XXIX.

Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern.

[Journal für reine und angewandte Mathematik, Bd. 121, S. 40—123 (1900).]

Die vorliegende Abhandlung ist im Laufe des Winters 1897/98 durch Umarbeitung eines aus dem Jahre 1871 oder 1872 stammenden Entwurfes entstanden; ihr Hauptergebnis habe ich (Februar 1873) in meiner Anzeige*) der Vorlesungen über die Kreisteilung von P. Bachmann bei Besprechung des kubischen Reziprozitätsgesetzes mit den folgenden Worten kurz angedeutet: „Bedeutet k eine ganze rationale Zahl, deren Kubikwurzel irrational ist, so entspringt aus der Gleichung $x^3 = k$ ein reiner kubischer Körper, dessen Grundzahl die Form $D = -3g^2$ hat, wo g eine aus k leicht abzuleitende ganze Zahl ist. Fragt man nun nach allen in k nicht aufgehenden Primzahlen p von der Form $3n+1$, von welchen die gegebene Zahl k kubischer Rest ist, so gelangt man mit Hilfe des Reziprozitätssatzes zu folgendem interessanten Resultat, welches im wesentlichen schon Gauß bekannt gewesen ist (und sich auf beliebige kubische Körper ausdehnen läßt): Die sämtlichen nicht äquivalenten, ursprünglichen positiven quadratischen Formen $ax^2 + bxy + cy^2$, in welchen $b^2 - 4ac = D$, zerfallen in drei Abteilungen von gleich vielen Individuen, deren erste eine Gruppe bildet, durch deren Formen alle und nur solche Primzahlen p dargestellt werden, von welchen k kubischer Rest ist. Mit Hilfe desselben wird die Bestimmung der Anzahl der Idealklassen des kubischen Körpers auf einen bekannten Teil der Theorie der Thetafunktionen zurückgeführt.“ Zur Vergleichung bemerke ich, daß die hier gebrauchten Zeichen k, x, g in der folgenden Abhandlung bzw. durch ∂, Θ, k ersetzt sind; der Satz über die für den kubischen Körper

*) Schlömilchs Zeitschrift für Mathematik und Physik, Jahrgang 18; 1873. Literaturzeitung S. 22, 43.

charakteristische Drittelung der Gruppe der quadratischen Formen von der Diskriminante D findet sich in § 11. Die eingeklammerten Worte, welche sich auf die Ausdehnung dieses Satzes auf alle kubischen Körper beziehen, habe ich damals, weil ich im Besitze des Beweises zu sein glaubte, dem Manuskripte der Anzeige gleich nachgeschickt, ihre Einfügung an der bezeichneten Stelle ist aber über dem großen Leipziger Setzerstrike versäumt, und sie sind erst im folgenden Hefte der Literaturzeitung (S. 43) abgedruckt. Durch Überhäufung mit Amtsgeschäften wurde ich in jener Zeit für mehrere Jahre an jeder wissenschaftlichen Tätigkeit gehindert, und erst später habe ich erkannt, daß die mir zu Gebote stehenden Mittel zum Beweise der Allgemeingültigkeit des Satzes nicht ausreichten. Seitdem bin ich nur vorübergehend und ohne den gewünschten Erfolg zu dieser Untersuchung zurückgekehrt; doch zweifle ich auch heute nicht an der Wahrheit des Satzes, den ich in allen Beispielen bestätigt gefunden habe, und ich glaube auch, daß für Körper von negativer Grundzahl die jetzt mehr ausgebildete Theorie der komplexen Multiplikation der elliptischen Funktionen zum Beweise wohl ausreichen wird; vielleicht wird, wenn dies gelingt, hierdurch auch ein Weg zur Lösung des großen Rätsels gebahnt, welche algebraische Zahlkörper den Klassen der binären quadratischen Formen (oder Moduln) von positiver Diskriminante entsprechen. Meine bisherigen auf diese Fragen bezüglichen Versuche gedenke ich in einer Abhandlung über die Invarianten beliebiger kubischer Körper mitzuteilen. Die gegenwärtige Abhandlung, welche sich ausschließlich mit den reinen kubischen Körpern beschäftigt, verfolgt lediglich das in der oben erwähnten Anzeige vom Jahre 1873 angedeutete Ziel und endigt mit der Einmündung der Untersuchung in die Theorie der komplexen Multiplikation. Ich erwähne schließlich, daß die Theorie der reinen kubischen Körper meines Wissens bisher nur von A. Markoff behandelt ist; seine Abhandlung*) „Sur les nombres entiers dépendants d'une racine cubique d'un nombre entier ordinaire“ beschränkt sich im wesentlichen auf die (von mir in §§ 1—5 behandelte) Bestimmung der in dem Körper vorhandenen Ideale, wobei die Auffassung von Zolotareff zugrunde gelegt ist; außerdem gibt sie am Schlusse eine sehr wertvolle Tabelle von Einheiten (vgl. unten § 13).

*) Mémoires de l'Académie impériale des sciences de St.-Pétersbourg, VIIe série, tome 38.

§ 1.

Reine kubische Zahlkörper.

Ist die rationale Zahl ∂ nicht die dritte Potenz einer rationalen Zahl, so sind die drei Kubikwurzeln $\Theta = \sqrt[3]{\partial}$ irrational, und es kann auch keine von ihnen die Wurzel einer quadratischen Gleichung $\Theta^2 + m\Theta + n = 0$ mit rationalen Koeffizienten m, n sein; multipliziert man nämlich mit Θ, so würde hieraus $(n - m^2)\Theta + (\partial - mn) = 0$, also, weil Θ irrational ist, $n = m^2$ und $\partial = mn = m^3$ folgen, was im Widerspruch mit unserer Annahme über ∂ steht. Mithin ist jede der drei Wurzeln Θ eine algebraische Zahl dritten Grades (vgl. § 167, S. 492 der vierten Auflage von Dirichlets Zahlentheorie, die ich mit D. zitieren werde). Im folgenden bezeichnen wir mit Θ die reelle Kubikwurzel aus ∂, mit Θ', Θ'' die beiden imaginären Wurzeln

$$\Theta' = \Theta\varrho, \quad \Theta'' = \Theta\varrho^2,$$

wo ϱ eine imaginäre dritte Einheitswurzel, also

$$\varrho^2 + \varrho + 1 = 0$$

ist.

Aus dem Körper R der rationalen Zahlen entsteht durch Adjunktion der Zahl Θ der reine kubische Zahlkörper $K = R(\Theta)$ vom Grade $(K, R) = 3$; er besteht aus allen Zahlen von der Form

$$\varkappa = x_1\Theta^2 + x_2\Theta + x_3,$$

wo x_1, x_2, x_3 beliebige Zahlen in R bedeuten, und jede Zahl $\varkappa$ kann auch nur auf eine einzige Art in dieser Form dargestellt werden, weil die drei Potenzen Θ^2, Θ, 1 eine irreduzible Basis von K bilden (D. § 164, S. 472). Die beiden Körper R und K sind die einzigen Divisoren von K; denn wenn der Körper L in K enthalten ist, so folgt (nach D. § 164, S. 473), daß $(K, L)(L, R) = (K, R) = 3$, also entweder $(K, L) = 3$, $(L, R) = 1$, $L = R$ oder $(K, L) = 1$, $(L, R) = 3$, $L = K$ ist. Betrachtet man nun irgend eine in K enthaltene Zahl $\varkappa$ von der obigen Form, so ist der von ihr erzeugte Körper $R(\varkappa)$ jedenfalls Divisor von K, und zwar tritt der Fall $R(\varkappa) = R$ immer und nur dann ein, wenn $\varkappa$ rational, also $x_1 = x_2 = 0$ ist; jede irrationale Zahl $\varkappa$ des Körpers K erzeugt daher stets denselben Körper $R(\varkappa) = K$ und ist folglich eine algebraische Zahl dritten Grades.

Diese Schlüsse sind offenbar unabhängig von der Voraussetzung, daß Θ reell ist, und gelten daher ebenso für die beiden reinen kubischen Körper $K' = R(\Theta')$ und $K'' = R(\Theta'')$. Bedeutet z. B. $\varkappa'$ eine irrationale Zahl des Körpers K', so ist $R(\varkappa') = K'$, und folglich kann $\varkappa'$ nicht reell sein, weil sonst K' aus lauter reellen Zahlen bestehen würde, während doch die imaginäre Zahl $\Theta' = \Theta\varrho$ in K' enthalten ist; mithin enthalten die Körper K', K'' außer den rationalen nur imaginäre Zahlen, während K nur aus reellen Zahlen besteht. Die beiden Körper K', K'' sind aber nicht allein von K, sondern auch voneinander verschieden; denn wäre $K' = K''$, so müßte die Zahl $\Theta'' = \Theta'\varrho$, also auch die Zahl $\varrho = \Theta'' : \Theta'$ in K' enthalten sein, was nach dem Obigen nicht angeht, weil ϱ eine algebraische Zahl zweiten Grades ist.

Der Körper K besitzt drei Permutationen (D. § 165), durch welche er in die drei konjugierten Körper K, K', K'' übergeht; jede in K enthaltene Zahl $\varkappa$ von der obigen Form

$$\varkappa = x_1\Theta^2 + x_2\Theta + x_3$$

geht durch die erste, die identische Permutation in sich selbst, durch die zweite und dritte in die konjugierten Zahlen $\varkappa' = x_1\Theta'^2 + x_2\Theta' + x_3$ und $\varkappa'' = x_1\Theta''^2 + x_2\Theta'' + x_3$ über; ist $\varkappa' = u + vi$, wo u, v reelle Zahlen bedeuten, während $i = \sqrt{-1}$ ist, so ist $\varkappa'' = u - vi$.

§ 2.

Invarianten des Körpers K.

Jede von Null verschiedene rationale Zahl ∂ kann offenbar immer und nur auf eine einzige Weise in der Form

$$\partial = ab^2c^3$$

dargestellt werden, wo c rational ist, und a, b natürliche Zahlen bedeuten, deren Produkt ab durch kein Primzahlquadrat teilbar ist; da in unserem Falle ∂ nicht die dritte Potenz einer rationalen Zahl ist, so ist außerdem

$$ab > 1.$$

Setzt man nun $\Theta = c\alpha$, so wird die positive Zahl $\alpha = \sqrt[3]{ab^2}$, und da α irrational und in K enthalten ist, so ist auch $K = R(\alpha)$; da ferner $\alpha^2 = \sqrt[3]{a^2b^4} = b\sqrt[3]{a^2b}$ ist, so wird, wenn man $\sqrt[3]{a^2b} = \beta$ setzt,

$$\alpha^2 = b\beta,\quad \beta^2 = a\alpha,\quad \alpha\beta = ab;$$
$$\alpha^3 = ab^2,\quad \beta^3 = a^2b,$$

und die allgemeine Form aller in K enthaltenen Zahlen $\varkappa$ ist:

$$\varkappa = z + x\alpha + y\beta,$$

wo z, x, y beliebige Zahlen in R bedeuten.

Die mit α und die mit β konjugierten Zahlen α', α'' und β', β'' ergeben sich aus

$$c\alpha = \Theta, \quad c\alpha' = \Theta' = \Theta\varrho = c\alpha\varrho, \quad c\alpha'' = \Theta'' = \Theta\varrho^2 = c\alpha\varrho^2$$

und aus

$$ab = \alpha\beta = \alpha'\beta' = \alpha''\beta'',$$

nämlich

$$\alpha' = \alpha\varrho, \quad \alpha'' = \alpha\varrho^2, \quad \beta' = \beta\varrho^2, \quad \beta'' = \beta\varrho,$$

und hieraus folgt allgemein

$$\varkappa' = z + x\alpha\varrho + y\beta\varrho^2, \quad \varkappa'' = z + x\alpha\varrho^2 + y\beta\varrho$$

oder

$$\varkappa' = (x\alpha - z)\varrho + (y\beta - z)\varrho^2; \quad \varkappa'' = (x\alpha - z)\varrho^2 + (y\beta - z)\varrho.$$

Für das Supplement und die Norm der Zahl $\varkappa$ erhält man daher (nach D. § 176, S. 542 und § 167, S. 486) die Darstellungen

$$\begin{aligned}\varkappa'\varkappa'' &= (x\alpha - z)^2 - (x\alpha - z)(y\beta - z) + (y\beta - z)^2 \\ &= (z^2 - abxy) + (ay^2 - zx)\alpha + (bx^2 - zy)\beta\end{aligned}$$

und

$$N(\varkappa) = \varkappa\varkappa'\varkappa'' = z^3 - 3abzxy + ab^2x^3 + a^2by^3.$$

Wir stellen uns jetzt die Aufgabe, alle diejenigen Zahlen $\varkappa$ in K zu finden, deren dritte Potenz rational ist. Nehmen wir an, es sei $\varkappa^3 = e$, wo e eine rationale Zahl bedeutet, so folgt auch $\varkappa'^3 = e$, also muß

$$\varkappa' = \varkappa \quad \text{oder} \quad \varkappa' = \varkappa\varrho \quad \text{oder} \quad \varkappa' = \varkappa\varrho^2$$

sein; da aber allgemein

$$\begin{aligned}\varkappa' - \varkappa &= (1 - \varrho^2)(x\alpha\varrho - y\beta), \\ \varkappa' - \varkappa\varrho &= (1 - \varrho)(z - y\beta\varrho), \\ \varkappa' - \varkappa\varrho^2 &= (\varrho^2 - \varrho)(z\varrho - x\alpha),\end{aligned}$$

und außerdem die Zahl ϱ nicht in K enthalten ist, so muß im ersten, zweiten, dritten Falle entsprechend

$$\begin{aligned} &x = y = 0, \quad \varkappa = z, \quad e = z^3, \\ &z = y = 0, \quad \varkappa = x\alpha, \quad e = ab^2x^3, \\ &z = x = 0, \quad \varkappa = y\beta, \quad e = a^2by^3 \end{aligned}$$

sein. Im ersten Falle ist $\varkappa$ rational, also $R(\varkappa) = R$, und dasselbe gilt auch für den zweiten und dritten Fall, wenn x bzw. $y = 0$ ist;

in allen diesen Fällen ist e die dritte Potenz einer rationalen Zahl. Soll also die Zahl $\varkappa$ (ebenso wie Θ) die Kubikwurzel aus einer rationalen Zahl e sein, welche (wie ∂) nicht die dritte Potenz einer rationalen Zahl ist, so geschieht dies nur im zweiten oder dritten Falle, wenn x bzw. y von Null verschieden gewählt wird, und gleichzeitig wird $R(\varkappa) = K$; vergleicht man ferner die Formen $e = ab^2x^3$, $e = ba^2y^3$ der Zahl e mit der Form $\partial = ab^2c^3$, so ergibt sich, daß alle diese irrationalen Zahlen $\varkappa$ des Körpers K, deren dritte Potenz e rational ist, auf dasselbe Paar a, b oder b, a führen. Wir nennen daher diese beiden natürlichen Zahlen a, b, durch welche der reine kubische Körper K vollständig bestimmt ist, die Invarianten des Körpers K.

Nr.	ab	a	b	ab^2	a^2b	k	k''	h
1	2	2	1	2	4	6	1	1
2	3	3	1	3	9	9	1	1
3	5	5	1	5	25	15	2	1
4	6	6	1	6	36	18	3	1
5	6	3	2	12	18	18	3	1
6	7	7	1	7	49	21	2	3
(7)	10	10	1	10	100	10	2	1
8	10	5	2	20	50	30	6	3
9	11	11	1	11	121	33	4	2
10	13	13	1	13	169	39	4	3
11	14	14	1	14	196	42	6	3
(12)	14	7	2	28	98	14	2	3
13	15	15	1	15	225	45	6	2
14	15	5	3	45	75	45	6	1
(15)	17	17	1	17	289	17	2	1
(16)	19	19	1	19	361	19	2	3
17	21	21	1	21	441	63	6	3
18	21	7	3	63	147	63	6	6
19	22	22	1	22	484	66	12	3
(20)	22	11	2	44	242	22	4	1
21	23	23	1	23	529	69	8	1

Da der Körper K durch Vertauschung von a mit b nicht geändert wird, so kann man, um alle reinen kubischen Körper K und jeden nur einmal zu erhalten, so verfahren: man betrachte alle natürlichen Zahlen, welche > 1 und durch kein Primzahlquadrat teilbar sind, und zerlege jede auf alle Arten in zwei Faktoren a, b, von denen a der größere ist; bezeichnet man dann mit α und β die positiven Kubikwurzeln aus ab^2 und a^2b, so ist $R(\alpha) = R(\beta)$ ein reeller reiner kubischer Körper K, zu welchem jedesmal zwei konjugierte imaginäre reine kubische Körper K', K'' gehören. Hier folgt der Anfang einer solchen Tabelle (siehe S. 153) aller reinen kubischen Körper K; die in ihr auftretenden Spalten k und k'' werden später (§§ 3, 4, 9) erklärt werden, und h bedeutet die Anzahl der Idealklassen des Körpers.

§ 3.

Die in $3\,ab$ aufgehenden Primideale.

Es sei $\mathfrak{o}$ die Hauptordnung des Körpers K, d. h. der Inbegriff aller in ihm enthaltenen g a n z e n algebraischen Zahlen, und

$$\Delta(\mathfrak{o}) = D$$

die Diskriminante oder Grundzahl von K (D. § 175, S. 538). Um $\mathfrak{o}$ und D zu bestimmen, betrachten wir zunächst den Modul

$$\mathfrak{n} = [1, \alpha, \beta],$$

d. h. den Inbegriff aller derjenigen Zahlen $\varkappa = z + x\alpha + y\beta$, welche durch beliebige g a n z e rationale Zahlen z, x, y erzeugt werden; da die Basiszahlen 1, α, β ganze (algebraische) Zahlen sind, so gilt dasselbe von allen diesen Zahlen $\varkappa$, d. h. der Modul $\mathfrak{n}$ ist teilbar durch den Modul $\mathfrak{o}$, was in Zeichen durch $\mathfrak{n} > \mathfrak{o}$ oder $(\mathfrak{n}, \mathfrak{o}) = 1$ ausgedrückt wird (D. § 171, S. 510); zugleich ist

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

wo $(\mathfrak{o}, \mathfrak{n})$ die Anzahl der nach dem Modul $\mathfrak{n}$ inkongruenten Zahlen in $\mathfrak{o}$ bedeutet (D. § 175, S. 539). Zufolge der Definition der Diskriminante eines Moduls (D. § 175, S. 536) ist nun $\Delta(\mathfrak{n})$ das Quadrat der Determinante

$$\begin{vmatrix} 1, \alpha, & \beta \\ 1, \alpha', & \beta' \\ 1, \alpha'', & \beta'' \end{vmatrix} = \begin{vmatrix} 1, \alpha, & \beta \\ 1, \alpha\varrho, & \beta\varrho^2 \\ 1, \alpha\varrho^2, & \beta\varrho \end{vmatrix} = 3\,\alpha\beta\,(\varrho^2 - \varrho),$$

und da $\alpha\beta = ab$, und $(\varrho^2 - \varrho)^2 = -3$ ist, so ergibt sich

$$\Delta(\mathfrak{n}) = -3\,(3\,ab)^2;$$

aus der Vergleichung mit der obigen Form von $\Delta(\mathfrak{n})$ folgt, daß die Anzahl $(\mathfrak{o}, \mathfrak{n})$ ein Divisor von $3\,ab$, also

$$3\,ab = k\,(\mathfrak{o}, \mathfrak{n}),\ D = -3\,k^2$$

ist, wo k eine natürliche Zahl bedeutet. Die Bestimmung dieser für alles Folgende sehr wichtigen Zahl k wird erleichtert, wenn wir vorher alle in $3\,ab$ aufgehenden Primideale des Körpers K aufsuchen, unter welchen sich jedenfalls auch alle in der Grundzahl D aufgehenden

Primideale befinden; mit dieser ohnehin unerläßlichen Aufgabe wollen wir uns daher jetzt beschäftigen.

Betrachten wir zunächst ein in a aufgehendes Primideal $\mathfrak{p}$, so muß die durch $\mathfrak{p}$ teilbare natürliche Primzahl p, welche zugleich die kleinste in $\mathfrak{p}$ enthaltene natürliche Zahl ist (D. § 179, S. 563), ebenfalls in a aufgehen, und da ab nicht durch p^2 teilbar ist, so wird

$$\alpha^3 = ab^2 = pq,$$

wo q nicht durch p, also auch nicht durch $\mathfrak{p}$ teilbar ist; da nun $\mathfrak{p}$ in p, pq, α^3, also auch in α aufgeht, so muß $\mathfrak{p}^3$ in pq, also auch in p aufgehen; nach einem allgemeinen, aus der Betrachtung der Normen folgenden Satze kann aber die Anzahl der (gleichen oder verschiedenen) Primideale, deren Produkt $= \mathfrak{o}p$ ist, nicht größer als der Grad des Körpers, in unserem Falle also nicht größer als 3 sein; mithin ist

$$\mathfrak{o}p = \mathfrak{p}^3, \quad N(\mathfrak{p}) = (\mathfrak{o}, \mathfrak{p}) = p,$$

d. h. $\mathfrak{o}p$ ist die dritte Potenz eines Primideals $\mathfrak{p}$ vom ersten Grade (D. § 180, S. 565). Ganz dasselbe gilt offenbar für alle in b aufgehenden natürlichen Primzahlen p und Primideale $\mathfrak{p}$.

Ein anderer Weg, um zu dem vorstehenden Resultate zu gelangen, stützt sich auf die Multiplikation und Reduktion der endlichen Moduln (D. § 170, S. 502 und § 172, S. 519); wir wollen ihn kurz andeuten, seine nähere Ausführung aber, weil sie keine Schwierigkeit darbietet, dem Leser überlassen. Jeder natürliche Divisor m von ab hat die Form $m = a_1 b_1$, wo a_1 Divisor von a, b_1 Divisor von b ist; betrachtet man nun den Modul

$$\mathfrak{m} = [m, \alpha, \beta],$$

so findet man leicht

$$\mathfrak{m}^2 = [m, a_1\alpha, b_1\beta], \ \mathfrak{m}^3 = m\mathfrak{n};$$

da nun $\mathfrak{o}\mathfrak{n} = \mathfrak{o}$ ist, weil $\mathfrak{n}$ die Zahl 1 enthält, so ergibt sich

$$\mathfrak{o}m = (\mathfrak{o}\mathfrak{m})^3,$$

wo $\mathfrak{o}\mathfrak{m}$ offenbar ein Ideal ist. Als spezieller Fall entspringt hieraus für das oben mit $\mathfrak{p}$ bezeichnete Primideal die Darstellung

$$\mathfrak{p} = \mathfrak{o}[p, \alpha, \beta].$$

Unsere Aufgabe, alle in $3ab$ aufgehenden Primideale zu finden, ist durch das Vorstehende offenbar erledigt, wenn ab durch 3 teilbar ist; im entgegengesetzten Falle, wo

$$a^2 \equiv b^2 \equiv 1 \pmod{3},$$

kommt es aber noch darauf an, die Zerlegung von $\mathfrak{o}\,3$ in Primideale zu finden, und hierbei werden wir auf eine wichtige Einteilung aller reinen kubischen Körper K in zwei verschiedene Arten geführt werden. Hierzu betrachten wir die irrationale ganze Zahl

$$\mu = \alpha - a,$$

welche zufolge $\alpha^3 = a b^2$ der irreduziblen Gleichung

$$\mu^3 + 3\,a\,\mu^2 + 3\,a^2\,\mu + a(a^2 - b^2) = 0$$

genügt. Da der Koeffizient $3\,a^2$ von μ im dritten Gliede nicht durch 9 teilbar ist, so kann μ nicht durch 3 teilbar sein (D. § 173, S. 531), aber das erste Glied μ^3 ist durch 3 teilbar, weil dies von allen folgenden Gliedern gilt. Aus der Existenz einer durch 3 nicht teilbaren Zahl μ, deren dritte Potenz durch 3 teilbar ist, folgt bekanntlich, daß $\mathfrak{o}\,3$ nicht ein Produkt von lauter verschiedenen Primidealen, sondern durch das Quadrat eines Primideals $\mathfrak{p}$ teilbar ist; setzt man demgemäß

$$\mathfrak{o}\,3 = \mathfrak{p}^2\,\mathfrak{p}_1,$$

so folgt aus der Betrachtung der Normen leicht, daß $\mathfrak{p}$ und $\mathfrak{p}_1$ Primideale ersten Grades sind; denn wenn man $N(\mathfrak{p}) = 3^m$, $N(\mathfrak{p}_1) = 3^n$ setzt, wo $m \geqq 1$, $n \geqq 0$, so folgt $N(\mathfrak{o}\,3) = 3^3 = 3^{2m+n}$, also $3 = 2m + n$, mithin $m = n = 1$; es ist daher

$$N(\mathfrak{p}) = N(\mathfrak{p}_1) = 3,$$

und folglich ist auch $\mathfrak{p}_1$ ein Primideal. Aber nun entsteht die Frage, ob $\mathfrak{p}_1$ identisch mit $\mathfrak{p}$ ist oder nicht; hierauf antwortet der folgende

Satz: Die in der Zerlegung $\mathfrak{o}\,3 = \mathfrak{p}^2\,\mathfrak{p}_1$ auftretenden Primideale ersten Grades $\mathfrak{p}$, $\mathfrak{p}_1$ sind gleich oder verschieden, je nachdem $a^2 - b^2$ unteilbar oder teilbar durch 9 ist.

Zum Beweise benutzen wir die obige kubische Gleichung, welche zufolge $\mu + a = \alpha$ die Form

$$\mu^3 + 3\,a\,\alpha\,\mu + a(a^2 - b^2) = 0$$

annimmt, und bezeichnen mit r den Exponenten der höchsten in $(a^2 - b^2)$ aufgehenden Potenz von 3, welcher jedenfalls $\geqq 1$ ist, während a und α relative Primzahlen zu 3 sind. Ist nun erstens $\mathfrak{p} = \mathfrak{p}_1$, also $\mathfrak{o}\,3 = \mathfrak{p}^3$, und $\mathfrak{p}^s$ die höchste in μ aufgehende Potenz von $\mathfrak{p}$, so ist $1 \leqq s \leqq 2$, weil μ durch $\mathfrak{p}$, aber nicht durch 3 teilbar ist, und die Exponenten der höchsten in μ^3, $3\,a\,\alpha\,\mu$, $a(a^2 - b^2)$ aufgehenden Potenzen von $\mathfrak{p}$ sind der Reihe nach $3\,s$, $3 + s$, $3\,r$. Die beiden ersteren sind voneinander verschieden, weil $3+s$ nicht durch 3 teilbar ist, und da der kleinere von ihnen zufolge der obigen Gleichung mit dem dritten $3r$ übereinstimmen muß, so ergibt sich $3r = 3s < 3+s \leqq 5$, also $r = s = 1$, mithin ist $(a^2 - b^2)$ nicht durch 9, und μ nicht durch $\mathfrak{p}^2$ teilbar. Ist aber zweitens $\mathfrak{p}$ verschieden von $\mathfrak{p}_1$, also $\mathfrak{o}\,3 = \mathfrak{p}^2\mathfrak{p}_1$ nicht teilbar durch $\mathfrak{p}_1^2$, so ist $\mathfrak{p}_1^r$ die höchste in $(a^2 - b^2)$ aufgehende Potenz von $\mathfrak{p}_1$; da nun μ^3 durch 3, also μ gewiß durch $\mathfrak{p}_1$ teilbar ist, so sind die Zahlen μ^3, $3a\alpha\mu$ mindestens durch $\mathfrak{p}_1^2$ teilbar; zufolge der obigen Gleichung muß daher auch $(a^2 - b^2)$ durch $\mathfrak{p}_1^2$ teilbar sein, mithin ist $r \geqq 2$, also $(a^2 - b^2)$ teilbar durch 9. — Die beiden einander ausschließenden Annahmen über $\mathfrak{p}$ und $\mathfrak{p}_1$, welche alle Fälle erschöpfen, führen also zu zwei Folgerungen über die Zahl $(a^2 - b^2)$, welche ebenfalls einander ausschließen und alle Fälle erschöpfen; mithin muß umgekehrt $\mathfrak{p} = \mathfrak{p}_1$ oder $\mathfrak{p}$ von $\mathfrak{p}_1$ verschieden sein, je nachdem $(a^2 - b^2)$ unteilbar oder teilbar durch 9 ist, w. z. b. w.

An den vorstehenden Satz knüpfen wir noch die folgenden Bemerkungen. Obgleich derselbe nur für den Fall ausgesprochen und bewiesen ist, wo ab nicht durch 3 teilbar ist, so umfaßt er doch offenbar auch den schon vorher erledigten Fall, wo ab durch 3 teilbar ist, weil dann ebenfalls $\mathfrak{o}\,3 = \mathfrak{p}^3$, und $a^2 - b^2$ nicht einmal durch 3, geschweige durch 9 teilbar ist. Wir teilen daher alle reinen kubischen Körper K nach dem Verhalten der Zahl 3 in zwei Arten ein und nennen K einen Körper erster oder zweiter Art, je nachdem $a^2 - b^2$ unteilbar oder teilbar durch 9 ist, oder — was nach dem Vorstehenden hiermit gleichbedeutend ist — je nachdem die in der Zerlegung $\mathfrak{o}\,3 = \mathfrak{p}^2\mathfrak{p}_1$ auftretenden Primideale $\mathfrak{p}$, $\mathfrak{p}_1$ gleich oder verschieden sind.

Hierauf wollen wir den Fall eines Körpers K von zweiter Art noch etwas näher betrachten; dann kann man

$$a^2 \equiv b^2 \equiv 1 - 3c \pmod{9}$$

setzen, wo c eine nach dem Modul 3 bestimmte ganze rationale Zahl bedeutet. Da das Produkt $a^2 - b^2$ der beiden Faktoren $a \pm b$ durch 9 teilbar, ihre Summe $2a$ aber unteilbar durch 3 ist, so können sie nicht beide durch 3 teilbar sein, und folglich muß einer von ihnen durch 9 teilbar sein; mithin ist

$$a \equiv \pm b \pmod{9},$$

und umgekehrt folgt hieraus, daß K ein Körper zweiter Art ist. Unter den 21 Körpern der Tabelle am Schlusse von § 2 sind daher die 5 durch Einklammerung ihrer Nummern (7), (12), (15), (16), (20) kenntlich gemachten Körper von zweiter, die übrigen 16 von erster Art. Wir wollen nun darauf ausgehen, die beiden in 3 aufgehenden Primideale $\mathfrak{p}$, $\mathfrak{p}_1$ deutlich zu unterscheiden. Da die dritte Potenz der Zahl $\mu = \alpha - a$ durch 3 teilbar ist, so muß μ durch $\mathfrak{p}\mathfrak{p}_1$, also μ^2 durch $\mathfrak{p}^2\mathfrak{p}_1^2 = 3\,\mathfrak{p}_1$, mithin auch durch 3 teilbar sein; nun ist aber

$$\mu^2 = (\alpha - a)^2 = \alpha^2 - 2\,a\alpha + a^2 = b\beta - 2\,a\alpha + a^2$$
$$= (1 + a\alpha + b\beta) + (a^2 - 1 - 3\,a\alpha),$$

und da der zweite eingeklammerte Bestandteil offenbar durch 3 teilbar ist, so gilt dasselbe auch von dem ersten; setzen wir daher

$$\gamma = \frac{1 + a\alpha + b\beta}{3},$$

so ist γ eine ganze Zahl; durch Einführung derselben geht die obige Gleichung, weil $a^2 - 1 \equiv -3\,c \pmod{9}$ ist, in die Kongruenz

$$\mu^2 \equiv 3(\gamma - c - a\alpha) \pmod{9}$$

über, und da die Zahlen μ^2 und 9 durch $3\,\mathfrak{p}_1$ teilbar sind, so folgt $\gamma \equiv c + a\alpha \pmod{\mathfrak{p}_1}$; da ferner $\mu = \alpha - a$ durch $\mathfrak{p}_1$ teilbar, also $\alpha \equiv a$, $a\alpha \equiv a^2 \equiv 1 \pmod{\mathfrak{p}_1}$ ist, so ergibt sich

$$\gamma \equiv c + 1 \pmod{\mathfrak{p}_1}.$$

Um eine ähnliche Kongruenz für das andere Primideal $\mathfrak{p}$ zu erhalten, setze man die kubische Gleichung, deren Wurzel μ ist, in die Form

$$\mu(\mu^2 + 3\,a\alpha) + a(a^2 - b^2) = 0;$$

da $a^2 - b^2$ durch 9, also durch $\mathfrak{p}^4$ teilbar ist, so folgt hieraus die Kongruenz

$$\mu(\mu^2 + 3\,a\alpha) \equiv 0 \pmod{\mathfrak{p}^4};$$

nun ist μ zwar durch $\mathfrak{p}\mathfrak{p}_1$, aber nicht durch $\mathfrak{p}^2$ teilbar (weil sonst μ durch $\mathfrak{p}^2\mathfrak{p}_1$, also durch 3 teilbar wäre), mithin

$$\mu^2 + 3\,a\alpha \equiv 0 \pmod{\mathfrak{p}^3};$$

vergleicht man dies mit der obigen Kongruenz

$$\mu^2 + 3\,a\alpha \equiv 3(\gamma - c) \pmod{9},$$

welche, weil 9 durch $\mathfrak{p}^4$ teilbar ist, auch für den Modul $\mathfrak{p}^3$ gilt, so folgt, daß $3(\gamma - c)$ durch $\mathfrak{p}^3$ teilbar ist, und da 3 zwar durch $\mathfrak{p}^2$, aber nicht durch $\mathfrak{p}^3$ teilbar ist, so ergibt sich die gesuchte Kongruenz

$$\gamma \equiv c \pmod{\mathfrak{p}}.$$

Besonders hervorzuheben ist aber noch das obige Resultat, daß es in jedem Körper zweiter Art eine ganze Zahl γ gibt, welche nicht in dem Modul $\mathfrak{n}$ enthalten ist; hieraus folgt, daß die Hauptordnung $\mathfrak{o}$ ein echter Teiler von $\mathfrak{n}$, also $(\mathfrak{o}, \mathfrak{n}) > 1$ ist.

§ 4.

Die Grundzahl D.

Mit Hilfe der eben geführten Untersuchung über die in $3ab$ aufgehenden Primideale gelingt es nun ohne Schwierigkeit, die Hauptordnung $\mathfrak{o}$ jedes reinen kubischen Körpers K und hiermit seine Grundzahl D sowie die in den Gleichungen

$$3ab = k(\mathfrak{o}, \mathfrak{n}), \quad D = -3k^2$$

auftretenden natürlichen Zahlen k und $(\mathfrak{o}, \mathfrak{n})$ zu bestimmen. Nach einem allgemeinen Satze der Modultheorie (D. § 171, I., S. 511) ist $\mathfrak{o}(\mathfrak{o}, \mathfrak{n}) > \mathfrak{n}$, d. h. jede Zahl des Moduls $\mathfrak{o}$ wird durch Multiplikation mit $(\mathfrak{o}, \mathfrak{n})$ in eine Zahl des Moduls $\mathfrak{n}$ verwandelt. Bedeutet daher ω jede beliebige ganze Zahl des Körpers K, d. h. jede in $\mathfrak{o}$ enthaltene Zahl, so wird $(\mathfrak{o}, \mathfrak{n})\omega$, also auch $k(\mathfrak{o}, \mathfrak{n})\omega = 3ab\omega$ in dem Modul $\mathfrak{n}$ enthalten sein, und folglich ist

$$3ab\omega = z + x\alpha + y\beta,$$

wo z, x, y ganze rationale Zahlen bedeuten; um daher alle Zahlen ω zu finden, haben wir alle Systeme z, x, y zu suchen, für welche

$$z + x\alpha + y\beta \equiv 0 \pmod{3ab}$$

wird. Bedeutet nun zunächst p eine in a aufgehende natürliche Primzahl, so ist, wie in § 3 gezeigt ist, $\mathfrak{o}p = \mathfrak{p}^3$, und da $\alpha^3 = ab^2$, $\beta^3 = a^2b$ ist, so leuchtet ein, daß $\mathfrak{p}$ die höchste in α, und $\mathfrak{p}^2$ die höchste in β aufgehende Potenz des Primideals $\mathfrak{p}$ ist. Aus der Kongruenz

$$z + x\alpha + y\beta \equiv 0 \pmod{\mathfrak{p}^3}$$

folgt daher zunächst $z \equiv 0 \pmod{\mathfrak{p}}$, mithin muß z als rationale Zahl auch durch p, also durch $\mathfrak{p}^3$ teilbar sein (D. § 179, S. 563), und hierdurch kommt die vorstehende Kongruenz auf

$$x\alpha + y\beta \equiv 0 \pmod{\mathfrak{p}^3}$$

zurück. Aus dieser Kongruenz folgt wieder $x\alpha \equiv 0$ (mod. $\mathfrak{p}^2$), und da α nicht durch $\mathfrak{p}^2$ teilbar ist, so muß die rationale Zahl x durch $\mathfrak{p}$, also auch durch p teilbar sein. Hierdurch reduziert sich unsere Kongruenz auf $y\beta \equiv 0$ (mod. $\mathfrak{p}^3$), und da β nicht durch $\mathfrak{p}^3$ teilbar ist, so muß auch die rationale Zahl y durch $\mathfrak{p}$, also auch durch p teilbar sein. Mithin sind alle drei Zahlen z, x, y durch p teilbar.

Offenbar gilt ganz dasselbe für jede in b, also für jede in ab aufgehende natürliche Primzahl p, und da ab ein Produkt von lauter verschiedenen Primzahlen p ist, so müssen die ganzen rationalen Zahlen z, x, y alle durch ab teilbar, also von der Form

$$z = abw, \quad x = abu, \quad y = abv$$

sein, wo w, u, v wieder ganze rationale Zahlen bedeuten; zugleich wird

$$3\omega = w + u\alpha + v\beta,$$

mithin ist $\mathfrak{o}3 > \mathfrak{n}$, d. h. jede ganze Zahl ω wird schon durch Multiplikation mit 3 in eine Zahl des Moduls $\mathfrak{n}$ verwandelt.

Ist nun ab teilbar durch 3, gehört also die Zahl 3 zu den eben betrachteten Primzahlen p, so müssen auch die Zahlen w, u, v durch 3 teilbar sein, mithin ist jede Zahl ω auch in $\mathfrak{n}$ enthalten, d. h. es ist $\mathfrak{o} = \mathfrak{n}$, $(\mathfrak{o}, \mathfrak{n}) = 1$, $k = 3ab$. Betrachten wir ferner den anderen Fall, in welchem K ebenfalls ein Körper erster Art, also $a^2 \equiv b^2 \equiv 1$ (mod. 3), aber $a^2 - b^2$ nicht durch 9 teilbar ist, so ist (nach § 3) auch jetzt $\mathfrak{o}3 = \mathfrak{p}^3$, und die Zahl $\mu = \alpha - a$ ist durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar. Multipliziert man nun mit b und bedenkt, daß $b\beta = \alpha^2 = (\mu + a)^2$ ist, so wird

$$\begin{aligned} 3b\omega &= bw + bu(\mu + a) + v(\mu + a)^2 \\ &= x_0 + x_1\mu + x_2\mu^2, \end{aligned}$$

wo die Zahlen

$$x_0 = bw + abu + a^2v, \quad x_1 = bu + 2av, \quad x_2 = v$$

ebenfalls ganze rationale Zahlen sind und der Kongruenz

$$x_0 + x_1\mu + x_2\mu^2 \equiv 0 \quad (\text{mod. } \mathfrak{p}^3)$$

genügen; da aber $\mathfrak{p}$ und $\mathfrak{p}^2$ die höchsten bzw. in μ und μ^2 aufgehenden Potenzen von $\mathfrak{p}$ sind, so ergibt sich ebenso wie oben, daß die Zahlen x_0, x_1, x_2 der Reihe nach durch $\mathfrak{p}$, also auch durch 3 teilbar sind, und hieraus folgt offenbar, daß auch die Zahlen v, u, w der Reihe nach durch 3 teilbar sind; mithin ist auch in diesem Falle jede Zahl ω in dem Modul $\mathfrak{n}$ enthalten, und es gilt folglich der

Satz. Ist K ein Körper erster Art, so ist

$$\mathfrak{o} = \mathfrak{n} = [1, \alpha, \beta],$$
$$k = 3ab, \quad D = -3k^2.$$

Zugleich ergibt sich für diesen Fall, wie der Leser aus § 3 leicht ableiten wird, die folgende Darstellung aller in der Grundzahl D aufgehenden Primideale $\mathfrak{p}$. Geht $\mathfrak{p}$ in ab auf, so ist

$$\mathfrak{p} = [p, \alpha, \beta],$$

wo p wieder die durch $\mathfrak{p}$ teilbare natürliche Primzahl bedeutet; geht aber $\mathfrak{p}$ nicht in ab auf, ist also $p = 3$, und ab nicht teilbar durch 3, so ist

$$\mathfrak{p} = [3, \alpha - a, \beta - b].$$

Hierauf wenden wir uns zu den Körpern K von zweiter Art, also zu den Körpern K, welche durch die Kongruenz $a \equiv \pm b$ (mod. 9) charakterisiert sind, woraus zugleich folgt, daß ab nicht durch 3 teilbar ist. Wir haben schon am Schlusse von § 3 hervorgehoben, daß in diesem Falle die Hauptordnung $\mathfrak{o}$ ein echter Teiler des Moduls $\mathfrak{n}$, also $(\mathfrak{o}, \mathfrak{n}) > 1$ ist; da ferner in dem gegenwärtigen § 4 bewiesen ist, daß der Modul $\mathfrak{n}$ immer ein Teiler des Hauptideals $\mathfrak{o}\,3$ ist, so ist nach zwei allgemeinen Sätzen der Modul- und Idealtheorie (D. § 171, S. 510 und § 180, S. 564)

$$(\mathfrak{o}, \mathfrak{n})(\mathfrak{n}, \mathfrak{o}\,3) = (\mathfrak{o}, \mathfrak{o}\,3) = N(\mathfrak{o}\,3) = N(3) = 3^3,$$

also ist $(\mathfrak{o}, \mathfrak{n})$ eine der Potenzen $3, 3^2, 3^3$; zufolge § 3 ist aber auch $3ab = k(\mathfrak{o}, \mathfrak{n})$, und da ab nicht durch 3 teilbar ist, so ergibt sich $(\mathfrak{o}, \mathfrak{n}) = 3$, $k = ab$. Es ist nun auch leicht, die Hauptordnung $\mathfrak{o}$ als endlichen Modul darzustellen. Zu diesem Zwecke erinnern wir an das in § 3 gewonnene Resultat, daß die in $\mathfrak{n}$ nicht enthaltene Zahl

$$\gamma = \frac{1 + a\alpha + b\beta}{3}$$

eine ganze Zahl, also in $\mathfrak{o}$ enthalten ist; setzen wir daher

$$\mathfrak{o}_1 = \mathfrak{n} + [\gamma] = [1, \alpha, \beta, \gamma],$$

so ist der Modul $\mathfrak{o}_1$ ein Vielfaches von $\mathfrak{o}$ und zugleich ein Teiler von $\mathfrak{n}$ (nämlich der größte gemeinsame Teiler von $\mathfrak{n}$ und $[\gamma]$), und hieraus folgt nach dem schon vorher benutzten Modulsatze

$$(\mathfrak{o}, \mathfrak{o}_1)(\mathfrak{o}_1, \mathfrak{n}) = (\mathfrak{o}, \mathfrak{n}) = 3;$$

da endlich die in $\mathfrak{o}_1$ enthaltene Zahl γ nicht in $\mathfrak{n}$ enthalten, also $\mathfrak{o}_1$ ein echter Teiler von $\mathfrak{n}$, mithin $(\mathfrak{o}_1, \mathfrak{n}) > 1$ ist, so folgt*), daß $(\mathfrak{o}_1, \mathfrak{n}) = 3$, $(\mathfrak{o}, \mathfrak{o}_1) = 1$, also $\mathfrak{o} = \mathfrak{o}_1$ sein muß, womit die gesuchte Darstellung von $\mathfrak{o}$ gefunden ist. Bedenkt man noch, daß $1 = 3\gamma - a\alpha - b\beta$ ist, so leuchtet ein, daß $\mathfrak{o}$ auch als dreigliedriger Modul $[\gamma, \alpha, \beta]$ darstellbar ist. Das Resultat unserer Untersuchung besteht daher in dem folgenden

Satz. Ist K ein Körper zweiter Art, so ist

$$\mathfrak{o} = \mathfrak{n} + [\gamma] = [1, \alpha, \beta, \gamma] = [\gamma, \alpha, \beta],$$
$$k = ab, \quad D = -3k^2.$$

Auch für diesen Fall läßt sich die Darstellung der in D aufgehenden Primideale $\mathfrak{p}$ in Form von endlichen Moduln leicht aus § 3 ableiten; da sie aber für den weiteren Verlauf unserer Untersuchung nicht erforderlich ist, so begnügen wir uns, die Resultate kurz anzugeben. Geht die durch $\mathfrak{p}$ teilbare natürliche Primzahl p in ab auf, so ist

$$\mathfrak{p} = [p\gamma, \alpha, \beta] = \mathfrak{o}[p, \alpha, \beta];$$

ist aber $p = 3$, so findet man für die in der Zerlegung $\mathfrak{o}3 = \mathfrak{p}^2\mathfrak{p}_1$ auftretenden Primideale $\mathfrak{p}$, $\mathfrak{p}_1$ und deren Produkt die Darstellungen

$$\mathfrak{p}\mathfrak{p}_1 = [3, \alpha - a, \beta - b],$$
$$\mathfrak{p} = \mathfrak{p}\mathfrak{p}_1 + [\gamma - c] = [3, \gamma - c, \alpha - a, \beta - b],$$
$$\mathfrak{p}_1 = \mathfrak{p}\mathfrak{p}_1 + [\gamma - c - 1] = [3, \gamma - c - 1, \alpha - a, \beta - b],$$

und das Produkt $\mathfrak{p}\mathfrak{p}_1$ ist zugleich der Führer der Ordnung $\mathfrak{n}$, d. h. der Quotient $\mathfrak{n} : \mathfrak{o}$ oder auch der größte gemeinsame Teiler aller in der Ordnung $\mathfrak{n}$ enthaltenen Ideale (D. § 180, S. 572).

Nachdem in allen Fällen gezeigt ist, wie die Grundzahl $D = -3k^2$ von den beiden Invarianten a, b abhängt, bemerken wir zum Schluß, daß — im Gegensatz zu der Theorie der quadratischen Körper — der reine kubische Körper K oder vielmehr das System der drei konjugierten Körper K, K', K'' offenbar durch die gemeinsame Grundzahl D im allgemeinen noch nicht vollständig bestimmt ist; so z. B. tritt in den beiden Zeilen 4 und 5 der Tabelle (§ 2) derselbe Wert $k = 18$ auf, mithin haben die beiden gänzlich ver-

*) Diese Folgerung $(\mathfrak{o}_1, \mathfrak{n}) = 3$ bestätigt sich leicht durch die Bemerkung, daß die drei Zahlen 0, γ, 2γ offenbar ein Restsystem von $\mathfrak{o}_1$ nach $\mathfrak{n}$ bilden (D. § 171, S. 509).

schiedenen Körpersysteme K, K', K'', von denen das eine durch $\sqrt[3]{6}$, das andere durch $\sqrt[3]{12}$ erzeugt wird, dieselbe Grundzahl $D = -2^2 \cdot 3^5$, und ähnliches wiederholt sich in den Zeilen 13, 14 und in den Zeilen 17, 18 der Tabelle. Daß dieselbe Erscheinung auch bei Körpern zweiter Art auftritt, zeigt die Vergleichung des Invariantenpaars $a = 34 = 2 \cdot 17$, $b = 7$ mit dem Invariantenpaar $a = 119 = 7 \cdot 17$, $b = 2$, denen derselbe Wert $k = ab = 2 \cdot 7 \cdot 17$, also dieselbe Grundzahl $D = -3 \cdot 2^2 \cdot 7^2 \cdot 17^2$ entspricht, weil in beiden Fällen $a \equiv b \pmod{9}$ ist.

§ 5.

Die in der Grundzahl nicht aufgehenden Primideale.

Wir wenden uns jetzt zu der Aufgabe, auch alle diejenigen natürlichen Primzahlen p, welche nicht in der Grundzahl D aufgehen, in ihre idealen Primfaktoren $\mathfrak{p}$ zu zerlegen. Um die Körper von erster und zweiter Art gemeinsam zu behandeln, erinnern wir daran, daß (nach § 4) jede ganze Zahl ω in K durch Multiplikation mit 3 jedenfalls in eine Zahl des Moduls $\mathfrak{n} = [1, \alpha, \beta]$ verwandelt wird; da $p \equiv \pm 1 \pmod{3}$, so ist also auch das Produkt $(1 \mp p)\omega$, welches $\equiv \omega \pmod{p}$ ist, in $\mathfrak{n}$ enthalten, und man kann daher immer

$$\omega \equiv z + x\alpha + y\beta \pmod{p}$$

setzen, wo z, x, y ganze rationale Zahlen bedeuten. Durchläuft jede von ihnen ein bestimmtes System von p inkongruenten Zahlen (mod. p), so nimmt der Ausdruck rechter Hand p^3 verschiedene Werte ν an, und jede in $\mathfrak{n}$ enthaltene Zahl ist wenigstens einer dieser Zahlen ν kongruent (mod. p); zufolge der vorstehenden Kongruenz ist aber auch jede ganze, d. h. jede in $\mathfrak{o}$ enthaltene Zahl ω mit einer Zahl ν kongruent, und da die Anzahl $(\mathfrak{o}, \mathfrak{o}p)$ aller nach p inkongruenten Zahlen ω ebenfalls $= N(\mathfrak{o}p) = N(p) = p^3$ ist, so ergibt sich, daß die genannten Zahlen ν sämtlich inkongruent (mod. p) sind und folglich ein Restsystem von $\mathfrak{o}$ nach $\mathfrak{o}p$ bilden (D. § 180, S. 564); es kann daher auch nur dann $\omega \equiv 0 \pmod{p}$ werden, wenn $z \equiv x \equiv y \equiv 0 \pmod{p}$ ist*).

---

*) In der Zeichensprache der Modul- und Idealtheorie (D. § 169, S. 496, 498 und § 171, S. 510 und § 180, S. 564) drücken sich diese Beziehungen zwischen $\mathfrak{o}$, $\mathfrak{n}$ und p auf folgende Weise aus: $\mathfrak{n} + \mathfrak{o}p = \mathfrak{o}$, $\mathfrak{n} - \mathfrak{o}p = \mathfrak{n}p$, also $(\mathfrak{n}, \mathfrak{o}p) = (\mathfrak{n}, \mathfrak{n}p) = (\mathfrak{o}, \mathfrak{o}p) = N(p) = p^3$.

Benutzt man nun den für alle ganzen algebraischen Zahlen $\xi, \eta, \zeta \cdots$ geltenden Satz (D. § 185, S. 617)

$$(\xi + \eta + \zeta + \cdots)^p \equiv \xi^p + \eta^p + \zeta^p + \cdots \pmod{p}$$

und bedenkt, daß nach Fermat für jede ganze rationale Zahl z immer $z^p \equiv z \pmod{p}$ ist, so ergibt sich

$$\omega^p \equiv z + x\alpha^p + y\beta^p \pmod{p}$$

und durch Wiederholung dieses Verfahrens allgemein

$$\omega^{p^n} \equiv z + x\alpha^{p^n} + y\beta^{p^n} \pmod{p},$$

wo n jede natürliche Zahl bedeutet. Das Verhalten der Primzahl p ist nun ganz verschieden, je nachdem $p \equiv +1$ oder $p \equiv -1 \pmod{3}$ ist; wir trennen daher unsere Untersuchung in zwei Hauptteile und betrachten zuerst den einfacheren Fall

I. $$p = 3m - 1 \equiv -1 \pmod{3}.$$

Dann ist $p^2 - 1 = (p+1)(p-1) = 3m(p-1)$, und da ab nicht durch p teilbar ist, so folgt aus dem Satze von Fermat

$$\alpha^{p^2-1} = (ab^2)^{m(p-1)} \equiv 1 \pmod{p}$$

$$\beta^{p^2-1} = (a^2b)^{m(p-1)} \equiv 1 \pmod{p},$$

also

$$\alpha^{p^2} \equiv \alpha, \ \beta^{p^2} \equiv \beta \pmod{p},$$

und folglich genügt jede ganze Zahl ω des Körpers K der Kongruenz

$$\omega^{p^2} \equiv \omega \pmod{p}.$$

Hieraus folgt erstens, daß p durch kein Primidealquadrat teilbar sein kann; denn wenn in irgendeinem endlichen Körper jede ganze Zahl ω einer Kongruenz von der Form

$$\omega \equiv \lambda\omega^2 + \mu\omega^3 + \nu\omega^4 + \cdots \pmod{\mathfrak{a}}$$

genügt, wo $\mathfrak{a}$ ein bestimmtes Ideal und $\lambda, \mu, \nu \cdots$ bestimmte ganze Zahlen dieses Körpers sind, so müßte, wenn $\mathfrak{a}$ durch das Quadrat eines Primideals $\mathfrak{p}$ teilbar wäre, jede durch $\mathfrak{p}$ teilbare Zahl ω auch durch $\mathfrak{p}^2$ teilbar, d. h. es müßte $\mathfrak{p}$ selbst durch $\mathfrak{p}^2$ teilbar sein, was unmöglich ist.

Da ferner die Anzahl der inkongruenten Wurzeln ω der obigen Kongruenz $= (\mathfrak{o}, \mathfrak{o}p) = p^3$, also größer als ihr Grad p^2 ist, so folgt zweitens (D. § 180, S. 570), daß $\mathfrak{o}p$ selbst kein Primideal, also ein Produkt von zwei oder drei verschiedenen Primidealen ist. Im letzteren Falle müßten diese drei Primideale, weil das Produkt ihrer Normen $= N(\mathfrak{o}p) = p^3$ ist (D. § 180, S. 564), alle vom ersten Grade sein, es müßte daher (D. § 180, V, S. 570), wenn ω jede ganze Zahl bedeutet, $\omega^p - \omega$ durch jedes dieser Primideale, also auch durch ihr Produkt $\mathfrak{o}\,p$ teilbar sein; nun ist aber z. B. $\alpha^{p-2} = \alpha^{3(m-1)} = (a b^2)^{m-1}$ und $\alpha^2 = b\beta$, also $\alpha^p = g\beta$, wo g eine ganze rationale Zahl bedeutet, mithin ist die in $\mathfrak{n}$ enthaltene Zahl $\alpha - \alpha^p = \alpha - g\beta$ nicht durch p teilbar, und folglich unsere Annahme unzulässig. Das Resultat unserer Untersuchung besteht also darin, daß $\mathfrak{o}\,p$ ein Produkt von zwei verschiedenen Primidealen $\mathfrak{p}$, $\mathfrak{p}_1$ ist; offenbar muß das eine vom ersten, das andere vom zweiten Grade sein, und wir können daher

$$\mathfrak{o}\,p = \mathfrak{p}\,\mathfrak{p}_1, \quad N(\mathfrak{p}) = p, \quad N(\mathfrak{p}_1) = p^2$$

setzen. — Hierauf wenden wir uns zu dem Fall

II. $$p = 3m + 1 \equiv +1 \pmod{3}.$$

Dann hat bekanntlich (D. § 31, S. 73) die Kongruenz $u^3 \equiv 1 \pmod{p}$ drei inkongruente rationale Wurzeln $u \equiv 1, r, r^2$, wo

$$r^2 + r + 1 \equiv 0 \pmod{p}$$

ist; bedeutet ferner c irgendeine durch p nicht teilbare ganze rationale Zahl, so ist $c^{p-1} = c^{3m} \equiv 1 \pmod{p}$ und folglich $c^m \equiv r^e \pmod{p}$, wo der Exponent e nach dem Modul 3 bestimmt ist; je nachdem e durch 3 teilbar oder unteilbar ist, ist die Zahl c kubischer Rest oder Nichtrest von p, d. h. die Kongruenz $w^3 \equiv c \pmod{p}$ hat im ersten Fall drei inkongruente Wurzeln w, im letzteren gar keine.

Wendet man dies auf die Zahl $c = ab^2$ an und bedenkt, daß $(ab^2)(a^2b) = (ab)^3$ ist, so kann man gleichzeitig

$$(ab^2)^m \equiv r^e, \quad (a^2 b)^m \equiv r^{2e} \pmod{p}$$

setzen, und hieraus folgt

$$\left.\begin{array}{lll} \alpha^p \equiv \alpha r^e, & \alpha^{p^2} \equiv \alpha r^{2e}, & \alpha^{p^3} \equiv \alpha \\ \beta^p \equiv \beta r^{2e}, & \beta^{p^2} \equiv \beta r^e, & \beta^{p^3} \equiv \beta \end{array}\right\} \pmod{p},$$

mithin genügt jede ganze Zahl ω der Kongruenz

$$\omega^{p^3} \equiv \omega \pmod{p}.$$

Hieraus folgt wieder erstens, daß p durch kein Primidealquadrat teilbar ist. Wir wollen zweitens beweisen, daß p durch kein Primideal zweiten Grades $\mathfrak{p}$ teilbar sein kann; wäre dies nämlich der Fall, so müßte (D. § 180, V, S. 570) jede ganze Zahl ω außer der vorstehenden auch den Kongruenzen $\omega^{p^2} \equiv \omega \pmod{\mathfrak{p}}$, $\omega^{p^3} \equiv \omega^p \pmod{\mathfrak{p}}$, mithin auch der Kongruenz $\omega^p \equiv \omega \pmod{\mathfrak{p}}$ genügen; dann wäre aber die Anzahl $(\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p}) = p^2$ der inkongruenten

Wurzeln ω dieser letzten Kongruenz größer als ihr Grad p, was unmöglich ist (D. § 180, S. 570), und folglich ist unsere Annahme p sei durch ein Primideal zweiten Grades teilbar, unzulässig.

Es bleiben daher nur zwei Fälle übrig: entweder ist $\mathfrak{o}p$ ein Produkt von drei verschiedenen Primidealen ersten Grades $\mathfrak{p}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$, oder $\mathfrak{o}p$ ist selbst ein Primideal dritten Grades. Im ersteren Fall ist $\omega^p - \omega$ für jede ganze Zahl ω durch jedes der drei Primideale $\mathfrak{p}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$, also auch durch ihr Produkt $\mathfrak{o}p$ teilbar; wendet man dies auf die Zahl $\omega = \alpha$ an, so folgt, daß $\alpha(1 - r^e)$ durch p teilbar ist, und da α relative Primzahl zu p ist, so ergibt sich $r^e \equiv 1 \pmod{p}$, also $e \equiv 0 \pmod{3}$, d. h. die Zahl ab^2 (und ebenso a^2b) ist kubischer Rest von p. Umgekehrt, wenn dies der Fall, also e durch 3 teilbar ist, so folgt $\alpha^p \equiv \alpha$, $\beta^p \equiv \beta \pmod{p}$, also auch allgemein $\omega^p \equiv \omega$ $(\text{mod. } p)$, und es kann daher $\mathfrak{o}p$ kein Primideal sein, weil sonst die Anzahl $(\mathfrak{o}, \mathfrak{o}p) = p^3$ der inkongruenten Wurzeln ω dieser Kongruenz größer als ihr Grad p wäre. Das Resultat unserer Untersuchung besteht also hierin: Es ist

$$\mathfrak{o}p = \mathfrak{p}\mathfrak{p}_1\mathfrak{p}_2, \quad N(\mathfrak{p}) = N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p,$$

wo $\mathfrak{p}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$ drei verschiedene Primideale bedeuten, oder es ist $\mathfrak{o}p$ selbst ein Primideal dritten Grades, je nachdem die Zahl ab^2 kubischer Rest oder Nichtrest von p ist.

§ 6.

Die Dirichletsche Idealfunktion.

Das Ziel, welches wir in der gegenwärtigen Abhandlung zu erreichen suchen, besteht in der Bestimmung der Anzahl h der Idealklassen im Körper K. Die hierzu führende, von Dirichlet vorgezeichnete Methode stützt sich bekanntlich (D. § 184, S. 609—611) auf die Betrachtung der Funktion

$$J = \sum \frac{1}{N(\mathfrak{a})^s} = \Pi \frac{1}{1 - \dfrac{1}{N(\mathfrak{p})^s}},$$

wo $\mathfrak{a}$ in der Summe alle Ideale und $\mathfrak{p}$ in dem Produkte alle Primideale des Körpers durchläuft, und zwar kommt alles darauf an zu untersuchen, wie sich diese Funktion J der Variablen s für unendlich kleine positive Werte von $s - 1$ verhält. Bezieht sich nämlich das Grenzzeichen lim auf diese Annäherung der Variablen s an die Zahl 1, so wird

$$\lim (s-1) J = g h,$$

wo h die Klassenanzahl der Ideale und g eine wesentlich von der Grundzahl D und von den Einheiten des Körpers abhängende Konstante bedeutet, deren allgemeiner Ausdruck

$$g = \frac{2^\nu \pi^{n-\nu} E}{\sqrt{(D)}}$$

jetzt für unseren Fall eines reinen kubischen Körpers K zu spezialisieren ist. Der Nenner $\sqrt{(D)}$ ist die positive Quadratwurzel aus dem absoluten Werte (D) der Grundzahl $D = -3k^2$, also $\sqrt{(D)} = k\sqrt{3}$, wo $\sqrt{3}$ positiv und $k = 3ab$ oder $= ab$ ist, je nachdem K ein Körper erster oder zweiter Art ist. Das Zeichen π hat die gewöhnliche Bedeutung der Ludolfschen Zahl 3,14159..., und n ist der Grad des Körpers K, also $n = 3$. Die Zahl ν ist dadurch bestimmt, daß $(2\nu - n)$ die Anzahl der reellen, also $2(n-\nu)$ die Anzahl der imaginären unter den mit K konjugierten Körpern K, K', K'' ist; mithin ist $\nu = 2$. Die Konstante E bestimmt sich durch $rE = S'$, wo r die Anzahl 2 aller in dem (reellen) Körper K enthaltenen Einheitswurzeln ± 1 und S' den Regulator eines Fundamentalsystems S von $(\nu - 1)$ Einheiten in K bedeutet (D. § 183, S. 597, 602); da $\nu = 2$ ist, so besteht S aus einer einzigen Einheit $\varepsilon > 1$, und der Regulator S' ist $= log\, \varepsilon$, mithin $E = \frac{1}{2} log\, \varepsilon$ (und alle Einheiten in K haben die Form $\pm \varepsilon^m$, wo m alle ganzen rationalen Zahlen durchläuft). Durch das Eintragen aller dieser Werte in den obigen Ausdruck erhalten wir

$$g = \frac{2\pi\, log\, \varepsilon}{k\sqrt{3}},$$

mithin

$$\lim (s-1) J = h \frac{2\pi\, log\, \varepsilon}{k\sqrt{3}}.$$

Für die Bildung der Funktion J, zu welcher wir jetzt übergehen, legen wir die Produktform zu Grunde; durchläuft p alle natürlichen Primzahlen, und bezeichnen wir mit $F(p)$ denjenigen Faktor von J, welcher von allen verschiedenen in p aufgehenden Primidealen $\mathfrak{p}$ herrührt, so wird

$$J = \Pi F(p);$$

setzen wir ferner zur Abkürzung

$$P_n = \frac{1}{1 - \frac{1}{p^{ns}}},$$

wo n irgendeine natürliche Zahl bedeutet, so ergeben sich (nach §§ 3, 5) die folgenden Regeln zur Bestimmung des Faktors $F(p)$.

1. Geht p in k auf, so ist $\mathfrak{o}p = \mathfrak{p}^3$, wo $\mathfrak{p}$ ein Primideal ersten Grades, also $N(\mathfrak{p}) = p$, mithin $F(p) = P_1$.

2. Geht p nicht in k, aber in D auf, so ist $p = 3$ und K ein Körper zweiter Art; dann ist $\mathfrak{o}p = \mathfrak{o}3 = \mathfrak{p}^2\mathfrak{p}_1$, wo $\mathfrak{p}$ und $\mathfrak{p}_1$ zwei verschiedene Primideale ersten Grades bedeuten, also $N(\mathfrak{p}) = N(\mathfrak{p}_1) = 3 = p$, mithin $F(p) = P_1^2$.

3. Geht p nicht in D auf, und ist $p \equiv -1 \pmod{3}$, so ist $\mathfrak{o}p = \mathfrak{p}\mathfrak{p}_1$, $N(\mathfrak{p}) = p$, $N(\mathfrak{p}_1) = p^2$, mithin $F(p) = P_1 P_2$.

4. Geht p nicht in D auf, ist ferner $p \equiv +1 \pmod{3}$ und ab^2 kubischer Rest von p, so ist $\mathfrak{o}p = \mathfrak{p}\mathfrak{p}_1\mathfrak{p}_2$, $N(\mathfrak{p}) = N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$, mithin $F(p) = P_1^3$.

5. Geht p nicht in D auf, ist ferner $p \equiv +1 \pmod{3}$ und ab^2 kubischer Nichtrest von p, so ist $\mathfrak{o}p$ ein Primideal dritten Grades, mithin $F(p) = P_3$.

§ 7.

Der quadratische Körper von der Grundzahl -3.

Aus der Vergleichung der beiden letzten Regeln für die Primzahlen p, welche $\equiv +1 \pmod{3}$ sind und nicht in D aufgehen, leuchtet ein, daß zur Bildung unserer Funktion J die Theorie der kubischen Reste durchaus erforderlich ist. Gauß hat sich seit dem Jahre 1805 mit dieser Theorie und derjenigen der biquadratischen Reste beschäftigt*) und hierbei bald die überaus folgenreiche Entdeckung gemacht, daß, um dieselben auf einen gleichen Grad von Vollkommenheit zu erheben wie die Lehre von den quadratischen Resten, das Gebiet der höheren Arithmetik, in welcher bis dahin nur rationale ganze Zahlen betrachtet waren, durch die Einführung von neuen ganzen Zahlen erweitert werden muß, welche aus dritten oder vierten Wurzeln der Einheit gebildet sind, und hiermit war zugleich der Grund für die allgemeine Theorie der ganzen algebraischen

*) Vgl. Bd. II seiner Werke, S. 50, 67, 102, 161, 165, 166, 171.

Zahlen gelegt. Gauß hat aber von seinen Untersuchungen nur die auf die biquadratischen Reste bezüglichen teilweise veröffentlicht, und die in seinem Nachlaß vorgefundenen Aufzeichnungen über die aus dritten Wurzeln der Einheit gebildeten Zahlen sind wegen ihrer Unvollständigkeit nicht in die Herausgabe seiner Werke aufgenommen*) [[1])]. Den in diesem Zahlengebiete Q (dem quadratischen Körper von der Grundzahl -3) geltenden Reziprozitätssatz für die kubischen Reste hat zuerst Jacobi**) bekanntgemacht und in seinen Vorlesungen bewiesen; derselbe aus der Theorie der Kreisteilung gezogene Beweis ist später von Eisenstein***), der ihn ohne Zweifel unabhängig von Jacobi gefunden hat, zuerst veröffentlicht. Da dieser Gegenstand seitdem von mehreren Autoren†) behandelt und als hinreichend bekannt anzusehen ist, so begnügen wir uns, die wichtigsten, für unsere Untersuchung notwendigen Tatsachen kurz in Erinnerung zu bringen.

Der durch die imaginäre dritte Einheitswurzel ϱ erzeugte quadratische Körper Q von der Grundzahl -3 besteht aus allen Zahlen ω von der Form $x + y\varrho$, wo x, y rationale Zahlen bedeuten, und jede solche Zahl ω geht durch die nicht identische Permutation des Körpers in die konjugierte Zahl $\omega' = x + y\varrho^2 = x - y - y\varrho$ über. Da von den Zahlen des reinen kubischen Körpers K im folgenden gar nicht mehr die Rede sein wird, so bezeichnen wir die Norm $\omega\omega' = x^2 - xy + y^2$ unbedenklich mit $N(\omega)$, und ebenso setzen wir die aus allen ganzen Zahlen ω bestehende Hauptordnung $[1, \varrho] = \mathfrak{o}$. Die sechs Einheiten des Körpers sind die Zahlen ± 1, $\pm\varrho$, $\pm\varrho^2$, die wir gemeinsam immer mit σ bezeichnen. Alle Ideale des Körpers sind Hauptideale, d. h. jede von 0 und den Einheiten σ verschiedene

---

*) Vgl. unten § 11.

**) Über die Kreisteilung und ihre Anwendung auf die Zahlentheorie (Monatsberichte der Berliner Akademie vom Jahre 1837, wieder abgedruckt in Crelles Journal, Bd. 30, 1846).

***) Beweis des Reziprozitätssatzes für die kubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten komplexen Zahlen (Crelles Journal, Bd. 27, 1844). — Nachtrag zum kubischen Reziprozitätssatz für die aus dritten Wurzeln der Einheit zusammengesetzten komplexen Zahlen. Kriterien des kubischen Charakters der Zahl 3 und ihrer Teiler (Crelles Journal, Bd. 28, 1844).

†) Vgl. namentlich Bachmann: Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie. Leipzig 1872 (Vorlesungen 14 und 15).

[[1]) Man vgl. C. F. Gauß, Werke Bd. VIII, S. 5—20 und die dazu gehörigen Bemerkungen von Fricke.]

ganze Zahl ist entweder eine Primzahl π des Körpers, oder sie ist zusammengesetzt, und im letzteren Falle kann sie stets und wesentlich nur auf eine einzige Art als Produkt von lauter Primzahlen π dargestellt werden, wobei die sechs mit einer Zahl ω assoziierten Zahlen $\sigma\omega$ als nicht wesentlich verschieden angesehen werden. Das System aller Primzahlen π ergibt sich in folgender Weise aus der Betrachtung der durch sie teilbaren natürlichen Primzahlen p. Die Zahl $p = 3 = (1-\varrho)(1-\varrho^2) = -\varrho^2(1-\varrho)^2$ ist wesentlich das Quadrat der Primzahl ersten Grades $\pi = 1 - \varrho$; ist $p \equiv +1$ (mod. 3), so ist $p = \pi\pi' = N(\pi) = N(\pi')$ das Produkt von zwei konjugierten, wesentlich verschiedenen Primzahlen ersten Grades π und π'; ist $p \equiv -1$ (mod. 3), so ist p selbst eine Primzahl zweiten Grades π in Q, also $N(\pi) = p^2$. Mit Ausnahme des ersten dieser drei Fälle ist daher immer $N(\pi) \equiv +1$ (mod. 3).

Ist μ irgendeine von 0 verschiedene Zahl in $\mathfrak{o}$, so ist $N(\mu)$ die Anzahl $(\mathfrak{o}, \mathfrak{o}\mu)$ aller nach μ inkongruenten Zahlen in $\mathfrak{o}$; bezeichnen wir ferner mit $\varphi'(\mu)$ die Anzahl derjenigen inkongruenten Zahlen ω, welche relative Primzahlen zu μ sind, so ist $\varphi'(\sigma) = 1$ und, wenn μ keine Einheit ist,

$$\varphi'(\mu) = N(\mu)\,\Pi\left(1 - \frac{1}{N(\pi)}\right),$$

wo π alle wesentlich verschiedenen, in μ aufgehenden Primzahlen durchläuft; zugleich ist

$$\omega^{\varphi'(\mu)} \equiv 1 \pmod{\mu}.$$

Ist π eine von $(1-\varrho)$ verschiedene Primzahl, also $N(\pi) = 3m + 1$, $\varphi'(\pi) = 3m$, so genügt jede durch π nicht teilbare Zahl ω der Kongruenz

$$\omega^{3m} - 1 = (\omega^m - 1)(\omega^m - \varrho)(\omega^m - \varrho^2) \equiv 0 \pmod{\pi},$$

und da bekanntlich keine der drei Kongruenzen

$$\omega^m \equiv \varrho^e \pmod{\pi},$$

wo $e \equiv 0, 1, 2$ (mod. 3) zu setzen ist, mehr als m inkongruente Wurzeln ω haben kann, so muß jede von ihnen genau m solche Wurzeln haben. Diejenigen m Zahlen ω, für welche $e \equiv 0$ (mod. 3) wird, sind die k u b i s c h e n R e s t e d e r P r i m z a h l π, d. h. für jede dieser Zahlen ω (und nur für diese) gibt es eine oder vielmehr drei inkongruente Wurzeln ξ der Kongruenz $\xi^3 \equiv \omega$ (mod. π). Die übrigen $2m$ Zahlen ω sind die k u b i s c h e n N i c h t r e s t e von π, und sie ver-teilen sich in gleicher Anzahl m auf die beiden Fälle $e \equiv 1, 2$ (mod. 3). In allen Fällen nennen wir die durch ω vollständig bestimmte Einheitswurzel ϱ^e den kubischen Charakter oder kurz den Charakter der Zahl ω in bezug auf die Primzahl π und setzen nach Jacobi

$$\left(\frac{\omega}{\pi}\right) = \varrho^e,$$

weil hier und in der Folge eine Verwechselung mit dem Symbol von Legendre in der Theorie der quadratischen Reste nicht zu befürchten ist*). Unser Symbol wird also vollständig erklärt durch

$$\left(\frac{\omega}{\pi}\right)^3 = 1, \quad \left(\frac{\omega}{\pi}\right) \equiv \omega^m \quad (\text{mod. } \pi),$$

wo m die obige Bedeutung hat. Hieraus folgt zunächst, daß der Wert des Symbols ungeändert bleibt, wenn die Primzahl π durch eine assoziierte Zahl $\sigma\pi$, oder wenn ω durch eine nach π kongruente Zahl ersetzt wird, und da für je zwei durch π nicht teilbare Zahlen ω_1, ω_2 offenbar das Gesetz

$$\left(\frac{\omega_1\,\omega_2}{\pi}\right) = \left(\frac{\omega_1}{\pi}\right)\left(\frac{\omega_2}{\pi}\right)$$

gilt, so fällt das Symbol, als Funktion aller durch π nicht teilbaren Zahlen ω angesehen, unter den allgemeinen Begriff eines Charakters einer Abelschen Gruppe, welche letztere hier von den $3m$ Zahlklassen ω (mod. π) gebildet wird (D. § 184, S. 612); diejenigen m Zahlklassen, welche aus den kubischen Resten von π, also aus den Zahlen ω bestehen, deren Charakter $= 1$ ist, bilden ebenfalls eine Gruppe, d. h. sie reproduzieren sich durch Multiplikation. Da $\pm 1 = (\pm 1)^3$, so ist stets

$$\left(\frac{\pm 1}{\pi}\right) = 1.$$

Beaenkt man ferner, daß jede Potenz ϱ^e durch die nicht identische Permutation des Körpers in ϱ^{2e}, also die obige Kongruenz $\omega^m \equiv \varrho^e$ (mod. π) in die Kongruenz $\omega'^m \equiv \varrho^{2e}$ (mod. π') übergeht, so ergibt sich aus der Definition des Symbols das Gesetz

$$\left(\frac{\omega'}{\pi'}\right) = \left(\frac{\omega}{\pi}\right)^2.$$

---

*) Von dieser Ausdrucks- und Bezeichnungsweise weicht die von Eisenstein benutzte ein wenig ab.

Wenden wir dies auf den Fall an, wo ω eine **rationale** Zahl c, also $c' = c$ ist, so ergibt sich

$$\left(\frac{c}{\pi'}\right) = \left(\frac{c}{\pi}\right)^2.$$

Ist nun erstens die durch π teilbare natürliche Primzahl $p \equiv -1$ (mod. 3), so sind π und π' assoziiert mit $p = p'$, mithin

$$\left(\frac{c}{p}\right) = 1, \quad \text{wenn } p \equiv -1 \quad (\text{mod. } 3);$$

dasselbe ergibt sich auch daraus, daß in diesem Falle $3m = (p+1)(p-1)$, also m teilbar durch $p-1$, und folglich $c^m \equiv 1$ (mod. p) ist. Wenn aber zweitens $p = 3m + 1 \equiv +1$ (mod. 3) ist, so sind π, π' zwei wesentlich verschiedene Primzahlen ersten Grades, und es ist entweder

$$\left(\frac{c}{\pi}\right) = \left(\frac{c}{\pi'}\right) = 1$$

oder

$$\left(\frac{c}{\pi}\right) = \varrho, \quad \left(\frac{c}{\pi'}\right) = \varrho^2$$

oder

$$\left(\frac{c}{\pi}\right) = \varrho^2, \quad \left(\frac{c}{\pi'}\right) = \varrho.$$

Im ersten dieser drei Fälle, und nur in diesem, ist c kubischer Rest von π, also $c^m \equiv 1$ (mod. π), und da hieraus offenbar auch $c^m \equiv 1$ (mod. p) folgt, so ist (nach § 5, II) die Zahl c auch kubischer Rest von p im Körper der rationalen Zahlen; und umgekehrt, wenn letzteres der Fall ist, so leuchtet unmittelbar ein, daß c auch im Körper Q kubischer Rest von π (und π') ist; mithin tritt der erste der drei obigen Fälle dann und nur dann ein, wenn c im Körper der rationalen Zahlen kubischer Rest von p ist.

An dieser Stelle brechen wir die Aufzählung der für uns wichtigen Eigenschaften des Körpers Q vorläufig ab, um sie später wieder aufzunehmen. Das Vorstehende reicht nämlich schon aus, um die in § 6 begonnene Darstellung der Idealfunktion J des reinen kubischen Körpers K wesentlich zu vereinfachen. Zu diesem Zweck führen wir, wenn die Invarianten a, b des Körpers K und die daraus abgeleiteten Zahlen k und $D = -3k^2$ ihre frühere Bedeutung (§§ 3, 4) behalten, für jede Primzahl π des quadratischen Körpers Q eine **Funktion** $\psi(\pi)$ ein, welche für alles Folgende von der größten

Wichtigkeit ist; bedeutet p wieder die durch π teilbare natürliche Primzahl, so definieren*) wir auf folgende Weise:

I. Geht π, also auch p in k auf, so setzen wir

$$\psi(\pi) = 0.$$

II. Geht π, also auch p nicht in k, wohl aber in D auf, so ist $p = 3$, also π assoziiert mit $(1 - \varrho)$, und der Körper K ist von zweiter Art; in diesem Fall setzen wir

$$\psi(\pi) = 1.$$

III. In den übrigen, also in allen denjenigen Fällen, wo π, also auch p nicht in D aufgeht, setzen wir

$$\psi(\pi) = \left(\frac{ab^2}{\pi}\right),$$

wo das Symbol rechter Hand die oben angegebene Bedeutung hat, also eine Potenz von ϱ ist.

Aus dieser Definition folgen offenbar für alle Primzahlen π zunächst die beiden Sätze

IV. $$\psi(\sigma\pi) = \psi(\pi), \quad \psi(\pi') = \psi(\pi)^2.$$

Man überzeugt sich ferner leicht, daß in allen fünf Fällen, welche am Schlusse von § 6 aufgezählt sind, die dort erklärte Funktion $F(p)$ durch den Ausdruck

$$F(p) = \frac{1}{1 - \frac{1}{p^s}} \cdot \Pi \frac{1}{1 - \frac{\psi(\pi)}{N(\pi)^s}}$$

dargestellt wird, wo das Produktzeichen Π sich auf alle wesentlich verschiedenen, in p aufgehenden Primzahlen π bezieht. Um dies zu beweisen, bezeichnen wir den Ausdruck rechter Hand vorläufig mit $F_1(p)$; gehen wir die fünf Fälle am Schlusse von § 6 unter Beibehaltung der dortigen Bedeutung von P_n einzeln durch, so ergibt sich folgendes:

1. Zufolge der Definition I ist $\psi(\pi) = 0$ für jede in p aufgehende Primzahl, mithin $F_1(p) = P_1$.

---

*) Die hier für die Primzahlen π, später für alle ganzen Zahlen ω des Körpers Q erklärte Funktion ψ hängt offenbar unsymmetrisch, aber so von den Invarianten a, b des Körpers K ab, daß sie durch deren Vertauschung in ihr Quadrat übergeht.

2. Zufolge der Definition II ist $\psi(\pi) = 1$ für die wesentlich einzige in p aufgehende Primzahl $\pi = \sigma(1-\varrho)$, und da $N(\pi) = 3 = p$ ist, so wird $F_1(p) = P_1^2$.

3. Die wesentlich einzige in p aufgehende Primzahl π ist p selbst; zufolge der Definition III und weil $p \equiv -1 \pmod{3}$ ist, wird daher

$$\psi(\pi) = \left(\frac{ab^2}{p}\right) = 1,$$

und da $N(\pi) = p^2$ ist, so wird $F_1(p) = P_1 P_2$.

4. In diesem (wie in dem folgenden) Falle ist p durch zwei wesentlich verschiedene Primzahlen π, π' teilbar, deren Normen $N(\pi) = N(\pi') = p$ sind; da ferner ab^2 kubischer Rest von p, also auch von π und π' ist, so ist zufolge der Definition III:

$$\psi(\pi) = \left(\frac{ab^2}{\pi}\right) = 1, \quad \psi(\pi') = \left(\frac{ab^2}{\pi'}\right) = 1,$$

mithin wird $F_1(p) = P_1^3$.

5. Da in diesem Falle ab^2 kubischer Nichtrest von p, also auch von π, π' ist, so folgt aus der Definition III entweder

$$\psi(\pi) = \left(\frac{ab^2}{\pi}\right) = \varrho, \quad \psi(\pi') = \left(\frac{ab^2}{\pi'}\right) = \varrho^2$$

oder

$$\psi(\pi) = \left(\frac{ab^2}{\pi}\right) = \varrho^2, \quad \psi(\pi') = \left(\frac{ab^2}{\pi'}\right) = \varrho,$$

mithin wird in beiden Fällen

$$F_1(p) = \frac{1}{1-\frac{1}{p^s}} \cdot \frac{1}{1-\frac{\varrho}{p^s}} \cdot \frac{1}{1-\frac{\varrho^2}{p^s}} = P_3.$$

Nachdem hiermit für alle Fälle die Identität $F(p) = F_1(p)$ bewiesen ist, ergibt sich für die Idealfunktion $J = \Pi F(p)$, wo p alle natürlichen Primzahlen durchläuft, die folgende Zerlegung

$$J = GH;$$

hier ist

$$G = \Pi \frac{1}{1-\frac{1}{p^s}} = \sum \frac{1}{n^s},$$

wo sich das Produktzeichen Π auf alle natürlichen Primzahlen p, das Summenzeichen $\sum$ auf alle natürlichen Zahlen n bezieht, während

$$H = \Pi \frac{1}{1 - \frac{\psi(\pi)}{N(\pi)^s}}$$

ist, wo das Produktzeichen Π sich auf alle wesentlich verschiedenen Primzahlen π des Körpers Q bezieht. Wir wollen nun dieses unendliche Produkt H ebenfalls in Form einer unendlichen Reihe darstellen.

Sobald eine Funktion $\psi(\pi)$ für alle Primzahlen π in Q, und zwar so definiert ist, daß für alle sechs mit π assoziierten Primzahlen $\sigma\pi$ immer $\psi(\sigma\pi) = \psi(\pi)$ wird, so läßt sich die Funktion ψ stets zu einer Funktion $\psi(\omega)$ jeder ganzen Zahl ω in Q so erweitern, daß für je zwei solche Zahlen ω_1, ω_2 das Gesetz

V. $$\psi(\omega_1\omega_2) = \psi(\omega_1)\psi(\omega_2)$$

gilt; schließt man noch die beiden leicht zu behandelnden, für uns aber gänzlich interesselosen singulären Fälle aus, wo die gegebenen Zahlen $\psi(\pi)$ alle $= 1$ oder alle $= 0$ sind, so kann eine solche Erweiterung der Funktion ψ auch nur auf eine einzige Weise ausgeführt werden. Soll nämlich das Gesetz V bestehen, so muß zunächst $\psi(0) = \psi(0)\psi(\pi)$, mithin

VI. $$\psi(0) = 0$$

sein; da ferner nach unserer Voraussetzung $\psi(\sigma\pi) = \psi(\pi)$ ist, so muß $\psi(\sigma)\psi(\pi) = \psi(\pi)$, also

VII. $$\psi(\sigma) = 1$$

und folglich auch immer

VIII. $$\psi(\sigma\omega) = \psi(\omega)$$

sein. Wählt man nun aus jedem System von sechs assoziierten Primzahlen eine bestimmte nach Belieben aus und nennt dieselbe etwa eine primäre Primzahl, so ist jede zusammengesetzte Zahl ω von der Form

$$\omega = \sigma\pi_1\pi_2\pi_3 \cdots,$$

wo σ eine bestimmte Einheit und wo das System der primären Primzahlen π_1, π_2, $\pi_3 \cdots$ ebenfalls vollständig bestimmt ist; nach dem obigen Gesetze, welches offenbar für eine beliebige Anzahl von Faktoren gelten muß, ist dann

IX. $$\psi(\omega) = \psi(\pi_1)\psi(\pi_2)\psi(\pi_3) \cdots,$$

und folglich ist die geforderte Erweiterung der Funktion ψ nur auf eine einzige Weise möglich. Daß aber umgekehrt die durch die vorstehenden Bestimmungen VI, VII, IX erhaltene Funktion ψ auch dem obigen Multiplikationsgesetz V genügt, leuchtet unmittelbar ein. Zugleich ergibt sich aus IV für unsere Funktion ψ der Satz

X. $$\psi(\omega') = \psi(\omega)^2.$$

Entwickelt man nun jeden Faktor des unendlichen Produktes H, in welchem π ausschließlich alle primären Primzahlen durchläuft, in eine geometrische Reihe

$$\frac{1}{1 - \frac{\psi(\pi)}{N(\pi)^s}} = 1 + \frac{\psi(\pi)}{N(\pi)^s} + \frac{\psi(\pi)^2}{N(\pi)^{2s}} + \frac{\psi(\pi)^3}{N(\pi)^{3s}} + \cdots,$$

so nimmt die letztere zufolge der Erweiterung unserer Funktion ψ die Form

$$1 + \frac{\psi(\pi)}{N(\pi)^s} + \frac{\psi(\pi^2)}{N(\pi^2)^s} + \frac{\psi(\pi^3)}{N(\pi^3)^s} + \cdots = \sum \frac{\psi(\pi^n)}{N(\pi^n)^s}$$

an, wo n den Wert 0 und alle natürlichen Zahlen durchläuft. Multipliziert man ferner alle diese den primären Primzahlen π entsprechenden Reihen, so erhält man

$$H = \sum \frac{\psi(\omega)}{N(\omega)^s},$$

wo ω jede Zahl von der Form

$$\omega = \pi_1^{n_1} \pi_2^{n_2} \pi_3^{n_3} \cdots$$

einmal durchläuft, in welcher $\pi_1, \pi_2, \pi_3 \cdots$ voneinander verschiedene primäre Primzahlen und $n_1, n_2, n_3 \cdots$ ganze, nicht negative Zahlen bedeuten. Bedenkt man endlich, daß je zwei verschiedene solche Zahlen ω auch nicht assoziiert sind, und daß zu jeder Zahl ω sechs assoziierte Zahlen $\mu = \sigma\omega$ gehören, denen dieselbe Norm $N(\mu) = N(\omega)$ und derselbe Wert $\psi(\mu) = \psi(\omega)$ zukommt, so erhält man das Resultat

$$6H = \sum \frac{\psi(\mu)}{N(\mu)^s},$$

wo das Summenzeichen sich auf alle von Null verschiedenen ganzen Zahlen μ des Körpers Q bezieht.

Aus der Definition der Funktion ψ geht hervor, daß $\psi(\mu)$ immer und nur dann $= 0$ ist, wenn μ durch eine in der Zahl k aufgehende Primzahl π teilbar ist; läßt man alle diese verschwindenden Glieder weg, so ist die obige Summe nur noch auf alle diejenigen Zahlen μ

auszudehnen, welche relative Primzahlen zu der Zahl k sind, und $\psi(\mu)$ ist immer eine Potenz von ϱ. Um aber die allgemeine Form aller Zahlen μ zu finden, für welche $\psi(\mu)$ einen vorgeschriebenen Wert 1 oder ϱ oder ϱ^2 besitzt, bedürfen wir des kubischen Reziprozitätssatzes.

§ 8.

Der kubische Reziprozitätssatz.

Indem wir die in § 7 begonnene Aufzählung der für unsere Untersuchung wichtigen Eigenschaften des Körpers Q wieder aufnehmen, schreiten wir zunächst zu einer schon von Jacobi empfohlenen und auch von Eisenstein benutzten Erweiterung des Symbols

$$\left(\frac{\omega}{\mu}\right)$$

für alle Fälle, wo μ relative Primzahl zu 3ω ist, während bisher μ als Primzahl π vorausgesetzt war; diese Erweiterung ist genau auf dieselbe Weise durchzuführen wie diejenige der Funktion ψ in § 7. Wir setzen daher

$$\left(\frac{\omega}{\sigma}\right) = 1,$$

wo σ wieder jede Einheit bedeutet; ist ferner die zusammengesetzte Zahl

$$\mu = \pi_1 \pi_2 \pi_3 \cdots$$

als Produkt von lauter Primzahlen $\pi_1, \pi_2, \pi_3 \cdots$ dargestellt, so setzen wir

$$\left(\frac{\omega}{\mu}\right) = \left(\frac{\omega}{\pi_1}\right)\left(\frac{\omega}{\pi_2}\right)\left(\frac{\omega}{\pi_3}\right)\cdots,$$

und diese Definition ist eine durchaus eindeutige, weil das vorstehende Produkt ungeändert bleibt, wenn die Primzahlen π durch assoziierte Primzahlen $\sigma\pi$ ersetzt werden. Aus den früher erwähnten Eigenschaften des einfachen Symbols ergeben sich offenbar für das neue Symbol die Gesetze

$$\left(\frac{\omega}{\mu}\right)^3 = 1,\quad \left(\frac{\omega}{\sigma\mu}\right) = \left(\frac{\omega}{\mu}\right),\quad \left(\frac{\pm 1}{\mu}\right) = 1,\quad \left(\frac{\omega'}{\mu'}\right) = \left(\frac{\omega}{\mu}\right)^2,$$

$$\left(\frac{\omega_1\omega_2}{\mu}\right) = \left(\frac{\omega_1}{\mu}\right)\left(\frac{\omega_2}{\mu}\right),\quad \left(\frac{\omega}{\mu_1\mu_2}\right) = \left(\frac{\omega}{\mu_1}\right)\left(\frac{\omega}{\mu_2}\right),$$

und wenn μ_0 das Produkt aller wesentlich verschiedenen, in μ aufgehenden Primzahlen π oder auch irgendeine durch dieses Produkt teilbare Zahl (z. B. μ) bedeutet, so folgt aus

$$\omega_1 \equiv \omega_2 \text{ (mod. } \mu_0) \text{ auch } \left(\frac{\omega_1}{\mu}\right) = \left(\frac{\omega_2}{\mu}\right).$$

Unser Symbol ist daher, als Funktion des Zählers ω angesehen, auch jetzt ein Charakter der Abelschen Gruppe, welche von den $\varphi'(\mu)$ Zahlklassen ω (mod. μ) gebildet wird.

Ist nun der Nenner μ des Symbols assoziiert mit der dritten Potenz einer Zahl ν (in Q), so leuchtet ein, daß für alle $\varphi'(\mu)$ Zahlklassen ω das Symbol den Wert 1 hat, weil aus $\mu = \sigma\nu^3$ auch

$$\left(\frac{\omega}{\mu}\right) = \left(\frac{\omega}{\sigma\nu^3}\right) = \left(\frac{\omega}{\nu^3}\right) = \left(\frac{\omega}{\nu}\right)^3 = 1$$

folgt. In jedem anderen Falle gibt es aber unter den höchsten in μ aufgehenden Primzahlpotenzen π^e mindestens eine, deren Exponent e nicht durch 3 teilbar ist, und man kann nach § 7 einen kubischen Nichtrest λ der Primzahl π so wählen, daß

$$\left(\frac{\lambda}{\pi}\right) = \varrho^e$$

wird; setzt man nun $\mu = \nu\pi^e$, so ist ν relative Primzahl zu π^e, und man kann bekanntlich eine Zahl ω_1 (mod. μ) durch die Kongruenzen

$$\omega_1 \equiv 1 \text{ (mod. } \nu), \quad \omega_1 \equiv \lambda \text{ (mod. } \pi^e)$$

bestimmen; dann ist ω_1 relative Primzahl zu μ, und aus den obigen Sätzen ergibt sich

$$\left(\frac{\omega_1}{\mu}\right) = \left(\frac{\omega_1}{\nu}\right)\left(\frac{\omega_1}{\pi}\right)^e = \left(\frac{1}{\nu}\right)\left(\frac{\lambda}{\pi}\right)^e = \varrho^{e^2} = \varrho;$$

bezeichnet man nun mit ω_0 alle diejenigen nach μ inkongruenten Zahlen, welche der Bedingung

$$\left(\frac{\omega_0}{\mu}\right) = 1$$

genügen und offenbar für sich eine Gruppe bilden, so folgt leicht, daß

$$\left(\frac{\omega}{\mu}\right) = 1 \text{ oder } \varrho \text{ oder } \varrho^2$$

wird, je nachdem

$$\omega \equiv \omega_0 \text{ oder } \omega_0\omega_1 \text{ oder } \omega_0\omega_1^2 \text{ (mod. } \mu)$$

ist, und jede dieser drei Arten von Zahlen besteht aus $\frac{1}{3}\varphi'(\mu)$ Zahlklassen ω (mod. μ).

Die durch die Primzahl $(1-\varrho)$ nicht teilbaren Zahlen μ zerfallen in bezug auf die vier Moduln $1-\varrho$, $(1-\varrho)^2$, $(1-\varrho)^3$, $(1-\varrho)^4$ bzw. in 2, 6, 18, 54 Zahlklassen, welche auf folgende Weise dargestellt werden können:

$$\mu \equiv \pm 1 \pmod{1-\varrho}, \quad \mu \equiv \sigma \pmod{3},$$
$$\mu \equiv \sigma \cdot 4^m \pmod{3-3\varrho}, \quad \mu \equiv \sigma \cdot 4^m \cdot (4-3\varrho)^n \pmod{9},$$

wo σ jede Einheit und jeder der Exponenten m, n die Zahlen 0, 1, 2 durchläuft; aus der letzten Darstellung gehen die anderen sukzessive hervor, weil $4-3\varrho \equiv 1 \pmod{3-3\varrho}$, $4 \equiv 1 \pmod{3}$, $\sigma \equiv \pm 1 \pmod{1-\varrho}$ ist; zugleich wird

$$N(\mu) = \mu\mu' \equiv 4^{2m} \equiv 1 + 6m \pmod{9}.$$

Legen wir diese Darstellung der Zahlen μ zugrunde, so nehmen die zuerst von Eisenstein aufgestellten und bewiesenen sogenannten Ergänzungssätze folgende Formen an:

$$\left(\frac{\varrho}{\mu}\right) = \varrho^{\frac{N(\mu)-1}{3}} = \varrho^{2m}, \quad \left(\frac{1-\varrho}{\mu}\right) = \varrho^{m+n},$$
$$\left(\frac{\varrho-\varrho^2}{\mu}\right) = \varrho^n, \quad \left(\frac{3}{\mu}\right) = \varrho^{2n};$$

der erste dieser vier Sätze folgt sehr leicht aus der ursprünglichen Definition des kubischen Charakters in bezug auf eine Primzahl π, während der zweite eine tiefer liegende Begründung erfordert, die man am angegebenen Orte findet; durch Multiplikation ergibt sich hieraus der dritte und endlich durch Quadrieren der vierte Satz, weil $(\varrho-\varrho^2)^2 = -3$ ist. Aus diesen Sätzen folgt, daß die vier vorstehenden Symbole ungeändert bleiben, wenn die Zahl μ durch irgendeine nach dem Modul 9 kongruente Zahl ersetzt wird; für das erste Symbol gilt dies sogar schon dann, wenn diese Kongruenz in bezug auf den Modul $(3-3\varrho)$ stattfindet.

Wir wenden uns endlich zu dem von Eisenstein bewiesenen allgemeinen Reziprozitätssatze. Da jede durch $(1-\varrho)$ unteilbare Zahl mit einer, und nur einer der sechs Einheiten σ nach dem Modul 3 kongruent ist, so finden sich unter den sechs mit ihr assoziierten Zahlen immer zwei Zahlen μ, welche der Bedingung $\mu \equiv \pm 1$ (mod. 3) oder, was dasselbe sagt, der Bedingung $\mu^2 \equiv 1$ (mod. 3) genügen; für je zwei relative Primzahlen μ, ν, welche zugleich diese Bedingung $\mu^2 \equiv \nu^2 \equiv 1 \pmod{3}$ erfüllen, gilt dann das Gesetz

$$\left(\frac{\mu}{\nu}\right) = \left(\frac{\nu}{\mu}\right);$$

falls aber die Zahlen μ, ν die genannte Bedingung nicht erfüllen, so findet zwischen den beiden vorstehenden Symbolen eine Beziehung statt, welche mit Hilfe des ersten der obigen vier Ergänzungssätze immer leicht abzuleiten ist.

Wir benutzen jetzt die vorstehenden Sätze zu einer wesentlichen Umformung unserer in § 7 erklärten Funktion $\psi(\mu)$ unter der Voraussetzung, daß μ relative Primzahl zu k ist. Hierbei müssen wir die beiden Fälle unterscheiden, wo der reine kubische Körper K von erster oder zweiter Art ist (§ 3).

Im ersten Falle ist $k = 3ab$, und da ab durch 3, aber nicht durch 9 teilbar sein kann, so bezeichnen wir mit 3^u, 3^v die höchsten in a, b aufgehenden Potenzen von 3 und setzen

$$a = 3^u \cdot a_1, \quad b = 3^v \cdot b_1,$$

wo entweder $u = v = 0$, oder $u = 1$, $v = 0$ oder $u = 0$, $v = 1$ ist, während a_1 und b_1 nicht durch 3 teilbar sind. Ist nun μ relative Primzahl zu k, und stellen wir dieselbe in der Form $\mu = \pi_1\pi_2\pi_3\cdots$ als Produkt von lauter Primzahlen π dar (von denen keine in $D = -3k^2$ aufgehen kann), so folgt aus den Definitionen III und IX in § 7 zunächst

$$\psi(\mu) = \left(\frac{ab^2}{\pi_1}\right)\left(\frac{ab^2}{\pi_2}\right)\left(\frac{ab^2}{\pi_3}\right)\cdots = \left(\frac{ab^2}{\mu}\right) = \left(\frac{3}{\mu}\right)^{u+2v}\left(\frac{a_1 b_1^2}{\mu}\right);$$

wählt man nun eine Einheit σ so, daß $\sigma\mu \equiv \pm 1 \pmod{3}$ wird, und bedenkt, daß auch $a_1 b_1^2 \equiv \pm 1 \pmod{3}$ ist, so folgt aus dem allgemeinen Reziprozitätssatze

$$\left(\frac{a_1 b_1^2}{\mu}\right) = \left(\frac{a_1 b_1^2}{\sigma\mu}\right) = \left(\frac{\sigma\mu}{a_1 b_1^2}\right),$$

und wir erhalten das Resultat

XI. $$\psi(\mu) = \left(\frac{3}{\mu}\right)^{u+2v}\left(\frac{\sigma\mu}{a_1 b_1^2}\right),$$

$$\sigma\mu \equiv \pm 1 \pmod{3}, \quad k = 3ab = 3^{1+u+v}\cdot a_1 b_1.$$

Im zweiten Falle, wo K von zweiter Art, also $k = ab \equiv \pm 1 \pmod{3}$, und $a^2 \equiv b^2 \pmod{9}$, also auch $ab^2 \equiv a^3 \equiv \pm 1 \pmod{9}$

ist, ergibt sich aus den obigen Ergänzungssätzen (wo μ, σ, m, n bzw. durch ab^2, ± 1, 0, 0 zu ersetzen sind)

$$\left(\frac{\varrho}{ab^2}\right) = 1, \quad \left(\frac{1-\varrho}{ab^2}\right) = 1$$

und, weil jede Einheit $\sigma = \pm \varrho^r$ ist, auch

$$\left(\frac{\sigma}{ab^2}\right) = 1.$$

Ist nun μ relative Primzahl zu k, so kann man stets

$$\mu = \sigma(1-\varrho)^r \nu$$

setzen, wo σ eine Einheit, und $\nu \equiv 1 \pmod{3}$, also ν relative Primzahl zu $3k$, mithin auch zu D ist; aus den vorstehenden Gleichungen ergibt sich mit Hilfe des Reziprozitätssatzes

$$\left(\frac{\mu}{ab^2}\right) = \left(\frac{\sigma}{ab^2}\right)\left(\frac{1-\varrho}{ab^2}\right)^r \left(\frac{\nu}{ab^2}\right) = \left(\frac{\nu}{ab^2}\right) = \left(\frac{ab^2}{\nu}\right).$$

Gehen wir jetzt zur Bestimmung von $\psi(\mu)$ über, so folgt aus der obigen Darstellung von μ mit Rücksicht auf V, VII, II in § 7 zunächst $\psi(\mu) = \psi(\nu)$; stellt man ferner die Zahl ν als Produkt $\pi_1 \pi_2 \pi_3 \cdots$ von lauter Primzahlen dar, von denen keine in D aufgehen kann, so folgt aus III und IX in § 7

$$\psi(\nu) = \left(\frac{ab^2}{\pi_1}\right)\left(\frac{ab^2}{\pi_2}\right)\left(\frac{ab^2}{\pi_3}\right) \cdots = \left(\frac{ab^2}{\nu}\right),$$

und wir erhalten daher das einfache Resultat

XII. $$\psi(\mu) = \left(\frac{\mu}{ab^2}\right), \text{ wenn } k = ab.$$

Aus diesen Darstellungen XI und XII der Funktion $\psi(\mu)$ ergeben sich die folgenden wichtigen Sätze.

XIII. Die Funktion $\psi(\mu)$ hat für alle Zahlen μ, welche derselben Zahlklasse in bezug auf den Modul k angehören, einen und denselben Wert.

Dies leuchtet für den zweiten Fall unmittelbar aus XII ein, weil k durch jede in ab^2 aufgehende Primzahl π teilbar ist, mithin aus $\mu_1 \equiv \mu \pmod{k}$ auch

$$\left(\frac{\mu_1}{ab^2}\right) = \left(\frac{\mu}{ab^2}\right),$$

also $\psi(\mu_1) = \psi(\mu)$ folgt. Dasselbe ergibt sich für den ersten Fall auf folgende Weise aus XI. Da $k = 3ab$ ist, so folgt aus $\mu_1 \equiv \mu$ (mod. k) auch $\mu_1 \equiv \mu$ (mod. 3); ist daher die Einheit σ so gewählt, daß $\sigma\mu \equiv \pm 1$ (mod. 3) wird, so ist auch $\sigma\mu_1 \equiv \pm 1$ (mod. 3), also

$$\psi(\mu_1) = \left(\frac{3}{\mu_1}\right)^{u+2v}\left(\frac{\sigma\mu_1}{a_1 b_1^2}\right);$$

da nun $\sigma\mu_1 \equiv \sigma\mu$ (mod. k), und k durch jede in $a_1 b_1^2$ aufgehende Primzahl π teilbar ist, so folgt

$$\left(\frac{\sigma\mu_1}{a_1 b_1^2}\right) = \left(\frac{\sigma\mu}{a_1 b_1^2}\right)$$

und hieraus, falls $u + 2v = 0$ ist, $\psi(\mu_1) = \psi(\mu)$; wenn aber $u + 2v > 0$, also k durch 9 teilbar ist, so ist auch $\mu_1 \equiv \mu$ (mod. 9), also

$$\left(\frac{3}{\mu_1}\right) = \left(\frac{3}{\mu}\right),$$

mithin ist auch in diesem Falle $\psi(\mu_1) = \psi(\mu)$, w. z. b. w.

XIV. Ist $\mu \equiv r$ (mod. k), wo r eine rationale relative Primzahl zu k bedeutet, so ist $\psi(\mu) = 1$.

Bedeutet μ' wie früher die mit μ konjugierte Zahl, so folgt aus unserer Annahme auch $\mu' \equiv r$, also*) $\mu \equiv \mu'$ (mod. k), mithin zufolge XIII auch $\psi(\mu) = \psi(\mu')$; da ferner nach X in § 7 stets $\psi(\mu') = \psi(\mu)^2$ ist, so folgt $\psi(\mu) = 1$, w. z. b. w.

XV. Ist p eine in k aufgehende natürliche Primzahl, und $k = pq$, so gibt es immer eine relative Primzahl μ zu k, welche den beiden Bedingungen

$$\mu \equiv 1 \text{ (mod. } q), \quad \psi(\mu) = \varrho$$

genügt.

Bei dem Beweise haben wir eine Reihe von Fällen zu unterscheiden, und wir wollen zunächst den Fall $p = 3$ betrachten, welcher nur dann eintreten kann, wenn der kubische Körper K von erster Art ist; wir haben für den Beweis also die Darstellung XI der Funktion ψ zu benutzen und dabei zu berücksichtigen, daß $q = ab = 3^{u+v} \cdot a_1 b_1$ ist; sodann müssen wir die drei Fälle trennen, welche die beiden dort mit u, v bezeichneten Zahlen darbieten können.

*) Aus $\mu \equiv \mu'$ (mod. k) folgt umgekehrt, daß μ einer rationalen Zahl kongruent ist (mod. k).

Ist erstens $u = v = 0$, also $a_1 = a$, $b_1 = b$, so ist $ab \equiv \pm 1$ (mod. 3), aber es kann nicht $ab^2 \equiv \pm 1$ (mod. 9) sein, weil hieraus $a^2 b^4 \equiv 1$, also auch $a^2 \equiv b^2$ (mod. 9) folgen würde, was unmöglich ist, weil der Körper K von erster, nicht von zweiter Art ist. Man kann daher

$$ab^2 \equiv \pm 4^m \pmod{9}$$

setzen, wo m nicht durch 3 teilbar ist, und nach dem ersten Ergänzungssatze ist zugleich

$$\left(\frac{\varrho}{a b^2}\right) = \varrho^{2m}.$$

Da nun $q = ab$ relative Primzahl zu 3 ist, so gibt es bekanntlich immer Zahlen μ, welche den beiden Kongruenzen

$$\mu \equiv 1 \pmod{q}, \quad \mu \equiv \varrho^m \pmod{3}$$

genügen, und jede solche Zahl μ ist offenbar relative Primzahl zu $k = 3q$. Zufolge der ersten dieser beiden Kongruenzen ist die erste, im Satze an die Zahl μ gestellte Forderung erfüllt, und da $q = ab$ durch jede in ab^2 aufgehende Primzahl π teilbar ist, so folgt zugleich

$$\left(\frac{\mu}{a b^2}\right) = \left(\frac{1}{a b^2}\right) = 1.$$

Aus der zweiten der vorstehenden Kongruenzen folgt ferner, daß die Einheit $\sigma = \varrho^{2m}$ die in XI geforderte Bedingung $\sigma\mu \equiv 1$ (mod. 3) erfüllt, mithin wird

$$\psi(\mu) = \left(\frac{\sigma\mu}{a b^2}\right) = \left(\frac{\sigma}{a b^2}\right)\left(\frac{\mu}{a b^2}\right) = \left(\frac{\varrho^{2m}}{a b^2}\right) = \varrho^{4m^2} = \varrho,$$

d. h. die Zahl μ genügt auch der zweiten, im Satze an sie gestellten Forderung, w. z. b. w.

Ist zweitens $u = 1$, $v = 0$, also $a = 3a_1$, $b = b_1$, $k = 9a_1 b$, $q = 3a_1 b$, so gibt es, weil $a_1 b$ relative Primzahl zu 9 ist, Zahlen μ, welche den beiden Kongruenzen

$$\mu \equiv 1 \pmod{a_1 b}, \quad \mu \equiv (4 - 3\varrho)^2 \pmod{9}$$

genügen, und jede solche Zahl μ ist relative Primzahl zu k. Aus der zweiten Kongruenz folgt $\mu \equiv 1$ (mod. 3), und hieraus in Verbindung mit der ersten Kongruenz auch $\mu \equiv 1$ (mod. q), also ist die erste, im Satze an μ gestellte Forderung erfüllt. Zugleich ergibt sich, daß die in XI auftretende Einheit $\sigma = 1$ gewählt werden kann, und es wird folglich

$$\psi(\mu) = \left(\frac{3}{\mu}\right)\left(\frac{\mu}{a_1 b^2}\right).$$

Da jede in $a_1 b^2$ aufgehende Primzahl π auch in dem Modul $a_1 b$ der ersten Kongruenz aufgeht, so ist

$$\left(\frac{\mu}{a_1 b^2}\right) = \left(\frac{1}{a_1 b^2}\right) = 1,$$

und da aus der zweiten Kongruenz in Verbindung mit dem vierten Ergänzungssatze (wo $n = 2$ zu setzen ist)

$$\left(\frac{3}{\mu}\right) = \varrho^4 = \varrho$$

folgt, so wird auch $\psi(\mu) = \varrho$, wie gefordert war.

Ist drittens $u = 0$, $v = 1$, also $a = a_1$, $b = 3b_1$, $k = 9ab_1$, $q = 3ab_1$, so werden die Forderungen des Satzes erfüllt, wenn man μ durch die beiden Kongruenzen

$$\mu \equiv 1 \pmod{ab_1}, \quad \mu \equiv 4 - 3\varrho \pmod{9}$$

bestimmt. Den Beweis, welcher auf dieselbe Weise wie im vorigen Falle zu führen ist, dürfen wir dem Leser überlassen.

Nachdem hiermit der Fall $p = 3$ erledigt ist, nehmen wir jetzt an, es sei p verschieden von 3. Um die hierbei auftretenden Unterfälle so viel wie möglich zusammenzufassen, setzen wir $e = 1$ oder $= 2$, je nachdem p in a oder in b aufgeht; dann ist p^e die höchste in ab^2 aufgehende Potenz von p. Da p im Körper Q entweder eine Primzahl oder ein Produkt von zwei verschiedenen Primzahlen ist, so kann es in Q keine Zahl geben, deren dritte Potenz mit p assoziiert wäre, und hieraus folgt nach einer früheren Bemerkung (S. 178) die Existenz einer relativen Primzahl ω zu p, welche der Bedingung

$$\left(\frac{\omega}{p}\right) = \varrho$$

genügt. Mag nun der kubische Körper K von erster oder zweiter Art, mag also k durch 3 teilbar sein oder nicht, immer sind die beiden Faktoren p, q der Zahl $k = pq$ relative Primzahlen, mithin gibt es immer Zahlen μ, welche den beiden Kongruenzen

$$\mu \equiv 1 \pmod{q}, \quad \mu \equiv \omega^e \pmod{p}$$

genügen, und jede solche Zahl μ ist relative Primzahl zu k. Durch die erste Kongruenz ist die erste, im Satze an μ gestellte Forderung erfüllt, wir haben daher nur noch zu zeigen, daß $\psi(\mu) = \varrho$ ist, und hierzu müssen wir die beiden Hauptfälle voneinander trennen.

Ist $k = 3ab$, so haben wir die Darstellung XI zu Grunde zu legen. Da q durch 3, im Falle $u + 2v > 0$ sogar durch 9 teilbar ist, so folgt aus der ersten Kongruenz und aus dem vierten Ergänzungssatz zunächst

$$\left(\frac{3}{\mu}\right)^{u+2v} = 1,$$

und da außerdem die Einheit $\sigma = 1$ der Bedingung $\sigma\mu \equiv 1 \pmod{3}$ genügt, so wird

$$\psi(\mu) = \left(\frac{\mu}{a_1 b_1^2}\right) = \left(\frac{\mu}{c}\right)\left(\frac{\mu}{p}\right)^e,$$

wo $a_1 b_1^2 = c p^e$ gesetzt, also c nicht durch p teilbar ist. Jede in c aufgehende Primzahl π geht daher auch in q auf, und da $\mu \equiv 1 \pmod{q}$ ist, so folgt

$$\left(\frac{\mu}{c}\right) = \left(\frac{1}{c}\right) = 1.$$

Aus der zweiten, bisher nicht benutzten Kongruenz $\mu \equiv \omega^e \pmod{p}$ folgt ferner

$$\left(\frac{\mu}{p}\right) = \left(\frac{\omega^e}{p}\right) = \left(\frac{\omega}{p}\right)^e = \varrho^e, \quad \left(\frac{\mu}{p}\right)^e = \varrho,$$

mithin ist auch $\psi(\mu) = \varrho$, w. z. b. w.

Ist aber $k = ab$, so haben wir die Darstellung XII anzuwenden. Setzen wir jetzt $ab^2 = cp^e$, so ist c nicht teilbar durch p, und es wird wie in dem vorigen Fall

$$\psi(\mu) = \left(\frac{\mu}{a b^2}\right) = \left(\frac{\mu}{c}\right)\left(\frac{\mu}{p}\right)^e = \left(\frac{1}{c}\right)\left(\frac{\omega}{p}\right)^{e^2} = \varrho.$$

Der hiermit vollständig bewiesene Satz läßt sich allgemeiner in folgender Weise aussprechen.

XVI. Ist $k = mn$, wo m, n natürliche Zahlen bedeuten, deren erstere $m < k$ ist, so gibt es relative Primzahlen μ zu k, welche den Bedingungen

$$\mu \equiv 1 \pmod{m}, \quad \psi(\mu) = \varrho$$

genügen.

Da nämlich $n > 1$ ist, so gibt es mindestens eine in n, also auch in k aufgehende natürliche Primzahl p, und wenn man $k = pq$ setzt, so ist q teilbar durch m; nach dem vorigen Satze gibt es aber Zahlen μ, welche den Bedingungen $\mu \equiv 1$ (mod. q), $\psi(\mu) = \varrho$ genügen, und da aus der ersteren auch $\mu \equiv 1$ (mod. m) folgt, so ist unser Satz bewiesen.

§ 9.

Die Funktion ψ als Gruppencharakter.

Mit Hilfe der im vorstehenden bewiesenen Eigenschaften der Funktion ψ wird es gelingen, die am Schlusse von § 7 betrachtete Summe H so umzuformen, daß die Bestimmung der Anzahl h der Idealklassen im Körper K auf die Theorie der komplexen Multiplikation der elliptischen Funktionen zurückgeführt wird. Hierbei werde ich öfter ein Symbol benutzen, welches mir seit Jahren bei meinen Studien in der Gruppen- und Körpertheorie nützliche Dienste geleistet hat. Sind $\mathfrak{A}$, $\mathfrak{B}$ Komplexe von Elementen einer Gruppe $\mathfrak{K}$ (in welcher die Gruppenoperation wie eine Multiplikation bezeichnet wird), so soll das Zeichen $\mathfrak{A}\mathfrak{B}$ den Inbegriff aller verschiedenen Elemente bedeuten, welche in der Form $\alpha\beta$ darstellbar sind, wo α jedes Element von $\mathfrak{A}$, ebenso β jedes Element von $\mathfrak{B}$ durchläuft. Sind $\mathfrak{A}$, $\mathfrak{B}$ selbst Gruppen, also Teiler von $\mathfrak{K}$ (was durch $\mathfrak{A}\mathfrak{A} = \mathfrak{A}$, $\mathfrak{B}\mathfrak{B} = \mathfrak{B}$ ausgedrückt wird), so soll das Symbol $(\mathfrak{A}, \mathfrak{B})$ die Anzahl der voneinander verschiedenen Komplexe $\mathfrak{A}\beta$ bedeuten, welche allen Elementen β der Gruppe $\mathfrak{B}$ entsprechen, und aus welchen der Komplex $\mathfrak{A}\mathfrak{B}$ besteht*). Dann ist immer $(\mathfrak{A}, \mathfrak{B}) = (\mathfrak{D}, \mathfrak{B})$, wo $\mathfrak{D}$ den größten gemeinsamen Teiler der beiden Gruppen $\mathfrak{A}$, $\mathfrak{B}$ bedeutet. Wenn ferner der Komplex $\mathfrak{A}\mathfrak{B}$ selbst eine Gruppe ist (was durch $\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A}$ ausgedrückt wird und immer dann eintritt, wenn $\mathfrak{K}$ eine Abelsche Gruppe ist), so ist zugleich $(\mathfrak{A}, \mathfrak{B}) = (\mathfrak{A}, \mathfrak{A}\mathfrak{B})$. Endlich erwähne ich noch den Satz $(\mathfrak{E}, \mathfrak{G}) = (\mathfrak{E}, \mathfrak{F})(\mathfrak{F}, \mathfrak{G})$, welcher immer gilt, wenn die Gruppe $\mathfrak{E}$ ein Teiler der Gruppe $\mathfrak{F}$, und diese ein Teiler der Gruppe $\mathfrak{G}$ ist.

---

*) Ist $\mathfrak{K}$ die Gruppe aller Permutationen eines Normalkörpers C, und sind A, B die zu den Gruppen $\mathfrak{A}$, $\mathfrak{B}$ gehörigen Körper (so daß z. B. A der Inbegriff aller derjenigen Zahlen in C ist, welche durch jede Permutation der Gruppe $\mathfrak{A}$ in sich selbst übergehen), so ist das Gruppensymbol $(\mathfrak{A}, \mathfrak{B})$ identisch mit dem Symbol (A, B), welches ich in der Körpertheorie gebrauche (D. § 164, S. 471).

Nachdem dies vorausgeschickt ist, beschäftigen wir uns mit der Abelschen Gruppe $\mathfrak{K}$, deren Elemente diejenigen $\varphi'(k)$ Zahlklassen (mod. k) sind, in welche die sämtlichen, im Körper Q enthaltenen, relativen Primzahlen zu k zerfallen. Bezeichnen wir mit $\mathfrak{o}$ wieder den Inbegriff aller ganzen Zahlen ω, während μ eine bestimmte relative Primzahl zu k bedeutet, so wollen wir die aus allen Zahlen von der Form $\mu + \omega k$ bestehende Zahlklasse kurz die Klasse μ nennen, wobei der Repräsentant μ durch jede andere Zahl derselben Klasse ersetzt werden darf. Die Gruppenoperation besteht in der Multiplikation dieser Klassen: multipliziert man jede Zahl der Klasse μ_1 mit jeder Zahl der Klasse μ_2, so sind alle Produkte in derselben Klasse $\mu_1\mu_2$ enthalten, welche deshalb auch das Produkt jener beiden Klassen μ_1 und μ_2 heißen mag. Die Klasse 1 ist das Hauptelement unserer Gruppe $\mathfrak{K}$ und bildet für sich allein eine Gruppe; mit Benutzung des oben erklärten Symbols wird daher $(1, \mathfrak{K}) = \varphi'(k)$. Um diese Zahl (den Grad der Gruppe $\mathfrak{K}$) zu bestimmen, haben wir den in § 7 angegebenen Satz anzuwenden; da k rational, also $N(k) = k^2$ ist, so erhalten wir

$$\varphi'(k) = k^2 \Pi\left(1 - \frac{1}{N(\pi)}\right),$$

wo π alle wesentlich verschiedenen, in k aufgehenden Primzahlen π des Körpers Q durchläuft. Bedeutet nun p jede in k aufgehende natürliche Primzahl, und bezeichnet man zur Abkürzung mit p_0 diejenige der drei Zahlen $0, \pm 1$, welche der Bedingung $p_0 \equiv p \pmod{3}$ genügt*), so liefern die in p aufgehenden Primzahlen π zu dem vorstehenden Produkte den Beitrag

$$\left(1 - \frac{1}{p}\right)\left(1 - \frac{p_0}{p}\right),$$

und folglich wird

$$\varphi'(k) = \varphi(k)\varphi''(k),$$

wo

$$\varphi(k) = k\Pi\left(1 - \frac{1}{p}\right), \qquad \varphi''(k) = k\Pi\left(1 - \frac{p_0}{p}\right)$$

gesetzt ist.

Hier bedeutet $\varphi(k)$ wie üblich die Anzahl derjenigen nach k inkongruenten rationalen Zahlen, welche relative Primzahlen zu k

*) Offenbar ist p_0 identisch mit dem hier zu vermeidenden Symbol $\left(\frac{p}{3}\right)$ von Legendre und mit meinem Symbol $(-3, p)$ (D. S. 637, 655).

sind, also die Anzahl derjenigen Zahlklassen unserer Gruppe $\mathfrak{K}$, in welchen sich auch rationale Zahlen r befinden; dieselben bilden offenbar für sich eine Gruppe, einen Teiler von $\mathfrak{K}$, den wir mit $\mathfrak{R}$ bezeichnen wollen, und die Bedeutung der obigen Zerlegung von $\varphi'(k)$ kann durch

$$(1, \mathfrak{R}) = \varphi(k), \quad (\mathfrak{R}, \mathfrak{K}) = \varphi''(k)$$

ausgedrückt werden, weil $(1, \mathfrak{K}) = (1, \mathfrak{R})(\mathfrak{R}, \mathfrak{K})$ ist. Wir wollen schon jetzt bemerken, daß für alle hier in Betracht kommenden Zahlen k, die nach § 4 aus den Invarianten a, b des kubischen Körpers K abzuleiten sind, $\varphi''(k)$ durch 9 teilbar ist. Da nämlich $k = 3ab$ oder $= ab$ ist, je nachdem K von erster oder zweiter Art ist, und da ab durch kein Primzahlquadrat p^2 teilbar ist, so wird $k = c\Pi p$, wo $c = 3$ oder $= 1$ ist, je nachdem ab durch 3 teilbar ist oder nicht, mithin

$$\varphi''(k) = c\Pi(p - p_0).$$

Da nun jeder Faktor $(p - p_0)$ durch 3 teilbar ist, so leuchtet unsere Behauptung für alle die Fälle ein, wo k durch mindestens zwei verschiedene Primzahlen p teilbar ist. Wenn aber k nur durch eine einzige Primzahl p teilbar, also $\varphi''(k) = c(p - p_0)$ ist, so sind zwei Fälle zu unterscheiden. Ist K von erster Art, also $k = 3ab$, so ist $p = 3$, $p_0 = 0$, und da $ab > 1$ ist, so muß $ab = 3$, $k = 9$, $c = 3$, also $\varphi''(k) = 3 \cdot 3 = 9$ sein. Ist aber K von zweiter Art, also $a^2 \equiv b^2 \pmod{9}$, so ist $k = ab = p$ verschieden von 3, also $p_0^2 = 1$, $c = 1$, und der Symmetrie halber dürfen wir annehmen, es sei $a = p$, $b = 1$; hieraus folgt $a^2 - b^2 = (p - p_0)(p + p_0) \equiv 0 \pmod{9}$, und da von den beiden Faktoren $(p - p_0)$, $(p + p_0)$ nur der erste durch 3 teilbar ist, so folgt $\varphi''(k) = p - p_0 \equiv 0 \pmod{9}$. Nachdem hiermit unsere Behauptung für alle Fälle erwiesen ist, wollen wir, wo es bequem erscheint,

$$\varphi''(k) = 9k''$$

setzen; die Werte der hierdurch erklärten natürlichen Zahl k'' sind für die ersten 21 Körper K in der vorletzten Spalte der Tabelle am Schlusse von § 2 angegeben.

Wir kehren nun zur Betrachtung der Funktion $\psi(\mu)$ zurück, wo μ jede in Q enthaltene relative Primzahl zu k bedeutet. Da $\psi(\mu)$ nach Satz XIII in § 8 für alle Zahlen μ, welche derselben Klasse (mod. k) angehören, einen und denselben Wert hat, so können wir die Funktion ψ von den Zahlen μ auf die Klassen μ übertragen, welche die Elemente der Gruppe $\mathfrak{K}$ bilden, und da (nach V in § 7) für je zwei solche Klassen μ_1, μ_2 und deren Produkt $\mu_1 \mu_2$ das Gesetz $\psi(\mu_1 \mu_2) = \psi(\mu_1)\psi(\mu_2)$ gilt, so ist ψ ein Charakter der Gruppe $\mathfrak{K}$ (D. § 184, S. 612). Außerdem wissen wir (vgl. den Schluß von § 7), daß $\psi(\mu)$ immer eine Potenz von ϱ ist, also keine anderen Werte als 1, ϱ, ϱ^2 annehmen kann; zufolge VII in § 7 ist nun gewiß $\psi(1) = 1$, und da aus dem Satze XV oder XVI in § 8 (weil immer $k > 1$ ist) beiläufig folgt, daß es eine Zahl τ gibt, für welche $\psi(\tau) = \varrho$, also auch $\psi(\tau^2) = \varrho^2$ wird, so nimmt $\psi(\mu)$ wirklich alle drei Werte 1, ϱ, ϱ^2 an. Bezeichnen wir nun mit μ_0 alle diejenigen Klassen, welche der Bedingung $\psi(\mu_0) = 1$ genügen, so folgt aus dem Multiplikationsgesetz des Charakters ψ, daß diese Klassen eine Gruppe*) bilden, welche wir im folgenden stets mit ψ_0 bezeichnen wollen. Behält ferner τ die eben festgesetzte Bedeutung, so leuchtet ein, daß alle in dem Komplex $\psi_0 \tau$ enthaltenen Klassen $\mu_1 = \mu_0 \tau$ der Bedingung $\psi(\mu_1) = \varrho$ genügen; umgekehrt, wenn μ_1 der Repräsentant einer solchen Klasse ist, für welche $\psi(\mu_1) = \varrho$ wird, so kann man immer, weil τ relative Primzahl zu k ist, eine Zahl μ so bestimmen, daß $\mu\tau \equiv \mu_1 \pmod{k}$ wird, und da hieraus $\psi(\mu_1) = \psi(\mu\tau) = \psi(\mu)\psi(\tau)$, also $\psi(\mu) = 1$ folgt, so ist die Klasse μ in der Gruppe ψ_0 der Klassen μ_0 enthalten, mithin ist der Komplex $\psi_0 \tau$ der Inbegriff aller verschiedenen Klassen μ_1, welche der Bedingung $\psi(\mu_1) = \varrho$ genügen. Genau ebenso ergibt sich, daß der Komplex $\psi_0 \tau^2$ der Inbegriff aller verschiedenen Klassen μ_2 ist, für welche $\psi(\mu_2) = \varrho^2$ wird, und da jeder der drei Komplexe ψ_0, $\psi_0 \tau$, $\psi_0 \tau^2$ aus gleich vielen verschiedenen Klassen besteht, so ist

$$(1, \psi_0) = \tfrac{1}{3}\varphi'(k) = 3k''\varphi(k), \qquad (\psi_0, \mathfrak{K}) = 3,$$

weil jede Klasse der Gruppe $\mathfrak{K}$ einem und nur einem dieser drei Komplexe angehören muß**).

---

*) Vertauscht man die beiden Invarianten a, b des Körpers K miteinander, wodurch die Funktion ψ in ihr Quadrat übergeht (§ 7, Anm. auf S. 173), so bleibt diese Gruppe ψ_0 ungeändert, d. h. sie ist ebenfalls eine Invariante des Körpers K.

**) Ist ψ ein beliebiger Charakter einer beliebigen Abelschen Gruppe $\mathfrak{K}$, bedeutet ferner ψ_0 die Gruppe aller derjenigen Elemente von $\mathfrak{K}$, für welche $\psi = 1$ wird, und setzt man $(\psi_0, \mathfrak{K}) = n$, so ist n zugleich die Anzahl aller verschiedenen Werte von ψ, und diese Werte ψ sind die sämtlichen Wurzeln der Gleichung $\psi^n = 1$; zugleich ist $\mathfrak{K} = \psi_0 \mathfrak{P}$, wo $\mathfrak{P}$ eine Periode, d. h. eine Gruppe bedeutet, welche aus den Potenzen eines einzigen Elementes τ besteht. Umgekehrt, Nach dem Satze XIV in § 8 ist nun gewiß $\psi(\mu) = 1$, wenn μ einer rationalen Zahl r kongruent ist (mod. k), d. h. wenn μ einer der $\varphi(k)$ Zahlklassen der oben mit $\mathfrak{R}$ bezeichneten Gruppe angehört; mithin ist $\mathfrak{R}$ ein Teiler der Gruppe ψ_0, und für alle $\varphi(k)$ Klassen eines Komplexes $\mathfrak{R}\nu$ hat der Charakter ψ denselben Wert $\psi(\nu)$. Dies wollen wir jetzt auf die am Schlusse von § 7 betrachtete Summe

$$6H = \sum \frac{\psi(\mu)}{N(\mu)^s}$$

anwenden, wo μ alle relativen Primzahlen zu k durchläuft. Da die Gesamtgruppe $\mathfrak{K}$ aller $\varphi'(k)$ Zahlklassen μ aus $\varphi''(k)$ Komplexen von der Form $\mathfrak{R}\nu$ besteht, so wollen wir zur Abkürzung

$$S(\mathfrak{R}\nu) = \sum \frac{1}{N(\mu)^s}$$

setzen, wo μ alle Zahlen der in dem Komplex $\mathfrak{R}\nu$ enthaltenen $\varphi(k)$ Klassen durchläuft; dann wird offenbar

$$6H = \Sigma\,\psi(\nu)\,S(\mathfrak{R}\nu),$$

wo die Summe Σ auf ein System von $\varphi''(k)$ geeignet gewählten Zahlen ν auszudehnen ist, der Art, daß die entsprechenden Komplexe $\mathfrak{R}\nu$ alle Zahlklassen der Gruppe $\mathfrak{K}$ erschöpfen. Die weitere Umformung des vorstehenden Ausdrucks bildet den Hauptgegenstand unserer ferneren Untersuchungen.

§ 10.

Die Wurzeln der Ordnung $[1, k\varrho]$.

Betrachtet man einen bestimmten Klassenkomplex von der Form $\mathfrak{R}\nu$, so ist die eben definierte entsprechende Summe $S(\mathfrak{R}\nu)$ über alle und nur diejenigen Zahlen μ auszudehnen, welche $\equiv r\nu$ (mod. k) sind, wo r jede rationale Zahl bedeutet, welche relative Primzahl zu k ist. Das System aller dieser Zahlen μ bildet einen Teil des Systems aller derjenigen Zahlen λ, welche $\equiv x\nu$ (mod. k) sind, wo x jede ganze rationale Zahl bedeutet; jede solche Zahl λ ist also von der

---

wenn $\mathfrak{K} = \mathfrak{H}\mathfrak{P}$ ist, wo $\mathfrak{H}$ und $\mathfrak{P}$ Gruppen bedeuten, deren letztere $\mathfrak{P}$ eine Periode ist, so gibt es, wenn $(\mathfrak{H}, \mathfrak{K}) = (\mathfrak{H}, \mathfrak{P}) = n$ gesetzt wird, genau $\varphi(n)$ verschiedene Charaktere ψ der Gruppe $\mathfrak{K}$, welche der Bedingung $\psi_0 = \mathfrak{H}$ genügen. — Ist ferner $\mathfrak{A}$ eine in $\mathfrak{K}$ enthaltene Gruppe, so ist die über alle Elemente α von $\mathfrak{A}$ ausgedehnte Summe $\Sigma\psi(\alpha)$ immer und nur dann $= 0$, wenn $\mathfrak{A}$ kein Teiler von ψ_0 ist.

Form $\omega k + x\nu$, wo ω alle Zahlen in $\mathfrak{o}$ (d. h. alle ganzen Zahlen des Körpers Q), und x alle Zahlen des Moduls $[1]$ durchläuft, und umgekehrt ist jede in dieser Form darstellbare Zahl $\lambda \equiv x\nu$ (mod. k). Das durch k und ν vollständig bestimmte System dieser Zahlen λ, welches wir kurz mit k_ν bezeichnen wollen, ist offenbar ein endlicher Modul, und wenn man die in der Modultheorie übliche (auch oben in §§ 3, 4 benutzte) Bezeichnung anwendet, so wird

$$k_\nu = [k, k\varrho, \nu] = \mathfrak{o}k + [\nu];$$

wir wollen vorläufig diese Form eines dreigliedrigen Moduls beibehalten und erst später die Zurückführung auf einen zweigliedrigen Modul mit irreduzibler Basis betrachten. Die Theorie dieser Moduln k_ν, welche ich die Wurzeln der Ordnung $k_1 = \mathfrak{o}k + [1] = [1, k\varrho]$ genannt habe, ist in Dirichlets Vorlesungen über Zahlentheorie ausführlich dargestellt (§ 181, S. 622—627 der dritten, und § 187, S. 651—657 der vierten Auflage), und ich werde mich später auf diese Darstellung berufen; für unseren nächsten Schritt ist aber diese Theorie noch entbehrlich. Offenbar sind zwei solche Moduln k_μ, k_ν stets und nur dann identisch, wenn die beiden Zahlen μ, ν (die immer als relative Primzahlen zu k vorausgesetzt werden) denselben Klassenkomplex $\mathfrak{R}\mu = \mathfrak{R}\nu$ erzeugen, und folglich ist die Anzahl $\varphi''(k)$ aller verschiedenen, in $\mathfrak{K}$ enthaltenen Komplexe $\mathfrak{R}\nu$ zugleich die Anzahl aller verschiedenen Moduln k_ν. Setzen wir nun zur Abkürzung

$$S(k_\nu) = \sum \frac{1}{N(\lambda)^s},$$

wo λ alle Zahlen des Moduls k_ν mit einziger Ausnahme der Zahl Null, und zwar jede solche Zahl nur einmal durchläuft, so enthält diese Summe alle Glieder der in § 9 mit $S(\mathfrak{R}\nu)$ bezeichneten Summe und außerdem unendlich viele andere Glieder; aber wir wollen beweisen, daß trotzdem

$$6H = \sum \psi(\nu) S(\mathfrak{R}\nu) = \sum \psi(\nu) S(k_\nu)$$

ist, wo die zweite Summe $\sum$ auf alle $\varphi''(k)$ verschiedenen Moduln k_ν auszudehnen ist.

Um den Gang des Beweises, welcher auf dem Satze XVI in § 8 beruht, nicht zu unterbrechen, schicken wir folgende Betrachtungen über gewisse Teiler der Gruppe $\mathfrak{K}$ voraus. Ist $k = mn$, wo m, n natürliche Zahlen bedeuten, so ist jede relative Primzahl μ zu k von selbst auch relative Primzahl zu m, und wir wollen den Inbegriff aller derjenigen von diesen Zahlen μ, welche $\equiv 1 \pmod{m}$ sind, mit $\mathfrak{N}$ bezeichnen; derselbe besteht offenbar aus einer gewissen Anzahl von Zahlklassen (mod. k), welche eine Gruppe, einen Teiler der Gruppe $\mathfrak{K}$ bilden. Umgekehrt, wenn eine gegebene Zahl ω relative Primzahl zu m ist, so folgt hieraus im allgemeinen zwar noch nicht, daß ω auch zu k relative Primzahl ist, aber man überzeugt sich leicht*), daß es immer Zahlen gibt, welche $\equiv \omega \pmod{m}$ und zugleich relative Primzahlen zu k sind, und wenn ω_1 irgendeine bestimmte solche Zahl bedeutet, so wird ihre Gesamtheit durch den in der Gruppe $\mathfrak{K}$ enthaltenen Klassenkomplex $\mathfrak{N}\omega_1$ dargestellt; wendet man daher das in § 9 erklärte Gruppensymbol an, so wird

$$(1, \mathfrak{N}) = \frac{\varphi'(k)}{\varphi'(m)}, \quad (\mathfrak{N}, \mathfrak{K}) = \varphi'(m),$$

weil zu jeder der $\varphi'(m)$ Zahlklassen ω (mod. m) ein und nur ein Komplex $\mathfrak{N}\omega_1$ gehört, und weil $(1, \mathfrak{N})(\mathfrak{N}, \mathfrak{K}) = (1, \mathfrak{K}) = \varphi'(k)$ ist**).

Bedeutet nun $\mathfrak{R}$ wie bisher die Gruppe aller derjenigen $\varphi(k)$ Klassen in $\mathfrak{K}$, in welchen sich auch rationale Zahlen r befinden, so leuchtet ein, daß die Gruppe $\mathfrak{R}\mathfrak{N}$ aus lauter solchen Klassen besteht, deren Zahlen nach dem Modul m mit rationalen Zahlen kongruent sind; umgekehrt, wenn μ relative Primzahl zu k und zugleich $\equiv z \pmod{m}$ ist, wo z rational, so ist z gewiß relative Primzahl zu m, man kann daher eine ebenfalls rationale Zahl r, welche zugleich relative Primzahl zu k ist, so wählen, daß $r \equiv z \pmod{m}$, also auch $\mu \equiv r \pmod{m}$ wird, und hieraus folgt nach dem Obigen, daß μ in einer Klasse des Komplexes $\mathfrak{N}r$, also auch in einer Klasse der Gruppe $\mathfrak{R}\mathfrak{N}$ enthalten ist. Mithin ist diese Gruppe $\mathfrak{R}\mathfrak{N}$ der Inbegriff aller derjenigen Klassen in $\mathfrak{K}$, deren Zahlen nach dem Modul m mit rationalen Zahlen kongruent sind, und es ist auch leicht, den Grad dieser Gruppe, d. h. die Anzahl $(1, \mathfrak{R}\mathfrak{N})$ der in ihr enthaltenen Klassen zu bestimmen. Da nämlich $\varphi(m)$ die Anzahl

---

*) Die Kongruenz $\omega_1 \equiv \omega \pmod{m}$ ist (nach D. § 180, II, S. 568) vereinbar mit $\omega_1 \equiv 1 \pmod{\varkappa}$, wo $\varkappa$ das Produkt aller Primzahlen π bedeutet, die in k, aber nicht in m aufgehen.

**) Dieselben Sätze wiederholen sich in der Zahlentheorie jedes endlichen Körpers Ω bei der Vergleichung der Zahlklassen, die sich auf irgend ein Ideal $\mathfrak{k}$ beziehen, mit den Zahlklassen, die sich auf ein in $\mathfrak{k}$ aufgehendes Ideal $\mathfrak{m}$ beziehen. Ist Ω der Körper der rationalen Zahlen, so bilden die entsprechenden Sätze eine wesentliche Grundlage für die gesamte Theorie der Kreisteilung.

derjenigen nach m inkongruenten rationalen Zahlen z ist, welche relative Primzahlen zu m sind, und da jeder dieser Zahlen z ein Komplex $\mathfrak{N}r$ von $(1, \mathfrak{N})$ Klassen in $\mathfrak{R}\mathfrak{N}$ entspricht, deren Zahlen $\mu \equiv z$ (mod. m) sind, so ist

$$(1, \mathfrak{R}\mathfrak{N}) = \varphi(m)(1, \mathfrak{N}) = \varphi(m)\frac{\varphi'(k)}{\varphi'(m)} = \frac{\varphi'(k)}{\varphi''(m)}.$$

Da ferner $(1, \mathfrak{R})(\mathfrak{R}, \mathfrak{R}\mathfrak{N}) = (1, \mathfrak{R}\mathfrak{N})$, und $(1, \mathfrak{R}) = \varphi(k)$ ist, so ergibt sich zugleich

$$(\mathfrak{R}, \mathfrak{R}\mathfrak{N}) = \frac{\varphi'(k)}{\varphi(k)\varphi''(m)} = \frac{\varphi''(k)}{\varphi''(m)}.$$

Zu denselben Resultaten gelangt man auch, wenn man bedenkt, daß $(\mathfrak{R}, \mathfrak{R}\mathfrak{N}) = (\mathfrak{R}, \mathfrak{N}) = (\mathfrak{D}, \mathfrak{N})$ ist, wo $\mathfrak{D}$ den größten gemeinsamen Teiler der Gruppen $\mathfrak{R}, \mathfrak{N}$ bedeutet; denn jede in $\mathfrak{D}$ enthaltene Klasse wird durch eine rationale Zahl r repräsentiert, welche relative Primzahl zu k und zugleich $\equiv 1$ (mod. m) ist, mithin ist ihre Anzahl

$$(1, \mathfrak{D}) = \frac{\varphi(k)}{\varphi(m)},$$

und da

$$(1, \mathfrak{D})(\mathfrak{D}, \mathfrak{N}) = (1, \mathfrak{N}) = \frac{\varphi'(k)}{\varphi'(m)}$$

sein muß, so ergibt sich für $(\mathfrak{D}, \mathfrak{N})$, also für $(\mathfrak{R}, \mathfrak{R}\mathfrak{N})$ wieder der obige Ausdruck.

Aus der eben festgestellten Bedeutung der Gruppe $\mathfrak{R}\mathfrak{N}$ ziehen wir endlich noch folgenden Schluß. Ist ω wieder eine gegebene relative Primzahl zu m, und bedeutet ω_1 wie oben eine bestimmte relative Primzahl zu k, welche $\equiv \omega$ (mod. m) ist, so war $\mathfrak{N}\omega_1$ der Komplex aller der Klassen in $\mathfrak{K}$, deren Zahlen ebenfalls $\equiv \omega$ (mod. m) sind; ebenso leuchtet jetzt ein, daß $\mathfrak{R}\mathfrak{N}\omega_1$ der Komplex aller der Klassen in $\mathfrak{K}$ ist, deren Zahlen $\equiv z\omega$ (mod. m) sind, wo z alle rationalen relativen Primzahlen zu m durchläuft.

Nach diesen Vorbereitungen wenden wir uns zum Beweise des oben ausgesprochenen Satzes über die Umformung der Summe $6H$. Wir heben zunächst die charakteristische Eigenschaft aller in den Moduln k_ν enthaltenen Zahlen λ hervor, welche darin besteht, daß der größte gemeinsame Teiler von k und λ immer eine natürliche Zahl ist. Da nämlich $\lambda \equiv x\nu$ (mod. k), und x rational, ferner ν relative Primzahl zu k ist, so ist der rationale (positiv genommene) größte gemeinsame Teiler n der beiden rationalen Zahlen k, x

auch derjenige von k und $x\nu$, also (nach D. § 180, S. 566) auch derjenige von k und λ; setzt man daher $k = mn$, so wird $\lambda = \omega n$, wo ω relative Primzahl zu m ist.

Umgekehrt, wenn eine solche Zahl $\lambda = \omega n$ gegeben ist, so suchen wir alle Moduln k_ν, in denen λ enthalten ist. Die erforderliche und hinreichende Bedingung dafür, daß λ in k_ν enthalten sei, besteht in der Existenz einer rationalen Zahl x, welche der Kongruenz $x\nu \equiv \lambda = \omega n \pmod{k}$ genügt, und da $k = mn$, und ν relative Primzahl zu k ist, so muß zunächst x durch n teilbar, also $x = ny$ sein; hieraus folgt $y\nu \equiv \omega \pmod{m}$, und weil ω relative Primzahl zu m ist, so gilt dasselbe auch von der rationalen Zahl y; es gibt daher rationale Zahlen z, welche der Kongruenz $yz \equiv 1 \pmod{m}$ genügen, und hieraus folgt $\nu \equiv z\omega \pmod{m}$; zufolge der obigen Bemerkung muß daher ν einer Klasse des Komplexes $\mathfrak{R}\mathfrak{N}\omega_1$ angehören, wo ω_1 wieder eine relative Primzahl zu k bedeutet, welche $\equiv \omega \pmod{m}$ ist, und umgekehrt leuchtet ein, daß dann die Zahl λ wirklich in dem Modul k_ν enthalten ist, weil aus $\nu \equiv z\omega \pmod{m}$ rückwärts $y\nu \equiv \omega \pmod{m}$, $x\nu \equiv \omega n = \lambda \pmod{k}$ folgt, wo $yz \equiv 1 \pmod{m}$ und $x = ny$ ist. Mithin ist der Komplex $\mathfrak{R}\mathfrak{N}\omega_1$ der Inbegriff aller derjenigen Zahlklassen ν, welche die Eigenschaft haben, daß die gegebene Zahl $\lambda = \omega n$ in dem Modul k_ν enthalten ist*), und die Anzahl dieser verschiedenen Moduln k_ν, d. h. die Anzahl der in dem Komplexe $\mathfrak{R}\mathfrak{N}\omega_1$ enthaltenen verschiedenen Komplexe $\mathfrak{N}\nu$, ist $= (\mathfrak{N}, \mathfrak{R}\mathfrak{N}) = \varphi''(k) : \varphi''(m)$. Wir haben nun zwei wesentlich verschiedene Fälle zu betrachten.

Ist die gegebene Zahl λ selbst relative Primzahl zu k, so ist $n = 1$, $m = k$, $\mathfrak{R} = 1$; die Zahl λ tritt daher nur in einem einzigen Modul $k_\nu = k_\lambda$ auf und erzeugt nur ein einziges, mit dem Koeffizienten $\psi(\lambda)$ behaftetes Glied $N(\lambda)^{-s}$, und dieses Glied findet sich ebenso in der ersten wie in der zweiten Summe, deren Identität wir zu beweisen haben.

Ist aber λ nicht relative Primzahl zu k, ist also $n > 1$, $m < k$, so liefert λ gar keinen Beitrag zu der ersten Summe; da aber die Zahl λ in $(\mathfrak{N}, \mathfrak{R}\mathfrak{N})$ verschiedenen Moduln k_ν enthalten ist, so liefert

*) Dasselbe ergibt sich auch aus dem leicht zu beweisenden Satze $\mathfrak{o}n - k_\nu = nm_\nu$, wo $\mathfrak{o}n - k_\nu$ das kleinste gemeinsame Vielfache der beiden Moduln $\mathfrak{o}n$, k_ν und $m_\nu = \mathfrak{o}m + [\nu] = k_\nu m_1$ ist.

sie zu der zweiten Summe ebensoviele Beiträge $\psi(\nu) N(\lambda)^{-s}$; um daher auch für diesen Fall die Identität der beiden Summen und hiermit unseren Satz zu beweisen, brauchen wir nur noch zu zeigen, daß die über alle diese Moduln k_ν erstreckte Summe $\sum \psi(\nu) = 0$ ist. Hierzu berufen wir uns auf den Satz XVI in § 8, den wir nach unserer jetzigen Bezeichnung offenbar so aussprechen können, daß es in der Gruppe $\mathfrak{N}$ eine Zahlklasse μ gibt, für welche $\psi(\mu) = \varrho$, also nicht $= 1$ wird. Die Gruppe $\mathfrak{N}$ ist daher kein Teiler*) der in § 9 definierten Gruppe ψ_0, und folglich ist der größte gemeinsame Teiler $\mathfrak{E}$ dieser beiden Gruppen ein echter Teiler von $\mathfrak{N}$, d. h. $\mathfrak{E}$ ist verschieden von $\mathfrak{N}$, mithin $(\mathfrak{E}, \mathfrak{N}) = (\psi_0, \mathfrak{N}) = (\psi_0, \psi_0 \mathfrak{N}) > 1$, und da $(\psi_0, \psi_0 \mathfrak{N})(\psi_0 \mathfrak{N}, \mathfrak{K}) = (\psi_0, \mathfrak{K}) = 3$ sein muß, so folgt $(\mathfrak{E}, \mathfrak{N}) = 3$ (und $(\psi_0 \mathfrak{N}, \mathfrak{K}) = 1$, also $\psi_0 \mathfrak{N} = \mathfrak{K}$). Mithin besteht die Gruppe $\mathfrak{N}$ aus den drei verschiedenen Komplexen $\mathfrak{E}$, $\mathfrak{E}\mu$, $\mathfrak{E}\mu^2$, und für die in ihnen enthaltenen Klassen nimmt der Charakter ψ bzw. die Werte 1, ϱ, ϱ^2 an, während $\psi(\mu^3) = \psi(\mu)^3 = 1$, also $\mathfrak{E}\mu^3 = \mathfrak{E}$ ist. Bedenkt man ferner, daß die Gruppe $\mathfrak{R}$ (nach § 9) ein Teiler der Gruppe ψ_0, also die Gruppe $\mathfrak{R}\mathfrak{E}$ ein gemeinsamer Teiler der beiden Gruppen ψ_0, $\mathfrak{R}\mathfrak{N}$ ist**), so ergibt sich ebenso, daß die Gruppe $\mathfrak{R}\mathfrak{N}$ aus den drei verschiedenen Komplexen $\mathfrak{R}\mathfrak{E}$, $\mathfrak{R}\mathfrak{E}\mu$, $\mathfrak{R}\mathfrak{E}\mu^2$ und folglich der Komplex $\mathfrak{R}\mathfrak{N}\omega_1$ aus den drei verschiedenen Komplexen $\mathfrak{R}\mathfrak{E}\omega_1$, $\mathfrak{R}\mathfrak{E}\mu\omega_1$, $\mathfrak{R}\mathfrak{E}\mu^2\omega_1$ besteht. Zerlegt man nun die Gruppe $\mathfrak{R}\mathfrak{E}$ in lauter verschiedene Komplexe von der Form $\mathfrak{R}\varepsilon$ (deren Anzahl offenbar $= \varphi''(k) : 3\varphi''(m)$ ist), so ist hiermit auch der Komplex $\mathfrak{R}\mathfrak{N}\omega_1$ in lauter verschiedene Komplexe $\mathfrak{R}\nu$ zerlegt, und zwar hat ν alle Klassen $\varepsilon\omega_1$, $\varepsilon\mu\omega_1$, $\varepsilon\mu^2\omega_1$ zu durchlaufen, welche den verschiedenen Klassen ε entsprechen. Hiermit sind zugleich alle Moduln k_ν gefunden, in denen die Zahl λ enthalten ist; vereinigt man nun immer die drei Klassen ν, welche derselben Klasse ε entsprechen, und be-

*) Vgl. den Schluß der zweiten Anmerkung zu § 9 auf S. 189, worin das Wesen des obigen Beweises enthalten ist.

**) Offenbar ist $\mathfrak{R}\mathfrak{E}$ der größte gemeinsame Teiler von ψ_0, $\mathfrak{R}\mathfrak{N}$, und dieser Satz gilt allgemein für irgendwelche Teiler ψ_0, $\mathfrak{R}$, $\mathfrak{N}$ einer beliebigen Abelschen Gruppe $\mathfrak{K}$, wenn $\mathfrak{R}$ Teiler von ψ_0 und $\mathfrak{E}$ der größte gemeinsame Teiler von ψ_0, $\mathfrak{N}$ ist. Bedient man sich einer kürzlich von mir vorgeschlagenen Ausdrucksweise (§ 4 des Aufsatzes „Über Zerlegungen von Zahlen durch ihre größten gemeinsamen Teiler" in der Festschrift zur Braunschweiger Naturforscher-Versammlung 1897), so ist diese Eigenschaft so auszusprechen, daß die sämtlichen Teiler einer beliebigen Abelschen Gruppe immer eine Dualgruppe vom Modultypus bilden.

denkt man, daß $\psi(\varepsilon\omega_1) = \psi(\omega_1)$, $\psi(\varepsilon\mu\omega_1) = \varrho\,\psi(\omega_1)$, $\psi(\varepsilon\mu^2\omega_1) = \varrho^2\psi(\omega_1)$ und folglich die Summe dieser drei Werte $= 0$ ist, so ergibt sich, daß auch die über alle Klassen ν erstreckte Summe $\Sigma\,\psi(\nu) = 0$ ist, und hiermit ist unser obiger Satz vollständig bewiesen.

§ 11.

Binäre quadratische Formen.

Die sämtlichen $\varphi''(k)$ verschiedenen Moduln $k_\nu = \mathfrak{o}k + [\nu]$ sind (nach D. § 187, S. 651—657) dadurch vollständig charakterisiert, daß sie die Ordnung $k_1 = [1, k\varrho]$ haben und der Bedingung $\mathfrak{o}k_\nu = \mathfrak{o}$ genügen, und da $k_\mu k_\nu = k_{\mu\nu}$ ist, so bilden sie hinsichtlich ihrer Multiplikation eine Abelsche Gruppe. Da ferner unsere Funktion ψ für alle diejenigen in einem solchen Modul k_ν enthaltenen Zahlen, welche relative Primzahlen zu k sind, denselben Wert besitzt, so kann man sie von den Zahlen oder Zahlklassen ν auf die Moduln k_ν eindeutig übertragen, indem man $\psi(k_\nu) = \psi(\nu)$ setzt; aus der Eigenschaft $\psi(\mu\nu) = \psi(\mu)\psi(\nu)$ folgt dann $\psi(k_\mu k_\nu) = \psi(k_{\mu\nu}) = \psi(\mu\nu) = \psi(k_\mu)\psi(k_\nu)$, mithin ist ψ jetzt auch ein Charakter der eben genannten Gruppe aller Moduln k_ν. Zugleich wird

$$6H = \Sigma\,\psi(k_\nu)S(k_\nu),$$

wo die Summe Σ über alle $\varphi''(k)$ Moduln k_ν auszudehnen ist, und hier ist

$$S(k_\nu) = \sum \frac{1}{N(\lambda)^s},$$

wo λ alle Zahlen des Moduls k_ν (mit Ausnahme der Null) zu durchlaufen hat.

Bezeichnet man nun die Moduln k_ν mit $\mathfrak{k}_0, \mathfrak{k}_1, \mathfrak{k}_2$, je nachdem $\psi(k_\nu) = \psi(\nu) = 1, \varrho, \varrho^2$ ist, so nimmt der obige Ausdruck die Form

$$6H = \Sigma\,S(\mathfrak{k}_0) + \varrho\,\Sigma\,S(\mathfrak{k}_1) + \varrho^2\,\Sigma\,S(\mathfrak{k}_2)$$

an, wo die erste, zweite, dritte Summe bzw. über alle Moduln $\mathfrak{k}_0, \mathfrak{k}_1, \mathfrak{k}_2$ auszudehnen ist. Die Moduln $\mathfrak{k}_0$ bilden für sich eine Gruppe, welche offenbar der Gruppe ψ_0 in § 9 entspricht, und wenn man wieder $\varphi''(k) = 9k''$ setzt (wie in § 9), so ist ihre Anzahl $= 3k''$, und ebenso groß ist die der Moduln $\mathfrak{k}_1$ wie die der Moduln $\mathfrak{k}_2$.

Da zwischen den in §§ 6, 7 erklärten Funktionen J, G, H der Variablen s die Relation $J = GH$ besteht, und da J und G durchaus reell sind, so gilt dasselbe auch für H; hieraus folgt, daß in dem vorstehenden Ausdruck $\sum S(\mathfrak{k}_1) = \sum S(\mathfrak{k}_2)$ und folglich

$$6H = \sum S(\mathfrak{k}_0) - \sum S(\mathfrak{k}_1)$$

sein muß. Dasselbe bestätigt sich leicht auf folgende Weise. Ist ν relative Primzahl zu der rationalen Zahl k, so gilt dasselbe von der mit ν konjugierten Zahl ν', und die beiden Moduln $k_\nu = \mathfrak{o}k + [\nu]$, $k_{\nu'} = \mathfrak{o}k + [\nu']$ sind ebenfalls miteinander konjugiert, d. h. jede Zahl λ des Moduls k_ν ist konjugiert mit einer Zahl λ' des Moduls $k_{\nu'}$, und umgekehrt. Da nun $N(\lambda) = N(\lambda')$, so ist auch $S(k_\nu) = S(k_{\nu'})$; da ferner $\psi(\nu') = \psi(\nu)^2$ ist (nach § 7, X), so wird, je nachdem k_ν ein Modul $\mathfrak{k}_0, \mathfrak{k}_1, \mathfrak{k}_2$ ist, $k_{\nu'}$ ein Modul $\mathfrak{k}_0, \mathfrak{k}_2, \mathfrak{k}_1$ sein*); die Moduln $\mathfrak{k}_2$ sind daher die sämtlichen mit den Moduln $\mathfrak{k}_1$ konjugierten Moduln, und folglich ist $\sum S(\mathfrak{k}_1) = \sum S(\mathfrak{k}_2)$, w. z. b. w.

Eine zweite Vereinfachung ergibt sich aus der Betrachtung der äquivalenten Moduln k_ν. Die sämtlichen mit der Ordnung k_1 äquivalenten Moduln k_μ sind (nach D. S. 655) von der Form σk_1, wo σ alle Einheiten ± 1, $\pm \varrho$, $\pm \varrho^2$ durchläuft, und da jeder Modul durch Multiplikation mit (-1) in sich selbst übergeht, so sind nur die drei Moduln

$$k_1 = \mathfrak{o}k + [1], \quad \varrho k_1 = \mathfrak{o}k + [\varrho] = k_\varrho, \quad \varrho^2 k_1 = \mathfrak{o}k + [\varrho^2] = k_{\varrho^2}$$

zu betrachten; diese drei äquivalenten Moduln sind aber wirklich voneinander verschieden, weil $k > 1$ ist, und weil folglich die drei Klassenkomplexe $\mathfrak{R}$, $\mathfrak{R}\varrho$, $\mathfrak{R}\varrho^2$ verschieden sind. Bezeichnet man mit $\mathfrak{S}$ die Gruppe der durch die sechs Einheiten σ repräsentierten Klassen (welche alle verschieden sind, weil $k > 2$ ist), so haben $\mathfrak{R}$ und $\mathfrak{S}$ die beiden Klassen ± 1 gemein, und die Gruppe $\mathfrak{R}\mathfrak{S}$ besteht aus den drei Komplexen $\mathfrak{R}$, $\mathfrak{R}\varrho$, $\mathfrak{R}\varrho^2$; zugleich ist $(\mathfrak{R}\mathfrak{S}, \mathfrak{K}) = 3k''$, und man erkennt leicht, daß jedem Komplex $\mathfrak{R}\mathfrak{S}\nu$ ein Tripel von drei verschiedenen Moduln

$$k_\nu, \quad k_{\nu\varrho} = \varrho k_\nu, \quad k_{\nu\varrho^2} = \varrho^2 k_\nu$$

entspricht, welche miteinander, aber mit keinem anderen Modul äquivalent sind. Da nun, wenn λ alle Zahlen in k_ν durchläuft, $\varrho\lambda$ alle Zahlen in ϱk_ν und $\varrho^2\lambda$ alle Zahlen in $\varrho^2 k_\nu$ durchläuft, so folgt

*) Dasselbe ergibt sich auch aus dem Satze $k_\nu k_{\nu'} = k_{\nu\nu'} = k_1$, welcher daraus folgt, daß die Zahl $\nu\nu'$ rational ist, also einer Klasse der Gruppe $\mathfrak{R}$ angehört (vgl. D. S. 645, 653).

$S(k_\nu) = S(k_{\nu\varrho}) = S(k_{\nu\varrho^2})$, weil $N(\lambda) = N(\varrho\lambda) = N(\varrho^2\lambda)$ ist; da außerdem $\psi(\sigma) = 1$, also $\psi(k_\nu) = \psi(k_{\nu\varrho}) = \psi(k_{\nu\varrho^2})$ ist, so gehören je drei solche äquivalente Moduln entweder alle zu den Moduln $\mathfrak{k}_0$, oder alle zu den Moduln $\mathfrak{k}_1$, oder alle zu den Moduln $\mathfrak{k}_2$. Behält man daher von je drei Moduln $k_\nu, k_{\nu\varrho}, k_{\nu\varrho^2}$ immer nur einen bei, so geht unsere obige Gleichung in

$$2H = \Sigma' S(\mathfrak{k}_0) - \Sigma' S(\mathfrak{k}_1)$$

über, wo die Summationen Σ' auf alle nicht äquivalenten Moduln $\mathfrak{k}_0$, $\mathfrak{k}_1$ auszudehnen sind; jede dieser beiden Summen besteht daher aus k'' Gliedern.

Die Anzahl aller nicht äquivalenten Ordnungswurzeln k_ν ist daher $= 3k''$, und ebenso groß ist (nach D. S. 656) die Anzahl aller derjenigen nicht äquivalenten endlichen Moduln $\mathfrak{m}$ des Körpers Q, deren Ordnung $\mathfrak{m}^0 = k_1 = [1, k\varrho]$ ist. Dies beruht wesentlich darauf, daß alle Ideale (und Idealbrüche) des Körpers Q (d. h. alle Moduln von der Ordnung $\mathfrak{o}$) nur eine einzige Klasse bilden, also äquivalent sind, oder daß, was dasselbe sagt, je zwei Zahlen η, θ des Körpers Q stets (und zwar auf sechs verschiedene Arten) in die Form $\eta = \alpha\delta$, $\theta = \beta\delta$ gesetzt werden können, wo α, β ganze relative Primzahlen bedeuten*); ist nun $\mathfrak{m}$ irgendein endlicher Modul von der Ordnung $\mathfrak{m}^0 = k_1$, so enthält er gewiß zwei voneinander unabhängige Zahlen und ist folglich (nach D. § 172, VI) ein zweigliedriger Modul $\mathfrak{m} = [\eta, \theta] = \delta[\alpha, \beta] = \delta\mathfrak{k}$; der mit $\mathfrak{m}$ äquivalente Modul $\mathfrak{k} = [\alpha, \beta]$ hat (nach D. § 181, S. 579 oder § 187, S. 655) dieselbe Ordnung $\mathfrak{k}^0 = \mathfrak{m}^0 = k_1$, und da zugleich $\mathfrak{o}\mathfrak{k} = \mathfrak{o}\alpha + \mathfrak{o}\beta = \mathfrak{o}$ ist, so ist $\mathfrak{k}$ eine der Wurzeln k_ν der Ordnung k_1, w. z. b. w.

Um nun die dem Modul k_ν entsprechende Summe $S(k_\nu) = \Sigma N(\lambda)^{-s}$ zu bilden, wo λ alle Zahlen in k_ν (mit Ausnahme der Null) durchläuft, ist es zweckmäßig, die dreigliedrige Basis des Moduls

$$k_\nu = \mathfrak{o}k + [\nu] = [k, k\varrho, \nu]$$

durch eine irreduzible, also aus zwei Zahlen α, β bestehende Basis zu ersetzen, was bekanntlich auf unendlich viele Arten geschehen kann (D. § 172, S. 517—523). Wir bemerken zuvor, daß k_ν ein Teiler von $\mathfrak{o}k$ ist und, weil ν relative Primzahl zu k ist, aus k Zahl-

*) Daß α, β hier und im folgenden eine ganz andere Bedeutung haben wie in §§ 2—5, kann wohl keine Störung verursachen.

klassen (mod. k) besteht, deren Repräsentanten die Zahlen $0, \nu, 2\nu \cdots (k-1)\nu$ sind; nach der Bezeichnung der Modultheorie ist daher

$$(k_\nu, \mathfrak{o}k) = k,$$

und da $\mathfrak{o}$ ein Teiler von k_ν, also $(\mathfrak{o}, k_\nu)(k_\nu, \mathfrak{o}k) = (\mathfrak{o}, \mathfrak{o}k) = N(k) = k^2$ ist, so folgt auch

$$(\mathfrak{o}, k_\nu) = k.$$

Setzt man nun

$$k_\nu = [\alpha, \beta],$$

so folgt aus $\mathfrak{o}k_\nu = \mathfrak{o}$, daß α, β relative Primzahlen sind, und wenn man

$$\alpha = a_1 + a_2\varrho, \quad \beta = b_1 + b_2\varrho$$

setzt, wo a_1, a_2, b_1, b_2 ganze rationale Zahlen bedeuten, so ist (nach D. § 172, VII, S. 523) die Determinante $a_1 b_2 - b_1 a_2 = \pm(\mathfrak{o}, k_\nu) = \pm k$. Da nun der Modul k_ν durch Vertauschung der beiden Basiszahlen α, β nicht geändert wird, so dürfen und wollen wir festsetzen, daß immer

$$a_1 b_2 - b_1 a_2 = + k$$

sein soll, und demgemäß soll α die erste, β die zweite Basiszahl von k_ν heißen; zufolge dieser Bezeichnung wird gleichzeitig

$$k_\nu = [\alpha, \beta] = [-\alpha, -\beta] = [\beta, -\alpha] = [-\beta, \alpha],$$

und die allgemeinste Darstellung ist

$$k_\nu = [\alpha_1, \beta_1], \quad \alpha_1 = a\alpha + c\beta, \quad \beta_1 = b\alpha + d\beta,$$

wo a, b, c, d vier ganze rationale Zahlen bedeuten, die der Bedingung

$$ad - bc = +1$$

genügen*). Führt man die mit α, β konjugierten Zahlen α', β' ein, so ist der mit k_ν konjugierte Modul

$$k_{\nu'} = [\alpha', -\beta'].$$

Benutzt man ferner die bekannte Bezeichnung für die Zusammensetzung der Substitutionen (D. § 55, S. 134), so wird

$$\begin{pmatrix}\alpha, & \beta \\ \alpha', & \beta'\end{pmatrix} = \begin{pmatrix}1, & \varrho \\ 1, & \varrho^2\end{pmatrix}\begin{pmatrix}a_1, & b_1 \\ a_2, & b_2\end{pmatrix},$$

und wenn man die Determinanten nimmt, so drückt sich die obige Unterscheidung zwischen der ersten und zweiten Basiszahl durch die Gleichung

$$\alpha\beta' - \beta\alpha' = k(\varrho^2 - \varrho) = -k(1 + 2\varrho) = -k\sqrt{-3}$$

---

*) Die Zahlen a, b sind natürlich nicht zu verwechseln mit den Invarianten des kubischen Körpers K in §§ 2—9.

aus, welche zugleich lehrt, wie aus α, β rückwärts die Zahl k, also auch die Ordnung $k_1 = [1, k\varrho]$ des Moduls $[\alpha, \beta]$ zu bestimmen ist.

Zufolge dieser letzten Bemerkung gilt auch die folgende Umkehrung: wenn zwei relative Primzahlen α, β der vorstehenden Bedingung $\alpha\beta' - \beta\alpha' = k(\varrho^2 - \varrho)$ genügen, so ist der Modul $\mathfrak{k} = [\alpha, \beta]$ gewiß eine Wurzel der Ordnung $k_1 = [1, k\varrho]$. Da nämlich $\alpha\beta' - \beta\alpha'$ nicht verschwindet, so folgt zunächst, daß die Basis α, β irreduzibel ist, mithin besitzt $\mathfrak{k}$ (nach D. S. 642) eine Ordnung $\mathfrak{k}^0$ von der Form $[1, m\varrho]$, wo m eine natürliche Zahl ist; da ferner α, β relative Primzahlen sind, so folgt $\mathfrak{o}\mathfrak{k} = \mathfrak{o}$, mithin ist $\mathfrak{k}$ (nach D. S. 651—652) eine Wurzel der Ordnung $\mathfrak{k}^0$, und hieraus folgt nach der obigen Untersuchung, daß $\alpha\beta' - \beta\alpha' = m(\varrho^2 - \varrho)$, also $m = k$, $\mathfrak{k}^0 = [1, k\varrho]$, mithin $\mathfrak{k}$ einer der Moduln k_ν ist, w. z. b. w.

Hat man nun eine bestimmte Basis α, β des Moduls k_ν gewählt, so ist jede in k_ν enthaltene Zahl λ stets und nur auf eine einzige Weise in der Form

$$\lambda = \alpha x + \beta y$$

darstellbar, wo x als erste und y als zweite Variable unabhängig voneinander alle ganzen rationalen Zahlen durchlaufen; zugleich wird

$$N(\lambda) = \lambda\lambda' = (\alpha x + \beta y)(\alpha' x + \beta' y) = A x^2 + B x y + C y^2,$$

wo zur Abkürzung

$$A = \alpha\alpha', \quad B = \alpha\beta' + \beta\alpha', \quad C = \beta\beta'$$

gesetzt ist, und dem Modul k_ν entspricht die Summe

$$S(k_\nu) = \sum \frac{1}{(A x^2 + B x y + C y^2)^s},$$

welche über alle Paare x, y mit Ausnahme des Paares 0, 0 auszudehnen ist.

Offenbar sind A, C positive und, wie auch B, ganze rationale Zahlen, und da α relative Primzahl zu β, also auch α' relative Primzahl zu β' ist, so können A, B, C keinen gemeinsamen Teiler haben; denn wenn π eine in A und C aufgehende Primzahl des Körpers Q bedeutet, so sind von den vier Zahlen α, β', α', β entweder nur die beiden ersten oder nur die beiden letzten durch π teilbar, und in beiden Fällen kann π nicht in B aufgehen. Da ferner

$$B^2 - 4AC = (\alpha\beta' - \beta\alpha')^2 = -3k^2 = D$$

ist, so entspricht jeder Basis α, β des Moduls k_ν eine bestimmte positive, ursprüngliche, binäre quadratische Form (A, $\frac{1}{2}B$, C), deren Diskriminante*) die Grundzahl D des kubischen Körpers K ist (§ 4). Ersetzt man aber α, β durch die oben angegebene allgemeinste Basis α_1, β_1, und bezeichnet man mit x_1, y_1 die zugehörigen Variablen, welche wieder alle ganzen rationalen Zahlen durchlaufen, so folgt aus der doppelten Darstellung

$$\lambda = \alpha x + \beta y = \alpha_1 x_1 + \beta_1 y_1,$$

daß die alten und neuen Variablen durch die Gleichungen

$$x = a x_1 + b y_1, \quad y = c x_1 + d y_1$$

verbunden sind; mithin geht die Form (A, $\frac{1}{2}B$, C) durch die Substitution $\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$ in diejenige Form über, welche der neuen Basis α_1, β_1 entspricht. Alle diese Formen sind daher eigentlich äquivalent (D. § 56, S. 136) und bilden die sämtlichen Individuen einer bestimmten Formenklasse $\mathfrak{F}_\nu$, welche dem Modul k_ν entspricht. Dieselbe Formenklasse entspricht aber auch den beiden anderen, mit k_ν äquivalenten Moduln

$$k_{\nu\varrho} = \varrho k_\nu = [\alpha\varrho, \beta\varrho], \quad k_{\nu\varrho^2} = \varrho^2 k_\nu = [\alpha\varrho^2, \beta\varrho^2],$$

weil die Zahlen A, B, C offenbar ungeändert bleiben, wenn α, β bzw. durch $\alpha\varrho$, $\beta\varrho$ oder durch $\alpha\varrho^2$, $\beta\varrho^2$ ersetzt werden; es ist daher $\mathfrak{F}_\nu = \mathfrak{F}_{\nu\varrho} = \mathfrak{F}_{\nu\varrho^2}$.

Umgekehrt, wenn irgendeine positive ursprüngliche Form (A, $\frac{1}{2}B$, C) von der Diskriminante

$$B^2 - 4AC = D = -3k^2$$

gegeben ist, so fragen wir, ob es eine Basis α, β eines Moduls $k_\nu = [\alpha, \beta]$ gibt, welcher diese Form im obigen Sinne entspricht. Um dies zu untersuchen, betrachten wir die beiden konjugierten, offenbar ganzen Zahlen

$$\Theta = \frac{B + k\sqrt{-3}}{2} = \frac{B+k}{2} + k\varrho,$$

$$\Theta' = \frac{B - k\sqrt{-3}}{2} = \frac{B-k}{2} - k\varrho,$$

welche mit A, B, C, k durch die Gleichungen

$$\Theta + \Theta' = B, \quad \Theta\Theta' = AC, \quad \Theta' - \Theta = -k(1 + 2\varrho)$$

*) Vgl. D. § 145. Anmerkung auf S. 388—389.

verbunden sind. Soll nun die gegebene Form der Basis α, β entsprechen, so ist erforderlich und hinreichend, daß α, β relative Primzahlen sind, welche den obigen Bedingungen $\alpha\beta' - \beta\alpha' = -k(1+2\varrho)$, $\alpha\alpha' = A$, $\alpha\beta' + \beta\alpha' = B$, $\beta\beta' = C$, also den Bedingungen

$$\alpha\alpha' = A, \quad \beta\alpha' = \Theta, \quad \alpha\beta' = \Theta', \quad \beta\beta' = C$$

genügen. Durch die beiden ersten und ebenso durch die beiden letzten dieser vier Bedingungen ist zunächst das Verhältnis der beiden gesuchten relativen Primzahlen α, β aus den gegebenen Zahlen A, Θ, Θ', C vollständig zu bestimmen in den beiden Formen

$$\frac{\beta}{\alpha} = \frac{\Theta}{A} = \frac{C}{\Theta'},$$

welche vermöge der Relation $AC = \Theta\Theta'$ miteinander übereinstimmen. Offenbar gibt es immer nur sechs verschiedene solche Paare von relativen Primzahlen α, β; denn die beiden gegebenen Zahlen A, Θ besitzen im Körper Q sechs verschiedene assoziierte größte gemeinsame Teiler γ, und jeder von ihnen liefert ein entsprechendes Zahlenpaar

$$\alpha = \frac{A}{\gamma}, \quad \beta = \frac{\Theta}{\gamma}.$$

Hat man nun eine bestimmte Wahl über γ, also auch über α, β getroffen, so folgt aus $C\alpha = \Theta'\beta$, daß C durch β, ebenso Θ' durch α teilbar ist; wir haben daher eine Zerlegung von der Form

$$A = \alpha\gamma, \quad \Theta = \beta\gamma, \quad \Theta' = \alpha\delta, \quad C = \beta\delta,$$

wo δ ein durch die Wahl von γ bestimmter, größter gemeinsamer Teiler von Θ', C ist. Durch den Übergang zu den konjugierten Zahlen ergibt sich hieraus die zweite Zerlegung

$$A = \alpha'\gamma', \quad \Theta = \alpha'\delta', \quad \Theta' = \beta'\gamma', \quad C = \beta'\delta',$$

mithin muß α' als gemeinsamer Teiler von A, Θ ein Teiler von γ sein, und wenn man $\gamma = \alpha'\varepsilon$ setzt, so folgt aus $A = \alpha\alpha'\varepsilon$, daß $\varepsilon = \varepsilon'$ eine natürliche Zahl ist, weil dasselbe von $\alpha\alpha'$ und von dem ersten Koeffizienten A der positiven Form $(A, \frac{1}{2}B, C)$ gilt; aus der doppelten Darstellung von Θ folgt ferner $\beta\gamma = \beta\alpha'\varepsilon = \alpha'\delta'$, also $\delta' = \beta\varepsilon$, $\delta = \beta'\varepsilon$, und die beiden obigen Zerlegungen fließen zusammen in die folgende:

$$A = \alpha\alpha'\varepsilon, \quad \Theta = \beta\alpha'\varepsilon, \quad \Theta' = \alpha\beta'\varepsilon, \quad C = \beta\beta'\varepsilon.$$

Die natürliche Zahl ε ist daher gemeinsamer Teiler von A, C, Θ, Θ', also auch von $B = \Theta + \Theta'$, und da $(A, \frac{1}{2}B, C)$ eine ursprüngliche Form ist, so folgt $\varepsilon = 1$, also

$$A = \alpha\alpha', \quad \Theta = \beta\alpha', \quad \Theta' = \alpha\beta', \quad C = \beta\beta'.$$

Jedes der auf die obige Weise aus den gegebenen Zahlen A, Θ abgeleiteten sechs Paare von relativen Primzahlen α, β ist daher wirklich eine Basis eines Moduls k_ν, der die gegebene Form $(A, \frac{1}{2}B, C)$ entspricht, und außer diesen Basen gibt es keine andere. Bezeichnet man eine bestimmte von ihnen mit α, β, so haben sie die gemeinsame Form $\alpha\sigma$, $\beta\sigma$, wo σ alle sechs Einheiten ± 1, $\pm\varrho$, $\pm\varrho^2$ durchläuft, und sie liefern immer drei verschiedene, aber äquivalente Moduln

$$k_\nu = [\alpha, \beta], \quad k_{\nu\varrho} = [\alpha\varrho, \beta\varrho], \quad k_{\nu\varrho^2} = [\alpha\varrho^2, \beta\varrho^2].$$

Das hiermit gewonnene Resultat können wir so aussprechen:

Jedem Tripel von äquivalenten Moduln k_ν, $k_{\nu\varrho}$, $k_{\nu\varrho^2}$ entspricht eine bestimmte Klasse $\mathfrak{F}_\nu$ von eigentlich äquivalenten quadratischen Formen der Diskriminante $D = -3k^2$, und umgekehrt entspricht jede solche Formenklasse immer einem, und nur einem solchen Tripel von Moduln. Die gemeinsame Anzahl der Modultripel und Formenklassen ist $= 3k''$.

Jeder Basis α, β des Moduls k_ν entspricht, wie oben bemerkt, eine Basis α', $-\beta'$ des mit k_ν konjugierten Moduls $k_{\nu'}$; ersetzt man aber α, β bzw. durch α', $-\beta'$, so gehen die drei Zahlen A, B, C bzw. in A, $-B$, C über, also entsprechen diesen Basen der Moduln k_ν, $k_{\nu'}$ die beiden entgegengesetzten Formen $(A, \frac{1}{2}B, C)$ und $(A, -\frac{1}{2}B, C)$; zugleich ist $k_{\nu'\varrho^2}$ mit $k_{\nu'\varrho}$ [1])], und ebenso $k_{\nu'\varrho}$ mit $k_{\nu\varrho^2}$ konjugiert, und zwei solchen konjugierten Tripeln entsprechen zwei entgegengesetzte Formenklassen $\mathfrak{F}_\nu$ und $\mathfrak{F}_{\nu'}$.

Hinsichtlich der Auswahl der Basen α, β und der entsprechenden Formen $(A, \frac{1}{2}B, C)$ erwähnen wir zwei verschiedene Regeln, deren jede sich durch besondere Vorzüge empfiehlt. Die eine besteht darin, daß man (nach D. § 187, S. 652—655) für die erste Basiszahl α eine natürliche Zahl m wählt; setzt man dann die zweite Basiszahl

[1]) Es muß offenbar $k_{\nu\varrho}$ heißen.]

$\beta = t + n\varrho$, so wird immer $mn = k$, und die entsprechende Form hat die Koeffizienten

$$A = m^2, \quad B = m(2t - n), \quad C = t^2 - tn + n^2;$$

diese Formen bilden einen speziellen Fall derjenigen Formen, welche Gauß in den Artikeln 254, 255 der Disquisitiones Arithmeticae betrachtet (vgl. D. §§ 150, 151). Nach der zweiten Regel wählt man die Basis immer so, daß ihr eine sogenannte reduzierte Form $(A, \frac{1}{2}B, C)$ entspricht, in welcher absolut genommen $B \leqq A \leqq C$ und welche aus der ersten Form leicht abzuleiten ist (Art. 171 der Disqu. Arithm. oder D. § 164).

Wir erinnern noch daran, daß (nach D. § 187) der Multiplikation der Moduln, welche durch $k_\mu k_\nu = k_{\mu\nu}$ ausgedrückt wird, die Komposition der Formenklassen $\mathfrak{F}_\mu \mathfrak{F}_\nu = \mathfrak{F}_{\mu\nu}$ entspricht, und knüpfen hieran die folgende Betrachtung. Da jeder Formenklasse $\mathfrak{F}_\nu$ ein und nur ein Tripel von Moduln k_ν, $k_{\nu\varrho}$, $k_{\nu\varrho^2}$ entspricht, welche denselben Charakter $\psi(\nu)$ haben, so kann man diesen Charakter eindeutig auf die Formenklasse übertragen, indem man $\psi(\mathfrak{F}_\nu) = \psi(k_\nu) = \psi(\nu)$ setzt, und da hieraus $\psi(\mathfrak{F}_\mu \mathfrak{F}_\nu) = \psi(\mathfrak{F}_\mu)\psi(\mathfrak{F}_\nu)$ folgt, so ist jetzt ψ ein Charakter der Abelschen Gruppe $\mathfrak{H}$, welche aus den $3k''$ Formenklassen $\mathfrak{F}$ besteht. Wir haben oben mit $\mathfrak{k}_0$ alle diejenigen Moduln k_ν bezeichnet, deren Charakter $\psi(k_\nu) = 1$ ist; sie bilden eine aus k'' Tripeln bestehende Gruppe, und ebenso bilden die zugehörigen k'' Formenklassen eine Gruppe $\mathfrak{G}$, welche wieder der Gruppe ψ_0 in § 9 entspricht; zugleich ist $(\mathfrak{G}, \mathfrak{H}) = 3$, und wenn man mit $\mathfrak{F}_\tau$ eine bestimmt gewählte Formenklasse bezeichnet, deren Charakter $= \varrho$ ist, so besteht die Gesamtgruppe $\mathfrak{H}$ der $3k''$ Formenklassen aus den drei Komplexen $\mathfrak{G}$, $\mathfrak{G}\mathfrak{F}_\tau = \mathfrak{G}_1$, $\mathfrak{G}\mathfrak{F}_\tau^2 = \mathfrak{G}_2$, denen bzw. die Charaktere $1, \varrho, \varrho^2$ zukommen. In welcher Beziehung steht nun diese Gruppe $\mathfrak{G}$ zu unserem kubischen Körper K? Um diese Frage zu beantworten, betrachten wir alle diejenigen in D nicht aufgehenden natürlichen Primzahlen p, welche $\equiv 1 \pmod{3}$ sind, von welchen also die Grundzahl D quadratischer Rest ist. Im quadratischen Körper Q ist daher $p = \pi\pi'$, wo π, π' zwei konjugierte, wesentlich verschiedene Primzahlen bedeuten, die nicht in $3k$ aufgehen; diese Primzahlen sind bzw. in den beiden konjugierten Moduln k_π, $k_{\pi'}$ enthalten, und da $p = N(\pi) = N(\pi')$ ist, so ist p darstellbar durch jede in den beiden entgegengesetzten Formenklassen $\mathfrak{F}_\pi$, $\mathfrak{F}_{\pi'}$ enthaltene Form $(A, \frac{1}{2}B, C)$. Da umgekehrt (nach D. § 60) jede solche Form, durch welche p darstellbar ist, mit einer Form $(p, \frac{1}{2}r, q)$ äquivalent ist, wo $r^2 = D + 4pq \equiv D \pmod{4p}$, und da die letztere Form, wie oben gezeigt ist, immer nur drei äquivalenten Moduln $k_\nu = [\alpha, \beta]$ entspricht, wo $\alpha\alpha' = p$, also α mit π oder π' assoziiert und folglich auch relative Primzahl zu k ist, so muß $k_\nu = k_{\sigma\pi}$ oder $= k_{\sigma\pi'}$ sein, mithin gehört die Form $(p, \frac{1}{2}r, q)$ einer der beiden Formenklassen $\mathfrak{F}_\pi$, $\mathfrak{F}_{\pi'}$ an, und die natürliche Primzahl p ist daher ausschließlich darstellbar durch die Formen dieser beiden Klassen (vgl. D. §§ 86, 87). Nun gehört die Formenklasse $\mathfrak{F}_\pi$ dem Komplexe $\mathfrak{G}$, $\mathfrak{G}_1$, $\mathfrak{G}_2$, und gleichzeitig gehört die Formenklasse $\mathfrak{F}_{\pi'}$ dem Komplexe $\mathfrak{G}$, $\mathfrak{G}_2$, $\mathfrak{G}_1$ an, je nachdem $\psi(\pi) = 1, \varrho, \varrho^2$ ist; nach der Definition der Funktion ψ in § 7 tritt aber der erste dieser drei Fälle dann, und nur dann ein, wenn ab^2 kubischer Rest der natürlichen Primzahl p ist, wo a, b die Invarianten des kubischen Körpers K bedeuten. Wollen wir diesen Körper K nicht ausdrücklich erwähnen, so besteht das hiermit gewonnene Resultat in dem folgenden

Satz. Ist mindestens eine der beiden natürlichen Zahlen $a, b > 1$ und ab durch kein Quadrat einer natürlichen Primzahl teilbar, setzt man ferner $k = 3ab$ oder $= ab$, je nachdem $(a^2 - b^2)$ durch 9 unteilbar oder teilbar ist, so ist die Anzahl aller nicht äquivalenten, positiven, ursprünglichen binären quadratischen Formen $(A, \frac{1}{2}B, C)$ von der Diskriminante $B^2 - 4AC = D = -3k^2$ immer ein Vielfaches $3k''$ von 3, und ein Drittel der durch diese Formen vertretenen Formenklassen bildet eine Kompositionsgruppe $\mathfrak{G}$, welche durch die folgende Eigenschaft charakterisiert ist: Bedeutet p jede natürliche Primzahl, welche $\equiv 1 \pmod{3}$ ist und nicht in D aufgeht, so sind durch die k'' Formen der Gruppe $\mathfrak{G}$ alle und nur solche Primzahlen p darstellbar, von denen ab^2, also auch a^2b kubischer Rest ist, während durch die Formen der übrigen $2k''$ Klassen alle und nur solche Primzahlen p darstellbar sind, von denen ab^2 kubischer Nichtrest ist.

Wollen wir aber die Bedeutung der quadratischen Formen für den kubischen Körper K hervorheben, so erinnern wir uns daran, daß (nach § 5) die natürliche Primzahl p, je nachdem ab^2 kubischer Rest oder Nichtrest von p ist, im Körper K durch drei verschiedene Primideale ersten Grades teilbar oder selbst eine Primzahl dritten Grades ist, und erhalten den folgenden*)

Satz. Bedeutet D die Grundzahl eines kubischen Körpers K, so ist die Anzahl der Klassen, in welche die ursprünglichen binären quadratischen Formen von der Diskriminante D zerfallen, ein Vielfaches von 3, und ein Drittel dieser Klassen bildet eine durch folgende Eigenschaft charakterisierte Kompositionsgruppe $\mathfrak{G}$: Bedeutet p jede, in D nicht aufgehende, natürliche Primzahl, von welcher D quadratischer Rest ist, so wird p im Körper K durch drei verschiedene Primideale teilbar oder selbst eine Primzahl sein, je nachdem p durch eine Form der Gruppe $\mathfrak{G}$ darstellbar ist oder nicht.

Auf einem der Papiere aus dem Nachlasse von Gauß, welche mir — wahrscheinlich im Jahre 1860 — zur Ansicht, aber nicht zur Herausgabe mitgeteilt wurden, befand sich eine Bemerkung über kubische Reste, welche nach meiner Abschrift folgendermaßen lautet [¹)]:

Observatio venustissima inductione facta.

2 est Residuum vel non Residuum cubicum numeri primi p formae $3n+1$, prout p repraesentabilis est per formam

$$xx + 27yy$$
$$\text{vel } 4xx + 2xy + 7yy.$$

3 est Residuum vel non Residuum, prout p repraesentabilis est per

$$xx + 243yy \text{ aut } 4xx + 2xy + 61yy$$
$$\text{vel } 7xx + 6xy + 36yy \text{ aut } 9xx + 6xy + 28yy.$$

---

*) Die Form, in welcher ich diesen Fundamentalsatz hier ausspreche, ist so gewählt, daß sie, wie ich glaube, für alle kubischen Körper ohne Ausnahme, selbst für die Kreiskörper gilt; den allgemeinen Beweis dieses Satzes zu finden, ist mir aber bisher nicht gelungen. Dagegen bietet die Zerlegung aller anderen Primzahlen p in Primideale keine erhebliche Schwierigkeit dar.

[¹) C. F. Gauß, Werke Bd. VIII, S. 5.]

$$\begin{array}{ccc}
\text{5 est Residuum} & & \text{Nonresiduum}\\
\left.\begin{array}{rrr}(1, & 0, & 675)\\(25, & 0, & 27)\\(13, & 1, & 52)\\(4, & 1, & 169)\end{array}\right\} & \begin{array}{c}\text{si}\\ p\\ \text{reprae-}\\ \text{senta-}\\ \text{tur per}\end{array} & \left\{\begin{array}{rrr}(7, & 2, & 97)\\(9, & 3, & 76)\\(19, & 3, & 36)\\(25, & 5, & 28)\\(25, & 10, & 31)\\(27, & 9, & 28)\end{array}\right.
\end{array}$$

In diesen Sätzen muß man ohne Zweifel die frühesten Entdeckungen erblicken, die Gauß auf dem Gebiete der kubischen (und biquadratischen) Reste gemacht hat, und durch welche er bald darauf zu der Erweiterung des Begriffs der ganzen Zahl geführt ist (vgl. § 7).

Noch bevor dieses merkwürdige Fragment mir bekannt geworden war, hatte ich den ersten dieser drei Sätze bei dem Versuche gefunden, die Methode, durch welche Gauß den biquadratischen Charakter der Zahl 2 bestimmt (Theoria residuorum biquadraticorum I, Art. 15—23), auf die Theorie der kubischen Reste zu übertragen. Der Beweis, den ich am 7. Januar 1858 in einer algebraischen Vorlesung zu Göttingen vorgetragen habe, ergibt sich in der Tat sehr einfach aus Art. 358 der Disquisitiones Arithmeticae; behält man nämlich die dortige Bezeichnung bei, bedeutet also n eine natürliche Primzahl, welche $\equiv 1 \pmod{3}$ ist, so zeigt Gauß, daß immer

$$4n = MM + 27NN$$

und gleichzeitig, wenn $M \equiv 1 \pmod{3}$ gewählt wird,

$$9a = n + 1 + M$$

ist, wo $a - 1 = (\mathfrak{R}\mathfrak{R})$ die Anzahl derjenigen inkongruenten kubischen Reste z von n bedeutet, welche die Eigenschaft besitzen, daß auch $(z + 1)$ kubischer Rest von n ist. Setzt man nun $z + 1 \equiv z_1 \pmod{n}$ und bedenkt, daß die Zahl (-1) immer kubischer Rest von n ist, so folgt aus $-z_1 + 1 \equiv -z \pmod{n}$, daß die Zahl $(-z_1)$ dieselbe Eigenschaft wie z besitzt. Man kann daher alle diese $(a - 1)$ Zahlklassen z in eine Reihe von Paaren z und $(-z-1)$ ordnen, und folglich wird $a - 1$ eine gerade Zahl sein, wenn nicht etwa der Fall vorkommt, daß die beiden Zahlen derselben Klasse angehören, also $2z \equiv -1 \pmod{n}$ ist; dies geschieht immer und nur dann, wenn die Zahl 2 selbst ein kubischer Rest von n ist, und da es in diesem Falle auch nur für eine einzige Klasse z geschieht, so ergibt sich, daß a gerade oder ungerade ist, je nachdem die Zahl 2 kubischer Rest oder Nichtrest von n ist*). Da ferner immer $a \equiv M \equiv N$ (mod. 2) ist, so folgt, daß die Primzahl n im ersten Falle und nur in diesem durch die Hauptform $(1, 0, 27) = xx + 27\,yy$ darstellbar ist; wenn aber 2 kubischer Nichtrest von n ist, so muß n durch die beiden anderen reduzierten Formen $(4, \pm 1, 7) = 4\,xx \pm 2\,xy + 7\,yy$ der Determinante -27 oder der Diskriminante -108 darstellbar sein. Hiermit ist der obige Satz vollständig bewiesen, und man überzeugt sich leicht, daß er mit unserer allgemeinen Theorie übereinstimmt, weil die Invarianten des durch die Zahl $\sqrt[3]{2}$ erzeugten kubischen Körpers K_1 die Zahlen 2 und 1 sind, woraus $k = 6$, $k'' = 1$ folgt.

Unterhalb 100 gibt es nur zwei Primzahlen n oder p, von denen die Zahl 2 kubischer Rest ist, nämlich

$$31 = 2^2 + 27 \cdot 1^2, \qquad 43 = 4^2 + 27 \cdot 1^2,$$

und wenn t eine willkürliche Zahl bedeutet, so ist

$$t^3 - 2 \equiv (t-4)(t-7)(t+11) \quad (\text{mod. } 31),$$
$$t^3 - 2 \equiv (t+9)(t+11)(t-20) \quad (\text{mod. } 43),$$

wie man leicht mit Hilfe des Canon Arithmeticus von Jacobi findet.

Gehen wir jetzt zu den beiden anderen Sätzen über, um sie ebenfalls mit unserer Theorie zu vergleichen, so ist es auch hier zweckmäßig, zu jeder der von Gauß angegebenen reduzierten Formen, falls sie nicht eine zweiseitige (eine forma anceps) ist, die entgegengesetzte Form hinzuzufügen. In dem zweiten Satze, der von dem kubischen Charakter der Zahl 3 handelt, ist das Formensystem der Determinante -243 außerdem noch durch die beiden oben fehlenden Formen $(13, \pm 2, 19)$ zu ergänzen, und wir wollen (wie im folgenden § 12) zur Abkürzung

$$\begin{array}{lll}
(1, \;\; 0, 243) = (00), & (7, -3, 36) = (10), & (7, \;\; 3, 36) = (20), \\
(4, \;\; 1, \;\; 61) = (01), & (9, \;\; 3, 28) = (11), & (13, -2, 19) = (21), \\
(4, -1, \;\; 61) = (02), & (13, \;\; 2, 19) = (12), & (9, -3, 28) = (22)
\end{array}$$

setzen. Die Bedeutung dieser Bezeichnung ist folgende. Jede Form (yz), wo die beiden Zahlen y, z durch beliebige nach dem Modul 3 kon-

*) Aus der Bedeutung der Gaußschen Zahlen $b = (\mathfrak{K}\mathfrak{K}')$, $c = (\mathfrak{K}\mathfrak{K}'')$, welche nicht beide ungerade sein können, ergibt sich allgemeiner, daß die Zahl 2 dem Komplex $\mathfrak{K}$ oder $\mathfrak{K}'$ oder $\mathfrak{K}''$ angehört, je nachdem $a \equiv b \equiv c \equiv 0$ oder $a + 1 \equiv b + 1 \equiv c \equiv 0$ oder $a + 1 \equiv b \equiv c + 1 \equiv 0$ (mod. 2) ist.

gruente Zahlen ersetzt werden dürfen, soll auch als Zeichen für die durch sie repräsentierte Formenklasse angesehen werden; dann ist die aus den Klassen $(y_1 z_1)$ und $(y_2 z_2)$ zusammengesetzte Klasse

$$(y_1 z_1)(y_2 z_2) = (yz), \quad \text{wo} \quad y \equiv y_1 + y_2, \quad z \equiv z_1 + z_2 \pmod{3},$$

also auch

$$(yz) = (10)^y (01)^z, \qquad (10)^3 = (01)^3 = (00),$$

und der Satz von Gauß besteht darin, daß die Zahl 3 kubischer Rest oder Nichtrest der natürlichen Primzahl p ist, je nachdem p durch eine der drei Formen (00), (01), (02) darstellbar ist oder nicht. Die kleinsten durch die Formen (00), (01) darstellbaren Primzahlen sind

$$307 = 8^2 + 243 \cdot 1^2, \qquad 61 = 4 \cdot 0^2 + 2 \cdot 0 \cdot 1 + 61 \cdot 1^2,$$

und es ist

$$t^3 - 3 \equiv (t + 79)(t + 113)(t + 115) \pmod{307},$$
$$t^3 - 3 \equiv (t - 4)(t - 5)(t + 9) \pmod{61}.$$

Vergleichen wir nun diesen zweiten Satz von Gauß mit unserer Theorie, so ergibt sich folgendes. Die Invarianten des durch die Zahl $\sqrt[3]{3}$ erzeugten Körpers K_2 sind die Zahlen 3, 1, und da folglich $k = 9$, $k'' = 1$ ist, so müssen schon die drei reduzierten Formen

$$(1, \tfrac{1}{2}, 61), \qquad (7, \pm \tfrac{3}{2}, 9)$$

der Diskriminante -243 die Entscheidung über den kubischen Charakter der Zahl 3 geben; die oben mit $\mathfrak{G}$ bezeichnete Gruppe besteht allein aus der Hauptklasse $(1, \frac{1}{2}, 61)$, und die Zahl 3 ist daher kubischer Rest von allen und nur von denjenigen Primzahlen p, welche durch diese Form darstellbar sind. In der Tat ist wieder

$$307 = 7^2 + 7 \cdot 2 + 61 \cdot 2^2, \qquad 61 = 0^2 + 0 \cdot 1 + 61 \cdot 1^2,$$

und man erkennt leicht, daß der Satz von Gauß vollständig mit dem unsrigen übereinstimmt. Dies beruht auf den allgemeinen Sätzen über den Zusammenhang zwischen den Formen verschiedener Ordnung; jede Gruppe $\mathfrak{G}$ innerhalb der Gesamtgruppe $\mathfrak{H}$ aller Formen der Diskriminante D liefert eine entsprechende Gruppe $\mathfrak{G}'$ innerhalb der Gesamtgruppe $\mathfrak{H}'$ aller Formen, deren Diskriminante D' irgend ein quadratisches Vielfaches De^2 von D ist, und zwar bleibt die Anzahl $(\mathfrak{G}', \mathfrak{H}')$ invariant $= (\mathfrak{G}, \mathfrak{H})$, weil jede Formenklasse der Diskriminante D sich in gleich viele Formenklassen der Diskriminante D' zerteilt*).

*) Vgl. D. §§ 150, 151, 187 und die obige Anmerkung zu § 10 auf S. 192.

Jede solche, aus einer Gruppe $\mathfrak{G}$ **abgeleitete** Gruppe $\mathfrak{G}'$ ist daran kenntlich, daß sie die Gruppe aller derjenigen Formenklassen der Diskriminante D' in sich enthält, welche durch Komposition mit der Hauptklasse der Diskriminante D diese selbe Hauptklasse erzeugen. In unserem Falle ist $e = 2$, $D = -3(9)^2$, $D' = -3(18)^2$, und je drei Formenklassen $(y\,z)$ der letzteren Diskriminante liefern durch Komposition mit der Klasse $(1, \frac{1}{2}, 61)$ eine Klasse der Diskriminante D, was in leicht verständlicher Weise durch

$$\begin{aligned}
\{(00), (01), (02)\}\,(1, \tfrac{1}{2}, 61) &= (1, \ \ \tfrac{1}{2}, 61)\\
\{(10), (11), (12)\}\,(1, \tfrac{1}{2}, 61) &= (7, -\tfrac{3}{2}, \ 9)\\
\{(20), (21), (22)\}\,(1, \tfrac{1}{2}, 61) &= (7, \ \ \tfrac{3}{2}, \ 9)
\end{aligned}$$

oder durch

$$(y\,z)\,(1, \tfrac{1}{2}, 61) = (7, -\tfrac{3}{2}, 9)^y$$

bezeichnet werden kann.

Aus demselben Grunde könnte man in umgekehrter Weise den **ersten Satz von Gauß** so umformen, daß zur Entscheidung über den kubischen Charakter der Zahl 2 die Formen der Diskriminante $D = -3(6)^2$ durch je drei Formen der Diskriminante $D' = -3(18)^2$ ersetzt werden; in der Tat ist

$$\begin{aligned}
\{(00), (11), (22)\}\,(1, 0, 27) &= (1, \ \ 0, 27)\\
\{(01), (12), (20)\}\,(1, 0, 27) &= (4, -1, \ 7)\\
\{(02), (10), (21)\}\,(1, 0, 27) &= (4, \ \ 1, \ 7)
\end{aligned}$$

oder

$$(y\,z)(1, 0, 27) = (4, -1, 7)^{2y+z},$$

und die Zahl 2 ist kubischer Rest oder Nichtrest einer Primzahl p, je nachdem letztere darstellbar oder nicht darstellbar durch eine der drei Formen (00), (11), (22) ist; so z. B. werden die beiden oben genannten Primzahlen 31 und 43, von denen 2 kubischer Rest ist, durch die Form $(11) = (9, 3, 28)$ dargestellt:

$$31 = 9 \cdot 1^2 + 6 \cdot 1 \cdot (-1) + 28 \cdot (-1)^2, \quad 43 = 9 \cdot 1^2 + 6 \cdot 1 \cdot 1 + 28 \cdot 1^2.$$

Ganz ähnlich verhält es sich mit dem **dritten Satz von Gauß**, wo zur Entscheidung über die Zahl 5 die 18 Formen der Diskriminante $D' = -3(30)^2$ benutzt werden, während nach unserer Theorie schon die 6 Formen der Diskriminante $D = -3(15)^2$ hierzu ausreichen. Um die Komposition der ersteren 18 Formen miteinander übersichtlich darzustellen (wie bei dem zweiten Satze), wollen wir sie gemeinsam durch $(y\,z)$ bezeichnen, wo z wieder nach dem Modul 3, aber y jetzt nach dem Modul 6 zu nehmen ist; setzen wir

$$(10) = (7, 2, 97),\quad (01) = (4, 1, 169),\quad (y\,z) = (10)^y (01)^z,$$

so wird

$$(60) = (03) = (00),$$

ferner

$$\begin{array}{llllll}
(00) = & (1, \;\; 0, 675), & (01) = & (4, \;\; 1, 169), & (02) = & (4, -1, 169) \\
(10) = & (7, \;\; 2, \;\; 97), & (11) = & (27, -9, \;\; 28), & (12) = & (25, \;\; 5, \;\; 28) \\
(20) = & (19, \;\; 3, \;\; 36), & (21) = & (25, \;\; 10, \;\; 31), & (22) = & (9, -3, \;\; 76) \\
(30) = & (25, \;\; 0, \;\; 27), & (31) = & (13, \;\; 1, \;\; 52), & (32) = & (13, -1, \;\; 52) \\
(40) = & (19, -3, \;\; 36), & (41) = & (9, \;\; 3, \;\; 76), & (42) = & (25, -10, \;\; 31) \\
(50) = & (7, -2, \;\; 97), & (51) = & (25, -5, \;\; 28), & (52) = & (27, \;\; 9, \;\; 28)
\end{array}$$

und die Komposition dieser Formenklassen mit der Hauptklasse $(1, \frac{1}{2}, 169)$ kann durch

$$\begin{aligned}
\{(00), (01), (02)\}(1, \tfrac{1}{2}, 169) &= (1, \;\; \tfrac{1}{2}, \;\; 169) \\
\{(10), (11), (12)\}(1, \tfrac{1}{2}, 169) &= (7, -\tfrac{5}{2}, \;\; 25) \\
\{(20), (21), (22)\}(1, \tfrac{1}{2}, 169) &= (9, -\tfrac{3}{2}, \;\; 19) \\
\{(30), (31), (32)\}(1, \tfrac{1}{2}, 169) &= (13, \;\; \tfrac{1}{2}, \;\; 13) \\
\{(40), (41), (42)\}(1, \tfrac{1}{2}, 169) &= (9, \;\; \tfrac{3}{2}, \;\; 19) \\
\{(50), (51), (52)\}(1, \tfrac{1}{2}, 169) &= (7, \;\; \tfrac{5}{2}, \;\; 25)
\end{aligned}$$

oder kurz durch

$$(y\,z)(1, \tfrac{1}{2}, 169) = (7, -\tfrac{5}{2}, 25)^y$$

dargestellt werden. Die Zahl 5 ist dann und nur dann kubischer Rest der Primzahl p, wenn p durch eine der beiden zweiseitigen Formen

$$(1, \tfrac{1}{2}, 169),\qquad (13, \tfrac{1}{2}, 13)$$

darstellbar ist; offenbar ist 13 die kleinste solche Primzahl, und sie ist darstellbar durch die Formen (31), (32); zugleich ist

$$t^3 - 5 \equiv (t+2)(t+5)(t+6) \pmod{13}.$$

Die 18 Formen $(y\,z)$ der Diskriminante $D' = -3\,(30)^2$ geben, weil je sechs von ihnen aus einer Form der Diskriminante $D = -3\,(6)^2$ entstehen, auch wieder die Entscheidung über den kubischen Charakter der Zahl 2; aus

$$(10)(1, 0, 27) = (01)(1, 0, 27) = (4, 1, 7)$$

folgt

$$(y\,z)(1, 0, 27) = (4, 1, 7)^{y+z},$$

mithin entspricht der Hauptklasse (1, 0, 27) die Gruppe der sechs Klassen (00), (12), (21), (30), (42), (51), welche die Potenzen der

Klasse (12) oder (51) sind, und die Zahl 2 ist dann und nur dann kubischer Rest der Primzahl p, wenn p durch eine Form dieser Gruppe darstellbar ist; so z. B. wird die oben angeführte Primzahl 43 durch die beiden Formen (12), (51), und ebenso die Primzahl 31 durch die beiden Formen (21), (42) dargestellt.

Wir haben an den drei Sätzen von Gauß soeben gezeigt, wie der kubische Charakter einer Zahl ab^2, der nach unserer Theorie von den Formen der Diskriminante $D = -3k^2$ abhängt, auch durch die Formen jeder Diskriminante $D' = De^2 = -3(ke)^2$ bestimmt werden kann, welche ein quadratisches Vielfaches von D ist. Aus der Definition der Funktion ψ in § 7 und aus dem Satze XVI in § 8 folgt aber auch, wie der Leser leicht finden wird, daß die Grundzahl D des kubischen Körpers K wirklich die absolut kleinste Diskriminante ist, deren Formen die fragliche Entscheidung geben, und hierin liegt eine wesentliche Vervollständigung des oben in doppelter Form ausgesprochenen allgemeinen Satzes. Noch wichtiger ist aber der Umstand, daß die in § 10 bewiesene Umformung der Funktion H nicht mehr gelten würde, wenn man statt der Moduln k_ν, denen die Formenklassen $\mathfrak{F}_\nu$ von der Diskriminante D entsprechen, solche Moduln $(ke)_\nu$ einführen wollte, denen Formen von absolut größerer Diskriminante $D' = De^2$ entsprechen; auch dies beruht auf dem Satze XVI in § 8, doch wollen wir uns hier begnügen, die Tatsache an den folgenden Beispielen nachzuweisen.

§ 12.

Beispiele.

Wir haben schon am Schlusse von § 4 hervorgehoben, daß ein (reeller) reiner kubischer Körper K durch seine Grundzahl $D = -3k^2$ im allgemeinen noch nicht vollständig bestimmt ist, daß es also verschiedene Körper K geben kann, welche demselben Werte der natürlichen Zahl k entsprechen. Zu allen diesen Körpern K gehört dann auch dasselbe System von Moduln k_ν des quadratischen Körpers Q (in § 10) und dasselbe System $\mathfrak{H}$ von binären Formen (in § 11); aber diese Körper K werden sich immer voneinander unterscheiden durch die zugehörige Funktion ψ (in § 7) und folglich durch die Gruppe $\mathfrak{G}$ (in § 11), welche aus einem Drittel der Gruppe $\mathfrak{H}$ besteht. Zufolge der Tabelle in § 2 tritt dieser Fall zuerst für den Wert $k = 18$ ein, welchem die beiden durch die Zahlen $\sqrt[3]{6}$ und $\sqrt[3]{12}$ erzeugten Körper K_4

und K_5 entsprechen, und da die Zahl 18 durch die beiden ersten in der Tabelle auftretenden Werte 6 und 9 von k teilbar ist, so wird die Untersuchung des Falles $k = 18$ zugleich die Theorie der durch die Zahlen $\sqrt[3]{2}$ und $\sqrt[3]{3}$ erzeugten Körper K_1 und K_2 umfassen, mit welchen wir uns eben schon in § 11 beschäftigt haben; die Durchführung dieses Beispiels wird daher besonders lehrreich sein.

Zunächst kommt es nach § 9 darauf an, im quadratischen Körper Q alle ganzen Zahlen μ übersichtlich darzustellen, welche relative Primzahlen zum Modul $k = 18$ sind; da 2 und 3 die einzigen in 18 aufgehenden natürlichen Primzahlen sind, so erhalten wir

$$\varphi(k) = \varphi(18) = 18(1 - \tfrac{1}{2})(1 - \tfrac{1}{3}) = 6,$$
$$\varphi''(k) = 9k'' = \varphi''(18) = 18(1 - \tfrac{-1}{2})(1 - \tfrac{0}{3}) = 27,$$

also $k'' = 3$, und die Anzahl der inkongruenten Zahlen μ ist

$$\varphi'(k) = \varphi(k)\varphi''(k) = \varphi'(18) = 162 = 2 \cdot 3^4.$$

Die Gruppe $\mathfrak{K}$ dieser Zahlklassen μ läßt sich durch

$$\mu \equiv 5^w \varrho^x (4 - 3\varrho)^y (1 + 9\varrho)^z \pmod{18}$$

darstellen, wo der Exponent w nach dem Modul 6, die Exponenten x, y, z aber nach dem Modul 3 zu nehmen sind, weil

$$5^6 \equiv \varrho^3 \equiv (4 - 3\varrho)^3 \equiv (1 + 9\varrho)^3 \equiv 1 \pmod{18}$$

ist. Daß diese Darstellung vollständig und wesentlich nur auf eine einzige Weise möglich ist, erkennt man leicht daraus, daß sie aus den beiden folgenden Darstellungen

$$\mu \equiv (-1)^w \varrho^x \cdot 4^w (4 - 3\varrho)^y \pmod{9},$$
$$\mu \equiv \varrho^{x+y+2z} \pmod{2}$$

zusammengesetzt ist; die erstere stimmt mit der in § 8, S. 179 angegebenen überein und dient dazu, um aus der gegebenen Zahl μ die Exponenten w (mod. 6), x (mod. 3) und y (mod. 3) zu bestimmen, während aus der letzteren Darstellung sich die Zahl z (mod. 3) ergibt; zugleich folgt aus § 8, S. 179 die Bestimmung

$$\left(\frac{3}{\mu}\right) = \varrho^{2y}.$$

Setzen wir ferner

$$\sigma = \varrho^{2x},$$

so genügt diese Einheit der Bedingung $\sigma\mu \equiv \pm 1$ (mod. 3), und zugleich wird

$$\sigma\mu \equiv \varrho^{y+2z} \pmod{2};$$

da nun die Zahl 2 auch im Körper Q eine Primzahl und $N(2) = 4 = 3 \cdot 1 + 1$ ist, so folgt aus der Definition des kubischen Charakters in § 7 auch

$$\left(\frac{\sigma \mu}{2}\right) = \varrho^{y+2z}.$$

Endlich bemerken wir, daß aus der obigen Darstellung der Zahlen μ (mod. 18) auch die Darstellung

$$\mu' \equiv 5^w \varrho^{2x} (4 - 3\varrho)^{2y} (1 + 9\varrho)^{2z} \quad (\text{mod. } 18)$$

der konjugierten Zahlen μ' folgt, weil $4 - 3\varrho^2 \equiv (4 - 3\varrho)^2$ und $1 + 9\varrho^2 \equiv (1 + 9\varrho)^2$ (mod. 18) ist.

Gehen wir nun dazu über, nach den Regeln in §§ 10, 11 die 27 Moduln k_μ zu bestimmen, so ist zunächst zu bemerken, daß die Gruppe $\mathfrak{R}$ derjenigen Klassen, welche auch rationale Zahlen enthalten, aus den 6 Klassen

$$5^w \equiv 1, 5, 7, 17, 13, 11 \quad (\text{mod. } 18),$$

und die Gruppe $\mathfrak{R}\mathfrak{S}$ (in § 11, S. 197) aus den 18 Klassen $5^w \varrho^x$ besteht. Wir werden daher alle Moduln k_μ und jeden nur einmal erhalten, wenn wir in der obigen Darstellung immer $w = 0$ setzen, während jede der Zahlen x, y, z ihre drei Werte durchlaufen muß. Da ferner diese 27 Moduln in 9 Tripel von der Form $k_\mu, k_{\mu\varrho}, k_{\mu\varrho^2}$ zerfallen, welche je einem Komplex $\mathfrak{R}\mathfrak{S}\mu$ entsprechen, und da für unseren Zweck von je drei solchen äquivalenten Moduln nur einer erforderlich ist, so dürfen wir auch $x = 0$ setzen und erhalten die folgende, sogleich zu erläuternde Tabelle:

y	z	μ	$(18)_\mu$	9_μ	6_μ	ψ_1	ψ_2	ψ_4	ψ_5
0	0	1	$1, 18\varrho$	$1, 9\varrho$	$1, 6\varrho$	1	1	1	1
1	0	$4 + 15\varrho$	$6, 2 + 3\varrho$	$3, 2 + 3\varrho$	$2, 3\varrho$	ϱ	ϱ^2	1	ϱ
2	0	$7 + 3\varrho$	$6, 1 + 3\varrho$	$3, 1 + 3\varrho$	$2, 1 + 3\varrho$	ϱ^2	ϱ	1	ϱ^2
0	1	$1 + 9\varrho$	$2, 1 + 9\varrho$	$1, 9\varrho$	$2, 1 + 3\varrho$	ϱ^2	1	ϱ^2	ϱ
1	1	$13 + 6\varrho$	$3, 1 + 6\varrho$	$3, 2 + 3\varrho$	$1, 6\varrho$	1	ϱ^2	ϱ^2	ϱ^2
2	1	$16 + 3\varrho$	$6, 4 + 3\varrho$	$3, 1 + 3\varrho$	$2, 3\varrho$	ϱ	ϱ	ϱ^2	1
0	2	$10 + 9\varrho$	$2, 9\varrho$	$1, 9\varrho$	$2, 3\varrho$	ϱ	1	ϱ	ϱ^2
1	2	$13 + 15\varrho$	$6, 5 + 3\varrho$	$3, 2 + 3\varrho$	$2, 1 + 3\varrho$	ϱ^2	ϱ^2	ϱ	1
2	2	$7 + 12\varrho$	$3, 2 + 6\varrho$	$3, 1 + 3\varrho$	$1, 6\varrho$	1	ϱ	ϱ	ϱ

Die Zahlen y, z der beiden ersten Spalten bestimmen in Verbindung mit $w = x = 0$ die Zahlenklasse μ (mod. 18) der dritten Spalte, und in der folgenden Spalte ist für den zugehörigen Modul $(18)_\mu = [18, 18\varrho, \mu]$ eine zweigliedrige Basis angegeben, deren erstes Glied eine natürliche Zahl ist; diese Basis ist nach bekannten Regeln (D. § 172, S. 519—520) immer leicht zu finden. Die 9 Moduln $(18)_\mu$ bilden eine Gruppe, und das Gesetz ihrer Multiplikation ergibt sich aus ihrer Darstellung

$$(18)_\mu = [6, 2 + 3\varrho]^y [2, 1 + 9\varrho]^z.$$

Die binären quadratischen Formen $(A, \frac{1}{2}B, C)$ von der Diskriminante $-3(18)^2$, welche den hier angegebenen Modulbasen entsprechen (§ 11), sind nicht reduziert, aber es hat (nach D. § 64) keine Schwierigkeit, die ihnen äquivalenten reduzierten Formen herzustellen, und diese letzteren sind mit denjenigen identisch, welche wir in § 11 bei der Besprechung des zweiten Satzes von Gauß mit (yz) bezeichnet haben. In der fünften und sechsten Spalte findet man zweigliedrige Basen für die durch die Zahl μ bestimmten Moduln

$$9_\mu = [9, 9\varrho, \mu] = (18)_\mu [1, 9\varrho] = (18)_\mu 9_1,$$
$$6_\mu = [6, 6\varrho, \mu] = (18)_\mu [1, 6\varrho] = (18)_\mu 6_1,$$

und die ihnen entsprechenden Formenklassen von den Diskriminanten $-3 \cdot 9^2$ und $-3 \cdot 6^2$ ergeben sich durch Komposition der Formen (yz) mit den Formen $(1, \frac{1}{2}, 61)$ und $(1, 0, 27)$, wie ebenfalls schon in § 11 besprochen ist.

Die vier letzten Spalten enthalten endlich die Werte der Charaktere $\psi(\mu)$ für die durch $\sqrt[3]{2}$, $\sqrt[3]{3}$, $\sqrt[3]{6}$, $\sqrt[3]{12}$ erzeugten reinen kubischen Körper K_1, K_2, K_4, K_5, welche den Zeilen 1, 2, 4, 5 der Tabelle in § 2 entsprechen. Da alle vier Körper von erster Art sind, so ist die Formel XI in § 8 (S. 180) anzuwenden, also

$$\psi(\mu) = \left(\frac{3}{\mu}\right)^{u+2v} \left(\frac{\sigma\mu}{a_1 b_1^2}\right),$$

wo die Einheit σ der Bedingung $\sigma\mu \equiv \pm 1$ (mod. 3) genügen muß, und wo die Zahlen u, v, a_1, b_1 aus den Invarianten a, b des Körpers K so zu bestimmen sind, daß

$$a = 3^u \cdot a_1, \qquad b = 3^v \cdot b_1,$$

und a_1, b_1 nicht durch 3 teilbar werden. Die Einheit σ ist oben schon für jede Zahl μ bestimmt, und zugleich ist

$$\left(\frac{3}{\mu}\right) = \varrho^{2y}, \quad \left(\frac{\sigma\mu}{2}\right) = \varrho^{y+2z};$$

hieraus ergeben sich für unsere vier Körper die folgenden Bestimmungen:

Körper K_1; $k = 6$; $k'' = 1$.

$$a = 2,\ b = 1;\ \ u = 0,\ v = 0;\ \ a_1 = 2,\ b_1 = 1;$$

$$\psi_1(\mu) = \left(\frac{\sigma\mu}{2}\right) = \varrho^{y+2z}.$$

Körper K_2; $k = 9$; $k'' = 1$.

$$a = 3,\ b = 1;\ \ u = 1,\ v = 0;\ \ a_1 = 1,\ b_1 = 1;$$

$$\psi_2(\mu) = \left(\frac{3}{\mu}\right) = \varrho^{2y}.$$

Körper K_4; $k = 18$; $k'' = 3$.

$$a = 6,\ b = 1;\ \ u = 1,\ v = 0;\ a_1 = 2,\ b_1 = 1;$$

$$\psi_4(\mu) = \left(\frac{3}{\mu}\right)\left(\frac{\sigma\mu}{2}\right) = \varrho^{2z}.$$

Körper K_5; $k = 18$; $k'' = 3$.

$$a = 3,\ b = 2;\ \ u = 1,\ v = 0;\ \ a_1 = 1,\ b_1 = 2;$$

$$\psi_5(\mu) = \left(\frac{3}{\mu}\right)\left(\frac{\sigma\mu}{4}\right) = \left(\frac{3}{\mu}\right)\left(\frac{\sigma\mu}{2}\right)^2 = \varrho^{y+z}.$$

Nachdem hiermit die vier letzten Spalten unserer Tabelle ausgefüllt sind, ergeben sich aus diesen Werten von ψ die (nicht äquivalenten) Moduln $\mathfrak{k}_0$, $\mathfrak{k}_1$, $\mathfrak{k}_2$, für welche $\psi(\mathfrak{k}_0) = 1$, $\psi(\mathfrak{k}_1) = \varrho$, $\psi(\mathfrak{k}_2) = \varrho^2$ und deren gemeinsame Anzahl $= k''$ ist:

Körper K_1.

$$\mathfrak{k}_0 = [1,\ 6\varrho],\ \mathfrak{k}_1 = [2,\ 3\varrho],\ \mathfrak{k}_2 = [2,\ 1 + 3\varrho].$$

Körper K_2.

$$\mathfrak{k}_0 = [1,\ 9\varrho],\ \mathfrak{k}_1 = [3,\ 1 + 3\varrho],\ \mathfrak{k}_2 = [3,\ 2 + 3\varrho].$$

Körper K_4.

$$\mathfrak{k}_0 = [1,\ 18\varrho],\ [6,\ 1 + 3\varrho],\ [6,\ 2 + 3\varrho],$$
$$\mathfrak{k}_1 = [2,\ 9\varrho],\ [3,\ 2 + 6\varrho],\ [6,\ 5 + 3\varrho],$$
$$\mathfrak{k}_2 = [2,\ 1 + 9\varrho],\ [3,\ 1 + 6\varrho],\ [6,\ 4 + 3\varrho].$$

Körper K_5.

$$\mathfrak{k}_0 = [1, 18\varrho], [6, 4 + 3\varrho], [6, 5 + 3\varrho],$$
$$\mathfrak{k}_1 = [2, 1 + 9\varrho], [3, 2 + 6\varrho], [6, 2 + 3\varrho],$$
$$\mathfrak{k}_2 = [2, 9\varrho], [3, 1 + 6\varrho], [6, 1 + 3\varrho].$$

Die zu diesen 15 Moduln gehörigen reduzierten quadratischen Formen sind schon früher angegeben, und hiermit sind zugleich die beiden ersten Sätze von Gauß in § 11 durch unsere allgemeine Theorie bestätigt. Um nun für die hier betrachteten vier Körper K_1, K_2, K_4, K_5 auch die entsprechenden Funktionen H_1, H_2, H_4, H_5 zu bestimmen, welche in § 11 (S. 198) in der Form

$$2H = \Sigma' S(\mathfrak{k}_0) - \Sigma' S(\mathfrak{k}_1)$$

dargestellt sind, setzen wir zur Abkürzung

$$U = S[1, 18\varrho] = \Sigma(x^2 + 243y^2)^{-s},$$
$$U_1 = S[3, 1 + 6\varrho] = S[3, 2 + 6\varrho] = \Sigma(9x^2 + 6xy + 28y^2)^{-s},$$
$$U_2 = S[2, 9\varrho] = S[2, 1 + 9\varrho] = \Sigma(4x^2 + 2xy + 61y^2)^{-s},$$
$$U_4 = S[6, 1 + 3\varrho] = S[6, 2 + 3\varrho] = \Sigma(7x^2 + 6xy + 36y^2)^{-s},$$
$$U_5 = S[6, 4 + 3\varrho] = S[6, 5 + 3\varrho] = \Sigma(13x^2 + 4xy + 19y^2)^{-s},$$

ferner

$$V_1 = S[1, 6\varrho] = \Sigma(x^2 + 27y^2)^{-s},$$
$$W_1 = S[2, 3\varrho] = S[2, 1 + 3\varrho] = \Sigma(4x^2 + 2xy + 7y^2)^{-s},$$
$$V_2 = S[1, 9\varrho] = \Sigma(x^2 + xy + 61y^2)^{-s},$$
$$W_2 = S[3, 1 + 3\varrho] = S[3, 2 + 3\varrho] = \Sigma(7x^2 + 3xy + 9y^2)^{-s}$$

und erhalten

$$2H_1 = V_1 - W_1, \quad 2H_2 = V_2 - W_2,$$
$$2H_4 = (U + 2U_4) - (U_1 + U_2 + U_5),$$
$$2H_5 = (U + 2U_5) - (U_1 + U_2 + U_4).$$

Wir wollen jetzt, wie wir schon am Schlusse von § 11 angekündigt haben, diese Beispiele benutzen, um noch einmal auf die in § 10 bewiesene Umformung der Funktion H zurückzukommen. Wir haben dort, wenn k_ν irgendeine Wurzel der Ordnung $k_1 = [1, k\varrho]$ bedeutet, mit $S(k_\nu)$ die Summe der Größen $N(\lambda)^{-s}$ bezeichnet, wo λ alle (von Null verschiedenen) Zahlen des Moduls k_ν durchläuft; wir wollen jetzt unter dem Zeichen k_ν^* den Inbegriff aller derjenigen von diesen Zahlen λ verstehen, welche relative Primzahlen zu k sind, und wollen den von diesen Zahlen herrührenden Teil der Summe $S(k_\nu)$ mit $S(k_\nu^*)$

bezeichnen; offenbar ist diese letztere Summe identisch mit der am Schlusse von § 9 erklärten Summe $S(\mathfrak{R}\nu)$, und der in § 10 bewiesene Satz lautet

$$6H = \Sigma\,\psi(\nu)\,S(k_\nu^*) = \Sigma\,\psi(\nu)\,S(k_\nu),$$

wo k_ν alle Wurzeln der Ordnung k_1 durchläuft. Wir haben dann in § 11 die zweite Summe durch die Betrachtung der Paare von konjugierten Moduln und der Tripel von äquivalenten Moduln vereinfacht, und da dieselbe Vereinfachung offenbar auch für die erste Summe gilt, so nimmt der vorstehende Satz die folgende Form an:

$$2H = \Sigma' S(\mathfrak{k}_0^*) - \Sigma' S(\mathfrak{k}_1^*) = \Sigma' S(\mathfrak{k}_0) - \Sigma' S(\mathfrak{k}_1),$$

wo die Summationen nur auf alle nicht äquivalenten Moduln $\mathfrak{k}_0$, $\mathfrak{k}_1$ auszudehnen sind. Diese beiden Ausdrücke für $2H$ unterscheiden sich dadurch voneinander, daß in beiden Bestandteilen des ersten Ausdrucks nur solche Glieder $N(\lambda)^{-s}$ auftreten, in welchen λ, also auch $N(\lambda)$ relative Primzahl zu k ist, während in beiden Bestandteilen des zweiten Ausdrucks auch solche Glieder $N(\lambda)^{-s}$ auftreten, in welchen $N(\lambda)$ nicht relative Primzahl zu k ist, und der Satz besteht also darin, daß diese letzteren Glieder sich gegenseitig aufheben. Dies wollen wir jetzt wenigstens an unseren Beispielen bestätigen.

Es ist in § 10 schon gezeigt, daß der größte gemeinsame Teiler von k und irgend einer in k_ν enthaltenen Zahl λ immer mit einer natürlichen Zahl n assoziiert ist, und wenn man $k = mn$ setzt, so überzeugt man sich leicht, daß der Inbegriff aller der in k_ν enthaltenen Zahlen λ, welchen dieselbe Zahl n entspricht, $= n \cdot m_\nu^*$, d. h. der Inbegriff aller mit n multiplizierten Zahlen des Systems m_ν^* ist, und hieraus ergibt sich offenbar der allgemeine Satz

$$S(k_\nu) = \Sigma \frac{S(m_\nu^*)}{n^{2s}},$$

wo das Summenzeichen sich auf alle Zerlegungen $k = mn$ bezieht; multipliziert man mit k^{2s}, so erhält man

$$k^{2s} S(k_\nu) = \Sigma\, m^{2s} S(m_\nu^*),$$

wo m alle natürlichen Divisoren von k durchläuft, und hieraus folgt nach bekannten Regeln (D. § 138, S. 362), wie umgekehrt die Summen von der Form $S(k_\nu^*)$ sich durch Summen von der Form $S(m_\nu)$ darstellen lassen.

Um diesen Satz auf unsere Beispiele anzuwenden, betrachten wir auch die Moduln 3_ν, 2_ν, welche je ein Tripel bilden, und den Modul $1_\nu = [1, \varrho]$ und setzen

$$X = S[1, 3\varrho] = \Sigma(x^2 + xy + 7y^2)^{-s},$$
$$Y = S[1, 2\varrho] = \Sigma(x^2 + 3y^2)^{-s},$$
$$Z = S[1, \varrho] = \Sigma(x^2 + xy + y^2)^{-s}.$$

Bezeichnen wir ferner, falls $S(m_\nu) = M$ gesetzt ist, mit M^* immer die Summe $S(m_\nu^*)$, so erhalten wir die Relationen

$$Z = Z^*,\ Y = Y^* + 2^{-2s}Z^*,\ X = X^* + 3^{-2s}Z^*,$$
$$V_1 - V_1^* = W_1 - W_1^* = 3^{2s}T,$$
$$V_2 - V_2^* = W_2 - W_2^* = 3^{-2s}X,$$
$$U - U^* = 3^{-2s}V_1^* + 2^{-2s}V_2^* + T,$$
$$U_1 - U_1^* = 3^{-2s}V_1^* + 2^{-2s}W_2^* + T,$$
$$U_2 - U_2^* = 3^{-2s}W_1^* + 2^{-2s}V_2^* + T,$$
$$U_4 - U_4^* = U_5 - U_5^* = 3^{-2s}W_1^* + 2^{-2s}W_2^* + T,$$

wo zur Abkürzung

$$T = 6^{-2s}X^* + 9^{-2s}Y^* + (18)^{-2s}Z^*$$

gesetzt ist, und hieraus folgt

$$2H_1 = V_1 - W_1 = V_1^* - W_1^*,$$
$$2H_2 = V_2 - W_2 = V_2^* - W_2^*,$$
$$2H_4 = (U + 2U_4) - (U_1 + U_2 + U_5)$$
$$= (U^* + 2U_4^*) - (U_1^* + U_2^* + U_5^*),$$
$$2H_5 = (U + 2U_5) - (U_1 + U_2 + U_4)$$
$$= (U^* + 2U_5^*) - (U_1^* + U_2^* + U_4^*),$$

wodurch die in § 10 bewiesene Umformung bestätigt wird.

Bei der Besprechung des zweiten Satzes von Gauß über den kubischen Charakter der Zahl 3 haben wir bemerkt, daß derselbe vollständig mit unserer Theorie übereinstimmt, obgleich Gauß die Darstellung der Primzahlen p durch quadratische Formen von der Diskriminante $-3 \cdot (18)^2$ benutzt, während schon die Darstellung durch quadratische Formen von der Diskriminante $-3 \cdot 9^2$ dieselbe Entscheidung liefert; jede der letzteren Formen löst sich gewissermaßen in drei Formen der höheren Diskriminante auf. Ganz dasselbe gilt von dem ersten Satze über den kubischen Charakter der Zahl 2; jede der von Gauß (in Übereinstimmung mit unserer Theorie) betrachteten Formen der Diskriminante $-3 \cdot 6^2$ könnte durch drei entsprechende Formen der höheren Diskriminante $-3\cdot(18)^2$ ersetzt werden. Aber um so wichtiger ist es hervorzuheben, daß die Wahl der einen oder der anderen Diskriminante durchaus nicht freisteht, wenn es sich um die Herstellung der Funktion

$$2H = \Sigma' S(\mathfrak{k}_0) - \Sigma' S(\mathfrak{k}_1)$$

handelt. In der Tat, wollte man (nach § 11) die Formen von den Diskriminanten $-3\cdot 6^2$ und $-3\cdot 9^2$ durch je drei entsprechende Formen der Diskriminante $-3\cdot(18)^2$ ersetzen, so würde man für $2H_1$ und $2H_2$ die beiden Ausdrücke

$$P_1 = (U + 2U_1) - (U_2 + U_4 + U_5),$$
$$P_2 = (U + 2U_2) - (U_1 + U_4 + U_5)$$

erhalten, die aber von den oben gefundenen Ausdrücken $(V_1 - W_1)$ und $(V_2 - W_2)$ wesentlich verschieden sind. Behält man von den Gliedern $N(\lambda)^{-s}$ dieser Summen nur diejenigen bei, in denen $N(\lambda)$ relative Primzahl zu 18 ist, so erhält man die beiden entsprechenden Ausdrücke

$$P_1^* = (U^* + 2U_1^*) - (U_2^* + U_4^* + U_5^*),$$
$$P_2^* = (U^* + 2U_2^*) - (U_1^* + U_4^* + U_5^*),$$

und aus den obigen Formeln ergibt sich

$$P_1 = P_1^* + 3\cdot 3^{-2s}(V_1^* - W_1^*),$$
$$P_2 = P_2^* + 3\cdot 2^{-2s}(V_2^* - W_2^*).$$

Hieraus folgt zunächst, daß P_1, P_2 bzw. verschieden sind von P_1^*, P_2^*; ferner leuchtet aus der ersten Gleichung ein, daß P_1 auch von $2H_1$, d. h. von $(V_1^* - W_1^*)$ verschieden ist, weil sonst das Aggregat P_1^* auch solche Glieder $N(\lambda)^{-s}$ enthalten müßte, in denen $N(\lambda)$ durch 3 teilbar ist, was nicht der Fall ist; daß aber auch P_2 verschieden von $2H_2$, d. h. von $(V_2^* - W_2^*)$ ist, folgt aus der zweiten Gleichung erst dann, wenn man aus §§ 6, 7 noch die Tatsache hinzuzieht, daß H_2 von der Form $(1 - 2^{-2s})^{-1}M$ ist, wo M nur solche Glieder $N(\lambda)^{-s}$ enthält, in denen $N(\lambda)$ relative Primzahl zu 2 ist.

Um nun den Zusammenhang zwischen den Funktionen H_1, P_1, P_1^* und den zwischen H_2, P_2, P_2^* vollständig aufzuklären, wollen wir bemerken, daß außer dem obigen Satze über die Zerlegung der Summe $k^{2s}S(k_\nu)$ in Summen von der Form $m^{2s}S(m_\nu^*)$ noch eine Reihe von Relationen zwischen unseren Summen $S(m_\nu)$ besteht, die mit der Transformation der elliptischen Funktionen nahe zusammenhängen, und denen ebenso viele Relationen zwischen den Summen $S(m_\nu^*)$ entsprechen.

Für unseren Zweck genügt es, den einfachsten Fall dieses allgemeinen Satzes zu betrachten, der sich in sehr verschiedenen Einkleidungen darstellen läßt; wir wählen die folgende. Sind α, β zwei Konstanten von irrationalem Verhältnis, und ist p eine natürliche Primzahl, so bilden wir zwei Systeme von je $(p+1)$ zweigliedrigen Moduln; das erste System $\mathfrak{M}_1$ soll aus den $(p+1)$ Moduln

$$[\alpha, \beta], \quad [p\alpha, p\beta], \quad [p\alpha, p\beta], \quad \cdots [p\alpha, p\beta]$$

bestehen, welche mit Ausnahme des ersten $[\alpha, \beta]$ sämtlich mit $[p\alpha, p\beta]$ identisch sind, während das zweite System $\mathfrak{M}_2$ aus den $(p+1)$ Moduln

$$[\alpha, p\beta], \quad [p\alpha, \beta], \quad [p\alpha, \alpha+\beta], \quad \cdots [p\alpha, (p-1)\alpha+\beta]$$

bestehen soll, welche mit Ausnahme des ersten $[\alpha, p\beta]$ von der Form $[p\alpha, c\alpha+\beta]$ sind, wo c die p Zahlen $0, 1, 2 \cdots (p-1)$ durchläuft. Alle in diesen $(2p+2)$ Moduln enthaltenen Zahlen λ sind von der Form $\lambda = x\alpha + y\beta$, wo x, y ganze rationale Zahlen bedeuten, und jede solche Zahl λ tritt, wie der Leser leicht finden wird, ebensooft in den Moduln des Systems $\mathfrak{M}_1$ wie in den Moduln des Systems $\mathfrak{M}_2$ auf; sind nämlich beide Zahlen x, y durch p teilbar, so ist λ in allen $(p+1)$ Moduln des Systems $\mathfrak{M}_1$ und in allen $(p+1)$ Moduln des Systems $\mathfrak{M}_2$ enthalten; ist aber mindestens eine der beiden Zahlen x, y unteilbar durch p, so ist λ in einem einzigen Modul des Systems $\mathfrak{M}_1$ und in einem einzigen Modul des Systems $\mathfrak{M}_2$ enthalten. Man kann daher sagen, daß $\mathfrak{M}_1$ und $\mathfrak{M}_2$ denselben Gehalt von Zahlen λ besitzen, wobei zugleich die Häufigkeit des Auftretens dieser Zahlen berücksichtigt werden soll. Wir nehmen jetzt ferner an, daß das Verhältnis der Konstanten α, β nicht reell ist, und setzen wie früher $N(\lambda) = \lambda\lambda' = (x\alpha + y\beta)(x\alpha' + y\beta')$, wo λ' die mit λ konjugierte komplexe Zahl bedeutet, und

$$S[\alpha, \beta] = \Sigma N(\lambda)^{-s},$$

wo λ alle von Null verschiedenen Zahlen des Moduls $[\alpha, \beta]$ einfach durchläuft, während die Konstante $s > 1$ ist; dann folgt aus der obigen Übereinstimmung der Systeme $\mathfrak{M}_1$, $\mathfrak{M}_2$ der Satz

$$S[\alpha, \beta] + pS[p\alpha, p\beta] = S[\alpha, p\beta] + \Sigma S[p\alpha, c\alpha + \beta],$$

wo das Summenzeichen Σ sich auf die p Zahlen c bezieht; die linke Seite dieser Gleichung läßt sich offenbar auch in der Form

$$(1 + p \cdot p^{-2s}) S[\alpha, \beta]$$

darstellen, und die Beispiele $p = 2$, $p = 3$ liefern die beiden folgenden Sätze

$$(1 + 2 \cdot 2^{-2s}) S[\alpha, \beta] = S[\alpha, 2\beta] + S[2\alpha, \beta] + S[2\alpha, \alpha + \beta],$$
$$(1 + 3 \cdot 3^{-2s}) S[\alpha, \beta] = S[\alpha, 3\beta] + S[3\alpha, \beta] + S[3\alpha, \alpha + \beta] + S[3\alpha, 2\alpha + \beta].$$

Wendet man den ersten Satz auf die vier Moduln

$$[\alpha, \beta] = [1, \varrho], \quad [1, 3\varrho], \quad [1, 9\varrho], \quad [3, 1 + 3\varrho],$$

den zweiten auf die fünf Moduln

$$[\alpha, \beta] = [1, \varrho], \quad [1, 2\varrho], \quad [1, 3\varrho], \quad [1, 6\varrho], \quad [2, 3\varrho]$$

an, und berücksichtigt die Identitäten

$$[2, \varrho] = \varrho[1, 2\varrho], \quad [2, 1 + \varrho] = \varrho^2[1, 2\varrho],$$
$$[3, \varrho] = \varrho[1, 3\varrho], \quad [3, 1 + \varrho] = \varrho^2[1, 3\varrho], \quad [3, 2 + \varrho] = (2 + \varrho)[1, \varrho],$$
$$[3, 2\varrho] = \varrho[2, 1 + 3\varrho], \quad [3, 2 + 2\varrho] = \varrho^2[2, 3\varrho], \quad [3, 1 + 2\varrho] = (1 + 2\varrho)[1, 2\varrho],$$
$$[3, 3\varrho] = 3[1, \varrho], \quad [3, 6\varrho] = 3[1, 2\varrho], \quad [6, 3\varrho] = 3\varrho[1, 2\varrho],$$

so erhält man die folgenden neun Relationen

$$(1 + 2 \cdot 2^{-2s}) Z = 3Y; \quad (1 + 3 \cdot 3^{-2s} - 3^{-s}) Z = 3X,$$
$$(1 + 3 \cdot 3^{-2s} - 3^{-s}) Y = (1 + 2 \cdot 2^{-2s}) X = V_1 + 2W_1,$$
$$(1 + 3 \cdot 3^{-2s}) X - 3^{-2s} Z = V_2 + 2W_2,$$
$$(1 + 3 \cdot 3^{-2s}) V_1 - 3^{-2s} Y = U + 2U_1,$$
$$(1 + 3 \cdot 3^{-2s}) W_1 - 3^{-2s} Y = U_2 + U_4 + U_5,$$
$$(1 + 2 \cdot 2^{-2s}) V_2 = U + 2U_2,$$
$$(1 + 2 \cdot 2^{-2s}) W_2 = U_1 + U_4 + U_5,$$

von denen aber nur acht voneinander unabhängig sind.

Drückt man nun jede Summe M nach den obigen Formeln durch Summen von der Form M^* aus, so ergeben sich für die letzteren die einfacheren Relationen

$$(1 - 2^{-2s}) Z^* = 3Y^*; \quad (1 - 3^{-s}) Z^* = 3X^*,$$
$$(1 - 3^{-s}) Y^* = (1 - 2^{-2s}) X^* = V_1^* + 2W_1^*; \quad X^* = V_2^* + 2W_2^*,$$
$$V_1^* = U^* + 2U_1^*; \quad W_1^* = U_2^* + U_4^* + U_5^*,$$
$$(1 - 2^{-2s}) V_2^* = U^* + 2U_2^*; \quad (1 - 2^{-2s}) W_2^* = U_1^* + U_4^* + U_5^*.$$

Wir wollen bemerken, daß man diese letzteren Relationen auch auf einem ganz anderen Wege ableiten kann, bei welchem der leicht zu beweisende Hilfssatz zur Anwendung kommt, daß, wenn μ (ebenso wie ν) relative Primzahl zu k ist, der Inbegriff der durch μ teilbaren Zahlen in k_ν identisch mit $\mu \cdot k_{\nu\mu'}$ ist, wo μ' wieder die mit μ konjugierte

Zahl bedeutet. Ist nun p eine natürliche Primzahl und ν relative Primzahl zu pk, so kann man jede der $\varphi(k)$ Zahlklassen (mod. k), aus welchen das System k_ν^* besteht, in p^2 Zahlklassen (mod. pk) zerlegen, welche sich, wenn p in k aufgeht, in Systeme von der Form $(pk)_\mu^*$ zusammenfassen lassen, während im entgegengesetzten Falle auch noch die Zahlen in k_ν^* zu gruppieren sind, welche nicht relative Primzahlen zu p sind. Für unseren Zweck genügt es, die Resultate für die beiden Primzahlen $p = 2$, $p = 3$ anzugeben. Ist k gerade, so besteht das System k_ν^* aus den beiden Systemen

$$(2k)_\nu^*, \quad (2k)_{\nu(1+k\varrho)}^*,$$

d. h. jede in k_ν^* enthaltene Zahl findet sich in einem und nur einem dieser beiden Systeme, und umgekehrt sind alle Zahlen dieser beiden Systeme auch in k_ν^* enthalten. Ist aber k ungerade, so besteht k_ν^* aus den vier Systemen

$$2 \cdot k_\nu^*, \quad (2k)_\nu^*, \quad (2k)_{\nu(1+k\varrho)}^*, \quad (2k)_{\nu(1+k\varrho^2)}^*,$$

deren erstes der Inbegriff aller mit 2 multiplizierten Zahlen des Systems k_ν^* ist. Wenn ferner k durch 3 teilbar ist, so besteht k_ν^* aus den drei Systemen

$$(3k)_\nu^*, \quad (3k)_{\nu(1+k\varrho)}^*, \quad (3k)_{\nu(1+k\varrho^2)}^*,$$

und wenn k nicht durch 3 teilbar ist, so besteht k_ν^* aus den vier Systemen

$$(1-\varrho) \cdot k_{\nu(2+\varrho)}^*, \quad (3k)_\nu^*, \quad (3k)_{\nu(3+k\varrho)}^*, \quad (3k)_{\nu(3+k\varrho^2)}^*.$$

Der erste dieser vier Sätze kann hier nicht zur Anwendung kommen, weil 18 nicht durch 4 teilbar ist; wendet man aber den zweiten, dritten, vierten Satz bzw. auf die Beispiele

$$k_\nu = [1, \varrho], \quad [1, 3\varrho], \quad [1, 9\varrho], \quad [3, 1+3\varrho],$$
$$k_\nu = [1, 3\varrho], \quad [1, 6\varrho], \quad [2, 3\varrho],$$
$$k_\nu = [1, \varrho], \quad [1, 2\varrho]$$

an und bildet die entsprechenden Summen $S(k_\nu^*)$, so erhält man die obigen neun Relationen zwischen den Funktionen M^*, von denen die eine aus den übrigen folgt.

Aus den letzten vier dieser Relationen ergeben sich nun für die oben mit P_1^*, P_2^* bezeichneten Aggregate die Ausdrücke

$$P_1^* = V_1^* - W_1^*, \quad P_2^* = (1 - 2^{-2s})(V_2^* - W_2^*),$$

deren Form sich dadurch erklärt, daß jede relative Primzahl zu 6 auch relative Primzahl zu 18 ist, während die relativen Primzahlen zu 9 nicht alle auch relative Primzahlen zu 18 sind. Berücksichtigt man noch die oben gefundenen Beziehungen zwischen P_1^*, P_2^* und P_1, P_2, so vervollständigen sich unsere früheren Ausdrücke für die beiden Funktionen $2H_1$, $2H_2$ in folgender Weise:

$$2H_1 = V_1 - W_1 = V_1^* - W_1^* = P_1^* = \frac{P_1}{1 + 3 \cdot 3^{-2s}},$$

$$2H_2 = V_2 - W_2 = V_2^* - W_2^* = \frac{P_2^*}{1 - 2^{-2s}} = \frac{P_2}{1 + 2 \cdot 2^{-2s}},$$

und hiermit ist unsere Absicht, diese Funktionen durch die Formen der Diskriminante $-3\,(18)^2$ darzustellen, wirklich erreicht.

§ 13.

Der Grenzsatz von Kronecker.

Nachdem wir durch die vorhergehenden Beispiele die Bildung des Charakters ψ, der Moduln k_ν, und hiermit auch der Funktion

$$2H = \Sigma' S(\mathfrak{k}_0) - \Sigma' S(\mathfrak{k}_1)$$

hinreichend erläutert haben, wenden wir uns zur Lösung der Aufgabe, welche wir uns in § 6 gestellt haben. Es handelt sich darum, die Anzahl h der Idealklassen des reinen kubischen Körpers K durch die wirkliche Ausführung des in der Gleichung

$$h\,\frac{2\pi \log \varepsilon}{k\sqrt{3}} = \lim\,(s-1)J$$

angedeuteten Grenzprozesses zu bestimmen, welcher darin besteht, daß die positive Variable $(s-1)$ unendlich klein wird. In § 7 ist die Dirichletsche Idealfunktion J in die beiden Faktoren G, H zerlegt, von denen der erste die über alle natürlichen Zahlen n ausgedehnte Summe

$$G = \sum \frac{1}{n^s}$$

ist, während der zweite Faktor H nach manchen Umformungen in § 11 die obige Gestalt angenommen hat. Da nun bekanntlich

$$\lim\,(s-1)\,G = 1$$

ist, so wird

$$h\,\frac{2\pi \log \varepsilon}{k\sqrt{3}} = \lim H,$$

und dieser Grenzwert läßt sich mit Hilfe eines berühmten Satzes von Kronecker leicht bestimmen. Da die Anzahl k'' der nicht äquivalenten Moduln $\mathfrak{k}_0$ mit der der Moduln $\mathfrak{k}_1$ übereinstimmt, so genügt hierzu schon der Ausdruck für den Grenzwert der Differenz

$$\Sigma(A x^2 + B x y + C y^2)^{-s} - \Sigma(A_1 x^2 + B_1 x y + C_1 y^2)^{-s},$$

wo $(A, \frac{1}{2}B, C)$, $(A_1, \frac{1}{2}B_1, C_1)$ irgend zwei positive Formen von derselben negativen Diskriminante $D = B^2 - 4AC$ bedeuten. Die Darstellung dieses Grenzwertes durch Thetafunktionen hat Kronecker zuerst im Monatsbericht der Berliner Akademie vom 22. Januar 1863 ohne Beweis mitgeteilt. Es lag nun nahe, diesen ersten Satz als Ausfluß eines zweiten aufzufassen, durch welchen das Verhalten der von einer einzelnen Form $(A, \frac{1}{2}B, C)$ erzeugten Summe

$$\Sigma(A x^2 + B x y + C y^2)^{-s}$$

für unendlich kleine positive Werte von $(s - 1)$ genauer ermittelt wird. Bekanntlich hat Dirichlet zuerst bewiesen, daß diese Funktion unendlich groß wird wie

$$\frac{2\pi}{(s-1)\sqrt{-D}},$$

und hierin besteht eine wesentliche Grundlage seiner Methode, die Klassenanzahl der Formen von der negativen Diskriminante D zu bestimmen. Jetzt kam es darauf an, einen Schritt weiter zu gehen, nämlich den endlichen Grenzwert der Differenz

$$\Sigma(A x^2 + B x y + C y^2)^{-s} - \frac{2\pi}{(s-1)\sqrt{-D}}$$

zu ermitteln. Diese Aufgabe ist zuerst für beliebige reelle Koeffizienten A, B, C von H. Weber in einem an mich gerichteten Briefe vom 12. Oktober 1881 vollständig gelöst, dessen Inhalt er später veröffentlicht hat im Bd. 33 der Mathematischen Annalen (1889) und in § 113 seines Werkes „Elliptische Funktionen und Algebraische Zahlen“ (1891). Inzwischen ist aber auch Kronecker in zahlreichen Aufsätzen über die elliptischen Funktionen auf diesen Gegenstand zurückgekommen; schon im Sitzungsberichte der Berliner Akademie vom 30. Juli 1885 findet sich seine, von der Weberschen wesentlich verschiedene Ableitung des fraglichen Grenzwertes, zunächst für rationale Koeffizienten, und endlich hat er im Sitzungsberichte vom

21. Februar 1889 den Satz auch auf Formen mit komplexen Koeffizienten ausgedehnt. Wir beschränken uns hier auf Formen mit reellen Koeffizienten und stellen den Satz in der für unseren Zweck geeigneten Form folgendermaßen dar.

Es seien α und $\beta = \alpha\omega$ irgend zwei komplexe Konstanten von imaginärem Verhältnis ω, und zwar setzen wir fest, daß der reelle Teil von $i\omega$ negativ sei; bezeichnen wir immer mit α' die mit α konjugierte komplexe Zahl und mit $N(\alpha)$ das stets positive Produkt $\alpha\alpha'$, so können wir dies auch durch die Bedingung

$$\Delta = i(\alpha\beta' - \beta\alpha') = i(\omega' - \omega) N(\alpha) > 0$$

ausdrücken, und wir nennen zugleich α die erste, β die zweite Basiszahl des binären Moduls $\mathfrak{k} = [\alpha, \beta] = \alpha[1, \omega]$, dessen Zahlen von der Form $\lambda = \alpha x + \beta y$ sind, wo x, y alle ganzen rationalen Zahlen durchlaufen. Sind α_1 und $\beta_1 = \alpha_1\omega_1$ ebenfalls eine erste und zweite Basiszahl desselben Moduls $\mathfrak{k} = [\alpha, \beta] = [\alpha_1, \beta_1]$, so bestehen zwischen diesen beiden Basen Relationen von der Form

$$\alpha_1 = a\alpha + c\beta, \quad \beta_1 = b\alpha + d\beta,$$

wo a, b, c, d vier ganze rationale Zahlen bedeuten, die der Bedingung

$$ad - bc = +1$$

genügen (vgl. § 11). Hieraus geht hervor, daß die oben mit Δ bezeichnete positive Größe eine Invariante des Moduls $\mathfrak{k}$, d. h. unabhängig von der Wahl seiner Basis ist. Bedient man sich ferner einer in der Theorie der elliptischen Modulfunktionen üblichen Ausdrucksweise*), so gehören die durch die Gleichung

$$\omega_1 = \frac{b + d\omega}{a + c\omega}$$

verbundenen Zahlen ω, ω_1 derselben Klasse äquivalenter Zahlen an, und diese Klasse ist also ebenfalls eine Invariante des Moduls $\mathfrak{k}$, oder vielmehr eine Invariante der Modulklasse, welche aus allen mit $\mathfrak{k}$ äquivalenten Moduln besteht. Von hervorragender Wichtigkeit für die eben genannte Theorie ist die Funktion

$$\eta(\omega) = e^{\frac{\pi i \omega}{12}} \Pi(1 - e^{2\pi i \omega n}),$$

*) Vgl. meinen Aufsatz in diesem Journal, Bd. 83, und meine Erläuterungen zum Fragment XXVIII in der zweiten Auflage von Riemanns Werken (1892). Eine ausführliche Darstellung der ganzen Theorie findet man in dem oben zitierten Werke von H. Weber und in den Vorlesungen über die Theorie der elliptischen Modulfunktionen von F. Klein und R. Fricke (1890—1892).

wo n in dem Produkte Π alle natürlichen Zahlen durchläuft; das Gesetz ihrer linearen Transformation wird durch die Gleichung

$$\eta(\omega_1) = r(a + c\omega)^{1/2}\eta(\omega)$$

ausgedrückt, wo $r^{24} = 1$ und ω_1 die obige Bedeutung hat; berücksichtigt man noch, daß $\eta(-\omega')$ die mit $\eta(\omega)$ konjugierte Größe, und daß

$$\omega_1' - \omega_1 = \frac{\omega' - \omega}{(a + c\omega)(a + c\omega')}$$

ist, so ergibt sich hieraus leicht, daß die Größe

$$H(\omega) = H(-\omega') = \eta(\omega)\eta(-\omega')\sqrt{i(\omega' - \omega)},$$

wo die Quadratwurzel immer positiv genommen werden soll, für alle mit ω äquivalenten Zahlen einen und denselben positiven Wert besitzt, welcher mithin eine Invariante der aus allen diesen Zahlen bestehenden Klasse ist. Durchläuft nun λ alle von Null verschiedenen Zahlen des Moduls $\mathfrak{k}$, und bezeichnen wir (wie in §§ 10, 11, 12) mit $S(\mathfrak{k})$ die Summe aller entsprechenden Potenzen $N(\lambda)^{-s}$, so besteht der Satz von Kronecker darin, daß

$$S(\mathfrak{k}) = \frac{2\pi}{\Delta}\left\{\frac{1}{s-1} - 2\Gamma'(1) - \log\Delta - 2\log H(\omega)\right\} + (0)$$

ist, wo die Funktion (0) gleichzeitig mit $(s-1)$ unendlich klein wird, während $-\Gamma'(1) = 0{,}5772\cdots$ die bekannte Eulersche Konstante ist.

Um nun diesen Satz auf unsere Moduln $\mathfrak{k} = k_\nu$ anzuwenden, bemerken wir zunächst, daß die obige Unterscheidung zwischen der ersten und zweiten Basiszahl mit der in § 11 festgesetzten übereinstimmt, wenn wir jetzt noch annehmen, daß dort unter ϱ immer diejenige Kubikwurzel der Einheit verstanden wird, für welche

$$1 + 2\varrho = \sqrt{-3} = i\sqrt{3}$$

wird, wo $\sqrt{3}$ positiv zu nehmen ist; behält man die dortigen Bezeichnungen bei, so wird zugleich

$$\Delta = i(\alpha\beta' - \beta\alpha') = k\sqrt{3}$$

und

$$\omega = \frac{\beta}{\alpha} = \frac{b_1 + b_2\varrho}{a_1 + a_2\varrho} = \frac{B + ik\sqrt{3}}{2A},$$

wo $(A, \frac{1}{2}B, C)$ wieder die der Basis α, β entsprechende binäre quadratische Form bedeutet. Hat man nun für jeden der k'' Moduln $\mathfrak{k}_0$

und für jeden der k'' Moduln $\mathfrak{k}_1$ nach Belieben eine Basis α, β gewählt, und bezeichnet man mit ω_0, ω_1 die entsprechenden Werte von ω, so liefert der Satz von Kronecker das Resultat

$$\lim H = \frac{2\pi}{k\sqrt{3}}\left\{\Sigma' \log H(\omega_1) - \Sigma' \log H(\omega_0)\right\},$$

und hieraus ergibt sich die Bestimmung der Anzahl h der Idealklassen im Körper K durch die Gleichung

$$\varepsilon^h = \frac{\Pi H(\omega_1)}{\Pi H(\omega_0)},$$

wo ε die Fundamentaleinheit des Körpers K bedeutet, und wo die Produktzeichen Π im Nenner und Zähler sich auf alle nicht äquivalenten Zahlen ω_0, ω_1 beziehen.

Mit diesem Resultat, in welchem der Zusammenhang zwischen den reinen kubischen Körpern und den aus der komplexen Multiplikation der elliptischen Funktionen entspringenden algebraischen Zahlkörpern enthalten ist, brechen wir die gegenwärtige Abhandlung ab; doch fügen wir noch die folgenden Bemerkungen hinzu, die sich auf die wirkliche Berechnung der Klassenanzahl h beziehen. Für diesen Zweck ist, wie wir gestehen müssen, die Brauchbarkeit des gewonnenen Resultats noch an gewisse Bedingungen gebunden, die zurzeit keineswegs als allgemein erfüllt anzusehen sind. Vor allem ist zu bemerken, daß hierzu die Kenntnis der Fundamentaleinheit ε des Körpers K erforderlich ist; nun haben sich zwar verschiedene ausgezeichnete Mathematiker damit beschäftigt, die zuerst von Jacobi*) angegebene und an einigen Beispielen durchgeführte Methode zu vervollkommnen, aber ein einfacher und zugleich nachweislich unfehlbarer Weg zur Gewinnung von ε, der sich mit der Lösung der Pellschen Gleichung in der Theorie der quadratischen Körper vergleichen ließe, ist meines Wissens bisher noch immer nicht gefunden. Für die Beispiele der in § 2 aufgestellten Tabelle ist es freilich ohne große Mühe möglich, die Aufgabe zu lösen, und zwar gelingt dies meistens durch die Zerlegung einiger wenigen Zahlen des Körpers in ihre idealen Primfaktoren; für diejenigen, welche solche Berechnungen anstellen mögen, bemerke ich folgendes. Gibt man den Buchstaben

*) Allgemeine Theorie der kettenbruchähnlichen Algorithmen, in welchen jede Zahl aus drei vorhergehenden gebildet wird (Journal für reine und angewandte Mathematik, Bd. 69).

a, b, α, β wieder dieselbe Bedeutung wie in § 2, so findet man leicht, daß jede im Körper K enthaltene Zahl

$$\varkappa = z + x\alpha + y\beta,$$

von deren rationalen Koordinaten z, x, y höchstens eine verschwindet, auch als Quotient in den Formen

$$\varkappa = \frac{y_1\alpha - bx_1}{bx - y\alpha} = \frac{x_1\beta - ay_1}{ay - x\beta} = \frac{z_1 - y_1\beta}{z - x\alpha} = \frac{z_1 - x_1\alpha}{z - y\beta}$$

darstellbar ist, wo

$$z_1 = z^2 - abxy, \quad x_1 = ay^2 - zx, \quad y_1 = bx^2 - zy$$

die Koordinaten ihres Supplements

$$\varkappa'\varkappa'' = z_1 + x_1\alpha + y_1\beta$$

bedeuten. Hierdurch wird man veranlaßt, nur solche Zahlen $\varkappa$ zu betrachten, in welchen eine der Koordinaten x, y verschwindet, während die beiden anderen ganze Zahlen ohne gemeinsamen Teiler sind; eine solche Zahl $\varkappa$ ist nur durch Primideale ersten Grades teilbar, und $\varkappa$ kann auch nicht durch zwei verschiedene, in derselben natürlichen Primzahl p aufgehende Primideale teilbar sein, ausgenommen den Fall $p = 3$ bei den Körpern zweiter Art, wo $\mathfrak{o}\,3 = \mathfrak{p}^2\mathfrak{p}_1$, und wo jede Zahl $\varkappa$ entweder relative Primzahl zu 3 oder teilbar durch $\mathfrak{p}\mathfrak{p}_1$, aber niemals teilbar durch $\mathfrak{p}^2$ ist. Auf Grund dieser Eigenschaften schließt man aus der Norm von $\varkappa$, welche die leicht zu berechnende Form $z^3 + ab^2x^3$ oder $z^3 + a^2by^3$ hat, sofort auf die Zerlegung des Ideals $\mathfrak{o}\varkappa$ in seine Primfaktoren. Um zu bewirken, daß eine solche Zahl $\varkappa$ durch ein in der natürlichen Primzahl p aufgehendes Primideal ersten Grades $\mathfrak{p}$ teilbar wird, braucht man nur mit Hilfe des Canon Arithmeticus die beiden rationalen Zahlen u, v zu bestimmen, für welche $\alpha \equiv u$, $\beta \equiv v \pmod{\mathfrak{p}}$, also $u^3 \equiv ab^2$, $v^3 \equiv a^2b$, $uv \equiv ab \pmod{p}$ wird; dann ist der Modul $[p, \alpha - u, \beta - v]$ das kleinste gemeinsame Vielfache $\mathfrak{p} - \mathfrak{n}$ von $\mathfrak{p}$ und der Ordnung $\mathfrak{n} = [1, \alpha, \beta]$, und unter den in ihm enthaltenen Zahlen $\varkappa$ wird man vorzugsweise diejenigen wählen, deren Koordinaten so klein wie möglich sind. In allen Beispielen der Tabelle in § 2 und einigen anderen, die ich untersucht habe, findet man bald, daß aus wenigen so zerlegten Zahlen $\varkappa$ sich zwei Produkte von verschiedenem Absolutwert bilden lassen, welche aus denselben Primidealen zusammengesetzt sind, deren Quotient folglich eine irrationale

Einheit ist. Die Aufsuchung der Fundamentaleinheit ε, welche hierdurch bekanntlich in endliche Grenzen eingeschlossen ist, kann freilich noch ziemlich mühselig sein, obgleich die Anzahl der anzustellenden Versuche durch Zuziehung gewisser Kongruenzen sich noch beschränken läßt.

Am Schlusse der in der Einleitung erwähnten Abhandlung gibt Herr Markoff eine wertvolle Tabelle von Einheiten für diejenigen 52 aus $\alpha = \sqrt[3]{ab^2}$ gebildeten Körper, in welchen $ab^2 \leqq 70$ ist (von den 54 in der Tabelle angegebenen Einheiten treten zwei je zweimal auf, die eine bei $ab^2 = 12$ und $ab^2 = 18$, die andere bei $ab^2 = 20$ und $ab^2 = 50$); daß der von ihm eingeschlagene Weg der Berechnung mit dem eben beschriebenen wesentlich übereinstimmt, geht teils aus der Darstellungsform dieser Einheiten hervor, teils aus der in § 5 (S. 20) enthaltenen Bemerkung: „Ne nous arrêtant pas aux méthodes sûres mais fatigantes pour déterminer l'unité complexe fondamentale nous remarquons, que pour les valeurs petites de a et b il est facile de trouver les unités complexes par le tâtonnement en considérant plusieurs nombres ξ composés des mêmes facteurs premiers“. Unter diesen 52 Körpern befinden sich auch alle in meiner Tabelle (§ 2) angegebenen 21 Körper ($ab \leqq 23$), und die in diesem Umfange angestellte Vergleichung mit meinen Rechnungen hat ergeben, daß die von Herrn Markoff gefundenen Einheiten sämtlich fundamental sind mit einziger Ausnahme des Beispiels $ab^2 = 28$, in welchem die von ihm angegebene Einheit das Quadrat der Fundamentaleinheit ist.

Während die von Herrn Markoff und mir angewandte Methode auf der Zerlegung der Zahlen in ihre idealen Primfaktoren beruht, hat Herr Mehmke schon seit dem Jahre 1885 den zuerst von Jacobi angegebenen, später von Herrn Bachmann*) behandelten Algorithmus der Annäherung wieder aufgenommen und durch gewisse Modifikationen zu vervollkommnen gesucht, worüber er mir brieflich in den Jahren 1889 bis 1893 interessante Mitteilungen gemacht hat, die mir die Veröffentlichung seiner Methoden sehr wünschenswert erscheinen lassen; mit bestem Danke erwähne ich einer von ihm

---

*) Zur Theorie von Jacobis Kettenbruch-Algorithmen (dieses Journal Bd. 75, 1873). Vgl. Fr. Meyer, Über kettenbruchähnliche Algorithmen (Verhandlungen des Mathematikerkongresses in Zürich 1897).

berechneten Tabelle von 39 Einheiten, unter denen sich acht auf die Beispiele $ab^2 = 76, 124, 126, 140, 198, 207, 234, 350$ beziehen, also nicht in der Markoffschen Tabelle enthalten sind.

Die weiter unten zu benutzenden Fundamentaleinheiten ε der in § 12 mit K_1, K_2, K_4, K_5 bezeichneten Körper und ihre reziproken Werte ε^{-1} sind die folgenden:

$$\begin{aligned} \varepsilon_1 &= 1 + \alpha + \beta, & \varepsilon_1^{-1} &= -1 + \alpha, \\ \varepsilon_2 &= 4 + 3\alpha + 2\beta, & \varepsilon_2^{-1} &= -2 + \beta, \\ \varepsilon_4 &= 109 + 60\alpha + 33\beta, & \varepsilon_4^{-1} &= 1 - 6\alpha + 3\beta, \\ \varepsilon_5 &= 55 + 24\alpha + 21\beta, & \varepsilon_5^{-1} &= 1 + 3\alpha - 3\beta. \end{aligned}$$

Wenden wir uns jetzt zu der Berechnung der Funktion $H(\omega)$, welche für alle einander äquivalenten Zahlen ω denselben Wert besitzt, so ist es vorteilhaft, für den Repräsentanten einer solchen Klasse immer die in derselben enthaltene reduzierte Zahl ω zu wählen, welche den Bedingungen

$$-1 \leqq \omega + \omega' \leqq +1, \quad \omega\omega' \geqq 1$$

genügt, weil dann der analytische Modul (oder absolute Betrag) von $e^{2\pi i\omega}$ bekanntlich so klein wie möglich wird; da es ohnehin feststeht, daß h eine ganze Zahl ist, so genügt in der Regel die Annäherung

$$\eta(\omega) = e^{\frac{\pi i \omega}{12}}, \quad \eta(-\omega') = e^{-\frac{\pi i \omega'}{12}},$$

$$H(\omega) = e^{-\frac{\pi i(\omega' - \omega)}{12}} \sqrt{i(\omega' - \omega)}.$$

Setzt man wie oben

$$\omega = \frac{B + ik\sqrt{3}}{2A}, \quad -\omega' = \frac{-B + ik\sqrt{3}}{2A}, \quad i(\omega' - \omega) = \frac{k\sqrt{3}}{A},$$

wo $(A, \frac{1}{2}B, C)$ die der reduzierten Zahl ω entsprechende reduzierte Form von der Diskriminante $B^2 - 4AC = D = -3k^2$ bedeutet, so wird

$$\log H(\omega) = -\frac{\pi k \sqrt{3}}{12 A} - \tfrac{1}{2} \log A + \tfrac{1}{2} \log (k\sqrt{3});$$

setzt man hierin für ω die k'' Werte ω_0 und die k'' Werte ω_1 ein und bezeichnet die entsprechenden Werte von A mit A_0 und A_1, so ergibt sich

$$h \log \varepsilon = \frac{\pi k \sqrt{3}}{12} \left\{ \sum \frac{1}{A_0} - \sum \frac{1}{A_1} \right\} + \tfrac{1}{2} \left\{ \sum \log A_0 - \sum \log A_1 \right\};$$

führt man endlich statt der natürlichen Logarithmen *log* die gemeinen Logarithmen *Log* ein und setzt zur Abkürzung

$$M = \frac{\pi\sqrt{3}}{12}\, Log\, e = 0{,}196\,930\,8\cdots, \quad Log\, M = 0{,}294\,313\,7\cdots - 1,$$

so erhält man die Annäherung

$$h\, Log\, \varepsilon = Mk\left\{\sum \frac{1}{A_0} - \sum \frac{1}{A_1}\right\} + \tfrac{1}{2}\left\{\sum Log\, A_0 - \sum Log\, A_1\right\},$$

welche, wie gesagt, zur Berechnung der ganzen Zahl h in der Regel vollständig ausreicht*). Um eine Probe für die Genauigkeit dieser Formel zu machen, deren rechte Seite mit $\mathfrak{M}$ bezeichnet werden möge, wollen wir sie auf die vier Körper K_1, K_2, K_4, K_5 anwenden, für welche die Werte der Zahlen A_0, A_1 in § 12 angegeben sind; die hiernach zu berechnenden Werte von $\mathfrak{M}$ sind dann mit den obigen Werten der Fundamentaleinheiten ε zu vergleichen.

Körper K_1.

$$k = 6,\ k'' = 1;\ A_0 = 1;\ A_1 = 4;\ \mathfrak{M} = 0{,}585\,158\,6;$$
$$\varepsilon = 3{,}847\,322\,1,\ Log\, \varepsilon = 0{,}585\,158\,5.$$

Körper K_2.

$$k = 9,\ k'' = 1;\ A_0 = 1;\ A_1 = 7;\ \mathfrak{M} = 1{,}096\,631\,5;$$
$$\varepsilon = 12{,}486\,916\,4,\ Log\, \varepsilon = 1{,}096\,455\,0.$$

Körper K_4.

$$k = 18,\ k'' = 3;\ A_0 = 1,\ 7,\ 7;\ A_1 = 4,\ 9,\ 13;\ \mathfrak{M} = 2{,}514\,792\,9;$$
$$\varepsilon = 326{,}990\,833\,6,\ Log\, \varepsilon = 2{,}514\,535\,6.$$

Körper K_5.

$$k = 18,\ k'' = 3;\ A_0 = 1,\ 13,\ 13;\ A_1 = 4,\ 7,\ 9;\ \mathfrak{M} = 2{,}216\,900\,7;$$
$$\varepsilon = 164{,}981\,855\,8,\ Log\, \varepsilon = 2{,}217\,436\,2.$$

In allen diesen Beispielen schließt man aus der obigen Näherungsformel $h\, Log\, \varepsilon = \mathfrak{M}$ mit Sicherheit, daß die Klassenanzahl $h = 1$ ist, weil $\mathfrak{M}$ nahezu mit $Log\, \varepsilon$ übereinstimmt.

Auf dieselbe Weise habe ich die Klassenanzahl h für alle Körper der Tabelle in § 2 und außerdem für die drei Beispiele $ab^2 = 35$, 53, 91 berechnet, denen die Werte $h = 3$, 1, 9 entsprechen.

---

*) Nach einer oberflächlichen Schätzung ist für jede reduzierte Zahl ω der absolute Betrag der Differenz $Log\,\eta(\omega) - \frac{\pi i \omega}{12} Log\, e$ immer $< 0{,}001\,894\,3$.

Bedenkt man, daß für diese Bestimmungsart der Klassenanzahl h außer der Kenntnis der Fundamentaleinheit ε auch die Aufstellung der Moduln $\mathfrak{k}$ und ihrer Charaktere ψ erforderlich ist, welche für größere Werte von ab immer zeitraubender wird, so kann man dem oben gewonnenen Resultate nur einen sehr geringen oder gar keinen praktischen Wert beilegen. Auf Grund des schönen Satzes von Herrn Minkowski*), daß es in jeder Idealklasse mindestens ein Ideal gibt, dessen Norm absolut kleiner ist als die Quadratwurzel aus der Grundzahl des Körpers, gestaltet sich die Berechnung von h viel kürzer; die oben beschriebene Zerlegung der Zahlen $\varkappa$ von der Form $z + x\alpha$ oder $z + y\beta$ in ihre idealen Primfaktoren liefert (in allen 24 von mir behandelten Beispielen) so viele Äquivalenzen zwischen den fraglichen Idealen, daß sie sich wirklich in h Klassen einordnen, und es kommt nur noch darauf an zu zeigen, daß diese Klassen auch voneinander verschieden sind, was meistens keine Schwierigkeit macht; in den Fällen, wo ab durch Primzahlen p von der Form $3m + 1$ teilbar ist, dient hierzu namentlich die Bemerkung, daß $N(z + x\alpha + y\beta) \equiv z^3 \pmod{ab}$, also die Norm jedes Hauptideals kubischer Rest von jeder solchen Primzahl p ist, worauf zugleich die Einteilung der Idealklassen in Geschlechter beruht. Ich bemerke schließlich, daß auch Herr Markoff in § 6 seiner Abhandlung für einige Beispiele die Klassenanzahl h auf ganz ähnliche Weise bestimmt hat.

Ich habe im Vorwort leider versäumt, die kürzlich in der Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich (1897, Jahrgang 42) veröffentlichte nachgelassene Abhandlung: „Zur Theorie der zerlegbaren Formen, insbesondere der kubischen“ von Arnold Meyer zu erwähnen; sie ist schon im Jahre 1870 verfaßt und bietet, abgesehen von der Ermittlung der Idealzahlen, nur wenige Berührungspunkte mit meiner Arbeit dar.

---

*) Théorèmes arithmétiques (Compte rendu der Pariser Akademie vom 26. Januar 1891).

Erläuterungen zur vorstehenden Abhandlung.

Dedekind verwendet in dieser Arbeit zum erstenmal die bekannte Dirichlet-Dedekindsche Grenzformel zur Bestimmung der Klassenanzahl in Körpern, welche nicht Unterkörper eines Kreisteilungskörpers sind, und zwar mit Methoden, die auch für allgemeinere Untersuchungen bedeutungsvoll sind. Die in der Einleitung und früher in der Anzeige der Bachmannschen Vorlesungen ausgesprochene Vermutung, daß die Resultate über den Zusammenhang zwischen kubischen Resten und Klassen der quadratischen Formen auch für beliebige kubische Körper richtig bleiben, ist von Takagi [Comptes rendus **171** (1920), S. 1202—1205] bewiesen. Der Satz folgt als Spezialfall eines allgemeineren Satzes über auflösbare Körper vom Primzahlgrad, und der Beweis beruht auf den allgemeinen Zerlegungsgesetzen in relativ-Abelschen Körpern, entspricht also der Dedekindschen Vermutung, daß das Problem bei beliebigen kubischen Körpern unter Anwendung der Theorie der komplexen Multiplikation behandelt werden könnte. Die Klassenzahl der Körper der komplexen Multiplikation hat zuerst Fueter [Gött. Nachr. **1907**, S. 288—298, Rendiconti di Palermo **29** (1910), S. 380—395] bestimmt.

Zu §§ 1—5. Die in diesen Paragraphen enthaltenen Resultate über Diskriminante und Primidealzerlegung bei reinen kubischen Körpern hätte man auch einfach aus den allgemeineren Abhandlungen XV und XIV, Bd. I folgern können. Die Abhandlung über die Invarianten beliebiger kubischer Körper, die Dedekind in der Einleitung in Aussicht stellt, hat er leider nicht publiziert.

Für allgemeine kubische Körper hat eine Reihe von Autoren sich mit der Aufstellung einer Basis, Bestimmung der Körperdiskriminante und Primidealzerlegung und mit der damit eng verbundenen Berechnung der Klassenzahl beschäftigt. Es sollen hier nur einige der wichtigsten Arbeiten erwähnt werden: G. Woronoj, Diss. St. Petersburg 1894; L. W. Reid, Amer. Journ. of Math. **23** (1901), S. 68—84; L. Sapolsky, Diss. Göttingen 1902; W. E. Berwick, Proc. London Math. Soc. (2) **12** (1913), S. 393—429; (2) **23** (1925), S. 359—378; G. E. Wahlin, Amer. Journ. of Math. **44** (1922), S. 191—203. Eine vollständige Untersuchung der kubischen Körper und ihrer Invarianten mittels der Theorie der Klassenkörper gab H. Hasse [Math. Zeitschr. **31** (1930), S. 565—582].

§§ 7—8. Die neuere Literatur über Reziprozitätsgesetze findet man bei Hasse: Bericht usw. Teil II: Reziprozitätsgesetze. Ergänzungsband VI, Jahresbericht d. Deutschen Math.-Ver. 1930.

Den Quotienten aus der Zetafunktion eines Körpers und der Zetafunktion eines Unterkörpers (wie speziell die Dedekindsche Funktion H, S. 174—175) hat Artin [Math. Ann. **89** (1923), S. 147—156] für metazyklische und andere Körper untersucht, ganz allgemein in der Arbeit über die L-Reihen [Hamburg. Abhandl. **3** (1924), S. 89—108].

Für beliebige kubische Körper hat C. G. Jaeger [Amer. Journ. of Math. **52** (1930), S. 85—96] ein Charaktersymbol ψ eingeführt, das ähnliche Eigenschaften wie das Dedekindsche besitzt.

§ 11. Das auf S. 206—207 erwähnte Fragment von Gauß ist in Bd. VIII, S. 5 seiner Werke mit verschiedenen anderen, teilweise weitergehenden Notizen über kubische und biquadratische Reste abgedruckt. Nach den Erläuterungen von Fricke war die Notiz auf dem Vorsatzblatt des Einbandes von Gauß' Handexemplar der Disquisitiones geschrieben und stammt wahrscheinlicherweise aus der Zeit 1804—1805.

§ 13. Ein einfacher Beweis des Kroneckerschen Grenzsatzes findet sich z. B. in H. Weber, Lehrbuch der Algebra, Bd. III, § 141 (2. Auflage). Neuere Untersuchungen über den Kroneckerschen Grenzsatz findet man bei Fueter [Rendiconti di Palermo **29** (1910), S. 380—395] und Herglotz [Leipziger Berichte **75** (1923), S. 3—14, 31—37]; vgl. auch L. J. Mordell, Proc. Roy. Soc. London **125** (1929), S. 262—276.

Hinsichtlich der notwendigen Berechnung der Fundamentaleinheit soll bemerkt werden, daß die oben erwähnte, in russischer Sprache verfaßte Arbeit von G. Woronoj angeblich eine Methode zur Bestimmung der Fundamentaleinheit in beliebigen kubischen Körpern mit negativer Diskriminante enthalten soll.

Es ist hier nicht möglich, auf die reichhaltige Literatur über die Dedekindsche Zetafunktion näher einzugehen; es muß nur auf die fundamentalen Arbeiten von Hecke, Landau, Artin u. a. verwiesen werden. Unter Benutzung der Dedekindschen Vorarbeiten studierte Landau die Eigenschaften der Zetafunktionen reiner kubischer Körper (Festschrift zu H. A. Schwarz, 1914, S. 244—273).

Ore.