B$ völlig bestimmten Geschlechts von der zu diesen Zahlen gehörigen Determinante $A\mathsf{BB}$ ($\mathsf{B}$ bedeutet den Quotienten aus $B$ und dem größten Divisor von $A$ und $B$) transformiert werden kann, und zwar, mit Ausnahme des Falles $n = 2$, $-A \equiv 5 \pmod 8$, $C_2 = -1$, in eine Form der ersten Art.

Wenn $n > 2$ ist, kann unter Umständen noch ein zweites Geschlecht von der Determinante $A\mathsf{BB}$ und mit denselben Invarianten $I$, $A$, $B$ vorhanden sein, nämlich wenn diese Determinante und diese Invarianten ganzzahligen, uneigentlich primitiven Formen angehören können; die Hauptreste dieses Geschlechts in bezug auf Moduln $2^t$ müßten dann aus lauter Formen $\begin{pmatrix} 2\alpha & \beta \\ \beta & 2\gamma \end{pmatrix}$ mit ungeraden $\alpha$ und $\beta$ und eventuell noch einer Form $2\alpha\xi^2$ mit ungeradem $\alpha$ zusammengesetzt sein, was zu den Bedingungen $n \equiv 0$, $A \equiv 1 \pmod 2$, $c = 1$, $c_2 = C_2$ oder $n \equiv 1$, $A \equiv 0 \pmod 2$, $c_2 = C_2$ führen würde. Haben diese Beziehungen statt, so existiert jenes zweite Geschlecht wirklich, und wählt man dann, was für $n > 2$ immer möglich ist, einen jener Hauptreste so, daß die Zahl $\gamma$ in irgendeinem seiner binären Teilreste durch 2, aber nicht durch 4 aufgeht, so kommt man durch eine mit den Variablen dieses Teilrestes vorgenommene Transformation $\begin{vmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{vmatrix}$ auf eine Form des ersten, eigentlich primitiven Geschlechts zurück.

# ZUR GEOMETRIE DER ZAHLEN

VIII.

# Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen.

(Crelles Journal für die reine und angewandte Mathematik, Band 107, S. 278—297.)

Die wesentlich positiven quadratischen Formen verdienen und gestatten eine besondere Behandlung durch den Umstand, daß sie die einfachsten Formen sind, bei welchen durch den Wert der Form zugleich die Werte sämtlicher Veränderlichen begrenzt sind. Aus diesem Grunde erscheinen sie als ein naturgemäßes Hilfsmittel für die Untersuchung von Reihen diskreter Größen, und in diesem Sinne sind sie namentlich von Herrn Hermite zu wiederholten Malen mit bedeutendem Erfolge verwendet worden.

Wenn ihren Koeffizienten auch ganz beliebige reelle Werte, nicht durchaus rationale beigelegt werden, so stellen sie doch immer geeignete Formen für Zahlen vor, d. h. es hat einen Sinn, die Unbestimmten in ihnen auf die Reihe der ganzen Zahlen zu beschränken. Bei einer solchen Auffassung können diese Formen im speziellen als der analytische Ausdruck gewisser einfacher geometrischer Gebilde gelten, der parallelepipedisch angeordneten regelmäßigen Punktsysteme, und es müssen irgend zwei Formen als äquivalent betrachtet werden, welche auseinander durch lineare Substitutionen mit ganzzahligen Koeffizienten und von einer Determinante $\pm 1$ hervorgehen.

Nun entsteht die Aufgabe, eine Vereinigung äquivalenter Formen, eine Klasse, vollständig durch Invarianten zu charakterisieren. Erst für binäre Formen hat durch die Untersuchungen von Herrn Kronecker diese Aufgabe insofern eine vollkommene Lösung gefunden, als hier in hinreichender Anzahl invariante Bildungen als explizite Funktionen eines beliebigen Elements der Klasse und in einer Gestalt, welche die Invarianteneigenschaft unmittelbar in Evidenz treten läßt, gewonnen sind Ähnliche Aufschlüsse hinsichtlich der Formen mit höherer Variablenzahl mögen aus den jüngsten Arbeiten dieses Forschers zu erwarten sein.

Indes ist die genannte Aufgabe einer Lösung noch in einem anderen

Sinne fähig. Gelingt es, aus den unendlich vielen Formen einer Klasse durch bestimmte Bedingungen eine einzige auszusondern, so stellt eine solche sogenannte reduzierte Form gewissermaßen ebenfalls ein vollständiges Invariantensystem der Klasse vor, nur daß der Ausdruck dieses Systems von irgendeiner gegebenen Form der Klasse auch jedesmal erst durch ein gewisses besonderes Verfahren (das dafür aber nur arithmetische Operationen in beschränkter Zahl erfordern darf) hergeleitet werden kann.

In solcher Art hat Lagrange*) die Theorie der binären quadratischen Formen in Angriff genommen und zu einem glänzenden Abschlusse gebracht. Seine Resultate über die definiten Formen erhielten durch Legendre**) eine Fassung, welche wohl auf ihre Verallgemeinerungsfähigkeit hinweisen konnte.

Aus der fünften Sektion der „Disquisitiones arithmeticae" entnahm Seeber***) die Anregung zu einem Studium der analogen Fragen betreffs der ternären definiten Formen. Seine äußerst mühsame und nicht erfolglose Arbeit fand eine angemessene Würdigung in einer von Gauß†) herrührenden, höchst bemerkenswerten Anzeige. Namentlich durch zweierlei ist diese Anzeige ausgezeichnet: einmal durch den Hinweis auf das von uns schon erwähnte geometrische Äquivalent einer Klasse von positiven quadratischen Formen, dann durch eine eigentümliche Identität, mittels deren eine wichtige, von Seeber nur durch Induktion gefundene Grenze für die Koeffizienten seiner reduzierten Formen direkt in Erscheinung tritt.

Die beschwerliche Methode und die verwickelten Beweise von Seeber veranlaßten Dirichlet††), für den das nicht Einfache überall nur ein Zeichen des Unvollkommenen war, zu einer von Grund aus neuen Behandlung, bei welcher er besonders auch durch die von Gauß nur mehr in ihren Umrissen angedeutete geometrische Einkleidung eine außerordentliche Durchsichtigkeit erzielte. Der große Fortschritt von Dirichlet bestand darin, daß er nicht mit dem schwerfälligen rechnerischen Ausdrucke der Ungleichungen operierte, durch welche Seeber reduzierte Formen definiert hatte, sondern mit deren wohlerkannter innerer Bedeutung, welche darauf hinausging, die reduzierte Form von gewissen in dem zu-

---

*) Recherches d'Arithmétique. Mémoires de l'Académie de Berlin, 1773, p. 265. (Oeuvres, T. III, p. 695.)

**) Théorie des Nombres, 3me éd., T. I § VIII.

***) Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen, Freiburg i. B., 1831.

†) Göttingische gelehrte Anzeigen, Jahrg. 1831, 2. S. 1065 (auch Crelles Journal, Bd. 20, S. 312 und Werke, Bd. II, S. 188).

††) Ueber die Reduction der positiven quadratischen Formen mit drei unbestimmten ganzen Zahlen, Crelles Journal, Bd. 40, 1850, S. 209. (Werke, Bd. II, S. 21.)

gehörigen Punktsysteme vorkommenden kleinsten Entfernungen abhängig zu machen.

Dasselbe ebenso einfache wie sachgemäße Prinzip, doch in rein arithmetischer Fassung, befolgte Herr Hermite*) in seinen zahlentheoretischen Briefen an Jacobi, welche in demselben Bande von Crelles Journal gedruckt sind, in dem die ausführlichere Darstellung Dirichlets nach einem bereits vorher im Monatsbericht der Akademie (Jahrg. 1848) gegebenen Auszuge erschien. Die Untersuchungen von Herrn Hermite beziehen sich auf Formen mit beliebiger Variablenzahl; sie beginnen mit der Aufstellung des Fundamentalsatzes der Reduktion, wonach die kleinste, durch eine positive quadratische Form von $n$ Variablen mittels ganzer Zahlen darstellbare, von Null verschiedene Größe in ihrem dimensionslosen Verhältnis zur $n^{\text{ten}}$ Wurzel aus der Determinante der Form niemals einen gewissen, nur von der Zahl $n$ abhängigen Betrag übersteigt; und sie stellen sich in ihrem Verlaufe als ein ununterbrochenes Zeugnis für die Fruchtbarkeit dieses Satzes in fast jedem Abschnitte der Zahlenlehre dar; es seien nur die Anwendungen auf Kettenbrüche, komplexe Einheiten und approximative Auflösung von Gleichungen hervorgehoben.

Insbesondere ergibt sich aus jenem Satze mit Leichtigkeit und noch auf mannigfache Weise die Endlichkeit der Klassenanzahl bei Beschränkung auf ganzzahlige Werte der Koeffizienten und einen festen ganzzahligen Wert der Determinante. Für diese spezielle Folgerung mußte offenbar bereits ein Verfahren genügen, um aus jeder Klasse überhaupt nur eine endliche Anzahl von Formen, nicht gerade eine einzige auszusondern. Eine wertvolle Ergänzung lieferte deshalb Herr Camille Jordan**) durch den Nachweis, daß bei gewissen Festsetzungen wenigstens eine bloß von der Variablenzahl abhängige Grenze für die Anzahl der im Maximum aus einer Klasse ausgesonderten Formen besteht, indem überhaupt die Substitutionen, durch welche die ausgesonderten Formen ineinander bei Äquivalenz oder in sich selbst übergehen könnten, von vornherein mit der Variablenzahl und zwar in beschränkter Anzahl angewiesen erscheinen.

Neue Gesichtspunkte eröffneten Korkine und Zolotareff***), indem sie jene besonderen Formen heranzogen und bis zur Variablenzahl fünf vollständig bestimmten, für welche das in dem Fundamentalsatze von Hermite genannte Verhältnis (des durch ganze Zahlen erreichbaren Minimum zur $n^{\text{ten}}$ Wurzel aus der Determinante) ein Maximum ist.

---

*) Crelles Journal, Bd. 40, 1850, S. 261—315. (Oeuvres, T. I, pp. 100—163.)

**) Mémoire sur l'équivalence des formes. Journal de l'École Polytechnique T. XXIX, Cah. 48, 1880, p. 111.

***) Mathematische Annalen, Bd. 6, 1873, S. 366 und Bd. 11, 1877, S. 242.

In dem vorliegenden Aufsatze versuche ich hauptsächlich, gewisse Lücken auszufüllen, welche sich in der Theorie der positiven quadratischen Formen gegenwärtig noch fühlbar machen. So geht bei den bisher eingeführten reduzierten Formen mit höheren Variablenanzahlen der den ursprünglichen binären reduzierten Formen von Lagrange innewohnende Charakter verloren, durch eine Reihe von linearen Ungleichungen in den Koeffizienten definiert zu sein. Es erscheint mir aber theoretisch als eine Tatsache von ganz hervorragender Bedeutung, daß man imstande ist, aus der $\frac{1}{2}n(n+1)$-fachen Mannigfaltigkeit, in welcher eine jede quadratische Form von $n$ Variablen durch einen Punkt, unter Zugrundelegung der Werte der Koeffizienten als Koordinaten, repräsentiert wird, aus dieser Mannigfaltigkeit mit Hilfe einer beschränkten Anzahl von lauter ebenen $\left(\frac{1}{2}n(n+1)-1\right)$-fachen Mannigfaltigkeiten ein zusammenhängendes Gebiet abzugrenzen, in welchem — die Grenzen sind nur teilweise mit einzurechnen — jeder Punkt je eine Klasse von positiven Formen vertritt, und jede solche Klasse auch einmal und nur einmal vertreten ist.

Ein solches Gebiet wird durch die $\left(\frac{1}{2}n(n+1)-1\right)$-fache Mannigfaltigkeit aller Formen von einer festen positiven, im übrigen beliebigen Determinante in zwei Teile geschieden, von denen der am Nullpunkt befindliche einen endlichen Inhalt hat. Der Ausdruck dieses Inhalts wird hier allgemein mitgeteilt. Es steht dieser Inhalt mit interessanten mittleren Werten der Zahlentheorie im Zusammenhang.

Die Überführung irgendeiner gegebenen Form in eine reduzierte muß durch ausschließliche Verwendung einer beschränkten Zahl a priori anzuweisender Operationen geleistet werden können, und die Ausgangsform darf jedesmal nur in bezug auf Reihenfolge und Wiederholung der Operationen maßgebend sein; dieser berechtigten Forderung wird hier genügt werden.

Mit Hilfe einer auch auf Formen mit mehr als drei Veränderlichen übertragenen geometrischen Ausdrucksweise gelingt es, den Fundamentalsatz von Hermite über das Minimum einer positiven quadratischen Form nicht allein als in gewissem Sinne evident hinzustellen, sondern auch die in diesem Satze und in Erweiterungen desselben benötigten Grenzen den bisher angezeigten gegenüber beträchtlich zu verengern. Dadurch werden dann neue, folgenreiche Anwendungen dieses Satzes möglich. —

## 1. Die Grundeigenschaft der wesentlich positiven quadratischen Formen.

*Eine wesentlich positive quadratische Form kann nur für eine endliche Anzahl von ganzzahligen Wertsystemen ihrer Veränderlichen Werte annehmen, die eine gegebene Größe nicht überschreiten.*

Denn eine solche Form $f$ mit $n$ Variablen $x_1, x_2, \ldots, x_n$ ist bekanntlich immer als Summe der Quadrate von $n$ unabhängigen reellen Linearformen ihrer Variablen darstellbar:

$$f = \xi_1^2 + \xi_2^2 + \cdots + \xi_n^2,$$

$$(1\,a) \quad \xi_a = \pi_{a1}x_1 + \pi_{a2}x_2 + \cdots + \pi_{an}x_n, \quad |\pi_{ab}| \neq 0. \quad (a, b = 1, 2, \ldots, n)$$

Eine Ungleichung $f \leqq G$ mit positivem $G$ hat nun für jede der Linearformen abs. $\xi_a \leqq \sqrt{G}$ zur Folge. Lautet die Auflösung dieser Formen nach ihren Variablen:

$$(1\,b) \qquad x_b = \varphi_{1b}\xi_1 + \varphi_{2b}\xi_2 + \cdots + \varphi_{nb}\xi_n, \qquad (b = 1, 2, \ldots, n)$$

so muß daher

$$\text{abs. } x_b \leqq \sqrt{G}\,(\text{abs. } \varphi_{1b} + \text{abs. } \varphi_{2b} + \cdots + \text{abs. } \varphi_{nb}) \quad (b = 1, 2, \ldots, n)$$

sein. Diesem Systeme von Ungleichungen können aber nur eine endliche Anzahl von ganzzahligen Systemen $x_1, x_2, \ldots, x_n$ entsprechen. Natürlich brauchen diese dann nicht sämtlich ein $f(x_1, x_2, \ldots, x_n) \leqq G$ zu ergeben.

## 2. Die geometrische Interpretation der wesentlich positiven quadratischen Formen.

In einer ebenen $n$-fachen Mannigfaltigkeit mögen die Werte der Linearformen $\xi_1, \xi_2, \ldots, \xi_n$ solche Koordinaten für einen veränderlichen Punkt $P$ abgeben, daß das Quadrat des von $P$ ausgehenden Linearelements durch die Summe der Quadrate der Differentiale $d\xi_1, d\xi_2, \ldots, d\xi_n$ ausgedrückt erscheint. Der Nullpunkt der so vorausgesetzten rechtwinkligen Koordinaten heiße $O$. Jedem Wertsysteme der Variablen $x_1, x_2, \ldots, x_n$ entspricht gemäß (1a) ein Wertsystem $\xi_1, \xi_2, \ldots, \xi_n$ und kommt jetzt ein Punkt $P$ zu; die Form $f(x_1, x_2, \ldots, x_n)$ stellt offenbar das Quadrat der Entfernung dieses Punktes $P$ von dem festen Nullpunkte $O$ dar.

Welche Punkte gehören nun den ganzzahligen Systemen $x_1, x_2, \ldots, x_n$ an? Um diese Punkte zu finden, hat man zuvörderst diejenigen $n$ Punkte $P_1, P_2, \ldots, P_n$ kenntlich zu machen, für welche jedesmal eine der $n$ Größen $x_1, x_2, \ldots, x_n$ den Wert 1 und die anderen $n - 1$ den Wert Null haben. Liegen diese $n$ Punkte vom Nullpunkte $O$ beziehlich um die Strecken $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ ab, so wird der Punkt, welcher einem willkürlich gewählten Systeme $x_1, x_2, \ldots, x_n$ angehört, gefunden, indem man vom Nullpunkte aus die Strecke

$$\mathfrak{p}_1 x_1 + \mathfrak{p}_2 x_2 + \cdots + \mathfrak{p}_n x_n$$

konstruiert, wobei die Additionen in geometrischem Sinne zu verstehen sind.

Hiernach würde man folgendermaßen zu den sämtlichen Punkten mit ganzzahligen Bestimmungsstücken $x_1, x_2 \ldots, x_n$ gelangen können: Man stelle in die am Punkte $O$ von den dort ausgehenden $n$ Strecken $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$

gebildete $n$-kantige Ecke — das Vorhandensein einer solchen wirklichen Ecke ist die Folge der Unabhängigkeit der Gleichungen (1a) — ein mit diesen $n$ Strecken als Kanten konstruiertes $n$-dimensionales Parallelepipedum. Von den $2n$ $(n-1)$-dimensionalen Begrenzungsebenen dieses Parallelepipedum wollen wir die $n$ durch den Punkt $O$ nicht hindurchgehenden in ihrer ganzen Ausdehnung, d. h. mit allen ihren Grenzlinien verschiedener Dimensionen, also im besonderen mit allen übrigen Eckpunkten, als nicht mehr zu dem *Bereiche* des Parallelepipedum gehörig betrachten; in ähnlichem Sinne wollen wir uns auch künftighin den Bereich jedes irgend einmal vorkommenden Parallelepipedum festgesetzt denken. An jede der $2n$ Begrenzungsflächen dieses Grundparallelepipedum lege man gleichgerichtet ein vollkommen gleiches Parallelepipedum, an die noch freien Begrenzungsflächen dieser Parallelepipeda wieder ein gleiches, und dieses Verfahren denke man sich unbegrenzt fortgesetzt. Dann finden sich die gesuchten Punkte in den einzelnen Hauptecken dieser nacheinander konstruierten Parallelepipeda.

Das vollständige System dieser Punkte mit ganzzahligen Bestimmungsstücken $x_1, x_2, \ldots, x_n$ ist um jeden einzelnen seiner Punkte in gleicher Weise gelagert. Wir nennen es deshalb ein *regelmäßiges Punktsystem*. Wir werden ein solches System mitunter einfach mit dem Buchstaben $\mathfrak{P}$ ohne weiteren Zusatz, oder wenn die Dimension des Systems kenntlich gemacht werden soll, mit $\mathfrak{P}^{(n)}$ bezeichnen. Ein System $\mathfrak{P}$ besetzt nach irgendeiner Parallelverschiebung entweder vollständig neue Punkte oder tritt wieder ganz in die anfänglichen Lagen seiner Punkte ein.

Da die zu konstruierenden Parallelepipeda den ganzen vorausgesetzten $n$-dimensionalen Raum lückenlos erfüllen werden, und da sie überdies nach den Punkten des Systems zählbar, d. h. ihnen eindeutig zugeordnet sind — nach unseren Festsetzungen über den Bereich dieser Parallelepipeda ist ein jeder Punkt des Raumes einem und nur einem der Parallelepipeda zuzuteilen —, so wird innerhalb eines, überallhin gleichmäßig ins Unendliche ausgedehnten Gebiets (man denke beispielsweise an einen $n$-dimensionalen Würfel mit unendlich großer Kante) im Durchschnitt ein Punkt des Systems auf einen Raumteil gleich dem Volumen des Grundparallelepipedum kommen. In der Maßzahl dieses Volumens erkennen wir hiernach eine für das Punktsystem an sich charakteristische und von der Wahl des Gerüsts, durch welches wir die Punkte verbunden haben, völlig unabhängige Konstante; und den reziproken Wert dieser Maßzahl werden wir passend als die *mittlere Dichtigkeit des Punktsystems* bezeichnen können.

Zu jedem Punktsysteme gibt es offenbar ein geometrisch ähnliches Punktsystem von der mittleren Dichtigkeit 1.

### 3. Erneuter Beweis der Grundeigenschaft.

Die in 1. bewiesene Grundeigenschaft der wesentlich positiven quadratischen Formen läßt sich nun auch leicht geometrisch einsehen.

Die gesamten Begrenzungsflächen der vorhin konstruiert gedachten Parallelepipeda sind enthalten in $n$ verschiedenen Scharen von lauter parallelen und äquidistanten $(n-1)$-dimensionalen Ebenen, als deren Durchschnitte eben die Punkte unseres Systems sich ergeben. Die Distanzen in den einzelnen Scharen werden durch die $n$ Höhen des Grundparallelepipedum geliefert; die Längen dieser Höhen mögen $h_1, h_2, \ldots, h_n$ heißen.

In jeder einzelnen Schar sind die Elemente nach einer bestimmten der $n$ Zahlen $x_1, x_2, \ldots, x_n$ zu numerieren. Im Nullpunkte $O$ kreuzen sich die Nullelemente aller Scharen; in einem Punkte $P$ mit ganzzahligen Bestimmungsstücken $x_1, x_2, \ldots, x_n$ das $x_1^{\text{te}}$ Element der ersten, das $x_2^{\text{te}}$ der zweiten, ..., das $x_n^{\text{te}}$ der $n^{\text{ten}}$ Schar. Nun kann der Abstand $OP$ nicht kleiner sein als der senkrechte Abstand zweier durch $O$ und $P$ gehenden $(n-1)$-dimensionalen Parallelebenen. Soll also der Abstand $OP$ eine gegebene Länge $\sqrt{G}$ nicht überschreiten, d. h. soll:

$$f(x_1, x_2, \ldots, x_n) \leqq G$$

sein, so müssen um so mehr die Ungleichungen statthaben:

$$h_a \operatorname{abs}. x_a \leqq \sqrt{G}, \qquad (a = 1, 2, \ldots, n) \tag{3}$$

und diesen kann wieder nur eine beschränkte Anzahl von ganzen Zahlen genügen.

### 4. Positive quadratische Form und Parallelepipedum.

Die mit Ausnahme des Falles $n = 1$ immer vorhandene Willkür in der Darstellung einer positiven quadratischen Form $f$ als Summe von $n$ Quadraten linearer Formen betrifft geometrisch nur die Neigung der Elementarparallelepipeda gegen die rechtwinkligen Koordinatenachsen, auf welchen die linearen Formen ihre Auslegung finden: es sind nämlich die Projektionen der Strecken $\mathfrak{p}_b$ auf die Achsen der $\xi_1, \xi_2, \ldots, \xi_n$ genau die Koeffizienten $\pi_{1b}, \pi_{2b}, \ldots, \pi_{nb}$ der zugehörigen Variablen $x_b$ in den linearen Formen $\xi_1, \xi_2, \ldots, \xi_n$.

Die Figur des Elementarparallelepipedum, ohne Rücksicht auf ihre Stellung im vorausgesetzten $n$-dimensionalen Raume, aber mit Kennzeichnung ihrer Ursprungsecke und der Reihenfolge der Kanten an dieser Ecke, bestimmt eindeutig den Ausdruck der Form $f$ in ihren Koeffizienten. Soll dieser:

$$f = \sum q_{ab} x_a x_b \qquad \begin{pmatrix} a, b = 1, 2, \ldots, n \\ q_{ab} = q_{ba}, a \neq b \end{pmatrix} \tag{4}$$

lauten, so bedeutet jedesmal ein Koeffizient $q_{aa}$ mit gleichen Indizes das Quadrat der Länge der Strecke $\mathfrak{p}_a$, und ein Koeffizient $q_{ab}$ mit verschiedenen Indizes das Produkt aus den Längen der Strecken $\mathfrak{p}_a$ und $\mathfrak{p}_b$ und dem Kosinus des Neigungswinkels dieser Strecken. Ferner bedeuten: 1. die Determinante der Form, $|q_{ab}| = \Delta$, das Quadrat des Inhalts des Parallelepipedum, 2. die symmetrischen Unterdeterminanten $\frac{\partial \Delta}{\partial q_{aa}}$ die Quadrate der Inhalte seiner paarweise einander gleichen Begrenzungsebenen, so daß für die $n$ Höhen des Parallelepipedum die Ausdrücke resultieren:

$$h_a = \sqrt{\frac{\Delta}{\frac{\partial \Delta}{\partial q_{aa}}}}. \qquad (a = 1, 2, \ldots, n)$$

Alle diese Beziehungen sind am einfachsten durch ein Zurückgehen auf das rechtwinklige Koordinatensystem der $\xi_1, \xi_2, \ldots, \xi_n$ einzusehen, werden übrigens sofort noch klarer hervortreten.

Umgekehrt gehören dagegen zur gegebenen wesentlich positiven Form $f$ (Formel (4)) in dem gleichen Raume von $n$ Dimensionen immer zwei verschiedene Arten von $n$-kantigen begrenzten Ecken, und dementsprechende Parallelepipeda. Denn zunächst haben wir jedenfalls in 2. eine solche Art gefunden, und zwar auf Grund irgendeiner Darstellung von $f$ als Summe der Quadrate von $n$ linearen Formen. Um das dabei angewandte Verfahren beschreiben zu können, ohne auf die Bedeutung der $\xi$-Koordinaten wieder eingehen zu müssen, wollen wir uns auf den positiven Seiten der rechtwinkligen Koordinatenachsen der $\xi_1, \xi_2, \ldots, \xi_n$ die $n$ Punkte $E_1, E_2, \ldots, E_n$ markiert denken, welche in der Einheit der Entfernung von $O$ abliegen, und die geometrischen Strecken nach diesen Punkten mit $\mathfrak{e}_1, \mathfrak{e}_2, \ldots, \mathfrak{e}_n$ bezeichnen. Dann entsteht die erste, zur Form $f$ gehörige Ecke $O(P_1 P_2 \ldots, P_n)$ aus 2. einfach, indem in $O$ die Strecken:

$$\mathfrak{p}_b = \pi_{1b}\mathfrak{e}_1 + \pi_{2b}\mathfrak{e}_2 + \cdots + \pi_{nb}\mathfrak{e}_n \qquad (b = 1, 2, \ldots, n) \tag{4a}$$

angefügt werden. Der günstige Erfolg dieser Operation läßt sich am besten mit Hilfe einer von Graßmann eingeführten Symbolik übersehen: Das Produkt aus den Längen zweier Strecken $\mathfrak{l}$ und $\mathfrak{m}$ und dem Kosinus ihres Neigungswinkels mag das *innere Produkt* dieser Strecken heißen und $\mathfrak{l}|\mathfrak{m}$ geschrieben werden. Offenbar gilt für diese Art von Multiplikation neben den Regeln $\mathfrak{e}_a|\mathfrak{e}_a = 1$, $\mathfrak{e}_a|\mathfrak{e}_b = 0$ $(a \neq b)$ das distributive Gesetz, und daraus geht sofort $\mathfrak{p}_a|\mathfrak{p}_b = q_{ab}$ hervor. Andererseits aber folgt allein aus den Beziehungen $\mathfrak{p}_a|\mathfrak{p}_b = q_{ab}$, sowie man mit Hilfe der aus (1b) entnommenen Koeffizienten $n$ Strecken:

$$\mathfrak{e}_a = \varphi_{a1}\mathfrak{p}_1 + \varphi_{a2}\mathfrak{p}_2 + \cdots + \varphi_{an}\mathfrak{p}_n \qquad (a = 1, 2, \ldots, n) \tag{4b}$$

bildet, mit Notwendigkeit: $\mathfrak{e}_a|\mathfrak{e}_a = 1$, $\mathfrak{e}_a|\mathfrak{e}_b = 0 (a \neq b)$, und also jedesmal eine rechtwinklige Ecke mit $n$ Kanten gleich der Längeneinheit.

Von solchen rechtwinkligen Ecken gibt es nun in einem Raume von $n$ Dimensionen (genau so wie im speziellen Falle $n = 3$) immer zwei Arten, die innerhalb dieses Raumes nicht in allen ihren entsprechenden Kanten zugleich zur Deckung zu bringen sind. Eine Art können wir als durch die Ecke $O(E_1 E_2 \ldots E_n)$ der Koordinatenachsen definiert betrachten. Dann entsteht die zweite Art durch Spiegelung dieser Ecke an irgendeiner $(n-1)$-dimensionalen Ebene, und durch die nämliche Spiegelung muß aus der zuerst gefundenen Ecke $O(P_1 P_2 \ldots P_n)$ eine zweite zu $f$ gehörige Ecke hervorgehen. Der Spiegelung an einer Ebene:

$$\varphi_1 \xi_1 + \varphi_2 \xi_2 + \cdots + \varphi_n \xi_n = 0$$

entspricht die Umwandlung der Koeffizienten $\pi_{ab}$ in:

$$\pi_{ab} - 2\left(\frac{\pi_{1b}\varphi_1 + \pi_{2b}\varphi_2 + \cdots + \pi_{nb}\varphi_n}{\varphi_1^{\,2} + \varphi_2^{\,2} + \cdots + \varphi_n^{\,2}}\right)\varphi_a. \quad (a, b = 1, 2, \ldots, n)$$

Man überzeugt sich leicht, daß dabei die Quadratsumme der linearen Formen $\xi_1, \xi_2, \ldots, \xi_n$ den Ausdruck $f$ ungeändert beibehält, die Determinante $|\pi_{ab}|$ hingegen in den entgegengesetzten Wert übergeht, was eben das Zeichen dafür ist, daß in der Tat eine Ecke neuer Art gewonnen ist.

Überhaupt können wir nämlich in $n$ Dimensionen zwei Arten von $n$-kantigen wirklichen Ecken unterscheiden, in diesem Sinne: $n$-kantige Ecken gleicher Art sind durch kontinuierliche Abänderungen, ohne daß sie aufhören, wirkliche Ecken zu bleiben, zum Zusammenfallen in allen ihren entsprechenden Kanten zu bringen; bei $n$-kantigen Ecken ungleicher Art ist solches nicht möglich. Daß $n$ Strecken $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ eine *wirkliche* Ecke bilden, heißt soviel, wie daß sie auf ein Parallelepipedum von nichtverschwindendem $n$-dimensionalem Inhalte führen. Den fraglichen Inhalt können wir als eine Art von Produkt auffassen und $\mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_n$ schreiben. Wir haben es alsdann mit der sogenannten *äußeren Multiplikation* von Strecken zu tun (es ist das wieder eine Bezeichnung von Graßmann), für welche neben dem distributiven und dem assoziativen Gesetze offenbar die Regel gilt, daß das Produkt einer Strecke in sich selbst Null ist, woraus für zwei Strecken $\mathfrak{l}$ und $\mathfrak{m}$ durch Betrachtung von $(\mathfrak{l} + \mathfrak{m})(\mathfrak{l} + \mathfrak{m})$ sich $\mathfrak{l}\mathfrak{m} = -\mathfrak{m}\mathfrak{l}$ ergibt; und mit Hilfe dieser Regeln folgt aus (4a): $\mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_n = |\pi_{ab}| \mathfrak{e}_1 \mathfrak{e}_2 \ldots \mathfrak{e}_n$. Das Nichtverschwinden der Determinante $|\pi_{ab}|$ ist hiernach für die Bildung einer wirklichen Ecke charakteristisch, und nach dem Vorzeichen dieser Determinante richtet sich dann, wie man leicht einsieht, die Art der Ecke.

In dem aus einer Ecke $(\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n)$ folgenden Parallelepipedum befindet sich der betreffenden Ecke diametral gegenüber eine Ecke mit den Kanten $-\mathfrak{p}_1, -\mathfrak{p}_2, \ldots, -\mathfrak{p}_n$; diese zweite Ecke gehört offenbar zu derselben quadratischen Form, ergibt aber bei ungeradem $n$ ein entgegen-

gesetztes Kantenprodukt. Bei ungeradem $n$ sind demnach die Parallelepipeda, welche aus zwei zusammengehörigen Ecken ungleicher Art entstehen, im wesentlichen identisch, sie erscheinen nur verschieden aufgefaßt, während bei geradem $n$ eine Deckung solcher zweier Parallelepipeda in der Regel erst innerhalb eines dimensionsreicheren Raumes zu erzielen sein wird. —

Da die quadratische Form $f$ als Ausdruck eines parallelepipedisch geordneten, regelmäßigen Punktsystems in einem gegebenen Raume, wie wir sehen, eine Zweideutigkeit bestehen läßt, so erscheint es vielleicht angebrachter, als solchen Ausdruck die *lineare* Form:

$$\mathfrak{p}_1 x_1 + \mathfrak{p}_2 x_2 + \cdots + \mathfrak{p}_n x_n = \mathfrak{p}$$

zu nehmen. In dieser sind die Koeffizienten allerdings nicht reine Zahlen, sie bedeuten vielmehr Strecken, bestimmt in Richtung und Länge; aber durch ausschließliche Betrachtung dieser Strecken sind keine weiteren Zahlgrößen zu entnehmen, als eben die Koeffizienten von $f$. Das Volumen $\mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_n$ setzen wir immer als von Null verschieden voraus. Nach der vorhin erklärten Ausdrucksweise würde $f$ als das innere Produkt dieser linearen Form $\mathfrak{p}$ in sich selbst, als ihr inneres Quadrat, zu bezeichnen sein.

## 5. Anschauliche Auslegung des Äquivalenzbegriffs.

Ist ein, auf irgendeine Weise in parallelepipedischer Anordnung gegebenes regelmäßiges Punktsystem $\mathfrak{P}^{(n)}$ noch weiterer solcher Anordnungen fähig?

Bei jeder solchen Anordnung müßte jeder Punkt des Systems als Ausgangspunkt einer, in $n$ anderen Punkten des Systems endenden Ecke eines jedesmal gleichen Parallelepipedum erscheinen, in dessen Bereich — wenn die dem Punkte nicht anliegenden Begrenzungsflächen immer vollständig ausgeschlossen werden — kein weiterer Punkt des Systems fallen dürfte. Verbinden wir also zunächst einen beliebigen Punkt $O$ des Systems mit $n$ beliebigen anderen Punkten des Systems, die nur nicht sämtlich mit $O$ zusammen bereits in einer $(n-1)$-dimensionalen Ebene liegen sollen. Die Strecken von $O$ nach diesen $n$ Punkten mögen $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_n$ heißen. Da diese Strecken lauter Punkte des Systems verbinden, so werden sie mit den für die gegebene Anordnung charakteristischen Strecken $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ durch irgendwelche Relationen:

$$\mathfrak{q}_b = s_{1b}\mathfrak{p}_1 + s_{2b}\mathfrak{p}_2 + \cdots + s_{nb}\mathfrak{p}_n \qquad (b = 1, 2, \ldots, n)$$

mit lauter ganzzahligen Koeffizienten $s_{ab}$ verbunden sein, die nur ein nichtverschwindendes Volumen $\mathfrak{q}_1 \mathfrak{q}_2 \ldots \mathfrak{q}_n$ (d. i. eine nichtverschwindende Determinante $|s_{ab}|$) zu ergeben haben; und deshalb wird dann weiter auch

jede beliebige, von $O$ aus konstruierte Strecke $\mathfrak{q}_1 y_1 + \mathfrak{q}_2 y_2 + \cdots + \mathfrak{q}_n y_n = \mathfrak{q}$ mit ganzzahligen Bestimmungsstücken $y_1, y_2, \ldots, y_n$ auf einen Punkt des Systems auslaufen müssen.

Ein von $O$ aus, der eben genannten linearen Form $\mathfrak{q}$ gemäß, in parallelepipedischer Anordnung aufgebautes Punktsystem $\mathfrak{Q}$ wird also ganz in dem vorausgesetzten Punktsysteme $\mathfrak{P}$ enthalten sein. Dieses System $\mathfrak{Q}$ wird mit $\mathfrak{P}$ zusammenfallen, also eine neue parallelepipedische Anordnung von $\mathfrak{P}$ darbieten, wenn die Parallelepipeda von $\mathfrak{Q}$ in ihren Bereichen — dieselben in dem früher festgesetzten Sinne genommen — außer ihrer jedesmaligen Hauptecke keine weiteren Punkte von $\mathfrak{P}$ enthalten. Jedenfalls enthält nun jedes dieser Parallelepipeda gleich viele Punkte aus $\mathfrak{P}$, sagen wir $s$, und an lauter entsprechenden Stellen, da die Parallelverschiebungen, durch welche $\mathfrak{Q}$ mit sich selbst zur Deckung kommt, ja nichts weiter als ein Teil der Deckbewegungen von $\mathfrak{P}$ sind. In 2. sahen wir, daß innerhalb eines unendlich großen $n$-dimensionalen Würfels aus dem Punktsysteme $\mathfrak{P}$ im Durchschnitt ein Punkt auf einen Raumteil gleich dem Volumen $\mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_n$ kommt, und nun sollen offenbar $s$ solcher Punkte im Durchschnitt auf einen Raumteil gleich dem Volumen $\mathfrak{q}_1 \mathfrak{q}_2 \ldots \mathfrak{q}_n = |s_{ab}| \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_n$ kommen. Mithin kann die Zahl $s$ nur den absoluten Wert der Determinante $|s_{ab}|$ vorstellen, und die Bedingung für eine neue parallelepipedische Anordnung des Punktsystems $\mathfrak{P}$ lautet: $|s_{ab}| = \pm 1$. Es ist geometrisch evident, daß bei Erfüllung dieser Bedingung umgekehrt auch $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ als lineare Funktionen von $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_n$ lauter ganzzahlige Koeffizienten werden aufweisen müssen.

Die Form $\mathfrak{q}$ geht aus der Form $\mathfrak{p} = \mathfrak{p}_1 x_1 + \mathfrak{p}_2 x_2 + \cdots + \mathfrak{p}_n x_n$ vermittels der Substitution:

$$x_a = s_{a1} y_1 + s_{a2} y_2 + \cdots + s_{an} y_n \qquad (a = 1, 2, \ldots, n)$$

hervor, und es ist klar, daß durch dieselbe Substitution aus der quadratischen Form $\mathfrak{p}|\mathfrak{p} = f$ eine quadratische Form $g$ entsteht, welche als das innere Quadrat von $\mathfrak{q}$ erscheinen wird. Die Eigenschaften der zugehörigen Punktsysteme machen es verständlich, daß man die, durch eine solche lineare Substitution mit ganzzahligen Koeffizienten aus einer Form $f$ hervorgehende Form $g$ als *enthalten* in der Form $f$ bezeichnet, ebenso, daß man sie der Form $f$ *äquivalent* nennt, wenn die Determinante $|s_{ab}| = \pm 1$ ist. Man spricht von eigentlicher oder uneigentlicher Äquivalenz, je nachdem $|s_{ab}| = 1$ oder $= -1$ ist, je nachdem also die für $f$ und $g$ übereinstimmenden Punktsysteme aus Ecken gleicher oder ungleicher Art herzuleiten sind. Da bei ungeradem $n$ vermöge der Substitution $x_1 = -y_1$, $x_2 = -y_2, \ldots, x_n = -y_n$ jede Form sich selbst auch uneigentlich äquivalent ist, so hat diese letztere Unterscheidung nur bei geradem $n$ einen Wert;

natürlich können auch hier unter Umständen Formen einander eigentlich und uneigentlich äquivalent zu gleicher Zeit sein.

Eine *Klasse* von äquivalenten Formen entspricht nun dem Inbegriff aller möglichen parallelepipedischen Anordnungen eines Punktsystems $\mathfrak{P}$.

## 6. Von dem Minimum einer wesentlich positiven quadratischen Form.

In einem parallelepipedisch geordneten, regelmäßigen Punktsysteme $\mathfrak{P}^{(n)}$ denken wir uns um irgendeinen Punkt $O$ des Systems als Zentrum zwei $n$-dimensionale Kugeln konstruiert; der Radius der einen sei die kleinste der Höhen des Elementarparallelepipedum, der Radius der anderen die kleinste der Längen seiner Kanten. Nach (3) kann in das Innere der ersten Kugel außer $O$ kein weiterer Punkt des Systems fallen; dagegen liegen gewiß zwei solcher Punkte an den Enden eines bestimmten Durchmessers der zweiten, mithin jedenfalls nicht kleineren Kugel. Nach 1. oder 3. können wir alle Punkte bestimmen, welche in der Schicht zwischen den beiden Kugeln, die Begrenzungen mit eingerechnet, sich vorfinden; ihre Anzahl ist nach den dortigen Sätzen eine beschränkte. Unter diesen Punkten werden dann ein oder vielleicht mehrere Paare vorhanden sein, welche dem Punkte $O$ am nächsten liegen. Die Entfernung dieser nächstgelegenen Punkte von $O$ bezeichnen wir mit $\sqrt{M}$; wegen der Regelmäßigkeit des Punktsystems ist dieses dann überhaupt die kleinste Entfernung zweier Punkte, welche im Systeme vorkommt. Zugleich ist $M$ die kleinste, von Null verschiedene Größe, welche durch die, zur gegebenen Anordnung des Systems gehörige quadratische Form $f$ mittels ganzer Zahlen darstellbar ist; wir nennen $M$ das *Minimum* dieser Form $f$. Fast evident erscheint nun die folgende wichtige Eigenschaft:

*Die kleinste Entfernung zweier Punkte in einem regelmäßigen Punktsysteme kann nicht einen gewissen, durch die mittlere Dichtigkeit des Systems bestimmten Betrag übersteigen.*

Denn denken wir uns um jeden Punkt des Systems einen $n$-dimensionalen Würfel von der Kante $\frac{1}{\sqrt{n}}\sqrt{M}$ abgegrenzt, indem wir jedesmal den Punkt als Mittelpunkt des Würfels nehmen — wir können uns etwa alle diese Würfel parallel orientiert vorstellen —, so sind die vom Mittelpunkte am weitesten abliegenden Punkte eines solchen Würfels jedesmal seine Eckpunkte, und die Entfernung dieser vom Mittelpunkte beträgt das $\frac{1}{2}\sqrt{n}$-fache der Kante, also hier $\frac{1}{2}\sqrt{M}$. Wegen der Bedeutung der Länge $\sqrt{M}$ können daher diese Würfel sich niemals durchdringen, sie können höchstens unter Umständen in ihren Eckpunkten zusammentreffen, müssen im übrigen aber außerhalb ihrer Seitenflächen noch einen freien

Raum zwischen sich lassen. Ziehen wir diesen freien Raum in Betracht, so kommt also in einem, überallhin gleichmäßig ins Unendliche ausgedehnten Raume auf einen Raumteil gleich dem Volumen eines der Würfel im Durchschnitt weniger als ein Punkt des Systems. Dieses Volumen muß also nach den Betrachtungen in 2. kleiner sein als das Volumen des Elementarparallelepipedum, d. h. wir haben:

$$\left(\frac{1}{\sqrt{n}}\sqrt{M}\right)^n < \sqrt{\Delta},$$

oder:

$$M < n\sqrt[n]{\Delta}, \tag{6a}$$

womit unsere Behauptung erwiesen ist. In dem sehr einfachen Falle $n = 1$, den wir hier stillschweigend übergangen haben, müßte in diesen Formeln offenbar das Gleichheitszeichen statt $<$ genommen werden.

Wir haben so den folgenreichen Satz von Herrn Hermite über das Minimum einer positiven quadratischen Form in das rechte Licht gesetzt und zugleich in $n\sqrt[n]{\Delta}$ eine sehr viel engere Grenze für dieses Minimum gefunden, als sie, die kleinsten Zahlen $n$ ausgenommen, bisher bekannt ist (s. unten 10.). Wir können aber sofort auch diese Grenze noch einschränken. Konstruieren wir nämlich um jeden Punkt des Systems als Mittelpunkt eine $n$-dimensionale Kugel mit dem Radius $\frac{1}{2}\sqrt{M}$, so müssen auch diese, den vorhin konstruierten Würfeln umschriebenen Kugeln sich gegenseitig vollständig ausschließen und zwischen sich noch einen freien Raum lassen, und es muß also auch das Volumen einer solchen Kugel kleiner sein als das Volumen des Elementarparallelepipedum. Nun beträgt das Volumen einer $n$-dimensionalen Kugel vom Radius 1 bekanntlich:

$$\frac{\left\{\Gamma\left(\frac{1}{2}\right)\right\}^n}{\Gamma\left(1+\frac{n}{2}\right)},$$

d. h. je nachdem $n$ gerade oder ungerade ist:

$$\frac{\pi^{\frac{n}{2}}}{1\cdot 2\cdot 3\cdots\frac{n}{2}} \quad \text{oder} \quad \frac{2^{\frac{n+1}{2}}\,\pi^{\frac{n-1}{2}}}{1\cdot 3\cdot 5\cdots n};$$

also finden wir:

$$\frac{\left\{\Gamma\left(\frac{1}{2}\right)\right\}^n}{\Gamma\left(1+\frac{n}{2}\right)}\left(\frac{1}{2}\sqrt{M}\right)^n < \sqrt{\Delta}. \tag{6b}$$

Durch Benutzung des asymptotischen Ausdrucks der $\Gamma$-Funktion folgt daraus leicht:

$$M < \frac{2n}{\pi e}\sqrt[n]{n\pi e^{\frac{1}{3n}}}\sqrt[n]{\Delta},$$

so daß diese zweite Grenze für das Minimum bei großen Werten von $n$ ungefähr das $\frac{2}{\pi e} = 0{,}234\ldots$-fache der früher gefundenen ausmacht. Später werden wir noch engere Grenzen für das Minimum kennen lernen.

## 7. Anwendung auf die Theorie der algebraischen Zahlen.

Eine der ersten Anwendungen, welche Herr Hermite von der Existenz einer Grenze für das Minimum positiver quadratischer Formen gemacht hat, betraf die Theorie der algebraischen Zahlen. Die großen Fortschritte, welche auf diesem Gebiete seitdem erzielt sind, und andererseits die im vorhergehenden gefundene natürlichere Grenze für das Minimum ermöglichen es uns, diese Anwendung wesentlich zu vertiefen und sie zugleich in vollkommenerer Form zur Darstellung zu bringen.

Es sei $\theta$ eine Wurzel einer irreduktiblen ganzzahligen Gleichung von einem Grade $n$, welcher größer als Eins sei; und es bedeute $\mathfrak{o}$ das System aller ganzen algebraischen Zahlen, welche unter den rationalen Funktionen von $\theta$ mit ganzzahligen Koeffizienten überhaupt zu finden sind. Es sei ferner $\omega_1, \omega_2, \ldots, \omega_n$ irgendeine Reihe von $n$ Zahlen aus $\mathfrak{o}$, für welche das Quadrat der Determinante

$$|\omega_k^{(h)}| \qquad (h, k = 1, 2, \ldots, n)$$

aus den $n$ konjugierten Reihen von Null verschieden und dazu dem absoluten Betrage nach möglichst klein ausfalle, und der dabei eintretende Wert dieses Quadrats, die sogenannte *Diskriminante* von $\mathfrak{o}$, heiße $D$. Das System $\mathfrak{o}$ stimmt dann genau überein mit den Werten der Form

$$\omega_1 x_1 + \omega_2 x_2 + \cdots + \omega_n x_n = \omega$$

für alle möglichen ganzen Zahlen $x_1, x_2, \ldots, x_n$, und diese Werte sind untereinander alle verschieden*). Wenden wir dieselben Zeichen $x_1, x_2, \ldots, x_n$ für die Unbestimmten einer beliebigen, wesentlich positiven Form $f$ mit entsprechender Zahl $n$ an, so kann daher ein, dieser Form $f$ gemäß parallelepipedisch aufgebautes regelmäßiges Punktsystem $\mathfrak{D}$ gewissermaßen

*) Kronecker, Grundzüge einer arithmetischen Theorie der algebraischen Größen. Festschrift zu Herrn Kummers Doktorjubiläum. Crelles Journal Bd. 92, S. 99. (Werke, Bd. II, S. 360.) — Dedekind, Allgemeine Zahlentheorie (Suppl. XI zu den Vorlesungen über Zahlentheorie von Dirichlet, III. [[oder IV.]] Aufl.). — Für unsern speziellen Zweck liegen die Dedekindschen Begriffsbestimmungen besonders günstig; auf das soeben genannte Werk beziehen sich im folgenden die Zitate mit dem Buchstaben $D$.

als Träger des gesamten Zahlensystems $\mathfrak{o}$ betrachtet werden; wir haben nur festzusetzen, welcher Punkt der Zahl $\omega = 0$ entsprechen soll.

Unter einem *Ideal* des Gebietes $\mathfrak{o}$ versteht man nach Herrn Dedekind jedes in $\mathfrak{o}$ enthaltene und nicht aus der Zahl Null allein bestehende Zahlensystem $\mathfrak{a}$, dessen Inhalt keine Bereicherung erfahren könnte, weder wenn man Summen und Differenzen aus seinen Zahlen, noch wenn man Produkte aus seinen Zahlen in Zahlen aus $\mathfrak{o}$ hinzunehmen wollte (*D.* § 168 [[IV. Aufl., § 177]]). Als Träger eines Ideals $\mathfrak{a}$ erscheint ein, im Punktsysteme $\mathfrak{D}$ im Sinne von 5. enthaltenes, ebenfalls parallelepipedischer Anordnungen fähiges, regelmäßiges $n$-dimensionales Punktsystem $\mathfrak{A}$; der Quotient aus der mittleren Dichtigkeit des Punktsystems $\mathfrak{D}$ und der mittleren Dichtigkeit dieses darin enthaltenen Punktsystems $\mathfrak{A}$ heißt die *Norm* des Ideals $\mathfrak{a}$, in Zeichen: $\mathrm{Nm}(\mathfrak{a})$. Es gibt immer nur eine beschränkte Anzahl von Idealen, welche dieselbe Norm haben. Das System $\mathfrak{o}$, selbst ein Ideal, ist offenbar das einzige von der Norm 1. Die Gesamtheit aller Zahlen in $\mathfrak{o}$, welche durch eine bestimmte, von Null verschiedene Zahl $\eta$ aus $\mathfrak{o}$ teilbar sind, konstituiert ein sogenanntes *Hauptideal* $\mathfrak{o}\eta$; die Norm eines solchen ist der absolute Wert der Norm von $\eta$, d. i. des Produkts der $n$ konjugierten Zahlen $\eta', \eta'', \ldots, \eta^{(n)}$, welche zu den einzelnen $n$ Wurzeln der irreduktiblen Ausgangsgleichung in derselben Beziehung stehen wie die Zahl $\eta$ zu der Wurzel $\theta$ dieser Gleichung.

Unter dem *Produkte* $\mathfrak{a}\mathfrak{b}$ zweier Ideale $\mathfrak{a}$ und $\mathfrak{b}$ versteht man den Inbegriff aller Zahlen, welche sich als ein Produkt aus einer Zahl in $\mathfrak{a}$ und einer Zahl in $\mathfrak{b}$ oder als Summe mehrerer solcher Produkte darstellen lassen; das Produkt $\mathfrak{a}\mathfrak{b}$ ist wieder ein Ideal und seine Norm das Produkt der Normen von $\mathfrak{a}$ und von $\mathfrak{b}$ (*D.* § 170 [[IV. Aufl., § 177 u. § 180]]). Beziehungen zwischen Produkten aus Idealen lassen ganz analoge Folgerungen zu wie Beziehungen zwischen Produkten aus rationalen ganzen Zahlen; das Ideal $\mathfrak{o}$ spielt dabei die Rolle der Zahl 1.

Zu jeder von Null verschiedenen Zahl $\mu$ eines Ideals $\mathfrak{a}$ gibt es ein bestimmtes Ideal $\mathfrak{m}$, welches die Gleichung $\mathfrak{o}\mu = \mathfrak{a}\mathfrak{m}$ befriedigt und also die Fähigkeit besitzt, durch sein Hinzutreten als Faktor das Ideal $\mathfrak{a}$ in ein Hauptideal zu verwandeln (*D.* § 175 [[IV. Aufl., § 178]]). Die Ideale werden nach den Multiplikatoren klassifiziert, welche geeignet sind, sie in Hauptideale zu verwandeln und über diese Multiplikatoren wollen wir nun einen wichtigen Satz ableiten. Zu dem Ende legen wir jedoch eine quadratische Form $f$ von besonderer Beschaffenheit zugrunde, nämlich wir setzen:

$$f = \sum_h \lambda_h (\mathrm{abs.}\, \omega_1^{(h)} x_1 + \omega_2^{(h)} x_2 + \cdots + \omega_n^{(h)} x_n)^2 \qquad (h = 1, 2, \ldots, n);$$

die linearen Formen in diesem Ausdrucke sollen die $n$ mit der Form $\omega$

konjugierten Formen vorstellen; unter $(\text{abs.})^2$ soll das Quadrat des absoluten Betrags einer solchen Form verstanden werden, die Variablen als reelle Größen gedacht; ferner sollen die $\lambda_h$ beliebige positive Konstanten bedeuten. Ein solches $f$ ist eine wesentlich positive quadratische Form, und die Determinante dieser Form hat den Ausdruck $\prod_h \lambda_h \operatorname{abs.} D$, unter $\operatorname{abs.} D$ den absoluten Wert der Diskriminante $D$ verstanden. Die mittlere Dichtigkeit in dem, zu einem Ideal $\mathfrak{a}$ gehörigen Punktsysteme $\mathfrak{A}$ wird demnach

$$1 : \operatorname{Nm}(\mathfrak{a}) \sqrt{\prod_h \lambda_h \cdot \operatorname{abs.} D}$$

betragen. Fassen wir nun in dem Punktsysteme $\mathfrak{A}$ einen Punkt ins Auge, welcher möglichst nahe dem Nullpunkte liegt, und benutzen wir die in (6a) gegebene Grenze für die kleinste Entfernung zweier Punkte in einem regelmäßigen Punktsysteme, so können wir aus dem Orte dieses Punktes $n$ Zahlen $x_1, x_2, \ldots, x_n$ erschließen, für welche

$$\omega_1 x_1 + \omega_2 x_2 + \cdots + \omega_n x_n = \mu$$

eine Zahl in $\mathfrak{a}$ ist, und zugleich erweist sich für diese Zahlen der Ausdruck

$$\sum_h \lambda_h (\operatorname{abs.} \mu^{(h)})^2 < n \sqrt[n]{\prod_h \lambda_h \cdot (\operatorname{Nm} \mathfrak{a})^2 \operatorname{abs.} D}. \quad (h = 1, 2, \ldots, n)$$

Ein besonderer Nachdruck ist aus einem bald ersichtlichen Grunde darauf zu legen, daß hier das Zeichen $<$ und nicht etwa $\leqq$ sich einfindet. Benutzen wir nun, daß eine Summe von $n$ positiven Größen niemals kleiner ist als das $n$-fache der $n^{\text{ten}}$ Wurzel aus dem Produkte der $n$ Größen, und setzen wir zugleich $(\operatorname{Nm} \mu)^2$ für $\prod_h (\operatorname{abs.} \mu^{(h)})^2$, so können wir aus der vorstehenden Ungleichung die weitere entnehmen:

$$n \sqrt[n]{\prod_h \lambda_h \cdot (\operatorname{Nm} \mu)^2} < n \sqrt[n]{\prod_h \lambda_h \cdot (\operatorname{Nm} \mathfrak{a})^2 \operatorname{abs.} D}. \quad (h = 1, 2, \ldots, n)$$

Ist $\mathfrak{m}$ das Ideal, welches die Gleichung $\mathfrak{o}\mu = \mathfrak{a}\mathfrak{m}$ befriedigt, so haben wir $\operatorname{Nm}(\mathfrak{a}) \operatorname{Nm}(\mathfrak{m}) = \pm \operatorname{Nm}(\mu)$, und wir finden demnach:

$$\operatorname{Nm}(\mathfrak{m}) < \sqrt{\operatorname{abs.} D}.$$

*Zu jedem Ideal gibt es behufs Herstellung eines Hauptideals mindestens einen Multiplikator, bei welchem die Norm weniger beträgt als die Wurzel aus dem absoluten Werte der Diskriminante.*

Als eine spezielle Folgerung geht daraus der bekannte Satz hervor, daß eine endliche Anzahl von Multiplikatoren ausreichend ist, um alle Ideale in Hauptideale zu verwandeln*). Eine andere, sehr bemerkenswerte

*) Dieser Satz ist auf Herrn Kronecker zurückzuführen. Vgl. die Bemerkungen auf S. 64 der Festschrift zu Herrn Kummers Doktorjubiläum, Crelles Journal, Bd. 92. (Werke, Bd. II, S. 320.)

Folgerung ist diese: Da die Norm eines Ideals eine ganze Zahl, mindestens gleich Eins ist, so ergibt die letzte Ungleichung $1 < \sqrt{\text{abs. } D}$, also muß $D$ von $\pm 1$ verschieden sein, d. h.:

*Jede Diskriminante enthält Primzahlen als Faktoren.*

Diese das Wesen der algebraischen Zahlen tief berührende Eigenschaft findet sich auf Seite 21 der eben zitierten Festschrift von Herrn Kronecker ausgesprochen; doch ist ein Beweis dieser Eigenschaft bisher nicht veröffentlicht worden.

Überhaupt kommen die kleinsten positiven wie negativen Zahlen bis zu gewissen von der jedesmaligen Ordnung $n$ abhängigen Grenzen als Werte von Diskriminanten nicht vor.

Denn benutzen wir die zweite in 6. gefundene Grenze für das Minimum einer positiven quadratischen Form, so finden wir im übrigen nach genau demselben Verfahren, wie bei der ersten Grenze, eine schärfere Ungleichung, nämlich die folgende:

$$\text{(7b)} \qquad \text{Nm}(\mathfrak{m}) < \frac{\Gamma\left(1+\frac{n}{2}\right)}{\left\{\Gamma\left(\frac{1}{2}\right)\right\}^n} \frac{2^n}{n^{\frac{n}{2}}} \sqrt{\text{abs. } D},$$

und diese können wir wieder mit der Ungleichung $1 \leqq \text{Nm}(\mathfrak{m})$ verbinden; so zeigt sich, daß der absolute Wert einer Diskriminante $n^{\text{ter}}$ Ordnung sicherlich immer die Größe $\frac{\left(\frac{\pi e}{2}\right)^n}{n \pi e^{\frac{1}{3n}}}$ übertrifft.

Die zuletzt gefundene Grenze für die Norm eines Multiplikators wollen wir noch in einem Beispiele anwenden. Herr Wolfskehl*) hat vor kurzem den Nachweis geliefert, daß der zweite Faktor der Klassenanzahl für die aus den $13^{\text{ten}}$ Wurzeln der Einheit gebildeten Zahlen gleich Eins ist. Dieser Nachweis erforderte außer einer Benutzung der Reuschleschen Tafeln noch recht verwickelte Rechnungen. Wir können hier einfacher zu demselben Satze gelangen und noch hinzufügen, daß die gleiche Erscheinung auch bei den $17^{\text{ten}}$ und $19^{\text{ten}}$ Wurzeln der Einheit eintritt; ja später werden wir sogar durch ähnliche Mittel dieses Resultat noch weiter auszudehnen imstande sein.

Stellt $\lambda$ eine ungerade Primzahl vor, so bedeutet der zweite Faktor der Klassenanzahl für die aus den $\lambda^{\text{ten}}$ Einheitswurzeln gebildeten Zahlen — wir machen augenblicklich von der Kummerschen Terminologie Gebrauch — dasselbe wie die Klassenanzahl für die aus den $\frac{\lambda-1}{2}$ zwei-

*) Crelles Journal, Bd. 99, S. 173.

gliedrigen Perioden dieser Einheitswurzeln gebildeten Zahlen. Die Diskriminante des Systems dieser letzteren Zahlen hat den Ausdruck $\lambda^{\frac{1}{2}(\lambda-3)}$; setzen wir in die Ungleichung (7b) diese Größe für $D$ und zugleich $\frac{\lambda-1}{2}$ für $n$, so erlangt die rechte Seite dort folgende Werte:

für $\lambda = 5,$ 7, 11, 13, 17, 19,

$1, \ldots,$ $2, \ldots,$ $13, \ldots,$ $34, \ldots,$ $311, \ldots,$ $1027, \ldots.$

Bis zu diesen Grenzen hätten wir also höchstens die Normen der Multiplikatoren zur Hervorbringung wirklicher Zahlen zu suchen, und wenn alle Zahlen bis zu diesen Grenzen sich in wirkliche Faktoren zerlegen lassen sollten, so kommen in den hier betrachteten Fällen ideale Multiplikatoren und demgemäß auch ideale Zahlen überhaupt nicht vor. Nun entnehmen wir aus den Reuschleschen Tafeln, daß für die soeben aufgezählten Werte von $\lambda$ alle Zahlen unter 1000 sich in wirkliche Faktoren zerlegen lassen. Wir haben also nur noch in bezug auf $\lambda = 19$ festzustellen, daß hier die Primzahlen zwischen 1000 und 1027, das sind 1009, 1013, 1019, 1021, ebenfalls einer solchen Zerlegung innerhalb des durch die entsprechenden zweigliedrigen Perioden bestimmten Gebiets fähig sind. Nun gehören in bezug auf die Primzahl 19 die Zahlen 1009 und 1021 zum Exponenten 18, die Zahl 1013 zum Exponenten 9; diese Zahlen sind also in dem fraglichen Zahlengebiet der zweigliedrigen Perioden selbst noch Primzahlen. Die Zahl 1019 endlich gehört modulo 19 zum Exponenten 6, ihre Primfaktoren werden also von den drei sechsgliedrigen Perioden der $19^{\text{ten}}$ Einheitswurzeln abhängen. Diese sind die Wurzeln der Gleichung $\eta^3 + \eta^2 - 6\eta - 7 = 0$, deren Diskriminante den Wert $D = 19^2$ hat. Da nun in dem durch diese Wurzeln bestimmten Gebiete nach den Reuschleschen Tafeln die Zahlen bis zu $\sqrt{D} = 19$ in wirkliche Faktoren zerlegbar sind, so können in diesem Gebiete ideale Teiler nicht existieren, und demnach muß auch 1019 in drei wirkliche Faktoren zerlegt werden können.

## IX.

# Théorèmes arithmétiques.

Extrait d'une lettre de M. H. Minkowski à M. Hermite.

(Comptes rendus de l'Académie des Sciences, t. 112, pp. 209—212.)

» La méthode géométrique de mon travail*), traduite en langue purement analytique, conduit à ce théorème susceptible d'une application très étendue:

» *Soit $n$ un nombre plus grand que* 1; *soient* $\xi$, $\eta$, $\zeta$, ..., $n$ *formes linéaires indépendantes à* $n$ *variables* $x$, $y$, $z$ .... *Parmi ces formes, soient* $\beta$ *paires d'imaginaires conjugées et les autres* $n - 2\beta = \alpha$ *formes réelles. L'un ou l'autre des nombres* $\alpha$ *et* $\beta$ *peut aussi être égal à zéro. Soit* $\Delta$ *le déterminant des formes* $\xi$, $\eta$, $\zeta$, .... *Soit enfin* $p$ *une quantité quelconque* $\geqq 1$. *On peut toujours assigner à* $x$, $y$, $z$, ... *des valeurs entières, de sorte que la somme*

$$(\text{abs. } \xi)^p + (\text{abs. } \eta)^p + (\text{abs. } \zeta)^p + \cdots$$

*soit différente de zéro et en même temps plus petite que la quantité*

$$\left\{ \left(\frac{2}{\pi}\right)^{\beta} \frac{\Gamma\left(1+\frac{n}{p}\right)}{\left[\Gamma\left(1+\frac{1}{p}\right)\right]^{\alpha} 2^{-\frac{2\beta}{p}} \left[\Gamma\left(1+\frac{2}{p}\right)\right]^{\beta}} \text{abs. } \Delta \right\}^{\frac{p}{n}},$$

*qui est elle-même plus petite que*

$$n\,(\text{abs. } \Delta)^{\frac{p}{n}}.$$

Ici abs. signifie « valeur absolue de » et $\Gamma$ désigne la fonction gamma.

» En suivant une voie indiquée dans vos admirables lettres à Jacobi, je tirerai du théorème que je viens d'exposer plusieurs conclusions fondamentales sur les nombres algébriques.

---

*) *Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen* (Journal de Crelle, t. 107, p. 278). Diese Ges. Abhandlungen, Bd. I, S. 243—260.

» Soit un corps algébrique quelconque, irréductible et d'ordre $n$, et soit $\xi$ une forme linéaire qui, pour toutes les valeurs entières de ses $n$ variables $x, y, z, \ldots$, représente tous les entiers algébriques de ce corps; soient, de plus, $\eta, \zeta, \ldots$ les $n-1$ formes conjuguées à $\xi$. Le discriminant du corps est représenté par le carré du déterminant $\Delta$, et ce carré est un entier rationnel $D$ du signe $(-1)^\beta$. En faisant usage de l'inégalité

$$(\text{abs.}\,\xi\eta\zeta\ldots)^p \leqq \left[\frac{(\text{abs.}\,\xi)^p + (\text{abs.}\,\eta)^p + (\text{abs.}\,\zeta)^p + \cdots}{n}\right]^n,$$

et en remarquant que abs. $\xi\eta\zeta\ldots$ est un entier $\geqq 1$, pourvu que $x, y, z, \ldots$ soient des entiers et qu'ils ne s'évanouissent pas tous, les inégalités du théorème énoncé entraîneront celles-ci:

$$1 < \left\{\left(\frac{2}{\pi}\right)^\beta \frac{n^{-\frac{n}{p}}\,\Gamma\left(1+\frac{n}{p}\right)}{\left[\Gamma\left(1+\frac{1}{p}\right)\right]^\alpha 2^{-\frac{2\beta}{p}}\left[\Gamma\left(1+\frac{2}{p}\right)\right]^\beta}\right\}^2 \text{abs.}\,D < \text{abs.}\,D.$$

» Faisant d'abord abstraction du terme intermédiaire, nous avons ainsi démontré le postulat profond de M. Kronecker*), que chaque discriminant est différent de $\pm 1$, c'est-à-dire que *chaque discriminant contient des nombres premiers comme facteurs.* C'est là un détail bien digne d'attention. Tout nombre algébrique irrationnel a ainsi ses nombres premiers critiques, comme toute fonction algébrique irrationnelle a ses points d'embranchement.

» Le terme dont nous n'avons pas tenu compte nous fournit pour la valeur absolue d'un discriminant des limites inférieures plus complètes. Ces autres limites, où figure encore le nombre $\beta$, s'accroissant indéfiniment avec l'ordre $n$, il est évident qu'*un nombre donné quelconque ne peut être discriminant que pour un nombre fini d'ordres n.*

» De quelle manière fixera-t-on le mieux la quantité $p$, assujettie jusqu'à présent à la seule condition de ne pas être moindre que l'unité? On se convaincra aisément que les limites dont nous venons de parler devront s'agrandir aussi longtemps que la valeur de $p$ décroît. Ce n'est donc pas quand $p$ est égal à 2, valeur qui répond aux formes quadratiques, mais dans le cas de $p = 1$, que ces limites seront le plus avancées. Il en résulte enfin ce théorème:

» *Le discriminant d'un corps algébrique, faisant partie de n corps conjugués dont $2\beta$ sont imaginaires et $n - 2\beta$ réels, est en valeur absolue toujours plus grand que*

$$\left[\left(\frac{\pi}{4}\right)^\beta \frac{n^n}{2\cdot 3\ldots n}\right]^2.$$

*) Journal de Crelle, t. 92, (Werke, Bd. II, S. 269).

» Par exemple, un discriminant du deuxième ordre doit être ou $> 4$ ou $< -2$, .... Les valeurs les plus petites 5 et $-3$ se trouvent dans les équations $\omega^2 + \omega - 1 = 0$ et $\omega^2 + \omega + 1 = 0$.

» Un discriminant du troisième ordre doit être ou $> 20$, ... ou $< -12$, .... De la limite précise du minimum des formes quadratiques positives ternaires on aurait tiré, en suivant une marche tout analogue, les inégalités $D \geqq 13{,}5$ ou $\leqq -13{,}5$. La limite que nous avons trouvée plus haut n'est donc pas, il est vrai, une limite précise, mais malgré cela elle nous fournit déjà des résultats que les formes quadratiques n'ont pas encore donnés. »

X.

# Über Geometrie der Zahlen.

Bericht über einen Vortrag zu Halle.
(Verhandlungen der 64. Naturforscher- und Ärzteversammlung zu Halle, 1891, S. 13
und
Jahresbericht der Deutschen Mathematiker-Vereinigung, Band 1, S. 64—65.)

Wenn man für den Raum rechtwinklige Koordinaten einführt, so entsprechen den Systemen von drei *ganzen* Zahlen diskrete Punkte, welche derart über den Raum verstreut liegen, daß sie eine gewisse Nähe in bezug auf jede beliebige Raumstelle erreichen. Den Inbegriff aller dieser Punkte mit lauter Koordinaten, die ganze Zahlen sind, nennt der Vortragende das dreidimensionale *Zahlengitter*; unter dem Titel *„Geometrie der Zahlen“* begreift er geometrische Studien über das dreidimensionale Zahlengitter und über das entsprechende Gebilde in der Ebene, und in weiterem Sinne auch die Ausdehnung der Ergebnisse solcher Studien auf Mannigfaltigkeiten beliebiger Ordnung. Natürlich besitzt jede Aussage über die Zahlengitter einen rein arithmetischen Kern. Das Wort „Geometrie“ erscheint aber durchaus am Platze im Hinblick auf Fragestellungen, zu welchen die geometrische Anschauung verhilft, und auf Untersuchungsmethoden, welche fortwährend durch geometrische Begriffe ihre Richtung angewiesen erhalten.

Der Vortragende hat sich in betreff der Zahlengitter hauptsächlich zwei Fragen gestellt; sie ergänzen einander in gewisser Beziehung, und folgendes ist ihnen gemeinsam: Es handelt sich, wenn speziell vom Raume gesprochen wird, jedesmal um eine sehr allgemeine Kategorie von Körpern, welche so konstruiert werden, daß sie einen bestimmten Punkt des Zahlengitters — es sei dies etwa der Nullpunkt — in gewisser Weise umschließen, und es soll dann jedesmal bei diesen Körpern eine gewisse Eigenschaft in bezug auf das Zahlengitter allein durch die Größe des Inhalts der Körper zustande kommen.

Die erste Kategorie von Körpern besteht aus allen denjenigen Körpern, welche im Nullpunkte einen Mittelpunkt haben, und deren Begrenzung nach außen hin nirgends konkav ist; und die fragliche Eigen-

schaft für diese Kategorie lautet: Wenn der Inhalt eines Körpers dieser Kategorie $\geqq 2^3$ ist, so schließt der Körper notwendig noch weitere Punkte des Zahlengitters außer dem Nullpunkte ein.

Die zweite Kategorie von Körpern ist noch umfassender; sie besteht aus allen Körpern, welche den Nullpunkt enthalten, und deren Oberfläche, vom Nullpunkte aus gesehen, nach jeder Richtung hin nur einen Punkt darbietet; und die fragliche Eigenschaft für diese zweite Kategorie lautet: Wenn der Inhalt eines Körpers dieser Kategorie

$$\leqq 1 + \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + \cdots$$

ist, so können stets Deformationen des Körpers angegeben werden, bei welchen der Inhalt sich nicht ändert, der Nullpunkt fest bleibt und gerade Linien gerade Linien bleiben, und nach deren Ausführung alle Punkte des Zahlengitters mit Ausnahme des Nullpunkts ihren Ort außerhalb des Körpers finden.

Der Vortragende weist auf die außerordentliche Tragweite dieser, in ihrer Allgemeinheit ebenso einfach wie plausibel klingenden Sätze hin.

---

## XI.

# Extrait d'une lettre adressée à M. Hermite.

(Bulletin des Sciences mathématiques, 2e série, t. XVII, pp. 24—29.)

Veuillez bien permettre, Monsieur, que je vous donne un rapide résumé de mon Ouvrage.*) La plus grande partie du livre traite des fonctions $\varphi$ à $n$ variables $x_1, x_2, \ldots, x_n$, qui, comme la racine carrée d'une forme quadratique positive, satisfont aux conditions

$$\text{(A)}\quad \begin{cases} \varphi(x_1, x_2, \ldots, x_n) > 0, \quad \text{si l'on n'a pas} \quad x_1 = 0, \quad x_2 = 0, \ \ldots, \ x_n = 0, \\ \varphi(0, 0, \ldots, 0) = 0, \\ \varphi(tx_1, tx_2, \ldots, tx_n) = t\varphi(x_1, x_2, \ldots, x_n), \quad \text{si} \quad t > 0, \end{cases}$$

$$\text{(B)}\quad \varphi(x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) \leqq \varphi(x_1, x_2, \ldots, x_n) + \varphi(y_1, y_2, \ldots, y_n),$$

$$\text{(C)}\quad \varphi(-x_1, -x_2, \ldots, -x_n) = \varphi(x_1, x_2, \ldots, x_n).$$

Soient $\xi_1, \xi_2, \ldots, \xi_\nu$ un nombre fini de formes linéaires à coefficients réels et aux variables $x_1, x_2, \ldots, x_n$, et parmi ces formes soient $n$ formes à déterminant différent de zéro. Soit

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

le maximum parmi les valeurs absolues de $\xi_1, \xi_2, \ldots, \xi_\nu$. Une telle fonction $\Phi$ satisfera évidemment aux conditions d'une fonction $\varphi$.

J'établis d'abord ce théorème:

$\varphi$ étant une solution quelconque de (A), (B), (C), et $\delta$ une quantité positive choisie à volonté, on peut toujours trouver des fonctions $\Phi$ comme je viens de les caractériser, de sorte que, pour toutes les valeurs possibles de $x_1, x_2, \ldots, x_n$, on ait

$$1 \leqq \frac{\varphi}{\Phi} < 1 + \delta.$$

Il en résulte que l'intégrale $\int\int \ldots \int dx_1\, dx_2 \ldots dx_n$ étendue sur le domaine $\varphi(x_1, x_2, \ldots, x_n) \leqq 1$ aura toujours une valeur déterminée. Soit $J$ cette valeur. Je démontre alors que *l'on peut toujours trouver des nombres entiers* $x_1, x_2, \ldots, x_n$ *pour lesquels on ait*

$$\text{(I)}\quad 0 < \varphi(x_1, x_2, \ldots, x_n) \leqq \frac{2}{\sqrt[n]{J}}.$$

*) Gemeint ist die „Geometrie der Zahlen." (Anm. d. Herausg.)

J'ajoute ce théorème supplémentaire:

Le cas qu'il n'existe pas de nombres entiers $x_1, x_2, \ldots, x_n$, pour lesquels on ait

$$0 < \varphi(x_1, x_2, \ldots, x_n) < \frac{2}{\sqrt[n]{J}},$$

ne peut se présenter que chez des fonctions $\Phi$ provenant d'un nombre $\nu$ de formes linéaires $\leqq 2^n - 1$.

La plus simple application du théorème (I) est la suivante:

$\xi_1, \xi_2, \ldots, \xi_n$ étant $n$ formes linéaires à coefficients réels quelconques et à déterminant égal à $\pm 1$, on peut toujours donner à $x_1, x_2, \ldots, x_n$ des valeurs entières qui ne s'évanouissent pas toutes et de sorte que les valeurs absolues de $\xi_1, \xi_2, \ldots, \xi_n$ soient toutes $\leqq 1$.

L'énoncé plus exact de ce théorème est que l'on peut trouver des nombres entiers $x_1, x_2, \ldots, x_n$, qui ne s'évanouissent pas tous, et de sorte que les valeurs absolues de $\xi_1, \xi_2, \ldots, \xi_n$ soient toutes $< 1$, excepté le cas où les formes $\xi_1, \xi_2, \ldots, \xi_n$, par une substitution linéaire à coefficients entiers et à déterminant $\pm 1$, peuvent être transformées de manière que, abstraction faite de l'ordre, elles deviennent

$$x_1, \quad a_{21}x_1 + x_2, \quad \ldots, \quad a_{n1}x_1 + a_{n2}x_2 + \cdots + x_n.$$

Ainsi, par exemple, $a_1, a_2, \ldots, a_{n-1}$ étant des quantités réelles quelconques et $T$ une quantité $> 1$, il y aura des nombres entiers $x_1, x_2, \ldots, x_{n-1}, x_n$, parmi lesquels $x_n$ est différent de zéro, de sorte que les valeurs absolues de

$$x_1 - a_1 x_n, \quad x_2 - a_2 x_n, \quad \ldots, \quad x_{n-1} - a_{n-1} x_n, \quad \frac{x_n}{T^n}$$

soient toutes $< \frac{1}{T}$, excepté le cas où $T$ est un nombre entier, et $a_1, a_2, \ldots, a_{n-1}$, abstraction faite de l'ordre, ont des expressions $\frac{T_1}{T}, \frac{T_2}{T^2}, \ldots, \frac{T_{n-1}}{T^{n-1}}$, dans lesquelles $T_1, T_2, \ldots, T_{n-1}$ sont des nombres entiers premiers à $T$.

En appliquant le théorème (I) à la fonction $\Phi$ qui est définie à l'aide des $2n-2$ formes

$$x_1 - a_1 x_n \pm \frac{x_n}{S}, \quad x_2 - a_2 x_n \pm \frac{x_n}{S}, \quad \ldots, \quad x_{n-1} - a_{n-1} x_n \pm \frac{x_n}{S},$$

on conclut que l'on peut toujours trouver des nombres entiers $x_1, x_2, \ldots, x_{n-1}, x_n$, sans diviseur commun et parmi lesquels $x_n$ est positif, de sorte que les valeurs absolues de

$$\frac{x_1}{x_n} - a_1, \quad \frac{x_2}{x_n} - a_2, \quad \ldots, \quad \frac{x_{n-1}}{x_n} - a_{n-1}$$

soient plus petites qu'une quantité positive $\varepsilon$ choisie à volonté, et en même temps

$$< \frac{n-1}{n\, x_n^{\frac{n}{n-1}}}.$$

A l'aide de certaines autres fonctions $\varphi$, on obtient les théorèmes analogues pour les quantités complexes.

Les théorèmes que j'ai exposés dans ma dernière lettre sont aussi des conséquences spéciales du théorème (I). De ce théorème découlent enfin les théorèmes de Dirichlet sur les unités complexes.

Ensuite j'établis cette généralisation du théorème (I):

Pour toute fonction $\varphi$, satisfaisant aux conditions (A), (B), (C), on peut trouver $n^2$ nombres entiers $l_{hk}$ à déterminant différent de zéro, de sorte que l'on ait

$$\varphi(l_{11}, l_{21}, \ldots, l_{n1})\, \varphi(l_{12}, l_{22}, \ldots, l_{n2}) \ldots \varphi(l_{1n}, l_{2n}, \ldots, l_{nn}) \leqq \frac{2^n}{J}.$$

Le déterminant $|l_{hk}|$ sera alors toujours $\leqq 1 \cdot 2 \ldots n$.

Je fais aussi quelques remarques sur les cas extrêmes de cette relation. Des applications de ce théorème, je ne cite ici que ces deux:

Soient $a_{hk} (h, k = 1, 2, \ldots, n)$ $n^2$ quantités réelles à déterminant différent de zéro, et soit $D$ la valeur absolue de ce déterminant. Il y aura ou $n^2$ nombres entiers $l_{hk}$ à déterminant différent de zéro, de sorte que le système composé

$$\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix} \begin{pmatrix} l_{11} & \ldots & l_{1n} \\ \ldots & \ldots & \ldots \\ l_{1n} & \ldots & l_{nn} \end{pmatrix} = \begin{pmatrix} b_{11} & \ldots & b_{1n} \\ \ldots & \ldots & \ldots \\ b_{n1} & \ldots & b_{nn} \end{pmatrix}$$

satisfasse à toutes les $n^n$ inégalités

$$\pm b_{h_1 1} b_{h_2 2} \ldots b_{h_n n} < D, \quad (h_1 = 1, 2, \ldots, n;\ h_2 = 1, 2, \ldots, n;\ \ldots;\ h_n = 1, 2, \ldots, n),$$

ou $n^2$ nombres entiers $l_{hk}$ à déterminant $\pm 1$, de sorte que ce système composé, après une permutation convenable des lignes, prenne une forme

$$\begin{pmatrix} c_{11} & \ldots & c_{1n} \\ \ldots & \ldots & \ldots \\ c_{n1} & \ldots & c_{nn} \end{pmatrix},$$

satisfaisant aux conditions

$$\begin{aligned} c_{hk} &= 0, \qquad h > k, \\ 0 < c_{11} &\leqq c_{22} \leqq \ldots \leqq c_{nn}, \\ 0 \leqq c_{hk} &< c_{hh}, \qquad h < k. \end{aligned}$$

Une forme quadratique positive à $n$ variables et à déterminant $D$ peut toujours, par une substitution à coefficients entiers et à déterminant différent

de zéro $\left[\text{dont la valeur absolue est} < 2^n \frac{\Gamma\left(1+\frac{n}{2}\right)}{\left(\Gamma\left(\frac{1}{2}\right)\right)^n}\right]$, être transformée en une forme $\sum b_{hk} y_h y_k$, satisfaisant aux conditions

$$0 < b_{11} \leqq b_{22} \leqq \cdots \leqq b_{nn}, \qquad \pm 2 b_{hk} \leqq b_{hh}, \qquad (h < k),$$

$$b_{11} b_{22} \cdots b_{nn} < \left[\frac{2^n \Gamma\left(1+\frac{n}{2}\right)}{\left(\Gamma\left(\frac{1}{2}\right)\right)^n}\right]^2 D.$$

Dans un autre Chapitre, je donne une nouvelle démonstration des théorèmes que Kronecker a établis dans son Mémoire *Näherungsweise ganzzahlige Auflösung linearer Gleichungen* (Werke, Bd. III, 1, S. 47).

Enfin je procède à la méthode de réduction des formes quadratiques positives que vous avez donnée en dernier lieu dans vos lettres à Jacobi. Il résulte de vos développements que l'on peut transformer toute forme quadratique positive $f$ à $n$ variables par une substitution à coefficients entiers et à déterminant $\pm 1$ en une forme $\sum b_{hk} y_h y_k$, qui satisfait à toutes les inégalités

$$\sum b_{hk} p_h p_k \geqq b_{mm},$$

où $m$ est un des nombres $1, 2, \ldots, n$ et où $p_1, p_2, \ldots, p_n$ sont des nombres entiers quelconques, pour lesquels le plus grand diviseur commun de $p_m, p_{m+1}, \ldots, p_n$ est égal à 1.

Je démontre que parmi ces inégalités on trouve un nombre fini d'où dérivent toutes les autres.

Pour une forme donnée $f$, il y aura, en général, $2^{n-1}$ formes satisfaisant à ces inégalités, et qui se déduiront d'une seule par les $2^n$ substitutions

$$y_1 = \pm z_1, \quad y_2 = \pm z_2, \quad \cdots, \quad y_n = \pm z_n.$$

Ces inégalités étant linéaires dans les coefficients $b_{hk}$, on en conclut que, pour la somme

$$\chi(D+1) + \chi(D+2) + \cdots + \chi(D+d),$$

$\chi(\Delta)$ désignant le nombre des classes de formes à coefficients entiers et à déterminant $\Delta$, il existe une expression asymptotique

$$\gamma D^{\frac{n-1}{2}} d.$$

Je démontre que l'on a

$$\gamma = \frac{\Gamma\left(\frac{2}{2}\right)\Gamma\left(\frac{3}{2}\right)\cdots\Gamma\left(\frac{n}{2}\right)}{\left[\Gamma\left(\frac{1}{2}\right)\right]^{2+3+\cdots+n}} S_2 S_3 \cdots S_n,$$

$S_h$ désignant la somme

$$1 + \frac{1}{2^h} + \frac{1}{3^h} + \frac{1}{4^h} + \cdots.$$

A l'aide de ce résultat, j'arrive enfin au théorème suivant:

*$\psi(x_1, \ldots, x_n)$ étant une fonction quelconque, continue aux variables $x_1, \ldots, x_n$ et satisfaisant aux conditions* (A) *des fonctions $\varphi$ [ou aux conditions* (A) *et* (C)], *et $J$ désignant la valeur de l'intégrale $\int \ldots \int dx_1 \ldots dx_n$ étendue sur le domaine $\psi(x_1, \ldots, x_n) \leqq 1$, on peut toujours trouver $n^2$ quantités réelles $a_{hk}$ à déterminant* 1, *de sorte que la relation*

$$0 < \psi(a_{11} y_1 + \cdots + a_{1n} y_n, \ldots, a_{n1} y_1 + \cdots + a_{nn} y_n) \leqq \sqrt[n]{\frac{S_n}{J}} \left( \text{ou} \leqq \sqrt[n]{\frac{2 S_n}{J}} \right)$$

*ne soit vérifiée par aucun système de nombres entiers $y_1, \ldots, y_n$.*

En appliquant ce théorème à la fonction $\psi = \sqrt{x_1^2 + \cdots + x_n^2}$, il résulte une certaine limite inférieure de la limite précise du minimum des formes quadratiques positives, et cette limite donne lieu à l'observation suivante:

$\beta_n \sqrt[n]{D}$ désignant la limite précise du minimum des formes quadratiques positives à $n$ variables et à déterminant $D$, on a

$$\lim_{n=\infty} \left( \frac{\log \beta_n}{\log n} \right) = 1.$$

XII.

# Über Eigenschaften von ganzen Zahlen, die durch räumliche Anschauung erschlossen sind.

(Mathematical Papers read at the international Mathematical Congress held in connection with the world's Columbian Exposition Chicago, 1893, pp. 201—207, und, von R. Laugel ins Französische übersetzt, in den Nouvelles Annales de Mathématiques, 3e série, t. XV, 1896 unter dem Titel: Sur les propriétés des nombres entiers qui sont dérivées de l'intuition de l'espace.)

In der Zahlentheorie wird, wie in jedem anderen Gebiete der Analysis, häufig die Erfindung mittels geometrischer Überlegungen vor sich gehen, während schließlich vielleicht nur die analytischen Verifikationen mitgeteilt werden. Ich würde deshalb schon an sich nicht in der Lage sein, mein Thema zu erschöpfen; es ist dies auch nicht meine Absicht. Ich will hier ganz allein von demjenigen geometrischen Gebilde sprechen, welches die einfachste Beziehung zu den ganzen Zahlen hat, von dem *Zahlengitter*. Darunter hat man, irgendwelche Parallelkoordinaten $x$, $y$, $z$ im Raume vorausgesetzt, den Inbegriff derjenigen Punkte $x$, $y$, $z$ zu verstehen, für welche $x$, wie $y$, wie $z$ ganze Zahlen sind; der besseren Anschaulichkeit wegen denke man sich unter $x$, $y$, $z$ gewöhnliche rechtwinklige Koordinaten.

Eine Figur, die sich als ein Ausschnitt aus dem Zahlengitter darstellt, ist es, die man beim Beweise der Multiplikationsregel $(ab)c = a(bc)$ heranzuziehen pflegt. Ich würde des weiteren die wichtigen Relationen über größte Ganze zu erwähnen haben, die Dirichlet (Crelles Journal, Bd. 47, *Über ein die Division betreffendes Problem;* Werke, Bd. II) auf geometrischem Wege erhalten hat. Ich will mich jedoch hier auf Fragen beschränken, bei denen der Begriff des Unendlichen hineinspielt, nämlich das *ganze* Gitter, nicht bloß Ausschnitte daraus in Betracht kommen. (Das Folgende gibt in der Hauptsache einiges aus meinem Buche „Geometrie der Zahlen" (1896, bei B. G. Teubner) wieder, wobei ich bemerke, daß dort die Beschränkung auf Systeme aus *drei* ganzen Zahlen nicht statthat.)

I. Der wichtigste Begriff, der mit dem Zahlengitter in Zusammen-

hang steht, ist der des *Volumens* eines Körpers; dieser Begriff bildet dann weiter die Grundlage für den Begriff des dreifachen Integrals. Man nehme jeden Punkt des Zahlengitters zum Mittelpunkt eines Würfels mit Seitenflächen parallel den Koordinatenebenen und von der Kante 1; zu einem Würfel soll stets die Begrenzung miteingerechnet werden. Man erlangt so ein Netz $N$ von Würfeln, welches den Raum lückenlos erfüllt, und die einzelnen Würfel darin sind untereinander in ihren inneren Punkten durchweg verschieden. Nun sei $K$ irgendeine solche Punktmenge, welche sich ganz auf eine endliche Anzahl von Würfeln aus $N$ verteilt. Man dilatiere diese Menge $K$ von einem beliebigen Punkte $p$ im Raume aus in allen Richtungen in einem beliebigen Verhältnisse $\Omega : 1$. Aus $K$ entstehe so $K_\Omega^p$. Sodann sei $a_\Omega^p$ die Anzahl aller *der* Würfel aus $N$, in welchen jeder einzige Punkt sich als ein *innerer* Punkt von $K_\Omega^p$ erweist, und es sei $u_\Omega^p$ die Anzahl aller Würfel aus $N$, welche überhaupt *mindestens einen* Punkt von $K_\Omega^p$ enthalten. Dann konvergieren nach dem, was C. Jordan (Journal de Mathématiques, 4e série, T. 8, 1892, p. 77) gezeigt hat, immer $\Omega^{-3} \cdot a_\Omega^p$ und $\Omega^{-3} \cdot u_\Omega^p$ für ein unendlich wachsendes $\Omega$, unabhängig von $p$, je nach einem bestimmten Grenzwerte $A$ und $U$, dem *inneren* und dem *äußeren* Volumen von $K$. Man spricht vom *Volumen* von $K$ *schlechthin*, wenn sich $A = U$ herausstellt.

II. Die tieferen Eigenschaften des Zahlengitters nun hängen mit einer Verallgemeinerung des Begriffs der *Länge einer geraden Linie* zusammen, bei der allein der Satz, daß in einem Dreiecke die Summe zweier Seiten niemals kleiner als die dritte ist, erhalten bleibt.

Man denke sich eine Funktion $S(ab)$ von zwei beliebig variablen Punkten $a$ und $b$ zunächst nur mit folgenden Eigenschaften: (1) Es soll $S(ab)$ immer positiv sein, wenn $b$ von $a$ verschieden ist, und Null, wenn $b$ und $a$ identisch sind; (2) sind $a$, $b$, $c$, $d$ vier Punkte und darunter $b$ von $a$ verschieden, und besteht zwischen ihnen eine Beziehung $d - c = t(b - a)$ mit positivem $t$, so soll immer $S(cd) = tS(ab)$ sein; die genannte Beziehung ist im Sinne des baryzentrischen Kalkuls aufzufassen und bedeutet, daß $cd$ und $ab$ Strecken von gleicher Richtung und mit Längen (im gewöhnlichen Sinne) im Verhältnisse $t : 1$ sind. Zum Unterschiede von der gewöhnlichen Länge möge $S(ab)$ *Strahldistanz von $a$ nach $b$* heißen.

Es sei $o$ der Nullpunkt; offenbar werden alle Werte $S(ab)$ festgelegt sein, sowie die Menge der Punkte $u$ gegeben ist, für welche $S(ou) \leqq 1$ ist; diese Punktmenge heiße der *Eichkörper* der Strahldistanzen, es wird zu ihm in jeder Richtung von $o$ aus eine Strecke von $o$ aus mit endlicher, nichtverschwindender Länge gehören müssen.

Wenn nun ferner für irgend drei Punkte $a$, $b$, $c$ immer

$$S(ac) \leqq S(ab) + S(bc) \tag{3}$$

ist, sollen die Strahldistanzen *einhellig* heißen. Dann besitzt ihr Eichkörper die Eigenschaft, daß mit irgend zwei Punkten $u$, $v$ in ihm immer die ganze Strecke $uv$ zu diesem Körper gehört, und andererseits ist jeder *nirgends konkave Körper* mit dem Nullpunkt im Inneren Eichkörper für ganz bestimmte einhellige Strahldistanzen.

Mit $E(ab)$ werde die halbe Kante desjenigen Würfels mit Seitenflächen parallel den Koordinatenebenen bezeichnet, der $a$ als Mittelpunkt hat und seine Begrenzung durch $b$ schickt. Die $E(ab)$ sind als die einfachsten einhelligen $S(ab)$ anzusehen. Die vollständige analytische Auflösung der Bedingungen (1), (2), (3) habe ich im ersten Kapitel meiner „Geometrie der Zahlen" gegeben. Es zeigt sich, daß auf Grund von (3) insbesondere immer die Funktion $S(ab)$ eine *stetige* der Koordinaten von $a$ und von $b$ ist, ferner zwei positive Größen $g$ und $G$ vorhanden sind, so daß man

$$gE(ab) \leqq S(ab) \leqq GE(ab)$$

für alle $a$ und $b$ hat, endlich der Eichkörper ein bestimmtes Volumen $J$ besitzt. Die Bedeutung von $g$ und $G$ ist offenbar die, daß der Würfel $E(ou) \leqq \frac{1}{G}$ ganz im Eichkörper enthalten ist und letzterer seinerseits ganz im Würfel $E(ou) \leqq \frac{1}{g}$.

*Wechselseitig* sollen die $S(ab)$ heißen, wenn durchweg

$$S(ba) = S(ab) \tag{4}$$

ist. Solches hat dann und nur dann statt, wenn der Eichkörper den Nullpunkt als *Mittelpunkt* hat.

III. Es gibt im Zahlengitter offenbar Punkte $r$, für die $E(or) = 1$ ist. Irgendwelche *einhellige* $S(ab)$ vorausgesetzt, wird für diese Gitterpunkte $r$ dann $S(or) \leqq G$ sein. Diese letztere Bedingung nun kann überhaupt nur von solchen Punkten $r$ erfüllt werden, für welche $E(or) \leqq \frac{G}{g}$ ist, und dieser Bedingung wieder genügen sicher nur eine endliche Anzahl Gitterpunkte. Aus *diesen* Gitterpunkten muß dann notwendig die *kleinste* Strahldistanz $M$ zu ersehen sein, welche von $o$ nach allen anderen Gitterpunkten zusammengenommen existiert und die nun jedenfalls $\leqq G$ ist. Wird sodann für einen beliebigen ersten Gitterpunkt $a$ der Körper $S(au) \leqq \frac{1}{2}M$, für einen beliebigen anderen Gitterpunkt $c$ der Körper $S(uc) \leqq \frac{1}{2}M$ konstruiert, so sind solche zwei Körper zufolge (3) in ihren inneren Punkten durchweg verschieden. Werden nun die Strahldistanzen auch

noch *wechselseitig* vorausgesetzt, so ist der zweite Körper mit $S(cu) \leqq \frac{1}{2} M$ identisch, und stoßen dann also die verschiedenen Körper $S(au) \leqq \frac{1}{2} M$ für die verschiedenen Gitterpunkte $a$ höchstens in den Begrenzungen zusammen.

Nun sei $\Omega$ irgendeine positive und gerade ganze Zahl, und man konstruiere die hier bezeichneten Körper für die sämtlichen im Würfel $E(ou) \leqq \frac{\Omega}{2}$ enthaltenen $(\Omega + 1)^3$ Gitterpunkte

$$x,\ y,\ z = 0, \pm 1, \pm 2, \ldots, \pm \frac{\Omega}{2}.$$

Aus $S(au) \leqq \frac{1}{2} M \leqq \frac{1}{2} G$ folgt $E(au) \leqq \frac{1}{2} \frac{G}{g}$, und werden deshalb alle diese Körper in dem Würfel $E(ou) \leqq \frac{1}{2}\left(\Omega + \frac{G}{g}\right)$ enthalten sein, dessen Volumen $\left(\Omega + \frac{G}{g}\right)^3$ beträgt. Indem sie nun sämtlich auseinander liegen und je vom Volumen $\left(\frac{M}{2}\right)^3 J$ sind, geht daraus die Ungleichung

$$\left(\Omega + \frac{G}{g}\right)^3 \geqq (\Omega + 1)^3 \left(\frac{M}{2}\right)^3 J$$

hervor; nun stellen $M$ und $J$ bestimmte Größen vor und $\Omega$ kann beliebig groß genommen werden, mithin entnimmt man daraus:

$$1 \geqq \left(\frac{M}{2}\right)^3 J, \tag{5}$$

*muß es also mindestens einen, von o verschiedenen Gitterpunkt q geben, für den* $S(oq) \leqq \frac{2}{\sqrt[3]{J}}$ *ist.*

Das hiermit gewonnene Theorem über die nirgends konkaven Körper mit Mittelpunkt scheint mir zu den fruchtbarsten in der ganzen Zahlentheorie zu gehören. Ich hatte es, durch das Studium der Aufsätze von Dirichlet und von Hermite über quadratische Formen (Crelles Journal, Bd. 40, S. 209 u. S. 261; Dirichlets Werke, Bd. II, S. 27; Oeuvres d'Hermite, T. I, p. 100) angeregt, zunächst für die Ellipsoide gefunden (Crelles Journal, Bd. 107, S. 291; diese Ges. Abhandlungen, Bd. I, S. 255); ein noch größeres Interesse aber bieten die Folgerungen dar, welche dieses Theorem hinsichtlich linearer Formen zuläßt und von denen ich sogleich einige hervorheben werde.

Das Gleichheitszeichen in (5) tritt dann und nur dann ein, wenn die Körper $S(au) \leqq \frac{1}{2} M$ um die einzelnen Gitterpunkte $a$ den Raum *lückenlos* erfüllen. Dazu muß vor allem die vollständige Begrenzung des Eichkörpers durch eine endliche Anzahl von Ebenen, und zwar durch nicht mehr als $2(2^3 - 1)$ Ebenen, gebildet werden; nämlich es muß dann jede

ebene Wand von $S(au) \leqq M$ noch exklusive des Randes mindestens einen Gitterpunkt $x, y, z$ enthalten, und können für derartige Gitterpunkte in zwei, nicht in bezug auf $o$ symmetrischen Wänden niemals $x, y, z$ gleiche Reste modulo 2 ergeben, wie auch für keinen dieser Punkte $x, y, z \equiv 0, 0, 0 \pmod 2$ sein können. Das Gleichheitszeichen in (5) tritt beispielsweise niemals für ein Oktaeder ein.

IV. Es seien $\xi, \eta, \zeta$ drei lineare Formen in $x, y, z$ mit einer von Null verschiedenen Determinante $D$, es seien entweder alle drei reell, oder $\xi$ reell und $\eta, \zeta$ zwei Formen mit konjugiert imaginären Koeffizienten; weiter sei $p$ irgendeine reelle Größe. Der durch

$$\left(\frac{|\xi|^p + |\eta|^p + |\zeta|^p}{3}\right)^{\frac{1}{p}} \leqq 1 \tag{6}$$

definierte Körper $K_p$ stellt dann, sowie $p \geqq 1$ ist, einen nirgends konkaven Körper vor; für das Volumen $J_p$ dieses Körpers findet man:

$$J_p = \frac{2^3}{\lambda_p^3 |D|}, \quad \lambda_p^3 = \frac{3^{-\frac{3}{p}} \Gamma\left(1+\frac{3}{p}\right)}{\left\{\Gamma\left(1+\frac{1}{p}\right)\right\}^3} \text{ oder } = \frac{2}{\pi} \frac{3^{-\frac{3}{p}} \Gamma\left(1+\frac{3}{p}\right)}{\Gamma\left(1+\frac{1}{p}\right) 2^{-\frac{2}{p}} \Gamma\left(1+\frac{2}{p}\right)};$$

es zeigt sich ferner, daß für einen Körper $K_p$, wenn $p$ endlich ist, in (5) niemals das Gleichheitszeichen in Betracht kommt. Man gewinnt so den Satz:

*Ist $p \geqq 1$, so gibt es immer ganze Zahlen $x, y, z$, die nicht sämtlich Null sind und für welche man*

$$\left(\frac{|\xi|^p + |\eta|^p + |\zeta|^p}{3}\right)^{\frac{1}{p}} < \lambda_p |D|^{\frac{1}{3}}$$

*hat.*

Hält man $x, y, z$ fest, so nimmt der Ausdruck links in (6), wenn nicht gerade $|\xi| = |\eta| = |\zeta|$ ist, in welchem Falle dieser Ausdruck von $p$ unabhängig sein würde, mit $p$ für alle Werte $p \geqq 0$ kontinuierlich ab (sogar für alle $p$, wenn keine der Größen $|\xi|, |\eta|, |\zeta|$ Null ist). Es wird danach ein jeder Körper $K_p$ in allen anderen von diesen Körpern mit kleinerem $p$ enthalten sein und also $\frac{1}{J_p}$ und $\lambda_p$ mit $p$ kontinuierlich zunehmen; für $p = \infty$ konvergiert $\lambda_p^3$ nach 1, bzw. $\frac{2}{\pi}$. Für $p = \infty$ geht $K_p$ in das Parallelepipedum $-1 \leqq \xi \leqq 1$, $-1 \leqq \eta \leqq 1$, $-1 \leqq \zeta \leqq 1$ oder den elliptischen Zylinder $-1 \leqq \xi \leqq 1$, $\eta^2 + \zeta^2 \leqq 1$ über; $K_1$ hingegen stellt ein Oktaeder oder einen Doppelkegel vor. Endlich wird aus der Funktion links in (6) für $p = 0$ das geometrische Mittel $\sqrt[3]{|\xi\eta\zeta|}$, sodaß man den Satz hinzufügen kann:

Es gibt immer ganze Zahlen $x$, $y$, $z$, die nicht sämtlich Null sind und für welche man $|\xi\eta\zeta| < \lambda_1^3 |D|$, umsomehr also $< |D|$, hat.

Diese Sätze und die analogen für $n$ lineare Formen mit $n$ Variablen lassen insbesondere fundamentale Anwendungen in der Theorie der algebraischen Zahlen zu, beim Beweise der Dirichletschen Sätze über die komplexen Einheiten, der Endlichkeit der Anzahl der Idealklassen, und sie haben zuerst den wichtigen Nachweis ermöglicht, daß in der Diskriminante eines jeden algebraischen Zahlkörpers immer mindestens eine Primzahl aufgeht.

V. Es seien $a$ und $b$ irgend zwei reelle Größen und $t$ eine beliebige Größe $> 1$. Die Anwendung der Sätze in III. auf das Parallelepipedum

$$-1 \leqq x - az \leqq 1, \quad -1 \leqq y - bz \leqq 1, \quad -1 \leqq \frac{z}{t} \leqq 1$$

führt dazu, daß es immer ganze Zahlen $x$, $y$, $z$ gibt, für welche

$$0 < z \leqq t^{\frac{2}{3}}, \quad |x - az| < \frac{1}{t^{\frac{1}{3}}}, \quad |y - bz| < \frac{1}{t^{\frac{1}{3}}}$$

ist. Dieses Resultat, jedoch nur für den Fall ganzzahliger Werte von $t$, hat bereits Kronecker (Berichte der Berliner Akademie, 1884, S. 1073; Werke, Bd. III, 1, S. 36) mittels des scheinbar trivialen, dessen ungeachtet aber äußerst erfolgreichen Prinzips (s. Dirichlet, *Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen*; Werke, Bd. I, S. 636) bewiesen, daß, wenn eine Anzahl von Größensystemen in eine kleinere Anzahl von Bereichen fallen, mindestens zwei Systeme darunter in einen und denselben Bereich zu liegen kommen müssen; es ist dies einer der wenigen Fälle, wo bereits dieses einfachere Prinzip wesentlich gleiche Folgerungen ermöglicht wie das arithmetische Theorem in III.

Die Betrachtung des Oktaeders

$$|x - az| + \left|\frac{z}{t}\right| \leqq 1, \quad |y - bz| + \left|\frac{z}{t}\right| \leqq 1$$

($t \geqq 3$ vorausgesetzt), zeigt die Existenz von ganzen Zahlen $x$, $y$, $z$, für welche die Ausdrücke hier links beide $< \left(\frac{3}{t}\right)^{\frac{1}{3}}$ ausfallen und zugleich $z > 0$ ist, und für solche Zahlen findet man dann noch:

$$\left|\frac{x}{z} - a\right| < \frac{2}{3z^{\frac{3}{2}}}, \quad \left|\frac{y}{z} - b\right| < \frac{2}{3z^{\frac{3}{2}}}.$$

Diese Sätze weisen auf einen Weg, auf dem mit Erfolg die Ergebnisse der Lehre von den Kettenbrüchen zu verallgemeinern sind.

VI. Betrachtet man beliebige einhellige und wechselseitige $S(ab)$, so erscheint $2^3$ als kleinste obere Grenze für $M^3 J$. Beschränkt man sich auf solche $S(ab)$, deren Eichkörper aus *einem* gegebenen Körper durch

alle möglichen linearen Transformationen hervorgehen, so findet man auch in dieser beschränkten Klasse von Funktionen bereits immer solche, für welche

$$M^3 J > 1 + \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + \cdots$$

ist. Der Nachweis dieses Satzes erfordert eine arithmetische Theorie der kontinuierlichen Gruppe aus allen linearen Transformationen.

Endlich ist zu erwähnen, daß die Ungleichung $M^3 J \leqq 2^3$ für die nirgends konkaven Körper mit Mittelpunkt noch eine wesentliche Verallgemeinerung zuläßt, auf die ich indes hier nicht mehr eingehen will.

Bonn, im Juni 1893.

## XIII.

# Zur Theorie der Kettenbrüche.*)

(Annales de l'École Normale supérieure, 3e série, t. XIII, pp. 41—60.)

Durch das Studium der Aufsätze von Herrn Hermite in den Bänden 40, 41 und 47 des Crelleschen Journals (Oeuvres, T. I, p. 94, p. 100, p. 164, p. 193, p. 200) bin ich zu einigen Verallgemeinerungen der Theorie der Kettenbrüche geführt, über die ich im folgenden kurz berichten will.

I. Ich werde zunächst von den Annäherungen an *eine einzelne reelle Größe* mittels rationaler Brüche sprechen.

Es sei $\Omega$ irgendein Wert $\geqq 1$. Für eine beliebige reelle Größe $a$, welche weder eine ganze Zahl noch die Hälfte einer ganzen Zahl ist, kann man in folgender Weise eine Folge von ganzen Zahlen $p_n$, $q_n$ $(n = 0, 1, 2, \ldots)$ bestimmen. Zuerst sei $p_0 = 1$, $q_0 = 0$; es sei $f_0$ die nächste ganze Zahl an $a$ und $p_1 = f_0$, $q_1 = 1$. Sodann sei für ein $n \geqq 1$ und solange als $p_n - aq_n \neq 0$ ist, $\varepsilon_n$ das Vorzeichen von $\frac{p_{n-1} - aq_{n-1}}{p_n - aq_n}$, und es werde der absolute Betrag dieses Quotienten $= e_n + r_n$ gesetzt, so daß $e_n$ eine ganze Zahl und $0 \leqq r_n < 1$ ist; hernach mache man $s_n = e_n - \varepsilon_n \frac{q_{n-1}}{q_n}$, und, wenn $r_n = 0$ ist, $f_n = e_n$, wenn aber $r_n > 0$ ist, $f_n = e_n$ oder $= e_n + 1$, je nachdem

$$\text{(A)} \qquad \frac{(s_n+1)^\Omega - 1}{1-(1-r_n)^\Omega} \underset{\leqq}{>} \text{ oder } \frac{s_n{}^\Omega - 1}{1 - r_n{}^\Omega}$$

ist, endlich $p_{n+1} = f_n p_n - \varepsilon_n p_{n-1}$, $q_{n+1} = f_n q_n - \varepsilon_n q_{n-1}$. Man hat alsdann:

$$\frac{p_n}{q_n} = f_0 - \cfrac{\varepsilon_1}{f_1 - \ddots \cfrac{}{f_{n-2} - \cfrac{\varepsilon_{n-1}}{f_{n-1}}}} \qquad (n = 1, 2, \ldots),$$

und die Reihe der Zahlen $p_n$, $q_n$ besitzt folgende Eigenschaften:

---

*) Statt der a. a. O. veröffentlichten, von L. Laugel herrührenden Übersetzung, welche den Titel trägt: *Généralisation de la théorie des fractions continues,* gelangt hier das deutsche Originalmanuskript des Verfassers zum Abdruck. (Anm. d. Herausg.)

1. Wenn $a$ rational ist, bricht die Reihe mit irgendeinem Index $\nu$ ab, für den $\frac{p_\nu}{q_\nu} = a$ ist.

2. Man hat $0 < q_1 < q_2 < \cdots$.

3. Die Zahlen $p_n$ und $q_n$ sind immer relativ prim; man hat

$$p_n q_{n+1} - q_n p_{n+1} = \delta_n = \varepsilon_1 \ldots \varepsilon_n.$$

4. Man setze $t_0 = \infty$, und, wenn $n \geqq 1$ ist,

$$|p_{n-1} - a q_{n-1}|^\Omega + t_n q_{n-1}^\Omega = |p_n - a q_n|^\Omega + t_n q_n^\Omega = T_n;$$

es sind dann $t_0, t_1, t_2, \ldots$ und $T_1, T_2, \ldots$ Reihen von fortwährend abnehmenden positiven Größen, und sie konvergieren nach Null, wenn $a$ irrational ist. Dabei ist immer*)

$$T_n \leqq \frac{\left[\Gamma\left(1+\frac{2}{\Omega}\right)\right]^{\frac{\Omega}{2}}}{\left[\Gamma\left(1+\frac{1}{\Omega}\right)\right]^{\Omega}} \sqrt{t_n}.$$

Ist $a$ rational, so werde noch $t_{\nu+1} = 0$ gesetzt.

5. Ist $t$ irgendein positiver Wert, der nicht in der Reihe $t_0, t_1, t_2, \ldots$ vorkommt, und $t_n > t > t_{n+1}$, und ist $x, y$ irgendein von 0, 0, von $p_n, q_n$ und von $-p_n, -q_n$ verschiedenes System von ganzen Zahlen, so hat man immer

$$|x - a y|^\Omega + t|y|^\Omega > |p_n - a q_n|^\Omega + t|q_n|^\Omega.$$ **)

Besonders bemerkenswert sind folgende Spezialfälle dieser Entwicklung:

1) $\Omega = \infty$. Alsdann hat man für ein $n \geqq 1$ immer $f_n = e_n$, $\varepsilon_{n+1} = -1$, und $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$ sind die Näherungsbrüche der gewöhnlichen Kettenbruchentwicklung für $a$, mit Ausschluß des ersten Näherungsbruches, falls der Überschuß von $a$ über die größte in $a$ enthaltene ganze Zahl $> \frac{1}{2}$ ist.

2) $\Omega = 2$. Die Ungleichungen (A) werden hier

$$\frac{1}{r_n} \begin{matrix} > \\ \text{oder} \\ \leqq \end{matrix} \frac{2s_n + 1}{s_n + 2},$$

und nach der Eigenschaft 5. wird man diejenige Entwicklung in einen Kettenbruch vor sich haben, auf welche Herr Hermite im 41. Bande des Crelleschen Journals, S. 195 (Oeuvres, T. I, p. 108) geführt wurde.

---

*) Vgl. hierzu „Geometrie der Zahlen“ S. 122. (Anm. d. Herausg.)

**) In der französischen Übersetzung findet sich noch folgender Abschnitt:

6. Lorsque a est irrationnel et racine d'une équation du second degré à coefficients rationnels, il existe un indice $l$ et un nombre $\mu$ tels que, à partir de $n = l$, on aura toujours

$$f_n = f_{n+\mu},\ \varepsilon_{n+1} = \varepsilon_{n+1+\mu}.$$ (Anm. d. Herausg.)

3) $\Omega = 1$. Die Ungleichungen (A) gehen dann in

$$\frac{1}{r_n} + \frac{1}{s_n} \begin{matrix} > \\ \text{oder} \\ \leqq \end{matrix} 2$$

über. Man hat immer $T_n \leqq \sqrt{2t_n}$ und tritt hier das Zeichen $=$ nur ein, wenn man $a = \frac{2PQ \mp 1}{2Q^2}$ $(Q > 0)$ hat und dabei $P$, $Q$ ganze Zahlen ohne gemeinsamen Teiler sind, und zwar alsdann nur für einen Index $n$, für welchen $t_n = \frac{1}{2Q^2}$, $q_{n-1} < Q < q_n$ wird. Man wird danach für jeden Index $n$:

$$\left| \frac{p_n}{q_n} - a \right| < \frac{1}{2q_n^2}$$

haben. — Ist weiter $b$ eine beliebige reelle Größe, so erfüllen für mindestens ein System von ganzen Zahlen $X$, $Y$, für die man

$$X - 1 < \frac{q_n b}{\delta_{n-1}} < X + 1, \quad Y - 1 < \frac{-q_{n-1} b}{\delta_{n-1}} < Y + 1$$

hat, $x = p_{n-1} X + p_n Y$, $y = q_{n-1} X + q_n Y$ die Ungleichung:

$$|x - ay - b| + t_n |y| < \sqrt{t_n}.$$

Wenn von den Gleichungen $x - ay = 0$, $x - b = 0$, $x - ay - b = 0$ keine in ganzen Zahlen $x$, $y$ lösbar ist, existieren hiernach unendlich viele verschiedene ganze Zahlen $x$, $y$, für welche

$$y \neq 0, \qquad |x - ay - b| < \frac{1}{4|y|}$$

ist. Dieses Theorem hat Herr Hermite im 88. Bande des Crelleschen Journals, S. 15 (Oeuvres, T. III) mit der weniger scharfen Grenze $\sqrt{\frac{2}{27}}$ an Stelle von $\frac{1}{4}$ gegeben.

II. Nunmehr betrachte ich den folgenden Ausdruck

$$\varphi = \left| \frac{\xi}{\varrho} \right|^\Omega + \left| \frac{\eta}{\sigma} \right|^\Omega + \left| \frac{\zeta}{\tau} \right|^\Omega;$$

darin seien $\xi$, $\eta$, $\zeta$ drei lineare Formen mit drei Variablen $x$, $y$, $z$, mit lauter *reellen* Koeffizienten und einer von Null verschiedenen Determinante $\Delta$, und $\varrho$, $\sigma$, $\tau$ positive Parameter. Indem man anstatt $\xi$, $\eta$, $\zeta$ auch das System $-\xi$, $-\eta$, $-\zeta$ behandeln kann, möge $\Delta > 0$ vorausgesetzt werden. Auf diesen Ausdruck $\varphi$ lassen sich dieselben Gesichtspunkte in Anwendung bringen, die mich zu den Sätzen in I. geführt haben.

Man deute $x$, $y$, $z$ als Parallelkoordinaten (z. B. rechtwinklige) für die Punkte im Raume. Durch die Bedingung $\varphi \leqq 1$ wird dann, so oft $\Omega$ einen Wert $\geqq 1$ hat, jedesmal ein *konvexer* Körper definiert, z. B. für

$\Omega = 1$ ein *Oktaeder*, für $\Omega = 2$ ein *Ellipsoid*, für $\Omega = \infty$ das *Parallelepipedum*, das von den sechs Ebenen

$$\xi = \pm \varrho, \quad \eta = \pm \sigma, \quad \zeta = \pm \tau$$

begrenzt wird. Dieses Parallelepipedum werde ich mit $\{\varrho, \sigma, \tau\}$ bezeichnen und seine drei begrenzenden Ebenenpaare der Reihe nach seine $\xi$-, $\eta$-, $\zeta$-*Seiten* nennen.

Im vorhergehenden trat die gewöhnliche Kettenbruchentwicklung gerade bei der Annahme $\Omega = \infty$ zutage; im folgenden will ich mich deshalb auf diese Annahme beschränken.

1. Das System aller Punkte mit ganzzahligen Koordinaten $x$, $y$, $z$ heiße das *Gitter* und ein einzelner Punkt daraus ein *Gitterpunkt*. Die Substitution $x = -x^*$, $y = -y^*$, $z = -z^*$ führt das Gitter und desgleichen ein jedes $\{\varrho, \sigma, \tau\}$ in sich über. Ein $\{\varrho, \sigma, \tau\}$ heiße *frei*, wenn es in seinem *Inneren* keinen Gitterpunkt außer dem Nullpunkte enthält. Ein freies $\{\varrho, \sigma, \tau\}$, welches diese Eigenschaft bei noch so kleiner Vergrößerung eines beliebigen seiner Parameter jedesmal verliert, werde ein *äußerstes* Parallelepipedum für $\xi$, $\eta$, $\zeta$ genannt; ein solches wird also mit mindestens einem Gitterpunkte im Inneren einer jeden Seitenfläche versehen sein müssen. Nach einem Satze, den ich im Bulletin des Sciences mathématiques, janvier 1893, *Lettre à M. Hermite* (diese Ges. Abhandlungen Bd. I, S. 266) zum ersten Male ausgesprochen habe, hat man in einem freien $\{\varrho, \sigma, \tau\}$ immer

$$\varrho\sigma\tau \leqq \Delta,$$

d. h. ein $\{\varrho, \sigma, \tau\}$, wofür $\varrho\sigma\tau = \Delta$ ist, muß immer außer dem Nullpunkte noch weitere Gitterpunkte, sei es im Inneren, sei es nur an der Grenze, enthalten. Auf diesen Umstand kann man die Ermittlung eines äußersten $\{\varrho, \sigma, \tau\}$ gründen.

2. Eine lineare Substitution werde ich hier, ohne die Variablen zu benennen, bloß durch das quadratische System der Koeffizienten bezeichnen, wobei aus den einzelnen Gleichungen die Horizontalreihen entstammen sollen; und ein System von linearen Formen denke man sich zum Zwecke seiner Bezeichnung als eine lineare Substitution.

Um einige Besonderheiten auszuschließen, deren Berücksichtigung nur etwas mehr Raum erfordern, aber keinerlei Schwierigkeiten bereiten würde, setze ich von nun an voraus, *daß von den drei Formen $\xi$, $\eta$, $\zeta$ keine einzige für ganzzahlige Werte $x$, $y$, $z$ außer für* 0, 0, 0 *verschwinde.* Es gelten dann folgende Sätze:

*Ist $\{a, g, l\}$ ein äußerstes Parallelepipedum für $\xi$, $\eta$, $\zeta$, so hat man immer*

(1) $$agl < \Delta.$$

*Es enthält $\{a, g, l\}$ genau einen Gitterpunkt auf jeder Seitenfläche, auf den gegenüberliegenden Flächen Gitterpunkte mit entgegengesetzten Koordinaten. Man kann darunter immer auf eine und nur eine Weise drei Gitterpunkte $r, s, t$; $r', s', t'$; $r'', s'', t''$ auf nicht gegenüberliegenden Flächen $\xi = \varepsilon a$, $\eta = \varepsilon' g$, $\zeta = \varepsilon'' l$ finden, so daß $\varepsilon\varepsilon'\varepsilon'' = +1$ ist, und wenn das System $\varepsilon\xi$, $\varepsilon'\eta$, $\varepsilon''\zeta$ durch*

$$P = \begin{pmatrix} r, & r', & r'' \\ s, & s', & s'' \\ t, & t', & t'' \end{pmatrix} \quad in \quad \Phi = \begin{pmatrix} a, & \pm b, & \pm c \\ \pm f, & g, & \pm h \\ \pm j, & \pm k, & l \end{pmatrix}$$

*übergeht, die Größen $a, b, c, f, g, h, j, k, l$ sämtlich positiv sind und ihre Vorzeichen eines der folgenden sechs Systeme ergeben:*

| I. | II. | III. | IV. | V. | VI. |
|---|---|---|---|---|---|
| $+\ +\ +$ | $+\ -\ -$ | $+\ -\ -$ | $+\ +\ -$ | $+\ -\ +$ | $+\ -\ -$ |
| $-\ +\ -$ | $+\ +\ +$ | $-\ +\ -$ | $-\ +\ +$ | $+\ +\ -$ | $-\ +\ -$ |
| $-\ -\ +$ | $-\ -\ +$ | $+\ +\ +$ | $+\ -\ +$ | $-\ +\ +$ | $-\ -\ +$ |

*Dabei erweist sich dann die Determinante von $P$ in den Fällen* I. *bis* V. *gleich* 1, *im Falle* VI. *gleich* 0, *und hat man*

(2) $$a > b, \quad a > c; \quad g > h, \quad g > f; \quad l > j, \quad l > k,$$

*und dazu noch je nach den einzelnen Fällen, die hier durch ihre Nummer kenntlich gemacht sind, folgende weitere Bedingungen:*

| I. | II. | III. |
|---|---|---|
| $b + c > a$, $f > h$ oder $j > k$ | $h + f > g$, $k > j$ oder $b > c$ | $j + k > l$, $c > b$ oder $h > f$ |

| IV. | V. | VI. |
|---|---|---|
| $b > c$ oder $h > f$ oder $j > k$ | $c > b$ oder $f > h$ oder $k > j$ | $b + c = a$, $h + f = g$, $j + k = l$. |

Von den hier durch das Wort *oder* verbundenen zwei oder drei Bedingungen hat jedesmal *wenigstens eine* statt.

Es heiße $\{a, g, l\}$ in den Fällen I.—V. von der *ersten*, im Falle VI. von der *zweiten Art*, und von der Substitution $P$, welche ihrerseits $\{a, g, l\}$ vollkommen bestimmt, sage man, sie sei eine zu $\xi$, $\eta$, $\zeta$ *gehörende* Substitution.

*Ist eine ganzzahlige Substitution $P$ mit der Determinante* 1 *so beschaffen, daß durch sie $\varepsilon\xi$, $\varepsilon'\eta$, $\varepsilon''\zeta$ mit geeigneten Vorzeichen $\varepsilon$, $\varepsilon'$, $\varepsilon''$ in ein System $\Phi$ übergehen, welches eine der vorstehenden Bedingungen* I. *bis* V. *erfüllt, so ist sie stets eine zu $\xi$, $\eta$, $\zeta$ gehörende Substitution.*

3. Man bilde für ein äußerstes $\{a, g, l\}$ die Systeme $P$ und $\Phi$. Ist darin $b > c$, so befindet sich in $\{b, g, l\}$ der Gitterpunkt $r', s', t'$ auf dem

*Rande* einer $\xi$- und einer $\eta$-Seite und der Gitterpunkt $r''$, $s''$, $t''$ im *Inneren* einer $\zeta$-Seite. Es muß dann $\left\{b, \frac{\Delta}{bl}, l\right\}$, dem in (1) liegenden Satze zufolge, ein bestimmtes äußerstes $\{b, g_1, l\}$ mit einem Parameter $g_1 > g$ enthalten, und dieses wird dann *unter allen möglichen äußersten* $\{a_0, g_0, l_0\}$, *in welchen* $g_0 \geqq g$, $l_0 \geqq l$ *und* $a_0 < a$ *ist, dasjenige mit größtem Parameter* $a_0$ sein. Wenn $b < c$ ist, kommt die nämliche Eigenschaft einem gewissen äußersten $\{c, g, l_1\}$ $(l_1 > l)$ zu. Dieses so in jedem Falle bestimmte $\{b, g_1, l\}$, beziehlich $\{c, g, l_1\}$ heiße *der* $\xi$-*Nachbar von* $\{a, g, l\}$. Zu diesem $\xi$-Nachbar kann man wieder den $\xi$-Nachbar bilden usf. ins Unendliche, dabei kommt man offenbar auf lauter verschiedene äußerste Parallelepipeda für $\xi$, $\eta$, $\zeta$. Analog kann man sodann einen $\eta$-*Nachbar* und einen $\zeta$-*Nachbar* von $\{a, g, l\}$ definieren. $\{a, g, l\}$ selbst wird, je nachdem $b > c$ oder $b < c$ ist, der $\eta$-Nachbar oder der $\zeta$-Nachbar seines $\xi$-Nachbars sein. Nun besteht der folgende Hauptsatz:

*Von einem beliebigen äußersten Parallelepipedum für* $\xi$, $\eta$, $\zeta$ *ausgehend kommt man durch fortgesetzte Bildung aller Nachbarn zu allen vorhandenen äußersten Parallelepipeda für* $\xi$, $\eta$, $\zeta$.

Denn es seien irgend zwei verschiedene äußerste Parallelepipeda $\{a, g, l\}$ und $\{a_0, g_0, l_0\}$ gegeben. Da keines im anderen enthalten sein kann, ist bei jedem mindestens ein Parameter größer und also auch bei einem nur *ein* Parameter größer; so sei etwa $a > a_0$, $g < g_0$, $l \leqq l_0$. Die beiden Parallelepipeda haben dann $\Pi = \{a_0, g, l\}$ gemeinsam. Man bilde das System $P$ für $\{a, g, l\}$; der Punkt $r'$, $s'$, $t'$ darin kann nicht im *Inneren* von $\{a_0, g_0, l_0\}$ liegen und ist daher $b \geqq a_0$. Wenn nun $b > c$ oder aber $b < c$ und dabei $l < l_0$ ist, wird der $\xi$-Nachbar von $\{a, g, l\}$, der dann $\{b, g_1, l\}$ $(g_1 > g)$ oder $\{c, g, l_1\}$ $(l_1 > l)$ lautet, mit $\{a_0, g_0, l_0\}$ ein Parallelepipedum $\Pi_1$ gemein haben, *welches* $\Pi$ *enthält und dabei größer ist.* Ist aber $b < c$ und zugleich $l = l_0$, so hat der $\xi$-Nachbar von $\{a, g, l\}$, der dann $\{c, g, l_1\}$ $(l_1 > l)$ lautet, zwar mit $\{a_0, g_0, l_0\}$ wieder nur $\Pi$, aber, indem dann $c > a_0$, $g < g_0$, $l_1 > l_0$ ist, dem eben behandelten Falle gemäß, mit dem $\eta$-Nachbar von $\{a_0, g_0, l_0\}$ gewiß ein Parallelepipedum $\Pi_1$ gemein, *das* $\Pi$ *enthält und dabei größer ist.* Die zwei Parallelepipeda, die hier jedesmal auf das mit $\Pi_1$ bezeichnete Parallelepipedum führen, können nun identisch sein, anderenfalls operiere man mit ihnen wie mit den beiden, von welchen man ausging, usw. Dem in (1) enthaltenen Satze zufolge muß nun jedes äußerste Parallelepipedum, das $\Pi$ enthält, ganz im Inneren von $\left\{\frac{\Delta}{gl}, \frac{\Delta}{la_0}, \frac{\Delta}{a_0 g}\right\}$ liegen. Für die drei Parameter bei $\Pi$, $\Pi_1$, usw. kommen daher nur eine endliche Anzahl von Werten in Frage, und eine *endliche* Anzahl von Schritten, wie der hier bezeichnete, muß zu einer

vollständigen Verbindung von $\{a, g, l\}$ und $\{a_0, g_0, l_0\}$ durch Nachbarn führen.

Es bilden so alle vorhandenen äußersten $\{a, g, l\}$ eine bestimmte *Kette, in welcher an jedem Gliede in gewisser Weise unmittelbar seine drei Nachbarn haften und dadurch ein Zusammenhang aller Glieder zustande kommt.*

*Man findet die Nachbarn eines äußersten $\{a, g, l\}$ zweiter Art stets sämtlich von der ersten Art.* Um die ganze zu $\xi, \eta, \zeta$ gehörige Kette von äußersten Parallelepipeda zu bilden, wird man nun von einem Gliede der ersten Art in ihr ausgehen; dann bedarf man nur des *Algorithmus*, durch den man von einem äußersten $\{a, g, l\}$ *der ersten Art* zu einem beliebigen Nachbar, und, falls dieser von der zweiten Art wird, weiter direkt zu den Nachbarn dieses Nachbars gelangt. Man bilde die Systeme $P$ und $\Phi$ für $\{a, g, l\}$, und es sei

$$\begin{pmatrix} A, & F, & J \\ B, & G, & K \\ C, & H, & L \end{pmatrix}$$

das adjungierte System zu $\Phi$, das System, welches symbolisch durch $\Delta\Phi^{-1}$ anzudeuten wäre. Es wird hinreichen, den $\xi$-Nachbar von $\{a, g, l\}$ und noch unter der Annahme $b > c$ zu behandeln, indem die übrigen möglichen Fälle aus diesem durch die geeigneten Permutationen von $\xi, \eta, \zeta$ und der zugehörigen Bezeichnungen hervorgehen; dabei ist zu beachten, daß in $\Phi$ den Formen $\xi, \eta, \zeta$ nicht bloß die Horizontalreihen, sondern ebenso die Vertikalreihen einzeln zugeordnet sind.

Man erhält, wenn $b > c$ ist, den $\xi$-Nachbar von $\{a, g, l\}$ durch den nachstehend dargestellten Algorithmus. Voran steht dabei jedesmal, welcher von den Fällen I. bis V. aus 2. bei dem Systeme $\Phi$ zutreffen soll. Die Klammer [ ] dient in der bekannten Weise als Zeichen für *größte Ganze.* Die aufgeschriebene Substitution ist jedesmal die, mit welcher $P$ rechts zu multiplizieren ist, um die zu dem $\xi$-Nachbar gehörende Substitution zu erhalten; die drei Einheiten daneben sind die Quotienten aus den Einheiten $\varepsilon, \varepsilon', \varepsilon''$ für den $\xi$-Nachbar und für $\{a, g, l\}$; die römische Nummer darunter besagt, welche von den sechs Vorzeichenkombinationen aus 2. sich bei dem $\xi$-Nachbar einstellt.

### *Fall* II. *und Fall* V.

Von den doppelten Vorzeichen bezieht sich das obere auf den Fall II., das untere auf den Fall V.

$$\left[\frac{G}{F}\right] = M, \quad \left[\frac{\pm H}{F}\right] = N; \quad a - bM - cN = u, \quad \pm j + kM - lN = v.$$

| | | | $m$ | $n$ | $\delta$ |
|---|---|---|---|---|---|
| 1) | $u < c,$ | $v > k$ | $M-1$ | $N+1$ | $+1$ |
| 2) | $u < b-c,$ | $v < 0$ | $M$ | $N-1$ | $-1$ |
| 3), 4) | $u < b,$ aber nicht 1) noch 2) | | $M$ | $N$ | |
| | | 3) $v > 0$ | | | $-1$ |
| | | 4) $v < 0$ | | | $+1$ |
| 5) | $u > b,$ | $v > 0$ | $M$ | $N+1$ | $+1$ |
| 6) | $u > b,$ | $v < 0$ | $M+1$ | $N$ | $-1$ |

$$\begin{pmatrix} 0, & \mp\delta, & 0 \\ \pm\delta, & \mp\delta m, & 0 \\ 0, & -\delta n, & 1 \end{pmatrix} \quad \mp\delta, \mp\delta, +1;$$

$\delta = +1$, I.; $\delta = -1$, IV.

*Fall* I.

1) $j > k,$

$$\begin{pmatrix} 0, & -1, & 0 \\ 1, & 1, & 0 \\ 0, & 0, & 1 \end{pmatrix} \quad +, +, +;$$

V.

2) $j < k,$

$$\begin{pmatrix} 0, & 1, & 0 \\ 1, & -1, & 0 \\ 0, & -1, & -1 \end{pmatrix} \quad +, -, -;$$

III.

*Fall* III.

1) $a + c < 2b,$

$$\begin{pmatrix} 0, & 1, & 0 \\ 1, & 1, & 0 \\ 0, & -1, & -1 \end{pmatrix} \quad -, +, -;$$

II.

*Fall* IV.

1) $a < 2b,\ f < h,\ j + k < l,$

$$\begin{pmatrix} 0, & -1, & 0 \\ 1, & 1, & 0 \\ 0, & 0, & 1 \end{pmatrix} \quad +, +, +;$$

II.

*Fall* III., 2) *und Fall* IV., 2).

Die Bedingungen bei 1) sollen alsdann nicht erfüllt sein. Von den doppelten Vorzeichen bezieht sich im folgenden durchweg das obere auf den Fall III., das untere auf den Fall IV.

$$\begin{pmatrix} 0, & 0, & 0 \\ -1, & 1, & 0 \\ 0, & \mp 1, & \pm 1 \end{pmatrix} \quad \pm, +, \pm; \qquad \text{VI.}$$

Von der zweiten Art wird also der $\xi$-Nachbar nur unter diesen letzten Umständen. Alsdann ist der Weg, um von $\{a, g, l\}$ direkt zu den Nachbarn des $\xi$-Nachbars überzugehen, durch folgende Tabelle vorgezeichnet. Darin haben jedesmal die hingeschriebene Substitution, die daneben stehenden Einheiten und römischen Ziffern dieselbe Bedeutung für das gesuchte Parallelepipedum, wie die entsprechenden Zeichen oben für den $\xi$-Nachbar. Die Herleitung von $m, n, \delta$ hat in den späteren Fällen nach derselben Regel wie im ersten Falle zu erfolgen.

*Algorithmus für den $\xi$-Nachbar des $\xi$-Nachbars.*

1) $b - c > c$;

$$\left[\frac{\pm G}{F}\right] = M, \qquad \left[\frac{\pm G + H}{F}\right] = N;$$

$$a - (b-c)M - cN = u, \qquad -j + (l-k)M - lN = v;$$

$$b - c = u^0, \qquad c = u', \qquad l - k = v'.$$

| | | | $m$ | $n$ | $\delta$ |
|---|---|---|---|---|---|
| 1) | $u < u'$, | $v > v'$ | $M-1$ | $N+1$ | $+1$ |
| 2) | $u < u'$, | $v' > v > 0$ | $M$ | $N+1$ | $-1$ |
| 3) | $u > u'$, | $v > 0$ | $M$ | $N+1$ | $+1$ |
| 4) | $u < u^0$, | $v < 0$ | $M$ | $N$ | $+1$ |
| 5) | $u > u^0$, | $v < 0$ | $M+1$ | $N+1$ | $-1$ |

$$\begin{pmatrix} 0, & \mp\delta, & 0 \\ -1, & -\delta m, & 0 \\ \pm 1, & \pm\delta(m-n), & \mp\delta \end{pmatrix} \quad \begin{matrix} \pm 1, & -\delta, & \mp\delta; \\ \delta = +1, & \text{V.}; & \delta = -1, \quad \text{III.} \end{matrix}$$

2) $b - c < c$;

$$\left[\frac{\pm K + L}{J}\right] = M, \qquad \left[\frac{\pm K}{L}\right] = N;$$

$$a - cM - (b-c)N = u, \qquad \pm f + hM - (g+h)N = v;$$

$$c = u^0, \qquad b - c = u', \qquad h = v'.$$

$$\begin{pmatrix} 0, & 0, & \mp\delta \\ 0, & -\delta, & -\delta n \\ \mp 1, & \pm\delta, & \mp\delta(m-n) \end{pmatrix} \quad \begin{matrix} \pm 1, & -\delta, & \mp\delta; \\ \delta = +1, & \text{IV.}; & \delta = -1, \quad \text{II.} \end{matrix}$$

*Der $\eta$-Nachbar des $\xi$-Nachbars* ist $\{a, g, l\}$ selbst.

*Algorithmus für den $\xi$-Nachbar des $\xi$-Nachbars.*

1) $k < l - k$;

$$\left[\frac{-H}{F}\right] = M, \qquad \left[\frac{\mp G - H}{F}\right] = N;$$

$$j - (l-k)M - kN = u, \qquad -a + (b-c)M - bN = v;$$

$$l - k = u^0, \qquad k = u', \qquad b - c = v'.$$

$$\begin{pmatrix} 0, & \mp\delta, & 0 \\ \delta, & -\delta(m-n), & -1 \\ 0, & \pm\delta m, & \pm 1 \end{pmatrix} \qquad \begin{matrix} \mp\delta, & -\delta, & \pm 1; \\ \delta = +1, & \text{IV.}; & \delta = -1, \quad \text{I.} \end{matrix}$$

2) $k > l - k$;

$2)_1$ $j > k$,

$$\begin{pmatrix} \pm 1, & 0, & 0 \\ 0, & 1, & 1 \\ \mp 1, & \mp 1, & 0 \end{pmatrix} \qquad \underset{\text{II.}}{\pm, +, \pm};$$

$2)_2$ $j < k$,

im Falle III., 2):

$$\begin{pmatrix} -1, & 0, & 0 \\ -1, & -1, & 1 \\ 1, & 1, & 0 \end{pmatrix} \qquad \underset{\text{V.}}{-, -, +};$$

im Falle IV., 2):

$$\begin{pmatrix} 1, & 0, & 0 \\ 0, & -1, & 1 \\ 0, & -1, & 0 \end{pmatrix} \qquad \underset{\text{V.}}{+, -, -};$$

4. Es sei ein reeller algebraischer Zahlkörper dritten Grades $\Theta$ gegeben, dessen konjugierte Körper $\Theta'$, $\Theta''$ ebenfalls reell sind, also mit einer *positiven* Diskriminante $D$. Es seien $\alpha, \beta, \gamma$ drei ganze Zahlen aus $\Theta$ von solcher Art, daß die Form $\xi = \alpha x + \beta y + \gamma z$ für die rationalen ganzzahligen Werte von $x, y, z$ *alle* ganzen Zahlen aus $\Theta$ darstellt; $\eta = \xi'$ und $\zeta = \xi''$ seien die konjugierten Formen zu $\xi$ in den Körpern $\Theta'$ und $\Theta''$. Die Determinante von $\xi, \eta, \zeta$ ist dann $\sqrt{D}$, und zwar möge sie gleich dem positiven Werte dieser Wurzel angenommen werden, indem auch $-\alpha, -\beta, -\gamma$ die Stelle von $\alpha, \beta, \gamma$ übernehmen können. Das Produkt $\xi\eta\zeta = Nm\xi$ ist eine Form in $x, y, z$ mit lauter *rationalen ganzzahligen* Koeffizienten von der Diskriminante $D$. Wendet man auf diese Form eine Substitution $P$ der zu $\xi, \eta, \zeta$ gehörigen Kette an, so entsteht eine Form $\varphi$, wieder mit rationalen ganzzahligen Koeffizienten, von der Diskriminante $D$ oder 0, je nachdem die Determinante von $P$ Eins oder Null ist; dabei ergeben sich aus den Ungleichungen 2.(1) und 2.(2) gewisse, nur von $D$ abhängige obere Grenzen für die Beträge aller Koeffizienten in $\varphi$. *Es gehen danach aus $Nm\xi$ durch die sämtlichen unendlich vielen Substitutionen $P$ überhaupt nur eine endliche Anzahl verschiedener Formen*

$\varphi$ *hervor.* Unter einer *Einheit* des Körpers $\Theta$ soll eine *ganze* Zahl aus $\Theta$ mit der Norm 1 verstanden werden.

Es seien nun $P$ und $Q$ *zwei verschiedene* Substitutionen der Kette zu $\xi, \eta, \zeta$, welche $\xi\eta\zeta$ in *ein und dieselbe* Form $\varphi$ transformieren. Durch $P$ mögen $\xi, \eta, \zeta$ in $\Xi, \mathsf{H}, \mathsf{Z}$ übergehen; durch $Q$ müssen dann $\xi, \eta, \zeta$ in dieselben Formen bis auf Faktoren übergehen, und dabei kann mit Rücksicht auf die Ungleichungen 2.(2) auch *keine Änderung in der Reihenfolge der Formen* eintreten, so daß aus $\xi, \eta, \zeta$ durch $Q$ der Reihe nach wird $\omega\Xi$, $\omega'\mathsf{H}$, $\omega''\mathsf{Z}$. Dabei erweisen sich dann $\omega, \omega', \omega''$ als konjugierte Zahlen aus den Körpern $\Theta, \Theta', \Theta''$ und hat man $\omega\omega'\omega'' = 1$. Der Faktor $\omega$ wird also eine Einheit darstellen, sowie er eine *ganze* algebraische Zahl ist. Dies wird nun immer der Fall sein, wenn $P$ und $Q$ die Determinante 1 haben. Denn alsdann geht durch $QP^{-1}$ das System $\xi, \eta, \zeta$ in $\omega\xi$, $\omega'\eta$, $\omega''\zeta$, und also, wenn $E$ die identische Substitution, $w$ einen unbestimmten Parameter bedeutet, durch $QP^{-1} - wE$ (bei Anwendung einer bekannten Symbolik) $\xi, \eta, \zeta$ in $(\omega - w)\xi$, $(\omega' - w)\eta$, $(\omega'' - w)\zeta$ über; danach ist die Determinante von $QP^{-1} - wE$ gleich $(\omega - w)(\omega' - w)(\omega'' - w)$ und diese Relation erweist $\omega$ als ganze Zahl.

Auf zwei verschiedene Substitutionen $P$ und $Q$ von der Determinante 1, welche $Nm\xi$ in ein und dieselbe Form $\varphi$ transformieren, wird man z. B. mit Hilfe einer hinreichend verlängerten solchen Reihe von äußersten Parallelepipeda kommen können, in welcher jedes Parallelepipedum der $\xi$-Nachbar des vorhergehenden ist. Dabei stellt sich dann offenbar eine Einheit $\omega$ heraus, für welche von den Beträgen der Zahlen $\omega, \omega', \omega''$ der erste $< 1$, der zweite und dritte $> 1$ sind. Analog kann man eine Einheit $\omega$ finden, für welche von diesen Beträgen der zweite $< 1$, der dritte und erste $> 1$, oder endlich der dritte $< 1$, der erste und zweite $> 1$ sind. Es leuchtet ein, daß von solchen drei Einheiten je zwei immer *unabhängig,* d. h. nicht als Potenzen einer einzigen Einheit darstellbar sind.

Durch eine Substitution $O$ von der Determinante 1 geht das Gitter immer in sich selbst über, und wird aus einem äußersten Parallelepipedum mit einer Substitution $P$ daher wieder ein äußerstes Parallelepipedum, mit der Substitution $O^{-1}P$, das freilich nicht derselben Kette anzugehören braucht. Ist andererseits $\omega$ eine ganze Zahl aus $\Theta$, so geht immer $\omega\xi$ aus $\xi$ durch eine bestimmte ganzzahlige Substitution $O$ hervor; durch dieselbe geht dann $\omega'\eta$ aus $\eta$ und $\omega''\zeta$ aus $\zeta$ hervor, und wird dabei die Determinante von $O$ also gleich $\omega\omega'\omega''$, d. i. gleich 1, sowie $\omega$ eine Einheit vorstellt. Daraus ersieht man nun: *Ist* $\{\lambda, \mu, \nu\}$ *irgendein äußerstes Parallelepipedum für* $\xi, \eta, \zeta$, $P$ *die dazu gehörige Substitution,* $\omega$ *irgendeine Einheit aus* $\Theta$, $O$ *die ganzzahlige Substitution, welche* $\xi$ *in* $\omega\xi$ *transformiert,*

*so ist auch* $\left\{\frac{\lambda}{|\omega|}, \frac{\mu}{|\omega'|}, \frac{\nu}{|\omega''|}\right\}$ *immer ein äußerstes Parallelepipedum für* $\xi, \eta, \zeta$, *es gehört dazu die Substitution* $O^{-1}P$ *und transformiert diese* $Nm\,\xi$ *in genau dieselbe Form* $\varphi$ *wie* $P$. Zwei in der hier erörterten Beziehung zueinander stehende äußerste Parallelepipeda mögen *äquivalent* heißen.

Es entspringt daraus nun folgendes Verfahren, *alle* Einheiten des Körpers $\Theta$ zu finden. Man gehe von irgendeinem äußersten Parallelepipedum für $\xi, \eta, \zeta$ aus, bilde die Form $\varphi$ dazu, konstruiere einen Nachbar, bilde die Form $\varphi$ für ihn, und man setze immer von den erhaltenen Parallelepipeda aus die Bildung von Nachbarn und der Formen $\varphi$ dazu fort, soweit als dies angeht, ohne daß man zwei Parallelepipeda erster Art mit derselben Form $\varphi$ und zudem beide mit zwei gleichbenannten Nachbarn in der Reihe hat. Man kommt so notwendig auf eine begrenzte Anzahl von äußersten Parallelepipeda, welche man eine *Fundamentalreihe* für die zu $\xi, \eta, \zeta$ gehörige Kette nennen kann. Man bilde nun für zwei unter den erhaltenen Parallelepipeda $\{\lambda, \mu, \nu\}$, welchen dieselbe Form $\varphi$ entspricht, immer den Quotienten aus ihren Parametern $\lambda$; falls dieser eine ganze Zahl wird, stellt er, mit einem geeigneten Vorzeichen versehen, eine Einheit vor; man kommt so auf eine endliche Anzahl von Einheiten, aus welchen durch Multiplikation und Division alle vorhandenen Einheiten des Körpers $\Theta$ abzuleiten sind. Es müssen sich nach dem Obigen darunter gewiß zwei unabhängige Einheiten finden, und kann man immer leicht auch zwei solche Einheiten ermitteln, aus welchen allein schon durch Multiplikation und Division *alle* Einheiten hervorgehen. —

Der in diesem Aufsatze dargelegte Algorithmus, um die Einheiten in einem kubischen Körper mit positiver Diskriminante zu finden, ist durchaus analog der Lösung der Pellschen Gleichung durch Bildung einer Periode reduzierter indefiniter binärer quadratischer Formen, wofern man die Reduktionsbedingungen von Gauß verwendet. Auf die kubischen Körper mit negativer Diskriminante kann ich an dieser Stelle nicht mehr eingehen.

Der einfachste Körper $\Theta$ wird durch $2\cos\frac{2\pi}{7}$ bestimmt*); $\vartheta = 2\cos\frac{2\pi}{7}$, $\vartheta' = 2\cos\frac{4\pi}{7}$, $\vartheta'' = 2\cos\frac{6\pi}{7}$ sind drei konjugierte *ganze* algebraische Zahlen; sie haben angenähert die Werte

$$\vartheta = 1{,}25, \qquad \vartheta' = -0{,}45, \qquad \vartheta'' = -1{,}80$$

*) In der Abhandlung *De la réduction des formes quadratiques ternaires positives et de son application aux irrationnelles du troisième degré* (Annales de l'École Normale supérieure, 2e série, supplément au tome IX) hat Herr L. Charve unter anderen Beispielen diesen Körper ebenfalls behandelt.

und sind danach die Wurzeln der Gleichung

$$\vartheta^3 + \vartheta^2 - 2\vartheta - 1 = 0.$$

Die Diskriminante dieser Gleichung ist 49, also ein Quadrat, $\Theta$ somit ein Abelscher Körper. Man hat

$$(\vartheta' - \vartheta)(\vartheta'' - \vartheta)(\vartheta'' - \vartheta') = -7,$$

und entnimmt daraus

$$\vartheta' = \vartheta^2 - 2, \qquad \vartheta'' = -\vartheta^2 - \vartheta + 1$$

und die aus diesen durch zyklische Permutation von $\vartheta$, $\vartheta'$, $\vartheta''$ hervorgehenden Relationen. Man kann nun oben

$$\alpha, \beta, \gamma = -1, \quad -\vartheta, \quad -\vartheta^2$$

nehmen. Dann sind die Koeffizienten in $\xi$, $\eta$, $\zeta$:

$$\begin{pmatrix} -1, & -1{,}25, & -1{,}55 \\ -1, & 0{,}45, & -0{,}20 \\ -1, & 1{,}80, & -3{,}25 \end{pmatrix}.$$

Es gehen jetzt $-\xi$, $-\eta$, $\zeta$ durch

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

in

$$\Phi = \begin{pmatrix} 1{,}25, & 1, & -0{,}55 \\ -0{,}45, & 1, & 0{,}80 \\ 1{,}80, & -1, & 2{,}25 \end{pmatrix} = \begin{pmatrix} \vartheta, & 1, & 1-\vartheta^2 \\ \vartheta', & 1, & 1-\vartheta'^2 \\ -\vartheta'', & -1, & -1+\vartheta''^2 \end{pmatrix}$$

über. Dieses System $\Phi$ genügt den Bedingungen 2. IV. und ist somit $\{\vartheta, 1, -1+\vartheta''^2\} = (\Phi)$ ein äußerstes Parallelepipedum zu $\xi$, $\eta$, $\zeta$ und $P$ die dazu gehörige Substitution. Es geht sodann $\xi\eta\zeta$ durch $P$ in

$$\varphi = -x^3 - y^3 - z^3 + 2x^2y + 2y^2z + 2z^2x + xy^2 + yz^2 + zx^2 + xyz$$

über. Der Umstand, daß diese Form $\varphi$ bei den zyklischen Permutationen von $x$, $y$, $z$ ungeändert bleibt, setzt in Evidenz, daß $\Theta$ ein Abelscher Körper ist. *Man nimmt hier auch sofort eine charakteristische Eigenschaft aller in analoger Weise in bezug auf Abelsche Körper gebildeten Ketten wahr.*

Bei der Bestimmung des $\xi$-, wie des $\eta$-, wie des $\zeta$-Nachbars von $(\Phi)$ wird nun jedesmal die gleiche Regel Anwendung finden, hier die Regel für den Fall IV., 2), so daß diese Nachbarn sämtlich von der zweiten Art werden. Dabei wird aus $\Phi$:

$$\Psi = \begin{pmatrix} 1, & -0{,}45, & -0{,}55 \\ -1, & 1{,}80, & -0{,}80 \\ -1, & -1{,}25, & 2{,}25 \end{pmatrix}$$

$$\Psi' = \begin{pmatrix} 1{,}25, & -0{,}55, & -0{,}70 \\ -0{,}45, & 0{,}80, & -0{,}35 \\ -1{,}80, & -2{,}25, & 4{,}05 \end{pmatrix}$$

$$\Psi'' = \begin{pmatrix} 2{,}25, & -1, & -1{,}25 \\ -0{,}55, & 1, & -0{,}45 \\ -0{,}80, & -1, & 1{,}80 \end{pmatrix},$$

und $\varphi$ geht jedesmal in dieselbe Form

$$\psi = x^3 + y^3 + z^3 - x^2y - y^2z - z^2x - 2xy^2 - 2yz^2 - 2zx^2 + 2xyz$$

von der Diskriminante Null über. Der $\xi$-Parameter in den zugehörigen äußersten Parallelepipeda $(\Psi)$, $(\Psi')$, $(\Psi'')$ ist $1$, $\vartheta$, $1+\vartheta$, und indem die Quotienten dieser Größen sich als ganze Zahlen erweisen, sind diese Parallelepipeda äquivalent. Nun ist umgekehrt $(\Phi)$ der $\eta$-, $\zeta$-, $\xi$-Nachbar von $(\Psi)$, $(\Psi')$, $(\Psi'')$ und werden daher alle Nachbarn von $(\Psi)$, $(\Psi')$, $(\Psi'')$ mit $(\Phi)$ äquivalente Parallelepipeda sein. In $(\Phi)$, $(\Psi)$, $(\Psi')$, $(\Psi'')$ hat man somit bereits eine Fundamentalreihe der zu $\xi, \eta, \zeta$ gehörigen Kette erlangt, und man kommt zu dem Resultate, daß die Einheiten $\vartheta$, $\frac{-1}{1+\vartheta} = \vartheta'$, $\frac{-1-\vartheta}{\vartheta} = \vartheta''$, zwischen denen noch die Beziehung $\vartheta\vartheta'\vartheta'' = 1$ besteht, durch ihre Potenzen und deren Produkte alle Einheiten des Körpers $\Theta$ ergeben. Es entsprechen diesen Einheiten die Transformationen

$$\begin{pmatrix} 0, & 1, & -1 \\ 1, & 0, & 0 \\ -1, & 0, & -1 \end{pmatrix}, \quad \begin{pmatrix} 0, & 0, & 1 \\ 0, & -1, & -1 \\ 1, & -1, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, & -1, & 0 \\ -1, & 0, & 1 \\ 0, & 1, & 0 \end{pmatrix}$$

der Form $\varphi$ in sich selbst. —

Mit leichten Modifikationen lassen sich die Sätze der Abschnitte 2. und 3. auch auf solche lineare Formen ausdehnen, durch welche die Null rational darstellbar ist. Für drei Formen von der besonderen Gestalt

$$x + ay + bz, \quad y + cz, \quad z$$

hat man offenbar immer in $\{1, 1, 1\}$ ein äußerstes Parallelepipedum und damit einen ganz bestimmten Ausgangspunkt für die zu den Formen gehörige Kette. Aus den Sätzen dieses Abschnittes entnimmt man leicht, daß, wenn $\alpha, \beta, \gamma, \xi, \eta, \zeta$ die oben festgesetzte Bedeutung für den kubischen Körper $\Theta$ haben, jede Substitution $P$ der zu $\xi, \eta, \zeta$ gehörenden Kette, in deren Parallelepipedum $\{\lambda, \mu, \nu\}$ die Quotienten $\frac{\mu}{\lambda}$, $\frac{\nu}{\mu}$ gewisse Größen

übersteigen, auch in der zu den Formen

$$x + \frac{\beta}{\alpha} y + \frac{\gamma}{\alpha} z, \qquad y + \frac{\alpha\gamma' - \alpha'\gamma}{\alpha\beta' - \alpha'\beta} z, \qquad z$$

gehörigen Kette auftreten muß. Derjenige Satz, welcher diesem bei zwei linearen Formen entspricht, ist genau der Satz von Lagrange, daß für eine reelle quadratische Irrationalzahl die Entwicklung in einen gewöhnlichen Kettenbruch sich periodisch gestaltet.

Ich werde bei nächster Gelegenheit auf die Untersuchung dreier Formen von der Gestalt

$$x - az, \qquad y - bz, \qquad z,$$

worin $a$, $b$ beliebige reelle Größen sind, und eine andere, damit zusammenhängende und weit bemerkenswertere Verallgemeinerung dieses Satzes von Lagrange zurückkommen.

Königsberg, den 15. Oktober 1894.

XIV.

# Ein Kriterium für die algebraischen Zahlen.

(Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-physikalische Klasse. 1899. S. 64—88.)

(Vorgelegt in der Sitzung vom 11. Februar 1899 von D. Hilbert.)

Im Jahre 1770 hat Lagrange*) gezeigt, daß die Entwicklung einer reellen irrationalen Größe in einen gewöhnlichen Kettenbruch immer dann und nur dann periodisch ausfällt, wenn die Größe Wurzel einer quadratischen Gleichung mit rationalen Koeffizienten ist. Dieser Satz gibt offenbar ein vollständiges Mittel zur Unterscheidung der reellen algebraischen Zahlen zweiten Grades von allen anderen Größen. Seit jener Entdeckung von Lagrange durfte man vermuten, daß ein allgemeinerer Satz existiere, der ein vollständiges Kriterium für die reellen (oder komplexen) algebraischen Zahlen beliebigen $n^{\text{ten}}$ Grades gibt und der für $n = 2$ und reelle Zahlen eben auf jenen Satz von Lagrange hinauskommt. Eine solche Verallgemeinerung wird zum ersten Male**) im folgenden dargelegt.

## § 1. Arithmetische Hilfssätze.

1. Ich beginne mit der Ableitung einiger Hilfssätze, auf welche sich die späteren Beweisführungen gründen werden.

Es seien $\xi_1, \ldots, \xi_\nu$ eine Reihe linearer homogener Formen mit den $n$ reellen Variablen $x_1, \ldots, x_n$ und mit irgendwelchen reellen oder komplexen Koeffizienten; nur soll das System der Gleichungen $\xi_1 = 0, \ldots, \xi_\nu = 0$ bloß durch das *eine reelle* Wertsystem $x_1 = 0, \ldots, x_n = 0$ befriedigt werden können.

Der größte unter den absoluten Beträgen von $x_1, \ldots, x_n$ vorkommende Betrag soll mit $\max |x_k|$ bezeichnet werden. Setzt man für $x_1, \ldots, x_n$ irgendwelche reellen Werte, so soll der größte unter den absoluten Be-

*) Abhandlungen der Akademie zu Berlin, Bd. XXIV, 1770; Werke, Bd. II, S. 603 ff.

**) Über bisherige Versuche in dieser Richtung s. P. Bachmann, Vorlesungen über die Natur der Irrationalzahlen, 1892, Vorl. II und Vorl. X.

trägen von $\xi_1, \ldots, \xi_\nu$ vorkommende Betrag mit $\max |\xi_\varkappa(x_1, \ldots, x_n)|$ und zugleich mit $f(x_1, \ldots, x_n)$ bezeichnet werden.

Man hat dann

$$f(-x_1, \ldots, -x_n) = f(x_1, \ldots, x_n), \tag{1}$$

$$f(tx_1, \ldots, tx_n) = tf(x_1, \ldots, x_n), \text{ wenn } t > 0 \text{ ist.} \tag{2}$$

Die Funktion $f(x_1, \ldots, x_n)$ ist eine stetige der Argumente $x_1, \ldots, x_n$ und hat daher in dem durch $\max |x_k| = 1$ definierten *abgeschlossenen* Bereiche (d. i. auf der *Begrenzung* des durch $-1 \leqq x_1 \leqq 1, \ldots, -1 \leqq x_n \leqq 1$ definierten Würfels) ein bestimmtes Minimum $g$, das wegen der an die $\xi_1, \ldots, \xi_\nu$ oben gestellten Anforderung gewiß $> 0$ ist, und ein bestimmtes Maximum $G$. Sodann ist wegen (2) stets

$$g \max |x_k| \leqq f(x_1, \ldots, x_n) \leqq G \max |x_k|. \tag{3}$$

Endlich hat man, wenn $a_1, \ldots, a_n$ und $b_1, \ldots, b_n$ zwei reelle Systeme sind, stets

$$f(a_1 + b_1, \ldots, a_n + b_n) \leqq f(a_1, \ldots, a_n) + f(b_1, \ldots, b_n). \tag{4}$$

Denn für jede einzelne der linearen Formen $\xi_\iota$ gilt

$$|\xi_\iota(a_1 + b_1, \ldots, a_n + b_n)| \leqq |\xi_\iota(a_1, \ldots, a_n)| + |\xi_\iota(b_1, \ldots, b_n)|$$
$$\leqq \max |\xi_\varkappa(a_1, \ldots, a_n)| + \max |\xi_\varkappa(b_1, \ldots, b_n)|$$

und daher auch

$$\max |\xi_\varkappa(a_1 + b_1, \ldots, a_n + b_n)| \leqq \max |\xi_\varkappa(a_1, \ldots, a_n)| + \max |\xi_\varkappa(b_1, \ldots, b_n)|.$$

Hat man $f(a_1, \ldots, a_n) \leqq 1$ und $f(b_1, \ldots, b_n) \leqq 1$ und ist $0 < t < 1$, so folgt nach den Regeln (4) und (2)

$$f((1-t)a_1 + tb_1, \ldots, (1-t)a_n + tb_n) \leqq (1-t)f(a_1, \ldots, a_n) + tf(b_1, \ldots, b_n) \leqq 1. \tag{5}$$

Nach den Eigenschaften (5) und (1) ist der durch $f(x_1, \ldots, x_n) \leqq 1$ definierte Bereich $K$ in der Mannigfaltigkeit der $x_1, \ldots, x_n$ ein *nirgends konkaver Körper* und hat das System $x_1 = 0, \ldots, x_n = 0$ (den Nullpunkt) als *Mittelpunkt*. Der Bereich $K$ liegt wegen (3) ganz im Würfel $\max |x_k| \leqq \frac{1}{g}$ eingeschlossen und enthält in sich den Würfel $\max |x_k| \leqq \frac{1}{G}$. Das $n$-fache Integral $\int dx_1 \ldots dx_n$, über den Bereich $K$ erstreckt, (das Volumen von $K$) hat einen bestimmten positiven endlichen Wert $J$.*)

2. Der Inbegriff aller Systeme $x_1, \ldots, x_n$, bei welchen sowohl $x_1$, wie $x_2, \ldots$, wie $x_n$ ganze Zahlen sind, soll das *Zahlengitter*, die einzelnen Systeme daraus sollen *Gitterpunkte* heißen.

---

*) Man kann die Zahl $\nu$ oben auch unbegrenzt wachsen lassen, wenn man die Bedingung hinzufügt, daß in allen Formen $\xi_\iota$ die Beträge der Koeffizienten unter einer Grenze bleiben, und kommt dadurch zu dem Begriffe eines beliebigen nirgends konkaven Körpers mit dem Nullpunkt als Mittelpunkt. Alle im § 1 abgeleiteten Sätze gelten unverändert für jeden solchen Körper.

Eine Reihe von Systemen $x_1 = p_1^{(h)}, \ldots, x_n = p_n^{(h)}$ $(h = 1, \ldots, m$ und $m \leqq n)$ soll *unabhängig* heißen, wenn in der aus ihnen zu bildenden Matrix $\|p_k^{(h)}\|$ nicht jede $m$-reihige Determinante Null ist.

Es seien $p_1^{(h)}, \ldots, p_n^{(h)}$ für $h = 1, \ldots, n$ irgend $n$ unabhängige Gitterpunkte, also die Substitution $P$:

$$x_k = p_k^{(1)} z_1 + \cdots + p_k^{(n)} z_n \qquad (k = 1, \ldots, n) \tag{6}$$

eine ganzzahlige mit von Null verschiedener Determinante. Dann gibt es bekanntlich eine ganzzahlige Substitution $A$ mit einer Determinante $= \pm 1$:

$$x_k = a_k^{(1)} y_1 + \cdots + a_k^{(n)} y_n \qquad (k = 1, \ldots, n) \tag{7}$$

so daß die Formeln $P^{-1}A$ werden:

$$z_1 = \gamma_1^{(1)} y_1 + \cdots + \gamma_1^{(n)} y_n, \ldots, z_n = \gamma_n^{(n)} y_n \quad (\gamma_h^{(k)} = 0,\ h > k) \tag{8}$$

und dabei ferner die Ungleichungen erfüllt sind:

$$0 < \gamma_h^{(h)} \leqq 1, \qquad 0 \leqq \gamma_h^{(k)} < \gamma_h^{(h)} (h < k). \tag{9}$$

In der Tat, unter allen Gitterpunkten, deren Koordinaten von der Form $x_k = \gamma_1 p_k^{(1)}$ mit $0 < \gamma_1 \leqq 1$ $(k = 1, \ldots, n)$ sind, wird es einen geben, für den $\gamma_1$ am kleinsten ist; es sei für ihn $\gamma_1 = \gamma_1^{(1)}$, $x_k = a_k^{(1)}$. Dann kann man unter allen Gitterpunkten mit Koordinaten von der Form $x_k = \gamma_1 p_k^{(1)} + \gamma_2 p_k^{(2)}$ $(k = 1, \ldots, n)$ und den Umständen $0 \leqq \gamma_1 < \gamma_1^{(1)}$, $0 < \gamma_2 \leqq 1$ einen finden, für den $\gamma_2$ so klein als möglich ist; es sei für ihn $\gamma_2 = \gamma_2^{(2)}$, $\gamma_1 = \gamma_1^{(2)}$, $x_k = a_k^{(2)}$, usf. Zuletzt kann man unter den Gitterpunkten mit Koordinaten von der Form $x_k = \gamma_1 p_k^{(1)} + \cdots + \gamma_n p_k^{(n)}$ und $0 \leqq \gamma_1^{(1)}, \ldots, 0 \leqq \gamma_{n-1} < \gamma_{n-1}^{(n-1)}$, $0 < \gamma_n \leqq 1$ einen finden, für den $\gamma_n$ möglichst klein ist; für ihn sei $\gamma_n = \gamma_n^{(n)}, \ldots, \gamma_1 = \gamma_1^{(n)}$, $x_k = a_k^{(n)}$.

Nunmehr wird man, wenn $x_k$ $(k = 1, \ldots, n)$ ein beliebiger Gitterpunkt ist, sukzessive $y_n, y_{n-1}, \ldots, y_1$ als ganze Zahlen so bestimmen können, daß in der Umformung

$$x_k - (y_n a_k^{(n)} + y_{n-1} a_k^{(n-1)} + \cdots + y_1 a_k^{(1)}) = \gamma_n p_k^{(n)} + \gamma_{n-1} p_k^{(n-1)} + \cdots + \gamma_1 p_k^{(1)}$$
$$(k = 1, \ldots, n)$$

sich $0 \leqq \gamma_n < \gamma_n^{(n)}$, $0 \leqq \gamma_{n-1} < \gamma_{n-1}^{(n-1)}, \ldots, 0 \leqq \gamma < \gamma_1^{(1)}$ ergibt. Dann muß, da die linken Seiten jedenfalls Koordinaten eines Gitterpunktes sind, nach der Bedeutung von $\gamma_n^{(n)}, \ldots, \gamma_1^{(1)}$ hier notwendig $\gamma_n = 0$, $\gamma_{n-1} = 0, \ldots, \gamma_1 = 0$ sein; es folgen also die Relationen von der Form (7), woraus nach den Ausdrücken der $a_k^{(h)}$ weiter die Formeln (8) hervorgehen. Zu jedem Systeme von ganzen Zahlen $x_1, \ldots, x_n$ gehören so vermöge (7) bestimmte ganzzahlige Werte $y_1, \ldots, y_n$. Es müssen also in der Auflösung von (7):

$$y_h = b_h^{(1)} x_1 + \cdots + b_h^{(n)} x_n \qquad (h = 1, \ldots, n), \tag{10}$$

wie die Einführung der $n$ Systeme $x_j = 1$, $x_k = 0$ $(k \neq j)$ für $j = 1, \ldots, n$ zeigt, alle Koeffizienten $b_h^{(j)}$ ganze Zahlen sein. Somit ist auch ihre Determinante $|b_h^{(j)}|$ eine ganze Zahl, und da dieselbe der reziproke Wert der ebenfalls ganzzahligen Determinante $|a_k^{(h)}|$ ist, so folgt notwendig, daß diese: $|a_k^{(h)}| = \pm 1$ ist.

3. Betrachten wir wieder die in 1. definierte Funktion $f = f(x_1, \ldots, x_n)$. Es gibt wegen (3) nur eine endliche Anzahl von Gitterpunkten, für welche $f$ eine gegebene Größe nicht überschreitet. Andererseits gilt nach (3) $f \leqq G$ jedenfalls bei den $n$ *unabhängigen* Systemen $x_j = 1$, $x_k = 0$ $(k \neq j)$ für $j = 1, \ldots, n$. Man bestimme nun unter allen *vom Nullpunkte verschiedenen* Gitterpunkten, bei welchen $f \leqq G$ ist, einen ersten Gitterpunkt $p_1^{(1)}, \ldots, p_n^{(1)}$, so daß $f(p_1^{(1)}, \ldots, p_n^{(1)}) = F_1$ möglichst klein ist, sodann einen zweiten, *von diesem ersten unabhängigen* Gitterpunkt $p_1^{(2)}, \ldots, p_n^{(2)}$, so daß $f(p_1^{(2)}, \ldots, p_n^{(2)}) = F_2$ möglichst klein ist, usf. bis zu einem $n^{\text{ten}}$ Gitterpunkt $p_1^{(n)}, \ldots, p_n^{(n)}$, so daß schließlich die *Determinante* $|p_k^{(h)}| \neq 0$ ist und für diesen letzten $f(p_1^{(n)}, \ldots, p_n^{(n)}) = F_n$ möglichst klein ausfällt. Bei jedem einzelnen der zu wählenden Gitterpunkte hat man jedenfalls die Auswahl zwischen einem Paare entgegengesetzter Systeme ($p_1, \ldots, p_n$ und $-p_1, \ldots, -p_n$), unter Umständen aber zwischen einer gewissen Anzahl solcher Paare; trotz der dabei zugelassenen Willkür aber ist das System der $n$ Werte $F_1, F_2, \ldots, F_n$ von vornherein ein völlig bestimmtes.

In der Tat, jedenfalls ist

$$F_1 \leqq F_2 \leqq \ldots \leqq F_n. \tag{11}$$

Wir denken uns nun für die $n$ Gitterpunkte $p_1^{(h)}, \ldots, p_n^{(h)}$ $(h = 1, \ldots, n)$, an welche die Betrachtungen in 2. anknüpften, die hier ausgewählten $n$ Gitterpunkte gesetzt und können alsdann sämtliche dort eingeführten Bezeichnungen hier übernehmen. Vermöge der Substitution $A$ entsprechen sich genau die Gitterpunkte $x_1, \ldots, x_n$ und die ganzzahligen Systeme $y_1, \ldots, y_n$. Nach der Bedeutung der Werte $F_j$ hat man für einen Gitterpunkt, bei dem $z_j, z_{j+1}, \ldots, z_n$ nicht sämtlich Null sind oder also $y_j, y_{j+1}, \ldots, y_n$ nicht sämtlich Null sind, stets $f(x_1, \ldots, x_n) \geqq F_j$. Hat man nun irgend $n$ unabhängige Gitterpunkte $x_1^{(h)}, \ldots, x_n^{(h)}$ für $h = 1, \ldots, n$, so daß also die Determinante $|x_k^{(h)}| \neq 0$ ist, und entsprechen ihnen vermöge der Substitution (7) die Systeme $y_1^{(h)}, \ldots, y_n^{(h)}$, so ist auch die Determinante $|y_k^{(h)}| \neq 0$; es können daher, wenn $j$ einen der Werte $1, \ldots, n$ bedeutet, nicht bei $j$ oder gar mehr der Punkte alle $n - j + 1$ Größen $y_j, y_{j+1}, \ldots, y_n$ gleich Null sein, es sind also stets für mindestens $n - j + 1$ der Punkte die Werte $f(x_1, \ldots, x_n) \geqq F_j$. Ordnet man also die $n$ Werte $f(x_1^{(h)}, \ldots, x_n^{(h)})$ der Größe nach in die Reihe $F_1^*, \ldots, F_n^*$, so ist stets

$F_j^* \geqq F_j$ $(j = 1, \ldots, n)$, [also auch $\prod_{h=1}^{n} f(x_1^{(h)}, \ldots, x_n^{(h)}) \geqq F_1 \ldots F_n$, wobei das Gleichheitszeichen nur statthat, wenn die $n$ Werte $f(x_1^{(h)}, \ldots, x_n^{(h)})$ abgesehen von der Reihenfolge mit $F_1, \ldots, F_n$ zusammenfallen]. Danach sind die Werte $F_1, \ldots, F_n$ vollkommen bestimmt als das kleinste mögliche System von $n$ Werten der Funktion $f(x_1, \ldots, x_n)$ für $n$ unabhängige Gitterpunkte.

In dem fünften Kapitel meines Buches „Geometrie der Zahlen" (I. Heft, Leipzig, 1896) nun habe ich nachgewiesen, daß stets die Ungleichung

$$F_1 \ldots F_n J \leqq 2^n$$

gilt, wo $J$ das Volumen des Bereichs $f(x_1, \ldots, x_n) \leqq 1$ ist. Der Beweis dieser Ungleichung erfordert mancherlei Ausführungen. Für die im folgenden beabsichtigten Folgerungen kommt es jedoch nur darauf an, daß sich für $F_1 \ldots F_n J$ überhaupt irgendeine, nur von $n$ und nicht weiter von der Funktion $f(x_1, \ldots, x_n)$ abhängende obere Grenze angeben läßt. Durch wesentlich einfachere Überlegungen als a. a. O. läßt sich nun folgendes nachweisen.

Hilfssatz I. *Es gilt für den nirgends konkaven Bereich* $f(x_1, \ldots, x_n) \leqq 1$ *die Ungleichung:*

$$F_1 \ldots F_n J \leqq n!\, 2^n. \tag{12}$$

4. Um den Beweis dieser Ungleichung anzubahnen, ermitteln wir zunächst zu den einmal gewählten $n$ Gitterpunkten $p_1^{(h)}, \ldots, p_n^{(h)}$ für $h = 1, \ldots, n$ die Substitution (7) und führen damit gewisse neue Variablen $y_1, \ldots, y_n$ ein. Es sei $K$ der Körper $f(x_1, \ldots, x_n) \leqq 1$, und wir wollen für $j = 1, \ldots, n$ unter $K_j^+$ bzw. $K_j^-$ das Gebiet aus $K$ verstehen, für das $y_j \geqq 0$, bzw. $y_j \leqq 0$ und zudem, (wenn $j < n$ ist), $y_{j+1} = 0, \ldots, y_n = 0$ ist; die Vereinigung von $K_j^+$ und $K_j^-$ heiße $K_j$; der Bereich $K_n$ wird nichts anderes als $K$ selbst.

Es sei $y_1 = \delta_1^{(1)}, y_2 = 0, \ldots, y_n = 0$ der Punkt (das System $y_1, \ldots, y_n$) aus $K_1^+$, für den $y_1$ am größten ist, sodann $y_1 = \delta_1^{(2)}$, $y_2 = \delta_2^{(2)}$, $y_3 = 0, \ldots, y_n = 0$ ein solcher Punkt aus $K_2^+$, für den $y_2$ möglichst groß ist, usf., schließlich $y_1 = \delta_1^{(n)}$, $y_2 = \delta_2^{(n)}, \ldots, y_n = \delta_n^{(n)}$ ein solcher Punkt aus $K_n^+$, für den $y_n$ möglichst groß ist. Dabei sind natürlich $\delta_1^{(1)}, \delta_2^{(2)}, \ldots, \delta_n^{(n)}$ positiv. Diese Systeme mögen auch kurz die Punkte $\mathfrak{d}_1, \mathfrak{d}_2, \ldots, \mathfrak{d}_n$ und die ihnen entgegengesetzten Systeme die Punkte $-\mathfrak{d}_1, -\mathfrak{d}_2, \ldots, -\mathfrak{d}_n$ heißen.

Wir führen nun die Substitution ein:

$$y_1 = \delta_1^{(1)} v_1 + \cdots + \delta_1^{(n)} v_n, \ldots, y_n = \delta_n^{(n)} v_n \quad (\delta_h^{(k)} = 0,\ h > k), \tag{13}$$

und wir setzen ihre Determinante $\delta_1^{(1)} \delta_2^{(2)} \ldots \delta_n^{(n)} = \Delta$. Für den Punkt $\mathfrak{d}_j$

hat man dann $v_j = 1$, $v_k = 0$ $(k \neq j)$; als ein Körper, der den Nullpunkt zum Mittelpunkt hat, enthält $K$ mit $\mathfrak{d}_j$ jedesmal auch den Punkt $-\mathfrak{d}_j$, d. i. $v_j = -1$, $v_k = 0$ $(k \neq j)$, und mit diesen $2n$ Systemen $\pm\mathfrak{d}_1, \ldots, \pm\mathfrak{d}_n$ enthält $K$ als ein nirgends konkaver Körper (wegen (5)) sogleich den ganzen durch

$$|v_1| + |v_2| + \cdots + |v_n| \leqq 1 \tag{14}$$

definierten Bereich. (Für $n = 3$ stellt dieser Bereich ein Oktaeder vor.)

Es läßt sich nun ein zweiter einfacher Bereich (ein Parallelepipedum) angeben, welcher seinerseits ganz den Körper $K$ in sich enthält. Es habe $j$ einen der Werte $1, \ldots, n-1$. Wir suchen einen Ausdruck $\varphi = v_j + \varepsilon^{(j+1)} v_{j+1} + \cdots + \varepsilon^{(n)} v_n$ mit geeigneten Konstanten $\varepsilon^{(j+1)}, \ldots, \varepsilon^{(n)}$ herzustellen, so daß in $K$ durchweg $\varphi \leqq 1$ ist.

Zunächst gilt in $K_j$: $v_j \leqq 1$. Wir bilden nun $\varphi = v_j + \varepsilon v_{j+1}$ mit irgendeiner Konstante $\varepsilon$. In $K_j$ ist $v_{j+1} = 0$, $v_j \leqq 1$, also $\varphi \leqq 1$. Sowie $\varepsilon \leqq -1$ ist, hat man für den Punkt $-\mathfrak{d}_{j+1}$, für den $v_{j+1} = -1$, $v_j = 0$ ist, $\varphi \geqq 1$; dann muß in $K_{j+1}^+$ *durchweg* $\varphi \leqq 1$ sein. Denn hätte man $\varphi > 1$ für irgendeinen Punkt in $K_{j+1}^+$, so würde die Strecke von diesem Punkte nach $-\mathfrak{d}_{j+1}$ das Gebiet $K_j$ in einem Punkte treffen, für den ebenfalls $\varphi > 1$ wäre. Sowie andererseits $\varepsilon > 1$ ist, hat man in $K_{j+1}^+$ für den Punkt $\mathfrak{d}_{j+1}$ jedenfalls $\varphi > 1$. Danach ist das *Maximum* des Ausdrucks $\varphi = v_j + \varepsilon v_{j+1}$ für ein gegebenes $\varepsilon$ im Bereiche $K_{j+1}^+$ sicher $> 1$, wenn $\varepsilon > 1$ ist, und sicher $\leqq 1$, wenn $\varepsilon \leqq -1$ ist. Dieses Maximum aber ist offenbar eine Funktion von $\varepsilon$, die sich mit $\varepsilon$ stetig ändert, und wird es daher einen bestimmten *größten* Wert $\varepsilon = \varepsilon_j^{(j+1)}$ geben, im Intervalle $-1 \leqq \varepsilon \leqq 1$ gelegen, für den dieses Maximum noch $\leqq 1$, d. h. für den in $K_{j+1}^+$ noch durchweg $\varphi \leqq 1$ ist. Dann ist für jeden Wert $\varepsilon$, der $> \varepsilon_j^{(j+1)}$ ist, in $K_{j+1}^+$ notwendig irgendwo auch $\varphi > 1$ und daher, weil in $K_j$ überall $\varphi \leqq 1$ sein muß, in $K_{j+1}^-$ notwendig überall $\varphi \leqq 1$; letzteres muß dann auch noch für den Grenzwert $\varepsilon = \varepsilon_j^{(j+1)}$ gelten, und also ist für diesen Wert im ganzen Bereich $K_{j+1}$ stets $\varphi \leqq 1$.

Falls auch noch $j + 1 < n$ ist, betrachten wir den neuen Ausdruck $\varphi = v_j + \varepsilon_j^{(j+1)} v_{j+1} + \varepsilon v_{j+2}$ mit irgendeiner Konstante $\varepsilon$. In $K_{j+1}$ ist $v_{j+2} = 0$ und also stets $\varphi \leqq 1$. Für ein $\varepsilon \leqq -1$ und den Punkt $-\mathfrak{d}_{j+2}$ in $K_{j+2}^-$ ist $\varphi \geqq 1$ und daher in $K_{j+2}^+$ notwendig überall $\varphi \leqq 1$. Dagegen ist für ein $\varepsilon > 1$ in $K_{j+2}^+$ insbesondere $\varphi > 1$ für den Punkt $\mathfrak{d}_{j+2}$. Nunmehr wird es einen bestimmten *größten* Wert $\varepsilon = \varepsilon_j^{(j+2)}$ geben, im Intervalle $-1 \leqq \varepsilon \leqq 1$ gelegen, für den in $K_{j+2}^+$ noch überall $\varphi \leqq 1$ ist. Dann ist für jeden Wert $\varepsilon > \varepsilon_j^{(j+2)}$ in $K_{j+2}^+$ irgendwo $\varphi > 1$ und daher in $K_{j+2}^-$ überall $\varphi \leqq 1$, und dieses letztere muß schließlich auch für den Grenzwert $\varepsilon = \varepsilon_j^{(j+2)}$ gelten. Mithin ist $\varphi = v_j + \varepsilon_j^{(j+1)} v_{j+1} + \varepsilon_j^{(j+2)} v_{j+2}$ in $K_{j+2}$ durchweg $\leqq 1$.

Es ist nun klar, wie man fortzuschreiten hat, wenn noch $j+2<n$ ist, und daß man schließlich zu einem Ausdrucke

$$\varphi_j = v_j + \varepsilon_j^{(j+1)} v_{j+1} + \cdots + \varepsilon_j^{(n)} v_n$$

mit bestimmten Koeffizienten $\varepsilon_j^{(j+1)}, \ldots, \varepsilon_j^{(n)}$ kommen wird von solcher Art, daß in $K_n$, d. i. in $K$ überall $\varphi_j \leqq 1$ ist. Weil $K$ ein Körper mit dem Nullpunkt als Mittelpunkt ist, nimmt $-\varphi_j$ in $K$ dieselbe Wertmenge an wie $\varphi_j$, und also ist dann in $K$ auch $-\varphi_j \leqq 1$, d. h. $\varphi_j \geqq -1$.

Endlich hat man noch für $\varphi_n = v_n$ in $K$ stets $\pm \varphi_n \leqq 1$.

Man kann auf solche Weise $n$ Formen herstellen:

$$(15)\quad \varphi_1 = v_1 + \varepsilon_1^{(2)} v_2 + \cdots + \varepsilon_1^{(n)} v_n, \quad \varphi_2 = v_2 + \cdots + \varepsilon_2^{(n)} v_n, \ldots, \varphi_n = v_n,$$

so daß $K$ ganz in dem Bereiche

$$(16)\qquad -1 \leqq \varphi_1 \leqq 1, \qquad -1 \leqq \varphi_2 \leqq 1, \ldots, -1 \leqq \varphi_n \leqq 1$$

enthalten ist.

Nun ist über diesen Bereich ausgedehnt das Integral $\int dx_1 \ldots dx_n = \int dy_1 \ldots dy_n = \Delta \cdot \int dv_1 \ldots dv_n = \Delta \cdot \int d\varphi_1 \ldots d\varphi_n = 2^n \Delta$, wo $\Delta$ die Determinante der Gleichungen (13) bedeutet, und also folgt, weil $K$ in diesem Bereiche enthalten ist:

$$(17)\qquad J \leqq 2^n \Delta.$$

Andererseits ist für den Bereich (14) das Volumen $\int dx_1 \ldots dx_n = \Delta \cdot \int dv_1 \ldots dv_n = \frac{2^n}{n!}\Delta$ und hat man, weil dieser Bereich (14) ganz in $K$ enthalten ist,

$$(18)\qquad \frac{2^n}{n!}\Delta \leqq J.$$

5. Weil der Bereich (14) in $K$ enthalten ist, hat man auf der Begrenzung von $K$, d. h. wenn $f(x_1, \ldots, x_n) = 1$ ist, $|v_1| + \cdots + |v_n| \geqq 1 = f(x_1, \ldots, x_n)$. Wegen (2) und der entsprechenden Regel für den Ausdruck $|v_1| + \cdots + |v_n|$ gilt dann allgemein für jedes beliebige System $x_1, \ldots, x_n$:

$$(19)\qquad |v_1| + \cdots + |v_n| \geqq f(x_1, \ldots, x_n).$$

Wir bilden für ein beliebiges System $x_1, \ldots, x_n$ unter Benutzung der Substitutionen (7) und (13) den Ausdruck

$$(20)\qquad \left|\frac{v_1}{F_1}\right| + \cdots + \left|\frac{v_n}{F_n}\right| = \psi(x_1, \ldots, x_n).$$

Ist $x_1, \ldots, x_n$ ein vom Nullpunkte verschiedener Gitterpunkt und für ihn unter seinen Zahlen $y_1, \ldots, y_n$ etwa $y_j$ die letzte von Null verschiedene, so ist nach der Bedeutung der Werte $F_1, \ldots, F_n$ für ihn $f(x_1, \ldots, x_n) \geqq F_j$; alsdann folgt aus (19), indem, wenn $j<n$ ist, für ihn $v_{j+1}, \ldots, v_n$ Null sind, $|v_1| + \cdots + |v_j| \geqq F_j$ und mit Rücksicht auf (11) weiter

$$\psi(x_1, \ldots, x_n) = \left|\frac{v_1}{F_1}\right| + \cdots + \left|\frac{v_j}{F_j}\right| \geqq \frac{|v_1| + \cdots + |v_j|}{F_j} \geqq 1.$$

Danach kann sich für keinen einzigen Gitterpunkt außer dem Nullpunkte $\psi(x_1, \ldots, x_n) < 1$ herausstellen. Der durch

$$\psi(x_1, \ldots, x_n) \leqq 1 \tag{21}$$

definierte nirgends konkave Bereich (für $n = 3$ ein Oktaeder) enthält also außer dem Nullpunkte keinen Gitterpunkt im *Inneren* (d. h. die Begrenzung ausgenommen). Das Integral $\int dx_1 \ldots dx_n$ über diesen Bereich ist $= F_1 \ldots F_n \cdot \frac{2^n \Delta}{n!}$.

Sind $x_1 = 2r_1, \ldots, x_n = 2r_n$ und $x_1 = 2s_1, \ldots, x_n = 2s_n$ irgend zwei verschiedene Systeme von je $n$ *geraden* ganzen Zahlen, so können daher die zwei ihnen entsprechenden Bereiche

$$\psi(x_1 - 2r_1, \ldots, x_n - 2r_n) \leqq 1, \quad \psi(x_1 - 2s_1, \ldots, x_n - 2s_n) \leqq 1$$

niemals einen inneren Punkt gemein haben. Denn da man analog zu (4) und (1)

$$2\psi(s_1 - r_1, \ldots, s_n - r_n) \leqq \psi(x_1 - 2r_1, \ldots, x_n - 2r_n) + \psi(2s_1 - x_1, \ldots, 2s_n - x_n)$$
$$\psi(2s_1 - x_1, \ldots, 2s_n - x_n) = \psi(x_1 - 2s_1, \ldots, x_n - 2s_n)$$

hat, würde in solchem Falle $2\psi(s_1 - r_1, \ldots, s_n - r_n) < 2$ hervorgehen, läge also der vom Nullpunkte verschiedene Gitterpunkt $s_1 - r_1, \ldots, s_n - r_n$ im Inneren des Bereiches (21).

Man hat im Bereiche (21) stets $|v_j| \leqq F_j \leqq G$, sodann, wenn $\delta$ den größten Betrag unter den Beträgen der $\delta_h^{(j)}$ in (13) ist, $|y_h| \leqq n\delta G$, und wenn $a$ den größten Betrag unter den Beträgen der $a_k^{(h)}$ in (7) ist, weiter $|x_k| \leqq n^2 a \delta G$, welche Grenze $d$ heiße. In $\psi(x_1 - 2r_1, \ldots, x_n - 2r_n) \leqq 1$ gilt dann, wenn $r$ der größte Betrag unter denen von $r_1, \ldots, r_n$ ist, $|x_k - 2r_k| \leqq d$, $|x_k| \leqq 2r + d$.

Nun sei $\Omega$ irgendeine positive ganze Zahl und man betrachte alle diejenigen Gitterpunkte mit geraden Koordinaten $2r_1, \ldots, 2r_n$, für welche jede der Größen $r_k$ einen der Werte $0, \pm 1, \ldots, \pm \Omega$ hat. Von den zugehörigen Bereichen $\psi(x_1 - 2r_1, \ldots, x_n - 2r_n) \leqq 1$ haben keine zwei einen inneren Punkt gemein. Sie liegen alle im Würfel

$$-(2\Omega + d) \leqq x_k \leqq (2\Omega + d) \qquad (k = 1, \ldots, n)$$

eingeschlossen. Die Anzahl dieser Bereiche ist $(2\Omega + 1)^n$ und jeder hat dasselbe Volumen wie der Bereich (21). Danach folgt

$$(2\Omega + 1)^n \cdot F_1 \ldots F_n \frac{2^n}{n!} \Delta \leqq (4\Omega + 2d)^n. \tag{22}$$

Läßt man hierin die ganze Zahl $\Omega$ unbegrenzt wachsen, so geht

$$F_1 \ldots F_n \frac{2^n}{n!} \Delta \leqq 2^n \tag{23}$$

hervor, d. h. das Volumen des Bereichs (21) muß $\leqq 2^n$ sein. Vermittels (17) folgt daraus in der Tat der zu erweisende Hilfssatz I.

6. Ferner ist von Interesse:

Hilfssatz II. *Die Determinante* $|p_k^{(h)}|$ *für* $n$ *unabhängige Gitterpunkte* $p_1^{(h)}, \ldots, p_n^{(h)}$ $(h = 1, \ldots, n)$, *welche* $f(p_1^{(h)}, \ldots, p_n^{(h)}) = F_h$ *ergeben, ist stets dem Betrage nach* $\leqq n!$.

Nämlich auch der durch

$$|z_1| + \cdots + |z_n| \leqq 1 \tag{24}$$

definierte Bereich enthält keinen Gitterpunkt außer dem Nullpunkte im Inneren. Denn ist $x_1, \ldots, x_n$ ein vom Nullpunkte verschiedener Punkt im *Inneren* dieses Bereichs und von den Größen $z_1, \ldots, z_n$ für ihn $z_j$ die letzte von Null verschiedene, so folgt aus (6) vermöge (4), (1), (2)

$$\begin{aligned} f(x_1, \ldots, x_n) &\leqq |z_1| f(p_1^{(1)}, \ldots, p_n^{(1)}) + \cdots + |z_j| f(p_1^{(j)}, \ldots, p_n^{(j)}) \\ &\leqq (|z_1| + \cdots + |z_j|) F_j < F_j; \end{aligned}$$

nun ist auch unter den Größen $y_1, \ldots, y_n$ für ihn $y_j$ die letzte von Null verschiedene und kann hiernach der Punkt kein Gitterpunkt sein. Auf Grund derselben Überlegungen wie vorhin für den analogen Bereich (21) folgt nunmehr, daß auch das Volumen von (24) sicher $\leqq 2^n$ ist. Dieses Volumen ist gleich $\frac{2^n}{n!}$, multipliziert in den Betrag der Determinante $|p_k^{(h)}|$; mithin ist dieser Betrag $\leqq n!$.

Das gleiche Resultat ergibt sich bereits in folgender Weise. Der Betrag der Determinante $|p_k^{(h)}|$ ist nach (6), (7), (8) gleich dem reziproken Wert des Produktes $\gamma_1^{(1)} \ldots \gamma_n^{(n)}$. Für den Gitterpunkt $p_1^{(h)}, \ldots, p_n^{(h)}$ ist $z_h = 1$, $z_k = 0$ $(k \neq h)$, also $y_h = \frac{1}{\gamma_h^{(h)}}$, $y_k = 0$ $(k > h)$. Da nun dieser Punkt zum Bereiche $f\left(\frac{x_1}{F_h}, \ldots, \frac{x_n}{F_h}\right) \leqq 1$ gehört, muß für ihn nach der Bedeutung der Größen $\delta_h^{(h)}$ in 4. sich $\frac{y_h}{F_h} \leqq \delta_h^{(h)}$ erweisen. Also ist $\frac{1}{\gamma_h^{(h)}} \leqq F_h \delta_h^{(h)}$, mithin $\frac{1}{\gamma_1^{(1)} \ldots \gamma_n^{(n)}} \leqq F_1 \ldots F_n \Delta$, woraus vermöge (23) der Hilfssatz II hervorgeht.

Nach (6), (7), (8) sind die Koeffizienten $\gamma_h^{(k)}$ in (8) rationale Zahlen mit der Determinante $|p_k^{(h)}|$ als Nenner, also mit einem Generalnenner $\leqq n!$. Nach den Ungleichungen (9) kommen daher für diese Koeffizienten, also für die ganze Substitution $P^{-1}A$ von vornherein eine nur von $n$ abhängende Anzahl von möglichen Ausdrücken in Betracht.

7. Endlich fügen wir die folgende Bemerkung hinzu. Für das System $x_k = a_k^{(h)}$ $(k = 1, \ldots, n)$ in (7) ist $x_k = \gamma_1^{(h)} p_k^{(1)} + \cdots + \gamma_h^{(h)} p_k^{(h)}$. Indem nun die Größen $\gamma_1^{(h)}, \ldots, \gamma_h^{(h)}$ sämtlich $\geqq 0$ und $\leqq 1$ sind, folgt

aus (4) und (2):

$$f(a_1^{(h)}, \ldots, a_n^{(h)}) \leqq f(p_1^{(1)}, \ldots, p_n^{(1)}) + \cdots + f(p_1^{(h)}, \ldots, p_n^{(h)}) \leqq hF_h.$$

Berücksichtigt man nun (12), so zeigt sich, daß für die $n$ ganzzahligen Systeme $a_1^{(h)}, \ldots, a_n^{(h)}$ $(h = 1, \ldots, n)$, *deren Determinante* $|a_k^{(h)}| = \pm 1$ *ist*, die Ungleichung

$$f(a_1^{(1)}, \ldots, a_n^{(1)}) \ldots f(a_1^{(n)}, \ldots, a_n^{(n)}) \leqq (n!)^2 2^n \frac{1}{J} \tag{25}$$

erfüllt ist.

## § 2. Ein Kriterium für die algebraischen Zahlen $n^{\text{ten}}$ Grades.

8. Eine reelle oder komplexe Größe $a$ heißt eine *algebraische Zahl* und zwar $n^{\text{ten}}$ *Grades*, wenn sie einer algebraischen Gleichung $n^{\text{ten}}$ Grades

$$x_1 + x_2 a + \cdots + x_n a^{n-1} + x_{n+1} a^n = 0 \qquad (x_{n+1} \neq 0)$$

mit rationalen ganzzahligen Koeffizienten $x_1, x_2, \ldots, x_n, x_{n+1}$, deren letzter $\neq 0$ ist, und nicht bereits einer Gleichung derselben Art von niedrigerem Grade genügt. Dieses ist die *Definition* der algebraischen Zahlen $n^{\text{ten}}$ Grades. Im folgenden will ich nun ein *Theorem* entwickeln, *wonach die Entscheidung, ob eine gegebene reelle oder komplexe Größe a eine algebraische Zahl $n^{\text{ten}}$ Grades ist oder nicht, bereits durch Betrachtung der Werte des Ausdrucks*

$$\xi = x_1 + x_2 a + \cdots + x_n a^{n-1} \tag{26}$$

*für rationale ganze Zahlen $x_1, x_2, \ldots, x_n$ geliefert werden kann.*

Es sei $r$ irgendeine positive ganze Zahl, und wir lassen für $x_1, \ldots, x_n$ in (26) alle diejenigen Systeme von ganzen Zahlen zu, wobei jede Zahl dem Betrage nach $\leqq r$ ist, also der Reihe $0, \pm 1, \pm 2, \ldots, \pm r$ angehört, mit Ausschluß des einen Systems $x_1 = 0, \ldots, x_n = 0$. Unter den betreffenden Systemen kommen gewiß Vereine von $n$ *unabhängigen* (d. h. mit nichtverschwindender Determinante $|x_k^{(h)}|$) vor; z. B. sind die $n$ Systeme $x_h^{(h)} = 1$, $x_k^{(h)} = 0$ $(k \neq h)$ für $h = 1, \ldots, n$ unabhängig. Wir suchen unter allen jenen Systemen ein erstes $x_1 = p_1^{(1)}, \ldots, x_n = p_n^{(1)}$ aus, so daß der Betrag von $\xi$ möglichst klein ausfällt. Da wir dabei jedenfalls die Wahl zwischen Paaren entgegengesetzter Systeme haben, wollen wir das System noch derart voraussetzen, daß die letzte von Null verschiedene der Zahlen $p_k^{(1)}$ größer als Null ist. Es sei für das System $\xi = \alpha_1$. Sodann wählen wir unter jenen Systemen ein zweites, von $p_1^{(1)}, \ldots, p_n^{(1)}$ unabhängiges System $x_1 = p_1^{(2)}, \ldots, x_n = p_n^{(2)}$ aus, wofür nächstdem der Betrag von $\xi$ möglichst klein ausfällt, und es sei wieder unter den Zahlen $p_k^{(2)}$ die letzte nichtverschwindende $> 0$. Für dieses zweite System sei $\xi = \alpha_2$. Wir fahren so fort, bis wir schließlich unter jenen Systemen ein $n^{\text{tes}}$ von den früheren unabhängiges System $x_1 = p_1^{(n)}, \ldots,$

$x_n = p_n^{(n)}$ erlangen, wofür wieder der Betrag von $\xi$ möglichst klein ist, und es sei auch von den Zahlen $p_k^{(n)}$ die letzte von Null verschiedene $> 0$. Für dieses $n^{\text{te}}$ System sei $\xi = \alpha_n$. Dann hat endlich die Substitution $P$:

$$x_k = p_k^{(1)} z_1 + p_k^{(2)} z_2 + \cdots + p_k^{(n)} z_n \qquad (k = 1, 2, \ldots, n) \tag{27}$$

eine von Null verschiedene Determinante, und es geht $\xi$ durch $P$ in

$$\xi P = \chi = \alpha_1 z_1 + \alpha_2 z_2 + \cdots + \alpha_n z_n \tag{28}$$

über. Dabei ist jedenfalls

$$|\alpha_1| \leqq |\alpha_2| \leqq \cdots \leqq |\alpha_n|. \tag{29}$$

Unter speziellen Umständen in bezug auf die Größe $a$ ist es möglich, daß die Systeme $p_1^{(h)}, \ldots, p_n^{(h)}$ durch die angegebenen Bedingungen noch nicht eindeutig bestimmt sind, die Festsetzung von $P$ für das gegebene $r$ also noch in mehrfacher Weise geschehen kann. Durch entsprechende Betrachtungen wie in 3. aber erkennt man, daß jedenfalls das System der $n$ absoluten Beträge $|\alpha_1|, |\alpha_2|, \ldots, |\alpha_n|$ durch die Zahl $r$ völlig eindeutig bestimmt ist. Es heiße $P$ eine *zur Zahl r gehörende Substitution*.

Man bilde nun eine zur Zahl $r_1 = 1$ gehörende Substitution $P_1$. Diese kann auch noch zu $r = 2, 3, \ldots$ gehören. Gehört sie nicht zu jeder Zahl $r$, so sei der größte Wert $r$, zu dem sie gehört, $r = r_2 - 1$ (wo $r_2 \geqq 2$ ist). Es sei sodann $P_2$ eine zu $r_2$ gehörende Substitution, und sie gehöre zu den Zahlen $r$, die $\geqq r_2$ und $< r_3$ sind. Sodann sei $P_3$ eine zu $r_3$ gehörende Substitution usf. Wir wollen noch die Festsetzung treffen, daß, wenn für eine dieser Substitutionen $P_\iota$ in der zugehörigen Form $\xi P_\iota = \chi$ ein Teil der Koeffizienten $\alpha_1, \ldots, \alpha_n$ (etwa $\alpha_1, \ldots, \alpha_j$) $= 0$ wird, die betreffenden Vertikalreihen $p_1^{(h)}, \ldots, p_n^{(h)}$ $(h = 1, \ldots, j)$ für alle folgenden Substitutionen $P_\varkappa$ $(\varkappa > \iota)$ unverändert beibehalten werden sollen. Die so entstehende (sei es abbrechende, sei es unendliche) Reihe von Substitutionen $P_1, P_2, P_3, \ldots$ soll die zu $a$ gehörende *Kette von Substitutionen* heißen.

Es sei allgemein $\chi_\iota = \alpha_1^{(\iota)} z_1 + \cdots + \alpha_n^{(\iota)} z_n$ die Form, in welche $\xi$ durch $P_\iota$ übergeht. Man hat für zwei aufeinanderfolgende Substitutionen $P_\iota, P_{\iota+1}$ der Kette:

$$|\alpha_1^{(\iota+1)}| \leqq |\alpha_1^{(\iota)}|, \ldots, |\alpha_n^{(\iota+1)}| \leqq |\alpha_n^{(\iota)}| \qquad (\iota = 1, 2, \ldots), \tag{30}$$

wo jedenfalls nicht alle $n$ Gleichheitszeichen auf einmal gelten können; denn sonst würde ja $P_\iota$ auch zur Zahl $r_{\iota+1}$ gehören, während sie nur zu den Werten $r \geqq r_\iota$ und $\leqq r_{\iota+1} - 1$ gehört. In $P_\iota$ sind jedesmal die Beträge aller Koeffizienten $\leqq r_\iota$ und ist wenigstens einer darunter $> r_\iota - 1$, also eben $= r_\iota$. Man erkennt nach diesen Umständen, daß die Reihe der Zahlen $r_1, r_2, r_3, \ldots$ eine durch die Größe $a$ völlig bestimmte ist.

9. Ohne an die Aufgabe der einfachsten sukzessiven Ermittlung der Kettenglieder näher heranzutreten, beweise ich nur den folgenden Satz, der bei der Behandlung dieser Aufgabe die wesentlichsten Dienste leistet.

*Für eine jede Substitution der Kette ist die Determinante dem Betrage nach* $\leqq n!$.

Es sei $P$ in (27) eine Substitution der Kette, zu einer Zahl $r$ gehörend, und $\chi$ in (28) die Form, in welche $\xi$ durch $P$ übergeht. Dann kann der durch

$$|z_1| + \cdots + |z_n| \leqq 1 \tag{31}$$

definierte Bereich im Inneren (d. h. soweit das Zeichen $<$ gilt), keinen Gitterpunkt außer dem Nullpunkte enthalten. Denn ist $z_1, \ldots, z_n$ irgendein, von $0, \ldots, 0$ verschiedenes System im Inneren dieses Bereichs (31) und von diesen Größen $z_j$ die letzte von Null verschiedene, so hat man dafür

$$\xi = \alpha_1 z_1 + \cdots + \alpha_j z_j, \quad x_k = p_k^{(1)} z_1 + \cdots + p_k^{(j)} z_j.$$

Ist *erstens* $|\alpha_j| > 0$, so folgt $|\xi| \leqq |\alpha_j|(|z_1| + \cdots + |z_j|) < |\alpha_j|$, $|x_k| \leqq r(|z_1| + \cdots + |z_j|) < r$; alsdann ist das betreffende System $x_1, \ldots, x_n$ kein Gitterpunkt, denn für einen Gitterpunkt, bei dem die Beträge $|x_k| \leqq r$ sind und $z_j \neq 0$ ist, muß $|\xi| \geqq |\alpha_j|$ sein.

Ist *zweitens* $\alpha_j = 0$, so sei $P_\varkappa$ die erste Substitution der Kette, für welche sich $\alpha_1^{(\varkappa)} = \cdots = \alpha_j^{(\varkappa)} = 0$ findet, während, wenn $\varkappa > 1$ ist, in der zu $P_{\varkappa-1}$ gehörenden Form $\chi_{\varkappa-1}$ der erste nichtverschwindende Koeffizient $\alpha_{j'}^{(\varkappa-1)}$ mit einem Index $j' \leqq j$ sei. Dann ist also $r_\varkappa$ die kleinste Zahl, für welche die ersten $j'$ Vertikalreihen einer zugehörigen Substitution sämtlich $\xi = 0$ machen. Nun gehören zufolge einer in 8. getroffenen Festsetzung die ersten $j$ Vertikalreihen von $P$ bereits zu $P_\varkappa$ und, wenn $\varkappa > 1$ und $j' > 1$ ist, die ersten $j' - 1$ Vertikalreihen von $P$ bereits zu $P_{\varkappa-1}$. Für das System $z_1, \ldots, z_n$ folgt jetzt $\xi = 0$, $|x_k| \leqq r_\varkappa(|z_1| + \cdots + |z_j|) < r_\varkappa$. Im Falle $\varkappa = 1$ ist $r_1 = 1$ und kann also $x_1, \ldots, x_n$ hier kein Gitterpunkt sein. Ist aber $\varkappa > 1$ und wäre $x_1, \ldots, x_n$ hier ein Gitterpunkt, so wäre derselbe, da $z_j \neq 0$ ist, ja vom Nullpunkte verschieden und zudem, falls $j' > 1$ ist, auch von den Gitterpunkten in den ersten $j' - 1$ Vertikalreihen von $P_{\varkappa-1}$ unabhängig; also würde bereits zu einer gewissen Zahl $< r_\varkappa$ eine Substitution gehören müssen, in welcher mindestens $j'$ Vertikalreihen sämtlich $\xi = 0$ machen.

Aus dem Umstande, daß (31) keinen Gitterpunkt im Inneren enthält, folgt wie im ersten Beweise des Hilfssatzes II (s. 6.), daß die Determinante $|p_k^{(h)}|$ von $P$ dem Betrage nach $\leqq n!$ ist.

10. Es sei $n > 1$. Ferner wollen wir von dem Falle absehen, daß $n = 2$ und $a$ komplex ist; alsdann würde $|\xi| = |x_1 + a x_2|$ unter einer

gegebenen Grenze nur für eine endliche Anzahl von ganzzahligen Systemen $x_1, x_2$ liegen, wäre also die Substitutionenkette zu $a$ jedenfalls eine abbrechende; andererseits ist eine komplexe Größe $a = b + ic$ dann und nur dann eine algebraische Zahl zweiten Grades, wenn $b$ sowie $c^2$ rational sind.

Auf Grund der in 8. entwickelten Begriffe entsteht nun folgendes vollständige

*Kriterium für die algebraischen Zahlen $n^{ten}$ Grades:*

Es sei $a$ eine beliebige reelle oder komplexe Größe, im ersten Falle $\sigma = 1$, im zweiten $\sigma = 2$ und $n > \sigma$. Es sei

$$\xi = x_1 + ax_2 + \cdots + a^{n-1}x_n,$$

sodann $P_1, P_2, P_3, \ldots$ die zu $a$ gehörige Kette von Substitutionen mit $n$ Variablen, und $\chi_1, \chi_2, \chi_3, \ldots$ seien die Formen, in welche $\xi$ durch $P_1, P_2, P_3, \ldots$ übergeht.

1⁰ *Ist $a$ nicht eine algebraische Zahl $n^{ten}$ oder niederen Grades, so bricht die Kette niemals ab, und alle Gleichungen $\chi_1 = 0, \chi_2 = 0, \ldots$ sind verschieden* (d. h. keine zwei der Formen $\chi_1, \chi_2, \ldots$ unterscheiden sich bloß durch einen Faktor). In jeder Form $\chi_\varkappa$ sind alle Koeffizienten von Null verschieden.

2⁰ *Ist $a$ eine algebraische Zahl $n^{ten}$ Grades, so bricht die Kette niemals ab, unter den Gleichungen $\chi_1 = 0, \chi_2 = 0, \ldots$ kommen nur eine* ***endliche*** *Anzahl verschiedener vor* (d. h. alle diese unendlich vielen Formen entstehen aus einer endlichen Anzahl unter ihnen durch Multiplikation mit Faktoren), *in jeder Form $\chi_\varkappa$ sind alle Koeffizienten von Null verschieden.*

3⁰ Ist $a$ eine algebraische Zahl $n - m^{\text{ten}}$ Grades, wo $m > 0$ und $n - m > \sigma$ ist, so bricht die Kette niemals ab, unter den Gleichungen $\chi_1 = 0, \chi_2 = 0, \ldots$ kommen nur eine endliche Anzahl verschiedener vor, in den Formen $\chi_\varkappa$ sind von einer gewissen an stets die $m$ ersten Koeffizienten $= 0$, die übrigen $n - m$ sind beständig von Null verschieden.

4⁰ Ist $a$ eine algebraische Zahl $\sigma^{\text{ten}}$ Grades (also reell und rational oder komplex und vom zweiten Grade), so bricht die Kette nach einer endlichen Anzahl von Gliedern ab.

11. Wir beginnen den Nachweis dieses Satzes mit der Feststellung, daß, wenn zwei der Gleichungen $\chi_1 = 0, \chi_2 = 0, \ldots$ identisch sind, die Größe $a$ notwendig eine algebraische Zahl $n^{\text{ten}}$ oder niederen Grades ist.

Es seien also $\chi_\iota$ und $\chi_\varkappa$ zwei unter jenen Formen, die sich bloß durch einen Faktor $\theta$ unterscheiden, so daß $\chi_\varkappa = \theta\chi_\iota$ ist. Es sei $\iota < \varkappa$, so ist zufolge der Bemerkungen bei (30) der Betrag $|\theta| < 1$. Es seien $P_\iota$ und $P_\varkappa$ die Substitutionen der Kette, welche $\xi$ in $\chi_\iota$ und $\chi_\varkappa$ überführen. Durch $P_\varkappa P_\iota^{-1}$ geht dann $\xi$ in $\theta\chi_\iota P_\iota^{-1}$, d. i. in $\theta\xi$ über. Es sei

(32) $$|q_h^{(k)}| \qquad (h, k = 1, \ldots, n),$$

$h$ als den Index der Horizontal-, $k$ als den Index der Vertikalreihen gedacht, das Koeffizientensystem der Substitution $P_\varkappa P_\iota^{-1}$, so ergibt die Vergleichung der Koeffizienten in den Formen $\theta\xi$ und $\xi P_\varkappa P_\iota^{-1}$:

(33) $$\theta a^{k-1} = q_1^{(k)} + a q_2^{(k)} + \cdots + a^{n-1} q_n^{(k)} \qquad (k = 1, \ldots, n).$$

Die Koeffizienten $q_h^{(k)}$ sind sämtlich rationale Zahlen. Man entnimmt aus diesen Gleichungen, daß die Determinante

(34) $$|\theta e_h^{(k)} - q_h^{(k)}| = 0 \qquad \begin{pmatrix} e_h^{(k)} = 0,\ h \neq k;\ e_h^{(h)} = 1 \\ h, k = 1, \ldots, n \end{pmatrix}$$

ist, eine Gleichung, die symbolisch $|\theta P_\iota P_\iota^{-1} - P_\varkappa P_\iota^{-1}| = 0$ geschrieben werden kann.

Nimmt man zwei aufeinanderfolgende der Gleichungen (33), für $k = j$ und $k = j + 1$ $(j = 1, \ldots, n-1)$, so entsteht aus ihnen durch Elimination von $\theta$:

(35) $$q_1^{(j+1)} + a(q_2^{(j+1)} - q_1^{(j)}) + \cdots + a^{n-1}(q_n^{(j+1)} - q_{n-1}^{(j)}) - a^n q_n^{(j)} = 0.$$

Man hat $n-1$ solcher Gleichungen für $j = 1, \ldots, n-1$.

*Entweder* ist nun wenigstens eine unter ihnen so beschaffen, daß in ihr nicht alle Koeffizienten der Potenzen von $a$ Null sind; dann erweist sich durch die betreffende Gleichung die Größe $a$ als eine algebraische Zahl $n^{\text{ten}}$ oder niederen Grades.

*Oder* aber, es wären die Ausdrücke in $a$ auf den linken Seiten der Gleichungen (35) für $j = 1, \ldots, n-1$ sämtlich identisch gleich Null; dann hätte man

(36) $$q_1^{(j+1)} = 0, \quad q_2^{(j+1)} = q_1^{(j)}, \ldots, q_n^{(j+1)} = q_{n-1}^{(j)}, \quad 0 = q_n^{(j)}$$

für $j = 1, \ldots, n-1$, also zuvörderst

$$q_1^{(2)} = 0,\ q_1^{(3)} = 0,\ \ldots,\ q_1^{(n)} = 0; \quad q_n^{(1)} = 0,\ q_n^{(2)} = 0,\ \ldots,\ q_n^{(n-1)} = 0,$$

sodann allgemein, wenn $k > h$ ist, $q_h^{(k)} = q_{h-1}^{(k-1)} = \cdots = q_1^{(k-h+1)} = 0$, und wenn $k < h$ ist, $q_h^{(k)} = q_{h+1}^{(k+1)} = \cdots = q_n^{(n-h+k)} = 0$, endlich noch $q_1^{(1)} = q_2^{(2)} = \cdots = q_n^{(n)}$, welcher Wert $= q$ gesetzt werde. Nunmehr würden die Gleichungen (33) in $\theta a^{k-1} = q a^{k-1}$ $(k = 1, \ldots, n)$ übergehen; man fände $\theta = q$ und hätte allgemein $q_h^{(k)} = q e_h^{(k)}$, also $P_\varkappa P_\iota^{-1} = q P_\iota P_\iota^{-1}$, mithin $P_\varkappa = \theta P_\iota$; jeder Koeffizient in $P_\varkappa$ wäre gleich dem entsprechenden Koeffizienten aus $P_\iota$, multipliziert in $\theta$. Nun hat von den Koeffizienten in $P_\varkappa$ wenigstens einer einen Betrag $= r_\varkappa$ und die Beträge der Koeffizienten in $P_\iota$ sind sämtlich $\leqq r_\iota$; es würde somit $r_\varkappa \leqq |\theta| r_\iota$ folgen, was mit $r_\varkappa > r_\iota$ und $|\theta| < 1$ im Widerspruch stünde. Die zweite Annahme, daß keine der Gleichungen (34) eine Bedingung für $a$ gibt, ist danach unzulässig, und mithin ist notwendig $a$ eine algebraische Zahl $n^{\text{ten}}$ oder niederen Grades.

12. Wir ziehen jetzt die Ergebnisse des § 1 heran. Es sei $\varepsilon$ eine beliebige positive Größe; wir nehmen für die linearen Formen $\xi_1, \xi_2, \ldots$, an welche die Betrachtungen in § 1 anknüpfen, die $n+1$ Formen

$$x_1, \ldots, x_n \quad \text{und} \quad \frac{\xi}{\varepsilon} = \frac{1}{\varepsilon}(x_1 + a x_2 + \cdots + a^{n-1} x_n).$$

Der Körper $K$ wird dann der durch

$$-1 \leqq x_1 \leqq 1, \ \ldots, \ -1 \leqq x_n \leqq 1, \quad |\xi| \leqq \varepsilon \tag{37}$$

bestimmte Bereich. In diesem Bereich ist offenbar stets

$$|\xi| \leqq 1 + |a| + \cdots + |a^{n-1}|,$$

welche Größe $C^*$ heiße; wir wollen deshalb jedenfalls $\varepsilon \leqq C^*$ voraussetzen. Wir haben nach (12) die fundamentale Ungleichung

$$F_1 \ldots F_n J \leqq n! \, 2^n, \tag{12b}$$

wo $J$ das Volumen von $K$ ist und die Bedeutung von $F_1, \ldots, F_n$ aus 3. zu ersehen ist.

Es werde $\sigma = 1$ gesetzt, wenn $a$ reell ist, $\sigma = 2$, wenn $a$ komplex ist, und im letzteren Falle setze man $\xi = \eta + i\zeta$, so daß $\eta$ und $\zeta$ Formen mit reellen Koeffizienten sind. Die Bedingung $|\xi| \leqq \varepsilon$ kommt für $\sigma = 1$ auf $-\varepsilon \leqq \xi \leqq \varepsilon$, für $\sigma = 2$ auf $\eta^2 + \zeta^2 \leqq \varepsilon^2$ hinaus. Denkt man sich zu $\xi$, bzw. zu $\eta$, $\zeta$ weitere $n - \sigma$ reelle lineare Formen $v_1, \ldots, v_{n-\sigma}$ hinzugenommen, so daß $n$ Formen mit einer Determinante 1 entstehen, so erkennt man, daß mit nach Null abnehmendem $\varepsilon$ das Verhältnis $\frac{J}{2\varepsilon}$ für $\sigma = 1$ oder $\frac{J}{\pi\varepsilon^2}$ für $\sigma = 2$ nach dem Werte des über den Bereich

$$|\xi| = 0, \quad -1 \leqq x_1 \leqq 1, \ \ldots, \ -1 \leqq x_n \leqq 1$$

erstreckten Integrals $\int dv_1 \ldots dv_{n-\sigma}$, also nach einer bestimmten positiven Größe konvergiert. Danach wird man eine endliche von $a$ abhängende, *von* $\varepsilon$ aber *unabhängige* Größe $M$ angeben können, so daß für alle Werte $\varepsilon \leqq C^*$ stets

$$\left(\frac{n! \, 2^n}{J}\right)^{\frac{1}{\sigma}} \varepsilon \leqq M \tag{38}$$

ist. Die Ungleichung (12b) geht dann in

$$\varepsilon (F_1 \ldots F_n)^{\frac{1}{\sigma}} \leqq M \tag{39}$$

über. Wegen $F_1 \leqq \cdots \leqq F_n$ erhält man daraus insbesondere

$$\varepsilon F_1^{\frac{n}{\sigma}} \leqq M \tag{40}$$

und ferner

$$\varepsilon^\sigma F_1^{n-1} F_n \leqq M^\sigma. \tag{41}$$

Nunmehr sollen einige Folgerungen aus diesen Ungleichungen (40) und (41) entwickelt werden.

13. Wenn in einer Form $\chi$ zur Kette der erste Koeffizient $\alpha_1 = 0$ ausfällt, erweist sich durch diese Gleichung $a$ als eine algebraische Zahl $n-1^{\text{ten}}$ oder niederen Grades. Eine solche Beschaffenheit von $a$ wollen wir zunächst ausschließen. Dann ist also für jedes Kettenglied gewiß $|\alpha_1| > 0$. Wir zeigen, daß alsdann im Verlauf der Kette der Betrag $|\alpha_1|$ schließlich unter jede Grenze sinken muß.

Es sei $P$ in (27) eine zur Zahl $r$ gehörende Substitution, $\chi$ in (28) die zugehörige Transformierte von $\xi$. Wir nehmen in 12. den Parameter $\varepsilon = \frac{|\alpha_1|}{r}$; (diese Größe ist $\leqq C^*$, weil $|p_1^{(1)}|, \ldots, |p_n^{(1)}| \leqq r$ ist). Man hat hier ein von $0, \ldots, 0$ verschiedenes ganzzahliges System $x_1, \ldots, x_n$, wofür $|x_k| \leqq r$ $(k = 1, \ldots, n)$ und $\left|\frac{\xi}{\varepsilon}\right| = \frac{|\alpha_1|}{\left|\frac{\alpha_1}{r}\right|} = r$ ist, aber kein System dieser Art, wofür stets $|x_k| < r$ und $\left|\frac{\xi}{\varepsilon}\right| < r$ wäre. Nach der Bedeutung von $F_1$ (s. 3.) ist daher dann $F_1 = r$. Die Ungleichung (40) ergibt nunmehr

$$|\alpha_1| \leqq M r^{-\frac{n-\sigma}{\sigma}}. \tag{42}$$

Diese Abschätzung für $|\alpha_1|$ zeigt in der Tat, daß mit wachsendem $r$ der Wert $|\alpha_1|$ schließlich unter jede Grenze sinken muß.*) In den bezeichneten Fällen, in denen $\alpha_1$ niemals Null werden kann, hat infolgedessen die Kette notwendig einen unendlichen Verlauf, sie kann niemals abbrechen.

Insbesondere bricht auf diese Weise die Kette niemals ab, wenn $a$ *nicht* eine algebraische Zahl $n^{\text{ten}}$ oder niedrigeren Grades ist. Verbindet

*) Sind $\alpha$, $\beta$ zwei reelle Größen und ist $0 < |\beta| \leqq |\alpha|$, so hat man eine ganze Zahl $y$, so daß $|\alpha + y\beta| \leqq \frac{1}{2}|\beta|$ ist. Sind $\alpha$, $\beta$, $\gamma$ drei reelle oder komplexe Größen, so daß $0 < |\gamma| \leqq |\beta| \leqq |\alpha|$ und $\frac{\gamma}{\beta} = \delta + i\varepsilon$ nicht reell, also $\varepsilon \neq 0$ ist, so kann man zwei reelle Größen $v$, $w$ finden, so daß $\alpha + v\beta + w\gamma = \alpha + (v + \delta w)\beta + iw\varepsilon\beta = 0$ ist, und sind dann $z$ und $y$ zwei ganze Zahlen, so daß $|z - w| \leqq \frac{1}{2}$ und $|y + \delta z - v - \delta w| \leqq \frac{1}{2}$ ist, so wird $|\alpha + y\beta + z\gamma| \leqq \frac{1}{\sqrt{2}}|\beta|$. Mit diesen Hilfsmitteln kann man direkt einsehen, daß in den Formen $\chi$ zur Kette sogar $|\alpha_n|$ schließlich unter jede Grenze sinkt, mit Ausnahme des Falles, daß $n = 3$, $a$ komplex und der reelle Teil von $a$ rational ist, in welchem Falle nur $|\alpha_1|$ und $|\alpha_2|$ unter jede Grenze sinken, aber für $|\alpha_3|$ eine positive untere Grenze besteht, und ferner der Fälle, daß $a$ eine algebraische Zahl $\sigma^{\text{ten}}$ Grades ist, in welchen Fällen die Kette mit einem letzten Gliede abbricht.

man hiermit das Ergebnis aus 11., wonach unter derselben Voraussetzung niemals zwei der Formen $\chi_z$ sich bloß durch einen Faktor unterscheiden, so ist zunächst der Punkt $1^0$ unseres Kriteriums völlig sichergestellt.

14. Um den Punkt $2^0$ zu erweisen, nehmen wir nunmehr an, daß $a$ als eine algebraische Zahl $n^{\text{ten}}$ Grades gegeben ist. In diesem Falle können wir außer mit der Ungleichung (39) noch mit dem Satze operieren, daß die *Norm* einer von Null verschiedenen *ganzen* algebraischen Zahl eine von Null verschiedene *ganze rationale* Zahl und daher dem Betrage nach $\geqq 1$ ist.

Es sei

$$g_0 a^n + g_1 a^{n-1} + \cdots + g_n = 0 \tag{43}$$

die Gleichung $n^{\text{ten}}$ Grades mit rationalen ganzen Koeffizienten ohne gemeinsamen Teiler und positivem $g_0$, der $a$ genügt. Es sei, wenn $a$ komplex, $\sigma = 2$ ist, $a^0$ die zu $a$ konjugiert imaginäre Größe. Die Wurzeln jener Gleichung $n^{\text{ten}}$ Grades außer $a$, bzw. außer $a$ und $a^0$, mögen $a', a'', \ldots, a^{(n-\sigma)}$ heißen. Ferner sollen die zu einer Zahl $\xi$ des Körpers von $a$ konjugierten Zahlen in den Körpern von $(a^0), a', \ldots, a^{(n-\sigma)}$ mit $(\xi^0), \xi', \ldots, \xi^{(n-\sigma)}$ bezeichnet werden.

Das Multiplum $g_0 a$ ist eine *ganze* algebraische Zahl $n^{\text{ten}}$ Grades. Infolgedessen ist für ein ganzzahliges, von $0, \ldots, 0$ verschiedenes System $x_1, \ldots, x_n$ der Wert von $g_0^{n-1}\xi$ stets eine von Null verschiedene *ganze* Zahl im Körper von $a$ und daher deren Norm in diesem Körper $Nm(g_0^{n-1}\xi) = g_0^{n(n-1)}\xi(\xi^0)\xi' \ldots, \xi^{(n-\sigma)}$ dem Betrage nach $\geqq 1$; der eingeklammerte Faktor $\xi^0$ kommt für $\sigma = 2$ in Betracht und dann ist $|\xi^0| = |\xi|$. Es sei $C$ der größte Wert unter den $n - \sigma$ Ausdrücken $1 + |a^{(j)}| + \cdots + |a^{(j)}|^{n-1}$ für $j = 1, \ldots, n - \sigma$. Sind $x_1, \ldots, x_n$ in ihren Beträgen $\leqq r$, wo $r$ eine positive Größe ist, so hat man

$$|\xi^{(j)}| \leqq Cr \qquad (j = 1, \ldots, n - \sigma) \tag{44}$$

und entsteht nunmehr die Ungleichung $g_0^{n(n-1)} C^{n-\sigma} |\xi|^\sigma r^{n-\sigma} \geqq 1$ oder

$$|\xi|^\sigma r^{n-\sigma} \geqq b^\sigma, \tag{45}$$

wo $b$ eine gewisse, nur von $a$, nicht von der Größe von $r$ abhängende Konstante vorstellt.

Es sei wieder $P$ die zu einer ganzen Zahl $r$ gehörende Substitution der Kette und $\chi$ in (28) die Form $\xi P$. Dann geht, wenn für $x_1, \ldots, x_n$ die erste Vertikalreihe von $P$ genommen wird, aus (45) zuvörderst

$$|\alpha_1| \geqq b r^{-\frac{n-\sigma}{\sigma}} \tag{46}$$

hervor.

Es sei sodann $\varepsilon$ wieder eine beliebige positive Größe $\leqq C^*$ und betrachten wir die Ungleichung (41) dafür. Nach der Bedeutung von $F_1$

in 12. hat man ein von $0, \ldots, 0$ verschiedenes ganzzahliges System $x_1, \ldots, x_n$, wofür $|x_k| \leqq F_1$ $(k = 1, \ldots, n)$ und $\left|\frac{\xi}{\varepsilon}\right| \leqq F_1$, also $|\xi| \leqq \varepsilon F_1$ ist. Die Ungleichung (45) ergibt daher $(\varepsilon F_1)^\sigma F_1^{n-\sigma} \geqq b^\sigma$ oder

$$\varepsilon F_1^{\frac{n}{\sigma}} \geqq b. \tag{47}$$

Führt man die hierdurch angewiesene untere Grenze in (41) ein, so folgt

$$\varepsilon F_n^{\frac{n}{\sigma}} \leqq B, \tag{48}$$

wo $B = \frac{M^n}{b^{n-1}}$ wieder eine nur von $a$, nicht von $\varepsilon$ abhängende Konstante vorstellt.

Nunmehr wollen wir speziell $\varepsilon = \frac{|\alpha_n|}{r}$ nehmen, wo $\alpha_n$ der letzte Koeffizient in $\chi$ ist. Dann ist $F_n = r$; denn man hat hier $n$ unabhängige ganzzahlige Systeme $x_1, \ldots, x_n$, für welche $|x_k| \leqq r$ $(k = 1, \ldots, n)$ und $\left|\frac{\xi}{\varepsilon}\right| \leqq \frac{|\alpha_n|}{\left|\frac{\alpha_n}{r}\right|} = r$ ist, aber nach der Bedeutung von $|\alpha_n|$ jedenfalls nicht $n$ unabhängige ganzzahlige Systeme $x_1, \ldots, x_n$, für welche $|x_k| < r (k = 1, \ldots, n)$ und $\left|\frac{\xi}{\varepsilon}\right| < r$ wäre. Die Formel (48) ergibt nunmehr

$$|\alpha_n| \leqq B r^{-\frac{n-\sigma}{\sigma}}. \tag{49}$$

Wir stellen (46), (49) und (29) zusammen in:

$$b r^{-\frac{n-\sigma}{\sigma}} \leqq |\alpha_1| \leqq \cdots \leqq |\alpha_n| \leqq B r^{-\frac{n-\sigma}{\sigma}}. \tag{50}$$

Man ersieht daraus zunächst, daß im Verlauf der Kette selbst $|\alpha_n|$ schließlich unter jede Grenze sinkt. Die Kette bricht also jedenfalls niemals ab.

Gewisse weitere Ungleichungen erschließen wir für die Normen der Zahlen $\alpha_k (k = 1, \ldots, n)$ und für ihre konjugierten Zahlen $\alpha_k^{(j)}$. Nach (44) werden wir, da die Zahlen der $k^{\text{ten}}$ Vertikalreihe von $P$, welche $\xi = \alpha_k$ machen, $\leqq r$ sind,

$$|\alpha_k^{(j)}| \leqq Cr \qquad (j = 1, \ldots, n - \sigma) \tag{51}$$

haben. Nehmen wir dazu die in (49) erhaltene obere Grenze für $|\alpha_k|$, womit noch im Falle $\sigma = 2$ sich $|\alpha_k^0|$ deckt, so folgt

$$|Nm(g_0^{n-1}\alpha_k)| \leqq g_0^{n(n-1)} B^\sigma C^{n-\sigma}, \tag{52}$$

wo die Grenze rechts nur von $a$, nicht von der Zahl $r$ abhängig erscheint. Nun ist $Nm(g_0^{n-1}\alpha_k)$ eine ganze rationale Zahl und daher nach dieser Ungleichung nur einer endlichen Anzahl von Werten bei allen möglichen Werten von $r$ fähig.

Andererseits hat man, indem diese Zahl $Nm(g_0^{n-1}\alpha_k)$ von Null verschieden ist:

$$|Nm(g_0^{n-1}\alpha_k)| = g_0^{n(n-1)}|\alpha_k(\alpha_k^0)\alpha_k' \cdots \alpha_k^{(n-\sigma)}| \geqq 1. \tag{53}$$

Führt man hierin für $|\alpha_k|(|\alpha_k^0|)$ die obere Grenze aus (50) und für die Beträge $|\alpha_k'|, \ldots, |\alpha_k^{(n-\sigma)}|$ mit Ausnahme eines Faktors $|\alpha_k^{(j)}|$ die obere Grenze aus (51) ein, so folgt für diesen noch übrigen Betrag:

$$|\alpha_k^{(j)}| \geqq cr \qquad (j = 1, \ldots, n-\sigma), \tag{54}$$

wo $c = \frac{1}{g_0^{n(n-1)}B^\sigma C^{n-\sigma-1}}$ wieder nur von $a$, nicht von $r$ abhängig ist.

Sind nun $h$, $k$ irgend zwei der Indizes $1, 2, \ldots, n$, so hat man wegen (50):

$$\left|\frac{\alpha_k}{\alpha_h}\right| \left(= \left|\frac{\alpha_k^0}{\alpha_h^0}\right|\right) \leqq \frac{B}{b} \tag{55}$$

und aus (51) und (54):

$$\left|\frac{\alpha_k^{(j)}}{\alpha_h^{(j)}}\right| \leqq \frac{C}{c} \qquad (j = 1, \ldots, n-\sigma). \tag{56}$$

Zudem sind $g_0^{n-1}\alpha_h$ und $g_0^{n-1}\alpha_k$ und alle ihre konjugierten Zahlen ganze algebraische Zahlen und liegt nach (52) die ganze rationale Zahl $|Nm(g_0^{n-1}\alpha_h)|$ unter einer bestimmten von $a$ allein abhängenden Grenze. Aus diesen Umständen geht hervor, daß in der algebraischen Gleichung $n^{\text{ten}}$ Grades für $t$:

$$Nm(g_0^{n-1}\alpha_h) \cdot \left(t - \frac{\alpha_k}{\alpha_h}\right)\left(\left(t - \frac{\alpha_k^0}{\alpha_h^0}\right)\right)\left(t - \frac{\alpha_k'}{\alpha_h'}\right) \cdots \left(t - \frac{\alpha_k^{(n-\sigma)}}{\alpha_h^{(n-\sigma)}}\right) = 0 \tag{57}$$

alle $n+1$ Koeffizienten der linken Seite ganze rationale Zahlen sind und in ihren Beträgen unterhalb bestimmter nur von $a$ abhängender Grenzen liegen. Danach kommen für die Koeffizienten dieser Gleichung von vornherein für alle $r$ nur eine endliche Anzahl von Wertsystemen und also für ein jedes Verhältnis $\frac{\alpha_k}{\alpha_h}$ von vornherein für alle $r$ nur eine endliche Anzahl von algebraischen Zahlen in Betracht. Mithin können in der Tat die sämtlichen unendlich vielen Linearformen $\chi_1, \chi_2, \ldots$ der Kette hier, wo $a$ eine algebraische Zahl $n^{\text{ten}}$ Grades ist, nur eine *endliche* Anzahl von verschiedenen Verhältnissen $\alpha_1 : \alpha_2 : \ldots : \alpha_n$ der Koeffizienten darbieten, sie gehen also sämtlich aus einer endlichen Anzahl unter ihnen durch Multiplikation mit Faktoren hervor. Damit ist der Punkt $2^0$ unseres Kriteriums völlig erwiesen.

15. Wir können noch eine Bemerkung über die Natur derjenigen Faktoren $\theta$ hinzufügen, die hier in Beziehungen $\chi_\varkappa = \theta\chi_\iota$ auftreten und die als Quotienten von Zahlen im Körper von $a$ jedenfalls auch in diesem Körper liegen.

Zu jeder Substitution $P_\iota$ der Kette kann man nach der in 2. auseinandergesetzten Methode eine ganzzahlige Substitution $A_\iota$ mit einer Determinante $\pm 1$ bestimmen, so daß die Koeffizienten in $P_\iota^{-1}A_\iota$ den in (8) und (9) für die Zahlen $\gamma_h^{(k)}$ angegebenen Bedingungen entsprechen. In dieser Substitution $P_\iota^{-1}A_\iota$ sind die Koeffizienten rationale Zahlen mit der Determinante von $P_\iota$ als Nenner. Letztere ist nach dem in 9. Bewiesenen stets dem Betrage nach $\leqq n!$. Nach den Bedingungen (8) und (9) kommen dadurch für alle Koeffizienten von $P_\iota^{-1}A_\iota$ von vornherein nur eine endliche Anzahl verschiedener Werte in Frage. Verbindet man damit das soeben in 14. erzielte Resultat, so erkennt man, daß auch für den Inbegriff der Gleichung $\chi_\iota = 0$ und der Substitution $P_\iota^{-1}A_\iota$ zusammen in der ganzen unendlichen Kette nur eine endliche Anzahl von verschiedenen Bestimmungen vorkommen.

Hat man nun für zwei Indizes $\iota$ und $\varkappa$ sowohl $\chi_\varkappa = \theta\chi_\iota$, wo $\theta$ ein Faktor ist, als auch $P_\varkappa^{-1}A_\varkappa = P_\iota^{-1}A_\iota$, so wird $P_\varkappa P_\iota^{-1} = A_\varkappa A_\iota^{-1}$, also eine ganzzahlige Substitution mit einer Determinante $\pm 1$. Durch diese Substitution geht die Linearform $\xi$ (in (26)) in $\theta\xi$ über, während $A_\iota A_\iota^{-1}$, d. i. die identische Substitution, $\xi$ in $\xi$ überführt. Für den Faktor $\theta$ erhält man dadurch eine Gleichung $n^{\text{ten}}$ Grades, welche sich in der oben bei (34) erklärten symbolischen Weise $|\theta A_\iota A_\iota^{-1} - A_\varkappa A_\iota^{-1}| = 0$ oder $|\theta A_\iota - A_\varkappa| = 0$ schreiben läßt. In dieser Gleichung sind alle Koeffizienten ganze rationale Zahlen und ist sowohl der erste wie der letzte Koeffizient gleich $\pm 1$. Also ist dann sowohl $\theta$ wie $\frac{1}{\theta}$ eine ganze algebraische Zahl, mithin $\theta$ eine Einheit in dem Zahlenkörper von $a$. Sonach gilt der Zusatz: Unter den Formen $\chi_1, \chi_2, \ldots$ der Kette kann man eine endliche Anzahl angeben so, daß aus ihnen alle Formen der Kette durch Multiplikation mit solchen Faktoren hervorgehen, welche *Einheiten* im Körper von $a$ sind.

Ist $\chi_\iota = \alpha_1 z_1 + \cdots + \alpha_n z_n$, $\chi_\varkappa = \beta_1 z_1 + \cdots + \beta_n z_n$ und sind $r_\iota$, $r_\varkappa$ die Zahlen, zu denen $P_\iota$, $P_\varkappa$ gehören, so hat man ferner nach (51) und (54)

$$cr_\iota \leqq |\alpha_k^{(j)}| \leqq Cr_\iota, \quad cr_\varkappa \leqq |\beta_k^{(j)}| \leqq Cr_\varkappa \quad \begin{pmatrix} k = 1, \ldots, n, \\ j = 1, \ldots, n-\sigma \end{pmatrix};$$

indem $\beta_k = \theta\alpha_k$ ist, folgt daraus

$$\frac{c}{C}\frac{r_\varkappa}{r_\iota} \geqq |\theta^{(j)}| \leqq \frac{C}{c}\frac{r_\varkappa}{r_\iota} \qquad (j = 1, \ldots, n-\sigma).$$

Man hat sodann die von den Zahlen $r_\iota$, $r_\varkappa$ freie Beziehung

$$\frac{c^2}{C^2} \leqq \left|\frac{\theta^{(j_*)}}{\theta^{(j)}}\right| \leqq \frac{C^2}{c^2} \quad (j_* \neq j; j, j_* = 1, \ldots, n-\sigma). \tag{58}$$

Für die Einheiten $\theta$, auf die man hier geführt wird, liegen also die Verhältnisse der Beträge der $n-\sigma$ konjugierten Werte $\theta', \ldots, \theta^{(n-\sigma)}$ stets zwischen zwei von vornherein anzuweisenden Grenzen, ein Umstand, der

für die weitere Erforschung der Substitutionenketten zu algebraischen Zahlen $n^{\text{ten}}$ Grades von hervorragender Bedeutung ist.

16. Es sei jetzt $a$ eine algebraische Zahl $n - m^{\text{ten}}$ Grades, wo $m > 0$ und $< n$ ist, und es sei

$$g_{n-m} + g_{n-m-1}a + \cdots + g_0 a^{n-m} = 0 \tag{59}$$

die Gleichung $n - m^{\text{ten}}$ Grades mit rationalen ganzen Koeffizienten ohne gemeinsamen Teiler und positivem $g_0$, der $a$ genügt. Es sei unter den Beträgen der Koeffizienten dieser Gleichung der größte Wert $g^*$. Man entnimmt aus (59)

$$g_{n-m}a^{h-1} + g_{n-m-1}a^h + \cdots + g_0 a^{n-m+h-1} = 0 \quad (h = 1, \ldots, m),$$

d. i. $x_1 + ax_2 + \cdots + a^{n-1}x_n = 0$ für gewisse $m$ besondere, von $0, \ldots, 0$ verschiedene ganzzahlige Systeme $x_1, \ldots, x_n$. Diese $m$ Systeme sind voneinander unabhängig, denn schreibt man sie in $m$ Vertikalreihen auf, so hat man in den letzten $m$ Horizontalreihen der entstehenden Matrix, welche die Werte $x_{n-m+1}, \ldots, x_n$ enthalten, ein quadratisches Schema, wobei in der Hauptdiagonale alle Elemente $= g_0$ und unterhalb derselben alle Elemente $= 0$ sind, ein Schema also, das die von Null verschiedene Determinante $g_0^m$ ergibt. Alle jene Zahlen $x_1, \ldots, x_n$ sind ferner dem Betrage nach $\leqq g^*$.

Es sei nun $P$ eine zur Zahl $r$ gehörende Substitution der Kette und $\chi$ die Form, in welche $\xi$ durch $P$ übergeht. Aus dem eben Gesagten erkennt man, daß, sowie $r \geqq g^*$ ist, in $\chi$ jedenfalls $\alpha_1 = 0, \ldots, \alpha_m = 0$ sein muß. Dagegen muß stets $\alpha_{m+1}$ von Null verschieden bleiben. Denn hätte man $m + 1$ unabhängige ganzzahlige Systeme $x_1, \ldots, x_n$, wofür $\xi = 0$ ausfiele, so würde man aus den betreffenden $m + 1$ Gleichungen durch $m$ Mal hintereinander vorgenommene Elimination der jedesmal sich darbietenden höchsten Potenz von $a$ schließlich eine Gleichung für $a$ mit rationalen Koeffizienten von einem Grade $< n - m$ gewinnen können.

Es sei wieder $\sigma = 1$ oder $= 2$, je nachdem $a$ reell oder komplex ist, und im letzteren Falle sei $a^0$ die zu $a$ konjugiert imaginäre Zahl. Ferner seien $a', a'', \ldots, a^{(n-m-\sigma)}$ die Wurzeln der Gleichung $n - m^{\text{ten}}$ Grades für $a$ außer $a$, bzw. außer $a$ und $a^0$. Endlich, wenn $\alpha$ eine Zahl im Körper von $a$ bedeutet, so seien allgemein $(\alpha^0), \alpha', \ldots, \alpha^{(n-m-\sigma)}$ die konjugierten Zahlen in den Körpern von $(a^0), a', \ldots, a^{(n-m-\sigma)}$.

Wir können jetzt die in 14. gewonnenen Sätze über die Substitutionenketten mit $n$ Variablen zu algebraischen Zahlen $n^{\text{ten}}$ Grades in der Weise heranziehen, daß wir die Zahl $n$ dort durch den Wert $n - m$ hier ersetzen. Das in (49) liegende Resultat zeigt alsdann, daß man im gegenwärtigen Falle zur beliebigen Zahl $r$ stets $n-m$ ganzzahlige Systeme $y_1 = y_1^{(k)}, \ldots, y_{n-m} = y_{n-m}^{(k)} (k = 1, \ldots, n-m)$ mit von Null verschiedener Determinante finden

kann, so daß alle Zahlen $y_h^{(k)}$ darin dem Betrage nach $\leqq r$ sind, und daß für jedes einzelne dieser $n-m$ Systeme

$$|y_1 + ay_2 + \cdots + a^{n-m-1}y_{n-m}| \leqq \overline{B} r^{-\frac{n-m-\sigma}{\sigma}}$$

ausfällt, wo $\overline{B}$ eine gewisse nur von $a$, nicht von $r$ abhängende Konstante ist. Setzt man zu jedem dieser Systeme $y_1, \ldots, y_{n-m}$ dann $x_1 = y_1, \ldots, x_{n-m} = y_{n-m}$, $x_{n-m+1} = 0, \ldots, x_n = 0$, so bekommt man $n-m$ ganzzahlige Systeme $x_1, \ldots, x_n$, die von den oben erwähnten speziellen $m$ solchen Systemen unabhängig sind. Danach wird man, sowie $r \geqq g^*$ ist, außer $|\alpha_1| = \cdots = |\alpha_m| = 0$ weiter stets

$$0 < |\alpha_{m+1}| \leqq \cdots \leqq |\alpha_n| \leqq \overline{B} r^{-\frac{n-m-\sigma}{\sigma}} \tag{60}$$

haben.

Es sei jetzt zuvörderst $n - m > \sigma$. Alsdann erkennt man aus (60), daß die Beträge $|\alpha_{m+1}|, \ldots, |\alpha_n|$ im Verlauf der Kette unter jede Grenze sinken, ohne jemals Null zu werden; die Kette bricht also jedenfalls nicht ab. Man hat ferner stets

$$|\alpha_k^{(j)}| \leqq \overline{C} r \qquad \begin{pmatrix} k = m+1, \ldots, n, \\ j = 1, \ldots, n-m-\sigma \end{pmatrix}, \tag{61}$$

wenn $\overline{C}$ der größte unter den Werten $1 + |a^{(j)}| + \cdots + |a^{(j)}|^{n-1}$ $(j = 1, \ldots, n-m-\sigma)$ ist. Andererseits ist $g_0 a$ eine ganze algebraische Zahl, desgleichen daher jede Zahl $g_0^{n-1}\alpha_k$ $(k = m+1, \ldots, n)$, und da diese Zahlen von Null verschieden sind, müssen mithin ihre Normen im Körper von $a$ dem Betrage nach $\geqq 1$ sein; man hat also

$$g_0^{(n-m)(n-1)} |\alpha_k|^\sigma |\alpha'_k \cdots \alpha_k^{(n-m-\sigma)}| \geqq 1 \qquad (k = m+1, \ldots, n). \tag{62}$$

Führt man hierin für $n-m-\sigma$ der $n-m-\sigma+1$ absoluten Beträge $|\alpha_k|, |\alpha_k'|, \ldots, |\alpha_k^{(n-m-\sigma)}|$ die in (60) bzw. (61) angewiesenen oberen Grenzen ein, so erhält man für den noch übrigen dieser Beträge eine untere Grenze; man findet

$$|\alpha_k| \geqq \overline{b} r^{-\frac{n-m-\sigma}{\sigma}}, \; |\alpha_k^{(j)}| \geqq \overline{c} r \begin{pmatrix} k = m+1, \ldots, n, \\ j = 1, \ldots, n-m-\sigma \end{pmatrix} \tag{63}$$

mit gewissen von $r$ nicht abhängenden Konstanten $\overline{b}$ und $\overline{c}$, und daraus folgt dann

$$\left|\frac{\alpha_k}{\alpha_h}\right| \left(= \left|\frac{\alpha_k^0}{\alpha_h^0}\right|\right) \leqq \frac{\overline{B}}{\overline{b}}, \quad \left|\frac{\alpha_k^{(j)}}{\alpha_h^{(j)}}\right| \leqq \frac{\overline{C}}{\overline{c}} \quad \begin{pmatrix} h, k = m+1, \ldots, n; h \neq k \\ j = 1, \ldots, n-m-\sigma \end{pmatrix}. \tag{64}$$

Andererseits findet man aus (60) und (61) die von $r$ nicht abhängende Größe $g_0^{(n-m)(n-1)} \overline{B}^\sigma \overline{C}^{n-m-\sigma}$ als obere Grenze für die Beträge der Normen von $g_0^{n-1}\alpha_k$ $(k = m+1, \ldots, n)$. Aus (64) und aus diesem letzten Umstande schließt man endlich durch die entsprechende Überlegung wie bei (57), daß für die Verhältnisse der Koeffizienten $\alpha_{m+1}, \ldots, \alpha_n$ in $\chi$ (die

Zahl $r \geqq g^*$ angenommen) nur eine endliche Anzahl von algebraischen Zahlen in Betracht kommen. Danach sind in der Tat sämtliche Formen $\chi_1, \chi_2, \ldots$ der Kette aus einer endlichen Anzahl unter ihnen durch Multiplikation mit Faktoren abzuleiten. Damit ist der Punkt $3^0$ des Kriteriums erwiesen. Indem man noch den Umstand heranzieht, daß auch im gegenwärtigen Falle nach 9. die Determinante jeder Substitution der Kette dem Betrage nach $\leqq n!$ ist, kann man wieder hinzufügen, daß sich unter den Formen $\chi_1, \chi_2, \ldots$ eine endliche Anzahl hervorheben läßt, aus denen alle diese Formen durch Multiplikation mit solchen Faktoren entstehen, welche *Einheiten* in dem Zahlenkörper von $a$ sind.

Es sei endlich $n - m = \sigma$. Ist $\sigma = 2$, also $a$ komplex, so bleiben in $\chi$ für $r \geqq g^*$ allein die Koeffizienten $\alpha_{n-1}, \alpha_n$ von Null verschieden. In den quadratischen Gleichungen

$$(t - g_0^{n-1}\alpha_{n-1})(t - g_0^{n-1}\alpha_{n-1}^0) = 0, \quad (t - g_0^{n-1}\alpha_n)(t - g_0^{n-1}\alpha_n^0) = 0$$

sind die Koeffizienten ganze rationale Zahlen und hat man durch (60) von $r$ unabhängige obere Grenzen für die Beträge derselben. Danach kommen für $\alpha_{n-1}, \alpha_n$ nur eine endliche Anzahl von Werten in Betracht. Da nun nach einer Bemerkung bei (30) alle Formen $\chi_\varkappa$ der Kette verschieden ausfallen, muß danach die Kette nach einer endlichen Anzahl von Gliedern abbrechen. — Ist $\sigma = 1$, also $a$ reell und rational, so bleibt für $r \geqq g^*$ nur $\alpha_n$ von Null verschieden, dabei ist $g_0^{n-1}\alpha_n$ eine ganze rationale Zahl und liegt zufolge (60) dem Betrage nach unterhalb einer gewissen von $r$ unabhängigen Grenze. Die Kette bricht daher auch hier nach einer endlichen Anzahl von Gliedern ab. Damit ist auch der letzte Punkt des in 10. aufgestellten Satzes bewiesen.

Zürich, den 9. Februar 1899.

XV.

# Zur Theorie der Einheiten in den algebraischen Zahlkörpern.

(Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-physikalische Klasse. 1900. S. 90—93.)
(Vorgelegt von D. Hilbert in der Sitzung vom 3. März 1900.)

In der Theorie der algebraischen Zahlen ist die Frage von Interesse, ob in einem beliebigen Galoisschen Körper stets eine Einheit existiert, welche unter ihren konjugierten Zahlen ein vollständiges System unabhängiger Einheiten des Körpers darbietet. Durch die folgenden Betrachtungen wird diese Frage in bejahendem Sinne entschieden.

1. Ich benutze dabei hauptsächlich den nachstehenden Satz über das Nichtverschwinden einer gewissen Determinante:

Hilfssatz. *Sind in einer $m$-reihigen Determinante*

$$A = |a_{hk}| \qquad (h, k = 1, 2, \ldots, m)$$

*von $m^2$ reellen Größen alle Glieder $a_{hk}$ außerhalb der Hauptdiagonale (also für $h \neq k$) $< 0$ und sind ferner die Summen*

$$a_{h1} + a_{h2} + \cdots + a_{hm} = s_h \qquad (h = 1, 2, \ldots, m)$$

*der Glieder in den einzelnen Horizontalreihen durchweg $> 0$, so ist die Determinante stets $> 0$.*

Beweis. Für $m = 1$ ist der Satz selbstverständlich. Um ihn für einen bestimmten Wert $m > 1$ zu erweisen, nehmen wir an, daß er für alle kleineren Werte des $m$ bereits sichergestellt sei. Wir setzen $a_{hh} = s_h + a_{hh}^*$ $(h = 1, 2, \ldots, m)$ und entwickeln die Determinante $A$ nach den $m$ Größen $s_1, s_2, \ldots, s_m$. Das von $s_1, s_2, \ldots, s_m$ freie Glied dieser Entwicklung wird eine $m$-reihige Determinante $A^*$, bei welcher in jeder Horizontalreihe die Summe aller Glieder Null ist und welche daher den Wert Null hat. Weiter wird der Koeffizient eines Produkts $s_{k_1} s_{k_2} \ldots s_{k_l}$, wenn $l \geqq 1$ und $< m$ ist, eine Determinante von $m - l$, also weniger als $m$ Reihen, in welcher alle Glieder außerhalb der Hauptdiagonale negativ sind und in jeder Horizontalreihe die Summe der Glieder größer als die Summe der Glieder der entsprechenden Horizontalreihe von $A^*$, also gewiß $> 0$ ist. Auf Grund

der von uns gemachten Voraussetzung erweist sich daher jeder dieser Koeffizienten $> 0$. Außerdem erscheint in jener Entwicklung noch das Glied $s_1 s_2 \ldots s_m$. Nach dieser Zusammensetzung der Determinante $A$ aus lauter positiven Termen ist sie offenbar $> 0$.

2. Es sei jetzt $\theta$ eine *algebraische Zahl* $n^{\text{ten}}$ *Grades* und unter den $n$ verschiedenen konjugierten algebraischen Zahlen $\theta_1, \theta_2, \ldots, \theta_n$, von denen $\theta$ ein Wert ist, seien $r$ reelle und $\frac{1}{2}(n-r)$ Paare von konjugiert imaginären Zahlen vorhanden. Von dem Falle $n = 2$, $r = 0$ wollen wir absehen. Wir setzen $r + \frac{1}{2}(n-r) = m + 1$, und wir wollen annehmen, daß in der Reihe der $m+1$ ersten Zahlen $\theta_1, \theta_2, \ldots, \theta_{m+1}$ die sämtlichen reellen jener Zahlen und ferner je eine Zahl aus jedem der Paare konjugiert imaginärer Zahlen sich befinden; zudem möge die Zahl $\theta$ selbst unter diesen $m+1$ Zahlen vorhanden sein. Ist $\varepsilon$ eine Einheit in dem algebraischen Körper von $\theta$, so wollen wir mit $l_h(\varepsilon)$ für $h = 1, 2, \ldots, m+1$ den reellen Teil des Logarithmus der zu $\varepsilon$ konjugierten Zahl im Körper von $\theta_h$ oder das Doppelte dieses reellen Teils verstehen, je nachdem die Zahl $\theta_h$ reell oder imaginär ist. Da die Norm einer Einheit gleich $\pm 1$ ist, gilt dann stets:

$$l_1(\varepsilon) + l_2(\varepsilon) + \cdots + l_{m+1}(\varepsilon) = 0. \tag{1}$$

Wie Dirichlet gezeigt hat, kann man in dem Körper von $\theta$ stets eine Einheit derart bestimmen, daß von ihren konjugierten Zahlen in den Körpern von $\theta_1, \theta_2, \ldots, \theta_{m+1}$ alle bis auf eine Zahl in einem beliebig angenommenen dieser Körper absolute Beträge $< 1$ haben. Es sei in solcher Weise $\varepsilon^{(h)}$ für $h = 1, 2, \ldots, m$ eine Einheit, für welche $l_1(\varepsilon^{(h)}), \ldots, l_{h-1}(\varepsilon^{(h)}), l_{h+1}(\varepsilon^{(h)}), \ldots, l_{m+1}(\varepsilon^{(h)})$, also sämtliche Werte $l_k(\varepsilon^{(h)})$ für $k \neq h$ *negativ* ausfallen. Dann ist mit Rücksicht auf (1):

$$l_1(\varepsilon^{(h)}) + \cdots + l_h(\varepsilon^{(h)}) + \cdots + l_m(\varepsilon^{(h)}) > 0.$$

Die Determinante

$$|l_k(\varepsilon^{(h)})| \qquad (h, k = 1, 2, \ldots, m)$$

trägt danach diesen Charakter, daß in ihr jeder Koeffizient außerhalb der Hauptdiagonale negativ ist und die Summe der Glieder in jeder Horizontalreihe positiv ist. Dem Hilfssatze in 1. zufolge ist daher diese Determinante $> 0$. Somit bilden die hier charakterisierten Einheiten $\varepsilon^{(1)}, \varepsilon^{(2)}, \ldots, \varepsilon^{(m)}$ ein *vollständiges* System von unabhängigen Einheiten im Körper von $\theta$.

Bei der Methode, welche Dirichlet zur Herstellung eines vollständigen Systems von unabhängigen Einheiten in einem Zahlkörper gegeben hat, werden die Einheiten des Systems sukzessive bestimmt, wobei zur Ermittlung einer weiteren Einheit, so lange das System noch nicht vollständig ist, gewisse Determinanten aus den Logarithmen der früher bestimmten Einheiten und ihrer konjugierten Zahlen bekannt sein müssen.

Nach dem hier Auseinandergesetzten ist es dagegen stets möglich, Einheiten in der erforderlichen Anzahl gesondert, jede für sich, zu bestimmen mit dem Erfolge, daß sie zusammen ein vollständiges System unabhängiger Einheiten ergeben.

3. Es sei jetzt der Körper von $\theta$ ein Galois scher Körper, so daß sich jede der Zahlen $\theta_1, \theta_2, \ldots, \theta_n$ als eine rationale Funktion mit rationalen Koeffizienten von jeder anderen dieser Zahlen darstellen läßt. Es sei in solcher Weise

$$\theta_h = R_h(\theta), \ \theta = S_h(\theta_h) \qquad (h = 1, 2, \ldots, n),$$

wo $R_h$, $S_h$ Zeichen für rationale Funktion mit rationalen Koeffizienten sind, so gilt $S_h(R_h(\theta)) = \theta$ und infolgedessen auch allgemein $S_h(R_h(\theta_k)) = \theta_k$ für jeden Index $k = 1, 2, \ldots, n$. Je nachdem $\theta$ reell oder imaginär ist, sind auch die konjugierten Zahlen alle reell oder alle imaginär, und hat man also $m + 1 = n$ oder $= \frac{1}{2} n$.

Wir bestimmen im Körper von $\theta$ eine Einheit $\varepsilon = f(\theta)$, wo $f(\theta)$ eine rationale Funktion mit rationalen Koeffizienten von $\theta$ bedeute, so daß von den $m + 1$ konjugierten Zahlen $f(\theta_1), f(\theta_2), \ldots, f(\theta_{m+1})$ alle mit Ausnahme der einen Zahl $f(\theta)$ absolute Beträge $< 1$ haben. Sodann sei $\varepsilon_h$ für $h = 1, 2, \ldots, m + 1$ die konjugierte Zahl zu $\varepsilon$ in dem Körper von $\theta_h$, also $\varepsilon_h = f(\theta_h) = f(R_h(\theta))$; dabei ist $\varepsilon_h$ jedesmal selbst eine Zahl im Körper von $\theta$ und sind deren konjugierte Zahlen in den Körpern von $\theta_1, \theta_2, \ldots, \theta_{m+1}$ bezüglich

$$f(R_h(\theta_1)), f(R_h(\theta_2)), \ldots, f(R_h(\theta_{m+1})). \tag{2}$$

Nun hat man bei beliebigen Werten $h, k$ aus der Reihe $1, 2, \ldots, m + 1$ stets $R_h(\theta_k) = R_h(R_k(\theta)) = \theta_g$, wo $g$ einen der Indizes $1, 2, \ldots, n$ bedeutet. Dabei kann nicht für zwei verschiedene Indizes $k$ bei demselben Index $h$ hier derselbe Wert $\theta_g$ und können auch nicht konjugiert imaginäre Werte $\theta_g$ resultieren, da aus dieser Relation umgekehrt $\theta_k = S_h(\theta_g)$ folgt und unter den Zahlen $\theta_1, \theta_2, \ldots, \theta_{m+1}$ keine zwei gleich oder konjugiert imaginär sind. Danach sind die absoluten Beträge der Größen in (2) abgesehen von der Reihenfolge identisch mit den Beträgen der Größen $f(\theta_1), f(\theta_2), \ldots, f(\theta_{m+1})$, es ist also einer jener Beträge $> 1$ und die $m$ anderen sind sämtlich $< 1$, und zwar ist für denjenigen Index $k$ der Betrag $|f(R_h(\theta_k))| > 1$, für den $R_h(\theta_k)$ gleich $\theta$ bezüglich gleich der konjugiert imaginären Zahl, also $\theta_k$ gleich $S_h(\theta)$ bezüglich gleich der konjugiert imaginären Zahl ist. Für verschiedene Werte $h$ der Reihe $1, 2, \ldots, m + 1$ wird der hier in Betracht kommende Index $k$ aus der Reihe $1, 2, \ldots, m + 1$ jedesmal ein anderer sein. Nach den Auseinandersetzungen in 2. bilden nunmehr irgend $m$ der Zahlen $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{m+1}$ ein vollständiges System von unabhängigen Ein-

heiten in dem Galoisschen Körper von $\theta$. Auf diese Weise resultiert der Satz:

*In einem Galoisschen Körper kann man stets eine solche Einheit angeben, daß eine jede Einheit dieses Körpers ein Produkt aus einer Einheitswurzel und aus Potenzen dieser Einheit und ihrer konjugierten Einheiten mit rationalen Exponenten ist.*

Da ein jeder algebraischer Körper ein Unterkörper eines Galoisschen Körpers ist und seine Einheiten dann zugleich als Einheiten des Galoisschen Körpers auftreten, ist hierdurch zugleich ein bemerkenswerter Satz über die Einheiten in einem beliebigen algebraischen Körper gewonnen.

Zürich, den 23. Februar 1900.

XVI.

# Über die Annäherung an eine reelle Größe durch rationale Zahlen.

(Mathematische Annalen, Band 54, S. 91—124.)

Obwohl die Theorie der Annäherung an eine reelle Größe mit Hilfe von Kettenbrüchen seit Euler und Lagrange noch mannigfache Behandlung erfahren hat, scheint einer der interessantesten Sätze auf diesem Gebiete bisher nicht bemerkt worden zu sein. Nämlich unter den verschiedenen möglichen Kettenbruchentwicklungen für eine reelle Größe $a$, wobei die Teilzähler $\pm 1$ und die Teilnenner positive ganze Zahlen sind, gibt es eine bestimmte Art der Entwicklung (und zwar die am besten konvergierende), *für welche die sämtlichen Näherungsbrüche* $\frac{x}{y}$ *sich von vornherein in einfachster Weise charakterisieren lassen: Als Zähler und Nenner der einzelnen Näherungsbrüche erscheinen dabei genau die sämtlichen Paare von ganzen Zahlen* $x$, $y$, *für die* $y > 0$ *ist,* $x$ *und* $y$ *relativ prim sind und dazu die Bedingung*

$$|(x - ay)y| < \frac{1}{2}$$

*erfüllt ist.* Von dem Falle, daß $a$ gleich einer ganzen Zahl $+\frac{1}{2}$ ist, hat man hierbei abzusehen.*)

---

*) Bekanntlich läßt sich eine nach fallenden Potenzen von $z$ fortschreitende konvergente Reihe

$$f(z) = c_{-m}z^m + c_{-m+1}z^{m-1} + \cdots + c_0 + \frac{c_1}{z} + \frac{c_2}{z^2} + \cdots$$

in einen Kettenbruch

$$F_0(z) + \frac{1}{|F_1(z)} + \frac{1}{|F_2(z)} + \cdots$$

umwandeln, so daß $F_0(z)$ eine ganze rationale Funktion von $z$ und $F_1(z)$, $F_2(z)$, ... ganze rationale Funktionen von $z$ mindestens vom Grade 1 sind. Dabei gilt der Satz: Ein Quotient $\frac{P(z)}{Q(z)}$ zweier relativ primer ganzer rationaler Funktionen von $z$ ist immer dann und nur dann Näherungsbruch dieses Kettenbruchs, wenn die Entwicklung von

$$(P(z) - f(z)\,Q(z))\,Q(z)$$

nach fallenden Potenzen von $z$ mit einer Potenz von $z$, deren Exponent negativ ist,

Auf die betreffende noch durch weitere bemerkenswerte Eigenschaften ausgezeichnete Kettenbruchentwicklung habe ich bereits an anderer Stelle*) hingewiesen, ohne jedoch damals wahrzunehmen, daß die eben erwähnte Ungleichung für die Näherungsbrüche diese Entwicklung bereits vollständig charakterisiert.

Im folgenden gebe ich eine auf geometrischen Betrachtungen gegründete und dadurch sehr anschauliche *Theorie des Systems zweier linearer Formen* $\alpha x + \beta y$, $\gamma x + \delta y$ mit *beliebigen* reellen Koeffizienten und mit *ganzzahligen* Unbestimmten. Eine Anwendung der dabei zutage tretenden Resultate auf die spezielleren Ausdrücke $x - ay$, $y$ liefert dann insbesondere jene Sätze über die Annäherung an eine Größe $a$.

## § 1.

Satz I. *Sind* $\xi = \alpha x + \beta y$, $\eta = \gamma x + \delta y$ *zwei lineare Formen mit beliebigen reellen Koeffizienten* $\alpha, \beta, \gamma, \delta$ *und einer Determinante* $\alpha\delta - \beta\gamma = 1$, *so gibt es stets ganze Zahlen* $x, y$, *die nicht beide Null sind und für welche*

$$|\xi\eta| \leqq \frac{1}{2}$$

*ausfällt.*

Wird auf die Form $\xi\eta$ eine *ganzzahlige* Substitution $x = pX + p'Y$, $y = qX + q'Y$ mit einer *Determinante* $\pm 1$ angewandt, so nennen wir $\xi\eta$ der transformierten Form in den neuen Variablen $X, Y$ *äquivalent.* Zugleich mit dem Satze I beweisen wir den folgenden

Zusatz. *Ist* $\xi\eta$ *weder mit der Form* $XY$ *noch mit der Form* $\frac{1}{2}(X^2 - Y^2)$ *äquivalent, so gibt es stets ganze Zahlen* $x, y$, *wofür* $\xi \neq 0$, $\eta \neq 0$ *und* $|\xi\eta| < \frac{1}{2}$ *ausfällt.*

Beweis. Wir deuten $x, y$ als irgendwelche Parallelkoordinaten in einer Ebene, wobei noch für jede der zwei Koordinaten die Entfernung Eins parallel ihrer Achse in willkürlicher Weise angenommen sein kann. Es sei $O$ der *Nullpunkt* ($x = 0$, $y = 0$). Bedeutet $A$ einen von $O$ verschiedenen Punkt $x = p$, $y = q$, so soll der zu ihm in bezug auf $O$ symmetrische Punkt $x = -p$, $y = -q$ jedesmal mit $A_0$ bezeichnet werden.

Die Gesamtheit derjenigen Punkte, für welche $x$ wie $y$ ganze Zahlen sind, heiße das *Zahlengitter,* und die einzelnen Punkte daraus sollen *Gitterpunkte* heißen.

---

beginnt. Der Satz, den ich im Texte angebe, stellt das wohl von manchem Mathematiker vermißte Analogon in der Größenlehre zu diesem Satze der Funktionenlehre vor.

*) Annales de l'École Normale supérieure, 3e série, T. XIII; 1896. Diese Ges. Abhandlungen, Bd. I, S. 278.

Sind $\varrho$, $\sigma$ positive Parameter, so bilden die vier Punkte $R$, $R_0$, $S$, $S_0$, für welche $\xi = \varrho$, $\eta = 0$; $\xi = -\varrho$, $\eta = 0$; $\xi = 0$, $\eta = \sigma$; $\xi = 0$, $\eta = -\sigma$ ist, die Ecken für ein Parallelogramm mit $O$ als Mittelpunkt und mit den Linien $\xi = 0$, $\eta = 0$ als *Diagonalen*. Ein solches Parallelogramm werde mit $\mathfrak{P}(\varrho, \sigma)$ bezeichnet. Seine vier Seiten besitzen die Gleichungen $\pm\frac{\xi}{\varrho} \pm \frac{\eta}{\sigma} = 1$, wo für die zwei Vorzeichen alle vier Kombinationen $+, +$; $-, +$; $-, -$; $+, -$ in Betracht kommen, und der Bereich von $\mathfrak{P}(\varrho, \sigma)$ wird daher durch

$$\left|\frac{\xi}{\varrho}\right| + \left|\frac{\eta}{\sigma}\right| \leqq 1$$

dargestellt.

Wir können nun von so kleinen Werten für $\varrho$ und $\sigma$ ausgehen, daß das zugehörige Parallelogramm $\mathfrak{P}(\varrho, \sigma)$ jedenfalls keinen Gitterpunkt außer dem Nullpunkte $O$ in sich faßt. Dann lassen wir $\varrho$ und $\sigma$ *unter Festhaltung der Größe ihres Verhältnisses* $\varrho : \sigma$ wachsen. Dabei dehnt sich $\mathfrak{P}(\varrho, \sigma)$ nach allen Richtungen von $O$ aus in gleichem Maße aus. Wir müssen daher schließlich zu gewissen Werten $\varrho$, $\sigma$ kommen, wobei $\mathfrak{P}(\varrho, \sigma)$ auf seiner *Begrenzung* weitere Gitterpunkte aufnimmt, während immer noch $O$ der einzige Gitterpunkt im *Inneren* von $\mathfrak{P}(\varrho, \sigma)$ ist. Es sei bei diesen Werten $\varrho$, $\sigma$, bei denen wir nun verweilen, $A$ $(x = p, y = q)$ ein Gitterpunkt auf der Begrenzung von $\mathfrak{P}(\varrho, \sigma)$. Da zugleich mit $A$ auch der Gitterpunkt $A_0$ $(x = -p, y = -q)$ auf der Begrenzung von $\mathfrak{P}(\varrho, \sigma)$ auftritt, so können wir annehmen, für $A$ sei $\eta > 0$ oder $\eta = 0$, $\xi > 0$. Wir setzen für $A$: $\xi = \varepsilon\lambda$, $\eta = \mu$, so daß $\mu \geqq 0$, $\lambda \geqq 0$, $\varepsilon = \pm 1$ ist.

Die ganzen Zahlen $p$, $q$ haben gewiß keinen gemeinsamen Teiler $> 1$, weil die Strecke $OA$ keinen Gitterpunkt zwischen $O$ und $A$ enthält. Wir bestimmen zwei ganze Zahlen $r$, $s$ irgendwie so, daß $ps - qr = \varepsilon$ ist, und setzen

$$x = p\overline{X} + rY, \quad y = q\overline{X} + sY.$$

Dabei werde $\varepsilon\xi = \lambda\overline{X} + \bar{\lambda}Y$, $\eta = \mu\overline{X} + \bar{\mu}Y$. Dann haben $\varepsilon\xi$, $\eta$ in $\overline{X}$, $Y$ die Determinante $\varepsilon\varepsilon = 1$ und folgt

$$Y = \lambda\eta - \mu\varepsilon\xi. \tag{1}$$

Die Gitterpunkte $x$, $y$ werden genau die Punkte mit ganzzahligen Bestimmungsstücken $\overline{X}$, $Y$. Diese Punkte ergeben auf der Linie $Y = 0$, d. i. der Geraden durch $O$ und $A$ die unendliche Punktreihe zu den Werten $\overline{X} = \cdots -2, -1, 0, 1, 2, \cdots$, wobei $\overline{X} = 0$ den Nullpunkt, $\overline{X} = 1$ den Punkt $A$ liefert und alle diese Punkte sich in einem konstanten Abstande $= OA$ folgen. Sodann bilden sie auf einer jeden der zu $Y = 0$ parallelen Geraden $Y = 1$, $Y = -1$, $Y = 2$, $Y = -2, \cdots$ jedesmal eine äquidistante Punktreihe mit dem gleichen konstanten Abstande $= OA$ zwischen benachbarten Punkten. Von diesen sämtlichen

einander parallelen Geraden sind $Y = 1$ und $Y = -1$ die zwei an $Y = 0$ nächstgelegenen.

1. Wir nehmen zunächst an, daß $A$ *nicht* eine *Ecke* von $\mathfrak{P}(\varrho, \sigma)$, also $\lambda > 0$, $\mu > 0$ ist.*) Es sei $F$ der Punkt $\xi = -\varepsilon\lambda$, $\eta = \mu$. Das Parallelogramm mit den Ecken $A$, $F$, $A_0$, $F_0$ ist durch $-\lambda \leqq \xi \leqq \lambda$, $-\mu \leqq \eta \leqq \mu$ definiert und befindet sich, von den Ecken abgesehen, ganz im Inneren des Parallelogramms $\mathfrak{P}(\varrho, \sigma)$.

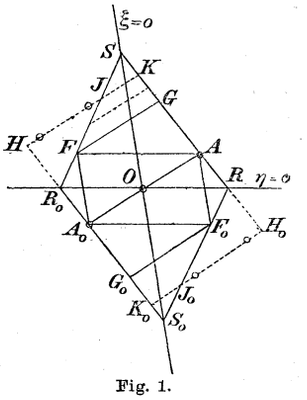

Fig. 1.

Nehmen wir weiter an, daß $A$ auch *nicht Mitte* einer Seite von $\mathfrak{P}(\varrho, \sigma)$ ist. Die zu $A_0OA$ parallele Gerade durch $F$ trifft dann die Begrenzung von $\mathfrak{P}(\varrho, \sigma)$ außer in $F$ in einem zweiten Punkte $G$, so daß die Strecke $FG$ offenbar *größer* als $OA$ ist. Ebenso würde jede parallele Gerade zu $A_0OA$, die in dem Streifen zwischen $A_0OA$ und $FG$ verläuft, eine Strecke $> OA$ ganz im Inneren von $\mathfrak{P}(\varrho, \sigma)$ liegen haben. Da nun im Inneren von $\mathfrak{P}(\varrho, \sigma)$ sich kein Gitterpunkt außer $O$ befindet, welcher Punkt auf $Y = 0$ liegt, müssen danach die Geraden $Y = \pm 1$ außerhalb des durch die Parallelen $FG$ und $F_0G_0$ begrenzten Streifens verlaufen, d. h. für den Punkt $F$ muß jedenfalls $|Y| < 1$ sein. Nun hat man für $F$: $Y = 2\lambda\mu$, also folgt

$$2\lambda\mu < 1.$$

Danach ist der Gitterpunkt $A$ hier von der im Satze I und dem Zusatze geforderten Beschaffenheit.

2. Ist $A$ *Mitte* einer Seite von $\mathfrak{P}(\varrho, \sigma)$, also $\lambda = \frac{1}{2}\varrho$, $\mu = \frac{1}{2}\sigma$, so ist $A_0OA$, also die Gerade $Y = 0$ parallel einer Seite von $\mathfrak{P}(\varrho, \sigma)$. Jede Parallele zu $A_0OA$, welche ins Innere von $\mathfrak{P}(\varrho, \sigma)$ eintritt, hat dann mit $\mathfrak{P}(\varrho, \sigma)$ eine Strecke $= A_0OA > OA$ gemein. Die Geraden $Y = \pm 1$ können daher nicht ins Innere von $\mathfrak{P}(\varrho, \sigma)$ eintreten, $\mathfrak{P}(\varrho, \sigma)$ liegt also ganz in dem Streifen $-1 \leqq Y \leqq 1$. Insbesondere gilt danach für den Punkt $F$: $Y \leqq 1$, d. h. man hat

$$2\lambda\mu \leqq 1.$$

Der Punkt $A$ hat also wieder die im Satze I verlangte Beschaffenheit.

Das Gleichheitszeichen in dieser Ungleichung, (dessen Eintreten zugleich $\varrho\sigma = 2$ bedeuten würde), hat dann statt, wenn eine Seite von

*) Wie die Buchstaben $R$ und $R_0$ in der Figur eingetragen sind, ist darin $\varepsilon = 1$ für den Punkt $A$ angenommen. Die Gitterpunkte sind hier und in den weiteren Figuren durch kleine Kreise angedeutet.

$\mathfrak{P}(\varrho, \sigma)$ auf die Gerade $Y = 1$ fällt. Da diese Seite an Länge $= 2OA$ ist, so enthält sie alsdann entweder *innerhalb* jeder ihrer durch $F$ getrennten Hälften je einen Gitterpunkt, in welchem Falle für diese Gitterpunkte nach dem bereits in 1. Ausgeführten sich $\xi \neq 0$, $\eta \neq 0$, $|\xi\eta| < \frac{1}{2}$ herausstellt, oder aber es sind auf ihr sowohl beide Ecken wie die Mitte $F$ Gitterpunkte. In diesem zweiten Falle wären in $\mathfrak{P}(\varrho, \sigma)$ alle vier Mitten der Seiten Gitterpunkte. Wir können dann $A$ als die Mitte von $RS$, d. h. $\varepsilon = 1$ voraussetzen. Ist für $F$ hier $Y = 1$, $\overline{X} = g$ und setzt man $\overline{X} = X + gY$, so sind $A\left(\xi = \frac{1}{2}\varrho,\ \eta = \frac{1}{2}\sigma\right)$ und $F\left(\xi = -\frac{1}{2}\varrho,\ \eta = \frac{1}{2}\sigma\right)$ durch $X = 1$, $Y = 0$ und $X = 0$, $Y = 1$ bestimmt, und hat man daher

$$\xi = \tfrac{1}{2}\varrho(X - Y),\ y = \tfrac{1}{2}\sigma(X + Y),\ \varrho\sigma = 2,\ \xi\eta = \tfrac{1}{2}(X^2 - Y^2).$$

3. Endlich nehmen wir an, daß der Gitterpunkt $A$ eine *Ecke* von $\mathfrak{P}(\varrho, \sigma)$, also dafür $\xi = 0$ oder $\eta = 0$ sei; dann ist selbstverständlich für diesen Punkt $|\xi\eta| = 0 < \frac{1}{2}$. In jedem Falle entspricht somit der Gitterpunkt $A$ den Bedingungen des Satzes I.

Um auch noch den Zusatz unter den letzten Umständen als richtig zu erkennen, stellen wir uns $A$ etwa als die Ecke $R(\xi = \varrho,\ \eta = 0)$ von $\mathfrak{P}(\varrho, \sigma)$ vor. Dann ist nach (1.): $Y = \varrho\eta$. Nunmehr halten wir $\varrho$ fest und denken uns den Parameter $\sigma$ als veränderlich. Dabei bleibt die Diagonale $R_0R(A_0OA)$ von $\mathfrak{P}(\varrho, \sigma)$ auf $Y = 0$ fest, während sich die Endpunkte $S_0, S$ der anderen Diagonale auf der Linie $\xi = 0$ verschieben. Bei hinreichend kleinem $\sigma$ liegt $\mathfrak{P}(\varrho, \sigma)$ ganz im Bereiche $-1 < Y < 1$, enthält dann also gewiß keinen Gitterpunkt außer $A_0$, $O$, $A$. Wird $\sigma = \frac{1}{\varrho}$, so erreicht $\mathfrak{P}(\varrho, \sigma)$ die Gerade $Y = 1$ mit der Ecke $S\ (\xi = 0, \eta = \sigma)$. Fällt dabei diese Ecke zugleich in einen Gitterpunkt, so sei für ihn $Y = 1$, $\overline{X} = g$. Setzt man alsdann $\overline{X} = X + gY$, so gilt für $S$: $\xi = 0$, $\eta = \sigma$; $X = 0$, $Y = 1$, für $R$: $\xi = \varrho$, $\eta = 0$; $X = 1$, $Y = 0$, also hat man in diesem Falle:

$$\xi = \varrho X,\quad \eta = \sigma Y,\quad \varrho\sigma = 1,\quad \xi\eta = XY.$$

Fällt hingegen der Punkt $\xi = 0$, $\eta = \frac{1}{\varrho}$ nicht in einen Gitterpunkt, so kann man $\sigma$ über $\frac{1}{\varrho}$ hinaus wachsen lassen, ohne daß zunächst neue Gitterpunkte in $\mathfrak{P}(\varrho, \sigma)$ eintreten. Dabei wird die Strecke, welche der Bereich von $\mathfrak{P}(\varrho, \sigma)$ aus der Linie $Y = 1$ herausschneidet und deren variable Endpunkte $J$, $K$ heißen mögen, nach beiden Enden zu immer ausgedehnter und wird sich schließlich einer dieser zwei Fälle ereignen:

Entweder fällt, so lange noch diese Strecke $JK < OA$ ist, einer

ihrer Endpunkte (wie in Fig. 2 der Punkt $J$) in einen Gitterpunkt $A'$ auf der Geraden $Y=1$. Dabei reicht dann wegen $JK<\frac{1}{2}A_0OA$ das Parallelogramm $\mathfrak{P}(\varrho, \sigma)$ noch nicht an $Y=2$ heran, enthält also gewiß keinen Gitterpunkt außer $O, A, A_0, A', A_0'$, und zugleich liegt der Punkt $A'$ auf $Y=1$ näher an $S$ (wofür $Y<2$ ist), als an dem anderen Endpunkte ($A_0$ in Fig. 2) der durch ihn gehenden Seite von $\mathfrak{P}(\varrho, \sigma)$, also ist $A'$ keinenfalls Mitte dieser Seite. In diesem Falle gilt für $A'$ nach den früheren Bemerkungen $\xi \neq 0,\ \eta \neq 0,\ |\xi\eta|<\frac{1}{2}$.

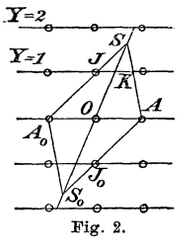

Fig. 2.

Der andere mögliche Fall ist, daß erst, wenn die Strecke $JK$ bis zur Länge $OA$ gewachsen ist, ihre beiden Endpunkte in Gitterpunkte zu liegen kommen. In dieser Endlage stößt dann $\mathfrak{P}(\varrho, \sigma)$ gerade mit der Ecke $S$ auf $Y=2$, so daß auch hier noch $\mathfrak{P}(\varrho, \sigma)$ keinen Gitterpunkt außer $O$ im Inneren enthält, aber in den Mitten aller vier Seiten Gitterpunkte aufweist. In diesem Falle erweist sich, wie schon oben unter 2. ausgeführt ist, $\xi\eta$ als äquivalent mit $\frac{1}{2}(X^2-Y^2)$. Werden alle erörterten Einzelheiten zusammengefaßt, so tritt die Richtigkeit des zum Satze I gemachten Zusatzes hervor. —

Den Beweis der Ungleichung $2\lambda\mu \leqq 1$ für den Gitterpunkt $A$ und damit des Satzes I können wir auch durch folgende, auf dem Begriffe des *Flächeninhalts* beruhende Betrachtung erhalten, die noch zu einem weiter reichenden Resultate führt.

Da wir im Hinblick auf die festzustellende Relation $|\xi\eta| \leqq \frac{1}{2}$ die Rolle der Formen $\xi, \eta$ vertauschen, auch $\xi$ durch $-\xi$ ersetzen können, wobei freilich als Wert der Determinante von $\xi, \eta$ auch $-1$ zuzulassen ist, so dürfen wir ohne wesentliche Einschränkung annehmen, $A$ falle auf die Seite $RS$ von $\mathfrak{P}(\varrho, \sigma)$ und noch derart, daß $RA \leqq AS$ ist, d. h. wir setzen $\varepsilon = 1$ und $\frac{\lambda}{\varrho} \geqq \frac{\mu}{\sigma}$ voraus. Indem $A$ auf der Begrenzung von $\mathfrak{P}(\varrho, \sigma)$ liegt, hat man

$$\frac{\lambda}{\varrho} + \frac{\mu}{\sigma} = 1, \tag{2}$$

also $\frac{\lambda}{\varrho} = \frac{1}{2} + \omega$, $\frac{\mu}{\sigma} = \frac{1}{2} - \omega$, $\frac{\lambda\mu}{\varrho\sigma} = \frac{1}{4} - \omega^2 \leqq \frac{1}{4}$. Nun werden wir beweisen, daß für ein Parallelogramm wie $\mathfrak{P}(\varrho, \sigma)$, welches einen Gitterpunkt $A$ auf der Berandung, im Inneren aber $O$ als einzigen Gitterpunkt enthält, stets

$$\varrho\sigma \leqq 2 \tag{3}$$

gilt. Daraus folgt dann unmittelbar $\lambda\mu \leqq \frac{1}{2}$. Dieser Satz (3) ist aber einschneidender.

Der *Flächeninhalt* von $\mathfrak{P}(\varrho, \sigma)$, d. h. das Doppelintegral $\iint dx\,dy$, über diesen Bereich erstreckt, ist, da $\xi, \eta$ die Determinante $\pm 1$ in $x, y$ haben, $= 4 \cdot \frac{1}{2}\varrho\sigma = 2\varrho\sigma$. Es seien nun $H, K$ (Fig. 1) die Schnittpunkte von $Y = 1$ mit den Geraden $S_0R_0$ und $RS$. Wegen (2) haben die Formen $\frac{\xi}{\varrho} + \frac{\eta}{\sigma}$ und $Y$ die Determinante 1 in den Variablen $\overline{X}$, $Y$ und dann eine Determinante $\pm 1$ in $x, y$. Also ist der Flächeninhalt des Parallelogramms $K_0H_0KH$ gleich 4.

Tritt nun die Strecke $HK$ in das *Innere* von $\mathfrak{P}(\varrho, \sigma)$ ein, so liegt $K$ auf $RS$ zwischen $A$ und $S$ und hat $HK$ mit $\mathfrak{P}(\varrho, \sigma)$ eine Strecke $JK$ gemein, die notwendig $\leqq OA$ ist, weil kein Gitterpunkt außer $O$ im Inneren von $\mathfrak{P}(\varrho, \sigma)$ liegt. Wegen $JK \leqq OA$ liegt $J$ auf $R_0S$ und so, daß $R_0J \geqq JS$ ist. Infolgedessen ist der Flächeninhalt des Dreiecks $JKS$ nicht größer als der des Dreiecks $JHR_0$. Nun entsteht das Parallelogramm $RSR_0S_0$ aus dem Parallelogramm $K_0H_0KH$, indem von letzterem die Dreiecke $J_0H_0R$ und $JHR_0$ fortgenommen und die Dreiecke $J_0K_0S_0$ und $JKS$ von nicht größerem Flächeninhalte hinzugefügt werden. Daraus folgt für die Flächeninhalte der zwei Parallelogramme das Verhältnis $2\varrho\sigma \leqq 4$.

Tritt jedoch die Strecke $HK$ überhaupt nicht in das Innere von $\mathfrak{P}(\varrho, \sigma)$ ein, so ist das Parallelogramm $RSR_0S_0$ ganz im Parallelogramme $K_0H_0KH$ enthalten und daher ebenfalls $2\varrho\sigma \leqq 4$.

## § 2.

1. Es mögen $\xi$ und $\eta$ dieselbe Bedeutung wie in Satz I haben. Wir wollen jedoch jetzt von vornherein die besonderen Fälle ausschließen, daß die Form $\xi\eta$ der Variablen $x, y$ mit der Form $XY$ oder mit der Form $\frac{1}{2}(X^2 - Y^2)$ der Variablen $X, Y$ äquivalent ist. Von diesen Ausnahmefällen abgesehen, gilt der

Satz II. *Sind $x = p$, $y = q$ zwei relativ prime ganze Zahlen, wofür $|\xi| > 0$ und $|\xi\eta| < \frac{1}{2}$ ausfällt, so kann man stets zwei ganze Zahlen $x = p'$, $y = q'$ finden, so daß $pq' - qp' = \pm 1$ ist und für welche ebenfalls $|\xi\eta| < \frac{1}{2}$ ist, aber $|\xi|$ kleiner ausfällt als für das erstere System.*

Beweis. Da wir anstatt $p, q$ ebensogut das System $-p, -q$ zugrunde legen können, nehmen wir an, für $x = p$, $y = q$ sei $\xi = \varepsilon\lambda$, $\eta = \mu$ und dabei $\mu > 0$, $\lambda > 0$, $\varepsilon = \pm 1$ oder $\mu = 0$, $\lambda > 0$, $\varepsilon = 1$. Wir bestimmen zwei ganze Zahlen $r, s$ irgendwie so, daß

$$ps - qr = \varepsilon$$

ist, und setzen

$$x = p\overline{X} + rY, \quad y = q\overline{X} + sY.$$

Alsdann sei

$$\varepsilon\xi = \lambda\overline{X} + \bar{\lambda}Y, \quad \eta = \mu\overline{X} + \bar{\mu}Y,$$

so folgt noch

$$\lambda\bar{\mu} - \mu\bar{\lambda} = 1, \quad Y = \lambda\eta - \mu\varepsilon\xi = \varepsilon(py - qx).$$

Wir bezeichnen den Gitterpunkt $x = p$, $y = q$ ($\xi = \varepsilon\lambda$, $\eta = \mu$) mit $A$, ferner, wenn $\mu > 0$ ist, mit $F$ den Punkt $\xi = -\varepsilon\lambda$, $\eta = \mu$. Für $F$ wird $Y = 2\lambda\mu$, d. i. $Y < 1$ auf Grund unserer Voraussetzung über den Gitterpunkt $A$. Die Geraden $Y = \pm 1$ schließen also das Parallelogramm mit den Ecken $A, F, A_0, F_0$ ganz zwischen sich ein, ohne es zu treffen, so daß insbesondere $F$ und $F_0$ gewiß nicht Gitterpunkte sind.

Die Gerade $Y = 1$ trifft nun die Linien $\xi = -\varepsilon\lambda$, $\xi = 0$, $\xi = \varepsilon\lambda$ in drei Punkten $H, J, K$ (Fig. 3), für die $\eta = \frac{1-\lambda\mu}{\lambda}$, $\eta = \frac{1}{\lambda}$, $\eta = \frac{1+\lambda\mu}{\lambda}$ ist, welche Größen sämtlich $> \mu$ sind. Da $HJ = JK = OA$ ist, so werden auf dieser Geraden $Y = 1$ entweder die drei Punkte $H, J, K$ Gitterpunkte sein, oder es liegt ein Gitterpunkt $B$ innerhalb der Strecke $HJ$ und ein Gitterpunkt $C$ innerhalb der Strecke $JK$. In diesem letzteren Falle sei dann $M$ der Schnittpunkt der Geraden $FB$ (oder $A_0B$ im Falle $\mu = 0$) mit der Geraden $\xi = 0$ und $N$ der Schnittpunkt der Geraden $AC$ mit der Geraden $\xi = 0$.

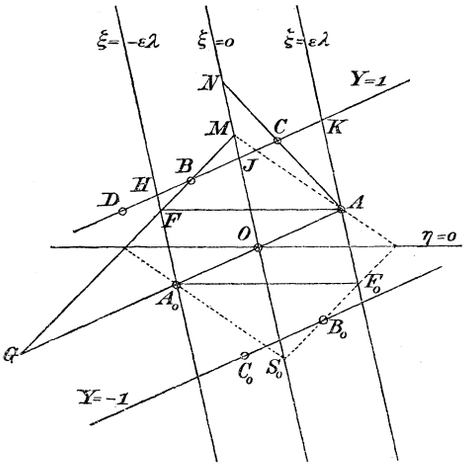

Fig. 3.

Wir bezeichnen nun mit $A'(x = p', y = q')$ *erstens*, wenn $J$ ein Gitterpunkt ist, diesen Gitterpunkt, *zweitens*, wenn in $J$ kein Gitterpunkt fällt und wenn zugleich $M$ näher an $O$ liegt als $N$, also $OM < ON$ ist, den Gitterpunkt $B$, *drittens*, wenn in $J$ kein Gitterpunkt fällt und dabei $OM \geqq ON$ ist, den Gitterpunkt $C$. Da $A'$ auf $Y = 1$ liegt, gilt jedesmal $pq' - qp' = \varepsilon = \pm 1$. Für $A'$ können wir sodann $\xi = \varepsilon'\lambda'$, $\eta = \mu'$ setzen, so daß $\lambda' = 0$ im ersten, $\varepsilon' = -\varepsilon$, $\lambda' > 0$ im zweiten, $\varepsilon' = \varepsilon$, $\lambda' > 0$ im dritten Falle ist, ferner in jedem Falle $\lambda' < \lambda$, $\mu' > \mu$. Im ersten Falle denken wir uns noch $\varepsilon' = -\varepsilon$. Wir wollen ferner hier unter $\mathfrak{P}(\varrho, \sigma)$ mit den Ecken $RSR_0S_0$ speziell dasjenige völlig bestimmte Parallelogramm mit $\xi = 0$, $\eta = 0$ als Diagonalen verstehen, dessen Berandung sowohl den Punkt $A$, wie den Punkt $A'$ aufnimmt. Die Ecke $S(\xi = 0, \eta = \sigma)$ kommt dabei im ersten Falle in $J$, im zweiten in $M$, im dritten in $N$ zu liegen. Wir können nun zeigen, daß in jedem Falle dieses Parallelogramm $\mathfrak{P}(\varrho, \sigma)$

keinen Gitterpunkt außer $O$ im Inneren enthält und daß darin auch $A'$ nicht Mitte einer Seite ist. Aus diesen Umständen folgt nach den Betrachtungen in § 1, daß $\lambda'\mu' < \frac{1}{2}$ ist, und, da zudem $\lambda > \lambda' \geqq 0$ gilt, wird danach in der Tat der Gitterpunkt $p', q'$ von der im Satze II geforderten Beschaffenheit sein. Wir unterscheiden nun die genannten drei Fälle:

Ist *erstens* $J$ ein Gitterpunkt, $A' = J$, so erreicht das Parallelogramm $\mathfrak{P}(\varrho, \sigma)$ die Gerade $Y = 1$ nur im Punkte $J$. Dieses Parallelogramm enthält daher keinen Gitterpunkt außer $O$ im Inneren und $A, A_0, J, J_0$ auf der Begrenzung. Dabei werden $J, J_0$ die Ecken $S, S_0$. Da ferner $H$ außerhalb dieses Parallelogramms $\mathfrak{P}(\varrho, \sigma)$ fällt, so liegt wegen $OH = AJ$ der Punkt $A$ von $S$ weiter entfernt als die Mitte $\xi = \frac{\varepsilon\varrho}{2}$, $\eta = \frac{\sigma}{2}$ der Seite, welche $A$ und $S$ enthält. Man hat also $\lambda > \frac{\varrho}{2}$, $\mu < \frac{\sigma}{2}$. Andererseits gilt $\lambda' = 0 < \frac{\varrho}{2}$, $\mu' = \sigma > \frac{\sigma}{2}$. — Zu bemerken ist noch, daß hier jedenfalls $\mu > 0$ ist. Denn wäre $\mu = 0$, also auch $A$ eine Ecke in $\mathfrak{P}(\varrho, \sigma)$, so enthielte dieses Parallelogramm in den vier Ecken Gitterpunkte. Dann wäre nach § 1, 3. die Form $\xi\eta$ der Variablen $x, y$ äquivalent mit der Form $XY$ der Variablen $X, Y$.

Wir verfolgen jetzt die Annahme, daß $J$ kein Gitterpunkt ist. Es bedeute noch $G$ den Schnittpunkt der Geraden $FB$ mit der Geraden $Y = 0$; dieser Punkt liegt im Falle $\mu > 0$ auf der Verlängerung von $A_0 O$ über $A_0$ hinaus, im Falle $\mu = 0$ fällt er mit $A_0$ zusammen. Aus den zwei ähnlichen Dreiecken $GOM$ und $BJM$ einerseits und aus den zwei ähnlichen Dreiecken $OAN$ und $JCN$ andererseits erhält man die Proportionen

$$\frac{JM}{OJ + JM} = \frac{BJ}{GO}, \qquad \frac{JN}{OJ + JN} = \frac{JC}{OA}. \tag{1}$$

Der *zweite* der obigen Fälle, $A' = B$, hat statt, wenn $J$ kein Gitterpunkt ist und dabei $OM < ON$ ist. Der gezeichneten Figur 3 ist speziell dieser Fall zugrunde gelegt. Dabei gibt dann $FBM$ ($A_0BM$ für $\mu = 0$) eine Seite von $\mathfrak{P}(\varrho, \sigma)$ ab. Für den Punkt $M$ gilt hier stets $Y < 2$. Denn entweder hat man $BJ < JC$; wegen $BJ + JC = A_0 O$ ist dann $BJ < \frac{1}{2} A_0 O \leqq \frac{1}{2} GO$ und folgt aus (1): $JM < OJ$. Ist aber $BJ \geqq JC$, so ist wegen $BJ + JC = OA$ jetzt $JC \leqq \frac{1}{2} OA$ und folgt aus der zweiten Relation in (1): $JN \leqq OJ$, und um so mehr gilt dann $JM < OJ$. In jedem Falle ist dann weiter $OM < 2\,OJ$, d. h. eben $Y < 2$ für den Punkt $M$.

Das Parallelogramm $\mathfrak{P}(\varrho, \sigma)$ liegt somit hier ganz im Bereiche $-2 < Y < 2$. Von der Geraden $Y = 1$ enthält es eine Strecke mit $B$ als einem Endpunkte und mit einem Punkte zwischen $J$ und $C$ als anderem

Endpunkte, von der Geraden $Y=0$ enthält es die Strecke $A_0OA$. Von Gitterpunkten finden sich also darin allein $O$ im Inneren und $A, A_0, B, B_0$ auf der Begrenzung. Da ferner $BC=OA$ ist, die Strecke $BC$ bei $B$ ins Innere von $\mathfrak{P}(\varrho,\sigma)$ eintritt, aber $C$ außerhalb $\mathfrak{P}(\varrho,\sigma)$ fällt, so liegt $B$ an $S\,(=M)$ *näher* als die Mitte $\xi=-\frac{\varepsilon\varrho}{2}$, $\eta=\frac{\sigma}{2}$ der $B$ und $S$ enthaltenden Seite von $\mathfrak{P}(\varrho,\sigma)$, man hat also $\lambda'<\frac{\varrho}{2}$, $\mu'>\frac{\sigma}{2}$; und andererseits liegt deshalb der Punkt $A$ von der Ecke $S\,(=M)$ *weiter* ab als die Mitte $\xi=\frac{\varepsilon\varrho}{2}$, $\eta=\frac{\sigma}{2}$ der $A$ und $S$ enthaltenden Seite von $\mathfrak{P}(\varrho,\sigma)$, mithin ist $\lambda>\frac{\varrho}{2}$, $\mu<\frac{\sigma}{2}$.

Über die Ermittlung des Gitterpunktes $A'$ in diesen beiden ersten Fällen bemerken wir folgendes: Man hat für $A'$ hier $\xi=-\varepsilon\lambda'$, $\eta=\mu'$ und $0\leqq\lambda'<\lambda$, andererseits $\overline{X}=g$, $Y=1$, wo $g$ eine ganze Zahl ist, und dann $p'=r+gp$, $q'=s+gq$. Nun folgt $-\varepsilon\lambda'=\varepsilon(\bar{\lambda}+g\lambda)$, also soll $0\leqq-\bar{\lambda}-g\lambda<\lambda$ oder $0\leqq-\frac{\bar{\lambda}}{\lambda}-g<1$ sein. Danach ist $g$ die größte in $-\frac{\bar{\lambda}}{\lambda}$ enthaltene ganze Zahl:

$$g=\left[-\frac{\bar{\lambda}}{\lambda}\right].$$

Die Relation $Y=1$ für $A'$ ist gleichbedeutend mit $\lambda\mu'+\mu\lambda'=1$. Ist nun $-\frac{\bar{\lambda}}{\lambda}$ genau eine ganze Zahl, so wird $\lambda'=0$, $A'=J$. Anderenfalls wird $\lambda'>0$ und ist der Punkt $M$ auf der Geraden $FB$ ($A_0B$ für $\mu=0$) bestimmt durch $\xi=0$, $\frac{\eta-\mu'}{\xi+\varepsilon\lambda'}=\frac{\eta-\mu}{\xi+\varepsilon\lambda}$, also für $M$: $\eta(\lambda-\lambda')=\lambda\mu'-\mu\lambda'=2\lambda\mu'-1$, der Punkt $N$ auf der Geraden $AC$ hingegen ist, da $C$ hier den Werten $\xi=-\varepsilon\lambda'+\varepsilon\lambda$, $\eta=\mu'+\mu$ entspricht, bestimmt durch $\xi=0$, $\frac{\eta-\mu'-\mu}{\xi+\varepsilon\lambda'-\varepsilon\lambda}=\frac{\eta-\mu}{\xi-\varepsilon\lambda}$, also für $N$: $\eta\lambda'=\lambda\mu'+\mu\lambda'=1$. Die Relation $OM<ON$ kommt danach auf $\frac{2\lambda\mu'-1}{\lambda-\lambda'}<\frac{1}{\lambda'}$ d. i., da $\lambda>0$ ist, auf $2\lambda'\mu'<1$ hinaus.

Endlich nehmen wir als *dritten* Fall den, daß $J$ kein Gitterpunkt ist und dabei $OM\geqq ON$ gilt. Dann hat für $A'(\xi=\varepsilon'\lambda',\ \eta=\mu')$ der Punkt $C$ einzutreten, so daß $\varepsilon'=\varepsilon$ ist. Für $B$ ist dann $\xi=-\varepsilon(\lambda-\lambda')$, $\eta=\mu'-\mu$; es folgt also zunächst $\mu'-\mu>\mu$. Die Relation $OM\geqq ON$ kommt hier nach der eben gemachten Ausführung auf $2(\lambda-\lambda')(\mu'-\mu)\geqq 1$ hinaus.

Es sei zunächst $OM>ON$. Aus $JM>JN$ folgt nach (1), da $GO\geqq OA$ ist, $BJ>JC$. Diese Beziehung ist hier gleichbedeutend mit $\lambda-\lambda'>\lambda'$. Wegen $BJ+JC=OA$ hat man sodann $JC<\frac{1}{2}OA$,

und wegen (1) daher $JN < OJ$. Danach gilt für den Punkt $N$ jedenfalls $Y < 2$. Das Parallelogramm $\mathfrak{P}(\varrho, \sigma)$ reicht also nicht an $Y = 2$ heran. Von der Geraden $Y = 1$ enthält es eine Strecke mit einem Punkte zwischen $B$ und $J$ als einem Endpunkte und mit dem anderen Endpunkte in $C$, von der Geraden $Y = 0$ enthält es die Strecke $A_0 O A$. Danach enthält es keinen Gitterpunkt außer $O$ und $A, A_0, C, C_0$. Da ferner $B$ außerhalb dieses Parallelogramms liegt und $AC = OB$ ist, so ist $AC$ größer als die Hälfte der $A$ und $C$ enthaltenden Seite von $\mathfrak{P}(\varrho, \sigma)$ und befindet sich daher $C$ näher an $S (= N)$ und $A$ weiter von $S$ als die Mitte $\xi = \frac{\varepsilon \varrho}{2}$, $\eta = \frac{\sigma}{2}$ dieser Seite; man hat also $\lambda' < \frac{\varrho}{2} < \lambda$, $\mu' > \frac{\sigma}{2} > \mu$.

Jetzt sei $OM = ON$, so daß $M$ mit $N$ zusammenfällt. Nehmen wir zudem $\mu > 0$ an, so daß $A$ nicht Ecke in $\mathfrak{P}(\varrho, \sigma)$ wird, so ist $GO > A_0 O$ und daher wieder $BJ > JC$, $\lambda - \lambda' > \lambda'$, und gelten alle Überlegungen wie vorhin, nur daß außer $A, A_0, C, C_0$ noch die Gitterpunkte $B$ und $B_0$ auf die Begrenzung von $\mathfrak{P}(\varrho, \sigma)$ zu liegen kommen. Weil $OB$ parallel $AC$ ist, wird dabei $B$ Mitte einer Seite von $\mathfrak{P}(\varrho, \sigma)$, also $\lambda - \lambda' = \frac{\varrho}{2}$, $\mu' - \mu = \frac{\sigma}{2}$, dagegen ist, weil $OB = AC$ und weder $A$ noch $C$ eine Ecke von $\mathfrak{P}(\varrho, \sigma)$ ist, weder $C$ noch $A$ Mitte einer Seite von $\mathfrak{P}(\varrho, \sigma)$; man hat wieder $\lambda' < \frac{\varrho}{2} < \lambda$, $\mu' > \frac{\sigma}{2} > \mu$.

Hat man schließlich $OM = ON$ *und dazu* $\mu = 0$, so ist $A_0 O A$ Diagonale von $(\mathfrak{P}\varrho, \sigma)$ und fällt $G$ mit $A_0$ zusammen. Dann folgt $BJ = JC = \frac{1}{2} OA$, also $\lambda - \lambda' = \lambda'$ und weiter $JN = OJ$, $CN = AC = OB$. Unter diesen Umständen reicht $\mathfrak{P}(\varrho, \sigma)$ mit der Ecke $S$ gerade an $Y = 2$ heran, es enthält wieder im Inneren außer $O$ keinen Gitterpunkt, aber nicht bloß $B$, sondern auch $C$ ist darin Mitte einer Seite. Für $B$ wie für $C$ gilt dann $|\xi\eta| = \frac{1}{2}$. Es wäre dieses derjenige Fall, wo $\xi\eta$ sich als äquivalent mit der Form $\frac{1}{2}(X^2 - Y^2)$ erweist, ein Fall, der vorweg ausgeschlossen wurde.

Aus den Betrachtungen in § 1 folgt nunmehr in jedem Falle, daß der Gitterpunkt $A'$ den Forderungen des Satzes II entspricht. Zur Bestimmung dieses Gitterpunktes $x = p'$, $y = q'$ aus dem Gitterpunkte $A$ hat sich sogleich die folgende Regel herausgestellt:

*Man bezeichne mit $g$ die größte in $-\frac{\bar{\lambda}}{\lambda}$ enthaltene ganze Zahl und setze $h = g$ oder $h = g + 1$, je nachdem*

$$(-\bar{\lambda} - \lambda g)(\bar{\mu} + \mu g) < \text{ oder } \geqq \frac{1}{2}$$

*ist. Dann hat man $p' = r + ph$, $q' = s + qh$.*

2. Verändern wir die Parameter $\varrho, \sigma$ des in 1. betrachteten Parallelogramms $\mathfrak{P}(\varrho, \sigma)$ in der Weise, daß $\sigma$ verkleinert wird, also $S$ und $S_0$ näher an $O$ heranrücken, daß aber die Seiten noch fortwährend durch $A, A_0$ (und $F, F_0$) gehen, so erhalten wir, so lange die Abnahme von $\sigma$ eine gewisse Grenze nicht erreicht, ein neues Parallelogramm mit $\xi = 0$, $\eta = 0$ als Diagonalen, welches offenbar keine anderen Gitterpunkte außer $A_0$, $O$, $A$ enthält. Daraus geht der Satz hervor:

Satz III. *Ist ein Gitterpunkt $x = p$, $y = q$ so beschaffen, daß die Zahlen $p, q$ relativ prim sind und dafür $|\xi\eta| < \frac{1}{2}$ ausfällt, so kann man stets Parallelogramme*

$$\left|\frac{\xi}{\varrho}\right| + \left|\frac{\eta}{\sigma}\right| \leqq 1$$

*konstruieren, welche den Gitterpunkt auf der Begrenzung liegen haben und außer den drei Punkten $x, y = p, q$; $0, 0$; $-p, -q$ überhaupt keinen Gitterpunkt enthalten.*

Wenn andererseits für einen Gitterpunkt $x = p$, $y = q$ ein Parallelogramm der hier bezeichneten Art existiert, so zeigt der Beweis zum Satze I, daß umgekehrt stets $p, q$ relativ prim sind und dafür $|\xi\eta| < \frac{1}{2}$ ausfällt.

Auf Grund dieses Satzes III beweisen wir über das Verhältnis der in 1. mit $A$ und $A'$ bezeichneten zwei Gitterpunkte den folgenden wichtigen

Zusatz: *Es kann keinen von $A, A_0, A', A_0'$ verschiedenen Gitterpunkt $x, y$ geben, für den ebenfalls $x, y$ relativ prim sind und ebenfalls $|\xi\eta| < \frac{1}{2}$, dabei aber $\lambda \geqq |\xi| \geqq \lambda'$ wäre.*

Beweis. Nehmen wir an, es existierte ein Gitterpunkt $A^*$ der hier bezeichneten Art, und es sei für ihn $|\xi| = \lambda^*$, $|\eta| = \mu^*$. Wir bezeichnen (Fig. 4) mit $E$ den Punkt $\xi = \lambda$, $\eta = \mu$, mit $E'$ den Punkt $\xi = \lambda'$, $\eta = \mu'$, mit $R$ und $S$ die Schnittpunkte der Geraden $EE'$ mit $\eta = 0$ und $\xi = 0$, weiter mit $L$ den Punkt $\xi = \lambda$, $\eta = 0$, mit $L'$ den Punkt $\xi = \lambda'$, $\eta = 0$, endlich mit $E^*$ den Punkt $\xi = \lambda^*$, $\eta = \mu^*$. Nach dem Satze III müßte es zufolge unserer Voraussetzungen möglich sein, ein Parallelogramm $\mathfrak{P}(\varrho^*, \sigma^*)$ mit $\xi = 0$, $\eta = 0$ als Diagonalen zu konstruieren, dessen Begrenzung den Punkt $A^*$ aufnimmt, welches aber weder $A$ noch $A'$ enthielte. Sind $R^*, S^*$ die Ecken $\xi = \varrho^*$, $\eta = 0$ und $\xi = 0$, $\eta = \sigma^*$ dieses Parallelogramms, so enthält die Strecke $R^*S^*$ den Punkt $E^*$, es darf aber weder $E$, noch $E'$ dem Dreiecke $OR^*S^*$ an-

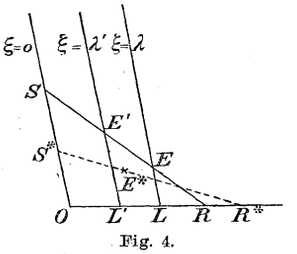

Fig. 4.

gehören. Da nun nach Voraussetzung $E^*$ in dem Parallelstreifen $\lambda' \leqq \xi \leqq \lambda$ liegt und noch dafür $\eta \geqq 0$ ist, müßte danach $E^*$ sich notwendig im Viereck $L'LEE'$ und dabei nicht auf der Seite $EE'$ desselben befinden. Aber das Parallelogramm $RSR_0S_0$ enthält im Inneren $O$ als einzigen Gitterpunkt, danach kann $E^*$ nicht in $L'LEE'$ bei Ausschluß der Strecke $EE'$ liegen. Ein Gitterpunkt, wie wir ihn in $A^*$ angenommen haben, kann also nicht existieren.

In entsprechender Weise leuchtet ein, daß es keinen von $A, A_0, A', A_0'$ verschiedenen Gitterpunkt geben kann, für den ebenfalls $x, y$ relativ prim sind und ebenfalls $|\xi\eta| < \frac{1}{2}$, dabei aber $\mu \leqq |\eta| \leqq \mu'$ wäre.

3. Durch die aus $A$ und $A'$ entnommene Substitution

$$T) \qquad x = pX + p'Y, \quad y = qX + q'Y,$$

deren Determinante $pq' - qp' = \pm 1$ ist, geht die Form $\xi\eta$ in eine äquivalente Form

$$\varphi X^2 + \chi XY + \psi Y^2 = (\varepsilon\lambda X + \varepsilon'\lambda' Y)(\mu X + \mu' Y)$$

über.

Man erhält sodann zunächst die Gleichung $\chi^2 - 4\varphi\psi = 1$.

Sodann ist $\varphi = \varepsilon\lambda\mu$, $\psi = \varepsilon'\lambda'\mu'$ und gilt $|\varphi| < \frac{1}{2}$, $|\psi| < \frac{1}{2}$. Weiter hat man, wenn $\varepsilon' = -\varepsilon$ ist, $\lambda\mu' + \mu\lambda' = 1$, $\lambda > \lambda' \geqq 0$, $\mu' > \mu \geqq 0$ und $\chi = \varepsilon(\lambda\mu' - \mu\lambda') = \varepsilon(1 - 2\mu\lambda')$; also ist in diesem Falle $0 < \varepsilon\chi \leqq 1$. Wenn dagegen $\varepsilon' = \varepsilon$ ist, hat man $\lambda\mu' - \mu\lambda' = 1$, $\lambda > 2\lambda' > 0$, $\mu' > 2\mu \geqq 0$ und $\chi = \varepsilon(\lambda\mu' + \mu\lambda') = \varepsilon(1 + 2\mu\lambda')$; da hier $2\mu\lambda' < \mu'\lambda' < \frac{1}{2}$ ist, folgt also $1 \leqq \varepsilon\chi < \frac{3}{2}$. Die Relation $(\lambda - \lambda')(\mu' - \mu) \geqq \frac{1}{2}$, die in diesem zweiten Falle besteht, ergibt $\varepsilon(\chi - \varphi - \psi) \geqq \frac{1}{2}$. — Die Vorzeichen $\varepsilon$ und $\varepsilon'$ entnimmt man hiernach bereits aus dem Werte von $\chi$ allein, außer wenn gerade $\chi = \pm 1$ (also $\varphi = 0$ oder $\psi = 0$) ist.

Da aus $pq' - qp' = \pm 1$ schon hervorgeht, daß $p$ und $q$ einerseits und andererseits $p'$ und $q'$ relativ prim sind, so sind die besonderen Umstände, welche hier für die zwei Gitterpunkte $A(\xi = \varepsilon\lambda,\ \eta = \mu)$ und $A'(\xi = \varepsilon'\lambda',\ \eta = \mu')$ gelten, völlig zusammengefaßt in den Beziehungen: $\lambda > 0$; $\mu > 0$, $\varepsilon = \pm 1$ oder $\mu = 0$, $\varepsilon = 1$; $pq' - qp' = \varepsilon$, ferner *entweder:*

$$\varepsilon' = -\varepsilon, \quad \lambda > \lambda' \geqq 0, \quad \lambda\mu < \tfrac{1}{2}, \quad \lambda'\mu' < \tfrac{1}{2}$$

*oder:*

$$\varepsilon' = \varepsilon, \quad \lambda > \lambda' > 0, \quad \lambda\mu < \tfrac{1}{2}, \quad (\lambda - \lambda')(\mu' - \mu) \geqq \tfrac{1}{2}.$$

Bemerkenswert ist noch, daß bei dieser zweiten Reihe von Bedingungen für $\varepsilon' = \varepsilon$ die Ungleichung $\lambda\mu < \frac{1}{2}$ eine Folge der übrigen Ungleichungen

ist. Denn man hat hier $\lambda\mu' - \lambda'\mu = 1$. Aus

$$(\lambda - \lambda')(\mu' - \mu) \geqq \frac{1}{2}$$

und $\lambda > \lambda'$ folgt zuvörderst $\mu' > \mu$; sodann kann diese Ungleichung ersetzt werden durch

$$\lambda\mu' + \lambda'\mu - \lambda\mu - \lambda'\mu' \geqq \frac{1}{2}(\lambda\mu' - \lambda'\mu),$$

d. i.

$$\frac{1}{2}\lambda\mu' + \frac{3}{2}\lambda'\mu - \lambda\mu - \lambda'\mu' \geqq 0$$

oder

$$\frac{1}{2}(\lambda - \lambda')(\mu' - 2\mu) \geqq \frac{1}{2}\lambda'(\mu' - \mu).$$

Daraus folgt $\mu' - 2\mu > 0$. Ersetzt man weiter hier $\lambda\mu'$ durch $1 + \lambda'\mu$, so entsteht endlich

$$\frac{1}{2} + 2\lambda'\mu \geqq \lambda\mu + \lambda'\mu', \quad \text{also} \quad \frac{1}{2} \geqq \lambda\mu + \lambda'(\mu' - 2\mu),$$

und daraus entnimmt man in der Tat $\frac{1}{2} > \lambda\mu$.

## § 3.

Fassen wir die Resultate des § 1 und § 2 zusammen und nehmen die Sätze hinzu, welche daraus bei Vertauschung der Rollen von $\xi$ und $\eta$, bei Ersetzung von $\xi, \eta$ durch $\eta, -\xi$, hervorgehen, so entsteht der folgende

Satz IV. *Es seien $\xi = \alpha x + \beta y$, $\eta = \gamma x + \delta y$ zwei lineare Formen mit beliebigen reellen Koeffizienten und einer Determinante $\alpha\delta - \beta\gamma = 1$; jedoch sei die Form $\xi\eta$ in $x, y$ nicht äquivalent mit der Form $XY$ oder der Form $\frac{1}{2}(X^2 - Y^2)$ in $X, Y$. Alsdann lassen sich die sämtlichen Systeme von ganzen Zahlen $x, y$, für welche $x, y$ relativ prim sind und $|\xi\eta| < \frac{1}{2}$ und zudem $\eta > 0$, bzw. $\eta = 0$, $\xi > 0$ ist, in eine Reihe nach wachsendem Werte $\eta$ ordnen. Dabei sind sie zugleich nach abnehmendem Werte $|\xi|$ geordnet.*

*Für je zwei aufeinanderfolgende Systeme $x = p$, $y = q$ und $x = p'$, $y = q'$ in der Reihe gilt dann stets*

$$pq' - qp' = \pm 1.$$

*Diese Reihe weist ein bestimmtes erstes System auf, wofür $\eta = 0$, $\xi > 0$, also $\frac{x}{\delta} = \frac{y}{-\gamma}$ und $> 0$ ist, wenn $\frac{\delta}{-\gamma}$ rational ist; sie weist ein bestimmtes letztes System auf, wofür $\xi = 0$, $\eta > 0$, also $\frac{x}{-\beta} = \frac{y}{\alpha}$ und $> 0$ ist, wenn $\frac{-\beta}{\alpha}$ rational ist. Sie ist ohne ein erstes System, wenn $\frac{\delta}{-\gamma}$ irrational ist,*

*ohne ein letztes System, wenn* $\frac{-\beta}{\alpha}$ *irrational ist; sie ist nach Anfang und Ende hin unbegrenzt, wenn sowohl* $\frac{\delta}{-\gamma}$ *wie* $\frac{-\beta}{\alpha}$ *irrational sind.*

*Ist die Reihe ohne ein letztes System, so konvergiert in ihrem Verlaufe* $|\xi|$ *nach Null und wächst* $\eta$ *über jede Grenze; ist sie ohne ein erstes System, so wächst bei umgekehrter Folge der Systeme in ihr* $|\xi|$ *über jede Grenze und konvergiert* $\eta$ *nach Null.*

Diese zuletzt erwähnte Tatsache folgt aus dem Umstande, daß überhaupt nur für eine endliche Anzahl von Systemen der Reihe $|\xi|$ oder $\eta$ zwischen gegebenen positiven Grenzen liegen kann. Denn soll etwa $\varrho_1 \geqq |\xi| \geqq \varrho_0 > 0$ sein, so folgt aus $|\xi\eta| < \frac{1}{2}$ und $|\xi| \geqq \varrho_0$ noch $|\eta| < \frac{1}{2\varrho_0}$; in einem Parallelogramme $|\xi| \leqq \varrho_1$, $|\eta| \leqq \frac{1}{2\varrho_0}$ liegen aber stets nur eine endliche Anzahl von Gitterpunkten $x, y$.

Die Reihe der hier in Betracht kommenden Gitterpunkte $x, y$, nach wachsendem Werte ihres $\eta$ geordnet, soll die *Kette zu* den Formen $\xi, \eta$ heißen, ein einzelner Gitterpunkt $x = p$, $y = q$ daraus ein *Kettenglied*, ferner die mittels zweier aufeinanderfolgender Kettenglieder $x = p$, $y = q$ und $x = p'$, $y = q'$ gebildete Substitution

$$x = pX + p'Y, \quad y = qX + q'Y$$

eine *Substitution der Kette* heißen.

Wir bezeichnen die nacheinander auftretenden Kettenglieder mit

$$p_i, \; q_i \qquad (i = \cdots -2, -1, 0, 1, 2, \cdots),$$

wobei wir, wenn ein erstes Glied vorhanden ist, *diesem* Gliede und anderenfalls einem beliebig gewählten Gliede den Index 0 erteilen wollen. Für $x = p_i$, $y = q_i$ setzen wir $\xi = \varepsilon_i \lambda_i$, $\eta = \mu_i$, so daß $\mu_i \geqq 0$, $\lambda_i \geqq 0$, $\varepsilon_i = \pm 1$ sei. Ferner schreiben wir allgemein, soweit die Indizes in Betracht kommen,

$$\frac{\varepsilon_i}{\varepsilon_{i-1}} = \vartheta_i.$$

Für ein etwa vorhandenes erstes Glied ist $\varepsilon_0 = 1$. Für einen etwa vorhandenen letzten Index $i = w$, wobei dann $\lambda_w = 0$ wäre, denken wir uns $\vartheta_w = -1$ gewählt. Die Substitution

$$x = p_{i-1}X_i + p_iY_i, \quad y = q_{i-1}X_i + q_iY_i$$

oder kurz $\begin{pmatrix} p_{i-1}, & p_i \\ q_{i-1}, & q_i \end{pmatrix}$ bezeichnen wir mit $T_i$.

Man hat dann allgemein:

$$\lambda_{i-1} > \lambda_i, \quad \mu_{i-1} < \mu_i,$$

ferner

$$(1) \qquad \lambda_{i-1}\mu_i - \vartheta_i\mu_{i-1}\lambda_i = 1, \quad p_{i-1}q_i - q_{i-1}p_i = \varepsilon_{i-1}.$$

Die am Schlusse von § 2, 1. entwickelte Regel, welche überhaupt dazu verhilft, aus einem Kettengliede das nächstfolgende abzuleiten, ergibt einen einfachen Zusammenhang zwischen drei aufeinanderfolgenden Kettengliedern: $p_{i-1}$, $q_{i-1}$; $p_i$, $q_i$; $p_{i+1}$, $q_{i+1}$. Wir können $p_i$, $q_i$ mit dem Gitterpunkte $p$, $q$ ($\varepsilon_i$ mit $\varepsilon$, $\lambda_i$ mit $\lambda$) und $p_{i+1}$, $q_{i+1}$ mit $p'$, $q'$ aus § 2 identifizieren. Für die Zahlen $r$, $s$ dort, welche der Bedingung $p_i s - q_i r = \varepsilon_i$ zu genügen haben, kann man dann mit Rücksicht auf (1): $s = -\vartheta_i q_{i-1}$, $r = -\vartheta_i p_{i-1}$ einführen, und dabei wird

$$\xi = \varepsilon_i \bar{\lambda} = -\vartheta_i \varepsilon_{i-1} \lambda_{i-1}.$$

Also ist dann $\bar{\lambda}$ durch $-\lambda_{i-1}$ zu ersetzen. Dadurch entsteht die folgende Regel:

*Man bezeichne mit $g_i$ die größte in $\frac{\lambda_{i-1}}{\lambda_i}$ enthaltene ganze Zahl und setze $h_i = g_i$ oder $= g_i + 1$, je nachdem*

$$(\lambda_{i-1} - g_i \lambda_i)(g_i \mu_i - \vartheta_i \mu_{i-1}) < \text{oder} \geqq \tfrac{1}{2}$$

*ist, dann gilt*

$$p_{i+1} = -\vartheta_i p_{i-1} + h_i p_i, \qquad q_{i+1} = -\vartheta_i q_{i-1} + h_i q_i$$

*und überdies wird $\vartheta_{i+1} = -1$ im ersten, $= 1$ im zweiten Falle.*

Man erhält hiernach

$$(2)\quad \begin{pmatrix} p_{i-1}, & p_i \\ q_{i-1}, & q_i \end{pmatrix} \begin{pmatrix} 0, & -\vartheta_i \\ 1, & h_i \end{pmatrix} = \begin{pmatrix} p_i, & p_{i+1} \\ q_i, & q_{i+1} \end{pmatrix},$$

$$\begin{pmatrix} \varepsilon_{i-1}\lambda_{i-1}, & \varepsilon_i \lambda_i \\ \mu_{i-1}, & \mu_i \end{pmatrix} \begin{pmatrix} 0, & -\vartheta_i \\ 1, & h_i \end{pmatrix} = \begin{pmatrix} \varepsilon_i \lambda_i, & \varepsilon_{i+1}\lambda_{i+1} \\ \mu_i & \mu_{i+1} \end{pmatrix}.$$

Es wird also

$$p_{i-1} X_i + p_i Y_i = p_i X_{i+1} + p_{i+1} Y_{i+1},$$
$$q_{i-1} X_i + q_i Y_i = q_i X_{i+1} + q_{i+1} Y_{i+1}$$

vermöge

$$X_i = -\vartheta_i Y_{i+1}, \qquad Y_i = X_{i+1} + h_i Y_{i+1}.$$

Setzt man allgemein $-\frac{X_i}{Y_i} = t_i$, so gilt daher weiter

$$(3)\quad \frac{-p_{i-1} t_i + p_i}{-q_{i-1} t_i + q_i} = \frac{-p_i t_{i+1} + p_{i+1}}{-q_i t_{i+1} + q_{i+1}},$$

während

$$(4)\quad t_i = \frac{\vartheta_i}{h_i - t_{i+1}}$$

ist. Dabei ist zu bemerken, daß Zähler und Nenner der rechten Seite von (3) genau die Ausdrücke sind, die bei der naturgemäßen Umformung des Zählers oder des Nenners der linken Seite je in einen Quotienten zweier ganzer Funktionen von $t_{i+1}$ als die Zähler dieser beiden Quotienten erscheinen. Aus (3) und (4) erhält man sogleich allgemeiner:

$$\frac{-p_{i-1}t_i+p_i}{-q_{i-1}t_i+q_i}=\frac{-p_{k-1}t_k+p_k}{-q_{k-1}t_k+q_k}, \qquad i<k, \tag{5}$$

wenn

$$t_i=\cfrac{\vartheta_i}{h_i-\cfrac{\vartheta_{i+1}}{h_{i+1}-\cdots-\cfrac{\vartheta_{k-1}}{h_{k-1}-t_k}}} \tag{6}$$

ist, und dabei gilt über die Entstehung von Zähler und Nenner der rechten Seite in (5) aus Zähler und Nenner der linken Seite eine ganz entsprechende Bemerkung wie bei den Beziehungen (3) und (4).

Ebenso wie $\xi$, $\eta$ haben $\eta$, $-\xi$ die Determinante 1. Die Kette zu $\eta$, $-\xi$ ist im wesentlichen die umgekehrte Kette zu $\xi$, $\eta$. Durchläuft $p_i$, $q_i$ die Gitterpunkte der Kette zu $\xi$, $\eta$ in umgekehrter Reihenfolge, d. h. so daß die Indizes $i$ abnehmen, so hat man dabei in den Systemen $x=-\varepsilon_i p_i$, $y=-\varepsilon_i q_i$, (für welche $-\xi\geqq 0$ ausfällt), die Glieder der Kette zu $\eta$, $-\xi$. Über den Fortgang in dieser letzteren Kette sei noch die aus (2) folgende Beziehung:

$$\begin{pmatrix}-\varepsilon_{i+1}p_{i+1}, & -\varepsilon_i p_i\\ -\varepsilon_{i+1}q_{i+1}, & -\varepsilon_i q_i\end{pmatrix}\begin{pmatrix}0, & -\vartheta_{i+1}\\ 1, & h_i\end{pmatrix}=\begin{pmatrix}-\varepsilon_i p_i, & -\varepsilon_{i-1}p_{i-1}\\ -\varepsilon_i q_i, & -\varepsilon_{i-1}q_{i-1}\end{pmatrix} \tag{7}$$

angemerkt.

## § 4.

An die Sätze in § 2 schließt sich folgendes Theorem an:

Satz V. *Sind $\xi=\alpha x+\beta y$, $\eta=\gamma x+\delta y$ zwei lineare Formen mit beliebigen reellen Koeffizienten und einer Determinante $\alpha\delta-\beta\gamma=1$ und sind $\xi_0$, $\eta_0$ irgendwelche gegebene reelle Größen, so gibt es stets ganze Zahlen $x$, $y$, für welche*

$$|(\xi-\xi_0)(\eta-\eta_0)|\leqq\frac{1}{4}$$

*ausfällt.*

Beweis. Betrachten wir vorweg die Fälle, daß es eine ganzzahlige Substitution mit einer Determinante $\pm 1$ gibt, durch welche die Form $\xi\eta$ der Variablen $x$, $y$ in die Form $XY$ oder in die Form $\frac{1}{2}(X^2-Y^2)$ der neuen Variablen $X$, $Y$ übergehe. Dem Wertsysteme $\xi=\xi_0$, $\eta=\eta_0$ entspreche dabei das System $X=X_0$, $Y=Y_0$, so erweist sich vermöge jener Substitution

$$(\xi-\xi_0)(\eta-\eta_0)=(X-X_0)(Y-Y_0), \text{ bzw. } =\tfrac{1}{2}((X-X_0)^2-(Y-Y_0)^2).$$

Bestimmen wir nun $X$ und $Y$ als ganze Zahlen so, daß $|X-X_0|\leqq\frac{1}{2}$, $|Y-Y_0|\leqq\frac{1}{2}$ ist, so wird im ersten Falle, wo $\xi\eta$ äquivalent $XY$ ist,

$|(\xi - \xi_0)(\eta - \eta_0)| \leqq \frac{1}{4}$. Dabei ist zu bemerken, daß das Gleichheitszeichen hier unter gewissen Umständen wirklich in Betracht kommt, nämlich wenn sowohl $X_0$ wie $Y_0$ gleich ganzen Zahlen vermehrt um $\frac{1}{2}$ sind. — Im zweiten Falle, wo $\xi\eta$ äquivalent $\frac{1}{2}(X^2 - Y^2)$ ist, stellt sich sogar $|(\xi - \xi_0)(\eta - \eta_0)| \leqq \frac{1}{8}$ heraus.

Nunmehr schließen wir die Fälle aus, daß $\xi\eta$ äquivalent mit $XY$ oder mit $\frac{1}{2}(X^2 - Y^2)$ ist.

Betrachten wir irgendeine Substitution

$$x = pX + p'Y, \qquad y = qX + q'Y$$

der zu $\xi$, $\eta$ gehörigen Kette. Wir bezeichnen den Gitterpunkt $p$, $q$ mit $A$, den Gitterpunkt $p'$, $q'$ mit $A'$. Nach § 2 haben wir ein ganz bestimmtes Parallelogramm $RSR_0S_0$ oder $\mathfrak{P}(\varrho, \sigma)$: $\left|\frac{\xi}{\varrho}\right| + \left|\frac{\eta}{\sigma}\right| \leqq 1$, dessen Berandung sowohl $A$, wie $A'$ aufnimmt. Der größeren Anschaulichkeit wegen wollen wir in der Zeichnungsebene die Koordinaten $x, y$ derart interpretieren, daß dieses Parallelogramm $\mathfrak{P}(\varrho, \sigma)$ ein *Quadrat* im gewöhnlichen Sinne wird. Für $p$, $q$ sei $\xi = \varepsilon\lambda$, $\eta = \mu$, $(\lambda \geqq 0, \mu \geqq 0, \varepsilon = \pm 1)$, für $p'$, $q'$ sei $\xi = \varepsilon'\lambda'$, $\eta = \mu'$, $(\lambda' \geqq 0, \mu' \geqq 0, \varepsilon' = \pm 1)$. Wir haben nun die beiden, auch in § 2 unterschiedenen Fälle $\varepsilon' = -\varepsilon$ und $\varepsilon' = \varepsilon$ gesondert zu untersuchen.

1°. Es sei zunächst $\varepsilon' = -\varepsilon$ und $\lambda > \lambda' \geqq 0$, $\mu' > \mu \geqq 0$. Ein gleichzeitiges Eintreten von $\mu = 0$ und $\lambda' = 0$ ist dadurch ausgeschlossen, daß $\xi\eta$ nicht äquivalent $XY$ sein soll. Es sei $M$ die Seitenmitte $\xi = \frac{\varepsilon\varrho}{2}$, $\eta = \frac{\sigma}{2}$ und $M'$ die Seitenmitte $\xi = -\frac{\varepsilon\varrho}{2}$, $\eta = \frac{\sigma}{2}$ in $\mathfrak{P}(\varrho, \sigma)$. Nach den Bemerkungen in § 2 kommen $A$ und $A'$ derart auf der Berandung von $\mathfrak{P}(\varrho, \sigma)$ zu liegen, daß bei einer Umlaufung derselben in einem gewissen Sinne sich $A$, $M$, $(S)$, $A'$, $M'$, $A_0$, $M_0$, $(S_0)$, $A_0'$, $M_0'$ folgen (s. Fig. 5; um die Figur nicht zu komplizieren, sind darin die Seiten von $\mathfrak{P}(\varrho, \sigma)$ nicht ausgezogen); $A$ ist von $M$, $A'$ von $M'$ verschieden.

Da wir die Rollen von $\xi$ und $\eta$ vertauschen, anstatt $\xi$, $\eta$ auch $\eta$, $-\xi$ zugrunde legen können, so dürfen wir noch die Annahme $\lambda'\mu' \geqq \lambda\mu$ machen; (weil nicht zugleich $\lambda' = 0$, $\mu = 0$ sein kann, wird dann gewiß $\lambda' > 0$, also $A'$ von $S$ verschieden sein). Da auf jeder Seite des Quadrates $\mathfrak{P}(\varrho, \sigma)$ der Wert $\left|\frac{\xi\eta}{\varrho\sigma}\right|$ stets von der Mitte der Seite nach ihren Enden hin abnimmt und dabei auf allen vier Seiten gleichen Wert erhält bei der nämlichen *Entfernung* von der Seitenmitte, den Begriff der Entfernung

im gewöhnlichen Sinne genommen, so läuft jene Annahme darauf hinaus, daß $A'M' \leqq AM$ sein soll.

Wir konstruieren weiter das Quadrat $\mathfrak{P}\left(\frac{\varrho}{2}, \frac{\sigma}{2}\right)$, dessen Ecken auf $\eta = 0$, $\xi = 0$ halb so große Entfernungen von $O$ haben wie $R$, $R_0$, $S$, $S_0$. Die Berandung von $\mathfrak{P}\left(\frac{\varrho}{2}, \frac{\sigma}{2}\right)$ nimmt die Punkte $X = \pm\frac{1}{2}$, $Y = 0$ und $X = 0$, $Y = \pm\frac{1}{2}$ auf. Legen wir sodann um jeden einzigen Gitterpunkt als Mittelpunkt ein Quadrat, welches dem Quadrate $\mathfrak{P}\left(\frac{\varrho}{2}, \frac{\sigma}{2}\right)$ gleich und in den Seiten parallel gestellt ist, so ergeben diese Quadrate das Bild der in Fig. 5 mit ausgezogener Umrandung gezeichneten Quadrate. Die einzelnen Gitterpunkte sind in dieser Figur durch ihre Koordinaten $X$, $Y$ angedeutet. Das erste Quadrat $\mathfrak{P}\left(\frac{\varrho}{2}, \frac{\sigma}{2}\right)$ um den Nullpunkt stößt mit Stücken seiner Seiten an die Quadrate mit den Mittelpunkten $A$, $A'$, $A_0$, $A_0'$, während es die übrigen Quadrate überhaupt nicht trifft. Danach liegen jene Quadrate offenbar so, daß keine zwei ineinander eingreifen, und zwischen sich lassen sie noch lauter gleiche und parallel liegende Lücken in Form von Rechtecken, welche die einzelnen Punkte $X + \frac{1}{2}$, $Y + \frac{1}{2}$ mit ganzzahligen $X$, $Y$ zu Mittelpunkten haben.

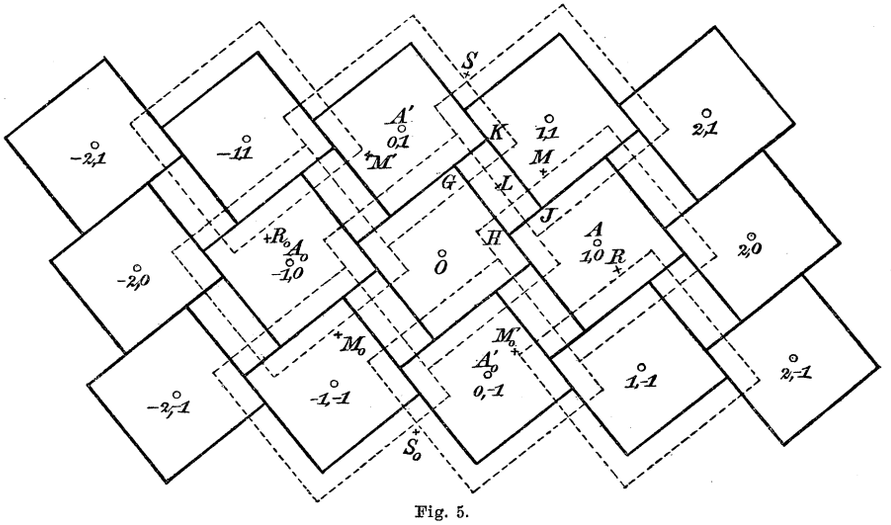


Fig. 5.

Es sei beispielsweise $GHJK$ die rechteckige Lücke mit dem Mittelpunkte $X = \frac{1}{2}$, $Y = \frac{1}{2}$ oder $L$, so daß die Seiten $GH$, $HJ$, $JK$, $KG$ sich an die Quadrate mit den Mittelpunkten $X, Y = 0, 0;\ 1, 0;\ 1, 1;\ 0, 1$

anlegen. Da $AH$, $M'GM$, $A'K$ sämtlich parallel der Linie $\eta = 0$ sind, so ist $GH = MA \leqq MS$ und $GK = M'A' < M'S$, also $GH \geqq GK$ und überdies $\frac{1}{2} RS \geqq GH$, $\frac{1}{2} RS > GK$; (man beachte, daß $A'$ nicht in $S$ fällt). In jeder der rechteckigen Lücken ist daher eine Seite kleiner, die andere höchstens so groß als die Seite des Quadrates $\mathfrak{P}\left(\frac{\varrho}{2}, \frac{\sigma}{2}\right)$.

Unter dem *Inhalt* einer Figur wollen wir den Wert des Integrales $\iint dX\,dY$ über ihre Fläche verstehen. Der Inhalt des Quadrates $\mathfrak{P}\left(\frac{\varrho}{2}, \frac{\sigma}{2}\right)$ ist dann, weil $\alpha\delta - \beta\gamma = 1$, $pq' - qp' = \pm 1$ ist, gleich $\frac{1}{2}\varrho\sigma$ und der Inhalt des Rechteckes $GHJK$ ist $< \frac{1}{2}\varrho\sigma$. Nun kommt in der ganzen Ebene auf jeden Gitterpunkt $X = X^*$, $Y = Y^*$ einerseits ein Parallelogramm $-\frac{1}{2} \leqq X - X^* \leqq \frac{1}{2}$, $-\frac{1}{2} \leqq Y - Y^* \leqq \frac{1}{2}$ vom Inhalte 1, wobei diese Parallelogramme die ganze Ebene lückenlos erfüllen, ohne gegenseitig ineinander einzudringen, andererseits kommt hier auf jeden Gitterpunkt $X^*$, $Y^*$ ein Quadrat mit dem Mittelpunkte $X^*$, $Y^*$ vom Inhalte $\frac{1}{2}\varrho\sigma$ und ein Rechteck mit dem Mittelpunkte $X^* + \frac{1}{2}$, $Y^* + \frac{1}{2}$ von einem gewissen Inhalte $< \frac{1}{2}\varrho\sigma$, und alle diese Quadrate und Rechtecke erfüllen ebenfalls die ganze Ebene lückenlos, ohne gegenseitig ineinander einzudringen. Danach folgt offenbar

$$\frac{1}{2}\varrho\sigma < 1 < 2 \cdot \frac{1}{2}\varrho\sigma. \tag{1}$$

Es verhalte sich die Entfernung des Punktes $O$ von der Geraden $GH$ zu der des Punktes $L$ von dieser Geraden, also $\frac{1}{2} M'S : \frac{1}{2} M'A'$ wie $1 : \varkappa - 1$, dabei ist $1 < \varkappa < 2$. Konstruieren wir dann das Quadrat $\mathfrak{P}\left(\frac{\varkappa\varrho}{2}, \frac{\varkappa\sigma}{2}\right)$ mit $O$ als Mittelpunkt, dessen Seiten denen von $\mathfrak{P}\left(\frac{\varrho}{2}, \frac{\sigma}{2}\right)$ parallel sind, so geht dessen Berandung durch $L$ und wird deshalb dieses Quadrat eine Hälfte der Lücke $GHJK$ vollständig überdecken. Legen wir nun um jeden Gitterpunkt als Mittelpunkt ein diesem Quadrate $\mathfrak{P}\left(\frac{\varkappa\varrho}{2}, \frac{\varkappa\sigma}{2}\right)$ gleiches und parallel gestelltes Quadrat, so werden daher diese Quadrate zweiter Art, die in Fig. 5 mit gestrichelter Berandung gezeichnet sind, jedenfalls die *ganze* Ebene, ohne Lücken zu lassen, überdecken. Also wird der Punkt, für den die Bestimmungsstücke $\xi, \eta$ gleich den gegebenen Werten $\xi_0$, $\eta_0$ sind, in wenigstens eines dieser Quadrate fallen müssen; für den Gitterpunkt $x$, $y$, welcher der Mittelpunkt des betreffenden Quadrates ist, gilt dann

$$\left|\frac{\xi - \xi_0}{\varrho}\right| + \left|\frac{\eta - \eta_0}{\sigma}\right| \leqq \frac{\varkappa}{2}. \tag{2}$$

In das Innere des Quadrates $\mathfrak{P}\left(\frac{\varkappa\varrho}{2}, \frac{\varkappa\sigma}{2}\right)$ dringen von allen übrigen dieser Quadrate zweiter Art nur die vier Quadrate mit den Mittelpunkten $A$, $A_0$, $A'$, $A_0'$. Dabei liegen diese vier Quadrate selbst völlig auseinander, auch reichen sie nicht bis an den Nullpunkt $O$ heran. Danach zeigt sich, daß die Gesamtheit dieser Quadrate zweiter Art die Ebene so überdecken, daß sie kein Gebiet mehr als *zweifach* überlagern, während noch gewisse ⌐-förmige Partien mit den einzelnen Gitterpunkten als Mittelpunkten vorhanden sind, die jedesmal nur je einem dieser Quadrate angehören. Infolgedessen ist der Inhalt des Quadrates $\mathfrak{P}\left(\frac{\varkappa\varrho}{2}, \frac{\varkappa\sigma}{2}\right)$ notwendig $< 2$, d. h. man hat

$$\frac{1}{2}\varkappa^2\varrho\sigma < 2. \tag{3}$$

Aus (2) folgt, weil das geometrische Mittel zweier Beträge nicht größer als ihr arithmetisches Mittel ist,

$$\left|\frac{(\xi-\xi_0)(\eta-\eta_0)}{\varrho\sigma}\right| \leqq \left(\frac{\varkappa}{4}\right)^2,$$

und daraus mit Rücksicht auf (3)

$$|(\xi-\xi_0)(\eta-\eta_0)| < \frac{1}{4}.$$

2⁰. Zweitens sei $\varepsilon' = \varepsilon$ und $\lambda > \lambda' > 0$, $\mu' > \mu \geqq 0$. Die Punkte $A$ und $A'$ werden hier von einer und derselben Seite von $\mathfrak{P}(\varrho, \sigma)$ aufgenommen, wobei weder $A$ noch $A'$ in die Mitte der Seite fallen und $A$, aber nicht $A'$ eine Ecke sein kann. Die Länge der betreffenden Seite ist $\leqq 2AA'$.

Gehen wir nunmehr zu dem Quadrat $\mathfrak{P}\left(\frac{\varrho}{2}, \frac{\sigma}{2}\right)$ über und konstruieren um jeden Gitterpunkt als Mittelpunkt ein diesem gleiches und parallel gestelltes Quadrat, so liefern diese Quadrate das Bild der in Fig. 6 mit ausgezogener Umrandung gezeichneten Quadrate. Die Gitterpunkte sind dort durch ihre Koordinaten $X$, $Y$ bezeichnet. Diese verschiedenen Quadrate nun greifen nicht ineinander ein und lassen zwischen sich im allgemeinen wieder lauter gleiche und parallel gelagerte rechteckige Lücken mit den einzelnen Punkten $X+\frac{1}{2}$, $Y+\frac{1}{2}$ für ganzzahlige $X$, $Y$ als Mittelpunkten. Diese Lücken kommen nur zum Fortfall, wenn auch der Gitterpunkt $X=-1$, $Y=1$ auf die Begrenzung von $\mathfrak{P}(\varrho, \sigma)$ fällt, (wenn $(\lambda-\lambda')(\mu'-\mu) = \frac{1}{2}$ ist). Es sei, wenn nicht dieser Spezialfall statthat, $GHJK$ die rechteckige Lücke mit dem Mittelpunkte $L$: $X=\frac{1}{2}$, $Y=\frac{1}{2}$, wobei $GH$, $HJ$, $JK$, $KG$ ihre an die Quadrate um $X, Y = 0,0;\ 1,0;\ 1,1;\ 0,1$ anstoßenden Seiten seien. Dann ist die Seite $GK$ gleich der Seite des

Quadrates $\mathfrak{P}\left(\frac{\varrho}{2}, \frac{\sigma}{2}\right)$, die Seite $GH$ kleiner als diese Seite. Der Grenzfall, daß $GH = GK$ wäre, würde nur eintreten, wenn $A$ und $A'$ beide in Ecken von $\mathfrak{P}(\varrho, \sigma)$ fielen, was dadurch ausgeschlossen ist, daß $\xi\eta$ nicht äquivalent der Form $XY$ sein soll. Nunmehr erweist sich durch eine entsprechende Überlegung wie in 1°, daß der Inhalt des Quadrates $\mathfrak{P}\left(\frac{\varrho}{2}, \frac{\sigma}{2}\right)$ zusammen mit dem des Rechteckes $GHJK$ gleich 1 sein muß, woraus

$$\frac{1}{2}\varrho\sigma \leqq 1 < 2 \cdot \frac{1}{2}\varrho\sigma \tag{1}$$

hervorgeht. Die Gleichung $\frac{1}{2}\varrho\sigma = 1$ hat statt, wenn die Lücken zum Fortfall kommen, also $H$ mit $G$, $J$ mit $K$ zusammenfällt.

Es verhalte sich die Entfernung des Punktes $A$ von der Geraden $HJ$ zu der des Punktes $L$ von dieser Geraden wie $1 : \varkappa - 1$, so ist $1 \leqq \varkappa < 2$. Konstruieren wir nun das Quadrat $\mathfrak{P}\left(\frac{\varkappa\varrho}{2}, \frac{\varkappa\sigma}{2}\right)$, so wird es die Hälfte der

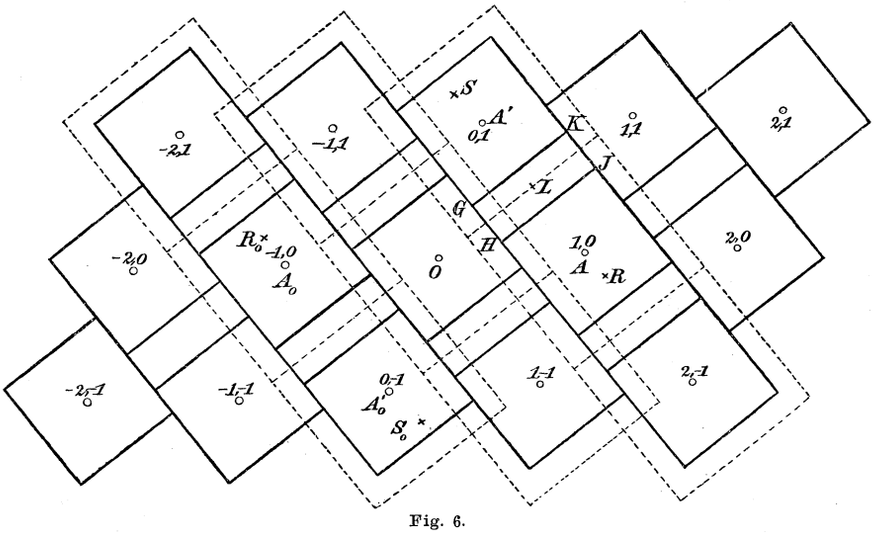


Fig. 6.

Lücke mit dem Mittelpunkte $X = -\frac{1}{2}$, $Y = \frac{1}{2}$ vollständig überdecken. Legen wir dann gleiche und parallel gestellte Quadrate um jeden Gitterpunkt als Mittelpunkt, so erfüllen daher diese Quadrate jedenfalls die ganze Ebene. Also wird derjenige Punkt, für den die Bestimmungsstücke $\xi$, $\eta$ die gegebenen Werte $\xi = \xi_0$, $\eta = \eta_0$ haben, in wenigstens eines dieser Quadrate fallen müssen; alsdann gilt für den Gitterpunkt $x, y$, welcher der Mittelpunkt des betreffenden Quadrates ist,

$$\left|\frac{\xi - \xi_0}{\varrho}\right| + \left|\frac{\eta - \eta_0}{\sigma}\right| \leqq \frac{\varkappa}{2}. \tag{2}$$

Andererseits überdecken diese neuen Quadrate keinen Teil der Ebene mehr als *zweimal*, während noch gewisse Rechtecke mit den einzelnen Gitterpunkten als Mittelpunkten da sind, welche jedesmal nur je einem dieser Quadrate angehören. Infolgedessen muß der Inhalt des Quadrates $\mathfrak{P}\left(\frac{\varkappa\varrho}{2}, \frac{\varkappa\sigma}{2}\right)$ kleiner als 2, also

$$\frac{1}{2}\varkappa^2\varrho\sigma < 2 \tag{3}$$

sein. Aus (2) und (3) ergibt sich wie oben

$$|(\xi - \xi_0)(\eta - \eta_0)| < \frac{1}{4}.$$

Damit ist der Satz V vollständig bewiesen. —

Wir bemerken noch folgendes: Aus $1 < \varrho\sigma$ und $\varkappa^2\varrho\sigma < 4$ entnimmt man $\varkappa^2 < 4$. Aus (2) erhält man daher $|\xi - \xi_0| < \varrho$; nach § 2 ist aber stets $\varrho < 2\lambda$. Hat nun die Kette zu $\xi, \eta$ kein letztes Glied, ist also $\frac{-\beta}{\alpha}$ irrational, so konvergiert im Verlaufe ihrer Glieder die Größe $\lambda$ nach Null. In solchem Falle kann man daher einen Gitterpunkt $x, y$ bestimmen, wofür $|(\xi - \xi_0)(\eta - \eta_0)| < \frac{1}{4}$ ausfällt und zudem $|\xi - \xi_0|$ unter einer beliebig vorgeschriebenen positiven Größe liegt.

## § 5.

Es sei jetzt $a$ eine beliebige reelle Größe, und wir setzen $\xi = x - ay$, $\eta = y$. Die Form $(x - ay)y$ ist nur dann äquivalent mit der Form $XY$, wenn $a$ eine ganze Zahl ist, und nur dann äquivalent mit $\frac{1}{2}(X^2 - Y^2)$, wenn $a$ gleich einer ganzen Zahl vermehrt um $\frac{1}{2}$ ist. Von diesen zwei Fällen wollen wir absehen. Die Kette zu $\xi, \eta$ hat hier ein bestimmtes erstes Glied $p_0, q_0$; für dasselbe soll $\frac{p_0}{1} = \frac{q_0}{0}$ und $> 0$ sein, also hat man $p_0 = 1$, $q_0 = 0$. Für das zweite Kettenglied $p_1, q_1$ soll $p_0q_1 - q_0p_1 = \varepsilon_0 = 1$, also $q_1 = 1$ und $|(p_1 - aq_1)q_1| < \frac{1}{2}$ sein; also ist dann $p_1$ gleich der an der Größe $a$ *nächstgelegenen* ganzen Zahl $h_0$, für die $|h_0 - a| < \frac{1}{2}$ ist. Setzt man sodann in den Formeln (5) und (6) des § 3: $i = 1$, $t_k = 0$, so resultiert $\frac{p_k}{q_k} = h_0 - t_1$. Die in § 3 erhaltenen Resultate führen nunmehr zu folgendem Satze:

Satz VI. *Es sei $a$ eine beliebige reelle Größe, jedoch weder eine ganze Zahl, noch gleich einer ganzen Zahl $+\frac{1}{2}$. Man bilde in folgender Weise eine Reihe von ganzzahligen Systemen $p_i, q_i$ $(i = 0, 1, 2, \ldots)$.*

*Zunächst sei* $p_0 = 1$, $q_0 = 0$, *sodann* $q_1 = 1$ *und* $p_1 = h_0$ *die an der Größe* $a$ *nächstgelegene ganze Zahl so, daß* $|h_0 - a| < \frac{1}{2}$ *ist. Allgemein, wenn man bis zu einem Systeme* $p_i, q_i$ *gelangt ist, wofür noch* $p_i - aq_i \neq 0$ *ausfällt, stelle man den Quotienten* $\frac{p_{i-1} - aq_{i-1}}{p_i - aq_i}$ *her. Es sei* $\vartheta_i$ *sein Vorzeichen und* $g_i$ *die größte in dem absoluten Betrage dieses Quotienten enthaltene ganze Zahl, weiter* $h_i = g_i$ *oder* $= g_i + 1$, *je nachdem*

$$|((p_{i-1} - aq_{i-1}) - \vartheta_i g_i (p_i - aq_i))(g_i q_i - \vartheta_i q_{i-1})| < \text{oder} \geqq \frac{1}{2}$$

*ist. Man setze sodann*

$$p_{i+1} = h_i p_i - \vartheta_i p_{i-1}, \quad q_{i+1} = h_i q_i - \vartheta_i q_{i-1}.$$

*Der auf diese Weise ermittelten Reihe von Systemen* $p_i$, $q_i$ *kommen folgende Eigenschaften zu:*

1⁰. *Wenn* $a$ *rational ist, bricht die Reihe mit einem gewissen System* $p_w$, $q_w$ *ab, wofür* $p_w - aq_w = 0$ *ist. Wenn* $a$ *irrational ist, so läßt sich die Reihe dieser Systeme unbegrenzt fortsetzen.*

2⁰. *Für je zwei aufeinanderfolgende Systeme gilt stets*

$$p_i q_{i+1} - q_i p_{i+1} = \vartheta_1 \vartheta_2 \cdots \vartheta_i = \pm 1.$$

*Die Zahlen* $p_i$, $q_i$ *sind stets relativ prim.*

3⁰. *Man hat*

$$\frac{p_k}{q_k} = h_0 - \frac{\vartheta_1|}{|h_1} - \frac{\vartheta_2|}{|h_2} - \cdots - \frac{\vartheta_{k-1}|}{|h_{k-1}}, \qquad (k = 1, 2, \ldots).$$

*Dabei sind* $p_k$ *und* $q_k$ *selbst denjenigen Ausdrücken gleich, die bei der naturgemäßen Darstellung der rechten Seite als Quotient zweier ganzer Funktionen der* $h_i$ *und* $\vartheta_i$ *den Zähler bzw. Nenner abgeben.*

4⁰. *Man hat*

$$0 < q_1 < q_2 < q_3 \cdots,$$
$$\frac{1}{2} > |p_1 - aq_1| > |p_2 - aq_2| > |p_3 - aq_3|, \ldots.$$

*Umsomehr nehmen die Beträge* $\left|\frac{p_k}{q_k} - a\right|$ *mit wachsendem Index ab. Wenn* $a$ *irrational ist, konvergieren die Brüche* $\frac{p_k}{q_k}$ *mit wachsendem Index nach der Größe* $a$.

5⁰. *Für jedes der Systeme* $p_k$, $q_k$ $(k = 1, 2, \ldots)$ *gilt*

$$|(p_k - aq_k)q_k| < \frac{1}{2}.$$

*Umgekehrt: Ist* $x, y$ *irgendein System von relativ primen ganzen Zahlen, wofür* $y > 0$ *und*

$$|(x - ay)y| < \frac{1}{2}$$

*gilt, so findet sich das Zahlenpaar $x$, $y$ stets unter den Systemen $p_k$, $q_k (k = 1, 2 \ldots)$.*

Aus dem Satze V entnimmt man noch: *Sind $b$, $c$ irgend zwei weitere reelle Größen, so kann man stets ganze Zahlen $x$, $y$ finden, so daß*

$$|(x - ay - b)(y - c)| < \tfrac{1}{4}$$

*ist, und zwar, wenn $a$ irrational ist, noch derart, daß zugleich $|x - ay - b|$ unter einer beliebig kleinen positiven Größe liegt.**)

Die hier definierte Kettenbruchentwicklung mit den Näherungsbrüchen $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$ zur Annäherung an die Größe $a$ soll der *Diagonalkettenbruch* für $a$ heißen, mit Rücksicht darauf, daß diese Näherungsbrüche zu den Parallelogrammen mit den Linien $x - ay = 0$ und $y = 0$ als *Diagonalen* in einer ganz entsprechenden Beziehung stehen, wie die Näherungsbrüche bei der gewöhnlichen Kettenbruchentwicklung

$$a = l_0 + \frac{1|}{|l_1} + \frac{1|}{|l_2} + \cdots,$$

wo $l_0$ eine ganze Zahl, $l_1, l_2, \ldots$ lauter positive Zahlen sind, zu den Parallelogrammen mit dem Nullpunkt als Mittelpunkt und mit Seiten *parallel* zu $x - ay = 0$, $y = 0$. Für diese *gewöhnliche* (auch sogenannte *regelmäßige* oder *normale*) Kettenbruchentwicklung würde ich alsdann den charakteristischeren Namen *Parallelkettenbruch* in Vorschlag bringen.

Nach einem bekannten Satze von Lagrange kommt jedes Zahlenpaar $x$, $y$, wobei $x$, $y$ relativ prim sind, $y > 0$ und $\left|\frac{x}{y} - a\right| < \frac{1}{2y^2}$ ist, als Zähler und Nenner eines Näherungsbruches der gewöhnlichen Kettenbruchentwicklung für $a$ vor. Danach erscheinen alle Näherungsbrüche des Diagonalkettenbruches für $a$ auch unter den Näherungsbrüchen des Parallelkettenbruches für $a$ und wird also, falls nicht beide Entwicklungen zusammenfallen, der Parallelkettenbruch stets langsamer konvergieren.

Der Diagonalkettenbruch für $a$ möge mit $a = DK\binom{\vartheta_1, \vartheta_2, \ldots}{h_0, h_1, h_2, \ldots}$, der Parallelkettenbruch für $a$ mit $a = PK(l_0, l_1, l_2, \ldots)$ bezeichnet

---

*) Tschebyscheff hat (in einem russisch geschriebenen Aufsatze in den Mémoires der Petersburger Akademie, T. X, Appendix 4, 1866; Oeuvres, T. I, p. 679) gezeigt, daß, wenn $a$, $b$ reelle Größen sind, stets ganze Zahlen $x$, $y$ existieren, wofür $|(x - ay - b)y| < 2$ ist. Hermite hat (Crelles Journal, Bd. 88, 1880; Oeuvres, T. III) bewiesen, daß der Ausdruck links durch ganze Zahlen $x$, $y$ kleiner als $\sqrt{\frac{2}{27}}$ gemacht werden kann. Der Satz im Texte ergibt ein schärferes Resultat, weil $\frac{1}{4} < \sqrt{\frac{2}{27}}$ ist.

werden. Die schon vorhin angedeutete geometrische Auffassung der Parallelkettenbrüche, welche der hier gegebenen Ableitung der Diagonalkettenbrüche entspricht, führt leicht zu folgendem Satze:

*Um aus der Reihe der Systeme $p_i$, $q_i (i = 0, 1, 2, \ldots)$ für den Diagonalkettenbruch von $a$ die Reihe der Zähler und Nenner der sämtlichen Näherungsbrüche des Parallelkettenbruches von $a$ zu erhalten, hat man nur die erstere Reihe in der Weise zu erweitern, daß, so oft eine Zahl $\vartheta_i = 1$ (für ein $i \geqq 1$) ausfällt, zwischen die beiden Systeme $p_{i-1}$, $q_{i-1}$ und $p_i$, $q_i$ noch das neue System $p_i - p_{i-1}$, $q_i - q_{i-1}$ eingefügt wird.*

Man leitet aus diesem Satze die nachstehende Regel ab, welche erlaubt, aus einem Diagonalkettenbruche $a = DK\begin{pmatrix} \vartheta_1, \vartheta_2, \ldots \\ h_0, h_1, h_2, \ldots \end{pmatrix}$ sogleich den Parallelkettenbruch $a = PK(l_0, l_1, l_2, \ldots)$ zu entnehmen:

*Aus der Reihe der Zahlen $h_0, h_1, h_2, \ldots$ entsteht die Reihe der Zahlen $l_0, l_1, l_2, \ldots$, indem an Stelle einer jeden Zahl $h_i$ substituiert wird:*

$$\begin{array}{lll} h_i, & \text{wenn} & \vartheta_i = -1, \quad \vartheta_{i+1} = -1, \\ h_i - 1, & \text{wenn} & \vartheta_i = \phantom{-}1, \quad \vartheta_{i+1} = -1, \\ h_i - 1, 1, & \text{wenn} & \vartheta_i = -1, \quad \vartheta_{i+1} = \phantom{-}1, \\ h_i - 2, 1, & \text{wenn} & \vartheta_i = \phantom{-}1, \quad \vartheta_{i+1} = \phantom{-}1 \end{array}$$

*ist; dabei hat man sich noch $\vartheta_0 = -1$ zu denken und dann von dieser Vorschrift auch für $i = 0$ Gebrauch zu machen.*

Die Diagonalkettenbrüche sind hiernach nicht bloß wegen der einfacheren Charakterisierung ihrer Näherungsbrüche leichter zu handhaben, sie enthalten auch alle Einzelheiten über die darzustellenden Größen, welche die Parallelkettenbrüche erkennen lassen.

Beispiel: Der Parallelkettenbruch für $\sqrt{13}$ ist

$$PK(3, 1, 1; 1, 1, 6, 1, 1; 1, 1, 6, 1, 1; \ldots)$$

mit den Näherungsbrüchen

$$\frac{3}{1}, \frac{4}{1}, \frac{7}{2}; \frac{11}{3}, \frac{18}{5}, \frac{119}{33}, \frac{137}{38}, \frac{256}{71}; \frac{393}{109}, \frac{649}{180}, \frac{4287}{1189}, \frac{4936}{1369}, \frac{9223}{2558}; \ldots,$$

der Diagonalkettenbruch für $\sqrt{13}$ ist

$$DK\begin{pmatrix} +, -, +, +, -, +, +, \ldots \\ 4, 2; 2, 8, 2; 2, 8, 2; \ldots \end{pmatrix}$$

mit den Näherungsbrüchen

$$\frac{4}{1}, \frac{7}{2}; \frac{18}{5}, \frac{137}{38}, \frac{256}{71}; \frac{649}{180}, \frac{4936}{1369}, \frac{9223}{2558}; \ldots$$

d. i. dem $2, 3; 5, 7, 8; \ldots 5k, 5k + 2, 5k + 3; \ldots$ ten Näherungsbruch der ersteren Entwicklung.

Dagegen würde diejenige Kettenbruchentwicklung

$$K\begin{pmatrix}\vartheta_1, \vartheta_2, \ldots \\ h_0, h_1, h_2, \ldots\end{pmatrix} = h_0 - \frac{\vartheta_1|}{|h_1} - \frac{\vartheta_2|}{|h_2} - \cdots,$$

wobei $\vartheta_1 = \pm 1$, $\vartheta_2 = \pm 1, \ldots$ und die $h_1, h_2, \ldots$ positive ganze Zahlen sind derart, daß die Reste $-\frac{\vartheta_k|}{|h_k} - \frac{\vartheta_{k+1}|}{|h_{k+1}} - \cdots$ stets zwischen $-\frac{1}{2}$ und $\frac{1}{2}$ liegen, für $\sqrt{13}$:

$$K\begin{pmatrix}1, 1, -1, 1, 1, -1, 1, \ldots \\ 4, 3; 2, \quad 7, 3; 2, \quad 7, 3; \ldots\end{pmatrix}$$

sein mit den Näherungsbrüchen

$$\frac{4}{1}, \frac{11}{3}; \frac{18}{5}, \frac{137}{38}, \frac{393}{109}; \frac{649}{180}, \frac{4936}{1369}, \frac{14159}{3927}; \ldots$$

d. i. dem $2, 4; 5, 7, 9; \ldots 5k, 5k+2, 5k+4; \ldots$ ten Näherungsbruche des Parallelkettenbruches für $\sqrt{13}$. Also erfüllt bei dieser Art der Entwicklung einerseits nicht jeder Näherungsbruch $\frac{x}{y}$ die Bedingung

$$\left|\frac{x}{y} - \sqrt{13}\right| < \frac{1}{2y^2},$$

andererseits kommt nicht jeder Bruch $\frac{x}{y}$ mit dieser Eigenschaft unter den Näherungsbrüchen vor.

Der Diagonalkettenbruch für die Basis der natürlichen Logarithmen lautet:

$$e = DK\begin{pmatrix}1, -1, 1, -1, \ldots, & 1, -1, \ldots \\ 3, 3, \quad 2, 5, \quad 2, \ldots, 2m+1, & 2, \ldots\end{pmatrix}.$$

Die Zähler und Nenner der Näherungsbrüche dieses Kettenbruches geben also die sämtlichen Auflösungen der Bedingung

$$-\frac{1}{2} < (x - ey)y < \frac{1}{2}$$

in relativ primen positiven ganzen Zahlen $x$, $y$.

## § 6.

1. Ein unendlicher Diagonalkettenbruch

$$DK\begin{pmatrix}\vartheta_1, \vartheta_2, \ldots \\ h_0, h_1, h_2, \ldots\end{pmatrix} \tag{1}$$

für eine irrationale Größe $a$ soll *periodisch* heißen, wenn es eine positive Zahl $v$ gibt, so daß von einem gewissen Index $j$ an stets

$$\vartheta_k = \vartheta_{k+v}, \quad h_k = h_{k+v} \qquad (k = j, j+1, j+2, \ldots) \tag{2}$$

ist. Das System der Werte

$$\begin{pmatrix} \vartheta_j, \vartheta_{j+1}, \ldots, \vartheta_{j+v-1} \\ h_j, h_{j+1}, \ldots, h_{j+v-1} \end{pmatrix}$$

heiße dann eine *Periode* des Kettenbruches.

Wir beweisen zunächst die folgende Tatsache:

*Ist der Diagonalkettenbruch für eine irrationale Größe a periodisch, so ist a Wurzel einer quadratischen Gleichung mit rationalen Koeffizienten.*

Wir verwenden für die Kette zu den Formen $\xi = x - ay$, $\eta = y$ die in § 3 eingeführten Bezeichnungen. Durch die Substitution

$$T_i = \begin{pmatrix} p_{i-1}, p_i \\ q_{i-1}, q_i \end{pmatrix}$$

geht $\xi$ in $\varepsilon_{i-1}\lambda_{i-1} X_i + \varepsilon_i \lambda_i Y_i$ über, man hat also die Formel der Komposition:

$$(1, -a)\, T_i = (\varepsilon_{i-1}\lambda_{i-1}, \varepsilon_i \lambda_i).$$

Aus § 3, Gleich. (2) leitet man allgemeiner die Regel

$$(\varepsilon_{i-1}\lambda_{i-1}, \varepsilon_i\lambda_i) \begin{pmatrix} 0, -\vartheta_i \\ 1, \quad h_i \end{pmatrix} \begin{pmatrix} 0, -\vartheta_{i+1} \\ 1, \quad h_{i+1} \end{pmatrix} \cdots \begin{pmatrix} 0, -\vartheta_{k-1} \\ 1, \quad h_{k-1} \end{pmatrix} = (\varepsilon_{k-1}\lambda_{k-1}, \varepsilon_k \lambda_k),$$
$$i < k$$

ab, und daraus entnimmt man insbesondere eine Beziehung:

$$\varepsilon_k \lambda_k = \varepsilon_{i-1}\lambda_{i-1} r_{i,k} + \varepsilon_i \lambda_i s_{i,k},$$

wo $r_{i,k}$, $s_{i,k}$ gewisse ganze Zahlen sind, die bloß von den Werten $\vartheta_i$, $h_i$, $\vartheta_{i+1}$, $h_{i+1}, \ldots, \vartheta_{k-1}$, $h_{k-1}$ abhängen. Da mit unbegrenzt wachsendem $k$ die Größe $\lambda_k$ nach Null konvergiert, ersieht man danach, daß das Verhältnis $\frac{\varepsilon_{i-1}\lambda_{i-1}}{\varepsilon_i \lambda_i}$ durch die unendliche Reihe der Größen $\vartheta_k$, $h_k$ für die sämtlichen Indizes $k \geqq i$ vollständig bestimmt ist.

Wenn nun mit irgendeinem Werte $v$ für alle Indizes $k \geqq j$ die Beziehungen (2) statthaben, muß daher notwendig

$$\frac{\varepsilon_{j+v-1}\lambda_{j+v-1}}{\varepsilon_{j+v}\lambda_{j+v}} = \frac{\varepsilon_{j-1}\lambda_{j-1}}{\varepsilon_j \lambda_j}$$

sein. Setzen wir $\frac{\varepsilon_{j+v-1}\lambda_{j+v-1}}{\varepsilon_{j-1}\lambda_{j-1}} = \tau$, wobei $0 < |\tau| < 1$ sein wird, so folgt

$$\varepsilon_{j+v-1}\lambda_{j+v-1} = \tau\, \varepsilon_{j-1}\lambda_{j-1}, \quad \varepsilon_{j+v}\lambda_{j+v} = \tau\, \varepsilon_j \lambda_j.$$

Nun hat man

$$(1, -a)\, T_{j+v} = (\tau\varepsilon_{j-1}\lambda_{j-1}, \tau\varepsilon_j\lambda_j), \quad (\varepsilon_{j-1}\lambda_{j-1}, \varepsilon_j\lambda_j)\, T_j^{-1} = (1, -a);$$

daraus entsteht

$$(1, -a)\, T_{j+v} T_j^{-1} = (\tau, -\tau a).$$

Bezeichnet man mit $\begin{pmatrix} \mathrm{p}, & \mathrm{r} \\ \mathrm{q}, & \mathrm{s} \end{pmatrix}$ das Koeffizientenschema der Substitution $T_{j+v}\, T_j^{-1}$, so bedeutet diese letzte Formel

$$\mathrm{p} - a\,\mathrm{q} = \tau, \quad \mathrm{r} - a\,\mathrm{s} = -\tau a.$$

Daraus erhält man

$$(\mathrm{r} - a\,\mathrm{s}) + (\mathrm{p} - a\,\mathrm{q})\, a = 0,$$

und hierin kann nicht $\mathrm{q} = 0$ sein, denn sonst müßte $\mathrm{p} = \tau$ sein, während $\tau$ keine ganze Zahl ist, da $|\tau|$ zwischen 0 und 1 fällt.

2. Wir beweisen jetzt die Umkehrung der eben festgestellten Tatsache:

Satz VII. *Ist eine irrationale Größe $a$ Wurzel einer quadratischen Gleichung mit rationalen Koeffizienten, so ist der Diagonalkettenbruch für $a$ stets periodisch.*

Beweis. Es sei

$$n_0 a^2 + n_1 a + n_2 = 0$$

diejenige Gleichung für $a$, in der $n_0$, $n_1$, $n_2$ relativ prime ganze Zahlen sind und $n_0 > 0$ ist. Man hat $a = \frac{-n_1 \pm \sqrt{n_1^{\,2} - 4 n_0 n_2}}{2 n_0}$, so daß die ganze Zahl $D = n_1^{\,2} - 4 n_0 n_2$ positiv und wegen der vorausgesetzten Irrationalität von $a$ jedenfalls nicht das Quadrat einer ganzen Zahl ist. Die zweite Wurzel jener Gleichung $\frac{-n_1 \mp \sqrt{D}}{2 n_0}$ werde mit $\bar{a}$ bezeichnet.

Wir setzen

$$\xi = x - a y = \alpha x + \beta y, \quad \eta = \frac{1}{a - \bar{a}}\,(x - \bar{a} y) = \gamma x + \delta y, \quad \zeta = y.$$

Dabei haben $\xi$, $\eta$ ebenso wie $\xi$, $\zeta$ die Determinante 1, und gilt eine Beziehung:

$$\zeta = \eta + b\xi, \quad b = -\frac{1}{a - \bar{a}} = \mp \frac{n_0}{\sqrt{D}}.$$

Sodann entsteht

$$\mp \sqrt{D}\, \xi \eta = f = n_0 x^2 + n_1 x y + n_2 y^2.$$

Wir betrachten nunmehr die Kette zu den Formen $\xi$, $\eta$. Diese Kette wird jedenfalls nach beiden Seiten unbegrenzt sein. Wir verwenden für diese Kette die in § 3 eingeführten Bezeichnungen. Außerdem mögen $\xi_i$, $\eta_i$ die Ausdrücke bedeuten, in welche $\xi$, $\eta$ durch die Substitution

$$(T_i) \qquad x = p_{i-1} X_i + p_i Y_i, \quad y = q_{i-1} X_i + q_i Y_i$$

übergehen, und es bedeute $\mathsf{T}_i$ das quadratische Schema $\begin{pmatrix} \varepsilon_{i-1}\lambda_{i-1}, & \varepsilon_i \lambda_i \\ \mu_{i-1}, & \mu_i \end{pmatrix}$ der Koeffizienten von $\xi_i$, $\eta_i$, wobei dann $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} T_i = \mathsf{T}_i$ gilt.

Durch die ganzzahlige Substitution $T_i$, deren Determinante $\pm 1$ ist, geht die Form $f = \pm \sqrt{D}\, \xi \eta$ in eine Form

$$f_i = \pm \sqrt{D}\, \xi_i \eta_i = N_0 X_i^2 + N_1 X_i Y_i + N_2 Y_i^2$$

über. Dabei sind $N_0, N_1, N_2$ ganze rationale Zahlen und folgt $N_1^2 - 4N_0N_2 = D$; da $D$ nicht eine Quadratzahl ist, hat man gewiß $N_0 \neq 0$, $N_2 \neq 0$. Zudem bestehen dabei nach § 2, 3 diese Beziehungen:

*entweder*

$$\frac{N_2}{N_0} < 0, \quad \frac{N_1}{N_0} > 0, \quad |N_0| < \tfrac{1}{2}\sqrt{D}, \quad |N_2| < \tfrac{1}{2}\sqrt{D}, \quad |N_1| < \sqrt{D}$$

*oder*

$$\frac{N_2}{N_0} > 0, \quad \frac{N_1}{N_0} > 0, \quad |N_0| < \tfrac{1}{2}\sqrt{D}, \quad |N_2| < \tfrac{1}{2}\sqrt{D}, \quad \sqrt{D} < |N_1| < \tfrac{3}{2}\sqrt{D},$$
$$|N_1 - N_0 - N_2| > \tfrac{1}{2}\sqrt{D}.$$

In jedem Falle kommen hiernach für die ganzzahligen Koeffizienten $N_0$, $N_1$, $N_2$ einer Form $f_i$ von vornherein nur eine endliche Anzahl von möglichen Wertsystemen in Betracht. Man wird also jedenfalls irgend zwei Indizes $i = j$ und $i = j + v$, wo $v > 0$ ist, finden können, für welche die beiden Formen $f_j$ und $f_{j+v}$ in den Koeffizienten $N_0$, $N_1$, $N_2$ übereinstimmen.

Ersetzt man $X_{j+v}$, $Y_{j+v}$ in den Formen $\xi_{j+v}$, $\eta_{j+v}$ durch die Zeichen $X_j$, $Y_j$ der Variablen in $\xi_j$, $\eta_j$, so werden dadurch Beziehungen

$$\xi_{j+v} = \mathsf{A}\xi_j + \mathsf{B}\eta_j, \qquad \eta_{j+v} = \Gamma\xi_j + \Delta\eta_j$$

hergestellt, wobei die Koeffizienten $\mathsf{A}$, $\mathsf{B}$, $\Gamma$, $\Delta$ durch $\mathsf{T}_{j+v} = \begin{pmatrix} \mathsf{A}, & \mathsf{B} \\ \Gamma, & \Delta \end{pmatrix} \mathsf{T}_j$ bestimmt sind, und vermöge dieser Beziehungen muß dann $\xi_{j+v}\eta_{j+v} = \xi_j\eta_j$ entstehen. Vergleicht man die Koeffizienten von $\xi_j^2$, $\eta_j^2$, $\xi_j\eta_j$ auf beiden Seiten dieser Gleichung, so folgt $\mathsf{A}\Gamma = 0$, $\mathsf{B}\Delta = 0$, $\mathsf{A}\Delta + \mathsf{B}\Gamma = 1$. Danach muß entweder

$$(3) \qquad \mathsf{B} = 0, \quad \Gamma = 0, \quad \mathsf{A} = \frac{1}{\Delta} = \tau; \qquad \xi_{j+v} = \tau\xi_j, \ \eta_{j+v} = \frac{1}{\tau}\eta_j$$

oder

$$(3^*) \qquad \mathsf{A} = 0, \quad \Delta = 0, \quad \mathsf{B} = \frac{1}{\Gamma} = \tau; \qquad \xi_{j+v} = \tau\eta_j, \ \eta_{j+v} = \frac{1}{\tau}\xi_j$$

mit einem von Null verschiedenen Faktor $\tau$ sein. Die zweite Art von Beziehungen aber ist unmöglich, weil in der Form $\eta_j$ der zweite Koeffizient einen größeren absoluten Betrag hat als der erste Koeffizient, in der Form $\xi_{j+v}$ aber das Entgegengesetzte statthaben muß. Also gelten notwendig die Beziehungen (3) und die Vergleichung der Koeffizienten in $\eta_j$ und $\eta_{j+v}$ zeigt noch, daß $\tau$ positiv und $< 1$ ist.

Die Gleichungen (3) ergeben

$$\mathsf{T}_{j+v} = \begin{pmatrix} \tau, & 0 \\ 0, & \frac{1}{\tau} \end{pmatrix} \mathsf{T}_j, \qquad \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} T_{j+v} T_j^{-1} = \begin{pmatrix} \tau, & 0 \\ 0, & \frac{1}{\tau} \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}.$$

Ist $\begin{pmatrix} \mathrm{p}, & \mathrm{r} \\ \mathrm{q}, & \mathrm{s} \end{pmatrix}$ das Koeffizientenschema der Substitution $T_{j+v} T_j^{-1}$, wobei p, q, r, s ganze Zahlen sind und $\mathrm{ps} - \mathrm{qr} = \pm 1$ ist, so verwandeln sich hiernach $\xi$, $\eta$, wenn man darin $x$, $y$ durch $\mathrm{p}x + \mathrm{r}y$, $\mathrm{q}x + \mathrm{s}y$ ersetzt, in die Ausdrücke $\tau\xi$, $\frac{1}{\tau}\eta$. Diese zwei Ausdrücke ergeben dasselbe Produkt wie $\xi$ und $\eta$. Durch die umgekehrte Substitution werden $\xi$, $\eta$ in $\frac{1}{\tau}\xi$, $\tau\eta$ übergehen. Hat man nun einen Gitterpunkt $x$, $y$, für den $x$, $y$ relativ prim sind und $\xi = \varepsilon\lambda$, $\eta = \mu$ ($\mu > 0$, $\lambda > 0$, $\varepsilon = \pm 1$), $\lambda\mu < \frac{1}{2}$ ist, so existiert dann also ein anderer Gitterpunkt, für den ebenfalls $x$, $y$ relativ prim sind und $\xi = \tau\varepsilon\lambda$, $\eta = \frac{1}{\tau}\mu$ ist, und ferner ein Gitterpunkt, für den $x$, $y$ relativ prim sind und $\xi = \frac{1}{\tau}\varepsilon\lambda$, $\eta = \tau\mu$ ist; und diese zwei weiteren Gitterpunkte müssen dann ebenso wie der erste als Glieder der Kette zu $\xi$, $\eta$ auftreten.

Nach (3) haben wir $\varepsilon_{j+v}\lambda_{j+v} = \tau\varepsilon_j\lambda_j$, $\mu_{j+v} = \frac{1}{\tau}\mu_j$. Nun müssen weiter die Punkte $\xi = \varepsilon_{j+v+1}\lambda_{j+v+1}$, $\eta = \mu_{j+v+1}$ und $\xi = \tau\varepsilon_{j+1}\lambda_{j+1}$, $\eta = \frac{1}{\tau}\mu_{j+1}$, welche beide als Glieder der Kette auftreten, identisch sein. Denn hätte man $\mu_{j+v+1} > \frac{1}{\tau}\mu_{j+1}$, so würde der Punkt $\xi = \tau\varepsilon_{j+1}\lambda_{j+1}$, $\eta = \frac{1}{\tau}\mu_{j+1}$ ein Kettenglied sein, für das $\mu_{j+v} < \eta < \mu_{j+v+1}$ wäre, während $\eta = \mu_{j+v}$ und $\eta = \mu_{j+v+1}$ ja zwei aufeinanderfolgenden Kettengliedern entsprechen. Hätte man dagegen $\mu_{j+v+1} < \frac{1}{\tau}\mu_{j+1}$, so würde $\xi = \frac{1}{\tau}\varepsilon_{j+v+1}\lambda_{j+v+1}$, $\eta = \tau\mu_{j+v+1}$ ein Kettenglied sein, wofür $\mu_j < \eta < \mu_{j+1}$ wäre, was ebenfalls nicht möglich ist. Also muß $\mu_{j+v+1} = \frac{1}{\tau}\mu_{j+1}$ sein und müssen sodann jene zwei Punkte zusammenfallen.

Auf dieselbe Art erschließt man sukzessive weiter

$$\varepsilon_{k+v}\lambda_{k+v} = \tau\varepsilon_k\lambda_k, \qquad \mu_{k+v} = \frac{1}{\tau}\mu_k \tag{4}$$

für $k = j+2, j+3, \ldots$. Sodann kann man in der Reihe der Indizes rückwärts gehen und diese Beziehungen (4), welche auch für $k = j-1$ bereits durch (3) feststehen, nacheinander für $k = j-2, j-3, \ldots$ erhalten. Also gelten diese Beziehungen (4) überhaupt für jeden möglichen Index $k$. Man hat nunmehr für jeden Index $i$: $\mathsf{T}_{i+v} = \begin{pmatrix} \tau, & 0 \\ 0, & \frac{1}{\tau} \end{pmatrix} \mathsf{T}_i$; andererseits gilt nach § 3, (2) die Regel $\mathsf{T}_{i+1} = \mathsf{T}_i \begin{pmatrix} 0, & -\vartheta_i \\ 1, & h_i \end{pmatrix}$. Wendet man

die erstere Formel für zwei aufeinanderfolgende Indizes $i = k$, $i = k+1$ an und hernach die letztere für $i = k$ und $i = k+v$, so folgt zuerst $\mathsf{T}_{k+v}^{-1}\mathsf{T}_{k+v+1} = \mathsf{T}_k^{-1}\mathsf{T}_{k+1}$ und sodann:

$$\vartheta_{k+v} = \vartheta_k, \qquad h_{k+v} = h_k \qquad (k = \cdots -2, -1, 0, 1, 2, \ldots). \tag{5}$$

Nach diesen Beziehungen (5) kann die Kette zu $\xi$, $\eta$ als *vollkommen periodisch* bezeichnet werden.

Wir ziehen endlich auch die Form $\zeta = y$ heran. Für ein jedes Glied $x = p_i$, $y = q_i$ der Kette zu den Formen $\xi$, $\eta$ gilt $\eta > 0$ und $|\xi\eta| < \frac{1}{2}$. Gleichzeitig ist dabei $\sqrt{D}|\xi\eta|$ stets eine rationale ganze Zahl. Indem diese Zahl $< \frac{1}{2}\sqrt{D}$ ist, kann sie nicht die größte in $\frac{1}{2}\sqrt{D}$ enthaltene ganze Zahl überschreiten. Wir setzen letztere ganze Zahl $\left[\frac{1}{2}\sqrt{D}\right] = \frac{1}{2}\sqrt{D} - d$, dabei wird $0 < d < 1$. Aus $\sqrt{D}|\xi\eta| \leqq \frac{1}{2}\sqrt{D} - d$ folgt mit Rücksicht auf $\zeta = y = \eta + b\xi$:

$$|\xi\zeta| \leqq \frac{1}{2} - \frac{d}{\sqrt{D}} + |b\xi^2|, \qquad \zeta \geqq \eta - |b\xi|.$$

Nun nimmt, wenn man die Reihe der Kettenglieder zu $\xi$, $\eta$ durchläuft, darin sowohl $|\xi|$ wie $\left|\frac{\xi}{\eta}\right|$ beständig ab. Geht man soweit in dieser Reihe, daß $|b\xi^2| < \frac{d}{\sqrt{D}}$ und $\left|\frac{\xi}{\eta}\right| < \frac{1}{|b|}$ ist, so hat man dann also $|\xi\zeta| < \frac{1}{2}$, $\zeta > 0$ und müssen daher die betreffenden Systeme $x = p_i$, $y = q_i$, die man nun antrifft, sämtlich auch Glieder der Kette zu den Formen $\xi$, $\zeta$ sein.

Ist umgekehrt $x$, $y$ ein Glied der Kette zu den Formen $\xi$, $\zeta$, so ist dafür $\zeta > 0$ und $|\xi\zeta| < \frac{1}{2}$; daraus folgt

$$\sqrt{D}|\xi\eta| < \frac{1}{2}\sqrt{D} + |\sqrt{D}b\xi^2|, \qquad \eta \geqq \zeta - |b\xi|.$$

Geht man nun in der Reihe der Kettenglieder zu $\xi$, $\zeta$ so weit, daß $|\sqrt{D}b\xi^2| \leqq 1 - d$ und $\left|\frac{\xi}{\zeta}\right| < \frac{1}{|b|}$ ist, so folgt hier $\eta > 0$ und andererseits $\sqrt{D}|\xi\eta| < \left[\frac{1}{2}\sqrt{D}\right] + 1$. Da aber $\sqrt{D}|\xi\eta|$ hierbei stets eine ganze rationale Zahl wird, muß dann überhaupt $\sqrt{D}|\xi\eta| \leqq \left[\frac{1}{2}\sqrt{D}\right] < \frac{1}{2}\sqrt{D}$, mithin $|\xi\eta| < \frac{1}{2}$ sein. Danach findet sich alsdann das betreffende System $x$, $y$ stets auch unter den Gliedern der Kette zu $\xi$, $\eta$.

Auf diese Weise stimmen überhaupt die zu $\xi$, $\eta$ und die zu $\xi$, $\zeta$ gehörige Kette von gewissen zwei Gliedern an in dem ganzen weiteren Verlaufe ihrer Kettenglieder völlig miteinander überein. Da nun die einzelnen Werte $\vartheta_i$, $h_i$ in einer Kette jedesmal aus drei aufeinanderfolgenden

Kettengliedern abzuleiten sind, so werden sich danach auch die Relationen (5) von einem gewissen Index an auf die Kette zu $\xi = x - ay$, $\zeta = y$ übertragen, d. h. eben der Diagonalkettenbruch für die Größe $a$ ist periodisch.

In entsprechender Beziehung wie der Diagonalkettenbruch für $a$ zu der Kette steht, die zu den Formen $\xi$, $\eta$ gehört, steht der Diagonalkettenbruch für die konjugierte algebraische Zahl $\bar{a}$ zu der Kette, die zu den Formen $(a - \bar{a})\eta$, $-\frac{1}{a - \bar{a}}\xi$ oder, was auf dasselbe hinauskommt, zu $\eta$, $-\xi$ gehört. Der einfache Zusammenhang der Kette zu $\xi$, $\eta$ und der Kette zu $\eta$, $-\xi$ ist am Schlusse von § 3 erörtert; aus der dort angegebenen Beziehung (7) erhellt nun, daß, wenn $\begin{pmatrix} \vartheta_j, & \vartheta_{j+1}, \cdots, & \vartheta_{j+\nu-1} \\ h_j, & h_{j+1}, \cdots, & h_{j+\nu-1} \end{pmatrix}$ eine Periode des Diagonalkettenbruches für $a$ ist, $\begin{pmatrix} \vartheta_j, & \vartheta_{j+\nu-1}, \cdots, & \vartheta_{j+1} \\ h_{j+\nu-1}, & h_{j+\nu-2}, \cdots, & h_j \end{pmatrix}$ eine Periode des Diagonalkettenbruches für $\bar{a}$ sein wird.

Zürich, den 31. Dezember 1899.

XVII.

# Quelques nouveaux théorèmes sur l'approximation des quantités a l'aide de nombres rationnels.

(Bulletin des Sciences mathématiques, 2e série, t. XXV, pp. 72—76.)

Dans plusieurs de ses Mémoires classiques sur la théorie des nombres M. Hermite s'est occupé de la recherche des minima de formes algébriques pour des valeurs entières des variables. Cette recherche l'a conduit à certaines approximations, dont il a mis parfaitement en évidence le *caractère algébrique*. Mais pour la plupart des inégalités que l'on obtient dans ce domaine, il y a encore une grande difficulté à déterminer les *limites les plus étroites* des inégalités et les *formes extrêmes* auxquelles en chaque cas ces limites sont rattachées. Dans quelques cas particulièrement simples je donnerai ici de telles limites précises; pour les démonstrations, un peu longues, je dois renvoyer le lecteur au deuxième cahier de ma *Géométrie des nombres*, qui paraîtra prochainement chez B. G. Teubner.*)

## I.

1. *Théorème.* — *Soient* $\varphi$, $\chi$, $\psi$, $\omega$ *quatre formes linéaires à trois variables* $x$, $y$, $z$, *à coefficients réels quelconques et de sorte que l'on ait*

$$\varphi + \chi + \psi + \omega = 0.$$

*Supposons que le déterminant de trois de ces formes soit toujours différent de zéro et désignons sa valeur absolue par* $4D$.

*Alors il existe toujours trois nombres entiers* $x$, $y$, $z$, *qui ne sont pas tous égaux à zéro et de sorte que toutes les quatre formes* $\varphi$, $\chi$, $\psi$, $\omega$ *soient en valeur absolue moindres que*

$$\sqrt[3]{\frac{4D}{1-\left(\frac{2}{3}\right)^3}}.$$

La limite $d = \sqrt[3]{\frac{108}{19}D}$ donnée ici est précise. En général, on peut aussi trouver des nombres entiers $x$, $y$, $z$ différents du système 0, 0, 0 et tels que les valeurs absolues de $\varphi$, $\chi$, $\psi$, $\omega$ soient toutes $< d$. Mais

*) Vgl. Diophantische Approximationen, Kap. III und insbesondere Kap. VI. (Anm. d. Herausg.)

il y a un cas d'exception, où il sera impossible de satisfaire à cette autre condition, c'est lorsqu'il existe une substitution linéaire à coefficients entiers et à déterminant $\pm 1$, transformant les formes $\varphi$, $\chi$, $\psi$, $\omega$, abstraction faite de l'ordre, en

$$d\left(X - \tfrac{2}{3}Y\right), \quad d\left(Y - \tfrac{2}{3}Z\right), \quad d\left(-\tfrac{2}{3}X + Z\right), \quad -\tfrac{1}{3}d(X + Y + Z).$$

2. Le théorème que nous venons d'énoncer est susceptible d'une interprétation géométrique, qui peut-être trouvera une application dans la cristallographie:

Imaginons un système d'octaèdres, tous congruents entre eux et parallèlement orientés, en nombre infini et placés dans l'espace de manière que deux de ces corps n'aient jamais une partie commune et que leurs centres de gravité forment un réseau parallélépipédique de points, comme Bravais l'a considéré dans sa théorie de la structure des cristaux. (Tous les octaèdres peuvent alors être déduits de l'un quelconque d'entre eux par le même système de translations). Il y aura une situation où les lacunes laissées par les octaèdres seront les plus étroites, ou, ce qui est la même chose, l'espace occupé par les corps sera le plus grand possible; c'est la situation où chacun des octaèdres a au moins un point commun avec quatorze autres de ces corps, et alors *le rapport de l'espace occupe par les octaèdres à l'espace laissé libre par ces corps sera de* 18 *à* 1.

3. Soient $\xi$, $\eta$, $\zeta$ trois formes en $x$, $y$, $z$ à coefficients réels et à déterminant $\pm D$, où $D > 0$. On pourra prendre dans le théorème du n° 1:

$$\varphi = -\xi + \eta + \zeta, \quad \chi = \xi - \eta + \zeta, \quad \psi = \xi + \eta - \zeta, \quad \omega = -\xi - \eta - \zeta.$$

*Il existe alors des nombres entiers* $x$, $y$, $z$ *différents du système* 0, 0, 0 *et de sorte que l'on ait*

$$|\xi| + |\eta| + |\zeta| \leqq \sqrt[3]{\tfrac{108}{19}D}.$$

Dans le cas limite, pour lequel le signe $=$ est réservé, on peut toujours faire en sorte que l'on n'ait pas à la fois $|\xi| = |\eta| = |\zeta|$.

On en tire alors

$$|\xi\eta\zeta| < \tfrac{4}{19}D.$$

Or on doit remarquer que, dans cette dernière inégalité, le facteur $\frac{4}{19}$ pourrait encore être remplacé par un nombre plus petit.

4. D'autre part, on peut aussi prendre dans le n° 1:

$$\frac{\varphi}{\sqrt[3]{2}}, \quad \frac{\chi}{\sqrt[3]{2}}, \quad \frac{\psi}{\sqrt[3]{2}}, \quad \frac{\omega}{\sqrt[3]{2}} = \xi + \zeta, \quad -\xi + \zeta, \quad \eta - \zeta, \quad -\eta - \zeta.$$

On voit alors qu'*il existe des nombres entiers* $x$, $y$, $z$ *différents du système* 0, 0, 0 *de sorte que l'on ait*

$$|\xi| + |\zeta| \leqq \sqrt[3]{\frac{54}{19} D}, \qquad |\eta| + |\zeta| \leqq \sqrt[3]{\frac{54}{19} D}.$$

Dans le cas limite où l'on doit prendre ici un des deux signes $=$, on peut toujours faire en sorte que l'on n'ait ni $\pm \xi = \zeta$ ni $\pm \eta = \zeta$.

En faisant usage alors des inégalités

$$\left|\left(\frac{\xi}{2}\right)^2 \zeta\right| \leqq \left(\frac{2\left|\frac{\xi}{2}\right| + |\zeta|}{3}\right)^3, \qquad \left|\left(\frac{\eta}{2}\right)^2 \zeta\right| \leqq \left(\frac{2\left|\frac{\eta}{2}\right| + |\zeta|}{3}\right)^3,$$

on trouve

$$|\xi^2 \zeta| < \frac{8}{19} D, \qquad |\eta^2 \zeta| < \frac{8}{19} D.$$

Dans ces dernières inégalités, la limite n'est plus précise.

5. Soient *a, b deux quantités réelles* quelconques. Posons, dans les inégalités du n° 4:

$$\xi = x - az, \qquad \eta = y - bz, \qquad \zeta = \frac{z}{t^3},$$

$t$ étant un paramètre positif. On voit qu'on peut trouver des nombres entiers $x, y, z$, parmi lesquels $z$ est positif, et de sorte que $x - az$, $y - bz$ soient en valeur absolue plus petites qu'une quantité $\varepsilon$ donnée à volonté, et *que dans cette approximation on ait en même temps*

$$\left|\frac{x}{z} - a\right| < \sqrt{\frac{8}{19}} \frac{1}{z^{\frac{3}{2}}}, \qquad \left|\frac{y}{z} - b\right| < \sqrt{\frac{8}{19}} \frac{1}{z^{\frac{3}{2}}}.$$

La constante $\sqrt{\frac{8}{19}} = 0{,}648\ldots$, qui entre ici, est plus petite que $\frac{2}{3}$.

II.

6. *Théorème. — Soient* $\xi = \alpha x + \beta y$, $\eta = \gamma x + \delta y$ *deux formes linéaires à coefficients complexes quelconques et soit* $D = |\alpha\delta - \beta\gamma| > 0$. *On peut toujours trouver, dans le corps algébrique de* $i = \sqrt{-1}$, *des nombres entiers complexes* $x, y$ *différents du système* 0, 0 *de sorte que l'on ait*

$$|\xi| \leqq \sqrt{\frac{\sqrt{3}+1}{\sqrt{6}} D}, \qquad |\eta| \leqq \sqrt{\frac{\sqrt{3}+1}{\sqrt{6}} D}.$$

La limite $d = \sqrt{\frac{\sqrt{3}+1}{\sqrt{6}} D}$ donnée ici est précise. En général, on aura aussi des nombres entiers complexes $x, y \neq 0, 0$ de sorte que $|\xi| < d$, $|\eta| < d$. Mais dans un seul cas il sera impossible de satisfaire à ces autres inégalités; c'est lorsqu'il existe une substitution

$$x = pX + rY, \qquad y = qX + sY,$$

où $p, q, r, s$ sont des nombres entiers dans le corps de $i$ et le détermi-

nant $ps - qr = \pm 1$ ou $\pm i$, de sorte que, par cette substitution, $\xi$, $\eta$ soient transformées en

$$\lambda d\left\{X + \left[\frac{1}{2} - i\left(1 - \frac{\sqrt{3}}{2}\right)\right] Y\right\}, \qquad \mu d\left\{\left[\frac{i}{2} + \left(1 - \frac{\sqrt{3}}{2}\right)\right] X + Y\right\},$$

$\lambda$ et $\mu$ étant des quantités dont la valeur absolue est égale à 1.

7. *Théorème. — Soient* $\xi = \alpha x + \beta y$, $\eta = \gamma x + \delta y$ *deux formes linéaires à coefficients complexes quelconques et soit* $D = |\alpha\delta - \beta\gamma| > 0$. *On peut toujours trouver, dans le corps algébrique de* $j = \frac{-1+\sqrt{-3}}{2}$, *des nombres entiers complexes* $x$, $y$ *différents du système* 0, 0 *de sorte que l'on ait*

$$|\xi| \leqq \sqrt{D}, \qquad |\eta| \leqq \sqrt{D}.$$

Cette limite $d = \sqrt{D}$ est ici précise. En général, il y aura aussi des nombres entiers $x$, $y \neq 0$, 0 de sorte que $|\xi|$ et $|\eta|$ soient $< d$, excepté dans le cas où, dans le corps de $j$, il existe une substitution linéaire à coefficients entiers et à déterminant égal à une unité du corps, à l'aide de laquelle $\xi$, $\eta$, abstraction faite de l'ordre, se changent en $\lambda d X$, $\mu d(\tau X + Y)$, $\lambda$ et $\mu$ étant des quantités dont la valeur absolue est égale à 1, et $\tau$ une quantité complexe quelconque.

On remarquera ce fait intéressant que, de ces deux théorèmes correspondants, l'un, qui est relatif au corps algébrique de la *troisième racine de l'unité*, est beaucoup plus simple que l'autre, relatif au corps algébrique de la *quatrième racine de l'unité.*

8. Soit *a une quantité complexe* quelconque. En posant

$$\xi = x - ay, \quad \eta = \frac{y}{t^2},$$

$t$ étant un paramètre réel quelconque $> 1$, on voit que, *dans le corps de* $\frac{-1+\sqrt{-3}}{2}$ (mais pas dans le corps de $\sqrt{-1}$), *il y aura toujours des nombres entiers complexes* $x$, $y$ *tels que*

$$0 < |y| \leqq t, \qquad |x - ay| < \frac{1}{t},$$

d'où l'on tire encore

$$|(x - ay)y| < 1.$$

XVIII.

# Über periodische Approximationen algebraischer Zahlen.

(Acta Mathematica, Band 26, (Niels Henrik Abel in memoriam), S. 333—351.)

Abel sagt an einer Stelle (Oeuvres, T. II, p. 217) mit Bezug auf das Problem der algebraischen Auflösung der Gleichungen: „Au lieu de demander une relation dont on ne sait pas si elle existe ou non, il faut demander si une telle relation est en effet possible“. Eben diese Weisung befolgend, können wir auch einer anderen, noch unerledigten Aufgabe auf dem mannigfaltigen Gebiete der Auflösung der Gleichungen näherzutreten versuchen. Wir wollen hier die Frage behandeln:

*Welche algebraische Zahlen besitzen analoge periodische Approximationen, wie sie die reellen algebraischen Zahlen zweiten Grades vermöge der Periodizität ihrer Entwicklungen in gewöhnliche Kettenbrüche aufweisen.*

## § 1. Periodische Substitutionenketten.

1. Es sei $\alpha$ eine beliebige Größe und es werde $l = 1$ oder $= 2$ gesetzt, je nachdem $\alpha$ reell oder komplex ist. Wenn $\alpha$ eine *algebraische Zahl* $n^{\text{ten}}$ *Grades*, d. h. eine Wurzel einer im Bereiche der rationalen Zahlen irreduziblen Gleichung $n^{\text{ten}}$ Grades ist, so kann der Ausdruck

$$\xi = x_1 + \alpha x_2 + \cdots + \alpha^{n-1} x_n$$

für ganze rationale Zahlen $x_1, x_2, \ldots, x_n$, die nicht sämtlich Null sind, niemals verschwinden, aber, wofern $n > l$ ist, wohl dem Werte Null beliebig nahe kommen. Wir machen hier stets die Annahme $n > l$. Über die Annäherungen dieser Form $\xi$ an Null gelten dann, wie ich in dem Aufsatze *„Ein Kriterium für die algebraischen Zahlen“* (Göttinger Nachrichten v. 11. Febr. 1899; diese Ges. Abhandlungen, Bd. I, S. 293—315) gezeigt habe, die folgenden Sätze:

*Wir können zur Zahl $\alpha$ in bezug auf jede beliebige reelle Größe $r \geqq 1$ stets eine Substitution*

$$S) \qquad x_h = s_h^{(1)} y_1 + s_h^{(2)} y_2 + \cdots + s_h^{(n)} y_n \qquad (h = 1, 2, \ldots, n)$$

*mit folgenden Eigenschaften konstruieren:*

a) *Alle Koeffizienten* $s_h^{(k)}$ *sind ganze rationale Zahlen, und gehen die Quotienten* $\frac{s_h^{(k)}}{r}$ *dem Betrage nach nicht über eine gewisse, von* $r$ *unabhängige Größe hinaus.*

b) *Die Determinante von* $S$ *ist* $\neq 0$ *und liegt dem Betrage nach unter einer gewissen, von* $r$ *nicht abhängigen Grenze.*

c) *Geht* $\xi$ *durch* $S$ *in*

$$\varphi = \varrho_1 y_1 + \varrho_2 y_2 + \cdots + \varrho_n y_n$$

*über, so liegen die Beträge von*

$$\varrho_1 r^{\frac{n-l}{l}}, \quad \varrho_2 r^{\frac{n-l}{l}}, \ldots, \varrho_n r^{\frac{n-l}{l}}$$

*sämtlich unter einer gewissen, von* $r$ *nicht abhängigen Grenze.*

d) *Für die Verhältnisse* $\varrho_1 : \varrho_2 : \ldots : \varrho_n$ *kommen von vornherein nur eine endliche Anzahl verschiedener Systeme in Betracht, die von* $r$ *nicht abhängen.*

Diesen Bedingungen wird z. B., wie in jener Arbeit ausgeführt ist, stets genügt, wenn wir $S$ unter allen denjenigen Substitutionen, für welche die Koeffizienten $s_h^{(k)}$ lauter Zahlen aus der Reihe $0, \pm 1, \pm 2, \cdots, \pm [r]$ sind und die Determinante $\neq 0$ ist, derart auswählen, daß dabei zunächst $|\varrho_1|$, nächstdem $|\varrho_2|, \ldots$ endlich $|\varrho_n|$ möglichst klein werden. Dabei fällt dann die Determinante von $S$ dem Betrage nach sicher stets $\leqq n!$ aus.

Durch die Substitution $S$ erlangen wir zugleich gewisse rationale Approximationen für alle Zahlen des Körpers von $\alpha$, wenn $\alpha$ reell ist, bzw., wenn $\alpha$ komplex ist, für alle reellen Zahlen *des* Körpers, der aus dem Körper von $\alpha$ und dem dazu konjugiert imaginären Körper zusammengesetzt ist.

Umgekehrt gilt der Satz: *Die Größe* $\alpha$ *ist,* ($n > l$ *angenommen*), *notwendig eine algebraische Zahl* $n^{\text{ten}}$ *Grades, wenn für sie in bezug auf jede reelle Größe* $r \geqq 1$ *stets eine den Bedingungen* a), b), c), d) *entsprechende Substitution* $S$ *hergestellt werden kann.*

2. Wir denken uns weiterhin $\alpha$ stets als eine algebraische Zahl $n^{\text{ten}}$ Grades und $n > l$. Nehmen wir nun eine unbegrenzte Reihe wachsender Zahlen $r_1 \geqq 1, r_2, r_3, \ldots$ an und konstruieren wir in der eben erörterten Weise zu diesen Zahlen Substitutionen $S_1, S_2, S_3, \ldots$. *Eine derartige Substitutionenkette für die Zahl* $\alpha$ *soll periodisch heißen, wenn die daraus vermöge der Kompositionsformeln*

$$S_2 = S_1 Q_1, \quad S_3 = S_2 Q_2, \ldots, S_{j+1} = S_j Q_j, \ldots$$

*hergeleitete Reihe von Substitutionen* $Q_1, Q_2, Q_3, \ldots$, *abgesehen von einer endlichen Anzahl von Gliedern am Anfange, in periodischer Wiederholung ein und derselben endlichen Folge von Substitutionen besteht,* wenn also ein

Index $j_0$ und eine positive Zahl $p_0$ angebbar sind, so daß für jeden beliebigen Index $j \geqq j_0$ stets $Q_j = Q_{j+p_0}$ ist.

*Wir fragen nach dem Charakter derjenigen algebraischen Zahlen $\alpha$, für welche periodische Substitutionenketten existieren.*

3. Ist die Kette $S_1, S_2, S_3, \ldots$ für $\alpha$ periodisch, so erhalten wir mit den soeben eingeführten Bezeichnungen

$$Q_j = S_j^{-1} S_{j+1}, \quad S_j^{-1} S_{j+1} = S_{j+p_0}^{-1} S_{j+p_0+1}, \quad j \geqq j_0,$$

also

$$S_{j+p_0} S_j^{-1} = S_{j+p_0+1} S_{j+1}^{-1},$$

wenn $j \geqq j_0$ ist. Setzen wir $S_{j_0+p_0} S_{j_0}^{-1} = P_0$, so folgt daraus allgemein

$$S_{j+p_0} = P_0 S_j, \quad S_{j+fp_0} = P_0^f S_j$$

für jeden Index $j \geqq j_0$ und jeden Exponenten $f = 1, 2, 3, \ldots$.

Es bedeute $\varphi_j$ die Linearform, in welche $\xi$ durch $S_j$ übergeht. Unter den unendlich vielen Substitutionen $S_{j_0+fp_0}$ für $f = 0, 1, 2, \ldots$ werden wir, da nach b) für ihre Determinanten und weiter nach d) für die Verhältnisse der Koeffizienten $\varrho_1 : \varrho_2 : \ldots : \varrho_n$ in den zugehörigen Formen $\varphi_{j_0+fp_0}$ nur eine endliche Anzahl von Wertsystemen in Betracht kommen, jedenfalls irgend zwei Substitutionen $S_{j_0+cp_0} = S$ und $S_{j_0+dp_0} = T$ $(d > c)$ in solcher Weise auffinden können, *daß erstens* $TS^{-1} = P = P_0^{d-c}$ *eine ganzzahlige Substitution mit der Determinante* 1 *wird und zudem zweitens in den beiden Formen* $\varphi_{j_0+cp_0} = \varphi$ *und* $\varphi_{j_0+dp_0} = \psi$ *die n Koeffizienten jedesmal genau dieselben Verhältnisse besitzen,* daß also $\psi = \vartheta\varphi$ gilt, wo $\vartheta$ ein konstanter Faktor ist. (Die erstere Forderung wird z. B. gewiß erfüllt sein, wenn wir $S$ und $T$ derart auswählen, daß ihre Determinanten gleichen Wert haben und zudem in ihnen nach dieser Determinante als Modul je zwei entsprechende Koeffizienten immer gleichrestig sind.) Der Faktor $\vartheta$ wird als Quotient der Koeffizienten in $\psi$ und $\varphi$ wie diese Zahlen im Körper von $\alpha$ liegen. Setzen wir $(d-c)p_0 = p$, so gehen aus $T = PS$, $\psi = \vartheta\varphi$ vermöge $Q_j = Q_{j+p}$ $(j \geqq j_0)$ die Beziehungen

$$S_{j+p} = PS_j, \quad \varphi_{j+p} = \vartheta\varphi_j$$

für jeden Index $j \geqq j_0$ hervor. Wir erhalten sodann allgemeiner

$$S_{j+fp} = P^f S_j, \quad \varphi_{j+fp} = \vartheta^f \varphi_j \qquad (j \geqq j_0)$$

für $f = 1, 2, 3, \ldots$. Da in den Formen $\varphi_j$ mit wachsendem Index $j$ die Beträge der Koeffizienten jedenfalls nach Null abnehmen, muß $|\vartheta| < 1$ sein.

4. Wenn $\alpha$ komplex ist, bedeute $\alpha^0$ die zu $\alpha$ konjugiert imaginäre Größe. Die $n - l$ Wurzeln der irreduziblen Gleichung für $\alpha$ außer $\alpha$, bzw. außer $\alpha$ und $\alpha^0$ mögen $\alpha', \alpha'', \ldots, \alpha^{(n-l)}$ heißen. Ferner bezeichnen wir die zu einer Zahl $\vartheta$ oder einer Form $\xi$ des Körpers von $\alpha$ konjugierten Zahlen oder Formen in den Körpern von $(\alpha^0), \alpha', \ldots, \alpha^{(n-l)}$ analog durch

Hinzufügung oberer Indizes (0), $1, \ldots, n-l$. Durch die Substitution $P = S_{j_0+p} S_{j_0}^{-1}$ geht $\xi$ in $\vartheta\xi$ und gehen daher wegen der Irreduzibilität der Gleichung $n^{\text{ten}}$ Grades für $\alpha$ weiter $(\xi^0), \xi', \ldots, \xi^{(n-l)}$ in $(\vartheta^0\xi^0), \vartheta'\xi', \ldots, \vartheta^{(n-l)}\xi^{(n-l)}$ über. Bedeutet nun $t$ einen unbestimmten Parameter, $E$ die identische Substitution, so gehen $\xi, \ldots, \xi^{(n-l)}$ durch die Substitution $tE - P$ in $(t-\vartheta)\xi, \ldots, (t-\vartheta^{(n-l)})\xi^{(n-l)}$ über und ist infolgedessen $|tE-P|$, d. h. die *Determinante* von $tE-P$, gleich dem Produkte $(t-\vartheta)\ldots(t-\vartheta^{(n-l)})$. Diese in $t$ identisch erfüllte Beziehung zeigt, daß $\vartheta$ der Gleichung $|tE-P| = 0$ genügt. Indem $P$ eine ganzzahlige Substitution und ihre Determinante 1 ist, erweist sich dadurch $\vartheta$ als eine *ganze Zahl* und als eine *Einheit* im Körper von $\alpha$.

5. Es sei nun $a_0$ eine solche ganze rationale Zahl, daß $a_0\alpha$ eine *ganze* algebraische Zahl wird, so hat das Produkt $a_0^{n-1}\xi$ als Koeffizienten lauter *ganze* algebraische Zahlen und *sind* daher auch *in jeder einzelnen Form* $a_0^{n-1}\varphi_j$ *die bezüglichen n Koeffizienten* $a_0^{n-1}\varrho_k (k = 1, 2, \ldots, n)$ *stets lauter von Null verschiedene ganze algebraische Zahlen, also deren Normen im Körper von* $\alpha$ *stets dem Betrage nach* $\geqq 1$. Wegen der Eigenschaft a) der Substitutionen $S_j$ liegt dabei jeder Betrag

$$\frac{|\varrho_k^{(h)}|}{r_j} \qquad (h = 1, \ldots, n-l; k = 1, 2, \ldots, n)$$

nicht über einer gewissen von $j$ unabhängigen Grenze. Verwenden wir nun die hierdurch gegebenen Ungleichungen für alle Indizes $h = 1, \ldots, n-l$ mit Ausnahme eines beliebigen Index $g$ dieser Reihe und berücksichtigen wir außerdem die Eigenschaft c) für $S_j$ und, falls $l = 2$ ist, noch die Beziehung $|\varrho_k| = |\varrho_k^0|$, so gewinnen wir aus der Ungleichung

$$|Nm\, a_0^{n-1}\varrho_k| \geqq 1$$

eine gewisse, von $r_j$ unabhängige, *positive untere* Grenze für den einen darin übrig bleibenden Faktor $\frac{|\varrho_k^{(g)}|}{r_j}$. *Danach befinden sich nun alle Beträge* $\frac{|\varrho_k^{(g)}|}{r_j}$ *in bezug auf die Form* $\varphi_j$ *zwischen zwei bestimmten endlichen positiven, von* $r_j$ *unabhängigen Grenzen,* und werden infolgedessen weiter auch *die Quotienten aus irgend zwei der je* $n-l$ *konjugierten Werte*

$$\varrho_k', \varrho_k'', \ldots, \varrho_k^{(n-l)} \qquad (k = 1, 2, \ldots, n)$$

bei sämtlichen Formen $\varphi_j$ stets absolut genommen zwischen zwei, unabhängig von den Werten $r_j$ feststehenden positiven endlichen Grenzen liegen. Beachten wir nun die Relationen $\varphi_{j+fp} = \vartheta^f\varphi_j$ für $f = 1, 2, 3, \ldots$, so zeigt sich schließlich, daß auch die Beträge der Quotienten aus irgend zwei der je $n-l$ Größen

$$\vartheta'^f, \vartheta''^f, \ldots, (\vartheta^{(n-l)})^f$$

zwischen gewissen zwei festen positiven endlichen Grenzen liegen müssen, *und zwar gelten diese Grenzen für alle Werte* $f = 1, 2, 3, \ldots$ *auf einmal.* Danach kann die Einheit $\vartheta$ nicht anders beschaffen sein, als daß für sie die Gleichungen

$$|\vartheta'| = |\vartheta''| = \cdots = |\vartheta^{(n-l)}|$$

statthaben. Bezeichnen wir den gemeinsamen Wert dieser letzten Beträge mit $\eta$ und setzen $|\vartheta| = \varepsilon$, womit im Falle $l = 2$ noch $|\vartheta^0|$ zusammenfällt, so geht die Gleichung $Nm\,\vartheta = 1$ in $\varepsilon^l \eta^{n-l} = 1$ über, und wegen $\varepsilon < 1$ folgt $\eta > 1$. Wir gelangen auf diese Weise zu dem Satze:

*Damit eine algebraische Zahl* $n^{ten}$ *Grades* $\alpha$ *eine periodische Substitutionenkette besitze, muß es im Körper von* $\alpha$ *eine Einheit* $\vartheta$ *von einem Betrage* $< 1$ *geben, für welche die konjugierten Zahlen in den konjugierten Körpern (abgesehen von der Zahl* $\vartheta^0$ *in dem Körper der konjugiert imaginären Zahl* $\alpha^0$*, falls* $\alpha$ *komplex ist) sämtlich untereinander gleichen Betrag haben.*

6. *Die hier gefundene Bedingung ist zugleich hinreichend für das Vorhandensein einer periodischen Substitutionenkette zur Zahl* $\alpha$. Denn nehmen wir an, es existiere im Körper von $\alpha$ eine Einheit $\vartheta_0$ von dem fraglichen Charakter. Es bedeute dann $P_0$ diejenige lineare Substitution, durch welche die $n$ Formen $\xi, (\xi^0), \ldots, \xi^{(n-l)}$ in die Formen $\vartheta_0 \xi, (\vartheta_0{}^0 \xi^0), \ldots, \vartheta_0^{(n-l)} \xi^{(n-l)}$ übergehen; diese Substitution hat lauter *rationale* Koeffizienten und eine *Determinante* $= \pm 1$. Durch $P_0{}^f$, wenn $f$ eine der Zahlen $1, 2, 3, \ldots$ bedeutet, gehen dann $\xi, \ldots, \xi^{(n-l)}$ in $\vartheta_0{}^f \xi, \ldots, (\vartheta_0^{(n-l)})^f \xi^{(n-l)}$ über. Da diese Potenzen $\vartheta_0{}^f$ lauter *ganze* algebraische Zahlen sind, werden, wie leicht zu sehen ist, in allen jenen Substitutionen $P_0{}^f$ die Koeffizienten solche ganze rationale Zahlen sein, daß ihre Nenner nicht über eine gewisse, durch die Größe $\alpha$ bestimmte, aber von den Exponenten $f$ unabhängige Zahl hinausgehen, während zugleich ihre Determinanten durchweg $= \pm 1$ sind. Wir werden infolgedessen unter jenen unendlich vielen Substitutionen $P_0{}^f$ gewiß irgend zwei solche, $P_0{}^c$ und $P_0{}^d$ $(d > c)$, finden können, daß $P_0{}^d (P_0{}^c)^{-1} = P$ eine Substitution mit *ganzzahligen* Koeffizienten wird. Setzen wir dann $\vartheta_0^{d-c} = \vartheta$, $|\vartheta|^{-\frac{l}{n-l}} = \eta$, so haben wir in der Reihe

$$S_1 = E, \quad S_2 = P, \quad S_3 = P^2, \ldots$$

eine periodische Substitutionenkette für die Zahl $\alpha$ mit den in 1. und 2. angegebenen Eigenschaften, wenn wir noch für die zugeordneten Größen $r_j$ die Festsetzung $r_j = \eta^{j-1}$ $(j = 1, 2, 3, \ldots)$ treffen.

## § 2. Einheiten von besonderem Charakter.

7. Wir wollen jetzt die Forderung der Existenz der besonderen Einheit $\vartheta$ im Körper von $\alpha$ weiter verfolgen. Die ganze Funktion $n^{\text{ten}}$ Grades in $t$:

$$F(t) = (t - \vartheta) \ldots (t - \vartheta^{(n-l)})$$

hat *rationale ganze* Koeffizienten; unter ihren Wurzeln haben $l$ den Betrag $\varepsilon < 1$ und $n - l$ den Betrag $\eta > 1$. Jeder im Bereiche der rationalen Zahlen irreduzible Faktor dieser Funktion $F(t)$ verschwindet für wenigstens eine der Zahlen $\vartheta, \ldots, \vartheta^{(n-l)}$ und muß daher, wegen der Irreduzibilität der Gleichung mit den Wurzeln $\alpha, \ldots, \alpha^{(n-l)}$, jedesmal für alle diese Zahlen $\vartheta, \ldots, \vartheta^{(n-l)}$ verschwinden; infolgedessen ist $F(t)$ notwendig eine Potenz einer einzigen irreduziblen Funktion. Wegen der Beträge der Wurzeln sind nun offenbar nur diese beiden Fälle möglich: *Entweder* ist $F(t)$ selbst irreduzibel und bestimmt alsdann $\vartheta$ bereits den Körper von $\alpha$, *oder* es ist $\alpha$ komplex, $l = 2$, aber $\vartheta = \vartheta^0$ reell und $F(t)$ das Quadrat einer irreduziblen Funktion; in letzterem Falle bestimmt $\vartheta$ einen reellen Unterkörper vom $\frac{n^{\text{ten}}}{2}$ Grade des komplexen Körpers von $\alpha$. Wir bemerken noch, daß jede Potenz $\vartheta^2, \vartheta^3, \ldots$ denselben Bedingungen genügt, wie sie hier für $\vartheta$ vorausgesetzt werden.

8. Nach einem Satze von Dirichlet gibt es in dem Körper der Zahl $\alpha$, wenn nur $n > l$ ist, gewiß eine solche Einheit, deren Betrag $< 1$ ist. Daraus ersehen wir bereits, daß im Körper von $\alpha$ eine Einheit $\vartheta$ der hier verlangten Art sich gewiß in folgenden Fällen vorfindet:

a) *wenn $\alpha$ reell und $n = 2$ ist,* b) *wenn $\alpha$ reell ist, $n = 3$ und der Körper von $\alpha$ zwei komplexe konjugierte Körper besitzt,*

c) *wenn $\alpha$ komplex und $n = 3$ ist,* d) *wenn $\alpha$ komplex ist, $n = 4$ und der Körper von $\alpha$ lauter komplexe konjugierte Körper besitzt.*

Denn in diesen Fällen besteht die Reihe $\vartheta', \ldots, \vartheta^{(n-l)}$ entweder in einer einzigen reellen Zahl oder zwei konjugiert imaginären, im speziellen auch zwei gleichen reellen Zahlen. Weiter haben wir im Körper von $\alpha$ eine Einheit $\vartheta$ der verlangten Art jedenfalls auch in folgenden Fällen:

e) *wenn $\alpha$ komplex ist, $n = 4$ und der Körper von $\alpha$ einen reellen Unterkörper zweiten Grades hat,* f) *wenn $\alpha$ komplex ist, $n = 6$ und der Körper von $\alpha$ einen reellen Unterkörper dritten Grades besitzt, dessen zwei konjugierte Körper komplex sind.*

Denn in diesen Fällen können wir für $\vartheta$ eine reelle Einheit von einem Betrage $< 1$ in dem betreffenden Unterkörper von $\alpha$ wählen, alsdann ist $\vartheta^0 = \vartheta$ und die Reihe $\vartheta', \ldots, \vartheta^{(n-l)}$ besteht aus zwei gleichen reellen bzw. zwei gleichen Paaren konjugiert imaginärer Zahlen. Wir können jetzt den Satz beweisen:

*Die hier aufgezählten sechs Fälle sind die einzigen, in denen der Körper von $\alpha$ eine Einheit $\vartheta$ der fraglichen Art aufweist, also die einzigen Fälle, in denen die Zahl $\alpha$ periodische Substitutionenketten besitzt.*

9. Wir diskutieren zuerst den Fall *einer reellen Zahl* $\alpha$; hier ist $l = 1$, $\vartheta = \pm\varepsilon$, $\varepsilon\eta^{n-1} = 1$. Wir haben folgende Möglichkeiten ins Auge zu fassen:

a) Unter den Zahlen $\alpha', \ldots, \alpha^{(n-1)}$ finden sich *wenigstens zwei reelle*, etwa $\alpha^{(h)}$ und $\alpha^{(k)}$. Dann sind auch $\vartheta^{(h)}$ und $\vartheta^{(k)}$ reell, und da diese Zahlen nicht einander gleich sein können, aber denselben Betrag haben, müßte $\vartheta^{(h)} = -\vartheta^{(k)}$ und daher $(\vartheta^{(h)})^2 = (\vartheta^{(k)})^2$ sein. Aber die Zahl $\vartheta^2 = \varepsilon^2$ ist von ihren $n-1$ konjugierten Zahlen verschieden, sie genügt daher ebenfalls einer irreduziblen Gleichung $n^{\text{ten}}$ Grades, und müßten daher ihre $n-1$ konjugierten Zahlen auch untereinander durchweg verschieden sein. Danach ist dieser Fall unmöglich.

b) Unter den Zahlen $\alpha', \ldots, \alpha^{(n-1)}$ kommt *nur eine reelle* Zahl, $\alpha^{(g)}$, vor. Für $n = 2$ liegt dann der oben unter 8. a) aufgeführte Fall vor. Ist $n > 2$, so haben wir unter jenen Zahlen weiter wenigstens ein Paar konjugiert imaginärer Zahlen, etwa $\alpha^{(h)}$ und $\alpha^{(k)}$. Die Zahl $\vartheta^2 = \varepsilon^2$ genügt einer irreduziblen Gleichung $n^{\text{ten}}$ Grades; unter den Wurzeln dieser Gleichung ist weiter eine $= (\vartheta^{(g)})^2 = \eta^2$ und sind die $n-2$ übrigen dem Betrage nach $= \eta^2$. Nun können wir eine Gleichung mit rationalen Koeffizienten vom Grade $\frac{n(n-1)}{2}$ angeben, welche die Produkte aus je zwei verschiedenen der $n$ Größen $\vartheta, \vartheta', \ldots, \vartheta^{(n-1)}$ zu Wurzeln hat. Diese Gleichung besitzt $n-1$ Wurzeln vom Betrage $\varepsilon\eta$, die übrigen Wurzeln vom Betrage $\eta^2$, darunter insbesondere die Wurzel $\vartheta^{(h)}\vartheta^{(k)} = \eta^2$, sie müßte also auch alle anderen Wurzeln jener irreduziblen Gleichung $n^{\text{ten}}$ Grades für $\eta^2$ besitzen; sie hätte aber, da $\varepsilon < 1 < \eta$ ist, gewiß nicht die Wurzel $\varepsilon^2$. Danach ist dieser Fall für $n > 2$ unmöglich.

c) Die Zahlen $\alpha', \ldots, \alpha^{(n-1)}$ sind *sämtlich komplex*, sie zerfallen dann in $\frac{n-1}{2}$ Paare konjugiert imaginärer Größen. Für $n = 3$ liegt der oben unter 8. b) aufgeführte Fall vor. Jetzt sei $n > 3$. Wir bilden die Gleichung $\frac{n(n-1)^{\text{ten}}}{2}$ Grades mit rationalen Koeffizienten, welche als Wurzeln die Produkte aus je zwei der $n$ Größen $\vartheta^{-n+1}, \vartheta'^{-n+1}, \ldots, (\vartheta^{(n-1)})^{-n+1}$ hat. Diese Gleichung besitzt $n-1$ Wurzeln vom Betrage $(\varepsilon\eta)^{-n+1} = \eta^{(n-1)(n-2)}$ und im übrigen lauter Wurzeln vom Betrage $\eta^{-2(n-1)} = \varepsilon^2$, darunter $\frac{n-1}{2}$ Wurzeln $= \varepsilon^2 = \vartheta^2$; sie müßte daher auch alle die Größen $\vartheta'^2, \ldots, (\vartheta^{(n-1)})^2$ vom Betrage $\eta^2$ zu Wurzeln besitzen, es müßte also $\eta^2 = \eta^{(n-1)(n-2)}$, d. h. $n = 3$ sein. Für $n > 3$ ist danach dieser Fall unmöglich.

10. Wir behandeln jetzt weiter den *Fall einer komplexen Zahl* $\alpha$; hier ist $l = 2$, $\varepsilon^2 \eta^{n-2} = 1$.

*Machen wir zunächst die Annahme, daß* $\vartheta = \vartheta^0$, *also reell ist.* Die Größe $\vartheta$ ist dann Wurzel einer irreduziblen Gleichung $\frac{n}{2}^{\text{ten}}$ Grades. Der Körper von $\alpha$ besitzt also einen reellen Unterkörper vom Grade $\frac{n}{2}$, und in diesem soll $\vartheta$ eine Einheit von einem Betrage $< 1$ sein, für welche die konjugierten Zahlen in den konjugierten Körpern sämtlich untereinander gleiche Beträge haben. Wir können daher die in 9. gemachten Ausführungen verwenden, und es muß entweder $\frac{n}{2} = 2$ sein oder aber $\frac{n}{2} = 3$ und dabei der Körper von $\vartheta$ zwei komplexe konjugierte Körper aufweisen. Wir kommen damit auf die oben unter 8. e) und 8. f) aufgezählten Umstände für den Körper von $\alpha$.

*Wir nehmen jetzt andererseits an, daß* $\vartheta \neq \vartheta^0$ *sei.* Alsdann genügt $\vartheta$ einer irreduziblen Gleichung $n^{\text{ten}}$ Grades und bestimmt bereits völlig den Körper von $\alpha$. Wir unterscheiden wieder drei Fälle:

a) Unter den Zahlen $\alpha', \ldots, \alpha^{(n-2)}$ sind *wenigstens zwei reelle* vorhanden, $\alpha^{(h)}$ und $\alpha^{(k)}$. Dann sind auch $\vartheta^{(h)}$ und $\vartheta^{(k)}$ reell, und da sie gleichen Betrag haben, aber verschieden sind, kann nur $\vartheta^{(h)} = -\vartheta^{(k)}$ sein. Alsdann ist $(\vartheta^{(h)})^2 = (\vartheta^{(k)})^2$. Die rationale Gleichung $n^{\text{ten}}$ Grades mit den Wurzeln $\vartheta^2, \ldots, (\vartheta^{(n-2)})^2$ hat daher lauter Doppelwurzeln und muß infolgedessen $\vartheta^2 = (\vartheta^0)^2$ sein. Die Potenz $\vartheta^2$ bestimmt somit einen reellen Unterkörper $\frac{n}{2}^{\text{ten}}$ Grades für den Körper von $\alpha$, und da überdies $(\vartheta^{(h)})^2$ reell ist, kann nach dem vorhin Bemerkten hier nur der unter 8. e) aufgeführte Fall mit $n = 4$ vorliegen.

b) Unter den Zahlen $\alpha', \ldots, \alpha^{(n-2)}$ ist *nur eine reelle* Zahl, $\alpha^{(g)}$, vorhanden. Für $n = 3$ liegt der unter 8. c) genannte Fall vor. Ist $n > 3$, so haben wir unter jenen Zahlen noch $\frac{n-3}{2}$ Paare konjugiert imaginärer Größen. Es ist $\vartheta^{(g)} = \pm \eta$; da $-\vartheta^{(g)}$ hier nicht derselben Gleichung mit rationalen Koeffizienten wie $\vartheta^{(g)}$ genügt, muß notwendig auch $\vartheta^0 \neq -\vartheta$, also $(\vartheta^0)^2 \neq \vartheta^2$ und daher $\vartheta^2 \neq \pm \varepsilon^2$, $(\vartheta^0)^2 \neq \pm \varepsilon^2$ sein. Danach ist die rationale Gleichung $n^{\text{ten}}$ Grades mit den Wurzeln $\vartheta^2, \ldots, (\vartheta^{(n-2)})^2$ irreduzibel und unter den Wurzeln dieser Gleichung sind zwei nicht reelle Wurzeln vom Betrage $\varepsilon^2$ und ist ferner eine Wurzel $= \eta^2$ vorhanden. Bilden wir nun die rationale Gleichung $\frac{n(n-1)}{2}^{\text{ten}}$ Grades, welche die Produkte aus je zwei der $n$ Größen $\vartheta, \ldots, \vartheta^{(n-2)}$ zu Wurzeln hat, so besitzt diese Gleichung eine Wurzel $= \varepsilon^2$, sodann $2(n-2)$ Wurzeln vom Betrage $\varepsilon\eta$, die übrigen Wurzeln vom Betrage $\eta^2$ und darunter $\frac{n-3}{2}$ Wurzeln $= \eta^2$. Wegen der

letzteren Wurzeln müßte sie aber alle Wurzeln jener irreduziblen Gleichung für $\eta^2$ besitzen. Danach ist dieser Fall für $n > 3$ unmöglich.

c) Die Zahlen $\alpha', \ldots, \alpha^{(n-2)}$ sind *sämtlich komplex*, zerfallen also in $\frac{n-2}{2}$ Paare konjugiert imaginärer Größen; $n$ ist hier gerade. Für $n = 4$ liegt der oben unter 8. d) aufgeführte Fall vor. Jetzt sei $n \geqq 6$. Bilden wir die Gleichung $\frac{n(n-1)^{\text{ten}}}{2}$ Grades, welche die Produkte aus je zwei der $n$ Größen $\vartheta, \ldots, \vartheta^{(n-2)}$ zu Wurzeln hat, so besitzt diese Gleichung mit rationalen Koeffizienten eine Wurzel $= \varepsilon^2$, sodann $2(n-2)$ Wurzeln vom Betrage $\varepsilon\eta$, die übrigen Wurzeln vom Betrage $\eta^2$, darunter $\frac{n-2}{2}$ gleich $\eta^2$. Bilden wir andererseits die Gleichung $\frac{n(n-1)^{\text{ten}}}{2}$ Grades, deren Wurzeln die $\frac{n-2^{\text{ten}}}{2}$ Potenzen der Wurzeln dieser letzten Gleichung sind, so hat diese neue Gleichung mit rationalen Koeffizienten eine Wurzel $= \varepsilon^{-(n-2)} = \eta^{\frac{(n-2)^2}{2}}$, sodann $2(n-2)$ Wurzeln vom Betrage $(\varepsilon\eta)^{\frac{-(n-2)}{2}} = \eta^{\frac{(n-2)(n-4)}{4}}$, die übrigen Wurzeln vom Betrage $\eta^{-(n-2)} = \varepsilon^2$, darunter $\frac{n-2}{2}$ gleich $\varepsilon^2$. Diese zweite Gleichung besitzt nun keine Wurzel vom Betrage $\varepsilon\eta$, und wenn wir uns zuerst $n > 6$ denken, auch keine Wurzel vom Betrage $\eta^2$. Im Falle $n > 6$ könnte daher der gemeinsame Faktor der beiden eben gebildeten Gleichungen nur die eine Wurzel $\varepsilon^2$ besitzen, es müßte dann also $\varepsilon^2 = \vartheta\vartheta^0$ rational sein; nun wäre aber $\varepsilon^2$ ebenso wie $\vartheta$ eine Einheit, eine algebraische Zahl von der Norm $\pm 1$, es müßte daher notwendig $\varepsilon^2 = 1$ sein, was gegen die Voraussetzung $\varepsilon < 1$ wäre. Also ist die Annahme $n > 6$ hier unzulässig.

*Im Falle* $n = 6$ endlich hat die zuerst erwähnte Gleichung eine Wurzel $= \varepsilon^2$, 8 Wurzeln vom Betrage $\varepsilon\eta$, 6 vom Betrage $\eta^2$, die an zweiter Stelle gebildete Gleichung eine Wurzel $= \eta^8$, 8 Wurzeln vom Betrage $\eta^2$, 6 vom Betrage $\varepsilon^2$, darunter 2 gleich $\varepsilon^2$. Die im Bereiche der rationalen Zahlen irreduzible Gleichung mit $\varepsilon^2$ als Wurzel kann danach, da sie in diesen beiden Gleichungen als Faktor eingeht, außer $\varepsilon^2$ nur Wurzeln vom Betrage $\eta^2$ enthalten, und sie wird wegen $\varepsilon^2\eta^4 = 1$ und da $\varepsilon^2 = \vartheta\vartheta^0$ jedenfalls eine Einheit vorstellt, im ganzen zwei solcher Wurzeln enthalten; diese zwei Wurzeln können dann einander weder gleich noch entgegengesetzt, also auch nicht reell $= \pm \eta^2$ sein, sie müssen komplex und zueinander konjugiert imaginär sein. Nehmen wir an, daß hier $\vartheta'$ mit $\vartheta''$ und $\vartheta'''$ mit $\vartheta^{(4)}$ konjugiert imaginär sind, so können wir annehmen, indem wir noch die Bezeichnungen von $\vartheta'''$ und $\vartheta^{(4)}$ vertauschen dürfen, die Wurzeln jener Gleichung für $\varepsilon^2$ seien $\vartheta\vartheta^0$, $\vartheta'\vartheta'''$, $\vartheta''\vartheta^{(4)}$.

Die Größe $\varepsilon^2$ bestimmt danach einen kubischen Körper, dessen zwei konjugierte Körper komplex sind. Denken wir uns jetzt die im Bereiche der rationalen Zahlen irreduzible ganze Funktion $F(t)$, welche für $t = \vartheta$ verschwindet, im Körper von $\varepsilon^2$ in irreduzible Faktoren zerlegt, und es sei $G(t)$ derjenige Faktor darunter, welcher die Wurzel $t = \vartheta$ erhält. Da $\varepsilon^2$ reell ist, bekommt $G(t)$ ebenfalls lauter reelle Koeffizienten und wird daher mit der Wurzel $\vartheta$ auch die konjugiert imaginäre Größe $\vartheta^0 = \frac{\varepsilon^2}{\vartheta}$ als Wurzel besitzen, so daß auch $G\left(\frac{\varepsilon^2}{\vartheta}\right) = 0$ ist. Alsdann muß die Gleichung $G\left(\frac{\varepsilon^2}{t}\right) = 0$ überhaupt für jede Wurzel der im Körper von $\varepsilon^2$ irreduziblen Gleichung $G(t) = 0$ bestehen. Die Größen $\frac{\varepsilon^2}{\vartheta'}$, $\frac{\varepsilon^2}{\vartheta''}$, $\frac{\varepsilon^2}{\vartheta'''}$, $\frac{\varepsilon^2}{\vartheta^{(4)}}$ aber besitzen sämtlich den Betrag $\frac{\varepsilon^2}{\eta} \neq \eta$ und $\neq \varepsilon$ und sind daher nicht Wurzeln von $F(t) = 0$, also auch nicht Wurzeln von $G(t) = 0$, daher kann $G(t)$ auch keine der Größen $\vartheta', \vartheta'', \vartheta''', \vartheta^{(4)}$ als Wurzel haben; somit können wir einfach $G(t) = (t - \vartheta)(t - \vartheta^0)$ schreiben. Danach ist $\vartheta$ Wurzel einer quadratischen Gleichung im Körper von $\varepsilon^2$ und besitzt der Körper sechsten Grades von $\vartheta$, d. i. der Körper von $\alpha$, in dem Körper von $\varepsilon^2$ einen reellen Unterkörper dritten Grades, dessen zwei konjugierte Körper komplex sind. Wir kommen also auf den oben unter 8. f) aufgezählten Fall.

Wir können die Bildungsweise des Körpers von $\alpha$ unter den hier angenommenen Umständen noch genauer festlegen. Die zu $G(t)$ konjugierten Funktionen in den Körpern von $\vartheta'\vartheta'''$ und $\vartheta''\vartheta^{(4)}$ werden $(t - \vartheta')(t - \vartheta''')$ und $(t - \vartheta'')(t - \vartheta^{(4)})$ sein. Da $|\vartheta'| = |\vartheta'''|$ ist, wird $\frac{\vartheta' - \vartheta'''}{\vartheta' + \vartheta'''}$ rein imaginär, also $\left(\frac{\vartheta' - \vartheta'''}{\vartheta' + \vartheta'''}\right)^2$ eine negative reelle Größe sein. Diese Größe liegt wie $\vartheta' + \vartheta'''$ und $\vartheta'\vartheta'''$ in dem Körper von $\vartheta'\vartheta'''$; da sie nun reell ist, wird sie identisch mit ihrer konjugierten Größe in dem konjugiert imaginären Körper von $\vartheta''\vartheta^{(4)}$ und muß daher rational sein und daher gleichzeitig auch gleich der konjugierten Größe $\left(\frac{\vartheta - \vartheta^0}{\vartheta + \vartheta^0}\right)^2$ im Körper von $\vartheta\vartheta^0$. Danach ist $\frac{\vartheta}{\vartheta^0}$ entweder $= \frac{\vartheta'}{\vartheta'''}$ oder $= \frac{\vartheta'''}{\vartheta'}$. Da wir die Bezeichnung der Paare $\vartheta', \vartheta''$ und $\vartheta''', \vartheta^{(4)}$ vertauschen dürfen, können wir annehmen, es sei $\frac{\vartheta}{\vartheta^0} = \frac{\vartheta'}{\vartheta'''}$; letzterer Wert ist weiter $= \frac{\vartheta^{(4)}}{\vartheta''}$. Setzen wir $\frac{\vartheta}{\vartheta^0} = \delta$, so ist $\delta = \frac{\vartheta^2}{\vartheta\vartheta^0}$ und sind die konjugierten Zahlen dazu $\frac{\vartheta'^2}{\vartheta'\vartheta'''} = \delta$, $\frac{(\vartheta^{(4)})^2}{\vartheta''\vartheta^{(4)}} = \delta$ und die drei hierzu reziproken Werte $= \frac{1}{\delta}$. Dabei hat $\delta$ den Betrag 1 und ist wie $\vartheta$ eine Einheit; danach ist entweder $\delta = -1$, oder es ist $\delta$ eine solche Einheits-

wurzel, die einen Körper zweiten Grades bestimmt. Im ersteren Falle ist $\vartheta^0 = -\vartheta$, $\vartheta = \pm i\varepsilon$, $\vartheta^2 = (\vartheta^0)^2$. Im zweiten Falle kämen für $\delta$ zunächst die dritten, vierten, sechsten Einheitswurzeln in Betracht. Nun folgt $\vartheta = \delta^{\frac{1}{2}}\varepsilon$, $\vartheta^0 = \frac{1}{\delta^{\frac{1}{2}}}\varepsilon$ und weiter unter Verwendung von $\varepsilon\eta^2 = \varepsilon\vartheta'\vartheta'' = 1$ die Beziehung

$$Nm(\vartheta + \vartheta^0) = (\vartheta + \vartheta^0)(\vartheta' + \vartheta''')(\vartheta'' + \vartheta^{(4)}) = \frac{\delta + 1}{\delta^{\frac{1}{2}}}\left(1 + \frac{1}{\delta}\right)(1 + \delta).$$

Danach muß noch $\frac{\delta + 1}{\delta^{\frac{1}{2}}}$ rational sein, und solches trifft nur zu, wenn $\delta$ eine *dritte* Einheitswurzel vorstellt, $\delta^3 = 1$ ist. Dann folgt endlich $\vartheta = \pm\frac{\varepsilon}{\delta}$, $\vartheta^0 = \pm\delta\varepsilon$, $\vartheta^3 = (\vartheta^0)^3$ und $\vartheta + \vartheta^0 = \mp\varepsilon$, so daß der Körper von $\varepsilon^2$ auch die Größe $\varepsilon$ selbst enthält, und der Körper von $\alpha$ aus dem Körper dritten Grades von $\varepsilon$ und dem Körper zweiten Grades von $\delta = \frac{-1 \pm \sqrt{-3}}{2}$ zusammengesetzt ist.

## § 3. Die komplexen kubischen Irrationalzahlen.

11. *In den Fällen, wo für die algebraische Zahl $\alpha$ periodische Substitutionenketten möglich sind, entsteht nun die Aufgabe, eine solche Kette für $\alpha$ bereits herzustellen, wenn allein $\alpha$ seinem Werte nach gegeben ist, die konjugierten algebraischen Zahlen von $\alpha$ indes noch unbekannt sind.* Bei den reellen algebraischen Zahlen zweiten Grades wird gerade durch die periodische Entwicklung in einen gewöhnlichen Kettenbruch das hier Verlangte geleistet. Wir wollen nun zeigen, daß auch noch in einem anderen Falle, nämlich, wenn es sich um *eine komplexe Größe $\alpha$* handelt, *welche Wurzel einer irreduziblen Gleichung dritten Grades sein soll,* der hier gestellten Forderung entsprochen werden kann, und *wir kommen dadurch zu einem völlig analogen Kriterium für die komplexen algebraischen Zahlen dritten Grades, wie es durch* Lagrange *für die reellen algebraischen Zahlen zweiten Grades in der Periodizität der Kettenbruchentwicklung nachgewiesen worden ist.*

Es sei jetzt $\alpha$ eine komplexe Größe, welche einer im Bereiche der rationalen Zahlen irreduziblen Gleichung dritten Grades genügt, so ist mit $\alpha$ ohne weiteres auch die konjugiert imaginäre Größe $\alpha^0$ gegeben; dagegen haben wir uns der Kenntnis der dritten reellen Wurzel $\alpha'$ jener Gleichung vorläufig zu entschlagen. Wir setzen

$$\xi = x_1 + \alpha x_2 + \alpha^2 x_3.$$

Zu jeder ganzen rationalen Zahl $r \geqq 1$ bestimmen wir eine Substitution $S$:

$$x_h = s_h^{(1)} y_1 + s_h^{(2)} y_2 + s_h^{(3)} y_3 \qquad (h = 1, 2, 3),$$

Druck von B. G. Teubner in Leipzig.