IX.

Über die Elemente der Wahrscheinlichkeitsrechnung.

[Vierteljahrsschrift der naturforschenden Gesellschaft in Zürich, 1860, S. 66—75.]

In den meisten Lehrbüchern findet man die Sätze über die sogenannten zusammengesetzten Wahrscheinlichkeiten in folgender Weise aufgestellt: „Ist a die Wahrscheinlichkeit eines Ereignisses A, b die eines zweiten B, so ist $a + b$ die Wahrscheinlichkeit, daß A oder B, und ab die Wahrscheinlichkeit, daß A und B eintritt". Man überzeugt sich aber leicht, daß von diesen beiden Sätzen immer höchstens einer richtig sein kann, und daß auch in unzähligen Fällen beide falsch sind. Dies findet seinen Grund darin, daß die Wahrscheinlichkeit eines zusammengesetzten Ereignisses durchaus nicht allein von den Wahrscheinlichkeiten der einzelnen Ereignisse, sondern außerdem noch von der gegenseitigen Beziehung derselben zueinander abhängt. Die so häufig vorkommende Vernachlässigung dieses Umstandes mag die nachfolgende Darstellung eines so elementaren Gegenstandes entschuldigen, auf welche in einer späteren Mitteilung Bezug genommen wird.

1.

Bei der ursprünglichen Begriffsbestimmung der mathematischen Wahrscheinlichkeit eines Ereignisses A muß man immer von der Voraussetzung ausgehen, daß sich gewisse Elementarfälle aufzählen lassen, welche die doppelte Bedingung erfüllen, erstens, daß einer, aber auch nur einer von ihnen eintreten muß; zweitens, daß wir keinen Grund haben, das Eintreten eines dieser Fälle eher zu erwarten als das eines anderen. Sind diese beiden Bedingungen erfüllt, und ist p die Anzahl derjenigen dieser Fälle, in welchen A eintritt, q die Anzahl der übrigen, so ist der Bruch $\frac{p}{p+q}$ das Maß für die Wahrscheinlichkeit, mit welcher wir das Eintreten des Ereignisses A erwarten. Ist dagegen eine der beiden Bedingungen nicht zu erfüllen, so bleibt eine genaue Schätzung der Wahrscheinlichkeit von A unmöglich.

Handelt es sich nun um Eintreten oder Nichteintreten von zwei Ereignissen A und B (deren Identität nicht ausgeschlossen ist), so

denken wir uns die sämtlichen Elementarfälle in vier Gruppen zerlegt; es sei nämlich die Anzahl aller Elementarfälle, in welchen

1. A und B eintritt, gleich m,
2. A allein eintritt, gleich p,
3. B allein eintritt, gleich q,
4. weder A noch B eintritt, gleich n.

Jeder Elementarfall gehört jedenfalls einer, aber auch nur einer dieser vier Gruppen an, so daß $m + p + q + n$ die Anzahl aller Elementarfälle ist. Zufolge der vorhergehenden Definition ist dann

$$a = \frac{m+p}{m+p+q+n} \text{ die Wahrscheinlichkeit von } A;$$

$$b = \frac{m+q}{m+p+q+n} \text{ die Wahrscheinlichkeit von } B.$$

Man sieht nun, daß die Wahrscheinlichkeit eines von dem Eintreten oder Nichteintreten von A und B abhängigen Ereignisses im allgemeinen von den drei Verhältnissen zwischen den vier Zahlen m, p, q, n abhängt, also durch alleinige Angabe der zwei Zahlen a, b noch nicht vollständig bestimmt ist. Es muß daher noch eine dritte Zahl, ein Element gegeben sein, welches dazu dient, die Art des Zusammenhanges zwischen den beiden Ereignissen A und B zu charakterisieren. Im allgemeinen wird nämlich das Eintreten eines dieser beiden Ereignisse die Wahrscheinlichkeit des andern abändern. Tritt z. B. das Ereignis B ein, so ist die Wahrscheinlichkeit von A — da dann die Fälle der zweiten und vierten Gruppe ausgeschlossen sind — jetzt

$$\alpha = \frac{m}{m+q};$$

und ähnlich ist die, durch die Gewißheit von A modifizierte Wahrscheinlichkeit von B

$$\beta = \frac{m}{m+p}.$$

Ist nun außer a und b noch eine der beiden modifizierten Wahrscheinlichkeiten α, β gegeben, so läßt sich die Wahrscheinlichkeit eines jeden aus A und B zusammengesetzten Ereignisses bestimmen. Zunächst muß zwischen den vier Zahlen a, b, α, β, welche nur von den Verhältnissen zwischen m, p, q, n abhängen, eine Relation bestehen; eliminiert man m, p, q, n, so erhält man

$$a\beta = b\alpha, \tag{1}$$

und zwar ist der gemeinschaftliche Wert dieser beiden Produkte gleich

$$\frac{m}{m+p+q+n} = \omega;$$

also gleich der Wahrscheinlichkeit, daß A und B eintreten. Ferner ist die Wahrscheinlichkeit, daß A allein eintritt, gleich

$$(2) \qquad \frac{p}{m+p+q+n} = a - b\alpha = a(1-\beta) = a - \omega;$$

ebenso ist

$$(3) \qquad \frac{q}{m+p+q+n} = b(1-\alpha) = b - a\beta = b - \omega$$

die Wahrscheinlichkeit, daß B allein eintritt; und

$$(4) \qquad \frac{n}{m+p+q+n} = 1 - a - b + b\alpha = 1 - a - b + a\beta = 1 - a - b + \omega$$

ist die Wahrscheinlichkeit, daß weder A noch B eintritt.

Ferner ist:

$$(5) \qquad \frac{m+n}{m+p+q+n} = 1 - a - b + 2\omega$$

die Wahrscheinlichkeit, daß keines der beiden Ereignisse A, B allein eintritt;

$$(6) \qquad \frac{m+p+q}{m+p+q+n} = a + b - b\alpha = a + b - a\beta = a + b - \omega$$

die, daß mindestens eins der beiden Ereignisse eintritt;

$$(7) \qquad \frac{p+q+n}{m+p+q+n} = 1 - b\alpha = 1 - a\beta = 1 - \omega$$

die, daß höchstens eins der beiden Ereignisse eintritt;

$$(8) \qquad \frac{m+q+n}{m+p+q+n} = 1 - a + b\alpha = 1 - a(1-\beta) = 1 - a + \omega$$

die, daß A nicht allein eintritt; und endlich ist

$$(9) \qquad \frac{m+p+n}{m+p+q+n} = 1 - b(1-\alpha) = 1 - b + a\beta = 1 - b + \omega$$

die Wahrscheinlichkeit, daß B nicht allein eintritt.

Um die Bedeutung von α, β noch anschaulicher zu machen, mögen hier noch folgende Bemerkungen Platz finden. Man sagt, zwei Ereignisse A und B schließen einander aus, wenn das Eintreten des einen das des andern unmöglich macht; der arithmetische Ausdruck dafür ist

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

(vorausgesetzt, daß a und b nicht selbst $= 0$ sind); dann ist die Wahrscheinlichkeit, daß mindestens eins der beiden Ereignisse eintritt, d. h. daß wirklich eins eintritt,

$$= a + b.$$

Man sagt ferner, zwei Ereignisse sind voneinander unabhängig, wenn das Eintreten des einen durchaus keinen Einfluß auf die Wahrscheinlichkeit des andern ausübt, d. h. wenn

$$\alpha = a, \quad \beta = b, \quad \omega = ab$$

ist; in diesem Falle ist die Wahrscheinlichkeit, daß mindestens eins der beiden Ereignisse eintritt,

$$= a + b - ab.$$

Und umgekehrt sieht man, daß der erste der beiden zu Anfang erwähnten Sätze nur dann richtig ist, wenn die beiden Ereignisse einander ausschließen, und der zweite nur dann, wenn sie voneinander unabhängig sind; und nur dann sind beide Sätze zu gleicher Zeit richtig, wenn mindestens eins der beiden Ereignisse unmöglich ist.

Ist ferner $\alpha = 1$, so zieht das Eintreten von B das von A als notwendige Folge nach sich, und dann ist $b = a\beta \gtrless a$. Ist außerdem $\beta = 1$, so ist $a = b$, und die beiden Ereignisse sind gewissermaßen identisch; aber es ist wohl zu bemerken, daß nicht umgekehrt aus $a = b$ diese Identität der Ereignisse folgt.

2.

Es hat nun keine Schwierigkeit, diese Sätze auf Kombinationen von mehr als zwei Ereignissen auszudehnen; sind z. B. $W_1, W_2, \dots W_n$ Ereignisse, von denen je zwei einander ausschließen, und sind w_1, $w_2, \dots w_n$ ihre Wahrscheinlichkeiten, so ist die Summe

$$w_1 + w_2 + \cdots + w_n$$

die Wahrscheinlichkeit, daß eins dieser Ereignisse eintritt, wovon man sich leicht durch den Schluß von n auf $(n+1)$ überzeugt.

Man kann sich dieses Satzes häufig bedienen, um die Wahrscheinlichkeit a eines Ereignisses A zu bestimmen, ohne auf die Aufzählung der einzelnen gleich möglichen Elementarfälle zurück-

zugehen. Gesetzt, man habe verschiedene einander ausschließende Eventualitäten $B_1, B_2, \dots B_n$, in welchen das Ereignis A eintreten kann, in so erschöpfender Weise aufgestellt, daß das Eintreten von A unter keiner anderen Eventualität möglich ist. Es sei b die Wahrscheinlichkeit, daß die Eventualität B_r eintritt, und α_r sei die Wahrscheinlichkeit, daß, wenn B_r eintritt, auch A eintritt. Dann ist

$$a = b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n;$$

denn irgend ein Glied $b_r\alpha_r = w_r$ ist die Wahrscheinlichkeit des Ereignisses W_r, daß gleichzeitig B_r und A eintritt, und das Ereignis A ist identisch mit demjenigen, daß von diesen n einander ausschließenden Ereignissen $W_1 \dots W_n$ irgend eins eintritt.

Umgekehrt kann man nun auch, wenn das Ereignis A wirklich eingetreten ist, die Wahrscheinlichkeit a posteriori bestimmen, daß dies infolge der Eventualität B_r geschehen ist; denn diese Wahrscheinlichkeit β_r ist nichts anderes, als die durch die Gewißheit von A modifizierte Wahrscheinlichkeit von B_r, so daß

$$a\beta_r = b_r\alpha_r, \quad \text{also} \quad \beta_r = \frac{b_r\alpha_r}{b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n},$$

und die hieraus sich ergebende Gleichung

$$\beta_1 + \beta_2 + \cdots + \beta_n = 1$$

ist nur ein Ausdruck für unsere ursprüngliche Annahme, daß das Eintreten von A nur unter einer der Eventualitäten $B_1, B_2, \dots B_n$ und auch unter keiner anderen möglich ist. Von diesem Satze über die Wahrscheinlichkeit a posteriori wird in einer folgenden Mitteilung Gebrauch gemacht werden.

	1	2	3	4	x
1	(10)	(8)	(1)	(1)	
2	(8)	(9)	(7)	(6)	
3	(1)	(7)	(1)	(1)	
4	(1)	(6)	(1)	(2)	
y					

Ein Beispiel, welches zugleich zu einer weiteren Bemerkung Veranlassung geben wird, mag das Bisherige erläutern. Es seien

16 Urnen in quadratischer Anordnung aufgestellt, so daß sie vier Vertikalreihen ($x = 1, 2, 3, 4$) und vier Horizontalreihen ($y = 1, 2, 3, 4$) von je vier Urnen bilden; die einzelnen Urnen können dann durch Angabe der Vertikalreihe x und der Horizontalreihe y, in denen sie sich finden, voneinander unterschieden werden. In jeder Urne seien zehn Kugeln enthalten, von denen so viele weiß sind, wie die in Klammern gesetzte Zahl angibt (also enthält z. B. die Urne ($x = 1$, $y = 1$) nur weiße Kugeln, die Urne ($x = 4$, $y = 3$) enthält eine weiße und neun schwarze Kugeln). [*)] Wir nehmen an, daß der Zug ebensowohl aus der einen wie aus jeder anderen Urne geschehen kann; dann ist die Wahrscheinlichkeit, daß eine weiße Kugel gezogen wird

$$a = \Sigma b_{x,y}\alpha_{x,y} = \frac{1}{16}\Sigma\alpha_{x,y} = \frac{7}{16},$$

wo $b_{x,y}$ die Wahrscheinlichkeit $\frac{1}{16}$ bedeutet, daß der Zug aus der Urne (x, y) geschehen wird, und $\alpha_{x,y}$ die Wahrscheinlichkeit, daß der Zug, wenn er aus der Urne (x, y) geschieht, eine weiße Kugel geben wird.

Nun sei umgekehrt eine weiße Kugel gezogen, ohne daß man die Urne kennt, aus welcher sie gezogen ist. Dann ist die Wahrscheinlichkeit a posteriori, daß dieser Zug aus der Urne (x, y) geschehen ist,

$$\beta_{x,y} = \frac{b_{x,y}\alpha_{x,y}}{\Sigma b_{x,y}\alpha_{x,y}} = \frac{\alpha_{x,y}}{\Sigma\alpha_{x,y}} = \frac{\alpha_{x,y}}{7}.$$

Am wahrscheinlichsten ist es daher, daß der Zug aus der Urne (1, 1) geschehen ist; d. h. also, das wahrscheinlichste System der beiden Unbekannten x, y ist das System $x = 1$, $y = 1$.

Man findet nun häufig die ganz unrichtige Ansicht, daß der Wert einer unbekannten Größe, der ihr in dem wahrscheinlichsten System von mehreren Unbekannten zukommt, zugleich auch ihr wahrscheinlichster Wert sein müsse. Daß dem nicht so ist, lehrt recht augenfällig das vorliegende Beispiel; denn wir finden für die Wahrscheinlichkeit, daß der Zug aus der ersten, zweiten, dritten, vierten Vertikalreihe geschehen ist, d. h. daß x den Wert 1, 2, 3, 4 hat, resp. den Wert

$$\frac{2}{7}, \frac{3}{7}, \frac{1}{7}, \frac{1}{7};$$

[*) In der Originalarbeit ist die Tabelle über die Anzahlen weißer Kugeln nicht frei von Druckfehlern.]

und dieselben Zahlen drücken auch (infolge der Symmetrie des obigen Schemas) die Wahrscheinlichkeiten aus, daß die Unbekannte y den Wert 1, 2, 3 4 hat. Wir finden also, daß der wahrscheinlichste Wert von x gleich 2, der von y gleich 2 ist; und doch haben wir vorher gesehen, daß das wahrscheinlichste Wertsystem der beiden Unbekannten das System $x = 1$, $y = 1$ ist. Die Wichtigkeit dieser Bemerkung wird in einer späteren Mitteilung sich herausstellen.

Ganz ähnlich verhält es sich, wenn die Werte der unbekannten Größen ein Gebiet stetig erfüllen. Ist z. B.

$$\frac{1}{2\pi}(x^2 + 3y^2)e^{-(x^2+y^2)}dx\,dy$$

die Wahrscheinlichkeit, daß die Abszisse eines unbekannten Punktes in dem unendlich kleinen Intervall zwischen x und $x + dx$, und daß seine Ordinate zugleich zwischen y und $y + dy$ liegt, so findet man

$$\frac{1}{4\sqrt{\pi}}(2x^2 + 3)e^{-x^2}dx$$

als Wahrscheinlichkeit, daß seine Abszisse zwischen x und $x + dx$ liegt, und ebenso

$$\frac{1}{4\sqrt{\pi}}(6y^2 + 1)e^{-y^2}dy$$

als Wahrscheinlichkeit, daß seine Ordinate zwischen y und $y + dy$ liegt. Die erste Wahrscheinlichkeit wird ein Maximum für die beiden Systeme

$$x = 0, \quad y = \pm 1;$$

die zweite für den Wert

$$x = 0;$$

die dritte für die beiden Werte

$$y = \pm\sqrt{\frac{5}{6}}.$$

In diesem Falle stimmt das System der beiden wahrscheinlichsten Werte zwar sehr nahe, aber doch nicht vollständig mit dem wahrscheinlichsten Wertsystem überein.

X.

Über die Bestimmung der Präzision einer Beobachtungsmethode nach der Methode der kleinsten Quadrate.

[Vierteljahrsschrift der naturforschenden Gesellschaft in Zürich, 1860, S. 76—83.]

In seiner ersten Begründung der Methode der kleinsten Quadrate ging Gauß (Theoria motus corp. coel.) von der Voraussetzung aus, daß der wahrscheinlichste Wert einer beliebig oft auf dieselbe Weise direkt gemessenen Größe das arithmetische Mittel aus den durch diese Messungen erhaltenen Werten ist, und kam auf diese Weise zu dem Ausdruck

$$\frac{h}{\sqrt{\pi}}e^{-h^2t^2}dt$$

für die Wahrscheinlichkeit, daß ein Beobachtungsfehler seinem Werte nach in dem unendlich kleinen Intervall zwischen t und $t + dt$ liegt; in diesem Ausdruck bedeutet h eine positive Konstante, welche für verschiedene Beobachtungsmethoden im allgemeinen auch verschiedene Werte hat, und zwar leuchtet ein, daß eine Beobachtungsmethode desto zuverlässiger ist, je größer der Wert der ihr zugehörigen Konstante h ist; denn die Wahrscheinlichkeit

$$\frac{h}{\sqrt{\pi}}\int_{-a}^{+a} e^{-h^2t^2}dt = \frac{1}{\sqrt{\pi}}\int_{-ha}^{+ha} e^{-u^2}du$$

dafür, daß ein Fehler seinem absoluten Werte nach die positive Größe a nicht überschreitet, ist desto größer, je größer h ist. Aus diesem Grunde hat Gauß die Größe h die Präzision der Beobachtungsmethode genannt; in einer späteren Abhandlung (Zeitschrift für Astronomie usw. von Lindenau und Bohnenberger, Bd. I, 1816) hat er ferner gezeigt, wie man den wahrscheinlichsten Wert der Präzision einer Beobachtungsmethode bestimmen kann, wenn eine Reihe wirklich gemachter Beobachtungsfehler bekannt ist. Es wird für das Folgende nützlich sein, hier den von Gauß zu diesem Zwecke eingeschlagenen Weg wieder in Erinnerung zu bringen, welcher auf dem Satze über die Wahrscheinlichkeit a posteriori beruht.

Ist h die wahre Präzision der Beobachtungsmethode, so ist die Wahrscheinlichkeit, daß bei m aufeinanderfolgenden Beobachtungen die Fehler

$$t_1,\ t_2,\ \ldots,\ t_m$$

gemacht werden, gleich

$$\alpha = \left(\frac{h}{\sqrt{\pi}}\right)^m e^{-h^2 S}\, dt_1\, dt_2 \ldots dt_m,$$

worin zur Abkürzung

$$S = t_1^2 + t_2^2 + \cdots + t_m^2$$

gesetzt ist. A priori, d. h. ehe irgend eine Messung vorgenommen ist, haben wir keinen Grund, der Präzision einer uns unbekannten Beobachtungsmethode einen Wert h eher beizulegen als einen anderen; folglich ist a posteriori, d. h. nachdem wirklich die Beobachtungsfehler $t_1, t_2, \ldots t_m$ gemacht sind, die Wahrscheinlichkeit der Hypothese, daß h der wahre Wert der Präzision ist, proportional dem α, also proportional dem Ausdruck

$$h^m e^{-h^2 S},$$

welcher für

$$\frac{1}{2h^2} = \frac{S}{m}, \quad \text{also} \quad h = \sqrt{\frac{m}{2S}}$$

ein Maximum wird; es ist also dies der wahrscheinlichste Wert der Präzision der Beobachtungsmethode.

In allen wirklichen Fällen liegt aber die Sache ganz anders. Die Objekte der Beobachtungen sind lineare Funktionen

$$v_1,\ v_2,\ \ldots\ v_m$$

von gewissen unbekannten Größen $x, y, z \ldots$, deren Anzahl n höchstens gleich der Anzahl m der Beobachtungen und deren Wertbestimmung gerade der Zweck dieser Beobachtungen ist. Sind nun

$$k_1,\ k_2,\ \ldots\ k_m$$

die durch die Beobachtungen gelieferten Werte von $v_1, v_2, \ldots v_m$, so bestimmt die aus dem obigen Wahrscheinlichkeitsgesetz eines beliebigen Fehlers t gefolgerte Methode der kleinsten Quadrate die Werte der Unbekannten $x, y, z \ldots$ durch die Forderung, daß die Quadratsumme

$$(k_1 - v_1)^2 + (k_2 - v_2)^2 + \cdots + (k_m - v_m)^2 = \Omega$$

ein Minimum werden soll. Wären nun diese wirklich die wahren Werte der Unbekannten, so wären die entsprechenden Werte der Differenzen

$$k_1 - v_1,\ k_2 - v_2,\ \ldots\ k_m - v_m$$

auch die wahren Beobachtungsfehler, und man könnte versucht sein, den wahrscheinlichsten Wert der Präzision h nach der früheren Regel zu bestimmen, indem man statt S nur das Minimum Ω_0 der Funktion Ω zu substituieren brauchte, so daß also

$$\sqrt{\frac{m}{2\Omega_0}}$$

als wahrscheinlichster Wert von h anzusehen wäre. Daß diese Formel aber nicht richtig sein kann, bemerkt man am deutlichsten in dem Falle, wo $n = m$ ist; dann können nämlich die gemachten Beobachtungen sämtlich durch ein und dasselbe Wertsystem $x, y, z, \ldots$ befriedigt werden, Ω_0 ist $= 0$, und man würde $h = \infty$, also das Resultat erhalten, daß die Beobachtungsmethode höchstwahrscheinlich absolut genau ist, während doch erst dann ein Urteil über die Präzision gestattet ist, wenn ein Überschuß von Beobachtungen vorliegt.

In einer späteren Abhandlung (Theoria combinationis etc. art. 39) in welcher das Prinzip des arithmetischen Mittels und damit zugleich das obige Wahrscheinlichkeitsgesetz eines Fehlers t ganz verlassen ist, hat Gauß für eine ähnliche Frage (die nach dem wahrscheinlichsten Werte des sogenannten mittleren Fehlers) die richtige Antwort gegeben, welche, auf die frühere Darstellungsweise übertragen, den Ausdruck

$$\sqrt{\frac{m-n}{2\Omega_0}}$$

als wahrscheinlichsten Wert der Präzision h liefert, so daß also das Minimum Ω_0 als eine Summe von nur $(m-n)$ Fehlerquadraten zu behandeln ist. Man sieht, daß diese Formel in dem Falle $n = m$ unter die ganz unbestimmte Form $\frac{0}{0}$ tritt, und in der Tat ist in diesem Falle gar kein Schluß auf die Präzision gestattet.

Es erscheint nun wünschenswert, einen Beweis dieses Satzes auch aus dem obigen Wahrscheinlichkeitsgesetz abzuleiten, da dies meines Wissens in befriedigender Weise noch nicht geschehen ist*). Dazu führt folgender einfache Weg.

*) So z. B. geht Wittstein (Anhang zu der Übersetzung von Naviers Differentialrechnung) von dem unrichtigen Satze aus, daß, wenn h die wahre Präzision ist, der wahrscheinlichste Wert eines Fehlerquadrates $= \frac{1}{2h^2}$, statt 0 ist.

In der Hypothese B, daß $h, x, y, z, \ldots$ die wahren Werte der Präzision, der ersten, zweiten, dritten usw. Unbekannten sind, ist die Wahrscheinlichkeit, daß für die Funktionen

$$v_1,\ v_2,\ \ldots\ v_m$$

die Werte

$$k_1,\ k_2,\ \ldots\ k_m$$

durch Beobachtung geliefert, daß also die Beobachtungsfehler

$$k_1 - v_1,\ \ k_2 - v_2,\ \ \ldots\ \ k_m - v_m$$

gemacht werden, proportional dem Ausdruck

$$h^m e^{-h^2\Omega};$$

da nun alle denkbaren Hypothesen B a priori gleich wahrscheinlich sind, so ist a posteriori, d. h. nachdem wirklich die Werte $k_1, k_2, \ldots k_m$ beobachtet sind, die Wahrscheinlichkeit der Hypothese B proportional demselben Ausdruck; dieselbe ist daher

$$= C h^m e^{-h^2\Omega} dh\, dx\, dy\, dz \ldots,$$

worin

$$\frac{1}{C} = \int_0^\infty dh \int_{-\infty}^{+\infty} dx \int_{-\infty}^{+\infty} dy \int_{-\infty}^{+\infty} dz \ldots h^m e^{-h^2\Omega}.$$

Fragt man nun nach dem wahrscheinlichsten Wertsystem von $h, x, y, z, \ldots$, so würde man untersuchen müssen, für welche Werte $h, x, y, z, \ldots$ der Ausdruck

$$h^m e^{-h^2\Omega}$$

ein Maximum wird. Allein wir fragen nach dem wahrscheinlichsten Werte der Präzision allein; wir haben daher zunächst den Ausdruck der Wahrscheinlichkeit herzustellen, daß der Wert der Präzision zwischen h und $h + dh$ liegt. Diesen erhält man aus dem Vorhergehenden durch Integration über alle reellen Werte von $x, y, z, \ldots$ Es ist aber nach bekannten Sätzen

$$\int_{-\infty}^{+\infty} dx \int_{-\infty}^{+\infty} dy \int_{-\infty}^{+\infty} dz \ldots e^{-h^2\Omega} = K \frac{1}{h^n} e^{-h^2\Omega_0},$$

worin K von h unabhängig ist; folglich ist das aus den gemachten Beobachtungen resultierende Wahrscheinlichkeitsgesetz für die Präzision von der Form

$$H . h^{m-n} e^{-h^2\Omega_0} dh,$$

worin

$$\frac{1}{H} = \int_0^\infty h^{m-n} e^{-h^2\Omega_0} dh$$

ist. Vergleicht man diese Form mit der früheren

$$H' h^m e^{-h^2 S} dh, \quad \text{wo} \quad \frac{1}{H'} = \int_0^\infty h^m e^{-h^2 S} dh,$$

welche sich ergab, wenn m wahre Beobachtungsfehler vorlagen, deren Quadratsumme $= S$ war, so findet man in der Tat vollständige Übereinstimmung, wenn man das Minimum Ω_0 der Summe von m Fehlerquadraten wie eine Summe von $m - n$ wirklichen Fehlerquadraten ansieht. Der wahrscheinlichste Wert zu der Präzision ist daher wirklich

$$= \sqrt{\frac{m-n}{2\Omega_0}}.$$

Hiermit ist der eigentliche Gegenstand dieser Mitteilung beendigt; zum Schluß mag noch folgende Bemerkung gemacht werden. Wir haben als wahrscheinlichsten Wert h einen anderen gefunden, als denjenigen, welcher dem h in dem wahrscheinlichsten System von Werten $h, x, y, z, \ldots$ zukommt. Man könnte nun befürchten, daß auch die Bestimmung der wahrscheinlichsten Werte von $x, y, z, \ldots$, wenn sie nach demselben Prinzip ausgeführt, wenn also für jede einzelne Unbekannte besonders der wahrscheinlichste Wert aufgesucht würde, von der durch die Methode der kleinsten Quadrate geforderten Regel abweichen könnte. Allein man überzeugt sich leicht, daß diese Befürchtung ungegründet ist, und daß das System der wahrscheinlichsten Werte von $x, y, z, \ldots$ übereinstimmt mit dem wahrscheinlichsten Wertsystem dieser Unbekannten.

Das letztere ist offenbar dasjenige, für welches die Quadratsumme Ω ein Minimum wird, und darin besteht ja gerade der Hauptsatz der Methode der kleinsten Quadrate; die entsprechenden Werte der n Unbekannten $x, y, z, \ldots$ findet man bekanntlich dadurch, daß man, was immer möglich ist, die Funktion Ω auf die Form

$$\Omega = Y^2 + Z^2 + \cdots + X^2 + \Omega_0$$

bringt, worin Y eine lineare Funktion aller n Unbekannten ist, die dadurch bestimmt wird, daß $\Omega - Y^2$ unabhängig von y wird; ähnlich

ist Z eine lineare Funktion der übrigen $(n-1)$ Unbekannten, und dadurch bestimmt, daß $\Omega - Y^2 - Z^2$ unabhängig von y, z wird, usf., so daß endlich X eine lineare Funktion von der n^{ten} Unbekannten x allein ist. Die Werte, welche Ω zu einem Minimum machen, sind diejenigen, welche die n Gleichungen

$$X = 0, \quad \ldots \quad Z = 0, \quad Y = 0$$

befriedigen, und das letzte Glied Ω_0 in dieser Form stellt offenbar den Minimumwert von Ω dar.

Fragt man nun aber nach dem wahrscheinlichsten Wert der Unbekannten x allein, so hat man zunächst den Ausdruck der Wahrscheinlichkeit abzuleiten, daß der Wert dieser Unbekannten zwischen den Grenzen x und $x + dx$ enthalten ist. Diesen erhält man durch Integration des obigen Wertes

$$C h^m e^{-h^2 \Omega} dh\, dx\, dy\, dz \ldots$$

in bezug auf alle zulässigen Werte der Unbekannten $h, y, z, \ldots$ Bringt man die Summe Ω auf die oben erwähnte Form, so gibt die sukzessive Integration in bezug auf die $(n-1)$ Unbekannten $y, z, \ldots$ ein Resultat

$$C' h^{m-n+1} e^{-h^2 (X^2 + \Omega_0)} dh\, dx,$$

worin C' unabhängig von h und x ist; integriert man endlich noch in bezug auf h, so erhält man für die gesuchte Wahrscheinlichkeit den Ausdruck

$$\frac{c\, dx}{(X^2 + \Omega_0)^{\frac{m-n+2}{2}}},$$

worin

$$\frac{1}{c} = \int_{-\infty}^{+\infty} \frac{dx}{(X^2 + \Omega_0)^{\frac{m-n+2}{2}}};$$

und hieraus folgt, daß derjenige Wert von x, für welchen $X = 0$ wird, unter allen der wahrscheinlichste ist. Dieser Wert stimmt daher wirklich mit dem durch die Methode der kleinsten Quadrate erhaltenen überein.

XI.

Zur Theorie der Maxima und Minima.

[Vierteljahrsschrift der naturforschenden Gesellschaft in Zürich, 1860, S. 84—88.]

In den Elementen der Differentialrechnung wird folgender Satz bewiesen:

„Sind innerhalb eines gewissen Wertengebietes der unabhängigen Variabeln $x, y, z, \ldots$ die partiellen Derivierten erster Ordnung

$$\frac{du}{dx}, \quad \frac{du}{dy}, \quad \frac{du}{dz}, \quad \ldots$$

einer Funktion u dieser Variabeln überall endlich und stetig, so kann ein Maximum oder Minimum von u nur da eintreten, wo diese Derivierten sämtlich verschwinden."

Hat nämlich z. B. $\frac{du}{dx}$ einen von Null verschiedenen Wert, so erleidet u, wenn man der Variabeln x zwei beliebig kleine Änderungen von entgegengesetzten Vorzeichen gibt, ebenfalls Änderungen von entgegengesetzten Vorzeichen, so daß der entsprechende Wert von u weder ein Maximum noch ein Minimum sein kann.

Man bedient sich dieses Satzes, um die Stellen $x, y, z, \ldots$ aufzusuchen, wo die Funktion ein Maximum oder Minimum wird; aber dies kann auch an solchen Stellen eintreten, wo die partiellen Derivierten unstetig werden, und zwar bietet sich dieser Fall häufig in ganz einfachen Aufgaben dar, wofür das folgende Beispiel einen Beleg geben mag, bei welchem diese Erscheinung bis jetzt unbeachtet geblieben ist.

Aufgabe: Es sind drei Punkte m_1, m_2, m_3 gegeben; es soll ein vierter Punkt m gefunden werden, für welchen die Summe der absoluten Distanzen mm_1, mm_2, mm_3 so klein wie möglich ausfällt.

Auflösung. Man nehme willkürlich im Raume ein rechtwinkliges Koordinatensystem, nenne x, y, z die Koordinaten des gesuchten

Punktes m, und r_1, r_2, r_3 die absoluten Werte seiner Distanzen von den drei gegebenen Punkten m_1, m_2, m_3, so daß

$$u = r_1 + r_2 + r_3$$

die Funktion von x, y, z ist, deren Minimumwert bestimmt werden soll. Verfährt man nun nach der gewöhnlichen Regel, so hat man

$$\frac{dr_1}{dx} + \frac{dr_2}{dx} + \frac{dr_3}{dx} = 0, \quad \frac{dr_1}{dy} + \frac{dr_2}{dy} + \frac{dr_3}{dy} = 0,$$
$$\frac{dr_1}{dz} + \frac{dr_2}{dz} + \frac{dr_3}{dz} = 0$$

zu setzen. Da man aber die Achsen mit jeder beliebigen Richtung h zusammenfallen lassen kann, so lassen sich diese drei Gleichungen in die einzige

$$cos(p_1 h) + cos(p_2 h) + cos(p_3 h) = 0$$

zusammenfassen, in welcher p_1, p_2, p_3 die vom Punkte m nach m_1, m_2, m_3 laufenden Richtungen, und $(p_1 h)$, $(p_2 h)$, $(p_3 h)$ die Winkel bedeuten, welche dieselben mit der willkürlichen Richtung h einschließen.

Nimmt man h senkrecht auf p_2 und p_3, so folgt, daß h auch senkrecht auf p_1 ist, daß also die drei Richtungen p_1, p_2, p_3 und folglich auch die vier Punkte m, m_1, m_2, m_3 in einer Ebene liegen, was sich ohnehin erwarten ließ.

Läßt man ferner h sukzessive mit p_1, p_2, p_3 zusammenfallen, so erhält man

$$1 + cos(p_2 p_1) + cos(p_3 p_1) = 0,$$
$$cos(p_1 p_2) + 1 + cos(p_3 p_2) = 0,$$
$$cos(p_1 p_3) + cos(p_2 p_3) + 1 = 0,$$

woraus

$$cos(p_2 p_3) = cos(p_3 p_1) = cos(p_1 p_2) = -\tfrac{1}{2}$$
$$(p_2 p_3) = (p_3 p_1) = (p_1 p_2) = 120^0$$

folgt.

Man erhält daher die bekannte Antwort, daß der Punkt m in der Ebene der drei Punkte m_1, m_2, m_3 so zu konstruieren ist, daß je zwei der drei Richtungen mm_1, mm_2, mm_3 einen Winkel von 120° miteinander bilden. Diese Konstruktion ist auch stets möglich, und liefert einen vollständig bestimmten Punkt m, sobald keiner der drei Winkel des Dreiecks $m_1 m_2 m_3$ größer ist als 120°.

Ist aber einer der drei Winkel des Dreiecks $m_1 m_2 m_3$ größer als 120°, so wird diese Konstruktion unausführbar; es gibt dann

keinen Punkt m von der Beschaffenheit, daß je zwei der drei Richtungen mm_1, mm_2, mm_3 einen Winkel von 120° bilden; es gibt also keinen Punkt m, für welchen die partiellen Derivierten der Funktion u gleichzeitig verschwinden. Andererseits leuchtet aber aus dem Begriff der Funktion u, welche stets positiv ist und für unendlich entfernte Punkte unendlich wächst, unmittelbar ein, daß sie irgendwo in endlicher Entfernung doch einen Minimumwert haben muß. Wir müssen daraus schließen, daß dieser Minimumwert an einer solchen Stelle eintritt, wo die partiellen Derivierten von u unstetig werden. Da nun die Derivierten der absoluten Distanz eines beliebigen Punktes von einem festen Punkte nur in diesem letzteren selbst unstetig werden, und u eine Summe von drei solchen absoluten Distanzen ist, so werden die Derivierten nur in den drei gegebenen Punkten m_1, m_2, m_3 unstetig; es muß daher der gesuchte Punkt m mit einem dieser drei Punkte zusammenfallen. Da endlich für den Fall, daß der Dreieckswinkel bei m_1 um unendlich wenig kleiner als 120° ist, die frühere Konstruktion den gesuchten Punkt m unendlich nahe bei m_1 liefert, und auch, wenn dieser Winkel = 180° ist, der gesuchte Punkt offenbar mit m_1 zusammenfällt, so wird es daher so gut wie gewiß, daß auch für alle Werte des Winkels zwischen 120° und 180° die Spitze desselben der gesuchte Punkt ist.

Dies bestätigt sich analytisch, wenn man die unendlich kleine Änderung der Funktion u untersucht für den Fall, daß der variable Punkt m sich unendlich wenig von dem Punkte m_1 entfernt. Zieht man nämlich vom Punkte m_1 aus eine beliebige Richtung h, welche mit $m_1 m_2$ und $m_1 m_3$ die Winkel α und β einschließt, so ist die in dieser Richtung h genommene Derivierte der Funktion u gleich

$$1 - cos\,\alpha - cos\,\beta = 1 - 2\,cos\frac{\alpha+\beta}{2}\,cos\frac{\alpha-\beta}{2};$$

bezeichnet man ferner mit Θ den Winkel zwischen den Richtungen $m_1 m_2$ und $m_1 m_3$, von dem wir annehmen, daß er zwischen 120° und 180° liegt, so folgt aus den bekannten Eigenschaften

$$\alpha + \beta + \Theta \leqq 360^0, \quad \alpha + \beta \gtreqless \Theta,$$

der drei Winkel zwischen drei Richtungen, daß

$$120^0 \geqq \frac{\alpha+\beta}{2} \geqq 60^0,$$

also

$$-\frac{1}{2} \leqq \cos\frac{\alpha+\beta}{2} \leqq +\frac{1}{2},$$

daß also der absolute Wert von $2\cos\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2}$ ein echter Bruch ist. Mithin ist die obige Derivierte stets positiv, und folglich wächst u von dem Punkte m_1 aus nach allen Richtungen hin, was zu beweisen war.

Da der absolute Wert der Differenz $\alpha-\beta \leqq \Theta$, also $\cos\frac{\alpha-\beta}{2}$ positiv ist, so kann die obige Derivierte nur dann den Wert Null haben, wenn

$$\cos\frac{\alpha-\beta}{2} = 1; \quad \cos\frac{\alpha+\beta}{2} = +\frac{1}{2}$$

ist, d. h. wenn

$$\alpha = \beta = 60^0 \quad \text{und folglich auch} \quad \Theta = 120^0,$$

also h die Halbierungsrichtung zwischen m_1m_2 und m_1m_3 ist. Aber in diesem Falle überzeugt man sich leicht, daß die zweite in derselben Richtung genommene Derivierte einen positiven Wert hat.

XII.

Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers.

[Festschrift der Technischen Hochschule in Braunschweig zur Säkularfeier des Geburtstages von C. F. Gauß, Braunschweig 1877, S. 1—55.]

Die erhabenen Schöpfungen von Carl Friedrich Gauß haben die Bewunderung der Mathematiker dieses Jahrhunderts vor allem deshalb erregt, weil sie in fast beispielloser Weise die Wissenschaft mit einer außerordentlichen Fülle ganz neuer Gedanken befruchtet und vorher gänzlich unbekannte Felder zum ersten Male der Forschung erschlossen haben. Im höchsten Maße gilt dies von Gauß' Entdeckungen im Gebiete der höheren Arithmetik, die ihn nach seinem eigenen Ausspruche das ganze Leben hindurch vor allen anderen Teilen der Mathematik gefesselt hat. Mit der Theorie der Kreisteilung ist von ihm nicht bloß der Grund zu einem neuen Teile der Mathematik gelegt, welcher von der algebraischen Verwandtschaft der Zahlen handelt, sondern sie hat auch das erste und bis jetzt noch immer fruchtbarste Beispiel des innigen Zusammenhangs zwischen der höheren Algebra und der Zahlentheorie geliefert, welche bis dahin zwei vollständig getrennte Gebiete gebildet hatten. In der nächsten Beziehung zu dieser Erweiterung der Grenzen der Wissenschaft steht der kühne Gedanke, den Begriff der ganzen Zahl durch die Einführung der ganzen komplexen Zahlen von seiner bisherigen Beschränkung zu befreien, wodurch Gauß abermals der arithmetischen Forschung ein heute noch unermeßliches Feld eröffnet hat. Aber es ist nicht bloß dieser wunderbare Reichtum an neuen Gedanken und großen Entdeckungen, durch welchen Gauß sein Wirken auf allen von ihm beschrittenen Gebieten der Wissenschaft für alle Zeiten bezeichnet hat, sondern es steht diesem vollständig ebenbürtig die Tiefe der Methoden gegenüber, durch welche er die größten Schwierig-

keiten überwunden und die verborgensten Wahrheiten, die *mysteria numerorum*, in das hellste Licht gesetzt hat. Es genügte seinem stets auf das Große und auf die zukünftige Entwicklung der Wissenschaft blickenden Geiste nicht, einen Beweis gefunden und damit die Wahrheit außer Zweifel gesetzt zu haben, sondern er kehrte, wie er selbst so eindringlich beschreibt, unablässig zu den schon überwundenen Schwierigkeiten zurück, in der Hoffnung, durch erneute Anstrengungen neue Waffen zu gewinnen, welche eine über das unmittelbar vorliegende Ziel weit hinausreichende Tragweite besäßen. Und so ist es gekommen, daß dieselben von Gauß erdachten Methoden unmittelbar oder mit geringen Modifikationen auch bei der Behandlung von ähnlichen, aber allgemeineren Problemen sich als vollständig ausreichend erweisen. Diese schon oft als ein besonders charakteristisches Kennzeichen der Gedankentiefe von Gauß hervorgehobene Erscheinung an einem neuen Beispiel zu bestätigen, ist der Zweck der gegenwärtigen Abhandlung, welche dem Andenken des großen Mathematikers gewidmet ist.

Die Theorie der binären quadratischen Formen, zu deren Entstehung einige Sätze von Fermat die Veranlassung gegeben haben verdankt ihre Begründung den hervorragenden Arbeiten von Euler und Lagrange, aber sie ist erst von Gauß durch die in der fünften Sektion der Disquisitiones Arithmeticae niedergelegten Untersuchungen zu einem wissenschaftlichen Ganzen gestaltet, und namentlich hat sie durch die daselbst zum ersten Male behandelte Lehre von der Komposition der Formen die höchste Bereicherung erhalten. Unter den Anwendungen, welche Gauß von dieser neuen Theorie gemacht hat, ist eine der bemerkenswertesten die Bestimmung des Verhältnisses der Klassen-Anzahlen der Formen, welche zu zwei verschiedenen Ordnungen derselben Determinante D gehören; bezeichnet man mit $h(D)$ die Klassen-Anzahl für diejenige Ordnung der Determinante D, welche nur primitive Formen (und zwar entweder nur die eigentlichen oder nur die uneigentlichen) enthält, so kommt diese Aufgabe darauf hinaus, für zwei gegebene, in quadratischem Verhältnis stehende Determinanten D und D' das Verhältnis $h(D):h(D')$ zu ermitteln. Die aus der Theorie der Komposition der Formen geschöpfte Beantwortung dieser Frage ist im Art. 256, V. und VI. enthalten, und sie ist für den Fall negativer Determinanten eine so vollständige, daß der Wert des Verhältnisses $h(D):h(D')$ unmittelbar

aus den Werten von D und D' entnommen werden kann; nicht ebenso vollständig durchgeführt ist der Fall positiver Determinanten, über welchen Gauß folgendes sagt: „*Pro casu tertio autem, ubi D est numerus positivus non quadratus, regulam generalem pro comparanda multitudine formarum pr. primitivarum in V, V', V'' etc. cum multitudine classium diversarum inde resultantium hucusque non habemus. Id quidem asserere possumus, hanc vel illi aequalem vel ipsius partem aliquotam esse; quin etiam nexum singularem inter quotientem horum numerorum et valores minimos ipsorum t, u aequationi $tt - Duu = AA$ satisfacientes deteximus, quem hic explicare nimis prolixum foret; an vero possibile sit, illum quotientem in omnibus casibus ex sola inspectione numerorum D, A cognoscere (ut in casibus praecc.), de hac re nihil certi pronunciare possumus.*“

Das umfassendere und noch viel schwierigere Problem, die Klassen-Anzahl $h(D)$ selbst, d. h. die Abhängigkeit dieser Anzahl von der Determinante D zu bestimmen, ist schon während des Druckes der fünften Sektion der Disquisitiones Arithmeticae, wie aus Art. 306, X. hervorgeht, ein Gegenstand des höchsten Interesses für Gauß gewesen, und es ist ihm in der Tat bald darauf gelungen, die vollständige Lösung desselben zu finden, was er noch am Schlusse des großen Werkes mit folgenden Worten ankündigen konnte: „*Quaestionem hic propositam plene solvere nuper successit, quam disquisitionem plures partes tum Arithmeticae sublimioris tum Analyseos mirifice illustrantem in continuatione hujus operis trademus quam primum licebit.*“ Allein die hier in Aussicht gestellte Veröffentlichung dieser Untersuchung ist zu Gauß' Lebzeiten nicht erfolgt; der hierauf bezügliche Teil seines Nachlasses, welchen ich in dem 1863 erschienenen zweiten Bande seiner gesammelten Werke herausgegeben habe, enthält namentlich zwei Fragmente, die aus den Jahren 1834 und 1837 stammen und den gemeinsamen Titel führen: „*De nexu inter multitudinem classium, in quas formae binariae secundi gradus distribuuntur, earumque determinantem.*“ Obgleich jedes dieser Fragmente nach wenigen Seiten abbricht, so reicht ihr Inhalt doch aus, um den Weg vollständig überblicken zu lassen, auf welchem Gauß zu dem erstrebten Ziele gelangt ist.

Im Jahre 1839, also 38 Jahre nach dem Erscheinen der Disquisitiones Arithmeticae, trat Peter Gustav Lejeune Dirichlet,

der nach Gauß' eigenem Zeugnis zuerst von allen Mathematikern dieses Werk vollständig begriffen und die darin enthaltenen Untersuchungen selbständig weitergeführt hat, mit einer vollständigen und höchst eigentümlichen Lösung des Problems der Klassen-Anzahl hervor*). Ohne hier, was zu weit führen würde, auf eine nähere Vergleichung der Methode von Dirichlet mit derjenigen von Gauß einzugehen, bemerke ich nur, daß von beiden für die Klassen-Anzahl ein Ausdruck durch eine unendliche Reihe gewonnen wird, welche sich mit Hilfe gewisser, der Kreisteilung angehörender Sätze von Gauß summieren, also in geschlossener Form darstellen läßt. Aber es ist von Wichtigkeit, daß es schon vor Ausführung dieser Summation gelingt, aus dem erhaltenen Ausdruck den Wert des oben besprochenen Verhältnisses $h(D):h(D')$ abzuleiten. Auf diese Weise**) ist Dirichlet für den Fall negativer Determinanten zu demselben Resultat gelangt wie Gauß, und er hat außerdem für den Fall positiver Determinanten zum ersten Male das Gesetz vollständig ausgesprochen, nach welchem das gesuchte Verhältnis von den kleinsten Lösungen der unbestimmten Gleichungen $tt - Duu = 1$, $t't' - D'u'u' = 1$ abhängt. Aus der oben angeführten, auf diesen Fall bezüglichen Stelle der Disquisitiones Arithmeticae geht aber wohl mit Gewißheit hervor, daß Gauß ebenfalls dieses Gesetz schon vollständig gekannt hat, welches zwar einfach, aber doch keineswegs so einfach ist, daß man *ex sola inspectione numerorum* D, D' den Wert des gesuchten Verhältnisses erkennen könnte; auch habe ich gezeigt***), daß man wirklich auf dem von Gauß eingeschlagenen Wege, d. h. durch die Komposition der Formen, mit wenigen Schritten zu diesem, zuerst von Dirichlet ausgesprochenen Gesetz gelangen kann.

Beide Methoden, das Verhältnis der Klassen-Anzahlen zu bestimmen, sowohl die von Gauß, welche auf die Komposition der Formen gegründet ist, als auch diejenige von Dirichlet, zeichnen sich nun dadurch aus, daß sie auf ähnliche Probleme von sehr allgemeinem Charakter mit demselben Erfolg anwendbar

*) Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres (Crelles Journal, Bd. 19, 21).

**) Ebenda, Bd. 21, § 8.

***) Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet. Zweite Auflage. 1871. §. 150, 151. — Ich werde dieses Werk in der Folge kurz mit D. zitieren.

sind*). Die binären quadratischen Formen, von welchen bisher ausschließlich gesprochen ist, bilden nämlich nur einen äußerst speziellen Fall der sogenannten zerlegbaren Formen, d. h. der homogenen Funktionen von beliebig hohem Grade n mit n Variabelen, welche rationale Koeffizienten haben und in n lineare Faktoren mit algebraischen Koeffizienten zerlegbar sind. Das Verdienst, diese Formen zuerst betrachtet und eine charakteristische Fundamental-Eigenschaft derselben erkannt zu haben, gebührt Lagrange**), und eine weitere Verfolgung seines Gedankens hätte leicht schon früher zu der Theorie der Komposition der Formen führen können. Erst viel später hat sich Dirichlet eingehend mit diesem Gegenstand beschäftigt; leider ist von seinen tiefen Untersuchungen — abgesehen von der ebenfalls hierhergehörigen, aber speziellen Theorie der quadratischen Formen mit komplexen Koeffizienten und Variabelen***) — nur eine einzige veröffentlicht, welche die Theorie der Transformation dieser Formen in sich selbst, oder, anders ausgedrückt, die Theorie der Einheiten in dem entsprechenden Gebiete algebraischer Zahlen behandelt. Der in äußerst kurzen Umrissen von Dirichlet mitgeteilte Beweis****) für die Existenz und für die allgemeine Form aller dieser Einheiten, welcher ihm erst nach großen und anhaltenden Anstrengungen gelungen ist, muß zu seinen bedeutendsten Leistungen gezählt werden, da derselbe ein unerläßliches Fundament für die ganze Theorie bildet; und Dirichlet selbst, der seinen eigenen Schöpfungen gegenüber sich immer ein ganz unbefangenes Urteil bewahrte, legte auf dies Resultat einen ebenso hohen Wert, wie auf die Prinzipien, welche ihn zu dem Beweise des Satzes über die arithmetische Progression und zur Bestimmung der Klassen-Anzahl der binären quadratischen Formen geführt haben. Dirichlet hat auch die Klassen-Anzahl für solche zerlegbare Formen bestimmt, welche aus der Theorie der

*) Ob dasselbe auch von der scharfsinnigen Methode gilt, welche R. Lipschitz zur Lösung derselben Aufgabe angewandt hat (Crelles Journal, Bd. 53), wage ich für jetzt nicht zu beurteilen; doch spricht dafür der Erfolg, mit welchem er diese Methode auf ein höheres Problem übertragen hat (Crelles Journal, Bd. 54).

**) Sur la solution des problèmes indéterminés du second degré. § VI. Mém. de l'Ac. de Berlin. T. XXIII, 1769. — Élémens d'Algèbre par L. Euler; Additions § IX.

***) Crelles Journal, Bd. 24.

****) Monatsberichte der Berliner Akademie vom Oktober 1841, April 1842, März 1846. — Comptes rendus der Pariser Akademie 1840, T. X, S. 286.

Kreisteilung entspringen, aber hiervon ist nichts veröffentlicht*). Es folgte zunächst im Jahre 1844 eine wertvolle Untersuchung von Eisenstein**) über gewisse kubische Formen, welche aus der Kreisteilung entspringen; doch scheint dieselbe wegen ihres sehr speziellen Charakters keinen bedeutenden Einfluß auf die Entwicklung der allgemeinen Theorie ausgeübt zu haben. Den größten und folgenreichsten Schritt aber hat Kummer***) im Jahre 1847 durch die Einführung der idealen Zahlen getan; denn wenn auch seine Untersuchungen ebenfalls sich zunächst nur auf die Kreisteilung und einige derselben nahestehende Gebiete beziehen, so sind doch die ihnen zugrunde liegenden Gedanken von viel allgemeinerer Bedeutung. Der außerordentliche, von Kummer erreichte Erfolg hat mich schon seit dem Jahre 1856 angetrieben, meine Kräfte hauptsächlich diesem Gegenstand zu widmen, und es ist mir endlich gelungen, eine allgemeine, ausnahmslose Theorie der ganzen algebraischen Zahlen aufzustellen, deren Grundlagen ich in dem zehnten Supplement der zweiten Auflage von Dirichlets Vorlesungen über Zahlentheorie veröffentlicht habe****). Mit Hilfe dieser Prinzipien, welche ich hier als bekannt voraussetzen muß, läßt sich nun das auf die zerlegbaren Formen von beliebigem Grade oder auf die entsprechenden Ideal-Klassen übertragene Problem, das Verhältnis der Klassen-Anzahlen für verschiedene Ordnungen zu bestimmen, sowohl nach der Methode von Gauß, als auch nach derjenigen von Dirichlet vollständig lösen, und hierin besteht das Ziel der vorliegenden Abhandlung.

§ 1.

Theorie der ganzen Zahlen eines endlichen Körpers.

Obwohl diese Theorie, deren Mittelpunkt die Lehre von der Multiplikation der Ideale und von der Komposition der Ideal-Klassen bildet, hier als bekannt vorausgesetzt werden muß, so wird es doch

*) Vgl. Kummer, Gedächtnisrede auf G. P. Lejeune Dirichlet, 1860, S. 21—22.

**) Crelles Journal, Bd. 28.

***) Ebenda, Bd. 35.

****) Eine etwas ausführlichere Darstellung eines Teiles dieser Theorie erscheint gegenwärtig unter dem Titel *Sur la théorie des nombres entiers algébriques* in dem *Bulletin des sciences mathématiques et astronomiques* von Darboux und Houël. — Ich werde diese Abhandlung mit B. zitieren. [Vgl. Bd. 3 dieser Ausgabe.]

zweckmäßig sein, die wichtigsten ihr zugrunde liegenden Begriffe hier möglichst kurz in Erinnerung zu bringen, schon um den Anknüpfungspunkt der jetzigen Abhandlung an meine früheren Untersuchungen deutlicher hervorheben zu können.

Ist θ eine algebraische Zahl, und zwar eine Wurzel einer irreduktiblen Gleichung

$$f(\theta) = \theta^n + a_1\theta^{n-1} + \cdots + a_{n-1}\theta + a_n = 0$$

vom $n$ten Grade, deren Koeffizienten $a_1, a_2 \cdots a_{n-1}, a_n$ rationale Zahlen sind, und betrachtet man die sämtlichen Zahlen von der Form

$$\omega = \varphi(\theta) = x_0 + x_1\theta + x_2\theta^2 + \cdots + x_{n-1}\theta^{n-1},$$

wo $x_0, x_1, x_2 \cdots x_{n-1}$ willkürliche rationale Zahlen bedeuten, so besitzt der Inbegriff Ω aller dieser Zahlen ω die charakteristische Eigenschaft eines Körpers (D. § 159), welche darin besteht, daß die Summen, Differenzen, Produkte und Quotienten von je zwei solchen Zahlen ω ebenfalls in Ω enthalten sind; ein Körper Ω, dessen Zahlen auf die angegebene Art aus einer Wurzel θ einer irreduktiblen Gleichung $n$ten Grades gebildet sind, heißt speziell ein endlicher Körper vom Grade n. Hat man n Zahlen

$$\omega_1 = \varphi_1(\theta), \quad \omega_2 = \varphi_2(\theta) \cdots \omega_n = \varphi_n(\theta)$$

nach Belieben, nur mit der einzigen Beschränkung aus Ω ausgewählt, daß die aus den n^2 rationalen Koeffizienten x gebildete Determinante einen von 0 verschiedenen Wert besitzt, so läßt sich jede beliebige Zahl ω des Körpers Ω stets und nur auf eine einzige Weise in der Form

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n$$

darstellen, wo $h_1, h_2 \cdots h_n$ rationale Zahlen bedeuten. Ein solches System von n Zahlen $\omega_1, \omega_2 \cdots \omega_n$ heißt eine Basis des Körpers Ω, und die n rationalen Zahlen $h_1, h_2 \cdots h_n$ heißen die Koordinaten der Zahl ω in bezug auf diese Basis. Offenbar bilden die Zahlen $1, \theta, \theta^2 \cdots \theta^{n-1}$ selbst eine solche Basis.

Ist θ' ebenfalls eine Wurzel derselben irreduktiblen Gleichung $f(\theta') = 0$, so entspricht jeder bestimmten Zahl $\omega = \varphi(\theta)$ des Körpers Ω eine bestimmte Zahl $\omega' = \varphi(\theta')$, und der Inbegriff aller dieser Zahlen ω' bildet einen mit Ω konjugierten Körper Ω'; diese Korrespondenz besitzt die charakteristische Eigenschaft, daß, wenn α, β zwei beliebige Zahlen des Körpers Ω bedeuten, stets

$$(\alpha+\beta)' = \alpha'+\beta', \quad (\alpha-\beta)' = \alpha'-\beta', \quad (\alpha\beta)' = \alpha'\beta', \quad \left(\frac{\alpha}{\beta}\right)' = \frac{\alpha'}{\beta'}$$

ist; die Substitution, durch welche jede Zahl $\omega = \varphi(\theta)$ des Körpers Ω in die korrespondierende oder konjugierte Zahl $\omega' = \varphi(\theta')$ des Körpers Ω' übergeht, heiße eine Permutation des Körpers Ω. Sind $\theta', \theta'' \cdots \theta^{(n)}$ die sämtlichen Wurzeln der obigen irreduktiblen Gleichung, so entspricht einer jeden von ihnen, $\theta^{(r)}$, eine Permutation $P^{(r)}$ des Körpers Ω, durch welche jede in ihm enthaltene Zahl $\omega = \varphi(\theta)$ in die konjugierte Zahl $\omega^{(r)} = \varphi(\theta^{(r)})$ des Körpers $\Omega^{(r)}$ übergeht. Die n mit ω konjugierten Zahlen $\omega', \omega'' \cdots \omega^{(n)}$ sind dann immer die Wurzeln einer Gleichung $n$ten Grades mit rationalen Koeffizienten, welche aber nicht notwendig irreduktibel ist. Das Produkt $\omega'\omega'' \cdots \omega^{(n)}$ aus diesen n Zahlen ist eine rationale Zahl, welche die Norm der Zahl ω heißt und mit $N(\omega)$ bezeichnet wird; sie verschwindet nur dann, wenn $\omega = 0$ ist, und die Norm eines Produkts ist das Produkt aus den Normen der Faktoren. Sind ferner $\alpha_1, \alpha_2 \cdots \alpha_n$ beliebige Zahlen des Körpers, so ist das Quadrat der Determinante

$$\sum \pm \alpha_1' \alpha_2'' \cdots \alpha_n^{(n)},$$

welche aus den n^2 konjugierten Zahlen $\alpha_i^{(i)}$ gebildet ist, ebenfalls eine rationale Zahl, welche die Diskriminante des Systems $\alpha_1, \alpha_2 \cdots \alpha_n$ heißt und mit $\Delta(\alpha_1, \alpha_2 \cdots \alpha_n)$ bezeichnet wird; dieselbe ist stets und nur dann von 0 verschieden, wenn die Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ eine Basis des Körpers Ω bilden; dies ergibt sich leicht aus dem bekannten Satze

$$\Delta(1, \theta, \theta^2 \cdots \theta^{n-1}) = (-1)^{1/2 n(n-1)} N[f'(\theta)],$$

wo $f'(t)$ die Derivierte der Funktion $f(t)$ bedeutet.

Alle algebraischen Zahlen, deren Gesamtheit ebenfalls einen Körper, aber keinen endlichen Körper bildet, zerfallen nun in ganze und in gebrochene Zahlen; eine algebraische Zahl η heißt eine ganze Zahl, wenn sie die Wurzel einer Gleichung von der Form

$$\eta^m + c_1 \eta^{m-1} + c_2 \eta^{m-2} + \cdots + c_{m-1}\eta + c_m = 0$$

ist, wo $c_1, c_2 \cdots c_{m-1}, c_m$ ganze Zahlen im alten Sinne des Wortes bedeuten, die von nun an immer rationale ganze Zahlen genannt werden sollen. Aus dieser Definition, welche wohl die höchste Verallgemeinerung des ursprünglich so beschränkten Begriffes der ganzen Zahl enthält, folgt unmittelbar, daß die Summen, Differenzen und Produkte von je zwei ganzen Zahlen wieder ganze Zahlen sind, und hieran knüpft sich wieder der Begriff der Teilbarkeit der ganzen Zahlen: eine ganze Zahl α heißt teilbar durch eine ganze Zahl β,

oder ein Vielfaches (Multiplum) von β, wenn $\alpha = \beta\gamma$, und γ wieder eine ganze Zahl ist; zugleich heißt γ ein Teiler (Divisor) von α, oder man sagt auch, β gehe in α auf. Eine ganze Zahl ε, welche in der Zahl 1 und folglich auch in allen ganzen Zahlen aufgeht, heißt eine Einheit; zwei ganze Zahlen, deren jede in der anderen aufgeht, und deren Quotient notwendig eine Einheit ist, heißen assoziierte Zahlen*) oder Gefährten.

Kehrt man mit diesen allgemeinen Begriffen zu einem endlichen Körper Ω zurück, und bezeichnet man mit $\mathfrak{o}$ den Inbegriff aller in Ω enthaltenen ganzen Zahlen, zu welchen auch alle ganzen rationalen Zahlen gehören, so ergibt sich ohne Schwierigkeit die Existenz einer aus n ganzen Zahlen $\omega_1, \omega_2 \cdots \omega_n$ bestehenden Basis des Körpers Ω von der Beschaffenheit, daß die Koordinaten $h_1, h_2 \cdots h_n$ einer jeden in $\mathfrak{o}$ enthaltenen Zahl

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n$$

ganze rationale Zahlen sind; die Diskriminante

$$D = \Delta(\omega_1, \omega_2 \cdots \omega_n)$$

eines solchen Systems $\omega_1, \omega_2 \cdots \omega_n$, welches auch eine Basis des Gebietes $\mathfrak{o}$ heißen soll, ist eine ganze rationale, von 0 verschiedene Zahl, die ich ihrer Wichtigkeit wegen die Grundzahl oder die Diskriminante des Körpers Ω nenne und mit $\Delta(\Omega)$ bezeichne. Die Norm einer jeden von 0 verschiedenen Zahl μ des Gebietes $\mathfrak{o}$ ist eine ganze rationale, von 0 verschiedene Zahl, welche die folgende, wichtige Bedeutung besitzt; nennt man zwei ganze Zahlen α, β kongruent oder inkongruent in bezug auf den Modulus μ, je nachdem ihre Differenz $\alpha - \beta$ durch μ teilbar oder nicht teilbar ist, so ist die Anzahl aller in $\mathfrak{o}$ enthaltenen, nach μ inkongruenten Zahlen $= \pm N(\mu)$; die Kongruenz der Zahlen α, β in bezug auf μ wird durch $\alpha \equiv \beta \pmod{\mu}$ bezeichnet. Eine in $\mathfrak{o}$ enthaltene Einheit ist dadurch charakterisiert, daß ihre Norm $= \pm 1$ ist.

Die wichtigste Frage ist aber die nach der Zerlegung einer in $\mathfrak{o}$ enthaltenen Zahl μ in solche Faktoren, welche, wie im folgenden immer stillschweigend vorausgesetzt wird, ebenfalls dem Gebiet $\mathfrak{o}$ angehören. Die Divisoren einer Einheit sind sämtlich selbst Einheiten; ist aber μ keine Einheit, so sind zwei Fälle möglich; ist μ

*) Vgl. Gauß, Theoria residuorum biquadraticorum II, Art. 31.

das Produkt aus zwei Faktoren, von denen keiner eine Einheit, und folglich auch keiner mit μ assoziiert ist, so soll μ eine zerlegbare Zahl heißen; im entgegengesetzten Falle, d. h. wenn jeder Divisor von μ entweder ein Gefährte von μ oder eine Einheit ist, heißt μ unzerlegbar. Aus dem Satze über die Norm eines Produktes folgt nun offenbar, daß jede zerlegbare Zahl stets als Produkt aus einer endlichen Anzahl von unzerlegbaren Faktoren darstellbar ist; während aber in der Theorie der rationalen Zahlen (d. h. im Falle $n = 1$) diese Zerlegung, abgesehen von den Einheitsfaktoren ± 1, eine völlig bestimmte, einzige ist, so tritt bei Körpern höheren Grades sehr häufig die merkwürdige Erscheinung auf, daß eine Zahl μ als Produkt von unzerlegbaren Faktoren auf mehrere Arten darstellbar ist, welche in dem Sinne wesentlich verschieden sind, daß z. B. ein unzerlegbarer Faktor α der einen Darstellung $\mu = \alpha\beta\gamma\cdots$ mit keinem der unzerlegbaren Faktoren $\alpha_1, \beta_1 \cdots$ der anderen Darstellung $\mu = \alpha_1\beta_1\cdots$ assoziiert ist. Es folgt hieraus, daß eine unzerlegbare Zahl durchaus nicht immer den Charakter einer eigentlichen Primzahl besitzt, welcher darin besteht, daß ein Produkt nur dann durch eine Primzahl teilbar ist, wenn diese wenigstens in einem der Faktoren aufgeht. Diese unwillkommene Erscheinung, welche auf den ersten Blick jeden weiteren Fortschritt auf diesem Felde zu verbieten schien, ist aber die Quelle von einer der schönsten und fruchtbarsten Entdeckungen in der höheren Arithmetik geworden: in der Tat ist Kummer bei der Untersuchung solcher Gebiete o, welche aus der Kreisteilung entspringen, dahin gelangt, die Gesetze der Teilbarkeit durch Einführung idealer Zahlen in völligen Einklang mit denjenigen zu bringen, welche in der alten Theorie der rationalen Zahlen herrschen.

Es ist das Ziel meiner langjährigen Bemühungen gewesen, dasselbe Resultat für jeden endlichen Körper Ω zu erreichen, also diejenigen allgemeinen Gesetze der Teilbarkeit festzustellen, welche ohne Ausnahme jedem Gebiete o von der oben beschriebenen Art zukommen. Bei der Begründung dieser Theorie (D. § 163) habe ich den von Kummer eingeschlagenen Weg verlassen und statt der idealen Zahlen einen anderen Begriff, den des Ideals, einführen müssen, welcher von jeder, einem speziellen Körper Ω eigentümlichen Färbung frei ist und gerade deshalb die erforderliche Allgemeinheit besitzt, um als Grundlage der Theorie dienen zu können. Zum Verständnis der nachfolgenden Untersuchungen ist es unerläßlich, an die Hauptsätze dieser Theorie kurz zu erinnern.

1°. Ein System $\mathfrak{m}$ von unendlich vielen Zahlen des Gebietes o heißt ein Ideal, wenn es die beiden folgenden Eigenschaften besitzt:

I. Die Summen und Differenzen von je zwei Zahlen des Systems $\mathfrak{m}$ sind ebenfalls in $\mathfrak{m}$ enthalten.

II. Jedes Produkt aus einer Zahl des Systems $\mathfrak{m}$ und aus einer Zahl des Systems o ist eine Zahl des Systems $\mathfrak{m}$.

Bedeutet μ eine bestimmte, ω jede beliebige Zahl in o, so kommen diese beiden Eigenschaften offenbar dem System $\mathfrak{m}$ aller durch μ teilbaren Zahlen $\mu\omega$ zu; ein solches Ideal $\mathfrak{m}$ heißt ein Hauptideal und wird mit $o(\mu)$ oder kürzer mit $o\mu$ oder μo bezeichnet*); es bleibt ungeändert, wenn μ durch eine mit μ assoziierte Zahl ersetzt wird. Ist μ eine Einheit, so ist $o\mu = o$, und umgekehrt. Da die Kongruenz zweier Zahlen α, β in bezug auf den Modulus μ darin besteht, daß die Differenz $\alpha - \beta$ dem Ideal $o\mu$ angehört, so wird man zu der folgenden allgemeineren Definition der Kongruenz geführt:

2°. Zwei Zahlen α, β heißen kongruent in bezug auf ein Ideal $\mathfrak{m}$, und dies wird durch die Kongruenz $\alpha \equiv \beta \pmod{\mathfrak{m}}$ angedeutet, wenn $\alpha - \beta$ eine Zahl des Ideals $\mathfrak{m}$ ist; im entgegengesetzten Falle heißen α, β inkongruent nach $\mathfrak{m}$. Die immer endliche Anzahl aller in o enthaltenen, in bezug auf $\mathfrak{m}$ inkongruenten Zahlen heißt die Norm des Ideals $\mathfrak{m}$ und wird mit $N(\mathfrak{m})$ bezeichnet; die Norm eines Hauptideals $o\mu$ ist $= \pm N(\mu)$; das Hauptideal o ist das einzige Ideal, dessen Norm $= 1$ ist.

Die Teilbarkeit einer Zahl $\mu = \alpha\beta$ durch eine Zahl α besteht darin, daß alle Zahlen $\mu\omega = \alpha(\beta\omega)$ des Ideals $o\mu$ auch in dem Ideal $o\alpha$ enthalten sind; dies veranlaßt zu der folgenden Definition der Teilbarkeit der Ideale:

3°. Ein Ideal $\mathfrak{m}$ heißt teilbar durch ein Ideal $\mathfrak{a}$ oder ein Vielfaches von $\mathfrak{a}$, wenn alle Zahlen des Ideals $\mathfrak{m}$ auch dem Ideal $\mathfrak{a}$ angehören; zugleich heißt $\mathfrak{a}$ ein Teiler von $\mathfrak{m}$, oder man sagt auch, $\mathfrak{a}$ gehe in $\mathfrak{m}$ auf.

*) Früher habe ich die weniger zweckmäßige Bezeichnung $i(\mu)$ angewendet (D. § 163).

Da hiernach die Teilbarkeit der Zahlen nur einen speziellen Fall von der Teilbarkeit der Ideale bildet, so kommt es lediglich darauf an, die tatsächlich einfacheren Gesetze der letzteren festzustellen. Dies geschieht durch die folgenden Begriffe und Sätze:

4°. Ist das Ideal $\mathfrak{m}$ teilbar durch das Ideal $\mathfrak{a}$, und letzteres teilbar durch das Ideal $\mathfrak{b}$, so ist auch $\mathfrak{m}$ teilbar durch $\mathfrak{b}$.

5°. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Ideale, so bildet das System $\mathfrak{m}$ aller den Idealen $\mathfrak{a}$, $\mathfrak{b}$ gemeinschaftlich angehörenden Zahlen ein Ideal, welches das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$, $\mathfrak{b}$ heißt, weil es in jedem gemeinschaftlichen Vielfachen von $\mathfrak{a}$, $\mathfrak{b}$ aufgeht.

6°. Durchläuft α alle Zahlen eines Ideals $\mathfrak{a}$, ebenso β alle Zahlen eines Ideals $\mathfrak{b}$, so bildet das System $\mathfrak{d}$ aller in der Form $\alpha + \beta$ darstellbaren Zahlen ein Ideal, welches der größte gemeinschaftliche Teiler von $\mathfrak{a}$, $\mathfrak{b}$ heißt, weil jeder gemeinschaftliche Teiler von $\mathfrak{a}$, $\mathfrak{b}$ in dem Ideal $\mathfrak{d}$ aufgeht.

7°. Zwei Ideale, deren größter gemeinschaftlicher Teiler das Ideal $\mathfrak{o}$ ist, heißen relative Primideale.

8°. Ein von $\mathfrak{o}$ verschiedenes Ideal $\mathfrak{p}$ heißt ein Primideal, wenn es kein von $\mathfrak{o}$ und $\mathfrak{p}$ verschiedenes Ideal zum Teiler hat; im entgegengesetzten Falle heißt $\mathfrak{p}$ ein zusammengesetztes Ideal.

9°. Durchläuft α alle Zahlen eines Ideals $\mathfrak{a}$, ebenso β alle Zahlen eines Ideals $\mathfrak{b}$, so bilden die sämtlichen Produkte $\alpha\beta$ und alle Summen von solchen Produkten ein durch $\mathfrak{a}$ und durch $\mathfrak{b}$ teilbares Ideal, welches das Produkt aus den Faktoren $\mathfrak{a}$ und $\mathfrak{b}$ heißt und mit $\mathfrak{ab} = \mathfrak{ba}$ bezeichnet wird; zugleich ist $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. Die Ausdehnung dieses Begriffes auf beliebig viele Faktoren und die Bedeutung einer Potenz ist selbstverständlich.

10°. Umgekehrt: ist das Ideal $\mathfrak{m}$ teilbar durch das Ideal $\mathfrak{a}$, so gibt es ein und nur ein Ideal $\mathfrak{b}$ von der Art, daß $\mathfrak{ab} = \mathfrak{m}$ wird.

11°. Ein Produkt von Idealen ist nur dann durch ein Primideal teilbar, wenn dieses wenigstens in einem der Faktoren aufgeht.

12°. Jedes zusammengesetzte Ideal ist als Produkt von lauter Primidealen darstellbar, und zwar nur auf eine einzige Weise.

13°. Damit ein Ideal $\mathfrak{m}$ durch ein Ideal $\mathfrak{a}$ teilbar sei, ist erforderlich und hinreichend, daß alle in $\mathfrak{a}$ aufgehenden Potenzen von Primidealen auch in $\mathfrak{m}$ aufgehen.

14°. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Ideale, so gibt es ein durch $\mathfrak{a}$ teilbares Hauptideal $\mathfrak{am}$ von der Art, daß $\mathfrak{m}$ und $\mathfrak{b}$ relative Primideale werden.

Für den Fall $n = 1$, in welchem alle Ideale Hauptideale sind, gehen die vorstehenden Sätze, deren strenge Beweise mir erst nach Überwindung von erheblichen Schwierigkeiten gelungen sind, in die Fundamentalsätze über die Teilbarkeit der ganzen rationalen Zahlen über. Dieselben Gesetze gelten daher auch für jeden Körper Ω von beliebigem Grade n, sobald alle seine Ideale Hauptideale sind, und für einen solchen Körper ist offenbar die Einführung der Ideale gänzlich überflüssig. Dies ist aber, wie schon oben bemerkt, im allgemeinen keineswegs der Fall, und hieran knüpft sich die Einteilung aller Ideale eines Körpers Ω in bestimmte Ideal-Klassen (D. § 164). Zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ heißen äquivalent, wenn es ein Ideal $\mathfrak{c}$ gibt, für welches beide Produkte $\mathfrak{ac}$, $\mathfrak{bc}$ Hauptideale werden; da aus dieser Definition unmittelbar folgt, daß zwei mit einem dritten äquivalente Ideale auch miteinander äquivalent sind, so bildet das System A aller Ideale, welche einem bestimmten Ideal $\mathfrak{a}$ äquivalent sind, eine Klasse, welche ungeändert bleibt, wenn ihr Repräsentant $\mathfrak{a}$ durch ein beliebiges, derselben Klasse A angehörendes Ideal ersetzt wird. Die Anzahl h dieser Klassen ist immer eine endliche; wählt man aus jeder Klasse nach Belieben ein bestimmtes Ideal als Repräsentanten, so ist jedes Ideal mit einem und nur mit einem dieser h Ideale äquivalent. Das System aller Hauptideale bildet die Hauptklasse O; zu jeder Klasse A von Idealen $\mathfrak{a}$ gehört eine bestimmte entgegengesetzte oder reziproke, inverse Klasse A^{-1}, welche aus allen denjenigen Idealen besteht, die durch Multiplikation mit den Idealen $\mathfrak{a}$ in Hauptideale verwandelt werden. Durchläuft nun $\mathfrak{a}$ alle Ideale einer Klasse A, ebenso $\mathfrak{b}$ alle Ideale einer Klasse B, so gehören die sämtlichen Produkte $\mathfrak{ab}$ ein und derselben Klasse an, welche die aus A und B zusammengesetzte Klasse oder das Produkt aus A, B heißt und mit AB bezeichnet wird; diese Komposition oder Multiplikation der Ideal-Klassen gehorcht den Gesetzen $AB = BA$, $(AB)C = A(BC)$, $OA = A$, $AA^{-1} = O$, $A^r A^s = A^{r+s}$, $A^h = O$, und aus $AB = AC$ folgt $B = C$.

Aus dem Satze $A^h = O$ folgt beiläufig, wenn man von dem endlichen Körper Ω wieder zu dem Gebiete aller ganzen algebraischen Zahlen übergeht, das wichtige Resultat, daß je zwei ganze Zahlen

α, β, die nicht beide verschwinden, einen größten gemeinschaftlichen Divisor δ besitzen, welcher in der Form $\delta = \alpha\alpha_1 + \beta\beta_1$ darstellbar ist, wo α_1, β_1 ebenfalls ganze Zahlen bedeuten; natürlich kann auch hier δ durch jeden Gefährten von δ ersetzt werden.

Das größte Interesse nimmt aber die Bestimmung der Klassen-Anzahl h in Anspruch (D. § 167). Die Übertragung der Prinzipien, welche Dirichlet bei dem Beweise des Satzes über die arithmetische Progression und bei der Bestimmung der Klassen-Anzahl der binären quadratischen Formen geschaffen hat, führt zu der Betrachtung unendlicher Reihen und Produkte von der Form

$$\sum f(\mathfrak{a}) = \prod \frac{1}{1 - f(\mathfrak{p})},$$

wo $\mathfrak{a}$ alle Ideale, $\mathfrak{p}$ alle Primideale durchläuft, und $f(\mathfrak{a})$ eine reelle oder komplexe Funktion bedeutet, die der Bedingung $f(\mathfrak{ab}) = f(\mathfrak{a})f(\mathfrak{b})$ genügt und außerdem so beschaffen ist, daß die unendliche Reihe linker Hand eine von der Anordnung ihrer Glieder unabhängige endliche Summe besitzt. Diese Bedingungen sind erfüllt, wenn man

$$f(\mathfrak{a}) = \frac{1}{N(\mathfrak{a})^s}, \quad s > 1$$

nimmt; multipliziert man mit $(s-1)$ und teilt die Totalsumme in h Partialsummen, deren jede einer bestimmten Klasse von Idealen $\mathfrak{a}$ entspricht, so nähern sich diese Summen für unendlich kleine positive Werte von $(s-1)$ einem gemeinschaftlichen, endlichen, von 0 verschiedenen Grenzwert g, der sich nach den fundamentalen Untersuchungen Dirichlets über die Einheiten ohne Schwierigkeit bestimmen läßt, und man erhält folglich

$$gh = \lim \sum \frac{s-1}{N(\mathfrak{a})^s} = \lim (s-1) \prod \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}}.$$

Das Problem der Klassen-Anzahl wird daher gelöst sein, sobald es gelingt, den Grenzwert der unendlichen Reihe oder des mit ihr identischen Produkts noch auf eine zweite Art, nämlich unmittelbar aus der Natur der sämtlichen, dem Körper Ω angehörenden Primideale $\mathfrak{p}$ zu bestimmen. Dies ist bis jetzt nur für Kreisteilungskörper geglückt (zu welchen auch alle quadratischen Körper gehören), und eine aufmerksame Betrachtung dieser Fälle führt zu der

Überzeugung — in welcher ich durch meine demnächst zu veröffentlichenden Untersuchungen über die Anzahl der Ideal-Klassen in kubischen Körpern bestärkt werde —, daß die allgemeine Lösung des Problems der Klassen-Anzahl auf diesem Wege erst dann gelingen wird, wenn die algebraische Konstitution eines jeden Körpers und ihr Zusammenhang mit seinen Idealen uns vollständig bekannt sein wird — ein Ziel, von welchem wir noch außerordentlich weit entfernt sind; außerdem scheint auch eine viel genauere Ausbildung der Theorie der transzendenten Funktionen erforderlich zu sein.

Es ist nun noch mit einigen Worten die Beziehung zwischen den Idealen eines Körpers und den zugehörigen zerlegbaren Formen zu besprechen (D. § 165). Ist $\mathfrak{a}$ ein bestimmtes Ideal, so gibt es immer n partikuläre, in $\mathfrak{a}$ enthaltene Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ von der Beschaffenheit, daß die sämtlichen Zahlen α des Ideals $\mathfrak{a}$ durch den Ausdruck

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$

dargestellt werden, wenn die Variabelen $x_1, x_2 \cdots x_n$ alle ganzen rationalen Zahlen durchlaufen. Das System der Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ heißt eine Basis von $\mathfrak{a}$. Bildet man das Produkt aus allen n mit α konjugierten Ausdrücken, so erhält man

$$N(\alpha) = N(\mathfrak{a})X,$$

wo X eine homogene Funktion $n$ten Grades von den Variabelen $x_1, x_2 \cdots x_n$ bedeutet; die Koeffizienten dieser zerlegbaren Form X sind immer ganze rationale Zahlen ohne gemeinschaftlichen Teiler. Da das Ideal $\mathfrak{a}$ unendlich viele verschiedene Basen besitzt, so entspricht demselben eine Klasse von unendlich vielen äquivalenten Formen X, welche durch lineare Substitutionen mit ganzen rationalen Koeffizienten gegenseitig ineinander übergehen. Dieselben Formen entspringen aber auch aus jedem mit $\mathfrak{a}$ äquivalenten Ideal, und folglich entspricht jeder Ideal-Klasse eine bestimmte Formen-Klasse. Die Multiplikation der Ideale und der Ideal-Klassen führt zu der Komposition der Formen und der Formen-Klassen.

Aber diese Formen X umfassen nur einen unendlich kleinen Teil aller möglichen zu dem Körper Ω gehörenden Formen. Versteht man nämlich unter der Determinante einer aus n homogenen linearen Faktoren $f_1, f_2 \cdots f_n$ gebildeten Funktion F von

n Variabelen $h_1, h_2 \cdots h_n$ das Quadrat der Funktional-Determinante

$$\sum \pm \frac{\partial f_1}{\partial h_1} \frac{\partial f_2}{\partial h_2} \cdots \frac{\partial f_n}{\partial h_n},$$

so ergibt sich leicht, daß die Determinante aller oben betrachteten Formen X mit der Grundzahl $D = \Delta(\Omega)$ des Körpers Ω übereinstimmt; für den Fall $n = 2$ würde man z. B. nur zu solchen binären Formen $ax^2 + bxy + cy^2$ gelangen, deren Determinante $b^2 - 4ac = D$ durch kein ungerades Quadrat teilbar und entweder $\equiv 1 \pmod 4$, oder $\equiv 8, 12 \pmod{16}$ ist*).

Um nun eine allgemeinere Theorie der zu einem Körper Ω gehörenden Formen aufzustellen, muß man, wie ich schon früher bemerkt habe (D. § 165), den Begriff des Ideals so erweitern, daß an Stelle des bisher betrachteten Gebietes $\mathfrak{o}$, welches alle ganzen Zahlen des Körpers umfaßt, beschränktere Gebiete $\mathfrak{o}'$ treten, welche ich mit Rücksicht auf die in der Theorie der binären quadratischen Formen von Gauß gebrauchte Ausdrucksweise Ordnungen genannt habe. Diese Erweiterung bildet den nächsten Gegenstand dieser Abhandlung.

§ 2.

Sätze aus der Theorie der Moduln.

Um hierzu zu gelangen, und namentlich um beständige Wiederholungen über die Art zu vermeiden, in welcher aus gewissen Systemen von Zahlen neue Systeme gebildet werden, ist es notwendig, hier einige sehr einfache und zugleich sehr allgemeine Sätze über solche Systeme einzuschalten, die ich Moduln genannt habe (D. § 161). Da der Begriff eines Ideals in demjenigen eines Moduls als spezieller Fall enthalten ist, so wird bei einer systematischen Darstellung die Theorie der Moduln zweckmäßig der Theorie der Ideale vorausgeschickt werden. Hier wird es genügen, einige Hauptbegriffe zu entwickeln und einige Sätze anzuführen, deren Beweise ich unterdrücke, weil jeder sie leicht finden wird (vgl. D. § 161 und B. §§ 1 bis 4). Da manche dieser Sätze sich in Worten nur ziemlich umständlich aussprechen lassen, so wage ich es, die Ausdrucksweise durch Einführung einer Zeichensprache abzukürzen, und ich hoffe, daß man aus diesem Grunde die Benutzung der Zeichen $>$, $<$, $+$, $-$ entschuldigen wird. Ich bemerke nur noch, daß im folgenden die Einschränkung auf die Zahlen eines endlichen Körpers gänzlich wegfällt, also das Wort Zahl immer in seiner allgemeinsten Bedeutung gebraucht wird.

*) Die obige Erklärung einer Formen-Determinante stimmt für den Fall $n = 2$ nicht ganz mit derjenigen von Gauß überein; dies läßt sich aber kaum vermeiden, wenn sie allgemein für jeden Grad n gelten soll, und selbst in dem speziellen Falle $n = 2$ sprechen viele Erscheinungen zugunsten derselben, was ich aber hier nicht näher begründen kann.

1°. Ein System $\mathfrak{m}$ von reellen oder komplexen Zahlen heißt ein Modul, wenn alle Summen und Differenzen dieser Zahlen demselben System $\mathfrak{m}$ angehören. Die Zahl 0 findet sich in jedem Modul, und sie bildet auch für sich allein einen Modul. Ein Modul $\mathfrak{m}$ heißt teilbar durch einen Modul $\mathfrak{a}$ oder ein Vielfaches von $\mathfrak{a}$, wenn alle Zahlen des Moduls $\mathfrak{m}$ auch in $\mathfrak{a}$ enthalten sind; zugleich heißt $\mathfrak{a}$ ein Teiler von $\mathfrak{m}$, und wir bezeichnen die Teilbarkeit von $\mathfrak{m}$ durch $\mathfrak{a}$ sowohl durch $\mathfrak{m} > \mathfrak{a}$, als durch $\mathfrak{a} < \mathfrak{m}$. Ist jeder der beiden Moduln $\mathfrak{m}$, $\mathfrak{a}$ durch den anderen teilbar, so sind sie identisch, was durch $\mathfrak{m} = \mathfrak{a}$ angedeutet wird. Aus $\mathfrak{m} > \mathfrak{a}$, $\mathfrak{a} > \mathfrak{b}$ folgt $\mathfrak{m} > \mathfrak{b}$. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Moduln, so ist das System aller derjenigen Zahlen, welche beiden Moduln gemeinschaftlich angehören, selbst ein Modul, und zwar ein Vielfaches von $\mathfrak{a}$ und von $\mathfrak{b}$, welches durch $\mathfrak{a} - \mathfrak{b} = \mathfrak{b} - \mathfrak{a}$ bezeichnet werden soll; dasselbe heißt das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$, $\mathfrak{b}$, weil jedes gemeinschaftliche Vielfache von $\mathfrak{a}$, $\mathfrak{b}$ durch $\mathfrak{a} - \mathfrak{b}$ teilbar ist. Durchläuft α alle Zahlen eines Moduls $\mathfrak{a}$, ebenso β alle Zahlen eines Moduls $\mathfrak{b}$, so ist das System aller Zahlen von der Form $\alpha + \beta$ ein Modul, und zwar ein Teiler von $\mathfrak{a}$ und von $\mathfrak{b}$, der mit $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$ bezeichnet werden soll; derselbe heißt der größte gemeinschaftliche Teiler von $\mathfrak{a}$, $\mathfrak{b}$, weil jeder gemeinschaftliche Teiler von $\mathfrak{a}$, $\mathfrak{b}$ auch ein Teiler von $\mathfrak{a} + \mathfrak{b}$ ist. Diese Begriffe lassen sich leicht auf beliebig viele, sogar auf unendlich viele Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c} \cdots$ ausdehnen, und man beweist leicht die beiden folgenden charakteristischen Sätze

$$(\mathfrak{a} + \mathfrak{b}) - (\mathfrak{a} + \mathfrak{c}) = \mathfrak{a} + (\mathfrak{b} - (\mathfrak{a} + \mathfrak{c})),$$
$$(\mathfrak{a} - \mathfrak{b}) + (\mathfrak{a} - \mathfrak{c}) = \mathfrak{a} - (\mathfrak{b} + (\mathfrak{a} - \mathfrak{c})),$$

in welchen sich der zwischen den Begriffen des kleinsten gemeinschaftlichen Vielfachen und des größten gemeinschaftlichen Teilers durchgängig herrschende Dualismus kundgibt.

2°. Zwei Zahlen α, β heißen kongruent oder inkongruent in bezug auf einen Modul $\mathfrak{m}$, je nachdem ihre Differenz $\alpha - \beta$ in $\mathfrak{m}$ enthalten ist oder nicht; die Kongruenz wird durch $\alpha \equiv \beta \pmod{\mathfrak{m}}$ ausgedrückt. Alle mit einer bestimmten Zahl nach $\mathfrak{m}$ kongruenten Zahlen bilden eine Zahl-Klasse (mod. $\mathfrak{m}$). Mehrere Zahlen heißen inkongruent (mod. $\mathfrak{m}$), wenn jede derselben mit jeder der übrigen inkongruent (mod. $\mathfrak{m}$) ist. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Moduln, so kann es sein, daß $\mathfrak{a}$ nur eine endliche Anzahl inkongruenter Zahlen in bezug auf $\mathfrak{b}$ enthält, und dann soll diese Anzahl durch das Symbol $(\mathfrak{a}, \mathfrak{b})$ bezeichnet werden; gibt es aber in $\mathfrak{a}$ unendlich viele, in bezug auf $\mathfrak{b}$ inkongruente Zahlen, so soll $(\mathfrak{a}, \mathfrak{b}) = 0$ gesetzt werden, weil dann gewisse Determinanten-Sätze allgemein gültig bleiben. In beiden Fällen ist

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{a} - \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b}, \mathfrak{b});$$

ist $\mathfrak{a} > \mathfrak{b}$, so ist $(\mathfrak{a}, \mathfrak{b}) = 1$, und umgekehrt. Ist ferner $\mathfrak{m} > \mathfrak{a} > \mathfrak{b}$, so ist

$$(\mathfrak{b}, \mathfrak{m}) = (\mathfrak{b}, \mathfrak{a})(\mathfrak{a}, \mathfrak{m}).$$

Durch Kombination beider Sätze erhält man viele andere Sätze, die hier übergangen werden können. Sind ϱ, σ zwei gegebene Zahlen, so hat das System der beiden Kongruenzen

$$\omega \equiv \varrho \pmod{\mathfrak{a}}, \quad \omega \equiv \sigma \pmod{\mathfrak{b}}$$

stets und nur dann gemeinschaftliche Wurzeln ω, wenn

$$\varrho \equiv \sigma \pmod{\mathfrak{a} + \mathfrak{b}}$$

ist, und die sämtlichen Zahlen ω bilden eine bestimmte Zahlklasse (mod. $\mathfrak{a} - \mathfrak{b}$).

3°. Sind $\alpha_1, \alpha_2 \cdots \alpha_n$ Konstanten, während $x_1, x_2 \cdots x_n$ alle ganzen rationalen Zahlen durchlaufen, so bilden die sämtlichen, in der Form

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$

darstellbaren Zahlen α einen Modul $\mathfrak{a}$, der ein endlicher Modul heißen und mit $[\alpha_1, \alpha_2 \cdots \alpha_n]$ bezeichnet werden soll; die Konstanten $\alpha_1, \alpha_2 \cdots \alpha_n$ bilden eine Basis des Moduls $\mathfrak{a}$. Der Modul [1] ist das System aller ganzen rationalen Zahlen. Wenn alle Zahlen eines solchen endlichen Moduls $\mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_n]$ durch Multiplikation mit rationalen, von 0 verschiedenen Zahlen in Zahlen eines Moduls $\mathfrak{b}$ verwandelt werden können, so ist $(\mathfrak{a}, \mathfrak{b})$ von 0 verschieden, und $\mathfrak{a} - \mathfrak{b}$

ist ein endlicher Modul; man kann die ganzen rationalen Zahlen a so wählen, daß die n Zahlen

$$\begin{aligned}
\mu_1 &= a_1'\alpha_1, \\
\mu_2 &= a_1''\alpha_1 + a_2''\alpha_2, \\
\mu_3 &= a_1'''\alpha_1 + a_3'''\alpha_2 + a_3'''\alpha_3, \\
&\cdots\cdots\cdots\cdots \\
\mu_n &= a_1^{(n)}\alpha_1 + a_2^{(n)}\alpha_2 + a_3^{(n)}\alpha_3 + \cdots + a_n^{(n)}\alpha_n
\end{aligned}$$

eine Basis von $\mathfrak{a} - \mathfrak{b}$ bilden, und daß zugleich

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{a} - \mathfrak{b}) = a_1'a_2''a_3''' \cdots a_n^{(n)}$$

wird; unterwirft man die n ganzen rationalen Zahlen $x_1', x_2' \cdots x_n'$ den n Bedingungen

$$0 \leqq x_r' < a_r^{(r)},$$

so sind die entsprechenden, in $\mathfrak{a}$ enthaltenen Zahlen

$$\alpha' = x_1'\alpha_1 + x_2'\alpha_2 + \cdots + x_n'\alpha_n,$$

deren Anzahl $= (\mathfrak{a}, \mathfrak{b})$ ist, sämtlich inkongruent (mod. $\mathfrak{b}$) und deshalb auch inkongruent (mod. $\mathfrak{a} - \mathfrak{b}$).

4°. Ein System von n Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ soll ein irreduktibeles System, und diese Zahlen sollen voneinander unabhängig heißen, wenn die Summe

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$

für jedes System von rationalen, nicht sämtlich verschwindenden Zahlen $x_1, x_2 \cdots x_n$ einen von 0 verschiedenen Wert erhält. Ist nun wieder $\mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_n]$, und sind die Basiszahlen eines Moduls $\mathfrak{m} = [\mu_1, \mu_2 \cdots \mu_n]$ von der Form

$$\begin{aligned}
\mu_1 &= a_1'\alpha_1 + a_2'\alpha_2 + \cdots + a_n'\alpha_n, \\
\mu_2 &= a_1''\alpha_1 + a_2''\alpha_2 + \cdots + a_n''\alpha_n, \\
&\cdots\cdots\cdots\cdots \\
\mu_n &= a_1^{(n)}\alpha_1 + a_2^{(n)}\alpha_2 + \cdots + a_n^{(n)}\alpha_n,
\end{aligned}$$

wo die Koeffizienten a ganze rationale Zahlen bedeuten, so ist

$$(\mathfrak{a}, \mathfrak{m}) = \pm \sum \pm a_1'a_2'' \cdots a_n^{(n)}.$$

Von besonderer Wichtigkeit ist noch der folgende Satz: besteht eine Basis eines endlichen Moduls $\mathfrak{a}$ aus m Zahlen $\alpha_1', \alpha_2' \cdots \alpha_m'$, von denen aber nur n voneinander unabhängig sind, so gibt es immer eine aus n unabhängigen Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ bestehende Basis desselben Moduls $\mathfrak{a}$.

5°. Durchläuft α alle Zahlen eines Moduls $\mathfrak{a}$, ebenso β alle Zahlen eines Moduls $\mathfrak{b}$, so bilden die Produkte $\alpha\beta$ und alle Summen solcher Produkte einen Modul, der das Produkt aus den Faktoren $\mathfrak{a}$, $\mathfrak{b}$ heißen und mit $\mathfrak{ab}$ bezeichnet werden soll, aber keineswegs durch $\mathfrak{a}$ oder $\mathfrak{b}$ teilbar zu sein braucht. Offenbar ist $\mathfrak{ab} = \mathfrak{ba}$ und $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc}) = \mathfrak{abc}$; die Bedeutung einer Potenz $\mathfrak{a}^r$ ist selbstverständlich. Aus $\mathfrak{a}' > \mathfrak{a}$ und $\mathfrak{b}' > \mathfrak{b}$ folgt $\mathfrak{a}'\mathfrak{b}' > \mathfrak{ab}$; ferner ist

$$(\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{ac} + \mathfrak{bc},$$
$$(\mathfrak{a} - \mathfrak{b})\mathfrak{c} > \mathfrak{ac} - \mathfrak{bc},$$
$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} - \mathfrak{b}) > \mathfrak{ab};$$

ist ferner $[1] > \mathfrak{o}$, so ist $\mathfrak{a} > \mathfrak{oa}$, weil $\mathfrak{a}[1] = \mathfrak{a}$ ist. Ist $\mathfrak{b}$ ein eingliedriger Modul $[\mu]$, so besteht das Produkt $\mathfrak{ab}$ aus den Produkten $\alpha\mu$, wo α alle Zahlen des Moduls $\mathfrak{a}$ durchläuft; ein solches Produkt $\mathfrak{a}[\mu]$ soll bequemer durch $\mathfrak{a}\mu = \mu\mathfrak{a}$ bezeichnet werden; dann ist $(\mathfrak{a}\mu)\nu = \mathfrak{a}(\mu\nu)$, und aus $\mathfrak{a}\mu = \mathfrak{a}'\mu$ folgt immer $\mathfrak{a} = \mathfrak{a}'$, wenn μ von 0 verschieden ist.

6°. Ist $\mathfrak{a}$ ein beliebiger Modul, so bildet das System $\mathfrak{o}$ aller derjenigen Zahlen ω, für welche das Produkt $\mathfrak{a}\omega > \mathfrak{a}$ wird, einen Modul, welcher die Ordnung des Moduls $\mathfrak{a}$ heißen soll und offenbar stets ein Teiler des Moduls $[1]$ ist; hieraus folgt unmittelbar, daß $\mathfrak{ao} = \mathfrak{a}$, und $\mathfrak{o}^2 = \mathfrak{o}$ ist. Umgekehrt ist jeder Modul $\mathfrak{o}$, der ein Teiler von $[1]$ und von $\mathfrak{o}^2$ ist, eine Ordnung, nämlich diejenige des Moduls $\mathfrak{o}$ selbst. Der Begriff einer Ordnung bildet eigentlich nur einen speziellen Fall des Begriffes des Quotienten $\mathfrak{a} : \mathfrak{b}$ von zwei beliebigen Moduln $\mathfrak{a}$, $\mathfrak{b}$, worunter der größte gemeinschaftliche Teiler aller derjenigen Moduln $\mathfrak{c}$ zu verstehen ist, für welche das Produkt $\mathfrak{bc}$ durch $\mathfrak{a}$ teilbar wird; die Ordnung $\mathfrak{o}$ eines Moduls $\mathfrak{a}$ ist nämlich identisch mit dem Quotienten $\mathfrak{a} : \mathfrak{a}$, und die charakteristische Eigenschaft einer jeden Ordnung $\mathfrak{o}$ wird durch die Gleichung $\mathfrak{o} : \mathfrak{o} = \mathfrak{o}$ ausgedrückt. Doch wird von dem Begriff des Quotienten in dieser Abhandlung kein Gebrauch gemacht werden.

§ 3.

Ordnungen in einem endlichen Körper.

Nach diesen allgemeinen Vorbereitungen kehren wir definitiv zu den Zahlen eines endlichen Körpers Ω vom Grade n zurück, und beschränken zunächst den Begriff des Moduls in der Weise, daß unter einem Modul $\mathfrak{a}$ stets ein endlicher Modul $[\alpha_1, \alpha_2 \cdots \alpha_n]$ verstanden

wird, dessen Basiszahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ zugleich eine Basis des Körpers Ω bilden (§ 1) und folglich voneinander unabhängig sind (§ 2, 4°). Da hiernach jede Zahl des Körpers Ω durch Multiplikation mit einer rationalen, von 0 verschiedenen Zahl in eine Zahl des Moduls $\mathfrak{a}$ verwandelt werden kann, so ergibt sich aus den vorhergehenden allgemeinen Sätzen sehr leicht, daß das kleinste gemeinschaftliche Vielfache, der größte gemeinschaftliche Teiler, und ebenso das Produkt (und auch der Quotient) von je zwei solchen Moduln $\mathfrak{a}$, $\mathfrak{b}$ stets wieder ein solcher Modul, und daß $(\mathfrak{a}, \mathfrak{b})$ stets von 0 verschieden ist. Versteht man ferner wie früher, und wie es auch in der Folge stets geschehen soll, unter $\mathfrak{o}$ das Gebiet aller ganzen Zahlen des Körpers Ω, so kommt die Definition eines Ideals $\mathfrak{m}$ (§ 1, 1°) darauf hinaus, daß $\mathfrak{m}$ ein durch $\mathfrak{o}$ teilbarer Modul ist (I), welcher der Bedingung $\mathfrak{om} = \mathfrak{m}$ genügt (II); die dortigen Sätze 5°, 6°, 9° enthalten nur noch die Behauptung, daß das kleinste gemeinschaftliche Vielfache, der größte gemeinschaftliche Teiler und das Produkt von zwei beliebigen Idealen wieder Ideale sind; die Norm eines Ideals $\mathfrak{m}$ ist $= (\mathfrak{o}, \mathfrak{m})$.

Für die in Aussicht genommene Erweiterung des Ideal-Begriffs ist nun vor allem die Konstitution der Ordnung $\mathfrak{o}'$ eines beliebigen Moduls $\mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_n]$ von Wichtigkeit (§ 2, 6°). Damit eine Zahl ω' der Ordnung $\mathfrak{o}'$ des Moduls $\mathfrak{a}$ angehöre, ist offenbar erforderlich und hinreichend, daß die n Produkte $\omega'\alpha_1, \omega'\alpha_2 \cdots \omega'\alpha_n$ in $\mathfrak{a}$ enthalten sind, daß also

$$\begin{aligned}
\omega'\alpha_1 &= x_1'\alpha_1 + x_2'\alpha_2 + \cdots + x_n'\alpha_n,\\
\omega'\alpha_2 &= x_1''\alpha_1 + x_2''\alpha_2 + \cdots + x_n''\alpha_n,\\
&\cdots\cdots\cdots\cdots\cdots\\
\omega'\alpha_n &= x_1^{(n)}\alpha_1 + x_2^{(n)}\alpha_2 + \cdots + x_n^{(n)}\alpha_n
\end{aligned}$$

ist, wo die n^2 Koeffizienten x sämtlich ganze rationale Zahlen bedeuten. Aus jeder einzelnen dieser Gleichungen folgt zunächst, daß ω' eine Zahl des Körpers Ω ist, und wenn man die n Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$ eliminiert, so erhält man

$$\begin{vmatrix}
x_1' - \omega', & x_2' & \cdots & x_n'\\
x_1'' & , & x_2'' - \omega' & \cdots & x_n''\\
\cdots & \cdots & \cdots & \cdots & \cdots\\
x_1^{(n)} & , & x_2^{(n)} & \cdots & x_n^{(n)} - \omega'
\end{vmatrix} = 0,$$

d. h. ω' ist eine ganze algebraische Zahl, also in dem Gebiete $\mathfrak{o}$ enthalten; mithin ist $\mathfrak{o}'$ ein Vielfaches von $\mathfrak{o}$. Versteht man jetzt für

einen Augenblick unter ω' eine beliebige Zahl des Körpers Ω, so gehören auch die n Produkte $\omega'\alpha_1$, $\omega'\alpha_2 \cdots \omega'\alpha_n$ dem Körper Ω an, und folglich werden, da $\alpha_1, \alpha_2 \cdots \alpha_n$ eine Basis des Körpers Ω bilden, wieder n Gleichungen von der obigen Form stattfinden, in welchen aber die n^2 rationalen Koeffizienten x nicht mehr notwendig ganze Zahlen sind; es wird dann immer eine von 0 verschiedene, rationale Zahl m von der Art geben, daß die sämtlichen n^2 Produkte mx ganze Zahlen werden, und folglich wird das Produkt $m\omega'$ eine Zahl der Ordnung $\mathfrak{o}'$ sein; jede Zahl des Körpers Ω, also auch jede Zahl des Gebietes $\mathfrak{o}$ kann daher durch Multiplikation mit einer von 0 verschiedenen rationalen Zahl in eine Zahl der Ordnung $\mathfrak{o}'$ verwandelt werden, und da das Gebiet $\mathfrak{o} = [\omega_1, \omega_2 \cdots \omega_n]$ ein Teiler von $\mathfrak{o}'$ ist, so ist (nach § 2, 3⁰) $\mathfrak{o}'$ ein endlicher Modul $[\omega_1', \omega_2' \cdots \omega_n']$, dessen Basiszahlen mit denen von $\mathfrak{o}$ durch n Gleichungen von der Form

$$\begin{aligned}
\omega_1' &= k_1'\omega_1 + k_2'\omega_2 + \cdots + k_n'\omega_n,\\
\omega_2' &= k_1''\omega_1 + k_2''\omega_2 + \cdots + k_n''\omega_n,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\omega_n' &= k_1^{(n)}\omega_1 + k_2^{(n)}\omega_2 + \cdots + k_n^{(n)}\omega_n
\end{aligned}$$

verbunden sind, deren Koeffizienten ganze rationale Zahlen sind und eine von 0 verschiedene, positive Determinante

$$\sum \pm k_1' k_2'' \cdots k_n^{(n)} = (\mathfrak{o}, \mathfrak{o}') = k$$

besitzen. Die charakteristischen Eigenschaften einer solchen Ordnung $\mathfrak{o}'$ sind daher (§ 2, 6⁰) die folgenden:

1⁰. $\mathfrak{o}'$ ist ein durch $\mathfrak{o}$ teilbarer Modul im obigen beschränkten Sinne des Wortes; alle in $\mathfrak{o}'$ enthaltenen Zahlen sind ganze Zahlen des Körpers Ω.

2⁰. $\mathfrak{o}'$ ist ein Teiler von [1], d. h. alle ganzen rationalen Zahlen sind in $\mathfrak{o}'$ enthalten.

3⁰. $\mathfrak{o}'$ ist ein Teiler von $\mathfrak{o}'^2$, d. h. jedes Produkt von zwei in $\mathfrak{o}'$ enthaltenen Zahlen gehört ebenfalls dem System $\mathfrak{o}'$ an. Aus 2⁰ folgt dann $\mathfrak{o}'^2 = \mathfrak{o}'$.

Aus den obigen Gleichungen folgt nun durch Umkehrung, daß die n Produkte $k\omega_1$, $k\omega_2 \cdots k\omega_n$ der Ordnung $\mathfrak{o}'$ angehören, und folglich ist das Hauptideal $\mathfrak{o}k$ teilbar durch $\mathfrak{o}'$. Da ferner der größte gemeinschaftliche Teiler von je zwei durch $\mathfrak{o}'$ teilbaren Idealen selbst wieder ein durch $\mathfrak{o}'$ teilbares Ideal ist, so gibt es unter diesen, durch

$\mathfrak{o}'$ teilbaren Idealen ein einziges, völlig bestimmtes Ideal $\mathfrak{f}$ von kleinster Norm, und die genannten Ideale sind (nach § 1, 10⁰) identisch mit den sämtlichen Produkten $\mathfrak{a}\mathfrak{f}$, wo $\mathfrak{a}$ alle Ideale durchläuft. Dieses Ideal $\mathfrak{f}$ soll der Führer der Ordnung $\mathfrak{o}'$ heißen. Da das Hauptideal $\mathfrak{o}k$ durch $\mathfrak{o}'$ und folglich auch durch $\mathfrak{f}$ teilbar ist, so ist k^n als Norm von $\mathfrak{o}k$ teilbar durch

$$N(\mathfrak{f}) = (\mathfrak{o}, \mathfrak{f}) = (\mathfrak{o}, \mathfrak{o}')(\mathfrak{o}', \mathfrak{f}) = k(\mathfrak{o}', \mathfrak{f}).$$

Ist der Führer $\mathfrak{f}$ der Ordnung $\mathfrak{o}'$ und für jede der $(\mathfrak{o}', \mathfrak{f})$ Zahlklassen, aus denen $\mathfrak{o}'$ besteht, ein Repräsentant gegeben, so ist $\mathfrak{o}'$ vollständig definiert. Nicht jedes Ideal $\mathfrak{f}$ kann der Führer einer Ordnung sein, sondern hierzu ist eine gewisse Bedingung erforderlich, deren Auffindung keine großen Schwierigkeiten darbietet; doch würde die Ableitung derselben sowie ein näheres Eingehen auf die Konstitution der Ordnungen überhaupt, uns hier zu weit führen. Das Gebiet $\mathfrak{o}$ ist offenbar selbst eine Ordnung und auch zugleich der Führer derselben.

§ 4.

Ideale der Ordnung $\mathfrak{o}'$.

Es sei nun $\mathfrak{o}'$ eine bestimmte Ordnung im Körper Ω, und $\mathfrak{f}$ der Führer derselben, so wollen wir ein System $\mathfrak{a}'$ von unendlich vielen Zahlen ein Ideal der Ordnung $\mathfrak{o}'$ oder kürzer ein Ideal in $\mathfrak{o}'$ nennen, wenn es die folgenden drei Bedingungen erfüllt:

I. Die Summen und Differenzen von je zwei in $\mathfrak{a}'$ enthaltenen Zahlen gehören ebenfalls dem System $\mathfrak{a}'$ an, d. h. $\mathfrak{a}'$ ist ein Modul im allgemeinsten Sinne des Wortes.

II. Jedes Produkt aus einer Zahl des Systems $\mathfrak{a}'$ und aus einer Zahl der Ordnung $\mathfrak{o}'$ ist eine Zahl des Systems $\mathfrak{a}'$; d. h. $\mathfrak{o}'\mathfrak{a}'$ ist teilbar durch $\mathfrak{a}'$ und folglich auch $= \mathfrak{a}'$, weil $\mathfrak{o}'$ ein Teiler von [1] ist.

III. Der größte gemeinschaftliche Teiler $\mathfrak{a}' + \mathfrak{f}$ von $\mathfrak{a}'$ und $\mathfrak{f}$ ist $= \mathfrak{o}'$.

Für den Fall, daß die Ordnung $\mathfrak{o}'$ identisch mit $\mathfrak{o}$ ist, geht diese Definition eines Ideals $\mathfrak{a}'$ in $\mathfrak{o}'$ vollständig in die frühere Definition (§ 1, 1⁰) eines Ideals über, da die dritte Bedingung nur darauf hinauskommt, daß $\mathfrak{a}'$ durch $\mathfrak{o}$ teilbar ist. Wir werden daher diese Ideale künftig, wenn Mißverständnisse zu befürchten sind, Ideale in $\mathfrak{o}$ zu nennen haben. Im folgenden nehmen wir immer an, daß $\mathfrak{o}'$ von $\mathfrak{o}$ verschieden ist.

Ist nun α' eine beliebige, aber von 0 verschiedene Zahl in $\mathfrak{a}'$, und bilden die n Zahlen $\omega'_1, \omega'_2 \cdots \omega'_n$ eine Basis der Ordnung $\mathfrak{o}'$, so sind die n Produkte $\alpha'\omega'_1, \alpha'\omega'_2, \cdots \alpha'\omega'_n$, welche (zufolge II) in $\mathfrak{a}'$ enthalten sind, voneinander unabhängig und bilden folglich eine Basis des Körpers Ω; mithin kann jede Zahl des Körpers durch Multiplikation mit einer rationalen, von 0 verschiedenen Zahl in eine Zahl des Ideals $\mathfrak{a}'$ verwandelt werden, woraus wieder leicht folgt, daß $\mathfrak{a}'$ ein endlicher Modul $[\alpha'_1, \alpha'_2 \cdots \alpha'_n]$, also ein Modul in dem Sinne des § 3 ist. Die Basiszahlen haben die Form

$$\begin{aligned}
\alpha'_1 &= a'_1\omega'_1 + a'_2\omega'_2 + \cdots + a'_n\omega'_n,\\
\alpha'_2 &= a''_1\omega'_1 + a''_2\omega'_2 + \cdots + a''_n\omega'_n,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\alpha'_n &= a_1^{(n)}\omega'_1 + a_2^{(n)}\omega'_2 + \cdots + a_n^{(n)}\omega'_n,
\end{aligned}$$

wo die Koeffizienten ganze rationale Zahlen sind, deren Determinante

$$\sum \pm a'_1 a''_2 \cdots a_n^{(n)} = (\mathfrak{o}', \mathfrak{a}')$$

die Norm des Ideals $\mathfrak{a}'$ heißen und mit $N'(\mathfrak{a}')$ bezeichnet werden soll.

Es ergibt sich ferner leicht, daß $\mathfrak{o}'$ auch die Ordnung des Ideals $\mathfrak{a}'$ ist; in der Tat besteht die letztere, die wir mit $\mathfrak{o}_1$ bezeichnen wollen, zufolge ihrer Definition (§ 2, 6°) aus allen Zahlen ω_1, für welche $\mathfrak{a}'\omega_1 > \mathfrak{a}'$ wird, und da (nach II) $\mathfrak{a}'\mathfrak{o}' = \mathfrak{a}'$ ist, so ist jedenfalls $\mathfrak{o}' > \mathfrak{o}_1$, und es braucht nur noch bewiesen zu werden, daß umgekehrt auch $\mathfrak{o}_1 > \mathfrak{o}'$ ist. Da nun $\mathfrak{a}'$ ein endlicher Modul des Körpers, und folglich (nach § 3, 1° und 2°) $[1] > \mathfrak{o}_1 > \mathfrak{o}$ ist, so ergibt sich $\mathfrak{k}[1] > \mathfrak{k}\mathfrak{o}_1 > \mathfrak{k}\mathfrak{o}$, mithin $\mathfrak{k}\mathfrak{o}_1 = \mathfrak{k}$, weil $\mathfrak{k}[1] = \mathfrak{k}\mathfrak{o} = \mathfrak{k}$ ist; da außerdem (nach § 2, 6°) $\mathfrak{a}'\mathfrak{o}_1 = \mathfrak{a}'$, und (nach III) $\mathfrak{o}' = \mathfrak{k} + \mathfrak{a}'$ ist, so folgt $\mathfrak{o}'\mathfrak{o}_1 = \mathfrak{k}\mathfrak{o}_1 + \mathfrak{a}'\mathfrak{o}_1 = \mathfrak{k} + \mathfrak{a}'$, also $\mathfrak{o}'\mathfrak{o}_1 = \mathfrak{o}'$; nun ist aber $[1] > \mathfrak{o}'$, also auch $[1]\mathfrak{o}_1 > \mathfrak{o}'\mathfrak{o}_1$, d. h. $\mathfrak{o}_1 > \mathfrak{o}'$, was zu beweisen war.

Sind ferner $\mathfrak{a}'$, $\mathfrak{b}'$ zwei beliebige Ideale in $\mathfrak{o}'$, so überzeugt man sich leicht, daß $\mathfrak{a}' - \mathfrak{b}'$, $\mathfrak{a}' + \mathfrak{b}'$, $\mathfrak{a}'\mathfrak{b}'$ ebenfalls Ideale in $\mathfrak{o}'$ sind, und daß $\mathfrak{a}'\mathfrak{b}'$ sowohl durch $\mathfrak{a}'$ als durch $\mathfrak{b}'$ teilbar ist. Der Kürze wegen beschränke ich mich auf die Betrachtung des Produkts. Da $\mathfrak{o}'\mathfrak{a}' = \mathfrak{a}'$, so ergibt sich $\mathfrak{o}'(\mathfrak{a}'\mathfrak{b}') = (\mathfrak{o}'\mathfrak{a}')\mathfrak{b}' = \mathfrak{a}'\mathfrak{b}'$, also besitzt $\mathfrak{a}'\mathfrak{b}'$ die Eigenschaft II. Da ferner $\mathfrak{b}' > \mathfrak{o}'$ und $\mathfrak{o}'\mathfrak{a}' = \mathfrak{a}'$ ist, so folgt $\mathfrak{a}'\mathfrak{b}' > \mathfrak{a}'$; ebenso ist $\mathfrak{a}'\mathfrak{b}'$ durch $\mathfrak{b}'$ teilbar. Da endlich $\mathfrak{o}' = \mathfrak{a}' + \mathfrak{k}$ ist, so folgt $\mathfrak{b}' = \mathfrak{o}'\mathfrak{b}' = \mathfrak{a}'\mathfrak{b}' + \mathfrak{k}\mathfrak{b}'$, also $\mathfrak{o}' = \mathfrak{b}' + \mathfrak{k} = \mathfrak{a}'\mathfrak{b}' + \mathfrak{k}\mathfrak{b}' + \mathfrak{k}$; da nun $\mathfrak{k} = \mathfrak{k}\mathfrak{o}$, und $\mathfrak{b}' > \mathfrak{o}$ ist, so folgt $\mathfrak{k}\mathfrak{b}' + \mathfrak{k} = \mathfrak{k}(\mathfrak{b}' + \mathfrak{o}) = \mathfrak{k}\mathfrak{o} = \mathfrak{k}$, also $\mathfrak{o}' = \mathfrak{a}'\mathfrak{b}' + \mathfrak{k}$, womit auch die Eigenschaft III für $\mathfrak{a}'\mathfrak{b}'$ dargetan ist.

§ 5.

Korrespondenz zwischen den Idealen in $\mathfrak{o}'$ und $\mathfrak{o}$.

Man könnte nun eine Theorie der Ideale in $\mathfrak{o}'$ aufstellen, welche sowohl in den Sätzen wie in ihren Beweisen eine vollständige Analogie mit der früheren Theorie der Ideale in $\mathfrak{o}$ darbieten würde. Allein es ist viel bequemer, die neue Theorie auf die alte zurückzuführen. Dies geschieht durch die folgenden Sätze.

1°. Ist $\mathfrak{a}'$ ein Ideal in $\mathfrak{o}'$, so ist $\mathfrak{o}\mathfrak{a}'$ ein Ideal in $\mathfrak{o}$, und zwar relatives Primideal zu $\mathfrak{k}$; zugleich ist $\mathfrak{a}'$ das kleinste gemeinschaftliche Vielfache, $\mathfrak{o}$ der größte gemeinschaftliche Teiler von $\mathfrak{o}'$ und $\mathfrak{o}\mathfrak{a}'$, und folglich $N'(\mathfrak{a}') = N(\mathfrak{o}\mathfrak{a}')$. Ist ferner $\mathfrak{b}'$ ebenfalls ein Ideal in $\mathfrak{o}'$, und $\mathfrak{o}\mathfrak{a}' = \mathfrak{o}\mathfrak{b}'$, so ist $\mathfrak{a}' = \mathfrak{b}'$.

Beweis. Der Modul $\mathfrak{o}\mathfrak{a}'$ genügt der Bedingung $\mathfrak{o}(\mathfrak{o}\mathfrak{a}') = \mathfrak{o}\mathfrak{a}'$, weil $\mathfrak{o}^2 = \mathfrak{o}$ ist, und er ist teilbar durch $\mathfrak{o}\mathfrak{o}' = \mathfrak{o}$, weil $\mathfrak{a}' > \mathfrak{o}'$ und $[1] > \mathfrak{o}' > \mathfrak{o}$ ist; also ist $\mathfrak{o}\mathfrak{a}'$ ein Ideal in $\mathfrak{o}$. Aus $\mathfrak{o}' = \mathfrak{a}' + \mathfrak{k}$ folgt durch Multiplikation mit $\mathfrak{o}$ ferner $\mathfrak{o} = \mathfrak{o}\mathfrak{a}' + \mathfrak{k}$, also sind $\mathfrak{o}\mathfrak{a}'$ und $\mathfrak{k}$ relative Primideale. Hieraus ergibt sich ferner (entweder nach der bekannten Theorie der Ideale in $\mathfrak{o}$, oder auch unmittelbar), daß ihr kleinstes gemeinschaftliches Vielfaches $\mathfrak{k} - \mathfrak{o}\mathfrak{a}' = \mathfrak{k}\mathfrak{o}\mathfrak{a}' = \mathfrak{k}\mathfrak{a}'$ ist. Wendet man nun den allgemeinen Satz (§ 2, 1°)

$$(\mathfrak{a} + \mathfrak{b}) - (\mathfrak{a} + \mathfrak{c}) = \mathfrak{a} + (\mathfrak{b} - (\mathfrak{a} + \mathfrak{c}))$$

auf den Fall $\mathfrak{a} = \mathfrak{a}'$, $\mathfrak{b} = \mathfrak{k}$, $\mathfrak{c} = \mathfrak{o}\mathfrak{a}'$ an, so ergibt sich, weil $\mathfrak{a}' + \mathfrak{o}\mathfrak{a}' = (\mathfrak{o}' + \mathfrak{o})\mathfrak{a}' = \mathfrak{o}\mathfrak{a}'$ ist,

$$\begin{aligned}
\mathfrak{o}' - \mathfrak{o}\mathfrak{a}' &= \mathfrak{a}' + (\mathfrak{k} - \mathfrak{o}\mathfrak{a}') = \mathfrak{a}' + \mathfrak{k}\mathfrak{a}'\\
&= \mathfrak{a}'(\mathfrak{o}' + \mathfrak{k}) = \mathfrak{a}'\mathfrak{o}' = \mathfrak{a}'.
\end{aligned}$$

Ferner ist

$$\mathfrak{o}' + \mathfrak{o}\mathfrak{a}' = \mathfrak{k} + \mathfrak{a}' + \mathfrak{o}\mathfrak{a}' = \mathfrak{k} + \mathfrak{o}\mathfrak{a}' = \mathfrak{o}.$$

Hieraus ergibt sich (nach § 2, 2°)

$$(\mathfrak{o}', \mathfrak{o}\mathfrak{a}') = (\mathfrak{o}', \mathfrak{a}') = (\mathfrak{o}, \mathfrak{o}\mathfrak{a}'),$$

also $N'(\mathfrak{a}') = N(\mathfrak{o}\mathfrak{a}')$. Aus $\mathfrak{o}\mathfrak{a}' = \mathfrak{o}\mathfrak{b}'$ folgt endlich, weil $\mathfrak{a}' = \mathfrak{o}' - \mathfrak{o}\mathfrak{a}'$ und $\mathfrak{b}' = \mathfrak{o}' - \mathfrak{o}\mathfrak{b}'$ ist, auch $\mathfrak{a}' = \mathfrak{b}'$, was zu beweisen war.

2°. Ist $\mathfrak{a}$ ein Ideal in $\mathfrak{o}$, und zwar relatives Primideal zu $\mathfrak{k}$, so ist das kleinste gemeinschaftliche Vielfache $\mathfrak{a}'$ von $\mathfrak{o}'$, $\mathfrak{a}$ ein Ideal in $\mathfrak{o}'$, und zugleich ist $\mathfrak{o}\mathfrak{a}' = \mathfrak{a}$.

Beweis. Zunächst ist $\mathfrak{o}'\mathfrak{a}' > \mathfrak{o}\mathfrak{a} = \mathfrak{a}$, weil $\mathfrak{o}' > \mathfrak{o}$, $\mathfrak{a}' > \mathfrak{a}$ ist; außerdem ist $\mathfrak{o}'\mathfrak{a}' > \mathfrak{o}'$, weil $\mathfrak{a}' > \mathfrak{o}'$ und $\mathfrak{o}'\mathfrak{o}' = \mathfrak{o}'$ ist; mithin ist

$\mathfrak{o}'\mathfrak{a}'$ ein gemeinschaftliches Vielfaches von $\mathfrak{o}'$, $\mathfrak{a}$ und folglich auch teilbar durch $\mathfrak{a}'$, d. h. $\mathfrak{a}'$ genügt der Bedingung II. Nach einem für drei beliebige Moduln $\mathfrak{a}$, $\mathfrak{k}$, $\mathfrak{o}'$ geltenden Satze (§ 2, 1°) ist ferner

$$(\mathfrak{o}' - \mathfrak{a}) + (\mathfrak{o}' - \mathfrak{k}) = \mathfrak{o}' - (\mathfrak{a} + (\mathfrak{o}' - \mathfrak{k})),$$

und da in unserem Falle $\mathfrak{o}' - \mathfrak{a} = \mathfrak{a}'$, $\mathfrak{o}' - \mathfrak{k} = \mathfrak{k}$, $\mathfrak{a} + \mathfrak{k} = \mathfrak{o}$, $\mathfrak{o}' - \mathfrak{o} = \mathfrak{o}'$ ist, so ergibt sich $\mathfrak{a}' + \mathfrak{k} = \mathfrak{o}'$, also genügt $\mathfrak{a}'$ auch der Bedingung III und ist folglich ein Ideal in $\mathfrak{o}'$. Hieraus folgt (nach dem Satze 1°), daß $\mathfrak{o}\mathfrak{a}'$ ein Ideal in $\mathfrak{o}$, und daß zugleich $\mathfrak{o} = \mathfrak{o}\mathfrak{a}' + \mathfrak{k}$, also auch $\mathfrak{a} = \mathfrak{o}\mathfrak{a}'\mathfrak{a} + \mathfrak{k}\mathfrak{a}$ ist; da nun $\mathfrak{a}$, $\mathfrak{k}$ Ideale in $\mathfrak{o}$ sind, so ist $\mathfrak{k}\mathfrak{a} > \mathfrak{k} > \mathfrak{o}'$ und $\mathfrak{k}\mathfrak{a} > \mathfrak{a}$, also muß $\mathfrak{k}\mathfrak{a}$, als gemeinschaftliches Vielfaches von $\mathfrak{o}'$, $\mathfrak{a}$, durch $\mathfrak{a}'$ und folglich auch durch $\mathfrak{o}\mathfrak{a}'$ teilbar sein; da nun auch $\mathfrak{o}\mathfrak{a}'\mathfrak{a}$ durch $\mathfrak{o}\mathfrak{a}'$ teilbar, also $\mathfrak{o}\mathfrak{a}'$ ein gemeinschaftlicher Teiler von $\mathfrak{k}\mathfrak{a}$ und $\mathfrak{o}\mathfrak{a}'\mathfrak{a}$ ist, so folgt, daß $\mathfrak{a}$ als größter gemeinschaftlicher Teiler von $\mathfrak{o}\mathfrak{a}'\mathfrak{a}$ und $\mathfrak{k}\mathfrak{a}$ gewiß durch $\mathfrak{o}\mathfrak{a}'$ teilbar ist; umgekehrt ist aber auch $\mathfrak{o}\mathfrak{a}' > \mathfrak{a}$, weil $\mathfrak{a}' > \mathfrak{a}$ und $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$ ist; mithin ist $\mathfrak{o}\mathfrak{a}' = \mathfrak{a}$, was zu beweisen war.

Durch diese beiden Sätze ist eine eindeutige, gegenseitige Korrespondenz zwischen allen Idealen $\mathfrak{a}'$ in $\mathfrak{o}'$ und allen denjenigen Idealen $\mathfrak{a}$ in $\mathfrak{o}$ begründet, welche relative Primideale zum Führer $\mathfrak{k}$ der Ordnung $\mathfrak{o}'$ sind; die Korrespondenz zwischen $\mathfrak{a}$ und $\mathfrak{a}'$ besteht darin, daß gleichzeitig $\mathfrak{a} = \mathfrak{o}\mathfrak{a}'$, und $\mathfrak{a}' = \mathfrak{o}' - \mathfrak{a}$ ist. Offenbar entsprechen sich auf diese Weise die beiden Ideale $\mathfrak{o}$ und $\mathfrak{o}'$.

Es ist schon oben (§ 4) bewiesen, daß jedes Produkt $\mathfrak{a}'\mathfrak{b}'$ aus zwei Idealen $\mathfrak{a}'$, $\mathfrak{b}'$ in $\mathfrak{o}'$ wieder ein Ideal $\mathfrak{c}'$ in $\mathfrak{o}'$, und zwar durch $\mathfrak{a}'$ und durch $\mathfrak{b}'$ teilbar ist; da nun $\mathfrak{o}^2 = \mathfrak{o}$ ist, so ist gleichzeitig $\mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}' = \mathfrak{o}\mathfrak{a}'\mathfrak{b}' = \mathfrak{o}\mathfrak{c}'$, also (nach § 1, 9°) $N(\mathfrak{o}\mathfrak{a}'\mathfrak{b}') = N(\mathfrak{o}\mathfrak{a}')N(\mathfrak{o}\mathfrak{b}')$ und folglich auch

$$N'(\mathfrak{a}'\mathfrak{b}') = N'(\mathfrak{a}')N'(\mathfrak{b}').$$

Umgekehrt: wenn $\mathfrak{a}'$, $\mathfrak{c}'$ Ideale in $\mathfrak{o}'$ sind, und wenn $\mathfrak{c}'$ durch $\mathfrak{a}'$ teilbar ist, so ist auch $\mathfrak{o}\mathfrak{c}' > \mathfrak{o}\mathfrak{a}'$, und folglich (§ 1, 10°) gibt es ein und nur ein Ideal $\mathfrak{b}$ in $\mathfrak{o}$, für welches $\mathfrak{o}\mathfrak{c}' = \mathfrak{o}\mathfrak{a}'\mathfrak{b}$ wird; da nun $\mathfrak{o}\mathfrak{c}'$, also $\mathfrak{b}$, relatives Primideal zu $\mathfrak{k}$ ist, so gibt es (nach 2°) ein und nur ein Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$, für welches $\mathfrak{o}\mathfrak{b}' = \mathfrak{b}$ wird; es ist daher $\mathfrak{o}\mathfrak{c}' = \mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}' = \mathfrak{o}(\mathfrak{a}'\mathfrak{b}')$, woraus (nach 1°) $\mathfrak{c}' = \mathfrak{a}'\mathfrak{b}'$ folgt; wäre nun zugleich $\mathfrak{c}' = \mathfrak{a}'\mathfrak{b}'$ und $\mathfrak{b}'$ ebenfalls ein Ideal in $\mathfrak{o}'$, so würde $\mathfrak{o}\mathfrak{c}' = \mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}' = \mathfrak{o}\mathfrak{a}' \cdot \mathfrak{o}\mathfrak{b}'$, und hieraus (nach § 1, 10°) $\mathfrak{o}\mathfrak{b}' = \mathfrak{o}\mathfrak{b}'$, also auch $\mathfrak{b}' = \mathfrak{b}'$ folgen. Hiermit ist folgender Satz bewiesen:

3°. Ist das Ideal $\mathfrak{c}'$ in $\mathfrak{o}'$ teilbar durch das Ideal $\mathfrak{a}'$ in $\mathfrak{o}'$, so gibt es ein und nur ein Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$ von der Art, daß $\mathfrak{a}'\mathfrak{b}' = \mathfrak{c}'$ wird; außerdem ist immer $N'(\mathfrak{a}'\mathfrak{b}') = N'(\mathfrak{a}')N'(\mathfrak{b}')$.

Aus allem diesen ergibt sich ohne weiteres, daß die Gesetze der Teilbarkeit der Ideale in $\mathfrak{o}'$ und ihrer Multiplikation gänzlich mit den Gesetzen der Teilbarkeit derjenigen Ideale in $\mathfrak{o}$, welche relative Primideale zu $\mathfrak{k}$ sind, übereinstimmen und durch die genannte Korrespondenz aus den letzteren unmittelbar entnommen werden.

§ 6.

Hauptideale und Ideal-Klassen in $\mathfrak{o}'$.

Zwei Moduln $\mathfrak{a}$, $\mathfrak{b}$ des Körpers Ω, d. h. endliche Moduln, deren Basen zugleich Basen des Körpers sind (§ 3), sollen äquivalent heißen, wenn es eine Zahl μ von der Beschaffenheit gibt, daß $\mathfrak{a}\mu = \mathfrak{b}$, und folglich, da μ nicht verschwinden kann, auch $\mathfrak{b}\mu^{-1} = \mathfrak{a}$ wird. Offenbar muß μ eine Zahl des Körpers Ω sein, und wir wollen dem vorstehenden Begriff der Äquivalenz noch die Beschränkung hinzufügen, daß $\mathfrak{a}$, $\mathfrak{b}$ nur dann äquivalent heißen sollen, wenn eine Zahl μ von der genannten Beschaffenheit existiert, deren Norm zugleich positiv ist; wenn aber der Bedingung $\mathfrak{a}\mu = \mathfrak{b}$ nur durch solche Zahlen μ genügt werden kann, deren Normen negativ sind, so können $\mathfrak{a}$, $\mathfrak{b}$ halb-äquivalent genannt werden. Sind zwei Moduln $\mathfrak{b}$, $\mathfrak{c}$ mit einem dritten $\mathfrak{a}$ äquivalent, so sind $\mathfrak{b}$, $\mathfrak{c}$ offenbar auch miteinander äquivalent. Man kann daher die Moduln des Körpers Ω in Modul-Klassen einteilen, deren jede aus allen den Moduln besteht, welche mit einem bestimmten Modul, dem Repräsentanten der Klasse, äquivalent sind. Alle Moduln einer Klasse besitzen dieselbe Ordnung $\mathfrak{o}'$, welche die Ordnung der Klasse heißen soll; denn wenn $\mathfrak{a}\mu = \mathfrak{b}$, und ω' irgend eine Zahl ist, für welche $\mathfrak{a}\omega' > \mathfrak{a}$ wird, so folgt durch Multiplikation mit μ oder $[\mu]$, daß auch $\mathfrak{b}\omega' > \mathfrak{b}$ ist, und umgekehrt ergibt sich hieraus wieder $\mathfrak{a}\omega' > \mathfrak{a}$. Durchläuft $\mathfrak{a}$ alle Moduln einer Klasse A, ebenso $\mathfrak{b}$ alle Moduln einer Klasse B, so gehören offenbar alle Produkte $\mathfrak{a}\mathfrak{b}$ einer und derselben Klasse an, welche die aus A, B zusammengesetzte Klasse oder das Produkt aus A, B heißen und mit AB bezeichnet werden soll.

Wir beschränken uns aber hier auf die Betrachtung der Ideale und verstehen unter einer Ideal-Klasse der Ordnung $\mathfrak{o}'$ den Inbegriff A' aller Ideale in $\mathfrak{o}'$, welche mit einem bestimmten Ideal $\mathfrak{a}'$

in $\mathfrak{o}'$ äquivalent sind. Jedes mit $\mathfrak{o}'$ selbst äquivalente Ideal soll ein Hauptideal in $\mathfrak{o}'$, und der Inbegriff aller dieser Hauptideale soll die Hauptklasse in $\mathfrak{o}'$ heißen und mit O' bezeichnet werden. Ein solches Hauptideal ist daher von der Form $\mathfrak{o}'\mu$, wo μ in $\mathfrak{o}'$ enthalten ist, weil $\mathfrak{o}'\mu$ durch $\mathfrak{o}'$ teilbar sein muß; außerdem muß das zugehörige Ideal $\mathfrak{o}\mathfrak{o}'\mu = \mathfrak{o}\mu$ relatives Primideal zu $\mathfrak{k}$, d. h. μ muß relative Primzahl zu $\mathfrak{k}$ sein (D. § 163, 7.). Umgekehrt, ist die in $\mathfrak{o}'$ enthaltene Zahl μ relative Primzahl zu $\mathfrak{k}$, und ist $N(\mu) > 0$, so ist $\mathfrak{o}'\mu$ offenbar ein Hauptideal in $\mathfrak{o}'$. Nun besteht folgender Satz, von welchem wichtige Anwendungen zu machen sind:

1°. Ist $\mathfrak{a}'$ ein Ideal in $\mathfrak{o}'$, und $\mathfrak{n}'$ ein durch $\mathfrak{o}'$ teilbarer Modul, welcher der Bedingung $\mathfrak{o}'\mathfrak{n}' = \mathfrak{n}'$ genügt, so gibt es immer ein Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$ von der Art, daß $\mathfrak{a}'\mathfrak{b}'$ ein Hauptideal in $\mathfrak{o}'$, und $\mathfrak{b}' + \mathfrak{n}' = \mathfrak{o}'$ wird.

Beweis. Der Modul $\mathfrak{o}\mathfrak{n}'$ ist ein Ideal in $\mathfrak{o}$, weil er durch $\mathfrak{o}$ teilbar ist und der Bedingung $\mathfrak{o}(\mathfrak{o}\mathfrak{n}') = \mathfrak{o}\mathfrak{n}'$ genügt. Man zerlege nun $\mathfrak{o}\mathfrak{n}'$ in seine sämtlichen Primideal-Faktoren (§ 1, 12°) und bezeichne mit $\mathfrak{k}_1$ das Produkt aller derjenigen dieser Primideale, welche in $\mathfrak{k}$ aufgehen, mit $\mathfrak{n}_1$ das Produkt aller übrigen, so daß $\mathfrak{o}\mathfrak{n}' = \mathfrak{k}_1\mathfrak{n}_1$ wird. Nun gibt es (§ 1, 14° oder D. § 163, 7.) immer ein Ideal $\mathfrak{m}_1$ in $\mathfrak{o}$ von der Art, daß $\mathfrak{o}\mathfrak{a}'\mathfrak{m}_1 = \mathfrak{a}'\mathfrak{m}_1 = \mathfrak{o}\alpha$, d. h. ein Hauptideal in $\mathfrak{o}$, und daß zugleich $\mathfrak{m}_1 + \mathfrak{n}_1 = \mathfrak{o}$, also $\mathfrak{o}\alpha + \mathfrak{a}'\mathfrak{n}_1 = \mathfrak{o}\mathfrak{a}'$ wird. Da ferner $\mathfrak{a}'$ ein Ideal in $\mathfrak{o}'$, also $\mathfrak{o}\mathfrak{a}'$ relatives Primideal zu $\mathfrak{k}$ ist, so sind auch $\mathfrak{o}\mathfrak{a}'\mathfrak{n}_1 = \mathfrak{a}'\mathfrak{n}_1$ und $\mathfrak{k}\mathfrak{k}_1$ relative Primideale, und folglich (§ 2, 2° oder D. § 163, 7.) gibt es Zahlen μ, welche den beiden gleichzeitigen Kongruenzen

$$\mu \equiv \alpha \,(\text{mod. } \mathfrak{a}'\mathfrak{n}_1), \quad \mu \equiv 1 \,(\text{mod. } \mathfrak{k}\mathfrak{k}_1)$$

genügen; diese Zahlen μ bilden eine bestimmte Zahl-Klasse in bezug auf den Modul $\mathfrak{a}'\mathfrak{n}_1\mathfrak{k}\mathfrak{k}_1 = \mathfrak{k}\mathfrak{a}'\mathfrak{n}'$, und man kann, wie unten nachträglich bewiesen werden soll, die Zahl μ zugleich so wählen, daß $N(\mu) > 0$ wird. Aus der zweiten der beiden vorstehenden Kongruenzen folgt nun, daß μ relative Primzahl zu $\mathfrak{k}\mathfrak{k}_1$ und folglich auch zu $\mathfrak{k}$ ist; da ferner $\mathfrak{k}\mathfrak{k}_1 > \mathfrak{k} > \mathfrak{o}'$, und da die Zahl 1 in der Ordnung $\mathfrak{o}'$ enthalten ist, so ist zufolge der zweiten Kongruenz auch μ in $\mathfrak{o}'$ enthalten, und folglich ist $\mathfrak{o}'\mu$ ein Hauptideal in $\mathfrak{o}'$. Aus der ersten Kongruenz folgt ferner mit Rücksicht auf $\mathfrak{o}\alpha + \mathfrak{a}'\mathfrak{n}_1 = \mathfrak{o}\mathfrak{a}'$, daß auch $\mathfrak{o}\mu + \mathfrak{a}'\mathfrak{n}_1 = \mathfrak{o}\mathfrak{a}'$, und folglich $\mathfrak{o}\mu = \mathfrak{o}\mathfrak{a}'\mathfrak{b} = \mathfrak{a}'\mathfrak{b}$ ist, wo $\mathfrak{b}$ ein Ideal in $\mathfrak{o}$, und zwar relatives Primideal zu $\mathfrak{n}_1$ ist. Da ferner $\mathfrak{o}\mu$, und

folglich auch $\mathfrak{b}$ relatives Primideal zu $\mathfrak{k}\mathfrak{k}_1$ ist, so ist $\mathfrak{b}$ auch relatives Primideal zu $\mathfrak{k}\mathfrak{k}_1\mathfrak{n}_1 = \mathfrak{k}\mathfrak{n}'$, also $\mathfrak{b} + \mathfrak{k}\mathfrak{n}' = \mathfrak{o}$. Bedeutet ferner $\mathfrak{b}'$ das dem Ideal $\mathfrak{b}$ entsprechende Ideal in $\mathfrak{o}'$ (§ 5), so ist $\mathfrak{b} = \mathfrak{o}\mathfrak{b}'$, und aus $\mathfrak{o}\mu = \mathfrak{a}'\mathfrak{b}$, d. h. aus $\mathfrak{o}(\mathfrak{o}'\mu) = \mathfrak{o}(\mathfrak{a}'\mathfrak{b}')$ folgt $\mathfrak{o}'\mu = \mathfrak{a}'\mathfrak{b}'$. Nun ist $\mathfrak{k} > \mathfrak{o}'$ und nach Voraussetzung $\mathfrak{o}'\mathfrak{n}' = \mathfrak{n}'$, folglich $\mathfrak{k}\mathfrak{n}' > \mathfrak{n}'$, und da ebenfalls $\mathfrak{n}' > \mathfrak{o}'$ vorausgesetzt ist, so folgt $\mathfrak{k}\mathfrak{n}' > \mathfrak{o}'$, also $\mathfrak{o}' - \mathfrak{k}\mathfrak{n}' = \mathfrak{k}\mathfrak{n}'$; wendet man daher den allgemeinen Satz (§ 2, 1°)

$$(\mathfrak{a} - \mathfrak{b}) + (\mathfrak{a} - \mathfrak{c}) = \mathfrak{a} - (\mathfrak{b} + (\mathfrak{a} - \mathfrak{c}))$$

auf den Fall $\mathfrak{a} = \mathfrak{o}'$, $\mathfrak{c} = \mathfrak{k}\mathfrak{n}'$ an und berücksichtigt außerdem, daß $\mathfrak{o}' - \mathfrak{b} = \mathfrak{b}'$, und $\mathfrak{b} + \mathfrak{k}\mathfrak{n}' = \mathfrak{o}$ ist, so folgt $\mathfrak{b}' + \mathfrak{k}\mathfrak{n}' = \mathfrak{o}' - \mathfrak{o} = \mathfrak{o}'$, woraus mit Rücksicht auf $\mathfrak{k}\mathfrak{n}' > \mathfrak{n}' > \mathfrak{o}'$ sich endlich auch $\mathfrak{b}' + \mathfrak{n}' = \mathfrak{o}'$ ergibt, was zu beweisen war.

Es ist nun noch der oben vorläufig übergangene Beweis nachzuholen, daß man μ so wählen kann, daß $N(\mu)$ positiv wird. Dies geschieht offenbar durch den Beweis des folgenden allgemeineren Satzes:

2°. Ist $\mathfrak{m}$ ein Modul des Körpers Ω, und μ_0 eine bestimmte Zahl dieses Körpers, so gibt es unter den Zahlen μ, welche $\equiv \mu_0 \pmod{\mathfrak{m}}$ sind, unendlich viele, die eine positive Norm haben.

Beweis. Dieser Satz ist selbstverständlich, sobald die sämtlichen Wurzeln der Gleichung $f(\Theta) = 0$, aus welcher der Körper Ω abgeleitet ist, imaginär, und folglich die n Faktoren von $N(\mu) = \mu'\mu'' \cdots \mu^{(n)}$ aus $\frac{1}{2}n$ Paaren von zwei Zahlen $a + bi$, $a - bi$ bestehen; und wenn die Gleichung eine oder mehrere reelle Wurzeln hat, so braucht man offenbar nur die diesen Wurzeln entsprechenden Faktoren von $N(\mu)$ zu betrachten, weil das Produkt der übrigen gewiß positiv ist. Da nun nach Voraussetzung die Basiszahlen des endlichen Moduls $\mathfrak{m}$ zugleich eine Basis des Körpers Ω bilden, so kann die dem Körper angehörende Zahl 1 durch Multiplikation mit einer positiven rationalen Zahl m in eine Zahl m des Moduls $\mathfrak{m}$ verwandelt werden, und wenn h eine beliebige ganze rationale Zahl bedeutet, so wird $hm \equiv 0 \pmod{\mathfrak{m}}$, und folglich $\mu = \mu_0 + hm \equiv \mu_0 \pmod{\mathfrak{m}}$. Offenbar kann man nun die ganze rationale Zahl h positiv und so groß wählen, daß diejenigen Faktoren

$$\mu' = \mu_0' + hm, \quad \mu'' = \mu_0'' + hm \cdots \mu^{(n)} = \mu_0^{(n)} + hm,$$

welche den reellen Wurzeln der Gleichung $f(\Theta) = 0$ entsprechen, sämtlich positiv ausfallen, womit der Satz bewiesen ist.

§ 7.

Komposition der Ideal-Klassen.

Sind $\mathfrak{o}'$, $\mathfrak{o}''$ zwei beliebige Ordnungen des Körpers Ω, und $\mathfrak{f}'$, $\mathfrak{f}''$ ihre Führer, so ist offenbar ihr Produkt $\mathfrak{o}''' = \mathfrak{o}'\mathfrak{o}''$ ebenfalls eine Ordnung (§ 3), und da $\mathfrak{o}'''$ ein gemeinschaftlicher Teiler von $\mathfrak{o}'$, $\mathfrak{o}''$ ist, so muß der Führer $\mathfrak{f}'''$ der Ordnung $\mathfrak{o}'''$ auch ein gemeinschaftlicher Teiler von $\mathfrak{f}'$, $\mathfrak{f}''$ sein. Ist nun $\mathfrak{a}'$ ein beliebiges Ideal in $\mathfrak{o}'$, ebenso $\mathfrak{b}''$ ein beliebiges Ideal in $\mathfrak{o}''$, so wird $\mathfrak{a}'\mathfrak{b}'' = \mathfrak{c}'''$ ein Ideal in $\mathfrak{o}'''$; denn aus $\mathfrak{o}'\mathfrak{a}' = \mathfrak{a}'$, $\mathfrak{o}''\mathfrak{b}'' = \mathfrak{b}''$ folgt $\mathfrak{o}'''\mathfrak{c}''' = \mathfrak{o}'\mathfrak{o}''\mathfrak{a}'\mathfrak{b}'' = \mathfrak{a}'\mathfrak{b}'' = \mathfrak{c}'''$; aus $\mathfrak{a}' + \mathfrak{f}' = \mathfrak{o}'$, $\mathfrak{b}'' + \mathfrak{f}'' = \mathfrak{o}''$ ergibt sich ferner durch Multiplikation

$$\mathfrak{a}'\mathfrak{b}'' + \mathfrak{a}'\mathfrak{f}'' + \mathfrak{f}'\mathfrak{b}'' + \mathfrak{f}'\mathfrak{f}'' = \mathfrak{o}'''$$

und hieraus, weil jedes der Ideale $\mathfrak{a}'\mathfrak{f}''$, $\mathfrak{f}'\mathfrak{b}''$, $\mathfrak{f}'\mathfrak{f}''$ durch $\mathfrak{f}'''$, und $\mathfrak{f}'''$ durch $\mathfrak{o}'''$ teilbar ist, $\mathfrak{a}'\mathfrak{b}'' + \mathfrak{f}''' = \mathfrak{o}'''$; also besitzt der Modul $\mathfrak{a}'\mathfrak{b}''$ die charakteristischen Eigenschaften eines Ideals in $\mathfrak{o}'''$ (§ 4), und da allgemein bewiesen ist, daß die Ordnung eines Ideals in $\mathfrak{o}'$ identisch mit $\mathfrak{o}'$ ist, so ergibt sich, daß die Ordnung eines Produkts von Idealen gleich dem Produkt aus den Ordnungen der Faktoren ist*).

Ist $\mathfrak{a}'$ ein Repräsentant der Ideal-Klasse A' in $\mathfrak{o}'$, und $\mathfrak{b}''$ ein Repräsentant der Ideal-Klasse B'' in $\mathfrak{o}''$, so ist jedes Produkt von zwei beliebigen Idealen in A', B'' von der Form $\mathfrak{a}'\mu \cdot \mathfrak{b}''\nu = \mathfrak{a}'\mathfrak{b}''(\mu\nu)$, also ein mit $\mathfrak{a}'\mathfrak{b}''$ äquivalentes Ideal; alle diese Produkte gehören daher einer und derselben Ideal-Klasse in $\mathfrak{o}'''$ an, welche (wie bei den Moduln) die aus A', B'' zusammengesetzte Klasse oder das Produkt aus A', B'' heißen und mit $A'B''$ bezeichnet werden soll. Bedeuten A, B, C beliebige Ideal-Klassen beliebiger Ordnungen, so ist offenbar $AB = BA$, $(AB)C = A(BC)$.

Von dieser allgemeinsten Komposition der Ideal-Klassen aller Ordnungen kehren wir zurück zu der Betrachtung der Ideal-Klassen einer einzigen Ordnung $\mathfrak{o}'$; jedes Produkt von solchen Klassen gehört derselben Ordnung $\mathfrak{o}'$ an, weil $\mathfrak{o}'^2 = \mathfrak{o}'$ ist. Da das Produkt $\mathfrak{o}'\mu \cdot \mathfrak{a}' = \mu\mathfrak{a}'$ aus einem Hauptideal $\mathfrak{o}'\mu$ und einem beliebigen Ideal $\mathfrak{a}'$

*) Wenn, wie es bei den quadratischen Körpern der Fall ist, jede Modul-Klasse auch Ideale enthält, so gilt der obige Satz auch für Produkte aus Moduln; aber schon bei kubischen Körpern gibt es Moduln, welche keinem Ideale äquivalent sind, und der obige Satz darf nicht mehr auf alle Produkte von Moduln übertragen werden. Auf diese wichtige Frage werde ich bei einer anderen Gelegenheit zurückkommen.

mit diesem letzteren äquivalent ist, so folgt $O'A' = A'$, wo A' eine beliebige Ideal-Klasse in $\mathfrak{o}'$, und O' die Hauptklasse in $\mathfrak{o}'$ bedeutet. Da ferner, wenn $\mathfrak{a}'$ ein beliebiger Repräsentant der Ideal-Klasse A' in $\mathfrak{o}'$ ist, immer ein solches Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$ existiert, daß $\mathfrak{a}'\mathfrak{b}'$ ein Hauptideal in $\mathfrak{o}'$ wird, so gibt es eine Ideal-Klasse B' in $\mathfrak{o}'$ von der Art, daß $A'B' = O'$ wird; und zwar gibt es nur eine einzige solche Klasse B'; denn wenn C' ebenfalls eine Ideal-Klasse in $\mathfrak{o}'$, und wenn $AC' = O'$ ist, so folgt $A'B'C' = O'B' = O'C' = B' = C'$. Diese Klasse B' soll die zu A' gehörende entgegengesetzte, oder die reziproke, oder inverse Klasse heißen und durch A'^{-1} bezeichnet werden; offenbar ist A' zugleich die inverse Klasse von A'^{-1}. Sind nun A', B', C' beliebige Ideal-Klassen derselben Ordnung $\mathfrak{o}'$, so folgt aus $A'B' = A'C'$ durch Multiplikation mit A'^{-1} stets $B' = C'$*). Sind ferner A', B' beliebige Ideal-Klassen derselben Ordnung $\mathfrak{o}'$, so gibt es immer eine und nur eine Ideal-Klasse $C' = A'^{-1}B'$ der Ordnung $\mathfrak{o}'$, welche der Bedingung $A'C' = B'$ genügt.

§ 8.

Korrespondenz zwischen den Ideal-Klassen in $\mathfrak{o}$ und $\mathfrak{o}'$.

Ist $\mathfrak{o}$ wieder die aus allen ganzen Zahlen des Körpers Ω bestehende Ordnung, O die Klasse der Hauptideale in $\mathfrak{o}$, und $\mathfrak{o}'$ eine beliebige Ordnung, so wird durch jede bestimmte Ideal-Klasse A' der Ordnung $\mathfrak{o}'$ eine bestimmte Ideal-Klasse $OA' = A$ der Ordnung $\mathfrak{o}\mathfrak{o}' = \mathfrak{o}$ erzeugt, z. B. O selbst durch die Hauptklasse O' der Ordnung $\mathfrak{o}'$. Umgekehrt, ist A eine Ideal-Klasse der Ordnung $\mathfrak{o}$, so gibt es in ihr immer einen Repräsentanten $\mathfrak{a}$, der relatives Primideal zum Führer $\mathfrak{f}$ der Ordnung $\mathfrak{o}'$ ist (denn nach § 1, 14° oder § 6 oder D. § 163, 7. kann jedes Ideal der inversen Klasse A^{-1} durch Multiplikation mit einem solchen Ideal $\mathfrak{a}$ in ein Hauptideal verwandelt werden, und dies muß folglich in A enthalten sein); dann ist $\mathfrak{a}' = \mathfrak{o}' - \mathfrak{a}$ das korrespondierende Ideal in $\mathfrak{o}'$, und $\mathfrak{o}\mathfrak{a}' = \mathfrak{a}$ (§ 5, 2°), und wenn A' die Ideal-Klasse in $\mathfrak{o}'$ ist, welcher $\mathfrak{a}'$ angehört, so ist $OA' = A$; also wird jede Ideal-Klasse A der Ordnung $\mathfrak{o}$ durch mindestens eine Ideal-Klasse A' der Ordnung $\mathfrak{o}'$ auf diese Weise erzeugt. Wir suchen nun zunächst alle Ideal-Klassen B' der Ordnung $\mathfrak{o}'$, welche dieselbe

*) Dieser Satz verliert, wie man leicht sieht, seine allgemeine Gültigkeit, wenn die Klassen A', B', C' nicht derselben Ordnung angehören.

Klasse A hervorbringen, so daß $OB' = OA'$ wird; hieraus folgt aber $OB'A'^{-1} = OO'$, also, wenn

$$B'A'^{-1} = M', \quad B' = M'A'$$

gesetzt wird,

$$OM' = O.$$

Umgekehrt, wenn M' eine der vorstehenden Bedingung genügende Ideal-Klasse der Ordnung $\mathfrak{o}'$, und wenn $B' = M'A'$ ist, so ist auch wirklich $OB' = OA'$.

Der Komplex $\mathfrak{M}'$ aller dieser Ideal-Klassen M', unter denen sich auch O' und jede inverse Klasse M'^{-1} befindet, besitzt den Charakter einer Gruppe, insofern das Produkt von je zwei solchen Klassen M' offenbar wieder demselben Komplex $\mathfrak{M}'$ angehört. In den folgenden Paragraphen wird gezeigt werden, daß die Anzahl dieser Klassen M' eine endliche ist; wir wollen dieselbe mit m bezeichnen und zunächst ihre Bedeutung für das Problem nachweisen, welches den Hauptgegenstand dieser Abhandlung bildet. Ist A' eine bestimmte Ideal-Klasse in $\mathfrak{o}'$, und durchläuft M' alle m Klassen der Gruppe $\mathfrak{M}'$, so bilden die sämtlichen Produkte $M'A'$ einen Komplex von Klassen der Ordnung $\mathfrak{o}'$, der mit $\mathfrak{M}'A'$ bezeichnet werden mag; da aus $M_1'A' = M_2'A'$ auch $M_1' = M_2'$ folgt (§ 7), so besteht ein solcher Komplex $\mathfrak{M}'A'$ aus m verschiedenen Klassen. Enthalten ferner zwei solche Komplexe $\mathfrak{M}'A'$, $\mathfrak{M}'B'$ eine und dieselbe Klasse $M_1'A' = M_2'B'$, so ist $B' = M_2'^{-1}M_1'A' = M_3'A'$, wo $M_3' = M_1'^{-1}M_1'$ ebenfalls in $\mathfrak{M}'$ enthalten ist, und hieraus folgt offenbar, daß die sämtlichen m Klassen des Komplexes $\mathfrak{M}'B'$ mit denen von $\mathfrak{M}'A'$ vollständig übereinstimmen. Man kann daher alle Ideal-Klassen der Ordnung $\mathfrak{o}'$ in lauter verschiedene solche Komplexe von der Form $\mathfrak{M}'A'$, $\mathfrak{M}'B' \cdots$ einteilen. Nun ist oben gezeigt, daß jede bestimmte Ideal-Klasse A der Ordnung $\mathfrak{o}$ in der angegebenen Weise durch die sämtlichen m Klassen eines bestimmten solchen Komplexes $\mathfrak{M}'A'$, und durch keine andere Klasse der Ordnung $\mathfrak{o}'$ erzeugt wird, und daß umgekehrt alle m Klassen eines solchen Komplexes durch Multiplikation mit O eine und nur eine Klasse A der Ordnung $\mathfrak{o}$ erzeugen. Mithin ist die Anzahl aller dieser Komplexe identisch mit der Anzahl h der verschiedenen Ideal-Klassen der Ordnung $\mathfrak{o}$, deren Endlichkeit schon bewiesen ist (D. § 164, 2°), und zugleich ergibt sich, daß

$$h' = mh$$

die Anzahl aller verschiedenen Ideal-Klassen der Ordnung $\mathfrak{o}'$ ist.

§ 9.

Bestimmung des Verhältnisses m der Klassenanzahlen h' und h.

Es sei M' eine bestimmte Klasse der Gruppe $\mathfrak{M}'$, und $\mathfrak{m}'$ ein bestimmter Repräsentant von M'. Da $OM' = O$ ist, so ist $\mathfrak{o}\mathfrak{m}'$ ein Hauptideal in $\mathfrak{o}$, also von der Form $\mathfrak{o}\mu$, wo μ eine ganze Zahl von positiver Norm, und zwar relative Primzahl zu $\mathfrak{k}$ ist, wo $\mathfrak{k}$ wieder den Führer der Ordnung $\mathfrak{o}'$ bedeutet. Umgekehrt, ist μ eine solche Zahl, so ist $\mathfrak{o}\mu$ ein Hauptideal in $\mathfrak{o}$ und relatives Primideal zu $\mathfrak{k}$, mithin gibt es (§ 5, 2°) ein und nur ein Ideal $\mathfrak{m}'$ in $\mathfrak{o}'$, welches der Bedingung $\mathfrak{o}\mathfrak{m}' = \mathfrak{o}\mu$ genügt, und wenn M' die durch $\mathfrak{m}'$ repräsentierte Ideal-Klasse in $\mathfrak{o}'$ bedeutet, so ist $OM' = O$; jeder bestimmten Zahl μ von der angegebenen Beschaffenheit entspricht daher auf diese Weise eine und nur eine Ideal-Klasse M', welche der Gruppe $\mathfrak{M}'$ angehört. Auf diese Korrespondenz bezieht sich der folgende Satz:

Sind μ, μ_1 ganze Zahlen von positiver Norm und relative Primzahlen zu $\mathfrak{k}$, so besteht die erforderliche und hinreichende Bedingung dafür, daß beiden Zahlen eine und dieselbe Klasse M' der Gruppe $\mathfrak{M}'$ entspreche, in der Kongruenz

$$\mu_1 \equiv \mu\varepsilon\omega' \pmod{\mathfrak{k}},$$

wo ε eine Einheit in $\mathfrak{o}$, und ω' eine in $\mathfrak{o}'$ enthaltene relative Primzahl zu $\mathfrak{k}$ bedeutet, deren Normen beide positiv sind.

Beweis. Ist $\mathfrak{m}' = \mathfrak{o}' - \mathfrak{o}\mu$ das Ideal in $\mathfrak{o}'$, welches dem Ideal $\mathfrak{o}\mu$ entspricht und folglich der Bedingung $\mathfrak{o}\mathfrak{m}' = \mathfrak{o}\mu$ genügt, so kann man, weil $\mathfrak{m}' + \mathfrak{k} = \mathfrak{o}'$ ist, eine Zahl μ' so wählen, daß $\mu' \equiv 0 \pmod{\mathfrak{m}'}$ und $\mu' \equiv 1 \pmod{\mathfrak{k}}$ wird (§ 2, 2°); auch leuchtet ein, daß zugleich die Bedingung $N(\mu') > 0$ erfüllt werden kann (§ 6, 2°). Dann ist $\mathfrak{o}'\mu'$ ein durch $\mathfrak{m}'$ teilbares Hauptideal in $\mathfrak{o}'$, weil $\mathfrak{o}'\mu' + \mathfrak{k} = \mathfrak{o}'$ ist, und folglich gibt es ein Ideal $\mathfrak{n}'$ in $\mathfrak{o}'$, welches der Bedingung $\mathfrak{m}'\mathfrak{n}' = \mathfrak{o}'\mu'$ genügt und folglich der inversen Klasse M'^{-1} angehört. Hieraus folgt durch Multiplikation mit $\mathfrak{o}$, daß $\mathfrak{o}\mu' = \mathfrak{o}\mathfrak{n}'\mu$, also μ' durch μ teilbar ist; setzt man $\mu' = \mu\nu$, so ist ν eine ganze Zahl von positiver Norm und relative Primzahl zu $\mathfrak{k}$, weil $\mu\nu = \mu' \equiv 1 \pmod{\mathfrak{k}}$ ist; zugleich wird $\mathfrak{o}\mu\nu = \mathfrak{o}\mathfrak{n}'\mu$, und folglich $\mathfrak{o}\mathfrak{n}' = \mathfrak{o}\nu$.

Wenn nun das dem Ideal $\mathfrak{o}\mu_1$ entsprechende Ideal $\mathfrak{m}_1' = \mathfrak{o}' - \mathfrak{o}\mu_1$ derselben Klasse M' angehört, wie $\mathfrak{m}'$, so ist auch $\mathfrak{m}_1'\mathfrak{n}'$ ein Hauptideal in $\mathfrak{o}'$, also $\mathfrak{m}_1'\mathfrak{n}' = \mathfrak{o}'\omega'$, wo ω' eine Zahl in $\mathfrak{o}'$ von positiver Norm und relative Primzahl zu $\mathfrak{f}$ ist. Multipliziert man mit $\mathfrak{o}$ und berücksichtigt, daß $\mathfrak{o}\mathfrak{m}_1' = \mathfrak{o}\mu_1$ und $\mathfrak{o}\mathfrak{n}' = \mathfrak{o}\nu$ ist, so folgt $\mathfrak{o}\mu_1\nu = \mathfrak{o}\omega'$, und hieraus $\mu_1\nu = \varepsilon\omega'$, wo ε eine Einheit in $\mathfrak{o}$ bedeutet, deren Norm $= +1$ sein muß, weil die Normen der Zahlen μ_1, ν, ω' positiv sind. Multipliziert man mit μ, so ergibt sich die zu beweisende Kongruenz, weil $\mu\nu = \mu' \equiv 1 \pmod{\mathfrak{f}}$ und $\mathfrak{o}\mathfrak{f} = \mathfrak{f}$ ist.

Umgekehrt, wenn diese Kongruenz, in welcher μ, μ_1, ε, ω' die in dem Satze angegebene Bedeutung haben, erfüllt ist, so folgt durch Multiplikation mit $\nu\varepsilon^{-1}$ die Kongruenz

$$\nu\mu_1\varepsilon^{-1} \equiv \omega' \pmod{\mathfrak{f}},$$

aus welcher hervorgeht, daß die ganze Zahl $\alpha' = \nu\mu_1\varepsilon^{-1}$, welche relative Primzahl zu $\mathfrak{f}$ ist und eine positive Norm besitzt, der Ordnung $\mathfrak{o}'$ angehört, und folglich ist $\mathfrak{o}'\alpha'$ ein Hauptideal in $\mathfrak{o}'$. Da nun $\mathfrak{o}\nu = \mathfrak{o}\mathfrak{n}'$ und $\mathfrak{o}\mu_1\varepsilon^{-1} = \mathfrak{o}\mu_1 = \mathfrak{o}\mathfrak{m}_1'$ ist, so folgt $\mathfrak{o}(\mathfrak{o}'\alpha') = \mathfrak{o}(\mathfrak{n}'\mathfrak{m}_1')$, also auch $\mathfrak{o}'\alpha' = \mathfrak{n}'\mathfrak{m}_1'$ (§ 5, 1°), mithin gehören die Ideale $\mathfrak{n}'$, $\mathfrak{m}_1'$ zu entgegengesetzten Klassen, d. h. das dem Ideal $\mathfrak{o}\mu_1$ entsprechende Ideal $\mathfrak{m}_1'$ ist äquivalent mit $\mathfrak{m}'$, was zu beweisen war.

Mit Hilfe dieses Satzes ist es leicht, die Anzahl m der in der Gruppe $\mathfrak{M}'$ enthaltenen Klassen M' zu bestimmen. Wir bezeichnen mit $\psi(\mathfrak{f})$ die Anzahl aller der in $\mathfrak{o}$ enthaltenen Zahlen ω, welche inkongruent in bezug auf den Modul $\mathfrak{f}$ und zugleich relative Primzahlen zu $\mathfrak{f}$ sind; diese Anzahl ist (D. § 163, 7.)

$$\psi(\mathfrak{f}) = N(\mathfrak{f}) \prod \left(1 - \frac{1}{N(\mathfrak{q})}\right),$$

wo das Produktzeichen Π sich auf alle verschiedenen, in $\mathfrak{f}$ aufgehenden Primideale $\mathfrak{q}$ bezieht. Die Repräsentanten ω selbst können (nach § 6, 2°) immer so gewählt werden, daß sie positive Normen haben. Wenn eine dieser Zahlen (wie z. B. die Zahl 1) in $\mathfrak{o}'$ enthalten ist, so gehören auch alle mit ihr kongruenten Zahlen der Ordnung $\mathfrak{o}'$ an, weil $\mathfrak{f}$ durch $\mathfrak{o}'$ teilbar ist; die Anzahl dieser nach $\mathfrak{f}$ inkongruenten Zahlen ω' oder der zugehörigen Zahlklassen ist ebenfalls als bekannt anzusehen, sobald $\mathfrak{o}'$ gegeben ist, und soll mit $\psi'(\mathfrak{f})$ bezeichnet werden. Da $\mathfrak{o}'^2 = \mathfrak{o}'$ ist, so ist das Produkt aus je zwei Repräsentanten dieser Zahlklassen immer wieder einem solchen Repräsentanten kongruent, und der Komplex dieser $\psi'(\mathfrak{f})$ Repräsentanten hat daher den Charakter einer Gruppe. Multipliziert man dieselben mit einer beliebigen in $\mathfrak{o}$ enthaltenen Zahl ω, welche relative Primzahl zu $\mathfrak{f}$ ist, so erhält man $\psi'(\mathfrak{f})$ inkongruente Zahlen, welche ebenfalls relative Primzahlen zu $\mathfrak{f}$ sind, und deren Komplex kurz mit (ω) bezeichnet werden soll; zwei solche Komplexe (α), (β) sind (nach der in § 8 angewendeten Schlußweise) entweder gänzlich verschieden, d. h. keine der in (α) enthaltenen Zahlen ist kongruent mit einer der in (β) enthaltenen Zahlen, oder sie sind völlig identisch, d. h. alle durch den einen Komplex vertretenen $\psi'(\mathfrak{f})$ Zahlklassen stimmen gänzlich mit den Zahlklassen des anderen Komplexes überein. Es wird daher auch das System aller $\psi(\mathfrak{f})$ Repräsentanten in eine Anzahl solcher Komplexe (ω) zerfallen, d. h. $\psi(\mathfrak{f})$ wird teilbar sein durch $\psi'(\mathfrak{f})$; wir betrachten zunächst aber nur alle diejenigen Komplexe (ε), welche entstehen, wenn ε alle Einheiten des Gebietes $\mathfrak{o}$ durchläuft, deren Normen $= +1$ sind. Es sei s die Anzahl aller verschiedenen Komplexe

$$(\varepsilon_1),\ (\varepsilon_2) \cdots (\varepsilon_s)$$

dieser Art, so bilden die in ihnen enthaltenen $s\psi'(\mathfrak{f})$ Repräsentanten offenbar wieder eine Gruppe im obigen Sinne; jede Zahl von der Form $\varepsilon\omega'$ ist einer und nur einer dieser Zahlen kongruent, welche umgekehrt selbst in dieser Form enthalten sind. Ist nun μ eine in $\mathfrak{o}$ enthaltene relative Primzahl zu $\mathfrak{f}$, deren Norm positiv ist, und bezeichnet man mit $((\mu))$ den Komplex der $s\psi'(\mathfrak{f})$ inkongruenten, in den s Komplexen $(\mu\varepsilon_1)$, $(\mu\varepsilon_2) \cdots (\mu\varepsilon_s)$ enthaltenen Zahlen, so sind wieder zwei solche Komplexe $((\mu))$ und $((\mu_1))$ entweder gänzlich verschieden, oder völlig identisch, und folglich besteht das System aller $\psi(\mathfrak{f})$ Repräsentanten ω aus einer Anzahl von solchen Komplexen $((\mu))$; diese Anzahl muß aber notwendig $= m$, d. h. gleich der Anzahl der verschiedenen, in der Gruppe $\mathfrak{M}'$ enthaltenen Idealklassen M' sein, weil nach dem obigen Satze je zwei Hauptidealen $\mathfrak{o}\mu$, $\mathfrak{o}\mu_1$ dieselbe Klasse M' oder zwei verschiedene solche Klassen entsprechen, je nachdem die beiden Komplexe $((\mu))$, $((\mu_1))$ identisch oder verschieden sind. Mithin ist

$$\psi(\mathfrak{f}) = m s \psi'(\mathfrak{f}),$$

also

$$\frac{h'}{h} = m = \frac{\psi(\mathfrak{f})}{s\psi'(\mathfrak{f})}.$$

§ 10.

Umformung des Resultates.

Es ist nun noch von Wichtigkeit, die Anzahl s in bestimmter Weise darzustellen, und hierzu gelangt man mit Hilfe der in der Einleitung erwähnten Theorie der Einheiten von Dirichlet, welche ich zu diesem Zwecke in etwas verallgemeinerter Form dargestellt habe (D. § 166). Wir fragen zunächst: wie müssen zwei Einheiten $\varepsilon, \varepsilon_0$ von positiver Norm beschaffen sein, damit die oben mit (ε), (ε_0) bezeichneten Komplexe identisch ausfallen? Offenbar ist hierzu erforderlich, daß $\varepsilon \equiv \varepsilon_0 \omega' \pmod{\mathfrak{k}}$ sei, wo ω' eine der Ordnung $\mathfrak{o}'$ angehörende Zahl bedeutet; mithin muß $\varepsilon \varepsilon_0^{-1} \equiv \omega' \pmod{\mathfrak{k}}$, also $\varepsilon = \varepsilon' \varepsilon_0$ sein, wo $\varepsilon' = \varepsilon \varepsilon_0^{-1}$ eine der Ordnung $\mathfrak{o}'$ angehörende Einheit von positiver Norm bedeutet; und es leuchtet unmittelbar ein, daß diese Bedingung $\varepsilon = \varepsilon' \varepsilon_0$ auch hinreichend ist, daß sie also die Identität der Komplexe (ε), (ε_0) zur Folge hat. Bezeichnet man daher, wie oben, mit $(\varepsilon_1), (\varepsilon_2) \cdots (\varepsilon_s)$ die sämtlichen s verschiedenen Komplexe von der Form (ε), so ergibt sich, daß man alle Einheiten ε der Ordnung $\mathfrak{o}$, und jede nur ein einziges Mal erhält, wenn man jede der s partikulären Einheiten $\varepsilon_1, \varepsilon_2 \cdots \varepsilon_s$ mit allen Einheiten ε' der Ordnung $\mathfrak{o}'$ multipliziert. Hieraus folgt zunächst, daß die s-te Potenz ε^s einer jeden Einheit ε in $\mathfrak{o}$ immer eine Einheit ε' in $\mathfrak{o}'$ ist, weil die s Komplexe $(\varepsilon\varepsilon_1), (\varepsilon\varepsilon_2) \cdots (\varepsilon\varepsilon_s)$ notwendig mit den Komplexen $(\varepsilon_1), (\varepsilon_2) \cdots (\varepsilon_s)$, wenn auch in anderer Ordnung, übereinstimmen müssen, und weil folglich das Produkt

$$\varepsilon\varepsilon_1 \cdot \varepsilon\varepsilon_2 \cdots \varepsilon\varepsilon_s = \varepsilon^s \cdot \varepsilon_1 \varepsilon_2 \cdots \varepsilon_s$$

von der Form $\varepsilon' . \varepsilon_1 \varepsilon_2 \cdots \varepsilon_s$ ist, wo ε' eine Einheit der Ordnung $\mathfrak{o}'$ bedeutet.

Wir müssen nun das Hauptresultat der Theorie der Einheiten kurz in Erinnerung bringen. Es sei ν die Gesamtanzahl der $(2\nu - n)$ reellen Wurzeln und der $(n - \nu)$ Paare von je zwei konjugiert-imaginären Wurzeln $a \pm bi$ der irreduktiblen Gleichung $f(\Theta) = 0$, aus welcher der Körper Ω entsprungen ist (§ 1); behält man von jedem Paare imaginärer Wurzeln nur die eine bei, so bleiben ν Wurzeln übrig, die mit

$$\Theta', \Theta'' \cdots \Theta^{(\nu)}$$

bezeichnet werden mögen. Ist nun $\varepsilon = \varphi(\Theta)$ eine beliebige Einheit des Körpers Ω, so soll durch das Symbol $l'(\varepsilon)$ der reelle Teil des

Logarithmen von $\varphi(\Theta')$ oder das Doppelte dieses reellen Teils bezeichnet werden, je nachdem Θ' reell oder imaginär ist, und die Symbole $l''(\varepsilon), l'''(\varepsilon) \cdots l^{(\nu)}(\varepsilon)$ sollen die entsprechende Bedeutung in bezug auf die anderen Wurzeln $\Theta'', \Theta''' \cdots \Theta^{(\nu)}$ haben. Dann folgt aus $N(\varepsilon) = 1$, daß immer

$$l'(\varepsilon) + l''(\varepsilon) + \cdots + l^{(\nu)}(\varepsilon) = 0$$

ist. Es wird nun zunächst bewiesen (D. § 166, 5.), daß es in jeder Ordnung $\mathfrak{o}'$ immer $(\nu - 1)$ voneinander unabhängige, d. h. solche Einheiten $\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}'$ gibt, für welche die Determinante

$$\sum \pm l'(\varrho_1') l'(\varrho_2') \cdots l^{(\nu-1)}(\varrho_{\nu-1}'),$$

welche wir zur Abkürzung mit

$$L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')$$

bezeichnen wollen, einen von 0 verschiedenen (positiven) Wert besitzt. Läßt man nun $u_1, u_2 \cdots u_{\nu-1}$ alle ganzen rationalen Zahlen durchlaufen, so erhält man eine Gruppe R' von unendlich vielen in $\mathfrak{o}'$ enthaltenen Einheiten

$$\varrho_1'^{u_1} \varrho_2'^{u_2} \cdots \varrho_{\nu-1}'^{u_{\nu-1}},$$

die sich durch Multiplikation und Division reproduzieren; je zwei verschiedenen Systemen von Exponenten entsprechen zwei verschiedene Individuen der Gruppe R'. Die Einheiten $\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}'$, welche eine Basis der Gruppe R' bilden, können offenbar ohne Änderung von R' und $L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')$ durch je $(\nu - 1)$ Einheiten ersetzt werden, welche aus R' so ausgewählt sind, daß die aus den zugehörigen $(\nu - 1)^2$ Exponenten u gebildete Determinante $= 1$ wird. Bezeichnet man mit $R'\alpha$ den Inbegriff aller Produkte aus einer bestimmten Zahl α und jeder der in R' enthaltenen Einheiten, so sind zwei solche Komplexe entweder gänzlich identisch, oder sie haben keine einzige Zahl gemeinschaftlich; das System aller Einheiten ε' der Ordnung $\mathfrak{o}'$ besteht (D. § 166, 6.) aus einer endlichen, von R' abhängigen Anzahl r' solcher Komplexe, woraus leicht folgt, daß $\varepsilon'^{r'}$ stets der Gruppe R' angehört. Hieraus ergibt sich unmittelbar, daß unter allen Systemen von $(\nu - 1)$ unabhängigen Einheiten der Ordnung $\mathfrak{o}'$ auch solche Systeme $\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}'$ existieren, für welche die Determinante $L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')$ einen Minimumwert erhält; dann besteht das System aller Einheiten ε' der Ordnung $\mathfrak{o}'$ aus r' Komplexen von der Form

$$R', R'\varrho', R'\varrho'^2 \cdots R'\varrho'^{r'-1},$$

wo ϱ' eine primitive Wurzel der Gleichung $\varrho'^{r'} = 1$ bedeutet (D. § 166, 7.). Ein solches System von $(\nu - 1)$ unabhängigen Einheiten $\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1}$ heißt ein Fundamental-System der Ordnung $\mathfrak{o}'$, und wir wollen zur Abkürzung den durch die Ordnung $\mathfrak{o}'$ vollständig bestimmten Quotienten

$$\frac{L(\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1})}{r'} = \mathrm{E}(\mathfrak{o}')$$

setzen*). Es würde sich, wie wir beiläufig bemerken, durch Betrachtungen, welche den gleich folgenden sehr ähnlich sind (vgl. D. § 161), auch leicht beweisen lassen, daß Zähler und Nenner dieses Quotienten sich mit einer und derselben ganzen rationalen Zahl multiplizieren, wenn das Fundamental-System $\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1}$ durch ein beliebiges System von $(\nu - 1)$ unabhängigen Einheiten der Ordnung $\mathfrak{o}'$ ersetzt wird. Wir wollen nun beweisen, daß die in dem Verhältnis $h' : h = m$ auftretende Anzahl s der Komplexe $\varepsilon' \varepsilon_1$, $\varepsilon' \varepsilon_2 \cdots \varepsilon' \varepsilon_s$, aus welchen das System aller Einheiten ε der Ordnung $\mathfrak{o}$ besteht,

$$= \frac{\mathrm{E}(\mathfrak{o}')}{\mathrm{E}(\mathfrak{o})}$$

ist.

Zu diesem Zwecke bezeichnen wir mit $\varrho_1, \varrho_2 \cdots \varrho_{\nu-1}$ ein Fundamental-System von Einheiten der Ordnung $\mathfrak{o}$, mit R die zugehörige Gruppe der aus ihnen durch Multiplikation und Division gebildeten Einheiten, und mit r die Anzahl der Komplexe

$$R,\ R\varrho,\ R\varrho^2 \cdots R\varrho^{r-1},$$

aus welchen das System aller Einheiten ε der Ordnung $\mathfrak{o}$ besteht, wo nun ϱ eine primitive Wurzel der Gleichung $\varrho^r = 1$ bedeutet. Unter diesen Einheiten ε befinden sich auch alle Einheiten ε' der Ordnung $\mathfrak{o}'$, weil $\mathfrak{o}'$ durch $\mathfrak{o}$ teilbar ist. Ist nun e ein bestimmter Index aus der Reihe $0, 1, 2 \cdots (\nu - 1)$, so gibt es unter allen denjenigen Einheiten von der Form

$$\sigma'_e = \varrho^u \varrho_1^{u_1} \varrho_2^{u_2} \cdots \varrho_e^{u_e},$$

welche, wie z. B. ϱ_e^s, auch der Ordnung $\mathfrak{o}'$ angehören, mindestens eine

$$\varrho'_e = \varrho^{a^{(e)}} \varrho_1^{a_1^{(e)}} \varrho_2^{a_2^{(e)}} \cdots \varrho_e^{a_e^{(e)}},$$

*) In dem singulären Falle eines imaginären quadratischen Körpers ($n = 2$, $\nu = 1$) besteht R' aus der einzigen Einheit 1, r' bedeutet die endliche Anzahl aller in $\mathfrak{o}'$ enthaltenen Einheiten, und die Determinante $L(\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1})$ ist durch 1 zu ersetzen.

in welcher der letzte Exponent u_e seinen kleinsten positiven Wert $a_e^{(e)}$ erreicht, und es leuchtet ein, daß in jeder anderen Einheit σ'_e der letzte Exponent u_e notwendig durch $a_e^{(e)}$ teilbar, also von der Form $a_e^{(e)} x_e$ sein muß, wo x_e eine ganze rationale Zahl bedeutet; es wird daher

$$\sigma'_e \varrho'^{-x_e}_e$$

eine in $\mathfrak{o}'$ enthaltene Einheit von der Form σ'_{e-1}, oder $= 1$ sein, wenn $e = 0$ ist. In diesem letzteren Falle ist

$$\varrho' = \varrho^a,$$

und da $\varrho^r = 1$ eine Einheit der Ordnung $\mathfrak{o}'$ ist, so muß r durch a teilbar, also

$$r = ar'$$

sein, und folglich ist ϱ' eine primitive Wurzel der Gleichung $\varrho'^{r'} = 1$. Hat man nun nach der obigen Vorschrift für jeden Index $e = 0, 1, 2 \cdots (\nu - 1)$ eine solche partikuläre Einheit ϱ', ϱ'_1, $\varrho'_2 \cdots \varrho'_{\nu-1}$ der Ordnung $\mathfrak{o}'$ aufgestellt, so ergibt sich, daß jede Einheit ε' der Ordnung $\mathfrak{o}'$, d. h. jede Einheit $\sigma'_{\nu-1}$, von der Form

$$\sigma'_{\nu-2} \varrho'^{x_{\nu-1}}_{\nu-1} = \sigma'_{\nu-3} \varrho'^{x_{\nu-2}}_{\nu-2} \varrho'^{x_{\nu-1}}_{\nu-1} = \text{usw.},$$

also schließlich von der Form

$$\varepsilon' = \varrho'^{x} \varrho_1'^{x_1} \varrho_2'^{x_2} \cdots \varrho_{\nu-1}'^{x_{\nu-1}}$$

ist, wo $x, x_1, x_2 \cdots x_{\nu-1}$ ganze rationale Zahlen bedeuten, deren erste x auf die r' Werte $0, 1, 2 \cdots (r' - 1)$ einzuschränken ist; umgekehrt leuchtet ein, daß alle Zahlen ε' von der vorstehenden Form auch wirklich Einheiten der Ordnung $\mathfrak{o}'$ sind. Da die Zahlen $a, a'_1, a''_2 \cdots a_{\nu-1}^{(\nu-1)}$ sämtlich positiv sind, so ist auch ihr Produkt

$$A = a a'_1 a''_2 \cdots a_{\nu-1}^{(\nu-1)}$$

positiv; nun ergibt sich aus der Bildung der Einheiten $\varrho'_1, \varrho''_2 \cdots \varrho'_{\nu-1}$, daß

$$L(\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1}) = \frac{A}{a} L(\varrho_1, \varrho_2 \cdots \varrho_{\nu-1})$$

einen von 0 verschiedenen, positiven Wert hat; mithin bilden dieselben ein System von $(\nu - 1)$ unabhängigen Einheiten der Ordnung $\mathfrak{o}'$, ja sogar ein Fundamental-System, weil für jedes beliebige System von $(\nu - 1)$ Einheiten $\varepsilon'_1, \varepsilon'_2 \cdots \varepsilon'_{\nu-1}$ dieser Ordnung $\mathfrak{o}'$ offenbar $L(\varepsilon'_1, \varepsilon'_2 \cdots \varepsilon'_{\nu-1}) = pL(\varrho'_1, \varrho'_2 \cdots \varrho'_{\nu-1})$ wird, wo p eine ganze rationale Zahl bedeutet. Bezeichnet man wieder mit R' die Gruppe aller Einheiten, welche

aus $\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}'$ durch Multiplikation und Division gebildet werden können, so besteht das System aller Einheiten ε' der Ordnung $\mathfrak{o}'$ aus den r' verschiedenen Komplexen

$$R', R'\varrho', R'\varrho'^2 \cdots R'\varrho'^{r'-1}.$$

Da ferner oben $r = ar'$ gefunden ist, so ergibt sich aus der vorhergehenden Gleichung

$$\mathrm{E}(\mathfrak{o}') = A\,\mathrm{E}(\mathfrak{o}).$$

Nun ist offenbar A die Anzahl aller derjenigen in $\mathfrak{o}$ enthaltenen Einheiten

$$\varepsilon_0 = \varrho^v \varrho_1^{v_1} \varrho_2^{v_2} \cdots \varrho_{\nu-1}^{v_{\nu-1}},$$

deren Exponenten den Bedingungen

$$0 \leqq v < a, \quad 0 \leqq v_1 < a_1' \cdots 0 \leqq v_{\nu-1} < a_{\nu-1}^{(\nu-1)}$$

genügen. Da ferner jede Einheit der Ordnung $\mathfrak{o}'$ die Form

$$\varepsilon' = \varrho'^x \varrho_1'^{x_1} \varrho_2'^{x_2} \cdots \varrho_{\nu-1}'^{x_{\nu-1}} = \varrho^w \varrho_1^{w_1} \varrho_2^{w_2} \cdots \varrho_{\nu-1}^{w_{\nu-1}}$$

hat, wo

$$\begin{aligned}
w_{\nu-1} &= a_{\nu-1}^{(\nu-1)} x_{\nu-1} \\
w_{\nu-2} &= a_{\nu-2}^{(\nu-1)} x_{\nu-1} + a_{\nu-2}^{(\nu-2)} x_{\nu-2} \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
w_1 &= a_1^{(\nu-1)} x_{\nu-1} + a_1^{(\nu-2)} x_{\nu-2} + \cdots + a_1' x_1 \\
w &= a^{(\nu-1)} x_{\nu-1} + a^{(\nu-2)} x_{\nu-2} + \cdots + a' x_1 + a x
\end{aligned}$$

ist, so kann man, wenn eine beliebige Einheit

$$\varepsilon = \varrho^u \varrho_1^{u_1} \varrho_2^{u_2} \cdots \varrho_{\nu-1}^{u_{\nu-1}}$$

der Ordnung $\mathfrak{o}$ gegeben ist, die Einheit ε', d. h. die Exponenten $x_{\nu-1}, x_{\nu-2} \cdots x_1, x$ stets und nur auf einzige Weise so wählen, daß die Zahlen

$$v = u - w, \quad v_1 = u_1 - w_1 \cdots v_{\nu-1} = u_{\nu-1} - w_{\nu-1}$$

den obigen Bedingungen genügen, daß also $\varepsilon\varepsilon'^{-1}$ eine der A Einheiten ε_0 wird; jede Einheit ε der Ordnung $\mathfrak{o}$ läßt sich daher stets und nur auf eine einzige Weise in die Form $\varepsilon'\varepsilon_0$ setzen, wo ε' eine Einheit in $\mathfrak{o}'$, ε_0 eine der obigen A Einheiten in $\mathfrak{o}$ bedeutet. Durchläuft ε' alle Einheiten der Ordnung $\mathfrak{o}'$, während ε_0 konstant bleibt, so erhält man einen Komplex von unendlich vielen Einheiten $\varepsilon = \varepsilon'\varepsilon_0$, und zwei solche Komplexe, welche zwei verschiedenen Werten von ε_0 entsprechen, sind gänzlich verschieden voneinander; mithin besteht

das System aller Einheiten ε der Ordnung $\mathfrak{o}$ aus A solchen Komplexen. Aber es ist oben gezeigt, daß die Anzahl dieser Komplexe $= s$ ist; mithin ist $s = A$, d. h.

$$s = \frac{\mathrm{E}(\mathfrak{o}')}{\mathrm{E}(\mathfrak{o})},$$

was zu beweisen war.

Hiernach nimmt das frühere Resultat für das Verhältnis der Klassenanzahlen die folgende Form an

$$\frac{h'}{h} = m = \frac{\psi(\mathfrak{k})}{\psi'(\mathfrak{k})} \cdot \frac{\mathrm{E}(\mathfrak{o})}{\mathrm{E}(\mathfrak{o}')},$$

in welcher die Lösung unseres Problems nach der Methode von Gauß enthalten ist.

§ 11.

Zerlegbare Formen, welche den Idealen von beliebiger Ordnung entsprechen.

Bevor wir zu der Ableitung desselben Resultates nach der Methode von Dirichlet übergehen, wird es zweckmäßig sein, mit einigen Worten den Zusammenhang zwischen den Idealen von beliebiger Ordnung und den zerlegbaren Formen des Körpers Ω zu besprechen.

Bilden die Zahlen $\omega_1, \omega_2 \cdots \omega_n$ eine bestimmte Basis der aus allen ganzen Zahlen des Körpers bestehenden Ordnung $\mathfrak{o}$, so wollen wir die n Basiszahlen

$$\omega_i' = k_1^{(i)} \omega_1 + k_2^{(i)} \omega_2 + \cdots + k_n^{(i)} \omega_n$$

der Ordnung $\mathfrak{o}'$ (§ 3) und die n Basiszahlen

$$\alpha_i' = a_1^{(i)} \omega_1' + a_2^{(i)} \omega_2' + \cdots + a_n^{(i)} \omega_n'$$

eines Ideals $\mathfrak{a}'$ in $\mathfrak{o}'$ (§ 4) immer so wählen, daß die Determinanten

$$\begin{aligned}
\sum \pm k_1' k_2'' \cdots k_n^{(n)} &= (\mathfrak{o}, \mathfrak{o}') = k, \\
\sum \pm a_1' a_2'' \cdots a_n^{(n)} &= (\mathfrak{o}', \mathfrak{a}') = N'(\mathfrak{a}')
\end{aligned}$$

werden, also positive Werte erhalten.

Die sämtlichen Zahlen des Ideals $\mathfrak{a}'$ sind von der Form

$$\alpha' = x_1 \alpha_1' + x_2 \alpha_2' + \cdots + x_n \alpha_n',$$

wo die Variablen $x_1, x_2 \cdots x_n$ alle ganzen rationalen Zahlen durchlaufen, und es ergibt sich, genau wie für die Ideale in $\mathfrak{o}$ (D. § 165), daß

$$N(\alpha') = N'(\mathfrak{a}')X$$

ist, wo X eine homogene Funktion n-ten Grades der n Variablen $x_1, x_2 \cdots x_n$ mit ganzen rationalen Koeffizienten bedeutet, welche, wie aus § 6 folgt, keinen gemeinschaftlichen Teiler haben; die Determinante dieser Form X (§ 1) ist

$$= D(\mathfrak{o}, \mathfrak{o}')^2 = Dk^2,$$

wo $D = \Delta(\Omega)$ wieder die Grundzahl des Körpers Ω bedeutet. Alle Formen X, welche allen verschiedenen Basen aller mit $\mathfrak{a}'$ äquivalenten Ideale entsprechen, sind äquivalent, d. h. sie gehen durch lineare Substitutionen mit ganzen rationalen Koeffizienten, deren Determinanten $= +1$ sind, ineinander über; jeder Idealklasse entspricht also eine bestimmte Formenklasse. Der Multiplikation zweier Ideale $\mathfrak{a}'$, $\mathfrak{b}''$ der Ordnungen $\mathfrak{o}'$, $\mathfrak{o}''$ oder der Komposition der sie enthaltenden Idealklassen A', B'' entspricht die Komposition der zu den Idealen $\mathfrak{a}'\,\mathfrak{b}''$ gehörigen Formen X, Y zu einer dem Ideal $\mathfrak{a}'\,\mathfrak{b}''$ entsprechenden Form Z, deren Determinante

$$= D(\mathfrak{o}, \mathfrak{o}'\,\mathfrak{o}'')^2$$

ist, und zugleich folgt hieraus die Komposition der Formenklassen*).

Um die Rückkehr von diesen allgemeinen Untersuchungen zu dem Falle der quadratischen Körper und Formen zu erleichtern, füge ich noch folgende Bemerkungen hinzu, von deren Richtigkeit man sich leicht überzeugen wird (vgl. D. §§ 168 bis 170). Jede Wurzel einer irreduktiblen quadratischen Gleichung ist von der Form $a + b\sqrt{c}$, wo c eine ganze rationale Zahl bedeutet, welche keine Quadratzahl und auch durch keine Quadratzahl außer 1 teilbar ist; a und b sind rationale Zahlen, und b ist von 0 verschieden. Die Grundzahl D des quadratischen Körpers Ω, welcher aus der Zahl $a + b\sqrt{c}$ entspringt, ist $= c$ oder $= 4c$, je nachdem $c \equiv 1$, oder $c \equiv 2, 3 \pmod 4$ ist; setzt man

$$\Theta = \frac{D + \sqrt{D}}{2},$$

so bilden die Zahlen 1, Θ eine Basis der Ordnung $\mathfrak{o}$, welche aus allen ganzen Zahlen

$$\omega = \frac{t + u\sqrt{D}}{2}$$

*) Da, wie schon oben (§ 7, Anmerkung) bemerkt ist, Moduln existieren, welche keinem Ideal äquivalent sind, so ist, was ich hervorheben zu müssen glaube, in dem Obigen noch nicht die Theorie aller zerlegbaren Formen enthalten, welche den sämtlichen Moduln eines Körpers Ω entsprechen.

des Körpers besteht, wo t, u alle, der Bedingung $t \equiv Du \pmod 2$ genügenden Paare von ganzen rationalen Zahlen zu durchlaufen haben. Jede Ordnung $\mathfrak{o}'$ ist dann von der Form $[1, k\Theta]$, wo $k = (\mathfrak{o}, \mathfrak{o}')$ eine beliebige positive ganze rationale Zahl bedeutet; der Führer k einer solchen Ordnung ist das Hauptideal $\mathfrak{o}k = [k, k\Theta]$, und es ist $N(\mathfrak{f}) = k^2$. Setzt man, wenn p eine positive rationale Primzahl bedeutet,

$$(D, p) = 0, +1 \text{ oder } -1,$$

je nachdem $\mathfrak{o}p$ das Quadrat eines Primideals, das Produkt aus zwei verschiedenen Primidealen, oder selbst ein Primideal ist (vgl. D. § 168), so ist

$$\psi(\mathfrak{o}k) = k^2 \prod \left(1 - \frac{1}{p}\right)\left(1 - \frac{(D, p)}{p}\right),$$

wo p alle verschiedenen in k aufgehenden Primzahlen durchläuft; da ferner jede Zahl der Ordnung $\mathfrak{o}'$ mit einer rationalen Zahl kongruent ist in bezug auf $\mathfrak{o}k$, so ist

$$\psi'(\mathfrak{o}k) = \varphi(k) = k \prod \left(1 - \frac{1}{p}\right),$$

und folglich

$$\frac{\psi(\mathfrak{o}k)}{\psi'(\mathfrak{o}k)} = k \prod \left(1 - \frac{(D, p)}{p}\right).$$

Ist nun der Körper Ω imaginär, also D negativ, so ist (vgl. § 10 Anmerkung)

$$\frac{\mathrm{E}(\mathfrak{o})}{\mathrm{E}(\mathfrak{o}')} = \frac{r'}{r},$$

wo r die Anzahl aller Einheiten in $\mathfrak{o}$, und r' die Anzahl aller Einheiten in $\mathfrak{o}'$ bedeutet. Die letztere Anzahl r' ist (wenn $\mathfrak{o}'$ von $\mathfrak{o}$ verschieden ist) immer $= 2$, und ebenso ist r immer $= 2$, ausgenommen die beiden Fälle $D = -3$, wo $r = 6$, und $D = -4$, wo $r = 4$ ist. Es ist daher im allgemeinen

$$\frac{h'}{h} = m = k \prod \left(1 - \frac{(D, p)}{p}\right),$$

aber dieses Produkt ist im Falle $D = -3$ durch 3, im Falle $D = -4$ durch 2 zu dividieren. Ist der Körper Ω reell, also D positiv, so ist $r = r' = 2$, und folglich

$$\frac{\mathrm{E}(\mathfrak{o})}{\mathrm{E}(\mathfrak{o}')} = \frac{\log \varepsilon}{\log \varepsilon'},$$

wo, wenn $k\sqrt{D} = \sqrt{D'}$ gesetzt wird,

$$\varepsilon = \frac{T + U\sqrt{D}}{2}, \quad \varepsilon' = \frac{T' + U'\sqrt{D'}}{2}$$

die Fundamentaleinheiten der Ordnungen $\mathfrak{o}$, $\mathfrak{o}'$ bedeuten, und man erhält

$$\frac{h'}{h} = \frac{\log \varepsilon}{\log \varepsilon'} \cdot k \prod \left(1 - \frac{(D, p)}{p}\right).$$

Was das Zeichen (D, p) betrifft, so ist sein Wert $= 0$, wenn p in D aufgeht; ist $p = 2$ und D ungerade, also $D \equiv 1 \pmod 4$, so ist $(D, p) = +1$ oder $= -1$, je nachdem $D \equiv 1 \pmod 8$ oder $D \equiv 5 \pmod 8$; ist endlich p ungerade, und D nicht teilbar durch p, so ist unter Anwendung der Bezeichnung von Legendre

$$(D, p) = \left(\frac{D}{p}\right).$$

Jeder Idealklasse in $\mathfrak{o}'$ entspricht nach den obigen Festsetzungen eine Klasse von äquivalenten quadratischen Formen $ax^2 + bxy + cy^2$, deren konstante Koeffizienten a, b, c ganze rationale Zahlen ohne gemeinschaftlichen Teiler sind, und die gemeinschaftliche Determinante*) dieser Formen ist $D' = b^2 - 4ac = Dk^2$; wenn D negativ ist, so treten nur sogenannte positive, d. h. solche Formen auf, deren äußere Koeffizienten a, c positiv sind. Umgekehrt entspricht eine bestimmte Klasse von äquivalenten quadratischen Formen, deren Determinante D' keine Quadratzahl ist, immer einer und nur einer Idealklasse eines quadratischen Körpers Ω, und wenn $\mathfrak{o}'$ die Ordnung dieser Idealklasse bedeutet, so ist $D' = D(\mathfrak{o}, \mathfrak{o}')^2 = Dk^2$, wo D die Grundzahl von Ω ist. Mithin sind in den obigen Formeln die verschiedenen Sätze enthalten, welche sich auf die Anzahl der quadratischen Formen in verschiedenen Ordnungen und auf die Unterscheidung der eigentlich und uneigentlich primitiven Formen beziehen.

§ 12.

Methode von Dirichlet.

Wir wenden uns nun der zweiten Lösung desselben allgemeinen Problems zu, welche auf den von Dirichlet eingeführten Prinzipien

*) Es ist wohl darauf zu achten, daß die hier im Sinne von § 1 definierte Determinante das Vierfache der Zahl ist, welche von Gauß die Determinante der Form genannt wird, während der Begriff der (eigentlichen) Äquivalenz der Formen derselbe bleibt.

beruht. Durchläuft $\mathfrak{a}'$ alle Ideale der Ordnung $\mathfrak{o}'$, so konvergiert die Reihe

$$S' = \sum \frac{s-1}{N'(\mathfrak{a}')^s}$$

für alle positiven Werte von $(s-1)$; denn weil $N'(\mathfrak{a}') = N(\mathfrak{o}\,\mathfrak{a}')$ ist (§ 5, 1°), so bilden die Glieder dieser Reihe nur einen Teil der gleichfalls aus lauter positiven Gliedern bestehenden Reihe

$$S = \sum \frac{s-1}{N(\mathfrak{a})^s},$$

in welcher $\mathfrak{a}$ alle Ideale der Ordnung $\mathfrak{o}$ durchläuft, und deren Konvergenz schon früher bewiesen ist (D. § 167); übrigens ergibt sich die Konvergenz der Reihe S' auch aus den weiter unten folgenden Untersuchungen.

Unsere Hauptaufgabe besteht darin, den Grenzwert zu ermitteln, welchem die Summe S' sich für unendlich kleine positive Werte von $(s-1)$ annähert. Zu diesem Zwecke betrachten wir aber zunächst nur denjenigen Teil S'' der Reihe S', welcher allen, durch ein gegebenes Ideal $\mathfrak{m}'$ der Ordnung $\mathfrak{o}'$ teilbaren Hauptidealen $\mathfrak{a}'$ entspricht. Die allgemeine Form dieser Ideale $\mathfrak{a}'$ ergibt sich auf die folgende Weise.

1. Jedes Ideal $\mathfrak{a}'$ ist von der Form $\mu\mathfrak{o}'$, wo μ eine in $\mathfrak{o}'$ enthaltene Zahl bedeutet, welche relative Primzahl zu dem Führer $\mathfrak{f}$ der Ordnung $\mathfrak{o}'$ ist.

2. Die Zahl μ muß in dem gegebenen Ideal $\mathfrak{m}'$ enthalten sein.

3. Die Norm der Zahl μ muß positiv sein.

Umgekehrt, wenn μ diese drei Bedingungen erfüllt, so ist $\mu\mathfrak{o}'$ jedenfalls eins von den Idealen $\mathfrak{a}'$, auf welche sich die Summe S'' erstreckt.

Bilden nun die Zahlen $\mu_1, \mu_2 \cdots \mu_n$ eine Basis des gegebenen Ideals $\mathfrak{m}'$, so ist zur Erfüllung der Bedingung 2 erforderlich und hinreichend, daß

$$\mu = m_1\mu_1 + m_2\mu_2 + \cdots + m_n\mu_n$$

sei, wo $m_1, m_2 \cdots m_n$ ganze rationale Zahlen bedeuten, und da $\mathfrak{m}'$ durch $\mathfrak{o}'$ teilbar ist, so ist jede solche Zahl μ auch in $\mathfrak{o}'$ enthalten. Aber sie soll zufolge 1. auch relative Primzahl zu $\mathfrak{f}$ sein. Bezeichnen wir nun wieder (wie in § 9) mit $\psi'(\mathfrak{f})$ die Anzahl aller in $\mathfrak{o}'$ ent-

haltenen Zahlen ω', welche inkongruent in bezug auf $\mathfrak{k}$ und zugleich relative Primzahlen zu $\mathfrak{k}$ sind, so muß gleichzeitig

$$\mu \equiv \omega' \pmod{\mathfrak{k}}, \quad \mu \equiv 0 \pmod{\mathfrak{m}'}$$

sein; da $\mathfrak{k} + \mathfrak{m}' = \mathfrak{o}'$ ist, so gibt es (nach § 2, 2^0) immer Zahlen μ, welche einem solchen Kongruenzpaar genügen, und sie bilden eine bestimmte Zahlklasse in bezug auf den Modul $\mathfrak{k} - \mathfrak{m}'$, welcher offenbar $= \mathfrak{k}\mathfrak{m}'$ ist; denn da $\mathfrak{m}' > \mathfrak{o}\mathfrak{m}'$ ist, so ist $\mathfrak{k} - \mathfrak{m}'$ ein gemeinschaftliches Vielfaches der beiden relativen Primideale $\mathfrak{k}, \mathfrak{o}\mathfrak{m}'$, also auch ein Vielfaches ihres Produkts $\mathfrak{k}\mathfrak{o}\mathfrak{m}' = \mathfrak{k}\mathfrak{m}'$, und umgekehrt ist $\mathfrak{k}\mathfrak{m}'$ ein gemeinschaftliches Vielfaches von $\mathfrak{k}$ und $\mathfrak{m}'$, weil $\mathfrak{m}' > \mathfrak{o}$, $\mathfrak{k} > \mathfrak{o}'$ und $\mathfrak{k}\mathfrak{o} = \mathfrak{k}$, $\mathfrak{o}'\mathfrak{m}' = \mathfrak{m}'$ ist. Die sämtlichen Zahlen μ, welche den Bedingungen 1 und 2 genügen, bilden daher $\psi'(\mathfrak{k})$ verschiedene Zahlklassen (mod. $\mathfrak{k}\mathfrak{m}'$). Jede solche Zahlklasse besteht aber, weil $k\mathfrak{m}' > \mathfrak{k}\mathfrak{m}''$ ist, aus $(\mathfrak{k}\mathfrak{m}, k\mathfrak{m}')$ verschiedenen Zahlklassen (mod. $k\mathfrak{m}'$), und folglich ist

$$c = \psi'(\mathfrak{k})\,(\mathfrak{k}\mathfrak{m}', k\mathfrak{m}')$$

die Anzahl der Zahlklassen (mod. $k\mathfrak{m}'$), aus welchen das System aller dieser Zahlen μ besteht. Es läßt sich leicht zeigen, daß diese Anzahl c von $\mathfrak{m}'$ unabhängig ist. In der Tat, aus

$$(\mathfrak{o}, \mathfrak{m}') = (\mathfrak{o}, \mathfrak{o}')\,(\mathfrak{o}', \mathfrak{m}') = (\mathfrak{o}, \mathfrak{o}\mathfrak{m}')\,(\mathfrak{o}\mathfrak{m}', \mathfrak{m}')$$

folgt

$$k\,N'(\mathfrak{m}') = N(\mathfrak{o}\mathfrak{m}')\,(\mathfrak{o}\mathfrak{m}', \mathfrak{m}'),$$

mithin, weil $N'(\mathfrak{m}') = N(\mathfrak{o}\mathfrak{m}')$ ist (§ 5, 1^0), $(\mathfrak{o}\mathfrak{m}', \mathfrak{m}') = k$, also auch

$$(k\mathfrak{o}\mathfrak{m}', k\mathfrak{m}') = k,$$

weil offenbar für je zwei Moduln $\mathfrak{a}, \mathfrak{b}$ der Satz $(\eta\mathfrak{a}, \eta\mathfrak{b}) = (\mathfrak{a}, \mathfrak{b})$ gilt, sobald η eine von 0 verschiedene Zahl ist. Da ferner

$$(\mathfrak{o}, k\mathfrak{o}\mathfrak{m}') = (\mathfrak{o}, \mathfrak{k}\mathfrak{m}')\,(\mathfrak{k}\mathfrak{m}', k\mathfrak{o}\mathfrak{m}'),$$

also

$$(\mathfrak{k}\mathfrak{m}', k\mathfrak{o}\mathfrak{m}') = \frac{N(k\mathfrak{o}\mathfrak{m}')}{N(\mathfrak{k}\mathfrak{m}')} = \frac{N(k\mathfrak{o})}{N(\mathfrak{k})} = \frac{k^n}{N(\mathfrak{k})}$$

ist, so ergibt sich

$$(\mathfrak{k}\mathfrak{m}', k\mathfrak{m}') = (\mathfrak{k}\mathfrak{m}', k\mathfrak{o}\mathfrak{m}')\,(k\mathfrak{o}\mathfrak{m}', k\mathfrak{m}') = \frac{k^{n+1}}{N(\mathfrak{k})},$$

und folglich ist

$$c = \frac{\psi'(\mathfrak{k})}{N(\mathfrak{k})}\,k^{n+1}$$

die Anzahl der fraglichen Zahlklassen in bezug auf den Modul

$$k\mathfrak{m}' = [k\mu_1, k\mu_2 \cdots k\mu_n].$$

Wählt man aus jeder dieser Klassen einen bestimmten Repräsentanten

$$a_1\mu_1 + a_2\mu_2 + \cdots + a_n\mu_n,$$

so werden alle Zahlen μ derselben Klasse durch die Form

$$\text{(I)} \qquad \mu = (a_1 + kz_1)\,\mu_1 + (a_2 + kz_2)\,\mu_2 + \cdots + (a_n + kz_n)\,\mu_n$$

erzeugt, wenn $z_1, z_2 \cdots z_n$ alle ganzen rationalen Zahlen durchlaufen; und die sämtlichen Zahlen μ, welche den Bedingungen 1 und 2 genügen, werden durch c solche lineare Formen erzeugt, und zwar jede nur einmal.

Von diesen Zahlen μ sind aber nur diejenigen beizubehalten, welche auch der dritten Bedingung

$$\text{(II)} \qquad N(\mu) > 0$$

genügen. Umgekehrt erzeugt jede solche Zahl μ ein Hauptideal $\mu\mathfrak{o}'$ in $\mathfrak{o}'$, welches durch das gegebene Ideal $\mathfrak{m}'$ teilbar ist.

Aber es leuchtet ein, daß, wenn μ alle diese Zahlen durchläuft, jedes bestimmte, durch $\mathfrak{m}'$ teilbare Hauptideal $\mathfrak{a}'$ unendlich oft erzeugt wird. Ist nämlich μ_0 eine bestimmte von diesen Zahlen μ, so wird dasselbe Hauptideal $\mathfrak{o}'\mu_0$ offenbar durch alle, und nur durch die Zahlen μ erzeugt, welche von der Form $\mu = \varepsilon'\mu_0$ sind, wo ε' eine beliebige in $\mathfrak{o}'$ enthaltene Einheit (von positiver Norm) bedeutet. Um dies zu vermeiden, muß man den Zahlen μ neue Beschränkungen auferlegen. Zu diesem Zwecke kehren wir zu den Betrachtungen und Bezeichnungen des § 10 zurück und erweitern die Bedeutung der dort erklärten ν Symbole $l', l'' \cdots l^{(\nu)}$. Ist $\omega = \varphi(\Theta)$ eine beliebige von 0 verschiedene Zahl des Körpers Ω, und $\omega' = \varphi(\Theta')$, so verstehen wir unter $l'(\omega)$ den reellen Teil des Logarithmen von

$$\frac{\omega'}{\sqrt[n]{N(\omega)}}$$

oder das Doppelte dieses reellen Teiles, je nachdem Θ' eine reelle oder imaginäre Wurzel der irreduktiblen Gleichung $f(\Theta') = 0$ ist; legt man ferner den Symbolen $l''(\omega), l'''(\omega) \cdots l^{(\nu)}(\omega)$ die entsprechende Bedeutung in bezug auf die Wurzeln $\Theta'', \Theta''' \cdots \Theta^{(\nu)}$ bei, so ist offenbar

$$l'(\omega) + l''(\omega) + \cdots + l^{(\nu)}(\omega) = 0.$$

Bilden nun $\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}'$ ein bestimmtes Fundamentalsystem $\mathfrak{R}$ von Einheiten der Ordnung $\mathfrak{o}'$, so wollen wir unter den Exponenten

der Zahl ω in bezug auf $\mathfrak{N}$ diejenigen völlig bestimmten reellen Werte $x_1(\omega)$, $x_2(\omega) \cdots x_{\nu-1}(\omega)$ verstehen, welche den ν Gleichungen

$$\begin{array}{c} l'\,(\varrho_1')\,x_1(\omega) + l'\,(\varrho_2')\,x_2(\omega) + \cdots + l'\,(\varrho_{\nu-1}')\,x_{\nu-1}(\omega) = l'\,(\omega) \\ l''\,(\varrho_1')\,x_1(\omega) + l''(\varrho_2')\,x_2(\omega) + \cdots + l''(\varrho_{\nu-1}')\,x_{\nu-1}(\omega) = l''(\omega) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ l^{(\nu)}(\varrho_1')\,x_1(\omega) + l^{(\nu)}(\varrho_2')x_2(\omega) + \cdots + l^{(\nu)}(\varrho_{\nu-1}')\,x_{\nu-1}(\omega) = l^{(\nu)}(\omega) \end{array}$$

genügen, deren letzte eine Folge der übrigen ist. Da $l'(\alpha\beta) = l'(\alpha) + l'(\beta)$ ist, und dasselbe für die anderen Symbole l'', $l''' \cdots l^{(\nu)}$ gilt, so ist auch $x_1(\alpha\beta) = x_1(\alpha) + x_1(\beta)$, und dasselbe gilt auch für die anderen Exponenten x_2, $x_3 \ldots x_{\nu-1}$. Die Exponenten der Einheit

$$\varepsilon' = \varrho'^{u}\,\varrho_1'^{u_1}\,\varrho_2'^{u_2} \cdots \varrho'^{u_{\nu-1}}_{\nu-1},$$

wo ϱ' wieder eine primitive Wurzel der Gleichung $\varrho'^{r'} = 1$ bedeutet, sind offenbar die ganzen rationalen Zahlen u_1, $u_2 \cdots u_{\nu-1}$.

Ist nun μ_0 eine bestimmte der oben definierten Zahlen μ, d. h. eine Zahl, welche in einer der c linearen Formen (I) enthalten ist und zugleich der Bedingung (II) genügt, so sind die sämtlichen Produkte $\mu = \varepsilon'\mu_0$, welche den sämtlichen Einheiten ε' der Ordnung $\mathfrak{o}'$ entsprechen, eben solche Zahlen, und alle diese Zahlen μ und keine anderen liefern, wie oben bemerkt, ein und dasselbe durch $\mathfrak{m}'$ teilbare Hauptideal $\mathfrak{a}' = \mathfrak{o}'\mu_0 = \mathfrak{o}'\mu$ der Ordnung $\mathfrak{o}'$. Da nun

$$x_1(\mu) = x_1(\mu_0) + u_1 \cdots x_{\nu-1}(\mu) = x_{\nu-1}(\mu_0) + u_{\nu-1}$$

ist, so kann man die ganzen rationalen Zahlen u_1, $u_2 \cdots u_{\nu-1}$ offenbar stets und nur auf eine einzige Art so wählen, daß

(III) $$0 \leqq x_1(\mu) < 1 \cdots 0 \leqq x_{\nu-1}(\mu) < 1$$

wird, und da hierbei der in ε' auftretende Faktor ϱ'^{u} seine sämtlichen r' Werte

$$1,\ \varrho',\ \varrho'^{2} \cdots \varrho'^{r'-1}$$

durchlaufen darf, so werden durch diese Bedingungen (III) aus dem System aller mit μ_0 assoziierten Zahlen $\mu = \varepsilon'\mu_0$ genau r' Zahlen μ herausgehoben, während alle übrigen ausgeschlossen werden. Läßt man daher μ alle diejenigen Zahlen durchlaufen, welche in den c linearen Formen (I) enthalten sind und zugleich den Bedingungen (II) und (III) genügen, so wird jedes durch $\mathfrak{m}'$ teilbare Hauptideal $\mathfrak{a}' = \mathfrak{o}'\mu$ der Ordnung $\mathfrak{o}'$ genau r'-mal erzeugt, und folglich ist der von uns betrachtete Teil S'' der Summe S' identisch mit

$$\frac{1}{r'} \sum \frac{s-1}{N'(\mathfrak{o}'\mu)^s} = \frac{1}{r'} \sum \frac{s-1}{N(\mu)^s}.$$

Nun zerlegen wir diese Summe abermals in c Partialsummen, indem wir jedesmal die Beiträge derjenigen Zahlen μ zu einer Partialsumme sammeln, welche in einer und derselben Linearform (I) enthalten sind und außerdem den Bedingungen (II) und (III) genügen. Es sei t eine beliebige positive Größe, und T die entsprechende Anzahl dieser Zahlen μ, für welche zugleich

(IV) $$N(\mu) \leqq t$$

wird, so wollen wir beweisen, daß der Quotient $T:t$ mit unendlich wachsendem t sich einem endlichen Grenzwerte nähert. Zu diesem Zwecke bezeichnen wir mit

$$h_1,\ h_2 \cdots h_n$$

ein System von reellen, stetig veränderlichen Größen und betrachten die n homogenen linearen Funktionen ω', $\omega'' \cdots \omega^{(n)}$, welche aus

$$\omega = h_1\mu_1 + h_2\mu_2 + \cdots + h_n\mu_n$$

dadurch hervorgehen, daß die dem Körper Ω angehörigen Konstanten μ_1, $\mu_2 \cdots \mu_n$ durch die mit ihnen konjugierten Zahlen ersetzt werden, welche der Reihe nach den Wurzeln Θ', $\Theta'' \cdots \Theta^{(n)}$ der Gleichung $f(\Theta) = 0$ entsprechen. Setzen wir auch in allen Fällen, wo die Werte der Variablen h_1, $h_2 \cdots h_n$ nicht sämtlich rational sind, der Kürze wegen

$$\omega'\omega'' \cdots \omega^{(n)} = N(\omega),$$

so ist $N(\omega)$ eine homogene Funktion n-ten Grades von den Variabeln h_1, $h_2 \cdots h_n$. Wir beschränken nun zunächst die Variabilität dieser Größen durch die Bedingung

(V) $$0 < N(\omega) \leqq 1$$

und definieren hierauf ein System von ν Funktionen

$$l'(\omega),\ l''(\omega) \cdots l^{(\nu)}(\omega)$$

und aus diesem ein System von $(\nu - 1)$ Funktionen

$$x_1(\omega),\ x_2(\omega) \cdots x_{\nu-1}(\omega)$$

genau nach denselben Regeln, wie dies oben für den Fall geschehen ist, daß die sämtlichen Variablen h_1, $h_2 \cdots h_n$ rationale Werte haben, und folglich ω eine Zahl des Körpers Ω ist. Hierauf beschränken

wir die Variabilität der Größen $h_1, h_2 \cdots h_n$ ferner durch die $(\nu - 1)$ Bedingungen

(VI) $$0 \leqq x_1(\omega) < 1 \cdots 0 \leqq x_{\nu-1}(\omega) < 1.$$

Hierdurch, sowie durch die Bedingung (V), ist den Variablen $h_1, h_2 \cdots h_n$ ein bestimmtes Gebiet G angewiesen, und zwar ist (vgl. D. § 167) das über dieses Gebiet G ausgedehnte n-fache Integral

$$g = \int dh_1\, dh_2 \cdots dh_n = \frac{\sigma L(\varrho_1', \varrho_2' \cdots \varrho_{\nu-1}')}{\sqrt{\pm \Delta}\,(\mu_1, \mu_2 \cdots \mu_n)} = \frac{\sigma r' \mathrm{E}(\mathfrak{o}')}{k N'(\mathfrak{m}')\sqrt{\pm D}},$$

wo $\sigma = 2^{r-1}\pi^{n-\nu}$, im Falle $n = 2\nu$ aber $= (2\pi)^\nu$ ist; $\sqrt{\pm D}$ bedeutet die positive Quadratwurzel aus dem absoluten Werte der Grundzahl D des Körpers Ω.

Die oben mit T bezeichnete Anzahl der in einer bestimmten Linearform (I) erhaltenen Zahlen μ, welche außerdem den Bedingungen (II), (III), (IV) genügen, besitzt nun die folgende Bedeutung für das eben definierte Gebiet G. Setzt man

$$h_1 = \frac{a_1 + kz_1}{\sqrt[n]{t}}, \quad h_2 = \frac{a_2 + kz_2}{\sqrt[n]{t}} \cdots h_n = \frac{a_n + kz_n}{\sqrt[n]{t}},$$

so bringt jedes System von n ganzen rationalen Zahlen $z_1, z_2 \cdots z_n$, welchem eine solche Zahl μ entspricht, ein System von n reellen Werten $h_1, h_2 \cdots h_n$ hervor, welches dem Gebiete G angehört; denn da $N(\omega)$ eine homogene Funktion n-ten Grades, jede der Funktionen $x_1(\omega), x_2(\omega) \cdots x_{\nu-1}(\omega)$ aber eine homogene Funktion 0-ten Grades von den Variablen $h_1, h_2 \cdots h_n$ ist, so gehen die Bedingungen (II) und (IV) in die Bedingung (V), und die Bedingungen (III) in die Bedingungen (VI) über. Setzt man ferner

$$\frac{k}{\sqrt[n]{t}} = \delta; \quad \frac{a_1}{\sqrt[n]{t}} = h_1^0, \quad \frac{a_2}{\sqrt[n]{t}} = h_2^0 \cdots \frac{a_n}{\sqrt[n]{t}} = h_n^0,$$

so ist das durch $z_1, z_2 \cdots z_n$ hervorgebrachte, dem Gebiet G angehörende Wertsystem $h_1, h_2 \cdots h_n$ von der Beschaffenheit, daß die Größen

$$\frac{h_1 - h_1^0}{\delta} = z_1, \quad \frac{h_2 - h_2^0}{\delta} = z_2 \cdots \frac{h_n - h_n^0}{\delta} = z_n$$

ganze rationale Zahlen werden; und umgekehrt leuchtet ein, daß jedes dem Gebiet G angehörende Wertsystem $h_1, h_2 \cdots h_n$, welches dieser letzten Bedingung genügt, rückwärts ein System von ganzen rationalen Zahlen $z_1, z_2 \cdots z_n$ und dadurch eine Zahl μ der Linearform (I) hervorbringt, welche auch den Bedingungen (II), (III), (IV) genügt. Mithin ist T die Anzahl derjenigen dem Gebiet G angehörenden Wertsysteme $h_1, h_2 \cdots h_n$, für welche die Quotienten

$$\frac{h_1 - h_1^0}{\delta}, \quad \frac{h_2 - h_2^0}{\delta} \cdots \frac{h_n - h_n^0}{\delta}$$

ganze rationale Zahlen werden. Wächst nun t über alle Grenzen, so wird δ unendlich klein, und aus dem Begriffe eines n-fachen bestimmten Integrals ergibt sich, daß

$$\lim (T\delta^n) = k^n \lim \left(\frac{T}{t}\right) = \int dh_1\, dh_2 \cdots dh_n = g$$

ist, mögen die Größen $h_1^0, h_2^0 \cdots h_n^0$ von δ unabhängig sein oder nicht. Nach einem Fundamentalsatze von Dirichlet (D. § 118) folgt hieraus, daß die auf alle Zahlen μ der einen Linearform (I) ausgedehnte Partialsumme

$$\frac{1}{r'} \sum \frac{s-1}{N(\mu)^s}$$

für alle positiven Werte von $(s-1)$ konvergiert und für unendlich kleine Werte von $(s-1)$ sich dem Grenzwerte

$$\frac{1}{r'} \lim \left(\frac{T}{t}\right) = \frac{g}{k^n r'} = \frac{\sigma \mathrm{E}(\mathfrak{o}')}{k^{n+1} N'(\mathfrak{m}')\sqrt{\pm D}}$$

nähert. Da derselbe von den Zahlen $a_1, a_2 \cdots a_n$, welche diese eine Linearform charakterisieren, gänzlich unabhängig ist, und da die Anzahl der Partialsummen, aus welchen die bis jetzt von uns betrachtete Summe S'' besteht,

$$= c = \frac{\psi'(\mathfrak{k})}{N(\mathfrak{k})} k^{n+1}$$

ist, so erhalten wir das Resultat

$$\lim S'' = \lim \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \frac{\psi'(\mathfrak{k})}{N(\mathfrak{k})} \cdot \frac{\sigma \mathrm{E}(\mathfrak{o}')}{N'(\mathfrak{m}')\sqrt{\pm D}},$$

wo links die Summe über alle durch $\mathfrak{m}'$ teilbaren Hauptideale $\mathfrak{a}'$ der Ordnung $\mathfrak{o}'$ ausgedehnt ist.

§ 13.

Resultat dieser Methode.

Mit Hilfe des eben bewiesenen Satzes ist es leicht, unsere Aufgabe zu lösen. Nimmt man $\mathfrak{m}' = \mathfrak{o}'$, also $N'(\mathfrak{m}') = 1$, so ergibt sich

$$\lim \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \frac{\psi'(\mathfrak{f})}{N(\mathfrak{f})} \cdot \frac{\sigma \mathrm{E}(\mathfrak{o}')}{\sqrt{\pm D}},$$

wo die Summe links über alle Ideale $\mathfrak{a}'$ ausgedehnt ist, welche der Hauptklasse O' der Ordnung $\mathfrak{o}'$ angehören.

Nun sei B' eine beliebige Ideal-Klasse der Ordnung $\mathfrak{o}'$, und $\mathfrak{m}'$ ein bestimmtes Ideal der inversen Klasse B'^{-1}. Durchläuft $\mathfrak{b}'$ alle Ideale der Klasse B', während $\mathfrak{m}'$ unverändert bleibt, so werden die Produkte $\mathfrak{b}'\mathfrak{m}'$ lauter Hauptideale $\mathfrak{a}'$ der Ordnung $\mathfrak{o}'$, welche durch $\mathfrak{m}'$ teilbar sind; und umgekehrt, ist $\mathfrak{a}'$ ein durch $\mathfrak{m}'$ teilbares Hauptideal der Ordnung $\mathfrak{o}'$, so gibt es (nach § 5, 3°) ein und nur ein Ideal $\mathfrak{b}'$ in $\mathfrak{o}'$ von der Art, daß $\mathfrak{b}'\mathfrak{m}' = \mathfrak{a}'$ wird, und $\mathfrak{b}'$ muß notwendig der Klasse B' angehören, weil $\mathfrak{m}'$ ein Ideal der inversen Klasse ist. Da außerdem $N'(\mathfrak{b}'\mathfrak{m}') = N'(\mathfrak{b}')N'(\mathfrak{m}')$ ist, so ist die über alle Ideale $\mathfrak{b}'$ der Klasse B' ausgedehnte Summe

$$\sum \frac{s-1}{N'(\mathfrak{b}')^s} = N'(\mathfrak{m}')^s \sum \frac{s-1}{N'(\mathfrak{a}')^s},$$

wo $\mathfrak{a}'$ alle durch $\mathfrak{m}'$ teilbaren Hauptideale der Ordnung $\mathfrak{o}'$ durchläuft. Hieraus ergibt sich nach dem Schlußsatz des vorigen Paragraphen für unendlich kleine positive Werte von $(s-1)$

$$\lim \sum \frac{s-1}{N'(\mathfrak{b}')^s} = \frac{\psi'(\mathfrak{f})}{N(\mathfrak{f})} \cdot \frac{\sigma \mathrm{E}(\mathfrak{o}')}{\sqrt{\pm D}},$$

d. h. der Grenzwert der über alle Ideale einer beliebigen Klasse in $\mathfrak{o}'$ ausgedehnten Summe ist für jede Klasse derselbe, und zwar offenbar von 0 verschieden.

Für den Spezialfall, in welchem $\mathfrak{o}'$ das Gebiet $\mathfrak{o}$ aller ganzen Zahlen des Körpers Ω ist, ergibt sich hieraus, weil

$$\mathfrak{f} = \mathfrak{o}, \quad N(\mathfrak{f}) = \psi'(\mathfrak{f}) = 1$$

wird, und weil die Anzahl h aller Ideal-Klassen der Ordnung $\mathfrak{o}$ endlich ist (D. § 164), das Resultat

$$\lim S = \lim \sum \frac{s-1}{N(\mathfrak{a})^s} = h \frac{\sigma \mathrm{E}(\mathfrak{o})}{\sqrt{\pm D}},$$

wo die Summe über alle Ideale $\mathfrak{a}$ der Ordnung $\mathfrak{o}$ auszudehnen ist.

Durchläuft nun $\mathfrak{a}'$ alle Ideale der Ordnung $\mathfrak{o}'$, so durchläuft $\mathfrak{o}\mathfrak{a}'$ alle diejenigen Ideale der Ordnung $\mathfrak{o}$, welche relative Primideale zu dem Führer $\mathfrak{f}$ sind, und jedes nur ein einziges Mal. Da zugleich $N'(\mathfrak{a}') = N(\mathfrak{o}\mathfrak{a}')$ ist, so ist die über alle Ideale $\mathfrak{a}'$ der Ordnung $\mathfrak{o}'$ ausgedehnte Summe

$$S' = \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \sum \frac{s-1}{N(\mathfrak{o}\mathfrak{a}')^s};$$

durchläuft aber $\mathfrak{p}$ alle verschiedenen in $\mathfrak{f}$ aufgehenden Primideale in $\mathfrak{o}$, so ist nach den allgemeinen Gesetzen der Teilbarkeit die über alle Ideale $\mathfrak{a}$ der Ordnung $\mathfrak{o}$ ausgedehnte Summe

$$\sum \frac{1}{N(\mathfrak{a})^s} = \prod \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}} \cdot \sum \frac{1}{N(\mathfrak{o}\mathfrak{a}')^s} = \prod \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}} \cdot \sum \frac{1}{N'(\mathfrak{a}')^s},$$

und folglich, weil

$$\prod \left(1 - \frac{1}{N(\mathfrak{p})}\right) = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})}$$

ist,

$$\lim \sum \frac{s-1}{N'(\mathfrak{a}')^s} = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})} \lim \sum \frac{s-1}{N(\mathfrak{a})^s},$$

d. h.

$$\lim S' = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})} \lim S.$$

Da die rechte Seite einen endlichen Wert hat, so folgt zunächst, daß die Anzahl h' der Ideal-Klassen in $\mathfrak{o}'$ endlich sein muß, weil oben für jeden Bestandteil der linken Seite, welcher einer einzelnen Klasse entspricht, ein und derselbe von 0 verschiedene Grenzwert gefunden ist. Setzt man diesen Wert und ebenso den Grenzwert der rechten Seite ein, so ergibt sich

$$h' \frac{\psi'(\mathfrak{f})}{N(\mathfrak{f})} \cdot \frac{\sigma \mathrm{E}(\mathfrak{o}')}{\sqrt{\pm D}} = \frac{\psi(\mathfrak{f})}{N(\mathfrak{f})} \cdot h \frac{\sigma \mathrm{E}(\mathfrak{o})}{\sqrt{\pm D}},$$

und hieraus

$$\frac{h'}{h} = \frac{\psi(\mathfrak{f})}{\psi'(\mathfrak{f})} \cdot \frac{\mathrm{E}(\mathfrak{o})}{\mathrm{E}(\mathfrak{o}')},$$

was mit dem in § 10 nach der Methode von Gauß gefundenen Resultat übereinstimmt.

Erläuterungen zur vorstehenden Abhandlung.

Diese Abhandlung findet ihre Ergänzung in dem im Nachlaß veröffentlichten Überblick über die allgemeine Modultheorie (Brief an Frobenius von 1883); beides war — wie dort und an anderen Stellen ausgesprochen ist — gedacht als Grundlage für die allgemeinen Reziprozitätsgesetze.

In der Tat ist die in der Abhandlung behandelte Klasseneinteilung eine Strahlklasseneinteilung, wie sie der Klassenkörpertheorie zugrunde liegt, wenn auch noch nicht die allgemeinste. Der Ausdruck für das Verhältnis der Klassenanzahlen (§ 10, Schluß) findet sich genau in der allgemeingültigen Form; auch die gruppentheoretischen Beweismethoden sind ähnlich, wenn auch noch etwas komplizierter, als in der späteren allgemeinen Theorie (H. Weber, Math. Ann., Bd. 48, S. 433 ff.). In § 12 werden die transzendenten Methoden zum ersten Male auf solche allgemeineren Klasseneinteilungen übertragen, was später viel weitergehend von H. Weber im allgemeinsten Falle entwickelt wurde (Math. Ann., Bd. 49, S. 83 ff.). Auf Weber aber baut Takagi auf.

Idealtheoretisch liegt die Bedeutung der Abhandlung darin, daß zum ersten Male die Beziehung zwischen Idealen verschiedener Ringe vermöge Zuordnung von Durchschnitts- und Erweiterungsideal behandelt wird. Die hier entwickelten Begriffe lassen sich auf beliebige Ringe ausdehnen und führen zu einer Zuordnung von Klassen von Idealen im Unter- und Oberring, wobei wieder Durchschnitts-(Verengungs-)Ideal und Erweiterungsideal eine ausgezeichnete Rolle spielen (vgl. H. Grell, Beziehungen zwischen den Idealen verschiedener Ringe, Math. Ann., Bd. 97, 1927).

Noether.

XIII.

Erläuterungen zu zwei Fragmenten von Riemann.

[Bernhard Riemanns gesammelte mathematische Werke und wissenschaftlicher Nachlaß, 2. Aufl., S. 466—478 (1892)].

Die Entstehungszeit (September 1852) des ersten der beiden Fragmente[*)] macht es wahrscheinlich, daß Riemann darauf ausging, für die Abhandlung über die trigonometrischen Reihen[**)] Beispiele von Funktionen zu finden, die unendlich oft in jedem Intervall unstetig werden, und vielleicht sollte die zweite Untersuchung[***)], welche sich auf einem kaum leserlichen Blatte findet, demselben Zwecke dienen. Die hier von Riemann benutzte Methode zur Bestimmung des Verhaltens der in der Theorie der elliptischen Funktionen auftretenden Modulfunktionen für den Fall, daß das komplexe Periodenverhältnis

$$\omega = \frac{K'i}{K} = \frac{\log q}{\pi i} \tag{1}$$

sich einem rationalen Werte nähert, gestattet aber zugleich eine sehr interessante Anwendung auf die sogenannte Theorie der unendlich vielen Formen der ϑ-Funktionen, nämlich auf die Bestimmung der bei der Transformation erster Ordnung auftretenden Konstanten, welche bekanntlich von Jacobi und Hermite auf die Gaußschen Summen, also auf die Theorie der quadratischen Reste zurückgeführt ist. Die Darstellung dieses Zusammenhangs bildet den Gegenstand der folgenden Erläuterungen.

Den Mittelpunkt der Theorie dieser Modulfunktionen, welche man auch ganz unabhängig von der der elliptischen Funktionen aufstellen kann, und welche seit dem Erscheinen der ersten Auflage von Riemanns Werken der Gegenstand zahlreicher Untersuchungen geworden ist, bildet in gewissem Sinne die Funktion

$$\eta(\omega) = 1^{\frac{\omega}{24}} \Pi(1 - 1^{\omega\nu}) = q^{\frac{1}{12}} \Pi(1 - q^{2\nu}), \tag{2}$$

wo zur Abkürzung

$$e^{2\pi i z} = 1^z, \quad \text{also} \quad q = 1^{\frac{\omega}{2}} \tag{3}$$

[*) B. Riemanns ges. mathem. Werke usw., 2. Aufl., S. 455—461.]
[**) B. Riemanns ges. mathem. Werke usw., 2. Aufl., S. 227—264.]
[***) B. Riemanns ges. mathem. Werke usw., 2. Aufl., S. 461—465.]

gesetzt ist, und wo das Produktzeichen sich auf alle natürlichen Zahlen ν erstreckt. Da diese Funktion der komplexen Variablen $\omega = x + yi$, deren Ordinate x stets positiv ist, im Innern des hierdurch begrenzten, einfach zusammenhängenden Gebietes nirgends Null oder unendlich groß wird, so sind auch alle Potenzen von $\eta(\omega)$ mit beliebigen Exponenten, und ebenso $log\,\eta(\omega)$ durchaus einwertige Funktionen von ω, sobald ihr Wert an einer bestimmten Stelle festgesetzt ist. Die Funktion $log\,\eta(\omega)$ soll dadurch definiert werden, daß, wenn y über alle Grenzen wächst, also q verschwindet, die Größe

$$log\,\eta(\omega) - \frac{\omega\pi i}{12} = 0 \tag{4}$$

wird; dann ist $log\,\eta(\omega)$ konjugiert mit $log\,\eta(-\omega')$, wo ω', wie immer im folgenden, die mit ω konjugierte Größe bedeutet. Nun ist bekanntlich (Fundam. nova § 36)

$$\eta(2\omega)\eta\left(\frac{\omega}{2}\right)\eta\left(\frac{1+\omega}{2}\right) = 1^{\frac{1}{48}}\eta(\omega)^3,$$

$$\sqrt[4]{k} = 1^{\frac{1}{48}}\sqrt{2}\,\frac{\eta(2\omega)}{\eta\left(\frac{1+\omega}{2}\right)},$$

$$\sqrt[4]{k'} = 1^{\frac{1}{48}}\frac{\eta\left(\frac{\omega}{2}\right)}{\eta\left(\frac{1+\omega}{2}\right)},$$

$$\sqrt{\frac{2K}{\pi}} = 1^{-\frac{1}{24}}\frac{\eta\left(\frac{1+\omega}{2}\right)^2}{\eta(\omega)},$$

also nach der obigen Festsetzung:

$$\begin{cases} log\,\eta(2\omega) + log\,\eta\left(\frac{\omega}{2}\right) + log\,\eta\left(\frac{1+\omega}{2}\right) = \frac{\pi i}{24} + 3\,log\,\eta(\omega), \\ log\,k = log\,4 + \frac{\pi i}{6} + 4\,log\,\eta(2\omega) - 4\,log\,\eta\left(\frac{1+\omega}{2}\right), \\ log\,k' = \frac{\pi i}{6} + 4\,log\,\eta\left(\frac{\omega}{2}\right) - 4\,log\,\eta\left(\frac{1+\omega}{2}\right), \\ log\,\frac{2K}{\pi} = -\frac{\pi i}{6} + 4\,log\,\eta\left(\frac{1+\omega}{2}\right) - 2\,log\,\eta(\omega), \end{cases} \tag{5}$$

wo die Logarithmen linker Hand (wie in den Fund. nova § 40) als einwertige Funktionen von ω so definiert sind, daß die drei Größen

$$log\,k - log\,4 - \frac{\omega\pi i}{2} = log\,k - log\,4\sqrt{q},$$

$$log\,k' \quad \text{und} \quad log\,\frac{2K}{\pi}$$

mit q unendlich klein werden.

Aus diesem Verhalten der Funktionen ergibt sich nun mit Hilfe der Transformation erster Ordnung der ϑ-Funktionen das von Riemann untersuchte Verhalten bei Annäherung von ω an einen reellen rationalen Wert, wobei q sich zugleich einer bestimmten Einheitswurzel q_0 nähert. Setzt man

$$\vartheta_1(z, \omega) = \sum 1^{\left(s+\frac{1}{2}\right)^2\frac{\omega}{2} + \left(s+\frac{1}{2}\right)\left(z-\frac{1}{2}\right)}$$

$$= 2\,\eta(\omega)\,1^{\frac{\omega}{12}}\sin z\pi\,\Pi(1 - 1^{\omega\nu+z})(1 - 1^{\omega\nu-z}),$$

wo die Summation auf alle ganzen Zahlen s auszudehnen ist, so wird, wenn man die nach z genommene Derivierte durch einen Akzent bezeichnet,

$$\vartheta_1'(0, \omega) = 2\pi\,\eta(\omega)^3.$$

Sind nun $\alpha, \beta, \gamma, \delta$ vier der Bedingung

$$\alpha\delta - \beta\gamma = 1 \tag{6}$$

genügende ganze Zahlen, so ist bekanntlich

$$\vartheta_1\left(z, \frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = c\sqrt{\alpha+\beta\omega}\,1^{\frac{1}{2}\beta(\alpha+\beta\omega)z^2}\,\vartheta_1\Big((\alpha+\beta\omega)z, \omega\Big),$$

wo c eine von $\alpha, \beta, \gamma, \delta$ und der Wahl der Quadratwurzel abhängige achte Einheitswurzel bedeutet, deren Bestimmung von Hermite auf die Gaußschen Summen zurückgeführt ist (Liouvilles Journal, Serie II, T. III, 1858). Für $z = 0$ ergibt sich hieraus

$$\vartheta_1'\left(0, \frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = c(\alpha+\beta\omega)^{\frac{3}{2}}\,\vartheta_1'(0, \omega),$$

also

$$\eta\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = c^{\frac{1}{3}}(\alpha+\beta\omega)^{\frac{1}{2}}\,\eta(\omega), \tag{7}$$

und aus dieser Transformation von $\eta(\omega)$ ist diejenige von $log\,\eta(\omega)$ abzuleiten.

Der Fall $\beta = 0$ erledigt sich unmittelbar durch die Definitionen (2) und (4) von $\eta(\omega)$, $log\,\eta(\omega)$ und gibt

$$log\,\eta(1+\omega) = log\,\eta(\omega) + \frac{\pi i}{12}, \tag{8}$$

oder allgemeiner, wenn n irgend eine ganze Zahl ist,

$$log\,\eta(n+\omega) = log\,\eta(\omega) + \frac{n\pi i}{12}. \tag{9}$$

Ist aber β von Null verschieden, so wird die Größe

$$\mu = -(\alpha+\beta\omega)^2$$

nirgends negativ, und man kann folglich $log\,\mu$ eindeutig so definieren, daß der imaginäre Bestandteil stets zwischen $\pm\pi i$ bleibt, und folglich konjugierten Werten von μ auch konjugierte Werte von $log\,\mu$ entsprechen; dann wird zufolge (7)

$$log\,\eta\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = log\,\eta(\omega) + \frac{1}{4}log\left\{-(\alpha+\beta\omega)^2\right\} + (\alpha,\beta,\gamma,\delta)\frac{\pi i}{12}, \tag{10}$$

wo $(\alpha, \beta, \gamma, \delta)$ eine durch $\alpha, \beta, \gamma, \delta$ vollständig bestimmte ganze Zahl bedeutet, welche dieselbe bleibt, wenn diese vier Zahlen mit (-1) multipliziert werden. Die vollständige Bestimmung dieser Zahl leistet offenbar noch sehr viel mehr, als die der obigen Einheitswurzel c, und bildet den eigentlichen Gegenstand der folgenden Untersuchung.

Zunächst läßt sich $(\alpha, \beta, \gamma, \delta)$ auf eine nur von α, β abhängige Zahl zurückführen. Genügen nämlich die Zahlen γ', δ' ebenfalls der Bedingung $\alpha\delta' - \beta\gamma' = 1$, so ist bekanntlich $\gamma' = \gamma + n\alpha$, $\delta' = \delta + n\beta$, wo n jede ganze Zahl bedeutet; mithin wird nach (9)

$$log\,\eta\left(\frac{\gamma'+\delta'\omega}{\alpha+\beta\omega}\right) = log\,\eta\left(n + \frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = log\,\eta\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) + \frac{n\pi i}{12},$$

und hieraus folgt nach (10), daß

$$(\alpha, \beta, \gamma', \delta') - \frac{\delta'}{\beta} = (\alpha, \beta, \gamma, \delta) - \frac{\delta}{\beta}$$

nur von den beiden Zahlen α, β abhängt; man kann daher

$$\beta(\alpha, \beta, \gamma, \delta) = \alpha + \delta - 2(\alpha, \beta), \tag{11}$$

also

$$log\,\eta\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = log\,\eta(\omega) + \frac{1}{4}log\left\{-(\alpha+\beta\omega)^2\right\} + \frac{\alpha+\delta-2(\alpha,\beta)}{12\beta}\pi i \tag{12}$$

setzen, wo $2(\alpha, \beta)$ und, wie sich später ergibt, auch (α, β) selbst eine ganze, lediglich von den beiden relativen Primzahlen α, β abhängende Zahl bedeutet; zugleich ergibt sich

$$(-\alpha, -\beta) = -(\alpha, \beta). \tag{13}$$

Ersetzt man ferner alle Glieder der Gleichung (12) durch die zugehörigen konjugierten Größen, so erhält man nach den obigen Bemerkungen

$$log\,\eta\left(-\frac{\gamma+\delta\omega'}{\alpha+\beta\omega'}\right) = log\,\eta(-\omega') + \frac{1}{4}log\left\{-(\alpha+\beta\omega')^2\right\} - \frac{\alpha+\delta-2(\alpha,\beta)}{12\beta}\pi i,$$

und da die linke Seite nach (12) auch in der Form

$$log\,\eta\left(\frac{-\gamma+\delta(-\omega')}{\alpha-\beta(-\omega')}\right) = log\,\eta(-\omega') + \frac{1}{4}log\left\{-(\alpha+\beta\omega')^2\right\} + \frac{\alpha+\delta-2(\alpha,-\beta)}{12(-\beta)}\pi i$$

dargestellt werden kann, so ergibt sich

$$(\alpha, -\beta) = (\alpha, \beta) \tag{14}$$

und zufolge (13) auch

$$(-\alpha, \beta) = -(\alpha, \beta). \tag{15}$$

Soll ferner der Satz (12) auch noch für den Fall $\beta = 0$, $\alpha = \delta = \pm 1$ gelten, so ist die Definition des Symbols (α, β) durch die Festsetzung

$$(\pm 1, 0) = \pm 1 \tag{16}$$

zu vervollständigen, welche auch mit (13), (14), (15) harmoniert.

Aus (15) folgt $(0, \pm 1) = 0$; setzt man daher $\alpha = 0$, $\beta = 1$, $\gamma = -1$, $\delta = 0$, so geht der Satz (12) über in den speziellen Fall der komplementären Transformation

$$log\,\eta\left(\frac{-1}{\omega}\right) = log\,\eta(\omega) + \frac{1}{4}log(-\omega^2). \tag{17}$$

Ersetzt man nun in dem Satze (12) die Größe ω durch $1+\omega$ und durch $\frac{-1}{\omega}$, und drückt die Größen

$$log\,\eta\left(\frac{\gamma+\delta+\delta\omega}{\alpha+\beta+\beta\omega}\right) \quad \text{und} \quad log\,\eta\left(\frac{\delta-\gamma\omega}{\beta-\alpha\omega}\right)$$

wieder nach dem Satze (12) durch $log\,\eta(\omega)$ aus, so erhält man mit Rücksicht auf (8) und (17) leicht die beiden folgenden, für jedes Paar von relativen Primzahlen α, β geltenden Sätze

$$(\alpha+\beta, \beta) = (\alpha, \beta), \tag{18}$$

$$2\alpha(\alpha, \beta) + 2\beta(\beta, \alpha) = 1 + \alpha^2 + \beta^2 - 3|\alpha\beta|, \tag{19}$$

wo $|\alpha\beta|$ den absoluten Wert von $\alpha\beta$ bedeutet. Mit Zuziehung des letzteren Satzes, welcher in naher Beziehung zu dem Reziprozitätssatz in der Theorie der quadratischen Reste steht, kann man der Gleichung (11) auch die Form

(20) $$(\alpha, \beta, \gamma, \delta) = 2\gamma(\alpha, \beta) + 2\delta(\beta, \alpha) - (\alpha\gamma + \beta\delta) \pm 3\alpha\delta$$

geben, wo das Vorzeichen $\pm$ so zu wählen ist, daß $\pm\alpha\beta$ der absolute Wert von $\alpha\beta$ wird; hierdurch erscheint die zuerst in (10) auftretende Zahl $(\alpha, \beta, \gamma, \delta)$ wieder in Form einer ganzen Zahl.

Es leuchtet nun ein, daß die beiden Sätze (18) und (19) nicht nur die früheren Eigenschaften (13) bis (16) in sich schließen, sondern auch ausreichen, um in jedem Falle den Wert des Symbols (α, β) durch eine Kettenbruch-Entwicklung vollständig, und zwar als ganze Zahl zu bestimmen. Dies geht schon aus dem Satze

(21) $$(\alpha, \alpha + \beta) = (\alpha, \beta) - (\beta, \alpha) + \beta - \alpha, \quad \text{wenn} \quad \alpha\beta \gtrless 0,$$

hervor, welcher leicht aus (18) und (19) abgeleitet wird; und umgekehrt leuchtet ein, daß dieser Satz (21) in Verbindung mit (18), d. h. mit dem Satze

(22) $$(\alpha', \beta) = (\alpha, \beta), \quad \text{wenn} \quad \alpha' \equiv \alpha \,(\text{mod. } \beta),$$

ebenfalls die vollständige Bestimmung des Symbols (α, β) enthält und eine sehr bequeme Berechnung einer Tabelle liefert. Es ist endlich sehr zweckmäßig, dem Symbol (α, β) auch dann eine bestimmte Bedeutung beizulegen, wenn die ganzen Zahlen α, β nicht relative Primzahlen sind, sondern einen beliebigen (positiven) größten gemeinsamen Teiler p haben; in diesem Falle setzen wir

(23) $$(\alpha, \beta) = p\left(\frac{\alpha}{p}, \frac{\beta}{p}\right),$$

weil dann offenbar die beiden Sätze (21), (22) ungeändert bestehen bleiben, während freilich das erste Glied 1 auf der rechten Seite des Satzes (19) durch p^2 zu ersetzen ist; aber in den beiden Sätzen (21), (22) ist jetzt auch ohne Zuziehung von (23) die vollständige Bestimmung von (α, β) enthalten, und sie gelten sogar für den Fall $\alpha = \beta = 0$, wenn

(24) $$(0, 0) = 0$$

gesetzt wird. Durch diese Erweiterung des Symbols (α, β) gelingt es oft, solche Sätze, die sonst in verschiedene Fälle zerfallen würden, in einem einzigen Ausspruch zu vereinigen (vgl. die in (28), (34) enthaltenen Sätze).

Obgleich nun das Symbol (α, β) durch die Eigenschaften (21), (22) für jedes Paar von ganzen rationalen Zahlen α, β vollständig bestimmt ist, so würde es doch schwer sein, aus ihnen einen allgemeinen Ausdruck für dasselbe abzuleiten. Mit Hilfe der von Riemann in dem zweiten Fragment angewandten Methode gelingt es aber, einen solchen Ausdruck in Form einer endlichen Summe aufzustellen. Diese Methode besteht in der Untersuchung des Verhaltens der Modulfunktionen, wenn $\omega = x + yi$ sich einem rationalen, in den kleinsten Zahlen ausgedrückten Bruche $\frac{-\alpha}{\beta}$ annähert. Geschieht diese Annäherung in der Weise, daß $\alpha + \beta x$ unendlich klein von höherer Ordnung wird als $\sqrt{y}$, so wird die Ordinate der in dem Satze (12) auftretenden Größe

$$\omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega} = \frac{\delta}{\beta} - \frac{1}{\beta(\alpha + \beta\omega)}$$

positiv unendlich groß, mithin nach (4)

$$log\,\eta(\omega_1) - \frac{\omega_1 \pi i}{12} = 0,$$

also

$$log\,\eta(\omega) + \frac{\pi i}{12\beta(\alpha + \beta\omega)} + \frac{1}{4} log\left\{-(\alpha + \beta\omega)^2\right\} = \frac{2(\alpha, \beta) - \alpha}{12\beta}\pi i;$$

ersetzt man, um sich der Bezeichnung von Riemann zu nähern, α, β durch $-m$, n, so kann man diesen Satz so aussprechen: Nähert sich die Variable $\omega = x + yi$ dem irreduzibelen Bruche $m:n$ so an, daß $nx - m$ von höherer Ordnung unendlich klein wird als $\sqrt{y}$, so wird zuletzt

(25) $$log\,\eta(\omega) + \frac{\pi i}{12n(n\omega - m)} + \frac{1}{4} log\left\{-(n\omega - m)^2\right\} = \frac{m - 2(m, n)}{12n}\pi i.$$

Unterwirft man aber die Annäherung der schärferen Bedingung, daß $nx - m$ von höherer Ordnung unendlich klein wird als y^2, so verschwinden gleichzeitig die imaginären Bestandteile des zweiten und dritten Gliedes links, und folglich ergibt sich durch Subtraktion der konjugierten Größen der Annäherungssatz

(26) $$log\,\eta(\omega) - log\,\eta(-\omega') = \frac{m - 2(m, n)}{6n}\pi i,$$

welcher zufolge der obigen Erweiterung des Symbols (m, n) auch dann gilt, wenn die ganzen Zahlen m, n irgendwelchen gemeinsamen Teiler haben.

Bevor wir denselben benutzen, um unsere Aufgabe zu lösen, bemerken wir noch folgendes. Sind a, d positive ganze Zahlen und c eine beliebige ganze Zahl, und genügt die Annäherung von ω an ihren rationalen Grenzwert der letzten, schärferen Bedingung, so gilt dasselbe offenbar auch für die Annäherung der Größe

$$\frac{c+d\omega}{a} \quad \text{an den Wert} \quad \frac{cn+dm}{an},$$

und folglich wird gleichzeitig mit (26) auch die Annäherung

$$log\,\eta\Big(\frac{c+d\omega}{a}\Big) - log\,\eta\Big(-\frac{c+d\omega'}{a}\Big) = \frac{cn+dm-2(cn+dm,\,an)}{6\,an}\pi i,$$

eintreten. Nun besteht, wenn p eine Primzahl ist, der aus der Transformation $p$ter Ordnung oder aus (2) leicht abzuleitende Satz

$$(27) \qquad log\,\eta(p\omega) + \sum log\,\eta\Big(\frac{s+\omega}{p}\Big) = \frac{(p-1)\pi i}{24} + (p+1)\,log\,\eta(\omega),$$

wo s in der Summe die p Zahlen 0, 1, 2, $\cdots$, $(p-1)$ zu durchlaufen hat; zieht man hiervon die durch den Übergang zu den konjugierten Größen entstehende Gleichung ab, so ergibt sich durch die Grenzannäherung der Satz

$$(28) \qquad p(pm, n) + \sum (m + ns, np) = p(p+1)(m, n),$$

wo s ein beliebiges vollständiges Restsystem (mod. p) durchlaufen muß. Aus dem Satze (27) lassen sich auf verschiedene Weise allgemeinere Sätze ableiten, die für beliebige zusammengesetzte Zahlen p gelten, und aus jedem dieser Sätze entspringt wieder ein ähnlicher Satz über das Symbol (m, n); doch dürfen wir auf diese, an sich sehr interessanten Eigenschaften der Funktion $log\,\eta(\omega)$ und des Symbols (m, n) hier nicht eingehen.

Indem wir uns nun unserer Aufgabe zuwenden, benutzen wir die aus (2) und (4) folgende Darstellung

$$(29) \qquad log\,\eta(\omega) = \frac{\omega\pi i}{12} + \sum log\,(1 - 1^{\omega\nu}),$$

wo ν alle natürlichen Zahlen durchläuft, und die Logarithmen rechts zugleich mit 1^{ω} verschwinden; es wird daher

$$log\,(1 - 1^{\omega\nu}) = -\sum \frac{1^{\omega\nu\mu}}{\mu},$$

wo auch μ alle natürlichen Zahlen durchläuft, und wenn man die Summation nach ν ausführt, so erhält man die Umformung von Jacobi (Fund. nova § 39)

$$(30) \qquad log\,\eta(\omega) = \frac{\omega\pi i}{12} - \sum \frac{1}{\mu}\cdot\frac{1^{\omega\mu}}{1 - 1^{\omega\mu}},$$

mithin

$$log\,\eta(\omega) - log\,\eta(-\omega') = \frac{(\omega+\omega')\pi i}{12} - \sum \frac{a_\mu}{\mu},$$

wo zur Abkürzung

$$a_\mu = \frac{1}{1 - 1^{\omega\mu}} - \frac{1}{1 - 1^{-\omega'\mu}}$$

gesetzt ist.

Jetzt lassen wir die positive Ordinate y der Größe $\omega = x + yi$ unendlich klein werden, während die Abszisse x von vornherein den konstanten rationalen Wert $m:n$ besitzen soll, wodurch die obige, schärfere Bedingung offenbar erfüllt ist. Die ganzen Zahlen m, n dürfen im folgenden einen beliebigen gemeinsamen Teiler haben, doch nehmen wir den Nenner n als positiv an. Setzen wir zur Abkürzung

$$1^z = 1^{\frac{m}{n}} = e^{\frac{2m\pi i}{n}} = \theta; \quad 1^{yi} = e^{-2\pi y} = r,$$

so genügt die Konstante θ der Bedingung $\theta^n = 1$, und r bedeutet einen variablen positiven echten Bruch, der wachsend sich dem Werte 1 annähert; zugleich ist

$$a_\mu = \frac{1}{1 - \theta^\mu r^\mu} - \frac{1}{1 - \theta^{-\mu} r^\mu},$$

und es handelt sich um die Bestimmung des Grenzwertes von

$$log\,\eta(\omega) - log\,\eta(-\omega') = \frac{m\pi i}{6\,n} - \sum \frac{a_\mu}{\mu}.$$

Durch Vereinigung von je zwei Zählern a_μ, welche den Zahlen $\mu = sn + \nu$ und $\mu = (s+1)n - \nu$ entsprechen, wo $0 < \nu < \frac{1}{2}n$, ergibt sich nun leicht, daß der absolute Betrag der Summe

$$A_\mu = a_1 + a_2 + \cdots + a_\mu$$

für alle Werte von r einschließlich $r = 1$ unterhalb einer von r und μ unabhängigen, endlichen Konstanten bleibt, und hieraus folgt nach einem allgemeinen Satze*), daß die Reihe

$$\sum \frac{a_\mu}{\mu} = \sum A_\mu\Big(\frac{1}{\mu} - \frac{1}{\mu+1}\Big),$$

*) Dirichlet, Vorlesungen über Zahlentheorie, 2. Aufl., § 143.

wenn ihre Glieder nach wachsenden μ geordnet werden, auch noch für $r = 1$ konvergiert und an dieser Stelle stetig ist; mit Rücksicht auf den Satz (26) ergibt sich daher

$$\frac{(m,n)\pi i}{3n} = \sum \frac{b_\mu}{\mu},$$

wo

$$b_\mu = \lim a_\mu = 0 \quad \text{oder} \quad = \frac{1}{1-\theta^\mu} - \frac{1}{1-\theta^{-\mu}},$$

je nachdem $\theta^\mu = 1$ ist oder nicht; durch Anwendung der Transformation

$$\frac{1}{1-\theta^\mu} = -\frac{1}{n}\sum \sigma\theta^{\mu\sigma},$$

wo σ die Werte $1, 2, \cdots, (n-1)$ durchläuft, erhält man aber die für alle μ geltende Darstellung

$$b_\mu = \frac{1}{n}\sum \sigma(\theta^{-\mu\sigma} - \theta^{\mu\sigma}),$$

aus welcher sich die Summe unserer unendlichen Reihe auch ohne Benutzung bestimmter Integrale sehr leicht ergibt.

Ist z irgend ein reeller Wert, so wollen wir den von z um eine ganze Zahl abstehenden, zwischen $\pm\frac{1}{2}$ liegenden Wert der Deutlichkeit halber nicht mit (z), sondern mit $((z))$ bezeichnen; für solche Werte von z aber, welche in der Mitte zwischen zwei ganzen Zahlen liegen, soll nach Riemann (S. 242 und 457)[*)] die hier unstetige periodische Funktion $((z)) = 0$, also gleich dem arithmetischen Mittel aus den beiden unendlich nahe benachbarten Werten $((z+0)) = -\frac{1}{2}$ und $((z-0)) = +\frac{1}{2}$ gesetzt werden. Nach einem sehr bekannten Satze aus der Theorie der trigonometrischen Reihen, der sich auch unmittelbar aus der Logarithmen-Reihe ergibt, gilt dann stets die Darstellung

$$2\pi i((z)) = \sum \frac{(-1)^\mu(1^{-z\mu} - 1^{z\mu})}{\mu},$$

wo μ die natürlichen Zahlen wachsend durchläuft, also auch

$$2\pi i\left(\left(z-\frac{1}{2}\right)\right) = \sum \frac{1^{-z\mu} - 1^{z\mu}}{\mu}. \tag{31}$$

[*)] Die Seitenangaben beziehen sich auf die 2. Aufl. von B. Riemanns ges. mathem. Werken usw.]

Hieraus folgt

$$\sum \frac{\theta^{-\mu\sigma} - \theta^{\mu\sigma}}{\mu} = 2\pi i\left(\left(\frac{\sigma m}{n} - \frac{1}{2}\right)\right),$$

mithin

$$\frac{(m,n)}{6n} = \sum \frac{\sigma}{n}\left(\left(\frac{\sigma m}{n} - \frac{1}{2}\right)\right);$$

da aber, wie sich durch Verwandlung von σ in $n - \sigma$ ergibt,

$$\frac{1}{2}\sum\left(\left(\frac{\sigma m}{n} - \frac{1}{2}\right)\right) = 0$$

ist, so erhält man hieraus leicht durch Subtraktion den folgenden Ausdruck

$$(m,n) = 6n\sum\left(\left(\frac{s}{n} - \frac{1}{2}\right)\right)\left(\left(\frac{ms}{n} - \frac{1}{2}\right)\right), \tag{32}$$

wo n positiv angenommen ist, und s ein beliebiges vollständiges Restsystem (mod. n) durchläuft. Dieser Ausdruck für das Symbol (m, n) in Form einer endlichen Summe gestattet noch manche Umformungen und Vereinfachungen, auf welche wir unten noch näher eingehen wollen. Daß derselbe auch dann gilt, wenn die Zahlen m, n einen beliebigen (positiven) gemeinschaftlichen Teiler p haben, läßt sich mit Rücksicht auf (23) nachträglich mit Hilfe des auch sonst wichtigen Satzes

$$\sum\left(\left(\frac{x+p'}{p} - \frac{1}{2}\right)\right) = \left(\left(x - \frac{1}{2}\right)\right) \tag{33}$$

leicht bestätigen, in welchem x eine beliebige reelle Zahl bedeutet und p' ein vollständiges Restsystem (mod. p) durchläuft.

Machen wir jetzt die Voraussetzung, daß m, n relative Primzahlen sind, und setzen wir zur Abkürzung

$$B = \frac{\pi i}{24n(n\omega - m)}, \quad C = \frac{1}{4}log\left\{-(n\omega - m)^2\right\},$$
$$\mu = \frac{1-(-1)^m}{2}, \qquad \nu = \frac{1-(-1)^n}{2},$$

so ist $(1-\mu)(1-\nu) = 0$, $m \equiv \mu$, $n \equiv \nu$ (mod. 2), und aus dem Annäherungs-Satze (25)

$$log\,\eta(\omega) = \frac{m - 2(m,n)}{12n}\pi i - 2B - C$$

folgt gleichzeitig

$$\log\eta(2\omega) = \frac{m-(2m,n)}{6n}\pi i-(4-3\nu)B-C+\frac{\nu}{2}\log 2,$$

$$\log\eta\left(\frac{\omega}{2}\right) = \frac{m-2(m,2n)}{24n}\pi i-(4-3\mu)B-C+\frac{1-\mu}{2}\log 2,$$

$$\log\eta\left(\frac{1+\omega}{2}\right) = \frac{m+n-2(m+n,2n)}{24n}\pi i+(2-3\mu-3\nu)B-C+\frac{\mu+\nu-1}{2}\log 2;$$

die hier auftretenden Symbole sind zufolge (28) durch die stets geltende Relation

$$2(2m,n)+(m,2n)+(m+n,2n) = 6(m,n) \tag{34}$$

miteinander verbunden. Gleichzeitig ergeben sich hieraus zufolge (5) die Annäherungen

$$(35)\begin{cases} \log k = \frac{3m+2(m+n,2n)-4(2m,n)}{6n}\pi i+(\mu+2\nu-2)(12B-2\log 2), \\ \log k' = \frac{(m+n,2n)-(m,2n)}{3n}\pi i+(2\mu+\nu-2)(12B-2\log 2), \\ \log\frac{2K}{\pi} = \frac{(m,n)-(m+n,2n)}{3n}\pi i+(1-\mu-\nu)(12B-2\log 2)-2C. \end{cases}$$

Die Vergleichung dieser Sätze mit den acht Formeln des zweiten Fragments ergibt, daß Riemann auf die Bestimmung der unendlich großen reellen Bestandteile, welche in den Gliedern mit B, C enthalten sind, weniger Wert gelegt hat; sie sind zum Teil ungenau dargestellt, zum Teil ganz weggelassen. Auch in den imaginären Bestandteilen fanden sich (bei der dritten, vierten und fünften Formel) einige kleine Versehen, die sich aber ohne Zwang schon in der ersten Auflage berichtigen ließen, während die reellen Teile auch jetzt ungeändert abgedruckt werden. Daß die Riemannschen Formeln in den imaginären Bestandteilen mit den vorstehenden Sätzen (35) übereinstimmen, ist nicht überall auf den ersten Blick zu erkennen, und es würde zu weit führen, diese Übereinstimmung hier vollständig nachzuweisen; doch wollen wir, weil der Gegenstand wichtig genug ist, zur Erleichterung noch folgende Bemerkungen hinzufügen.

Unter dem Nenner einer rationalen Zahl x verstehen wir immer die kleinste positive ganze Zahl n, für welche das Produkt nx ebenfalls eine ganze Zahl m wird, und diese nennen wir den Zähler von x. Es gibt dann immer unendlich viele Zahlen x', welche denselben Nenner n haben, und deren Zähler m' der Kongruenz $mm' \equiv 1 \pmod n$

genügen, und jede solche Zahl x' soll ein Gefährte (socius) von x heißen (vgl. Art. 77 der Disqu. Arithm.). Nennt man zwei Zahlen x, y schlechthin kongruent, wenn ihre Differenz eine ganze Zahl ist, und bezeichnet dies durch $x \equiv y$, so entspricht jeder Klasse von kongruenten Zahlen x eine und nur eine Klasse von Zahlen x', und wenn p eine ganze Zahl, und zwar relative Primzahl zu n bedeutet, so ist $p(px')' \equiv x$. Setzen wir nun zur Abkürzung

$$D(x) = \frac{(m,n)}{n} = 6\sum\left(\left(\frac{s}{n}-\frac{1}{2}\right)\right)\left(\left(\frac{ms}{n}-\frac{1}{2}\right)\right), \tag{36}$$

so hat diese Funktion, wie sich aus dem vorstehenden Ausdrucke, oder auch aus (18), (15), (12), (34) leicht ergibt, die Eigenschaften

$$(37)\begin{cases} D(x) = D(x+1) = -D(-x) = D(x'), \\ D(2x)+D\left(\frac{x}{2}\right)+D\left(\frac{x+1}{2}\right) = 3D(x). \end{cases}$$

Ersetzt man die in den Riemannschen Formeln bisweilen benutzte Funktion $E(x)$, welche die größte in x enthaltene ganze Zahl bedeutet, durch den Ausdruck

$$E(x) = x-\frac{1}{2}-\left(\left(x-\frac{1}{2}\right)\right), \tag{38}$$

in welchem nur, wenn x selbst eine ganze Zahl ist, statt $E(x)$ wieder das arithmetische Mittel $x-\frac{1}{2}$ aus $E(x+0)$ und $E(x-0)$ zu nehmen ist, so treten in den meisten dieser Formeln zuletzt nur noch Funktionen von der Form

$$R(x) = \sum((\nu x)), \quad S(x) = \sum\left(\left(\nu x-\frac{1}{2}\right)\right) \tag{39}$$

auf, wo die Summationen sich auf alle diejenigen, nicht negativen ganzen Zahlen ν beziehen, welche kleiner als der halbe Nenner von x sind; diese Funktionen haben die Eigenschaften

$$(40)\begin{cases} R(x) = R(x+1) = -R(-x) \\ S(x) = S(x+1) = -S(-x) \\ R(x)-S(x) = R(x')-S(x') = \frac{1}{2}h, \end{cases}$$

wo h den Überschuß der Anzahl der positiven Glieder $((\nu x))$ über die der negativen bedeutet, und stehen in folgenden Beziehungen zu der Funktion $D(x)$. Allgemein ist nach (36)

$$6S(x') = D(2x)-2D(x). \tag{41}$$

Hat die Zahl x einen geraden Nenner n, so ist

$$(42)\quad \begin{cases} R(x) = -S(x) = \frac{1}{4}h = \frac{1}{3}D(x) - \frac{1}{6}D(2x), \\ R\left(\frac{x}{2}\right) + R\left(\frac{x+1}{2}\right) = 2R(x). \end{cases}$$

Hat aber die Zahl x einen ungeraden Nenner n, so zerfallen die Zahlen y, welche der Bedingung $2y \equiv x$ genügen, also $\equiv \frac{1}{2}x$ oder $\equiv \frac{1}{2}(x+1)$ sind, in zwei Klassen von Zahlen, von denen diejenigen, welche denselben Nenner n haben, mit x_1, die übrigen mit x_2 bezeichnet werden sollen; die letzteren haben den Nenner $2n$. Dann ist

$$(43)\qquad R(x_2) = R(x) - S(x) = 2R(x) - S(2x)$$

und

$$(44)\quad \begin{cases} D(x) &= 6R(x_2) - 4R(x) - 4R(x'), \\ D(2x) &= 6R(x_2) - 8R(x) - 2R(x'), \\ D(x_1) &= 6R(x_2) - 2R(x) - 8R(x'), \\ D(x_2) &= 6R(x_2) - 2R(x) - 2R(x'), \end{cases}$$

wodurch wieder die obige Bedingung

$$(45)\qquad D(2x) + D(x_1) + D(x_2) = 3D(x)$$

erfüllt wird. Die Übereinstimmung der drei ersten Darstellungen in (44) ergibt sich aus den früheren Eigenschaften von $R(x)$ mit Rücksicht auf die Beziehungen

$$x_1 \equiv x_2 + \frac{1}{2} \equiv (2x')', \quad \left(x + \frac{1}{2}\right)' \equiv (4x)' + \frac{1}{2}, \quad (x_2)' \equiv (x')_2;$$

und umgekehrt ist

$$(46)\quad \begin{cases} 6R(x) &= 3D(x) - 2D(2x) - D(x_1) = D(x_2) - D(2x) \\ 6R(x') &= 3D(x) - D(2x) - 2D(x_1) = D(x_2) - D(x_1) \\ 6R(x_2) &= 5D(x) - 2D(2x) - 2D(x_1) = 2D(x_2) - D(x). \end{cases}$$

Die Herleitung dieser und zahlreicher anderer Relationen, welche alle in naher Beziehung zu der Theorie der quadratischen Reste stehen, müssen wir uns aber für eine andere Gelegenheit versparen.

Erläuterungen zur vorstehenden Abhandlung.

Die Bedeutung der Abhandlung geht weit hinaus über ihre erste Absicht, nur eine Erläuterung zu den beiden Riemannschen „Fragmenten über die Grenzfälle der elliptischen Modulfunktionen“ sein zu wollen. Die Methoden der Abhandlung führen nicht nur zur Bestimmung derjenigen bei der linearen Transformation der ϑ-Funktionen auftretenden Einheitswurzeln, die bereits von Jacobi und Hermite berechnet wurden (vgl. den Anfang der Abhandlung), sondern auch zur Bestimmung der 24sten Einheitswurzel, die bei der linearen Transformation der 24sten Wurzel der Diskriminante

$$\sqrt[24]{\Delta(\omega_1, \omega_2)} = \sqrt{\frac{2\pi}{\omega_2}}\eta(\omega)$$

auftritt. Über den letzteren Gegenstand vgl. man die Dissertation von Th. Molien: „Über die lineare Transformation der elliptischen Funktionen“ (Dorpat, 1885).

Das Problem Dedekinds umfaßt sofort alle Wurzeln aus η, indem er das Verhalten der in der positiven ω-Halbebene eindeutigen Funktion $log\,\eta(\omega)$ gegenüber der Modulgruppe festzustellen anstrebt. Das Problem wird zurückgeführt auf die Bestimmung der durch das Symbol (m, n) bezeichneten ganzen Zahl. Es wird zunächst die Berechnung von (m, n) durch ein Kettenbruchverfahren gelehrt und sodann eine allgemein gültige Darstellung von (m, n) in einer endlichen Summe mittels des Restsymbols $((x))$ entwickelt.

Dedekind betont den Zusammenhang des Symbols (m, n) mit der Theorie der quadratischen Reste und hat demselben mit Recht überhaupt eine große zahlentheoretische Bedeutung zuerkannt. Aber auch die Darstellung von (m, n) durch das Restsymbol $((x))$ gibt noch keineswegs einen tieferen Einblick in die Abhängigkeit der ganzen Zahl (m, n) von m und n. Man weiß lediglich, daß die Zahlen (m, n) mod 24 mit gewissen rationalen Ausdrücken in m und n kongruent sind. Es hängt dies, um beim Legendreschen Integralmodul k^2 zu bleiben, mit dem Umstand zusammen, daß von allen Wurzeln aus k^2 nur k^2, k, $\sqrt{k}$ und $\sqrt[4]{k}$ sogenannte „Kongruenzmoduln“ sind, d. h. daß sich nur die zu ihnen gehörenden Teiler der Modulgruppe durch Kongruenzen erklären lassen. Es sind Versuche gemacht, zu arithmetischen Aussagen über die zu höheren Wurzeln aus k^2 gehörenden Teiler der Modulgruppe zu gelangen. Diese Versuche schlossen mit dem negativen Ergebnis, daß diese Teiler eben „Nicht-Kongruenzgruppen“ seien, worüber die Arbeiten von G. Pick, Mathem. Ann., Bd. 28, S. 119 (1886) und R. Fricke, ebenda, Bd. 28, S. 99 (1886) zu vergleichen sind. Von einer tieferen Erforschung des Dedekindschen Symbols (m, n) darf man neue Aufschlüsse in dieser Richtung erwarten.

Fricke.

XIV.

Schreiben an Herrn Borchardt über die Theorie der elliptischen Modulfunktionen.

[Journal für reine und angewandte Mathematik, Bd. 83, S. 265—292 (1877)].

Sie haben mich aufgefordert, eine etwas ausführlichere Darstellung der Untersuchungen auszuarbeiten, von welchen ich, durch das Erscheinen der Abhandlung von Fuchs*) veranlaßt, mir neulich erlaubt habe Ihnen eine kurze Übersicht mitzuteilen; indem ich Ihrer Einladung hiermit Folge leiste, beschränke ich mich im wesentlichen auf den Teil dieser Untersuchungen, welcher mit der eben genannten Abhandlung zusammenhängt, und ich bitte Sie auch, die Übergehung einiger Nebenpunkte entschuldigen zu wollen, da es mir im Augenblick an Zeit fehlt, alle Einzelheiten auszuführen. Die in Rede stehenden Untersuchungen habe ich schon vor einer Reihe von Jahren angestellt, als ich erkannte, daß die Bestimmung der Anzahl der Idealklassen in kubischen Körpern (d. h. in Gebieten von Zahlen, welche aus Wurzeln von Gleichungen dritten Grades gebildet sind) innig zusammenhängt mit der Theorie der singulären Moduln der elliptischen Funktionen, für welche die komplexe Multiplikation stattfindet. Bei meinen Versuchen, tiefer in diese mir unentbehrliche Theorie einzudringen und mir einen einfachen Weg zu den ausgezeichnet schönen Resultaten von Kronecker zu bahnen, die leider noch immer so schwer zugänglich sind, erkannte ich sogleich die fundamentale Wichtigkeit des Punktes, auf welchen auch Hermite neulich in einer Anmerkung zu der Abhandlung von Fuchs (S. 29) aufmerksam gemacht hat, und welcher in der Tat zur Grundlage für meine Theorie geworden ist. Es handelt sich um folgendes. Bedeutet

$$\omega = \frac{K'i}{K}$$

[*) Journ. f. reine u. angew. Mathem., Bd. 83, S. 13—37.]

das Periodenverhältnis der elliptischen Funktionen (= Hi nach der Bezeichnung von Fuchs), so ist das Quadrat $k = \varkappa^2$ des Integralmoduls $\varkappa$ eine einwertige Funktion von ω, welche Hermite mit $\varphi(\omega)^8$ bezeichnet, und aus der Transformation erster Ordnung folgt leicht, daß k unverändert bleibt, wenn ω durch

$$\omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}$$

ersetzt wird, wo α, β, γ, δ vier ganze rationale Zahlen bedeuten, welche der Bedingung $\alpha\delta - \beta\gamma = 1$ genügen, und von denen β, γ gerade sind. Der zu beweisende Satz besteht nun darin, daß außer diesen Zahlen ω_1 keine andere existiert, welche denselben Wert $k = \varphi(\omega)^8 = \varphi(\omega_1)^8$ hervorbringt. Bevor ich zur Darstellung meiner Theorie übergehe, will ich zunächst zeigen, daß dieser Satz sich auch aus der gewöhnlichen Theorie der elliptischen Funktionen ohne Schwierigkeit ableiten läßt.

Bedeutet ω eine komplexe Größe mit positiv-imaginärem Bestandteil, ferner z eine willkürliche Variable, und bedient man sich der folgenden Bezeichnungen

$$1^z = e^{2\pi i z},$$

$$\vartheta(z,\omega) = \sum 1^{s^2\frac{\omega}{2} + s\left(z-\frac{1}{2}\right)},$$

$$\vartheta_1(z,\omega) = \sum 1^{\left(s+\frac{1}{2}\right)^2\frac{\omega}{2} + \left(s+\frac{1}{2}\right)\left(z-\frac{1}{2}\right)},$$

$$\vartheta_2(z,\omega) = \sum 1^{\left(s+\frac{1}{2}\right)^2\frac{\omega}{2} + \left(s+\frac{1}{2}\right)z},$$

$$\vartheta_3(z,\omega) = \sum 1^{s^2\frac{\omega}{2} + sz},$$

wo s alle ganzen Zahlen von $-\infty$ bis $+\infty$ durchläuft, ferner

$$\sqrt{\varkappa} = \frac{\vartheta_2(0,\omega)}{\vartheta_3(0,\omega)} = \varphi(\omega)^2; \quad \sqrt{\varkappa'} = \frac{\vartheta(0,\omega)}{\vartheta_3(0,\omega)} = \psi(\omega)^2,$$

so ist

$$\varkappa^2 + \varkappa'^2 = 1,$$

und man kann

$$\sqrt{x} = \frac{1}{\sqrt{\varkappa}}\frac{\vartheta_1(z,\omega)}{\vartheta(z,\omega)} = sin\,am(2Kz, \varkappa),$$

$$\sqrt{1-x} = \frac{\sqrt{\varkappa'}}{\sqrt{\varkappa}}\frac{\vartheta_2(z,\omega)}{\vartheta(z,\omega)} = cos\,am(2Kz, \varkappa),$$

$$\sqrt{1-\varkappa^2 x} = \sqrt{\varkappa'}\frac{\vartheta_3(z,\omega)}{\vartheta(z,\omega)} = \Delta am(2Kz, \varkappa),$$

$$\frac{d\sqrt{x}}{dz} = 2K\sqrt{1-x}\sqrt{1-\varkappa^2 x}$$

setzen, wo

$$2K = \frac{\vartheta_3(0,\omega)\vartheta_1'(0,\omega)}{\vartheta(0,\omega)\vartheta_2(0,\omega)} = \pi\vartheta_3(0,\omega)^2$$

ist. Wenn nun die Größe ω_1 ebenfalls einen positiv-imaginären Bestandteil hat und denselben Wert

$$\frac{\vartheta_2(0,\omega_1)^4}{\vartheta_3(0,\omega_1)^4} = \varkappa_1^2 = \varkappa^2 = k$$

hervorbringt, wie ω, so setze man

$$2K_1 = \pi\vartheta_3(0,\omega_1)^2$$

und führe eine neue Variable z_1 durch die Gleichung

$$K_1 z_1 = Kz$$

ein; wenn ferner mit $\sqrt{x_1}$, $\sqrt{1-x_1}$, $\sqrt{1-kx_1}$ die Größen bezeichnet werden, welche ebenso von z_1, ω_1 abhängen, wie $\sqrt{x}$, $\sqrt{1-x}$, $\sqrt{1-kx}$ von z, ω, so ergibt sich

$$\frac{d\sqrt{x}}{\sqrt{1-x}\sqrt{1-kx}} = \frac{d\sqrt{x_1}}{\sqrt{1-x_1}\sqrt{1-kx_1}},$$

und hieraus durch Integration

$$\sqrt{x}\sqrt{1-x_1}\sqrt{1-kx_1} - \sqrt{x_1}\sqrt{1-x}\sqrt{1-kx} = C(1-kxx_1);$$

die Konstante C muß aber gleich Null sein, weil für $z=0$ auch $z_1=0$ ist, also $\sqrt{x}$ und $\sqrt{x_1}$ gleichzeitig verschwinden. Hieraus folgt, daß identisch $x = x_1$ ist (ja sogar $\sqrt{x}=\sqrt{x_1}$, $\sqrt{1-x}=\sqrt{1-x_1}$, $\sqrt{1-kx}=\sqrt{1-kx_1}$); mithin wird jede der vier Funktionen

$$\vartheta(z,\omega),\quad \vartheta_1(z,\omega),\quad \vartheta_2(z,\omega),\quad \vartheta_3(z,\omega)$$

stets und nur dann verschwinden, wenn die entsprechende der vier Funktionen

$$\vartheta(z_1,\omega_1),\quad \vartheta_1(z_1,\omega_1),\quad \vartheta_2(z_1,\omega_1),\quad \vartheta_3(z_1,\omega_1)$$

verschwindet. Die Funktion $\vartheta_1(z,\omega)$ verschwindet aber für alle Werte $z = r + s\omega$ und nur*) für diese, wo r, s willkürliche ganze Zahlen bedeuten; setzt man daher

$$z_1 = 1, \quad \text{so wird} \quad z = \frac{K_1}{K} = \alpha + \beta\omega,$$

$$z_1 = \omega_1, \quad \text{so wird} \quad z = \frac{K_1}{K}\omega_1 = \gamma + \delta\omega,$$

*) Dies folgt aus der Darstellung von $\vartheta_1(z,\omega)$ als unendliches Produkt, oder auch aus dem Satze $\int d\,log\,\vartheta_1(z,\omega) = 2\pi i$, wo die Integration durch die Begrenzung eines elementaren Parallelogramms erstreckt ist.

wo α, β, γ, δ ganze rationale Zahlen bedeuten; mithin ist

$$(1)\qquad \omega_1 = \frac{\gamma+\delta\omega}{\alpha+\beta\omega}, \quad (\alpha+\beta\omega)z_1 = z.$$

Setzt man umgekehrt

$$z = 1, \quad \text{so wird} \quad z_1 = \alpha_1 + \beta_1\omega_1$$
$$z = \omega, \quad \text{so wird} \quad z_1 = \gamma_1 + \delta_1\omega_1,$$

wo α_1, β_1, γ_1, δ_1 ebenfalls ganze Zahlen bedeuten; es wird daher

$$(\alpha+\beta\omega)\alpha_1 + (\gamma+\delta\omega)\beta_1 = 1,$$
$$(\alpha+\beta\omega)\gamma_1 + (\gamma+\delta\omega)\delta_1 = \omega,$$

woraus, weil ω nicht reell ist,

$$\alpha\alpha_1 + \gamma\beta_1 = 1, \quad \beta\alpha_1 + \delta\beta_1 = 0,$$
$$\alpha\gamma_1 + \gamma\delta_1 = 0, \quad \beta\gamma_1 + \delta\delta_1 = 1,$$

also

$$(\alpha\delta - \beta\gamma)(\alpha_1\delta_1 - \beta_1\gamma_1) = 1,$$

mithin

$$\alpha\delta - \beta\gamma = \alpha_1\delta_1 - \beta_1\gamma_1 = \pm 1$$

folgt*). Hierin darf aber zufolge (1) nur das obere Zeichen genommen werden, weil der Koeffizient von i in beiden Größen ω und ω_1 dasselbe (positive) Vorzeichen hat; also ist

$$(2)\qquad \alpha\delta - \beta\gamma = +1.$$

Da ferner die Werte von z_1, für welche $\vartheta(z_1,\omega_1)$ verschwindet, mit den Werten $r + (s+\frac{1}{2})\omega_1$ zusammen fallen, so wird gleichzeitig

$$z = \frac{\omega}{2}, \quad z_1 = r + (s+\tfrac{1}{2})\omega_1;$$

mithin ist zufolge (1)

$$(\alpha+\beta\omega)r + (\gamma+\delta\omega)(s+\tfrac{1}{2}) = \frac{\omega}{2},$$
$$\alpha r + \gamma(s+\tfrac{1}{2}) = 0,$$

also

$$(3)\qquad \gamma \equiv 0 \pmod 2.$$

Auf dieselbe Weise ergibt sich aus dem gleichzeitigen Verschwinden der Funktionen $\vartheta_2(z,\omega)$, $\vartheta_2(z_1,\omega_1)$ für $z=\frac{1}{2}$ auch

$$(4)\qquad \beta \equiv 0 \pmod 2,$$

womit der in Rede stehende Satz vollständig bewiesen ist.

Dieser Beweis beruht offenbar darauf, daß die elliptischen Funktionen $sin\,am\,(u,\varkappa)$, $cos\,am\,(u,\varkappa)$, $\Delta\,am\,(u,\varkappa)$ einwertige Funktionen auch von $k=\varkappa^2$ sind. Der Satz selbst reizte mich aber bald, den

*) Dies ist nur ein spezieller Fall eines allgemeinen Satzes aus der Theorie der Zahlensysteme, welche ich *endliche Moduln* genannt habe.

Zusammenhang zwischen den Größen ω, k, K ganz unabhängig von der Theorie der elliptischen Funktionen zu erforschen, und in diesem Streben bestärkte mich eine Bemerkung von Hermite, welcher an einer Stelle seiner kurzen Übersicht über die Theorie der elliptischen Funktionen hervorhebt, daß noch kein anderer Weg zu diesen Modulfunktionen führe, als der, welchen die Gründer der Theorie der elliptischen Funktionen eingeschlagen haben. Ich erlaube mir nun, Ihnen meine damals entstandene Theorie in ihren Grundzügen zu entwickeln; die Anwendung auf die Theorie der singulären Moduln, derentwegen die ganze Untersuchung angestellt ist, darf ich Ihnen vielleicht ein anderes Mal vorlegen.

§ 1.

Äquivalente Zahlen.

Zwei Zahlen ω, ω_1 sollen im folgenden *äquivalent* heißen, wenn es vier ganze (rationale) Zahlen α, β, γ, δ gibt, welche den beiden Bedingungen

$$\omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \quad \alpha\delta - \beta\gamma = 1$$

genügen; offenbar ist die hierdurch ausgedrückte Beziehung zwischen ω, ω_1 eine gegenseitige, da zugleich die vier Zahlen δ, $-\beta$, $-\gamma$, α den Bedingungen

$$\omega = \frac{(-\gamma) + \alpha\omega_1}{\delta + (-\beta)\omega_1}, \quad \delta\alpha - (-\beta)(-\gamma) = 1$$

genügen. Ist nun ω_2 ebenfalls äquivalent mit ω, gibt es also vier ganze Zahlen α_1, β_1, γ_1, δ_1, welche den Bedingungen

$$\omega = \frac{\gamma_1 + \delta_1\omega_2}{\alpha_1 + \beta_1\omega_2}, \quad \alpha_1\delta_1 - \beta_1\gamma_1 = 1$$

genügen, so setze man in üblicher Weise

$$\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}\begin{pmatrix}\alpha_1, \beta_1\\ \gamma_1, \delta_1\end{pmatrix} = \begin{pmatrix}\alpha', \beta'\\ \gamma', \delta'\end{pmatrix},$$

d. h.

$$\alpha' = \alpha\alpha_1 + \beta\gamma_1, \quad \beta' = \alpha\beta_1 + \beta\delta_1,$$
$$\gamma' = \gamma\alpha_1 + \delta\gamma_1, \quad \delta' = \gamma\beta_1 + \delta\delta_1;$$

da diese Zahlen α', β', γ', δ' den beiden Bedingungen

$$\omega_1 = \frac{\gamma' + \delta'\omega_2}{\alpha' + \beta'\omega_2}, \quad \alpha'\delta' - \beta'\gamma' = 1$$

genügen, so folgt, daß je zwei mit einer und derselben Zahl ω äquivalente Zahlen ω_1, ω_2 auch miteinander äquivalent sind. Aus diesem Grunde wird man das gesamte Zahlengebiet in Klassen einteilen können, indem man je zwei Zahlen in dieselbe oder in zwei verschiedene Klassen aufnimmt, je nachdem sie äquivalent sind oder nicht. Jede Zahl ω kann als Repräsentant derjenigen Klasse angesehen werden, welche aus allen mit ω äquivalenten Zahlen besteht.

Nennt man die reellen Zahlen x, y die Koordinaten, und zwar x die Abszisse, y die Ordinate der aus ihnen gebildeten komplexen Zahl $\omega = x + yi$, so ergibt sich leicht, daß die Ordinaten von je zwei äquivalenten Zahlen ω, ω_1 dasselbe Vorzeichen haben, oder beide verschwinden. Wir werden im folgenden das Gebiet S derjenigen ω betrachten, deren Ordinaten positiv sind, und außerdem nur noch die rationalen reellen Zahlen, welche letzteren offenbar eine einzige Klasse R bilden, weil sie sämtlich mit der Zahl 0 äquivalent sind; es wird sich zeigen, daß diese Klasse R, welche zugleich die Zahl ∞ enthält, als die vollständige Begrenzung des Gebietes S anzusehen ist.

§ 2.

Vollständiges Repräsentantensystem.

Es kommt nun darauf an, ein vollständiges System von Repräsentanten ω_0 aller Klassen aufzustellen, aus welchen das Gebiet S besteht, in der Weise, daß jede Zahl ω dieses Gebietes mit einem, und im allgemeinen auch nur mit einem dieser Repräsentanten ω_0 äquivalent ist. Dies geschieht durch den folgenden Satz, in welchem das Zeichen $N(x + yi)$ die Norm $(x^2 + y^2)$ der komplexen Zahl $x + yi$ bedeutet:

In jeder Klasse des Gebietes S einschließlich R gibt es einen, und im allgemeinen auch nur einen Repräsentanten ω_0, welcher den drei Bedingungen

(1) $\quad N(\omega_0 - 1) \geqq N(\omega_0)$,

(2) $\quad N(\omega_0 + 1) \geqq N(\omega_0)$,

(3) $\quad N(\omega_0) \geqq 1$

genügt.

Der Beweis kann mit denselben Mitteln geführt werden, durch welche in der Theorie der binären quadratischen Formen von negativer Determinante bewiesen wird, daß jede solche Form einer, und

im allgemeinen auch nur einer reduzierten Form äquivalent ist. Ich will mich hier begnügen, den ersten Teil des Satzes durch die folgende Betrachtung zu erledigen. Ist ω eine bestimmte Zahl des Gebietes S, so gibt es, weil ω nicht reell ist, unter allen Paaren von relativen Primzahlen α, β mindestens eins, für welches $N(\alpha+\beta\omega)$ so klein wie möglich wird; nachdem α, β so gewählt sind, erhält man alle Lösungen der Gleichung $\alpha\delta-\beta\gamma=1$ in ganzen Zahlen γ, δ aus einer einzigen Lösung γ', δ', indem man $\gamma=\gamma'-m\alpha$, $\delta=\delta'-m\beta$ setzt und m alle ganzen Zahlen von $-\infty$ bis $+\infty$ durchlaufen läßt; wählt man m so, daß

$$N\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right)=N\left(\frac{\gamma'+\delta'\omega}{\alpha+\beta\omega}-m\right)$$

möglichst klein wird, so hat die mit ω äquivalente Zahl

$$\omega_0=\frac{\gamma+\delta\omega}{\alpha+\beta\omega},$$

die in (1), (2), (3) ausgedrückten Eigenschaften. Denn aus der Definition von α, β folgt, daß ω_0 der Bedingung (3) genügt, und ebenso aus der Definition von m, daß ω_0 den Bedingungen (1) und (2) genügt.

Geometrisch wird der Inbegriff aller dieser Zahlen ω_0 durch ein Stück der Halbebene S dargestellt, welches das Hauptfeld heißen und mit (ω_0) bezeichnet werden soll. Dasselbe ist begrenzt durch drei Linien, welche den Gleichheitszeichen in den Bedingungen (1), (2), (3) entsprechen; setzt man $\omega_0=x_0+y_0 i$, so nehmen die letzteren die folgende Gestalt an:

(1) $\quad x_0 \leqq \frac{1}{2}$,

(2) $\quad x_0 \geqq -\frac{1}{2}$,

(3) $\quad x_0^2+y_0^2 \geqq 1$;

das Feld (ω_0) liegt daher zwischen den beiden Geraden, welche in den Abständen $\pm\frac{1}{2}$ parallel mit der Ordinatenachse laufen, und zugleich außerhalb des Halbkreises, welcher mit dem Radius Eins aus dem Nullpunkte beschrieben ist. Dieses Feld wird offenbar durch die Ordinatenachse in zwei symmetrische Hälften zerlegt. Die beiden Parallelen (2) und (1) schneiden sich im Punkte ∞, dem Repräsentanten der Klasse R der rationalen Zahlen, und sie schneiden den Kreis in den Punkten

$$\varrho=\frac{-1+i\sqrt{3}}{2} \quad \text{und} \quad -\varrho^2=1+\varrho=\frac{-1}{\varrho},$$

während die Symmetrieachse den Kreis im Punkte

$$i=\frac{-1}{i}$$

schneidet.

Wenn nun ω_0 der Grenzlinie (2) angehört, d. h. wenn $x_0=-\frac{1}{2}$ ist, so leuchtet ein, daß die äquivalente Zahl $1+\omega_0$ der Grenzlinie (1) angehört, und diese beiden Punkte ω_0, $1+\omega_0$ liegen symmetrisch zu beiden Seiten der Ordinatenachse. Wenn ferner ω_0 der Kreislinie (3) angehört, so gilt dasselbe von der äquivalenten Zahl $\frac{-1}{\omega_0}=-x_0+y_0 i$, und diese beiden Punkte ω_0, $\frac{-1}{\omega_0}$ liegen ebenfalls symmetrisch zu beiden Seiten der Ordinatenachse. Je zwei symmetrische Punkte der Begrenzung von (ω_0) sind daher Repräsentanten einer und derselben Klasse. Es ließe sich nun auch leicht zeigen, daß außer diesen Fällen niemals zwei verschiedene Punkte oder Zahlen des Feldes (ω_0) derselben Klasse angehören können, mögen sie im Innern oder auf der Begrenzung von (ω_0) liegen. Der Kürze halber unterdrücke ich diesen Beweis, welcher, wie schon oben bemerkt, genau ebenso lautet, wie der Beweis des Satzes, daß zwei verschiedene reduzierte binäre quadratische Formen von negativer Determinante nur in gewissen Ausnahmefällen äquivalent sein können (vgl. Zahlentheorie von Dirichlet, zweite Auflage, § 65); es wird genügen zu bemerken, daß, wenn x, y willkürliche Variable bedeuten, die binäre quadratische Form

$$N(x+y\omega_0)=(1, x_0, x_0^2+y_0^2),$$

deren Determinante $=-y_0^2$, immer eine reduzierte ist, wenn dieser Begriff auf Formen mit gebrochenen oder irrationalen reellen Koeffizienten übertragen wird.

Sind nun α, β, γ, δ vier bestimmte ganze Zahlen, welche der Bedingung $\alpha\delta-\beta\gamma=1$ genügen, und setzt man

$$\omega_0=\frac{\gamma+\delta\omega}{\alpha+\beta\omega}, \quad \omega=\frac{-\gamma+\alpha\omega_0}{\delta-\beta\omega_0},$$

so entspricht, wie man leicht erkennt, dem Hauptfelde (ω_0) ein Feld (ω), welches von drei Kreisbogen begrenzt wird, deren Mittelpunkte stets in der Abszissenachse liegen, und welche in gerade Linien ausarten können; die den Eckpunkten

$$\varrho, \quad -\varrho^2, \quad \infty$$

des Hauptfeldes entsprechenden Eckpunkte des Feldes (ω) sind

$$\frac{-\gamma+\alpha\varrho}{\delta-\beta\varrho},\quad \frac{-\gamma-\alpha\varrho^2}{\delta+\beta\varrho^2},\quad \frac{-\alpha}{\beta},$$

deren letzter der Klasse R angehört. Offenbar entspricht den vier Zahlen $-\alpha$, $-\beta$, $-\gamma$, $-\delta$ dasselbe Feld (ω); sonst aber entsprechen, wie die genaue Untersuchung zeigt, zwei verschiedenen Systemen von vier Zahlen α, β, γ, δ immer zwei verschiedene Felder (ω), welche ganz außerhalb einander liegen und höchstens eine Grenzlinie oder auch nur einen Eckpunkt gemeinsam haben können. Die ganze Halbebene S einschließlich R besteht aus unendlich vielen solchen, den verschiedenen Systemen oder Substitutionen $\pm\alpha$, $\pm\beta$, $\pm\gamma$, $\pm\delta$ entsprechenden Kreisbogendreiecken (ω), welche sich in unendlicher Anzahl und Verkleinerung an die Abszissenachse andrängen.

Niemals enthält aber ein solches Feld (ω) einen irrationalen reellen Wert, und in diesem Sinne sage ich, daß bei unserer Untersuchung die Klasse R der rationalen Zahlen die vollständige Begrenzung des Gebiets S bildet. Ist r eine bestimmte rationale Zahl, so gibt es unendlich viele Felder (ω), welche diesen Wert r gemeinschaftlich haben (vgl. § 4, III); das aus allen diesen Feldern bestehende Gebiet $G(r)$ ist durch unendlich viele solche Kreisbogen begrenzt, welche der Linie (3) entsprechen. Ist nun x ein konstanter reeller, aber irrationaler Wert, und nimmt y von $+\infty$ bis 0 ab, so durchläuft $\omega = x + yi$ unendlich viele solche Gebilde $G(r)$, und die Zahlen r, deren Nenner immer größer werden, nähern sich dem Werte x unendlich an. Solange ω einem und demselben Gebiete $G(r)$ angehört, beschreibt die äquivalente Zahl ω_0 im Hauptfelde Kreisbogen, welche immer nach einer bestimmten der beiden Linien (1), (2) hinführen, von hier zu dem symmetrischen Punkte springen und sich durch Verschiebung zu einem einzigen Kreise zusammensetzen lassen; endlich aber muß ein letzter solcher Kreisbogen in die Linie (3) führen; dann tritt ω in das folgende Gebiet $G(r')$, und nun beginnt ω_0 von dem symmetrischen Punkte der Linie (3) aus, eine neue Kreisbogenbewegung in (ω_0), welche dem Durchgange der Variablen ω durch eine endliche Anzahl von Feldern des Gebietes $G(r')$ entspricht (vgl. den Schluß von § 6). Die Annäherung der Zahlen r, r' ... an den Wert x ist nicht ohne Interesse, und ich verspreche mir (vielleicht mit Unrecht) von der näheren Untersuchung derselben noch ein brauchbares Resultat, wenigstens für den Fall, daß x die Wurzel einer quadratischen Gleichung mit rationalen Koeffizienten ist.

§ 3.

Die Valenz.

Nach diesen Vorbereitungen gehe ich zu dem Fundamentalsatze meiner Untersuchung über, welcher folgendermaßen lautet:

Es gibt eine Funktion v der Variablen ω im Gebiete S und auf dessen Begrenzung R, welche für alle äquivalenten Werte ω Einen bestimmten Wert besitzt, und zwar so, daß umgekehrt Jedem Werte der unbeschränkten komplexen Variablen v Eine bestimmte Klasse von äquivalenten Werten ω entspricht.

Der Beweis ergibt sich aus den Prinzipien von Riemann (Art. 21 der Inaugural-Dissertation). Man bilde die eine der beiden symmetrischen Hälften des Hauptfeldes (ω_0) auf einer der beiden Hälften der v-Ebene ab, in welche dieselbe durch die Achse der reellen v zerfällt; hierbei bleiben drei reelle Konstanten willkürlich, da zu einem inneren und zu einem Begrenzungspunkte des Orginals die entsprechenden Bildpunkte willkürlich gewählt werden dürfen. Hierauf setze man die Abbildung durch die Symmetrieachse des Feldes (ω_0) hindurch in die andere Hälfte in der Weise fort, daß je zwei zur Achse symmetrischen Punkten ω_0 zwei konjugierte komplexe Werte v entsprechen; hiermit ist das ganze Feld (ω_0) so auf der ganzen v-Ebene abgebildet, daß je zwei äquivalenten Werten ω_0, d. h. je zwei symmetrischen Punkten der Begrenzung von (ω_0) ein und derselbe (reelle) Wert v entspricht; je zwei nicht-äquivalenten Werten ω_0 entsprechen zwei verschiedene Werte v, und umgekehrt entspricht jedem Werte v ein einziger Wert ω_0, oder es entsprechen ihm zwei äquivalente Werte ω_0, welche der Begrenzung von (ω_0) angehören. Man kann daher die Abbildung von (ω_0) auf alle Felder (ω) der ganzen Halbebene S und deren Begrenzung R so ausdehnen, daß je zwei äquivalenten Werten ω ein und derselbe Wert v entspricht, und es leuchtet ein, daß bei dem Übergange von einem Felde (ω) durch die Begrenzung desselben zu einem benachbarten Felde die Funktion v sich stetig ändert.

Sind nun A, B, C, D beliebige reelle Konstanten, so hat die Funktion

$$\frac{C+Dv}{A+Bv}$$

dieselben Eigenschaften wie v, und sie nimmt ebenfalls jeden reellen Wert einmal an, wenn ω_0 die ganze Begrenzung der einen symmetrischen Hälfte des Feldes (ω_0) durchläuft; die drei verfügbaren Konstanten sollen nun so gewählt werden, daß

dem Werte $\omega_0 = \varrho$ der Wert $v = 0$,
„ „ $\omega_0 = i$ „ „ $v = 1$,
„ „ $\omega_0 = \infty$ „ „ $v = \infty$

entspricht. Die hierdurch bestimmte Funktion v will ich die Valenz von ω nennen und mit $\mathrm{val}(\omega)$ bezeichnen. Äquivalente Zahlen ω sind demnach Zahlen von gleicher Valenz.

§ 4.
Windungspunkte.

Um von dieser Definition der Funktion v zu ihrer analytischen Bestimmung zu gelangen, betrachten wir zunächst die umgekehrte Funktion; ist ω ein Zweig derselben, so ist jeder andere von der Form

$$\omega_1 = \frac{\gamma+\delta\omega}{\alpha+\beta\omega},$$

wo α, β, γ, δ vier ganze Zahlen bedeuten, welche der Bedingung $\alpha\delta - \beta\gamma = 1$ genügen, und es fragt sich, ob zwei solche im allgemeinen verschiedene Zweige in einem Windungspunkte v, für welchen $\omega = \omega_1 = \tau$ wird, zusammenhängen können. Hierzu ist erforderlich, daß τ eine Wurzel der Gleichung

$$\beta\tau^2 + (\alpha-\delta)\tau - \gamma = 0,$$

also

$$(2\beta\tau + \alpha - \delta)^2 = (\alpha+\delta)^2 - 4$$

ist, und da τ entweder rational ist oder eine positive Ordinate hat, so sind nur folgende drei Fälle möglich:

(I) $$\alpha + \delta = 0.$$

Da $\alpha^2 + 1 = (\alpha+i)(\alpha-i) = -\beta\gamma$ ist, und β positiv angenommen werden darf, so ergibt sich aus der Theorie der ganzen komplexen Zahlen von Gauß mit Leichtigkeit, daß man

$$-\alpha+i = (\alpha'-\beta'i)(\gamma'+\delta'i); \qquad \gamma = -(\gamma'+\delta'i)(\gamma'-\delta'i),$$
$$\beta = (\alpha'+\beta'i)(\alpha'-\beta'i); \quad \alpha+i = -(\alpha'+\beta'i)(\gamma'-\delta'i)$$

setzen kann, wo α', β', γ', δ' vier ganze rationale Zahlen bedeuten, welche offenbar der Bedingung $\alpha'\delta' - \beta'\gamma' = 1$ genügen müssen; die ganzen komplexen Zahlen $\alpha'+\beta'i$, $\gamma'+\delta'i$ sind relative Primzahlen, und man erhält

$$\tau = \frac{-\alpha+i}{\beta} = \frac{\gamma}{\alpha+i} = \frac{\gamma'+\delta'i}{\alpha'+\beta'i},$$

d. h. τ ist äquivalent mit i, und folglich ist $v = 1$. Nimmt man nun z. B. $\tau = i$, so ist

$$\alpha = 0, \quad \beta = 1, \quad \gamma = -1, \quad \delta = 0,$$

und die beiden in Rede stehenden Zweige sind

$$\omega_0 \quad \text{und} \quad \frac{-1}{\omega_0}.$$

Diese hängen aber wirklich an der Stelle $v = 1$, $\omega = i$ zusammen; denn wenn v, von Werten mit positiver Ordinate ausgehend, einen positiven Umlauf um $v = 1$ macht, also die Achse der reellen v zuerst zwischen 0 und 1, und nachher zwischen 1 und $+\infty$ kreuzt, so geht ω_0 aus derjenigen Hälfte des Hauptfeldes (ω_0), in welcher die Abszissen negativ sind, durch den Kreisbogen (3) zwischen ϱ und i zunächst in die Hälfte des Feldes $\left(\frac{-1}{\omega_0}\right)$ über, in welcher die Abszissen negativ sind, und dann durch die Ordinatenachse hindurch in die andere Hälfte desselben Feldes $\left(\frac{-1}{\omega_0}\right)$, in welcher die Abszissen positiv sind. Hieraus ergibt sich, daß $(1-v)$ unendlich klein wie $(\omega-i)^2$ wird, und folglich bleibt in diesem Windungspunkte das Produkt

$$(1-v)^{-1/2}\frac{dv}{d\omega}$$

endlich und von Null verschieden. Dasselbe gilt für je zwei Zweige

$$\omega = \frac{\gamma'+\delta'\omega_0}{\alpha'+\beta'\omega_0} \quad \text{und} \quad \omega_1 = \frac{-\delta'+\gamma'\omega_0}{-\beta'+\alpha'\omega_0},$$

welche sich für $v = 1$ in irgend einem mit i äquivalenten Werte

$$\tau = \frac{\gamma'+\delta'i}{\alpha'+\beta'i}$$

vereinigen, und zwischen welchen die Relation

$$\omega_1 = \frac{\gamma-\alpha\omega}{\alpha+\beta\omega} = \frac{-(\gamma'^2+\delta'^2)+(\alpha'\gamma'+\beta'\delta')\omega}{-(\alpha'\gamma'+\beta'\delta')+(\alpha'^2+\beta'^2)\omega}$$

besteht.

(II) $$\alpha + \delta = \pm 1.$$

Setzt man zur Abkürzung

$$\varepsilon = \frac{1 - \alpha + \delta}{2},$$

so ist, je nachdem das obere oder untere Zeichen gilt,

$$\varepsilon = 1 - \alpha = \delta \quad \text{oder} \quad \varepsilon = -\alpha = 1 + \delta,$$

folglich in beiden Fällen

$$(\varepsilon + \alpha - 1)(\varepsilon + \alpha) = 0,$$

also

$$\alpha\delta = \alpha(2\varepsilon + \alpha - 1) = \varepsilon - \varepsilon^2;$$

mithin ist

$$-\beta\gamma = \varepsilon^2 - \varepsilon + 1 = (\varepsilon + \varrho)(\varepsilon + \varrho^2),$$

und da β positiv angenommen werden darf, so ergibt sich hieraus zufolge der Theorie der aus ϱ gebildeten ganzen komplexen Zahlen, daß man

$$\varepsilon + \varrho = (\alpha' + \beta'\varrho^2)(\gamma' + \delta'\varrho); \qquad \gamma = -(\gamma' + \delta'\varrho)(\gamma' + \delta'\varrho^2),$$
$$\beta = (\alpha' + \beta'\varrho)(\alpha' + \beta'\varrho^2); \quad \varepsilon + \varrho^2 = (\alpha' + \beta'\varrho)(\gamma' + \delta'\varrho^2)$$

setzen kann, wo α', β', γ', δ' vier ganze rationale Zahlen bedeuten, welche offenbar der Bedingung $\alpha'\delta' - \beta'\gamma' = 1$ genügen müssen; die ganzen komplexen Zahlen $\alpha' + \beta'\varrho$, $\gamma' + \delta'\varrho$ sind relative Primzahlen, und man erhält

$$\tau = \frac{\varepsilon + \varrho}{\beta} = \frac{-\gamma}{\varepsilon + \varrho^2} = \frac{\gamma' + \delta'\varrho}{\alpha' + \beta'\varrho},$$

d. h. τ ist äquivalent mit ϱ, und folglich ist $v = 0$. Nimmt man nun z. B. $\tau = \varrho$, so ist $\varepsilon = 0$, $\beta = 1$, also entweder

$$\alpha = 1, \quad \beta = 1, \quad \gamma = -1, \quad \delta = 0,$$

oder

$$\alpha = 0, \quad \beta = 1, \quad \gamma = -1, \quad \delta = -1,$$

und in der Tat geht, wenn v aus einem Werte mit positiver Ordinate einen positiven Umlauf um $v = 0$ macht, von den drei Zweigen

$$\omega_0, \quad \frac{-1 - \omega_0}{\omega_0}, \quad \frac{-1}{1 + \omega_0}$$

der erste in den zweiten, dieser in den dritten, und dieser wieder in den ersten über. (Macht v denselben Umlauf aus einem Werte mit negativer Ordinate, so gehen die drei Zweige

$$\frac{-1}{\omega_0}, \quad -1 + \omega_0, \quad \frac{-\omega_0}{-1 + \omega_0},$$

welche ebenfalls den Eckpunkt ϱ gemeinschaftlich haben, zyklisch ineinander über.) Hieraus folgt, daß in diesem Windungspunkte das Produkt

$$v^{-2/3}\frac{dv}{d\omega}$$

endlich und von Null verschieden bleibt. Ähnlich verhält es sich für alle anderen mit ϱ äquivalenten Werte τ.

(III) $$(\alpha + \delta)^2 = 4.$$

In diesem und nur in diesem Falle wird τ rational, also ein Repräsentant der Begrenzung R, und folglich wird $v = \infty$. Setzt man (was erlaubt ist) $\alpha + \delta = +2$, und

$$\tau = \frac{1 - \alpha}{\beta} = \frac{-\gamma}{1 - \alpha} = \frac{m}{n},$$

wo m, n relative Primzahlen, so ergibt sich

$$\alpha = 1 + gmn, \quad \beta = -gn^2, \quad \gamma = +gm^2, \quad \delta = 1 - gmn,$$

wo g eine willkürliche ganze Zahl bedeutet. Nimmt man z. B. $m = 1$, $n = 0$, also $\tau = \infty$, so erkennt man leicht, daß jeder der unendlich vielen Zweige $(g + \omega_0)$ durch einen positiven Umlauf von v um $v = \infty$ in den folgenden Zweig $(g + 1 + \omega_0)$ übergeht. Für unendlich große Werte von ω ist daher die unendlich kleine Größe

$$q^2 = 1^{\omega}$$

eine einändrige Funktion von v, und da umgekehrt v überall eine einwertige Funktion von 1^{ω} ist, so bleibt für $\omega = \infty$ das Produkt

$$v\,1^{\omega}$$

endlich und von Null verschieden, und zugleich wird

$$v^{-1}\frac{dv}{d\omega} = \frac{d\log v}{d\omega} = -2\pi i.$$

Hieraus läßt sich leicht das Verhalten von v für alle anderen rationalen Werte $\omega = \frac{m}{n}$ ableiten.

§ 5.

Differentialgleichungen.

Bedeuten u, v zwei beliebige voneinander abhängige Variable, so wollen wir zur Abkürzung den Differentialausdruck dritter Ordnung

(1) $$\frac{-4}{\sqrt{\frac{dv}{du}}}\frac{d}{dv}\frac{d}{dv}\sqrt{\frac{dv}{du}} = [v, u]$$

setzen; man findet leicht, daß derselbe die beiden Eigenschaften

$$[u, v] = -[v, u]\left(\frac{dv}{du}\right)^2, \tag{2}$$

$$[v, u]\,dv^2 + [w, v]\,dw^2 + [u, w]\,du^2 = 0 \tag{3}$$

besitzt, wo w ebenfalls eine beliebige Funktion von u, also auch von v bedeutet. Sind ferner u, w kollineare Variable, womit ausgedrückt sein soll, daß

$$w = \frac{C + Du}{A + Bu} \tag{4}$$

ist, wo A, B, C, D Konstanten bedeuten, so ist

$$[u, w] = [w, u] = 0, \tag{5}$$

und folglich, was auch v sein mag,

$$[v, u] = [v, w]; \tag{6}$$

und umgekehrt, wenn $[u, w] = 0$ ist, so sind u, w kollinear, d. h. die Gleichung (4) ist das allgemeine Integral der Differentialgleichung (5).

Diese allgemeinen Sätze wenden wir auf folgendes Beispiel an. Es sei wieder $v = \mathrm{val}(\omega)$, so ist offenbar

$$[v, \omega] = f(\omega)$$

eine einwertige Funktion von ω, da sie auf rationale Weise aus den Derivierten erster, zweiter und dritter Ordnung von v in bezug auf ω gebildet ist; wir wollen nun beweisen, daß sie auch eine einwertige Funktion von v ist. In der Tat, setzt man $v_1 = \mathrm{val}(\omega_1)$, wo ω_1 eine neue Variable bedeutet, so ist $f(\omega_1) = [v_1, \omega_1]$; und wenn ω_1 mit ω durch die Gleichung

$$\omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}$$

verbunden wird, wo α, β, γ, δ ganze Zahlen bedeuten, welche der Bedingung $\alpha\delta - \beta\gamma = 1$ genügen, so ist $v_1 = v$, also $f(\omega_1) = [v, \omega_1]$; da außerdem ω, ω_1 kollinear sind, so folgt aus (6), daß $[v, \omega] = [v, \omega_1]$, also $f(\omega) = f(\omega_1)$ ist; mithin entspricht jedem Werte v nur ein einziger Wert $f(\omega)$. Wir können daher

$$[v, \omega] = F(v) \tag{7}$$

setzen, wo $F(v)$ eine einwertige Funktion von v bedeutet. Aus ihrer Bildung geht hervor, daß sie für alle Werte v, mit Ausnahme von 1, 0, ∞ endlich bleibt, und da für diese Werte von v, denen man

die Werte i, ϱ, ∞ von ω entsprechen lassen darf, respektive das Produkt

$$(1-v)^{-1/2}\frac{dv}{d\omega}, \quad v^{-2/3}\frac{dv}{d\omega}, \quad v^{-1}\frac{dv}{d\omega}$$

endlich und von Null verschieden bleibt, so ergibt sich, daß entsprechend

$$(1-v)^2F(v) = \tfrac{3}{4}, \quad v^2F(v) = \tfrac{8}{9}, \quad v^2F(v) = 1$$

wird; da folglich die einwertige Funktion $v^2(1-v)^2F(v)$ für alle endlichen Werte von v endlich bleibt und für $v = \infty$ unendlich groß von zweiter Ordnung wird, so ist sie eine ganze Funktion zweiten Grades, deren Koeffizienten aus den vorstehenden drei Gleichungen sich unmittelbar ergeben; auf diese Weise findet man

$$\begin{cases} F(v) = \dfrac{36v^2 - 41v + 32}{36v^2(1-v)^2} \\ \qquad = \dfrac{8}{9v^2} + \dfrac{23}{36v} + \dfrac{3}{4(1-v)^2} + \dfrac{23}{36(1-v)}. \end{cases} \tag{8}$$

Die Funktion $v = \mathrm{val}(\omega)$ ist daher eine Lösung v' der Differentialgleichung dritter Ordnung

$$[v'\,\omega] = F(v'); \tag{9}$$

um ihr allgemeines Integral v' zu finden, setze man $v' = \mathrm{val}(\omega')$, wo ω' eine neue Variable bedeutet; dann ist $[v', \omega'] = F(v')$, also $[v', \omega'] = [v', \omega]$, woraus mit Rücksicht auf (2) und (3) folgt, daß $[\omega, \omega'] = 0$, also

$$\omega' = \frac{C + D\omega}{A + B\omega}, \quad v' = \mathrm{val}\left(\frac{C + D\omega}{A + B\omega}\right) \tag{10}$$

ist, wo A, B, C, D willkürliche Konstanten bedeuten. Zugleich ergibt sich aus (3), daß das System der beiden Gleichungen

$$v = \mathrm{val}(\omega), \quad v' = \mathrm{val}\left(\frac{C + D\omega}{A + B\omega}\right) \tag{11}$$

das allgemeine Integral der Differentialgleichung dritter Ordnung

$$[v, v']\,dv^2 = F(v)\,dv^2 - F(v')\,dv'^2 \tag{12}$$

bildet (vgl. Fund. nova §§ 32, 33).

§ 6.

Die elliptischen Modulfunktionen.

Aus der Bildung des Ausdrucks $[v, \omega]$ geht hervor, daß $\sqrt{\frac{dv}{d\omega}}$ einer linearen Differentialgleichung zweiter Ordnung in bezug auf v genügt; allein es ist offenbar zweckmäßiger, die Größe

$$w = const\, v^{-1/3}(1-v)^{-1/4}\left(\frac{dv}{d\omega}\right)^{1/2} \tag{1}$$

einzuführen, welche für alle Werte von ω innerhalb S endlich und von Null verschieden bleibt, während sie in der Begrenzung R stets unendlich klein wird; mithin ist $\log w$ und jede Potenz von w, sobald ihr Wert an einer Stelle des einfach zusammenhängenden Gebietes S gegeben ist, eine völlig bestimmte, durchaus einwertige Funktion von ω. Aus der obigen Differentialgleichung dritter Ordnung (7) in § 5 folgt nun, daß w der hypergeometrischen Differentialgleichung

$$v(1-v)\frac{d^2w}{dv^2} + (\tfrac{2}{3} - \tfrac{7}{6}v)\frac{dw}{dv} - \tfrac{1}{144}w = 0 \tag{2}$$

genügt, deren allgemeines Integral $(const + const\,\omega)w$ in der Form

$$const \cdot F(\tfrac{1}{12}, \tfrac{1}{12}, \tfrac{2}{3}, v) + const \cdot F(\tfrac{1}{12}, \tfrac{1}{12}, \tfrac{1}{3}, 1-v)$$

enthalten ist, wo F die Reihe von Gauß bedeutet. Dasselbe hätte man auch durch direkte Untersuchung der Größe w als einer Riemannschen P-Funktion erhalten, und noch einfacher würde man, wie mein Freund Heinrich Weber in Königsberg mir vor einem Jahre mitgeteilt hat, durch die Betrachtungen zum Ziele gelangen können, welche den Gegenstand der Abhandlung XXV in Riemanns Werken bilden. Endlich bemerke ich, daß das in § 3 behandelte Abbildungsproblem sich auch durch die Untersuchungen von Weierstrass und Schwarz erledigen läßt.

Von besonderem Interesse ist nun die Quadratwurzel der Größe w, und ich will dieselbe durch

$$\eta(\omega) = const\, v^{-1/6}(1-v)^{-1/6}\left(\frac{dv}{d\omega}\right)^{1/4} \tag{3}$$

bezeichnen; sie ist, wie schon bemerkt, eine einwertige Funktion von ω, welche für alle Werte von ω innerhalb S endlich und von Null verschieden bleibt; für $\omega = \infty$ wird sie unendlich klein wie $v^{-1/24}$, also wie $1^{\omega/24}$; ich wähle die Konstante so, daß für $\omega = \infty$ das Produkt

$$1^{-\frac{\omega}{24}}\eta(\omega) = 1 \tag{4}$$

wird, und hierdurch ist $\eta(\omega)$ für das ganze Gebiet S vollständig bestimmt. Bedeuten α, β, γ, δ wieder vier ganze Zahlen, welche der Bedingung $\alpha\delta - \beta\gamma = 1$ genügen, so folgt aus

$$\mathrm{val}\left(\frac{\gamma + \delta\,\omega}{\alpha + \beta\,\omega}\right) = \mathrm{val}(\omega)$$

die Eigenschaft

$$\eta\left(\frac{\gamma + \delta\,\omega}{\alpha + \beta\,\omega}\right) = c(\alpha + \beta\,\omega)^{1/2}\eta(\omega), \tag{5}$$

wo $c^{24} = 1$ ist; speziell ergibt sich leicht

$$\eta(1+\omega) = 1^{1/24}\eta(\omega); \quad \eta\left(\frac{-1}{\omega}\right) = 1^{-1/8}\omega^{1/2}\eta(\omega), \tag{6}$$

wo $\omega^{1/2} = 1^{1/8}$ wird, wenn $\omega = 1^{1/4} = i$ ist. Die Funktion ist durch die genannten Eigenschaften vollständig bestimmt; denn wenn $f(\omega)$ ebenso beschaffen ist, so ist der Quotient $f(\omega) : \eta(\omega)$ zufolge (6) eine einwertige Funktion von $v = \mathrm{val}(\omega)$, welche für alle endlichen Werte von v endlich bleibt und zufolge (4) für $v = \infty$ den Wert Eins annimmt, und folglich $const = 1$ ist.

Um nun den Zusammenhang zwischen dieser Funktion $\eta(\omega)$ und dem Modul der elliptischen Integrale oder dessen Quadrat k herzustellen, betrachte ich die der Transformation zweiter Ordnung entsprechenden Funktionen

$$\eta_1(\omega) = \eta(2\omega); \quad \eta_2(\omega) = \eta\left(\frac{\omega}{2}\right); \quad \eta_3(\omega) = \eta\left(\frac{1+\omega}{2}\right), \tag{7}$$

welche folgende Eigenschaften besitzen. Aus (6) folgt

$$\eta_1(1+\omega) = 1^{1/12}\eta_1(\omega); \quad \eta_1\left(\frac{-1}{\omega}\right) = 1^{-1/8}\left(\frac{\omega}{2}\right)^{1/2}\eta_2(\omega),$$

$$\eta_2(1+\omega) = \eta_3(\omega) \quad ; \quad \eta_2\left(\frac{-1}{\omega}\right) = 1^{-1/8}(2\omega)^{1/2}\eta_1(\omega),$$

$$\eta_3(1+\omega) = 1^{1/24}\eta_2(\omega); \quad \eta_3\left(\frac{-1}{\omega}\right) = 1^{-1/8}\omega^{1/2}\eta_3(\omega),$$

und für $\omega = \infty$ folgt aus (4)

$$1^{-\frac{\omega}{12}}\eta_1(\omega) = 1; \quad 1^{-\frac{\omega}{48}}\eta_2(\omega) = 1; \quad 1^{-\frac{\omega}{48}}\eta_3(\omega) = 1^{1/48}.$$

Hieraus ergibt sich, daß die Funktion

$$f(\omega) = \frac{\eta_1(\omega)\,\eta_2(\omega)\,\eta_3(\omega)}{\eta(\omega)^3}$$

die Eigenschaften

$$f(1+\omega) = f(\omega), \quad f\left(\frac{-1}{\omega}\right) = f(\omega)$$

besitzt und folglich eine einwertige Funktion von $v = \mathrm{val}(\omega)$ ist, weil alle Substitutionen $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ sich aus den beiden Substitutionen $\begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix}$ und $\begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}$ zusammensetzen lassen; sie bleibt vermöge ihrer Definition endlich für alle endlichen Werte v und wird $= 1^{1/48}$ für $\omega = \infty$, $v = \infty$, folglich ist sie eine Konstante. Es ist daher

$$\eta_1(\omega)\,\eta_2(\omega)\,\eta_3(\omega) = 1^{1/48}\eta(\omega)^3, \tag{8}$$

und ein ähnlicher Satz gilt für Transformationen von beliebiger Ordnung. Ebenso ergibt sich, daß die Funktion

$$f_1(\omega) = \frac{2^4\eta_1(\omega)^8 + \eta_2(\omega)^8 + 1^{1/3}\eta_3(\omega)^8}{\eta(\omega)^8}$$

die Eigenschaften

$$f_1(1+\omega) = 1^{1/3} f_1(\omega), \quad f_1\left(\frac{-1}{\omega}\right) = f_1(\omega)$$

besitzt, woraus folgt, daß $f_1(\omega)^3$ eine einwertige Funktion von $v = \mathrm{val}(\omega)$ ist, welche für jeden endlichen Wert von v endlich ist; für $\omega = \infty$, $v = \infty$ wird ferner $f_1(\omega)1^{\omega/6} = 0$, also auch $f_1(\omega)^3 v^{-1/2} = 0$; also kann $f_1(\omega)^3$ nicht einmal von der Ordnung $v^{1/2}$ unendlich groß werden, und folglich ist $f_1(\omega)^3$, also auch $f_1(\omega)$ eine Konstante, und zwar $= 0$, wie sich aus $f_1(1+\omega) = 1^{1/3} f_1(\omega)$ ergibt. Es ist daher

$$2^4\eta_1(\omega)^8 + \eta_2(\omega)^8 + 1^{1/3}\eta_3(\omega)^8 = 0. \tag{9}$$

Führt man nun die folgenden Bezeichnungen ein (welche mit denen von Hermite übereinstimmen)

$$\begin{cases} \varphi(\omega) = 1^{1/48}\sqrt{2}\cdot\dfrac{\eta_1(\omega)}{\eta_3(\omega)} = \sqrt[4]{\varkappa} = \sqrt[8]{k}, \\ \psi(\omega) = 1^{1/48}\dfrac{\eta_2(\omega)}{\eta_3(\omega)} = \sqrt[4]{\varkappa'} = \varphi\left(\dfrac{-1}{\omega}\right), \\ \chi(\omega) = 1^{1/48}\sqrt[6]{2}\cdot\dfrac{\eta(\omega)}{\eta_3(\omega)}, \end{cases} \tag{10}$$

so folgt aus (9)

$$\varphi(\omega^8) + \psi(\omega)^8 = 1, \quad \varkappa^2 + \varkappa'^2 = 1 \tag{11}$$

und aus (8)

$$\varphi(\omega)\psi(\omega) = \chi(\omega)^3; \tag{12}$$

außerdem kann man die Größen K, K' durch die Gleichungen

$$\sqrt{\frac{2K}{\pi}} = 1^{-1/24}\frac{\eta_3(\omega)^2}{\eta(\omega)}, \quad K'i = K\omega \tag{13}$$

definieren.

Für die Funktion $k = \varkappa^2 = \varphi(\omega)^8$ ergeben sich nun aus dem Obigen die Eigenschaften

$$\varphi(1+\omega)^8 = -2^4\frac{\eta_1(\omega)^8}{\eta_2(\omega)^8} = \frac{k}{k-1} \tag{14}$$

$$\varphi\left(\frac{-1}{\omega}\right)^8 = 1^{1/6}\frac{\eta_2(\omega)^8}{\eta_3(\omega)^8} = \varkappa'^2 = 1-k, \tag{15}$$

und außerdem ist

$$k\,1^{-\frac{\omega}{2}} = 2^4 \quad \text{für} \quad \omega = \infty. \tag{16}$$

Hieraus folgt, daß die Funktion

$$f_2(\omega) = \frac{(k+\varrho)^3(k+\varrho^2)^3}{k^2(1-k)^2}$$

die Eigenschaften

$$f_2(1+\omega) = f_2(\omega), \quad f_2\left(\frac{-1}{\omega}\right) = f_2(\omega)$$

besitzt, mithin eine einwertige Funktion von $v = \mathrm{val}(\omega)$ ist; sie kann nur dann unendlich werden, wenn $k = 0$, 1, ∞ wird; da aber k und $(1-k)$ Quotienten von η-Funktionen sind, so kann dies nur dann geschehen, wenn $v = \infty$ wird, also z. B. für $\omega = \infty$; in diesem Fall wird aber k zufolge (16) unendlich klein wie $1^{\omega/2}$, also wie $v^{-1/2}$, und folglich $f_2(\omega)$ unendlich groß wie v; mithin ist $f_2(\omega)$ eine ganze Funktion ersten Grades von v, also

$$\frac{(k+\varrho)^3(k+\varrho^2)^3}{k^2(1-k)^2} = av + b.$$

Um die Konstante b zu bestimmen, setze man $\omega = \varrho$, also $v = 0$; da nun

$$\eta_3(\varrho) = \eta\left(\frac{1+\varrho}{2}\right) = \eta\left(\frac{-1}{2\varrho}\right),$$

und folglich

$$\eta_3(\varrho)^8 = \eta\left(\frac{-1}{2\varrho}\right)^8 = (2\varrho)^4\eta(2\varrho)^8 = (2\varrho)^4\eta_1(\varrho)^8$$

ist, so ergibt sich für k der Wert

$$\varphi(\varrho)^8 = 1^{1/6}2^4\frac{\eta_1(\varrho)^8}{\eta_3(\varrho)^8} = -\varrho, \tag{17}$$

und folglich ist $b = 0$. Um a zu bestimmen, setze man $\omega = i$, also $v = 1$; dann ergibt sich für k der Wert

$$\varphi(i)^8 = \varphi\left(\frac{-1}{i}\right)^8 = 1 - \varphi(i)^8 = \tfrac{1}{2}, \tag{18}$$

woraus $a = \frac{27}{4}$ folgt. Auf diese Weise erhalten wir das Resultat

$$v = \mathrm{val}(\omega) = \tfrac{4}{27}\frac{(k+\varrho)^3(k+\varrho^2)^3}{k^2(1-k)^2}. \tag{19}$$

In dieser Form erscheint die Funktion v an mehreren Stellen der berühmten Abhandlung von Hermite über die Theorie der Modulargleichungen; ich bemerke zugleich, daß auch Gauß (Werke III, S. 386) die Absicht gehabt hat, eine solche Funktion einzuführen.

Man kann, in ähnlicher Weise, wie dies oben für $\eta(\omega)$ geschehen ist, beweisen, daß die Funktion $k = \varphi(\omega)^8$ durch die an-

gegebenen Eigenschaften vollständig bestimmt ist; die Prinzipien, auf welche sich der Nachweis der Existenz der Funktion v gestützt hat, führen auch ebenso leicht zur unmittelbaren Bestimmung der Funktion k; dieselbe erfordert, wie aus der Kombination von (14) und (15) hervorgeht, zu ihrer vollen Ausbreitung im Gebiete S sechs ganze oder zwölf halbe Felder (ω), welche letzteren so gewählt werden können, daß sie symmetrisch zu beiden Seiten der rein imaginären ω liegen. Man erhält auf diese Weise die Differentialgleichung dritter Ordnung

$$[k, \omega] = \frac{(k+\varrho)(k+\varrho^2)}{k^2(1-k)^2}, \tag{20}$$

und ebenso, wie wir oben zu einer linearen Differentialgleichung zweiter Ordnung für $w = const \cdot \eta(\omega)^2$ gelangt sind, ergibt sich hier, wenn man

$$\frac{dk}{d\omega} = \frac{-4}{\pi i} k(1-k)K^2 \tag{21}$$

setzt, die bekannte lineare Differentialgleichung

$$\frac{d}{dk}\left(k(1-k)\frac{dK}{dk}\right) = \tfrac{1}{4}K, \tag{22}$$

welche den Ausgangspunkt der Abhandlung von Fuchs bildet. Natürlich würde man dieselben Resultate auch aus dem Zusammenhang zwischen k und v finden, welcher in (19) ausgedrückt ist.

Da k durch die obigen Eigenschaften als Funktion von ω vollständig bestimmt ist, und da die in der Theorie der elliptischen oder ϑ-Funktionen auftretende Funktion

$$\frac{\vartheta_2(0,\omega)^4}{\vartheta_3(0,\omega)^4}$$

wirklich dieselben Eigenschaften besitzt, so ergibt sich aus dieser Identität beider Funktionen leicht, daß

$$\begin{cases} \vartheta(0,\omega) = \dfrac{\eta_3(\omega)^2}{\eta(\omega)}; \quad \vartheta_1'(0,\omega) = 2\pi\eta(\omega)^3, \\ \vartheta_2(0,\omega) = 2\dfrac{\eta_1(\omega)^2}{\eta(\omega)}; \quad \vartheta_3(0,\omega) = 1^{-\frac{1}{24}}\dfrac{\eta_3(\omega)^2}{\eta(\omega)}, \end{cases} \tag{23}$$

und folglich

$$\eta(\omega) = 1^{\omega/24}\Pi(1-1^{\omega\nu}) = q^{1/12}\Pi(1-q^{2\nu}) \tag{24}$$

ist, wo ν alle positiven ganzen Zahlen durchläuft und

$$q = 1^{\omega/2} \tag{25}$$

gesetzt ist. Allein es ist mir bisher nicht geglückt, diese Darstellung von $\eta(\omega)$ als explizite Funktion von ω lediglich aus ihrer obigen Definition, also ohne die Hilfe der Theorie der ϑ-Funktionen abzuleiten.

Die eingehende Beschäftigung mit dieser Funktion $\eta(\omega)$, zu welcher mich zuerst die Untersuchung über die Anzahl der Idealklassen in kubischen Körpern veranlaßt hatte, ist mir später von großem Nutzen bei der Bearbeitung des zweiten Fragmentes XXVII aus dem Nachlasse von Riemann gewesen. Die Zahlen (m, n), auf welche ich durch das Studium desselben geführt bin, besitzen in der Tat sehr interessante Eigenschaften; ist z. B. n eine positive ungerade Zahl, und m relative Primzahl zu n, so ist

$$\left(\frac{m}{n}\right) \equiv \frac{n+1}{2} - (m,n) \pmod 4,$$

wo $\left(\frac{m}{n}\right)$ das Zeichen von Legendre und Jacobi aus der Theorie der quadratischen Reste bedeutet; ist m ebenfalls positiv und ungerade, so ergibt sich hieraus unter Zuziehung des Satzes

$$2m(m,n) + 2n(n,m) = 1 + m^2 + n^2 - 3mn$$

sofort der verallgemeinerte Reziprozitätssatz in der Form

$$\left(\frac{m}{n}\right) + \left(\frac{n}{m}\right) \equiv 2\left(1 + \frac{m-1}{2}\cdot\frac{n-1}{2}\right) \pmod 4.$$

Ich erlaube mir hier auf eine Stelle der Abhandlung von Fuchs aufmerksam zu machen, in welche, wie mir scheint, sich ein Irrtum eingeschlichen hat. Sind m, n relative Primzahlen, und nähert sich $\omega = x + yi$ dem rationalen Werte $\frac{m}{n}$ so an, daß x konstant $= \frac{m}{n}$ bleibt, und y positiv unendlich klein wird, so nähert sich k, wie aus dem Fragment von Riemann oder auch aus der obigen Theorie folgt, dem Werte

$$\begin{aligned} k &= \infty, \quad \text{wenn} \quad m \equiv 1, \quad n \equiv 1 \pmod 2, \\ k &= 1, \quad \text{„} \quad m \equiv 0, \quad n \equiv 1 \quad \text{„} \\ k &= 0, \quad \text{„} \quad m \equiv 1, \quad n \equiv 0 \quad \text{„} \end{aligned}$$

ist; wenn dagegen $\omega = x + yi$ sich auf dieselbe Weise einem irrationalen reellen Wert x nähert, so ergibt sich aus der obigen Theorie (vgl. den Schluß von § 2), daß k sich keinem bestimmten Werte nähert, sondern unaufhörliche Schwankungen erleidet. Dies steht im Widerspruch mit dem Satze II auf S. 27 der genannten

Abhandlung, in welchem behauptet wird, daß die Größe u ($= k^{-1}$ nach meiner Bezeichnung) sich immer einem der beiden Werte Null oder Eins annähern müsse, und mir scheint, als sei der Beweis dieser Behauptung gerechten Bedenken unterworfen, namentlich in dem Teile, welcher auf die Worte „ou n'y parvînt pas“ (S. 26) folgt. Doch ist diese Abweichung von keiner wesentlichen Bedeutung für den Hauptgegenstand der sehr interessanten Abhandlung.

§ 7.

Transformation.

Ich will nun noch zum Schluß die Theorie der algebraischen Gleichungen zwischen Valenzen begründen, welche den Modulargleichungen in der Theorie der Transformation der elliptischen oder ϑ-Funktionen entsprechen. Es sei wieder $v = \mathrm{val}(\omega)$, und

$$v_n = \mathrm{val}\left(\frac{C + D\omega}{A + B\omega}\right),$$

wo A, B, C, D vier beliebige ganze Zahlen ohne gemeinschaftlichen Teiler und von positiver Determinante

$$AD - BC = n$$

bedeuten. Die Anzahl aller möglichen solchen Funktionen v_n, welche einer gegebenen positiven ganzen Zahl n entsprechen, ist endlich und leicht zu bestimmen. Es sei nämlich, wenn A, B, C, D gegeben sind, ∂ der größte positive gemeinschaftliche Teiler der beiden Zahlen

$$B = \partial\beta, \quad D = \partial\delta,$$

so ist

$$n = a\partial, \quad \text{wo} \quad a = A\delta - C\beta;$$

nun kann man, da β, δ relative Primzahlen sind, die beiden ganzen Zahlen α, γ stets und nur auf eine einzige Art so bestimmen, daß $\alpha\delta - \beta\gamma = 1$ wird, und daß zugleich die Zahl

$$c = C\alpha - A\gamma$$

der Bedingung

$$0 \leqq c < a$$

genügt; dann ist

$$\begin{pmatrix} A, & B \\ C, & D \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix},$$

mithin

$$v_n = \mathrm{val}\left(\frac{C + D\omega}{A + B\omega}\right) = \mathrm{val}\left(\frac{c + \partial\omega}{a}\right),$$

und da A, B, C, D keinen gemeinschaftlichen Teiler haben, so gilt dasselbe auch von den drei Zahlen a, c, ∂. Um daher für eine gegebene Zahl n alle möglichen Funktionen v_n zu erhalten, braucht man nur a alle positiven Divisoren von n durchlaufen zu lassen; für jeden solchen Divisor a bestimmt sich ∂ durch die Gleichung $a\partial = n$; ist nun e der größte gemeinschaftliche Teiler von a und ∂, so darf, wenn $\varphi(e)$ die Anzahl derjenigen Zahlen 0, 1, 2, … $(e-1)$ bedeutet, welche relative Primzahlen zu e sind, die Zahl c alle diejenigen $\frac{a}{e}\varphi(e)$ Zahlen durchlaufen, welche relative Primzahlen zu e sind und zugleich der Bedingung $0 \leqq c < a$ genügen. Es läßt sich ferner leicht zeigen, daß je zwei verschiedenen Systemen von drei solchen Zahlen a, c, ∂ auch zwei nichtidentische Funktionen

$$v_n = \mathrm{val}\left(\frac{c + \partial\omega}{a}\right)$$

entsprechen, und folglich ist die Anzahl aller wirklich verschiedenen Funktionen v_n gleich

$$\sum \frac{a}{e}\varphi(e) = \psi(n),$$

wo a alle Divisoren von n durchläuft, und e jedesmal die oben angegebene Bedeutung hat. Aus dieser Form folgt sofort, wenn n, n' relative Primzahlen sind, der Satz

$$\psi(nn') = \psi(n)\psi(n');$$

der Fall einer Primzahlpotenz ist leicht zu erledigen, und hieraus ergibt sich allgemein

$$\psi(n) = n\Pi\left(1 + \frac{1}{p}\right),$$

wo p alle verschiedenen in n aufgehenden Primzahlen durchläuft.

Setzt man zur Abkürzung $\psi(n) = \nu$, und bezeichnet mit

$$f_1(\omega), f_2(\omega), \ldots, f_\nu(\omega)$$

die sämtlichen verschiedenen in der Form

$$\mathrm{val}\left(\frac{C + D\omega}{A + B\omega}\right)$$

enthaltenen Funktionen v_n, so sind, wenn α, β, γ, δ vier bestimmte ganze Zahlen bedeuten, welche der Bedingung $\alpha\delta - \beta\gamma = 1$ genügen, auch die ν Funktionen

$$f_1\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right), \quad f_2\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right), \quad \ldots, \quad f_\nu\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right)$$

voneinander verschieden; da ferner jedes System von vier ganzen Zahlen A, B, C, D ohne gemeinschaftlichen Teiler, welche die Bedingung $AD - BC = n$ befriedigen, durch die Zusammensetzung

$$\begin{pmatrix} A, & B \\ C, & D \end{pmatrix}\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} A', & B' \\ C', & D' \end{pmatrix}$$

wieder ein System von vier ganzen Zahlen A', B', C', D' liefert, welche keinen gemeinschaftlichen Teiler haben und der Bedingung $A'D' - B'C' = n$ genügen, so ist jede dieser Funktionen identisch mit einer der ν Funktionen v_n, und folglich ist ihr Komplex identisch mit dem der Funktionen v_n. Bedeutet daher σ eine willkürliche, von ω unabhängige Größe, so ist das über alle ν Funktionen v_n ausgedehnte Produkt

$$\Pi(\sigma - v_n)$$

eine einwertige Funktion von ω, welche ungeändert bleibt, wenn ω durch eine beliebige äquivalente Größe

$$\frac{\gamma + \delta\,\omega}{\alpha + \beta\,\omega}$$

ersetzt wird, und folglich kann man

$$\Pi(\sigma - v_n) = F_n(\sigma, v)$$

setzen, wo $F_n(\sigma, v)$ eine ganze Funktion ν^{ten} Grades von σ bedeutet, deren Koeffizienten einwertige Funktionen von $v = \operatorname{val}(\omega)$ sind. Ist v endlich, so gehört ω dem Innern des Gebietes S an, und folglich ist jeder der ν Werte v_n, also auch $F_n(\sigma, v)$ endlich. Wird aber $v = \infty$, so darf man annehmen, daß auch $\omega = \infty$ wird; da nun in diesem Falle

$$1^{\omega}\operatorname{val}(\omega) = m,$$

also

$$1^{\frac{\delta}{a}\omega}\operatorname{val}\left(\frac{c + \partial\,\omega}{a}\right) = m\,1^{-\frac{c}{a}}$$

wird, wo m endlich und von Null verschieden ist [nämlich $= 2^{-6}3^{-3}$, wie sich aus (16) und (19) in § 6 ergibt], so folgt, daß $F_n(\sigma, v)$ gleichzeitig mit v unendlich groß wird, und zwar von der Ordnung

$$\sum \frac{\partial}{a}\cdot\frac{a}{e}\varphi(e) = \sum \frac{\partial}{e}\varphi(e) = \sum \frac{a}{e}\varphi(e) = \nu;$$

mithin ist

$$F_n(\sigma, v) = \sigma^{\nu} + V_1\sigma^{\nu-1} + V_2\sigma^{\nu-2} + \cdots + V_{\nu}$$

auch eine ganze Funktion ν^{ten} Grades von v, und es ist z. B.

$$-V_1 = \sum v_n = \frac{1}{m^{n-1}}v^n + \cdots$$

eine ganze Funktion n^{ten} Grades von v. Die ν Funktionen v_n sind daher algebraische Funktionen von v, nämlich die Wurzeln der Gleichung

$$F_n(v_n, v) = 0.$$

Diese Valenzgleichung ist irreduktibel. Genügt nämlich die Funktion $v_n' = \operatorname{val}(n\,\omega)$ einer Gleichung von der Form

$$G(v_n', v) = 0,$$

wo $G(\sigma, v)$ eine ganze rationale Funktion der beiden Größen σ, v bedeutet, so ist identisch

$$G(\operatorname{val}(n\,\omega), \operatorname{val}(\omega)) = 0,$$

folglich auch, wenn die vier ganzen Zahlen α, β, γ, δ der Bedingung $\alpha\delta - \beta\gamma = 1$ genügen,

$$G\left(\operatorname{val}\left(\frac{n\gamma + n\delta\,\omega}{\alpha + \beta\,\omega}\right),\ \operatorname{val}(\omega)\right) = 0;$$

läßt sich nun zeigen, wie gleich geschehen soll, daß die Funktion

$$\operatorname{val}\left(\frac{n\gamma + n\delta\,\omega}{\alpha + \beta\,\omega}\right)$$

durch geeignete Wahl der vier Zahlen α, β, γ, δ zur Übereinstimmung mit jeder der ν Funktionen

$$v_n = \operatorname{val}\left(\frac{c + \partial\,\omega}{a}\right)$$

gebracht werden kann, so genügt jede Funktion v_n der Gleichung $G(v_n, v) = 0$, mithin ist $G(\sigma, v)$ teilbar durch $F_n(\sigma, v)$, woraus die Irreduktibilität dieser letzteren Funktion folgt. Es ist also nur noch zu beweisen, daß, wenn drei Zahlen a, c, ∂ ohne gemeinschaftlichen Teiler gegeben sind, welche der Bedingung $a\,\partial = n$ genügen, man immer acht ganze Zahlen α, β, γ, δ, α', β', γ', δ' so wählen kann, daß $\alpha\delta - \beta\gamma = \alpha'\delta' - \beta'\gamma' = 1$ und

$$\begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix}\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix}\begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix}$$

wird. Die allgemeinste Art, solche Zahlen zu finden, ist die folgende (vgl. die zu Anfang dieses Paragraphen ausgeführte Reduktion). Man wähle für γ eine beliebige Zahl, welche relative Primzahl zu ∂ ist, und setze

$$\delta' = a\,\delta,$$

so kann man γ so wählen, daß die Zahl

$$\gamma' = \partial\,\gamma - c\,\delta$$

relative Primzahl zu δ' wird; denn wie man auch γ wählen mag, so ist γ' jedenfalls unteilbar durch diejenigen Primzahlen, welche gleichzeitig in a und in ∂, also in e aufgehen, weil a, c, ∂ keinen gemeinschaftlichen Teiler haben, und weil δ relative Primzahl zu ∂ ist; bezeichnet man ferner mit p das Produkt aller übrigen in a aufgehenden Primzahlen (oder die Einheit, falls keine solche vorhanden sind), so ist ∂ relative Primzahl zu p, also auch zu $p\delta$, und folglich durchläuft γ' gleichzeitig mit γ ein vollständiges Restsystem (mod. $p\delta$); mithin gibt es unendlich viele Werte von γ, für welche γ' relative Primzahl zu $p\delta$ und folglich auch zu $\delta' = a\delta$ wird. Nachdem δ, γ so gewählt sind, daß δ', γ' relative Primzahlen werden, wähle man eine beliebige Lösung α', β' der Gleichung

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

und setze

$$\alpha = a\alpha' + c\beta', \quad \beta = \partial\beta',$$

so wird

$$\alpha\delta - \beta\gamma = (a\alpha' + c\beta')\delta - \partial\beta'\gamma = \alpha'\delta' - \beta'\gamma' = 1,$$

und die gefundenen acht Zahlen erfüllen die obigen Forderungen weil

$$n\gamma = a\gamma' + c\delta', \quad n\delta = \partial\delta'$$

ist.

Die Funktion $F_n(\sigma, v)$ ist symmetrisch in bezug auf σ und v, wenn $n > 1$ ist. Denn aus der Identität

$$F_n(\mathrm{val}(n\omega), \mathrm{val}(\omega)) = 0$$

folgt, wenn man ω durch $\frac{\omega}{n}$ ersetzt, die Gleichung

$$F_n\left(v, \mathrm{val}\left(\frac{\omega}{n}\right)\right) = 0,$$

und da $\mathrm{val}\left(\frac{\omega}{n}\right)$ eine der ν Funktionen v_n ist, so ergibt sich aus der eben bewiesenen Irreduktibilität, daß $F_n(v, \sigma)$ durch $F_n(\sigma, v)$ teilbar und folglich $= \pm F_n(\sigma, v)$ sein muß; da aber im Falle des unteren Zeichens die irreduktible Funktion $F_n(\sigma, v)$ den Faktor $(\sigma - v)$ enthalten würde, so muß, wenn $n > 1$ ist, das obere Zeichen gelten.

Da die sämtlichen Funktionen v_n nur spezielle Fälle der in der Gleichung (11) des § 5 mit v' bezeichneten Funktion bilden, so besitzt die dortige Differentialgleichung (12) unendlich viele partikuläre Lösungen $v' = v_n$, welche algebraische Funktionen von v sind. Es

läßt sich auch zeigen, daß sie keine anderen algebraischen Lösungen besitzen kann, und hieraus kann man, wie ich glaube, den Satz ableiten, daß alle Koeffizienten der Funktion $F_n(\sigma, v)$ rationale Zahlen sind. Ich bemerke schließlich, daß man durch die Untersuchung der ganzen Funktion $F_n(v, v)$ oder auch der Diskriminante der Funktion $F_n(\sigma, v)$ zur Theorie der singulären Moduln geführt wird, für welche die komplexe Multiplikation der elliptischen Funktionen stattfindet; eine nähere Ausführung dieser Untersuchung, in welcher die Komposition der quadratischen Formen eine wesentliche Rolle spielt, muß ich mir aber für eine andere Gelegenheit versparen.

Braunschweig, den 12. Juni 1877.

Erläuterungen zur vorstehenden Abhandlung.

Es war zur Zeit der Entstehung dieser Abhandlung noch unbekannt, daß die hier von Dedekind beschriebene, später in der Theorie der Modulfunktionen so wichtig gewordene Dreiecksteilung der ω-Halbebene bereits weit früher aufgefunden worden war. Schon Gauß hat das Dreiecksnetz gekannt und benutzt, worüber man Bd. 8 seiner Werke, S. 102—105 vergleiche. Dasselbe gilt von Riemann, der in einer Vorlesung über die hypergeometrische Reihe im Wintersemester 1858/59 das Dreiecksnetz behandelt und zur Beschreibung der Abhängigkeit des Legendre-Jacobischen Integralmoduls k^2 vom Periodenverhältnis ω benutzt. Die Vorlesung ist s. Zt. durch v. Bezold nachgeschrieben; diese Nachschrift ist erst 1897 bekannt geworden und in den von M. Noether und W. Wirtinger herausgegebenen „Nachträgen zu Bernhard Riemanns gesammelten mathematischen Werken“ (Leipzig, 1902) allgemein zugänglich gemacht. Noch ehe die Abhandlung Dedekinds erschien, war F. Klein an die Theorie der elliptischen Modulfunktionen herangeführt. Seine erste ausführlichere Abhandlung über Modulfunktionen „Über die Transformation der elliptischen Funktionen und die Auflösung der Gleichungen fünften Grades“ (datiert Anfang Mai 1878) ist mit Dedekinds Arbeit eng verwandt. Klein hat sich über die Entstehung seiner Arbeiten über Modulfunktionen selbst ausführlich ausgesprochen in Band 3 seiner „Gesammelten mathematischen Abhandlungen“, S. 3—9.

Fricke.

XV.

Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen.

[Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Bd. 23, S. 1—23 (1878).]

Die neuen Prinzipien, durch welche ich zu einer ausnahmelosen und strengen Theorie der Ideale gelangt bin, habe ich zuerst vor sieben Jahren in der zweiten Auflage der Vorlesungen über Zahlentheorie von Dirichlet (§§ 159—170) entwickelt und neuerdings in dem Bulletin des sciences mathématiques et astronomiques (t. XI, p. 278; t. I (2e série), p. 17, 69, 144, 207) ausführlicher und in etwas veränderter Form dargestellt. Mit demselben Gegenstand hatte ich mich schon vorher, durch die große Entdeckung Kummers angeregt, eine lange Reihe von Jahren hindurch beschäftigt, wobei ich von einer ganz anderen Grundlage, nämlich von der Theorie der höheren Kongruenzen ausging; allein obgleich diese Untersuchungen mich dem erstrebten Ziele sehr nahe brachten, so konnte ich mich zu ihrer Veröffentlichung doch nicht entschließen, weil die so entstandene Theorie hauptsächlich an zwei Unvollkommenheiten leidet. Die eine besteht darin, daß die Untersuchung eines Gebietes von ganzen algebraischen Zahlen sich zunächst auf die Betrachtung einer bestimmten Zahl und der ihr entsprechenden Gleichung gründet, welche als Kongruenz aufgefaßt wird, und daß die so erhaltenen Definitionen der idealen Zahlen (oder vielmehr der Teilbarkeit durch die idealen Zahlen) zufolge dieser bestimmt gewählten Darstellungsform nicht von vornherein den Charakter der Invarianz erkennen lassen, welcher in Wahrheit diesen Begriffen zukommt; die zweite Unvollkommenheit dieser Begründungsart besteht darin, daß bisweilen eigentümliche Ausnahmefälle auftreten, welche eine besondere Behandlung verlangen. Meine neuere Theorie dagegen gründet sich ausschließlich auf solche Begriffe, wie die des Körpers,

der ganzen Zahl, des Ideals, zu deren Definition es gar keiner bestimmten Darstellungsform der Zahlen bedarf, und wie hierdurch der erstgenannte Mangel von selbst wegfällt, so bewährt sich die Kraft dieser äußerst einfachen Begriffe auch darin, daß bei dem Beweise der allgemeinen Gesetze der Teilbarkeit eine Unterscheidung mehrerer Fälle gar niemals mehr auftritt. Über den Zusammenhang zwischen beiden Begründungsarten habe ich in den Göttingischen gelehrten Anzeigen vom 20. September 1871 (S. 1488—1492) einige Bemerkungen und Sätze ohne Beweis mitgeteilt, und namentlich habe ich daselbst den Grund aufgedeckt, auf welchem das Auftreten der erwähnten eigentümlichen Ausnahmefälle beruht. Seitdem ist im Jahre 1874 eine Theorie der idealen Zahlen von Zolotareff erschienen, welche in russischer Sprache abgefaßt und unter dem Titel Théorie des nombres entiers complexes, avec une application au calcul intégral im Jahrbuch über die Fortschritte der Mathematik (Bd. 6, S. 117) angezeigt und kurz besprochen ist. Aus dieser Anzeige*) geht hervor, daß die Theorie von Zolotareff sich ebenfalls auf die Theorie der höheren Kongruenzen gründet, daß aber gerade die Behandlung der erwähnten Ausnahmefälle vorläufig ausgeschlossen und einer späteren Darstellung vorbehalten ist. Ich weiß nicht, ob diese in Aussicht gestellte Vervollständigung seitdem veröffentlicht worden ist; da aber der Zusammenhang zwischen den beiden Begründungsarten der allgemeinen Idealtheorie an sich ein hinreichendes Interesse besitzt, so erlaube ich mir, im folgenden die Beweise zu den in den Göttingischen gelehrten Anzeigen mitgeteilten Bemerkungen nachzuliefern. Hierbei muß ich sowohl meine Theorie der Ideale, als auch die Theorie der höheren Kongruenzen, von welcher ich früher in Borchardts Journal (Bd. 54, S. 1) eine gedrängte Darstellung gegeben habe, als bekannt voraussetzen; der Kürze halber werde ich diese Abhandlung über die Kongruenzen mit C., die zweite Auflage der Zahlentheorie von Dirichlet mit D., und die oben angeführte Abhandlung im Bulletin des sciences mathématiques mit B. zitieren.

*) Nur auf diese kann ich mich hier berufen; zwar habe ich das Originalwerk nach mehreren vergeblichen Versuchen, es mir im Buchhandel zu verschaffen, kürzlich durch die Güte des Herrn Prof. Wangerin geliehen erhalten, aber bei meiner Unkenntnis der russischen Sprache habe ich zu meinem großen Bedauern nur das Wenige verfolgen können, was schon aus dem Anblick der Formeln verständlich ist.

§ 1.

Es sei Ω ein endlicher Körper vom Grade n, und $\mathfrak{o}$ das Gebiet aller in Ω enthaltenen ganzen Zahlen, so gibt es immer eine aus n voneinander unabhängigen ganzen Zahlen

$$\omega_1,\ \omega_2 \cdots \omega_n$$

bestehende Basis des Gebietes $\mathfrak{o}$, d. h. das System $\mathfrak{o}$ ist identisch mit dem Inbegriffe

$$[\omega_1,\ \omega_2 \cdots \omega_n]$$

aller Zahlen ω von der Form

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n,$$

wo

$$h_1,\ h_2 \cdots h_n$$

willkürliche ganze rationale Zahlen bedeuten; die Diskriminante

$$\Delta(\omega_1,\ \omega_2 \cdots \omega_n) = \Delta(\Omega) = D,$$

welche von der Wahl der Basiszahlen $\omega_1,\ \omega_2 \cdots \omega_n$ unabhängig ist, heißt die Grundzahl oder die Diskriminante des Körpers Ω (D. §§ 159, 160, 162; B. §§ 13—18).

Ist nun θ eine bestimmte ganze Zahl des Körpers, so kann man

$$\begin{aligned}
1 &= c_1^0\omega_1 + c_2^0\omega_2 + \cdots + c_n^0\omega_n\\
\theta &= c_1'\omega_1 + c_2'\omega_2 + \cdots + c_n'\omega_n\\
\theta^2 &= c_1''\omega_1 + c_2''\omega_2 + \cdots + c_n''\omega_n\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\theta^{n-1} &= c_1^{(n-1)}\omega_1 + c_2^{(n-1)}\omega_2 + \cdots + c_n^{(n-1)}\omega_n
\end{aligned}$$

setzen, wo die sämtlichen n^2 Koeffizienten oder Koordinaten c ganze rationale Zahlen bedeuten, und es ist

$$\Delta(1,\ \theta,\ \theta^2 \cdots \theta^{n-1}) = Dk^2,$$

wo

$$k = \sum \pm c_1^0 c_2' \cdots c_n^{(n-1)}$$

eine ganze rationale Zahl ist; diese Zahl k, deren absoluter Wert von der Wahl der Basiszahlen $\omega_1,\ \omega_2 \cdots \omega_n$ unabhängig ist, soll im folgenden der Kürze halber der Index der ganzen Zahl θ genannt werden. Ist k, wie wir immer voraussetzen werden, von 0 verschieden, so sind die n Zahlen

$$1,\ \theta,\ \theta^2 \cdots \theta^{n-1}$$

voneinander unabhängig (D. § 159; B. §§ 4, 15, 17) und θ ist die Wurzel einer irreduktiblen Gleichung n^{ten} Grades

$$F(\theta) = \theta^n + a_1\theta^{n-1} + a_2\theta^{n-2} + \cdots + a_n = 0,$$

deren Koeffizienten $1,\ a_1,\ a_2 \cdots a_n$ ganze rationale Zahlen sind.

Bedeutet ferner $\varphi(t)$ jede beliebige Funktion der Variabelen t, — und ich bemerke ein für allemal, daß unter diesem Namen und unter einem Zeichen von der Form $\varphi(t),\ f(t) \cdots$ in der gegenwärtigen Abhandlung ausschließlich eine ganze Funktion von t verstanden werden soll, deren Koeffizienten ganze rationale Zahlen sind —, so bildet der Inbegriff $\mathfrak{o}'$ aller Zahlen von der Form

$$\omega' = \varphi(\theta)$$

eine sogenannte Ordnung (D. §§ 165, 166; B. § 23); alle diese Zahlen sind ganze Zahlen des Körpers Ω und folglich auch in $\mathfrak{o}$ enthalten. Offenbar ist es gestattet, nur solche Funktionen

$$\varphi(t) = x_0 + x_1 t + x_2 t^2 + \cdots + x_{n-1}t^{n-1}$$

zu betrachten, deren Grad kleiner als n ist; denn wenn der Grad einer Funktion $\varphi_1(t)$ gleich n oder größer ist, so liefert sie, durch die Funktion

$$F(t) = t^n + a_1 t^{n-1} + a_2 t^{n-2} + \cdots + a_{n-1}t + a_n$$

dividiert, einen Rest $\varphi(t)$ von niedrigerem Grade als n, und gleichzeitig ist $\varphi_1(\theta) = \varphi(\theta)$; mit Benutzung einer schon oben gebrauchten Bezeichnungsweise (B. § 3) kann man daher

$$\mathfrak{o}' = [1,\ \theta,\ \theta^2 \cdots \theta^{n-1}]$$

setzen. Außerdem ergibt sich aus der Irreduktibilität der Gleichung $F(\theta) = 0$, daß jede Zahl ω' nur auf eine einzige Weise in dieser letzteren Form $\varphi(\theta)$ darstellbar ist; doch werden wir uns im folgenden durchaus nicht immer auf diese Darstellungsform der Zahlen ω' beschränken, vielmehr auch Funktionen von beliebig hohem Grade zulassen.

Die sämtlichen Primzahlen p — mit welchem Namen stets rationale, positive Primzahlen bezeichnet sein sollen — zerfallen nun, nachdem einmal eine bestimmte Zahl θ gewählt und der Darstellung zugrunde gelegt ist, in zwei verschiedene Arten; die erste Art besteht aus den unendlich vielen Primzahlen, welche in dem Index k der Zahl θ nicht aufgehen; falls $k = \pm 1$ ist, gehören alle Primzahlen dieser ersten Art an, und $\mathfrak{o}'$ ist identisch mit $\mathfrak{o}$. Wenn aber $k^2 > 1$ ist, so gibt es eine endliche Anzahl von Primzahlen der zweiten Art, nämlich solchen, welche in k aufgehen. Es wird sich im folgenden Paragraphen zeigen, daß die Zerlegung der Primzahlen p der ersten Art, oder vielmehr die Zerlegung der ihnen entsprechenden

Hauptideale $\mathfrak{o}\,p$*) in Produkte aus lauter Primidealen sich vollständig zurückführen läßt auf die Zerlegung der Funktion $F(t)$ in ein Produkt aus lauter Primfunktionen in bezug auf den Modul p (C. 6), während dies für Primzahlen der zweiten Art nicht in gleich einfacher Weise möglich ist. Dieser Untersuchung sind folgende Bemerkungen vorauszuschicken.

Es sei p eine bestimmte Primzahl der ersten Art, also k nicht teilbar durch p. In diesem Falle ist eine in $\mathfrak{o}'$ enthaltene Zahl

$$\omega' = x_0 + x_1\theta + x_2\theta^2 + \cdots + x_{n-1}\theta^{n-1}$$

nur dann durch p teilbar (also von der Form $p\,\omega$, wo ω eine ganze, d. h. in $\mathfrak{o}$ enthaltene Zahl bedeutet), wenn alle Koeffizienten x_0, x_1, $x_2 \cdots x_{n-1}$ durch p teilbar sind; denn setzt man

$$\begin{aligned}
h_1 &= c_1^0 x_0 + c_1' x_1 + c_1'' x_2 + \cdots + c_1^{(n-1)} x_{n-1}\\
h_2 &= c_2^0 x_0 + c_2' x_1 + c_2'' x_2 + \cdots + c_2^{(n-1)} x_{n-1}\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
h_n &= c_n^0 x_0 + c_n' x_1 + c_n'' x_2 + \cdots + c_n^{(n-1)} x_{n-1},
\end{aligned}$$

so ist

$$\omega' = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n,$$

und wenn ω' durch p teilbar sein soll, so muß (zufolge der Bedeutung von ω_1, $\omega_2 \cdots \omega_n$) jede der Koordinaten h_1, $h_2 \cdots h_n$ durch p teilbar sein; hieraus ergibt sich aber weiter, daß die Produkte $k\,x_0$, $k\,x_1$, $k\,x_2 \cdots k\,x_{n-1}$, und folglich auch die Koeffizienten x_0, x_1, $x_2 \cdots x_{n-1}$ sämtlich durch p teilbar sein müssen, wie behauptet war. Denselben Satz kann man offenbar auch so aussprechen: ist eine Zahl ω' der Ordnung $\mathfrak{o}'$ teilbar durch eine Primzahl p der ersten Art, so ist auch der Quotient ω'/p eine Zahl derselben Ordnung $\mathfrak{o}'$. Umgekehrt, wenn alle Koeffizienten x_0, x_1, $x_2 \cdots x_{n-1}$ durch p teilbar sind, so ist selbstverständlich auch ω' durch p teilbar. Es sind daher zwei Zahlen $\varphi_1(\theta)$ und $\varphi_2(\theta)$ der Ordnung $\mathfrak{o}'$ stets und nur dann einander kongruent nach dem Modul p, d. h. ihre Differenz $\varphi_1(\theta) - \varphi_2(\theta)$ ist teilbar durch p, wenn je zwei entsprechende Koeffizienten der beiden Funktionen $\varphi_1(t)$ und $\varphi_2(t)$ einander nach p kongruent sind, d. h. in der Bezeichnungsweise der Theorie der höheren Kongruenzen, wenn

$$\varphi_1(t) \equiv \varphi_2(t) \pmod{p}$$

*) Diese Bezeichnung der Hauptideale ist zweckmäßiger als diejenige $\mathfrak{i}(p)$, welche ich früher (D. § 163) gebraucht habe.

ist (C. 1). Hierbei war aber vorausgesetzt, daß die Grade der Funktionen $\varphi_1(t)$, $\varphi_2(t)$ kleiner als n waren; ist dies nicht der Fall, so erhält man durch Division mit $F(t)$ eine Identität von der Form

$$\varphi_1(t) - \varphi_2(t) = F(t)\,\psi(t) + \psi_1(t),$$

wo $\psi_1(t)$ von niedrigerem Grade als n ist, und hieraus $\varphi_1(\theta) - \varphi_2(\theta) = \psi_1(\theta)$; soll nun

$$\varphi_1(\theta) \equiv \varphi_2(\theta) \pmod{p}$$

sein, so muß nach dem obigen $\psi_1(t) = p\,\psi_2(t)$, also

$$\varphi_1(t) - \varphi_2(t) = F(t)\,\psi(t) + p\,\psi_2(t)$$

sein; das Stattfinden einer solchen Identität bezeichnet man aber in der Theorie der höheren Kongruenzen durch

$$\varphi_1(t) - \varphi_2(t) \equiv F(t)\,\psi(t) \pmod{p}$$

oder noch kürzer (C. 7) durch

$$\varphi_1(t) \equiv \varphi_2(t) \quad (\text{modd. } p, F(t)).$$

Umgekehrt leuchtet ein, daß aus dieser letzten Funktionenkongruenz auch wieder die Zahlenkongruenz

$$\varphi_1(\theta) \equiv \varphi_2(\theta) \pmod{p}$$

folgt; beide Kongruenzen sind daher gleichbedeutend. Mithin gibt es in $\mathfrak{o}'$ genau ebenso viele nach p inkongruente Zahlen $\varphi(\theta)$, als es inkongruente Funktionen $\varphi(t)$ in bezug auf den Doppelmodul p, $F(t)$ gibt; da nun die Anzahl der letzteren $= p^n$ ist (C. 8), und da die Anzahl $(\mathfrak{o}, \mathfrak{o}\,p) = N(p)$ aller in $\mathfrak{o}$ enthaltenen, nach p inkongruenten Zahlen genau ebenso groß ist (B. § 18; D. § 162), so ergibt sich das wichtige Resultat: jede Zahl ω des Gebietes $\mathfrak{o}$ ist mit einer Zahl $\omega' = \varphi(\theta)$ der Ordnung $\mathfrak{o}'$ kongruent nach dem Modul p.

Zu derselben Folgerung gelangt man unmittelbar auch durch folgende einfache Betrachtung. Aus den n Relationen zwischen den Zahlen 1, θ, $\theta^2 \cdots \theta^{n-1}$ einerseits und den Zahlen ω_1, $\omega_2 \cdots \omega_n$ andererseits geht hervor, daß die Produkte $k\,\omega_1$, $k\,\omega_2 \cdots k\,\omega_n$ und folglich auch alle Produkte von der Form $k\,\omega$, wo ω jede beliebige Zahl in $\mathfrak{o}$ bedeutet, in der Ordnung $\mathfrak{o}'$ enthalten sind; man kann daher $k\,\omega = \varphi(\theta)$ setzen. Da nun k durch die Primzahl p nicht teilbar ist, so kann man die ganze rationale Zahl l so wählen, daß $k\,l \equiv 1 \pmod{p}$ wird, und hieraus folgt $\omega \equiv l\,k\,\omega \equiv l\,\varphi(\theta) \pmod{p}$; also ist ω wirklich mit einer Zahl $l\,\varphi(\theta)$ der Ordnung $\mathfrak{o}'$ kongruent nach dem Modul p.

Ganz anders verhält es sich dagegen, wenn p eine Primzahl der zweiten Art ist; da in diesem Falle die Determinante k durch p teilbar ist, so kann man nach einem Satze, dessen sehr leichten Beweis ich hier wohl übergehen darf, n ganze rationale Zahlen x_0, $x_1 \cdots x_{n-1}$, die nicht alle durch p teilbar sind, so wählen, daß die oben mit h_1, $h_2 \cdots h_n$ bezeichneten Summen sämtlich durch p teilbar werden; dann ist die entsprechende Zahl

$$\omega' = x_0 + x_1\theta + x_2\theta^2 + \cdots + x_{n-1}\theta^{n-1}$$

der Ordnung $\mathfrak{o}'$ wirklich teilbar durch p, obgleich ihre Koeffizienten x_0, $x_1 \cdots x_{n-1}$ nicht alle durch p teilbar sind. Hieraus folgt sofort, daß die Anzahl $(\mathfrak{o}', \mathfrak{o}p)$ der in $\mathfrak{o}'$ enthaltenen, nach p inkongruenten Zahlen kleiner als p^n ist, und folglich gibt es in $\mathfrak{o}$ Zahlen ω, welche mit keiner in $\mathfrak{o}'$ enthaltenen Zahl $\varphi(\theta)$ nach p kongruent sind, d. h. es gibt Zahlklassen (mod. p) in $\mathfrak{o}$, für welche in $\mathfrak{o}'$ kein Repräsentant vorhanden ist. Die genaue Bestimmung der Anzahl $(\mathfrak{o}', \mathfrak{o}p)$ ist für unseren Hauptzweck nicht erforderlich [*)].

§ 2.

In diesem Paragraphen machen wir durchweg die Voraussetzung, daß p eine Primzahl der ersten Art ist, und wir wollen beweisen, daß in diesem Falle die Theorie der höheren Kongruenzen ein einfaches Mittel gibt, um das Hauptideal $\mathfrak{o}p$ in seine Primfaktoren zu zerlegen. Dies geschieht dadurch, daß die Funktion $F(t)$, die wir kürzer auch durch F bezeichnen werden, nach dem Modul p als Produkt von lauter Primfunktionen $P(t)$ dargestellt wird (C. 6); der bequemeren Ausdrucksweise halber wollen wir, was erlaubt ist, jede Primfunktion P so wählen, daß ihr höchster Koeffizient $= 1$ ist, woraus folgt, daß zwei inkongruente Primfunktionen auch immer relative Primfunktionen sein werden (C. 5). Durch Vereinigung aller einander kongruenten Faktoren in eine Potenz erhält man

$$F \equiv P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} \pmod{p},$$

wo P_1, $P_2 \cdots P_m$ die sämtlichen inkongruenten, in F aufgehenden Primfunktionen bedeuten.

[*) Schon bei Zolotareff (Mélanges math. et astron. du Bulletin de l'academie, St. Petersburg, Bd. 5, 13./25. September 1877) findet man den Satz, daß die Ausnahmeprimzahlen eben diejenigen sind, wofür eine durch p teilbare Zahl ω' in der Ordnung $\mathfrak{o}'$ vorkommt, worin nicht alle Koeffizienten durch p teilbar sind. Zolotareff zeigt aber nicht, daß diese Primzahlen eben die Indexteiler sind.]

Ist nun P eine beliebige dieser m Primfunktionen, und $\varrho = P(\theta)$, so entspricht derselben ein bestimmtes Ideal $\mathfrak{p}$, welches wir als den größten gemeinschaftlichen Teiler der beiden Hauptideale $\mathfrak{o}p$ und $\mathfrak{o}\varrho$ definieren. Um die Eigenschaften dieses Ideals $\mathfrak{p}$ festzustellen, betrachten wir zunächst alle diejenigen in der Ordnung $\mathfrak{o}'$ enthaltenen Zahlen $\psi(\theta)$, welche durch $\mathfrak{p}$ teilbar (d. h. in $\mathfrak{p}$ enthalten) sind, und wir wollen beweisen, daß die Zahlenkongruenz

(1) $$\psi(\theta) \equiv 0 \pmod{\mathfrak{p}}$$

völlig gleichbedeutend ist mit der Funktionenkongruenz

(2) $$\psi(t) \equiv 0 \pmod{p, P}.$$

In der Tat, da das Ideal $\mathfrak{p}$ zufolge seiner Definition (D. § 163; B. § 19) der Inbegriff aller Zahlen von der Form

$$\varrho\alpha + p\beta$$

ist, wo α, β willkürliche Zahlen des Gebiets $\mathfrak{o}$ bedeuten, und da (nach § 1) jede Zahl α mit einer Zahl $\varphi(\theta)$ der Ordnung $\mathfrak{o}'$ kongruent ist nach dem Modul p, so folgt aus (1) eine Kongruenz von der Form

$$\psi(\theta) \equiv P(\theta)\,\varphi(\theta) \pmod{p};$$

hieraus ergibt sich aber (nach § 1) die Funktionenkongruenz

$$\psi(t) \equiv P(t)\,\varphi(t) \pmod{p, F},$$

also auch die Kongruenz (2), weil F durch P teilbar ist. Umgekehrt folgt aus (2) unmittelbar, daß $\psi(\theta)$ von der Form $\varrho\alpha + p\beta$, also $\equiv 0 \pmod{\mathfrak{p}}$ sein muß, womit die obige Behauptung bewiesen ist.

Mit Hilfe dieses Resultats kann man leicht die Norm des Ideals $\mathfrak{p}$, d. h. die Anzahl $(\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p})$ der in $\mathfrak{o}$ enthaltenen, nach $\mathfrak{p}$ inkongruenten Zahlen bestimmen. Sind nämlich α_1, α_2 zwei beliebige Zahlen in $\mathfrak{o}$, so gibt es (nach § 1) in $\mathfrak{o}'$ zwei Zahlen $\varphi_1(\theta)$, $\varphi_2(\theta)$, welche resp. den Zahlen α_1, α_2 nach p kongruent sind, und da p durch $\mathfrak{p}$ teilbar ist, so ist auch

$$\alpha_1 \equiv \varphi_1(\theta), \quad \alpha_2 \equiv \varphi_2(\theta) \pmod{\mathfrak{p}};$$

die beiden Zahlen α_1, α_2 sind daher stets und nur dann kongruent in bezug auf $\mathfrak{p}$, wenn

$$\varphi_1(\theta) \equiv \varphi_2(\theta) \pmod{\mathfrak{p}}$$

ist; diese Kongruenz ist aber nach dem obigen gleichbedeutend mit der Kongruenz

$$\varphi_1(t) \equiv \varphi_2(t) \pmod{p, P};$$

es gibt daher in $\mathfrak{o}$ genau ebenso viele inkongruente Zahlen α in bezug auf $\mathfrak{p}$, als es inkongruente Funktionen $\varphi(t)$ in bezug auf den Doppel-

modul p, P gibt, und da die Anzahl der letzteren $= p^f$ ist, wo f den Grad der Funktion P bedeutet (C. 8), so erhalten wir

$$N(\mathfrak{p}) = p^f.$$

Ebenso leicht ergibt sich, daß $\mathfrak{p}$ ein Primideal ist. Da nämlich $f \geqq 1$, also $N(\mathfrak{p}) > 1$ ist, so ist $\mathfrak{p}$ jedenfalls von $\mathfrak{o}$ verschieden, und es braucht daher nur noch gezeigt zu werden, daß $\mathfrak{p}$ kein zusammengesetztes Ideal, d. h. kein Produkt von der Form $\mathfrak{a}_1 \mathfrak{a}_2$ ist, wo die Ideale $\mathfrak{a}_1$, $\mathfrak{a}_2$ beide von $\mathfrak{o}$ verschieden sind (D. § 163; B. § 25, 4°). Ein solches zusammengesetztes Ideal $\mathfrak{m} = \mathfrak{a}_1 \mathfrak{a}_2$ besitzt die charakteristische Eigenschaft, daß immer zwei durch $\mathfrak{m}$ nicht teilbare Zahlen α_1, α_2 existieren, deren Produkt $\alpha_1 \alpha_2$ durch $\mathfrak{m}$ teilbar ist; denn weil die Ideale $\mathfrak{a}_1$, $\mathfrak{a}_2$ beide von $\mathfrak{o}$ verschieden sind, so kann auch keines von ihnen durch ihr Produkt $\mathfrak{m} = \mathfrak{a}_1 \mathfrak{a}_2$ teilbar sein, und folglich gibt es eine durch $\mathfrak{a}_1$, aber nicht durch $\mathfrak{m}$ teilbare Zahl α_1, und ebenso eine durch $\mathfrak{a}_2$, aber nicht durch $\mathfrak{m}$ teilbare Zahl α_2, und offenbar ist $\alpha_1 \alpha_2$ teilbar durch $\mathfrak{m}$. Es wird daher $\mathfrak{p}$ gewiß ein Primideal sein, wenn wir beweisen können, daß ein Produkt $\alpha_1 \alpha_2$ nur dann durch $\mathfrak{p}$ teilbar ist, wenn wenigstens einer der Faktoren α_1, α_2 durch $\mathfrak{p}$ teilbar ist. Zu diesem Zweck setzen wir, wie oben,

$$\alpha_1 \equiv \varphi_1(\theta), \quad \alpha_2 \equiv \varphi_2(\theta) \pmod{\mathfrak{p}},$$

so ist

$$\alpha_1 \alpha_2 \equiv \varphi_1(\theta)\, \varphi_2(\theta) \pmod{\mathfrak{p}};$$

soll nun $\alpha_1 \alpha_2 \equiv 0 \pmod{\mathfrak{p}}$ sein, so muß auch

$$\varphi_1(\theta)\, \varphi_2(\theta) \equiv 0 \pmod{\mathfrak{p}},$$

mithin

$$\varphi_1(t)\, \varphi_2(t) \equiv 0 \pmod{p, P}$$

sein; da aber P eine Primfunktion ist, so muß wenigstens eine der beiden Kongruenzen

$$\varphi_1(t) \equiv 0, \quad \varphi_2(t) \equiv 0 \pmod{p, P}$$

stattfinden (C. 6), also auch wenigstens eine der Kongruenzen

$$\varphi_1(\theta) \equiv 0, \quad \varphi_2(\theta) \equiv 0 \pmod{\mathfrak{p}},$$

d. h. wenigstens eine der beiden Zahlen α_1, α_2 muß $\equiv 0 \pmod{\mathfrak{p}}$ sein. Also ist $\mathfrak{p}$ ein Primideal; und zwar sagen wir (B. § 21), daß $\mathfrak{p}$ ein Primideal vom Grade f ist, weil $N(\mathfrak{p}) = p^f$ ist.

Jetzt wollen wir beweisen, daß der Exponent e der höchsten in F aufgehenden Potenz von P zugleich der Exponent der höchsten in p aufgehenden Potenz des Primideals $\mathfrak{p}$ ist. In der Tat, wenn F nach dem Modul p durch P^e, aber nicht durch P^{e+1} teilbar ist, so kann man

$$F \equiv S P^e \pmod{p}$$

setzen, wo S nicht teilbar durch P ist, woraus nach dem Obigen folgt, daß die Zahl

$$\sigma = S(\theta)$$

nicht durch $\mathfrak{p}$ teilbar ist. Da ferner $\mathfrak{p}$ der größte gemeinschaftliche Teiler der beiden Ideale $\mathfrak{o}\, p$ und $\mathfrak{o}\, \varrho$ ist, so können wir

$$\mathfrak{o}\, p = \mathfrak{p}\, \mathfrak{a}, \quad \mathfrak{o}\, \varrho = \mathfrak{p}\, \mathfrak{b}$$

setzen, wo $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale bedeuten, und wir haben zu beweisen, daß $\mathfrak{p}^{e-1}$ die höchste in $\mathfrak{a}$ aufgehende Potenz von $\mathfrak{p}$ ist. Zu diesem Zwecke betrachten wir die Zahl

$$\eta = \sigma\, \varrho^{e-1} = S(\theta)\, P(\theta)^{e-1};$$

dieselbe kann nicht durch p teilbar sein, weil der Grad der Funktion $S P^{e-1}$ kleiner als n, und weil ihr höchster Koeffizient $= 1$ ist; aber η ist teilbar durch $\mathfrak{p}^{e-1}$, weil ϱ durch $\mathfrak{p}$ teilbar ist. Vermöge der Kongruenz $F \equiv S P^e \pmod{p}$ ist nun das Produkt $\eta\, \varrho = \sigma\, \varrho^e$ teilbar durch p, also ist auch das Ideal $\eta\, \mathfrak{p}\, \mathfrak{b}$ teilbar durch $\mathfrak{p}\, \mathfrak{a}$, mithin $\eta\, \mathfrak{b}$ teilbar durch $\mathfrak{a}$, folglich η teilbar durch $\mathfrak{a}$, weil $\mathfrak{a}$ und $\mathfrak{b}$ relative Primideale sind. Man kann daher

$$\mathfrak{o}\, \eta = \mathfrak{a}\, \mathfrak{c}$$

setzen, wo $\mathfrak{c}$ ein Ideal bedeutet, welches nicht durch $\mathfrak{p}$ teilbar ist*), weil sonst η durch $\mathfrak{a}\, \mathfrak{p}$, also durch p teilbar wäre, was nicht der Fall ist. Da nun η durch $\mathfrak{p}^{e-1}$ teilbar ist, so muß auch $\mathfrak{a}$ durch $\mathfrak{p}^{e-1}$ teilbar sein. Wir haben jetzt nur noch zu zeigen, daß $\mathfrak{a}$ nicht durch $\mathfrak{p}^e$ teilbar ist. Da $e \geqq 1$ ist, so müßte, wenn $\mathfrak{a}$ durch $\mathfrak{p}^e$ teilbar wäre, jedenfalls $\mathfrak{a}$ durch $\mathfrak{p}$ selbst teilbar sein; sobald aber $\mathfrak{a}$ durch $\mathfrak{p}$ teilbar ist, kann $\mathfrak{b}$ nicht durch $\mathfrak{p}$ teilbar sein, und folglich ist dann ϱ nicht teilbar durch $\mathfrak{p}^2$; da ferner σ nicht durch $\mathfrak{p}$ teilbar ist, so ist in diesem Falle $\mathfrak{p}^{e-1}$ die höchste in der Zahl $\eta = \sigma\, \varrho^{e-1}$ aufgehende Potenz von $\mathfrak{p}$, und folglich kann das in η aufgehende Ideal $\mathfrak{a}$ nicht durch $\mathfrak{p}^e$ teilbar sein, w. z. b. w.

Nachdem die Untersuchung für eine bestimmte in F aufgehende Primfunktion P und für das ihr entsprechende Primideal $\mathfrak{p}$ so weit geführt ist, wenden wir dieselbe auf alle in der Funktion

$$F \equiv P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} \pmod{p}$$

*) Es ist daher $\mathfrak{a}$ der größte gemeinschaftliche Teiler, und folglich $\eta\, \mathfrak{p}$ das kleinste gemeinschaftliche Vielfache der beiden Ideale $\mathfrak{o}\, p$ und $\mathfrak{o}\, \eta$, d. h. $\mathfrak{p}$ ist der Inbegriff aller Wurzeln π der Kongruenz $\eta\, \pi \equiv 0 \pmod{p}$. Dies hätte auch als Definition des Ideals $\mathfrak{p}$ benutzt werden können.

aufgehenden, inkongruenten Primfunktionen

$$P_1,\ P_2 \cdots P_m$$

an, deren Grade wir resp. mit

$$f_1,\ f_2 \cdots f_m$$

bezeichnen; die diesen Funktionen entsprechenden Primideale

$$\mathfrak{p}_1,\ \mathfrak{p}_2 \cdots \mathfrak{p}_m$$

haben resp. dieselben Grade, d. h. es ist

$$N(\mathfrak{p}_1) = p^{f_1},\quad N(\mathfrak{p}_2) = p^{f_2} \cdots N(\mathfrak{p}_m) = p^{f_m},$$

und

$$\mathfrak{p}^{e_1},\ \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}$$

sind die höchsten in p aufgehenden Potenzen dieser Ideale. Diese m Primideale sind verschieden voneinander; denn da z. B. P_2 nicht durch P_1 teilbar ist (mod. p), so ist die durch $\mathfrak{p}_2$ teilbare Zahl $P_2(\theta)$ nicht durch $\mathfrak{p}_1$ teilbar, und folglich sind $\mathfrak{p}_1$, $\mathfrak{p}_2$ verschiedene Primideale. Endlich bemerken wir, daß p durch kein anderes Primideal teilbar sein kann; da nämlich

$$P_1(\theta)^{e_1} P_2(\theta)^{e_2} \cdots P_m(\theta)^{e_m} \equiv 0 \pmod{p}$$

ist, so muß ein in p aufgehendes Primideal auch in einer der m Zahlen $\varrho = P(\theta)$ aufgehen und folglich mit dem Primideal $\mathfrak{p}$ identisch sein, welches der größte gemeinschaftliche Teiler der beiden Ideale $\mathfrak{o}\,p$ und $\mathfrak{o}\,\varrho$ ist.

Aus allen diesem folgt (D. § 163; B. § 25), daß

$$\mathfrak{o}\,p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}$$

ist, und eine Bestätigung dieses Resultats ergibt sich durch die Betrachtung der Normen, wenn man berücksichtigt, daß

$$n = e_1 f_1 + e_2 f_2 + \cdots + e_m f_m$$

ist. Es ist somit folgender Satz bewiesen, den ich zuerst in den Göttingischen gelehrten Anzeigen vom 20. September 1871 ohne Beweis mitgeteilt habe:

I. Ist der Index k der Zahl θ, welche der irreduktiblen Gleichung n^{ten} Grades $F(\theta) = 0$ genügt, nicht teilbar durch die Primzahl p, und ist

$$F \equiv P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} \pmod{p},$$

wo $P_1,\ P_2 \cdots P_m$ inkongruente Primfunktionen resp. vom Grade $f_1,\ f_2 \cdots f_m$ bedeuten, so ist

$$\mathfrak{o}\,p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m},$$

wo $\mathfrak{p}_1,\ \mathfrak{p}_2 \cdots \mathfrak{p}_m$ voneinander verschiedene Primideale resp. vom Grade $f_1,\ f_2 \cdots f_m$ sind, und zwar entspricht je einer Primfunktion P ein bestimmtes Primideal $\mathfrak{p}$ in der Weise, daß $\mathfrak{p}$ der größte gemeinschaftliche Teiler der beiden Ideale $\mathfrak{o}\,p$ und $\mathfrak{o}\,P(\theta)$ ist.

§ 3.

Aus diesem Satze geht hervor, daß man bei Zugrundelegung einer bestimmten ganzen Zahl θ des Körpers Ω, welche zur Darstellung von unendlich vielen ganzen Zahlen $\varphi(\theta)$ dient, mit voller Sicherheit die Zerlegung aller derjenigen Primzahlen p findet, welche nicht in dem Index k dieser Zahl θ aufgehen; es ist daher von großer Wichtigkeit zu wissen, ob eine Primzahl p in dem Index k aufgeht oder nicht. Sobald freilich eine Basis $\omega_1,\ \omega_2 \cdots \omega_n$ des Gebiets $\mathfrak{o}$, oder auch nur die Grundzahl D des Körpers Ω bekannt ist, erledigt sich diese Frage sehr leicht, weil hieraus k direkt gefunden werden kann; denn aus den Koeffizienten der Gleichung $F(\theta) = 0$ läßt sich ihre Diskriminante

$$\Delta(1,\ \theta,\ \theta^2 \cdots \theta^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N(F'(\theta)) = D\,k^2,$$

und hieraus durch Division mit D das Quadrat des Index k bestimmen. Bei den meisten Untersuchungen liegt aber die Sache ganz anders, nämlich so, daß nur die Gleichung $F(\theta) = 0$, nicht aber die Grundzahl D des ihr entsprechenden Körpers Ω gegeben ist; es kommt darauf an zu entscheiden, ob eine bestimmte Primzahl p in dem noch unbekannten Index k der Zahl θ aufgeht oder nicht. Dies gelingt nun in der Tat, wie wir jetzt zeigen wollen, mit Hilfe der Theorie der höheren Kongruenzen, und zwar hängt die Entscheidung, wenn wir die früheren Bezeichnungen beibehalten, wesentlich von der Beschaffenheit der Funktion M ab, welche in der Identität

$$F = P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} - p\,M$$

auftritt. Dies ergibt sich aus den beiden folgenden Sätzen.

II. Ist der Index k der Zahl θ nicht teilbar durch p, so kann M nach dem Modul p durch keine Primfunktion P teilbar sein, deren Quadrat in F aufgeht.

Zum Beweise dürfen wir alle Folgerungen benutzen, welche im vorigen Paragraphen aus der Annahme gezogen sind, daß k nicht

durch p teilbar ist. Indem wir alle dort gebrauchten Bezeichnungen beibehalten, setzen wir $F \equiv S P^e \pmod{p}$, also

$$F = S P^e - p M,$$

und nehmen an, es sei $e \geqq 2$; dann ist p teilbar durch $\mathfrak{p}^2$, folglich $\mathfrak{a}$ teilbar durch $\mathfrak{p}$, mithin $\mathfrak{b}$ nicht teilbar durch $\mathfrak{p}$. Es ist daher $\mathfrak{p}^e$ die höchste in der Zahl

$$S(\theta)\, P(\theta)^e = p M(\theta)$$

aufgehende Potenz von $\mathfrak{p}$, und da p durch $\mathfrak{p}^e$ teilbar ist, so kann $M(\theta)$ nicht durch $\mathfrak{p}$ teilbar sein, und folglich kann die Funktion M auch nicht $\equiv 0 \pmod{p, P}$ sein, w. z. b. w.

Auch ohne Benutzung der im vorigen Paragraphen gewonnenen Resultate läßt sich derselbe Satz leicht in der folgenden indirekten, aber vollständig äquivalenten Form beweisen:

Ist F nach dem Modul p teilbar durch das Quadrat einer Primfunktion P, also

$$F = S P^e - p M,$$

wo $e \geqq 2$, und ist M teilbar durch P, so muß der Index k der Zahl θ durch die Primzahl p teilbar sein.

Behalten die Buchstaben ϱ, σ, η dieselbe Bedeutung, wie im vorigen Paragraphen, setzen wir also

$$\varrho = P(\theta), \quad \sigma = S(\theta), \quad \eta = \sigma \varrho^{e-1},$$

so wird (nach § 1) der Beweis unseres Satzes geführt sein, wenn wir zeigen, daß unter den jetzigen Annahmen die Zahl $\eta = S(\theta)\, P(\theta)^{e-1}$ durch p teilbar sein muß; denn die Funktion $S P^{e-1}$ ist von niedrigerem Grade als n und auch nicht $\equiv 0 \pmod{p}$. Die Zahl η wird ferner gewiß durch p teilbar sein, wenn bewiesen wird, daß alle in p aufgehenden Potenzen von Primidealen auch in η aufgehen (D. § 163, B. § 25). Zu diesem Zweck setzen wir

$$\mu = M(\theta)$$

und betrachten die Gleichung

$$\sigma \varrho^e = \eta \varrho = p \mu.$$

Ist nun $\mathfrak{p}$ ein in p, aber nicht in ϱ aufgehendes Primideal, so folgt aus $\eta \varrho = p \mu$ unmittelbar, daß η durch die höchste in p aufgehende Potenz von $\mathfrak{p}$ teilbar ist. Ist aber $\mathfrak{p}$ ein in p und gleichzeitig in ϱ aufgehendes Primideal, so ergibt sich folgendes. Da S und P relative

Primfunktionen sind, so existieren zwei Funktionen U, V, welche der Kongruenz

$$S U + P V \equiv 1 \pmod{p}$$

genügen (C. 4); hieraus ergeben sich die Zahlenkongruenzen

$$\sigma U(\theta) + \varrho V(\theta) \equiv 1 \pmod{p}$$
$$\sigma U(\theta) \equiv 1 \pmod{\mathfrak{p}},$$

und folglich ist σ nicht teilbar durch $\mathfrak{p}$. Sind daher $\mathfrak{p}^h$, $\mathfrak{p}^r$, $\mathfrak{p}^m$ die höchsten resp. in p, ϱ, μ aufgehenden Potenzen von $\mathfrak{p}$, so folgt aus $\sigma \varrho^e = p \mu$ und $\eta = \sigma \varrho^{e-1}$, daß

$$e r = h + m,$$

und daß der Exponent der höchsten in η aufgehenden Potenz von $\mathfrak{p}$ gleich

$$(e-1) r = h + m - r$$

ist; um daher wieder zu beweisen, daß η durch $\mathfrak{p}^h$ teilbar ist, brauchen wir nur noch zu zeigen, daß

$$m \geqq r$$

ist. Hierbei unterscheiden wir zwei Fälle. Ist erstens $r \geqq h$, so verwerten wir die erste Annahme unseres Satzes, derzufolge $e \geqq 2$ ist; hieraus folgt in der Tat $h + m = e r \geqq 2 r$, mithin $m - r \geqq r - h \geqq 0$, wie behauptet war. Ist aber zweitens $r \leqq h$, so benutzen wir die zweite Annahme unseres Satzes, derzufolge $M \equiv 0 \pmod{p, P}$, d. h. $M \equiv P T \pmod{p}$, also $\mu \equiv \varrho T(\theta) \pmod{p}$ ist; da nun sowohl ϱ, als auch p durch $\mathfrak{p}^r$ teilbar ist, so folgt aus dieser Kongruenz, daß auch μ durch $\mathfrak{p}^r$ teilbar, d. h. daß $m \geqq r$ ist, w. z. b. w.

Nachdem der Satz II auf zwei verschiedene Arten bewiesen ist, behaupten wir auch die Richtigkeit des umgekehrten Satzes:

III. Ist M durch keine solche Primfunktion P teilbar (mod. p), deren Quadrat zugleich in F aufgeht, so ist der Index k der Zahl θ nicht teilbar durch p.

Derselbe Satz kann offenbar auch in der folgenden Form ausgesprochen werden:

Ist der Index k der Zahl θ teilbar durch die Primzahl p, so gibt es eine in M aufgehende Primfunktion P, deren Quadrat zugleich in F aufgeht (mod. p).

Dem Beweise legen wir die letztere Form zugrunde, weil die Annahme, daß k durch p teilbar ist, eine leichtere Verwertung gestattet, insofern aus ihr (nach § 1) die Existenz einer durch p teilbaren Zahl

$$\varphi(\theta) = x_0 + x_1 \theta + x_2 \theta^2 + \cdots + x_{n-1} \theta^{n-1}$$

folgt, deren Koeffizienten $x_0, x_1, x_2 \cdots x_{n-1}$ nicht alle durch p teilbar sind. Bezeichnet man nun mit A den größten gemeinschaftlichen Teiler der beiden Funktionen $\varphi(t)$ und F nach dem Modul p, so ist der Grad von A kleiner als n, weil φ von niedrigerem Grade als n und auch nicht $\equiv 0 \pmod{p}$ ist; setzt man daher

$$F = AB - pM,$$

so ist B keine Konstante. Nun existieren zwei Funktionen φ_1, φ_2, welche der Kongruenz

$$\varphi(t)\,\varphi_1(t) + F(t)\,\varphi_2(t) \equiv A(t) \pmod{p}$$

genügen (C. 4); hieraus ergibt sich, daß die Zahl $A(\theta)$ ebenfalls durch p teilbar ist*) und folglich einer Gleichung von der Form

$$A(\theta)^s + p h_1 A(\theta)^{s-1} + p^2 h_2 A(\theta)^{s-2} + \cdots + p^s h_s = 0$$

genügt, wo $h_1, h_2 \cdots h_s$ ganze rationale Zahlen bedeuten (D. § 160; B. § 13). Da die Gleichung $F(\theta) = 0$ irreduktibel ist, so ergibt sich hieraus eine in bezug auf die Variable t identische Gleichung von der Form

$$A^s + p h_1 A^{s-1} + p^2 h_2 A^{s-2} + \cdots + p^s h_s = FG,$$

also auch die Kongruenz

$$A^s \equiv 0 \pmod{p, F};$$

mithin muß die Funktion A durch jede in F aufgehende Primfunktion nach dem Modul p teilbar sein (C. 5 und 6). Multipliziert man ferner die obige Gleichung, welcher die Zahl $A(\theta)$ genügt, mit $B(\theta)^s$, und bedenkt, daß $A(\theta)\,B(\theta) = pM(\theta)$ ist, so erhält man

$$M(\theta)^s + h_1 M(\theta)^{s-1} B(\theta) + h_2 M(\theta)^{s-2} B(\theta)^2 + \cdots + h_s B(\theta)^s = 0,$$

und hieraus eine Identität von der Form

$$M^s + h_1 M^{s-1} B + h_2 M^{s-2} B^2 + \cdots + h_s B^s = FH;$$

da nun $F \equiv 0 \pmod{p, B}$, so ergibt sich

$$M^s \equiv 0 \pmod{p, B},$$

und folglich ist die Funktion M durch jede in B aufgehende Primfunktion teilbar nach dem Modul p. Oben ist aber gezeigt, daß B keine Konstante ist, mithin gibt es wenigstens eine in B aufgehende

*) In ähnlicher Weise kann man leicht zeigen, daß das Kriterium für die Teilbarkeit einer Zahl $\varphi(\theta)$ durch p in der Kongruenz $\varphi(t) \equiv 0 \pmod{p, K}$ besteht, wo K einen völlig bestimmten Teiler der Funktion F nach dem Modul p bedeutet.

Primfunktion P, und diese muß folglich auch in M aufgehen. Da ferner P in F aufgeht, weil F durch B teilbar ist, und da oben gezeigt ist, daß jede in F aufgehende Primfunktion auch in A aufgeht, so geht P ebenfalls in A auf, und folglich ist F teilbar durch P^2, weil $F \equiv AB \pmod{p}$ ist. Wir haben mithin wirklich gezeigt, daß es eine in M aufgehende Primfunktion P gibt, deren Quadrat zugleich in F aufgeht, w. z. b. w.

Durch die Sätze II und III ist nun in der Tat die Entscheidung der Frage, ob der Index k der Zahl θ durch die Primzahl p teilbar ist, vollständig zurückgeführt auf die Zerlegung

$$F = P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} - pM,$$

durch welche die Funktion F als Produkt von lauter Primfunktionen nach dem Modul p dargestellt wird. Zeigt es sich, daß F durch kein Quadrat einer Primfunktion teilbar ist, daß also alle Exponenten $e_1, e_2 \cdots e_m = 1$ sind*), oder zeigt es sich, daß keine derjenigen Primfunktionen, deren Quadrate in F aufgehen, in M aufgeht, so ist k nicht durch p teilbar, und es gilt der Satz I des § 2. Gibt es aber eine in M aufgehende Primfunktion, deren Quadrat zugleich in F aufgeht, so ist k teilbar durch p, und aus dem zweiten Beweise des Satzes II geht leicht hervor, daß dann die Zerlegung des Ideals $\mathfrak{o}\,p$ in Primfaktoren eine andere ist, als die im Satz I behauptete.

Diesem Resultat fügen wir noch folgende Bemerkung hinzu. Sind die Funktionen $R_1, R_2 \cdots R_m$ resp. kongruent den Funktionen $P_1, P_2 \cdots P_m$, so sind sie ebenfalls Primfunktionen, und es wird

$$F = R_1^{e_1} R_2^{e_2} \cdots R_m^{e_m} - pN,$$

wo die Funktion N durchaus nicht $\equiv M \pmod{p}$ zu sein braucht. Da aber die Teilbarkeit des Index k der Zahl θ durch p von dieser Auswahl der Primfunktionen gänzlich unabhängig ist, so muß man schließen, daß die Eigenschaft der Funktion M, welche für diese Frage allein entscheidend ist, auch für jede Funktion N bestehen bleibt. Dies ließe sich leicht durch die Rechnung unmittelbar bestätigen; bezeichnet man mit Q das Produkt aller derjenigen in F aufgehenden Primfunktionen, deren Quadrate in F nicht aufgehen, so kann man durch geeignete Wahl der Funktionen $R_1, R_2 \cdots R_m$ stets zu einer Funktion N gelangen, die relative Primfunktion zu Q

*) Dies wird stets und nur dann der Fall sein, wenn die Diskriminante $\Delta(1, \theta, \theta^2 \cdots \theta^{n-1})$ der Gleichung $F(\theta) = 0$ nicht durch p teilbar ist.

ist; aber sobald M durch eine Primfunktion P teilbar ist, deren Quadrat in F aufgeht, so zeigt die Rechnung, daß auch jede Funktion N durch P teilbar ist*).

§ 4.

In den zuerst von Kummer behandelten Zahlengebieten $\mathfrak{o}$, welche aus einer primitiven Wurzel θ der Gleichung $\theta^m = 1$ entspringen, tritt der glückliche Umstand auf, daß die Potenzen $1, \theta, \theta^2 \cdots \theta^{n-1}$, wo $n = \varphi(m)$, eine Basis des Gebietes $\mathfrak{o}$ bilden, und daß folglich der Index k der Zahl θ, welche der ganzen Untersuchung zugrunde gelegt wird, stets $= 1$ ist. Bei der allgemeinen Untersuchung eines beliebigen endlichen Körpers Ω und des Gebietes $\mathfrak{o}$, welches aus allen in Ω enthaltenen ganzen Zahlen besteht, erkannte ich zwar sehr bald, daß derselbe einfache Fall nur ausnahmeweise auftritt, aber ich hielt es doch lange Zeit für sehr wahrscheinlich, daß für jede gegebene Primzahl p sich eine ganze Zahl θ des Körpers Ω würde finden lassen, deren Index nicht durch p teilbar wäre, und mit deren Hilfe es folglich gelingen würde, die Bestimmung der Idealfaktoren von p auf die Theorie der höheren Kongruenzen zurückzuführen. Da aber alle meine Versuche, die Existenz einer solchen Zahl θ nachzuweisen, fruchtlos blieben, so entschloß ich mich endlich, wo möglich die Unrichtigkeit dieser Vermutung darzutun, und zu diesem Ziele gelangte ich, wie ich schon in den Göttingischen gelehrten Anzeigen vom 20. September 1871 angedeutet

*) Hiernach beschränkt sich die Idealtheorie von Zolotareff auf den Fall, daß der Index k nicht durch p teilbar ist. Dies scheint wenigstens aus folgenden Worten hervorzugehen, welche sich in der oben erwähnten Anzeige finden (Jahrbuch über die Fortschritte der Mathematik, Bd. 6): „Um die Theorie in ihrer einfachsten Gestalt darzustellen, nimmt der Verfasser an, daß $F_1(x)$ durch keine der Funktionen V, V_1, $V_2 \cdots$ teilbar ist. Ist diese Bedingung nicht erfüllt, so kann man für einen gegebenen Modul p die Gleichung $F(x) = 0$ derart transformieren, daß jene Annahme erfüllt ist. Die Auseinandersetzung jener Transformation behält sich der Verfasser für eine andere Gelegenheit vor.“ — Da es nach meinen Untersuchungen (vgl. § 5 dieser Abhandlung) Körper gibt, in welchen die Indizes aller ganzen Zahlen θ durch dieselbe Primzahl p teilbar sind, und folglich auch alle Gleichungen $F(\theta) = 0$ diejenige störende Eigenschaft besitzen, welche sich der unmittelbaren Anwendung der Theorie von Zolotareff widersetzt, so vermute ich, daß in den eben zitierten Worten der Anzeige ein Mißverständnis obwaltet. Wahrscheinlich wird die von dem Verfasser beabsichtigte Vervollständigung seiner Theorie sich auf ähnliche Betrachtungen stützen, wie diejenigen, welche in der Theorie der idealen Zahlen von Selling entwickelt sind (Schlömilchs Zeitschrift, Bd. 10, S. 12ff.).

habe, durch die Betrachtungen, welche den Gegenstand dieses und des folgenden Paragraphen bilden.

Es sei p eine bestimmte Primzahl, und $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ seien die sämtlichen voneinander verschiedenen Primideale, welche in p aufgehen; ihre Grade wollen wir mit $f_1, f_2 \cdots f_m$ bezeichnen, so daß z. B. $N(\mathfrak{p}_1) = p^{f_1}$ ist. Existiert nun eine ganze Zahl θ in Ω, deren Index k nicht durch p teilbar ist, so folgt aus dem Satze I in § 2, daß es in bezug auf den Modul p auch m inkongruente Primfunktionen $P_1, P_2 \cdots P_m$ gibt, deren Grade resp. gleich $f_1, f_2 \cdots f_m$ sind. Es ist nun von der größten Wichtigkeit für unsere Untersuchung, daß diese Folgerung sich umkehren läßt, daß also folgender Satz besteht:

IV. Sind $f_1, f_2 \cdots f_m$ die Grade der sämtlichen verschiedenen, in der Primzahl p aufgehenden Primideale $\mathfrak{p}_1$, $\mathfrak{p}_2 \cdots \mathfrak{p}_m$, und gibt es m nach dem Modul p inkongruente Primfunktionen $P_1, P_2 \cdots P_m$ resp. vom Grade $f_1, f_2 \cdots f_m$, so existiert in Ω eine ganze Zahl θ, deren Index k nicht durch p teilbar ist.

Dem Beweise dieses Satzes schicken wir aber zunächst einige Betrachtungen voraus, welche zum Teil von den Voraussetzungen desselben unabhängig sind.

Es sei $\mathfrak{p}$ irgend ein in p aufgehendes Primideal vom Grade f, so genügen (D. § 163; B. § 28, 3°) alle ganzen Zahlen ω des Körpers Ω der Kongruenz

$$\omega^{p^f} - \omega \equiv 0 \pmod{\mathfrak{p}};$$

bedeutet nun t wieder eine Variable, so ist die Funktion

$$t^{p^f} - t$$

nach dem Modul p kongruent dem Produkte aus allen inkongruenten Primfunktionen, deren Grade Divisoren der Zahl f sind (C. 19); unter diesen wähle man nach Belieben eine solche Primfunktion P, deren Grad $= f$ ist; dies ist stets möglich, da es immer mindestens eine solche Funktion gibt (C. 20). Da nun

$$t^{p^f} - t \equiv P(t)\,H(t) \pmod{p},$$

also auch

$$\omega^{p^f} - \omega \equiv P(\omega)\,H(\omega) \pmod{p},$$

und da p durch $\mathfrak{p}$ teilbar ist, so folgt, daß jede in $\mathfrak{o}$ enthaltene Zahl ω der Kongruenz

$$P(\omega)\,H(\omega) \equiv 0 \pmod{\mathfrak{p}}$$

genügt; mithin ist die Anzahl ihrer nach $\mathfrak{p}$ inkongruenten Wurzeln $= (\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p}) = p^f$, also genau so groß, wie ihr Grad. Durch

dieselben einfachen Schlüsse, welche in der rationalen Zahlentheorie zu einem ähnlichen Zwecke angewendet werden (D. § 26), kann man nun leicht beweisen, was ich der Kürze halber hier übergehe, daß in dem Zahlengebiete o eine Kongruenz r^{ten} Grades, deren Modul ein Primideal dieses Gebietes ist, niemals mehr als r inkongruente Wurzeln haben kann, und hieraus folgt für unseren Fall, daß die Kongruenz $H(\omega) \equiv 0 \pmod{\mathfrak{p}}$ höchstens $(p^f - f)$ inkongruente Wurzeln besitzt, und daß folglich die Repräsentanten ω der f übrigen Zahlklassen notwendig der Kongruenz $P(\omega) \equiv 0 \pmod{\mathfrak{p}}$ genügen müssen. Für unseren Zweck reicht aber schon die Gewißheit aus, daß diese Kongruenz wenigstens eine Wurzel hat. Es sei α eine bestimmte solche Wurzel, also

$$P(\alpha) \equiv 0 \pmod{\mathfrak{p}};$$

wir betrachten nun alle Zahlen von der Form $\varphi(\alpha)$ und wollen beweisen, daß die Kongruenz

$$\varphi(\alpha) \equiv 0 \pmod{\mathfrak{p}}$$

mit der Funktionenkongruenz

$$\varphi(t) \equiv 0 \pmod{p, P}$$

gleichbedeutend ist. In der Tat, wenn die letztere stattfindet, wenn also

$$\varphi(t) \equiv P(t)\,\psi(t) \pmod{p}$$

ist, so folgt auch

$$\varphi(\alpha) \equiv P(\alpha)\,\psi(\alpha) \pmod{p},$$

und da die beiden Zahlen p und $P(\alpha)$ durch $\mathfrak{p}$ teilbar sind, so ist auch $\varphi(\alpha) \equiv 0 \pmod{\mathfrak{p}}$; ist aber zweitens $\varphi(t)$ nicht teilbar durch die Primfunktion $P(t)$, so sind $\varphi(t)$ und $P(t)$ relative Primfunktionen, und folglich existieren zwei Funktionen $\varphi_1(t)$, $\varphi_2(t)$, welche der Kongruenz

$$\varphi(t)\,\varphi_1(t) + P(t)\,\varphi_2(t) \equiv 1 \pmod{p}$$

genügen (C. 5); dann ist auch

$$\varphi(\alpha)\,\varphi_1(\alpha) + P(\alpha)\,\varphi_2(\alpha) \equiv 1 \pmod{p},$$

und da p und $P(\alpha)$ durch $\mathfrak{p}$ teilbar sind, so ist

$$\varphi(\alpha)\,\varphi_1(\alpha) \equiv 1 \pmod{\mathfrak{p}},$$

und folglich ist in diesem Falle $\varphi(\alpha)$ nicht $\equiv 0 \pmod{\mathfrak{p}}$. Hiermit ist unsere obige Behauptung vollständig bewiesen.

Für den Fall, daß p durch $\mathfrak{p}^2$ teilbar ist, wollen wir ferner die Wurzel α der Kongruenz $P(\alpha) \equiv 0 \pmod{\mathfrak{p}}$ so wählen, daß die Zahl $P(\alpha)$ nicht durch $\mathfrak{p}^2$ teilbar wird. Dies ist stets möglich; ist

nämlich α eine Wurzel der Kongruenz $P(\alpha) \equiv 0 \pmod{\mathfrak{p}^2}$, so wähle man nach Belieben eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare Zahl λ, und setze $\alpha' = \alpha + \lambda$, so ist

$$P(\alpha') = P(\alpha) + \lambda P'(\alpha) + \lambda^2 P''(\alpha) + \cdots \equiv \lambda P'(\alpha) \pmod{\mathfrak{p}^2}\ [*)];$$

da nun die derivierte Funktion $P'(t)$ den Grad $(f-1)$ hat und nicht $\equiv 0 \pmod{p}$ ist, so kann sie auch nicht $\equiv 0 \pmod{p, P}$ sein, und folglich ist nach dem obigen die Zahl $P'(\alpha)$ nicht teilbar durch $\mathfrak{p}$; mithin ist das Produkt $\lambda P'(\alpha)$, und folglich auch die Zahl $P(\alpha')$ wohl teilbar durch $\mathfrak{p}$, aber nicht teilbar durch $\mathfrak{p}^2$. Nachdem so die Existenz einer solchen Zahl α' bewiesen ist, lassen wir den Akzent wieder weg, und nehmen also an, daß $P(\alpha)$ durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist.

Ist nun $\mathfrak{p}^e$ die höchste in p aufgehende Potenz des Primideals $\mathfrak{p}$, so wollen wir beweisen, daß die Zahlenkongruenz

$$\varphi(\alpha) \equiv 0 \pmod{\mathfrak{p}^e}$$

mit der Funktionenkongruenz

$$\varphi(t) \equiv 0 \pmod{p, P^e}$$

gleichbedeutend ist. In der Tat, wenn die letztere stattfindet, so ist

$$\varphi(t) \equiv P(t)^e\,\psi(t) \pmod{p},$$

also auch

$$\varphi(\alpha) \equiv P(\alpha)^e\,\psi(\alpha) \pmod{p},$$

und da beide Zahlen p und $P(\alpha)^e$ durch $\mathfrak{p}^e$ teilbar sind, so folgt $\varphi(\alpha) \equiv 0 \pmod{\mathfrak{p}^e}$; wenn dagegen die Funktionenkongruenz nicht stattfindet, so ist der größte gemeinschaftliche Teiler, welchen die Funktionen $\varphi(t)$ und $P(t)^e$ nach dem Modul p haben, von der Form $P(t)^s$, wo $s < e$; bestimmt man die Funktionen $\varphi_1(t)$, $\varphi_2(t)$ so, daß

$$\varphi(t)\,\varphi_1(t) + P(t)^e\,\varphi_2(t) \equiv P(t)^s \pmod{p}$$

wird (C. 4), und bedenkt, daß p und $P(\alpha)^e$ durch $\mathfrak{p}^e$ teilbar sind, so ergibt sich

$$\varphi(\alpha)\,\varphi_1(\alpha) \equiv P(\alpha)^s \pmod{\mathfrak{p}^e};$$

da nun $s < e$, und $P(\alpha)$ nicht durch $\mathfrak{p}^2$ teilbar ist, so ist $P(\alpha)^s$ nicht teilbar durch $\mathfrak{p}^e$, und folglich ist auch $\varphi(\alpha)$ nicht $\equiv 0 \pmod{\mathfrak{p}^e}$. Unsere Behauptung ist daher erwiesen.

Man verfahre nun mit jedem der in p aufgehenden verschiedenen Primideale $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ so, wie es im vorhergehenden beschrieben

---

[*) Durch ein Versehen schreibt Dedekind $P''(\alpha)$ statt $\frac{P''(\alpha)}{2!}$; die Zahlen $\frac{P''(\alpha)}{2!}$, $\frac{P'''(\alpha)}{3!}$, $\cdots$ sind aber auch alle ganz.]

ist, d. h. man wähle nach Belieben m Primfunktionen $P_1, P_2 \cdots P_m$, welche resp. dieselben Grade $f_1, f_2 \cdots f_m$ haben, wie jene Primideale, und bestimme ebenso viele Zahlen $\alpha_1, \alpha_2 \cdots \alpha_m$ der Art, daß $P_1(\alpha_1)$, $P_2(\alpha_2) \cdots P_m(\alpha_m)$ resp. durch $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ teilbar werden, mit der eventuellen Beschränkung, daß eine solche Zahl $P_r(\alpha_r)$ nicht durch $\mathfrak{p}_r^2$ teilbar sein darf, falls p durch $\mathfrak{p}_r^2$ teilbar ist. Da nun die Primideale $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ voneinander verschieden, und ihre Quadrate folglich relative Primideale sind, so kann man stets eine Zahl θ so bestimmen, daß

$$\begin{aligned} \theta &\equiv \alpha_1 \pmod{\mathfrak{p}_1^2} \\ \theta &\equiv \alpha_2 \pmod{\mathfrak{p}_2^2} \\ &\cdots\cdots\cdots \\ \theta &\equiv \alpha_m \pmod{\mathfrak{p}_m^2} \end{aligned}$$

wird (D. § 163; B. § 26); da hieraus

$$\begin{aligned} P_1(\theta) &\equiv P_1(\alpha_1) \pmod{\mathfrak{p}_1^2} \\ P_2(\theta) &\equiv P_2(\alpha_2) \pmod{\mathfrak{p}_2^2} \\ &\cdots\cdots\cdots\cdots\cdots \\ P_m(\theta) &\equiv P_m(\alpha_m) \pmod{\mathfrak{p}_m^2} \end{aligned}$$

folgt, so ergibt sich, daß die Zahlen $P_1(\theta)$, $P_2(\theta) \cdots P_m(\theta)$ resp. durch $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ teilbar sind, daß aber, falls p durch $\mathfrak{p}_r^2$ teilbar ist, die Zahl $P_r(\theta)$ nicht durch $\mathfrak{p}_r^2$ teilbar ist. Die Zahl θ vereinigt daher in sich alle diejenigen Eigenschaften in bezug auf die sämtlichen m Primideale, welche einer jeden Zahl α_r in bezug auf das ihr korrespondierende Primideal $\mathfrak{p}_r$ zukommen. Ist daher

$$\mathfrak{o}\, p = \mathfrak{p}_1^{e_1}\, \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m},$$

also, wie aus der Bildung der Norm hervorgeht,

$$n = e_1 f_1 + e_2 f_2 + \cdots + e_m f_m,$$

so ist eine Zahl von der Form $\varphi(\theta)$ stets und nur dann durch eine der Potenzen $\mathfrak{p}_1^{e_1}, \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}$ teilbar, wenn die ihr entsprechende Funktionenkongruenz

$$\begin{aligned} \varphi(t) &\equiv 0 \quad (\text{modd. } p, P_1^{e_1}) \\ \varphi(t) &\equiv 0 \quad (\text{modd. } p, P_2^{e_2}) \\ &\cdots\cdots\cdots\cdots\cdots \\ \varphi(t) &\equiv 0 \quad (\text{modd. } p, P_m^{e_m}) \end{aligned}$$

stattfindet; da ferner eine ganze Zahl des Körpers stets und nur dann durch p teilbar ist, wenn sie durch jede der m Potenzen $\mathfrak{p}_1^{e_1}, \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}$ teilbar ist, so leuchtet ein, daß die eine Zahlenkongruenz

$$\varphi(\theta) \equiv 0 \pmod{p}$$

gleichbedeutend ist mit dem System der m vorstehenden Funktionenkongruenzen.

Bis hierher haben wir absichtlich über die Wahl der Primfunktionen $P_1, P_2 \cdots P_m$ nichts anderes festgesetzt, als daß ihre Grade resp. mit denen der Primideale $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ übereinstimmen sollen, und es war z. B., falls $f_1 = f_2$, nicht ausgeschlossen, $P_1 = P_2$ zu wählen. Wir wollen jetzt die besondere Annahme unseres Satzes hinzufügen, welche darin besteht, daß es m untereinander inkongruente Primfunktionen von den vorgeschriebenen Graden gibt, und wir wollen unter $P_1, P_2 \cdots P_m$ solche inkongruente Primfunktionen verstehen. Dann sind die Potenzen $P_1^{e_1}, P_2^{e_2} \cdots P_m^{e_m}$ relative Primfunktionen, und wenn man ihr Produkt

$$P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} = R$$

setzt, so ist (C. 5) das System der m obigen Funktionenkongruenzen, und folglich auch die eine Zahlenkongruenz

$$\varphi(\theta) \equiv 0 \pmod{p}$$

gleichbedeutend mit der einzigen Funktionenkongruenz

$$\varphi(t) \equiv 0 \quad (\text{modd. } p, R).$$

Da ferner der Grad des Produktes R gleich

$$e_1 f_1 + e_2 f_2 + \cdots + e_m f_m$$

und folglich $= n$ ist, so kann eine Zahl

$$\varphi(\theta) = x_0 + x_1 \theta + x_2 \theta^2 + \cdots + x_{n-1} \theta^{n-1}$$

nur dann durch p teilbar sein, wenn

$$\varphi(t) \equiv 0 \pmod{p},$$

d. h. wenn alle n Koeffizienten $x_0, x_1, x_2 \cdots x_{n-1}$ durch p teilbar sind. Der Index k der Zahl θ ist folglich (nach § 1) nicht teilbar durch p. Hiermit ist unser obiger Satz bewiesen, und wir fügen nur noch die folgende Bemerkung hinzu.

Da k nicht teilbar durch p ist, so ist k auch von 0 verschieden, und folglich ist die gefundene Zahl θ die Wurzel einer irreduktiblen Gleichung $F(\theta) = 0$ vom n^{ten} Grade; da nun $F(\theta) \equiv 0 \pmod{p}$, so muß die Funktion F durch R teilbar sein nach dem Modul p; da ferner beide Funktionen denselben Grad n und denselben höchsten Koeffizienten 1 haben, so muß $F \equiv R \pmod{p}$, d. h.

$$F \equiv P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} \pmod{p}$$

sein, und hiermit sind wir zum Ausgangspunkt unserer Untersuchung in § 2 zurückgekehrt.

§ 5.

Die letzte Untersuchung hat uns ein Kriterium geliefert, durch welches die Frage entschieden wird, ob es wirklich in Ω eine ganze Zahl θ gibt, deren Index durch eine gegebene Primzahl p nicht teilbar ist. Wenn

$$o\,p = \mathfrak{p}_1^{e_1}\,\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_m^{e_m}$$

ist, wo $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ verschiedene Primideale resp. von den Graden $f_1, f_2 \cdots f_m$ bedeuten, so wird der singuläre Fall, daß die Indizes aller in Ω enthaltenen ganzen Zahlen durch p teilbar sind, jedesmal und nur dann eintreten, wenn es unmöglich ist, m nach dem Modul p inkongruente Primfunktionen von den Graden $f_1, f_2 \cdots f_m$ aufzustellen. Es fragt sich daher nur noch, ob diese Erscheinung, daß nicht genug Primfunktionen existieren, wirklich jemals auftreten kann. Um hierüber zu entscheiden, wollen wir den denkbar einfachsten Versuch anstellen. Die inkongruenten Primfunktionen ersten Grades sind die folgenden

$$t,\ t+1,\ t+2 \cdots t+(p-1),$$

ihre Anzahl ist $= p$; der obige singuläre Fall wird daher gewiß in einem Körper Ω eintreten, in welchem die Primzahl p durch mindestens $(p+1)$ verschiedene Primideale ersten Grades teilbar ist; da aber, wie aus der Betrachtung der Normen hervorgeht, das Ideal $o\,p$ ein Produkt von höchstens n Primidealen ist, so muß der Grad n eines solchen Körpers mindestens $= p+1$ sein. Nimmt man, um den einfachsten Fall zu erhalten, die kleinste Primzahl $p = 2$, so entsteht also die Frage, ob es kubische Körper Ω gibt, in welchen die Zahl 2 durch drei verschiedene Primideale ersten Grades teilbar ist; in einem solchen Körper würden die Indizes aller ganzen Zahlen gerade sein. Diese Untersuchung ist in den Göttingischen gelehrten Anzeigen vom 20. September 1871 in voller Allgemeinheit angestellt, und sie hat zu einer bejahenden Antwort geführt; hier will ich mich begnügen, ein einziges, auch dort schon angeführtes Beispiel mitzuteilen [*)].

[*) Die eben erwähnte Anzeige enthält auch eine Ausführung über die Methode, wodurch Dedekind auf das hier behandelte Beispiel gekommen ist. Weiter wird ein anderes Beispiel eines Körpers mit gemeinsamen Indexteilern gegeben, nämlich ein Körper vierten Grades, worin die Primzahl 2 in zwei Primideale zweiten Grades zerfällt.]

Es sei α eine Wurzel der irreduktiblen Gleichung dritten Grades

$$F(\alpha) = \alpha^3 - \alpha^2 - 2\alpha - 8 = 0;$$

um ihre Diskriminante zu finden, betrachten wir die Zahl

$$F'(\alpha) = \delta = -2 - 2\alpha + 3\alpha^2$$

und bilden sukzessive, unter Zuziehung von $F(\alpha) = 0$, die Produkte

$$\delta\alpha = 24 + 4\alpha + \alpha^2$$
$$\delta\alpha^2 = 8 + 26\alpha + 5\alpha^2;$$

durch lineare Elimination von $1, \alpha, \alpha^2$ aus diesen drei Gleichungen erhält man

$$\begin{vmatrix} -2-\delta, & -2 & , & 3 \\ 24 & , & 4-\delta, & 1 \\ 8 & , & 26 & , & 5-\delta \end{vmatrix} = 0,$$

d. h.

$$\delta^3 - 7\delta^2 - 2012 = 0,$$

und folglich ist die Diskriminante

$$\Delta(1, \alpha, \alpha^2) = -N(\delta) = -2012 = -2^2 \cdot 503.$$

Da 503 eine Primzahl ist, so gehen in dieser Diskriminante nur die beiden Quadrate 1 und 4 auf, und folglich ist der Index k der Zahl α entweder $= 1$, oder $= 2$; es ist daher die Funktion

$$F(t) = t^3 - t^2 - 2t - 8$$

nur in bezug auf den Modul $p = 2$ zu untersuchen. Offenbar ist

$$F = P_1^2 P_2 - 2M \equiv P_1^2 P_2 \pmod 2,$$

wo

$$P_1 = t,\quad P_2 = t-1,\quad M = t+4;$$

da nun gleichzeitig P_1 in M, und P_1^2 in F aufgeht nach dem Modul 2, so muß (nach dem zweiten Beweise des Satzes II in § 3) die Zahl

$$P_1(\alpha)\,P_2(\alpha) = \alpha(\alpha-1)$$

durch 2 teilbar, und folglich $k = 2$ sein. Dies wird sich sofort dadurch bestätigen, daß die Zahl

$$\beta = \tfrac{1}{2}\alpha(\alpha-1) - 1$$

sich ebenfalls als eine ganze Zahl erweist; in der Tat, man erhält mit Rücksicht auf $F(\alpha) = 0$ die Gleichungen

$$\alpha^2 = 2 + \alpha + 2\beta$$
$$\beta^2 = -2 + 2\alpha - \beta$$
$$\alpha\beta = 4$$

und hieraus

$$\beta^3 + \beta^2 + 2\beta - 8 = 0.$$

Da ferner

$$1 = 1\cdot 1 + 0\cdot\alpha + 0\cdot\beta$$
$$\alpha = 0\cdot 1 + 1\cdot\alpha + 0\cdot\beta$$
$$\alpha^2 = 2\cdot 1 + 1\cdot\alpha + 2\cdot\beta,$$

so ist

$$\Delta(1, \alpha, \alpha^2) = \begin{vmatrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ 2, & 1, & 2 \end{vmatrix}^2 \Delta(1, \alpha, \beta) = 2^2 \Delta(1, \alpha, \beta),$$

also

$$\Delta(1, \alpha, \beta) = -503,$$

und da diese Zahl durch kein Quadrat (außer 1) teilbar ist, so ist sie die Grundzahl D unseres kubischen Körpers Ω, und die Zahlen $1, \alpha, \beta$ bilden eine Basis des aus allen ganzen Zahlen ω dieses Körpers Ω bestehenden Gebiets $\mathfrak{o}$, d. h. nach der schon mehrfach gebrauchten Bezeichnung, es ist

$$\mathfrak{o} = [1, \alpha, \beta];$$

jede solche ganze Zahl, d. h. jede in $\mathfrak{o}$ enthaltene Zahl ω ist von der Form

$$\omega = z + x\alpha + y\beta,$$

wo z, x, y willkürliche ganze rationale Zahlen bedeuten.

Wir wollen nun auf Grund dieses Resultats die Idealfaktoren der Zahl 2 bestimmen. Da

$$\left.\begin{aligned} \alpha^2 &= \quad 2 + \alpha + 2\beta \equiv \alpha \\ \beta^2 &= -2 + 2\alpha - \beta \equiv \beta \end{aligned}\right\} \pmod 2,$$

so folgt allgemein

$$(z + x\alpha + y\beta)^2 \equiv z^2 + x^2\alpha^2 + y^2\beta^2 \equiv z + x\alpha + y\beta \pmod 2,$$

d. h. jede Zahl ω des Gebietes $\mathfrak{o}$ genügt der Kongruenz

$$\omega^2 - \omega \equiv 0 \pmod 2.$$

Hieraus folgt zunächst, daß die Zahl 2 durch kein Quadrat eines Primideals teilbar sein kann; wäre nämlich $\mathfrak{o}(2) = \mathfrak{p}^2\mathfrak{q}$, wo $\mathfrak{p}$ ein Primideal oder wenigstens ein von $\mathfrak{o}$ verschiedenes Ideal bedeutet, so würde, da $\mathfrak{p}\mathfrak{q}$ nicht durch $\mathfrak{o}(2)$ teilbar ist, eine Zahl ω existieren, welche durch $\mathfrak{p}\mathfrak{q}$, aber nicht durch 2 teilbar wäre; dann wäre aber ω^2 teilbar durch $\mathfrak{p}^2\mathfrak{q}^2$, also auch durch 2, und dies widerspricht der vorstehenden Kongruenz $\omega^2 \equiv \omega \pmod 2$. Mithin ist $\mathfrak{o}(2)$ entweder ein Primideal oder ein Produkt aus lauter verschiedenen Primidealen. Es sei $\mathfrak{p}$ irgend ein in 2 aufgehendes Primideal, so genügt jede in $\mathfrak{o}$ enthaltene Zahl ω der Kongruenz

$$\omega^2 - \omega \equiv 0 \pmod{\mathfrak{p}},$$

und folglich ist die Anzahl ihrer inkongruenten Wurzeln $= (\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p})$; da diese Anzahl aber niemals größer als der Grad der Kongruenz sein kann, so ergibt sich $N(\mathfrak{p}) \leqq 2$, und folglich $N(\mathfrak{p}) = 2$, weil $\mathfrak{p}$ ein Primideal, also von $\mathfrak{o}$ verschieden, mithin $N(\mathfrak{p}) > 1$ ist. Jedes in 2 aufgehende Primideal ist daher vom ersten Grade, und folglich muß, da $N(2) = 2^3 = 8$ ist,

$$\mathfrak{o}(2) = \mathfrak{a}\,\mathfrak{b}\,\mathfrak{c}$$

sein, wo $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ drei voneinander verschiedene Primideale ersten Grades bedeuten. Hiermit ist das Auftreten der erwähnten singulären Erscheinung erwiesen, und es muß sich bestätigen, daß die Indizes aller Zahlen ω durch 2 teilbar sind. In der Tat, setzt man

$$z' = z^2 + 2x^2 - 2y^2 + 8xy$$
$$x' = x^2 + 2y^2 + 2xz$$
$$y' = 2x^2 - y^2 + 2yz,$$

so ist

$$\omega^2 = z' + x'\alpha + y'\beta,$$

und der Index der Zahl ω ist gleich der Determinante

$$\begin{vmatrix} 1, & 0, & 0 \\ z, & x, & y \\ z', & x', & y' \end{vmatrix} = xy' - yx' = 2x^3 - x^2y - xy^2 - 2y^3,$$

welche offenbar stets eine gerade Zahl ist.

Um unser Beispiel ganz zu vollenden, und um die aus der allgemeinen Theorie geschöpften Voraussagungen auch durch die Rechnung zu bestätigen, wollen wir endlich zur Darstellung der hier auftretenden Ideale in Form von endlichen, dreigliedrigen Moduln (D. § 161; B. § 3), d. h. zur Bestimmung dieser Ideale durch ihre Basiszahlen schreiten. Diese Darstellungen sind die folgenden

$$\mathfrak{a} = [2, \alpha, 1 + \beta]$$
$$\mathfrak{b} = [2, 1 + \alpha, \beta]$$
$$\mathfrak{c} = [2, \alpha, \beta].$$

Das System $\mathfrak{a}$ aller Zahlen von der Form

$$\alpha' = 2z + \alpha x + (1 + \beta)y,$$

wo z, x, y willkürliche ganze rationale Zahlen bedeuten, besitzt in der Tat die beiden fundamentalen Eigenschaften eines Ideals, nämlich:

I. Die Summen und Differenzen von je zwei Zahlen α' des Systems $\mathfrak{a}$ gehören demselben System $\mathfrak{a}$ an.

II. Jedes Produkt aus einer Zahl α' des Systems $\mathfrak{a}$ und aus einer Zahl ω des Gebiets $\mathfrak{o}$ ist wieder eine Zahl des Systems $\mathfrak{a}$.

Die erste Eigenschaft ist evident, und um die zweite nachzuweisen, genügt es, darzutun, daß die Produkte aus je einer der Basiszahlen 2, α, $(1+\beta)$ von $\mathfrak{a}$ und je einer der Basiszahlen 1, α, β von $\mathfrak{o}$ sämtlich in $\mathfrak{a}$ enthalten sind; dies ist unmittelbar evident für die fünf Produkte

$$2\cdot 1,\ \alpha\cdot 1,\ (1+\beta)\cdot 1,\ 2\cdot\alpha,\ 2\cdot\beta = -2+2(1+\beta),$$

und für die übrigen vier ergibt sich dasselbe aus den Gleichungen

$$\alpha\cdot\alpha = \alpha+2(1+\beta), \qquad \alpha\cdot\beta = 2\cdot 2,$$
$$(1+\beta)\alpha = 2\cdot 2+\alpha, \qquad (1+\beta)\beta = -2+2\alpha.$$

Ebenso wird bewiesen, daß die Systeme $\mathfrak{b}$ und $\mathfrak{c}$ Ideale sind.

Die Norm $N(\mathfrak{m})$ eines Ideals $\mathfrak{m}$ ist die Anzahl $(\mathfrak{o}, \mathfrak{m})$ der in $\mathfrak{o}$ enthaltenen, nach $\mathfrak{m}$ inkongruenten Zahlen (D. § 163; B. § 20), und diese Anzahl ist gleich der Determinante der Ausdrücke, welche in bezug auf die Basiszahlen von $\mathfrak{o}$ linear sind und die Basiszahlen von $\mathfrak{m}$ darstellen (D. § 161; B. § 4, 4°). Es ist daher z. B.

$$N(\mathfrak{a}) = \begin{vmatrix} 2, & 0, & 0 \\ 0, & 1, & 0 \\ 1, & 0, & 1 \end{vmatrix} = 2,$$

und ebenso ergibt sich

$$N(\mathfrak{b}) = N(\mathfrak{c}) = 2.$$

Wenn aber die Norm eines Ideals eine Primzahl ist, so muß das Ideal notwendig ein Primideal sein, weil allgemein $N(\mathfrak{a}_1\mathfrak{a}_2) = N(\mathfrak{a}_1)N(\mathfrak{a}_2)$ ist; mithin sind $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ Primideale. Sie sind ferner verschieden voneinander, weil die in $\mathfrak{b}$ und in $\mathfrak{c}$ enthaltene Zahl β nicht in $\mathfrak{a}$ enthalten, und weil die in $\mathfrak{c}$ enthaltene Zahl α nicht in $\mathfrak{b}$ enthalten ist. Es muß folglich die in allen drei Idealen enthaltene Zahl 2 auch in dem Produkte $\mathfrak{abc}$ enthalten sein; mithin ist $\mathfrak{o}(2) = \mathfrak{m}\,\mathfrak{abc}$, wo $\mathfrak{m}$ ein Ideal bedeutet; nimmt man aber die Norm, so ergibt sich

$$N(2) = 8 = N(\mathfrak{m})\,N(\mathfrak{a})\,N(\mathfrak{b})\,N(\mathfrak{c}) = 8\,N(\mathfrak{m});$$

mithin ist $N(\mathfrak{m}) = 1$, also $\mathfrak{m} = \mathfrak{o}$, und $\mathfrak{o}(2) = \mathfrak{abc}$. Aber auch dieses, aus allgemeinen Sätzen geschlossene Resultat wollen wir durch die eigentliche Rechnung, d. h. durch die wirkliche Ausführung der Multiplikation der Ideale bestätigen (D. § 165; B. § 12).

Unter dem Produkte $\mathfrak{ab}$ zweier Ideale wird das System aller Produkte $\alpha'\beta'$ und aller Summen von solchen Produkten $\alpha'\beta'$ verstanden, wo α', β' beliebige Zahlen resp. der Ideale $\mathfrak{a}$, $\mathfrak{b}$ bedeuten

(D. § 163; B. § 22). Ein solches Produkt erscheint daher zunächst als ein endlicher Modul, dessen Basiszahlen die sämtlichen Produkte aus je einer Basiszahl von $\mathfrak{a}$ und je einer Basiszahl von $\mathfrak{b}$ sind. In unserem Falle ist daher $\mathfrak{ab}$ der endliche Modul, dessen Basiszahlen die neun Produkte

$$2\cdot 2 = 4, \quad 2(1+\alpha) = 2+2\alpha, \quad 2\cdot\beta = 2\beta,$$
$$\alpha\cdot 2 = 2\alpha, \quad \alpha(1+\alpha) = 2+2\alpha+2\beta, \quad \alpha\beta = 4,$$
$$(1+\beta)\cdot 2 = 2+2\beta, \quad (1+\beta)(1+\alpha) = 5+\alpha+\beta,$$
$$(1+\beta)\beta = -2+2\alpha$$

sind; da aber von diesen neun Zahlen nur drei voneinander unabhängig sind (D. § 159; B. § 4), so ist die von mir ausführlich beschriebene Methode (B. § 4, 6°) anzuwenden, um diesen neungliedrigen Modul auf einen dreigliedrigen zurückzuführen; durch die Ausführung dieser sehr einfachen und leichten Rechnung erhält man die eine der sechs folgenden Gleichungen:

$$\mathfrak{a}^2 = [4, \ \alpha, \ 3+\beta]; \quad \mathfrak{bc} = [2, \ 2\alpha, \ \beta]$$
$$\mathfrak{b}^2 = [4, \ 1+\alpha, \ \beta]; \quad \mathfrak{ca} = [2, \ \alpha, \ 2\beta]$$
$$\mathfrak{c}^2 = [4, \ 2+\alpha, \ 2+\beta]; \quad \mathfrak{ab} = [2, \ 2\alpha, \ 1+\alpha+\beta].$$

Die übrigen ergeben sich auf dieselbe Weise; und wenn man abermals nach derselben Methode mit $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ multipliziert, so erhält man folgende zehn Hauptideale:

$$\mathfrak{abc} = [2, \ 2\alpha, \ 2\beta \ ] = \mathfrak{o}(2)$$
$$\mathfrak{a}^2\mathfrak{c} = [4, \ \alpha, \ 2+2\beta] = \mathfrak{o}\alpha$$
$$\mathfrak{b}^2\mathfrak{c} = [4, \ 2+2\alpha, \ \beta \ ] = \mathfrak{o}\beta$$
$$\mathfrak{ac}^2 = [4, \ 2+\alpha, \ 2\beta \ ] = \mathfrak{o}(\alpha-2)$$
$$\mathfrak{bc}^2 = [4, \ 2\alpha, \ 2+\beta \ ] = \mathfrak{o}(2-\beta)$$
$$\mathfrak{a}^2\mathfrak{b} = [4, \ 2\alpha, \ 3+\alpha+\beta] = \mathfrak{o}(3+\alpha+\beta)$$
$$\mathfrak{ab}^2 = [4, \ 2+2\alpha, \ 1+\alpha+\beta] = \mathfrak{o}(1+\alpha+\beta)$$
$$\mathfrak{a}^3 = [8, \ 4+\alpha, \ 3+\beta \ ] = \mathfrak{o}(3+2\alpha+\beta)$$
$$\mathfrak{b}^3 = [8, \ 1+\alpha, \ 4+\beta \ ] = \mathfrak{o}(1+\alpha)$$
$$\mathfrak{c}^3 = [8, \ 2+\alpha, \ 2+\beta \ ] = \mathfrak{o}(\alpha+\beta-4)$$

Die zehn Zahlen μ, welchen diese Hauptideale $\mathfrak{o}\mu = [\mu, \alpha\mu, \beta\mu]$ entsprechen, sind durch die folgenden, leicht zu verifizierenden Relationen miteinander verbunden:

$$\alpha(\alpha-2)(1+\alpha) = 2^3; \quad \alpha\beta = (\alpha-2)(1+\alpha+\beta) = 2^2$$
$$(\alpha-2)(3+\alpha+\beta) = 2\alpha; \quad \alpha(2-\beta) = 2(\alpha-2)$$
$$(\alpha-2)(3+2\alpha+\beta) = \alpha^2; \quad \alpha(\alpha+\beta-4) = (\alpha-2)^2.$$

Durch dieses Beispiel, welchem man viele andere an die Seite stellen könnte, ist außer Zweifel gesetzt, daß es Körper Ω gibt, in welchen die Indizes aller ganzen Zahlen durch eine und dieselbe Primzahl p teilbar sind. Dies Resultat ist in mancher Beziehung kein willkommenes. Es gibt in der Tat sehr wichtige Sätze der Idealtheorie, welche sich durch die Theorie der höheren Kongruenzen sehr leicht würden beweisen lassen, wenn der Satz I in § 2 nicht an die Voraussetzung gebunden wäre, daß der Index k der Zahl θ nicht durch p teilbar sein darf; wir haben aber jetzt gesehen, daß in manchen Fällen diese Voraussetzung auf keine Weise zu erfüllen ist, wie man auch die Zahl θ wählen mag, und hieraus geht hervor, daß solche Beweise, die sich auf den genannten Satz stützen, häufig die erforderliche Allgemeinheit nicht besitzen. Als Beispiel führe ich den folgenden, besonders wichtigen Satz an, den ich ebenfalls in den Göttingischen gelehrten Anzeigen vom 20. September 1871 zuerst ausgesprochen habe:

Die Grundzahl D eines Körpers Ω ist aus allen und nur aus denjenigen rationalen Primzahlen p zusammengesetzt, welche in diesem Körper durch das Quadrat eines Primideals teilbar sind.

Gibt es in Ω eine ganze Zahl, deren Index durch die Primzahl p nicht teilbar ist, so folgt für diese Primzahl p die Richtigkeit des Satzes augenscheinlich sehr leicht aus § 2. Aber auf diese Weise gelangt man offenbar nicht zu dem Beweise der allgemeinen Gültigkeit des Satzes, und es ist mir erst nach manchen vergeblichen Versuchen gelungen, den allgemeinen Beweis in aller Strenge zu führen. Die ausführliche Darstellung dieses Gegenstandes, bei welcher der Satz selbst noch eine wesentliche Erweiterung erfahren wird, muß ich aber für eine andere Gelegenheit mir vorbehalten.

Erläuterungen zur vorstehenden Abhandlung.

Das Problem der Verallgemeinerung der Kummerschen Theorie der Ideale in Kreisteilungskörpern auf beliebige Körper führt natürlich zu einer Definition der Ideale mittels höheren Kongruenzen. Schon Selling (Zeitschr. f. Math. u. Phys., Bd. 10, S. 17—47 (1865)) schlägt diesen Weg ein, und es gelingt ihm, zwar unter Anwendung von Galoisschen Imaginären und weiteren Hilfskörpern, eine ausnahmslose Theorie der Ideale in Galoisschen Körpern zu gewinnen. Die Primidealzerlegung einer Primzahl p wird aus der Zerlegung der definierenden Gleichung (mod. p^α) in diesen Hilfskörpern abgeleitet. Ein Nachweis der Invarianz dieser Ideale, d. h. ihre Unabhängigkeit von der gewählten Gleichung wird aber nicht gebracht.

Wie aus der Einleitung hervorgeht, hat auch Dedekind zuerst diese Methode versucht, aber wieder aufgegeben, um die Theorie der Ideale in der abstrakten Form zu schaffen, wie er sie in der zweiten Auflage von Dirichlets Zahlentheorie dargestellt hat. In dieser Form entsteht aber sofort die Frage, wie die Primidealzerlegung einer gegebenen Zahl im Körper bestimmt werden kann, und speziell wie Primideale bei gegebener, definierender Gleichung abgeleitet werden können. Diese Frage wird für Primzahlen, welche den Index nicht teilen, durch den Satz I, § 2 erledigt, aber die vollständige Lösung scheitert an dem Vorkommen der gemeinsamen Indexteiler (gemeinsame außerwesentliche Diskriminantenteiler).

In der mehrmals von Dedekind erwähnten Arbeit von Zolotareff (1874) wird umgekehrt die Primidealzerlegung durch die Zerlegung des Satzes I definiert. Wenn aber p ein Teiler des Index ist, genügt diese Definition nicht der Forderung der Invarianz. Eine ausnahmslose Theorie der Ideale gibt aber Zolotareff in der Arbeit: „Sur la théorie des nombres complexes“ (Journ. de Math., Bd. 6, S. 51—84, 129—166, 3e série (1880); man vgl. auch: Mélanges math. et astron., Bulletin de l'academie des sciences, St. Petersburg, Bd. 5, 13./25. September 1877), worin er auch eine Übersicht über seine erste Theorie gibt. Bei seiner allgemeinen Theorie der Ideale muß aber Zolotareff so wie Dedekind eine Definition der Ideale mittels der definierenden Gleichung aufgeben.

Man kann die Zolotareffsche Theorie kurz folgendermaßen beschreiben: Zuerst wird eine Methode angegeben, wodurch man in endlich vielen Schritten ein vollständiges Restsystem

$$(1) \qquad \alpha_1, \alpha_2, \ldots, \alpha_{p^n-1} \pmod{p} \text{ (die Null ausgenommen)}$$

aufstellen kann. Eine Zahl α in (1) heißt relativ prim zu p, wenn es keine Zahl γ in (1) gibt, wofür $\alpha\gamma$ durch p teilbar ist. Zwei Zahlen α und β heißen relativ prim in bezug auf p, wenn es keine Zahl γ in (1) gibt, wofür gleichzeitig $\alpha\gamma$ und $\beta\gamma$ durch p teilbar sind. Es können dann zwei Zahlen γ und δ so bestimmt werden, daß

$$\alpha\gamma + \beta\delta \equiv 1 \pmod{p},$$

und hieraus erhält man leicht eine Definition des größten gemeinsamen Teilers in bezug auf p. Die Primideale werden dann folgendermaßen eingeführt: Eine Zahl α enthält nur ein Primideal β von p, wenn jede Zahl in (1), welche nicht zu α relativ prim ist, die Zahl α als Teiler in bezug auf p enthält. Aus (1) können dann in endlich vielen Schritten die Anzahl der vorkommenden verschiedenen Primideale bestimmt werden.

Es würde hier zu weit führen, auf alle späteren Begründungen der Idealtheorie einzugehen. Es sollen hier nur ganz kurz die wichtigsten Methoden zur Bestimmung der Primideale erwähnt werden.

Die Kroneckersche Theorie der Formen (Journ. f. Math., Bd. 92, S. 1—122 (1882)) gibt eine theoretisch besonders einfache Bestimmung der Primidealzerlegung der rationalen Primzahlen. Wie zuerst in voller Allgemeinheit von Hensel (Journ. f. Math., Bd. 113, S. 61—83 (1894)) gezeigt worden ist, besteht in dieser Theorie für alle Primzahlen ein vollständiges Analogon zum Dedekindschen Satze.

Die Schwierigkeiten der gemeinsamen Indexteiler werden hier dadurch überwunden, daß man statt einer speziellen Gleichung eine Fundamentalgleichung

$F(x_1 \dots x_n) = 0$ des Körpers studiert. Wenn die Zahlen ω_i eine Minimalbasis bilden, ist $F(x_1 \dots x_n) = 0$ die Gleichung, welcher die Fundamentalform

$$\omega = \omega_1 x_1 + \cdots + \omega_n x_n \tag{2}$$

genügt. Die entsprechende Indexform ist dann eine Einheitsform, d. h. ihre Koeffizienten haben keinen gemeinsamen Teiler, und man erhält für die Fundamentalgleichung Resultate, welche dem Dedekindschen Satze I genau entsprechen.

Diese Lösung des Problems gibt aber keine Auskunft über den Zusammenhang zwischen den Eigenschaften der Gleichungen des Körpers und der Primidealzerlegung, wie es beim Dedekindschen Satze der Fall ist. In der von Hensel begründeten p-adischen Theorie der algebraischen Zahlen wird diese Lücke zum Teil ausgefüllt, indem man zeigt, daß die Zerlegung der definierenden Gleichung in irreduzible p-adische Faktoren der Zerlegung von p in Primidealpotenzen entspricht. Für die vollständige Bestimmung der Primidealzerlegung muß man aber auch hier auf die Kroneckersche Theorie zurückgreifen. (Man sehe K. Hensel: Theorie der algebraischen Zahlen I, Leipzig 1908.)

Man kann aber zeigen, daß die Schwierigkeiten der Dedekindschen Theorie dadurch vollständig beseitigt werden können, daß man statt Kongruenzen (mod. p) immer Kongruenzen (mod. p^α) betrachtet, wo α eine feste Zahl ist, und $\alpha > \delta$, wenn die Diskriminante der entsprechenden Gleichung genau durch p^δ teilbar ist. Die entsprechenden irreduziblen Faktoren sind dann zwar nicht (mod. p^α), aber doch (mod. $p^{\alpha-\delta}$) eindeutig bestimmt. Die gemeinsamen Indexteiler verlieren dadurch gänzlich ihre Ausnahmestellung und man erhält eine eindeutige Korrespondenz zwischen Primidealzerlegung und Faktoren der Gleichung (O. Ore, Math. Ann., Bd. 96, S. 315—352 (1926) und Bd. 97, S. 569—598 (1927)). Weiter kann die Dedekindsche Darstellung der Primideale in der Form $\beta = (p, \varphi(\vartheta))$ durch eine Methode bestimmt werden, welche mit der Bestimmung der Reihenentwicklung algebraischer Funktionen große Ähnlichkeit zeigt (O. Ore, Math. Ann., Bd. 99, S. 84—117 (1928)).

Die Resultate in § 4 der vorliegenden Abhandlung geben ein einfaches Kriterium für gemeinsame Indexteiler. Hensel (Journ. f. Math., Bd. 113, S. 128—160 (1894)) leitet ein weiteres Kriterium ab, indem er die Bedingung dafür aufstellt, daß die Indexform $k(x_1, \dots, x_n)$ zu (1) für alle ganzzahligen Werte der x_i einen gemeinsamen Teiler hat. Durch diese Untersuchung gelang es auch Hensel, die Kroneckersche Vermutung zu beweisen, daß für Körper mit gemeinsamen Indexteilern immer Erweiterungskörper K derart existieren, daß, wenn die Variablen x_i in (1) alle ganze Zahlen in K durchlaufen, keine gemeinsame Idealteiler der entsprechenden Werte der Indexform vorkommen können.

Das Henselsche Kriterium zeigt, daß für einen gemeinsamen Indexteiler p gleich $p < \frac{n(n-1)}{2}$ ist. E. v. Zylinsky (Math. Ann., Bd. 73, S. 273—274 (1913)) beweist unter Anwendung des Dedekindschen Kriteriums, daß sogar $p < n$ ist. M. Bauer (Math. Ann., Bd. 64, S. 573—576 (1907)) zeigt umgekehrt, daß, wenn diese Bedingung erfüllt ist, auch immer Körper n-ten Grades existieren, worin p gemeinsamer Indexteiler ist. Weiter wird die Existenz von Indexteilern mit speziellen Eigenschaften nachgewiesen. Diese Resultate folgen auch sofort aus dem allgemeinen Existenzsatz für Körper mit vorgeschriebenen Primidealzerlegungen gegebener Primzahlen (H. Hasse, Math. Ann., Bd. 95, S. 229—238 (1925); O. Ore, Math. Zeitschr., Bd. 20, S. 267—279 (1924)).

Ore.

XVI.

Sur la théorie des nombres complexes idéaux. (Extrait d'une lettre adressée à M. Hermite.)

[Comptes rendus hebdomadaires des séances de l'Académie des Sciences, Paris, Bd. 90, S. 1205—1207 (1880).]

Je prends la liberté de vous communiquer la remarque suivante sur les théorèmes signalés par M. Sylvester dans les *Comptes rendus* des 16 et 23 février, lesquels se rapportent à quelques congruences ressortant de la théorie de la division du cercle. Comme toute la théorie des congruences est entièrement contenue dans celle des *idéaux*, les théorèmes de M. Sylvester ne sont que des conséquences très spéciales d'un seul théorème, par lequel sont définis tous les idéaux qui se rencontrent dans la théorie des nombres, composés rationnellement de racines de l'unité. Ce théorème, comme je l'ai déjà fait remarquer dans le § 27 de mon Mémoire *Sur la théorie des nombres entiers algébriques* (Paris, 1877, p. 109), se déduit facilement des résultats obtenus par M. Kummer, à l'aide de certains principes généraux dont l'exposition complète dépasserait les bornes de cette Communication; pour le moment, il suffira d'énoncer le théorème en question.

Soit θ une racine primitive de l'équation $\theta^m = 1$; l'ensemble K_m de tous les nombres $\eta = F(\theta)$ qui se déduisent de θ par les opérations rationnelles de l'Arithmétique constitue ce que j'appelle un *corps* de nombres; la théorie des idéaux de ce corps cyclotomique K_m, dont le *degré* est égal à $\varphi(m)$, a été établie par M. Kummer (*Mémoires de l'Académie de Berlin*, 1856). Prenons maintenant un nombre déterminé $\eta = F(\theta)$, et cherchons le degré n de l'équation irréductible $\psi(\eta) = 0$, dont η est la racine; pour cela, il faut considérer le système de tous les nombres entiers rationnels qui sont premiers avec m et incongrus suivant m; parmi ces nombres, dont le nombre est égal à $\varphi(m)$, il y a un système (h), comprenant tous

les exposants h, qui satisfont à la condition $F(\theta^h) = F(\theta)$ et qui forment un *groupe*, c'est-à-dire que le produit de deux quelconques d'entre eux se trouve dans le même système (h); le nombre de ces exposants h est $\frac{\varphi(m)}{n}$.

L'ensemble de tous les nombres $\omega = f(\eta)$, composés rationnellement de η, constitue un corps cyclotomique Ω de degré n, lequel est un *diviseur* du corps K_m. Réciproquement, si Ω est un corps dont tous les nombres sont contenus dans le corps K_m, il existe toujours des nombres η qui engendrent le corps Ω de la manière indiquée ci-dessus. Le corps Ω est complètement déterminé par le groupe (h), et à chaque groupe (h) correspond un corps Ω.

Après avoir rappelé ces principes bien connus de la théorie de la division du cercle, je vais maintenant proposer le théorème général sur les idéaux d'un tel corps cyclotomique Ω. En me servant des notations dont j'ai fait usage dans le Mémoire cité plus haut, je désigne par ν l'idéal principal consistant en tous les nombres *entiers* contenus dans le corps Ω. Soit p un nombre premier quelconque (rationnel, positif); on peut poser $m = m'p'$, où p' désigne la plus haute puissance de p, laquelle divise le nombre m; soit en outre $\frac{\varphi(p')}{g}$ le nombre de tous ceux, parmi les nombres h contenus dans le groupe (h), qui sont égaux à $1 \pmod{m'}$, et soit f le plus petit exposant positif qui satisfasse à la condition que p^f soit congru, suivant le module m', à l'un des nombres h du groupe (h); alors le degré n du corps Ω sera divisible par le produit fg, et, si l'on pose $n = efg$, on aura la décomposition

$$\nu p = (\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_e)^g,$$

où les e idéaux premiers $\mathfrak{p}$ sont différents entre eux; le *degré* de ces idéaux est égal à f, c'est-à-dire que leur *norme* est donnée par l'équation

$$N(y) = p^f.$$

Ce théorème général revient à celui de M. Kummer pour le cas $n = \varphi(m)$.

Dans un Mémoire sur la dépendance entre la théorie des congruences et celle des idéaux (Göttingue, 1878), j'ai démontré que les équations irréductibles de degré n auxquelles satisfont les nombres entiers d'un corps quelconque Ω de degré n, prises par rapport à

un module premier p, se résolvent en facteurs irréductibles, dont les degrés coïncident, en général, avec les degrés des idéaux premiers $\mathfrak{p}$ qui divisent le nombre p. Par suite, la condition pour que ces congruences aient des racines *commensurables* [*)] consiste dans l'existence d'un tel idéal $\mathfrak{p}$ dont le degré soit égal à 1. En faisant l'application de ce fait à notre exemple, où il s'agit des équations $\psi(\eta) = 0$ de la division du cercle, on voit bien que les racines x de la congruence cyclotomique $\psi(x) \equiv 0 \pmod{p}$ ne seront commensurables que dans le cas $f = 1$, c'est-à-dire dans le cas que p soit congru, suivant le module m', à l'un des nombres h du groupe (h). Pour descendre finalement de la théorie générale aux théorèmes de M. Sylvester, il suffit d'observer que le corps Ω du degré $\frac{1}{2}\varphi(m)$, qui provient du nombre $\eta = \theta + \theta^{-1}$, correspond au groupe (h) des deux nombres $h \equiv \pm 1 \pmod{m}$[**)].

[*) D. h. im rationalen Bereiche lösbar sind.]

[**) Sylvester hat in zwei Noten [Compt. rend., Bd. 90, S. 287—289, 345—347 (1880)] gezeigt, daß dieses spezielle Polynom $\psi(x)$, abgesehen von Teilern von m, nur Primzahlteiler von der Form $p = tm \pm 1$ haben kann.]

XVII.

Réponse à une remarque de M. Sylvester concernant les Leçons sur la théorie des nombres de Dirichlet.

[Comptes rendus hebdomadaires des séances de l'Académie des Sciences, Paris. Bd. 91, S. 154—156 (1880).]

Dans le § 47 de la *Zahlentheorie* de Dirichlet (3e éd., p. 110), où il s'agit de l'algorithme connu qui sert à déterminer la valeur du symbole $\left(\frac{b}{a}\right)$, on rencontre cette phrase: „Es zeigt sich nun, daß die damals notwendige Zerlegung in Primzahlfaktoren (abgesehen von dem Faktor 2) ganz überflüssig geworden.“. Ce passage a donné lieu à la remarque suivante de M. Sylvester (*Comptes rendus* du 10 mai 1880, p. 1105): „Ce qui précède ici rend évident (il me semble) que cette exclusion du nombre 2 (due probablement à quelque mésintelligence de la part des auditeurs de Dirichlet) est elle-même (*überflüssig*) superflue“. Je me permets de répondre à M. Sylvester que sa remarque, dont je n'ai eu connaissance qu'aujourd'hui, 11 juillet 1880, repose sur un malentendu de sa part, en ce qu'il prend pour synonymes les deux mots *superflu* et *évitable*. En désignant comme superflue une opération, on veut bien dire qu'elle est aussi évitable; mais la réciproque n'est pas juste; une opération évitable peut en même temps être très-utile, et dans ce cas elle n'est pas du tout superflue. Comme M. Sylvester l'a remarqué dans une Note antérieure (*Comptes rendus*, du 3 mai 1880, p. 1054), il est évident qu'on peut toujours former une chaîne réductive impaire dont les deux premiers termes sont des nombres impairs donnés. Je me permets d'ajouter que certainement cette évidence n'a pu échapper à personne et que l'algorithme de M. Sylvester coïncide à peu près avec celui que Eisenstein a publié il y a trente-six ans (*Journal de Crelle*, t. 27, p. 317); mais, en excluant les restes pairs et en évitant ainsi la décomposition relative au nombre 2, on est amené très souvent à une chaîne réductive beaucoup plus longue; sans aucun doute, l'illustre géomètre anglais se serait aperçu de cette circonstance s'il avait voulu traiter, non seulement le deuxième et le troisième, mais aussi le premier des exemples proposés à l'endroit cité de la *Zahlentheorie* (p. 110). En effet, pour calculer d'après la méthode des restes impairs la valeur du symbole $\left(\frac{365}{1847}\right)$, il faut former la chaîne réductive contenant les 21 nombres suivants:

$$\begin{array}{rrrrrrr} 1847, & 365, & -343, & -321, & 299, & 277, & -255, \\ -233, & 211, & 189, & -167, & -145, & 123, & 101, \\ -79, & -51, & 35, & 13, & 9, & -5, & -1, \end{array}$$

tandis que, dans la méthode des plus petits restes, il suffit de former seulement les deux chaînes

$$1847,\ 365,\ 22 \quad \text{et} \quad 365,\ 11,\ 2.$$

Je suis persuadé que tout calculateur préférera la dernière méthode, et j'en conclus que la conservation des restes pairs et de la décomposition relative au nombre 2, bien qu'elle soit évitable, n'est pas du tout superflue, comme le veut M. Sylvester. Je laisse donc au lecteur le soin de juger de quel côté se trouve la mésintelligence; sans doute, j'aurais pu éviter d'entrer dans cette discussion, provoquée par M. Sylvester, mais j'espère que ma réponse ne sera pas tout à fait superflue.