5. Über den Dirichletschen biquadratischen Zahlkörper.

[Mathem. Annalen Bd. 45, S. 309—340 (1894).]

Einleitung.

Nachdem durch GAUSS die ganzen imaginären Zahlen in die Arithmetik eingeführt waren, untersuchte DIRICHLET in einer Reihe von Abhandlungen[1] denjenigen biquadratischen Zahlkörper, welcher die imaginäre Einheit i und mithin alle jene Gaußschen imaginären Zahlen enthält. Dieser biquadratische Körper werde der Dirichletsche Zahlkörper genannt. DIRICHLET hat auf denselben seine allgemeine analytische Methode zur Bestimmung der Anzahl der Idealklassen angewandt und insbesondere den Fall in Betracht gezogen, in welchem der biquadratische Zahlkörper außer dem durch i bestimmten quadratischen Körper noch zwei andere quadratische Körper enthält. Es ergibt sich dann das Resultat, daß die Anzahl der Idealklassen dieses speziellen Dirichletschen Zahlkörpers im wesentlichen gleich dem Produkt der Anzahl der Idealklassen in den beiden letzteren quadratischen Körpern ist. Diesen mit analytischen Hilfsmitteln gewonnenen rein arithmetischen Satz bezeichnet DIRICHLET als einen der schönsten in der Theorie der imaginären Zahlen, vornehmlich weil durch denselben ein Zusammenhang zwischen den Anzahlen der Idealklassen derjenigen beiden quadratischen Körper aufgedeckt wird, die durch Quadratwurzeln aus entgegengesetzten reellen Zahlen bestimmt sind.

Die vorliegende Abhandlung hat das Ziel, die Theorie des Dirichletschen biquadratischen Körpers auf rein arithmetischem Wege bis zu demjenigen Standpunkt zu fördern, auf welchem sich die Theorie der quadratischen Körper bereits seit GAUSS befindet. Es ist hierzu vor allem die Einführung des Geschlechtsbegriffs sowie eine Untersuchung derjenigen Einteilung aller Idealklassen notwendig, welche sich auf den Geschlechtsbegriff gründet. Nachdem in den ersten acht Paragraphen der Arbeit diese Aufgabe für den allgemeinen Dirichletschen Zahlkörper gelöst wird, behandeln die beiden letzten Paragraphen den vorhin charakterisierten speziellen Dirichletschen

[1] Untersuchungen über die Theorie der komplexen Zahlen; Recherches sur les formes quadratiques à coefficients et à indéterminées complexes. Werke 1, 505, 511, 533.

Zahlkörper. Es zeigt sich bei der Untersuchung, daß in diesem Körper die Idealklassen gewisser leicht zu kennzeichnender Geschlechter aus den Idealklassen der in ihm enthaltenen quadratischen Körper zusammensetzbar sind. Diese auf rein arithmetischem Wege gefundene Tatsache enthält zugleich den vorhin genannten Dirichletschen Satz über die Anzahl der Idealklassen des speziellen Dirichletschen Körpers.

§ 1. Die ganzen Zahlen des Dirichletschen Zahlkörpers.

Der durch die imaginäre Einheit i bestimmte quadratische Zahlkörper werde k genannt; die ganzen Zahlen dieses Körpers, d. h. die Zahlen von der Form $a+bi$, wo a und b ganze rationale Zahlen sind, mögen ganze imaginäre Zahlen heißen. Bedeutet δ eine ganze imaginäre Zahl, welche durch kein Quadrat einer ganzen imaginären Zahl teilbar und von ± 1 verschieden ist, so bildet die Gesamtheit aller durch i und $\sqrt{\delta}$ rational ausdrückbaren Zahlen einen Dirichletschen biquadratischen Zahlkörper. Derselbe werde mit K bezeichnet; K ist der allgemeinste biquadratische Körper, welcher die imaginäre Einheit i enthält.

Eine jede Zahl des Körpers K läßt sich in die Gestalt

$$\mathsf{A} = \frac{\alpha + \beta\sqrt{\delta}}{\gamma}$$

bringen, wo α, β, γ ganze imaginäre Zahlen sind. Die Veränderung von $\sqrt{\delta}$ in $-\sqrt{\delta}$ werde durch das Operationssymbol S bezeichnet.

Soll nun A eine ganze Zahl in K sein, so sind notwendig die Zahlen

$$\mathsf{A} + S\mathsf{A} \quad \frac{2\alpha}{\gamma} \quad \text{und} \quad \mathsf{A}\cdot S\mathsf{A} = \frac{\alpha^2 - \beta^2\delta}{\gamma^2}$$

ganze imaginäre Zahlen. Bezeichnet λ eine in γ aufgehende von $1+i$ verschiedene Primzahl in k, so folgt leicht, daß sowohl α als β durch λ teilbar sein müssen, und es kann mithin λ in Zähler und Nenner von A fortgehoben werden. Wäre ferner γ durch $(1+i)^3$ teilbar, so folgt in gleicher Weise, daß α und β durch $1+i$ teilbar sind, so daß der Faktor $1+i$ in Zähler und Nenner von A hebbar ist. Es bleiben mithin nur die beiden Fälle $\gamma = 1+i$ und $\gamma = 2$ zu untersuchen übrig. Also folgt, daß in diesen beiden Fällen die Zahl $\alpha^2 - \beta^2\delta$ durch 2 bezüglich durch 4 teilbar sein muß. Wäre β durch $1+i$ teilbar, so würde mithin das gleiche für α folgen und dann wäre wiederum $1+i$ im Zähler und Nenner von A hebbar. Nehmen wir andrerseits β nicht teilbar durch $1+i$ an, so folgt, daß $\delta \equiv \frac{\alpha^2}{\beta^2}$ nach 2 bezüglich nach 4 ist, d. h. δ muß im Zahlengebiete des Körpers k quadratischer Rest von 2 bezüglich von 4 sein. Nun ist δ quadratischer Rest von 4, sobald $\delta \equiv \pm 1$ nach 4 wird, dagegen quadratischer Rest von 2 und zugleich quadratischer Nichtrest von 4, falls $\delta \equiv \pm 3 + 2i$ nach 4

wird. In allen anderen Fällen, nämlich für $\delta \equiv i$ nach 2 und $\delta \equiv 0$ nach $1+i$ ist δ quadratischer Nichtrest von 2. Berücksichtigen wir, daß der nämliche biquadratische Körper K erhalten wird, wenn wir unter dem Wurzelzeichen statt δ die Zahl $-\delta$ setzen, da ja diese Änderung einer Multiplikation der Wurzel mit i gleichkommt, so können wir offenbar die Zahl δ stets so annehmen, daß beidemal das obere Vorzeichen zutrifft, d. h. $\delta \equiv 1$ bezüglich $\equiv 3+2i$ nach 4 wird. Es ergibt sich dann leicht das folgende Resultat:

Die Basis der ganzen Zahlen des Dirichletschen Körpers K besteht aus den Zahlen $1, i, \Omega, i\Omega$, *wo Ω folgende Bedeutung hat:*

$$\begin{aligned}
&\text{für} \quad \delta \equiv 1, && (4) \text{ ist:} && \Omega = \frac{1+\sqrt{\delta}}{2},\\
&\text{„} \quad \delta \equiv 3+2i, && (4) && \Omega = \frac{1+\sqrt{\delta}}{1+i},\\
&\text{„} \quad \delta \equiv i, && (2) && \Omega = 1+\sqrt{\delta},\\
&\text{„} \quad \delta \equiv 0, && (1+i) && \Omega = \sqrt{\delta}.
\end{aligned}$$

Wir berechnen ferner den Ausdruck $d = (\Omega - S\Omega)^2$; *derselbe werde die Partialdiskriminante des Körpers K genannt*:

$$\begin{aligned}
&\text{für} \quad \delta \equiv 1, && (4) \text{ ist:} && d = \delta,\\
&\text{„} \quad \delta \equiv 3+2i, && (4) && d = -2i\delta,\\
&\text{„} \quad \delta = i, \\
&\text{„} \quad \delta \equiv 0, && (1+i) && d = 4\delta.
\end{aligned} \qquad (2)$$

Die gewöhnliche Diskriminante D des biquadratischen Körpers K ergibt sich gleich $2^4|d|^2$, wo $|d|$ den absoluten Betrag der Partialdiskriminante d bedeutet.

§ 2. Die Primideale des Dirichletschen Körpers.

Zunächst behandeln wir die von $1+i$ verschiedenen und nicht in δ aufgehenden Primzahlen des Körpers k; es sind unter diesen zwei Arten zu unterscheiden, nämlich erstens die Primzahlen π, in bezug auf welche δ im Zahlengebiete des Körpers k quadratischer Rest ist und zweitens diejenigen Primzahlen $\varkappa$, in bezug auf welche δ quadratischer Nichtrest ist.

Die Primzahlen π der ersten Art gestatten eine Zerlegung in zwei voneinander verschiedene Primideale des Körpers K. Bedeutet nämlich η eine Zahl in k, welche der Kongruenz $\delta \equiv \eta^2$ nach dem Modul π genügt und wendet man eine früher von mir angegebene Bezeichnungsweise[1] an, der zu Folge $(\mathsf{A}, \mathsf{B}, \ldots)$ dasjenige Ideal darstellt, welches als der größte gemeinsame Teiler der Zahlen $\mathsf{A}, \mathsf{B}, \ldots$ definiert ist, so wird

$$\begin{aligned}
(\pi, \eta+\sqrt{\delta})\,(\pi, \eta-\sqrt{\delta}) &= (\pi^2, \pi[\eta+\sqrt{\delta}], \pi[\eta-\sqrt{\delta}], \eta^2-\delta)\\
&= (\pi, \eta^2-\delta) = \pi.
\end{aligned}$$

[1] Math. Ann. 44, 1. (Dieser Band, Abh. 3, S. 6.)

Wir erhalten somit die gewünschte Zerlegung

$$\pi = \mathfrak{P} \cdot S\mathfrak{P}, \qquad \mathfrak{P} = (\pi, \eta+\sqrt{\delta}),$$

wo $\mathfrak{P}$ ein Primideal bedeutet und das konjugierte Primideal $S\mathfrak{P}$ wegen $(\pi, \eta+\sqrt{\delta}, \eta-\sqrt{\delta}) = 1$ notwendig von $\mathfrak{P}$ verschieden ist.

Die Primzahlen $\varkappa$ der zweiten Art sind auch im Körper K Primzahlen. Denn wäre die Zahl $\varkappa$ zerlegbar, so wähle man in K eine ganze Zahl $\mathsf{A} = \alpha+\beta\sqrt{\delta}$, welche nicht durch $\varkappa$, wohl aber durch ein in $\varkappa$ aufgehendes Primideal teilbar ist. Da dann β notwendig prim zu $\varkappa$ sein muß, dagegen $\mathsf{A} \cdot S\mathsf{A} = \alpha^2 - \beta^2\delta$ durch $\varkappa$ teilbar wird, so würde $\delta \equiv \left(\frac{\alpha}{\beta}\right)^2$ nach $\varkappa$ folgen, was der Voraussetzung zuwider läuft.

Um ferner die von $1+i$ verschiedenen in δ aufgehenden Primzahlen des Körpers k in ihre idealen Faktoren zu zerlegen, bezeichnen wir dieselben mit $\lambda_1, \ldots, \lambda_r$ und setzen demgemäß $\delta = \lambda_1 \ldots \lambda_r$ bezüglich $\delta = (1+i)\lambda_1 \ldots \lambda_r$ je nachdem δ durch $1+i$ nicht teilbar oder teilbar ist. Es folgt leicht, daß

$$\mathfrak{L}_1 = S\mathfrak{L}_1 = (\lambda_1, \sqrt{\delta}), \ldots, \mathfrak{L}_r = S\mathfrak{L}_r = (\lambda_r, \sqrt{\delta})$$

Primideale im Körper K sind und daß

$$\lambda_1 = \mathfrak{L}_1^2, \ldots, \lambda_r = \mathfrak{L}_r^2$$

wird.

Was endlich die Zerlegung der Zahl $1+i$ betrifft, so untersuchen wir zunächst den Fall $\delta \equiv 1$ nach 4 und finden, daß $1+i$ unzerlegbar ist, falls $\delta \equiv 1+4i$ nach $(1+i)^5$ ausfällt. Ist dagegen $\delta \equiv 1$ nach $(1+i)^5$, so wird

$$1+i = (1+i, \Omega)\,(1+i, S\Omega),$$

wo die beiden Klammern rechter Hand Primideale des Körpers K darstellen, welche wegen $(\Omega, S\Omega) = 1$ notwendig voneinander verschieden sind. In allen anderen Fällen ist δ das Quadrat des Ideals $(1+i, \Omega) = (1+i, S\Omega)$, wie eine leichte Rechnung zeigt. Wir erkennen somit, daß $1+i$ dann und nur dann das Quadrat eines Primideals wird, wenn $1+i$ in der Partialdiskriminante d des Körpers K aufgeht. Die Zerlegung der Zahl $1+i$ ist in folgender Tabelle dargestellt:

$$\begin{aligned}
&\text{für} \quad \delta \equiv 1, && (1+i)^5 \text{ ist} && 1+i = \mathfrak{P} \cdot S\mathfrak{P},\\
&&&&& \mathfrak{P} = (1+i, \Omega),\ S\mathfrak{P} \neq \mathfrak{P},\\
&\text{„} \quad \delta \equiv 1+4i, && (1+i)^5 && \text{„} \quad 1+i = \mathfrak{P},\\
&\text{„} \quad \delta \equiv 3+2i, \\
&\text{„} \quad \delta \equiv i, \\
&\text{„} \quad \delta \equiv 0, && (1+i) && \text{„} \quad 1+i = \mathfrak{L}^2,\\
&&&&& \mathfrak{L} = S\mathfrak{L} = (1+i, \Omega).
\end{aligned} \qquad \begin{matrix} \\ \\ (4) \\ (2) \\ (1+i) \end{matrix}$$

Die gewonnenen Resultate der Zerlegung der Zahlen in k lassen sich übersichtlich zusammenfassen, wenn wir uns eines auch von DIRICHLET benutzten Symbols bedienen. Ist nämlich α eine beliebige Zahl und τ eine Primzahl in k, so verstehen wir unter $\left[\frac{\alpha}{\tau}\right]$ die Werte $+1$, -1 oder 0, je nachdem α im Zahlengebiete des Körpers k quadratischer Rest oder quadratischer Nichtrest von τ oder durch τ teilbar ist; doch bedeute insbesondere $\left[\frac{\alpha}{1+i}\right]$ die Werte $+1$, -1, 0, je nachdem α quadratischer Rest oder Nichtrest von $(1+i)^5$ oder durch $1+i$ teilbar ist. Es gilt dann der Satz:

Die Primzahl τ des Körpers k ist im Körper K in zwei verschiedene Primideale zerlegbar oder unzerlegbar oder gleich dem Quadrat eines Primideals, je nachdem $\left[\frac{d}{\tau}\right]=+1, =-1$ *oder* 0 *ist.*

§ 3. Die Einteilung der Idealklassen in Geschlechter.

Wenn A eine beliebige ganze oder gebrochene Zahl des Körpers K ist, so wird $\nu(\mathsf{A})=\mathsf{A}\cdot S\mathsf{A}$ die *Partialnorm* von A genannt. Diese Partialnorm ist offenbar eine Zahl im Körper k. Bedeutet nun λ eine von $1+i$ verschiedene in δ aufgehende Primzahl des Körpers k und ist die Partialnorm $\nu(\mathsf{A})$ eine durch λ nicht teilbare ganze Zahl oder eine gebrochene Zahl, deren Zähler und Nenner durch λ nicht teilbar sind, so wird $\nu(\mathsf{A})$ im Gebiet der ganzen imaginären Zahlen ein quadratischer Rest in bezug auf λ.

Um dies zu erkennen, setzen wir $\mathsf{A}=\frac{\alpha+\beta\sqrt{\delta}}{\gamma}$, wo α, β, γ ganze imaginäre Zahlen sind. Dann ist $\nu(\mathsf{A})=\frac{\alpha^2-\beta^2\delta}{\gamma^2}$. Enthielte nun γ den Primfaktor λ, so müßte wegen der über $\nu(\mathsf{A})$ gemachten Voraussetzung auch $\alpha^2-\beta^2\delta$ durch λ^2 teilbar sein und folglich enthielten sowohl α wie β den Faktor λ; derselbe ist mithin in Zähler und Nenner des Bruches A hebbar. Hätte andererseits α den Faktor λ, so müssen wegen der über $\nu(\mathsf{A})$ gemachten Voraussetzung notwendig auch γ und β durch λ teilbar sein, und dann ist wiederum der Faktor λ in Zähler und Nenner des Bruches A hebbar. Wir können daher annehmen, daß keine der beiden Zahlen α und γ den Faktor λ enthält. Dann aber folgt $\nu(\mathsf{A})\equiv\frac{\alpha^2}{\gamma^2}$ nach λ, womit die Behauptung bewiesen worden ist.

Wir führen jetzt das neue Symbol $\left[\frac{\sigma}{\lambda:\delta}\right]$ ein, wo σ eine beliebige Zahl in k und λ zunächst eine von $1+i$ verschiedene in δ aufgehende Primzahl bedeutet. Für den Fall, daß $\sigma=\alpha$ eine durch λ nicht teilbare ganze Zahl oder ein Bruch ist, dessen Zähler und Nenner durch λ nicht teilbar sind, wird das Symbol durch die Gleichung

$$\left[\frac{\alpha}{\lambda:\delta}\right]=\left[\frac{\alpha}{\lambda}\right]$$

definiert. Ist ferner $\sigma=\nu$ die Partialnorm einer beliebigen Zahl in K, so möge

$$\left[\frac{\nu}{\lambda:\delta}\right]=+1$$

sein. Der zu Anfang dieses Paragraphen bewiesene Satz zeigt, daß diese letztere Festsetzung mit der erst getroffenen Definition vereinbar ist.

Ferner benutzen wir die Tatsache, daß eine jede Zahl σ in k gleich dem Produkt zweier Zahlen α und ν gesetzt werden kann, wo α eine ganze nicht durch λ teilbare Zahl in k oder ein Bruch ist, dessen Zähler und Nenner nicht durch λ teilbar sind, und wo ν die Partialnorm einer Zahl in K ist. Um diese Tatsache zu beweisen, ist es offenbar nur nötig, jene Zerlegung für die Primzahl λ auszuführen. Zu dem Zweck wählen wir in K eine durch $\mathfrak{L}$, aber nicht durch $\lambda=\mathfrak{L}^2$ teilbare Zahl A, setzen $\nu=\nu(\mathsf{A})$ und berücksichtigen dann, daß $\frac{\lambda}{\nu}=\alpha$ in die Gestalt eines Bruches gebracht werden kann, dessen Zähler gleich 1 ist und dessen Nenner eine nicht durch λ teilbare Zahl ist. Es folgt somit die gewünschte Zerlegung $\lambda=\alpha\nu$.

Ist die beliebige Zahl $\sigma=\alpha\nu$ auf die beschriebene Weise zerlegt, so definieren wir das allgemeine Symbol durch die Gleichung

$$\left[\frac{\sigma}{\lambda:\delta}\right]=\left[\frac{\alpha}{\lambda}\right]$$

und erkennen ohne Schwierigkeit, daß dieses Symbol dadurch eindeutig bestimmt ist und die Eigenschaft

$$\left[\frac{\sigma\sigma'}{\lambda:\delta}\right]=\left[\frac{\sigma}{\lambda:\delta}\right]\left[\frac{\sigma'}{\lambda:\delta}\right]$$

besitzt, wo σ, σ' beliebige Zahlen des Körpers k sind.

In den Fällen, in welchen $1+i$ in d aufgeht, bedarf es einer genaueren Untersuchung über das Verhalten der Partialnormen und ihrer Reste nach den Potenzen von $1+i$. Um eine übersichtliche Darstellung der in Betracht kommenden Restsysteme zu erhalten, setzen wir

$$i'=3+2i, \quad i''=1+4i$$

und zeigen dann durch eine leichte Rechnung, daß, wenn t, t', t'' die Werte 0 oder 1 annehmen, in der Form $\pm i^t i'^{t'}$ sämtliche 8 zu $1+i$ primen Reste nach $(1+i)^4$ und in der Form $\pm i^t i'^{t'} i''^{t''}$ sämtliche 16 zu $1+i$ primen Reste nach $(1+i)^5$ enthalten sind. Wir bezeichnen der Kürze halber die beiden genannten Ausdrücke mit (tt') bezüglich $(tt't'')$.

Da im Falle $\delta\equiv(00)$ nach $(1+i)^4$ die Partialdiskriminante d nicht durch $1+i$ teilbar ist, so untersuchen wir lediglich die 7 Fälle $\delta\equiv(01), (10), (11)$ nach $(1+i)^4$ und $\equiv(1+i)(00), (1+i)(01), (1+i)(10), (1+i)(11)$ nach $(1+i)^5$. Die Rechnung zeigt, daß nur diejenigen zu $1+i$ primen Reste von $(1+i)^5$ unter den Partialnormen der Zahlen des Körpers K vertreten sind,

welche in der folgenden Tabelle unter der Rubrik α verzeichnet stehen und deren Exponenten t, t', t'' den in der letzten Rubrik angegebenen Bedingungen genügen:

$\delta \equiv$	$\alpha \equiv$	
(01)	(000), (001), (010), (011)	t gerade
(10)	(000), (001), (100), (101)	t' „
(11)	(000), (001), (110), (111)	$t+t'$ „
$(1+i)$(00)	(000), (011), (100), (111)	$t'+t''$ „
$(1+i)$(01)	(000), (011), (101), (110)	$t+t'+t''$ „
$(1+i)$(10)	(000), (010), (100), (110)	t'' „
$(1+i)$(11)	(000), (010), (101), (111)	$t+t''$ „

Um die Angaben dieser Tabelle übersichtlich zusammenzufassen, setzen wir $\delta \equiv (t_\delta t'_\delta)$ bezüglich $\equiv(1+i)(t_\delta t'_\delta)$ und $\alpha \equiv (t_\alpha t'_\alpha t''_\alpha)$; es bestätigt sich dann leicht, daß die Zahl α dann und nur dann nach $(1+i)^5$ einer Partialnorm kongruent ist, sobald die Zahl $t_\alpha t'_\delta + t'_\alpha t_\delta$ bezüglich $t_\alpha t'_\delta + t'_\alpha t_\delta + t'_\alpha + t''_\alpha$ gerade ist. Bemerkt sei noch, daß die Zahl α, wenn sie dieser Bedingung genügt, zugleich auch nach jeder höheren Potenz von $1+i$ der Partialnorm einer Zahl in K kongruent sein muß.

Wir definieren nun das Symbol $\left[\frac{\sigma}{1+i:\delta}\right]$ zunächst für den Fall, daß $\sigma=\alpha$ eine durch $1+i$ nicht teilbare Zahl oder ein Bruch ist, dessen Zähler und Nenner durch $1+i$ nicht teilbar sind. In diesem Falle nehmen wir $\alpha \equiv (t_\alpha t'_\alpha t''_\alpha)$ an und setzen

$$\left[\frac{\alpha}{1+i:\delta}\right] = (-1)^{t_\alpha t'_\delta + t'_\alpha t_\delta} \quad \text{bezüglich} \quad = (-1)^{t_\alpha t'_\delta + t'_\alpha t_\delta + t'_\alpha + t''_\alpha},$$

je nachdem $\delta \equiv (t_\delta t'_\delta)$ nach $(1+i)^4$ oder $\equiv(1+i)(t_\delta t'_\delta)$ nach $(1+i)^5$ wird. Ist ferner $\sigma=\nu$ die Partialnorm einer beliebigen Zahl des Körpers K, so setzen wir

$$\left[\frac{\nu}{1+i:\delta}\right] = +1.$$

Um endlich für ein beliebiges σ das Symbol zu definieren, benutzen wir die Zerlegung $\sigma=\alpha\nu$, wo α eine nicht durch $1+i$ teilbare Zahl oder ein Bruch ist, dessen Zähler und Nenner durch $1+i$ nicht teilbar sind, und wo ν eine Partialnorm ist und setzen

$$\left[\frac{\sigma}{1+i:\delta}\right] = \left[\frac{\alpha}{1+i:\delta}\right].$$

Wir erkennen wiederum leicht, daß dem soeben definierten Symbol die Eigenschaft

$$\left[\frac{\sigma\sigma'}{1+i:\delta}\right] = \left[\frac{\sigma}{1+i:\delta}\right]\left[\frac{\sigma'}{1+i:\delta}\right]$$

zukommt, wo σ, σ' beliebige Zahlen des Körpers K sind.

Im folgenden werden die sämtlichen s in der Partialdiskriminante d aufgehenden Primzahlen mit $\lambda_1, \ldots, \lambda_s$ bezeichnet. Unser Symbol ordnet dann einer jeden beliebigen Zahl σ des Körpers k die s Vorzeichen

$$\left[\frac{\sigma}{\lambda_1:\delta}\right], \ldots, \left[\frac{\sigma}{\lambda_s:\delta}\right]$$

zu, welche *das Charakterensystem der Zahl σ im* Dirichletschen Körper K heißen mögen. Um ferner vermittels unseres Symbols einem jeden Ideal $\mathfrak{J}$ in K ein bestimmtes Vorzeichensystem zuzuordnen, bilden wir $\mathfrak{J}\cdot S\mathfrak{J}$. Dieses Produkt ist gleich einer Zahl $\nu(\mathfrak{J})$ in k; dieselbe werde *die Partialnorm des Ideals* $\mathfrak{J}$ genannt. Da diese Partialnorm nur bis auf hinzutretende Einheitsfaktoren bestimmt ist, so bedarf es für unseren Zweck der Unterscheidung zweier Fälle, je nachdem das Charakterensystem des Einheitsfaktors i

$$\left[\frac{i}{\lambda_1:\delta}\right], \ldots, \left[\frac{i}{\lambda_s:\delta}\right]$$

aus lauter positiven Vorzeichen besteht oder ein negatives Vorzeichen enthält. *Im ersteren Falle sind offenbar die s Vorzeichen*

$$\left[\frac{\nu(\mathfrak{J})}{\lambda_1:\delta}\right], \ldots, \left[\frac{\nu(\mathfrak{J})}{\lambda_s:\delta}\right]$$

für das Ideal $\mathfrak{J}$ sämtlich eindeutig bestimmt. Das System dieser s Vorzeichen werde das Charakterensystem des Ideals $\mathfrak{J}$ genannt. Im zweiten Falle nehmen wir an, es sei etwa $\left[\frac{i}{\lambda_s:\delta}\right]=-1$; wählen wir dann den Wert der Partialnorm $\nu(\mathfrak{J})$ derart, daß $\left[\frac{\nu(\mathfrak{J})}{\lambda_s:\delta}\right]=+1$ wird, *so sind die $s-1$ Vorzeichen*

$$\left[\frac{\nu(\mathfrak{J})}{\lambda_1:\delta}\right], \ldots, \left[\frac{\nu(\mathfrak{J})}{\lambda_{s-1}:\delta}\right]$$

sämtlich durch $\mathfrak{J}$ eindeutig bestimmt und heißen das Charakterensystem des Ideals $\mathfrak{J}$.

Die Ideale derselben Klasse besitzen notwendig das gleiche Charakterensystem.

Ist nämlich $\mathfrak{J}'$ mit $\mathfrak{J}$ äquivalent, so gibt es in K eine ganze oder gebrochene Zahl A derart, daß $\mathfrak{J}'=\mathsf{A}\mathfrak{J}$ ist. Hieraus folgt $\nu(\mathfrak{J}')=\nu(\mathsf{A})\nu(\mathfrak{J})$ und daher wird $\left[\frac{\nu(\mathfrak{J}')}{\lambda:\delta}\right]=\left[\frac{\nu(\mathfrak{J})}{\lambda:\delta}\right]$.

Auf die dargelegte Weise ist einer jeden Idealklasse ein bestimmtes Charakterensystem zugeordnet. *Wir rechnen nun alle diejenigen Idealklassen, welche das gleiche Charakterensystem besitzen, in ein Geschlecht und definieren*

insbesondere das Hauptgeschlecht als die Gesamtheit aller derjenigen Klassen, deren Charakterensystem aus lauter positiven Vorzeichen besteht. Da das Charakterensystem der Hauptklasse offenbar von der letzteren Eigenschaft ist, so gehört die Hauptklasse stets zum Hauptgeschlecht.

§ 4. Die Erzeugung der Idealklassen des Hauptgeschlechtes.

Aus derjenigen Eigenschaft des Symbols, welche sich durch die Formel

$$\left[\frac{\sigma\sigma'}{\lambda:\delta}\right]=\left[\frac{\sigma}{\lambda:\delta}\right]\left[\frac{\sigma'}{\lambda:\delta}\right]$$

ausdrückt, entnehmen wir leicht die Tatsache, daß das Produkt der Idealklassen zweier Geschlechter die Idealklassen eines Geschlechtes liefert, dessen Charakterensystem durch Multiplikation der entsprechenden Charaktere beider Geschlechter erhalten wird. Im besonderen folgt hieraus, daß das Charakterensystem des Quadrats der Idealklasse eines beliebigen Geschlechtes stets aus lauter positiven Einheiten besteht und mithin das Quadrat einer Idealklasse stets dem Hauptgeschlecht angehört. Es ist von Bedeutung, daß die folgende Umkehrung dieses Satzes gilt:

Eine jede Idealklasse des Hauptgeschlechtes ist gleich dem Quadrat einer Idealklasse.

Um die Richtigkeit dieses Satzes zu erkennen, beweisen wir der Reihe nach folgende Sätze.

Satz 1. *Wenn ν in dem durch $\sqrt{\delta}$ bestimmten Dirichletschen Körper K_δ die Partialnorm eines Ideals ist und das Charakterensystem von ν in diesem Körper K_δ aus lauter positiven Einheiten besteht, so ist auch δ in dem durch $\sqrt{\nu}$ bestimmten Dirichletschen Körper K_ν Partialnorm eines Ideals und besitzt in K_ν ein aus lauter positiven Einheiten bestehendes Charakterensystem.*

Wir dürfen offenbar annehmen, daß ν keine quadratischen Faktoren des Körpers k enthält. Da ν eine Partialnorm sein soll, so muß ein jeder in der Partialdiskriminante d des Körpers K_δ nicht vorkommender Primteiler π der Zahl ν in zwei Primideale des Körpers K_δ zerfallen; es ist somit nach den Entwicklungen von § 2 notwendigerweise d quadratischer Rest von π, d. h. wenn π von $1+i$ verschieden ist:

$$\left[\frac{\delta}{\pi:\nu}\right]=+1.$$

Wir betrachten ferner die von $1+i$ verschiedenen in d aufgehenden Primteiler λ der Zahl ν. Es gilt im Körper K_δ die Zerlegung $\lambda=\mathfrak{L}^2$ und zugleich ist $\lambda+\sqrt{\delta}$ eine durch $\mathfrak{L}$, aber nicht durch λ teilbare Zahl des Körpers K_δ. Daher ist, wenn $\nu=\lambda\nu'$, $\delta=\lambda\delta'$ gesetzt wird:

$$\left[\frac{\nu}{\lambda:\delta}\right]=\left[\frac{\nu\cdot\nu\left(\frac{1}{\lambda+\sqrt{\delta}}\right)}{\lambda:o}\right]=\left[\frac{\nu}{\frac{\lambda^2-\delta}{\lambda}:\delta}\right]=\left[\frac{\nu'}{\frac{\lambda-\delta'}{\lambda}}\right]=\left[\frac{\nu'\delta'}{\lambda}\right].$$

In gleicher Weise folgt

$$\left[\frac{\delta}{\lambda:\nu}\right]=\left[\frac{\nu'\delta'}{\lambda}\right],$$

und da das Symbol $\left[\frac{\nu}{\lambda:\delta}\right]$ nach Voraussetzung den Wert $+1$ hat, so ist auch

$$\left[\frac{\delta}{\lambda:\nu}\right]=+1.$$

Was endlich den Primfaktor $1+i$ betrifft, so unterscheiden wir bei der folgenden Untersuchung zunächst 4 Hauptfälle:

I. Weder ν noch δ sind durch $1+i$ teilbar.

II. ν ist durch $1+i$ teilbar, aber nicht δ.

III. ν ist nicht durch $1+i$ teilbar, wohl aber δ.

IV. Sowohl ν als auch δ sind durch $1+i$ teilbar.

Im Hauptfalle I setzen wir $\nu\equiv(t_\nu t'_\nu)$ und $\delta\equiv(t_\delta t'_\delta)$ nach $(1+i)^4$ und unterscheiden dann 2 Unterfälle:

1. t_ν, t'_ν sind beide gerade. Unter dieser Bedingung kommt $1+i$ nicht in der Partialdiskriminante n des Dirichletschen Körpers K_ν vor, und es gibt daher im Körper K_ν kein auf den Faktor $1+i$ bezügliches Symbol.

2. t_ν, t'_ν sind nicht beide gleichzeitig gerade. Unter dieser Bedingung kommt $1+i$ in n vor und es ist

$$\left[\frac{\delta}{1+i:\nu}\right]=(-1)^{t_\delta t'_\nu+t'_\delta t_\nu}.$$

Sind t_δ, t'_δ beide gerade, so wird der Wert der rechten Seite $=+1$. Sind t_δ, t'_δ nicht beide zugleich gerade, so gibt es im Körper K_δ ein auf $1+i$ bezügliches Symbol, und zwar ist

$$\left[\frac{\nu}{1+i:\delta}\right]=(-1)^{t_\nu t'_\delta+t'_\nu t_\delta}.$$

Da dieses Symbol wegen der Voraussetzung den Wert $+1$ hat, so ist auch

$$\left[\frac{\delta}{1+i:\nu}\right]=+1.$$

Im Hauptfalle II setzen wir $\nu\equiv(1+i)(t_\nu t'_\nu)$ und $\delta\equiv(t_\delta t'_\delta t''_\delta)$ nach $(1+i)^5$ und unterscheiden dann folgende 2 Unterfälle.

1. t_δ, t'_δ sind gerade. Unter dieser Bedingung kommt $1+i$ nicht in der Partialdiskriminante d des Körpers K_δ vor. Da nun ν die Partialnorm eines Ideals in K_δ sein soll, so ist notwendigerweise $1+i$ in 2 Primideale des Körpers K_δ zerlegbar. Die Bedingung hierfür besteht nach § 2 darin, daß $\delta\equiv(000)$ nach $(1+i)^5$ ist, und mithin wird

$$\left[\frac{\delta}{1+i:\nu}\right]=+1.$$

2. t_δ, t'_δ sind nicht beide gleichzeitig gerade. Es ist dann $1+i$ Faktor der Partialdiskriminante d. Setzen wir $\omega = \frac{\Omega \cdot S\Omega}{1+i}$, so wird

$$\left[\frac{\nu}{1+i:\delta}\right] = \left[\frac{\nu \cdot \nu\left(\frac{1}{\Omega}\right)}{1+i:\delta}\right] = \left[\frac{(t_\nu t'_\nu)\,\omega}{1+i:\delta}\right] = \left[\frac{(t_\nu t'_\nu)}{1+i:\delta}\right]\left[\frac{\omega}{1+i:\delta}\right];$$

nun ist

$$\left[\frac{(t_\nu t'_\nu)}{1+i:\delta}\right] = (-1)^{t_\nu t'_\delta + t'_\nu t_\delta},$$

und eine leichte Rechnung zeigt, daß

$$\left[\frac{\omega}{1+i:\delta}\right] = (-1)^{t'_\delta + t''_\delta}$$

wird. Mithin ergibt sich

$$\left[\frac{\nu}{1+i:\delta}\right] = (-1)^{t_\nu t'_\delta + t'_\nu t_\delta + t'_\delta + t''_\delta}.$$

Andrerseits ist aber

$$\left[\frac{\delta}{1+i:\nu}\right] = (-1)^{t_\delta t'_\nu + t'_\delta t_\nu + t'_\delta + t''_\delta},$$

und wenn daher jenes erstere Symbol den Wert $+1$ hat, so ist auch

$$\left[\frac{\delta}{1+i:\nu}\right] = +1.$$

Im Hauptfall III setzen wir $\nu \equiv (t_\nu t'_\nu t''_\nu)$ und $\delta \equiv (1+i)\,(t_\delta t'_\delta)$ nach $(1+i)^5$ und unterscheiden dann wiederum 2 Unterfälle.

1. t_ν, t'_ν sind beide gerade. Unter dieser Bedingung ist $1+i$ in der Partialdiskriminante n des Körpers K_ν nicht enthalten. Wegen der Voraussetzung wird

$$\left[\frac{\nu}{1+i:\delta}\right] = (-1)^{t''_\nu} = +1.$$

Mithin ist t''_ν gerade, d. h. $\nu \equiv (000)$ nach $(1+i)^5$; hieraus folgt nach § 2, daß $1+i$ im Körper K_ν in zwei Primideale zerlegbar ist.

2. t_ν, t'_ν sind nicht beide gleichzeitig gerade. Es ist dann $1+i$ als Faktor in n enthalten, und es wird

$$\left[\frac{\nu}{1+i:\delta}\right] = (-1)^{t_\nu t'_\delta + t'_\nu t_\delta + t'_\nu + t''_\nu}.$$

Wie vorhin im Unterfalle 2. des Hauptfalles II erhalten wir den nämlichen Wert für das Symbol $\left[\frac{\delta}{1+i:\nu}\right]$, und da das erstere den Wert $+1$ hat, so ist auch

$$\left[\frac{\delta}{1+i:\nu}\right] = +1.$$

Im Hauptfalle IV setzen wir $\nu \equiv (1+i)\,(t_\nu t'_\nu t''_\nu)$ und $\delta \equiv (1+i)\,(t_\delta t'_\delta t''_\delta)$ nach $(1+i)^6$. Es wird dann

$$\begin{aligned}\left[\frac{\nu}{1+i:\delta}\right] &= \left[\frac{\nu \cdot \nu\left(\frac{1}{\sqrt{\delta}}\right)}{1+i:\delta}\right] = \left[\frac{(t_\nu t'_\nu t''_\nu)\,(t_\delta t'_\delta t''_\delta)}{1+i:\delta}\right] \\ &= (-1)^{(t_\nu + t_\delta)\,t'_\delta + (t'_\nu + t'_\delta)\,t_\delta + t'_\nu + t'_\delta + t''_\nu + t''_\delta} \\ &= (-1)^{t_\nu t'_\delta + t'_\nu t_\delta + t'_\nu + t'_\delta + t''_\nu + t''_\delta}.\end{aligned}$$

Denselben Wert erhalten wir auch für $\left[\frac{\delta}{1+i:\nu}\right]$, und da das erstere Symbol den Wert $+1$ hat, so ist auch

$$\left[\frac{\delta}{1+i:\nu}\right] = +1.$$

Die eben vollendete Entwicklung zeigt, daß das Charakterensystem der Zahl δ in dem Körper K_ν aus lauter positiven Einheiten besteht.

Andrerseits ist δ in K_ν notwendig die Partialnorm eines Ideals; denn wenn λ ein von $1+i$ verschiedener in n nicht aufgehender Primfaktor von δ ist, so ist, da alle Charaktere von ν in bezug auf den Körper K_δ gleich $+1$ sein sollen, notwendigerweise

$$\left[\frac{\nu}{\lambda:\delta}\right] = \left[\frac{\nu}{\lambda}\right] = +1,$$

und daher zerfällt λ nach § 2 in zwei Primideale des Körpers K_ν. Ist ferner $1+i$ in δ, aber nicht in der Partialdiskriminante n des Körpers K_ν als Faktor enthalten, so muß $\nu \equiv (00)$ nach $(1+i)^4$ sein, und es ist dann im Unterfalle 1 des Hauptfalles III bewiesen worden, daß $1+i$ im Körper K_ν zerlegbar ist. Da mithin sämtliche Primfaktoren von δ im Körper K_ν zerlegbar sind, so ist δ die Partialnorm eines Ideals in K_ν und hiermit ist der Satz 1 vollständig bewiesen.

Satz 2. *Wenn ν die Partialnorm einer ganzen oder gebrochenen Zahl in dem durch $\sqrt{\delta}$ bestimmten Dirichletschen Zahlkörper K_δ ist, so ist auch δ die Partialnorm einer ganzen oder gebrochenen Zahl in dem durch $\sqrt{\nu}$ bestimmten Dirichletschen Zahlkörper K_ν.*

Setzen wir nämlich

$$\nu = \nu(\alpha + \beta\sqrt{\delta}) = \alpha^2 - \beta^2\delta,$$

wo α und β Zahlen des Körpers k sind, so wird

$$\delta = \left(\frac{\alpha}{\beta}\right)^2 - \left(\frac{1}{\beta}\right)^2 \nu,$$

d. h. gleich der Partialnorm der in K_ν gelegenen Zahl $\frac{\alpha + \sqrt{\nu}}{\beta}$.

Satz 3. *Wenn ν Partialnorm eines Ideals in K_δ ist, und das Charakterensystem von ν in K_δ aus lauter positiven Einheiten besteht, so ist ν zugleich die Partialnorm einer gewissen ganzen oder gebrochenen Zahl des Körpers K_δ.*

Wenden wir den von H. Minkowski aufgestellten Satz[1] über die Diskriminante allgemeiner Zahlkörper auf den biquadratischen Dirichletschen Körper K_δ an, so erkennen wir, daß es in jeder Idealklasse des Dirichletschen Körpers K_δ ein Ideal $\mathfrak{J}$ gibt, dessen Norm $N(\mathfrak{J})$ absolut genommen kleiner als $\frac{3}{2\pi^2}\sqrt{|D|}$ ausfällt, wo D die Diskriminante des Körpers K_δ bedeutet. Da aber $D \leqq 2^8|\delta|^2$ und $\frac{3\cdot 2^3}{\pi^2} < \sqrt{6}$ ist und da ferner die Norm $N(\mathfrak{J})$ absolut genommen gleich dem Quadrat des absoluten Betrages der Partialnorm $\nu = \nu(\mathfrak{J})$ wird, so ergibt sich der Satz, daß in jeder Idealklasse des Körpers K_δ ein Ideal $\mathfrak{J}$ gefunden werden kann, für welches $|\nu(\mathfrak{J})|^2 < \sqrt{6}|\delta|$ ausfällt.

Wir beweisen nun zunächst durch Rechnung, daß der Satz 3 in allen Dirichletschen Körpern K_δ gilt, für welche $|\delta| < \sqrt{6}$ ist. Benutzen wir die soeben aus dem Minkowskischen Satz abgeleitete Ungleichung, so wird dieser Nachweis durch folgende Tabelle geführt, in welcher unter der Rubrik δ die sämtlichen absolut genommen unter $\sqrt{6}$ liegenden Werte von δ und unter der Rubrik ν die den Bedingungen des Satzes 3 und der Ungleichung $|\nu|^2 < \sqrt{6}|\delta|$ genügenden ν sich angegeben finden, während daneben in der letzten Rubrik die Zahl des Körpers K_δ hinzugefügt ist, deren Partialnorm gleich ν wird.

δ	ν	
$1 \pm 2i$	$1 \mp i$	$\frac{1+i\sqrt{1\pm 2i}}{1\pm i}$
$2 \pm i$	$2 \mp i$	$1 \mp i + i\sqrt{2 \pm i}$
	$1 \pm i$	$i + i\sqrt{2 \pm i}$
$1 \pm i$	$\pm i$	$i + i\sqrt{1 \pm i}$
i	$1 + i$	$1 + i\sqrt{i}$

Es sei jetzt δ eine ganze imaginäre Zahl, deren absoluter Betrag $|\delta| > \sqrt{6}$ ausfällt, und wir nehmen an, der Satz 3 sei bereits bewiesen für alle diejenigen Körper $K_{\delta'}$, für welche $|\delta'| < |\delta|$ wird. Ist dann ν die Partialnorm eines Ideals $\mathfrak{J}$, deren Charakterensystem in K_δ aus lauter positiven Einheiten besteht, so bestimme man in K_δ ein zu $\mathfrak{J}$ äquivalentes Ideal $\mathfrak{J}'$, dessen Partialnorm ν' absolut genommen und ins Quadrat erhoben $< \sqrt{6}|\delta|$ ausfällt. Da $\sqrt{6} < |\delta|$ ist, so wird $|\nu'| < |\delta|$. Da andrerseits ν' die Partialnorm eines Ideals in K_δ ist, deren Charakterensystem aus lauter positiven Einheiten besteht, so ist nach Satz 1 die ganze imaginäre Zahl δ in dem durch $\sqrt{\nu'}$ bestimmten Körper $K_{\nu'}$ die Partialnorm eines Ideals, deren Charakterensystem aus lauter positiven Einheiten besteht. Nun gilt wegen $|\nu'| < |\delta|$ Satz 3 im Körper $K_{\nu'}$, und es ist daher δ die Partialnorm einer gewissen ganzen oder gebrochenen Zahl des Körpers $K_{\nu'}$, und hieraus ergibt sich nach Satz 2, daß auch ν' die Partialnorm einer gewissen Zahl in K_δ ist. Da das Ideal $\mathfrak{J}$ äquivalent $\mathfrak{J}'$ ist, so ist der Quotient beider Ideale eine Zahl des Körpers K_δ, mithin ist der Quotient der Zahlen ν und ν' und folglich auch ν selbst gleich der Partialnorm einer gewissen Zahl des Körpers K_δ. Der Satz 3 gilt folglich für den Körper K_δ, und wir erkennen daraus seine allgemeine Gültigkeit[1].

Aus Satz 3 folgt endlich in sehr einfacher Weise der zu Anfang dieses Paragraphen ausgesprochene Satz über die Idealklassen des Hauptgeschlechts. Wenn nämlich $\mathfrak{J}$ ein Ideal des Hauptgeschlechts ist, so erfüllt seine Partialnorm $\nu(\mathfrak{J})$ — bezüglichenfalls, wenn sie nach der auf S. 31 angegebenen Vorschrift mit dem Einheitsfaktor i versehen ist — alle Bedingungen des Satzes 3. Es gibt daher auf Grund desselben im Körper K_δ eine Zahl A derart, daß $\nu(\mathfrak{J}) = \nu(\mathsf{A})$ wird. Setzen wir $\frac{\mathfrak{J}}{\mathsf{A}} = \frac{\mathfrak{H}}{\mathfrak{H}'}$, wo $\mathfrak{H}$ und $\mathfrak{H}'$ zueinander prime Ideale sind, so ist notwendigerweise $\frac{\mathfrak{H}\cdot S\mathfrak{H}}{\mathfrak{H}'\cdot S\mathfrak{H}'} = 1$ und mithin $\mathfrak{H}' = S\mathfrak{H}$. Da $\mathfrak{H}\cdot S\mathfrak{H}$ gleich einer Zahl α des Körpers k gesetzt werden kann, so ergibt sich $\mathfrak{J} = \frac{\mathsf{A}}{\alpha}\mathfrak{H}^2$, d. h. $\mathfrak{J}$ ist notwendigerweise dem Quadrat des Ideals $\mathfrak{H}$ äquivalent.

§ 5. Die ambigen Ideale.

Ein Ideal $\mathfrak{J}$ des Dirichletschen Körpers K, welches nach Anwendung der Operation S ungeändert bleibt und keine Zahl des Körpers k als Faktor enthält, werde *ein ambiges Ideal* genannt. Um alle ambigen Ideale aufzustellen, bezeichnen wir, wie in § 3, die sämtlichen s in der Partialdiskriminante d des Körpers K aufgehenden Primzahlen mit $\lambda_1, \ldots, \lambda_s$ und setzen $\lambda_1 = \mathfrak{L}_1^2, \ldots, \lambda_s = \mathfrak{L}_s^2$; es sind dann wegen $\mathfrak{L} = S\mathfrak{L}$ die s Ideale $\mathfrak{L}_1, \ldots, \mathfrak{L}_s$ ambige Ideale und desgleichen sind die sämtlichen 2^s Produkte $\mathfrak{A} = \Pi\mathfrak{L}$ ambig, welche aus diesen s Idealen $\mathfrak{L}_1, \ldots, \mathfrak{L}_s$ gebildet werden können. Wir

[1] Vgl. Comptes rendus **1891**. Für obigen Zweck reicht schon die von H. Minkowski, J. Math. **107**, 296 (1891), aufgestellte Ungleichung aus.

[1] Der eben bewiesene Satz 3 liefert zugleich alle Mittel zur Aufstellung der notwendigen und hinreichenden Bedingungen dafür, daß die ternäre diophantische Gleichung

$$\alpha\xi^2 + \beta\eta^2 + \gamma\zeta^2 = 0$$

mit beliebigen ganzen imaginären Koeffizienten α, β, γ in ganzen imaginären Zahlen ξ, η, ζ lösbar ist.

beweisen leicht den Satz, daß es im Körper K keine weiteren ambigen Ideale gibt. Wäre nämlich $\mathfrak{J}=\mathfrak{P}\mathfrak{Q}\ldots\mathfrak{R}$, wo $\mathfrak{P},\mathfrak{Q},\ldots,\mathfrak{R}$ Primideale sind, ein ambiges Ideal, so müßten wegen $\mathfrak{J}=S\mathfrak{J}$ die Primideale $S\mathfrak{P}$, $S\mathfrak{Q},\ldots,S\mathfrak{R}$ in einer gewissen Reihenfolge genommen, mit $\mathfrak{P},\mathfrak{Q},\ldots,\mathfrak{R}$ übereinstimmen. Wenn etwa $S\mathfrak{P}=\mathfrak{Q}$ sich ergeben würde, so enthielte $\mathfrak{J}$ den Faktor $\mathfrak{P}S\mathfrak{P}$, welcher gleich einer ganzen imaginären Zahl ist, und da dieser Umstand der Voraussetzung widerspricht, so folgt $\mathfrak{P}=S\mathfrak{P}$ und ebenso $\mathfrak{Q}=S\mathfrak{Q},\ldots,$ $\mathfrak{R}=S\mathfrak{R}$, d. h. die Ideale $\mathfrak{P},\mathfrak{Q},\ldots,\mathfrak{R}$ sind sämtlich ambige Primideale, und da das Quadrat eines solchen Ideals einer ganzen imaginären Zahl gleich wird, so schließen wir zugleich, daß die Ideale $\mathfrak{P},\mathfrak{Q},\ldots,\mathfrak{R}$ notwendig untereinander verschieden sind. Wir sprechen das gewonnene Resultat in folgendem Satze aus:

Satz 1. *Die s in der Partialdiskriminante d aufgehenden Primideale $\mathfrak{L}_1,\ldots,\mathfrak{L}_s$ und nur diese sind ambige Primideale. Die 2^s aus diesen zu bildenden Produkte $\mathfrak{A}=\Pi\mathfrak{L}$ machen die Gesamtheit aller ambigen Ideale des Körpers K aus.*

§ 6. Die ambigen Klassen.

Wenn $\mathfrak{J}$ ein Ideal der Klasse C ist, so werde diejenige Idealklasse, welcher das Ideal $S\mathfrak{J}$ angehört, mit SC bezeichnet. Ist insbesondere $C=SC$, so heißt *die Idealklasse C ambig*. Da das Produkt $\mathfrak{J}\cdot S\mathfrak{J}$ äquivalent 1 ist, so wird $C\cdot SC=1$ und folglich ist das Quadrat einer jeden ambigen Klasse gleich der Hauptklasse 1. Umgekehrt, wenn das Quadrat einer Klasse C gleich 1 ist, so wird $C=\frac{1}{C}=SC$ und folglich ist C eine ambige Klasse.

Es entsteht nun die Aufgabe, alle ambigen Klassen aufzustellen. Da offenbar ein jedes ambige Ideal $\mathfrak{J}$ vermöge seiner Eigenschaft $\mathfrak{J}=S\mathfrak{J}$ einer ambigen Klasse angehört, so haben wir vor allem zu untersuchen, wie viele voneinander verschiedene ambige Klassen aus den 2^s ambigen Idealen entspringen.

Das Produkt aller in δ aufgehenden Ideale $\mathfrak{L}$ ist gleich $\sqrt{\delta}$ und mithin ein Hauptideal. Wir bestimmen nun im Körper K eine Grundeinheit E, d. h. eine Einheit von der Beschaffenheit, daß jede andere Einheit des Körpers gleich $\varrho\mathsf{E}^m$ wird, wo ϱ eine Einheitswurzel und m eine positive oder negative ganze Zahl bedeutet. Da die irreduzible Gleichung, welcher ϱ genügt, notwendig vom 2-ten oder 4-ten Grade sein muß, so kann ϱ nur eine 2-te, 3-te, 4-te, 5-te oder 8-te Einheitswurzel oder eine aus diesen zusammengesetzte Einheitswurzel sein. Die 3-te Einheitswurzel kommt im Körper K nur vor, wenn $\delta=3$ ist. Es kann ferner leicht gezeigt werden, daß die 5-te Einheitswurzel im Körper K niemals vorkommt. Die 8-te Einheitswurzel endlich kommt im Körper K vor, falls $\delta=i$ ist. Die beiden Fälle $\delta=3$ und $\delta=i$ werden unten für sich besonders erledigt und bei der nachfolgenden allgemeinen Untersuchung ausgeschlossen, so daß nunmehr ϱ lediglich $=\pm 1$ oder $=\pm i$ sein kann.

Die Grundeinheit E ist bis auf einen Faktor ϱ völlig bestimmt. Die Entscheidung darüber, ob im Körper K außer 1 und $\sqrt{\delta}$ noch ein anderes ambiges Hauptideal vorhanden ist, hängt lediglich davon ab, ob $\nu(\mathsf{E})=\pm 1$ oder $=\pm i$ ausfällt.

Um dies zu erkennen, nehmen wir zunächst $\nu(\mathsf{E})=\pm 1$ an. Da es freisteht, $i\mathsf{E}$ an Stelle von E als Grundeinheit zu wählen, so können wir annehmen, daß $\nu(\mathsf{E})=+1$ wird. Wir setzen[1] $1+\mathsf{E}=\alpha\mathsf{A}$, wo α eine ganze imaginäre Zahl und A eine ganze Zahl des Körpers K bedeutet, welche durch keine ganze imaginäre Zahl teilbar ist. Aus der Gleichung $\frac{\mathsf{A}}{S\mathsf{A}}=\mathsf{E}$ ergibt sich, daß A ein ambiges Hauptideal ist. Dieses Hauptideal A ist ferner verschieden von 1 und von $\sqrt{\delta}$. Wäre nämlich $\mathsf{A}=\varrho\mathsf{E}^m$ oder $=\varrho\mathsf{E}^m\sqrt{\delta}$, so wäre

$$\frac{\mathsf{A}}{S\mathsf{A}}=\pm\left(\frac{\mathsf{E}}{S\mathsf{E}}\right)^m=\pm\mathsf{E}^{2m}$$

und diese Einheit kann nicht gleich E sein, da m eine ganze Zahl bedeutet und E keine Einheitswurzel ist. Ferner ist ersichtlich, daß ein jedes andere ambige Hauptideal des Körpers K aus $\sqrt{\delta}$ und A zusammengesetzt werden kann. Ist nämlich B ein beliebiges ambiges Hauptideal, so ist notwendig $\frac{\mathsf{B}}{S\mathsf{B}}=\varrho\mathsf{E}^m$ Aus der Gleichung $\nu\left(\frac{\mathsf{B}}{S\mathsf{B}}\right)=+1$ folgt $\varrho=\pm 1$; wir setzen $\varrho=(-1)^n$, wo n den Wert 0 oder 1 hat; dann genügt die Zahl $\Gamma=\mathsf{B}\left(\sqrt{\delta}\right)^n\mathsf{A}^{-m}$ der Gleichung $\frac{\Gamma}{S\Gamma}=+1$ und ist folglich eine Zahl des Körpers k, woraus die Behauptung ersichtlich wird.

Ist andrerseits die Partialnorm $\nu(\mathsf{E})=i$, so kann es kein von 1 und $\sqrt{\delta}$ verschiedenes ambiges Hauptideal geben. Denn wäre $\mathfrak{A}=\mathsf{A}$ ein solches, so ist notwendigerweise $\frac{\mathsf{A}}{S\mathsf{A}}=\varrho\mathsf{E}^m$. Da aber $\nu\left(\frac{\mathsf{A}}{S\mathsf{A}}\right)=1$ ist, so folgt notwendigerweise $[\nu(\mathsf{E})]^m=\pm 1$ und daher muß m eine gerade Zahl sein. Wegen $\mathsf{E}^2=\frac{i\mathsf{E}}{S\mathsf{E}}$ würde dann die Zahl $\mathsf{B}=\mathsf{A}\mathsf{E}^{-\frac{m}{2}}$ der Gleichung $\frac{\mathsf{B}}{S\mathsf{B}}=\varrho$ genügen und da $\nu\left(\frac{\mathsf{B}}{S\mathsf{B}}\right)=+1$ ist, so folgt $\varrho=\pm 1$. Berücksichtigen wir, daß B durch keine ganze imaginäre Zahl teilbar sein darf, so hat die Annahme $\frac{\mathsf{B}}{S\mathsf{B}}=+1$ notwendig $\mathsf{B}=\varrho$ und die Annahme $\frac{\mathsf{B}}{S\mathsf{B}}=-1$ notwendig $\mathsf{B}=\varrho\sqrt{\delta}$ zur Folge, womit die Behauptung bewiesen ist.

Wir drücken nun eines der s ambigen Primideale durch die $s-1$ übrigen ambigen Primideale und durch $\sqrt{\delta}$ und ferner, wenn die Partialnorm der

[1] Die linke Seite dieses Ansatzes ist ein besonderer Fall des von Kummer im J. Math. 50, 212 (1855) behandelten Ausdruckes.

Grundeinheit $= \pm 1$ ausfällt, noch eines dieser $s - 1$ ambigen Ideale durch die $s - 2$ übrigen und durch A aus. Bezeichnen wir dann allgemein eine Anzahl von Idealklassen als untereinander unabhängig, wenn keine derselben gleich 1 oder gleich einem Produkt der übrigen ist, so gilt offenbar der Satz:

Satz 2. *Die s ambigen Primideale bestimmen $s - 2$ oder $s - 1$ voneinander unabhängige ambige Klassen, je nachdem die Partialnorm der Grundeinheit $= \pm 1$ oder $= \pm i$ ist. Die sämtlichen 2^s ambigen Ideale bestimmen im ersteren Falle 2^{s-2}, im letzteren 2^{s-1} voneinander verschiedene ambige Idealklassen.*

Was die beiden oben ausgeschlossenen Fälle $\delta = 3$ und $\delta = i$ betrifft, so gilt im ersteren Falle ebenfalls der eben ausgesprochene allgemeine Satz, da das einzige ambige Ideal $\mathfrak{L} = \sqrt{3}$ ein Hauptideal ist und die Partialnorm der Grundeinheit gleich $\pm i$ ausfällt. Im zweiten Falle $\delta = i$ dagegen verliert das im Satze angegebene Kriterium seine Anwendbarkeit, da die Partialnorm der Einheitswurzel $\sqrt{i}$ gleich $-i$ wird. Man erkennt, daß auch im Falle $\delta = i$ das einzige vorhandene aus der Zerlegung von $1 + i$ entspringende ambige Ideal ein Hauptideal ist.

Es werde hier noch der allgemeinere Fall hervorgehoben, in welchem δ gleich einer Primzahl und überdies $\equiv \pm 1$ nach $(1 + i)^4$ ist. In diesem Falle wird ebenfalls $s = 1$ und die obige Entwicklung zeigt, daß notwendigerweise die Partialnorm der Grundeinheit $= \pm i$ sein muß.

Es bleibt noch übrig, die Frage zu beantworten, ob im Körper K ambige Klassen vorhanden sind, welche kein ambiges Ideal enthalten. Zu dem Zwecke wählen wir in der ambigen Klasse C ein beliebiges Ideal $\mathfrak{J}$ aus; es ist dann $\frac{\mathfrak{J}}{S\mathfrak{J}}$ gleich einer Zahl A des Körpers K. Da es freisteht i A an Stelle von A zu wählen, so können wir die Annahmen $\nu(\mathsf{A}) = +1$ oder $= +i$ zugrunde legen.

Im ersteren Falle betrachten wir die Zahl $\mathsf{B} = 1 + S\mathsf{A}$. Wegen $\frac{\mathsf{B}}{S\mathsf{B}} = \frac{1}{\mathsf{A}}$ wird $\frac{\mathsf{B}\mathfrak{J}}{S(\mathsf{B}\mathfrak{J})} = 1$ d. h. $\mathsf{B}\mathfrak{J} = S(\mathsf{B}\mathfrak{J})$. Setzen wir daher $\mathsf{B}\mathfrak{J} = \frac{\alpha}{\beta}\mathfrak{A}$, wo α und β ganze imaginäre Zahlen sind und das Ideal $\mathfrak{A}$ durch keine ganze imaginäre Zahl teilbar ist, so folgt, daß $\mathfrak{A}$ ein ambiges Ideal ist: die Klasse C enthält mithin ein ambiges Ideal.

Ziehen wir zweitens die Annahme $\nu(\mathsf{A}) = i$ in Betracht, so erkennen wir zunächst, daß in diesem Falle das Charakterensystem von i aus lauter positiven Einheiten bestehen muß. Für die vorliegende Frage kommt es nun darauf an, ob die Partialnorm der Grundeinheit $\nu(\mathsf{E}) = +1$ oder $= +i$ ausfällt. Ist letzteres der Fall, so setzen wir einfach $\frac{\mathsf{A}}{\mathsf{E}}$ an Stelle von A und zeigen dann durch die eben angewandte Schlußweise, daß in der Idealklasse C ein ambiges Ideal vorkommt. Ist dagegen $\nu(\mathsf{E}) = +1$, so enthält die Klasse C kein ambiges Ideal. Wäre nämlich $\mathfrak{A} = \mathsf{B}\mathfrak{J}$ ein solches, wo B eine Zahl in K bedeutet, so

würde $\frac{\mathfrak{A}}{S\mathfrak{A}} = \frac{\mathsf{B}}{S\mathsf{B}}\mathsf{A}$ folgen. Andrerseits müßte aber $\frac{\mathfrak{A}}{S\mathfrak{A}}$ gleich einer Einheit, etwa gleich $\varrho\mathsf{E}^m$ sein und da $\nu(\mathsf{E}) = 1$ ist, so würde hieraus $\nu(\mathsf{A}) = \pm 1$ folgen, was der Annahme widerspricht.

Wir treffen nun die Voraussetzung, daß im Körper K das Charakterensystem von i aus lauter positiven Einheiten besteht; nach Satz 3 in § 4 gibt es dann eine Zahl A, deren Partialnorm gleich i ist, und wenn wir noch $\nu(\mathsf{E}) = 1$ annehmen, so muß die Zahl A notwendig gebrochen sein. Setzen wir $\mathsf{A} = \frac{\mathfrak{J}}{\mathfrak{J}'}$, wo $\mathfrak{J}$ und $\mathfrak{J}'$ zueinander prime Ideale sind, so wird $\frac{\mathfrak{J} \cdot S\mathfrak{J}}{\mathfrak{J}' \cdot S\mathfrak{J}'} = 1$ und hieraus folgt $\mathfrak{J}' = S\mathfrak{J}$ d. h. $\mathfrak{J}$ ist äquivalent mit $S\mathfrak{J}$ und bestimmt folglich eine ambige Klasse C; diese Klasse C enthält nach dem vorhin Bewiesenen kein ambiges Ideal. Wir fassen die gewonnenen Resultate in folgendem Satze zusammen.

Satz 3. *Es gibt im Körper K dann und nur dann eine ambige Klasse, welche kein ambiges Ideal enthält, wenn das Charakterensystem von i aus lauter positiven Einheiten besteht und wenn zugleich die Partialnorm der Grundeinheit gleich ± 1 ist.*

Die nämlichen Hilfsmittel führen zugleich zur Darstellung sämtlicher ambigen Klassen der genannten Eigenschaft. Nehmen wir nämlich an es gäbe 2 ambige Idealklassen, die kein ambiges Ideal enthalten und wählen aus diesen je ein Ideal $\mathfrak{J}$ und $\mathfrak{J}'$ aus, so zeigt die obige Entwicklung, daß die Partialnormen der beiden Zahlen $\mathsf{A} = \frac{\mathfrak{J}}{S\mathfrak{J}}$ und $\mathsf{A}' = \frac{\mathfrak{J}'}{S\mathfrak{J}'}$ gleich $\pm i$ sein müssen und es wird folglich $\nu\left(\frac{\mathsf{A}}{\mathsf{A}'}\right) = \pm 1$. Nehmen wir, was frei steht, in dieser Gleichung das obere Vorzeichen an, so folgt, daß $\mathsf{B} = 1 + \frac{S\mathsf{A}}{S\mathsf{A}'}$ der Gleichung $\frac{\mathsf{B}}{S\mathsf{B}} = \frac{\mathsf{A}'}{\mathsf{A}}$ genügt. Dieselbe ergibt $\mathsf{B}\frac{\mathfrak{J}}{\mathfrak{J}'} = S\left(\mathsf{B}\frac{\mathfrak{J}}{\mathfrak{J}'}\right)$; setzen wir daher $\mathsf{B}\frac{\mathfrak{J}}{\mathfrak{J}'} = \frac{\alpha}{\beta}\mathfrak{A}$, wo α und β ganze imaginäre Zahlen und das Ideal $\mathfrak{A}$ durch keine ganze imaginäre Zahl teilbar ist, so erweist sich $\mathfrak{A}$ als ein ambiges Ideal und der Quotient der beiden Ideale $\mathfrak{J}$ und $\mathfrak{J}'$ ist mithin einem ambigen Ideale äquivalent. Wir gewinnen aus diesen Überlegungen den Satz:

Satz 4. *Wenn im Körper K eine ambige Idealklasse vorhanden ist, welche kein ambiges Ideal enthält, so entstehen alle übrigen Klassen der nämlichen Beschaffenheit dadurch, daß man jene Klasse der Reihe nach mit allen aus ambigen Idealen entspringenden Klassen multipliziert.*

Die bisherigen Resultate ermöglichen die Berechnung der Anzahl aller ambigen Klassen. Betrachten wir zunächst den Fall, daß das Charakterensystem von i aus lauter positiven Einheiten besteht, so erkennen wir aus den soeben bewiesenen Sätzen 2, 3 und 4, daß es in diesem Falle genau 2^{s-1} ambige Klassen gibt, wo s die Anzahl der Primteiler der Partialdiskriminante d bedeutet. Von diesen 2^{s-1} ambigen Klassen entspringen sämtliche oder nur die

Hälfte aus ambigen Idealen, je nachdem die Partialnorm der Grundeinheit gleich $\pm i$ oder gleich ± 1 ausfällt. Kommt jedoch im Charakterensystem von i eine negative Einheit vor, so ist die Norm der Grundeinheit notwendig gleich ± 1; nach den Sätzen 2 und 3 dieses Paragraphen gibt es dann nur 2^{s-2} ambige Klassen und diese entspringen sämtlich aus ambigen Idealen. Setzen wir nun $c = s$ oder $= s - 1$, je nachdem das Charakterensystem von i aus lauter positiven Einheiten besteht oder nicht, so bedeutet c nach den Darlegungen des § 3 die Anzahl der Einzelcharaktere, welche das Geschlecht einer Idealklasse bestimmen und wir erhalten den Satz:

Satz 5. *Es gibt genau $c - 1$ voneinander unabhängige ambige Klassen, wo c die Anzahl der Einzelcharaktere bedeutet, welche das Geschlecht einer Klasse bestimmen. Die Anzahl der sämtlichen voneinander verschiedenen ambigen Idealklassen ist demgemäß $= 2^{c-1}$.*

Dieser allgemeine Satz gilt auch, wie man leicht erkennt, für den besonderen durch $\sqrt{i}$ bestimmten Dirichletschen Körper, welcher oben von der Betrachtung ausgeschlossen wurde.

§ 7. Die Anzahl der existierenden Geschlechter.

Die in § 4, 5 und 6 gewonnenen Resultate setzen uns in den Stand, die Anzahl der in einem Dirichletschen Zahlkörper K vorhandenen Geschlechter zu berechnen. Da das Charakterensystem einer Idealklasse des Körpers K aus c Einzelcharakteren besteht, deren jeder den Wert $+1$ oder -1 annehmen kann, so sind im ganzen 2^c Charakterensysteme möglich und es entsteht die wichtige Frage, ob für jedes dieser 2^c möglichen Charakterensysteme ein Geschlecht existiert oder ob nur ein Teil dieser Charakterensysteme unter den Geschlechtern wirklich vertreten ist. Um über diese Frage Auskunft zu erhalten, bezeichnen wir die Anzahl der voneinander verschiedenen existierenden Geschlechter mit g und die Anzahl der Klassen des Hauptgeschlechtes mit f. Da offenbar auch jedes andere Geschlecht f Klassen enthalten muß, so ist die Anzahl sämtlicher Klassen des Körpers $= gf$.

Bezeichnen wir nun die Klassen des Hauptgeschlechts mit $H_1, \ldots, H_f$, so können wir nach dem in § 4 bewiesenen Satze $H_1 = Q_1^2, \ldots, H_f = Q_f^2$ setzen, wo $Q_1, \ldots, Q_f$ gewisse Klassen des Körpers bedeuten. Es sei jetzt C eine beliebige Klasse des Körpers K; da dann C^2 offenbar zum Hauptgeschlecht gehört, so ist $C^2 = Q_r^2$, wo Q_r eine der eben bestimmten Klassen $Q_1, \ldots, Q_f$ bedeutet. Es ist folglich $\frac{C}{Q_r}$ eine ambige Idealklasse A, d. h. es wird $C = AQ_r$. Da nach Satz 5 in § 6 die Anzahl der ambigen Klassen 2^{c-1} beträgt, so stellt der Ausdruck AQ genau $2^{c-1}f$ Idealklassen dar. Diese sind auch sämtlich voneinander verschieden. Denn wäre $AQ_r = A'Q_{r'}$, wo A' eine ambige Klasse und $Q_{r'}$ eine der vorhin bestimmten Klassen $Q_1, \ldots, Q_f$ bedeutet, so würde

$Q_r^2 = Q_{r'}^2$ d. h. $H_r = H_{r'}$ und folglich $r = r'$ sein. Aus $Q_r = Q_{r'}$ folgt auch zugleich $A = A'$, womit die Behauptung bewiesen ist.

Die Gleichsetzung der so gefundenen Anzahl $2^{c-1}f$ sämtlicher Klassen mit der vorhin angegebenen Zahl gf ergibt $g = 2^{c-1}$. Wir haben somit die am Anfang dieses Paragraphen gestellte Frage beantwortet und es gilt der Satz:

Die Anzahl der existierenden Geschlechter ist gleich der Hälfte der möglichen Charakterensysteme, nämlich $= 2^{c-1}$, wo c die Anzahl der das Geschlecht bestimmenden Charaktere bezeichnet.

§ 8. Das Reziprozitätsgesetz.

Nachdem im vorigen Paragraph gezeigt worden ist, daß nur die Hälfte aller möglichen Charakterensysteme wirklich unter den Geschlechtern vertreten ist, entsteht die Frage nach der Bedingung, welche ein Charakterensystem erfüllen muß, damit für dasselbe ein Geschlecht existiert. Diese Frage wird durch das schon von Dirichlet aufgestellte Reziprozitätsgesetz der quadratischen Reste und Nichtreste im Gebiete der ganzen imaginären Zahlen beantwortet.

Um zunächst den quadratischen Restcharakter der Zahl i zu bestimmen, nehmen wir an, es sei $\varkappa$ eine von $1 + i$ verschiedene Primzahl im Körper k und überdies $\equiv (00)$ nach $(1 + i)^4$. Da zufolge der in § 6 gemachten Bemerkung in dem durch $\sqrt{\varkappa}$ bestimmten Körper $K_\varkappa$ die Partialnorm der Grundeinheit $= \pm i$ ist, so muß nach dem zu Anfang des § 3 bewiesenen Satze i quadratischer Rest von $\varkappa$ sein. Ist $\varkappa$ eine Primzahl und $\equiv (10)$ nach $(1 + i)^4$, so ist $i\varkappa \equiv (00)$ und folglich wird auch in diesem Falle $\left[\frac{i}{\varkappa}\right] = +1$.

Wir betrachten ferner den durch $\sqrt{i}$ bestimmten Dirichletschen Körper K_i. In diesem ist offenbar $1 + i$ der einzige Primfaktor der Partialdiskriminante. Das Symbol $\left[\frac{i}{1+i:i}\right]$ wird $= +1$ und es gibt im Körper K_i nur den einen Charakter $\left[\frac{\nu}{1+i:i}\right]$. Die Zahl der möglichen Charakterensysteme in K_i ist folglich $= 2$ und da nur die Hälfte derselben durch Geschlechter vertreten ist, so gibt es nur ein Geschlecht und es ist folglich stets $\left[\frac{\nu}{1+i:i}\right] = +1$, wo ν die Partialnorm eines beliebigen Ideals bedeutet. Es sei nun $\varkappa$ eine Primzahl, und zwar $\equiv (t_\varkappa t'_\varkappa)$ nach $(1 + i)^4$; ist dann i quadratischer Rest von $\varkappa$, so ist $\varkappa$ nach § 2 die Partialnorm eines Primideals und hieraus ergibt sich $\left[\frac{\varkappa}{1+i:i}\right] = (-1)^{t'_\varkappa} = +1$ d. h. $t'_\varkappa = 0$. Dieses Resultat ist die Umkehrung des vorigen; beide Resultate zusammen ergeben den Satz:

Wenn $\varkappa$ eine Primzahl und $\equiv (t_\varkappa t'_\varkappa)$ nach $(1 + i)^4$ ist, so bestimmt sich der quadratische Restcharakter der Zahl i in bezug auf $\varkappa$ durch die Formel

$$\left[\frac{i}{\varkappa}\right] = (-1)^{t'_\varkappa}.$$

Um den quadratischen Restcharakter von $1+i$ zu berechnen, betrachte ich zunächst den durch $\sqrt[4]{\varkappa}$ bestimmten Körper $K_\varkappa$, wo $\varkappa$ eine Primzahl und $\equiv (000)$ nach $(1+i)^5$ ist. Da in diesem Körper nur ein Geschlecht vorhanden sein darf und, wie oben gezeigt, der Charakter $\left[\frac{i}{\varkappa:\varkappa}\right]=+1$ ist, so folgt, daß die Norm eines jeden Ideals ebenfalls den Charakter $+1$ haben muß. Da nach § 2 die Zahl $1+i$ in zwei Ideale des Körpers $K_\varkappa$ zerlegbar ist und folglich die Partialnorm eines Ideals ist, so folgt $\left[\frac{1+i}{\varkappa:\varkappa}\right]=\left[\frac{1+i}{\varkappa}\right]=+1$. Ist $\varkappa\equiv(100)$, so wird $i\varkappa\equiv(000)$ nach $(1+i)^5$ sein und mithin haben wir auch in diesem Falle $\left[\frac{1+i}{\varkappa}\right]=+1$.

Es sei jetzt $\varkappa$ eine Primzahl und $\equiv(t_\varkappa 0 t''_\varkappa)$ nach $(1+i)^5$. Nehmen wir nun $\left[\frac{1+i}{\varkappa}\right]=+1$ an, so ist $\varkappa$ in dem durch $\sqrt[4]{1+i}$ bestimmten Körper zerlegbar und da in diesem Körper nur ein Geschlecht existiert und i den Charakter $+1$ besitzt, so ergibt sich auch $\left[\frac{\varkappa}{1+i:1+i}\right]=(-1)^{t''_\varkappa}=+1$, d. h. $t''_\varkappa=0$. Beide Resultate zusammengenommen bestimmen den quadratischen Restcharakter von $1+i$ in bezug auf $\varkappa$ für $t'_\varkappa=0$, und zwar gilt unter dieser Voraussetzung die Formel

$$\left[\frac{1+i}{\varkappa}\right]=(-1)^{t'''_\varkappa}.$$

Es sei endlich $\varkappa$ eine Primzahl und $\equiv(t_\varkappa 1 t''_\varkappa)$ nach $(1+i)^5$. In dem durch $\sqrt[4]{(1+i)\varkappa}$ bestimmten Körper sind, wie man leicht ausrechnet, die Charaktere der Zahl i beide $=-1$ und es existiert folglich nur ein Geschlecht. Wenn daher ν die Partialnorm eines Ideals ist, so müssen die beiden Charaktere der Zahl ν, nämlich die Symbole $\left[\frac{\nu}{\varkappa:(1+i)\varkappa}\right]$ und $\left[\frac{\nu}{1+i:(1+i)\varkappa}\right]$ entweder beide positiv oder beide negativ sein. Hieraus ergibt sich, falls wir $\nu=\varkappa$ nehmen, die Formel:

$$\left[\frac{1+i}{\varkappa}\right]=(-1)^{1+t''_\varkappa}.$$

Die beiden soeben gewonnenen Formeln lassen sich in eine zusammenfassen und wir erhalten somit den Satz:

Wenn $\varkappa$ eine Primzahl und $\equiv(t_\varkappa t'_\varkappa t''_\varkappa)$ nach $(1+i)^5$ ist, so bestimmt sich der quadratische Restcharakter der Zahl $1+i$ in bezug auf $\varkappa$ durch die Formel:

$$\left[\frac{1+i}{\varkappa}\right]=(-1)^{t'_\varkappa+t''_\varkappa}.$$

Um endlich das Reziprozitätsgesetz für 2 beliebige von $1+i$ verschiedene Primzahlen abzuleiten, berücksichtigen wir den Umstand, daß von den beiden ganzen imaginären Zahlen α und $i\alpha$ stets die eine $\equiv(0t_\alpha)$ nach $(1+i)^4$ ist.

Wir nehmen bei der nachfolgenden Untersuchung die beiden Primzahlen $\varkappa$ und π in dieser Gestalt an, so daß stets $t_\varkappa=0$, $t_\pi=0$ zu setzen ist.

Es sei zunächst $\varkappa$ eine Primzahl $\equiv(00)$ nach $(1+i)^4$. Ist dann π eine Primzahl von der Art, daß $\left[\frac{\varkappa}{\pi}\right]=+1$ wird, so kann π in dem durch $\sqrt[4]{\varkappa}$ bestimmten Körper $K_\varkappa$ zerlegt werden und ist folglich die Partialnorm eines Ideals. Durch die oben angewandte Schlußweise folgt dann, daß $\left[\frac{\pi}{\varkappa}\right]=+1$ sein muß. Wir haben somit die beiden folgenden Tatsachen erkannt:

Aus $\varkappa\equiv(00)$, $\pi\equiv(00)$ nach $(1+i)^4$ und $\left[\frac{\varkappa}{\pi}\right]=+1$ folgt $\left[\frac{\pi}{\varkappa}\right]=+1$, (1)

„ $\varkappa\equiv(00)$, $\pi\equiv(01)$ „ $(1+i)^4$ „ $\left[\frac{\varkappa}{\pi}\right]=+1$ „ $\left[\frac{\pi}{\varkappa}\right]=+1$. (2)

Es sei ferner $\varkappa\equiv(01)$ nach $(1+i)^4$, so gibt es in dem durch $\sqrt[4]{\varkappa}$ bestimmten Körper $K_\varkappa$ zwei Charaktere, aber nur ein Geschlecht, weil das Charakterensystem der Zahl i, wie man leicht durch Rechnung findet, aus 2 negativen Einheiten besteht. Ist daher π eine Primzahl von der Art, daß $\left[\frac{\varkappa}{\pi}\right]=+1$ wird, so müssen auch die Charaktere $\left[\frac{\pi}{1+i:\varkappa}\right]$ und $\left[\frac{\pi}{\varkappa:\varkappa}\right]$ entweder beide positiv oder beide negativ sein; hieraus folgt $\left[\frac{\pi}{\varkappa}\right]=+1$ und wir haben somit die beiden folgenden Tatsachen erkannt:

Aus $\varkappa\equiv(01)$, $\pi\equiv(00)$ nach $(1+i)^4$ und $\left[\frac{\varkappa}{\pi}\right]=+1$ folgt $\left[\frac{\pi}{\varkappa}\right]=+1$, (3)

„ $\varkappa\equiv(01)$, $\pi\equiv(01)$ „ $(1+i)^4$ „ $\left[\frac{\varkappa}{\pi}\right]=+1$ „ $\left[\frac{\pi}{\varkappa}\right]=+1$. (4)

Diese 4 Sätze zeigen, daß unter der Voraussetzung $t_\varkappa=0$, $t_\pi=0$ allgemein $\left[\frac{\varkappa}{\pi}\right]=\left[\frac{\pi}{\varkappa}\right]$ ist.

Es sei nämlich zunächst $t'_\varkappa=0$, $t'_\pi=0$. Nach (1) folgt aus $\left[\frac{\varkappa}{\pi}\right]=+1$ notwendig $\left[\frac{\pi}{\varkappa}\right]=+1$. Ist aber $\left[\frac{\varkappa}{\pi}\right]=-1$, so muß auch $\left[\frac{\pi}{\varkappa}\right]=-1$ sein, da ja ebenfalls nach (1) bei Vertauschung von $\varkappa$ mit π aus $\left[\frac{\pi}{\varkappa}\right]=+1$ notwendig auch $\left[\frac{\varkappa}{\pi}\right]=+1$ folgen würde.

Es sei ferner $t'_\varkappa=0$, $t'_\pi=1$. Nach (2) folgt aus $\left[\frac{\varkappa}{\pi}\right]=+1$ notwendig $\left[\frac{\pi}{\varkappa}\right]=+1$. Ist aber $\left[\frac{\varkappa}{\pi}\right]=-1$, so muß auch $\left[\frac{\pi}{\varkappa}\right]=-1$ sein, da ja nach (3) aus $\left[\frac{\pi}{\varkappa}\right]=+1$ auch $\left[\frac{\varkappa}{\pi}\right]=+1$ folgen würde.

Endlich sei $t'_\varkappa=1$, $t'_\pi=1$. Nach (4) folgt aus $\left[\frac{\varkappa}{\pi}\right]=+1$ notwendig $\left[\frac{\pi}{\varkappa}\right]=+1$. Ist aber $\left[\frac{\varkappa}{\pi}\right]=-1$, so muß auch $\left[\frac{\pi}{\varkappa}\right]=-1$ sein, da ja eben-

falls nach (4) aus $\left[\frac{\pi}{\varkappa}\right] = +1$ notwendig auch $\left[\frac{\varkappa}{\pi}\right] = +1$ folgen würde. Um die eben gefundene Formel $\left[\frac{\varkappa}{\pi}\right] = \left[\frac{\pi}{\varkappa}\right]$ für 2 beliebige Primzahlen $\varkappa, \pi$ anzuwenden, für welche $t_\varkappa$ und t_π nicht notwendig $= 0$ sind, müssen wir in jener Formel an Stelle $\varkappa, \pi$ bezüglich $i^{t_\varkappa}\varkappa$, $i^{t_\pi}\pi$ einsetzen und erhalten dann den folgenden Satz:

Wenn $\varkappa$ und π von $1+i$ verschiedene Primzahlen und bezüglich $\equiv (t_\varkappa t'_\varkappa)$ bezüglich $\equiv (t_\pi t'_\pi)$ nach $(1+i)^4$ sind, so gilt das Reziprozitätsgesetz

$$\left[\frac{\varkappa}{\pi}\right]\left[\frac{\pi}{\varkappa}\right] = (-1)^{t_\varkappa t'_\pi + t'_\varkappa t_\pi}.$$

Wir definieren nun das allgemeine Symbol $\left[\frac{\alpha}{\beta}\right]$, wo $\alpha = \overset{\varkappa}{\Pi}\varkappa$ und $\beta = \overset{\pi}{\Pi}\pi$ zwei beliebige zueinander und zu $1+i$ prime Zahlen sind, durch die Gleichung

$$\left[\frac{\alpha}{\beta}\right] = \overset{\varkappa,\pi}{\Pi}\left[\frac{\varkappa}{\pi}\right];$$

hierin ist das Produkt über alle Primfaktoren $\varkappa$ und π der beiden Zahlen α bezüglich β zu erstrecken, wie sie in der Produktdarstellung von α bezüglich β vorkommen. Es folgt dann unmittelbar der Satz:

Wenn α und β beliebige zueinander und zu $1+i$ prime ganze Zahlen sind und $\alpha \equiv (t_\alpha t'_\alpha)$, $\beta \equiv (t_\beta t'_\beta)$ nach $(1+i)^4$ gesetzt wird, so ist

$$\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right] = (-1)^{t_\alpha t'_\beta + t'_\alpha t_\beta}.$$

Diese Formel setzt uns in den Stand die Bedingung anzugeben, welche in einem beliebigen Dirichletschen Körper zwischen den c Charakteren bestehen muß, damit dieselben das Charakterensystem eines existierenden Geschlechtes bilden.

Wir nehmen zunächst an, daß δ nicht durch $1+i$ teilbar sei und setzen dann in obiger Formel $\alpha = \delta$ und $\beta = \nu$, wo ν eine zu δ und zu $1+i$ prime Partialnorm eines Ideals im Körper K_δ bedeutet. Da dann nach § 2 die Zahl δ von allen in ν zu ungerader Potenz vorkommenden Primzahlen quadratischer Rest sein muß, so ist $\left[\frac{\delta}{\nu}\right] = +1$ und folglich wird

$$\left[\frac{\nu}{\delta}\right] = (-1)^{t_\delta t'_\nu + t'_\delta t_\nu}.$$

Ist nun $\delta \equiv (00)$ nach $(1+i)^4$, so wird die Partialdiskriminante $d = \delta$ und wenn wir daher sämtliche in derselben aufgehenden Primzahlen mit $\lambda_1, \ldots, \lambda_s$ bezeichnen, so wird

$$\left[\frac{\nu}{\lambda_1}\right] \cdots \left[\frac{\nu}{\lambda_s}\right] = \left[\frac{\nu}{\lambda_1 : \delta}\right] \cdots \left[\frac{\nu}{\lambda_s : \delta}\right] = +1.$$

Ist dagegen δ nicht $\equiv (00)$ nach $(1+i)^4$, so kommt $1+i$ in der Partialdiskriminante d des Körpers K_δ als Faktor vor. Wir bezeichnen dann die in

δ aufgehenden Primzahlen mit $\lambda_1, \ldots, \lambda_{s-1}$ und setzen $1+i = \lambda_s$. Wegen $\left[\frac{\nu}{1+i:\delta}\right] = (-1)^{t_\delta t'_\nu + t'_\delta t_\nu}$ erhalten wir wiederum:

$$\left[\frac{\nu}{\lambda_1 : \delta}\right] \cdots \left[\frac{\nu}{\lambda_s : \delta}\right] = +1.$$

Endlich sei δ durch $1+i$ teilbar; wir setzen $\delta = (1+i)\delta'$ und erteilen ν die obige Bedeutung. Da wiederum δ von allen in ν zu ungerader Potenz vorkommenden Primzahlen quadratischer Rest sein muß, so kann bei der Berechnung der Faktoren des Symbols $\left[\frac{\delta'}{\nu}\right]$ die Zahl δ' durch $1+i$ ersetzt werden; die oben gefundene Formel für den quadratischen Restcharakter von $1+i$ ergibt dann $\left[\frac{\delta'}{\nu}\right] = (-1)^{t'_\nu + t''_\nu}$. Setzen wir ferner in der allgemeinen Reziprozitätsgleichung $\alpha = \delta'$, $\beta = \nu$ und benutzen dann den soeben gefundenen Wert des Symbols $\left[\frac{\delta'}{\nu}\right]$, so erhalten wir $\left[\frac{\nu}{\delta'}\right] = (-1)^{t_{\delta'} t'_\nu + t'_{\delta'} t_\nu + t'_\nu + t''_\nu}$. Andererseits hat das Symbol $\left[\frac{\nu}{1+i:\delta}\right]$ den gleichen Wert und hieraus ergibt sich wiederum, wenn wir die sämtlichen in δ enthaltenen Primzahlen mit $\lambda_1, \ldots, \lambda_s$ bezeichnen, die Gleichung

$$\left[\frac{\nu}{\lambda_1 : \delta}\right] \cdots \left[\frac{\nu}{\lambda_s : \delta}\right] = +1.$$

Es gilt daher in allen Fällen der Satz:

Ein vorgelegtes Charakterensystem ist dann und nur dann durch ein Geschlecht vertreten, wenn das Produkt aller Charaktere desselben $= +1$ ist.

§ 9. Der spezielle Dirichletsche Körper.

Wenn der durch $\sqrt{\delta}$ bestimmte Dirichletsche Körper K außer dem Körper k noch einen anderen quadratischen Körper enthalten soll, so muß, wie man leicht erkennt, δ gleich einer reellen oder gleich einer rein imaginären Zahl sein. In diesem Falle bezeichnen wir den durch $\sqrt{\delta}$ bestimmten Dirichletschen biquadratischen Körper als einen *speziellen Dirichletschen Körper* und setzen $\partial = \pm\delta$ bezüglich $\partial = \pm 2i\delta$, so daß ∂ stets eine reelle positive Zahl bedeutet, welche durch kein Quadrat einer reellen Zahl teilbar ist. Der spezielle Dirichletsche Körper K ist ein Galoisscher Körper. Eine beliebige Zahl desselben kann in die Gestalt:

$$\mathsf{A} = a + bi + c\sqrt{\partial} + di\sqrt{\partial}$$

gebracht werden, wo a, b, c, d rationale Zahlen sind und wir erhalten die 3 zu A konjugierten Zahlen durch Anwendung der 3 Substitutionen:

$$\begin{aligned} S &= (\sqrt{\partial} : -\sqrt{\partial}), \\ S' &= (i : -i), \\ S'' &= SS' = (\sqrt{\partial} : -\sqrt{\partial},\ i : -i). \end{aligned}$$

Diesen 3 Substitutionen entsprechen 3 in K enthaltene quadratische Zahlkörper: alle Zahlen nämlich, welche bei Anwendung von S ungeändert bleiben, bilden den durch i bestimmten quadratischen Körper k und alle bei Anwendung der Substitution S' bezüglich S'' ungeändert bleibenden Zahlen des Körpers K bilden je einen quadratischen Körper, nämlich den durch $\sqrt{\partial}$ bezüglich durch $\sqrt{-\partial}$ bestimmten quadratischen Zahlkörper; der erstere möge mit k', der zweite mit k'' bezeichnet werden.

Wir fügen hier noch eine Entwicklung an, welche im folgenden Paragraph gebraucht werden wird.

Wenn ein Ideal des Körpers K als größter gemeinsamer Teiler von solchen Zahlen dargestellt werden kann, welche lediglich Zahlen der Unterkörper k' bezüglich k'' sind, so sagen wir, das Ideal „*liege*“ im Körper k' bezüglich k''. Ist $\mathfrak{J}$ irgendein Ideal in K, so liegt stets das Produkt $\mathfrak{J}\cdot S'\mathfrak{J}$ im Körper k'. Wählen wir nämlich irgendeine durch $\mathfrak{J}$ teilbare Zahl A und bestimmen dann eine ebenfalls durch $\mathfrak{J}$ teilbare Zahl B derart, daß $\frac{\mathsf{B}}{\mathfrak{J}}$ prim zu $\frac{\mathsf{A}}{\mathfrak{J}}S'\left(\frac{\mathsf{A}}{\mathfrak{J}}\right)$ ist, so wird notwendig auch $S'\left(\frac{\mathsf{B}}{\mathfrak{J}}\right)$ und daher auch $\frac{\mathsf{B}}{\mathfrak{J}}S'\left(\frac{\mathsf{B}}{\mathfrak{J}}\right)$ prim zu $\frac{\mathsf{A}}{\mathfrak{J}}S'\left(\frac{\mathsf{A}}{\mathfrak{J}}\right)$ und hieraus folgt $\mathfrak{J}\cdot S'\mathfrak{J} = (\mathsf{A}\cdot S'\mathsf{A},\ \mathsf{B}\cdot S'\mathsf{B})$, womit die Behauptung bewiesen ist. Ebenso wird gezeigt, daß $\mathfrak{J}\cdot S''\mathfrak{J}$ stets in dem Körper k'' liegt.

§ 10. Die Anzahl der Idealklassen des speziellen Dirichletschen Körpers K.

In diesem letzten Paragraph soll kurz der Weg gezeigt werden, welcher zu einem rein arithmetischen Beweise des in der Einleitung erwähnten Dirichletschen Satzes über die Anzahl der Idealklassen in K führt.

Zu dem Zweck stellen wir zunächst folgende Überlegungen an. Sind c', c'' irgend zwei Idealklassen der beiden quadratischen Körper k' bezüglich k'' und wählt man aus diesen beiden Klassen je ein Ideal $\mathfrak{j}'$, $\mathfrak{j}''$, so gehört jedes dieser beiden Ideale, als Ideal des biquadratischen Körpers K aufgefaßt, einer Idealklasse in K an; die beiden somit durch c', c'' bestimmten Idealklassen des biquadratischen Körpers K mögen mit $\overline{c'}$ bezüglich $\overline{c''}$ und ihr Produkt mit $\overline{c'c''}$ bezeichnet werden. Es gilt dann zunächst der Satz:

Jede Klasse des Hauptgeschlechtes im biquadratischen Körper K ist gleich einem Produkte $\overline{c'c''}$, wo c', c'' Klassen der quadratischen Körper k' bezüglich k'' sind.

Zum Beweise dieses Satzes benutzen wir die Tatsache, daß jedes Ideal $\mathfrak{H}$ des Hauptgeschlechtes dem Quadrate eines Ideals $\mathfrak{J}$ im biquadratischen Körper äquivalent ist. Es gilt andrerseits die Identität

$$\mathfrak{J}^2 = \frac{(\mathfrak{J}\cdot S'\mathfrak{J})\,(\mathfrak{J}\cdot S''\mathfrak{J})}{S'\mathfrak{J}\cdot S''\mathfrak{J}}.$$

Da das Produkt $S'\mathfrak{J}\cdot S''\mathfrak{J}$ bei Anwendung der Substitution S ungeändert bleibt, so ist dasselbe gleich einer Zahl in k und folglich ein Hauptideal. Da $\mathfrak{J}\cdot S'\mathfrak{J}$ und $\mathfrak{J}\cdot S''\mathfrak{J}$ bezüglich in den Körpern k' und k'' liegen, so erkennen wir, daß $\mathfrak{J}^2$ und mithin auch $\mathfrak{H}$ äquivalent dem Produkt eines in k' und eines in k'' liegenden Ideals ist.

Es seien nun $p_1, \ldots, p_\pi$ die in ∂ aufgehenden der Kongruenz $p \equiv 1$ nach 4 genügenden und $q_1, \ldots, q_\varkappa$ die in ∂ aufgehenden der Kongruenz $q \equiv 3$ nach 4 genügenden Primzahlen. Die ersteren Primzahlen lassen sich als Produkt zweier ganzer imaginärer Zahlen darstellen, und zwar sei $p_1 = \alpha_1\beta_1, \ldots, p_\pi = \alpha_\pi\beta_\pi$.

Wir bezeichnen jetzt im biquadratischen Körper K diejenigen Geschlechter als *die Geschlechter der Hauptart*, für welche die Charaktere der Norm ν den Bedingungen:

$$\left[\frac{\nu}{\alpha_1:\partial}\right]\left[\frac{\nu}{\beta_1:\partial}\right] = +1, \ldots, \left[\frac{\nu}{\alpha_\pi:\partial}\right]\left[\frac{\nu}{\beta_\pi:\partial}\right] = +1$$

und

$$\left[\frac{\nu}{q_1:\partial}\right] = +1, \ldots, \left[\frac{\nu}{q_\varkappa:\partial}\right] = +1$$

genügen. Unmittelbar aus dieser Definition folgt die Tatsache, daß genau der $2^{\pi+\varkappa-1}$-te Teil bezüglich der $2^{\pi+\varkappa}$-te Teil sämtlicher Geschlechter des Körpers K von der Hauptart ist, je nachdem ∂ ungerade oder gerade ist. Es gilt ferner der Satz:

Jedes Produkt $\overline{c'c''}$ gehört im biquadratischen Körper K einem Geschlechte der Hauptart an, und umgekehrt jede Klasse C des biquadratischen Körpers K, welche einem Geschlechte der Hauptart angehört, ist gleich einem Produkt $\overline{c'c''}$.

Um den ersten Teil dieses Satzes zu beweisen, berücksichtigen wir, daß die Partialnorm eines jeden in k' oder k'' liegenden Ideals eine ganze rationale Zahl wird und benutzen dann die beiden folgenden Tatsachen:

1. Ist $p = \alpha\beta$ eine rationale in k zerlegbare Primzahl, so ist jede rationale Zahl im Gebiet der ganzen imaginären Zahlen gleichzeitig quadratischer Rest oder Nichtrest in bezug auf die konjugiert imaginären Faktoren α und β.

2. Ist q eine rationale in k unzerlegbare Primzahl, so ist jede rationale Zahl im Gebiet der ganzen imaginären Zahlen quadratischer Rest in bezug auf q.

Um die Richtigkeit der Umkehrung zu erkennen, bemerken wir, daß jedenfalls entweder die Diskriminante des quadratischen Körpers k' oder die des quadratischen Körpers k'' den Faktor 2 enthalten muß. Aus der bekannten Theorie der quadratischen Körper folgt daher, daß notwendig in einem jener beiden quadratischen Körper ein Geschlecht existieren muß, dessen Charaktere in bezug auf die Primzahlen $p_1, \ldots, p_\pi$ der Reihe nach mit den Werten der Symbole $\left[\frac{\nu}{\alpha_1:\partial}\right], \ldots, \left[\frac{\nu}{\alpha_\pi:\partial}\right]$ übereinstimmen. Ist a eine Klasse dieses Geschlechtes im quadratischen Körper k' oder k'', so gehört, wie man leicht

erkennt, die Klasse $C\bar{a}$ im biquadratischen Körper K dem Hauptgeschlechte an und wird daher nach dem früher bewiesenen Satze gleich $\overline{c'c''}$; hieraus folgt $C = \frac{\overline{c'}\,\overline{c''}}{\bar{a}}$.

Das nächste Ziel ist die Berechnung der Anzahl derjenigen Paare von Klassen c', c'' der quadratischen Körper k' bezüglich k'', für welche $\overline{c'c''} = 1$ wird. Wir bedürfen dazu folgender Begriffe und Sätze aus der Theorie der quadratischen Körper:

Ein Ideal des quadratischen Körpers, welches gleich seinem konjugierten und überdies durch keine ganze rationale Zahl teilbar ist, werde ein *ambiges Ideal* genannt. Die ambigen Ideale setzen sich aus ambigen Primidealen zusammen und diese bestimmen sich durch die Eigenschaft, daß ihre Quadrate den in der Diskriminante des Körpers enthaltenen rationalen Primzahlen gleich sind.

Eine Klasse des quadratischen Körpers, deren Quadrat die Hauptklasse ist, heißt eine *ambige Klasse*. Ist der quadratische Körper imaginär, so enthält jede ambige Klasse desselben ein ambiges Ideal und die Anzahl der ambigen Klassen ist $= 2^{\sigma-1}$, wo σ die Anzahl der in der Diskriminante aufgehenden rationalen Primzahlen ist.

Es seien c', c'' zwei Klassen der quadratischen Körper k' bezüglich k'' von der Art, daß $\overline{c'\,c''} = 1$ wird. Wir wählen dann aus diesen Klassen c' und c'' je ein Ideal $\mathfrak{j}'$ bezüglich $\mathfrak{j}''$ aus und setzen $\mathfrak{j}'\mathfrak{j}'' = \mathsf{A}$, wo A eine Zahl des biquadratischen Körpers K bedeutet. Durch Anwendung der Substitution S'' ergibt sich leicht $(\mathfrak{j}'\cdot S''\mathfrak{j}')\mathfrak{j}''^2 = \mathsf{A}S''\mathsf{A}$ d. h. $\mathfrak{j}''^2 = \alpha''$, wo α'' eine Zahl im quadratischen Körper k'' ist. Es folgt mithin, daß $\mathfrak{j}''$ einer ambigen Klasse a'' in k'' angehört und da k'' ein imaginärer quadratischer Körper ist, so ist dem eben angeführten Satze zufolge $\mathfrak{j}''$ einem ambigen Ideale $\mathfrak{a}''$ in k'' äquivalent. Nun liegen, wie man leicht erkennt, sämtliche ambigen Primideale des Körpers k'' zugleich auch in dem quadratischen Körper k'; ausgenommen ist lediglich der Fall $\partial = 1$ nach 4, in welchem das durch Zerlegung der Zahl 2 entstehende ambige Primideal $\mathfrak{l}''$ im Körper k'', aber nicht im Körper k' liegt. Da $\mathfrak{l}'' = 1 + i$ und folglich ein Hauptideal des biquadratischen Körpers K ist, so wird, wenn l'' die durch $\mathfrak{l}''$ bezeichnete Klasse in k'' bezeichnet, offenbar $\overline{l''} = 1$. Es sei nun $\mathfrak{a}''$ nicht durch $\mathfrak{l}''$ teilbar und $\mathfrak{a}'$ dasjenige ambige Ideal in k', welches, als Ideal in K betrachtet, dem Ideal $\mathfrak{a}''$ gleich ist, und a' sei die durch $\mathfrak{a}'$ bestimmte ambige Klasse in k': es ist dann offenbar $\overline{a'a''} = 1$. Somit gilt der Satz:

Zu jeder ambigen Klasse a'' in k'' und nur zu diesen läßt sich eine Klasse a' in k' finden derart, daß $\overline{a'a''} = 1$ wird.

Es bleibt jetzt noch übrig, die Frage zu entscheiden, wann zu einer Klasse a'' des Körpers k'' mehr als eine Klasse c' existiert, für welche $\overline{c'a''} = 1$ wird.

Es ist hierzu offenbar notwendig, daß im Körper k' eine von 1 verschiedene Klasse c' existiert, für welche $\overline{c'} = 1$ ist.

Um hierüber zu entscheiden, nehmen wir an, es sei $\mathfrak{h}'$ ein Ideal in k', welches im biquadratischen Körper K ein Hauptideal ist. Setzen wir $\mathfrak{h}' = \mathsf{A}$, wo A eine Zahl in K ist, so wird offenbar $\frac{\mathsf{A}}{S'\mathsf{A}}$ eine Einheit des Körpers K, deren absoluter Betrag $= 1$ und welche daher eine Einheitswurzel ϱ ist. Setzen wir nun $\mathsf{B} = \mathsf{A}$, $= i\mathsf{A}$, $= \frac{\mathsf{A}}{1-i}$, oder $= \frac{\mathsf{A}}{1+i}$, je nachdem ϱ den Wert $+1$, -1, $+i$ oder $-i$ hat, so ergibt sich $\frac{\mathsf{B}}{S'\mathsf{B}} = 1$ d. h. B ist eine reelle Zahl. Folglich ist $\mathfrak{h}'$ entweder gleich einer reellen Zahl d. h. ein Hauptideal in k' oder $\mathfrak{h}'$ wird gleich einer reellen Zahl, multipliziert mit einem Ideal $\mathfrak{l}'$, welches als Ideal in K aufgefaßt, gleich $1 + i$ ist. Da somit $\mathfrak{l}'^2 = 2$ sein muß, so tritt dieser letztere Fall nur unter der Bedingung $\partial \equiv 3$ nach 4 oder $\partial \equiv 0$ nach 2 ein. Umgekehrt bestimmt das durch die Gleichung $\mathfrak{l}'^2 = 2$ definierte Ideal $\mathfrak{l}'$ stets in k' eine Klasse l', für welche $\overline{l'} = 1$ wird. Der Fall, in welchem K noch andere Einheitswurzeln enthält, ist leicht für sich erledigt. Es folgt aus unseren Entwicklungen das Resultat:

Die Anzahl der Paare von Klassen c', c'' in den Körpern k', bezüglich k'', für welche $\overline{c'c''} = 1$ wird, ist im Falle eines ungeraden ∂ gleich der Zahl $2^{\pi+\varkappa-1}$ oder $= 2^{\pi+\varkappa}$ und im Falle eines geraden ∂ gleich der Zahl $2^{\pi+\varkappa}$ oder gleich $2^{\pi+\varkappa+1}$, je nachdem die Zahl 2, abgesehen von einem Einheitsfaktor, das Quadrat einer Zahl des reellen quadratischen Körpers k' ist oder nicht.

Bezeichnen wir nun die Anzahl der Idealklassen c', c'' in den beiden Körpern k', k'' bezüglich mit h', h'', so erhalten wir $h'h''$ Kombinationen von der Gestalt $\overline{c'c''}$ und wenn wir diese Anzahl $h'h''$ durch die soeben gefundene Anzahl der die Bedingung $\overline{c'c''} = 1$ erfüllenden Klassenpaare dividieren, so ergibt sich die Anzahl der sämtlichen voneinander verschiedenen Klassen $\overline{c'c''}$ des biquadratischen Körpers, welche von der Hauptart sind. Da aber, wie oben angegeben worden ist, genau der $2^{\pi+\varkappa-1}$-te Teil bezüglich der $2^{\pi+\varkappa}$-te Teil sämtlicher Geschlechter des Körpers K der Hauptart angehört, je nachdem ∂ ungerade oder gerade ist, so gewinnen wir den Satz:

Die Anzahl der Idealklassen des speziellen Dirichletschen Zahlkörpers K ist gleich dem Produkt der Anzahlen der Idealklassen in den beiden quadratischen Körpern k' und k'' oder gleich der Hälfte dieses Produktes, je nachdem in dem reellen quadratischen Körper die Zahl 2, abgesehen von einem Einheitsfaktor, das Quadrat einer Zahl ist oder nicht.

Bezeichnet α' die Zahl in k', deren Quadrat, abgesehen von einem Einheitsfaktor, die Zahl 2 ergibt, so ist $\frac{1+i}{\alpha'}$ eine Einheit des biquadratischen Körpers K, deren Partialnorm $= \pm i$ wird. Es gilt auch umgekehrt der Satz, daß die

Zahl 2, abgesehen von einem Einheitsfaktor, gleich dem Quadrat einer Zahl in k' sein muß, sobald in K eine Einheit existiert, deren Partialnorm $= \pm i$ ist. Benutzen wir diese Tatsachen, so können wir den gefundenen Satz auch in folgender Weise aussprechen:

Die Anzahl der Idealklassen in K ist gleich dem Produkt der Klassenzahlen in k' und k'' oder gleich der Hälfte dieses Produktes, je nachdem die Partialnorm der Grundeinheit des Körpers K gleich $\pm i$ oder $= \pm 1$ wird.

Wir erkennen die inhaltliche Übereinstimmung dieses Satzes mit dem von DIRICHLET[1] bewiesenen Satze, wenn wir berücksichtigen, daß der von DIRICHLET ausgesprochene Satz die Anzahlen von *Formenklassen* mit gegebener Determinante betrifft, während es sich in unserem Satze um Anzahlen von *Idealklassen* der Körper handelt.

Königsberg, den 14. April 1894.

[1] Werke 1, 618.

6. Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper[1].

[Aus den Nachrichten der Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-physikalische Klasse. 1896. S. 29—39.]

L. KRONECKER hat in den Monatsberichten der Berliner Akademie vom Jahre 1853 zuerst den fundamentalen Satz aufgestellt, daß die Wurzeln aller Abelschen Gleichungen im Bereich der rationalen Zahlen sich durch Einheitswurzeln rational ausdrücken lassen. Bezeichnet man diejenigen Zahlkörper, die durch Einheitswurzeln bestimmt sind, und alle Unterkörper von solchen Körpern kurz als Kreiskörper, so spricht sich der genannte Satz wie folgt aus:

Fundamentalsatz. *Alle Abelschen Zahlkörper im Gebiete der rationalen Zahlen sind Kreiskörper.*

H. WEBER hat in den Acta Mathematica Bd. 8 einen vollständigen und allgemeinen Beweis dieses Satzes erbracht. Die vorliegende Note enthält einen neuen Beweis, welcher weder die Kummersche Zerlegung der Lagrangeschen Resolvente in Primideale noch die Anwendung der dem Wesen des Satzes fremdartigen transzendenten Methoden von DIRICHLET erfordert. Der folgende Beweis ist vielmehr rein arithmetischer Natur; er beruht wesentlich auf den allgemeinen Begriffsbildungen, die ich in der Note „Grundzüge einer Theorie des Galoisschen Zahlkörpers“[2] in diesen Nachrichten vom Jahre 1894 kurz dargelegt habe und ist vermutlich weitgehender Verallgemeinerungen fähig.

Wenn die Gruppe eines Abelschen Körpers aus den Potenzen einer einzigen Substitution besteht, so heiße der Abelsche Körper zyklisch. Wir konstruieren folgende besonderen zyklischen Körper. Es bedeute u eine ungerade Primzahl und u^{h+1} eine Potenz derselben; dann ist der durch $e^{\frac{2i\pi}{u^{h+1}}}$ bestimmte Körper $k\left(e^{\frac{2i\pi}{u^{h+1}}}\right)$ ein zyklischer Körper vom $u^h(u-1)$-ten Grade.

[1] Hierzu siehe auch die entsprechenden Stellen im „Zahlbericht“, dieser Band Abh. 7, S. 205—216.

[2] Dieser Band Abh. 4, S. 13.

Der zyklische Unterkörper vom u^h-ten Grade dieses Körpers werde mit U_h bezeichnet; die Diskriminante von U_h ist eine Potenz von u. Ferner bestimmt die Zahl $e^{\frac{i\pi}{2^{h+1}}} + e^{-\frac{i\pi}{2^{h+1}}}$ einen reellen zyklischen Körper vom 2^h-ten Grade. Dieser Körper werde mit Z_h bezeichnet; die Diskriminante desselben ist eine Potenz von 2. Endlich wählen wir eine rationale Primzahl p mit der Kongruenzeigenschaft $p \equiv 1$ nach l^h aus, wo l eine beliebige gerade oder ungerade Primzahl bedeutet; dann besitzt der Kreiskörper $k\left(e^{\frac{2i\pi}{p}}\right)$ vom Grade $p-1$ offenbar einen zyklischen Unterkörper vom Grade l^h, dessen Diskriminante eine Potenz von p ist. Dieser zyklische Körper l^h-ten Grades werde mit P_h bezeichnet. Die Körper U_h, Z_h, P_h sind sämtlich Kreiskörper.

Wir beweisen nun der Reihe nach folgende Hilfssätze über zyklische Körper.

Satz 1. Wenn ein beliebiger zyklischer Körper L_h, dessen Grad l^h die Potenz einer geraden oder ungeraden Primzahl l ist, keinen der beiden Körper U_1 oder Z_1 als Unterkörper enthält, so gibt es in dem durch die Zahl $\Theta = e^{\frac{2i\pi}{l^h}}$ bestimmten Körper $k(\Theta)$ stets eine ganze algebraische Zahl $\varkappa$ von der Art, daß der aus $k(\Theta)$ und L_h zusammengesetzte Körper $k(\Theta, L_h)$ durch die Zahlen Θ und $\sqrt[l^h]{\varkappa}$ bestimmt ist. Die Zahl $\varkappa$ besitzt obenein die Eigenschaft, daß $\varkappa^{t-r}$ die l^h-te Potenz einer Zahl in $k(\Theta)$ wird; dabei bedeutet r eine beliebige, nicht durch l teilbare ganze rationale Zahl, ferner $t = (\Theta : \Theta^r)$ die zugehörige Substitution der Gruppe des Kreiskörpers $k(\Theta)$ und endlich ist symbolisch $t\varkappa = \varkappa^t$, d. h. $\frac{t\varkappa}{\varkappa^r} = \varkappa^{t-r}$ gesetzt.

Beweis. Ist α eine den Körper L_h bestimmende ganze algebraische Zahl und sind $1, s, s^2, \ldots, s^{l^h-1}$ die Substitutionen der Gruppe von L_h, so setze man

$$K = \alpha + \Theta \cdot s\alpha + \Theta^2 \cdot s^2\alpha + \cdots + \Theta^{l^h-1} \cdot s^{l^h-1}\alpha .$$

Aus $sK = \Theta^{-1}K$ folgt leicht, daß die beiden Zahlen K^{l^h} und K^{t-r} Zahlen des Körpers $k(\Theta)$ sind. Die Zahl $\varkappa = K^{l^h}$ ist daher von der verlangten Beschaffenheit. Daß der durch Θ und $\sqrt[l^h]{\varkappa}$ bestimmte Körper mit dem durch Θ und α bestimmten Körper identisch ist, folgt leicht aus der Gleichheit ihrer Grade, da der letztere Körper den ersteren enthält.

Satz 2. Wenn ein beliebiger zyklischer Körper L_h, dessen Grad u^h die Potenz einer ungeraden Primzahl ist, den Körper U_{h-1} als Unterkörper enthält, so enthält der aus $\vartheta = e^{\frac{2i\pi}{u}}$ und aus L_h zusammengesetzte Körper $k(\vartheta, L_h)$ notwendig den durch $\Theta = e^{\frac{2i\pi}{u^h}}$ bestimmten Körper $k(\Theta)$ als Unterkörper. Es gibt nun in diesem Körper $k(\Theta)$ stets eine ganze algebraische Zahl $\varkappa$ derart, daß der Körper $k(\vartheta, L_h)$ auch durch die Zahlen ϑ und $\sqrt[u]{\varkappa}$

bestimmt ist. Bezeichnet ferner r eine Primitivzahl nach u^h und wird $t = (\Theta : \Theta^r)$ gesetzt, so besitzt die Zahl $\varkappa$ obenein die Eigenschaft, daß $\varkappa^{t-r}$ die u-te Potenz einer Zahl des Körpers $k(\Theta)$ wird.

Beweis. Ist α eine den Körper L_h bestimmende, ganze algebraische Zahl und sind $1, s, s^2, \ldots, s^{u^h-1}$ die Substitutionen der Gruppe von L_h, so setze man $S = s^{u^{h-1}}$ und

$$K = \alpha + \vartheta \cdot S\alpha + \vartheta^2 \cdot S^2\alpha + \cdots + \vartheta^{u-1} \cdot S^{u-1}\alpha .$$

Der Körper $k(\vartheta, L_h)$ enthält offenbar den Körper $k(\Theta)$ als Unterkörper, und zwar sind die Zahlen dieses Unterkörpers $k(\Theta)$ dadurch charakterisiert, daß sie bei der Substitution S ungeändert bleiben. Wegen $SK = \vartheta^{-1}K$ ist somit K^u eine Zahl in $k(\Theta)$. Es sei nun t' eine solche Substitution der Gruppe des Körpers $k(\vartheta, L_h)$, daß $t'\Theta = \Theta^r$ wird; dann ist $St'K = t'SK = \vartheta^{-r}t'K$; da mithin der Ausdruck $K^{t'-r}$ bei der Substitution S ungeändert bleibt, so ist $K^{t'-r}$ eine Zahl in $k(\Theta)$ und folglich wird $K^{u(t'-r)} = \varkappa^{t'-r}$ die u-te Potenz einer solchen Zahl. Der Kürze halber ist hier wiederum von der symbolischen Schreibweise $t'K = K^{t'}$ Gebrauch gemacht.

Satz 3. Wenn L_h ein beliebiger zyklischer Körper ist, dessen Grad l^h die Potenz einer beliebigen geraden oder ungeraden Primzahl ist, so kann man stets einen zyklischen Körper M_h vom Grade $l^{h'}$, wo $h' \leqq h$ ist, und mit folgenden beiden Eigenschaften finden. Erstens: der aus M_h und einem gewissen Kreiskörper K zusammengesetzte Körper enthält L_h als Unterkörper und zweitens: in der Diskriminante von M_h geht keine rationale Primzahl p mit der Kongruenzeigenschaft $p \equiv 1$ nach l^h auf.

Beweis. Ist p eine rationale Primzahl, welche die Kongruenzeigenschaft $p \equiv 1$ nach l^h besitzt und welche in der Diskriminante des Körpers L_h aufgeht, so konstruiere man den zyklischen Kreiskörper P_h vom Grade l^h, dessen Diskriminante eine Potenz von p ist, und betrachte den aus L_h und P_h zusammengesetzten Körper $k(L_h, P_h)$ vom $l^{h+h'}$-ten Grade. In P_h ist $p = \mathfrak{p}^{l^h}$, wo $\mathfrak{p}$ ein Primideal in P_h bedeutet. Es sei $\mathfrak{P}$ ein in $\mathfrak{p}$ aufgehendes Primideal des Körpers $k(L_h, P_h)$. Da das Primideal $\mathfrak{P}$ in der Gradzahl $l^{h+h'}$ des Körpers $k(L_h, P_h)$ nicht aufgeht, so ist dieser Körper $k(L_h, P_h)$ als Verzweigungskörper des Primideals $\mathfrak{P}$ relativ zyklisch, und zwar mindestens vom Relativgrade l^h in bezug auf den Trägheitskörper L_h' des Primideals $\mathfrak{P}$. Da ferner zyklische Körper von höherem als dem l^h-ten Grade in $k(L_h, P_h)$ nicht vorkommen, so hat $k(L_h, P_h)$ genau den Relativgrad l^h in bezug auf L_h'. Hieraus folgt, daß der Trägheitskörper L_h' vom Grade $l^{h'}$ ist; dieser Körper L_h' ist überdies zyklisch, da sonst, wie die Lehre von den Abelschen Gruppen zeigt, der Körper $k(L_h, P_h)$ nicht relativ zyklisch in bezug auf L_h' sein könnte. Das Grundideal des Trägheitskörpers L_h' ist nicht durch $\mathfrak{P}$ und daher auch die Diskriminante von L_h' nicht durch p teilbar; diese Diskriminante enthält

daher nur solche Primteiler, welche in der Diskriminante des Körpers L_h aufgehen und verschieden von p sind. Es handelt sich nun darum, ob in der Diskriminante von L'_h noch eine Primzahl q mit der Kongruenzeigenschaft $q \equiv 1$ nach l^h enthalten ist. In diesem Falle wenden wir das nämliche Verfahren auf den Körper L'_h an und gelangen so zu einem zyklischen Körper L''_h vom $l^{h''}$-ten Grade, welcher folgende Eigenschaften besitzt: der aus L''_h und einem gewissen zyklischen Kreiskörper Q_h zusammengesetzte Körper enthält L'_h als Unterkörper, und die Diskriminante des Körpers L''_h enthält nur solche Primzahlen, welche in der Diskriminante des Körpers L_h aufgehen und von p und q verschieden sind. Die wiederholte Anwendung des Verfahrens führt schließlich auf einen Körper M_h von der im Satze verlangten Beschaffenheit.

Satz 4. Wenn L_h ein zyklischer Körper ist, dessen Grad l^h die Potenz einer beliebigen geraden oder ungeraden Primzahl l ist und wenn L_1 den Unterkörper l-ten Grades von L_h bezeichnet, so besitzen sämtliche von l verschiedenen Primteiler p der Diskriminante von L_1 die Kongruenzeigenschaft $p \equiv 1$ nach l^h.

Beweis. Zunächst betrachten wir den Fall, daß l eine ungerade Primzahl und $h = 1$ ist. Es sei dann im Gegensatz zu unserer Behauptung p eine rationale in der Diskriminante von L_1 aufgehende Primzahl, welche $\not\equiv 1$ nach l ist. Ferner bezeichne $k(\vartheta)$ den durch $\vartheta = e^{\frac{2i\pi}{l}}$ bestimmten Körper, und es sei in $t = (\vartheta : \vartheta^r)$ r eine Primitivzahl nach l. Ist $\mathfrak{p}$ ein idealer Primfaktor von p in $k(\vartheta)$, so ist das Primideal $\mathfrak{p}$ wegen $p \not\equiv 1$ nach l, wie die Theorie des Kreiskörpers $k(\vartheta)$ lehrt, zugleich ein Primideal in einem Unterkörper von $k(\vartheta)$, und es gibt mithin eine Potenz t^m der Substitution t, deren Exponent $m < l-1$ ist und für welche dennoch $t^m\mathfrak{p} = \mathfrak{p}$ oder $\mathfrak{p}^{t^m-1} = 1$ wird. Desgleichen gelten auch für die zu $\mathfrak{p}$ konjugierten Primideale $\mathfrak{p}', \mathfrak{p}'', \ldots$ die entsprechenden Gleichungen $\mathfrak{p}'^{t^m-1} = 1, \mathfrak{p}''^{t^m-1} = 1, \ldots$. Nach Satz 1 gibt es eine ganze Zahl $\varkappa$ in $k(\vartheta)$, so daß die beiden Zahlen ϑ und $\sqrt[l]{\varkappa}$ den aus $k(\vartheta)$ und L_1 zusammengesetzten Körper $k(\vartheta, L_1)$ bestimmen und für welche obenein $\varkappa^{t-r}$ gleich der l-ten Potenz einer Zahl in $k(\vartheta)$ wird. Da $t-r$ und t^m-1 zwei ganze ganzzahlige Funktionen von t sind, welche im Sinne der Kongruenz nach l keinen gemeinsamen Faktor haben, so gibt es 3 ganze ganzzahlige Funktionen $\varphi(t)$, $\psi(t)$, $\chi(t)$ der Veränderlichen t, so daß

$$1 = (t^m - 1)\varphi(t) + (t - r)\psi(t) + l\chi(t)$$

ist und hieraus folgt

$$\varkappa = \varkappa^{(t^m-1)\varphi(t)+(t-r)\psi(t)+l\chi(t)} = \varkappa^{(t^m-1)\varphi(t)}\alpha^l,$$

wo α eine Zahl in $k(\vartheta)$ ist. Wegen der vorhin bewiesenen Gleichung für die Primideale $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ ist $\varkappa^{t^m-1}$ eine ganze oder gebrochene Zahl, deren

Zähler und Nenner keinen der Primfaktoren $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ enthalten und daher zu p prim sind; das gleiche gilt somit von der Zahl $\varkappa^{(t^m-1)\varphi(t)}$. Wir setzen $\varkappa^{(t^m-1)\varphi(t)} = \frac{\varrho}{a^l}$, wo ϱ eine ganze algebraische zu p prime Zahl und a eine ganze rationale Zahl bedeutet. Der Körper $k(\vartheta, L_1)$ wird mithin auch durch die beiden Zahlen ϑ und $\sqrt[l]{\varrho}$ bestimmt. Die Partialdiskriminante der Zahl $\sqrt[l]{\varrho}$ ist in bezug auf $k(\vartheta) = \pm l^l \varrho^{l-1}$, und da ϱ zu p prim ist, so ist mithin die Partialdiskriminante von $k(\vartheta, L_1)$ in bezug auf $k(\vartheta)$ prim zu p. Da andrerseits die Diskriminante von $k(\vartheta)$ nicht durch p teilbar ist, so ist auch die Diskriminante von $k(\vartheta, L_1)$ und folglich auch die Diskriminante des Körpers L_1 prim zu p, was unserer Annahme widerspricht.

In ähnlicher Weise schließen wir die Richtigkeit unseres Satzes bei ungeradem l, wenn der Exponent h beliebig angenommen wird. Wir setzen unter Beibehaltung der in Satz 1 angewandten Bezeichnungsweise $\Theta = e^{\frac{2i\pi}{l^h}}$ und $t = (\Theta : \Theta^r)$, wo r eine Primitivzahl nach l^h bedeuten möge. Es sei $\mathfrak{p}$ ein idealer Primfaktor der in der Diskriminante von L_1 aufgehenden Primzahl p in $k(\Theta)$. Nehmen wir $p \not\equiv 1$ nach l^h an, so liegt, wie die Theorie des Kreiskörpers $k(\Theta)$ lehrt, das Primideal $\mathfrak{p}$ jedenfalls auch in dem Unterkörper $k(\Theta^l)$, d. h. es ist $\mathfrak{p}^{l^{h-2}(l-1)} = \mathfrak{p}$ und ebenso gelten für die zu $\mathfrak{p}$ in $k(\Theta)$ konjugierten Primideale $\mathfrak{p}', \ldots$ die Gleichungen $\mathfrak{p}'^{l^{h-2}(l-1)-1} = 1, \ldots$. Da r Primitivzahl nach l^h ist, so wird $r^{l^{h-2}(l-1)} \not\equiv 1$ nach l^h und mithin lassen sich 3 ganze ganzzahlige Funktionen $\varphi(t)$, $\psi(t)$, $\chi(t)$ der Variablen t derart bestimmen, daß

$$l^{h-1} = (t^{l^{h-2}(l-1)} - 1)\varphi(t) + (t - r)\psi(t) + l^h\chi(t)$$

ist; hieraus folgt insbesondere, wenn $\varkappa$ die in Satz 1 bestimmte Zahl bedeutet

$$\varkappa^{l^{h-1}} = \varkappa^{(t^{l^{h-2}(l-1)}-1)\varphi(t)}\alpha^{l^h},$$

wo α eine Zahl in $k(\Theta)$ bedeutet. Wegen der vorhin bewiesenen Eigenschaft der Primideale $\mathfrak{p}, \mathfrak{p}', \ldots$ ist $\varkappa^{l^{h-2}(l-1)-1}$ und folglich auch $\varkappa^{(t^{l^{h-2}(l-1)}-1)\varphi(t)}$ eine Zahl, deren Zähler und Nenner zu p prim ausfallen. Wir können daher die letztere Zahl $= \frac{\varrho}{a^{l^h}}$ setzen, wo ϱ eine ganze algebraische zu p prime Zahl und a eine ganze rationale Zahl bedeutet. Es ist folglich $\sqrt[l]{\varkappa} = \frac{\alpha}{a}\sqrt[l^h]{\varrho}$, und daraus ergibt sich $\varrho = \sigma^{l^{h-1}}$, wo σ ebenfalls in $k(\Theta)$ liegt. Da der durch Θ und $\sqrt[l]{\varkappa}$ bestimmte Körper mit demjenigen Körper identisch ist, welcher durch Zusammensetzung aus $k(\Theta)$ und L_1 entsteht, und da die Partialdiskriminante der Zahl $\sqrt[l]{\sigma}$ in bezug auf $k(\Theta)$ den zu p primen Wert $\pm l^l \sigma^{l-1}$ besitzt, so ist die Partialdiskriminante des Körpers $k(\Theta, L_1)$ in bezug auf $k(\Theta)$ prim zu p. Andererseits ist die Diskriminante von $k(\Theta)$ ebenfalls nicht durch p teilbar, und folglich gilt das gleiche auch von den Diskriminanten des Kör-

pers $k(\Theta, L_1)$ und des Körpers L_1. Der letztere Umstand widerspricht unserer Annahme.

Um die Richtigkeit des Satzes 4 für $l=2$ zu erkennen, machen wir zunächst die Annahme $h=2$ und wenden dann auf den zyklischen Körper L_2 vom 4-ten Grade den Satz 1 an. Gemäß der dort gebrauchten Bezeichnungsweise setzen wir $\Theta = e^{\frac{i\pi}{2}} = i$ und wählen $r=3$. Dann ist $t=(i:-i)$. Es sei L_1 der quadratische Unterkörper von L_2 und p eine in der Diskriminante von L_1 aufgehende Primzahl, welche $\not\equiv 1$ nach 4 ist. Infolgedessen ist p in $k(i)$ unzerlegbar. Ist nun die durch Satz 1 in unserem Falle bestimmte Zahl $\varkappa$ durch p teilbar, so bilde man die Zahl $\varrho = \varkappa^{t-1}$. Da nach Satz 1 andererseits $\varkappa^{t-3} = \alpha^4$ sein soll, wo α in $k(i)$ liegt, so folgt $\varkappa^2 = \varrho\alpha^{-4}$, d. h. $\sqrt{\varkappa} = \alpha^{-1}\sqrt[4]{\varrho}$. Infolgedessen ist ϱ das Quadrat einer Zahl in $k(i)$; wir setzen $\varrho = \frac{\tau^2}{a^4}$, wo τ eine ganze algebraische zu p prime Zahl und a eine ganze rationale Zahl bedeutet. Da der Körper $k(i, L_1)$ mit dem Körper $k(i, \sqrt{\tau})$ übereinstimmt und da andererseits die Partialdiskriminante der Zahl $\sqrt{\tau}$ in bezug auf $k(i)$ zu p prim ist, so ist auch die Partialdiskriminante des Körpers $k(i, L_1)$ in bezug auf $k(i)$ prim zu p, und hieraus folgt, wie vorhin, daß die Diskriminante von L_1 nicht durch p teilbar sein kann.

Ist im Falle $l=2$ der Exponent $h>2$, so setzen wir $\Theta = e^{\frac{i\pi}{2^{h-1}}}$. Wäre dann die in der Diskriminante von L_1 aufgehende Primzahl $p \equiv 1$ nach 4 und $\not\equiv 1$ nach 2^h und ist $\mathfrak{p}$ ein idealer Primfaktor von p in $k(\Theta)$, so bleibt $\mathfrak{p}$ ungeändert bei der Substitution $t^{2^{h-2}}$, wo t entweder $=(\Theta:\Theta^5)$ oder $=(\Theta:\Theta^{-5})$ ist; folglich wird $\mathfrak{p}^{t^{2^{h-2}}-1} = 1$. Wegen $5^{2^{h-2}} \not\equiv 1$ nach 2^h gilt eine Gleichung von der Gestalt

$$2^{h-1} = (t^{2^{h-2}} - 1)\varphi(t) + (t-5)\psi(t) + 2^h\chi(t)$$

und aus dieser schließen wir, wie vorhin bei ungeradem l, auf einen Widerspruch mit der Annahme, wonach p in der Diskriminante von L_1 aufgeht.

Satz 5. Wenn die Diskriminante eines zyklischen Körpers L_1 von dem ungeraden Primzahlgrade u gleich einer positiven Potenz von u ist, so stimmt der Körper L_1 mit dem Körper U_1 überein. Wenn ferner ein zyklischer Körper L_h, dessen Grad u^h eine höhere als die erste Potenz der ungeraden Primzahl u ist, den Kreiskörper U_{h-1} als Unterkörper enthält, so stimmt der Körper L_h mit dem Körper U_h überein.

Beweis. Wir benutzen die in Satz 2 erklärte Bezeichnungsweise und setzen überdies $\lambda = 1 - \Theta$; es ist dann $\mathfrak{l} = (\lambda)$ ein Primideal in $k(\Theta)$ und es wird im Sinne der Idealtheorie

$$(1-\vartheta) = \mathfrak{l}^{u^{h-1}}, \quad (u) = (1-\vartheta)^{u-1} = \mathfrak{l}^{u^{h-1}(u-1)};$$

endlich gilt die Kongruenz

$$t\lambda = 1 - \Theta^r \equiv r\lambda, \qquad (\mathfrak{l}^2).$$

Wir betrachten nun die in Satz 2 konstruierte Zahl $\varkappa$. Da das Primideal $\mathfrak{l}$ in $k(\Theta)$ vom ersten Grade ist, so folgt, wenn $\varrho = \varkappa^{(t-1)(u-1)}$ gesetzt wird, für diese Zahl die Kongruenz $\varrho \equiv 1$ nach $\mathfrak{l}$. Wir setzen $\varrho \equiv 1 + a\lambda$ nach $\mathfrak{l}^2$, wo a eine ganze rationale Zahl bedeutet; dann ist $\sigma = \varrho\Theta^n \equiv 1$ nach $\mathfrak{l}^2$. Nunmehr führen wir den Nachweis dafür, daß im Körper $k(\Theta)$ eine Zahl α gefunden werden kann, so daß die Kongruenz $\sigma\alpha^u \equiv 1$ nach $(1-\vartheta)^u$ besteht. Zu dem Zwecke nehmen wir an, es sei e der größte Exponent von der Beschaffenheit, daß bei geeigneter Wahl der in $k(\Theta)$ liegenden Zahl α die Kongruenz $\sigma\alpha^u \equiv 1$ nach $\mathfrak{l}^e$ stattfindet und es sei unserer Behauptung entgegen $\mathfrak{l}^e$ nicht durch $(1-\vartheta)^u$ teilbar, d. h. es sei $e < u^h$; wir setzen demgemäß $\sigma\alpha^u \equiv 1 + a\lambda^e$ nach $\mathfrak{l}^{e+1}$, wo a eine nicht durch u teilbare ganze rationale Zahl bedeutet, und unterscheiden 2 Fälle, je nachdem e durch u teilbar ist oder nicht. Im ersten Falle gilt die Kongruenz

$$1 + a\lambda^e = \left(1 + a\lambda^{\frac{e}{u}}\right)^u, \qquad (\mathfrak{l}^{e+1})$$

und mithin ist

$$\sigma\left\{\alpha\left(1 + a\lambda^{\frac{e}{u}}\right)^{-1}\right\}^u \equiv 1, \qquad (\mathfrak{l}^{e+1}).$$

Diese Kongruenz widerstreitet der Annahme, wonach e der größte Exponent dieser Art sein sollte. Im zweiten Falle berücksichtigen wir, daß nach Satz 2 $\varkappa^{t-r}$ und folglich auch σ^{t-r} die u-te Potenz einer Zahl in $k(\Theta)$ ist; wir setzen etwa $(\sigma\alpha^u)^{t-r} = \beta^u$, wo β eine Zahl des Körpers $k(\Theta)$ ist. Dieser Umstand liefert die Kongruenz $1 + a(r\lambda)^e - ar\lambda^e \equiv \beta^u$ nach $\mathfrak{l}^{e+1}$. Da $e < u^h$ und nicht durch u teilbar ist, so würde hieraus $ar^e \equiv ar$ nach $\mathfrak{l}$ folgen, was ebenfalls unmöglich ist, da r Primitivzahl nach u sein soll. Diese Betrachtung lehrt also $e \geqq u^h$, womit unsere Behauptung bewiesen ist.

Wir setzen nun $\sigma\alpha^u = \frac{\tau}{a^{u(u-1)}}$, wo τ eine ganze algebraischeZahl mit der Kongruenzeigenschaft $\tau \equiv 1$ nach $(1-\vartheta)^u$ ist und a eine ganze rationale Zahl bedeutet. Nehmen wir dann an, der Körper L_h sei von dem Körper U_h verschieden, so wäre der aus $k(\Theta)$, U_h und L_h zusammengesetzte Körper $k(\sqrt[u]{\Theta}, \sqrt[u]{\tau})$ vom Grade $u^{h+1}(u-1)$. Es ist andererseits $\frac{1-\sqrt[u]{\tau}}{1-\vartheta}$ gleich einer ganzen Zahl des Körpers $k(\sqrt[u]{\Theta}, \sqrt[u]{\tau})$ und die Partialdiskriminante dieser Zahl in bezug auf $k(\sqrt[u]{\Theta})$ ist gleich $\varepsilon\tau^{u-1}$, wo ε eine Einheit ist. Da τ zu u prim ist, so ist mithin die Partialdiskriminante des Körpers $k(\sqrt[u]{\Theta}, \sqrt[u]{\tau})$ in bezug auf den Körper $k(\sqrt[u]{\Theta})$ ebenfalls prim zu u. Bezeichnen wir daher mit $\mathfrak{L}$ einen idealen Primfaktor von $\mathfrak{l}$ im Körper $k(\sqrt[u]{\Theta}, \sqrt[u]{\tau})$, so besitzt $\mathfrak{L}$ in diesem Körper einen Trägheitskörper T, welcher mindestens den Grad u hat. Die Diskriminante dieses Trägheitskörpers T ist prim zu u.

Nehmen wir zunächst $h=1$, so wäre der genannte Trägheitskörper $T=L_1$; dies ist nicht möglich, weil nach Voraussetzung die Diskriminante des Körpers L_1 eine positive Potenz von u ist. Der Beweis für den ersten Teil unseres Satzes ist hierdurch erbracht. Nehmen wir $h>1$ an, so müßte jener Trägheitskörper T des Ideals $\mathfrak{L}$ entweder $=U_1$ sein oder den Körper U_1 als Unterkörper enthalten. Beides ist nicht möglich, da die Diskriminante von U_1 eine Potenz von u ist und dieser Widerspruch lehrt die Richtigkeit des zweiten Teiles unseres Satzes 5.

Satz 6. Wenn ein reeller zyklischer Körper L_h vom Grade 2^h den Körper Z_{h-1} als Unterkörper enthält, so stimmt L_h mit Z_h überein.

Beweis. Der Körper Z_{h-1} wird durch die Zahl

$$\lambda = e^{\frac{i\pi}{2^h}} + e^{-\frac{i\pi}{2^h}}$$

und der Körper Z_h durch die Zahl

$$\mu = e^{\frac{i\pi}{2^{h+1}}} + e^{-\frac{i\pi}{2^{h+1}}}$$

bestimmt. Es ist $\mu^2=\lambda+2$, d. h. $\mu=\sqrt{\lambda+2}$. Im Sinne der Idealtheorie gilt ferner die Gleichung $(2)=\mathfrak{l}^{2^{h-1}}$, wo $\mathfrak{l}=(\lambda)$ ein Primideal in Z_{h-1} bedeutet. Der Körper L_h ist jedenfalls durch die Zahl λ und eine Zahl von der Form $\sqrt{\varkappa}$ bestimmt, wo $\varkappa$ eine ganze Zahl in Z_{h-1} bedeutet. Wäre nun der Körper L_h von Z_h verschieden und nehmen wir an, es sei $\varkappa$ durch $\mathfrak{l}^m$, aber nicht durch $\mathfrak{l}^{m+1}$ teilbar, so setze man $\varrho=\frac{\varkappa(\lambda+2)^m}{\lambda^{2m}}$; die beiden Zahlen λ und $\sqrt{\varrho}=\frac{\mu^m}{\lambda^m}\sqrt{\varkappa}$ definieren dann wiederum einen reellen zyklischen Körper L_h' vom 2^h-ten Grade und ϱ bedeutet eine ganze, nicht durch $\mathfrak{l}$ teilbare Zahl. Wir wollen zeigen, daß dieses unmöglich ist.

Zu dem Zwecke setzen wir $\Theta=e^{\frac{i\pi}{2^h}}$ und $t=(\Theta:\Theta^5)$. Da die Zahl $\sqrt{t\varrho}$ mit der Zahl λ zusammen ebenfalls den Körper L_h' definieren muß, so folgt $\sqrt{t\varrho}=\alpha\sqrt{\varrho}$, wo α in Z_{h-1} liegt, d. h. es ist $\varrho\cdot t\varrho$ das Quadrat einer Zahl in Z_{h-1}. Nunmehr führen wir den Nachweis dafür, daß im Körper Z_{h-1} eine Zahl α gefunden werden kann, welche der Kongruenz $\varrho\alpha^2\equiv 1$ nach $\mathfrak{l}^{2^{h-1}}$ genügt. Zu dem Zwecke nehmen wir an, es sei e der größte Exponent von der Beschaffenheit, daß bei geeigneter Wahl der in Z_{h-1} liegenden Zahl α die Kongruenz $\varrho\alpha^2\equiv 1$ nach $\mathfrak{l}^e$ stattfindet und es sei im Gegensatz zu unserer Behauptung $e<2^h-1$; wir setzen demgemäß $\varrho\alpha^2\equiv 1+\lambda^e$ nach $\mathfrak{l}^{e+1}$ und unterscheiden dann 2 Fälle, je nachdem e gerade oder ungerade ausfällt. Im ersteren Falle berücksichtigen wir die Kongruenz $\varrho\alpha^2\left(1+\lambda^{\frac{e}{2}}\right)^2\equiv 1$ nach $\mathfrak{l}^{e+1}$; dieselbe würde zeigen, daß e nicht der höchste Exponent von der verlangten Art wäre. Im zweiten Falle setzen wir $\varrho\alpha^2\equiv 1+\lambda^e+a\lambda^{e+1}$ nach $\mathfrak{l}^{e+2}$, wo a den Wert

0 oder 1 hat. Ist $a=1$, so berücksichtigen wir, daß für $e<2^h-1$ die Kongruenz $1+\lambda^{e+1}\equiv\left(1+\lambda^{\frac{e+1}{2}}\right)^2$ nach $\mathfrak{l}^{e+2}$ gilt. Setzen wir daher $\sigma=\varrho\alpha^2\left(1+\lambda^{\frac{e+1}{2}}\right)^{2a}$, so wird $\sigma\equiv 1+\lambda^e+b\lambda^{e+2}$ nach $\mathfrak{l}^{e+3}$, wo b den Wert 0 oder 1 hat. Wegen $t\lambda\equiv\lambda+\lambda^3$ nach $\mathfrak{l}^4$ folgt:

$$t\sigma\equiv 1+(\lambda+\lambda^3)^e+b\lambda^{e+2}\equiv 1+\lambda^e+(b+1)\lambda^{e+2}, \qquad (\mathfrak{l}^{e+3})$$

d. h. für $e=1$, bezüglich für $e\geqq 3$:

$$\sigma\cdot t\sigma\equiv(1+\lambda)(1+\lambda+\lambda^3)\equiv 1+\lambda^2+\lambda^3, \qquad (\mathfrak{l}^4)$$
$$\sigma\cdot t\sigma\equiv(1+\lambda^e)(1+\lambda^e+\lambda^{e+2})\equiv 1+\lambda^{e+2}, \qquad (\mathfrak{l}^{e+3}).$$

Die rechte Seite der ersteren Kongruenz kann nicht $\equiv\alpha^2$ nach $\mathfrak{l}^4$ sein; soll die rechte Seite der zweiten Kongruenz $\equiv\alpha^2$ nach $\mathfrak{l}^{e+3}$ sein, so muß $e+2\geqq 2^h+1$ werden, da 2^h+1, wie leicht ersichtlich, der kleinste unter allen ungeraden Exponenten f ist derart, daß $1+\lambda^f\equiv\alpha^2$ nach $\mathfrak{l}^{f+1}$ werden kann. Wegen $e\geqq 2^h-1$ ist unsere obige Behauptung bewiesen.

Wir setzen $\sigma=\varrho\alpha^2\equiv 1+a\lambda^{2^h-1}$ nach $\mathfrak{l}^{2^h}$, wo a den Wert 0 oder 1 hat. Es genügt folglich, wenn $\tau=(-1)^a\sigma$ gesetzt wird, die Zahl τ, gegebenenfalls nach Multiplikation mit dem Quadrat einer geeigneten Zahl aus Z_{h-1}, der Kongruenz $\tau\equiv 1$ nach 4. Die Zahlen λ und $\sqrt{\tau}$ definieren stets einen zyklischen Körper L_h'' vom Grade 2^h. Denn im Falle $a=0$ stimmt $L_h''=k(\lambda,\sqrt{\tau})$ mit L_h' überein und im Falle $a=1$ enthält der Körper L_h'', da er imaginär ist, sicher noch andere Zahlen, als in Z_{h-1} vorhanden sind. Da $\frac{1-\sqrt{\tau}}{2}$ eine ganze Zahl ist, deren Partialdiskriminante in bezug auf Z_{h-1} zu 2 prim ausfällt, so ist die Partialdiskriminante des Körpers L_h'' in bezug auf Z_{h-1} prim zu 2. Es ist daher die Zahl 2 im Körper L_h'' nicht gleich der 2^h-ten Potenz eines Primideals. Bezeichnet $\mathfrak{L}$ ein in $\mathfrak{l}$ enthaltenes Primideal des Körpers L_h'', so muß der Trägheitskörper von $\mathfrak{L}$ in L_h'' den zweiten Grad besitzen; dieser Trägheitskörper müßte daher gleich Z_1 sein, was nicht möglich ist, da die Diskriminante von Z_1 eine Potenz von 2 ist. Damit ist unsere ursprüngliche Annahme widerlegt, d. h. es ist bewiesen, daß die beiden Körper L_h und Z_h miteinander identisch sind.

Wir beweisen nunmehr den Kroneckerschen Fundamentalsatz in folgender Art. Zunächst ist leicht aus der Theorie der Abelschen Gruppen ersichtlich, daß ein jeder Abelsche Körper sich aus zyklischen Körpern L_h zusammensetzen läßt, deren Grade die Potenzen l^h einer Primzahl l sind; es ist daher nur nötig, zu zeigen, daß ein jeder solcher zyklische Körper L_h ein Kreiskörper ist. Infolge des Satzes 3 wird dieser Nachweis auf den Fall zurückgeführt, in welchem die Diskriminante des vorgelegten zyklischen Körpers L_h keine Primzahlen p mit der Kongruenzeigenschaft $p\equiv 1$ nach l^h enthält. Ist L_h ein zyklischer Körper dieser Art, so besitzt die Diskriminante des in L_h

enthaltenen Unterkörpers L_1 vom l-ten Grade ebenfalls keine Primteiler p mit der Kongruenzeigenschaft $p \equiv 1$ nach l^h. Wenden wir nun den Satz 4 an und berücksichtigen, daß nach einem von MINKOWSKI[1] bewiesenen Satze jede Diskriminante Primzahlen als Faktoren enthalten muß, so folgt, daß die Diskriminante des Körpers L_1 notwendig eine positive Potenz von l ist.

Wir unterscheiden beim weiteren Beweise 2 Fälle, je nachdem $l = u$ eine ungerade Primzahl oder $l = 2$ ist. Im ersteren Falle ist nach Satz 5 der Körper $L_1 = U_1$. Bezeichnen wir ferner die in L_h enthaltenen Unterkörper l^2-ten, l^3-ten, ..., l^{h-1}-ten Grades bezüglich mit $L_2, L_3, \ldots, L_{h-1}$, so schließen wir aus eben demselben Satze 5 der Reihe nach $L_2 = U_2$, $L_3 = U_3, \ldots, L_h = U_h$ und folglich ist L_h ein Kreiskörper. Im zweiten Falle bilden wir zunächst den aus dem imaginären quadratischen Körper $k(i)$ und aus L_h zusammengesetzten Körper $M_{h'} = k(i, L_h)$; derselbe ist vom 2^h-ten oder 2^{h+1}-ten Grade, je nachdem L_h imaginär oder reell ausfällt. Der größte reelle Unterkörper dieses Körpers $M_{h'}$ ist vom $2^{h'}$-ten Grade, wo $h' = h - 1$ oder gleich h ist; derselbe ist notwendig ein zyklischer Körper. Der in $M_{h'}$ enthaltene quadratische Unterkörper M_1 ist ebenfalls reell und stimmt, da seine Diskriminante eine Potenz von 2 ist, mit $Z_1 = k(\sqrt{2})$ überein. Bezeichnen wir nun die in M_h enthaltenen Unterkörper 2^2-ten, 2^3-ten, ... Grades bezüglich mit $M_2, M_3, \ldots$, so folgt nach Satz 6 der Reihe nach $M_2 = Z_2$, $M_3 = Z_3, \ldots, M_{h'} = Z_{h'}$ und folglich ist $M_{h'}$ ebenfalls ein Kreiskörper. Damit ist der Fundamentalsatz vollständig bewiesen und zugleich ist ersichtlich, in welcher Weise man alle Abelschen Körper von gegebener Gruppe und Diskriminante aufstellen kann.

Göttingen, den 25. Januar 1896.

[1] J. Math. 107, 295 (1891).

7. Die Theorie der algebraischen Zahlkörper.

[Jahresbericht der Deutschen Mathematiker-Vereinigung Bd. 4, S. 175—546 (1897).]

Vorwort.

Die Zahlentheorie gehört zu den ältesten Zweigen mathematischen Wissens, und es wurde der menschliche Geist sogar auf tief liegende Eigenschaften der natürlichen Zahlen frühzeitig aufmerksam. Doch als selbständige und systematische Wissenschaft ist sie durchaus ein Werk der neueren Zeit.

An der Zahlentheorie werden von jeher die Einfachheit ihrer Grundlagen, die Genauigkeit ihrer Begriffe und die Reinheit ihrer Wahrheiten gerühmt; ihr kommen diese Eigenschaften von Hause aus zu, während andere mathematische Wissenszweige erst eine mehr oder minder lange Entwicklung haben durchmachen müssen, bis die Forderungen der Sicherheit in den Begriffen und der Strenge in den Beweisen überall erfüllt worden sind.

Es nimmt uns daher die hohe Begeisterung nicht wunder, von der zu allen Zeiten die Jünger dieser Wissenschaft beseelt gewesen sind. „Fast alle Mathematiker, die sich mit der Zahlentheorie beschäftigen“, so sagt LEGENDRE, indem er EULERS Liebe zur Zahlentheorie schildert, „geben sich ihr mit einer gewissen Leidenschaft hin“. Weiter erinnern wir uns, welche Verehrung unser Meister GAUSS für die arithmetische Wissenschaft empfand, wie, als ihm zuerst der Beweis einer ausgezeichneten arithmetischen Wahrheit nach Wunsch gelungen war, „ihn die Reize dieser Untersuchungen so umstrickten, daß er sie nicht mehr lassen konnte“, und wie er FERMAT, EULER, LAGRANGE und LEGENDRE als „Männer von unvergleichlichem Ruhme“ preist, weil sie „den Zugang zu dem Heiligtume dieser göttlichen Wissenschaft erschlossen und gezeigt haben, von wie großen Reichtümern es erfüllt ist“.

Eine besondere Eigentümlichkeit der Zahlentheorie bildet die oft entgegentretende Schwierigkeit der Beweise einfacher und durch Induktion leicht entdeckter Wahrheiten. „Gerade dieses ist es“, sagt GAUSS, „was der höheren Arithmetik jenen zauberischen Reiz gibt, der sie zur Lieblingswissenschaft der ersten Geometer gemacht hat, ihres unerschöpflichen Reichtums nicht zu gedenken, woran sie alle anderen Teile der Mathematik so weit übertrifft.“

Bekannt ist auch LEJEUNE DIRICHLETS Vorliebe für die Arithmetik; KUMMERS wissenschaftliche Tätigkeit war weitaus in erster Linie der Zahlentheorie geweiht, und KRONECKER gab dem Empfinden seines mathematischen Herzens Ausdruck durch die Worte: „Die ganze Zahl schuf der liebe Gott, alles übrige ist Menschenwerk."

In Anbetracht der Schlichtheit ihrer Voraussetzungen ist sicher die Zahlentheorie *der* Wissenszweig der Mathematik, dessen Wahrheiten am leichtesten zu begreifen sind. Aber die arithmetischen Begriffe und Beweismethoden erfordern zu ihrer Auffassung und völligen Beherrschung einen hohen Grad von Abstraktionsfähigkeit des Verstandes, und dieser Umstand wird bisweilen als ein Vorwurf gegen die Arithmetik geltend gemacht. Ich bin der Meinung, daß alle die anderen Wissensgebiete der Mathematik wenigstens einen gleich hohen Grad von Abstraktionsfähigkeit des Verstandes verlangen — vorausgesetzt, daß man auch in diesen Gebieten die Grundlagen überall mit derjenigen Strenge und Vollständigkeit zur Untersuchung zieht, welche tatsächlich notwendig ist.

Was die *Stellung der Zahlentheorie* innerhalb der gesamten mathematischen Wissenschaft betrifft, so faßt GAUSS in der Vorrede zu den Disquisitiones arithmeticae die Zahlentheorie noch lediglich als eine Theorie der ganzen natürlichen Zahlen auf mit ausdrücklicher Ausschließung aller imaginären Zahlen. Dementsprechend rechnet er die Kreisteilung an und für sich nicht zur Zahlentheorie, fügt aber hinzu, daß „ihre Prinzipien einzig und allein aus der höheren Arithmetik geschöpft werden". Neben GAUSS geben auch JACOBI und LEJEUNE DIRICHLET wiederholt und nachdrücklich ihrer Verwunderung Ausdruck über den engen Zusammenhang zahlentheoretischer Fragen mit algebraischen Problemen, insbesondere mit dem Problem der Kreisteilung. Der innere Grund für diesen Zusammenhang ist heute völlig aufgedeckt. Die Theorie der algebraischen Zahlen und die Galoissche Gleichungstheorie haben nämlich in der allgemeinen *Theorie der algebraischen Körper* ihre gemeinsame Wurzel, und die Theorie der Zahlkörper insbesondere ist zugleich der wesentlichste Bestandteil der modernen Zahlentheorie geworden.

Das Verdienst, den ersten Keim für die Theorie der Zahlkörper gelegt zu haben, gebührt wiederum GAUSS. GAUSS erkannte die natürliche Quelle für die Gesetze der biquadratischen Reste in einer „Erweiterung des Feldes der Arithmetik", wie er sagt, nämlich in der Einführung der ganzen imaginären Zahlen von der Form $a + bi$; er stellte und löste das Problem, alle Sätze der gewöhnlichen Zahlentheorie, vor allem die Teilbarkeitseigenschaften und die Kongruenzbeziehungen, auf jene ganzen imaginären Zahlen zu übertragen. Durch die systematische und allgemeine Fortentwickelung dieses Gedankens, auf Grund der neuen weittragenden Ideen KUMMERS, gelangten später DEDEKIND und KRONECKER zu der heutigen Theorie des *algebraischen Zahlkörpers*.

Aber nicht nur mit der Algebra, sondern auch mit der *Funktionentheorie* steht die Zahlentheorie in innigster wechselseitiger Beziehung. Wir erinnern an die zahlreichen und merkwürdigen Analogien, welche zwischen gewissen Tatsachen aus der Theorie der Zahlkörper und aus der Theorie der algebraischen Funktionen einer Veränderlichen bestehen, ferner an die tiefsinnigen Untersuchungen von RIEMANN, durch welche die Beantwortung der Frage nach der Häufigkeit der Primzahlen von der Kenntnis der Nullstellen einer gewissen analytischen Funktion abhängig gemacht wird. Auch die Transzendenz der Zahlen e und π ist eine arithmetische Eigenschaft einer analytischen Funktion, nämlich der Exponentialfunktion. Endlich ruht die so wichtige und weittragende, von LEJEUNE DIRICHLET ersonnene Methode zur Bestimmung der Klassenanzahl eines Zahlkörpers auf analytischer Grundlage.

Am tiefsten aber berühren die periodischen Funktionen und gewisse Funktionen mit linearen Transformationen in sich das Wesen der Zahl: so ist die Exponentialfunktion $e^{2i\pi z}$ als die *Invariante* der ganzen rationalen Zahl aufzufassen, insofern sie die Grundlösung der Funktionalgleichung $f(z+1) = f(z)$ darstellt. Ferner hatte schon JACOBI den engen Zusammenhang zwischen der Theorie der elliptischen Funktionen und der Theorie der quadratischen Irrationalitäten empfunden; er gibt sogar der Vermutung Raum, daß bei GAUSS der oben erwähnte Gedanke der Einführung der ganzen imaginären Zahlen von der Form $a + bi$ nicht auf rein arithmetischem Boden erwachsen ist, sondern durch GAUSS' gleichzeitige Untersuchungen über die lemniskatischen Funktionen und deren komplexe Multiplikation mitbedingt wurde. Es sind die elliptische Funktion für geeignete Werte ihrer Perioden und die elliptische Modulfunktion jedesmal die *Invariante* der ganzen Zahl eines bestimmten imaginären quadratischen Zahlkörpers. Diese als *Invarianten* bezeichneten Funktionen vermögen für die bezüglichen Zahlkörper gewisse tiefliegende und schwierige Probleme zur Lösung zu bringen, und umgekehrt verdankt die Theorie der elliptischen Funktionen dieser arithmetischen Auffassung und Anwendung einen neuen Aufschwung.

So sehen wir, wie die Arithmetik, die „Königin" der mathematischen Wissenschaft, weite algebraische und funktionentheoretische Gebiete erobert und in ihnen die Führerrolle übernimmt. Daß dies aber nicht früher und nicht bereits in noch höherem Maße geschehen ist, scheint mir daran zu liegen, daß die Zahlentheorie erst in neuester Zeit in ihr reiferes Alter getreten ist. Sogar noch GAUSS klagt über die unverhältnismäßig großen Anstrengungen, die ihn die Bestimmung eines Wurzelzeichens in der Zahlentheorie gekostet: es habe ihn „manches andere wohl nicht so viel Tage aufgehalten, als dieses Jahre", und dann auf einmal, „wie der Blitz einschlägt", habe sich „das Rätsel gelöset". An Stelle eines solchen für das früheste Alter einer Wissenschaft charakteristischen, sprunghaften Fortschrittes ist heute durch den systema-

tischen Aufbau der Theorie der Zahlkörper eine sichere und stetige Entwickelung getreten.

Es kommt endlich hinzu, daß, wenn ich nicht irre, überhaupt die moderne Entwickelung der reinen Mathematik vornehmlich *unter dem Zeichen der Zahl* geschieht: DEDEKINDS und WEIERSTRASS' Definitionen der arithmetischen Grundbegriffe und CANTORS allgemeine Zahlgebilde führen zu einer *Arithmetisierung der Funktionentheorie* und dienen zur Durchführung des Prinzips, daß auch in der Funktionentheorie eine Tatsache erst dann als bewiesen gilt, wenn sie in letzter Instanz auf Beziehungen für ganze rationale Zahlen zurückgeführt worden ist. Die *Arithmetisierung der Geometrie* vollzieht sich durch die modernen Untersuchungen über Nicht-Euklidische Geometrie, in denen es sich um einen streng logischen Aufbau derselben und um die möglichst direkte und völlig einwandfreie Einführung der Zahl in die Geometrie handelt.

Der *Zweck des vorliegenden Berichtes* ist es, die Tatsachen aus der Theorie der algebraischen Zahlkörper mit ihren Beweisgründen in logischer Entwickelung und nach einheitlichen Gesichtspunkten darzustellen und so mitzuwirken, daß der Zeitpunkt näher komme, wo die Errungenschaften unserer großen Klassiker der Zahlentheorie Gemeingut aller Mathematiker geworden sind. Historische Erörterungen oder gar Prioritätsuntersuchungen sind ganz vermieden worden. Um die Darstellung auf einem verhältnismäßig so kleinen Raum zu ermöglichen, habe ich mich bemüht, überall den ergiebigsten Quellen nachzuspüren, und ich gab, wenn eine Auswahl sich bot, allemal den schärferen und weiter tragenden Hilfsmitteln den Vorzug. Die Frage, welcher von mehreren Beweisen der einfachste und naturgemäßeste ist, läßt sich meist nicht an sich entscheiden, sondern erst die Erwägung, ob die dabei zugrunde gelegten Prinzipien der Verallgemeinerung fähig und zur Weiterforschung brauchbar sind, gibt uns eine sichere Antwort.

Der *erste Teil des Berichtes* behandelt die allgemeine Theorie der algebraischen Zahlkörper; diese Theorie erscheint uns als ein mächtiger Bau, getragen von drei Grundpfeilern: dem Satze von der eindeutigen Zerlegung in Primideale, dem Satze von der Existenz der Einheiten und dem Satze von der transzendenten Bestimmung der Klassenanzahl. Der *zweite Teil* enthält die Theorie des Galoisschen Zahlkörpers, in der auch umgekehrt die Gesetze der allgemeinen Körpertheorie enthalten sind. Der *dritte Teil* ist dem klassischen Beispiel des quadratischen Körpers gewidmet. Der *vierte Teil* behandelt den Kreiskörper. Der *fünfte Teil* endlich entwickelt die Theorie desjenigen Körpers, den KUMMER bei seinen Untersuchungen über höhere Reziprozitätsgesetze zugrunde gelegt hat, und den ich deshalb nach diesem Mathematiker benannt habe. Es ist die Theorie dieses Kummerschen Körpers offenbar auf der Höhe des heutigen arithmetischen Wissens die äußerste erreichte Spitze, und man übersieht von ihr aus in weitem Rundblick das ganze durchforschte Gebiet,

da fast jeder wesentliche Gedanke und Begriff aus der Körpertheorie, zum wenigsten in spezieller Fassung, bei dem Beweise der höheren Reziprozitätsgesetze seine Anwendung findet. Ich habe versucht, den großen rechnerischen Apparat von KUMMER zu vermeiden, damit auch hier der Grundsatz von RIEMANN verwirklicht würde, demzufolge man die Beweise nicht durch Rechnung, sondern lediglich durch Gedanken zwingen soll.

Die im dritten, vierten und fünften Teile behandelten Theorien sind sämtlich Theorien besonderer Abelscher oder relativ-Abelscher Körper. Ein weiteres Beispiel für eine solche Theorie ist die komplexe Multiplikation der elliptischen Funktionen, indem wir diese als eine Theorie derjenigen Zahlkörper auffassen, welche in bezug auf einen gegebenen imaginären quadratischen Körper relativ-Abelsche sind. Die Untersuchungen über die komplexe Multiplikation der elliptischen Funktionen mußten jedoch von der Aufnahme in den vorliegenden Bericht ausgeschlossen werden, weil die Tatsachen dieser Theorie noch nicht bis zu dem Grade der Einfachheit und Vollständigkeit ausgearbeitet sind, daß eine befriedigende Darstellung derselben gegenwärtig möglich ist.

Die Theorie der Zahlkörper ist wie ein Bauwerk von wunderbarer Schönheit und Harmonie; als der am reichsten ausgestattete Teil dieses Bauwerkes erscheint mir die Theorie der Abelschen und relativ-Abelschen Körper, die uns KUMMER durch seine Arbeiten über die höheren Reziprozitätsgesetze und KRONECKER durch seine Untersuchungen über die komplexe Multiplikation der elliptischen Funktionen erschlossen haben. Die tiefen Einblicke, welche die Arbeiten dieser beiden Mathematiker in die genannte Theorie gewähren, zeigen uns zugleich, daß in diesem Wissensgebiete eine Fülle der kostbarsten Schätze noch verborgen liegt, winkend als reicher Lohn dem Forscher, der den Wert solcher Schätze kennt und die Kunst, sie zu gewinnen, mit Liebe betreibt.

Die erwähnten fünf Teile des Berichtes gliedern sich in *Kapitel* und *Paragraphen*, und in diesen schreitet die Entwickelung in der Weise fort, daß allemal die *Sätze* und *Hilfssätze* voranstehen und dann ihre *Beweise* folgen. Ich denke mir den Leser wie einen Reisenden: die Hilfssätze sind Haltestellen, die Sätze sind größere Stationen, im voraus bezeichnet, damit an ihnen das Auffassungsvermögen ausruhen kann. Diejenigen Sätze, die wegen ihrer prinzipiellen Bedeutung an sich Hauptziele sind, oder die als Ausgangspunkte zu weiterem Vordringen in noch unentdecktes Land hervorragend geeignet erscheinen, sind durch kursiven Druck ausgezeichnet; es sind dies die Sätze: 7 (S. 75), 31 (S. 85), 40 (S. 97), 44 (S. 100), 45 (S. 100), 47 (S. 102), 56 (S. 116), 82 (S. 142), 94 (S. 155), 100 (S. 168), 101 (S. 169), 131 (S. 206), 143 (S. 240), 144 (S. 242), 150 (S. 257), 158 (295), 159 (S. 302), 161 (S. 312), 164 (S. 329), 166 (S. 332), 167 (S. 332).

Wegen des genauen Inhaltes und der zur Erhöhung der Übersicht getroffenen Einrichtungen verweise ich auf die Verzeichnisse S. III – S. XII und

S. 356—S. 363; vor allem möchte ich hier auf das ganz an den Schluß gestellte Verzeichnis der im Berichte vorkommenden Begriffsnamen aufmerksam machen[1].

Mein Freund Hermann Minkowski hat die Korrekturbogen dieses Berichtes einer sorgfältigen Durchsicht unterworfen und auch den größten Teil des Manuskripts gelesen. Wesentliche und mannigfache Verbesserungen formaler und sachlicher Art erfolgten auf seine Anregung hin, und ich spreche ihm für diese Hilfe meinen herzlichsten Dank aus.

Mein Dank gilt auch meiner Frau, die das ganze Manuskript geschrieben und die Verzeichnisse angefertigt hat.

Endlich gebührt der Redaktionskommission der Deutschen Mathematiker-Vereinigung, insbesondere Herrn A. Gutzmer, für die Durchsicht der Korrekturbogen und der Verlagsbuchhandlung Georg Reimer für ihr weitgehendes Entgegenkommen bei Herstellung des Satzes meine dankbare Anerkennung.

Göttingen, den 10. April 1897.

David Hilbert.

[1] Dieses Verzeichnis ist unter Einbeziehung der übrigen Arbeiten dieses Bandes erweitert und an das Ende des Bandes gesetzt worden.

Erster Teil.

Die Theorie des allgemeinen Zahlkörpers.

1. Die algebraische Zahl und der Zahlkörper.

§1. Der Zahlkörper und die konjugierten Zahlkörper.

Eine Zahl α heißt eine **algebraische Zahl**, wenn sie einer Gleichung m-ten Grades von der Gestalt

$$\alpha^m + a_1 \alpha^{m-1} + a_2 \alpha^{m-2} + \cdots + a_m = 0$$

genügt, wo $a_1, a_2, \ldots, a_m$ rationale Zahlen sind.

Sind $\alpha, \beta, \ldots, \varkappa$ eine endliche Anzahl beliebiger algebraischer Zahlen, so bilden alle rationalen Funktionen von $\alpha, \beta, \ldots, \varkappa$ mit ganzzahligen Koeffizienten ein in sich abgeschlossenes System von algebraischen Zahlen, welches **Zahlkörper, Körper** oder **Rationalitätsbereich** genannt wird [Dedekind (*1,2*), Kronecker (*16*)]. Da insbesondere die Summe, die Differenz, das Produkt und der Quotient zweier Zahlen eines Rationalitätsbereiches oder Körpers wieder eine Zahl des Körpers ist, so verhält sich der Begriff des Rationalitätsbereichs oder Körpers gegenüber den vier Rechnungsoperationen der Addition, Subtraktion, Multiplikation und Division invariant.

Satz 1. In jedem Körper k gibt es eine Zahl ϑ derart, daß alle anderen Zahlen des Körpers ganze rationale Funktionen von ϑ mit rationalen Koeffizienten sind.

Der Grad m der Gleichung niedrigsten Grades mit rationalen Koeffizienten, der eine solche Zahl ϑ genügt, heißt der **Grad des Körpers** k. Die Zahl ϑ wird eine **den Körper bestimmende Zahl** genannt. Die Gleichung m-ten Grades für ϑ ist in dem durch die rationalen Zahlen bestimmten Rationalitätsbereiche irreduzibel. Umgekehrt bestimmt jede Wurzel einer solchen irreduzibeln Gleichung einen Zahlkörper m-ten Grades. Sind $\vartheta', \vartheta'', \ldots, \vartheta^{(m-1)}$ die $m-1$ anderen Wurzeln der Gleichung, so heißen die bezüglich durch $\vartheta', \vartheta'', \ldots, \vartheta^{(m-1)}$ bestimmten Körper $k', k'', \ldots, k^{(m-1)}$ die **zu k konjugierten Körper.** Ist α eine beliebige Zahl des Körpers k, und ist

$$\alpha = c_1 + c_2 \vartheta + \cdots + c_m \vartheta^{m-1},$$

wo $c_1, c_2, \ldots, c_m$ rationale Zahlen sind, so heißen die Zahlen

$$\alpha' = c_1 + c_2\vartheta' + \cdots + c_m\vartheta'^{m-1},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\alpha^{(m-1)} = c_1 + c_2\vartheta^{(m-1)} + \cdots + c_m(\vartheta^{(m-1)})^{m-1}$$

die bez. durch die Substitutionen $t' = (\vartheta : \vartheta'), \ldots, t^{(m-1)} = (\vartheta : \vartheta^{(m-1)})$ aus α entspringenden oder **zu α konjugierten Zahlen.**

§ 2. Die ganze algebraische Zahl.

Eine algebraische Zahl α heißt eine **ganze algebraische Zahl** oder kurz eine **ganze Zahl,** wenn sie einer Gleichung von der Gestalt

$$\alpha^m + a_1\alpha^{m-1} + a_2\alpha^{m-2} + \cdots + a_m = 0$$

genügt, deren Koeffizienten $a_1, a_2, \ldots, a_m$ sämtlich ganze rationale Zahlen sind.

Satz 2. Jede ganze ganzzahlige Funktion F, d. h. jede ganze rationale Funktion mit ganzzahligen Koeffizienten von beliebig vielen ganzen Zahlen $\alpha, \beta, \ldots, \varkappa$ ist wiederum eine ganze Zahl.

Beweis: Bezeichnen wir mit $\alpha', \alpha'', \ldots, \beta', \beta'', \ldots, \ldots, \varkappa', \varkappa'', \ldots$ bezüglich die zu $\alpha, \beta, \ldots, \varkappa$ konjugierten Zahlen, und bilden wir dann sämtliche Ausdrücke von der Gestalt

$$F(\alpha, \beta, \ldots, \varkappa), \quad F(\alpha', \beta, \ldots, \varkappa), \quad F(\alpha, \beta', \ldots, \varkappa), \ldots,$$
$$\ldots, F(\alpha, \beta, \ldots, \varkappa'), \ldots, F(\alpha', \beta', \ldots, \varkappa), \ldots,$$

so lehrt der bekannte Satz von den symmetrischen Funktionen, daß die Gleichung, welcher diese sämtlichen Ausdrücke genügen, lauter ganzzahlige Koeffizienten hat, während der Koeffizient der höchsten Potenz der Unbekannten $= 1$ ausfällt.

Insbesondere ist die Summe, die Differenz und das Produkt zweier ganzen Zahlen wiederum eine ganze Zahl. Der Begriff „ganz" verhält sich mithin gegenüber den drei Rechnungsoperationen der Addition, Subtraktion und Multiplikation invariant. Eine ganze Zahl γ heißt durch die ganze Zahl α **teilbar,** wenn eine ganze Zahl β existiert, so daß $\gamma = \alpha\beta$ ist.

Satz 3. Die Wurzeln einer Gleichung beliebigen Grades r von der Gestalt

$$\alpha^r + a_1\alpha^{r-1} + a_2\alpha^{r-2} + \cdots + a_r = 0$$

sind stets ganze algebraische Zahlen, sobald die Koeffizienten $a_1, a_2, \ldots, a_r$ ganze algebraische Zahlen sind.

Satz 4. Wenn eine ganze algebraische Zahl α zugleich rational ist, so ist sie eine ganze rationale Zahl.

Beweis: Wäre nämlich $\alpha = \frac{a}{b}$, wo a und b ganze rationale, zueinander prime Zahlen bedeuten und dabei $b > 1$, und genügt α einer Gleichung, deren

Koeffizienten $a_1, \ldots, a_m$ ganze rationale Zahlen sind, so würde durch Multiplikation dieser Gleichung mit b^{m-1}

$$\frac{a^m}{b} = -a_1a^{m-1} - a_2ba^{m-2} - \cdots - a_mb^{m-1} = A$$

folgen, wo A eine ganze rationale Zahl wäre, und dies ist nicht möglich [Dedekind (*1*), Kronecker (*16*)].

§ 3. Die Norm, die Differente, die Diskriminante einer Zahl. Die Basis des Zahlkörpers.

Ist α eine beliebige Zahl des Körpers k, und bedeuten $\alpha', \ldots, \alpha^{(m-1)}$ die zu α konjugierten Zahlen, so heißt das Produkt

$$n(\alpha) = \alpha\alpha' \ldots \alpha^{(m-1)}$$

die **Norm der Zahl** α. Die Norm einer Zahl α ist stets eine rationale Zahl. Ferner nenne ich das Produkt

$$\delta(\alpha) = (\alpha - \alpha')(\alpha - \alpha'') \ldots (\alpha - \alpha^{(m-1)})$$

die **Differente der Zahl** α. Die Differente einer Zahl ist wiederum eine Zahl des Körpers k. Es ist nämlich, wenn zur Abkürzung

$$f(x) = (x - \alpha)(x - \alpha') \ldots (x - \alpha^{(m-1)})$$

gesetzt wird, $\delta(\alpha) = \left[\frac{df(x)}{dx}\right]_{x=\alpha}$. Endlich heißt das Produkt

$$d(\alpha) = (\alpha - \alpha')^2(\alpha - \alpha'')^2(\alpha' - \alpha'')^2 \ldots (\alpha^{(m-2)} - \alpha^{(m-1)})^2$$
$$= \begin{vmatrix} 1, & \alpha, & \alpha^2, & \ldots, & \alpha^{m-1} \\ 1, & \alpha', & \alpha'^2, & \ldots, & \alpha'^{m-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1, & \alpha^{(m-1)}, & (\alpha^{(m-1)})^2, & \ldots, & (\alpha^{(m-1)})^{m-1} \end{vmatrix}^2$$

die **Diskriminante der Zahl** α. Die Diskriminante einer Zahl ist eine rationale Zahl, und zwar bis auf das Vorzeichen gleich der Norm der Differente; es ist nämlich $d(\alpha) = (-1)^{\frac{m(m-1)}{2}} n(\delta)$.

Ist α eine den Körper bestimmende Zahl, so sind ihre Differente und Diskriminante verschieden von 0. Umgekehrt, wenn Differente oder Diskriminante einer Zahl von 0 verschieden sind, so bestimmt diese den Körper. Ist α eine *ganze* Zahl, so sind ihre Norm, ihre Differente, ihre Diskriminante ebenfalls *ganz*.

Satz 5. In einem Zahlkörper m-ten Grades gibt es stets m ganze Zahlen $\omega_1, \omega_2, \ldots, \omega_m$ von der Beschaffenheit, daß jede andere ganze Zahl ω des Körpers sich in der Gestalt

$$\omega = a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m$$

darstellen läßt, wo $a_1, \ldots, a_m$ ganze rationale Zahlen sind.

C-Basis

Beweis: Ist α eine den Körper bestimmende ganze Zahl, so ist jede Zahl ω in der Gestalt

$$\omega = r_1 + r_2\alpha + \cdots + r_m\alpha^{m-1}$$

darstellbar, wo $r_1, r_2, \ldots, r_m$ rationale Zahlen sind. Durch Übergang zu den konjugierten Zahlen erhält man

$$\begin{aligned} \omega' &= r_1 + r_2\alpha' \quad + \cdots + r_m\alpha'^{m-1}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \omega^{(m-1)} &= r_1 + r_2\alpha^{(m-1)} + \cdots + r_m(\alpha^{(m-1)})^{m-1}; \end{aligned}$$

und hieraus folgt allgemein für $s = 1, 2, \ldots, m$ in leicht verständlicher Abkürzung:

$$r_s = \frac{|1, \alpha, \ldots, \omega, \quad \ldots, \alpha^{m-1}|}{|1, \alpha, \ldots, \alpha^{s-1}, \ldots, \alpha^{m-1}|} = \frac{|1, \alpha, \ldots, \omega, \ldots, \alpha^{m-1}|\,|1, \alpha, \ldots, \alpha^{s-1}, \ldots, \alpha^{m-1}|}{|1, \alpha, \ldots, \alpha^{s-1}, \ldots, \alpha^{m-1}|^2} = \frac{A_s}{d(\alpha)},$$

wo A_s als ganze ganzzahlige Funktion von $\alpha, \alpha', \ldots, \alpha^{(m-1)}, \omega, \omega', \ldots, \omega^{(m-1)}$ eine ganze Zahl ist. Da andererseits A_s gleich der rationalen Zahl $r_s d(\alpha)$ ist, so ist A_s nach Satz 4 eine ganze rationale Zahl. Jede ganze Zahl ω gestattet daher die Darstellung

$$\omega = \frac{A_1 + A_2\alpha + \cdots + A_m\alpha^{m-1}}{d(\alpha)}, \tag{1}$$

wo $A_1, A_2, \ldots, A_m$ ganze rationale Zahlen sind und $d(\alpha)$ die Diskriminante von α bedeutet.

Nun sei wiederum s eine bestimmte von den Zahlen $1, 2, \ldots, m$; wir denken uns alle ganzen Zahlen des Körpers von der Gestalt

$$\begin{aligned} \omega_s &= \frac{O_1 + O_2\alpha + \cdots + O_s\alpha^{s-1}}{d(\alpha)}, \\ \omega_s^{(1)} &= \frac{O_1^{(1)} + O_2^{(1)}\alpha + \cdots + O_s^{(1)}\alpha^{s-1}}{d(\alpha)}, \\ \omega_s^{(2)} &= \frac{O_1^{(2)} + O_2^{(2)}\alpha + \cdots + O_s^{(2)}\alpha^{s-1}}{d(\alpha)}, \\ &\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

berechnet, wo die Koeffizienten $O, O^{(1)}, O^{(2)}, \ldots$ sämtlich ganze rationale Zahlen sind; wir können annehmen, daß etwa $O_s \neq 0$ und der größte gemeinsame Teiler der sämtlichen Zahlen $O_s, O_s^{(1)}, O_s^{(2)}, \ldots$ ist. Dann bilden die betreffenden m ersten Zahlen $\omega_1, \ldots, \omega_m$ ein System von der verlangten Beschaffenheit. Ist nämlich eine beliebige ganze Zahl ω in der Gestalt (1) vorgelegt, so muß nach der eben gemachten Festsetzung $A_m = a_m O_m$ sein, wo a_m eine gewisse ganze rationale Zahl ist; dann aber ist die Differenz $\omega^* = \omega - a_m\omega_m$ von der Gestalt

$$\omega^* = \frac{A_1^* + A_2^*\alpha + \cdots + A_{m-1}^*\alpha^{m-2}}{d(\alpha)}.$$

Hier wird wiederum $A_{m-1}^* = a_{m-1}O_{m-1}$ sein; die Betrachtung der Differenz $\omega^{**} = \omega^* - a_{m-1}\omega_{m-1}$ und die Fortsetzung dieser Schlußweise zeigt die Richtigkeit des Satzes 5.

Die Zahlen $\omega_1, \ldots, \omega_m$ heißen eine Basis des Systems aller ganzen Zahlen des Körpers k, oder kurz eine **Basis des Körpers** k. Jede andere Basis $\omega_1^*, \ldots, \omega_m^*$ des Körpers ist durch Formeln von der Gestalt

$$\begin{aligned} \omega_1^* &= a_{11}\ \omega_1 + \cdots + a_{1m}\ \omega_m, \\ &\cdots\cdots\cdots\cdots\cdots \\ \omega_m^* &= a_{m1}\omega_1 + \cdots + a_{mm}\omega_m \end{aligned}$$

gegeben, wo die Determinante der ganzzahligen Koeffizienten a gleich ± 1 ist [Dedekind (*1*), Kronecker (*16*)].

2. Die Ideale des Zahlkörpers.

§ 4. Die Multiplikation der Ideale und ihre Teilbarkeit. Das Primideal.

Die erste wichtige Aufgabe der Theorie der Zahlkörper ist die Aufstellung der Gesetze über die Zerlegung (Teilbarkeit) der ganzen algebraischen Zahlen. Diese Gesetze sind von bewundernswerter Schönheit und Einfachheit. Sie zeigen eine genaue Analogie mit den elementaren Teilbarkeitsgesetzen in der Theorie der ganzen rationalen Zahlen und besitzen die gleiche fundamentale Bedeutung. Sie sind für den besonderen Fall des Kreiskörpers zuerst von Kummer entdeckt worden [Kummer (*5, 6*)]; ihre Ergründung für den allgemeinen Zahlkörper ist das Verdienst von Dedekind und Kronecker. Die grundlegenden Begriffe dieser Theorie sind folgende:

Ein System von unendlich vielen ganzen algebraischen Zahlen $\alpha_1, \alpha_2, \ldots$ des Körpers k, welches die Eigenschaft besitzt, daß eine jede lineare Kombination $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots$ derselben wiederum dem System angehört, heißt ein **Ideal** $\mathfrak{a}$; dabei bedeuten $\lambda_1, \lambda_2, \ldots$ ganze algebraische Zahlen des Körpers k.

Satz 6. In einem Ideal $\mathfrak{a}$ gibt es stets m Zahlen $\iota_1, \ldots, \iota_m$ von der Art, daß eine jede andere Zahl des Ideals gleich einer linearen Kombination derselben von der Gestalt

$$\iota = l_1\iota_1 + \cdots + l_m\iota_m$$

ist, wo $l_1, \ldots, l_m$ ganze rationale Zahlen sind.

Beweis: Es sei s eine bestimmte von den m Zahlen $1, 2, \ldots, m$; dann denken wir uns alle Zahlen des Ideals von der Gestalt

$$\begin{aligned} \iota_s &= J_1\ \omega_1 + \cdots + J_s\omega_s, \\ \iota_s^{(1)} &= J_1^{(1)}\omega_1 + \cdots + J_s^{(1)}\omega_s, \\ &\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

aufgestellt, wo $J, J^{(1)}, \ldots$ ganze rationale Zahlen sind, und wir nehmen an, daß etwa $J_s \neq 0$ und der größte gemeinsame Teiler der sämtlichen Zahlen

$J_s, J_s^{(1)}, \ldots$ ist. Dann folgt, wie auf S. 72, daß die m Zahlen $\iota_1, \ldots, \iota_m$ die verlangte Beschaffenheit haben.

Die Zahlen $\iota_1, \ldots, \iota_m$ heißen eine **Basis des Ideals** $\mathfrak{a}$. Jede andere Basis $\iota_1^*, \ldots, \iota_m^*$ des Ideals $\mathfrak{a}$ ist durch Formeln von der Gestalt

$$\begin{aligned} \iota_1^* &= a_{11}\,\iota_1 + \cdots + a_{1m}\,\iota_m, \\ &\cdots\cdots\cdots\cdots \\ \iota_m^* &= a_{m1}\,\iota_1 + \cdots + a_{mm}\,\iota_m \end{aligned}$$

gegeben, wo die Determinante der ganzzahligen Koeffizienten a gleich ± 1 ist.

Sind $\alpha_1, \ldots, \alpha_r$ irgend r solche Zahlen des Ideals $\mathfrak{a}$, durch deren lineare Kombination unter Benutzung ganzer algebraischer Koeffizienten λ des Körpers alle Zahlen des Ideals erhalten werden können, so schreibe ich kurz

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_r).$$

Wenn $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ und $\mathfrak{b} = (\beta_1, \ldots, \beta_s)$ zwei Ideale sind, so werde dasjenige Ideal, welches entsteht, wenn man alle Zahlen $\alpha_1, \ldots, \alpha_r$ und $\beta_1, \ldots, \beta_s$ zusammen nimmt, kurz mit $(\mathfrak{a}, \mathfrak{b})$ bezeichnet, d. h. ich schreibe

$$(\mathfrak{a}, \mathfrak{b}) = (\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s).$$

Ein Ideal, welches alle und nur die Zahlen von der Gestalt $\lambda\alpha$ enthält, wo λ jede beliebige ganze Zahl des Körpers darstellt und $\alpha \neq 0$ eine bestimmte ganze Zahl des Körpers bedeutet, heißt ein **Hauptideal** und wird mit (α) oder auch kurz mit α bezeichnet, falls eine Verwechselung mit der Zahl α ausgeschlossen erscheint.

Eine jede Zahl α des Ideals $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ heißt **kongruent** 0 nach dem Ideal $\mathfrak{a}$ oder in Zeichen:

$$\alpha \equiv 0, \quad (\mathfrak{a}).$$

Wenn die Differenz zweier Zahlen α und β kongruent 0 nach $\mathfrak{a}$ ist, so heißen α und β einander kongruent nach $\mathfrak{a}$ oder in Zeichen

$$\alpha \equiv \beta, \quad (\mathfrak{a});$$

sonst heißen sie einander **inkongruent** oder in Zeichen

$$\alpha \not\equiv \beta, \quad (\mathfrak{a}).$$

Wenn man jede Zahl eines Ideals $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ mit jeder Zahl eines zweiten Ideals $\mathfrak{b} = (\beta_1, \ldots, \beta_s)$ multipliziert und die so erhaltenen Zahlen linear mittels beliebiger ganzer algebraischer Koeffizienten des Körpers kombiniert, so wird das so entstehende neue Ideal das **Produkt der beiden Ideale** $\mathfrak{a}$ und $\mathfrak{b}$ genannt, d. h. in Zeichen

$$\mathfrak{a}\,\mathfrak{b} = (\alpha_1\beta_1, \ldots, \alpha_r\beta_1, \ldots, \alpha_1\beta_s, \ldots, \alpha_r\beta_s).$$

Ein Ideal $\mathfrak{c}$ heißt durch das Ideal $\mathfrak{a}$ **teilbar,** wenn ein Ideal $\mathfrak{b}$ existiert derart, daß $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ ist. Ist ein Ideal $\mathfrak{c}$ durch das Ideal $\mathfrak{a}$ teilbar, so sind alle Zahlen

von $\mathfrak{c}$ kongruent 0 nach dem Ideal $\mathfrak{a}$. Betreffs der Teiler eines Ideals gilt ferner die Tatsache:

Hilfssatz 1. Ein Ideal $\mathfrak{j}$ ist nur durch eine endliche Anzahl von Idealen teilbar.

Beweis: Man bilde die Norm n einer beliebigen Zahl $\iota\,(\neq 0)$ des Ideals $\mathfrak{j}$; ist dann etwa $\mathfrak{a}$ ein Teiler des Ideals $\mathfrak{j}$, so ist offenbar auch die ganze rationale Zahl $n \equiv 0$ nach $\mathfrak{a}$. Die m Basiszahlen von $\mathfrak{a}$ seien von der Gestalt

$$\alpha_1 = a_{11}\,\omega_1 + \cdots + a_{1m}\,\omega_m, \ \ldots, \ \alpha_m = a_{m1}\,\omega_1 + \cdots + a_{mm}\,\omega_m,$$

wo $a_{11}, \ldots, a_{mm}$ ganze rationale Zahlen sind. Bedeuten $a'_{11}, \ldots, a'_{mm}$ bezüglich die kleinsten positiven Reste der Zahlen $a_{11}, \ldots, a_{mm}$ nach n, so wird

$$\begin{aligned} \mathfrak{a} &= (a_{11}\,\omega_1 + \cdots + a_{1m}\,\omega_m, \ \ldots, \ a_{m1}\,\omega_1 + \cdots + a_{mm}\,\omega_m) \\ &= (a'_{11}\,\omega_1 + \cdots + a'_{1m}\,\omega_m, \ \ldots, \ a'_{m1}\,\omega_1 + \cdots + a'_{mm}\,\omega_m, n), \end{aligned}$$

und diese letztere Darstellung des Idealteilers $\mathfrak{a}$ läßt unmittelbar die Richtigkeit der Behauptung erkennen.

Ein von 1 verschiedenes Ideal, welches durch kein anderes Ideal teilbar ist, außer durch das Ideal 1 und durch sich selbst, heißt ein **Primideal.** Zwei Ideale heißen zu einander **prim,** wenn sie außer 1 keinen gemeinsamen Idealteiler besitzen. Zwei ganze Zahlen α und β, bez. eine ganze Zahl α und ein Ideal $\mathfrak{a}$ heißen zu einander prim, wenn die Hauptideale (α) und (β), bez. das Hauptideal (α) und das Ideal $\mathfrak{a}$ zueinander prim sind [Dedekind (*1*)].

§ 5. Die eindeutige Zerlegbarkeit eines Ideals in Primideale.

Es gilt die fundamentale Tatsache:

Satz 7. *Ein jedes Ideal* $\mathfrak{j}$ *läßt sich stets auf eine und nur auf eine Weise als Produkt von Primidealen darstellen.*

Dedekind hat seinen Beweis dieses Satzes kürzlich von neuem auseinandergesetzt [Dedekind (*1*)]. Das von Kronecker eingeschlagene Beweisverfahren beruht auf der von ihm geschaffenen Theorie der einem Zahlkörper zugehörigen algebraischen Formen. Die Bedeutung dieser Formentheorie tritt deutlicher hervor, wenn man zuerst direkt die Sätze der Idealtheorie ableitet; hierbei leistet folgender Hilfssatz wesentliche Dienste:

Hilfssatz 2. Wenn die Koeffizienten $\alpha_1, \alpha_2, \ldots, \beta_1, \beta_2, \ldots$ der beiden ganzen Funktionen einer Veränderlichen x

$$\begin{aligned} F(x) &= \alpha_1 x^r + \alpha_2 x^{r-1} + \cdots, \\ G(x) &= \beta_1 x^s + \beta_2 x^{s-1} + \cdots \end{aligned}$$

ganze algebraische Zahlen sind und die Koeffizienten $\gamma_1, \gamma_2, \ldots$ des Produktes beider Funktionen

$$F(x)\,G(x) = \gamma_1 x^{r+s} + \gamma_2 x^{r+s-1} + \cdots$$

sämtlich durch die ganze Zahl ω teilbar sind, so ist auch jede der Zahlen $\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_2\beta_1, \alpha_2\beta_2, \ldots$ durch ω teilbar [KRONECKER (*19*), DEDEKIND (*7*), MERTENS (*1*), HURWITZ (*1, 2*)].

Aus diesem Hilfssatze ergeben sich leicht der Reihe nach die Sätze [HURWITZ (*1*)]:

Satz 8. Zu jedem vorgelegten Ideale $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ läßt sich stets ein Ideal $\mathfrak{b}$ so finden, daß das Produkt $\mathfrak{a}\mathfrak{b}$ ein Hauptideal wird.

Beweis: Setzt man

$$F(x) = \alpha_1 x^r + \alpha_2 x^{r-1} + \cdots$$

und

$$F^{(i)}(x) = \alpha_1^{(i)} x^r + \alpha_2^{(i)} x^{r-1} + \cdots \qquad (i = 1, \ldots, m-1),$$

wo $\alpha_k^{(i)}$ die zu α_k konjugierten Zahlen sind und bildet

$$R = \prod_{i=1}^{m-1} F^{(i)}(x) = \beta_1 + \beta_2 x + \cdots,$$

wo $\beta_1, \beta_2, \ldots$ ganze Zahlen des Körpers k sind, so ist $FR = nU$, wo n eine ganze rationale Zahl und U eine ganzzahlige Funktion bedeutet, deren Koeffizienten keinen gemeinsamen Teiler haben. Hieraus folgt, daß $n \equiv 0$ nach dem Produkt der beiden Ideale $\mathfrak{a}$ und $\mathfrak{b} = (\beta_1, \ldots, \beta_s)$ ist. Der Hilfssatz 2 lehrt ferner, daß auch umgekehrt jede Zahl $\alpha_i\beta_k$ sich durch n teilen läßt. Es ist daher $\mathfrak{a}\mathfrak{b} = n$.

Satz 9. Wenn die drei Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ der Gleichung $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{c}$ genügen, wobei $\mathfrak{c} \neq 0$, so ist $\mathfrak{a} = \mathfrak{b}$.

Beweis: Es sei $\mathfrak{m}$ ein Ideal von der Art, daß $\mathfrak{c}\mathfrak{m}$ ein Hauptideal (α) wird. Aus der Voraussetzung folgt $\mathfrak{a}\mathfrak{c}\mathfrak{m} = \mathfrak{b}\mathfrak{c}\mathfrak{m}$ oder $\alpha\mathfrak{a} = \alpha\mathfrak{b}$ und mithin $\mathfrak{a} = \mathfrak{b}$.

Satz 10. Wenn alle Zahlen eines Ideals $\mathfrak{c} \equiv 0$ nach dem Ideal $\mathfrak{a}$ sind, so ist $\mathfrak{c}$ durch $\mathfrak{a}$ teilbar.

Beweis: Ist $\mathfrak{a}\mathfrak{m}$ gleich dem Hauptideal (α), so sind alle Zahlen des Ideals $\mathfrak{m}\mathfrak{c}$ durch α teilbar, und mithin gibt es ein Ideal $\mathfrak{b}$ derart, daß $\mathfrak{m}\mathfrak{c} = \alpha\mathfrak{b}$ wird. Folglich ist $\mathfrak{a}\mathfrak{m}\mathfrak{c} = \alpha\mathfrak{a}\mathfrak{b}$, d. h. $\alpha\mathfrak{c} = \alpha\mathfrak{a}\mathfrak{b}$, und folglich $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$.

Satz 11. Wenn das Produkt zweier Ideale $\mathfrak{a}\mathfrak{b}$ durch das Primideal $\mathfrak{p}$ teilbar ist, so ist wenigstens eines der Ideale $\mathfrak{a}$ und $\mathfrak{b}$ durch $\mathfrak{p}$ teilbar.

Beweis: Wäre $\mathfrak{a}$ nicht durch $\mathfrak{p}$ teilbar, so würde das Ideal $(\mathfrak{a}, \mathfrak{p})$ ein von $\mathfrak{p}$ verschiedenes und zugleich in $\mathfrak{p}$ aufgehendes Ideal, d. h. $= 1$ sein; demnach wäre $1 = \alpha + \pi$, wo α eine Zahl in $\mathfrak{a}$ und π eine Zahl in $\mathfrak{p}$ bedeutet, und hieraus ergibt sich durch Multiplikation mit einer beliebigen Zahl β in $\mathfrak{b}$ die Beziehung $\beta = \alpha\beta + \pi\beta \equiv \alpha\beta$ nach $\mathfrak{p}$. Zufolge der Voraussetzung ist $\alpha\beta \equiv 0$ nach $\mathfrak{p}$ und folglich auch $\beta \equiv 0$ nach $\mathfrak{p}$.

Nunmehr beweist man den Fundamentalsatz 7 der Idealtheorie, wie folgt: Ist $\mathfrak{j}$ nicht selbst ein Primideal, so sei $\mathfrak{j} = \mathfrak{a}\mathfrak{b}$, wo $\mathfrak{a}$ einen von $\mathfrak{j}$ und 1 verschiedenen Teiler von $\mathfrak{j}$ bedeutet. Ist nun einer der Faktoren $\mathfrak{a}$ und $\mathfrak{b}$ nicht ein Prim-

ideal, so stellen wir denselben in gleicher Weise als Produkt zweier Ideale dar und erhalten somit $\mathfrak{j} = \mathfrak{a}'\mathfrak{b}'\mathfrak{c}'$, und so fahren wir fort. Dieses Verfahren bricht notwendig ab; nach Hilfssatz 1 gibt es nämlich nur eine endliche Anzahl von Teilern des Ideals $\mathfrak{j}$. Ist r diese Anzahl, so kann jedenfalls $\mathfrak{j}$ nicht gleich einem Produkt von mehr als r Faktoren sein, da eine Darstellung $\mathfrak{j} = \mathfrak{a}_1 \ldots \mathfrak{a}_{r+1}$ die Existenz der $r+1$ untereinander verschiedenen Idealteiler

$$\mathfrak{a}_1, \quad \mathfrak{a}_1\mathfrak{a}_2, \quad \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3, \quad \ldots, \quad \mathfrak{a}_1 \ldots \mathfrak{a}_{r+1}$$

bedingen würde. Der letzte Schritt des eingeschlagenen Verfahrens liefert die gewünschte Darstellung

$$\mathfrak{j} = \mathfrak{p}\mathfrak{q} \ldots \mathfrak{l}.$$

Diese Darstellung ist eindeutig. Denn wäre zugleich $\mathfrak{j} = \mathfrak{p}'\mathfrak{q}' \ldots \mathfrak{l}'$, so wird $\mathfrak{j}$ durch $\mathfrak{p}'$ und folglich nach Satz 11 einer der Faktoren $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{l}$, etwa $\mathfrak{p}$, durch $\mathfrak{p}'$ teilbar sein, d. h. es wäre $\mathfrak{p} = \mathfrak{p}'$, und folglich ergibt sich nach Satz 9 die Gleichung $\mathfrak{q} \ldots \mathfrak{l} = \mathfrak{q}' \ldots \mathfrak{l}'$, welche wie die ursprüngliche zu behandeln ist.

Der Fundamentalsatz 7 läßt leicht die folgende Tatsache erkennen:

Satz 12. Ein jedes Ideal $\mathfrak{j}$ des Körpers k kann als größter gemeinsamer Teiler zweier ganzen Zahlen $\varkappa, \varrho$ dargestellt werden.

Beweis: Ist $\varkappa$ eine beliebige durch $\mathfrak{j}$ teilbare ganze Zahl, ϱ jedoch eine solche durch $\mathfrak{j}$ teilbare ganze Zahl, daß $\frac{\varrho}{\mathfrak{j}}$ zu $\frac{\varkappa}{\mathfrak{j}}$ prim ausfällt, so ist $\mathfrak{j} = (\varkappa, \varrho)$. Eine solche Zahl ϱ kann man folgendermaßen finden: Sind $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ sämtliche in $\varkappa$ aufgehenden Primideale, und ist $\mathfrak{j} = \mathfrak{p}_1^{a_1} \ldots \mathfrak{p}_r^{a_r}$, wobei die $a_i \geqq 0$ sind, so besitzen die r Ideale $\mathfrak{b}_i = \mathfrak{p}_1^{a_1+1} \ldots \mathfrak{p}_{i-1}^{a_{i-1}+1} \mathfrak{p}_{i+1}^{a_{i+1}+1} \ldots \mathfrak{p}_r^{a_r+1}$ keinen gemeinsamen Teiler; es gibt also r Zahlen δ_i, so daß δ_i in $\mathfrak{b}_i$ liegt und

$$\delta_1 + \delta_2 + \cdots + \delta_r = 1$$

ist. Bedeutet ferner α_i eine Zahl, die in $\mathfrak{p}_i^{a_i}$, aber nicht in $\mathfrak{p}_i^{a_i+1}$ liegt, so setze man

$$\varrho = \alpha_1\delta_1 + \cdots + \alpha_r\delta_r.$$

ϱ ist dann genau durch $\mathfrak{p}_i^{a_i}$, aber nicht durch $\mathfrak{p}_i^{a_i+1}$ teilbar.

§ 6. Die Formen des Zahlkörpers und ihre Inhalte.

Die Kroneckersche Formentheorie [KRONECKER (*16*)] erfordert folgende weitere Begriffsbildungen:

Eine ganze rationale Funktion F von beliebig vielen Veränderlichen $u, v, \ldots$, deren Koeffizienten ganze algebraische Zahlen des Körpers k sind, heißt eine **Form des Körpers** k. Werden in einer Form F statt der Koeffizienten der Reihe nach bezüglich die konjugierten Zahlen eingesetzt und die so entstehenden sogenannten **konjugierten Formen** $F', \ldots, F^{(m-1)}$ miteinander und

mit der ursprünglichen Form F multipliziert, so ergibt sich als Produkt eine ganze Funktion der Veränderlichen $u, v, \ldots$, deren Koeffizienten ganze rationale Zahlen sind; dieselbe werde in der Gestalt

$$n\,U(u, v, \ldots)$$

angenommen, wo n eine positive ganze rationale Zahl und U eine ganze rationale Funktion bedeutet, deren Koeffizienten ganze rationale Zahlen ohne gemeinsamen Teiler sind. n heißt die **Norm der Form** F. Wenn die Norm n einer Form gleich 1 ist, so heißt die Form eine **Einheitsform.** Eine ganze Funktion, deren Koeffizienten ganze rationale Zahlen ohne gemeinsamen Teiler sind, heißt eine **rationale Einheitsform.** Zwei Formen heißen einander **inhaltsgleich**[1] (in Zeichen $\simeq$), wenn ihr Quotient gleich dem Quotienten zweier Einheitsformen ist. Insbesondere ist jede Einheitsform $\simeq 1$. Eine Form H heißt durch die Form F **teilbar,** wenn eine Form G existiert, derart, daß $H \simeq FG$ ist. Eine Form P heißt eine **Primform,** wenn P im Sinne der Inhaltsgleichheit durch keine andere Form außer durch 1 und durch sich selbst teilbar ist.

Die Beziehung der Kroneckerschen Formentheorie zur Theorie der Ideale wird klar durch die Bemerkung, daß aus jedem Ideal $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ eine Form F gebildet werden kann, indem man die Zahlen $\alpha_1, \ldots, \alpha_r$ mit beliebigen voneinander verschiedenen Produkten aus Potenzen der Unbestimmten $u, v, \ldots$ multipliziert und zueinander addiert. Umgekehrt liefert eine jede Form F mit den Koeffizienten $\alpha_1, \ldots, \alpha_r$ ein Ideal $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$. Dieses Ideal $\mathfrak{a}$ nenne ich den **Inhalt** der Form F. Dann gilt folgende Tatsache:

Satz 13. Der Inhalt des Produktes zweier Formen ist gleich dem Produkte ihrer Inhalte.

Beweis: Es seien F und G Formen mit beliebigen Veränderlichen und den Koeffizienten $\alpha_1, \ldots, \alpha_r$ bezüglich $\beta_1, \ldots, \beta_s$, und es sei das Produkt $H = FG$ eine Form mit den Koeffizienten $\gamma_1, \ldots, \gamma_t$. Ferner sei $\mathfrak{p}^a$ die höchste in $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ und $\mathfrak{p}^b$ die höchste in $\mathfrak{b} = (\beta_1, \ldots, \beta_s)$ aufgehende Potenz des Primideals $\mathfrak{p}$. Man denke sich ferner die Glieder der beiden Formen F und G zunächst nach absteigenden Potenzen von u und dann die mit der nämlichen Potenz von u multiplizierten Glieder nach absteigenden Potenzen von v geordnet usf. Bei dieser Anordnung sei $\alpha u^h v^{h'} \ldots$ das erste in F vorkommende Glied, dessen Koeffizient α durch keine höhere als die a-te Potenz von $\mathfrak{p}$, und andererseits sei $\beta u^{h'} v^{h''} \ldots$ das erste in G vorkommende Glied, dessen Koeffizient β durch keine höhere als die b-te Potenz von $\mathfrak{p}$ teilbar ist: dann ist offenbar der Koeffizient γ des Gliedes $\gamma u^{h+h'} v^{l+l''} \ldots$ in H durch keine höhere als die $(a+b)$-te Potenz von $\mathfrak{p}$ teilbar. Alle übrigen Koeffizienten von H sind aber gewiß auch durch $\mathfrak{p}^{a+b}$ teilbar. Somit folgt die Behauptung $(\alpha_1, \ldots, \alpha_r)(\beta_1, \ldots, \beta_s) = (\gamma_1, \ldots, \gamma_t)$.

[1] Nach Kronecker „äquivalent in engerem Sinne".

Aus Satz 13 folgt insbesondere leicht, daß eine jede Einheitsform den Inhalt 1 besitzt, und daß umgekehrt jede Form, deren Koeffizienten den größten gemeinsamen Idealteiler 1 haben, eine Einheitsform ist. Mithin haben inhaltsgleiche Formen stets den nämlichen Inhalt, und umgekehrt sind alle Formen von dem nämlichen Inhalt einander inhaltsgleich. Speziell sind zwei beliebige Formen mit gleichen Koeffizienten stets einander inhaltsgleich.

Weitere Folgerungen aus Satz 13 sind:

Satz 14. Wenn F eine vorgelegte Form ist, so läßt sich dazu stets eine Form finden derart, daß FR einer ganzen Zahl inhaltsgleich ist.

Satz 15. Wenn das Produkt zweier Formen durch eine Primform P teilbar ist, so ist wenigstens eine der beiden Formen durch P teilbar.

Satz 16. Jede Form ist im Sinne der Inhaltsgleichheit auf eine und nur auf eine Weise als Produkt von Primformen darstellbar.

Diese Sätze laufen parallel bezüglich mit den Sätzen 8, 11 und dem Fundamentalsatze 7 der Idealtheorie.

Außer den von Dedekind und Kronecker eingeschlagenen Wegen führen noch zwei einfachere Methoden zum Beweise des Fundamentalsatzes 7; der einen Methode liegt die Theorie des Galoisschen Zahlkörpers zugrunde. Vgl. § 36 [Hilbert (*2, 3*)]. Die zweite Methode geht von dem Satze aus, daß sich die Ideale eines Körpers auf eine endliche Anzahl von Idealklassen verteilen. Der zum Beweise dieses Satzes erforderliche Grundgedanke kann als eine Verallgemeinerung desjenigen Ansatzes angesehen werden, auf welchem das bekannte Euklidische Divisionsverfahren zur Bestimmung des größten gemeinsamen Teilers zweier ganzen rationalen Zahlen beruht [Hurwitz (*3*)].

3. Die Kongruenzen nach Idealen.

§ 7. Die Norm eines Ideals und ihre Eigenschaften.

Die in Kapitel 2 entwickelte Theorie der Zerlegung der Ideale eines Körpers gestattet es, die elementaren Sätze der Theorie der rationalen Zahlen auf die Zahlen eines algebraischen Zahlkörpers zu übertragen. Wir stellen folgende allgemeine Begriffe und Sätze voran.

Die Anzahl aller nach einem Ideal $\mathfrak{a}$ einander inkongruenten ganzen Zahlen des Körpers heißt die **Norm des Ideals** $\mathfrak{a}$: in Zeichen $n(\mathfrak{a})$.

Satz 17. Die Norm eines Primideals $\mathfrak{p}$ ist eine Potenz der durch $\mathfrak{p}$ teilbaren rationalen Primzahl p.

Beweis: Es seien die f ganzen Zahlen $\omega_1, \ldots, \omega_f$ einer Basis des Körpers in dem Sinne voneinander unabhängig, das keine Kongruenz von der Gestalt

$$a_1\omega_1 + \cdots + a_f\omega_f \equiv 0, \quad (\mathfrak{p})$$

besteht, wo $a_1, \ldots, a_f$ ganze, nicht sämtlich durch p teilbare Zahlen bedeuten, und es möge überdies jede der anderen $m - f$ Zahlen der Körperbasis einem

Ausdruck von der Gestalt $a_1\omega_1 + \cdots + a_f\omega_f$ nach $\mathfrak{p}$ kongruent sein; dann kann dieser Ausdruck jeder Zahl nach $\mathfrak{p}$ kongruent werden, und es beträgt die Anzahl der einander inkongruenten Zahlen nach $\mathfrak{p}$ offenbar p^f.

Der Exponent f heißt der **Grad des Primideals $\mathfrak{p}$.**

Satz 18. Die Norm des Produktes zweier Ideale $\mathfrak{a}\mathfrak{b}$ ist gleich dem Produkt ihrer Normen.

Beweis: Es sei α eine nach Satz 12 gewählte durch $\mathfrak{a}$ teilbare Zahl von der Art, daß $\frac{\alpha}{\mathfrak{a}}$ ein zu $\mathfrak{b}$ primes Ideal ist. Durchläuft dann ξ ein System von $n(\mathfrak{a})$ nach $\mathfrak{a}$ einander inkongruenten Zahlen und η ein System von $n(\mathfrak{b})$ nach $\mathfrak{b}$ zueinander inkongruenten Zahlen, so stellt der Ausdruck $\alpha\eta + \xi$ ein volles System nach $\mathfrak{a}\mathfrak{b}$ einander inkongruenten Zahlen dar; ein solches System umfaßt mithin $n(\mathfrak{a})n(\mathfrak{b})$ Zahlen.

Satz 19. Ist

$$\begin{aligned} \iota_1 &= a_{11}\ \omega_1 + \cdots + a_{1m}\omega_m, \\ &\cdots\cdots\cdots\cdots \\ \iota_m &= a_{m1}\omega_1 + \cdots + a_{mm}\omega_m \end{aligned}$$

eine Basis des Ideals $\mathfrak{a}$, so ist seine Norm $n(\mathfrak{a})$ gleich dem absoluten Betrage der Determinante der Koeffizienten a.

Beweis. Legen wir die Basis des Ideals in der ursprünglich beim Beweise des Satzes 6 gefundenen Gestalt zugrunde, wo die Koeffizienten a_{rs} für $s > r$ sämtlich $= 0$ und die $a_{rr} > 0$ sind, so ist die Determinante jener Koeffizienten a gleich dem Produkt $a_{11} \ldots a_{mm}$. Andererseits stellt der Ausdruck

$$u_1\omega_1 + \cdots + u_m\omega_m$$

für

$$u_1 = 0,\ 1, \ldots,\ a_{11} - 1, \ldots,\ u_m = 0,\ 1, \ldots,\ a_{mm} - 1$$

ein vollständiges System nach $\mathfrak{a}$ einander inkongruenter Zahlen dar. Damit ist Satz 19 bewiesen. Zugleich leuchtet die Umkehrung dieses Satzes ein.

Der Zusammenhang mit der Kroneckerschen Formentheorie erhellt aus dem Satze:

Satz 20. Ist F eine Form mit dem Inhalte $\mathfrak{a}$, so ist die Norm der Form F gleich der Norm des Ideals $\mathfrak{a}$, d. h. $n(F) = n(\mathfrak{a})$. Insbesondere ist die Norm einer ganzen Zahl α dem absoluten Betrage nach stets gleich der Norm des Hauptideals $\mathfrak{a} = (\alpha)$.

Beweis: Ist $\iota_1, \ldots, \iota_m$ eine Basis des Ideals $\mathfrak{a}$, so bilde man die Form

$$F = \iota_1 u_1 + \cdots + \iota_m u_m;$$

dann ist

$$\begin{aligned} \omega_1 F &= l_{11}\ \iota_1 + \cdots + l_{1m}\iota_m, \\ &\cdots\cdots\cdots\cdots \\ \omega_m F &= l_{m1}\iota_1 + \cdots + l_{mm}\iota_m, \end{aligned}$$

wo $l_{11}, \ldots, l_{mm}$ lineare Formen von $u_1, \ldots, u_m$ mit ganzen rationalen Koeffizienten sind. Wir beweisen zunächst, daß die Determinante $|l_{rs}|$ der Formen $l_{11}, \ldots, l_{mm}$ eine rationale Einheitsform ist. In der Tat, wären im Gegenteil die Koeffizienten der Determinante $|l_{rs}|$ sämtlich durch eine Primzahl p teilbar, so müßten notwendig m Formen $L_1, \ldots, L_m$ existieren, deren Koeffizienten ganze rationale, nicht sämtlich durch p teilbare Zahlen sind, und welche den Bedingungen

$$\begin{aligned} L_1 l_{11} + \cdots + L_m l_{m1} &\equiv 0, \qquad (p) \\ &\cdots\cdots\cdots\cdots \\ L_1 l_{1m} + \cdots + L_m l_{mm} &\equiv 0, \qquad (p) \end{aligned}$$

genügen. Hieraus würde

$$(L_1\omega_1 + \cdots + L_m\omega_m)F \equiv 0, \qquad (p\,\mathfrak{a})$$

folgen, d. h. das Produkt $\mathfrak{l}\mathfrak{a}$ ist durch $p\mathfrak{a}$ teilbar, wobei $\mathfrak{l}$ den Inhalt der Form $L_1\omega_1 + \cdots + L_m\omega_m$ bezeichnet. Mithin wäre $\mathfrak{l}$ durch p teilbar, was nicht der Fall sein kann, da eine Zahl von der Gestalt $a_1\omega_1 + \cdots + a_m\omega_m$, wo $a_1, \ldots, a_m$ ganze rationale Zahlen bedeuten, nur dann durch p teilbar ist, sobald die Koeffizienten $a_1, \ldots, a_m$ sämtlich durch p teilbar sind.

Nach dem Multiplikationstheorem der Determinanten ist

$$\begin{vmatrix} \omega_1 & F, & \ldots, \omega_m & F \\ \omega_1' & F', & \ldots, \omega_m' & F' \\ \cdots & \cdots & \cdots & \cdots \\ \omega_1^{(m-1)} & F^{(m-1)}, & \ldots, \omega_m^{(m-1)} & F^{(m-1)} \end{vmatrix} = \begin{vmatrix} l_{11}, & \ldots, l_{1m} \\ l_{21}, & \ldots, l_{2m} \\ \cdots & \cdots \\ l_{m1}, & \ldots, l_{mm} \end{vmatrix} \cdot \begin{vmatrix} \iota_1, & \ldots, \iota_m \\ \iota_1', & \ldots, \iota_m' \\ \cdots & \cdots \\ \iota_1^{(m-1)}, & \ldots, \iota_m^{(m-1)} \end{vmatrix}$$

und mithin folgt nach Weghebung des Faktors

$$\begin{vmatrix} \omega_1, & \ldots, \omega_m \\ \omega_1', & \ldots, \omega_m' \\ \cdots & \cdots \\ \omega_1^{(m-1)}, & \ldots, \omega_m^{(m-1)} \end{vmatrix}$$

die Beziehung $FF' \ldots F^{(m-1)} \simeq n(\mathfrak{a})$ oder $n(F) = n(\mathfrak{a})$. Der zweite Teil des Satzes folgt, wenn wir $F = \alpha(u_1\omega_1 + \cdots + u_m\omega_m)$ nehmen.

Wendet man auf die sämtlichen Zahlen $\alpha_1, \alpha_2, \ldots$ des Ideals $\mathfrak{a}$ die Substitution $t' = (\vartheta : \vartheta')$ an, so heißt das dann entstehende Ideal $\mathfrak{a}' = (t'\alpha_1, t'\alpha_2, \ldots)$ das durch t' aus $\mathfrak{a}$ entspringende oder **zu $\mathfrak{a}$ konjugierte Ideal.** Betrachtet man den aus $k, k', \ldots, k^{(m-1)}$ zusammengesetzten Körper, so lehren die Sätze 18 und 20, daß das Produkt von $\mathfrak{a}$ und allen zu $\mathfrak{a}$ konjugierten Idealen eine ganze rationale Zahl, nämlich $n(\mathfrak{a})$ ist[1]. Aus diesem Umstande entspringt eine neue Definition der Norm des Ideals $\mathfrak{a}$, welche der Definition der Norm einer Zahl α genau entspricht und überdies einer wichtigen Verallgemeinerung fähig ist. Vgl. § 14.

[1] Siehe Seite 93 Zeile 3 von unten ff.

Satz 21. In einem jeden Ideal j lassen sich stets zwei Zahlen finden, deren Normen die Norm des Ideals j zum größten gemeinsamen Teiler haben.

Beweis. Man setze $a = n(\mathfrak{j})$ und bestimme nach Satz 12 eine Zahl α in j derart, daß $\frac{\alpha}{\mathfrak{j}}$ prim zu a ausfällt. Dann wird, wenn $\alpha', \ldots, \alpha^{(m-1)}$ die zu α konjugierten Zahlen und $\mathfrak{j}', \ldots, \mathfrak{j}^{(m-1)}$ die zu j konjugierten Ideale bedeuten, auch $\frac{\alpha'}{\mathfrak{j}'}, \ldots, \frac{\alpha^{(m-1)}}{\mathfrak{j}^{(m-1)}}$, und folglich $\frac{n(\alpha)}{n(\mathfrak{j})} = \frac{n(\alpha)}{a}$ prim zu a, d. h. es ist $n(\mathfrak{j}) = a = (a^m, n(\alpha)) = (n(a), n(\alpha))$.

§ 8. Der Fermatsche Satz in der Idealtheorie und die Funktion $\varphi(\mathfrak{a})$.

Auf Grund der nämlichen Schlüsse wie in der Theorie der rationalen Zahlen ergibt sich die folgende, dem Fermatschen Lehrsatz entsprechende Tatsache: [Dedekind (*I*)].

Satz 22. Ist $\mathfrak{p}$ ein Primideal vom Grade f, so genügt jede ganze Zahl ω des Körpers k der Kongruenz

$$\omega^{p^f} \equiv \omega, \quad (\mathfrak{p}).$$

Auch der verallgemeinerte Fermatsche Lehrsatz ist leicht auf die Körpertheorie übertragbar. Man beweist ferner ohne Mühe die folgenden Sätze: [Dedekind (*I*)].

Satz 23. Die Anzahl aller derjenigen nach einem Ideale $\mathfrak{a}$ einander inkongruenten Zahlen, welche prim zu $\mathfrak{a}$ sind, ist

$$\varphi(\mathfrak{a}) = n(\mathfrak{a})\left(1 - \frac{1}{n(\mathfrak{p}_1)}\right)\left(1 - \frac{1}{n(\mathfrak{p}_2)}\right)\cdots\left(1 - \frac{1}{n(\mathfrak{p}_r)}\right),$$

wo $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ die sämtlichen in $\mathfrak{a}$ aufgehenden und voneinander verschiedenen Primideale bedeuten. Für die Zahl φ gelten die beiden Formeln

$$\varphi(\mathfrak{a})\varphi(\mathfrak{b}) = \varphi(\mathfrak{a}\mathfrak{b}) \quad \text{und} \quad \sum \varphi(\mathfrak{t}) = n(\mathfrak{a}),$$

wo in der ersteren Formel $\mathfrak{a}$ und $\mathfrak{b}$ prim zueinander sind und in der letzteren sich die Summation über alle Idealteiler $\mathfrak{t}$ des Ideals $\mathfrak{a}$ erstreckt.

Satz 24. Jede zu dem Ideal $\mathfrak{a}$ prime ganze Zahl ω genügt der Kongruenz

$$\omega^{\varphi(\mathfrak{a})} \equiv 1, \quad (\mathfrak{a}).$$

So genügt beispielsweise jede durch ein Primideal $\mathfrak{p}$ vom Grade f nicht teilbare ganze Zahl ω des Körpers k der Kongruenz

$$\omega^{p^f(p^f-1)} \equiv 1, \quad (\mathfrak{p}^2).$$

Es gelten ferner die Tatsachen:

Satz 25. Wenn $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ Ideale bedeuten, von denen stets je zwei zueinander prim sind, und wenn $\alpha_1, \ldots, \alpha_r$ beliebige ganze Zahlen sind, so gibt es eine ganze Zahl ω, die den Kongruenzen

$$\omega \equiv \alpha_1, \quad (\mathfrak{a}_1), \quad \ldots, \quad \omega \equiv \alpha_r, \quad (\mathfrak{a}_r)$$

genügt.

Satz 26. Eine Kongruenz r-ten Grades nach dem Primideal $\mathfrak{p}$ von der Gestalt

$$\alpha x^r + \alpha_1 x^{r-1} + \cdots + \alpha_r \equiv 0, \quad (\mathfrak{p})$$

wo $\alpha, \alpha_1, \ldots, \alpha_r$ ganze Zahlen in k sind und $\alpha \not\equiv 0$ nach $\mathfrak{p}$ ist, besitzt höchstens r nach $\mathfrak{p}$ einander inkongruente Wurzeln.

Satz 27. Bedeutet $\mathfrak{p}$ ein in der rationalen Primzahl p aufgehendes Primideal, und ist α eine Wurzel der Kongruenz

$$\alpha x^r + \alpha_1 x^{r-1} + \cdots + \alpha_r \equiv 0, \quad (\mathfrak{p}),$$

wo $a, a_1, \ldots, a_r$ ganze rationale Zahlen bedeuten, so ist auch α^p eine Wurzel dieser Kongruenz.

Beweis: Bezeichnen wir die linke Seite der obigen Kongruenz mit $F(x)$, so gilt nach dem Fermatschen Satze identisch in x die Kongruenz $F(x^p) \equiv (F(x))^p$ nach p, und diese Tatsache bedingt die Richtigkeit der Behauptung.

§ 9. Die Primitivzahlen nach einem Primideal.

Eine ganze Zahl ϱ des Körpers k heißt eine **Primitivzahl nach dem Primideal** $\mathfrak{p}$, wenn die $p^f - 1$ ersten Potenzen derselben sämtliche $p^f - 1$ einander inkongruenten, zu $\mathfrak{p}$ primen Zahlen nach $\mathfrak{p}$ darstellen. Es wird wiederum durch die entsprechenden Schlüsse wie in der Theorie der rationalen Zahlen leicht der Nachweis für folgende Tatsache geführt:

Satz 28. Es gibt $\Phi(p^f - 1)$ Primitivzahlen für das Primideal $\mathfrak{p}$, wo $\Phi(p^f - 1)$ die Anzahl der einander inkongruenten, zu $p^f - 1$ primen rationalen Reste nach $p^f - 1$ bezeichnet.

Eine Theorie der Primitivzahlen für die Potenzen eines Primideals $\mathfrak{p}$ ist bisher noch nicht entwickelt worden; dagegen erkennt man ohne Mühe die folgenden Tatsachen: [Dedekind (*6*)].

Satz 29. Ist $\mathfrak{p}$ ein beliebig vorgelegtes Primideal des Körpers k, so kann man stets in k eine Zahl ϱ finden von der Art, daß jede andere ganze Zahl des Körpers einer gewissen ganzen Funktion von ϱ mit ganzen rationalen Koeffizienten kongruent ist nach einer beliebig hohen Potenz $\mathfrak{p}^l$ des Primideals $\mathfrak{p}$.

Beweis. Ist ϱ^* eine beliebige Primitivzahl für $\mathfrak{p}$, so sind offenbar alle ganzen Zahlen in k kongruent gewissen ganzzahligen Funktionen von ϱ^* nach $\mathfrak{p}$. Es sei

$$P(\varrho^*) \equiv 0, \quad (\mathfrak{p})$$

die Kongruenz niedrigsten Grades nach $\mathfrak{p}$ mit ganzen rationalen Koeffizienten, welcher ϱ^* genügt. Ist der Grad der Funktion P gleich f', so kann kein Ausdruck von der Gestalt $a_1 + a_2\varrho^* + \cdots + a_{f'}\varrho^{*f'-1}$ mit ganzzahligen Koeffizienten $a_1, a_2, \ldots, a_{f'}$ nach $\mathfrak{p}$ kongruent 0 sein; es sei denn, daß sämtliche Koeffizienten $a_1, a_2, \ldots, a_{f'}$ kongruent 0 nach p sind. Da andererseits

jede ganze Zahl des Körpers einem Ausdruck von der obigen Gestalt kongruent sein muß, so folgt $f' = f$.

In dem Fall, daß $P(\varrho^*) \equiv 0$ nach $\mathfrak{p}^2$ ist, setze man $\varrho = \varrho^* + \pi$, wo π eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare Zahl ist. Es ist dann, da nach Satz 27 $\frac{dP(\varrho^*)}{d\varrho^*} \equiv (\varrho^* - \varrho^{*p}) \cdots (\varrho^* - \varrho^{*p^{f-1}}) \not\equiv 0$ nach $\mathfrak{p}$ ist, notwendig

$$P(\varrho) = P(\varrho^* + \pi) \equiv P(\varrho^*) + \pi \frac{dP(\varrho^*)}{d\varrho^*} \not\equiv 0, \quad (\mathfrak{p}^2).$$

Die Zahl ϱ ist eine Zahl von der verlangten Beschaffenheit. Durchlaufen nämlich $\alpha_1, \alpha_2, \ldots, \alpha_f$ alle Ausdrücke von der Gestalt $a_1 + a_2\varrho + \cdots + a_f\varrho^{f-1}$, wo $a_1, a_2, \ldots, a_f$ Zahlen aus der Reihe $0, 1, \ldots, p-1$ bedeuten, so stellt, wie leicht ersichtlich, die Summe

$$\alpha_1 + \alpha_2 P(\varrho) + \cdots + \alpha_l \{P(\varrho)\}^{l-1}$$

lauter nach $\mathfrak{p}^l$ einander inkongruente ganze Zahlen dar, und da hier p^{fl} Zahlen vorliegen, so sind damit sämtliche nach $\mathfrak{p}^l$ inkongruenten Reste erschöpft. Offenbar kommt die gleiche Eigenschaft auch jeder Zahl zu, welche der Zahl ϱ nach $\mathfrak{p}^2$ kongruent ist.

Den letzteren Umstand benutzen wir zu der folgenden Darstellung des Ideals $\mathfrak{p}$:

Satz 30. Wenn ein Primideal $\mathfrak{p}$ vom f-ten Grade vorgelegt ist, so gibt es im Körper k stets eine ganze Zahl ϱ von der im Satze 29 verlangten Eigenschaft und überdies von der Art, daß man

$$\mathfrak{p} = (p, P(\varrho))$$

hat, wo $P(\varrho)$ eine ganze Funktion f-ten Grades von ϱ mit ganzen rationalen Koeffizienten ist.

Beweis: Es sei $p = \mathfrak{p}^e\mathfrak{a}$, wo das Ideal $\mathfrak{a}$ nicht durch $\mathfrak{p}$ teilbar ist. Ferner sei α eine nicht durch $\mathfrak{p}$, wohl aber durch $\mathfrak{a}$ teilbare ganze Zahl. Nach Satz 24 ist $\alpha^{p^f(p^f-1)} \equiv 1$ nach $\mathfrak{p}^2$. Ersetzen wir nun die im vorigen Beweise gefundene Zahl ϱ durch $\varrho\alpha^{p^f(p^f-1)}$, so behält diese neue Zahl ϱ die frühere Eigenschaft; da ferner der letzte Koeffizient der Funktion $P(\varrho)$ nicht durch p teilbar sein kann, so ist für die neue Zahl ϱ notwendig $P(\varrho)$ prim zu $\mathfrak{a}$, d. h. $\mathfrak{p} = (p, P(\varrho))$.

4. Die Diskriminante des Körpers und ihre Teiler.

§ 10. Der Satz über die Teiler der Diskriminante des Körpers. Hilfssätze über ganze Funktionen.

Die **Diskriminante** des Körpers k ist, wenn $\omega_1, \ldots, \omega_m$ eine Basis von k bedeutet, definiert durch die Gleichung

$$d = \begin{vmatrix} \omega_1, & \ldots, \omega_m \\ \omega_1', & \ldots, \omega_m' \\ \cdots & \cdots \\ \omega_1^{(m-1)}, & \ldots, \omega_m^{(m-1)} \end{vmatrix}^2;$$

sie ist eine ganze rationale Zahl. Für die Entwicklung der Körpertheorie ist die Untersuchung der in der Diskriminante des Körpers k aufgehenden idealen Faktoren von grundlegender Bedeutung. Es gilt der fundamentale Satz:

Satz 31. *Die Diskriminante d des Zahlkörpers k enthält alle und nur diejenigen rationalen Primzahlen als Faktoren, welche durch das Quadrat eines Primideals teilbar sind.*

Der Beweis dieses Satzes hat erhebliche Schwierigkeiten verursacht; er ist zum erstenmal von Dedekind geführt worden [Dedekind (6)]. Hensel hat einen zweiten Beweis dieses Satzes gegeben und dadurch die Kroneckersche Theorie der algebraischen Zahlen in einem wesentlichen Punkte ergänzt. Der Henselsche Beweis beruht auf folgenden von Kronecker geschaffenen Begriffen: [Kronecker (16), Hensel (4)].

Bedeuten $u_1, \ldots, u_m$ Unbestimmte, und ist $\omega_1, \ldots, \omega_m$ eine Basis, so heißt

$$\xi = \omega_1 u_1 + \cdots + \omega_m u_m$$

die **Fundamentalform** des Körpers k. Dieselbe genügt offenbar der Gleichung für x

$$(x - \omega_1 u_1 - \cdots - \omega_m u_m)(x - \omega_1' u_1 - \cdots - \omega_m' u_m) \cdots \cdots (x - \omega_1^{(m-1)} u_1 - \cdots - \omega_m^{(m-1)} u_m) = 0,$$

welche die Gestalt

$$x^m + U_1 x^{m-1} + U_2 x^{m-2} + \cdots + U_m = 0$$

annimmt, wo $U_1, \ldots, U_m$ gewisse ganze Funktionen von $u_1, \ldots, u_m$ mit ganzen rationalen Koeffizienten sind. Diese Gleichung m-ten Grades heißt die **Fundamentalgleichung.** Um mit den eben definierten Begriffen operieren zu können, ist es nötig, die Sätze über die Zerlegung von ganzen Funktionen einer Veränderlichen x nach einer rationalen Primzahl p [Serret (1)] auf den allgemeineren Fall zu übertragen, wo die ganzen Funktionen neben der einen Veränderlichen x noch die m Unbestimmten $u_1, \ldots, u_m$ als Parameter enthalten.

Im folgenden werde unter einer **ganzzahligen Funktion** stets eine solche ganze rationale Funktion der Veränderlichen oder Unbestimmten verstanden, deren Koeffizienten *ganze rationale* Zahlen sind. Es heiße ferner eine ganzzahlige Funktion $Z(x; u_1, \ldots, u_m)$ durch eine andere ganzzahlige Funktion $X(x; u_1, \ldots, u_m)$ **teilbar nach** p, wenn eine dritte ganzzahlige Funktion $Y(x; u_1, \ldots, u_m)$ existiert derart, daß identisch in den Veränderlichen $x, u_1, \ldots, u_m$ die Kongruenz

$$Z \equiv XY, \quad (p)$$

besteht. Ist eine ganzzahlige Funktion P nach p durch keine andere Funktion teilbar außer durch solche Funktionen, die einer ganzen rationalen Zahl oder

der Funktion P selbst oder dem Produkte aus P in eine ganze rationale Zahl nach p kongruent sind, so heißt die Funktion P eine **Primfunktion nach** p. Wie in der Theorie der Funktionen *einer* Veränderlichen gelten auch hier die gewöhnlichen Gesetze der Teilbarkeit; insbesondere heben wir den durch das bekannte *Euklidische* Rekursionsverfahren leicht zu beweisenden Satz hervor:

Satz 32. Wenn zwei ganzzahlige Funktionen X und Y von $x, u_1, \ldots, u_m$ nach der rationalen Primzahl p keinen gemeinsamen Teiler haben, so gibt es eine ganzzahlige, nach p nicht der 0 kongruente Funktion U von $u_1, \ldots, u_m$ allein, so daß man

$$U \equiv AX + BY, \qquad (p)$$

hat, wo A und B geeignete ganzzahlige Funktionen von $x, u_1, \ldots, u_m$ sind.

Unser nächstes Ziel ist die Zerlegung der linken Seite F der Fundamentalgleichung in Primfunktionen nach der rationalen Primzahl p. Wir beweisen zunächst folgende Hilfssätze:

Hilfssatz 3. Wenn $\mathfrak{p}$ ein in p aufgehendes Primideal f-ten Grades bezeichnet, so gibt es stets nach p eine Primfunktion $\Pi(x; u_1, \ldots, u_m)$ vom f-ten Grade in x, welche, wenn man an Stelle von x die Fundamentalform ξ setzt, folgende Eigenschaften besitzt: die Koeffizienten der Potenzen und Produkte von $u_1, \ldots, u_m$ in der Funktion $\Pi(\xi; u_1, \ldots, u_m)$ sind durch $\mathfrak{p}$, aber nicht sämtlich durch $\mathfrak{p}^2$ und auch nicht sämtlich durch ein von $\mathfrak{p}$ verschiedenes, in p aufgehendes Primideal teilbar.

Beweis: Es sei $p = \mathfrak{p}^e\mathfrak{a}$, wo das Ideal $\mathfrak{a}$ nicht mehr durch $\mathfrak{p}$ teilbar ist. Ferner sei ϱ eine solche Primitivzahl nach $\mathfrak{p}$, welche die in den Sätzen 29 und 30 angegebenen Eigenschaften besitzt. $P(\varrho)$ sei eine wie dort bestimmte, zu $\mathfrak{p}$ gehörige ganzzahlige Funktion f-ten Grades von der Art, daß $\mathfrak{p} = (p, P(\varrho))$ ist. $P(x)$ ist Primfunktion nach p, weil sonst ϱ einer Kongruenz niederen als f-ten Grades nach $\mathfrak{p}$ genügen würde. Wir setzen

$$\varrho = a_1\omega_1 + \cdots + a_m\omega_m,$$

wo $a_1, \ldots, a_m$ ganz rationale Zahlen sind, und nehmen den Koeffizienten von ϱ' in $P(\varrho)$ gleich 1 an. Da $P(\varrho) \equiv 0$ nach $\mathfrak{p}$ ist, so folgt nach Satz 27, daß auch $P(\varrho^p) \equiv 0$, $P(\varrho^{p^2}) \equiv 0, \ldots, P(\varrho^{p^{f-1}}) \equiv 0$ nach $\mathfrak{p}$ ist, d. h. die Kongruenz $P(x) \equiv 0$ nach $\mathfrak{p}$ besitzt die f einander inkongruenten Wurzeln ϱ, $\varrho^p, \ldots, \varrho^{p^{f-1}}$, und es ist mithin identisch in x

$$P(x) \equiv (x-\varrho)(x-\varrho^p)\ldots(x-\varrho^{p^{f-1}}), \qquad (\mathfrak{p})$$

d. h. die elementarsymmetrischen Funktionen von $\varrho, \varrho^p, \ldots, \varrho^{p^{f-1}}$ sind sämtlich nach $\mathfrak{p}$ gewissen ganzen rationalen Zahlen kongruent.

Da jede ganze Zahl des Körpers k nach $\mathfrak{p}$ einer ganzzahligen Funktion von ϱ kongruent ist, so können wir die Fundamentalform

$$\xi \equiv L(\varrho; u_1, \ldots, u_m)$$

nach $\mathfrak{p}$ setzen, wo L eine ganzzahlige Funktion von $\varrho, u_1, \ldots, u_m$ bedeutet. Nach dem eben Bewiesenen ist der Ausdruck

$$(x - L(\varrho; u_1, \ldots, u_m))(x - L(\varrho^p; u_1, \ldots, u_m)) \ldots (x - L(\varrho^{p^{f-1}}; u_1, \ldots, u_m))$$

nach $\mathfrak{p}$ einer ganzzahligen Funktion von $x, u_1, \ldots, u_m$ kongruent; wir setzen ihn in die Gestalt

$$\Pi(x; u_1, \ldots, u_m) = x^f + V_1 x^{f-1} + \cdots + V_f,$$

wo $V_1, \ldots, V_f$ ganzzahlige Funktionen von $u_1, \ldots, u_m$ bedeuten. Offenbar genügt die Fundamentalform ξ, für x gesetzt, der Kongruenz

$$\Pi(x; u_1, \ldots, u_m) \equiv 0, \quad (\mathfrak{p}).$$

Da die Funktion $\Pi(x; a_1, \ldots, a_m) \equiv P(x)$ nach p ist, so folgt, daß auch $\mathfrak{p} = (p, \Pi(\varrho; a_1, \ldots, a_m))$ ist, und mithin sind die Koeffizienten der Potenzen und Produkte von $u_1, \ldots, u_m$ in $\Pi(\xi; u_1, \ldots, u_m)$ nicht sämtlich durch $\mathfrak{p}^2$ und auch nicht sämtlich durch ein von $\mathfrak{p}$ verschiedenes, in $\mathfrak{a}$ aufgehendes Primideal teilbar. Da $P(x)$ Primfunktion ist, so gilt das gleiche um so mehr von der Funktion $\Pi(x; u_1, \ldots, u_m)$.

Hilfssatz 4. Jede ganzzahlige Funktion $\Phi(x; u_1, \ldots, u_m)$, welche identisch in $u_1, \ldots, u_m$ nach $\mathfrak{p}$ dem Wert 0 kongruent wird, sobald man für x die Fundamentalform ξ einsetzt, ist nach p durch $\Pi(x; u_1, \ldots, u_m)$ teilbar.

Beweis: Im gegenteiligen Falle hätten Φ und Π nach p keinen Teiler gemein, und es müßte folglich nach Satz 32 eine nach p dem Wert 0 nicht kongruente ganzzahlige Funktion U von $u_1, \ldots, u_m$ allein existieren, so daß $U \equiv A\Phi + B\Pi$ nach p wird, wo A, B ganzzahlige Funktionen von $x, u_1, \ldots, u_m$ sind. Hieraus würde, wenn man für x die Fundamentalform ξ einsetzt, $U \equiv 0$ nach $\mathfrak{p}$ und folglich auch nach p sich ergeben, was nicht der Fall ist.

Hilfssatz 5. Ist Φ eine ganzzahlige Funktion von $x, u_1, \ldots, u_m$, welche identisch in $u_1, \ldots, u_m$ nach $\mathfrak{p}^e$ dem Wert 0 kongruent wird, wenn man für x die Fundamentalform ξ einsetzt, so muß notwendig Φ nach p durch Π^e teilbar sein.

Beweis: Setzen wir $\Phi \equiv \Pi^{e'}F$ nach p, wo $e' < e$ ist und F eine ganzzahlige Funktion von $x, u_1, \ldots, u_m$ bedeutet, die nach p nicht mehr durch Π teilbar ist, so folgt, daß sämtliche Koeffizienten der Potenzen und Produkte von $u_1, \ldots, u_m$ in $\{\Pi(\xi; u_1, \ldots, u_m)\}^{e'}F(\xi; u_1, \ldots, u_m)$ durch $\mathfrak{p}^e$ teilbar sein

müssen. Wir denken uns nun sowohl $\Pi(\xi; u_1, \ldots, u_m)$ als $F(\xi; u_1, \ldots, u_m)$ nach fallenden Potenzen der Variabeln u_1 und die Koeffizienten der Potenzen von u_1 wiederum nach fallenden Potenzen von u_2 geordnet usf. Ist dann π der erste Koeffizient in $\Pi(\xi)$, welcher nicht durch $\mathfrak{p}^2$ teilbar ist, und zutreffendenfalls $\varkappa$ der erste Koeffizient in $F(\xi)$, welcher nicht durch $\mathfrak{p}$ teilbar ist, so würde $\pi^{\varepsilon'}\varkappa \equiv 0$ nach $\mathfrak{p}^{\varepsilon}$ folgen, was nicht möglich ist; d. h. sämtliche Koeffizienten von $F(\xi)$ sind durch $\mathfrak{p}$ teilbar, und hieraus folgt nach dem Hilfssatz 4, daß $F(x; u_1, \ldots, u_m)$ durch $\Pi(x; u_1, \ldots, u_m)$ nach p teilbar ist. Diese Folgerung widerspricht unserer Annahme.

§ 11. Die Zerlegung der linken Seite der Fundamentalgleichung. Die Diskriminante der Fundamentalgleichung.

Aus den Hilfssätzen 3, 4 und 5 folgen die nachstehenden wichtigen Tatsachen, welche die Zerlegung der linken Seite der Fundamentalgleichung betreffen:

Satz 33. Ist die Zerlegung der rationalen Primzahl p in Primideale durch die Formel $p = \mathfrak{p}^{\varepsilon}\mathfrak{p}'^{\varepsilon'} \ldots$ gegeben, so gestattet die linke Seite F der Fundamentalgleichung im Sinn der Kongruenz nach p die Darstellung

$$F \equiv \Pi^{\varepsilon}\Pi'^{\varepsilon'} \ldots, \qquad (p),$$

wo $\Pi, \Pi', \ldots$ gewisse verschiedene Primfunktionen von $x, u_1, \ldots, u_m$ nach p bedeuten; überdies ist, wenn

$$F = \Pi^{\varepsilon}\Pi'^{\varepsilon'} \ldots + pG$$

gesetzt wird, G eine ganzzahlige Funktion der Veränderlichen $x, u_1, \ldots, u_m$, welche nach p durch keine der Primfunktionen $\Pi, \Pi', \ldots$ teilbar ist.

Satz 34. Die aus der Fundamentalgleichung sich ergebende Kongruenz m-ten Grades

$$F(x; u_1, \ldots, u_m) \equiv 0, \quad (p)$$

ist zugleich die Kongruenz niedrigsten Grades mit ganzen rationalen Koeffizienten, welcher die Fundamentalform ξ, für x eingesetzt, nach p genügt.

Beweis: Es sei Φ eine ganzzahlige Funktion von $x, u_1, \ldots, u_m$ solcher Art, daß die Kongruenz $\Phi(x) \equiv 0$ nach p von der Fundamentalform ξ befriedigt wird. Ferner seien die voneinander verschiedenen, in p aufgehenden Primideale $\mathfrak{p}, \mathfrak{p}', \ldots$ bezüglich von den Graden $f, f', \ldots$; durch Bildung der Norm folgt $p^m = p^{fe+f'e'+\cdots}$, d. h. $m = fe + f'e' + \cdots$. Ferner mögen $\Pi, \Pi', \ldots$ bez. die zu den Primidealen $\mathfrak{p}, \mathfrak{p}', \ldots$ gehörigen Primfunktionen von $x, u_1, \ldots, u_m$ bedeuten, wie sie in den vorigen Hilfssätzen gebraucht worden sind. Aus dem Hilfssatz 5 folgt dann

$$\Phi \equiv \Pi^{\varepsilon}\Pi'^{\varepsilon'} \ldots \Psi, \qquad (p),$$

wo Ψ eine ganzzahlige Funktion bezeichnet. Da $\Pi, \Pi', \ldots$ bezüglich von den Graden $f, f', \ldots$ in x sind, so folgt, daß Φ mindestens vom m-ten Grade in x sein muß, und dieser Umstand liefert, wenn man an Stelle von Φ die linke Seite F der Fundamentalgleichung wählt, den ersten Teil des Satzes 33 und den Satz 34.

Wäre endlich $G(x)$ nach p etwa durch $\Pi(x)$ teilbar, so würde die Fundamentalform ξ, für x eingesetzt, der Kongruenz $G(x) \equiv 0$ nach $\mathfrak{p}$ und folglich auch der Kongruenz $\Pi^{\varepsilon}(x)\Pi'^{\varepsilon'}(x)\cdots \equiv 0$ nach $\mathfrak{p}^{\varepsilon+1}$ genügen müssen, was nach Hilfssatz 5 nicht möglich ist. Damit ist auch der zweite Teil des Satzes 33 bewiesen.

Die gefundenen Tatsachen bedingen eine Reihe von wichtigen Diskriminantensätzen:

Satz 35. Der größte Zahlenfaktor der Diskriminante der Fundamentalgleichung ist gleich der Diskriminante des Körpers.

Beweis: Wir setzen

$$\left.\begin{aligned} 1 &= U_{11}\,\omega_1 + \cdots + U_{1m}\,\omega_m, \\ \xi &= U_{21}\,\omega_1 + \cdots + U_{2m}\,\omega_m, \\ &\cdots\cdots\cdots\cdots \\ \xi^{m-1} &= U_{m1}\,\omega_1 + \cdots + U_{mm}\,\omega_m, \end{aligned}\right\} \qquad (2)$$

wo $U_{11}, \ldots, U_{mm}$ ganzzahlige Funktionen von $u_1, \ldots, u_m$ seien. Wäre nun die Determinante U dieser m^2 Funktionen eine solche Funktion, deren sämtliche Koeffizienten etwa durch die rationale Primzahl p teilbar sind, so gäbe es offenbar m nicht sämtlich dem Werte 0 nach p kongruente ganzzahlige Funktionen $V_1, \ldots, V_m$ von $u_1, \ldots, u_m$ der Art, daß identisch in $u_1, \ldots, u_m$

$$\begin{aligned} V_1 U_{11} + \cdots + V_m U_{m1} &\equiv 0, \qquad (p) \\ &\cdots\cdots\cdots\cdots \\ V_1 U_{1m} + \cdots + V_m U_{mm} &\equiv 0, \qquad (p) \end{aligned}$$

wird. Mithin müßte die Fundamentalform ξ der Kongruenz

$$V_1 + V_2\xi + \cdots + V_m\xi^{m-1} \equiv 0, \qquad (p)$$

genügen, welche von niederem als m-tem Grade ist. Da dies nach Satz 34 nicht statthaben kann, so folgt, daß die Determinante U eine rationale Einheitsform ist.

Die Gleichungen (2) ergeben mit Hilfe des Multiplikationssatzes der Determinanten:

$$\begin{vmatrix} 1, & \xi, & \ldots, & \xi^{m-1} \\ 1, & \xi', & \ldots, & \xi'^{m-1}, \\ \cdots & \cdots & \cdots & \cdots \\ 1, & \xi^{(m-1)}, & \ldots, & (\xi^{(m-1)})^{m-1} \end{vmatrix} = U \begin{vmatrix} \omega_1, & \ldots, & \omega_m \\ \omega_1', & \ldots, & \omega_m' \\ \cdots & \cdots & \cdots \\ \omega_1^{(m-1)}, & \ldots, & \omega_m^{(m-1)} \end{vmatrix}.$$

Durch Quadrieren dieser Beziehung folgt $d(\xi) = U^2 d$ oder $d(\xi) \simeq d$, wo $d(\xi)$

die Diskriminante der Fundamentalgleichung und d die Körperdiskriminante bedeutet.

Durch Auflösung der Gleichungen (2) ergibt sich ferner die folgende Tatsache:

Satz 36. Jede ganze Zahl des Körpers k ist gleich einer ganzen rationalen Funktion $(m-1)$-ten Grades der Fundamentalform ξ, und zwar sind die Koeffizienten dieser Funktion ganzzahlige Funktionen von $u_1, \ldots, u_m$, dividiert durch die rationale Einheitsform U [KRONECKER (*16*), HENSEL (*4*)].

§ 12. Die Elemente und die Differente des Körpers. Beweis des Satzes über die Teiler der Körperdiskriminante.

Der Satz 35 gestattet die Zerlegung der Körperdiskriminante d in gewisse ideale Faktoren. Die $m-1$ Ideale

$$\begin{aligned}
\mathfrak{e}' &= ((\omega_1 - \omega_1'), \quad \ldots, (\omega_m - \omega_m')),\\
\mathfrak{e}'' &= ((\omega_1 - \omega_1''), \quad \ldots, (\omega_m - \omega_m'')),\\
&\cdots\cdots\cdots\cdots\cdots\\
\mathfrak{e}^{(m-1)} &= ((\omega_1 - \omega_1^{(m-1)}), \ldots, (\omega_m - \omega_m^{(m-1)}))
\end{aligned}$$

nenne ich die $m-1$ **Elemente** des Körpers k. Dieselben sind Ideale, welche im allgemeinen dem Zahlkörper k nicht angehören; dagegen ist das Produkt $\mathfrak{d} = \mathfrak{e}'\mathfrak{e}'' \ldots \mathfrak{e}^{(m-1)}$ ein Ideal[1] des Körpers k. Bedenken wir nämlich, daß die Elemente $\mathfrak{e}', \ldots, \mathfrak{e}^{(m-1)}$ bez. die Inhalte der Formen $\xi - \xi', \ldots, \xi - \xi^{(m-1)}$ sind, so erkennen wir nach Satz 13, daß das Ideal $\mathfrak{d}$ den Inhalt von der Differente der Fundamentalform, nämlich von

$$\frac{\partial F}{\partial \xi} = (\xi - \xi') \ldots (\xi - \xi^{(m-1)})$$

bildet, und diese ist eine Form des Körpers k. Das Ideal $\mathfrak{d}$ nenne ich die **Differente[2] des Körpers.** Die Norm derselben ist gleich dem größten Zahlenfaktor der Diskriminante der Fundamentalform, und, da dieser nach Satz 35 gleich d ist, so folgt der Satz:

Satz 37. Die Norm der Differente des Körpers ist gleich der Diskriminante des Körpers.

Aus der Kongruenz

$$\frac{\partial F(x)}{\partial x} \equiv e\,\Pi^{e-1}\frac{\partial \Pi}{\partial x}\Pi'^{e'} \ldots + e'\,\Pi^{e}\,\Pi'^{e'-1}\frac{\partial \Pi'}{\partial x} \ldots + \cdots, \quad (\mathfrak{p})$$

folgt ferner, daß die Differente des Körpers stets durch $\mathfrak{p}^{e-1}$ teilbar ist, und daß sie jedenfalls dann keine höhere Potenz von $\mathfrak{p}$ enthält, sobald der Exponent e zu p prim ist. Durch Übergang zur Norm ergibt sich hieraus, daß die

[1] Siehe Seite 93 Zeile 3 v. u. ff. [2] Nach DEDEKIND „das Grundideal".

Diskriminante des Körpers stets durch $p^{f(e-1)+f'(e'-1)+\cdots}$ teilbar ist und überdies jedenfalls dann keine höhere Potenz von p enthält, wenn sämtliche Exponenten $e, e', \ldots$ zu p prim sind; damit ist zugleich der am Anfang des § 10 aufgestellte Fundamentalsatz 31 bewiesen.

§ 13. Die Aufstellung der Primideale. Der feste Zahlteiler der rationalen Einheitsform U.

Die wirkliche Berechnung der in einer rationalen Primzahl p aufgehenden Primideale kann auf Grund des Satzes 33 durch Zerlegung der linken Seite der Fundamentalgleichung ausgeführt werden. Doch ist es von Nutzen zu wissen, unter welchen Umständen hierbei den Parametern $u_1, \ldots, u_m$ in der Fundamentalgleichung spezielle Werte beigelegt werden dürfen. Wir stellen zu dem Zweck die folgenden Betrachtungen an.

Die Diskriminanten aller ganzen algebraischen Zahlen des Körpers erhält man, wenn man in $U^2 d$ die Parameter $u_1, \ldots, u_m$ alle ganzen rationalen Zahlen durchlaufen läßt. Der größte gemeinsame Teiler aller dieser Diskriminanten braucht nicht mit der Körperdiskriminante d übereinzustimmen, da sehr wohl der Fall eintreten kann, daß die rationale Einheitsform U für alle ganzzahligen Werte der $u_1, \ldots, u_m$ eine Reihe von Zahlen mit einem festen Teiler $\neq \pm 1$ darstellt. Dieser Umstand setzt die Bedeutung des Gebrauchs der Unbestimmten $u_1, \ldots, u_m$ in helles Licht. Man findet auch leicht eine notwendige und hinreichende Bedingung dafür, daß die rationale Primzahl p ein solcher fester Teiler von U ist. Diese Bedingung besteht nämlich darin, daß U in die Gestalt

$$pV + (u_1^p - u_1)V_1 + \cdots + (u_m^p - u_m)V_m$$

gebracht werden kann, wo $V, V_1, \ldots, V_m$ ganzzahlige Funktionen von $u_1, \ldots, u_m$ sind [HENSEL (*1, 2, 5*)].

Wenn es nun möglich ist, den Unbestimmten $u_1, \ldots, u_m$ solche ganzen rationalen Zahlenwerte $a_1, \ldots, a_m$ zu erteilen, daß für dieselben die rationale Einheitsform U eine durch p nicht teilbare Zahl wird, so darf bei der Zerlegung der rationalen Primzahl p die Fundamentalgleichung so spezialisiert werden, daß die Form ξ durch $\alpha = a_1\omega_1 + \cdots + a_m\omega_m$ ersetzt wird. In der Tat, unter der gemachten Annahme ist, wie leicht aus Satz 36 folgt, jede beliebige ganze Zahl ω des Körpers einer ganzzahligen Funktion von α nach p kongruent, und es ist daher eine ganzzahlige Funktion von niederem als m-tem Grade in α niemals durch p teilbar, wenn nicht ihre Koeffizienten sämtlich durch p teilbar sind. Bezeichnen wir die aus $\Pi(x; u_1, \ldots, u_m), \Pi'(x; u_1, \ldots, u_m), \ldots$ durch die Substitution $u_1 = a_1, \ldots, u_m = a_m$ hervorgehenden Funktionen von x allein mit $P(x), P'(x), \ldots$, so erkennen wir, daß diese Funktionen im Sinne der Kongruenz nach p voneinander verschiedene Primfunktionen sind, und daß

$$\mathfrak{p} = (p, P(\alpha)), \quad \mathfrak{p}' = (p, P'(\alpha)), \ldots$$

wird. In der Tat, würde etwa $P(\alpha)$ nach Forthebung des Faktors $\mathfrak{p}$ noch einen in p aufgehenden Primfaktor, z. B. $\mathfrak{p}'$, enthalten, so wäre

$$\{P(\alpha)\}^e\{P'(\alpha)\}^{e'-1}\{P''(\alpha)\}^{e''}\cdots\equiv 0\,,\quad (p)\,,$$

was nach obiger Bemerkung nicht der Fall sein kann, da die linke Seite dieser Kongruenz eine Funktion von niederem als m-tem Grade in α darstellt.

Umgekehrt gilt die leicht zu beweisende Tatsache: Wenn im Körper k die Zerlegung $p=\mathfrak{p}^e\mathfrak{p}'^{e'}\ldots$ gilt, wo $\mathfrak{p}$, $\mathfrak{p}'$, ... voneinander verschiedene Primideale bezüglich von den Graden f, f', ... sind, und wenn man dann diesen Primidealen $\mathfrak{p}$, $\mathfrak{p}'$, ... ebenso viele ganzzahlige Funktionen $P(x)$, $P'(x)$, ... der einen Veränderlichen x zuordnen kann, die im Sinne der Kongruenz nach p Primfunktionen bez. von den Graden f, f', ... und untereinander verschieden sind, so läßt sich stets eine Zahl $\alpha=a_1\omega_1+\cdots+a_m\omega_m$ finden, für welche der zugehörige Wert von U nicht durch p teilbar ist. Die Nichtexistenz solcher voneinander verschiedenen Primfunktionen $P(x)$, $P'(x)$, ... im Sinne der Kongruenz nach der rationalen Primzahl p bildet daher eine neue notwendige und hinreichende Bedingung dafür, daß die Primzahl p als fester Zahlteiler in U auftritt [Dedekind (*4*)].

Jede der beiden in diesem Paragraphen gefundenen, wesentlich voneinander verschiedenen Bedingungen kann zur Berechnung numerischer Beispiele für Zahlkörper dienen, in deren U wirklich feste Zahlteiler $\neq \pm 1$ der fraglichen Weise enthalten sind [Dedekind (*4*), Kronecker (*16*), Hensel (*1, 2, 5*)].

Es ist jedoch zu bemerken, daß die Form U die Eigenschaft, feste Zahlteiler zu enthalten, verliert, wenn man in derselben die Unbestimmten $u_1,\ldots,u_m$ alle ganzen algebraischen Zahlen eines geeignet gewählten Zahlkörpers durchlaufen läßt, indem die sämtlichen durch U auf diese Art darstellbaren Zahlen den größten gemeinsamen Teiler 1 erhalten [Hensel (*5*)].

5. Der Relativkörper.

§ 14. Die Relativnorm, die Relativdifferente und die Relativdiskriminante.

Die Begriffe Norm, Differente und Diskriminante sind einer wichtigen Verallgemeinerung fähig.

Ist K ein Körper vom Grade M, welcher sämtliche Zahlen des Körpers k vom m-ten Grade enthält, so heißt k ein **Unterkörper** von K. Der Körper K wird der **Oberkörper** von k oder der **Relativkörper** in bezug auf k genannt. Es sei Θ eine den Körper K bestimmende Zahl. Unter den unendlich vielen Gleichungen mit algebraischen, in k liegenden Koeffizienten, denen die Zahl Θ genügt, habe die folgende Gleichung vom Grade r

$$\Theta^r+\alpha_1\Theta^{r-1}+\cdots+\alpha_r=0 \qquad (3)$$

den niedrigsten Grad; $\alpha_1,\ldots,\alpha_r$ sind dann bestimmte Zahlen in k. Der Grad r

heißt der **Relativgrad** des Körpers K in bezug auf k; es ist $M=rm$. Die Gleichung (3) vom r-ten Grade ist im Rationalitätsbereich k irreduzibel. Sind $\Theta',\ldots,\Theta^{(r-1)}$ die $r-1$ anderen Wurzeln der Gleichung (3), so heißen diese $r-1$ algebraischen Zahlen die **zu Θ relativ konjugierten Zahlen,** und die bez. durch $\Theta',\ldots,\Theta^{(r-1)}$ bestimmten Körper $K',\ldots,K^{(r-1)}$ heißen die zu K **relativ konjugierten Körper.** Ist A eine beliebige Zahl des Körpers K, und ist

$$A=\gamma_1+\gamma_2\Theta+\cdots+\gamma_r\Theta^{r-1},$$

wo $\gamma_1,\gamma_2,\ldots,\gamma_r$ Zahlen in k sind, so heißen die Zahlen

$$\begin{aligned}A'&=\gamma_1+\gamma_2\Theta'\quad+\cdots+\gamma_r\Theta'^{r-1},\\ &\cdots\cdots\cdots\cdots\cdots\\ A^{(r-1)}&=\gamma_1+\gamma_2\Theta^{(r-1)}+\cdots+\gamma_r(\Theta^{(r-1)})^{r-1}\end{aligned}$$

die bez. durch die Substitutionen $T'=(\Theta:\Theta'),\ldots,T^{(r-1)}=(\Theta:\Theta^{(r-1)})$ aus A entspringenden oder **zu A relativ konjugierten Zahlen.** Wendet man auf die sämtlichen Zahlen eines Ideals $\mathfrak{J}$ die Substitution T' an, so heißt das dann entstehende Ideal $\mathfrak{J}'$ das durch T' aus $\mathfrak{J}$ entspringende oder **zu $\mathfrak{J}$ relativ konjugierte Ideal.**

Das Produkt einer Zahl A mit den relativ konjugierten Zahlen

$$N_k(A)=AA'\ldots A^{(r-1)}$$

heißt die **Relativnorm der Zahl** A bezüglich des Körpers oder Rationalitätsbereiches k. Die Relativnorm N_k ist eine Zahl in k. Ist $\mathfrak{J}=(A_1,\ldots,A_S)$ ein beliebiges Ideal in K, so heißt das Produkt von $\mathfrak{J}$ mit den sämtlichen relativ konjugierten Idealen von $\mathfrak{J}$

$$N_k(\mathfrak{J})=\mathfrak{J}\mathfrak{J}'\ldots\mathfrak{J}^{(r-1)}$$

die **Relativnorm des Ideals** $\mathfrak{J}$. Die Relativnorm $N_k(\mathfrak{J})$ ist ein Ideal des Körpers k. Bedeuten nämlich $U_1,\ldots,U_S$ Unbestimmte, so sind die Koeffizienten des Ausdruckes

$$(A_1U_1+\cdots+A_SU_S)(A_1'U_1+\cdots+A_S'U_S)\cdots(A_1^{(r-1)}U_1+\cdots+A_S^{(r-1)}U_S)$$

ganze Zahlen in k, deren größter gemeinsamer Teiler nach Satz 13 mit jenem Idealprodukte übereinstimmen muß.

Wenn $\alpha_1,\ldots,\alpha_s$ beliebige Zahlen in k sind und $j=(\alpha_1,\ldots,\alpha_s)$ das durch sie bestimmte Ideal in k bezeichnet, so wird durch die nämlichen Zahlen auch zugleich ein Ideal $\mathfrak{J}=(\alpha_1,\ldots,\alpha_s)$ im Körper K bestimmt. Dieses Ideal $\mathfrak{J}$ ist als nicht verschieden von j anzusehen. Ein Ideal $\mathfrak{J}=(A_1,\ldots,A_S)$ des Körpers K wird umgekehrt dann und nur dann auch als ein Ideal $\mathfrak{j}$ des Körpers k bezeichnet, wenn $\mathfrak{J}$ sich zugleich als größter gemeinsamer Teiler von gewissen ganzen Zahlen $\alpha_1,\ldots,\alpha_s$ des Körpers k darstellen läßt. Daß wir berechtigt sind, unter den angegebenen Umständen $(\alpha_1,\ldots,\alpha_s)$ zugleich als ein Ideal in k und in K anzusehen, lehrt der folgende Satz: Wenn $\alpha_1,\ldots,\alpha_s$

und $\alpha_1^*, \ldots, \alpha_{s^*}^*$ ganze Zahlen in k sind, so daß in K die beiden Ideale $\mathfrak{z} = (\alpha_1, \ldots, \alpha_s)$ und $\mathfrak{z}^* = (\alpha_1^*, \ldots, \alpha_{s^*}^*)$ miteinander übereinstimmen, so stimmen auch in k die beiden Ideale $\mathfrak{j} = (\alpha_1, \ldots, \alpha_s)$ und $\mathfrak{j}^* = (\alpha_1^*, \ldots, \alpha_{s^*}^*)$ miteinander überein. In der Tat, wegen der Voraussetzung gilt, wenn α^* eine der Zahlen $\alpha_1^*, \ldots, \alpha_{s^*}^*$ bedeutet, eine Gleichung von der Gestalt $\alpha^* = A_1\alpha_1 + \cdots + A_s\alpha_s$, wo $A_1, \ldots, A_s$ gewisse ganze Zahlen in K sind. Wenn wir nun von beiden Seiten dieser Gleichung die Relativnorm bilden, so erkennen wir, daß im Körper k die Zahl α^{*r} durch $\mathfrak{j}^r$ teilbar sein muß; infolgedessen ist in k auch α^* durch $\mathfrak{j}$ und daher auch $\mathfrak{j}^*$ durch $\mathfrak{j}$ teilbar. Da in gleicher Weise das Umgekehrte gezeigt werden kann, so haben wir notwendig in k die Gleichung $\mathfrak{j} = \mathfrak{j}^*$.

Der Ausdruck

$$\Delta_k(A) = (A - A')(A - A'') \cdots (A - A^{(r-1)})$$

stellt eine Zahl des Körpers K dar und heißt die **Relativdifferente der Zahl** A in bezug auf den Körper k. Der Ausdruck

$$D_k(A) = (A - A')^2 (A - A'')^2 \cdots (A^{(r-2)} - A^{(r-1)})^2$$

heißt die **Relativdiskriminante der Zahl** A. Dieselbe ist bis auf das Vorzeichen gleich der Relativnorm der Relativdifferente von A; es ist nämlich

$$D_k(A) = (-1)^{\frac{r(r-1)}{2}} N_k(\Delta_k(A)).$$

Sind $\Omega_1, \ldots, \Omega_M$ die M Basiszahlen des Körpers K, so heißt das durch Multiplikation der $r-1$ Elemente

$$\begin{aligned} \mathfrak{E}' &= ((\Omega_1 - \Omega_1'), \quad \ldots, (\Omega_M - \Omega_M')), \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \mathfrak{E}^{(r-1)} &= ((\Omega_1 - \Omega_1^{(r-1)}), \ldots, (\Omega_M - \Omega_M^{(r-1)})) \end{aligned}$$

entstehende Ideal

$$\mathfrak{D}_k = \mathfrak{E}'\mathfrak{E}'' \cdots \mathfrak{E}^{(r-1)}$$

die Relativdifferente des Körpers K in bezug auf k. Bezeichnet

$$\Xi = \Omega_1 U_1 + \cdots + \Omega_M U_M$$

die Fundamentalform von K, so ist die Relativdifferente von Ξ

$$\Delta_k(\Xi) = (\Xi - \Xi') \cdots (\Xi - \Xi^{(r-1)}).$$

Die Koeffizienten dieser Form sind Zahlen des Körpers K, und da nach dem Satze 13 der größte gemeinsame Teiler derselben die Relativdifferente $\mathfrak{D}_k$ ergeben muß, so ist $\mathfrak{D}_k$ ein Ideal des Körpers K.

Das Quadrat des größten gemeinsamen Teilers aller r-reihigen Determinanten der Matrix

$$\begin{vmatrix} \Omega_1, & \Omega_2, & \ldots, & \Omega_M \\ \Omega_1', & \Omega_2', & \ldots, & \Omega_M' \\ \cdots & \cdots & \cdots & \cdots \\ \Omega_1^{(r-1)}, & \Omega_2^{(r-1)}, & \ldots, & \Omega_M^{(r-1)} \end{vmatrix} \tag{4}$$

heißt die **Relativdiskriminante** D_k **des Körpers** K bezüglich k; dieselbe ist, wie leicht ersichtlich, ein Ideal des Körpers k.

§ 15. Eigenschaften der Relativdifferente und der Relativdiskriminante eines Körpers.

Hinsichtlich der soeben definierten Begriffe gelten folgende Sätze [HILBERT (*A*)]:

Satz 38. Die Relativdiskriminante des Körpers K in bezug auf den Unterkörper k ist gleich der Relativnorm der Relativdifferente von K, d. h.

$$D_k = N_k(\mathfrak{D}_k).$$

Beweis: Die Relativnorm von der Relativdifferente der Fundamentalform Ξ ist

$$\begin{aligned} N_k(\Delta_k(\Xi)) &= \pm (\Xi - \Xi')^2 (\Xi - \Xi'')^2 \cdots (\Xi^{(r-2)} - \Xi^{(r-1)})^2 \\ &= \pm \begin{vmatrix} 1, & \Xi, & \ldots, & \Xi^{r-1} \\ 1, & \Xi', & \ldots, & (\Xi')^{r-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1, & \Xi^{(r-1)}, & \ldots, & (\Xi^{(r-1)})^{r-1} \end{vmatrix}^2. \end{aligned}$$

Andererseits ist das rechtsstehende Determinantenquadrat eine Form des Körpers K, deren Inhalt gleich der Relativdiskriminante D_k ist. Drücken wir nämlich die Terme der obigen Determinante linear durch $\Omega_1, \ldots, \Omega_M$ bezüglich durch die konjugierten Basiszahlen des Körpers K aus, wobei die Koeffizienten in diesen Ausdrücken ganzzahlige Funktionen von $U_1, \ldots, U_M$ sind, so erkennen wir, daß jenes Determinantenquadrat lauter durch D_k teilbare Koeffizienten besitzt. Umgekehrt zeigt eine Übertragung des Satzes 36, daß eine jede r-reihige Determinante der Matrix (4) nach Multiplikation mit der r-ten Potenz einer gewissen in den Parametern $U_1, \ldots, U_M$ geschriebenen rationalen Einheitsform durch das Differenzenprodukt

$$(\Xi - \Xi')(\Xi - \Xi'') \cdots (\Xi^{(r-2)} - \Xi^{(r-1)})$$

teilbar wird. Daraus folgt $N_k(\Delta_k(\Xi)) \sim D_k$.

Satz 39. Bedeuten D und d die Diskriminanten des Oberkörpers K und des Unterkörpers k und bezeichnet $n(D_k)$ die Norm der Relativdiskriminante D_k, genommen im Körper k, so ist

$$D = \pm d^r n(D_k).$$

Beweis: Ist $\xi = \omega_1 u_1 + \cdots + \omega_m u_m$ die Fundamentalform des Körpers k, so genügt Ξ, für X gesetzt, einer Gleichung r-ten Grades in X von der Gestalt

$$\Phi(\mathsf{X}, \xi) = \Phi_0 \mathsf{X}^r + \Phi_1 \mathsf{X}^{r-1} + \cdots + \Phi_r = 0,$$

wo $\Phi_1, \ldots, \Phi_r$ ganzzahlige Funktionen von ξ und den Unbestimmten $u_1, \ldots, u_m, U_1, \ldots, U_M$ sind, und wo Φ_0 eine rationale Einheitsform der Unbestimmten $u_1, \ldots, u_m$ ist. Die übrigen Wurzeln der obigen Gleichung r-ten Grades sind $\mathsf{X} = \Xi', \ldots, \Xi^{(r-1)}$. Sodann sei $\xi^{(h)}$ eine der $m-1$ zu ξ konjugierten Fundamentalformen; die Wurzeln der Gleichung r-ten Grades $\Phi(\mathsf{X}, \xi^{(h)}) = 0$ mögen mit $\Xi_{(h)}, \Xi'_{(h)}, \ldots, \Xi^{(r-1)}_{(h)}$ bezeichnet werden. Da nun ξ einer Gleichung m-ten Grades genügt, so ist offenbar jede Potenz von Ξ nach Multiplikation mit einer Potenz von Φ_0 gleich einer ganzen Funktion von ξ und Ξ, welche in ξ höchstens bis zum Grade $m-1$ und in Ξ höchstens bis zum Grade $r-1$ ansteigt, und deren Koeffizienten ganzzahlige Funktionen der Parameter $u_1, \ldots, u_m, U_1, \ldots, U_M$ sind. Infolgedessen ist notwendigerweise die Diskriminante der Fundamentalform Ξ nach Multiplikation mit einer Potenz von Φ_0 durch das Quadrat der $M = rm$-reihigen Determinante

$$\Delta = \begin{vmatrix} 1, \Xi, \ldots, \Xi^{r-1}, & \xi, \xi\Xi, \ldots, \xi\Xi^{r-1}, & \ldots \\ & \ldots, \xi^{m-1}, \xi^{m-1}\Xi, \ldots, \xi^{m-1}\Xi^{r-1} & \\ 1, \Xi', \ldots, \Xi'^{r-1}, & \xi, \xi\Xi', \ldots, \xi\Xi'^{r-1}, & \ldots \\ & \ldots, \xi^{m-1}, \xi^{m-1}\Xi', \ldots, \xi^{m-1}\Xi'^{r-1} & \\ \ldots\ldots\ldots & \ldots\ldots\ldots & \\ 1, \Xi^{(r-1)}, \ldots, (\Xi^{(r-1)})^{r-1}, & \xi, \xi\Xi^{(r-1)}, \ldots, \xi(\Xi^{(r-1)})^{r-1}, & \ldots \\ & \ldots, \xi^{m-1}, \xi^{m-1}\Xi^{(r-1)}, \ldots, \xi^{m-1}(\Xi^{(r-1)})^{r-1} & \\ \ldots\ldots\ldots & \ldots\ldots\ldots & \end{vmatrix}$$

teilbar; hierbei sind in dem Schema nur die ersten r Horizontalreihen hingeschrieben; die übrigen $r(m-1)$ Horizontalreihen entstehen, wenn man der Reihe nach allen Buchstaben ξ die Zeichen $(h) = (1), \ldots, (m-1)$ als obere Indizes und zugleich allen Buchstaben Ξ die nämlichen Zeichen als untere Indizes anfügt.

Drückt man nun die Elemente der Determinante Δ linear durch die Basiszahlen $\Omega_1, \ldots, \Omega_M$ und deren Konjugierte aus, so erkennen wir die Richtigkeit der Formel

$$\Delta = \begin{vmatrix} \Omega_1, & \ldots, \Omega_M \\ \Omega'_1, & \ldots, \Omega'_M \\ \ldots\ldots & \\ \Omega_1^{(M-1)}, & \ldots, \Omega_M^{(M-1)} \end{vmatrix} F,$$

wo F eine ganzzahlige Funktion der Parameter $u_1, \ldots, u_m, U_1, \ldots, U_m$ bedeutet. Hieraus folgt, daß der Zahlenfaktor des Quadrates von Δ durch D teilbar ist. Da aber der Zahlenfaktor der Diskriminante von Ξ nach Satz 35 $= D$ wird, so folgt aus obiger Entwicklung, daß auch umgekehrt D durch den Zahlenfaktor des Quadrates von Δ teilbar ist; d. h. der Zahlenfaktor von Δ^2 ist gleich D.

Aus elementaren Sätzen der Determinantentheorie ergibt sich nun die Identität

$$\Delta = \begin{vmatrix} 1, \xi, & \ldots, \xi^{m-1} \\ 1, \xi', & \ldots, \xi'^{m-1} \\ \ldots\ldots & \\ 1, \xi^{(m-1)}, & \ldots, (\xi^{(m-1)})^{m-1} \end{vmatrix}^r \Pi,$$

wo

$$\Pi = \begin{vmatrix} 1, \Xi, & \ldots, \Xi^{r-1} \\ 1, \Xi', & \ldots, \Xi'^{r-1} \\ \ldots\ldots & \\ 1, \Xi^{(r-1)}, & \ldots, (\Xi^{(r-1)})^{r-1} \end{vmatrix} \begin{vmatrix} 1, \Xi_{(1)}, & \ldots, \Xi_{(1)}^{r-1} \\ 1, \Xi'_{(1)}, & \ldots, \Xi'^{r-1}_{(1)} \\ \ldots\ldots & \\ 1, \Xi^{(r-1)}_{(1)}, & \ldots, (\Xi^{(r-1)}_{(1)})^{r-1} \end{vmatrix} \ldots$$

$$\ldots \begin{vmatrix} 1, \Xi_{(m-1)}, \ldots, & \Xi_{(m-1)}^{r-1} \\ 1, \Xi'_{(m-1)}, \ldots, & \Xi'^{r-1}_{(m-1)} \\ \ldots\ldots & \\ 1, \Xi^{(r-1)}_{(m-1)}, \ldots, & (\Xi^{(r-1)}_{(m-1)})^{r-1} \end{vmatrix}$$

gesetzt ist, und hieraus folgt unmittelbar der Satz 39.

Der eben bewiesene Satz 39 zeigt nicht nur, daß die Diskriminante eines Körpers durch die Diskriminante eines jeden Unterkörpers teilbar ist, sondern gibt eine gewisse Potenz der letzteren an, welche in der Diskriminante des Oberkörpers aufgeht, und deckt auch zugleich die einfache Bedeutung des übrig bleibenden Faktors der Diskriminante des Oberkörpers auf.

§ 16. Die Zerlegung eines Elementes des Körpers k im Oberkörper K. Der Satz von der Differente des Oberkörpers K.

Satz 40. *Jedes Element des Unterkörpers k ist dem Produkt von gewissen r Elementen des Oberkörpers K gleich, und zwar gelten die Formeln:*

$$\xi - \xi^{(h)} \simeq (\Xi - \Xi_{(h)})(\Xi - \Xi'_{(h)}) \cdots (\Xi - \Xi^{(r-1)}_{(h)})$$
$$\simeq (\Xi - \Xi_{(h)})(\Xi' - \Xi_{(h)}) \cdots (\Xi^{(r-1)} - \Xi_{(h)}).$$

Beweis: Ist

$$F(\mathsf{X}) = \mathsf{X}^M + F_1 \mathsf{X}^{M-1} + \cdots + F_M = 0$$

die Fundamentalgleichung M-ten Grades des Körpers K, wobei $F_1, \ldots, F_M$ ganzzahlige Funktionen von $U_1, \ldots, U_M$ bedeuten, so gilt identisch in X die Gleichung

$$\Phi_0^m F(\mathsf{X}) = \Phi(\mathsf{X}, \xi)\Phi(\mathsf{X}, \xi') \cdots \Phi(\mathsf{X}, \xi^{(m-1)}).$$

Die Differente der Fundamentalform Ξ ist mithin wegen $\Phi(\Xi, \xi) = 0$ durch die Formel

$$\Delta(\Xi) = \frac{\partial F(\Xi)}{\partial \Xi} = \frac{1}{\Phi_0^m} \frac{\partial \Phi(\Xi, \xi)}{\partial \Xi} \Phi(\Xi, \xi') \cdots \Phi(\Xi, \xi^{(m-1)})$$

dargestellt. Nun ist einerseits

$$\Phi(\Xi, \xi^{(h)}) = \Phi_0(\Xi - \Xi_{(h)})(\Xi - \Xi'_{(h)}) \cdots (\Xi - \Xi^{(r-1)}_{(h)}), \qquad (5)$$
$$(h=1, 2, \ldots, m-1)$$

und andererseits ist

$$\Phi(\Xi, \xi^{(h)}) = \Phi(\Xi, \xi^{(h)}) - \Phi(\Xi, \xi) = (\xi - \xi^{(h)}) G^{(h)}, \qquad (6)$$

wo $G^{(h)}$ eine ganze algebraische Form bedeutet; aus diesen Formeln folgt:

$$\Phi_0^m \frac{\partial F(\Xi)}{\partial \Xi} = \frac{\partial \Phi(\Xi, \xi)}{\partial \Xi}(\xi - \xi') \cdots (\xi - \xi^{(m-1)}) G' \cdots G^{(m-1)}.$$

Da $\frac{1}{\Phi_0} \frac{\partial \Phi(\Xi, \xi)}{\partial \Xi}$ die Relativdifferente von Ξ darstellt, so folgt nach Satz 13 aus der letzten Formel

$$\mathfrak{D} = \mathfrak{D}_k \mathfrak{d} \mathfrak{F}, \qquad (7)$$

wo $\mathfrak{D}$ die Differente von K, $\mathfrak{D}_k$ die Relativdifferente von K in bezug auf k, $\mathfrak{d}$ die Differente von k und wo $\mathfrak{F}$ dasjenige Ideal bedeutet, welches den Inhalt der Form $G' \ldots G^{(m-1)}$ ausmacht. Durch Normbildung ergibt sich $D = n(D_k) d'^r N(\mathfrak{F})$, und folglich ist nach Satz 39 $N(\mathfrak{F}) = 1$, d. h. $\mathfrak{F} = 1$. Die Formen $G', \ldots, G^{(m-1)}$ sind daher sämtlich Einheitsformen, und die Formeln (5) und (6) beweisen unseren Satz 40.

Der Satz 40 liefert die Zerlegung der Elemente des Körpers k im Oberkörper K; er ist das Fundament der Theorie der Diskriminanten. Die Formel (7) liefert überdies die wichtige Tatsache:

Satz 41. Die Differente $\mathfrak{D}$ des Körpers K ist gleich dem Produkt der Relativdifferente $\mathfrak{D}_k$ von K in bezug auf den Unterkörper k und der Differente $\mathfrak{d}$ des Körpers k, d. h. es ist

$$\mathfrak{D} = \mathfrak{D}_k \mathfrak{d}.$$

Nach diesem Satze ist das Verhalten der Differenten beim Übergange von dem Unterkörper in den Oberkörper von merkwürdiger Einfachheit: man bekommt die Differente des höheren Körpers, indem man die Differente des niederen Körpers mit der betreffenden Relativdifferente multipliziert.

6. Die Einheiten des Körpers.

§ 17. Die Existenz konjugierter Zahlen, deren absolute Beträge gewissen Ungleichungen genügen.

Nachdem in Kapitel 2 die Teilbarkeitsgesetze der Zahlen eines algebraischen Körpers ausführlich behandelt sind, gehen wir dazu über, diejenigen Wahrheiten zu entwickeln, bei deren Ergründung der Größenbegriff eine wesentliche Rolle spielt. Das wichtigste Hilfsmittel bei diesen Untersuchungen bildet der folgende Satz [Minkowski (3)]:

Hilfssatz 6. Sind

$$\begin{aligned} f_1 &= a_{11} u_1 + \cdots + a_{1m} u_m, \\ &\cdots\cdots\cdots\cdots \\ f_m &= a_{m1} u_1 + \cdots + a_{mm} u_m \end{aligned}$$

m lineare homogene Formen von $u_1, \ldots, u_m$ mit beliebigen reellen Koeffizienten $a_{11}, \ldots, a_{mm}$ und der Determinante 1, so kann man $u_1, \ldots, u_m$ stets als ganze rationale Zahlen, die nicht sämtlich 0 sind, so bestimmen, daß die Werte jener m Formen $f_1, \ldots, f_m$, absolut genommen, sämtlich ≤ 1 werden.

Dieser Satz erhält durch eine leichte Umformung die Gestalt:

Hilfssatz 7. Sind $f_1, \ldots, f_m$ m lineare homogene Formen von $u_1, \ldots, u_m$ mit beliebigen reellen Koeffizienten und der positiven Determinante A, und bedeuten $\varkappa_1, \ldots, \varkappa_m$ beliebige positive Konstante, deren Produkt gleich A ist, so kann man $u_1, \ldots, u_m$ stets als ganze rationale Zahlen, die nicht sämtlich 0 sind, so bestimmen, daß die absoluten Werte jener m Formen den Bedingungen

$$|f_1| \leqq \varkappa_1, \ \ldots, \ |f_m| \leqq \varkappa_m$$

genügen.

Es sei bemerkt, daß in diesem Kapitel, abweichend von dem Früheren, der Körper k und die $m - 1$ zu k konjugierten Körper bezüglich mit $k = k^{(1)}, k^{(2)}, \ldots, k^{(m)}$ und dem entsprechend allgemein die in $k^{(s)}$ liegenden, zu $\omega_1, \ldots, \omega_m$ konjugierten Basiszahlen mit $\omega_1^{(s)}, \ldots, \omega_m^{(s)}$ bezeichnet werden.

Den Hilfssatz 7 verwenden wir zum Beweise der folgenden Tatsache:

Satz 42. Sind $\varkappa_1, \ldots, \varkappa_m$ beliebige reelle positive Konstante, deren Produkt gleich $|\sqrt{d}|$ ist, und die den Bedingungen $\varkappa_s = \varkappa_{s'}$ genügen, falls $k^{(s)}$ und $k^{(s')}$ konjugiert imaginäre Körper sind, so gibt es im Körper k immer eine ganze von 0 verschiedene Zahl ω so, daß

$$|\omega^{(1)}| \leqq \varkappa_1, \ \ldots, \ |\omega^{(m)}| \leqq \varkappa_m$$

wird.

Beweis: Wir ordnen den Körpern $k^{(1)}, \ldots, k^{(m)}$ gewisse Linearformen zu, und zwar nach folgendem Gesichtspunkte: Ist $k^{(r)}$ ein reeller Körper, so ordnen wir demselben die Linearform

$$f_r = \omega_1^{(r)} u_1 + \cdots + \omega_m^{(r)} u_m$$

zu; ist dagegen $k^{(s)}$ ein imaginärer Körper und $k^{(s')}$ der zu demselben konjugiert imaginäre Körper, so ordnen wir den beiden Körpern $k^{(s)}$ und $k^{(s')}$ die beiden Linearformen

$$\left.\begin{aligned} f_s &= \frac{1}{|2}\{(\omega_1^{(s)} + \omega_1^{(s')}) u_1 + \cdots + (\omega_m^{(s)} + \omega_m^{(s')}) u_m\}, \\ f_{s'} &= \frac{1}{i|2}\{(\omega_1^{(s)} - \omega_1^{(s')}) u_1 + \cdots + (\omega_m^{(s)} - \omega_m^{(s')}) u_m\} \end{aligned}\right\} \qquad (8)$$

zu, deren Koeffizienten wiederum reell sind. Die Determinante der m Formen $f_1, \ldots, f_m$ ist, absolut genommen, $= |\sqrt{d}|$. Der Hilfssatz 7 liefert dann unmittelbar die Behauptung, wenn man berücksichtigt, daß für die Paare imaginärer Körper

$$f_s^2 + f_{s'}^2 = 2|\omega_1^{(s)} u_1 + \cdots + \omega_m^{(s)} u_m|^2$$

ist.

Andererseits folgt leicht die Tatsache:

Satz 43. Wenn der Grad m und eine beliebige positive Konstante $\varkappa$ gegeben ist, so existiert nur eine endliche Anzahl von ganzen algebraischen Zahlen m-ten Grades, die nebst allen ihren Konjugierten, absolut genommen, $< \varkappa$ sind.

Beweis: Die m ganzzahligen Koeffizienten der Gleichung, der eine solche ganze Zahl genügt, müssen absolut sämtlich unterhalb einer nur von m und $\varkappa$ abhängigen Grenze liegen; sie sind daher ihrer Anzahl nach beschränkt.

§ 18. Sätze über die absolute Größe der Körperdiskriminante.

Wir beweisen die beiden folgenden Sätze:

Satz 44. *Die Diskriminante d eines Zahlkörpers k ist stets verschieden von* ± 1 [Minkowski (*1, 2, 3*)].

Satz 45. *Es gibt nur eine endliche Anzahl von Körpern m-ten Grades mit gegebener Diskriminante d* [Hermite (*1, 2*), Minkowski (*3*)].

Zum Beweise dieser Sätze dient der folgende Hilfssatz:

Hilfssatz 8. Wenn $f_1, \ldots, f_m$ die in Formel (8) definierten m reellen Linearformen der Unbestimmten $u_1, \ldots, u_m$ bedeuten, so existiert im Körper k stets eine solche von 0 verschiedene ganze Zahl $\alpha = a_1\omega_1 + \cdots + a_m\omega_m$, für welche die absoluten Beträge dieser Formen für $u_1 = a_1, \ldots, u_m = a_m$ den Bedingungen

$$|f_1| \leqq |\sqrt{d}|, \quad |f_2| < 1, \quad |f_3| < 1, \ \ldots, \ |f_m| < 1 \tag{9}$$

genügen.

Beweis: Nach Satz 43 kann es nur eine endliche Anzahl von ganzen Zahlen $\alpha, \alpha_1, \alpha_2, \ldots$ im Körper k geben, welche die Bedingungen

$$|f_1| < |\sqrt{d}| + 1, \quad |f_2| < 1, \ \ldots, \ |f_m| < 1$$

erfüllen. Diejenige unter diesen Zahlen $\alpha, \alpha_1, \alpha_2, \ldots$, für welche $|f_1|$ den kleinsten Wert besitzt, sei α, und dieser kleinste Wert selbst werde mit φ bezeichnet. Sollte es keine solche Zahl α geben, so setze man $\varphi = |\sqrt{d}| + 1$. Fällt nun $\varphi \leqq |\sqrt{d}|$ aus, so ist die Richtigkeit des Hilfssatzes 8 offenbar. Im anderen Falle bestimmen wir eine positive Zahl ε derart, daß $(1+\varepsilon)^{m-1}|\sqrt{d}| < \varphi$ wird. Nach Hilfssatz 7 gibt es dann stets ein System ganzer rationaler Zahlen $u_1, \ldots, u_m$, die nicht sämtlich Null sind, von der Art, daß

$$|f_1| \leqq (1+\varepsilon)^{m-1}|\sqrt{d}|, \quad |f_2| \leqq \frac{1}{1+\varepsilon}, \ \ldots, \ |f_m| \leqq \frac{1}{1+\varepsilon}$$

und folglich

$$|f_1| < \varphi, \qquad |f_2| < 1, \ \ldots, \qquad |f_m| < 1$$

wird; dies steht mit der von uns getroffenen Wahl der Zahl α im Widerspruch.

Um nun die beiden Sätze 44 und 45 zu beweisen, verfahren wir wie folgt. Ist $k = k^{(1)}$ ein reeller Körper, so ist die Form f_1 eine völlig bestimmte. Ist jedoch $k^{(1)}$ ein imaginärer Körper und $k^{(2)}$ der zu ihm konjugierte, so stehen uns für f_1 zwei Formen zur Auswahl; wir setzen

$$f_1 = \frac{1}{i\,|\,2}\{(\omega_1^{(1)} - \omega_1^{(2)})\,u_1 + \cdots + (\omega_m^{(1)} - \omega_m^{(2)})\,u_m\}.$$

Die Reihenfolge, in der wir die übrigen Formen $f_2, \ldots, f_m$ annehmen, ist gleichgültig. Der Hilfssatz 8 zeigt die Existenz einer ganzen Zahl α, welche den Bedingungen (9) genügt. Andererseits ist

$$\prod_{(r)} |f_r| \prod_{s,s'} \frac{f_s^2 + f_{s'}^2}{2} = |n(\alpha)|,$$

wo das erste Produkt über alle Formen f_r, das zweite über alle Formenpaare f_s, $f_{s'}$ zu erstrecken ist. Da notwendig $|n(\alpha)| \geqq 1$ ausfällt, so folgt $|f_1| > 1$ und daher $|\sqrt{d}| > 1$, womit der Satz 44 bewiesen ist.

Zugleich folgt aus den Ungleichungen $|f_1| > 1$, $|f_2| < 1$, $|f_3| < 1, \ldots$, $|f_m| < 1$, daß α eine Zahl des Körpers $k = k^{(1)}$ ist, welche sich von allen ihren Konjugierten unterscheidet, d. h. es ist die Differente $\delta(\alpha) \neq 0$. Nach der Bemerkung auf S. 71 unten ist daher α eine den Körper k bestimmende Zahl. Da ferner d eine vorgeschriebene Zahl ist, so gibt es nach Satz 43 nur eine endliche Anzahl von ganzen algebraischen Zahlen m-ten Grades, welche nebst ihren Konjugierten den Bedingungen (9) genügen, und daraus folgt unmittelbar die Richtigkeit des Satzes 45.

Der Satz 44 spricht die das Wesen der algebraischen Zahl tief berührende Eigenschaft aus, daß die Diskriminante eines jeden Zahlkörpers mindestens *eine* Primzahl enthalten muß.

Wenn wir statt des zu Anfang dieses Abschnitts genannten und dieser ganzen Untersuchung zugrunde liegenden Hilfssatzes 6 einen ebenfalls von Minkowski aufgestellten schärferen Satz benutzen, so führt die nämliche Schlußweise auf die Tatsache, daß der absolute Betrag der Diskriminante eines Körpers m-ten Grades sicherlich immer die Größe $\left(\frac{\pi}{4}\right)^{2r_2}\left(\frac{m^m}{m!}\right)^2$ und daher um so mehr die Größe $\left(\frac{\pi}{4}\right)^{2r_2} \frac{e^{2m-\frac{1}{6m}}}{2\pi m}$ übertrifft, wo r_2 die Anzahl derjenigen imaginären Körperpaare bedeutet, welche unter den m konjugierten Körpern $k^{(1)}, \ldots, k^{(m)}$ vorhanden sind [Minkowski (*1, 2, 3*)].

Die letztere Tatsache, in entsprechender Weise verwertet, zeigt, daß auch unter den Körpern aller möglicher Grade nur eine endliche Anzahl vorhanden sein kann, welche die vorgeschriebene Diskriminante d besitzt.

Aus den nämlichen Prinzipien folgt noch eine Tatsache, die für das nächste Kapitel 7 von Wichtigkeit ist [Minkowski (*1, 3*)]:

Satz 46. Ist $\mathfrak{a}$ ein vorgelegtes Ideal des Körpers k, so gibt es stets eine ganze von 0 verschiedene Zahl α des Körpers, welche durch $\mathfrak{a}$ teilbar ist, und deren Norm der Bedingung

$$|n(\alpha)| \leqq |n(\mathfrak{a})\sqrt{d}|$$

genügt.

Beweis: Sind

$$\begin{aligned} \iota_1 &= a_{11}\omega_1 + \cdots + a_{1m}\omega_m, \\ &\cdots\cdots\cdots\cdots \\ \iota_m &= a_{m1}\omega_1 + \cdots + a_{mm}\omega_m \end{aligned}$$

die m Basiszahlen des Ideals $\mathfrak{a}$, so mögen aus denselben genau, wie dies vorhin mittels $\omega_1, \ldots, \omega_m$ geschah, m lineare Formen $f_1, \ldots, f_m$ mit reellen Koeffizienten gebildet werden; die Determinante dieser m Formen ist dann dem Werte nach gleich

$$\begin{vmatrix} \iota_1^{(1)}, & \ldots, & \iota_m^{(1)} \\ \cdots & \cdots & \cdots \\ \iota_1^{(m)}, & \ldots, & \iota_m^{(m)} \end{vmatrix} = \begin{vmatrix} a_{11}, & \ldots, & a_{1m} \\ \cdots & \cdots & \cdots \\ a_{m1}, & \ldots, & a_{mm} \end{vmatrix} \begin{vmatrix} \omega_1^{(1)}, & \ldots, & \omega_m^{(1)} \\ \cdots & \cdots & \cdots \\ \omega_1^{(m)}, & \ldots, & \omega_m^{(m)} \end{vmatrix}$$

und folglich nach Satz 19, absolut genommen, gleich $|n(\mathfrak{a})\sqrt{d}|$. Ordnen wir nun den Formen $f_1, \ldots, f_m$ je eine von irgend m reellen positiven Konstanten $\varkappa_1, \ldots, \varkappa_m$ zu, deren Produkt $= |n(\mathfrak{a})\sqrt{d}|$ ist, und welche den Bedingungen $\varkappa_s = \varkappa_{s'}$ genügen, falls $k^{(s)}$ und $k^{(s')}$ konjugiert imaginäre Körper sind, so folgt aus Satz 42 die Richtigkeit des Satzes 46.

§ 19. Der Satz von der Existenz der Einheiten eines Körpers. Ein Hilfssatz über die Existenz einer Einheit von besonderer Eigenschaft.

Die wichtigste Grundlage für das tiefere Studium der ganzen algebraischen Zahlen bildet der folgende fundamentale Satz über die Einheiten des Körpers k [Dirichlet (*13, 14, 16*), Dedekind (*1*), Kronecker (*18, 20*), Minkowski (*3*)].

Eine ganze Zahl ε des Körpers k, deren reziproker Wert $\frac{1}{\varepsilon}$ wiederum eine ganze Zahl ist, heißt eine **Einheit** des Körpers k. Die Norm einer Einheit ist $= \pm 1$; umgekehrt, wenn die Norm einer ganzen Zahl des Körpers $= \pm 1$ wird, so ist diese eine Einheit des Körpers.

Satz 47. *Sind unter den m konjugierten Körpern $k^{(1)}, \ldots, k^{(m)}$ r_1 reelle Körper und $r_2 = \frac{m - r_1}{2}$ imaginäre Körperpaare vorhanden, so gibt es im Körper $k = k^{(1)}$ ein System von $r = r_1 + r_2 - 1$ Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ von der Beschaffenheit, daß jede vorhandene Einheit ε des Körpers k auf eine und nur auf eine Weise in der Gestalt*

$$\varepsilon = \varrho\, \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$$

dargestellt werden kann, wo $a_1, \ldots, a_r$ ganze rationale Zahlen sind, und wo ϱ eine in k vorkommende Einheitswurzel bedeutet.

Um den Beweis dieses Satzes vorzubereiten, ordnen wir die m konjugierten Körper $k^{(1)}, \ldots, k^{(m)}$ in bestimmter Weise, wie folgt, an. Voran stellen wir die r_1 reellen Körper $k^{(1)}, \ldots, k^{(r_1)}$; dann wählen wir aus jedem der r_2 Paare konjugiert imaginärer Körper je einen aus; diese Körper seien: $k^{(r_1+1)}, \ldots, k^{(r_1+r_2)}$; darauf lassen wir die zu diesen konjugiert imaginären Körper folgen: $k^{(r_1+r_2+1)}, \ldots, k^{(m)}$. Wir bilden nun mit den m beliebigen reellen Veränderlichen $u_1, \ldots, u_m$ die m Linearformen

$$\xi_s = \omega_1^{(s)} u_1 + \cdots + \omega_m^{(s)} u_m, \qquad (s = 1, 2, \ldots, m)$$

und schreiben noch $\xi_1 = \xi$. Sind $\xi_1, \ldots, \xi_m$ sämtlich $+ 0$, so setzen wir im Falle, daß $k^{(s)}$ ein reeller Körper ist,

$$\log|\xi_s| = l_s(\xi)$$

und im Falle, daß $k^{(s)}$ und $k^{(s')}$ konjugiert imaginäre Körper sind,

$$\begin{aligned} \log(\xi_s) &= \tfrac{1}{2} l_s(\xi) - i l_{s'}(\xi), \\ \log(\xi_{s'}) &= \tfrac{1}{2} l_s(\xi) + i l_{s'}(\xi), \end{aligned}$$

wo $l_1(\xi), \ldots, l_m(\xi)$ sämtlich reelle Größen sind und insbesondere die Werte $l_{s'}(\xi)$ den Ungleichungen

$$0 \leqq l_{s'}(\xi) < 2\pi$$

genügen sollen; die Größen $l_1(\xi), \ldots, l_m(\xi)$ sind hierdurch als eindeutige reelle Funktionen der reellen Veränderlichen $u_1, \ldots, u_m$ definiert; sie sollen die **Logarithmen zur Form** ξ heißen. Bezeichnet ferner $ln(\xi)$ den reellen Teil des Logarithmus von $n(\xi)$, so ist

$$l_1(\xi) + \cdots + l_{r+1}(\xi) = ln(\xi).$$

Sind $u_1, \ldots, u_m$ ganze rationale Zahlen, die nicht sämtlich verschwinden, so stellt $\xi = \xi_1$ eine ganze von 0 verschiedene Zahl α des Körpers $k = k^{(1)}$ dar. Die Größen $l_1(\xi), \ldots, l_m(\xi)$ sind dann eindeutig durch die Zahl α bestimmt und sollen die **Logarithmen zur Zahl** α heißen. Ist ε eine Einheit des Körpers k, so besteht wegen $n(\varepsilon) = \pm 1$ die Gleichung

$$l_1(\varepsilon) + l_2(\varepsilon) + \cdots + l_{r+1}(\varepsilon) = 0.$$

Die reellen Variabeln $u_1, \ldots, u_m$ sind umgekehrt durch die Werte der Logarithmen $l_1(\xi), \ldots, l_m(\xi)$ 2^{r_1}-deutig bestimmt, da durch letztere die r_1 reellen Werte $\xi_1, \ldots, \xi_{r_1}$ nur bis auf das Vorzeichen, dagegen die übrigen konjugiert imaginären Wertepaare $\xi_{r_1+1}, \ldots, \xi_m$ vollständig bestimmt sind.

Um die später anzuwendende Funktionaldeterminante dieses Abhängigkeitsverhältnisses zu berechnen, bezeichnen wir, wenn $f_1, \ldots, f_m$ m beliebige Funktionen der Variabeln $x_1, \ldots, x_m$ sind, die Funktionaldeterminante der

$f_1, \ldots, f_m$ bezüglich der $x_1, \ldots, x_m$ mit $\frac{f_1, \ldots, f_m}{x_1, \ldots, x_m}$; dann gelten für die absoluten Beträge die Formeln

$$\left|\frac{u_1, \ldots, u_m}{\xi_1, \ldots, \xi_m}\right| = \frac{1}{|\sqrt{d}|}, \quad \left|\frac{\xi_1, \ldots, \xi_m}{l_1(\xi), \ldots, l_m(\xi)}\right| = |\xi_1 \ldots \xi_m| = |n(\xi)|,$$

woraus durch Multiplikation der Wert von $\left|\frac{u_1, \ldots, u_m}{l_1(\xi), \ldots, l_m(\xi)}\right|$ sich ergibt.

Im folgenden werden vornehmlich die ersten r Logarithmen $l_1, \ldots, l_r$ zur Form ξ oder zu einer Zahl α betrachtet. Für die r ersten Logarithmen zu Formen ξ, η oder Zahlen α, β gelten offenbar die Gleichungen

$$\left.\begin{aligned} l_s(\xi\eta) &= l_s(\xi) + l_s(\eta) \\ l_s(\alpha\beta) &= l_s(\alpha) + l_s(\beta) \end{aligned}\right\} \qquad (s = 1, \ldots, r).$$

Nunmehr beweisen wir folgende Tatsache:

Hilfssatz 9. Im Körper k gibt es stets eine Einheit ε, welche die Bedingung

$$\gamma_1 l_1(\varepsilon) + \cdots + \gamma_r l_r(\varepsilon) \neq 0$$

erfüllt, wobei $\gamma_1, \ldots, \gamma_r$ beliebige vorgeschriebene, nicht sämtlich verschwindende reelle Konstante sind.

Beweis: Man setze, wenn ω irgendeine ganze von 0 verschiedene Zahl in k bedeutet, zur Abkürzung

$$L(\omega) = \gamma_1 l_1(\omega) + \cdots + \gamma_r l_r(\omega);$$

ferner bestimme man irgendein System von r reellen Größen $\lambda_1, \ldots, \lambda_r$, so daß $\gamma_1\lambda_1 + \cdots + \gamma_r\lambda_r = 1$ wird, und setze dann

$$\Lambda_1 = e^{\lambda_1 t}, \ldots, \Lambda_{r_1} = e^{\lambda_{r_1} t}, \Lambda_{r_1+1} = e^{\mathfrak{k}\lambda_{r_1+1} t}, \ldots, \Lambda_r = e^{\mathfrak{k}\lambda_r t},$$

wo t einen willkürlichen reellen Parameter bezeichnet. Es sind dann zwei Fälle zu unterscheiden, je nachdem sämtliche m konjugierte Körper $k^{(1)}, \ldots, k^{(m)}$ reell sind oder nicht. Im ersten Falle ordnen wir den $r = m - 1$ Körpern $k^{(1)}, \ldots, k^{(r)}$ die Größen $\Lambda_1, \ldots, \Lambda_r$ und dem übriggebliebenen letzten Körper $k^{(m)}$ die Konstante $\Lambda_m = \frac{|\sqrt{d}|}{\Lambda_1 \cdots \Lambda_{m-1}}$ zu. Im zweiten Fall ordnen wir den Körpern $k^{(1)}, \ldots, k^{(r)}$ wiederum die Größen $\Lambda_1, \ldots, \Lambda_r$ zu, dem imaginären Körper $k^{(r+1)}$ werde die Konstante $\Lambda_{r+1} = \left|\left\{\frac{\sqrt{d}}{\Lambda_1 \cdots \Lambda_{r_1} \Lambda_{r_1+1}^2 \cdots \Lambda_r^2}\right\}^{\mathfrak{k}}\right|$ zugeordnet. Endlich ordnen wir den $m - r - 1$ übriggebliebenen imaginären Körpern $k^{(r+2)}, \ldots, k^{(m)}$ bezüglich die nämlichen Konstanten zu, wie sie bereits den konjugiert imaginären Körpern zugeordnet sind; wir bezeichnen die betreffenden Konstanten mit $\Lambda_{r+2}, \ldots, \Lambda_m$. In beiden Fällen wird das Produkt

$$\Lambda_1 \cdots \Lambda_m = |\sqrt{d}|,$$

und die Konstanten $\Lambda_1, \ldots, \Lambda_m$ erfüllen mithin die Bedingungen, denen die Konstanten $\varkappa_1, \ldots, \varkappa_m$ des Satzes 42 genügen sollten.

Dem Satz 42 zufolge gibt es daher im Körper k eine von 0 verschiedene Zahl α derart, daß

$$|\alpha^{(1)}| \leqq \Lambda_1, \ldots, |\alpha^{(m)}| \leqq \Lambda_m \qquad (10)$$

und folglich zugleich $|n(\alpha)| \leqq |\sqrt{d}|$ wird. Wegen $|n(\alpha)| \geqq 1$ ist für alle Werte $s = 1, 2, \ldots, m$:

$$|\alpha^{(s)}| \geqq \frac{1}{|\alpha^{(1)}| \cdots |\alpha^{(s-1)}| \, |\alpha^{(s+1)}| \cdots |\alpha^{(m)}|};$$

wenn wir daher die Ungleichungen

$$\left|\frac{1}{\alpha^{(1)}}\right| \geqq \frac{1}{\Lambda_1}, \ldots, \left|\frac{1}{\alpha^{(m)}}\right| \geqq \frac{1}{\Lambda_m},$$

$$\Lambda_1 \cdots \Lambda_m = |\sqrt{d}|$$

berücksichtigen, so folgt

$$|\alpha^{(s)}| \geqq \frac{\Lambda_s}{|\sqrt{d}|}. \qquad (11)$$

Aus den beiden Ungleichungen (10) und (11) ergibt sich, wenn der reelle Wert von $\log|\sqrt{d}|$ mit δ bezeichnet wird,

oder

$$\left.\begin{aligned} \lambda_s t \geqq l_s(\alpha) &\geqq \lambda_s t - 2\delta \\ 0 \leqq |l_s(\alpha) - \lambda_s t| &\leqq 2\delta \end{aligned}\right\} \qquad (s = 1, 2, \ldots r),$$

woraus zu ersehen ist, daß der Ausdruck

$$\gamma_1\{l_1(\alpha) - \lambda_1 t\} + \cdots + \gamma_r\{l_r(\alpha) - \lambda_r t\} = L(\alpha) - t$$

zwischen gewissen endlichen Grenzen δ_1 und $\delta_2 > \delta_1$ liegt, welche nur von d und $\gamma_1, \ldots, \gamma_r$, dagegen nicht von dem Wert des Parameters t abhängig sind.

Es werde nun eine Größe $\Delta > \delta_2 - \delta_1$ bestimmt; bringt man dann für t der Reihe nach die Werte $t = 0, \Delta, 2\Delta, 3\Delta, \ldots$ in Anwendung, so wird man durch das beschriebene Verfahren eine unendliche Reihe von Zahlen $\alpha, \beta, \gamma, \ldots$ erhalten, deren Normen, absolut genommen, sämtlich $\leqq |\sqrt{d}|$ sind, und für welche außerdem die Bedingungen $L(\alpha) < L(\beta) < L(\gamma) < \cdots$ erfüllt sind. Da in den ganzen rationalen Zahlen, deren absolute Beträge $\leqq |\sqrt{d}|$ sind, nur eine endliche Anzahl untereinander verschiedener Ideale als Faktoren aufgehen, so kann in der unendlichen Reihe der Hauptideale (α), (β), (γ), ... nur eine endliche Anzahl verschiedener Ideale vorkommen, und es werden daher unendlich viele Male zwei dieser Ideale einander gleich. Ist etwa $(\alpha) = (\beta)$, so stellt $\varepsilon = \frac{\beta}{\alpha}$ eine Einheit dar, welche wegen $L(\varepsilon) = L(\beta) - L(\alpha) > 0$ die Bedingung unseres Hilfssatzes 9 erfüllt.

§ 20. Beweis des Satzes von der Existenz der Einheiten.

Um nunmehr den Satz 47 zu beweisen, wählen wir dem Hilfssatz 9 gemäß in k eine Einheit η_1, für welche $l_1(\eta_1) \neq 0$ ausfällt, dann eine Einheit η_2, für welche die Determinante

$$\begin{vmatrix} l_1(\eta_1), & l_1(\eta_2) \\ l_2(\eta_1), & l_2(\eta_2) \end{vmatrix} \neq 0,$$

ferner eine Einheit η_3, für welche die Determinante

$$\begin{vmatrix} l_1(\eta_1), & l_1(\eta_2), & l_1(\eta_3) \\ l_2(\eta_1), & l_2(\eta_2), & l_2(\eta_3) \\ l_3(\eta_1), & l_3(\eta_2), & l_3(\eta_3) \end{vmatrix} \neq 0$$

ausfällt usf.; man gelangt so zu einem System von Einheiten $\eta_1, \ldots, \eta_r$, für welche schließlich die Determinante

$$\begin{vmatrix} l_1(\eta_1), & \ldots, & l_1(\eta_r) \\ \cdot & \cdots & \cdot \\ l_r(\eta_1), & \ldots, & l_r(\eta_r) \end{vmatrix} \neq 0$$

ist. Infolgedessen lassen sich, wenn H eine beliebige Einheit im Körper ist, die r ersten Logarithmen zu H stets in die Gestalt

$$\begin{aligned} l_1(\mathsf{H}) &= e_1 l_1(\eta_1) + \cdots + e_r l_1(\eta_r), \\ &\cdots\cdots\cdots\cdots\cdots \\ l_r(\mathsf{H}) &= e_1 l_r(\eta_1) + \cdots + e_r l_r(\eta_r) \end{aligned}$$

bringen, wo $e_1, \ldots, e_r$ reelle Größen bedeuten. Diese Darstellung wiederum zeigt, daß

$$\begin{aligned} l_1(\mathsf{H}) &= m_1 l_1(\eta_1) + \cdots + m_r l_1(\eta_r) + E_1, \\ &\cdots\cdots\cdots\cdots\cdots \\ l_r(\mathsf{H}) &= m_1 l_r(\eta_1) + \cdots + m_r l_r(\eta_r) + E_r \end{aligned}$$

gesetzt werden kann, wo $m_1, \ldots, m_r$ die numerisch größten ganzen rationalen, bezüglich in $e_1, \ldots, e_r$ enthaltenen Zahlen bedeuten. Die Zahlen $E_1, \ldots, E_r$ sind nun ebenfalls von der Gestalt

$$\begin{aligned} E_1 &= \mu_1 l_1(\eta_1) + \cdots + \mu_r l_1(\eta_r), \\ &\cdots\cdots\cdots\cdots\cdots \\ E_r &= \mu_1 l_r(\eta_1) + \cdots + \mu_r l_r(\eta_r). \end{aligned}$$

Da hierin $\mu_1, \ldots, \mu_r$ reelle Größen $\geqq 0$ und < 1 bedeuten, so liegen die Werte $E_1, \ldots, E_r$, absolut genommen, sämtlich unterhalb einer Grenze $\varkappa$, welche nicht von H abhängig ist, d. h. die sämtlichen r ersten Logarithmen zur Einheit

$$\overline{\mathsf{H}} = \frac{\mathsf{H}}{\eta_1^{m_1} \cdots \eta_r^{m_r}}$$

liegen absolut unterhalb der Grenze $\varkappa$. Wegen $l_1(\overline{\mathsf{H}}) + \cdots + l_{r+1}(\overline{\mathsf{H}}) = 0$

liegt daher der absolute Wert von $l_{r+1}(\mathsf{H})$ unterhalb der Grenze $r\varkappa$, und mithin bestehen die Ungleichungen

$$|\overline{\mathsf{H}}^{(1)}| < e^{\varkappa}, \ \ldots, \ |\overline{\mathsf{H}}^{(r)}| < e^{\varkappa}, \quad |\overline{\mathsf{H}}^{(r+1)}| < e^{r\varkappa},$$

d. h. sämtliche konjugierten Werte der Einheit H sind absolut kleiner als die Größe $e^{r\varkappa}$.

Nach Satz 43 kann nur eine endliche Anzahl solcher Einheiten existieren. Bezeichnen wir dieselben mit $\mathsf{H}_1, \ldots, \mathsf{H}_G$, so folgt $\mathsf{H} = \mathsf{H}_S$ oder $\mathsf{H} = \mathsf{H}_S \eta_1^{m_1} \cdots \eta_r^{m_r}$, wo S einen der Werte $1, 2, \ldots, G$ hat. Ist H_T eine beliebige jener G Einheiten $\mathsf{H}_1, \ldots, \mathsf{H}_G$, und bildet man die ersten $G+1$ Potenzen von H_T, so werden nach dem eben Bewiesenen zwei geeignete von diesen Potenzen sich in der Gestalt $\mathsf{H}_S \eta_1^{m_1'} \cdots \eta_r^{m_r'}$ bezüglich $\mathsf{H}_S \eta_1^{m_1''} \cdots \eta_r^{m_r''}$ darstellen, wo H_S beidemal die gleiche jener G Einheiten bezeichnet; ihr Quotient besitzt mithin eine Darstellung von der Gestalt $\eta_1^{m_1} \cdots \eta_r^{m_r}$. Hiermit ist bewiesen, daß für jede Einheit H_T ein Exponent M_T existiert derart, daß $\mathsf{H}_T^{M_T}$ ein Produkt von Potenzen der Einheiten $\eta_1, \ldots, \eta_r$ ist. Bezeichnen wir das kleinste gemeinschaftliche Vielfache aller G Exponenten $M_1, \ldots, M_G$ mit M, so hat dieser Exponent M für alle G Einheiten $\mathsf{H}_1, \ldots, \mathsf{H}_G$ zugleich jene Eigenschaft, und hieraus folgt, daß die r ersten Logarithmen zu einer jeden beliebigen Einheit H des Körpers k die Darstellung

$$\left.\begin{aligned} l_1(\mathsf{H}) &= \frac{m_1 l_1(\eta_1) + \cdots + m_r l_1(\eta_r)}{M}, \\ &\cdots\cdots\cdots\cdots\cdots \\ l_r(\mathsf{H}) &= \frac{m_1 l_r(\eta_1) + \cdots + m_r l_r(\eta_r)}{M} \end{aligned}\right\} \qquad (12)$$

gestatten, wo $m_1, \ldots, m_r$ ganze rationale Zahlen sind.

Nunmehr wenden wir auf dieses unendliche System (12) der Logarithmen aller Einheiten die nämliche Schlußweise an, wie sie in Satz 5 (§ 3) zum Beweise der Existenz einer Körperbasis auseinandergesetzt worden ist; dann folgt, daß es ein System von r Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ gibt, durch deren zugehörige Logarithmen die Logarithmen zu jeder beliebigen Einheit H des Körpers sich in der Gestalt

$$\begin{aligned} l_1(\mathsf{H}) &= a_1 l_1(\varepsilon_1) + \cdots + a_r l_1(\varepsilon_r), \\ &\cdots\cdots\cdots\cdots\cdots \\ l_r(\mathsf{H}) &= a_1 l_r(\varepsilon_1) + \cdots + a_r l_r(\varepsilon_r) \end{aligned}$$

ausdrücken lassen, wo $a_1, \ldots, a_r$ *ganze* rationale Zahlen sind. Dieses System von Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ genügt den Bedingungen des Satzes 47.

In der Tat: ist H eine beliebige Einheit, deren zugehörige Logarithmen obige Gestalt besitzen, so ist $\varrho = \frac{\mathsf{H}}{\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}}$ eine Einheit, deren zugehörige Logarithmen offenbar sämtlich $= 0$ sind. Eine solche Einheit ϱ ist notwendig eine Einheitswurzel. Denn nach dem vorhin Bewiesenen ist $\varrho^M = \eta_1^{m_1} \cdots \eta_r^{m_r}$,

wo $m_1, \ldots, m_r$ gewisse ganze rationale Zahlen sind. Durch Übergang zu den Logarithmen folgt daraus

$$\begin{aligned} m_1 l_1(\eta_1) + \cdots + m_r l_1(\eta_r) &= 0, \\ \cdots\cdots\cdots\cdots\cdots & \\ m_1 l_r(\eta_1) + \cdots + m_r l_r(\eta_r) &= 0, \end{aligned}$$

d. h. $m_1 = 0, \ldots, m_r = 0$ und $\varrho^M = 1$. Hieraus ergibt sich die Darstellung der Einheit $\mathfrak{H}$, welche unser Satz 47 verlangt.

Aus der Bestimmungsweise der Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ folgt leicht:

$$\begin{vmatrix} l_1(\eta_1), \ldots, l_1(\eta_r) \\ \cdots\cdots\cdots \\ l_r(\eta_1), \ldots, l_r(\eta_r) \end{vmatrix} = AR,$$

wo A eine ganze rationale Zahl bedeutet und zur Abkürzung

$$R = \begin{vmatrix} l_1(\varepsilon_1), \ldots, l_1(\varepsilon_r) \\ \cdots\cdots\cdots \\ l_r(\varepsilon_1), \ldots, l_r(\varepsilon_r) \end{vmatrix}$$

gesetzt ist. Diese Determinante R ist $\neq 0$, und hieraus folgt, daß die Darstellung der Einheit $\mathfrak{H}$ durch die Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ nur auf eine Weise geschehen kann. Der Beweis des fundamentalen Satzes 47 ist somit in allen Teilen erbracht.

§ 21. Die Grundeinheiten. Der Regulator des Körpers. Ein System von unabhängigen Einheiten.

Das System der Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ mit der in Satz 47 dargelegten Eigenschaft heißt ein **System von Grundeinheiten** des Körpers k. Es folgt leicht, daß wenn $\varepsilon_1^*, \ldots, \varepsilon_r^*$ ein anderes System von Grundeinheiten bedeutet, die Determinante aus den zugehörigen r Systemen von je r ersten Logarithmen bis auf das Vorzeichen mit R übereinstimmt. Wir wählen die Reihenfolge der Grundeinheiten stets so, daß R eine positive Zahl wird. Die Zahl R ist dann durch den Körper k eindeutig bestimmt und wird der **Regulator des Körpers** k genannt.

Beim obigen Beweise des Hauptsatzes 47 erkannten wir zugleich, daß eine Einheit, deren zugehörige Logarithmen sämtlich $= 0$ sind, notwendig eine Einheitswurzel ist. Diese Tatsache erhält in dem folgenden Satz Ausdruck, welcher sich übrigens auch in unmittelbarer Weise leicht begründen läßt [Kronecker (6), Minkowski (3)]:

Satz 48. Eine jede Einheit, die selbst und deren Konjugierte sämtlich den absoluten Betrag 1 besitzen, ist eine Einheitswurzel.

Da in jedem Zahlkörper die beiden Einheitswurzeln $+1$ und -1 vorkommen, so ist die Anzahl aller Einheitswurzeln in k stets gerade; sie kann offenbar nur dann > 2 sein, wenn alle m konjugierten Körper imaginär sind.

Ein beliebiges System von t Einheiten $\eta_{l_1}, \ldots, \eta_{l_t}$ heißt ein **System von t unabhängigen Einheiten,** wenn zwischen denselben keine Gleichung von der Gestalt $\eta_{l_1}^{m_1} \cdots \eta_{l_t}^{m_t} = 1$ besteht, wo $m_1, \ldots, m_t$ ganze rationale, nicht sämtlich verschwindende Zahlen sind. Die Zahl t ist stets $\leq r$; insbesondere bilden die Grundeinheiten $\varepsilon_1, \ldots, \varepsilon_r$ ein System von r unabhängigen Einheiten. Hat man andererseits irgendein System von r unabhängigen Einheiten $\eta_{l_1}, \ldots, \eta_{l_r}$, so existiert stets eine ganze rationale Zahl M von der Art, daß für jede beliebige Einheit ε des Körpers k eine Gleichung von der Gestalt $\varepsilon^M = \eta_{l_1}^{m_1} \ldots \eta_{l_r}^{m_r}$ gilt, wo die Exponenten $m_1, \ldots, m_r$ ganze rationale Zahlen sind. Ist nämlich $\eta_{l_s} = \varrho_s \varepsilon_1^{a_{1s}} \ldots \varepsilon_r^{a_{rs}}$ für $s = 1, 2, \ldots, r$, wo ϱ_s Einheitswurzeln und $a_{1s}, \ldots, a_{rs}$ ganzzahlige Exponenten sind, so ist die Determinante der ganzzahligen Exponenten $a_{11}, \ldots, a_{rr}$ wegen der vorausgesetzten Unabhängigkeit der Einheiten $\eta_{l_1}, \ldots, \eta_{l_r}$ notwendig $\neq 0$. Wird diese Determinante A genannt, so folgt, daß die A-te Potenz jeder beliebigen Einheit ε des Körpers gleich einem Produkt von Potenzen der Einheiten $\eta_{l_1}, \ldots, \eta_{l_r}$, multipliziert in eine Einheitswurzel ϱ, wird. Ist $\varrho^E = 1$ für alle Einheitswurzeln ϱ in k, so ist offenbar die ganze Zahl $M = AE$ von der gewünschten Beschaffenheit.

Der obige Beweis unseres Hauptsatzes 47 zeigt zugleich die Möglichkeit, die Grundeinheiten $\varepsilon_1, \ldots, \varepsilon_r$ durch eine endliche Anzahl von rationalen Operationen aufzustellen. Die eingehendere Behandlung der Frage nach der einfachsten Berechnung der Einheiten führt auf die Theorie der kettenbruchähnlichen Algorithmen, wobei dann die weitere Frage nach der Periodizität solcher Entwicklungen im Vordergrund des Interesses steht [Minkowski (3, 4)].

7. Die Idealklassen des Körpers.

§ 22. Die Idealklasse. Die Endlichkeit der Anzahl der Idealklassen.

Jede ganze Zahl des Zahlkörpers k bestimmt ein Hauptideal; jede **gebrochene,** d. h. nicht ganze Zahl $\varkappa$ in k ist der Quotient zweier ganzen Zahlen α und β und somit als Quotient zweier Ideale $\mathfrak{a}$ und $\mathfrak{b}$ darstellbar: $\varkappa = \frac{\alpha}{\beta} = \frac{\mathfrak{a}}{\mathfrak{b}}$. Denken wir die Ideale $\mathfrak{a}$ und $\mathfrak{b}$ von allen gemeinsamen Idealfaktoren befreit, so ist diese Darstellung der gebrochenen Zahl $\varkappa$ als Idealquotient eine eindeutig bestimmte. Ist umgekehrt der Quotient $\frac{\mathfrak{a}}{\mathfrak{b}}$ zweier Ideale $\mathfrak{a}$ und $\mathfrak{b}$ — mögen dieselben einen gemeinsamen Teiler haben oder nicht — gleich einer ganzen oder gebrochenen Zahl $\varkappa = \frac{\alpha}{\beta}$ des Körpers, so werden die beiden Ideale $\mathfrak{a}$ und $\mathfrak{b}$ einander **äquivalent** genannt, d. i. in Zeichen $\mathfrak{a} \sim \mathfrak{b}$. Aus $\frac{\alpha}{\beta} = \frac{\mathfrak{a}}{\mathfrak{b}}$ folgt $(\beta)\mathfrak{a} = (\alpha)\mathfrak{b}$, und somit erkennen wir, daß zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ dann und nur dann einander äquivalent sind, wenn sie durch Multiplikation mit gewissen Hauptidealen in ein und das nämliche Ideal übergehen. Die Gesamtheit aller Ideale, welche einem gegebenen Ideal äquivalent sind, heißt eine **Idealklasse.**

Alle Hauptideale sind dem Ideal (1) äquivalent. Die durch sie gebildete Klasse heißt die **Hauptklasse** und wird mit 1 bezeichnet. Wenn $\mathfrak{a} \sim \mathfrak{a}'$ und $\mathfrak{b} \sim \mathfrak{b}'$ ist, so ist $\mathfrak{a}\mathfrak{a}' \sim \mathfrak{b}\mathfrak{b}'$. Ist A eine das Ideal $\mathfrak{a}$ enthaltende Idealklasse und B eine das Ideal $\mathfrak{b}$ enthaltende Klasse, so wird die Idealklasse, welche das Ideal $\mathfrak{a}\mathfrak{b}$ enthält, das **Produkt der Idealklassen** A und B genannt und mit AB bezeichnet. Es ist offenbar $1\,B = B$, und umgekehrt folgt aus $AB = B$ notwendig $A = 1$.

Es ist bisweilen vorteilhaft, auch Idealquotienten in die Rechnung einzuführen: eine Gleichung von der Gestalt $\frac{\mathfrak{a}}{\mathfrak{a}'} = \frac{\mathfrak{b}}{\mathfrak{b}'}$ oder eine Äquivalenz von der Gestalt $\frac{\mathfrak{a}}{\mathfrak{a}'} \sim \frac{\mathfrak{b}}{\mathfrak{b}'}$ soll gleichbedeutend sein mit derjenigen Gleichung oder Äquivalenz zwischen Idealen, welche daraus durch Multiplikation mit den in den Nennern stehenden Idealen hervorgeht, d. h. mit der Gleichung $\mathfrak{a}\mathfrak{b}' = \mathfrak{a}'\mathfrak{b}$ bez. mit der Äquivalenz $\mathfrak{a}\mathfrak{b}' \sim \mathfrak{a}'\mathfrak{b}$.

Es gilt der Satz:

Satz 49. Es gibt stets eine und nur eine Idealklasse B, die, mit einer gegebenen Idealklasse A multipliziert, die Hauptklasse ergibt.

Beweis. Ist $\mathfrak{a}$ ein Ideal der Klasse A und α eine durch $\mathfrak{a}$ teilbare ganze Zahl, so daß $\alpha = \mathfrak{a}\mathfrak{b}$ gesetzt werden kann, so ist, wenn B die Klasse des Ideals $\mathfrak{b}$ bezeichnet, $AB = 1$. Gäbe es nun noch eine andere Klasse B' so, daß $AB' = 1$ ist, so folgt durch Multiplikation mit B die Gleichung $ABB' = B' = B$.

Die Klasse B heißt die zu A **reziproke Klasse** und wird mit A^{-1} bezeichnet.

Es gilt ferner die folgende fundamentale Tatsache:

Satz 50. In jeder Idealklasse gibt es ein Ideal, dessen Norm die absolut genommene Quadratwurzel aus der Körperdiskriminante nicht übersteigt [Minkowski (*1*, *3*)]. Die Anzahl der Idealklassen eines Zahlkörpers ist endlich [Dedekind (*1*), Kronecker (*16*)].

Beweis. Ist A eine beliebige Idealklasse und $\mathfrak{j}$ ein Ideal der reziproken Klasse A^{-1}, so gibt es nach Satz 46 eine ganze, durch $\mathfrak{j}$ teilbare Zahl ι, deren Norm der Bedingung $|n(\iota)| \leqq n(\mathfrak{j})\,|\sqrt{d}|$ genügt. Setzen wir $\iota = \mathfrak{j}\,\mathfrak{a}$, so gehört $\mathfrak{a}$ der Idealklasse A an, und wegen $|n(\iota)| = n(\mathfrak{j})\,n(\mathfrak{a})$ ist $n(\mathfrak{a}) \leqq |\sqrt{d}|$. Es gibt also in der Klasse A ein der letzteren Bedingung genügendes Ideal $\mathfrak{a}$; da aber in den ganzen rationalen Zahlen, welche $\leqq |\sqrt{d}|$ sind, nur eine endliche Anzahl unter einander verschiedener Ideale als Faktoren enthalten ist, so folgt auch die Richtigkeit des zweiten Teiles des Satzes 50.

§ 23. Anwendungen des Satzes von der Endlichkeit der Klassenanzahl.

Der eben bewiesene Satz 50 gestattet mannigfache Folgerungen und Anwendungen, von denen die nachstehenden hervorzuheben sind:

Satz 51. Ist h die Anzahl der Idealklassen, so liefert die h-te Potenz einer jeden Klasse stets die Hauptklasse.

Beweis. In der Reihe $A, A^2, \ldots, A^{h+1}$ stimmen notwendig zwei Klassen, etwa A^r und A^{r+e}, miteinander überein. Aus $A^r A^e = A^r$ folgt $A^e = 1$. Ist e zugleich der kleinste Exponent (> 0) von der Beschaffenheit, daß $A^e = 1$ wird, so folgt, daß die e Klassen $A^0 = 1, A, \ldots, A^{e-1}$ sämtlich untereinander verschieden sind. Ist B eine von diesen e Klassen verschiedene Klasse, so sind die e Klassen $B, AB, \ldots, A^{e-1}B$ wiederum sämtlich untereinander und von den e vorigen Klassen verschieden; die Fortsetzung dieses Verfahrens zeigt, daß h ein Vielfaches von e sein muß, und hieraus folgt der zu beweisende Satz 51.

Die h-te Potenz eines jeden beliebigen Ideals $\mathfrak{a}$ ist nach diesem Satz stets ein Hauptideal.

Satz 52. Wenn α und β beliebige ganze Zahlen sind, so gibt es stets eine sowohl in α wie in β aufgehende ganze von 0 verschiedene Zahl γ, welche eine Darstellung $\gamma = \xi\alpha + \eta\beta$ gestattet, wo ξ, η geeignet gewählte ganze Zahlen sind. Die Zahlen γ, ξ, η gehören im allgemeinen nicht dem durch α und β bestimmten Zahlkörper an [Dedekind (*1*)].

Satz 53. Es seien $\varkappa, \varrho$ und $\varkappa^*, \varrho^*$ zwei Zahlenpaare des Körpers k; damit $\mathfrak{j} = (\varkappa, \varrho) = (\varkappa^*, \varrho^*)$ werde, ist es notwendig und hinreichend, daß man im Körper k vier ganze Zahlen $\alpha, \beta, \gamma, \delta$ finden kann, deren Determinante $\alpha\delta - \beta\gamma = 1$ ist, und durch welche die Gleichungen

$$\varkappa^* = \alpha\varkappa + \beta\varrho,$$
$$\varrho^* = \gamma\varkappa + \delta\varrho$$

erfüllt sind [Hurwitz (*4*)].

Beweis. Daß die genannte Bedingung hinreichend ist, folgt aus dem Umstande, daß diese beiden Gleichungen eine Umkehrung von der Gestalt

$$\varkappa = \alpha^*\varkappa^* + \beta^*\varrho^*,$$
$$\varrho = \gamma^*\varkappa^* + \delta^*\varrho^*$$

gestatten, wo $\alpha^*, \beta^*, \gamma^*, \delta^*$ ganze Zahlen sind. Die Bedingung ist ferner auch notwendig. Bezeichnet nämlich h die Anzahl der Idealklassen, so wird $\mathfrak{j}^h = (\varkappa^h, \varrho^h) = (\varkappa^{*h}, \varrho^{*h}) = (\tau)$, wo τ eine ganze Zahl des Körpers k ist. Es sei

$$\tau = \mu\varkappa^h + \nu\varrho^h = \mu^*\varkappa^{*h} + \nu^*\varrho^{*h},$$

wo μ, ν, μ^*, ν^* ganze Zahlen in k sind; dann erfüllen offenbar die vier ganzen Zahlen

$$\alpha = \frac{\mu\varkappa^*\varkappa^{h-1} + \nu^*\varrho\varrho^{*h-1}}{\tau}, \qquad \beta = \frac{\nu\varkappa^*\varrho^{h-1} - \nu^*\varkappa\varrho^{*h-1}}{\tau},$$
$$\gamma = \frac{\mu\varrho^*\varkappa^{h-1} - \mu^*\varrho\varkappa^{*h-1}}{\tau}, \qquad \delta = \frac{\nu\varrho^*\varrho^{h-1} + \mu^*\varkappa\varkappa^{*h-1}}{\tau}$$

die Bedingung des Satzes 53. Daß $\alpha\delta - \beta\gamma = 1$ ist, ergibt sich, wenn man die beiden Determinanten

$$-\tau = \begin{vmatrix} \mu\varkappa^{h-1}, & \varrho \\ \nu\varrho^{h-1}, & -\varkappa \end{vmatrix} \quad \text{und} \quad -\tau = \begin{vmatrix} \varkappa^*, & \nu^*\varrho^{*h-1} \\ \varrho^*, & -\mu^*\varkappa^{*h-1} \end{vmatrix}$$

nach dem Multiplikationssatze miteinander zusammensetzt.

Nach Satz 12 kann ein jedes Ideal in der Gestalt $\mathfrak{j} = (\varkappa, \varrho)$ dargestellt werden. Setzen wir $\vartheta = \frac{\varkappa}{\varrho}$, so bestimmt die ganze oder gebrochene Zahl ϑ vollständig die Idealklasse, zu welcher $\mathfrak{j}$ gehört. Wir nennen ϑ einen dieser Idealklasse zugeordneten **Zahlbruch.** Der Satz 53 zeigt, daß, wenn $\vartheta^* = \frac{\varkappa^*}{\varrho^*}$ ein anderer der Idealklasse zugeordneter Zahlbruch ist, notwendig vier ganze Zahlen $\alpha, \beta, \gamma, \delta$ mit der Determinante 1 im Körper k existieren müssen derart, daß $\vartheta^* = \frac{\alpha\vartheta + \beta}{\gamma\vartheta + \delta}$ wird.

§ 24. Aufstellung des Systems der Idealklassen. Engere Fassung des Klassenbegriffes.

Der Beweis des Satzes 50 gibt uns zugleich ein einfaches Mittel an die Hand, durch eine endliche Anzahl rationaler Prozesse ein volles System von nicht äquivalenten Idealen für jeden gegebenen Körper wirklich aufzustellen. Man braucht nur alle diejenigen Ideale in Betracht zu ziehen, deren Normen $\leqq |\sqrt{d}|$ sind. Um die zwischen diesen Idealen irgend vorhandenen Äquivalenzen sämtlich zu ermitteln, haben wir nur nötig, jedes von ihnen mit jedem zu multiplizieren und dann, wenn $\mathfrak{j}$ ein solches Produkt bedeutet, jedesmal in $\mathfrak{j}$ eine Zahl $\iota \neq 0$ mit absolut kleinster Norm aufzusuchen, um zu sehen, ob $\mathfrak{j} = (\iota)$ ist und somit die Faktoren reziproken Klassen angehören. Daß dies ebenfalls nur eine endliche Anzahl von Operationen erfordert, erkennen wir aus dem Satze 46. Ist nämlich $\iota_1, \ldots, \iota_m$ die Basis des Ideals $\mathfrak{j}$, so haben wir nur nötig, $u_1, \ldots, u_m$ als ganze rationale, nicht sämtlich verschwindende Zahlen so zu bestimmen, daß die absoluten Werte der reellen und imaginären Teile von $u_1 \iota_1^{(s)} + \cdots + u_m \iota_m^{(s)}$ für $s = 1, \ldots, m$ sämtlich unter gewissen gegebenen Grenzen bleiben. Hierzu bedarf es nur einer endlichen Anzahl von Versuchen. Auf gleiche Weise sehen wir auch ein, daß für jedes vorgelegte Ideal die Klasse, der dasselbe angehört, stets durch eine endliche Anzahl von rationalen Operationen bestimmt werden kann.

Es werde bemerkt, daß unter Umständen auch eine **engere Fassung des Äquivalenz- und Klassenbegriffes** von Nutzen ist, indem zwei Ideale nur dann äquivalent heißen, wenn ihr Quotient eine ganze oder gebrochene Zahl mit positiver Norm ist [DEDEKIND (*I*)].

§ 25. Ein Hilfssatz über den asymptotischen Wert der Anzahl aller Hauptideale, welche durch ein festes Ideal teilbar sind.

Nach dem Vorbilde von DIRICHLET, welcher die Anzahl der Klassen von binären quadratischen Formen mit gegebener Determinante auf transzendentem Wege ausgedrückt hat [DIRICHLET (7,8)], und auf Grund der in Kapitel 6 erhaltenen Resultate über die Einheiten eines Zahlkörpers gelang es

DEDEKIND, eine fundamentale Formel abzuleiten, vermöge welcher sich die Anzahl h der Idealklassen eines beliebigen Zahlkörpers als Grenzwert einer gewissen unendlichen Reihe darstellt [DEDEKIND (*I*)]. Um zu dieser Formel zu gelangen, beweisen wir zunächst folgenden Hilfssatz:

Hilfssatz 10. Ist t eine reelle positive Veränderliche und T die Anzahl aller derjenigen durch das gegebene Ideal $\mathfrak{a}$ teilbaren Hauptideale, deren Normen $\leqq t$ sind, so ist

$$\lim_{t=\infty} \frac{T}{t} = \frac{2^{r_1+r_2}\pi^{r_2}}{w} \cdot \frac{1}{n(\mathfrak{a})} \cdot \frac{R}{|\sqrt{d}|},$$

wo w die Anzahl der in k vorkommenden Einheitswurzeln und R den Regulator des Körpers k bezeichnet. Die Bedeutung von r_1, r_2 ist in Satz 47 erklärt. L dient zur Abkürzung für Limes.

Beweis. Es sei $\alpha_1, \ldots, \alpha_m$ eine Basis des Ideals $\mathfrak{a}$; jede durch $\mathfrak{a}$ teilbare ganze Zahl besitzt dann die Gestalt:

$$\eta = \eta(v) = v_1\alpha_1 + \cdots + v_m\alpha_m = f_1(v)\,\omega_1 + \cdots + f_m(v)\,\omega_m,$$

wo $v_1, \ldots, v_m$ ganze rationale Werte annehmen und $f_1(v), \ldots, f_m(v)$ lineare ganzzahlige Funktionen der $v_1, \ldots, v_m$ sind. Wenn wir $v_1, \ldots, v_m$ als reelle Veränderliche ansehen und

$$u_1 = \frac{f_1(v)}{\left|\sqrt[m]{n(\eta)}\right|}, \quad \ldots, \quad u_m = \frac{f_m(v)}{\left|\sqrt[m]{n(\eta)}\right|},$$

$$\xi = \xi(v) = u_1\omega_1 + \cdots + u_m\omega_m = \frac{\eta(v)}{\left|\sqrt[m]{n(\eta)}\right|}$$

setzen, so sind $u_1, \ldots, u_m$ eindeutige Funktionen von $v_1, \ldots, v_m$, und ξ ist eine Form, für welche $n(\xi) = \pm 1$ wird. Wir berechnen nun die r ersten Logarithmen zur Form ξ und hieraus r reelle Größen $e_1(\xi), \ldots, e_r(\xi)$ derart, daß, wenn $\varepsilon_1, \ldots, \varepsilon_r$ ein System von Grundeinheiten bezeichnen,

$$\begin{aligned} l_1(\xi) &= e_1(\xi)\,l_1(\varepsilon_1) + \cdots + e_r(\xi)\,l_1(\varepsilon_r), \\ &\cdots\cdots\cdots\cdots \\ l_r(\xi) &= e_1(\xi)\,l_r(\varepsilon_1) + \cdots + e_r(\xi)\,l_r(\varepsilon_r) \end{aligned}$$

ist; diese r Größen $e_1, \ldots, e_r$ werden in diesem § 25 kurz die r Exponenten von η genannt.

Nimmt man für $v_1, \ldots, v_m$ ganze rationale, nicht sämtlich verschwindende Zahlen, so ist klar, daß die so entstehende ganze Zahl η stets durch Multiplikation mit ganzen Potenzen der Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ in eine solche Zahl verwandelt werden kann, deren Exponenten $e_1, \ldots, e_r$ den Bedingungen

$$0 \leqq e_1 < 1, \quad \ldots, \quad 0 \leqq e_r < 1 \tag{13}$$

genügen. Umgekehrt sehen wir, daß zwei ganze Zahlen η, η^*, deren Normen und Exponenten gleich sind, sich nur um einen Faktor unterscheiden können, welcher eine Einheitswurzel ist. Wenn daher w die Anzahl der in k liegenden

Einheitswurzeln bezeichnet, so ist das w-fache der Anzahl T aller durch $\mathfrak{a}$ teilbaren Hauptideale mit einer Norm $\leqq t$ notwendig gleich der Anzahl der verschiedenen Systeme von ganzzahligen Wertsystemen $v_1, \ldots, v_m$, für welche $|n(\eta)| \leqq t$ ausfällt, und für welche überdies die Exponenten $e_1, \ldots, e_r$ den Bedingungen (13) genügen.

Nunmehr setzen wir

$$\tau = t^{-\frac{1}{m}}, \quad v_1 = \frac{\varphi_1}{\tau}, \ \ldots, \ v_m = \frac{\varphi_m}{\tau};$$

dabei bleiben die Form ξ und folglich auch die Größen $l_1(\xi), \ldots, l_r(\xi)$, $e_1, \ldots, e_r$ von τ unabhängig und enthalten lediglich die m neuen Veränderlichen $\varphi_1, \ldots, \varphi_m$. Die Ungleichung $|n(\eta)| \leqq t$ geht in $|n(\eta(\varphi))| \leqq 1$ über; da ferner in Folge der Bedingungen (13) die r Logarithmen $l_1(\xi), \ldots, l_r(\xi)$ und folglich wegen $l_1(\xi) + \cdots + l_{r+1}(\xi) = ln(\xi) = 0$ auch der Logarithmus $l_{r+1}(\xi)$ absolut unter einer endlichen, durch $\varepsilon_1, \ldots, \varepsilon_r$ bestimmten Grenze liegen, so folgt das Gleiche für die sämtlichen Größen $|\xi^{(1)}(\varphi)|, \ldots, |\xi^{(m)}(\varphi)|$, und damit liegen wegen $|n(\eta(\varphi))| \leqq 1$ auch die m Größen $|\eta^{(1)}(\varphi)|, \ldots, |\eta^{(m)}(\varphi)|$ sämtlich unterhalb einer endlichen Grenze. Hieraus folgt, daß die Ungleichungen (13) unter Zuhilfenahme der Ungleichung $|n(\eta(\varphi))| \leqq 1$ in dem durch die m Koordinaten $\varphi_1, \ldots, \varphi_m$ bestimmten m-dimensionalen Raume ein endliches Raumgebiet abgrenzen.

Bedenken wir nun, daß nach den Ausführungen in § 19 S. 103 die Funktionswerte $l_1(\eta), \ldots, l_m(\eta)$ die Werte der Variabeln $\varphi_1, \ldots, \varphi_m$ 2^{r_1}-deutig bestimmen, so ist nach der Definition des Begriffs eines vielfachen Integrals

$$\lim_{t=0} \{w T \tau^m\} = 2^{r_1} \int\int \ldots \int d\varphi_1 d\varphi_2 \ldots d\varphi_m,$$

wo das Integral rechter Hand über das durch die Ungleichungen

$$0 \leqq e_1 \leqq 1, \ \ldots, \ 0 \leqq e_r \leqq 1, \quad |n(\eta(\varphi))| \leqq 1$$

bestimmte m-dimensionale Raumgebiet zu erstrecken ist und daher einen endlichen bestimmten Wert besitzt.

Um diesen Wert zu ermitteln, führen wir statt der Integrationsveränderlichen $\varphi_1, \ldots, \varphi_m$ die neuen Veränderlichen

$$\psi_1 = e_1(\xi), \ldots, \psi_r = e_r(\xi), \quad \psi_{r+1} = |n(\eta)|, \quad \psi_{r+2} = l_{r+2}(\xi), \ \ldots, \ \psi_m = l_m(\xi)$$

ein, wo ξ und η von $\varphi_1, \ldots, \varphi_m$ abhängig zu nehmen sind. Da diese m Größen sämtlich analytische und in dem Integrationsgebiet

$$0 \leqq \psi_1 \leqq 1, \ \ldots, \ 0 \leqq \psi_r \leqq 1, \quad 0 \leqq \psi_{r+1} \leqq 1,$$
$$0 \leqq \psi_{r+2} \leqq 2\pi, \ \ldots, \ 0 \leqq \psi_m \leqq 2\pi$$

sich regulär verhaltende, eindeutige Funktionen von $\varphi_1, \ldots, \varphi_m$ sind, so ist

$$\int \ldots \int d\varphi_1 \ldots d\varphi_m = \int \ldots \int \left| \frac{\varphi_1, \ldots, \varphi_m}{\psi_1, \ldots, \psi_m} \right| d\psi_1 \ldots d\psi_m.$$

Nach den Ausführungen in § 19 S. 104 ist

$$\left| \frac{f_1, \ldots, f_m}{l_1(\eta), \ldots, l_m(\eta)} \right| = \left| \frac{n(\eta)}{\sqrt{d}} \right|.$$

Ferner bestehen wegen

$$ln(\eta) = l_1(\eta) + \cdots + l_{r+1}(\eta), \qquad l_s(\xi) = l_s(\eta) - \frac{1}{m} ln(\eta)$$
$$(s = 1, 2, \ldots, r)$$

offenbar die Beziehungen:

$$\left| \frac{l_1(\eta), \ldots, l_r(\eta), l_{r+1}(\eta)}{l_1(\eta), \ldots, l_r(\eta), ln(\eta)} \right| = 1, \qquad \left| \frac{l_1(\eta), \ldots, l_r(\eta), ln(\eta)}{l_1(\xi), \ldots, l_r(\xi), ln(\eta)} \right| = 1;$$

und da endlich

$$l_{r+2}(\eta) = l_{r+2}(\xi), \ \ldots, \ l_m(\eta) = l_m(\xi),$$
$$\left| \frac{ln(\eta)}{n(\eta)} \right| = \frac{1}{|n(\eta)|}, \qquad \left| \frac{\varphi_1, \ldots, \varphi_m}{f_1(\varphi), \ldots, f_m(\varphi)} \right| = \frac{1}{n(\mathfrak{a})}, \qquad \left| \frac{l_1(\xi), \ldots, l_r(\xi)}{\psi_1, \ldots, \psi_r} \right| = R$$

ist, so ergibt sich durch Multiplikation sämtlicher Gleichungen

$$\left| \frac{\varphi_1, \ldots, \varphi_m}{\psi_1, \ldots, \psi_m} \right| = \frac{R}{n(\mathfrak{a})\sqrt{d}}.$$

Das obige Integral besitzt daher den Wert $\frac{(2\pi)^{r_2} R}{n(\mathfrak{a})\sqrt{d}}$; hiermit ist der Beweis für den Hilfssatz 10 erbracht.

Wir setzen im folgenden zur Abkürzung

$$\varkappa = \frac{2^{r_1+r_2}\pi^{r_2}}{w} \cdot \frac{R}{\sqrt{d}},$$

so daß $\varkappa$ eine durch den Körper allein bestimmte und für diesen charakteristische Größe bedeutet.

§ 26. Die Bestimmung der Klassenanzahl durch das Residuum der Funktion $\zeta(s)$ für $s = 1$.

Satz 54. Wenn T die Anzahl aller Ideale einer Klasse A bedeutet, deren Normen $\leqq t$ ausfallen, so ist

$$\lim_{t=\infty} \frac{T}{t} = \varkappa.$$

Beweis. Ist $\mathfrak{a}$ ein Ideal der zu A reziproken Klasse A^{-1}, und durchläuft $\mathfrak{x}$ alle Ideale der Klasse A, so stellt das Produkt $\mathfrak{x}\mathfrak{a}$ alle durch $\mathfrak{a}$ teilbaren Hauptideale und jedes nur einmal dar. Setzen wir daher in der Formel des Hilfssatzes $10\, t = n(\mathfrak{a})t'$, so bedeutet T zugleich die Anzahl der Ideale $\mathfrak{x}$ in A, für welche $n(\mathfrak{x}) \leqq t'$ ist. Nach Fortheben des Faktors $n(\mathfrak{a})$ folgt die zu beweisende Formel für $t = t'$.

Da die Zahl $\varkappa$ von der Wahl der Klasse A unabhängig ist, so ergibt sich unmittelbar aus Satz 54 die folgende Tatsache:

Satz 55. Ist T die Anzahl aller Ideale des Körpers k, deren Normen $\leqq t$ ausfallen, und bedeutet h die Anzahl der Idealklassen, so ist

$$\lim_{t=\infty} \frac{T}{t} = h\varkappa .$$

Aus dieser Formel kann mit Hilfe analytischer Methoden ein fundamentaler Ausdruck für die Klassenanzahl h abgeleitet werden. Es ergibt sich nämlich folgende Tatsache:

Satz 56. *Die unendliche Reihe*

$$\zeta(s) = \sum_{(\mathfrak{j})} \frac{1}{n(\mathfrak{j})^s},$$

in welcher $\mathfrak{j}$ *alle Ideale des Körpers durchläuft, konvergiert für reelle Werte von* $s > 1$, *und es ist*

$$\lim_{s=1} \{(s-1)\,\zeta(s)\} = h\varkappa .$$

[Dedekind (*1*)].

Beweis. Bezeichnen wir mit $F(n)$ die Anzahl der verschiedenen Ideale mit der Norm n, so ist offenbar, wenn T die in Satz 55 angegebene Bedeutung hat,

$$\lim_{t=\infty} \frac{T}{t} = \lim_{n=\infty} \frac{F(1) + F(2) + \cdots + F(n)}{n}.$$

Der Limes rechter Hand kann nun, wie folgt, als Grenzwert einer unendlichen Reihe dargestellt werden [Dirichlet (*15*)]. Wir ordnen die sämtlichen Ideale $\mathfrak{j}$ des Körpers nach der Größe ihrer Normen, schreiben die entstehende Reihe $\mathfrak{j}_1, \mathfrak{j}_2, \ldots, \mathfrak{j}_t, \ldots$ und bezeichnen allgemein die Norm von $\mathfrak{j}_t$ mit n_t, dann ist

$$F(1) + \cdots + F(n_t - 1) < t \leqq F(1) + \cdots + F(n_t)$$

oder

$$\frac{F(1) + \cdots + F(n_t - 1)}{n_t - 1}\left(1 - \frac{1}{n_t}\right) < \frac{t}{n_t} \leqq \frac{F(1) + \cdots + F(n_t)}{n_t},$$

und hieraus folgt nach Satz 55: $\lim_{t=\infty} \frac{t}{n_t} = h\varkappa$, d. h.: wie klein auch die positive Größe δ gegeben sein mag, es ist stets möglich, die ganze Zahl t so groß zu wählen, daß die Ungleichungen

$$\frac{h\varkappa - \delta}{t'} < \frac{1}{n_{t'}} < \frac{h\varkappa + \delta}{t'} \tag{14}$$

für alle ganzen Zahlen $t' \geqq t$ gültig sind.

Andererseits ist bekannt, daß, wenn s eine reelle Zahl > 1 bedeutet, die Reihe $\sum_{(t)} \frac{1}{t^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$ konvergiert, und daß $\lim_{s=1} \left\{(s-1) \sum_{(t)} \frac{1}{t^s}\right\} = 1$ ist. Die letztere Gleichung zeigt, daß auch $\lim_{s=1} \left\{(s-1) \sum_{(t')} \frac{1}{t'^s}\right\} = 1$ ist, wo t' nur alle diejenigen ganzen Zahlen durchlaufen soll, welche oberhalb einer

beliebig hohen Grenze t gelegen sind. Zunächst folgt aus der Konvergenz der Reihe $\sum \frac{1}{t^s}$ mit Hilfe der Ungleichung $\frac{1}{n_{t'}} < \frac{h\varkappa + \delta}{t'}$ die Konvergenz der Reihe

$$\sum_{(t)} \frac{1}{n_t^s} = \sum_{(\mathfrak{j})} \frac{1}{n(\mathfrak{j})^s}$$

für $s > 1$, wo t alle ganzen positiven Zahlen und $\mathfrak{j}$ alle Ideale des Körpers k durchläuft. Ferner ergibt sich aus den Ungleichungen (14) die Formel:

$$(h\varkappa - \delta)^s (s-1) \sum_{(t')} \frac{1}{t'^s} < (s-1) \sum_{(t')} \frac{1}{n_{t'}^s} < (h\varkappa + \delta)^s (s-1) \sum_{(t')} \frac{1}{t'^s},$$

wo die Summen sich über alle ganzzahligen Werte von t' zu erstrecken haben, welche $\geqq t$ sind. Man kann zur Grenze $s = 1$ übergehen und findet:

$$h\varkappa - \delta \leqq \lim_{s=1} \left\{(s-1) \sum_{(t')} \frac{1}{n_{t'}^s}\right\} \leqq h\varkappa + \delta .$$

Nun ist

$$\lim_{s=1} \left\{(s-1) \sum_{(\mathfrak{j})} \frac{1}{n(\mathfrak{j})^s}\right\} = \lim_{s=1} \left\{(s-1) \sum_{(t)} \frac{1}{n_t^s}\right\} = \lim_{s=1} \left\{(s-1) \sum_{(t')} \frac{1}{n_{t'}^s}\right\}$$

ebenfalls $\geqq h\varkappa - \delta$ und $\leqq h\varkappa + \delta$ und also, da hierin δ eine beliebig kleine Größe bedeutet, $= h\varkappa$, womit der gewünschte Nachweis des Satzes 56 erbracht ist.

§ 27. Andere unendliche Entwicklungen der Funktion $\zeta(s)$.

Die Funktion $\zeta(s)$ kann noch auf drei andere Arten durch unendliche Entwicklungen dargestellt werden [Dedekind (*1*)]. Es ist, wie leicht ersichtlich:

$$\begin{aligned}\zeta(s) &= \sum_{(n)} \frac{F(n)}{n^s}, \\ &= \prod_{(\mathfrak{p})} \frac{1}{1 - n(\mathfrak{p})^{-s}}, \\ &= \prod_{(\mathfrak{p})} \left(\frac{1}{1 - p^{-f_1 s}} \frac{1}{1 - p^{-f_2 s}} \cdots \frac{1}{1 - p^{-f_e s}}\right);\end{aligned}$$

hier ist im ersten Ausdruck die Summe über alle ganzen rationalen positiven Werte von n, im zweiten Ausdruck ist das Produkt über alle Primideale $\mathfrak{p}$ des Körpers k, und im dritten Ausdruck ist das Produkt über alle rationalen Primzahlen zu erstrecken, wobei $f_1, f_2, \ldots, f_e$ die Gerade der e in p aufgehenden Primideale bedeuten. Alle diese unendlichen Summen und Produkte für $\zeta(s)$ konvergieren für $s > 1$, da die Glieder sämtlich positiv sind, in einer von der Reihenfolge der Summanden oder Faktoren unabhängigen Weise.

§ 28. Die Zusammensetzung der Idealklassen eines Körpers.

Betreffs der multiplikativen Darstellung der Idealklassen gilt der folgende wichtige Satz (SCHERING (*1*), KRONECKER (*11*)]:

Satz 57. Es gibt stets q Klassen $A_1, \ldots, A_q$, so daß jede andere Klasse A auf eine und nur auf eine Weise in der Gestalt $A = A_1^{x_1} \ldots A_q^{x_q}$ darstellbar ist; dabei durchlaufen $x_1, \ldots, x_q$ die ganzen Zahlen $0, 1, 2, \ldots$ bez. bis $h_1 - 1, \ldots, h_q - 1$, und es ist $A_1^{h_1} = 1, \ldots, A_q^{h_q} = 1$ und $h = h_1 \ldots h_q$.

Beweis. Man bilde für jede Klasse A den niedrigsten Exponenten $e_1 > 0$ derart, daß $A^{e_1} = 1$ wird. Der größte aller dieser Exponenten e_1 werde mit h_1 bezeichnet, und es sei H_1 eine hierbei auf h_1 führende Klasse. Nun bestimme man für jede Klasse A den niedrigsten Exponenten $e_2 > 0$ derart, daß A^{e_2} gleich einer Potenz von H_1 wird. Der höchste dieser Exponenten e_2 werde mit h_2 bezeichnet, und H_2 sei eine auf h_2 führende Klasse. Ferner bestimme man für jede Klasse A den niedrigsten Exponenten $e_3 > 0$ derart, daß A^{e_3} gleich einem Produkt von Potenzen der Klassen H_1, H_2 wird; es sei h_3 der höchste dieser Exponenten e_3 und H_3 eine auf h_3 führende Klasse. Fährt man so fort, so entsteht eine Reihe von Klassen $H_1, H_2, \ldots, H_q$, denen, wie man unmittelbar sieht, die Eigenschaft zukommt, daß eine jede Klasse A auf eine und nur auf eine Weise in der Gestalt $A = H_1^{x_1} \cdots H_q^{x_q}$ dargestellt werden kann, wo $x_1, \ldots, x_q$ die im Satze 57 angegebenen Werte annehmen.

Es sei nun
$$H_s^k = H_t^{a_t} H_{t-1}^{a_{t-1}} \cdots H_1^{a_1}, \qquad (a_t \neq 0) \tag{15}$$
wo $t < s$ ist und $a_t, a_{t-1}, \ldots, a_1$ gewisse ganzzahlige Exponenten bedeuten. Aus den gemachten Festsetzungen folgt $H_s^{h_s} = H_{t-1}^{b_{t-1}} \ldots H_1^{b_1}$, wo $b_{t-1}, \ldots, b_1$ gewisse ganze Zahlen sind; es muß h_t durch h_s teilbar sein, da im anderen Falle bereits eine niedere als die h_s-te Potenz von H_s als Produkt der Klassen $H_t, H_{t-1}, \ldots, H_1$ darstellbar sein würde. Wird $h_t = h_s l_t$ gesetzt, so folgt, daß $H_t^{a_t l_t}$ durch ein Produkt der Klassen $H_{t-1}, \ldots, H_1$ darstellbar ist; es ist daher notwendig $a_t l_t$ durch h_t, d. h. a_t durch h_s teilbar. Setzen wir $a_t = h_s c_s$ und wählen an Stelle der Klasse H_s die Klasse $H_s' = H_s H_t^{-c_s}$, so geht die Gleichung (15) über in die einfachere Gleichung $H_s'^{h_s} = H_{t-1}^{a_{t-1}} \ldots H_1^{a_1}$. Die Fortsetzung dieses Verfahrens führt schließlich zu einer Klasse A_s an Stelle von H_s, für welche die gewünschte Relation $A_s^{h_s} = 1$ stattfindet.

Die obige Darstellung der Klassen kann überdies so eingerichtet werden, daß die Zahlen $h_1, \ldots, h_q$ Primzahlen oder Primzahlpotenzen sind. Wäre nämlich g eine der Zahlen $h_1, \ldots, h_q$, welche noch nicht Primzahl oder Primzahlpotenz ist, und wäre etwa $g = p' p'' \ldots$, wo $p', p'', \ldots$ Potenzen verschiedener Primzahlen sind, so setze man, wenn B die zu g gehörige Klasse bezeichnet, $B' = B^{\frac{g}{p'}}$, $B'' = B^{\frac{g}{p''}}, \ldots$. Wir haben dann $B'^{p'} = 1$, $B''^{p''} = 1, \ldots$, und wenn
$$\frac{1}{g} = \frac{a'}{p'} + \frac{a''}{p''} + \cdots$$
gesetzt wird, so folgt $B = B'^{a'} B''^{a''} \ldots$. Es kann also $B', B'', \ldots$ an Stelle von B eingeführt werden. Sind die Klassen $A_1, \ldots, A_q$ in der zuletzt beschriebenen Weise gewählt, so heißen dieselben ein **System von Grundklassen.**

§ 29. Die Charaktere einer Idealklasse. Eine Verallgemeinerung der Funktion $\zeta(s)$.

Nachdem ein bestimmtes System von Grundklassen ausgewählt worden ist, ist eine jede vorhandene Klasse A durch die Exponenten $x_1, \ldots, x_q$ und mithin auch durch die q Einheitswurzeln
$$\chi_1(A) = e^{\frac{2i\pi x_1}{h_1}}, \quad \ldots, \quad \chi_q(A) = e^{\frac{2i\pi x_q}{h_q}}$$
eindeutig bestimmt. Diese q Einheitswurzeln $\chi(A)$ heißen die **Charaktere der Klasse A.** Sind $\chi(A), \chi(B)$ Charaktere der beiden Klassen A, bez. B, so ist offenbar $\chi(AB) = \chi(A)\chi(B)$. Der Charakter $\chi(A)$ einer Klasse wird zugleich auch als der Charakter $\chi(\mathfrak{a})$ eines jeden in A enthaltenen Ideals $\mathfrak{a}$ bezeichnet.

Mit Hilfe eines Charakters χ läßt sich dann eine Funktion bilden, welche eine Verallgemeinerung der oben betrachteten Funktion $\zeta(s)$ ist, und welche eine ähnliche Produktentwicklung gestattet [DEDEKIND (*1*)]. Diese Funktion ist
$$\sum_{(\mathfrak{j})} \frac{\chi(\mathfrak{j})}{n(\mathfrak{j})^s} = \prod_{(\mathfrak{p})} \frac{1}{1 - \chi(\mathfrak{p})\, n(\mathfrak{p})^{-s}},$$
wo die Summe über alle Ideale $\mathfrak{j}$ und das Produkt über alle Primideale $\mathfrak{p}$ des Körpers k zu erstrecken ist.

8. Die zerlegbaren Formen des Körpers.

§ 30. Die zerlegbaren Formen des Körpers. Die Formenklassen und ihre Zusammensetzung.

Wenn $\xi^{(1)}, \ldots, \xi^{(m)}$ m lineare Formen der m Veränderlichen $u_1, \ldots, u_m$ mit beliebigen reellen oder imaginären Koeffizienten sind, so heißt das Produkt
$$U(u_1, \ldots, u_m) = \xi^{(1)} \ldots \xi^{(m)}$$
eine **zerlegbare Form** m-ten Grades der m Veränderlichen $u_1, \ldots, u_m$. Die Koeffizienten der Produkte von $u_1, \ldots, u_m$ heißen die **Koeffizienten der Form.** Berücksichtigt man die Formeln
$$-\frac{\partial^2 \log U}{\partial u_r \partial u_s} = \frac{\partial \log \xi^{(1)}}{\partial u_r}\frac{\partial \log \xi^{(1)}}{\partial u_s} + \cdots + \frac{\partial \log \xi^{(m)}}{\partial u_r}\frac{\partial \log \xi^{(m)}}{\partial u_s},$$
$$(r, s = 1, \ldots, m)$$
so folgt leicht aus dem Multiplikationssatz der Determinanten, daß das Quadrat der Determinante der m linearen Formen $\xi^{(1)}, \ldots, \xi^{(m)}$ gleich $(-1)^m U^2 \sum \pm \frac{\partial^2 \log U}{\partial u_1 \partial u_1} \cdots \frac{\partial^2 \log U}{\partial u_m \partial u_m}$ und daher eine ganze ganzzahlige Funktion

der Koeffizienten von U ist; dasselbe werde die **Diskriminante der Form** U genannt. Eine Form U, deren Koeffizienten ganze rationale Zahlen ohne gemeinsamen Teiler sind, heißt eine **primitive Form;** dieselbe ist eine rationale Einheitsform.

Sind $\alpha_1, \ldots, \alpha_m$ eine Basis des Ideals $\mathfrak{a}$, so ist insbesondere die Norm $n(\xi) = n(\alpha_1 u_1 + \cdots + \alpha_m u_m)$ eine zerlegbare Form m-ten Grades. Die Koeffizienten derselben sind ganze rationale Zahlen mit dem größten gemeinsamen Teiler $n(\mathfrak{a})$. Nach Forthebung dieses Teilers entsteht eine primitive Form U, welche eine **zerlegbare Form des Körpers** k genannt wird, und welche folgende Eigenschaften besitzt. Wählt man an Stelle der Basis $\alpha_1, \ldots, \alpha_m$ eine andere Basis $\alpha_1^*, \ldots, \alpha_m^*$ des Ideals $\mathfrak{a}$, so erhält man eine Form U^*, welche aus U vermöge ganzzahliger linearer Transformation von der Determinante ± 1 hervorgeht. Faßt man alle diese transformierten Formen unter den Begriff der **Formenklasse** zusammen, so ist ersichtlich, daß einem jeden Ideal $\mathfrak{a}$ eine bestimmte Formenklasse zugehört. Die nämliche Formenklasse entsteht offenbar auch, wenn man statt des Ideals $\mathfrak{a}$ das Ideal $\alpha\mathfrak{a}$ zugrunde legt, wo α eine ganze oder gebrochene Zahl des Körpers bedeutet, d. h. einem jedem Ideal der nämlichen Idealklasse entspricht die nämliche Formenklasse.

Da die Diskriminante der Form $n(\xi) = n(\mathfrak{a})U$ offenbar gleich $n(\mathfrak{a})^2\, d$ ist, so folgt die Tatsache:

Satz 58. Die Diskriminante einer zerlegbaren Form U des Körpers k ist gleich der Körperdiskriminante d [Dedekind (*I*)].

Die genannten Eigenschaften der Formen U bestimmen das Wesen derselben vollständig; es gilt nämlich der umgekehrte Satz:

Satz 59. Wenn U eine primitive, im Körper k zerlegbare, aber in jedem Körper niederen Grades unzerlegbare Form m-ten Grades mit der Diskriminante d des Körpers ist, so gibt es in k mindestens eine und höchstens m Idealklassen, denen die Form U zugehört.

Beweis. Ist etwa $\eta = \mu_1 u_1 + \cdots + \mu_m u_m$ ein Linearfaktor von U, dessen Koeffizienten in k liegen, so multipliziere man η mit einer ganzen Zahl a derart, daß $\xi = a\eta = \alpha_1 u_1 + \cdots + \alpha_m u_m$ eine lineare Form mit ganzen Koeffizienten $\alpha_1, \ldots, \alpha_m$ wird. Setzen wir $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$, so ist nach Satz 20 $n(\xi) = n(\mathfrak{a})U$, und da die Diskriminante der Form U gleich der Körperdiskriminante sein soll, so ergibt sich hieraus:

$$\begin{vmatrix} \alpha_1, & \ldots, & \alpha_m \\ \alpha_1', & \ldots, & \alpha_m' \\ \cdots & \cdots & \cdots \\ \alpha_1^{(m-1)}, & \ldots, & \alpha_m^{(m-1)} \end{vmatrix}^2 = n(\mathfrak{a})^2 d,$$

wo die gestrichenen α bez. die konjugierten Zahlen bedeuten. Aus dieser Gleichung folgt, wenn wir die Umkehrung des Satzes 19 zu Hilfe nehmen, daß $\alpha_1, \ldots, \alpha_m$ eine Basis des Ideals $\mathfrak{a}$ bilden.

Gehören zu den beiden Idealen $\mathfrak{a}, \mathfrak{b}$ bezüglich die beiden Formen U, V, so heißt jede zu dem Ideale $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ gehörige Form W eine aus den Formen U und V **zusammengesetzte Form** [Dedekind (*I*)].

Die Entscheidung der Frage, ob zwei vorgelegte, zum Körper k gehörige Formen zu derselben oder zu verschiedenen Formenklassen gehören, kommt, der obigen Entwicklung zufolge, auf die Frage nach der Äquivalenz zweier vorgelegter Ideale hinaus und erfordert daher zu ihrer Entscheidung nur eine endliche Anzahl von Operationen. Vgl. § 24.

9. Die Zahlringe des Körpers.

§ 31. Der Zahlring. Das Ringideal und seine wichtigsten Eigenschaften.

Sind $\vartheta, \eta, \ldots$ irgend welche ganze algebraische Zahlen, deren Rationalitätsbereich der Körper k vom m-ten Grade ist, so wird das System aller ganzen Funktionen von $\vartheta, \eta, \ldots$, deren Koeffizienten ganze rationale Zahlen sind, ein **Zahlring, Ring** oder **Integritätsbereich**[1] genannt. Die Addition, Subtraktion und Multiplikation zweier Zahlen eines Ringes liefert wiederum eine Zahl des Ringes. Der Begriff des Ringes ist mithin gegenüber den drei Rechnungsoperationen der Addition, Subtraktion und Multiplikation invariant. Der größte Zahlring des Körpers k ist der durch $\omega_1, \ldots, \omega_m$ bestimmte Ring, wo $\omega_1, \ldots, \omega_m$ die Zahlen einer Körperbasis bedeuten. Derselbe umfaßt alle ganzen Zahlen des Körpers. Jeder Zahlring r enthält m ganze Zahlen $\varrho_1, \ldots, \varrho_m$ von der Art, daß jede andere Zahl ϱ des Ringes in der Gestalt

$$\varrho = a_1 \varrho_1 + \cdots + a_m \varrho_m$$

dargestellt werden kann, wo $a_1, \ldots, a_m$ ganze rationale Zahlen sind. Die Zahlen $\varrho_1, \ldots, \varrho_m$ heißen eine **Basis des Ringes.** Bezeichnen wir die zu $\varrho_1, \ldots, \varrho_m$ konjugierten Zahlen bez. mit $\varrho_1', \ldots, \varrho_m', \ldots, \varrho_1^{(m-1)}, \ldots, \varrho_m^{(m-1)}$, so ist das Quadrat der Determinante

$$\begin{vmatrix} \varrho_1, & \ldots, & \varrho_m \\ \varrho_1', & \ldots, & \varrho_m' \\ \cdots & \cdots & \cdots \\ \varrho_1^{(m-1)}, & \ldots, & \varrho_m^{(m-1)} \end{vmatrix}$$

eine rationale Zahl und heißt die **Diskriminante d_r des Ringes** r.

Ein **Ringideal** oder ein **Ideal des Ringes** r wird ein solches unendliches System von ganzen algebraischen Zahlen $\alpha_1, \alpha_2, \ldots$ des Ringes r genannt, welches die Eigenschaft besitzt, daß eine jede lineare Kombination $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots$ derselben wiederum dem System angehört, wobei die Koeffizienten $\lambda_1, \lambda_2, \ldots$ beliebige Zahlen des Ringes r sind. Jedes Ringideal enthält

[1] Nach Dedekind „eine Ordnung".

m ganze Zahlen $\iota_1, \ldots, \iota_m$ von der Art, daß eine jede Zahl des Ringideals gleich einer linearen Kombination derselben von der Gestalt $a_1\iota_1 + \cdots + a_m\iota_m$ ist, wo $a_1, \ldots, a_m$ ganze rationale Zahlen bedeuten. Die Zahlen $\iota_1, \ldots, \iota_m$ heißen eine **Basis des Ringideals.** Der Beweis für die Existenz einer Basis des Ringes und des Ringideals ist genau entsprechend den in § 3 und § 4 dargelegten Beweisen für die Existenz der Körperbasis und Idealbasis zu führen. Es gelten folgende Sätze: [DEDEKIND (3)].

Satz 60. Sind $\iota_1, \ldots, \iota_m$ irgend m ganze Zahlen des Körpers k, zwischen denen keine lineare Relation mit ganzen rationalen Zahlenkoeffizienten besteht, so gibt es stets einen Ring r, in welchem, wenn A eine geeignet gewählte ganze rationale Zahl bedeutet, die Produkte $A\iota_1, A\iota_2, \ldots, A\iota_m$ die Basis eines Ringideals bilden. Zum Beweise dieses Satzes 60 vergleiche den Beweis zu Satz 61.

Beweis. Es sei ϱ eine beliebige ganze Zahl des Körpers, für welche die m Zahlen $\varrho\iota_1, \ldots, \varrho\iota_m$ sämtlich gleich linearen Kombinationen der Zahlen $\iota_1, \ldots, \iota_m$ von der Gestalt $a_1\iota_1 + \cdots + a_m\iota_m$ werden, wo $a_1, \ldots, a_m$ ganze rationale Zahlen sind. Die Gesamtheit aller dieser ganzen Zahlen ϱ des Körpers bestimmt, wie leicht einzusehen, einen Ring von der verlangten Beschaffenheit.

Sind $\alpha_1, \ldots, \alpha_s$ irgend s Zahlen in r, durch deren lineare Kombination unter Benutzung ganzer algebraischer, in r liegender Koeffizienten alle Zahlen eines Ringideals $\mathfrak{j}_r$ erhalten werden können, so setzen wir kurz $\mathfrak{j}_r = [\alpha_1, \ldots, \alpha_s]$. Insbesondere ist $\mathfrak{j}_r = [\iota_1, \ldots, \iota_m]$.

Satz 61. Es gibt in jedem Ringe r stets Ringideale $\mathfrak{j}_r$, welche zugleich Körperideale sind.

Beweis. Drückt man $\omega_1, \ldots, \omega_m$ durch die Zahlen $\varrho_1, \ldots, \varrho_m$ der Basis des Ringes r aus, in der Gestalt

$$\omega_i = \frac{a_{i1}\varrho_1 + \cdots + a_{im}\varrho_m}{A}, \qquad (i = 1, 2, \ldots, m)$$

wo $a_{i1}, \ldots, a_{im}, A$ ganze rationale Zahlen sind, so folgt, daß jede durch A teilbare ganze Zahl in k eine Zahl des Ringes und mithin jedes durch A teilbare Ideal des Körpers k zugleich ein Ringideal des Ringes r ist.

Der größte gemeinsame Idealteiler aller derjenigen Körperideale, welche zugleich Ringideale in r sind, heißt der **Führer $\mathfrak{f}$ des Ringes r**. [DEDEKIND (3)]. Es folgt dann leicht der Satz:

Satz 62. Jedes durch den Führer $\mathfrak{f}$ teilbare Ideal $\mathfrak{j}$ des Körpers k ist zugleich ein Ringideal des Ringes r.

§ 32. Die durch eine ganze Zahl bestimmten Ringe. Der Satz von der Differente einer ganzen Zahl des Körpers.

Die wichtigsten Zahlringe des Körpers sind diejenigen, welche durch eine *einzige* ganze Zahl ϑ bestimmt werden. Auf die Eigenschaften dieser besonderen Zahlringe hat DEDEKIND seine Theorie der Diskriminanten algebraischer

Zahlkörper gegründet [DEDEKIND (6)]. Die hauptsächlichsten Resultate von DEDEKIND fassen wir in folgenden Satz zusammen:

Satz 63. Der größte gemeinsame Teiler der Differenten aller ganzen Zahlen des Körpers k ist gleich der Differente $\mathfrak{d}$ des Körpers. Ist δ die Differente einer ganzen Zahl ϑ, welche den Körper k bestimmt, und $\mathfrak{f}$ der Führer des durch ϑ bestimmten Zahlringes, so ist $\delta = \mathfrak{f}\mathfrak{d}$.

Beweis. Es sei $\omega_1, \ldots, \omega_m$ eine Körperbasis von k, und es seien bezüglich $\omega_1', \ldots, \omega_m', \ldots, \omega_1^{(m-1)}, \ldots, \omega_m^{(m-1)}$ die zu diesen m Zahlen konjugierten Zahlen. Wir bilden die m-reihige Determinante der m^2 Zahlen $\omega_h^{(l)}$:

$$\Omega = \begin{vmatrix} \omega_1, & \ldots, & \omega_m \\ \omega_1', & \ldots, & \omega_m' \\ \cdot & \cdots & \cdot \\ \omega_1^{(m-1)}, & \ldots, & \omega_m^{(m-1)} \end{vmatrix}$$

und bezeichnen die zu $\omega_1, \ldots, \omega_m$ adjungierten $(m-1)$-reihigen Unterdeterminanten von Ω bezüglich mit $\Omega_1, \ldots, \Omega_m$. Die m Produkte $\Omega\Omega_1, \ldots, \Omega\Omega_m$ sind dann ganze Zahlen des Körpers k, und zwar bilden dieselben die Basiszahlen eines Ideals des Körpers k.

Um das letztere zu beweisen, multiplizieren wir die $m-1$ Horizontalreihen der Determinante Ω_h bezüglich mit

$$u + \omega_i', \; u + \omega_i'', \; \ldots, \; u + \omega_i^{(m-1)}, \qquad (16)$$

wo u ein unbestimmter Parameter ist. Die entstehende $(m-1)$-reihige Determinante erhält dann, wie leicht ersichtlich, die Gestalt:

$$f_1(u)\Omega_1 + f_2(u)\Omega_2 + \cdots + f_m(u)\Omega_m,$$

wo $f_1, \ldots, f_m$ ganzzahlige Funktionen von u sind. Andererseits hat das Produkt der $m-1$ Linearfaktoren (16) die Form

$$u^{m-1} + (\omega_i' + \cdots + \omega_i^{(m-1)})u^{m-2} + \cdots = u^{m-1} + (a - \omega_i)u^{m-2} + \cdots,$$

wo a eine ganze rationale Zahl bedeutet. Die Vergleichung der Koeffizienten von u^{m-2} liefert das Resultat, daß $\omega_i\Omega_h$ eine lineare Kombination von $\Omega_1, \ldots, \Omega_m$ mit ganzen rationalen Zahlenkoeffizienten ist; hiermit ist der gewünschte Nachweis dafür geführt, daß $\Omega\Omega_1, \ldots, \Omega\Omega_m$ Basiszahlen eines Ideals sind.

Bezeichnen wir allgemein mit $\Omega_h^{(l)}$ die zu $\omega_h^{(l)}$ adjungierte $(m-1)$-reihige Unterdeterminante der Determinante Ω, so wird nach einem bekannten Determinantensatze die m-reihige Determinante $|\Omega_h^{(l)}| = \Omega^{m-1}$; folglich genügt die Norm des Ideals $\mathfrak{J} = (\Omega\Omega_1, \ldots, \Omega\Omega_m)$ der Gleichung

$$d n^2(\mathfrak{J}) = |\Omega\Omega_h^{(l)}|^2 = \Omega^{4m-2},$$

und hieraus folgt $n(\mathfrak{J}) = |d|^{m-1}$. Nun ist offenbar die Diskriminante d des Körpers durch $\mathfrak{J}$ teilbar; setzen wir $d = \mathfrak{J}\mathfrak{j}$, so folgt $n(\mathfrak{j}) = |d|$.

Es sei nun ϑ irgendeine den Körper k bestimmende Zahl; dann können wir die m Basiszahlen des Körpers k in der Gestalt voraussetzen:

$$\omega_1 = 1,$$
$$\omega_2 = \frac{a_1 + \vartheta}{f_1},$$
$$\omega_3 = \frac{a_2 + a_2'\vartheta + \vartheta^2}{f_2},$$
$$\cdots\cdots\cdots$$
$$\omega_m = \frac{a_{m-1} + a_{m-1}'\vartheta + \cdots + a_{m-1}^{(m-2)}\vartheta^{m-2} + \vartheta^{m-1}}{f_{m-1}},$$

wo $a_1, a_2, a_2', \ldots, a_{m-1}^{(m-2)}, f_1, \ldots, f_{m-1}$ ganze rationale Zahlen sind. Wir ermitteln nun den Führer $\mathfrak{f}$ des durch ϑ bestimmten Ringes und stellen die Basiszahlen desselben in der Gestalt dar:

$$\varrho_1 = f_1',$$
$$\varrho_2 = b_1 + f_2'\vartheta,$$
$$\varrho_3 = b_2 + b_2'\vartheta + f_3'\vartheta^2,$$
$$\cdots\cdots\cdots$$
$$\varrho_m = b_{m-1} + b_{m-1}'\vartheta + \cdots + b_{m-1}^{(m-2)}\vartheta^{m-2} + f_m'\vartheta^{m-1},$$

wo $b_1, b_2, b_2', \ldots, b_{m-1}^{(m-2)}, f_1', f_2', \ldots, f_m'$ ganze rationale Zahlen bedeuten. Da insbesondere nach Satz 62 $\varrho_1\omega_m, \varrho_2\omega_{m-1}, \ldots, \varrho_m\omega_1$ ganzzahlige Funktionen von ϑ werden müssen, so ergibt sich notwendigerweise, daß f_1' durch f_{m-1}, f_2' durch $f_{m-2}, \ldots, f_{m-1}'$ durch f_1 und folglich das Produkt $f_1' \ldots f_{m-1}'$ durch das Produkt $f = f_1 \ldots f_{m-1}$ teilbar sein muß. Da $n(\mathfrak{f}) = f_1 \ldots f_{m-1} f_1' \ldots f_{m-1}' f_m'$ ist, so wird $n(\mathfrak{f}) = f^2 g$, wo g eine ganze rationale Zahl ist.

Wir setzen ferner:

$$\Theta = \begin{vmatrix} 1, & \vartheta, & \ldots, & \vartheta^{m-1} \\ 1, & \vartheta', & \ldots, & \vartheta'^{m-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1, & \vartheta^{(m-1)}, & \ldots, & (\vartheta^{(m-1)})^{m-1} \end{vmatrix}, \qquad \mathsf{H} = \begin{vmatrix} 1, & \vartheta', & \ldots, & \vartheta'^{m-2} \\ \cdots & \cdots & \cdots & \cdots \\ 1, & \vartheta^{(m-1)}, & \ldots, & (\vartheta^{(m-1)})^{m-2} \end{vmatrix};$$

es gelten dann für die Differente δ der Zahl ϑ die Beziehungen $(-1)^{m-1}\delta = \frac{\Theta}{\mathsf{H}}$ und nach S. 71 $(-1)^{\frac{m(m-1)}{2}} n(\delta) = \Theta^2 = f^2 d$. Ferner ist

$$\sum_{(h=1,\ldots,m)} u_h \Omega\Omega_h = \frac{\Theta}{f^2} \begin{vmatrix} u_1, & f_1 u_2, & f_2 u_3, & \ldots, & f_{m-1} u_m \\ 1, & a_1 + \vartheta', & a_2 + a_2'\vartheta' + \vartheta'^2, & \ldots, & a_{m-1} + \cdots + \vartheta'^{m-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1, & a_1 + \vartheta^{(m-1)}, & a_2 + a_2'\vartheta^{(m-1)} + (\vartheta^{(m-1)})^2, & \ldots, & a_{m-1} + \cdots + (\vartheta^{(m-1)})^{m-1} \end{vmatrix}, \quad (17)$$

wo $u_1, \ldots, u_m$ Unbestimmte sind. Entwickeln wir hier die Determinante nach den Elementen der ersten Horizontalreihe und schreiben sie dabei in der Gestalt $u_1\mathsf{H}_1 + \cdots + u_m\mathsf{H}_m$, so sind, wie man leicht erkennt, die Zahlen $\frac{\mathsf{H}_1}{\mathsf{H}}, \ldots, \frac{\mathsf{H}_m}{\mathsf{H}}$ sämtlich ganze Zahlen des Körpers k; sie gehen, wie die Formel (17) zeigt, aus den Zahlen $\Omega\Omega_1, \ldots, \Omega\Omega_m$ dadurch hervor, daß man die letzteren mit ein und demselben in k liegenden Faktor multipliziert. Die m Zahlen $\frac{\mathsf{H}_1}{\mathsf{H}}, \ldots, \frac{\mathsf{H}_m}{\mathsf{H}}$ sind folglich wieder Basiszahlen eines Ideals; dieses Ideal heiße $\mathfrak{m}$.

Die Zahlen des Ideals $\mathfrak{m}$ sind sämtlich ganzzahlige Funktionen von ϑ. Dasselbe ist folglich durch $\mathfrak{f}$ teilbar, und wir setzen $\mathfrak{m} = \mathfrak{f}\mathfrak{l}$, wo $\mathfrak{l}$ ein gewisses Ideal in k bedeutet. Unsere Gleichung (17) zeigt dann, daß

$$\mathfrak{F} = \frac{\Theta\mathsf{H}}{f^2}\,\mathfrak{f}\mathfrak{l} = \frac{d\,\mathfrak{f}\mathfrak{l}}{\delta}$$

ist, und wenn man die Norm nimmt, so folgt hieraus:

$$|d|^{m-1} = \frac{|d|^m\, n(\mathfrak{f})\, n(\mathfrak{l})}{f^2\,|d|}, \quad \text{d. h.} \quad f^2 = n(\mathfrak{f})\, n(\mathfrak{l}).$$

Da andererseits vorhin $n(\mathfrak{f}) = f^2 g$ gefunden worden ist, so muß $g = 1, n(\mathfrak{l}) = 1$, $\mathfrak{l} = 1$ sein, und folglich wird $n(\mathfrak{f}) = f^2, \mathfrak{F}\delta = \mathfrak{f}d, \delta = \mathfrak{f}\mathfrak{j}$.

Nunmehr sei $\mathfrak{p}$ ein beliebig gegebenes Primideal des Körpers k, so beweisen wir zunächst, daß sich stets eine ganze Zahl $\vartheta = \varrho$ in k finden läßt von der Art, daß der Führer des durch ϱ bestimmten Ringes nicht durch $\mathfrak{p}$ teilbar ist. Es sei die durch $\mathfrak{p}$ teilbare rationale Primzahl $p = \mathfrak{p}^e\mathfrak{a}$, wo $\mathfrak{a}$ ein zu $\mathfrak{p}$ primes Ideal bedeutet; ferner sei ϱ als ganze Zahl in k derart ausgewählt, daß jede beliebige ganze Zahl des Körpers k nach jeder noch so hohen Potenz von $\mathfrak{p}$ kongruent einer ganzzahligen Funktion von ϱ wird. Die Existenz einer solchen Zahl ϱ ist in Satz 29 gezeigt worden; zugleich werde die Zahl ϱ so gewählt, daß sie $\equiv 0$ nach $\mathfrak{a}$ wird (Satz 25) und eine den Körper k bestimmende Zahl ist. Nunmehr sei die Diskriminante $d(\varrho)$ der Zahl ϱ gleich $p^h a$, wo a eine zu p prime, ganze rationale Zahl bedeutet. Es ist dann jede ganze Zahl ω des Körpers k in der Gestalt $\omega = \frac{F(\varrho)}{a\,\varrho^h}$ darstellbar, wo $F(\varrho)$ eine ganze ganzzahlige Funktion von ϱ bezeichnet. In der Tat: wird $\omega \equiv H(\varrho)$ nach $\mathfrak{p}^{eh}$, wo $H(\varrho)$ eine ganzzahlige Funktion von ϱ bedeutet, und setzen wir $\omega = H(\varrho) + \omega^*$, so folgt, daß $\omega^*\varrho^h$ durch p^h teilbar wird. Wir setzen $\omega^*\varrho^h = p^h\alpha$, wo α eine ganze Zahl des Körpers k bedeutet. Da nach § 3 eine jede ganze Zahl α in die Gestalt $\frac{G(\varrho)}{d(\varrho)}$ gebracht werden kann, wo $G(\varrho)$ eine ganze ganzzahlige Funktion von ϱ bedeutet, so folgt $\omega^* = \frac{G(\varrho)}{a\,\varrho^h}$ und weiter $\omega = \frac{a\,\varrho^h H(\varrho) + G(\varrho)}{a\,\varrho^h}$. Die eben gefundene Eigenschaft der Zahl ϱ lehrt, daß die Zahl $a\,\varrho^h$ jedenfalls in dem Führer des durch ϱ bestimmten Ringes vorkommt. Derselbe ist mithin nicht durch $\mathfrak{p}$ teilbar, d. h. die Zahl $\varrho = \vartheta$ ist eine Zahl von der oben verlangten Beschaffenheit.

Die letzten Entwicklungen zeigen, daß das Ideal $\mathfrak{j}$ genau der größte gemeinsame Teiler der Differenten aller ganzen Zahlen ist. Andererseits enthält dieser größte gemeinsame Teiler, wie aus der Definition der Körperdifferente $\mathfrak{d}$ folgt, notwendig dieses Ideal $\mathfrak{d}$ als Faktor; wir setzen $\mathfrak{j} = \mathfrak{h}\mathfrak{d}$. Da $n(\mathfrak{d})$ nach Satz 13 durch die Diskriminante d teilbar ist, so folgt $n(\mathfrak{j}) = n(\mathfrak{h})da$, wo a eine ganze rationale Zahl bedeutet. Wegen $n(\mathfrak{j}) = \pm d$ folgt hieraus $n(\mathfrak{h}) = 1$, $\mathfrak{h} = 1$, $a = \pm 1$, also $\mathfrak{j} = \mathfrak{d}$. Damit ist der Satz 63 vollständig bewiesen.

Aus dem Satze 63 folgen leicht der Satz 31 und 37, sowie die am Schluß des § 12 aufgestellte Behauptung über die in der Diskriminante des Körpers aufgehenden Primzahlen. Um die letztere abzuleiten, hat man nur nötig, die Zerlegung der linken Seite der Gleichung, welcher $\vartheta = \varrho$ genügt, nach der betreffenden Primzahl p vorzunehmen und in ähnlicher Weise zu verwerten, wie dies in § 11 für die linke Seite der Fundamentalgleichung geschehen ist.

§ 33. Die regulären Ringideale und ihre Teilbarkeitsgesetze.

Ist ein beliebiger Ring r und in ihm ein Ringideal $\mathfrak{j}_r = [\alpha_1, \ldots, \alpha_s]$ gegeben, so hat man in dem größten gemeinsamen Idealteiler der Zahlen des letzteren ein Körperideal; wir nennen dieses Ideal $\mathfrak{j} = (\alpha_1, \ldots, \alpha_s)$ das dem Ringideal $\mathfrak{j}_r$ **zugeordnete Körperideal.** Wenn insbesondere das Körperideal $\mathfrak{j}$ zum Führer $\mathfrak{f}$ des Ringes r prim ist, so heiße $\mathfrak{j}_r$ ein **reguläres Ringideal.** Es gilt der Satz:

Satz 64. Wenn $\mathfrak{j}$ ein beliebiges zu dem Führer $\mathfrak{f}$ primes Körperideal ist, so existiert im Ringe r stets ein Ringideal $\mathfrak{j}_r$, dem das Körperideal $\mathfrak{j}$ zugeordnet ist.

Beweis. Wir bestimmen das System aller der Zahlen des Ringes r, welche durch das gegebene Körperideal $\mathfrak{j}$ teilbar sind. Dieselben bilden in r ein Ringideal $\mathfrak{j}_r = [\alpha_1, \ldots, \alpha_s]$. Ferner wählen wir in dem Führer $\mathfrak{f}$ des Ringes r eine zu $\mathfrak{j}$ prime ganze Zahl φ und dann im Körperideal $\mathfrak{j}$ eine zu φ prime Zahl α. Alsdann gibt es stets ganze Zahlen ψ und β des Körpers derart, daß $\varphi\psi + \alpha\beta = 1$ wird. Da $\varphi\psi$ durch $\mathfrak{f}$ teilbar und daher eine Zahl des Ringes r ist, so liegt auch $\alpha\beta$ im Ringe r, und da andererseits $\alpha\beta$ durch $\mathfrak{j}$ teilbar ist, so stellt $\alpha\beta = 1 - \varphi\psi$ eine Zahl des Ringideals $\mathfrak{j}_r$ dar: das dem Ringideal $\mathfrak{j}_r$ zugeordnete Körperideal $\mathfrak{j}^* = (\alpha_1, \ldots, \alpha_s)$ ist folglich zu $\mathfrak{f}$ prim. Da $\mathfrak{j}^*$ durch $\mathfrak{j}$ teilbar ist und überdies in dem Produkt $\mathfrak{f}\mathfrak{j}$ aufgeht, so ergibt sich daraus $\mathfrak{j}^* = \mathfrak{j}$; d. h. $\mathfrak{j}_r$ erweist sich als ein reguläres Ringideal, dem das Körperideal $\mathfrak{j}$ zugeordnet ist. Damit ist der Satz 64 bewiesen.

Unter dem **Produkt zweier Ringideale** $\mathfrak{a}_r = [\alpha_1, \ldots, \alpha_s]$ und $\mathfrak{b}_r = [\beta_1, \ldots, \beta_t]$ wird das Ringideal

$$\mathfrak{a}_r \mathfrak{b}_r = [\alpha_1\beta_1, \ldots, \alpha_s\beta_1, \ldots, \alpha_1\beta_t, \ldots, \alpha_s\beta_t]$$

verstanden. Es ist dann der Satz unmittelbar ersichtlich:

Satz 65. Dem Produkt zweier regulärer Ringideale ist stets das Produkt der zugeordneten Körperideale zugeordnet.

Vermöge dieses Satzes 65 entsprechen die Teilbarkeits- und Zerlegungsgesetze der regulären Ringideale vollkommen den Gesetzen über die Teilbarkeit und Zerlegung der zu $\mathfrak{f}$ primen Körperideale.

Da wir im folgenden nur reguläre Ringideale betrachten, so lassen wir der Kürze halber den Zusatz „regulär" fort, so daß von nun an unter einem **Ringideal** stets ein reguläres Ringideal verstanden wird.

Es ist aus Satz 23 zu entnehmen, daß in dem Körper k stets $\varphi(\mathfrak{f})$ nach dem Ideal $\mathfrak{f}$ inkongruente, zu $\mathfrak{f}$ prime ganze Zahlen vorhanden sind. Wenn eine von diesen dem Ringe r angehört, so liegen offenbar auch alle diejenigen Zahlen im Ringe r, welche dieser Zahl nach dem Führer $\mathfrak{f}$ kongruent sind. Die Anzahl der nach $\mathfrak{f}$ inkongruenten und zu $\mathfrak{f}$ primen dem Ringe r angehörigen Zahlen ist ein Teiler von $\varphi(\mathfrak{f})$ und werde mit $\varphi_r(\mathfrak{f})$ bezeichnet.

Unter der **Norm** $n(\mathfrak{a}_r)$ **eines Ringideals** $\mathfrak{a}_r$ versteht man die Norm des dem Ringideal zugeordneten Körperideals $\mathfrak{a}$. Die elementaren Sätze über Normen von Ringidealen sind mit dieser Definition gegeben.

§ 34. Die Einheiten eines Ringes. Die Ringklassen.

Auch der Satz von der Existenz der Grundeinheiten ist ohne Schwierigkeit auf einen Ring übertragbar; dieser Satz folgt am einfachsten aus dem entsprechenden Satze für die Einheiten des Körpers, wenn man bedenkt, daß, wie aus Satz 24 folgt, jede Einheit des Körpers durch Erheben in die $\varphi(\mathfrak{f})$-te Potenz in eine Einheit des Ringes übergehen muß. Der Satz hat genau die für den Körper k geltende Form des Satzes 47; für die in Satz 47 mit r bezeichnete Anzahl werde hier s geschrieben. Es mögen $\varepsilon_1, \ldots, \varepsilon_s$ ein System von s Grundeinheiten des Ringes r bedeuten, d. h. ein System von s Einheiten im Ringe r, durch deren Produkte unter Zuhilfenahme der Einheitswurzeln des Ringes sich sämtliche Einheiten in r ausdrücken lassen. Dann heißt die positiv genommene Determinante der s ersten Logarithmen zu diesen Einheiten der Regulator R_r des Ringes r. Die Anzahl der im Ringe r gelegenen Einheitswurzeln werde mit w_r bezeichnet [Dedekind (3)].

Zwei Ringideale $\mathfrak{a}$ und $\mathfrak{b}$ heißen einander äquivalent, wenn zwei ganze Zahlen μ und λ existieren, so daß $\mu\mathfrak{a} = \lambda\mathfrak{b}$ ist. Dabei werde der Äquivalenzbegriff hier in der in § 24 erwähnten engeren Fassung genommen und demgemäß die Einschränkung gemacht, daß $\frac{\mu}{\lambda}$ eine positive Norm besitze. Alle einander äquivalenten Ringideale bilden eine **Ringklasse.** Ein Ringideal (α), wo α eine zu $\mathfrak{f}$ prime ganze Zahl mit positiver Norm bedeutet, wird ein Hauptringideal, die Klasse dieser die **Hauptringklasse** genannt. Die weiteren Definitionen und die Sätze über die Multiplikation der Ringklassen entsprechen genau denjenigen, die in §§ 22, 28, 29 für die Idealklassen eines Körpers aufgestellt sind; auch folgt ähnlich, wie in § 22 die Endlichkeit der Anzahl der

Ringklassen. Die Bestimmung dieser Anzahl kann nach zwei verschiedenen Methoden, nämlich entweder auf einem rein arithmetischen Wege oder mit Verwendung analytischer Hilfsmittel, entsprechend der in § 25 und § 26 dargelegten Weise ausgeführt werden. Das hierbei sich ergebende Resultat ist folgendes [DEDEKIND (3)]:

Satz 66. Sind h und h_r die Anzahlen der Idealklassen des Körpers k bez. des Ringes r, beide für die engere Fassung des Klassenbegriffes, so ist

$$\frac{h_r}{h} = \frac{\varphi(\mathfrak{f})\, w_r R}{\varphi_r(\mathfrak{f})\, w R_r}.$$

Auch die Begriffsbildungen des Kapitels 8 lassen sich auf den Ring übertragen; wir gelangen so zu dem Begriffe der zu einer Ringklasse gehörigen **zerlegbaren Form.**

§ 35. Der Modul und die Modulklasse.

Wenn $\mu_1, \ldots, \mu_m$ irgend m ganze Zahlen des Körpers k sind, zwischen denen keine lineare homogene Relation mit ganzen rationalen Koeffizienten besteht, so werde das System aller mittelst ganzer rationaler Koeffizienten $a_1, \ldots, a_m$ in der Gestalt $a_1\mu_1 + \cdots + a_m\mu_m$ darstellbaren Zahlen ein **Modul** des Körpers k genannt und mit $[\mu_1, \ldots, \mu_m]$ bezeichnet. Der Begriff des Moduls verhält sich mithin gegenüber den Operationen der Addition und Subtraktion invariant. Beispiele von Moduln sind das System aller ganzen Zahlen des Körpers k, das Ideal, der Ring, das Ringideal. Zwei Moduln $[\mu_1, \ldots, \mu_m]$ und $[\lambda_1, \ldots, \lambda_m]$ heißen einander **äquivalent,** wenn zwei ganze Zahlen μ und λ existieren, so daß $[\mu\mu_1, \ldots, \mu\mu_m] = [\lambda\lambda_1, \ldots, \lambda\lambda_m]$ ist. Alle einander äquivalenten Moduln bilden eine **Modulklasse.** DEDEKIND nimmt den Begriff des Moduls in seinen Untersuchungen über algebraische Zahlen als Grundlage [DEDEKIND (*1*, *3*, *6*, *9*)].

Das Quadrat der Determinante

$$\begin{vmatrix} \mu_1, & \ldots, & \mu_m \\ \mu_1', & \ldots, & \mu_m' \\ \cdot & \cdots & \cdot \\ \mu_1^{(m-1)}, & \ldots, & \mu_m^{(m-1)} \end{vmatrix}$$

ist, wie leicht ersichtlich, eine ganze rationale Zahl und überdies durch die quadrierte Norm des Ideals $\mathfrak{m} = (\mu_1, \ldots, \mu_m)$ teilbar; der Quotient beider Quadrate werde mit ∂ bezeichnet. Bildet man diese Quotienten für einen beliebigen zu $[\mu_1, \ldots, \mu_m]$ äquivalenten Modul, so ergibt sich jedesmal der nämliche Wert ∂. Die ganze rationale Zahl ∂ ist mithin für die durch $[\mu_1, \ldots, \mu_m]$ bestimmte Modulklasse charakteristisch und heißt die **Diskriminante der Modulklasse.**

Die Begriffe **zerlegbare Form** und **Formenklasse** werden für den Modul entsprechend definiert, wie dies in § 30 für den Körper selbst geschehen ist. [DEDEKIND (*3*)].

Zweiter Teil.

Der Galoissche Zahlkörper.

10. Die Primideale des Galoisschen Körpers und seiner Unterkörper.

§ 36. Die eindeutige Zerlegung der Ideale des Galoisschen Körpers in Primideale.

Ein solcher Zahlkörper K, welcher mit den sämtlichen zu ihm konjugierten Körpern übereinstimmt, heißt ein **Galoisscher Körper.** Ist k ein beliebiger Zahlkörper m-ten Grades, und sind $k', \ldots, k^{(m-1)}$ die zu k konjugierten Körper, so kann aus sämtlichen Zahlen der Körper $k, k', \ldots, k^{(m-1)}$ ein neuer Körper K zusammengesetzt werden; dieser Körper K ist dann notwendig ein Galoisscher Körper, welcher die Körper $k, k', \ldots, k^{(m-1)}$ als Unterkörper enthält. Ein jeder beliebige Körper k kann mithin stets als ein Körper aufgefaßt werden, welcher in einem Galoisschen Körper als Unterkörper enthalten ist. Infolge dieses Umstandes ist es keine wesentliche Einschränkung, wenn wir bei der Erforschung der Eigenschaften der algebraischen Zahlen von vornherein einen Galoisschen Körper zugrunde legen und dann entwickeln, in welcher Weise die Zerlegungsgesetze für die Ideale dieses Galoisschen Körpers sich auf einen beliebigen in ihm enthaltenen Unterkörper übertragen.

Was zunächst den Beweis für die eindeutige Zerlegung der Ideale in Primideale betrifft, so gestaltet sich derselbe für einen Galoisschen Körper außerordentlich einfach [HILBERT (*2*, *3*.)]. Um dies einzusehen, setzen wir zunächst einige Bezeichnungen fest.

Der Galoissche Körper K vom M-ten Grade werde durch die ganze Zahl Θ bestimmt; Θ genügt dann einer irreduziblen Gleichung M-ten Grades mit ganzen rationalen Koeffizienten. Die M Wurzeln dieser Gleichung seien

$$s_1\Theta = \Theta, \quad s_2\Theta, \ldots, s_M\Theta,$$

wo $s_1, \ldots, s_M$ rationale Funktionen von Θ mit rationalen Koeffizienten bedeuten. Werden $s_1, \ldots, s_M$ als Substitutionen aufgefaßt, so bilden sie eine Gruppe G vom M-ten Grade, da ja die aufeinander folgende Anwendung irgend zweier von den Substitutionen $s_1, \ldots, s_M$ wiederum eine dieser Substitutionen ergeben muß. G heiße die **Gruppe des Galoisschen Körpers** K.

Ein Ideal $\mathfrak{J}$, welches ungeändert bleibt, wenn man die Zahlen desselben durch ihre Konjugierten ersetzt, d. h. wenn man sie einer der $M-1$ Substitutionen $s_2, \ldots, s_M$ unterwirft, nenne ich ein **invariantes Ideal.** Ein invariantes Ideal $\mathfrak{J}$ besitzt die folgende Eigenschaft:

Hilfssatz 11. Die $M!$-te Potenz eines jeden invarianten Ideals $\mathfrak{J}$ ist gleich einer ganzen rationalen Zahl.

Beweis. Es sei A eine Zahl des Ideals $\mathfrak{J}$, und $A_1, A_2, \ldots, A_M$ seien die M elementaren symmetrischen Funktionen von $\mathsf{A} = s_1\mathsf{A}, s_2\mathsf{A}, \ldots, s_M\mathsf{A}$. Den größten gemeinsamen Teiler der M ganzen rationalen Zahlen

$$A_1^{\frac{M!}{1}}, \quad A_2^{\frac{M!}{2}}, \ldots, A_M^{\frac{M!}{M}} \tag{18}$$

bezeichnen wir mit A. In gleicher Weise denken wir uns zu jeder anderen Zahl $\mathsf{B}, \Gamma \ldots$ des Ideals $\mathfrak{J}$ und ihren konjugierten die betreffenden elementaren symmetrischen Funktionen berechnet und die Teiler $B, C, \ldots$ in entsprechender Weise abgeleitet. Der größte gemeinsame Teiler aller möglichen dabei auftretenden Zahlen $A, B, C, \ldots$ werde mit J bezeichnet. Dann ist $\mathfrak{J}^{M!} = J$. In der Tat: da die zu A konjugierten Zahlen ebenfalls Zahlen des Ideals $\mathfrak{J}$ sind, so ist

$$A_1 \equiv 0, (\mathfrak{J}), \quad A_2 \equiv 0, (\mathfrak{J}^2), \ldots, \quad A_M \equiv 0, (\mathfrak{J}^M);$$

und folglich sind die sämtlichen Zahlen (18) und mithin auch $A \equiv 0$ nach $\mathfrak{J}^{M!}$. Da das Gleiche auch von den Zahlen $B, C, \ldots$ gilt, so ist auch $J \equiv 0$ nach $\mathfrak{J}^{M!}$. Andererseits sind die Koeffizienten $A_1, A_2, \ldots, A_M$ der Gleichung M-ten Grades für A bezüglich durch $J^{\frac{1}{M!}}, J^{\frac{2}{M!}}, \ldots, J^{\frac{M}{M!}}$ teilbar, und somit ist A selbst durch $J^{\frac{1}{M!}}$ teilbar. Da das nämliche von allen Zahlen $\mathsf{B}, \Gamma, \ldots$ des Ideals $\mathfrak{J}$ gilt, so ist $\mathfrak{J}^{M!}$ durch J teilbar.

Aus dem eben bewiesenen Hilfssatz 11 folgt unmittelbar die weitere Tatsache:

Satz 67. Zu einem jeden beliebigen Ideal $\mathfrak{A}$ des Galoisschen Körpers K läßt sich stets ein Ideal $\mathfrak{B}$ so finden, daß das Produkt $\mathfrak{AB}$ ein Hauptideal wird.

Beweis. Das Ideal $\mathfrak{J} = \mathfrak{A} \cdot s_2\mathfrak{A} \ldots s_M\mathfrak{A}$ ist offenbar ein invariantes Ideal; es ist daher nach dem Hilfssatz 11 das Ideal

$$\mathfrak{B} = \mathfrak{J}^{M!-1} s_2\mathfrak{A} \ldots s_M\mathfrak{A}$$

ein Ideal von der Art, wie es Satz 67 verlangt.

Der Satz 67 gestattet, die weiteren Teilbarkeitsgesetze für die Ideale des Galoisschen Körpers in derselben Weise zu entwickeln, wie dies in § 5 auf Grund des Satzes 8 für einen beliebigen Zahlkörper k geschehen ist.

Um dann aus den Teilbarkeitsgesetzen innerhalb des Galoisschen Körpers die Teilbarkeitsgesetze für einen beliebigen Körper k abzuleiten, beweise man

entweder zunächst im Galoisschen Körper die Kroneckerschen Sätze 13 und 14 über Formen und schließe hieraus die Richtigkeit dieser Sätze für den Unterkörper k, oder man wende ein geeignetes direktes Übergangsverfahren an [Hilbert (3)].

§ 37. Die Elemente, die Differente und die Diskriminante des Galoisschen Körpers.

Im Galoisschen Körper K erhalten manche der früher eingeführten Begriffe eine einfachere Bedeutung. So sind die Elemente eines Galoisschen Körpers stets Ideale in diesem Körper selbst, und zwar gelten die Tatsachen:

Satz 68. Die Elemente eines Galoisschen Körpers K vertauschen sich untereinander bei Anwendung einer der M Substitutionen $s_1, \ldots, s_M$. Die Differente $\mathfrak{D}$ des Körpers K ist ein invariantes Ideal, und die Diskriminante $D = \pm N(\mathfrak{D})$ ist daher, als Ideal, die M-te Potenz der Differente $\mathfrak{D}$.

Beweis. Bezeichnen wir mit $\Omega_1, \ldots, \Omega_M$ eine Basis des Körpers K, so sind die Elemente von K Ideale von der Gestalt:

$$\mathfrak{E}_2 = (\Omega_1 - s_2\,\Omega_1, \ldots, \Omega_M - s_2\,\Omega_M),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\mathfrak{E}_M = (\Omega_1 - s_M\Omega_1, \ldots, \Omega_M - s_M\Omega_M).$$

Wenden wir irgendeine der Substitutionen s auf eines dieser Elemente $\mathfrak{E}_i$ an und bedenken, daß die Zahlen $s\Omega_1, \ldots, s\Omega_M$ wiederum eine Basis des Körpers darstellen müssen, so folgt, wenn $ss_i = s_{i'}s$ gesetzt wird:

$$s\,\mathfrak{E}_i = (s\Omega_1 - s_{i'}s\Omega_1, \ldots, s\Omega_M - s_{i'}s\Omega_M) = \mathfrak{E}_{i'}.$$

Die Invarianz der Körperdifferente folgt nunmehr aus ihrer Darstellung $\mathfrak{D} = \mathfrak{E}_2 \ldots \mathfrak{E}_M$.

§ 38. Die Unterkörper des Galoisschen Körpers.

Der Galoissche Körper gestattet ein sehr genaues Studium der Zerlegungsgesetze seiner Zahlen mit Rücksicht auf die in ihm enthaltenen Unterkörper, und die hierbei sich ergebenden Resultate sind vor allem für die Anwendung der *allgemeinen* Körpertheorie auf *besondere* Zahlkörper von Wichtigkeit [Hilbert (4)].

Um einen beliebigen Unterkörper des Galoisschen Körpers in einfacher Art zu charakterisieren, bedienen wir uns folgender Ausdrucksweise. Wenn r Substitutionen $s_1 = 1, s_2, \ldots, s_r$ der Gruppe G eine Untergruppe g vom r-ten Grade liefern, so bildet offenbar die Gesamtheit aller derjenigen Zahlen des Körpers K, welche bei Anwendung einer jeden Substitution von g ungeändert bleiben, einen in K enthaltenen Körper k vom Grade $m = \frac{M}{r}$. Dieser Körper k heiße der **zur Untergruppe g gehörige Unterkörper.** Der Galoissche Körper

selbst gehört zu der Gruppe, welche allein aus $s_1 = 1$ besteht; zur Gruppe G aller M Substitutionen s gehört der Körper der rationalen Zahlen. Umgekehrt gehört ein jeder Unterkörper k des Galoisschen Körpers zu einer gewissen Untergruppe g der Gruppe G. Diese Gruppe g heiße die **den Unterkörper k bestimmende Untergruppe.**

§ 39. Der Zerlegungskörper und der Trägheitskörper eines Primideals $\mathfrak{P}$.

Wählen wir nun ein bestimmtes Primideal $\mathfrak{P}$ vom Grade f im Galoisschen Körper K aus, so gibt es eine ganz bestimmte Reihe ineinander geschachtelter Unterkörper von K, welche für das Primideal $\mathfrak{P}$ charakteristisch sind, und deren merkwürdige Eigenschaften jetzt kurz entwickelt werden sollen.

Es sei p die durch $\mathfrak{P}$ teilbare rationale Primzahl; ferner seien $z, z', z'', \ldots$ diejenigen sämtlichen r_z Substitutionen der Gruppe G, welche das Primideal $\mathfrak{P}$ ungeändert lassen; dieselben bilden eine Gruppe vom r_z-ten Grade, welche die **Zerlegungsgruppe des Primideals $\mathfrak{P}$** genannt und mit g_z bezeichnet werden soll. Der zur Zerlegungsgruppe g_z gehörige Körper k_z werde **Zerlegungskörper des Primideals $\mathfrak{P}$** genannt; derselbe ist vom Grade $m_z = \frac{M}{r_z}$.

Weiter seien $t, t', t'', \ldots$ sämtliche unter den Substitutionen s der Gruppe G von der Beschaffenheit, daß für jede beliebige ganze Zahl Ω des Körpers K die Kongruenz $s\Omega \equiv \Omega$ nach $\mathfrak{P}$ erfüllt ist und r_t deren Anzahl; es folgt leicht, daß diese r_t Substitutionen eine Gruppe r_t-ten Grades bilden. Diese Gruppe werde die **Trägheitsgruppe des Primideals $\mathfrak{P}$** genannt und mit g_t bezeichnet. Der zur Trägheitsgruppe g_t gehörige Körper k_t werde **Trägheitskörper des Primideals $\mathfrak{P}$** genannt; derselbe ist vom Grade $m_t = \frac{M}{r_t}$.

Das Verhältnis der Trägheitsgruppe zur Zerlegungsgruppe wird durch folgende Tatsachen klargestellt:

Satz 69. Die Trägheitsgruppe g_t des Primideals $\mathfrak{P}$ ist eine invariante Untergruppe der Zerlegungsgruppe g_z. Man erhält alle Substitutionen der Zerlegungsgruppe und jede nur einmal, wenn man die Substitutionen der Trägheitsgruppe mit $1, z, z^2, \ldots, z^{f-1}$ multipliziert, wo z eine geeignet gewählte Substitution der Zerlegungsgruppe ist.

Beweis. Es sei t eine beliebige Substitution in g_t und Ω eine durch $\mathfrak{P}$ teilbare ganze Zahl des Körpers K. Setzen wir $\Omega' = t^{-1}\Omega$, so ist infolge der Eigenschaft der Trägheitsgruppe $\Omega' \equiv t\Omega' \equiv \Omega$ nach $\mathfrak{P}$, d. h. $\Omega' \equiv 0$ nach $\mathfrak{P}$. Die Anwendung der Substitution t ergibt $\Omega \equiv 0$ nach dem Primideal $t\mathfrak{P}$. Da diese Kongruenz für jede Zahl Ω des Primideals $\mathfrak{P}$ gilt, so muß $\mathfrak{P}$ durch $t\mathfrak{P}$ teilbar sein, und folglich ist $\mathfrak{P} = t\mathfrak{P}$, d. h. die Trägheitsgruppe g_t ist eine Untergruppe der Zerlegungsgruppe g_z.

Um die übrigen Behauptungen des Satzes 69 zu beweisen, bestimmen wir eine Primitivzahl P des Primideals $\mathfrak{P}$, welche kongruent 0 nach allen zu $\mathfrak{P}$ konjugierten und von $\mathfrak{P}$ verschiedenen Primidealen ist. Die Möglichkeit der Bestimmung einer solchen Primitivzahl folgt aus Satz 25; dann bilden wir die ganzzahlige Funktion M-ten Grades von x

$$F(x) = (x - s_1\mathsf{P})(x - s_2\mathsf{P}) \ldots (x - s_M\mathsf{P}).$$

Da P eine Wurzel der ganzzahligen Kongruenz $F(x) \equiv 0$ nach $\mathfrak{P}$ ist, so genügt nach Satz 27 auch P^p der nämlichen Kongruenz, und hieraus folgt, daß es unter den M Substitutionen $s_1, \ldots, s_M$ notwendig eine Substitution s von der Art gibt, daß $s\mathsf{P} \equiv \mathsf{P}^p$ nach $\mathfrak{P}$ wird. Wäre nun $s^{-1}\mathfrak{P} \neq \mathfrak{P}$, so bestände infolge der Wahl von P die Kongruenz $\mathsf{P} \equiv 0$ nach $s^{-1}\mathfrak{P}$, und folglich müßte $s\mathsf{P} \equiv 0$ nach $\mathfrak{P}$ sein, was der vorhin gefundenen Kongruenz widerspräche.

Wegen $s\mathfrak{P} = \mathfrak{P}$ gehört die Substitution s zur Zerlegungsgruppe. Wir setzen $s = z$. Die wiederholte Anwendung der Substitution z auf die Kongruenz $z\mathsf{P} \equiv \mathsf{P}^p$ nach $\mathfrak{P}$ liefert die weiteren Kongruenzen $z^2\mathsf{P} \equiv \mathsf{P}^{p^2}$, $z^3\mathsf{P} \equiv \mathsf{P}^{p^3}, \ldots, z^f\mathsf{P} \equiv \mathsf{P}^{p^f} \equiv \mathsf{P}$ nach $\mathfrak{P}$. Infolge der letzten Kongruenz ist z^f eine Substitution der Trägheitsgruppe. Denn jede beliebige ganze Zahl Ω des Körpers K kann in der Gestalt $\Omega = \mathsf{P}^a + \Pi$ oder $= \Pi$ dargestellt werden, wo a eine ganze rationale Zahl und Π eine durch $\mathfrak{P}$ teilbare Zahl des Körpers bedeutet. Wegen $z^f\mathfrak{P} = \mathfrak{P}$ folgt daraus in der Tat $z^f\Omega \equiv \Omega$ nach $\mathfrak{P}$.

Die Kongruenz $z\mathsf{P} \equiv \mathsf{P}^p$ nach $\mathfrak{P}$ lehrt, daß $z^{-1}tz\mathsf{P} \equiv \mathsf{P}$ nach $\mathfrak{P}$ ist, wo t eine beliebige Substitution der Trägheitsgruppe g_t bedeutet. Setzen wir $z' = z^{-1}tz$ und verstehen unter Ω eine beliebige ganze Zahl des Körpers K, so folgt, wenn Ω der Kongruenz $\Omega \equiv \mathsf{P}^a$ nach $\mathfrak{P}$ genügt, $z'\Omega \equiv (z'\mathsf{P})^a \equiv \mathsf{P}^a \equiv \Omega$ nach $\mathfrak{P}$, und desgleichen, wenn $\Omega \equiv 0$ nach $\mathfrak{P}$ ist, d. h. $z' = z^{-1}tz$ gehört der Trägheitsgruppe an.

Es sei nun $P(\mathsf{P})$ diejenige ganzzahlige Funktion f-ten Grades von P, welche $\equiv 0$ nach $\mathfrak{P}$ ist; nach Satz 27 hat die Kongruenz $P(x) \equiv 0$ nach $\mathfrak{P}$ die Wurzeln $\mathsf{P}, \mathsf{P}^p, \ldots, \mathsf{P}^{p^{f-1}}$, und nach Satz 26 besitzt sie keine anderen Kongruenzwurzeln.

Ist nun z^* eine beliebige Substitution der Zerlegungsgruppe, so folgt aus der Kongruenz $P(\mathsf{P}) \equiv 0$ nach $\mathfrak{P}$ notwendig $P(z^*\mathsf{P}) \equiv 0$, und daher muß $z^*\mathsf{P} \equiv \mathsf{P}^{p^i}$ nach $\mathfrak{P}$ sein, wo i einen der f Werte $0, 1, \ldots, f-1$ hat. Da andererseits $\mathsf{P}^{p^i} \equiv z^i\mathsf{P}$ ist, so wird $z^{-i}z^*\mathsf{P} \equiv \mathsf{P}$ nach $\mathfrak{P}$, und mithin ist $z^{-i}z^*$ eine Substitution t der Trägheitsgruppe, d. h. $z^* = z^it$. In dieser letzteren Gestalt sind also sämtliche Substitutionen $z, z', z'', \ldots$ der Zerlegungsgruppe darstellbar, und da auch umgekehrt z^it für $i = 0, 1, \ldots, f-1$ lauter von einander verschiedene Substitutionen darstellt, so ist der letzte Teil des Satzes 69 bewiesen. Endlich erhellt jetzt auch die Invarianz der Trägheitsgruppe aus der oben bewiesenen Tatsache, daß $z^{-1}tz$ stets zu dieser Gruppe gehört.

Zugleich ergibt sich $r_z = fr_t$.

§ 40. Ein Satz über den Zerlegungskörper.

Die wichtigste Eigenschaft des Zerlegungskörpers findet in folgendem Satze ihren Ausdruck:

Satz 70. Das Ideal $\mathfrak{p} = \mathfrak{P}^{r'}$ liegt im Zerlegungskörper k_z und ist in diesem ein Primideal ersten Grades. Im Zerlegungskörper k_z wird $p = \mathfrak{p}\mathfrak{a}$, wo $\mathfrak{a}$ ein zu $\mathfrak{p}$ primes Ideal ist.

Beweis. Die Relativnorm des Primideals $\mathfrak{P}$ in bezug auf den Körper k_z ist $N_{k_z}(\mathfrak{P}) = \mathfrak{P}^{r_z}$. Um nun die niedrigste in k_z liegende Potenz des Primideals $\mathfrak{P}$ zu ermitteln, denken wir uns den größten gemeinsamen Teiler aller derjenigen ganzen Zahlen des Körpers k_z bestimmt, welche durch $\mathfrak{P}$ teilbar sind. Dieser Teiler ist notwendig im Körper k_z ein Primideal $\mathfrak{p}$, und, da $\mathfrak{P}^{r_z}$ in k_z liegt, so ist $\mathfrak{p}$ jedenfalls eine Potenz von $\mathfrak{P}$; wir setzen $\mathfrak{p} = \mathfrak{P}^u$. Zur Bestimmung des Exponenten u dient die folgende Betrachtung. Soll eine durch $\mathfrak{P}$ nicht teilbare Zahl A des Körpers K der Kongruenz $\mathsf{A} \equiv z\mathsf{A}$ nach $\mathfrak{P}$ genügen, und ist etwa $\mathsf{A} \equiv \mathsf{P}^i$ nach $\mathfrak{P}$, so muß notwendig $i \equiv pi$ nach $p^f - 1$ und folglich i eine durch $1 + p + p^2 + \cdots + p^{f-1}$ teilbare Zahl sein, d. h. es gibt nur $p - 1$ einander nach $\mathfrak{P}$ inkongruente Zahlen von der gewünschten Beschaffenheit, und es wird daher $\mathsf{A} \equiv a$ nach $\mathfrak{P}$, wo a eine ganze rationale Zahl bedeutet. Aus dieser Betrachtung folgt insbesondere, daß jede Zahl α des Körpers k_z einer rationalen Zahl a nach $\mathfrak{P}$ und mithin auch nach $\mathfrak{p}$ kongruent ist, d. h. $\mathfrak{p}$ ist im Körper k_z ein Primideal ersten Grades, und die Norm $n(\mathfrak{p})$ im Körper k_z ist folglich gleich p. Andererseits ist die Norm von $\mathfrak{p}$ im Körper K durch die Formel $N(\mathfrak{p}) = [n(\mathfrak{p})]^{r_z}$ gegeben, und wegen $\mathfrak{p} = \mathfrak{P}^u$ und $N(\mathfrak{P}) = p^f$ folgt somit $p^{uf} = p^{r_z}$, d. h. $u = r_t$.

Aus der Definition der Zerlegungsgruppe ergibt sich $N(\mathfrak{P}) = \mathfrak{P}^{r_z}\mathfrak{A}$, wo $\mathfrak{A}$ ein zu $\mathfrak{P}$ primes Ideal bedeutet. Setzen wir $p = \mathfrak{p}\mathfrak{a}$, so wird $N(\mathfrak{P}) = p^f = \mathfrak{p}^f\mathfrak{a}^f$ und folglich $\mathfrak{a}^f = \mathfrak{A}$, womit auch der letzte Teil des Satzes 70 bewiesen ist.

§ 41. Der Verzweigungskörper eines Primideals $\mathfrak{P}$.

Um den Bau der Trägheitsgruppe näher zu erforschen, bezeichnen wir jetzt mit A eine feste durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbare Zahl des Körpers K und ermitteln für alle Substitutionen $t, t', t'', \ldots$ der Trägheitsgruppe die Kongruenzen

$$\left.\begin{aligned} t\,\mathsf{A} &\equiv \mathsf{P}^a\,\mathsf{A},\\ t'\,\mathsf{A} &\equiv \mathsf{P}^{a'}\,\mathsf{A},\\ t''\,\mathsf{A} &\equiv \mathsf{P}^{a''}\mathsf{A},\\ &\cdots\cdots \end{aligned}\right\} \quad (\mathfrak{P}^2),$$

wo $a, a', a'', \ldots$ Zahlen aus der Reihe $0, 1, 2, \ldots, p^f - 2$ bedeuten. Diejenigen unter den Substitutionen $t, t', t'', \ldots$, für welche die betreffenden Exponenten $a, a', a'', \ldots$ den Wert 0 haben, mögen mit $v, v', v'', \ldots$ bezeichnet werden; ihre Anzahl sei r_v; sie bilden, wie leicht ersichtlich, eine invariante Untergruppe der Trägheitsgruppe. Diese Untergruppe r_v-ten Grades werde die **Verzweigungsgruppe des Primideals** $\mathfrak{P}$ genannt und mit g_v bezeichnet. Der zu g_v gehörige Körper k_v heiße der **Verzweigungskörper des Primideals** $\mathfrak{P}$. Das Verhältnis der Verzweigungsgruppe zur Trägheitsgruppe wird genauer durch folgenden Satz charakterisiert:

Satz 71. Die Verzweigungsgruppe g_v ist eine invariante Untergruppe der Trägheitsgruppe; der Grad r_v derselben ist eine Potenz von p, etwa $r_v = p^l$. Man erhält alle Substitutionen der Trägheitsgruppe und jede nur einmal, indem man die Substitutionen der Verzweigungsgruppe mit $1, t, t^2, \ldots, t^{h-1}$ multipliziert, wo $h = \frac{r_t}{r_v}$ und t eine geeignet gewählte Substitution der Trägheitsgruppe ist. Die Zahl h ist ein Teiler von $p^f - 1$.

Beweis. Es sei $\mathfrak{P}^u$ eine so hohe Potenz von $\mathfrak{P}$, daß für jede von 1 verschiedene Substitution v der Verzweigungsgruppe die Inkongruenz $v\mathsf{A} \not\equiv \mathsf{A}$ nach $\mathfrak{P}^u$ gilt. Setzen wir nun $v\mathsf{A} \equiv \mathsf{A} + \mathsf{B}\mathsf{A}^2$ nach $\mathfrak{P}^3$, wo B eine ganze Zahl in K bedeutet, so folgt leicht $v^p\,\mathsf{A} \equiv \mathsf{A}$ nach $\mathfrak{P}^3$ und hieraus in entsprechender Weise $v^{p^2}\mathsf{A} \equiv \mathsf{A}$ nach $\mathfrak{P}^4$ usw., endlich $v^{p^{u-2}}\mathsf{A} \equiv \mathsf{A}$ nach $\mathfrak{P}^u$. Demnach ist $v^{p^{u-2}} = 1$, d. h. der Grad r_v der Verzweigungsgruppe ist gleich einer Potenz von p; wir setzen $r_v = p^l$.

Es sei nun a der kleinste von 0 verschiedene unter den Exponenten $a, a', a'', \ldots$, und es gebe im ganzen h verschiedene Zahlen unter diesen Exponenten. Dann sind diese Zahlen notwendig Vielfache von a und stimmen mit den Zahlen $0, a, 2a, \ldots, (h-1)a$ überein; es ist ferner $ha = p^f - 1$. Zugleich erkennen wir, daß alle Substitutionen der Trägheitsgruppe in die Gestalt $t^i v$ gebracht werden können, wo i die Werte $0, 1, \ldots, h-1$ annimmt und v alle Substitutionen der Verzweigungsgruppe g_v durchläuft. Es ist folglich $r_t = hr_v$.

§ 42. Ein Satz über den Trägheitskörper.

Über das Verhalten der Ideale $\mathfrak{P}$ und $\mathfrak{p}$ im Körper k_t gibt der folgende Satz Aufschluß:

Satz 72. Jede Zahl des Körpers K ist nach $\mathfrak{P}$ einer Zahl des Trägheitskörpers kongruent. Der Trägheitskörper bewirkt keine Zerlegung des Ideals $\mathfrak{p}$, sondern nur eine Graderhöhung desselben, insofern $\mathfrak{p}$ beim Übergang vom Körper k_z in den oberen Körper k_t aus einem Primideal ersten Grades sich in ein Primideal f-ten Grades verwandelt.

Beweis. Wir setzen

$$\pi = \{v\,\mathsf{P}\cdot v'\,\mathsf{P}\cdot v''\,\mathsf{P}\ldots\}^{p^{l(f-1)}},$$

$$\varkappa = \frac{1}{h}(\pi + t\pi + t^2\pi + \cdots + t^{h-1}\pi);$$

unter P wieder eine Primitivzahl nach $\mathfrak{P}$ und unter t die Substitution aus Satz 71

verstanden; die Zahl π liegt im Körper k_v und die Zahl $\varkappa$ im Körper k_t. Um letzteres zu beweisen, bedenke man, daß die Zahl $\varkappa$ bei Anwendung der Substitution t ungeändert bleibt, weil t^h zu g_v gehört, und daß die Zahlen $\pi, t\pi, t^2\pi, \ldots, t^{h-1}\pi$ bei Anwendung einer Substitution aus g_v ungeändert bleiben. Diese Zahlen π und $\varkappa$ sind, wie man leicht einsieht, beide nach dem Primideal $\mathfrak{P}$ der Primitivzahl P kongruent. Da es folglich im Körper k_t genau p^f nach $\mathfrak{P}$ inkongruente Zahlen gibt, so ist notwendigerweise $\mathfrak{p} = \mathfrak{P}^n$ im Körper k_t unzerlegbar und wird in demselben ein Primideal f-ten Grades.

§ 43. Sätze über die Verzweigungsgruppe und den Verzweigungskörper.

Es ist nun leicht, die charakteristische Eigenschaft der Verzweigungsgruppe zu erkennen; dieselbe ist folgende:

Satz 73. Zur Verzweigungsgruppe g_v gehören alle und nur solche Substitutionen s, bei deren Anwendung für sämtliche ganze Zahlen Ω des Körpers K die Kongruenz $s\Omega \equiv \Omega$ nach $\mathfrak{P}^2$ besteht.

Beweis. Es sei die beliebige Zahl Ω in K der Zahl ω des Trägheitskörpers nach $\mathfrak{P}$ kongruent, und dementsprechend werde $\Omega - \omega \equiv \mathsf{BA}$ nach $\mathfrak{P}^2$ gesetzt, wo A die Bedeutung wie in § 41 hat und B eine geeignete ganze Zahl in K ist. Durch die Anwendung einer Substitution v des Verzweigungskörpers ergibt sich $v\Omega - \omega \equiv v(\mathsf{BA}) \equiv \mathsf{BA} \equiv \Omega - \omega$, d. h. $v\Omega \equiv \Omega$ nach $\mathfrak{P}^2$.

Zugleich erkennen wir leicht den folgenden weiteren Satz über den Verzweigungskörper:

Satz 74. Das Ideal $\mathfrak{p}_v = \mathfrak{P}^{r_v}$ liegt im Verzweigungskörper und ist in demselben ein Primideal f-ten Grades: es findet somit im Verzweigungskörper die Spaltung des Ideals $\mathfrak{p} = \mathfrak{p}_v^h$ in h gleiche Primfaktoren statt.

§ 44. Die überstrichenen Verzweigungskörper eines Primideals $\mathfrak{P}$.

Unsere nächste Aufgabe besteht darin, weiter die Spaltung des Ideals $\mathfrak{p}_v$ in gleiche Faktoren zu verfolgen. Zu dem Zweck nehmen wir an, es sei L der höchste Exponent von der Art, daß für eine jede Substitution v der Verzweigungsgruppe die sämtlichen ganzen Zahlen des Körpers K der Kongruenz $v\Omega \equiv \Omega$ nach $\mathfrak{P}^L$ genügen, und bestimmen dann alle Substitutionen s der Verzweigungsgruppe, für welche $s\Omega \equiv \Omega$ nach $\mathfrak{P}^{L+1}$ wird; dieselben bilden eine Untergruppe $g_{\bar{v}}$ der Verzweigungsgruppe, die wir die **einmal überstrichene Verzweigungsgruppe des Primideals** $\mathfrak{P}$ nennen. Der zu $g_{\bar{v}}$ gehörige Körper $k_{\bar{v}}$ heiße der **einmal überstrichene Verzweigungskörper des Primideals.** Die wichtigsten Eigenschaften dieses Körpers sind folgende:

Satz 75. Die einmal überstrichene Verzweigungsgruppe $g_{\bar{v}}$ ist eine invariante Untergruppe der Verzweigungsgruppe g_v. Der Grad von $g_{\bar{v}}$ sei $r_{\bar{v}} = p^{\bar{\imath}}$. Man erhält alle Substitutionen der Verzweigungsgruppe g_v und jede nur einmal, indem man die Substitutionen der einmal überstrichenen Verzweigungsgruppe $g_{\bar{v}}$ mit gewissen $p^{\bar{e}}$ Substitutionen $v_1, \ldots, v_{p^{\bar{e}}}$ der Verzweigungsgruppe g_v multipliziert; dabei haben diese $p^{\bar{e}}$ Substitutionen die Besonderheit, daß für irgend zwei derselben v_i und $v_{i'}$ stets eine Relation von der Gestalt $v_i v_{i'} = v_{i''} v_i \bar{v}$ besteht, wo $\bar{v}$ eine Substitution in $g_{\bar{v}}$ ist. Das Ideal $\mathfrak{p}_{\bar{v}} = \mathfrak{P}^{r_{\bar{v}}}$ ist Primideal in $k_{\bar{v}}$: es findet somit in $k_{\bar{v}}$ die Spaltung des Ideals $\mathfrak{p}_v = \mathfrak{p}_{\bar{v}}^{p^{\bar{e}}}$ in $p^{\bar{e}}$ gleiche Primfaktoren statt; dabei ist der Exponent $\bar{e}$ eine Zahl, die den Grad f des Primideals $\mathfrak{P}$ nicht überschreitet.

Beweis. Es sei A eine durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbare ganze Zahl des Körpers K; wir bestimmen dann ein System von Substitutionen $v_1, \ldots, v_r$ der Verzweigungsgruppe von der Art, daß, wenn

$$v_1\mathsf{A} \equiv \mathsf{A} + \mathsf{B}_1\mathsf{A}^L, \ \ldots, \ v_r\mathsf{A} \equiv \mathsf{A} + \mathsf{B}_r\mathsf{A}^L, \quad (\mathfrak{P}^{L+1})$$

gesetzt wird, die ganzen Zahlen $\mathsf{B}_1, \ldots, \mathsf{B}_r$ sämtlich einander nach $\mathfrak{P}$ inkongruent sind und auch keine Substitution von g_v zu diesem Systeme $v_1, \ldots, v_r$ hinzugefügt werden kann, ohne der letzteren Forderung zu widersprechen. Wählen wir dann eine beliebige Substitution v^* der Verzweigungsgruppe g_v und setzen $v^*\mathsf{A} \equiv \mathsf{A} + \mathsf{BA}^L$ nach $\mathfrak{P}^{L+1}$, so muß B einer der Zahlen $\mathsf{B}_1, \ldots, \mathsf{B}_r$ nach $\mathfrak{P}$ kongruent sein; ist etwa $\mathsf{B} \equiv \mathsf{B}_i$ nach $\mathfrak{P}$, so folgt $v_i^{-1}v^*\mathsf{A} \equiv \mathsf{A}$ nach $\mathfrak{P}^{L+1}$. Aus Satz 72 folgt, daß jede ganze Zahl Ω in K einem Ausdrucke $\alpha_t + \beta_t\mathsf{A} + \cdots + \lambda_t\mathsf{A}^L$ nach $\mathfrak{P}^{L+1}$ kongruent ist, wo $\alpha_t, \beta_t, \ldots, \lambda_t$ ganze Zahlen des Trägheitskörpers sind, und hieraus ergibt sich für Ω die Kongruenz $v_i^{-1}v^*\Omega \equiv \Omega$ nach $\mathfrak{P}^{L+1}$, d. h. es ist $v_i^{-1}v^* = \bar{v}$ oder $v^* = v_i\bar{v}$. Diese Gleichung beweist die im Satze 75 behauptete Struktur der Gruppe $g_{\bar{v}}$.

Wir setzen $r_{\bar{v}} = p^{\bar{\imath}}$ und $\bar{e} = l - l$.

Es ist nunmehr ersichtlich, in welcher Weise das eingeschlagene Verfahren fortzusetzen ist. Bedeutet $\bar{L}$ den höchsten Exponenten von der Art, daß für jede Substitution $\bar{v}$ die sämtlichen Zahlen des Körpers K der Kongruenz $\bar{v}\Omega \equiv \Omega$ nach $\mathfrak{P}^{\bar{L}}$ genügen, so bestimmen wir alle die Substitutionen $\bar{v}$, für welche beständig $\bar{v}\Omega \equiv \Omega$ nach $\mathfrak{P}^{\bar{L}+1}$ wird. Dieselben bilden eine invariante Untergruppe $g_{\bar{\bar{v}}}$ der Gruppe $g_{\bar{v}}$: die **zweimal überstrichene Verzweigungsgruppe des Primideals** $\mathfrak{P}$; ihr Grad sei $r_{\bar{\bar{v}}} = p^{\bar{\bar{\imath}}}$; wir setzen $\bar{\bar{e}} = \bar{l} - \bar{\bar{l}}$. Es wird $\mathfrak{p}_{\bar{v}} = \mathfrak{p}_{\bar{\bar{v}}}^{p^{\bar{\bar{e}}}}$, wo $\mathfrak{p}_{\bar{v}}$ ein Primideal des zu $g_{\bar{\bar{v}}}$ gehörigen Körpers $k_{\bar{\bar{v}}}$ ist.

So fortfahrend, gelangen wir zur **dreimal überstrichenen Verzweigungsgruppe** $g_{\bar{\bar{\bar{v}}}}$ usw. Ist etwa die i-**mal überstrichene Verzweigungsgruppe des Primideals** $\mathfrak{P}$ diejenige, welche lediglich aus der Substitution 1 besteht, so ist der i-**mal überstrichene Verzweigungskörper des Primideals** $\mathfrak{P}$ der Körper K selbst und die Struktur der Verzweigungsgruppe g_v ist dann genau bekannt. Es leuchtet ein, daß für das Primideal $\mathfrak{P}$ überstrichene Verzweigungskörper nur dann vorhanden sein können, wenn der Grad M des Körpers K durch p teilbar ist.

§ 45. Kurze Zusammenfassung der Sätze über die Zerlegung einer rationalen Primzahl p im Galoisschen Körper.

Durch die in § 39—44 entwickelten Sätze erlangen wir einen vollständigen Einblick in die bei der Zerlegung einer rationalen Primzahl p in einem Galoisschen Körper sich abspielenden Vorgänge:

Es handle sich um einen bestimmten Primfaktor $\mathfrak{P}$ von p, so wird p zunächst im Zerlegungskörper von $\mathfrak{P}$ in der Form $p = \mathfrak{p}\mathfrak{a}$ zerlegt, wo $\mathfrak{p}$ ein Primideal ersten Grades und $\mathfrak{a}$ ein durch $\mathfrak{p}$ nicht teilbares Ideal des Zerlegungskörpers ist. Der Zerlegungskörper von $\mathfrak{P}$ ist als Unterkörper in dem Trägheitskörper von $\mathfrak{P}$ enthalten, welcher seinerseits keine weitere Zerlegung von $\mathfrak{p}$ bewirkt, sondern lediglich dieses Ideal $\mathfrak{p}$ zu einem Primideal f-ten Grades erweitert. Ist der Körper K selbst der Zerlegungskörper oder der Trägheitskörper, so ist nach diesem ersten Schritte die Zerlegung bereits abgeschlossen. Im anderen Falle läßt sich $\mathfrak{p}$ für K noch in gleiche Faktoren spalten, und zwar wird $\mathfrak{p}$ zunächst im Verzweigungskörper die Potenz eines Primideals $\mathfrak{p}_v$, wobei der Exponent in $p^f - 1$ aufgeht und folglich nicht durch p teilbar ist. Die Spaltung von $\mathfrak{p}$ ist mit diesem zweiten Schritte notwendig dann und nur dann abgeschlossen, wenn p im Grade der Trägheitsgruppe nicht aufgeht und mithin der Körper K selbst der Verzweigungskörper ist. In den nun folgenden überstrichenen Verzweigungskörpern schreitet die Spaltung ohne Aussetzen fort, und zwar sind die bezüglichen Potenzexponenten Zahlen von der Gestalt $p^{\overline{e}}, p^{\overline{\overline{e}}}, \ldots$, wo keiner der Exponenten $\overline{e}, \overline{\overline{e}}, \ldots$ den Grad f des Primideals $\mathfrak{P}$ überschreitet.

Die Übersicht über die entwickelten Resultate wird durch die folgende Tabelle erleichtert, in deren Zeilen der Reihe nach die betreffenden Körper, die

k_s	k_t	k_v	$k_{\overline{v}}$	$k_{\overline{\overline{v}}}$	K
r_s	r_t	r_v	$r_{\overline{v}}$	$r_{\overline{\overline{v}}}$	1
$m_s = \frac{M}{r_s}$	$m_t = \frac{M}{r_t}$	$m_v = \frac{M}{r_v}$	$m_{\overline{v}} = \frac{M}{r_{\overline{v}}}$	$m_{\overline{\overline{v}}} = \frac{M}{r_{\overline{\overline{v}}}}$	M
	$f = \frac{r_s}{r_t}$	$h = \frac{r_t}{r_v}$	$p^{\overline{e}} = \frac{r_v}{r_{\overline{v}}}$	$p^{\overline{\overline{e}}} = \frac{r_v}{r_{\overline{\overline{v}}}}$	$p^{\overline{\overline{e}}} = r_{\overline{\overline{v}}}$
$\mathfrak{p} = \mathfrak{p}_v^h = \mathfrak{P}^{r_t}$		$\mathfrak{p}_v = \mathfrak{p}_{\overline{v}}^{p^{\overline{e}}} = \mathfrak{P}^{r_v}$	$\mathfrak{p}_{\overline{v}} = \mathfrak{p}_{\overline{\overline{v}}}^{p^{\overline{\overline{e}}}} = \mathfrak{P}^{r_{\overline{v}}}$	$\mathfrak{p}_{\overline{\overline{v}}} = \mathfrak{P}^{p^{\overline{\overline{e}}}} = \mathfrak{P}^{r_{\overline{\overline{v}}}}$	$\mathfrak{P}$

Grade der zugehörigen Gruppen, die Grade der Körper, ihre Relativgrade in bezug auf den nächst niederen Körper, dann die Primideale der Körper und

ihre Darstellung als Potenzen von $\mathfrak{P}$ sich angegeben finden. Der Körper K ist dabei als ein dreimal überstrichener Verzweigungskörper angenommen. Die sämtlichen in der Tabelle vorkommenden Gradzahlen und Exponenten haben für jedes in p aufgehende Primideal des Körpers K die gleichen Werte wie für $\mathfrak{P}$ und sind daher durch die Primzahl p allein völlig bestimmt.

11. Die Differenten und Diskriminanten des Galoisschen Körpers und seiner Unterkörper.

§ 46. Die Differenten des Trägheitskörpers und der Verzweigungskörper.

Eine reiche Quelle neuer Wahrheiten entspringt, wenn wir die soeben gewonnenen Resultate mit denjenigen des Kapitels 5 in Zusammenhang bringen. So folgt unter Benutzung des Satzes 41 leicht ein Satz, welcher die wichtigste Eigenschaft des Trägheitskörpers aussagt; derselbe lautet:

Satz 76. Die Differente des zum Primideal $\mathfrak{P}$ gehörigen Trägheitskörpers ist nicht durch $\mathfrak{P}$ teilbar. Der Trägheitskörper umfaßt sämtliche in K enthaltenen Unterkörper, deren Differenten nicht durch $\mathfrak{P}$ teilbar sind.

Betreffs der Differenten der Verzweigungskörper gelten folgende Sätze:

Satz 77. Die Relativdifferente des Verzweigungskörpers in bezug auf den Trägheitskörper ist durch $\mathfrak{P}^{r_t - r_v} = \mathfrak{p}_v^{h-1}$ und durch keine höhere Potenz von $\mathfrak{P}$ teilbar.

Beweis. Nach Satz 41 gilt $\mathfrak{D}_t(K) = \mathfrak{D}_v(K)\,\mathfrak{d}_t(k_v)$, wo $\mathfrak{D}_t(K)$, $\mathfrak{D}_v(K)$, $\mathfrak{d}_t(k_v)$ bez. die Relativdifferenten von K in bezug auf k_t, von K in bezug auf k_v und von k_v in bezug auf k_t sind. Wenn Ξ die Fundamentalform von K ist, gilt also, daß der Inhalt der Form $\Pi(\Xi - t\,\Xi)$ gleich dem Inhalt der Form $\Pi(\Xi - v\,\Xi)$ mal $\mathfrak{d}_t(k_v)$ ist; dabei durchläuft in dem ersten Produkt t alle Substitutionen der Trägheitsgruppe, in dem zweiten Produkt v alle Substitutionen der Verzweigungsgruppe. Sämtliche Faktoren $\Xi - v\,\Xi$ treten auch unter den Faktoren $\Xi - t\,\Xi$ auf, die übrigen sind nach der Definition der Verzweigungsgruppe durch $\mathfrak{P}$ aber durch keine höhere Potenz von $\mathfrak{P}$ teilbar. Aus

$$(h-1)\,r_v = r_t - r_v$$

folgt dann die Behauptung. In ähnlicher Weise folgt die Tatsache:

Satz 78. Die Relativdifferente des einmal überstrichenen Verzweigungskörpers $k_{\overline{v}}$ in bezug auf den Verzweigungskörper k_v enthält genau die Potenz $\mathfrak{P}^{L(r_v - r_{\overline{v}})} = \mathfrak{p}_{\overline{v}}^{L(p^{\overline{e}}-1)}$. Die Relativdifferente des zweimal überstrichenen Verzweigungskörpers $k_{\overline{\overline{v}}}$ in bezug auf $k_{\overline{v}}$ enthält genau die Potenz $\mathfrak{P}^{L(r_{\overline{v}} - r_{\overline{\overline{v}}})} = \mathfrak{p}_{\overline{\overline{v}}}^{L(p^{\overline{\overline{e}}}-1)}$ usw.

§ 47. Die Teiler der Diskriminante des Galoisschen Körpers.

Satz 79. Der Exponent der Potenz, zu welcher die rationale Primzahl p in der Diskriminante D des Körpers K als Faktor vorkommt, ist

$$m_t\{r_t - r_v + L(r_v - r_{\bar{v}}) + \bar{L}(r_{\bar{v}} - r_{\bar{\bar{v}}}) + \cdots\}.$$

Beweis. Der Satz 41 lehrt in Verbindung mit den oben ausgesprochenen Sätzen 76, 77 und 78, daß die Differente $\mathfrak{D}$ des Körpers K das Primideal $\mathfrak{P}$ genau in der $r_t - r_v + L(r_v - r_{\bar{v}}) + \bar{L}(r_{\bar{v}} - r_{\bar{\bar{v}}}) + \cdots$-ten Potenz enthält. Hieraus folgt nach Satz 68 die Richtigkeit der Behauptung.

Im Falle, daß keine überstrichenen Verzweigungskörper vorhanden sind, kommt bereits das Glied mit L nicht mehr in Frage, und es folgt dann, daß der Exponent der in D aufgehenden Potenz von p den Wert $m_t(r_t - 1)$ besitzt. Nach dem Obigen tritt dieser Fall sicher dann ein, wenn der Grad M zu p prim ist. Man vergleiche die Bemerkungen am Schluß des § 12.

Satz 80. Der Exponent der in der Diskriminante D aufgehenden Potenz von der rationalen Primzahl p überschreitet nicht eine gewisse Grenze, die nur vom Grade M des Galoisschen Körpers K abhängt.

Beweis. Alle Exponenten $L, \bar{L}, \ldots$ für ein Primideal $\mathfrak{P}$ liegen unter einer durch M allein bestimmten Grenze. Um für L eine solche Grenze aufzufinden, bezeichnen wir mit ω eine durch $\mathfrak{p}_{\bar{v}}$, aber nicht durch $\mathfrak{p}_{\bar{v}}^2$ teilbare ganze Zahl in $k_{\bar{v}}$ und wählen ein System von $p^{\bar{v}}$ Substitutionen $v_1, v_2, \ldots, v_{p^{\bar{v}}}$ der Verzweigungsgruppe aus, welche durch Zusammensetzung mit $g_{\bar{v}}$ diese Gruppe g_v erzeugen. Die Zahl $\alpha = v_1\omega + v_2\omega + \cdots + v_{p^{\bar{v}}}\omega$ bleibt dann bei allen Substitutionen g_v ungeändert und gehört daher dem Körper k_v an. Andererseits ist $\omega \equiv v\omega$ nach $\mathfrak{P}^L$ und folglich $\alpha \equiv p^{\bar{v}}\omega$ nach $\mathfrak{P}^L$. Wäre nun $L > \bar{e}r_t + r_{\bar{v}}$, so müßte $\alpha \equiv 0$ nach $\mathfrak{p}^{\bar{v}}\mathfrak{p}_{\bar{v}}$, aber $\not\equiv 0$ nach $\mathfrak{p}^{\bar{v}}\mathfrak{p}_{\bar{v}}\mathfrak{P}$ sein. Setzen wir daher $p = \mathfrak{p}\mathfrak{a}$, wo $\mathfrak{a}$ ein zu $\mathfrak{p}$ primes Ideal des Zerlegungskörpers bedeutet, und bezeichnen mit γ eine durch $\mathfrak{a}$ teilbare und zu $\mathfrak{p}$ prime Zahl des Zerlegungskörpers, so ist $\beta = \frac{\alpha\gamma^{\bar{v}}}{p^{\bar{v}}}$ eine ganze Zahl in $k_{\bar{v}}$; dieselbe wäre durch $\mathfrak{p}_{\bar{v}}$, aber nicht durch $\mathfrak{p}_{\bar{v}}\mathfrak{P}$ teilbar, und mithin wäre $\mathfrak{p}_{\bar{v}}$ im Widerspruch mit Satz 75 ein Ideal des Körpers k_v. Da man in ähnlicher Weise auch für die übrigen Exponenten $\bar{L}, \ldots$ eine obere Grenze findet, so kann hiernach auch der in Satz 79 angegebene Exponent der in der Diskriminante D aufgehenden Potenz von p eine gewisse, nur vom Grade M des Körpers K abhängige Grenze nicht überschreiten.

Der Satz 80 ist besonders deshalb von Wichtigkeit, weil er die Möglichkeiten, die sich hinsichtlich der in M aufgehenden Primzahlen p bieten, von vornherein auf eine *endliche* Anzahl einschränkt. Rechnen wir alle diejenigen Körper vom Grade M, bei welchen die Zerlegung der in M aufgehenden Primzahlen für alle obigen Anzahlen die nämlichen Werte liefert, zu *einem* Typus, so folgt, daß es für einen gegebenen Grad M nur eine *endliche* Anzahl von möglichen Körpertypen gibt.

Als Beispiel für den Satz 80 diene der (im dritten Teil ausführlich behandelte) quadratische Körper, in dessen Diskriminante die ungeraden Primzahlen höchstens einfach und die Primzahl 2 höchstens zur dritten Potenz aufgeht (vgl. § 59 Satz 95).

12. Die Beziehungen der arithmetischen zu algebraischen Eigenschaften des Galoisschen Körpers.

§ 48. Der relativ-Galoissche, der relativ-Abelsche und der relativ-zyklische Körper.

Ist die Gruppe G der Substitutionen $s_1, \ldots, s_M$ eines Galoisschen Körpers K eine Abelsche Gruppe, d. h. sind die Substitutionen $s_1, \ldots, s_M$ untereinander vertauschbar, so heißt der Galoissche Körper K ein **Abelscher Körper.** Ist jene Substitutionsgruppe G insbesondere eine zyklische, d. h. sind die M Substitutionen $s_1, \ldots, s_M$ sämtlich als Potenzen einer einzigen unter ihnen darstellbar, so heißt der Abelsche Körper K ein **zyklischer Körper.**

Wenn wir die nämliche Betrachtung, welche in § 28 für die Idealklassen angestellt worden ist, auf die Substitutionen der Gruppe eines Abelschen Körpers anwenden, so ergibt sich der Satz, daß jeder Abelsche Körper aus zyklischen Körpern zusammengesetzt werden kann. Die zyklischen Körper ihrerseits lassen sich ferner stets aus solchen besonderen zyklischen Körpern zusammensetzen, deren Grade Primzahlen oder Primzahlpotenzen sind.

Die in Rede stehenden Begriffe lassen folgende Verallgemeinerung zu: Es sei Θ die Wurzel einer Gleichung l-ten Grades:

$$\Theta^l + \alpha_1\Theta^{l-1} + \cdots + \alpha_l = 0,$$

deren Koeffizienten $\alpha_1, \ldots, \alpha_l$ Zahlen eines Körpers k vom m-ten Grade sind. Diese Gleichung l-ten Grades sei überdies im Rationalitätsbereiche k irreduzibel und von der besonderen Eigenschaft, daß alle übrigen $l-1$ Wurzeln $\Theta', \ldots, \Theta^{(l-1)}$ derselben sich als ganze rationale Funktionen der Wurzel Θ darstellen lassen, wobei die Koeffizienten dieser Funktionen Zahlen des Körpers k sind. Unter dieser Voraussetzung heißt der aus Θ und den Zahlen von k gebildete Zahlkörper K vom $M = lm$-ten Grade ein **relativ-Galoisscher Körper in bezug auf** k. Der Grad l jener Gleichung ist der Relativgrad von K. Wird etwa

$$\Theta = S_1\Theta, \quad \Theta' = S_2\Theta, \ldots, \quad \Theta^{(l-1)} = S_l\Theta$$

gesetzt, so heißt die Gruppe der Substitutionen $S_1, \ldots, S_l$ die **Relativgruppe;** ist diese Gruppe eine Abelsche, so heißt der Körper K ein **relativ-Abelscher Körper in bezug auf** k. Ist die Relativgruppe zyklisch, so heißt der Körper K **relativ-zyklisch** in bezug auf k.

§ 49. Die algebraischen Eigenschaften des Trägheitskörpers und der Verzweigungskörper. Die Darstellung der Zahlen des Galoisschen Körpers durch Wurzeln im Bereiche des Zerlegungskörpers.

Mit Benutzung der eben definierten Begriffe lassen sich in sehr einfacher Weise einige wichtige algebraische Eigenschaften des Zerlegungs- und des Trägheitskörpers, sowie der Verzweigungskörper aussprechen, welche eine unmittelbare Folge der oben bewiesenen Eigenschaften ihrer Gruppen sind. Es ergeben sich folgende Tatsachen:

Satz 81. Der Trägheitskörper k_t ist relativ zyklisch vom Relativgrade f in bezug auf den Zerlegungskörper k_z. Der Verzweigungskörper k_v ist relativ zyklisch vom Relativgrade h in bezug auf den Trägheitskörper k_t. Der einmal überstrichene Verzweigungskörper $k_{\bar{v}}$ ist ein relativ Abelscher vom Relativgrade $p^{\bar{e}}$ in bezug auf den Verzweigungskörper k_v; der Körper $k_{\bar{\bar{v}}}$ ist ein relativ Abelscher vom Relativgrade $p^{\bar{\bar{e}}}$ in bezug auf $k_{\bar{v}}$ usf. Die Abelschen Relativgruppen der Körper $k_{\bar{v}}, k_{\bar{\bar{v}}}, \ldots$ enthalten lediglich Substitutionen vom p-ten Grade.

Nach diesem Satze 81 geschieht also die Spaltung in *gleiche* Faktoren stets mittels einer Kette Abelscher Gleichungen, und dieses Resultat drückt eine neue überraschende Eigenschaft des Zerlegungskörpers aus:

Satz 82. *Der Zerlegungskörper eines jeden Primideals in K bestimmt einen Rationalitätsbereich, in welchem die Zahlen des ursprünglichen Galoisschen Körpers K lediglich durch Wurzelausdrücke darstellbar sind.*

Dieser Satz 82 rückt zugleich die Bedeutung der Theorie der durch Wurzelziehen lösbaren Gleichungen in helles Licht; denn er zeigt, daß bei dem Prozeß der Zerlegung der Zahlen in Primideale die wichtigsten und schwierigsten Vorgänge sich gerade in solchen Relativkörpern abspielen, deren Zahlen in einem gewissen Rationalitätsbereiche durch Wurzelausdrücke darstellbar sind.

§ 50. Die Dichtigkeit der Primideale ersten Grades und der Zusammenhang dieser Dichtigkeit mit den algebraischen Eigenschaften eines Zahlkörpers.

Es ist eine merkwürdige Tatsache, daß die Häufigkeit gewisser Primideale ersten Grades in einem Zahlkörper Schlüsse auf die algebraische Natur desselben zuläßt [Kronecker (*14*)].

Es sei k ein beliebiger Zahlkörper m-ten Grades, und es bedeute allgemein p_i eine rationale Primzahl, in der genau i voneinander verschiedene Primideale ersten Grades aufgehen. Wenn dann der Limes

$$\lim_{s=1}\left\{\frac{\sum_{(p_i)}\frac{1}{p_i^s}}{\log\left(\frac{1}{s-1}\right)}\right\}$$

existiert, wo die im Zähler stehende Summe über alle Primzahlen p_i zu erstrecken ist, so sagen wir: die Primzahlen von der Art p_i besitzen eine Dichtigkeit; hat jener Limes den Wert Δ_i, so heiße Δ_i die **Dichtigkeit** der Primzahlen von der Art p_i. Kronecker macht bei seinen Untersuchungen die unausgesprochene Annahme, daß die Primzahlen von sämtlichen m Arten $p_1, \ldots, p_m$ Dichtigkeiten besitzen. Für den Fall, daß die Gruppe der zur Bestimmung des Körpers k dienenden Gleichungen die symmetrische ist, läßt sich bereits aus den Bemerkungen Kroneckers die Existenz der Dichtigkeiten $\Delta_1, \ldots, \Delta_m$ entnehmen; für einen beliebigen Körper k hat Frobenius die Existenz dieser Dichtigkeiten bewiesen und zugleich ihre Werte bestimmt; sie sind rationale Zahlen, die in einfacher Weise von der Gruppe der den Körper k bestimmenden Gleichungen abhängen [Frobenius (*1*)]. Es gelingt leicht der Nachweis des folgenden Satzes:

Satz 83. Wenn in einem beliebigen Körper m-ten Grades von den Primzahlen der m Arten $p_1, \ldots, p_m$ irgend $m-1$ Arten Dichtigkeiten besitzen, so besitzt auch die übrigbleibende Art eine Dichtigkeit, und die m Dichtigkeiten $\Delta_1, \ldots, \Delta_m$ erfüllen die Relation:

$$\Delta_1 + 2\Delta_2 + \cdots + m\Delta_m = 1.$$

Beweis: Wenn man die zweite der drei in § 27 angegebenen Darstellungen der Funktionen $\zeta(s)$ benutzt und den Logarithmus bildet, so ergibt sich

$$\log\zeta(s) = \sum_{(\mathfrak{p})}\frac{1}{n(\mathfrak{p})^s} + S,$$

$$S = \frac{1}{2}\sum_{(\mathfrak{p})}\frac{1}{n(\mathfrak{p})^{2s}} + \frac{1}{3}\sum_{(\mathfrak{p})}\frac{1}{n(\mathfrak{p})^{3s}} + \cdots,$$

wo die Summen über sämtliche Primideale $\mathfrak{p}$ des Körpers zu erstrecken sind. Bezeichnen wir nun die Primideale ersten Grades allgemein mit $\mathfrak{p}_1$, so wird offenbar

$$\sum_{(\mathfrak{p}_1)}\frac{1}{n(\mathfrak{p}_1)^s} = \sum_{(p_1)}\frac{1}{p_1^s} + \sum_{(p_2)}\frac{2}{p_2^s} + \cdots + \sum_{(p_m)}\frac{m}{p_m^s}, \tag{19}$$

wo links über alle Primideale $\mathfrak{p}_1$ und rechts bezüglich über alle rationalen Primzahlen $p_1, p_2, \ldots, p_m$ zu summieren ist.

Wir berücksichtigen andererseits, daß für alle Primideale $\mathfrak{p}$ von höherem als dem ersten Grade $n(\mathfrak{p}) \geqq p^2$ ist, und daß eine beliebige Primzahl p höchstens m Primideale enthält; dadurch ergibt sich:

$$\sum_{(\mathfrak{p})}\frac{1}{n(\mathfrak{p})^s} - \sum_{(\mathfrak{p}_1)}\frac{1}{n(\mathfrak{p}_1)^s} \leqq m\sum_{(p)}\frac{1}{p^{2s}} < m\sum_{(h)}\frac{1}{h^2},$$

wo die letzte Summe über alle ganzen rationalen Zahlen $h>1$ zu erstrecken ist. Desgleichen findet man:

$$S < m\left\{\sum_{(h)}\frac{1}{h^2} + \sum_{(h)}\frac{1}{h^3} + \cdots\right\} = m\sum_{(h)}\frac{1}{h(h-1)} = m.$$

Aus diesen Ungleichungen folgt, daß $\log \zeta(s) - \sum_{(\mathfrak{p}_1)} \frac{1}{n(\mathfrak{p}_1)^s}$ sich für $s = 1$ einer endlichen Grenze nähert. Nach Satz 56 hat auch der Ausdruck $\log \zeta(s) - \log \frac{1}{s-1}$ für $s = 1$ einen endlichen Grenzwert, und daher gilt das Nämliche auch von dem Ausdruck

$$\sum_{(\mathfrak{p}_1)} \frac{1}{n(\mathfrak{p}_1)^s} - \log \frac{1}{s-1},$$

d. h. es ist

$$\lim_{s=1} \frac{\sum_{(\mathfrak{p}_1)} \frac{1}{n(\mathfrak{p}_1)^s}}{\log \frac{1}{s-1}} = 1,$$

woraus unter Benutzung der Formel (19) die Behauptung folgt.

Für einen Galoisschen Körper K vom M-ten Grade ist $\Delta_1 = 0$, $\Delta_2 = 0, \ldots, \Delta_{M-1} = 0$, und daher folgt aus Satz 83:

Satz 84. In einem Galoisschen Körper M-ten Grades besitzen die in lauter Primideale ersten Grades zerfallenden Primzahlen p_M eine Dichtigkeit, und diese Dichtigkeit ist $\Delta_M = \frac{1}{M}$.

Ist k ein beliebiger Körper und K derjenige Galoissche Körper M-ten Grades, welcher aus k und den zu k konjugierten Körpern $k', \ldots, k^{(m-1)}$ zusammengesetzt ist, so stimmen, wie man leicht erkennt, die Primzahlen p_m in k mit den Primzahlen p_M in K überein, und daher besitzen die Primzahlen p_m in k eine Dichtigkeit, und diese ist gleich $\frac{1}{M}$, d. h. gleich dem reziproken Wert des Grades M seiner Galoisschen Resolvente [KRONECKER (14)].

13. Die Zusammensetzung der Zahlkörper.

§ 51. Der aus einem Körper und dessen konjugierten Körpern zusammengesetzte Galoissche Körper.

Satz 85. Wird aus den beiden Körpern k_1 und k_2 ein Körper K zusammengesetzt, so enthält die Diskriminante des zusammengesetzten Körpers K alle und nur diejenigen rationalen Primzahlen als Faktoren, welche in der Diskriminante von k_1 oder in derjenigen von k_2 oder in beiden aufgehen.

Der erste Teil dieses Satzes folgt unmittelbar aus Satz 39; der zweite Teil ergibt sich mit Hilfe von Satz 41 wie folgt:

Seien $\Omega_1, \ldots, \Omega_M$ bez. $\omega_1, \ldots, \omega_m$ eine Basis von K bez. k_1, dann läßt sich ω_i in der Form

$$\omega_i = a_{i1}\,\Omega_1 + \cdots + a_{iM}\,\Omega_M \qquad (i = 1, \ldots, m)$$

mit ganzen rationalen $a_{i1}, \ldots, a_{iM}$ darstellen. Sind ferner $\Omega_1^{(l)}, \ldots, \Omega_M^{(l)}$ die bezüglich k_2 relativkonjugierten Zahlen zu $\Omega_1, \ldots, \Omega_M$, so sind die Zahlen

$$\omega_i^{(l)} = a_{i1}\,\Omega_1^{(l)} + \cdots + a_{iM}\,\Omega_M^{(l)}$$

gewisse konjugierte zu ω_i, und hieraus folgt, daß die Elemente

$$(\Omega_1 - \Omega_1^{(l)}, \ldots, \Omega_M - \Omega_M^{(l)})$$

von K in gewissen Elementen von k_1 aufgehen. Nach der Definition der Relativdifferente und Satz 38 folgt hieraus die Behauptung.

Eine unmittelbare Folge des Satzes 85 ist die weitere Tatsache:

Satz 86. Wenn man aus dem Körper k vom m-ten Grade und den sämtlichen zu ihm konjugierten Körpern $k', \ldots, k^{(m-1)}$ einen Galoisschen Körper K zusammensetzt, so enthält die Diskriminante dieses Körpers K alle und nur diejenigen rationalen Primzahlen, welche in der Diskriminante des Körpers k aufgehen.

§ 52. Die Zusammensetzung zweier Körper, deren Diskriminanten zueinander prim sind.

Ein besonderes Interesse beansprucht der Fall, daß die Diskriminanten der zusammensetzenden Körper zueinander prim sind. Der wichtigste und fruchtbarste Satz über diesen Fall ist der folgende:

Satz 87. Zwei Körper k_1 und k_2 bezüglich von den Graden m_1 und m_2, deren Diskriminanten zueinander prim sind, ergeben durch Zusammensetzung stets einen Körper vom Grade $m_1 m_2$.

Beweis. Der aus k_1 und den sämtlichen zu k_1 konjugierten Körpern zusammengesetzte Galoissche Körper werde mit K_1 bezeichnet; die Diskriminante von K_1 ist nach Satz 86 prim zu der Diskriminante von k_2. Es sei ϑ eine den Körper k_1 bestimmende Zahl; dieselbe genügt einer irreduziblen Gleichung m_1-ten Grades mit ganzen rationalen Koeffizienten.

Wäre nun der aus k_1 und k_2 zusammengesetzte Körper von niederem als dem $(m_1 m_2)$-ten Grade, so müßte diese Gleichung im Rationalitätsbereich k_2 reduzibel werden, d. h. die Zahl ϑ würde dann einer Gleichung von der Gestalt

$$\vartheta^r + \alpha_1 \vartheta^{r-1} + \cdots + \alpha_r = 0$$

genügen, deren Grad $r < m_1$ ist, und deren Koeffizienten $\alpha_1, \ldots, \alpha_r$ Zahlen in k_2 sind. Der aus diesen Koeffizienten $\alpha_1, \ldots, \alpha_r$ zusammengesetzte Zahlkörper werde k genannt. Da $\alpha_1, \ldots, \alpha_r$ sich durch die r Wurzeln der obigen Gleichung rational ausdrücken lassen, so ist k ein Unterkörper von K_1, und da k auch zugleich ein Unterkörper von k_2 ist, so müßte die Diskriminante von k nach Satz 39 sowohl in der Diskriminante von k_1 als auch in derjenigen von k_2 als Faktor enthalten sein; hieraus würde für die Diskriminante dieses Körpers k der Wert 1 folgen, und dieser Umstand widerspricht dem Satze 44.

Wir heben noch folgende Tatsachen hervor, deren Richtigkeit nunmehr leicht erkannt wird:

Satz 88. Wenn k_1, k_2 zwei Körper bezüglich von den Graden m_1, m_2 und mit den zueinander primen Diskriminanten d_1, d_2 sind, so ist die Diskriminante des zusammengesetzten Körpers K gleich $d_1^{m_2} d_2^{m_1}$. Die $m_1 m_2$ Zahlen einer Basis des Körpers K erhält man, wenn man jede der m_1 Basiszahlen des Körpers k_1 mit jeder der m_2 Basiszahlen des Körpers k_2 multipliziert. Ist p eine rationale Primzahl, welche in k_1 die Zerlegung $p = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ und in k_2 die Zerlegung $p = \mathfrak{q}_1 \dots \mathfrak{q}_s$ erfährt, wo $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ und $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ voneinander verschiedene Primideale bez. in den Körpern k_1 und k_2 bedeuten, so gilt in K die Zerlegung $p = \prod_{i,l} \mathfrak{J}_{il}^{e_i}$, wo das Produkt über $i = 1, \dots, r$ und $l = 1, \dots, s$ zu erstrecken ist und $\mathfrak{J}_{il}$ dasjenige Ideal in K bedeutet, welches als der größte gemeinsame Teiler der beiden Ideale $\mathfrak{p}_i$ und $\mathfrak{q}_l$ definiert ist. Die Ideale $\mathfrak{J}_{il}$ sind nicht notwendig Primideale in K.

Werden zwei Körper k_1, k_2 mit beliebigen Diskriminanten zugrunde gelegt, so ist die Beantwortung der entsprechenden Fragen nur unter beschränkenden Annahmen über die Natur der zu zerlegenden Primzahlen einfach [Hensel (3)].

Die bisher in Kapitel 10 — 13 dargelegten Resultate scheinen mir die wichtigsten Grundzüge einer Theorie der Ideale und Diskriminanten des Galoisschen Körpers zu enthalten. Die befolgten Methoden gestatten noch nach mannigfachen Richtungen eine allgemeinere Ausführung; insbesondere gilt eine Reihe der in §§ 39 — 44 bewiesenen Sätze ohne wesentliche Änderung für relativ Galoissche Körper [Dedekind (8)].

14. Die Primideale ersten Grades und der Klassenbegriff.

§ 53. Die Erzeugung der Idealklassen durch Primideale ersten Grades.

Es ist von hohem Interesse, daß die in Kapitel 10 — 12 entwickelten Prinzipien auch über die Frage der Erzeugung und Natur der Idealklassen eines Zahlkörpers neues Licht verbreiten. In diesem und in dem folgenden Kapitel werden die wichtigsten auf diese Frage bezüglichen allgemeinen Sätze dargelegt. Der erste Satz betrifft die Erzeugung der Idealklassen eines beliebigen Galoisschen Zahlkörpers durch Primideale ersten Grades und lautet:

Satz 89. In jeder Idealklasse eines Galoisschen Körpers gibt es Ideale, deren Primfaktoren sämtlich Ideale ersten Grades sind.

Wir beweisen zunächst den folgenden Hilfssatz:

Hilfssatz 12. Wenn K ein Galoisscher Körper vom M-ten Grade mit der Diskriminante D ist, und $\mathfrak{P}$ ein in $DM!$ nicht aufgehendes Primideal von einem Grade $f > 1$ in diesem Körper bedeutet, so gibt es stets eine zu $DM!$ prime

ganze Zahl Ω in K, welche durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbar ist, und deren übrige Primfaktoren sämtlich von niederem als dem f-ten Grade sind.

Beweis. Es sei P eine ganze Zahl des Körpers K von der Art, daß jede andere ganze Zahl Ω einer ganzzahligen Funktion von P nach $\mathfrak{P}^2$ kongruent wird. Nach Satz 29 existiert eine solche Zahl P stets. Wir bezeichnen ferner die zu $\mathfrak{P}$ konjugierten und von $\mathfrak{P}$ verschiedenen Primideale mit $\mathfrak{P}', \mathfrak{P}'', \dots, \mathfrak{P}^{(m)}$ und bestimmen dann eine ganze Zahl A in K, welche den Kongruenzen

$$\begin{aligned} \mathsf{A} &\equiv \mathsf{P}, && (\mathfrak{P}^2) \\ \mathsf{A} &\equiv 0, && (\mathfrak{P}'\mathfrak{P}'' \dots \mathfrak{P}^{(m)}) \\ \mathsf{A} &\equiv 1, && (M!) \end{aligned}$$

genügt. Ist z eine solche Substitution der zu $\mathfrak{P}$ gehörigen Zerlegungsgruppe, für welche $z\,\mathsf{P} \equiv \mathsf{P}^p$ nach $\mathfrak{P}$ wird, so sind offenbar die $f-1$ Differenzen $\mathsf{A} - z\mathsf{A}$, $\mathsf{A} - z^2\mathsf{A}, \dots, \mathsf{A} - z^{f-1}\mathsf{A}$ zu $\mathfrak{P}$ prim. Ist ferner s eine nicht zur Zerlegungsgruppe gehörige Substitution, so wird $s\mathsf{A}$ durch $\mathfrak{P}$ teilbar, und folglich ist die Differenz $\mathsf{A} - s\mathsf{A}$ zu $\mathfrak{P}$ prim. Die Differente von A ist mithin zu $\mathfrak{P}$ prim, und daher folgt nach der Bemerkung auf S. 71, daß A eine den Körper K bestimmende Zahl darstellt. Mit Rücksicht auf Satz 31 ist K der Trägheitskörper von $\mathfrak{P}$, und daher genügt A einer Gleichung von der Gestalt:

$$\mathsf{A}^f + \alpha_1 \mathsf{A}^{f-1} + \dots + \alpha_f = 0,$$

wo $\alpha_1, \dots, \alpha_f$ Zahlen im Zerlegungskörper k des Primideals $\mathfrak{P}$ bedeuten. Die übrigen Unterkörper des Körpers K vom nämlichen Grade $\frac{M}{f}$ bezeichnen wir mit $k', k'', \dots$; es genügt A dann auch den Gleichungen

$$\begin{aligned} \mathsf{A}^f + \alpha_1' \mathsf{A}^{f-1} + \dots + \alpha_f' &= 0, \\ \mathsf{A}^f + \alpha_1'' \mathsf{A}^{f-1} + \dots + \alpha_f'' &= 0, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \end{aligned}$$

wo $\alpha_1', \dots, \alpha_f'$ Zahlen in k', $\alpha_1'', \dots, \alpha_f''$ Zahlen in k'' usf. sind. Nunmehr bestimme man f ganze rationale Zahlen $a_1, \dots, a_f$ so, daß

$$a_1 \equiv \alpha_1, \dots, \; a_f \equiv \alpha_f, \qquad (\mathfrak{P})$$

wird; dies ist möglich, weil nach Satz 70 das Ideal $\mathfrak{P}$ in k vom ersten Grade ist. Sodann seien $b_1, \dots, b_f$ solche f ganze rationale Zahlen, welche den Kongruenzen

$$M!\,b_1 \equiv a_1, \dots, \; M!\,b_f \equiv a_f, \qquad (p)$$

genügen, und für welche überdies keine der zum Index 1 gehörigen Verbindungen

$$\beta_1 = M!\,b_1 - \alpha_1, \quad \beta_1' = M!\,b_1 - \alpha_1', \quad \dots$$

verschwindet. Wir setzen ferner

$$\mathsf{B} = \mathsf{A}^f + M!\,(b_1 \mathsf{A}^{f-1} + b_2 \mathsf{A}^{f-2} + \dots + b_f).$$

Endlich bezeichnen wir die sämtlichen von p verschiedenen und in der Diskriminante A von A oder in den Normen der Zahlen $\beta_1, \beta_1', \ldots$ aufgehenden rationalen Primzahlen, soweit sie größer als M sind, mit $q_1, \ldots, q_l$. Ist q_i eine beliebige unter diesen, so muß, da sie in K höchstens M Primfaktoren enthalten kann, mindestens eine der $q_i (> M)$ Zahlen, $\mathsf{B}, \mathsf{B}+1, \mathsf{B}+2, \ldots, \mathsf{B}+q_i-1$ zu q_i prim sein; es sei etwa $\mathsf{B}+c_i$ prim zu q_i. Bestimmt man dann eine ganze rationale Zahl c, welche den l Kongruenzen $M!\,pc \equiv c_i$ nach q_i für $i = 1, 2, \ldots, l$ genügt, so ist

$$\Omega = \mathsf{B} + M!\,pc$$

eine Zahl von der Eigenschaft, wie sie unser Hilfssatz 12 verlangt.

In der Tat: wegen der Kongruenz $\mathsf{A} \equiv 1$ nach $M!$ ist die Zahl Ω prim zu allen denjenigen rationalen Primzahlen, welche $\leqq M$ sind; und andererseits ist Ω auf Grund der Bestimmungsweise der Zahl c prim zu allen denjenigen in A enthaltenen rationalen Primzahlen, welche größer als M sind. Die Zahl Ω ist daher prim zu den von p verschiedenen, in A aufgehenden rationalen Primzahlen.

Ferner ist Ω teilbar durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}', \mathfrak{P}'', \ldots, \mathfrak{P}^{(m)}$, da $M!\,b_f = a_f \not\equiv 0$ nach p wird. Die Zahl Ω ist in der Gestalt

$$\Omega = \mathsf{A}^f + m_1 \mathsf{A}^{f-1} + \cdots + m_f,$$

darstellbar, wo $m_1, \ldots, m_f$ ganze rationale Zahlen bedeuten. Da $\mathsf{A} \equiv \mathsf{P}$ nach $\mathfrak{P}^2$ ist und P keiner ganzzahligen Kongruenz von niederem als dem $(2f)$-ten Grade nach $\mathfrak{P}^2$ genügen kann, so folgt, daß Ω nicht durch $\mathfrak{P}^2$ teilbar ist.

Wäre ferner Ω durch ein Primideal $\mathfrak{Q}$ vom Grade $f' > f$ teilbar, und seien $1, z', z'^2, \ldots, z'^{f'-1}$ die f'Substitutionen der Zerlegungsgruppe von $\mathfrak{Q}$, durch welche diese aus der Trägheitsgruppe erzeugt wird, so müßten die f' Kongruenzen

$$\begin{aligned} &\mathsf{A}^f + m_1 \quad \mathsf{A}^{f-1} + \cdots + m_f \equiv 0, \qquad (\mathfrak{Q}) \\ &(z'\mathsf{A})^f + m_1 (z'\mathsf{A})^{f-1} + \cdots + m_f \equiv 0, \qquad (\mathfrak{Q}) \\ &\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

bestehen; diese würden zur Folge haben, daß die Diskriminante A der Zahl A durch $\mathfrak{Q}$ teilbar ist, was nach dem Obigen nicht zutrifft.

Es sei endlich Ω durch ein Primideal $\mathfrak{Q}$ vom Grade f teilbar; dann müßte einer der Körper $k, k', k'', \ldots$ Zerlegungskörper von $\mathfrak{Q}$ sein; es sei dies etwa der Körper k'. Unter dieser Annahme setze man Ω in die Gestalt

$$\Omega = \Omega - (\mathsf{A}^f + \alpha_1' \mathsf{A}^{f-1} + \cdots + \alpha_f') = \beta_1' \mathsf{A}^{f-1} + \cdots + \beta_f',$$

wo $\beta_1', \ldots, \beta_f'$ Zahlen in k' bedeuten. Sind $1, z', z'^2, \ldots, z'^{f-1}$ die f für $\mathfrak{Q}$ zur Erzeugung seiner Zerlegungsgruppe aus seiner Trägheitsgruppe dienenden Substitutionen, so folgt

$$\begin{aligned} &\beta_1' \mathsf{A}^{f-1} + \cdots + \beta_f' \equiv 0, \qquad (\mathfrak{Q}) \\ &\beta_1' (z'\mathsf{A})^{f-1} + \cdots + \beta_f' \equiv 0, \qquad (\mathfrak{Q}) \\ &\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

und diese Kongruenzen würden zur Folge haben, daß entweder A oder β_1' durch $\mathfrak{Q}$ teilbar ist, womit die obigen Festsetzungen im Widerspruch stehen.

Wenn wir berücksichtigen, daß in jeder Klasse ein Ideal gefunden werden kann, welches zu $DM!$ prim ist, so folgt aus dem somit bewiesenen Hilfssatz 12, wie man leicht sieht, der Satz 89. Derselbe ist für den Fall des Kreiskörpers bereits von Kummer bewiesen worden [Kummer (6)].

15. Der relativ-zyklische Körper vom Primzahlgrade.

§ 54. Die symbolische Potenz. Der Satz von den Zahlen mit der Relativnorm 1.

Es soll jetzt über relativ Abelsche Körper eine Reihe fundamentaler Sätze abgeleitet werden. Um dieselben leichter aussprechen und beweisen zu können, schicken wir einige Bezeichnungen und Festsetzungen voraus.

Es sei K ein Zahlkörper vom Grade lm; derselbe sei relativ-zyklisch in bezug auf den Körper k vom m-ten Grade; der Relativgrad l sei eine Primzahl. Die Substitutionen der zyklischen Relativgruppe seien $1, S, S^2, \ldots, S^{l-1}$. Endlich definieren wir den Begriff der **symbolischen Potenz** einer Zahl A des Körpers K, wie folgt: wenn A eine beliebige ganze oder gebrochene Zahl in K ist und $a, a_1, \ldots, a_{l-1}$ irgendwelche ganze rationale Zahlen bedeuten, so möge der Ausdruck

$$\mathsf{A}^a (S\,\mathsf{A})^{a_1} (S^2\,\mathsf{A})^{a_2} \ldots (S^{l-1}\,\mathsf{A})^{a_{l-1}}$$

zur Abkürzung mit

$$\mathsf{A}^{a+a_1 S+a_2 S^2+\cdots+a_{l-1}S^{l-1}} = \mathsf{A}^{F(S)}$$

bezeichnet werden, wo $F(S)$ die auf der linken Seite im Exponenten von A stehende ganzzahlige Funktion von S bedeutet. Die symbolische $F(S)$-te Potenz von A stellt hiernach stets wiederum eine ganze oder gebrochene Zahl des Körpers K dar. Diese symbolische Potenzierung kann als Verallgemeinerung einer Bezeichnungsweise angesehen werden, welche Kronecker im Falle des Kreiskörpers eingeführt hat [Kronecker (1)].

Wir beweisen nun der Reihe nach folgende Eigenschaften des relativ-zyklischen Körpers K:

Satz 90. Jede ganze oder gebrochene Zahl A in K, deren Relativnorm in bezug auf k gleich 1 ist, wird die symbolische $(1-S)$-te Potenz einer gewissen ganzen Zahl B des Körpers K.

Beweis. Es sei x eine Veränderliche und Θ eine den Körper K bestimmende Zahl; dann setze man:

$$\mathsf{A}_x = \frac{x+\Theta}{x+S\Theta}\,\mathsf{A} = (x+\Theta)^{1-S}\mathsf{A}$$

und

$$\mathsf{B}_x = 1 + \mathsf{A}_x^1 + \mathsf{A}_x^{1+S} + \mathsf{A}_x^{1+S+S^2} + \ldots + \mathsf{A}_x^{1+S+S^2+\cdots+S^{l-2}}.$$

Berücksichtigt man, daß nach Voraussetzung $\mathsf{A}^{1+S+\cdots+S^{l-1}} = 1$ ist und folglich auch $\mathsf{A}_x^{1+S+\cdots+S^{l-1}} = 1$ wird, so ergibt sich $\mathsf{B}_x^{1-S} = \mathsf{A}_x$. Da B_x eine rationale Funktion von x ist, welche, wie leicht ersichtlich, nicht identisch für alle x verschwindet, so kann man eine ganze rationale Zahl $x = a$ so wählen, daß B_a eine von 0 verschiedene Zahl in K wird. Die Zahl $\mathsf{B}^* = \frac{\mathsf{B}_a}{a+\Theta}$ genügt dann der Gleichung $\mathsf{A} = \mathsf{B}^{*1-S}$. Setzen wir $\mathsf{B}^* = \frac{\mathsf{B}}{b}$, wo B eine ganze algebraische Zahl in K und b eine ganze rationale Zahl bedeutet, so ist auch $\mathsf{A} = \mathsf{B}^{1-S}$.

§ 55. Das System von relativen Grundeinheiten und der Nachweis ihrer Existenz.

Ein zweiter wichtiger Satz über den Körper K betrifft eine Eigenschaft der Einheiten in K. Kommen unter den m konjugierten Körpern, welche durch k bestimmt sind, r_1 reelle Körper und r_2 Paare konjugiert imaginärer Körper vor, so ist nach Satz 47 die Zahl der Grundeinheiten in k gleich $r = r_1 + r_2 - 1$. Wir definieren nun den Begriff eines **Systems von relativen Grundeinheiten** des Körpers K bezüglich k. Unter einem solchen System verstehen wir ein System von $r+1$ Einheiten $\mathsf{H}_1, \ldots, \mathsf{H}_{r+1}$ im Körper K von der Eigenschaft, daß eine Einheit von der Gestalt $\mathsf{H}_1^{F_1(S)} \ldots \mathsf{H}_{r+1}^{F_{r+1}(S)}[\varepsilon]$ nur dann die symbolische $(1-S)$-te Potenz einer Einheit in K werden kann, wenn die ganzen algebraischen Zahlen $F_1(\zeta), \ldots, F_{r+1}(\zeta)$ sämtlich durch $1-\zeta$ teilbar sind. Dabei bedeuten $F_1(S), \ldots, F_{r+1}(S)$ ganzzahlige Funktionen von S; $[\varepsilon]$ bedeutet eine beliebige Einheit des Körpers k oder eine solche Einheit des Körpers K, deren l-te Potenz eine Einheit in k ist; ζ endlich bedeutet eine von 1 verschiedene l-te Einheitswurzel.

Satz 91. Wenn der Relativgrad l des relativ-zyklischen Körpers K in bezug auf den Körper k eine ungerade Primzahl ist, so existiert in K stets ein System von $r+1$ relativen Grundeinheiten, wobei r für k die Bedeutung wie in Satz 47 hat.

Beweis. Wegen $l \neq 2$ kommen unter den lm durch K bestimmten konjugierten Körpern lr_1, reelle Körper und lr_2 imaginäre Paare von Körpern vor. Es sei $\varepsilon_1, \ldots, \varepsilon_r$ ein System von $r = r_1 + r_2 - 1$ Grundeinheiten des Körpers k. Man wähle unter den Einheiten in K eine solche Einheit E_1 aus, daß $\mathsf{E}_1, \varepsilon_1, \ldots, \varepsilon_r$ ein System von unabhängigen Einheiten bilden; dann müssen auch die $r+l-1$ Einheiten $\mathsf{E}_1, \mathsf{E}_1^S, \ldots, \mathsf{E}_1^{S^{l-2}}, \varepsilon_1, \ldots, \varepsilon_r$ ein System unabhängiger Einheiten sein.

Zum Beweise hierfür machen wir die gegenteilige Annahme und denken uns $\mathsf{E}_1^{F(S)} = \varepsilon^*$, wo $F(S)$ eine nicht identisch verschwindende ganzzahlige Funktion vom $(l-2)$-ten Grade in S und ε^* eine Einheit des Körpers k bedeutet. Da die Funktion $1 + S + \cdots + S^{l-1}$ irreduzibel ist, (vgl. die Bemerkung am Schluß des § 91), so lassen sich zwei ganzzahlige Funktionen G_1, G_2 von S und eine von 0 verschiedene ganze rationale Zahl a derart bestimmen, daß

$$F G_1 + (1 + S + \cdots + S^{l-1}) G_2 = a$$

wird. Hieraus folgt unter Berücksichtigung von

$$\mathsf{E}_1^{1+S+\cdots+S^{l-1}} = \varepsilon^{**}$$

die Gleichung $\mathsf{E}_1^a = \varepsilon^{***}$, welche unserer Annahme zuwider läuft; dabei bedeuten ε^{**} und ε^{***} Einheiten in k.

Nunmehr wähle man eine Einheit E_2 so, daß $\mathsf{E}_2, \mathsf{E}_1, \mathsf{E}_1^S, \ldots, \mathsf{E}_1^{S^{l-2}}$, $\varepsilon_1, \ldots, \varepsilon_r$ ein System unabhängiger Einheiten bilden, und beweise dann in ähnlicher Weise, wie vorher, daß auch die Einheiten $\mathsf{E}_2, \mathsf{E}_2^S, \ldots, \mathsf{E}_2^{S^{l-2}}$, $\mathsf{E}_1, \mathsf{E}_1^S, \ldots, \mathsf{E}_1^{S^{l-2}}, \varepsilon_1, \ldots, \varepsilon_r$ unabhängige Einheiten sind. So fortfahrend, gelangen wir zu $r_1 + r_2 = r + 1$ Einheiten $\mathsf{E}_1, \ldots, \mathsf{E}_{r+1}$ von der Beschaffenheit, daß die Einheiten

$$\mathsf{E}_i,\ \mathsf{E}_i^S,\ \ldots,\ \mathsf{E}_i^{S^{l-2}},\ \varepsilon_1,\ \ldots,\ \varepsilon_r \quad (i = 1, 2, \ldots, r+1)$$

ein System von unabhängigen Einheiten bilden. Die Zahl dieser Einheiten beträgt

$$(r+1)(l-1) + r = lr_1 + lr_2 - 1\,.$$

Es sei nun l^m eine so hohe Potenz von l, daß ein Ausdruck

$$\mathsf{E}_1^{F_1(S)} \ldots \mathsf{E}_{r+1}^{F_{r+1}(S)}[\varepsilon], \tag{20}$$

in welchem $F_1(S), \ldots, F_{r+1}(S)$ beliebige ganzzahlige Funktionen vom $(l-2)$-ten Grade in S bedeuten und $[\varepsilon]$ die auf S. 150 erklärte Bedeutung hat, nicht anders eine l^m-te Potenz einer Einheit in K werden kann, als wenn alle Koeffizienten der $r+1$ Funktionen $F_1(S), \ldots, F_{r+1}(S)$ durch l teilbar sind. Daß es eine solche Potenz l^m stets geben muß, folgt, wenn man die $lr_1 + lr_2 - 1$ nach Satz 47 existierenden Grundeinheiten des Körpers K zu Hilfe zieht.

Wir berücksichtigen ferner die Identität

$$(1-S)^l = 1 - S^l + lG(S)\,,$$

in der G eine ganzzahlige Funktion bedeutet; da hiernach die $(1-S)^{l^m}$-te symbolische Potenz einer Zahl in K zugleich auch eine l^m-te wirkliche Potenz ist, so folgt, daß der Ausdruck (20) nicht anders die $(1-S)^{l^m}$-te symbolische Potenz einer Einheit werden kann, als wenn die ganzen algebraischen Zahlen $F_1(\zeta), \ldots, F_{r+1}(\zeta)$ sämtlich durch $1-\zeta$ teilbar sind.

Es sei nun e_1 die größte ganze rationale Zahl $\geqq 0$ von der Art, daß ein Ausdruck von der Gestalt (20) eine $(1-S)^{e_1}$-te symbolische Potenz einer Einheit ist, ohne daß sämtliche Zahlen $F_1(\zeta), \ldots, F_{r+1}(\zeta)$ durch $1-\zeta$ teilbar sind; wir nehmen an, es sei ein solcher Ausdruck:

$$\mathsf{E}_1^{F_1(S)} \ldots \mathsf{E}_{r+1}^{F_{r+1}(S)}[\varepsilon] = \mathsf{H}_1^{(1-S)^{e_1}},$$

wo $F_1(S), \ldots, F_{r+1}(S)$ gewisse ganze rationale Funktionen von S sind und etwa $F_1(\zeta)$ nicht durch $1-\zeta$ teilbar sein möge; $[\varepsilon]$ hat die frühere Bedeutung, und H_1 ist eine gewisse Einheit des Körpers K. Des weiteren nehmen wir an, es sei e_2 die größte ganze Zahl $\geqq 0$ von der Beschaffenheit, daß ein entsprechend aus den Einheiten $\mathsf{E}_2, \ldots, \mathsf{E}_{r+1}$ gebildeter Ausdruck existiert, der die $(1-S)^{e_2}$-te symbolische Potenz einer Einheit in K wird; es sei etwa ein solcher Ausdruck:

$$\mathsf{E}_2^{F_2(S)} \ldots \mathsf{E}_{r+1}^{F_{r+1}(S)}[\varepsilon] = \mathsf{H}_2^{(1-S)^{e_2}},$$

wo $F_2(S), \ldots, F_{r+1}(S)$ wiederum gewisse ganze rationale Funktionen von S sind und etwa $F_2(\zeta)$ nicht durch $1-\zeta$ teilbar sein möge; H_2 bedeutet eine Einheit in K. So fortfahrend, gelangen wir zu $r+1$ Einheiten $\mathsf{H}_1, \mathsf{H}_2, \ldots, \mathsf{H}_{r+1}$; dieselben bilden ein System von relativen Grundeinheiten des Körpers K.

Um dies zu zeigen, nehmen wir im Gegenteil an, es gäbe $r+1$ ganze rationale Funktionen $G_1(S), \ldots, G_{r+1}(S)$ derart, daß

$$\mathsf{H}_1^{G_1(S)} \ldots \mathsf{H}_{r+1}^{G_{r+1}(S)}[\varepsilon] = \mathsf{Z}^{1-S}$$

wird, wo Z eine Einheit in K bedeutet; es sei ferner unter den Zahlen $G_1(\zeta), \ldots, G_{r+1}(\zeta)$ etwa $G_k(\zeta)$ die erste nicht durch $1-\zeta$ teilbare Zahl: dann wäre offenbar auch der Teil

$$\mathsf{H}_k^{G_k(S)} \mathsf{H}_{k+1}^{G_{k+1}(S)} \ldots \mathsf{H}_{r+1}^{G_{r+1}(S)}[\varepsilon]$$

des letzten Produkts die $(1-S)$-te symbolische Potenz einer Einheit des Körpers K. Da aber in der Reihe der Zahlen $e_1, e_2, \ldots, e_{r+1}$ keine folgende größer ist als die vorhergehende, so stoßen wir, wenn wir den letzten Ausdruck in die $(1-S)^{e_k}$-te Potenz erheben und dann wieder die Einheiten $\mathsf{E}_k, \ldots, \mathsf{E}_{r+1}$ einführen, auf einen Widerspruch mit unseren Festsetzungen.

Der eben bewiesene Satz 91 gilt, wie leicht ersichtlich, auch für $l=2$, wenn in diesem Falle noch der Umstand hinzukommt, daß unter den durch K bestimmten $2m$ einander konjugierten Körpern doppelt so viel reelle Körper als unter den durch k bestimmten m konjugierten Körpern vorhanden sind.

§ 56. Die Existenz einer Einheit in K, welche die Relativnorm 1 besitzt und doch nicht dem Quotienten zweier relativ-konjugierten Einheiten gleich wird.

Satz 92. Falls der Relativgrad l des relativ-zyklischen Körpers K in bezug auf den Körper k eine ungerade Primzahl ist, gibt es in K stets eine Einheit H, deren Relativnorm in bezug auf k gleich 1 ausfällt, und welche doch nicht die symbolische $(1-S)$-te Potenz von einer Einheit des Körpers K ist.

Beweis. Wir nehmen zunächst an, daß der Körper k nicht die l-te Einheitswurzel ζ enthält. Es seien $\eta_1, \ldots, \eta_{r+1}$ irgend $r+1$ Einheiten in k;

dann folgt, daß es stets $r+1$ ganze rationale Zahlen $a_1, \ldots, a_{r+1}$ gibt, welche nicht sämtlich durch l teilbar sind, und für welche $\eta_1^{a_1} \ldots \eta_{r+1}^{a_{r+1}} = 1$ wird. In der Tat, wären in einer Gleichung von der letzteren Gestalt die Exponenten $a_1, \ldots, a_{r+1}$ sämtlich durch l teilbar, so müßte $\eta_1^{\frac{a_1}{l}} \ldots \eta_{r+1}^{\frac{a_{r+1}}{l}}$ eine l-te Einheitswurzel und demnach infolge der Voraussetzung $=1$ sein; hieraus ergibt sich durch Wiederholung des Verfahrens das Gesagte. Nehmen wir nun $\eta_1, \ldots, \eta_{r+1}$ gleich den Relativnormen von $\mathsf{H}_1, \ldots, \mathsf{H}_{r+1}$, wo $\mathsf{H}_1, \ldots, \mathsf{H}_{r+1}$ ein System von relativen Grundeinheiten in K sind, und setzen dann $\mathsf{H} = \mathsf{H}_1^{a_1} \ldots \mathsf{H}_{r+1}^{a_{r+1}}$, so folgt $N_k(\mathsf{H}) = \mathsf{H}^{1+S+S^2+\cdots+S^{l-1}} = 1$ und daher nach dem Satz 90: $\mathsf{H} = A^{1-S}$; da $\mathsf{H}_1, \ldots, \mathsf{H}_{r+1}$ relative Grundeinheiten sind, so ist die Zahl A keine Einheit.

Um den Satz 92 allgemein zu beweisen, werde angenommen, daß k die primitive l^h-te Einheitswurzel ζ', aber nicht die primitive l^{h+1}-te Einheitswurzel enthielte. Durch ein ähnliches Verfahren, wie das oben angewandte, wird erkannt, daß, wenn $\eta_1, \ldots, \eta_{r+2}$ irgendwelche $r+2$ Einheiten in k sind, stets eine ganze rationale Zahl a und ferner $r+2$ ganze rationale, nicht sämtlich durch l teilbare Zahlen $a_1, \ldots, a_{r+2}$ von der Art gefunden werden können, daß

$$\eta_1^{a_1} \ldots \eta_{r+2}^{a_{r+2}} = \zeta'^{al}$$

ist.

Andererseits bedenke man, daß die Relativnorm

$$N_k(\zeta) = \zeta^{1+S+S^2+\cdots+S^{l-1}} = 1$$

wird und daher nach Satz 90 ζ eine $(1-S)$-te symbolische Potenz werden muß. Gäbe es nun keine Einheit E in K, so daß $\zeta = \mathsf{E}^{1-S}$ ist, so wäre bereits ζ eine Zahl von der gewünschten Beschaffenheit. Im anderen Falle folgt $\mathsf{E}^{l(1-S)} = 1$, d. h. $\mathsf{E}^l = S\mathsf{E}^l$, und daher stellt E^l eine Einheit ε in k dar, während E selbst gewiß nicht in k liegt. Wegen $\mathsf{E} = \sqrt[l]{\varepsilon}$ ergibt sich $N_k(\mathsf{E}) = \mathsf{E}^l = \varepsilon$. Es sei $\mathsf{H}_1, \ldots, \mathsf{H}_{r+1}$ ein System von relativen Grundeinheiten in K; wir setzen nun:

$$\eta_1 = N_k(\mathsf{H}_1), \ldots, \eta_{r+1} = N_k(\mathsf{H}_{r+1}), \ \eta_{r+2} = N_k(\mathsf{E}) = \mathsf{E}^l,$$
$$\mathsf{H} = \mathsf{H}_1^{a_1} \ldots \mathsf{H}_{r+1}^{a_{r+1}} \mathsf{E}^{a_{r+2}} \zeta'^{-a} = \mathsf{H}_1^{a_1} \ldots \mathsf{H}_{r+1}^{a_{r+1}}[\varepsilon],$$

wo $a, a_1, \ldots, a_{r+2}$ die vorhin bestimmten Zahlen sind und $[\varepsilon]$ die l-te Wurzel aus einer Einheit des Körpers k bedeutet; dann wird $N_k(\mathsf{H}) = 1$. Die Zahlen $a_1, \ldots, a_{r+1}$ können nicht sämtlich durch l teilbar sein. Denn aus

$$\left(\eta_1^{\frac{a_1}{l}} \ldots \eta_{r+1}^{\frac{a_{r+1}}{l}} \mathsf{E}^{a_{r+2}} \zeta'^{-a}\right)^l = 1$$

würde dann

$$\eta_1^{\frac{a_1}{l}} \ldots \eta_{r+1}^{\frac{a_{r+1}}{l}} \mathsf{E}^{a_{r+2}} \zeta'^{-a} = \zeta^b$$

folgen, wo b eine ganze rationale Zahl bedeutet. Da a_{r+2} bei unserer Annahme nicht auch durch l teilbar sein darf, so würde aus der letzten Gleichung folgen, daß E in k liegt, was nicht zutrifft. Die Einheit H erfüllt daher alle Bedingungen des Satzes 92.

Die Sätze 90, 91 und 92 sind zum Teil und in anderer Form bereits von Kummer für den Fall bewiesen worden, daß der Unterkörper k der durch ζ bestimmte Kreiskörper $(l-1)$-ten Grades ist [Kummer (*14*, *20*, *21*)].

§ 57. Die ambigen Ideale und die Relativdifferente des relativ-zyklischen Körpers K.

Wenn ein Ideal $\mathfrak{A}$ des relativ-zyklischen Körpers K bei Anwendung der Substitution S ungeändert bleibt und überdies keinen Faktor enthält, welcher ein Ideal in k ist, so heißt $\mathfrak{A}$ ein **ambiges Ideal.** Insbesondere heißt ein Primideal des Körpers K, wenn dasselbe bei Anwendung der Substitution S ungeändert bleibt und nicht zugleich im Körper k liegt, ein **ambiges Primideal.**

Satz 93. Die Relativdifferente des relativ-zyklischen Körpers K in bezug auf k enthält alle und nur diejenigen Primideale $\mathfrak{P}$, welche ambig sind.

Beweis. Ist $\mathfrak{P}$ ein ambiges Ideal, so wird seine Relativnorm $N_k(\mathfrak{P}) = \mathfrak{P}^l$. Da nicht eine niedere Potenz von $\mathfrak{P}$ in k liegen kann, so ist $\mathfrak{P}^l = \mathfrak{p}$ ein Primideal in k. Umgekehrt, wenn ein Primideal $\mathfrak{p}$ in k gleich der l-ten Potenz eines Ideals $\mathfrak{P}$ in K wird, so ist $\mathfrak{P}$ ein ambiges Primideal.

Wir unterscheiden nun dreierlei Arten von Primidealen $\mathfrak{p}$ des Körpers k: erstens solche, die der l-ten Potenz eines Primideals $\mathfrak{P}$ in K gleich sind; zweitens solche, die in l voneinander verschiedene Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_l$ des Körpers K zerfallen, und drittens solche, die auch in K Primideale sind.

Liegt der erste Fall vor, so setzen wir die Norm $N(\mathfrak{P}) = p'$; hieraus folgt $N(\mathfrak{p}) = N(\mathfrak{P}^l) = p^{lf}$, und mithin ist die Norm $n(\mathfrak{p})$ des Primideals $\mathfrak{p}$ im Körper k ebenfalls gleich p^f. Die Gleichheit der Normen $N(\mathfrak{P})$ und $n(\mathfrak{p})$ läßt die Tatsache erkennen, daß eine jede ganze Zahl des Körpers K einer gewissen ganzen Zahl des Körpers k nach $\mathfrak{P}$ kongruent ist; aus diesem Umstande erkennt man leicht, daß die Relativdifferente von K in bezug auf k notwendig durch $\mathfrak{P}$ teilbar ist.

Im zweiten Falle läßt sich in K stets eine ganze Zahl A finden, welche nicht durch $\mathfrak{P}_i$, wohl aber durch alle übrigen $l-1$ Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_{i-1}, \mathfrak{P}_{i+1}, \ldots, \mathfrak{P}_l$ teilbar ist, und aus diesem Umstande folgt, daß die Relativdifferente der Zahl A und daher auch die des Körpers K nicht durch $\mathfrak{P}_i$ teilbar ist.

Was endlich die Primideale $\mathfrak{p}$ der dritten Art angeht, so sei P eine Primitivzahl nach dem Primideal $\mathfrak{p}$ in K und ϱ eine Primitivzahl nach $\mathfrak{p}$ in k, und zugleich sei P eine den Körper K bestimmende Zahl. Es genügt dann P einer Gleichung l-ten Grades von der Gestalt:

$$F(\mathsf{P}) = \mathsf{P}^l + \alpha_1 \mathsf{P}^{l-1} + \cdots + \alpha_l = 0,$$

deren Koeffizienten $\alpha_1, \ldots, \alpha_l$ ganze Zahlen in k sind. Wir setzen

$$\alpha_1 \equiv f_1(\varrho), \ \ldots, \ \alpha_l \equiv f_l(\varrho), \qquad (\mathfrak{p}),$$

wo $f_1(\varrho), \ldots, f_l(\varrho)$ ganzzahlige Funktionen von ϱ sind, und erhalten so für P die Kongruenz:

$$F(\mathsf{P}) \equiv \mathsf{P}^l + f_1(\varrho)\,\mathsf{P}^{l-1} + \cdots + f_l(\varrho) \equiv 0, \qquad (\mathfrak{p}).$$

Da wegen $N(\mathfrak{p}) = (n(\mathfrak{p}))^l$ die Anzahl der in K vorhandenen, nach $\mathfrak{p}$ inkongruenten ganzen Zahlen gleich der l-ten Potenz der Anzahl der in k vorhandenen nach $\mathfrak{p}$ inkongruenten ganzen Zahlen ist, so kann P keiner Kongruenz niederen als l-ten Grades von der nämlichen Art genügen, und daher ist notwendig $\frac{\partial F(\mathsf{P})}{\partial \mathsf{P}} \not\equiv 0$ nach $\mathfrak{p}$; d. h. die Relativdifferente der Zahl P ist nicht durch $\mathfrak{p}$ teilbar. Durch diese Betrachtungen ist gezeigt, daß die Relativdifferente des Körpers K stets prim zu den Primidealen der zweiten und dritten Art ist, und hieraus ergibt sich die Richtigkeit des Satzes 93.

§ 58. Der Fundamentalsatz von den relativ-zyklischen Körpern mit der Relativdifferente 1. Die Bezeichnung dieser Körper als Klassenkörper.

Die Sätze 90, 92 und 93 ermöglichen uns die Erkenntnis einer Tatsache, welche für die Theorie der Zahlkörper von weittragender Bedeutung ist. Diese Tatsache ist folgende:

Satz 94. *Wenn der relativ-zyklische Körper K von ungeradem Primzahl-Relativgrade l die Relativdifferente 1 in bezug auf k besitzt, so gibt es stets in k ein Ideal $\mathfrak{j}$, welches nicht Hauptideal in k ist, wohl aber ein Hauptideal in K wird. Die l-te Potenz dieses Ideals $\mathfrak{j}$ ist dann notwendig auch in k ein Hauptideal, und die Klassenanzahl des Körpers k ist mithin durch l teilbar.*

Beweis. Nach Satz 92 gibt es eine Einheit H mit der Relativnorm 1, welche nicht die $(1-S)$-te Potenz einer Einheit ist. Nach Satz 90 ist $\mathsf{H} = \mathsf{A}^{1-S}$, wo A eine ganze Zahl in K bedeutet; d. h. es ist $\mathsf{A} = \mathsf{H} \cdot S\mathsf{A}$. Für das Hauptideal $\mathfrak{A} = (\mathsf{A})$ folgt hieraus $\mathfrak{A} = S\mathfrak{A}$. Das Ideal $\mathfrak{A}$ liegt im Körper k. Denn ist $\mathfrak{P}$ irgendein in $\mathfrak{A}$ aufgehendes Primideal des Körpers K, welches nicht in k liegt, so ist nach Satz 93, da wegen der Voraussetzung die Relativdiskriminante keine Teiler besitzt, $\mathfrak{P} \neq S\mathfrak{P}$, und folglich enthält A auch die Relativnorm $N_k(\mathfrak{P})$, welche ein in k liegendes Primideal ist. Das Ideal A ist kein Hauptideal im Körper k; denn in diesem Falle wäre $\mathsf{A} = \mathsf{H}^*\alpha$, wo H^* eine Einheit und α

eine Zahl in k bedeutet; hieraus würde $\mathsf{H} = \mathsf{H}^{*1-S}$ folgen, was dem Obigen widerstreitet. Damit ist der erste Teil des Satzes 94 bewiesen.

Da $N_k(\mathsf{A}) = \alpha$ eine Zahl in k und folglich $N_k(\mathfrak{A}) = \mathfrak{A}^l = (\alpha)$ ein Hauptideal in k ist, so haben wir damit den vollständigen Beweis des Satzes 94 erbracht.

Die Sätze 92 und 94 gelten ebenfalls für $l = 2$ unter der oben auf S. 152 am Schluß von § 55 angegebenen Beschränkung.

Es bietet keine erheblichen prinzipiellen Schwierigkeiten dar, den Satz 94 für solche relativ-Abelsche Körper K mit der Relativdifferente 1 zu verallgemeinern, deren Relativgrad l eine zusammengesetzte Zahl ist.

Wegen der engen Beziehung, die nach Satz 94 der Körper K zu gewissen Idealklassen des Körpers k aufweist, werde K ein **Klassenkörper des Körpers** k genannt.

Dritter Teil.

Der quadratische Zahlkörper.

16. Die Zerlegung der Zahlen im quadratischen Körper.

§ 59. Die Basis und die Diskriminante des quadratischen Körpers.

Es bedeute m eine ganze rationale, positive oder negative Zahl, die durch keine Quadratzahl außer 1 teilbar und auch von $+1$ verschieden ist; die quadratische Gleichung

$$x^2 - m = 0$$

ist dann im Bereich der rationalen Zahlen irreduzibel. Wir verstehen im folgenden unter $\sqrt{m}$ stets im Falle $m > 0$ die positive Wurzel jener quadratischen Gleichung und im Falle $m < 0$ diejenige ihrer Wurzeln, welche positiv imaginär ist. Die so festgelegte algebraische Zahl $\sqrt{m}$ bestimmt einen quadratischen reellen, bezüglich imaginären Zahlkörper, der $k(\sqrt{m})$ oder auch schlechthin k heiße; dieser Körper ist stets ein Galoisscher Körper. Durch die Operation der Vertauschung von $\sqrt{m}$ mit $-\sqrt{m}$ in einer Zahl oder einem Ideal des Körpers k geht man zu der konjugierten Zahl bez. dem konjugierten Ideal über. Dieser Übergang werde durch Vorsetzung des Substitutionszeichens s angedeutet.

Unsere erste Aufgabe ist die Aufstellung einer Basis des quadratischen Körpers und die Ermittlung seiner Diskriminante [Dedekind (*1*)].

Satz 95. Eine Basis des quadratischen Körpers k bilden die Zahlen $1, \omega$, wenn

$$\omega = \frac{1+\sqrt{m}}{2}, \text{ bez. } \omega = \sqrt{m}$$

genommen wird, je nachdem die Zahl $m \equiv 1$ nach 4 ist oder nicht. Die Diskriminante von k ist, entsprechend diesen zwei Fällen,

$$d = m, \quad \text{bez.} \quad d = 4m.$$

Beweis. Die Zahl ω ist stets ganz, da sie der Gleichung

$$x^2 - x - \frac{m-1}{4} = 0, \text{ bez. } x^2 - m = 0 \tag{21}$$

genügt. Bezeichnet $\omega' = s\omega$ die zu ω konjugierte Zahl, so ist $d = (\omega - \omega')^2$

die Diskriminante der Zahl ω. Nach § 3 S. 72 ist daher jede ganze Zahl des Körpers k in der Gestalt

$$\alpha = \frac{u + v\omega}{d}$$

darstellbar, wo u, v ganze rationale Zahlen sind.

Im Falle, daß $m \equiv 1$ nach 4 ist, schließen wir aus der Kongruenz $2\alpha m = 2u + v + v\sqrt{m} \equiv 0$ nach m, daß $2u + v$ durch $\sqrt{m}$ teilbar sein muß. Die letztere Kongruenz in Verbindung mit der ersteren hat wiederum $v\sqrt{m} \equiv 0$ nach m zur Folge, d. h. v muß durch $\sqrt{m}$ und daher notwendig auch durch m teilbar sein. Da mithin die ganzen rationalen Zahlen u, v beide durch $m = d$ teilbar sind, so ist die im Nenner des obigen Ausdrucks für α stehende Zahl d hebbar.

Ist andererseits $m \not\equiv 1$ nach 4, so schließen wir aus der Kongruenz $4\alpha m = u + v\sqrt{m} \equiv 0$ nach m, wie vorhin, daß sowohl u wie v durch m teilbar sein muß und mithin jedenfalls m in Zähler und Nenner des Ausdrucks für α hebbar ist. Wir erhalten dadurch $\alpha = \frac{u' + v'\sqrt{m}}{4}$, wo u', v' ganze rationale Zahlen bedeuten. Man erkennt aber leicht durch Bildung der Norm $\alpha \cdot s\alpha$, sowohl für $m \equiv 2$ als auch für $m \equiv 3$ nach 4, daß ein Ausdruck $u' + v'\sqrt{m}$ mit ganzen rationalen Zahlen u', v' nur dann durch 2 teilbar sein kann, wenn u', v' beide gerade sind. Wendet man dieses auf 4α und sodann wieder auf 2α an, so zeigt sich, daß auch im Falle $m \not\equiv 1$ nach 4 eine jede ganze Zahl des Körpers k in der Gestalt $u + v\omega$ mit ganzen rationalen Zahlen u, v darstellbar ist.

Der zweite Teil des Satzes ergibt sich aus der Formel:

$$d = \begin{vmatrix} 1, & \omega \\ 1, & \omega' \end{vmatrix}^2 = (\omega - \omega')^2,$$

durch welche nach § 3 die Diskriminante des Körpers definiert wird.

§ 60. Die Primideale des quadratischen Körpers.

Das Problem der Zerlegung der rationalen Primzahlen in Primideale des Körpers k wird durch folgenden Satz zur vollständigen Erledigung gebracht:

Satz 96. Jede in d aufgehende rationale Primzahl l ist gleich dem Quadrat eines Primideals in k. Jede ungerade, in d nicht aufgehende rationale Primzahl p zerfällt in k entweder in das Produkt zweier verschiedener, zueinander konjugierter Primideale ersten Grades $\mathfrak{p}$ und $\mathfrak{p}'$ oder stellt selbst ein Primideal zweiten Grades vor, je nachdem d quadratischer Rest oder Nichtrest für p ist. Die Primzahl 2 ist im Falle $m \equiv 1$ nach 4 in k in ein Produkt zweier voneinander verschiedener konjugierter Primideale zerlegbar oder selber Primideal, je nachdem $m \equiv 1$ oder $\equiv 5$ nach 8 ausfällt.

Beweis. Der erste Teil dieser Behauptung, welcher sich auf die in d aufgehenden Primzahlen l bezieht, ist eine Folge des allgemeinen Satzes 31. Ist l eine in d aufgehende ungerade Primzahl, so finden wir

$$l = \mathfrak{l}^2,$$

wo $\mathfrak{l} = (l, \sqrt{m})$ ein Primideal ersten Grades ist, welches seinem konjugierten gleich wird. Geht die Primzahl 2 in d auf, so wird

$$2 = (2, \sqrt{m})^2, \text{ bzw. } 2 = (2, 1 + \sqrt{m})^2,$$

je nachdem $m \equiv 2$ oder $\equiv 3$ nach 4 ist.

Die Zerlegung der in d nicht aufgehenden Primzahlen geschieht auf Grund des Satzes 33 unter Berücksichtigung der zu demselben in § 13 S. 91 gemachten Bemerkung. Danach ist eine jede zu d prime rationale Primzahl p im Körper k entweder in zwei voneinander verschiedene Primideale zerlegbar oder selbst ein Primideal, je nachdem die linke Seite der in Betracht kommenden Gleichung (21) im Sinne der Kongruenz nach p reduzibel oder irreduzibel ist. Ist die betreffende Primzahl p ungerade, so finden wir die Kongruenz

$$(2x - 1)^2 - m \equiv 0, \text{ bez. } x^2 - m \equiv 0, \ (p)$$

offenbar dann reduzibel, wenn m quadratischer Rest nach p ist, und dann irreduzibel, wenn m quadratischer Nichtrest nach p ist. Setzen wir im ersteren Falle $m \equiv a^2$ nach p, so ergibt sich:

$$p = (p, a + \sqrt{m})(p, a - \sqrt{m}) = \mathfrak{p}\mathfrak{p}'.$$

Die beiden Primideale $\mathfrak{p}$ und $\mathfrak{p}'$ rechter Hand sind wegen

$$(p, a + \sqrt{m}, a - \sqrt{m}) = 1$$

in der Tat voneinander verschieden. Im Falle $m \equiv 1$ nach 4 ist die Kongruenz $x^2 - x - \frac{m-1}{4} \equiv 0$ nach 2 offenbar reduzibel oder irreduzibel, je nachdem $\frac{m-1}{4} \equiv 0$ oder $\equiv 1$ nach 2 ist, d. h. je nachdem $m \equiv 1$ oder $\equiv 5$ nach 8 ausfällt. Im ersteren Falle findet man:

$$2 = \left(2, \frac{1 + \sqrt{m}}{2}\right)\left(2, \frac{1 - \sqrt{m}}{2}\right).$$

Die beiden Primideale rechter Hand sind wegen

$$\left(2, \frac{1 + \sqrt{m}}{2}, \frac{1 - \sqrt{m}}{2}\right) = 1$$

in der Tat voneinander verschieden.

Als Basiszahlen der eben aufgestellten Primideale können dienen:

$$l, \frac{l + \sqrt{m}}{2}, \text{ bez. } l, \sqrt{m},$$

$$p, \frac{a \pm \sqrt{m}}{2}, \text{ „ } p, a \pm \sqrt{m},$$

$$2, \frac{1 \pm \sqrt{m}}{2}, \text{ „ } 2, \sqrt{m}; \ 2, 1 + \sqrt{m},$$

je nachdem $m \equiv 1$ oder $\equiv 2, 3$ nach 4 ist. Man erkennt diese Tatsache leicht aus einer Umkehrung des Satzes 19, wenn man jedesmal aus dem hier angegebenen Zahlenpaare und dem dazu konjugierten die Determinante bildet. In der zweiten Zeile der aufgestellten Tabelle soll a eine der Kongruenz $a^2 \equiv m$ nach p genügende und dazu im Falle $m \equiv 1$ nach 4 ungerade Zahl bedeuten.

§ 61. Das Symbol $\left(\frac{a}{w}\right)$.

Um die gewonnenen Resultate über die Zerlegung der rationalen Primzahlen in übersichtlicherer Weise aussprechen zu können, führen wir folgendes Symbol ein. Ist a eine beliebige ganze rationale Zahl und w eine ungerade rationale Primzahl, so bedeute **das Symbol** $\left(\frac{a}{w}\right)$ den Wert $+1$, -1 oder 0, je nachdem die Zahl $a \not\equiv 0$ und quadratischer Rest oder quadratischer Nichtrest nach w oder durch w teilbar ist; ferner bedeute $\left(\frac{a}{2}\right)$ den Wert $+1$, -1, oder 0, je nachdem a ungerade und quadratischer Rest oder quadratischer Nichtrest nach $2^3 = 8$ oder durch 2 teilbar ist. Mit Benutzung dieses Symbols erhält der obige Satz 96 folgende Fassung:

Satz 97. Eine beliebige rationale Primzahl p ($= 2$ oder $\neq 2$) ist im Körper k in zwei voneinander verschiedene Primideale zerlegbar oder selbst Primideal oder gleich dem Quadrat eines Primideals, je nachdem $\left(\frac{d}{p}\right) = +1, -1$ oder 0 ist [Dedekind (*1*)].

Wir unterscheiden, den bisherigen Entwicklungen entsprechend, drei Arten von Primidealen, nämlich:

1. die Primideale ersten Grades $\mathfrak{p}$, welche von ihren Konjugierten $\mathfrak{p}'$ verschieden sind;
2. die Primideale zweiten Grades (p), die durch die in k unzerlegbaren rationalen Primzahlen p dargestellt werden;
3. die Primideale ersten Grades $\mathfrak{l}$, deren Quadrate den in d aufgehenden rationalen Primzahlen gleich sind.

Nach den in § 39 und § 41 aufgestellten Definitionen bildet der Körper k für die Primideale $\mathfrak{p}$ der ersten Art den Zerlegungskörper, für die Primideale p der zweiten Art den Trägheitskörper und für die Primideale $\mathfrak{l}$ der dritten Art den Verzweigungskörper.

§ 62. Die Einheiten des quadratischen Körpers.

Was die Frage nach den Einheiten des Körpers k betrifft, so sind nach Satz 47 die zwei Fälle zu unterscheiden, ob k ein imaginärer oder ein reeller Körper ist.

Im ersteren Falle enthält k nur solche Einheiten, welche zugleich Einheitswurzeln sind, und da in einem quadratischen Körper außer ± 1 nur die primitiven 3-ten, 4-ten, 6-ten Wurzeln der Einheit vorkommen können, so sind die einzigen imaginären quadratischen Körper, welche noch andere Einheiten als ± 1 enthalten, die zwei Körper $k\left(\sqrt{-1}\right)$ und $k\left(\sqrt{-3}\right)$. Der erstere Körper enthält die beiden Einheiten $\pm i$, der letztere die 4 Einheiten $\pm \frac{1 \pm \sqrt{-3}}{2}$. Die Diskriminanten dieser zwei Körper sind -4 bez. -3; nach Satz 50 muß daher in jeder Idealklasse dieser Körper ein Ideal vorkommen, dessen Norm $\leqq 2$ bezüglich $\leqq |\sqrt{3}|$ ist. Da ferner im Körper $k\left(\sqrt{-1}\right)$ die Zahl 2 gleich der Norm des Hauptideals $(1 + i)$ wird, so folgt, daß jeder dieser beiden quadratischen Körper nur *eine* Idealklasse besitzt. Mithin gibt es in diesen Körpern nur Hauptideale, und es ist also jede positive ganze rationale Zahl, welche zur Norm eines Ideals in $k\left(\sqrt{-1}\right)$ bez. $k\left(\sqrt{-3}\right)$ geeignet ist, stets Norm einer ganzen algebraischen Zahl in dem betreffenden Körper; hieraus folgen die bekannten Sätze über die Darstellung ganzer rationaler positiver Zahlen in den Gestalten $x^2 + y^2$, bezüglich $x^2 + xy + y^2$, wo x und y ganze rationale Zahlen sein sollen.

Ist dagegen k ein reeller Körper, so gibt es nach Satz 47 stets eine Grundeinheit ε, welche verschieden von ± 1 ist, und durch welche sich jede vorhandene Einheit des Körpers auf *eine* Weise in der Gestalt $\pm \varepsilon^a$ darstellen läßt, wo a eine ganze rationale Zahl bedeutet.

Die Umstände, unter denen die Norm dieser Grundeinheit ε gleich $+1$ oder gleich -1 ausfällt, sind bisher nur in besonderen Fällen aufgedeckt worden [Arndt (*1*), Dirichlet (*4*), Legendre (*1*), Tano (*1*)]. Vgl. überdies S. 168 den ersten Abschnitt des Beweises zu Hilfssatz 13.

§ 63. Die Aufstellung des Systems der Idealklassen.

Die Ausführungen in § 24 ermöglichen für jeden besonderen Wert m die Aufstellung aller Idealklassen des quadratischen Körpers k und die Berechnung der Anzahl h dieser Klassen. Hierher gehörige Tabellen sind auf dem Grunde der Theorie der reduzierten quadratischen Formen angefertigt worden [Gauss (*1*), Cayley (*1*)].

17. Die Geschlechter im quadratischen Körper und ihre Charakterensysteme.

§ 64. Das Symbol $\left(\frac{n, m}{w}\right)$.

Bei der weiteren Entwickelung der Theorie der quadratischen Körper, insbesondere behufs einer gewissen Einteilung der Idealklassen eines und desselben Körpers, bedienen wir uns eines neuen Symbols. Sind n, m ganze rationale Zahlen, dabei m nicht Quadratzahl, und ist w eine beliebige rationale

Primzahl, so bezeichne das **Symbol** $\left(\frac{n, m}{w}\right)$ den Wert $+1$, sobald die Zahl n mit der Norm einer ganzen Zahl des durch $\sqrt{m}$ bestimmten quadratischen Körpers $k(\sqrt{m})$ kongruent ist nach der Primzahl w, und sobald außerdem auch für jede höhere Potenz von w eine ganze Zahl in $k(\sqrt{m})$ existiert, deren Norm der Zahl n nach jener Potenz von w kongruent ist; in *jedem anderen Falle* setzen wir $\left(\frac{n, m}{w}\right) = -1$. Diejenigen ganzen rationalen Zahlen n, für welche $\left(\frac{n, m}{w}\right) = +1$ ist, sollen **Normenreste des Körpers** $k(\sqrt{m})$ **nach** w diejenigen Zahlen n, für welche $\left(\frac{n, m}{w}\right) = -1$ ist, **Normennichtreste des Körpers** $k(\sqrt{m})$ **nach** w heißen. Ist m eine Quadratzahl, so werde unter $\left(\frac{n, m}{w}\right)$ stets $+1$ verstanden. Über die zur Berechnung dienenden Eigenschaften des Symbols $\left(\frac{n, m}{w}\right)$ gibt der folgende Satz Aufschluß:

Satz 98. Bedeuten n und m ganze rationale, nicht durch w teilbare Zahlen, so gelten folgende Regeln:

für ungerade Primzahlen w wird

$$\left(\frac{n, m}{w}\right) = +1, \tag{a'}$$

$$\left(\frac{n, w}{w}\right) = \left(\frac{w, n}{w}\right) = \left(\frac{n}{w}\right); \tag{a''}$$

für $w = 2$ wird

$$\left(\frac{n, m}{2}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}, \tag{b'}$$

$$\left(\frac{n, 2}{2}\right) = \left(\frac{2, n}{2}\right) = (-1)^{\frac{n^2-1}{8}}. \tag{b''}$$

Ferner gelten allgemein für beliebige ganze rationale Zahlen n, n', m, m' und in bezug auf jede Primzahl w die Formeln:

$$\left(\frac{-m, m}{w}\right) = +1, \tag{c'}$$

$$\left(\frac{n, m}{w}\right) = \left(\frac{m, n}{w}\right), \tag{c''}$$

$$\left(\frac{n n', m}{w}\right) = \left(\frac{n, m}{w}\right)\left(\frac{n', m}{w}\right), \tag{c'''}$$

$$\left(\frac{n, m m'}{w}\right) = \left(\frac{n, m}{w}\right)\left(\frac{n, m'}{w}\right). \tag{c''''}$$

Beweis. Zunächst ist folgende Tatsache selbstverständlich: Wenn n selbst Norm einer ganzen Zahl im Körper $k(\sqrt{m})$ ist, so gilt $\left(\frac{n, m}{w}\right) = +1$. Da insbesondere $-m$ die Norm von $\sqrt{m}$ ist, so folgt daraus die Richtigkeit der Formel (c'). Sind ferner n und n' zwei ganze rationale Zahlen $\neq 0$, deren Quotient

die Norm einer ganzen oder gebrochenen Zahl in $k(\sqrt{m})$ ist, so folgt $\left(\frac{n, m}{w}\right) = \left(\frac{n', m}{w}\right)$ aus der Definition dieser Symbole. Ist der Quotient $\frac{n}{n'}$ das Quadrat einer rationalen Zahl, so ergibt sich insbesondere die einfache Tatsache, daß der Wert des Symbols $\left(\frac{n, m}{w}\right)$ ungeändert bleibt, wenn man in n eine Quadratzahl als Faktor zusetzt oder einen darin vielleicht vorhandenen solchen Faktor unterdrückt. Wir nehmen im folgenden der Einfachheit halber an, daß weder n noch m durch das Quadrat einer Primzahl teilbar ist.

Um die Richtigkeit des ganzen Formelsystems zu erkennen, behandeln wir der Reihe nach die folgenden drei Fälle:

1. Es sei w eine ungerade, in m aufgehende Primzahl.

Ist n nicht auch durch w teilbar, so wird offenbar die Kongruenz

$$4n \equiv (2x + y)^2 - m y^2 \text{ bez. } n \equiv x^2 - m y^2, \ (w), \tag{22}$$

in ganzen rationalen Zahlen x, y dann und nur dann lösbar sein, wenn $\left(\frac{n}{w}\right) = +1$ ist. Umgekehrt, wenn die letztere Bedingung statthat, so ist die Kongruenz $n \equiv x^2$ auch nach jeder Potenz von w lösbar, und mithin gilt das nämliche offenbar von der Kongruenz (22). Unter den gemachten Annahmen ist daher $\left(\frac{n, m}{w}\right) = \left(\frac{n}{w}\right)$.

Wird andererseits auch n teilbar durch w vorausgesetzt, so folgt:

$$\left(\frac{n, m}{w}\right) = \left(\frac{-nm, m}{w}\right) = \left(\frac{-\frac{nm}{w^2}, m}{w}\right) = \left(\frac{-\frac{nm}{w^2}}{w}\right).$$

2. Es sei w eine ungerade, in m nicht aufgehende Primzahl.

Ist auch n nicht durch w teilbar, so hat die Kongruenz $n \equiv x^2 - m y^2$ nach w stets Lösungen. Denn die rechte Seite dieser Kongruenz ergibt für die Systeme $x = 1, 2, \ldots, \frac{w-1}{2}$, $y = 0$ sämtliche quadratischen Reste und im Falle

$$\left(\frac{-m}{w}\right) = -1$$

für die Systeme $x = 0$, $y = 1, 2, \ldots, \frac{w-1}{2}$ sämtliche quadratischen Nichtreste nach w. Hat man dagegen $\left(\frac{-m}{w}\right) = +1$, und ist etwa a der kleinste positive quadratische Nichtrest für die Primzahl w, so sei $y = b$ eine Wurzel der alsdann gewiß lösbaren Kongruenz $-m y^2 \equiv a - 1$ nach w; wegen $a \equiv 1 - m b^2$ nach w stellt dann die Form $x^2 - m(bx)^2$ für $x = 1, 2, \ldots, \frac{w-1}{2}$ die sämtlichen quadratischen Nichtreste nach w dar. Aus der Lösbarkeit der

Kongruenz $n \equiv x^2 - m y^2$ nach w folgt leicht, daß diese Kongruenz auch nach jeder Potenz von w lösbar ist, d. h. es wird unter den gegenwärtigen Annahmen

$$\left(\frac{n, m}{w}\right) = +1.$$

Setzen wir andererseits n durch w teilbar voraus, aber der anfänglichen Festsetzung zufolge nicht teilbar durch w^2, so würde eine Auflösung der Kongruenz $n \equiv x^2 - m y^2$ nach w^2 in $\alpha = x - \sqrt{m}\, y$ eine solche ganze Zahl des Körpers $k(\sqrt{m})$ darbieten, für welche die Norm $\alpha \cdot s\alpha = n(\alpha)$ nur w, aber nicht w^2 als Faktor enthielte, d. h. w zerfiele im Körper $k(\sqrt{m})$ in zwei voneinander verschiedene Primideale $\mathfrak{w}$ und $\mathfrak{w}'$; die notwendige Bedingung hierfür ist nach Satz 97: $\left(\frac{m}{w}\right) = +1$. Umgekehrt, wenn diese Bedingung erfüllt ist, so ist in der Tat w im Körper $k(\sqrt{m})$ ein Produkt $\mathfrak{w}\mathfrak{w}'$ zweier verschiedener Primideale. Bezeichnet dann α eine ganze Zahl in $k(\sqrt{m})$, welche durch w, aber weder durch $\mathfrak{w}^2$ noch durch $\mathfrak{w}'$ teilbar ist, so folgt:

$$\left(\frac{n, m}{w}\right) = \left(\frac{n \cdot n(\alpha), m}{w}\right) = \left(\frac{\frac{n \cdot n(\alpha)}{w^2}, m}{w}\right) = +1.$$

Damit ist bewiesen, daß unter der gegenwärtigen Annahme stets $\left(\frac{n, m}{w}\right) = \left(\frac{m}{w}\right)$ ist.

Die bisher gewonnenen Resultate lassen unmittelbar die Richtigkeit der Formeln (a'), (a'') erkennen; ferner ergeben sie für ungerade Primzahlen w vollständig die Formeln (c''), (c'''), wenn man der Reihe nach die verschiedenen möglichen Fälle in Hinsicht auf Teilbarkeit oder Nichtteilbarkeit der Zahlen n, n', m durch w in Betracht zieht.

3. Im Falle $w = 2$ stellen wir zunächst folgende Betrachtung an: Es sei $f(x, y)$ eine ganzzahlige homogene Funktion zweiten Grades von x, y und n eine ungerade ganze rationale Zahl; wenn die Kongruenz $n \equiv f(x, y)$ nach 2^3 durch ganze rationale Zahlen x, y lösbar ist, so ist diese Kongruenz auch nach jeder höheren Potenz $2^{e+1} (e \geqq 3)$ lösbar. Wir beweisen dies durch einen Schluß von e auf $e+1$. Es seien a, b zwei ganze rationale Zahlen, für welche $n \equiv f(a, b)$ nach 2^e gilt, wobei der Exponent $e \geqq 3$ sei. Ist dann nicht auch zugleich $n \equiv f(a, b)$ nach 2^{e+1}, sondern vielmehr $n \equiv f(a, b) + 2^e$ nach 2^{e+1}, so bestimmen wir, was wegen $e \geqq 3$ angängig ist, eine ganze rationale Zahl c derart, daß $c^2 \equiv 1 + 2^e$ nach 2^{e+1} ist; dann wird

$$f(ca, cb) = c^2 f(a, b) \equiv f(a, b) + 2^e f(a, b) \equiv f(a, b) + 2^e \equiv n, (2^{e+1}),$$

und hiermit ist die Behauptung bewiesen.

Um nun zunächst für ein ungerades n das Symbol $\left(\frac{n, m}{2}\right)$ zu bestimmen, müssen wir untersuchen, für welche zusammengehörigen Werte von n und m die Kongruenzen

$$n \equiv x^2 + xy - \frac{m-1}{4} y^2, \quad \text{bez.} \quad n \equiv x^2 - m y^2, \quad (2^3) \qquad (23)$$
$$((m \equiv 1, (4)) \qquad ((m \equiv 2, 3, (4))$$

lösbar sind. Eine kurze Rechnung liefert folgende Tabelle, in welcher unter der Rubrik m die sechs hier in Frage kommenden Reste von m nach 2^3 und unter der Rubrik n diejenigen ungeraden Reste von n nach 2^3 verzeichnet stehen, für welche jedesmal die zugehörige Kongruenz (23) nach 2^3 lösbar ist.

m	n
1	1, 3, 5, 7
2	1, 7
3	1, 5
5	1, 3, 5, 7
6	1, 3
7	1, 5

Diese Tabelle lehrt für den Fall, daß n, m ungerade sind, die Richtigkeit der Gleichung (b'); und für den Fall, daß n ungerade und m gerade, $= 2m'$, ist, entspringt aus ihr:

$$\left(\frac{n, 2m'}{2}\right) = (-1)^{\frac{n^2-1}{8} + \frac{n-1}{2} \cdot \frac{m'-1}{2}}.$$

Ist andererseits n gerade, $= 2n'$, und m ungerade, so haben wir die beiden Fälle $m \equiv 1$ und $m \equiv 3$ nach 4 zu unterscheiden. Im ersteren Falle muß die Zahl 2 im Körper $k(\sqrt{m})$ jedenfalls das Produkt zweier verschiedener Primideale sein, sobald $n = 2n'$ Normenrest nach 2 in $k(\sqrt{m})$ sein soll, d. h. es muß $\left(\frac{m}{2}\right) = +1$ sein. Ist diese Bedingung erfüllt, so kann man stets in $k(\sqrt{m})$ eine Zahl α finden, für welche die Norm $n(\alpha)$ durch 2, aber nicht durch 4 teilbar ist; dann folgt:

$$\left(\frac{2n', m}{2}\right) = \left(\frac{2n' \cdot n(\alpha), m}{2}\right) = \left(\frac{\frac{n' \cdot n(\alpha)}{2}, m}{2}\right),$$

und dieses letztere Symbol ist nach Formel (b') gleich $+1$; mithin gilt in diesem Falle die Formel:

$$\left(\frac{2n', m}{2}\right) = \left(\frac{m}{2}\right) = (-1)^{\frac{m^2-1}{8}}.$$

In dem anderen Falle, $m \equiv 3$ nach 4, hängt der Wert des fraglichen Symbols von der Lösbarkeit der Kongruenz $2n' \equiv x^2 - m y^2$ nach beliebig hohen Potenzen 2^e ab, und jede solche Kongruenz ist, wie man leicht sieht, dann und nur dann lösbar, wenn die Kongruenz $m \equiv x^2 - 2n' y^2$ nach der nämlichen Potenz 2^e lösbar ist; also findet man hier:

$$\left(\frac{2n', m}{2}\right) = \left(\frac{m, 2n'}{2}\right).$$

Sind endlich die Zahlen n und m beide durch 2 teilbar, und ist $n = 2n'$ und $m = 2m'$, so gilt die Formel:

$$\left(\frac{2n', 2m'}{2}\right) = \left(\frac{-2^2 n' m', 2m'}{2}\right) = \left(\frac{-n' m', 2m'}{2}\right).$$

Aus den gewonnenen Resultaten folgt unmittelbar die Formel (b''); zugleich erkennen wir, daß die Formeln (c''), (c''') auch für $w = 2$ gültig sind. Die Formel (c'''') folgt allgemein durch Verbindung von (c''') mit (c''). Damit ist der Beweis des Satzes 98 in allen Teilen erbracht.

Aus den Formeln (a'), (a''), (b'), (b'') in Satz 98 läßt sich folgende Tatsache ableiten:

Wenn man ein vollständiges System zu w primer und nach w^e inkongruenter Zahlen ins Auge faßt, wo $e \geqq 1$ und im Falle $w = 2$ sogar $e > 2$ sei, so sind entweder alle diese Zahlen Normenreste des quadratischen Körpers $k\left(\sqrt{m}\right)$ nach w oder nur die Hälfte, je nachdem w zu der Diskriminante von $k\left(\sqrt{m}\right)$ prim ist oder nicht.

§ 65. Das Charakterensystem eines Ideals.

Wir bezeichnen die verschiedenen in der Diskriminante des Körpers $k\left(\sqrt{m}\right)$ aufgehenden rationalen Primzahlen, deren Anzahl t sei, mit $l_1, \ldots, l_t$. Zu einer jeden beliebigen ganzen rationalen Zahl a gehören dann ganz bestimmte Werte ($= +1$ oder -1) der t einzelnen Symbole

$$\left(\frac{a, m}{l_1}\right), \ldots, \left(\frac{a, m}{l_t}\right),$$

deren Bedeutung aus dem vorigen Paragraphen zu ersehen ist; diese t Einheiten ± 1 sollen **das Charakterensystem der Zahl** a im Körper $k\left(\sqrt{m}\right)$ heißen. Um auch einem jeden Ideal $\mathfrak{a}$ des Körpers $k\left(\sqrt{m}\right)$ in bestimmter Weise ein Charakterensystem zuzuordnen, unterscheiden wir die zwei Fälle, ob k ein imaginärer oder ein reeller Körper ist. Im ersteren Falle sind die Normen von Zahlen in $k\left(\sqrt{m}\right)$ stets positiv; wir setzen $r = t$, $\overline{n} = +n(\mathfrak{a})$ und bezeichnen die r Einheiten

$$\left(\frac{\overline{n}, m}{l_1}\right), \ldots, \left(\frac{\overline{n}, m}{l_r}\right) \tag{24}$$

als das **Charakterensystem des Ideals** $\mathfrak{a}$; dasselbe ist durch das Ideal $\mathfrak{a}$ völlig eindeutig bestimmt. Im zweiten Falle bilden wir zunächst das Charakterensystem der Zahl -1:

$$\left(\frac{-1, m}{l_1}\right), \ldots, \left(\frac{-1, m}{l_t}\right). \tag{25}$$

Fallen diese t Einheiten sämtlich gleich $+1$ aus, so setzen wir wie im ersteren Falle $\overline{n} = +n(\mathfrak{a})$, $r = t$ und bezeichnen wieder die r Einheiten (24) als das **Charakterensystem des Ideals** $\mathfrak{a}$. Kommt dagegen unter den t Charakteren (25) die Einheit -1 vor, so nehmen wir an, es sei etwa $\left(\frac{-1, m}{l_t}\right) = -1$, und setzen $r = t - 1$ und $\overline{n} = \pm n(\mathfrak{a})$ mit solchem Vorzeichen $\pm$, daß $\left(\frac{\overline{n}, m}{l_t}\right) = +1$ wird, und nennen die bei dieser Annahme von r und $\overline{n}$ entspringenden r Einheiten (24) das **Charakterensystem des Ideals** $\mathfrak{a}$. Bei den so getroffenen Festsetzungen wird der folgende Satz 99 sich ergeben.

§ 66. Das Charakterensystem einer Idealklasse und der Begriff des Geschlechts.

Satz 99. Die Ideale einer und derselben Klasse im Körper $k\left(\sqrt{m}\right)$ besitzen alle dasselbe Charakterensystem.

Beweis. Gehören die Ideale $\mathfrak{a}$ und $\mathfrak{a}'$ in $k\left(\sqrt{m}\right)$ zu einer und derselben Idealklasse, so existiert eine ganze oder gebrochene Zahl α in $k\left(\sqrt{m}\right)$ von der Art, daß $\mathfrak{a}' = \alpha\mathfrak{a}$ wird. Alsdann ist $n(\mathfrak{a}') = \pm n(\alpha) n(\mathfrak{a})$, wo $\pm$ das Vorzeichen von $n(\alpha)$ bedeutet, und es wird daher:

$$\left(\frac{n(\mathfrak{a}'), m}{l}\right) = \left(\frac{\pm n(\mathfrak{a}), m}{l}\right)$$

für $l = l_1, \ldots, l_t$. Mit Rücksicht auf die Festsetzungen in § 65 erhält man sogleich den Satz 99.

Auf diese Weise ist einer jeden Idealklasse ein bestimmtes Charakterensystem zugeordnet. Wir rechnen nun alle diejenigen Idealklassen, welche ein und dasselbe Charakterensystem besitzen, in ein **Geschlecht** und definieren insbesondere das **Hauptgeschlecht** als die Gesamtheit aller derjenigen Klassen, deren Charakterensystem aus lauter positiven Einheiten besteht. Da das Charakterensystem der Hauptklasse offenbar von der letzteren Eigenschaft ist, so gehört die Hauptklasse stets zum Hauptgeschlecht. Aus der Formel (c''') auf S. 162 entnehmen wir leicht die Tatsache, daß die Multiplikation der Idealklassen zweier Geschlechter die Idealklassen eines Geschlechtes liefert, dessen Charakterensystem durch Multiplikation der entsprechenden Charaktere beider Geschlechter erhalten wird. Im besonderen folgt, daß das Charakterensystem des Quadrates einer Idealklasse aus einem ganz beliebigen Geschlecht stets aus lauter positiven Einheiten besteht und mithin das Quadrat einer jeden Idealklasse stets dem Hauptgeschlecht angehört.

Jedes Geschlecht enthält offenbar gleich viel Klassen.

§ 67. Der Fundamentalsatz über die Geschlechter des quadratischen Körpers.

Es entsteht nun die Frage, ob ein jedes beliebige System von r Einheiten ± 1 das Charakterensystem eines Geschlechtes des Körpers $k(\sqrt{m})$ sein kann. Die Beantwortung dieser Frage ist für die Theorie der quadratischen Körper von grundlegender Bedeutung; sie ist in folgendem Satz enthalten, dessen Beweis uns bis zum § 78 beschäftigen wird:

Satz 100. *Ein beliebig vorgelegtes System von r Einheiten ± 1 ist dann und nur dann Charakterensystem eines Geschlechtes des Körpers $k(\sqrt{m})$, wenn das Produkt der sämtlichen r Einheiten $= +1$ ist. Die Anzahl der im Körper $k(\sqrt{m})$ vorhandenen Geschlechter ist daher gleich 2^{r-1}* [Gauss (*I*)].

§ 68. Ein Hilfssatz über diejenigen quadratischen Körper, deren Diskriminanten nur durch eine einzige Primzahl teilbar sind.

Um uns dem durch den Satz 100 gesteckten Ziele zu nähern, beweisen wir zunächst folgenden Hilfssatz:

Hilfssatz 13. Wenn in der Diskriminante eines quadratischen Körpers $k = k(\sqrt{m})$ nur eine einzige rationale Primzahl l aufgeht, so ist die Anzahl der Idealklassen in k ungerade. Das Charakterensystem besteht für den Körper k aus dem einen, auf die Primzahl l bezüglichen Charakter; dieser Charakter ist stets $= +1$, d. h. es gibt im Körper k nur ein Geschlecht: das Hauptgeschlecht.

Beweis. Wir bezeichnen mit s diejenige Substitution für die Zahlen des Körpers k, welche aus ihnen die Konjugierten entstehen läßt. Es bedeute im Falle $m > 0$ wieder ε eine Grundeinheit des Körpers k, eine ebensolche Einheit stellen $-\varepsilon, \frac{1}{\varepsilon}, -\frac{1}{\varepsilon}$ vor; wir beweisen dann zunächst, daß bei der im Hilfssatze gemachten Voraussetzung notwendig $n(\varepsilon) = \varepsilon \cdot s\varepsilon = -1$ ausfallen muß. In der Tat, nehmen wir an, es wäre $n(\varepsilon) = +1$, so könnte man nach Satz 90 eine ganze Zahl α des Körpers k finden derart, daß man $\varepsilon = \frac{\alpha}{s\alpha}$ hätte; dann folgt $\alpha = \varepsilon \cdot s\alpha$, d. h. jeder in α aufgehende ideale Primfaktor ginge auch in $s\alpha$ auf. Da für $m > 0$ unter der im Hilfssatze gemachten Voraussetzung $\sqrt{m}$ der einzige, seinem konjugierten gleiche und nicht zugleich rationale Primfaktor in k ist, so muß entweder $\alpha = \eta a$ oder $= \eta\sqrt{m}\,a$ sein, wo η eine Einheit und a eine ganze rationale positive oder negative Zahl bedeutet; hieraus würde $\varepsilon = \pm\eta^{1-s} = \pm\eta^2$ hervorgehen, und dies widerspräche der Annahme, daß ε eine Grundeinheit des Körpers k ist.

Nunmehr gehen wir dazu über, den ersten Teil des Hilfssatzes zu beweisen. Wäre für den Körper k die Klassenanzahl h eine gerade Zahl, so müßte es nach Satz 57 in k ein nicht zur Hauptklasse gehöriges Ideal $\mathfrak{j}$ geben derart, daß $\mathfrak{j}^2 \sim 1$ ist; wegen $\mathfrak{j} \cdot s\mathfrak{j} \sim 1$ würde hieraus $\mathfrak{j} \sim s\mathfrak{j}$ folgen. Setzen wir $\mathfrak{j} = \alpha \cdot s\mathfrak{j}$ oder $\mathfrak{j}^{1-s} = \alpha$, so ist α eine Zahl in k, deren Norm $n(\alpha) = \pm 1$ sein muß. Im Falle, daß hier das positive Vorzeichen statthätte, setze man $\beta = \alpha$; der andere Fall ist von vornherein nur bei einem reellen Körper denkbar; wir setzen dann $\beta = \varepsilon\alpha$, wo ε, wie vorhin, die Grundeinheit in k bedeutet. Unter den getroffenen Festsetzungen hätte man jedesmal $n(\beta) = +1$, und mithin wäre nach Satz 90 stets $\frac{1}{\beta} = \gamma^{1-s}$, wo γ eine ganze Zahl in k bezeichnet. Aus $\alpha = \mathfrak{j}^{1-s}$ entstünde dann $(\gamma\mathfrak{j})^{1-s} = 1$, d. h. $(\gamma)\mathfrak{j} = s(\gamma\mathfrak{j})$, und hieraus würde, ähnlich wie vorhin, folgen, daß das Ideal $(\gamma)\mathfrak{j}$ entweder $= (a)$ oder $= (a)\mathfrak{l}$ sein muß, wo a eine ganze rationale Zahl und $\mathfrak{l}$ den einzigen in k vorhandenen, seinem Konjugierten gleichen und nicht zugleich rationalen Primfaktor bezeichnet. Nun ist für $m \neq -1$ dieser Primfaktor $\mathfrak{l} = \sqrt{m}$ und für $m = -1$ offenbar $\mathfrak{l} = 1 + \sqrt{-1}$, also stets $\mathfrak{l} \sim 1$; somit würde $\mathfrak{j} \sim 1$ folgen, was der über $\mathfrak{j}$ gemachten Annahme zuwiderläuft.

Ist k ein reeller Körper, so folgt zugleich aus $n(\varepsilon) = -1$, daß

$$\left(\frac{-1, m}{l}\right) = +1$$

ist, und es besteht mithin gemäß § 65 in jedem Falle das Charakterensystem für ein Ideal $\mathfrak{j}$ im Körper k aus der einen Einheit $\left(\frac{+n(\mathfrak{j}), m}{l}\right)$; dieser eine Charakter ist für jedes Ideal $\mathfrak{j}$ in k gleich $+1$, da sonst die Gesamtheit der Idealklassen von k in zwei Geschlechter zerfiele und somit die Klassenanzahl h gerade sein müßte.

Der eben bewiesene Hilfssatz 13 zeigt die Richtigkeit des Fundamentalsatzes 100 im einfachsten Falle, nämlich für diejenigen quadratischen Körper, deren Diskriminante d nur eine einzige rationale Primzahl enthält.

§ 69. Das Reziprozitätsgesetz für quadratische Reste. Ein Hilfssatz über das Symbol $\left(\frac{n, m}{w}\right)$.

Satz 101. *Sind p, q rationale positive, voneinander verschiedene, ungerade Primzahlen, so gilt die Regel:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

das sogenannte Reziprozitätsgesetz für quadratische Reste. Überdies gelten die folgenden Regeln:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

die sogenannten Ergänzungssätze zum quadratischen Reziprozitätsgesetz [Gauss (*I*)].

Beweis. Ist $k(\sqrt{m})$ ein Körper, dessen Diskriminante nur eine Primzahl l enthält, und bedeutet n die Norm eines Ideals in diesem Körper k, so ist nach dem Hilfssatze 13 stets $\left(\frac{n, m}{l}\right) = +1$. Nun ist nach Satz 96 oder 97 insbesondere jede positive ungerade und in m nicht aufgehende rationale Primzahl, von welcher m quadratischer Rest ist, Norm eines Ideals in $k(\sqrt{m})$. Die Benutzung dieses Umstandes liefert uns die nachstehende Tabelle; in derselben bedeuten p, p' irgend voneinander verschiedene positive rationale und der Zahl 1 nach 4 kongruente Primzahlen, und andererseits bedeuten q, q' voneinander verschiedene positive rationale und der Zahl 3 nach 4 kongruente Primzahlen, während r eine positive rationale ungerade Primzahl bezeichnet, von welcher kein bestimmter Restcharakter nach 4 vorausgesetzt wird.

				Wenn:	so ist:
	m	l	n	$\left(\frac{m}{n}\right) = +1$	$\left(\frac{n, m}{l}\right) = +1$
1.	-1	2	r	$\left(\frac{-1}{r}\right) = +1$	$\left(\frac{r, -1}{2}\right) = (-1)^{\frac{r-1}{2}} = +1$
2.	2	2	r	$\left(\frac{2}{r}\right) = +1$	$\left(\frac{r, 2}{2}\right) = (-1)^{\frac{r^2-1}{8}} = +1$
3.	p	p	p'	$\left(\frac{p}{p'}\right) = +1$	$\left(\frac{p', p}{p}\right) = \left(\frac{p'}{p}\right) = +1$
4.	p	p	q	$\left(\frac{p}{q}\right) = +1$	$\left(\frac{q, p}{p}\right) = \left(\frac{q}{p}\right) = +1$
5.	$-q$	q	p	$\left(\frac{-q}{p}\right) = +1$	$\left(\frac{p, -q}{q}\right) = \left(\frac{p}{q}\right) = +1$
6.	$-q$	q	q'	$\left(\frac{-q}{q'}\right) = +1$	$\left(\frac{q', -q}{q}\right) = \left(\frac{q'}{q}\right) = +1$

Nehmen wir die in einem Körper $k(\sqrt{p})$ aus $n(\varepsilon) = -1$ folgende Tatsache, daß $\left(\frac{-1}{p}\right) = +1$ ist, zur Zeile 1 dieser Tabelle hinzu, so folgt allgemein $\left(\frac{-1}{r}\right) = (-1)^{\frac{r-1}{2}}$. Wenden wir ferner die am Eingange dieses Beweises genannte Tatsache auf die Primzahl $n = 2$ an, und berücksichtigen wir, daß die Zahl 2 stets gleich der Norm eines Ideals in $k(\sqrt{p})$ oder in $k(\sqrt{-q})$ ist, sobald $(-1)^{\frac{p^2-1}{8}} = +1$, bezüglich $(-1)^{\frac{q^2-1}{8}} = +1$ statthat, so folgt, daß unter der letzteren Voraussetzung stets $\left(\frac{2, p}{p}\right) = \left(\frac{2}{p}\right) = +1$, bezüglich

$\left(\frac{2, -q}{q}\right) = \left(\frac{2}{q}\right) = +1$ ist, d. h.: wenn $(-1)^{\frac{r^2-1}{8}} = +1$ ist, so ist $\left(\frac{2}{r}\right) = +1$. Nehmen wir diese Tatsache zur Zeile 2 der obigen Tabelle hinzu, so folgt allgemein $\left(\frac{2}{r}\right) = (-1)^{\frac{r^2-1}{8}}$. Aus dem Inhalte der Zeile 3 folgt $\left(\frac{p}{p'}\right) = \left(\frac{p'}{p}\right)$. Aus Zeile 4 und 5 folgt $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$; Zeile 6 ergibt nur, daß aus

$$\left(\frac{-q}{q'}\right) = +1 \quad \text{auch} \quad \left(\frac{q'}{q}\right) = +1$$

folgt.

Um allgemein das Reziprozitätsgesetz für zwei rationale Primzahlen q, q', die beide kongruent 3 nach 4 sind, nachzuweisen, betrachtet man am einfachsten den quadratischen Körper $k(\sqrt{qq'})$. Da wegen $\left(\frac{-1, qq'}{q}\right) = -1$ die Norm der Grundeinheiten ε dieses Körpers jedenfalls gleich $+1$ sein muß, so gibt es nach Satz 90 eine ganze Zahl α in $k(\sqrt{qq'})$ von der Beschaffenheit, daß $\varepsilon = \alpha^{1-s} = \frac{\alpha}{s\alpha}$ wird, wo $s\alpha$ die zu α konjugierte Zahl bedeutet, und hieraus schließen wir leicht, daß das in q enthaltene ambige Primideal $\mathfrak{q}$ notwendig ein Hauptideal sein muß. Folglich ist bei geeigneter Wahl des Vorzeichens gleichzeitig

$$\left(\frac{\pm q, qq'}{q}\right) = +1 \quad \text{und} \quad \left(\frac{\pm q, qq'}{q'}\right) = +1,$$

es ist daher in jedem Falle

$$\left(\frac{q, qq'}{q}\right) = \left(\frac{q, qq'}{q'}\right),$$

das heißt mit Rücksicht auf die Formel (c') in Satz 98

$$-\left(\frac{q'}{q}\right) = \left(\frac{q}{q'}\right).$$

Hilfssatz 14. Wenn n und m zwei beliebige ganze rationale Zahlen bedeuten, welche nicht beide negativ sind, so ist

$$\prod_{(w)} \left(\frac{n, m}{w}\right) = +1,$$

wo das Produkt linker Hand über sämtliche rationale Primzahlen w zu erstrecken ist.

Beweis. Bedeuten p, q beliebige rationale ungerade, voneinander verschiedene Primzahlen, so folgen aus den Regeln (a''), (b'), (b'') in § 64 und aus Satz 101 leicht die Formeln:

$$\left(\frac{-1, 2}{2}\right) = +1, \qquad \left(\frac{-1, p}{2}\right)\left(\frac{-1, p}{p}\right) = +1,$$

$$\left(\frac{2, 2}{2}\right) = +1, \qquad \left(\frac{2, p}{2}\right)\left(\frac{2, p}{p}\right) = +1,$$

$$\left(\frac{p, p}{2}\right)\left(\frac{p, p}{p}\right) = +1, \qquad \left(\frac{p, q}{2}\right)\left(\frac{p, q}{p}\right)\left(\frac{p, q}{q}\right) = +1;$$

mit Rücksicht auf die Regel (a′) in § 64 besteht danach der Hilfssatz 14 für den Fall, daß die Zahlen n, m gleich ± 1 sind oder nur einen Primzahlfaktor enthalten. Wegen der Formeln (c‴), (c⁗) in § 64 gilt demnach der Hilfssatz 14 allgemein.

Zugleich folgt wegen $\left(\frac{-1,-1}{2}\right) = -1$, daß, wenn die Zahlen n und m beide negativ angenommen werden, das entsprechende Produkt $\prod_{(w)}$ den Wert -1 hat. Die im Hilfssatze 14 ausgesprochene und diese weitere Behauptung erhalten, wie man leicht erkennt, einen einheitlichen Ausdruck, wenn man sich des neuen Symbols $\left(\frac{n,m}{-1}\right) = \pm 1$ bedienen will, wo rechter Hand das positive oder das negative Vorzeichen gelten soll, je nachdem wenigstens eine der beiden Zahlen n, m positiv ist oder beide negativ ausfallen.

§ 70. Beweis der im Fundamentalsatz 100 ausgesprochenen Beziehung zwischen den sämtlichen Charakteren eines Geschlechts.

Der im § 69 bewiesene Hilfssatz 14 dient dazu, um den einen Teil unseres Fundamentalsatzes 100 zu beweisen. Bedeutet A irgendeine Idealklasse des Körpers $k\left(\sqrt{m}\right)$, ist dann $\mathfrak{a}$ ein zu 2 und zu d primes Ideal der Klasse A, und wird $\bar{n} = \pm n(\mathfrak{a})$ die mit dem betreffenden Vorzeichen gemäß § 65 versehene Norm des Ideals $\mathfrak{a}$, so ist das Produkt der sämtlichen Charaktere der Klasse A durch den Ausdruck:

$$\left(\frac{\bar{n},m}{l_1}\right) \cdots \left(\frac{\bar{n},m}{l_r}\right)$$

gegeben. Da $n(\mathfrak{a})$ die Norm eines Ideals ist, so muß eine jede in $\bar{n}$ zu ungerader Potenz vorkommende rationale Primzahl p im Körper $k\left(\sqrt{m}\right)$ zerlegbar sein; es ist mithin nach Satz 96 m von jeder solchen Primzahl p quadratischer Rest. Aus Hilfssatz 14 und unter Heranziehung der Formeln (c‴), (a′), (a″) aus Satz 98 folgt daher:

$$\prod_{(w)} \left(\frac{\bar{n},m}{w}\right) = +1,$$

wenn w alle in m enthaltenen ungeraden Primzahlen und die Primzahl 2 durchläuft.

Kommt nun in der Diskriminante d des Körpers $k\left(\sqrt{m}\right)$ die Primzahl 2 vor, so ist schon hiermit bewiesen, daß für jede Klasse in $k\left(\sqrt{m}\right)$ das Produkt sämtlicher Charaktere $= +1$ ist.

Kommt dagegen die Primzahl 2 in d nicht vor, so hat man, wegen $m \equiv 1$ nach 4, stets $\left(\frac{\bar{n},m}{2}\right) = +1$, und damit ist auch in diesem Falle der gewünschte Nachweis erbracht.

Durch den soeben geführten Nachweis, daß das Produkt aller Charaktere $= +1$ ist, erkennen wir zugleich, daß die Anzahl der Geschlechter im quadratischen Körper $k\left(\sqrt{m}\right)$ höchstens gleich der Hälfte aller an sich denkbaren Charakterensysteme, d. h. höchstens gleich 2^{r-1} sein kann.

18. Die Existenz der Geschlechter im quadratischen Körper.

§ 71. Der Satz von den Normen der Zahlen eines quadratischen Körpers.

Es bleibt noch übrig, den anderen Teil des Fundamentalsatzes 100 als richtig zu erkennen, d. h. den Nachweis zu führen, daß die eben gefundene Bedingung, welche ein System von r Einheiten ± 1 notwendig erfüllen muß, damit dasselbe als das Charakterensystem eines Geschlechtes in $k\left(\sqrt{m}\right)$ vorkommen kann, auch für diesen Umstand hinreichend ist. Dieser Nachweis kann auf zwei völlig verschiedenen Wegen erbracht werden; der erste Weg ist rein arithmetischer Natur, der zweite benutzt wesentlich transzendente Hilfsmittel. Der erste Beweis geschieht durch folgende Überlegungen:

Satz 102[1]. Wenn n, m zwei ganze rationale Zahlen bedeuten, von denen m keine Quadratzahl ist, und die für jede beliebige Primzahl w die Bedingung

$$\left(\frac{n,m}{w}\right) = +1$$

erfüllen, so ist die Zahl n stets gleich der Norm einer ganzen oder gebrochenen Zahl α des Körpers $k\left(\sqrt{m}\right)$.

Beweis. Wegen $\prod_{(w)} \left(\frac{n,m}{w}\right) = +1$ ist gemäß der Bemerkung auf S. 172 oben wenigstens eine der beiden Zahlen n, m positiv. Wir dürfen voraussetzen, daß n und m keine rationalen quadratischen Faktoren enthalten. Bedeutet dann p eine in n als Faktor enthaltene Primzahl, welche zugleich in der Diskriminante d des Körpers $k\left(\sqrt{m}\right)$ aufgeht, so ist p gleich der Norm eines Ideals in $k\left(\sqrt{m}\right)$. Bedeutet ferner p eine ungerade, in n, aber nicht in m aufgehende Primzahl, so ist, wegen

$$\left(\frac{n,m}{p}\right) = \left(\frac{m}{p}\right) = +1,$$

diese Primzahl p ebenfalls gleich der Norm eines Ideals in $k\left(\sqrt{m}\right)$. Ist endlich die Primzahl 2 in n, aber nicht in der Diskriminante des Körpers $k\left(\sqrt{m}\right)$ enthalten, so ist wegen $\left(\frac{n,m}{2}\right) = \left(\frac{2,m}{2}\right) = (-1)^{\frac{m^2-1}{8}} = +1$ wiederum die Primzahl 2 gleich der Norm eines Ideals in $k\left(\sqrt{m}\right)$, und mithin gibt es in $k\left(\sqrt{m}\right)$

[1] Die Kriterien für die Auflösbarkeit der quadratischen ternären diophantischen Gleichungen sind zuerst von LAGRANGE gefunden worden. [LAGRANGE (*I*).]

gewiß stets ein Ideal j derart, daß $|n| = n(\mathfrak{j})$ wird. Wir wählen nun in der durch j bestimmten Idealklasse ein solches Ideal j′ aus, dessen Norm $n(\mathfrak{j}') \leqq |\sqrt{d}|$ ist, wo d die Diskriminante des durch $\sqrt{m}$ bestimmten Körpers bedeutet. Dies ist nach Satz 50 stets möglich. Wir setzen dann $\mathfrak{j}' = \varkappa\mathfrak{j}$ und $n' = n \cdot n(\varkappa)$; dabei bedeutet $\varkappa$ eine ganze oder gebrochene Zahl in $k(\sqrt{m})$, und es wird $n' = \pm n(\mathfrak{j}')$, wo das positive oder das negative Vorzeichen gilt, je nachdem $n \cdot n(\varkappa)$ positiv oder negativ ausfällt. Die ganze rationale Zahl n' fällt daher insbesondere gewiß positiv aus, falls m negativ ist. Da d den Wert m oder $4m$ hat, so ist gewiß $|n'| \leqq 2|\sqrt{m}|$, und hieraus folgt $|n'| < |m|$, sobald $2|\sqrt{m}| < |m|$, d. h. $|m| > 4$ ist. Andererseits gilt wegen $n' = n \cdot n(\varkappa)$ die Gleichung $\left(\frac{n, m}{w}\right) = \left(\frac{n', m}{w}\right) = +1$ und dann nach Formel (c″) in Satz 98 auch $\left(\frac{m, n'}{w}\right) = +1$ für jede beliebige Primzahl w.

Wir machen nun die Annahme, daß der zu beweisende Satz 102 bereits für jeden Körper $k(\sqrt{m'})$ feststehe, bei welchem die bestimmende Zahl m', mag sie positiv oder negativ sein, der Ungleichung $|m'| < |m|$ genügt. Sowie die vorhin gefundene Zahl n' die Bedingung $|n'| < |m|$ erfüllt und keine Quadratzahl ist, muß dann, da auch die Bedingung $\left(\frac{m, n'}{w}\right) = +1$ für jede beliebige Primzahl w gilt, infolge der angenommenen Gültigkeit unseres Satzes 102, die Zahl m die Norm einer Zahl α' im Körper $k(\sqrt{n'})$ sein, d. h. es gibt zwei ganze oder gebrochene rationale Zahlen a und b derart, daß $m = a^2 - n'b^2$ wird; wenn aber n' eine Quadratzahl ist, so versteht sich die Möglichkeit dieser Gleichung ohne weiteres. Da $b \neq 0$ sein muß, so folgt hieraus $n' = \left(\frac{a}{b}\right)^2 - m\left(\frac{1}{b}\right)^2 = n(\lambda)$, d. h. es ist n' die Norm einer Zahl λ im Körper $k(\sqrt{m})$. Die Verbindung dieser Tatsache mit der Gleichung $n' = n \cdot n(\varkappa)$ ergibt $n = n(\alpha)$, wo $\alpha = \frac{\lambda}{\varkappa}$ wieder eine Zahl in $k(\sqrt{m})$ bedeutet.

Der vollständige Beweis unseres Satzes 102 wird hiernach offenbar geführt sein, sobald wir seine Richtigkeit für alle die Fälle erkannt haben, in denen $|m| \leqq 4$ und zugleich $|n| \leqq |\sqrt{d}|$ statthat. Bei dieser Einschränkung der Zahlen n, m treffen die Bedingungen des Satzes 102 nur in 8 Fällen zu. Die Gleichungen

$$\begin{aligned} 1 &= n(\sqrt{-1}), & -2 &= n(\sqrt{2}), \\ 2 &= n(1+\sqrt{-1}), & 2 &= n(\sqrt{-2}), \\ 2 &= n(2+\sqrt{2}), & -2 &= n(1+\sqrt{3}), \\ -1 &= n(1+\sqrt{2}), & -3 &= n(\sqrt{3}), \end{aligned}$$

zeigen, daß in diesen 8 Fällen unser Satz 102 gültig ist.

Man erkennt leicht, daß der Satz 102 auch in der Abänderung zutrifft, daß die Erfüllung der Bedingung $\left(\frac{n, m}{w}\right) = +1$ nur für alle ungeraden Primzahlen w verlangt, dann aber die Bedingung hinzugefügt wird, daß wenigstens eine der beiden Zahlen n, m positiv ist [Lagrange (*I*), Legendre (*I*), Gauss (*I*)]; in der Tat ist nach Hilfssatz 14 die Gleichung $\left(\frac{n, m}{2}\right) = +1$ dann von selbst miterfüllt.

§ 72. Die Klassen des Hauptgeschlechtes.

Am Schlusse des § 66 haben wir gezeigt, daß das Quadrat einer Idealklasse stets dem Hauptgeschlechte angehört. Durch den Satz 102 des § 71 haben wir ein Mittel, die umgekehrte Tatsache einzusehen.

Satz 103. In einem quadratischen Körper ist jede Klasse des Hauptgeschlechtes stets gleich dem Quadrat einer Klasse [Gauss (*I*)].

Beweis. Es sei H im Körper $k(\sqrt{m})$ eine Klasse des Hauptgeschlechts, $\mathfrak{h}$ ein solches Ideal aus der Klasse H, welches zur Diskriminante d des Körpers $k(\sqrt{m})$ prim ausfällt, und $\bar{n}$ sei die mit dem bezüglichen Vorzeichen gemäß § 65 versehene Norm des Ideals $\mathfrak{h}$. Diese Zahl $\bar{n}$ erfüllt dann für jede beliebige Primzahl w die Bedingung $\left(\frac{\bar{n}, m}{w}\right) = +1$, und es ist mithin dem Satze 102 zufolge $\bar{n} = n(\alpha)$, wo α eine ganze oder gebrochene Zahl des Körpers $k(\sqrt{m})$ bedeutet. Setzen wir $\frac{\mathfrak{h}}{\alpha} = \frac{\mathfrak{k}}{\mathfrak{k}'}$, wo $\mathfrak{k}$ und $\mathfrak{k}'$ zueinander prime Ideale seien, so folgt $\frac{\mathfrak{k} \cdot s\mathfrak{k}}{\mathfrak{k}' \cdot s\mathfrak{k}'} = 1$, und mithin ist notwendigerweise $\mathfrak{k}' = s\mathfrak{k}$. Da $\mathfrak{k} \cdot s\mathfrak{k} \sim 1$ ist, so folgt $\mathfrak{h} \sim \mathfrak{k}^2$.

Die eben bewiesene charakteristische Eigenschaft der Ideale des Hauptgeschlechts steht in engem Zusammenhange mit einer anderen gleichfalls charakteristischen Eigenschaft dieser Ideale, welche in folgendem Satze ihren Ausdruck findet:

Satz 104. Sind ω_1, ω_2 Basiszahlen des quadratischen Körpers k und η_1, η_2 Basiszahlen eines zum Hauptgeschlecht von k gehörigen Ideals $\mathfrak{h}$, und ist endlich N eine beliebig gegebene ganze rationale Zahl, so lassen sich stets vier rationale Zahlen $r_{11}, r_{12}, r_{21}, r_{22}$ finden, deren Nenner zu N prim sind, für welche die Determinante $r_{11}r_{22} - r_{12}r_{21}$ den Wert ± 1 hat, und vermittelst derer

$$\frac{\eta_1}{\eta_2} = \frac{r_{11}\omega_1 + r_{12}\omega_2}{r_{21}\omega_1 + r_{22}\omega_2}$$

wird.

Beweis. Man bestimme ein zu $\mathfrak{h}$ äquivalentes Ideal $\mathfrak{h}' = \beta\mathfrak{h}$, welches zu Nd prim ist. Wie in dem Beweise zum Satz 103 bereits benutzt wurde, ist $\bar{n} = \pm n(\mathfrak{h}')$, wenn das Vorzeichen gemäß § 65 gewählt wird, stets gleich

der Norm einer ganzen oder gebrochenen Zahl α im Körper k. Dabei kann α so gewählt werden, daß es eine zu Nd prime ganze rationale Zahl r gibt, so daß αr ganz wird. Das Ideal $r\alpha\mathfrak{h}' = r\alpha\beta\mathfrak{h}$ besitzt die Basiszahlen

$$r\alpha\beta\eta_1 = a_{11}\omega_1 + a_{12}\omega_2,$$
$$r\alpha\beta\eta_2 = a_{21}\omega_1 + a_{22}\omega_2,$$

wo $a_{11}, a_{12}, a_{21}, a_{22}$ ganze rationale Zahlen bedeuten. Wegen $n(\alpha\mathfrak{h}') = \overline{n}^2$ ist die Determinante $a_{11}a_{22} - a_{12}a_{21} = \pm r^2\overline{n}^2$ und daher besitzen die vier Zahlen $r_{11} = \frac{a_{11}}{r\overline{n}}$, $r_{12} = \frac{a_{12}}{r\overline{n}}$, $r_{21} = \frac{a_{21}}{r\overline{n}}$, $r_{22} = \frac{a_{22}}{r\overline{n}}$, die im Satze behauptete Eigenschaft.

§ 73. Die ambigen Ideale.

Im quadratischen Körper k werde ein Ideal $\mathfrak{a}$ ein **ambiges Ideal** genannt, wenn es nach Anwendung der Operation $s = (\sqrt{m} : -\sqrt{m})$ ungeändert bleibt, und wenn es außerdem keine ganze rationale Zahl $+ \pm 1$ als Faktor enthält. (Vgl. § 57.) Es gilt die Tatsache:

Satz 105. Die t in der Diskriminante d des Körpers k aufgehenden, voneinander verschiedenen Primideale $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$, und nur diese, sind ambige Primideale in k. Die 2^t Ideale $1, \mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_1\mathfrak{l}_2, \ldots, \mathfrak{l}_1\mathfrak{l}_2\ldots\mathfrak{l}_t$ machen die Gesamtheit aller ambigen Ideale des Körpers k aus.

Beweis. Daß die Primideale $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$, und nur diese, ambig sind, folgt aus Satz 96. Ist nun $\mathfrak{a} = \mathfrak{p}\mathfrak{q}\ldots\mathfrak{r}$ ein beliebiges, in Primideale zerlegtes ambiges Ideal, so müssen wegen $\mathfrak{a} = s\mathfrak{a}$ die zu den Primidealen $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}$ konjugierten Primideale $s\mathfrak{p}, s\mathfrak{q}, \ldots, s\mathfrak{r}$, von der Reihenfolge abgesehen, mit $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}$ übereinstimmen. Wenn etwa $s\mathfrak{p} = \mathfrak{q}$ sich herausstellen würde, so besäße $\mathfrak{a}$ den Faktor $\mathfrak{p}\cdot s\mathfrak{p}$, welcher gleich einer ganzen rationalen Zahl ist; da dieser Umstand der Erklärung des ambigen Ideals zuwider wäre, so muß notwendig $\mathfrak{p} = s\mathfrak{p}$ sein und ebenso $\mathfrak{q} = s\mathfrak{q}, \ldots, \mathfrak{r} = s\mathfrak{r}$, d. h. die einzelnen Primideale $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}$ sind sämtlich ambig. Da die Quadrate der Ideale $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ gleich ganzen rationalen Zahlen werden, so schließen wir ebenso, daß die Ideale $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}$ notwendig untereinander verschieden sind; damit ist auch der letzte Teil des Satzes 105 bewiesen.

§ 74. Die ambigen Idealklassen.

Wenn $\mathfrak{a}$ ein Ideal der Klasse A ist, so werde diejenige Idealklasse, der das Ideal $s\mathfrak{a}$ angehört, mit sA bezeichnet. Ist insbesondere $A = sA$, so heißt die Idealklasse A eine **ambige Idealklasse.** Da das Produkt $\mathfrak{a}\cdot s\mathfrak{a} \sim 1$ ist, so wird $A \cdot sA = 1$; und folglich ist das Quadrat einer jeden ambigen Klasse gleich der Hauptklasse 1. Umgekehrt, wenn das Quadrat einer Klasse A gleich 1 ist, so wird $A = \frac{1}{A} = sA$, und folglich ist A eine ambige Klasse.

§ 75. Die durch ambige Ideale bestimmten ambigen Idealklassen.

Es entsteht nun die Aufgabe, alle ambigen Klassen in k aufzustellen. Da offenbar ein jedes ambige Ideal $\mathfrak{a}$ vermöge seiner Eigenschaft $\mathfrak{a} = s\mathfrak{a}$ eine ambige Klasse bestimmt, so haben wir vor allem zu untersuchen, wie viele voneinander verschiedene ambige Klassen aus den 2^t ambigen Idealen entspringen. Wir bezeichnen allgemein irgend welche vorgelegte Idealklassen als **voneinander unabhängige Idealklassen,** wenn keine darunter die Klasse 1 ist und auch keine gleich einem Produkte von Potenzen der übrigen dieser Klassen gesetzt werden kann. Wir sprechen dann folgende Tatsache aus:

Satz 106. Die t ambigen Primideale bestimmen im Falle eines imaginären Körpers stets $t-1$ voneinander unabhängige ambige Klassen; im Falle eines reellen Körpers bestimmen sie $t-2$ oder $t-1$ voneinander unabhängige ambige Klassen, je nachdem die Norm der Grundeinheit ε des Körpers $n(\varepsilon) = +1$ oder $= -1$ ist. Die sämtlichen 2^t ambigen Ideale bestimmen im Falle eines imaginären Körpers 2^{t-1} und im Falle eines reellen Körpers, entsprechend der eben gemachten Unterscheidung, 2^{t-2} bez. 2^{t-1} voneinander verschiedene ambige Klassen.

Beweis. Das Produkt aus sämtlichen in m aufgehenden Primidealen ist gleich $\sqrt{m}$ und mithin ein Hauptideal in k. Ist zunächst m negativ, jedoch von -1 und -3 verschieden, und (α) ein ambiges Hauptideal in k, so muß α^{1-s} als Einheit notwendig $= (-1)^e$ sein, wo e die Werte 0 oder 1 haben kann; hieraus folgt:

$$\{\alpha(\sqrt{m})^e\}^{1-s} = 1 \quad \text{oder} \quad \alpha(\sqrt{m})^e = s\{\alpha(\sqrt{m})^e\},$$

d. h. $\alpha(\sqrt{m})^e$ ist dann eine ganze rationale Zahl. Damit ist bewiesen, daß in einem imaginären Körper $k(\sqrt{m})$ — von $k(\sqrt{-1})$ und $k(\sqrt{-3})$ abgesehen — gewiß außer 1 und $\sqrt{m}$ kein ambiges Hauptideal vorhanden ist. Die beiden hier zunächst ausgeschlossenen Fälle erledigen sich unmittelbar im Sinne des zu beweisenden Satzes 106.

Bei der Entscheidung der fraglichen Verhältnisse für einen reellen Körper k kommt es darauf an, ob die Norm der Grundeinheit ε des Körpers gleich $+1$ oder -1 ausfällt.

Ist nämlich $n(\varepsilon) = +1$, so kann man nach Satz 90 die Formel $\varepsilon = \alpha^{1-s}$ durch eine ganze Zahl α in k befriedigen und noch α ohne rationalen Faktor $+ \pm 1$ voraussetzen. Wegen $\alpha = \varepsilon\cdot s\alpha$ ist dann (α) ein ambiges Hauptideal. Dieses Hauptideal (α) ist von 1 und von $\sqrt{m}$ verschieden; denn wäre $\alpha = \pm\varepsilon^f$ oder $= \pm\varepsilon^f\sqrt{m}$, wo der Exponent f eine ganze rationale Zahl bedeutet, so würde

$$\alpha^{1-s} = (-1)^e\varepsilon^{(1-s)f} = (-1)^e\varepsilon^{2f} \qquad (e = 0 \text{ bzw. } 1)$$

folgen; letzterer Ausdruck aber ist stets von ε verschieden. Ist ferner α' ein

beliebiges ambiges Hauptideal des Körpers k, so ist notwendigerweise $\alpha'^{1-s} = (-1)^e \varepsilon'$, wo die Exponenten e und f ganze rationale Zahlen bedeuten. Setzen wir $\alpha'' = \frac{\alpha'}{(\sqrt{m})^e \alpha'}$, so folgt $\alpha''^{1-s} = 1$, d. h. α'' ist eine rationale Zahl, und danach gibt es außer 1, $\sqrt{m}$ und α nur noch ein ambiges Hauptideal, das durch Befreiung des Produkts $\sqrt{m} \cdot \alpha$ von etwaigen ganzen rationalen Faktoren $+ \pm 1$ entsteht.

Ist andererseits $n(\varepsilon) = -1$, so gibt es kein von 1 und $\sqrt{m}$ verschiedenes ambiges Hauptideal in k; denn ist (α) ein beliebiges ambiges Hauptideal in k, so gilt notwendigerweise eine Gleichung $\alpha^{1-s} = (-1)^e \varepsilon'$ mit ganzen rationalen e, f; wegen $n(\alpha^{1-s}) = +1$ ergibt sich $(n(\varepsilon))^f = +1$, d. h. f ist eine gerade Zahl. Setzen wir $\alpha' = \frac{\alpha}{\varepsilon^{\frac{f}{2}} (\sqrt{m})^{e + \frac{f}{2}}}$, so folgt $\alpha'^{1-s} = +1$, d. h. α' ist eine rationale Zahl.

Wir drücken nun von den t ambigen Primidealen in k ein geeignetes durch $\sqrt{m}$ und die $t-1$ übrigen ambigen Primideale und, wenn der Körper k reell und zugleich $n(\varepsilon) = +1$ ausfällt, weiter noch von diesen $t-1$ ambigen Primidealen ein geeignetes durch α und die $t-2$ übrigen dieser Ideale aus. Hierdurch erkennen wir die Richtigkeit des zweiten Teiles des Satzes 106.

§ 76. Die ambigen Idealklassen, welche kein ambiges Ideal enthalten.

Es gilt die folgende Tatsache:

Satz 107. Es gibt im quadratischen Körper k dann und nur dann eine ambige Klasse, welche kein ambiges Ideal enthält, wenn der Körper k reell ist, das Charakterensystem von -1 in ihm aus lauter positiven Einheiten besteht und endlich die Norm der Grundeinheit gleich $+1$ ausfällt. Sind diese Bedingungen erfüllt, so entstehen alle überhaupt vorhandenen Klassen von jener Beschaffenheit dadurch, daß man eine beliebige unter ihnen der Reihe nach mit allen aus den ambigen Idealen entspringenden Klassen multipliziert.

Beweis. Wenn der Körper k reell ist und das Charakterensystem von -1 in ihm aus lauter positiven Einheiten besteht, so gibt es nach Satz 102 in k stets eine ganze oder gebrochene Zahl α, deren Norm $= -1$ wird. Ist ferner die Norm der Grundeinheit $n(\varepsilon) = +1$, so ist diese Zahl α notwendig eine gebrochene. Setzen wir $\alpha = \frac{\mathfrak{j}}{\mathfrak{j}'}$, wo $\mathfrak{j}$ und $\mathfrak{j}'$ zueinander prime Ideale sein sollen, so wird $\frac{\mathfrak{j} \cdot s\mathfrak{j}}{\mathfrak{j}' \cdot s\mathfrak{j}'} = 1$, und hieraus folgt $\mathfrak{j}' = s\mathfrak{j}$, also $\mathfrak{j} \sim s\mathfrak{j}$, und $\mathfrak{j}$ bestimmt folglich eine ambige Klasse. Diese ambige Klasse enthält kein ambiges Ideal. Wäre nämlich ein Ideal $\mathfrak{a} = \mathfrak{j}\beta$, wo β eine ganze oder gebrochene Zahl des Körpers k bedeutet, ambig, so würde $\mathfrak{a}^{1-s} = \alpha\beta^{1-s}$ folgen, und mithin wäre $\alpha\beta^{1-s}$ gleich einer Einheit, etwa $= (-1)^e \varepsilon'$, und folglich $n(\alpha) = +1$, was der Konstruktion der Zahl α zuwiderliefe. Damit ist bewiesen, daß die durch $\mathfrak{j}$ bestimmte ambige Klasse kein ambiges Ideal enthält.

Es sei jetzt A eine beliebig gegebene ambige Klasse und $\mathfrak{j}$ ein Ideal derselben, so ist $\mathfrak{j}^{1-s}$ gleich einer ganzen oder gebrochenen Zahl α des Körpers k, und es wird die Norm $n(\alpha)$ entweder $= +1$ oder $= -1$ sein. Der erstere Fall ist der einzig mögliche, wenn der Körper k imaginär ist, oder wenn der Körper k reell ist und wenigstens einer von den Charakteren $\left(\frac{-1, m}{w}\right)$ den Wert -1 besitzt. Sowie nun $n(\alpha) = +1$ ist, folgt nach Satz 90, daß $\frac{1}{\alpha} = \beta^{1-s}$ wird, wo β eine ganze Zahl in k bedeutet; dann ist $(\mathfrak{j}\beta)^{1-s} = 1$, d. h. $\mathfrak{j}\beta$ gleich dem Produkt eines ambigen Ideals in eine rationale Zahl, und die Klasse A enthält mithin ein ambiges Ideal. Ist andererseits $n(\alpha) = -1$ und zugleich $n(\varepsilon) = -1$, so wird $n(\varepsilon\alpha) = +1$, und wir beweisen wie vorhin, daß die Klasse A ein ambiges Ideal enthält. Daraus ersehen wir, daß jede ambige Klasse ein ambiges Ideal enthält, falls der Körper k imaginär ist, und desgleichen, falls der Körper k reell ist und für ihn entweder einer der Charaktere von -1 den Wert -1 besitzt oder $n(\varepsilon) = -1$ ausfällt.

Nehmen wir endlich in dem weiteren Falle, daß keiner dieser Umstände zutrifft, an, es gebe in k mehrere ambige Idealklassen, die kein ambiges Ideal enthalten, und wählen aus zweien darunter je ein Ideal, $\mathfrak{j}$ und $\mathfrak{j}'$, aus, so zeigt die vorhin dargelegte Entwicklung, daß die Normen der beiden Zahlen $\alpha = \mathfrak{j}^{1-s}$ und $\alpha' = \mathfrak{j}'^{1-s}$ notwendig den Wert -1 besitzen, und es wird folglich $n\left(\frac{\alpha'}{\alpha}\right) = +1$. Nach Satz 90 ergibt sich hieraus eine Darstellung $\frac{\alpha}{\alpha'} = \beta^{1-s}$ mit Hilfe einer geeigneten ganzen Zahl β in k. Setzen wir $\frac{\mathfrak{j}'\beta}{\mathfrak{j}} = b\mathfrak{a}$, wo b eine rationale Zahl und $\mathfrak{a}$ ein Ideal ohne ganzen rationalen Faktor $+ \pm 1$ bedeute, so folgt wegen $\left(\frac{\mathfrak{j}'\beta}{\mathfrak{j}}\right)^{1-s} = 1$ die Gleichung $\mathfrak{a} = s\mathfrak{a}$, d. h. $\mathfrak{a}$ ist ein ambiges Ideal; und dabei ist $\mathfrak{j}' \sim \mathfrak{a}\mathfrak{j}$. Damit haben wir auch den letzten Teil unseres Satzes 107 bewiesen.

§ 77. Die Anzahl aller ambigen Klassen.

Die Sätze 106 und 107 ermöglichen die Berechnung der Anzahl aller ambigen Klassen.

Satz 108. Es gibt in jedem Falle im Körper k genau $r-1$ voneinander unabhängige ambige Klassen, wo r die Anzahl der Einzelcharaktere bedeutet, die das Geschlecht einer Klasse bestimmen. Die Anzahl der sämtlichen voneinander verschiedenen ambigen Klassen ist daher gleich 2^{r-1}.

Beweis. Es sei wieder t die Anzahl der verschiedenen in der Diskriminante d des Körpers k aufgehenden rationalen Primzahlen. Betrachten wir zunächst den Fall, daß k ein imaginärer Körper ist, so folgt aus den Sätzen 106 und 107 das Vorhandensein von genau 2^{t-1} ambigen Klassen in k; diese entspringen sämtlich aus ambigen Idealen. Jetzt sei der Körper k reell; besteht das Charakterensystem der Zahl -1 in k aus lauter positiven Einheiten, so folgt desgleichen aus den Sätzen 106 und 107 das Vorhandensein von genau 2^{t-1} ambigen Klassen in k; von diesen 2^{t-1} ambigen Klassen entspringen hier entweder sämtliche oder nur die Hälfte aus ambigen Idealen, je nachdem $n(\varepsilon) = -1$ oder $= +1$ ausfällt. Besitzt jedoch die Zahl -1 für k wenigstens einen negativen Charakter, so ist stets $n(\varepsilon) = +1$; nach den Sätzen 106 und 107 gibt es nur 2^{t-2} ambige Klassen in k, und diese entspringen sämtlich aus ambigen Idealen. Nun ist die Anzahl r der Einzelcharaktere $= t-1$, wenn der Körper k reell ist und überdies die Zahl -1 für k wenigstens einen negativen Charakter besitzt; es ist $r = t$ in jedem anderen Falle; damit ist unser Satz 108 bewiesen.

§ 78. Der arithmetische Beweis für die Existenz der Geschlechter.

Die gewonnenen Resultate setzen uns in den Stand, auf die Frage nach der Anzahl der Geschlechter die Antwort zu finden, die im Fundamentalsatze 100 ausgesprochen ist; wir können nämlich beweisen, daß diese Anzahl stets gleich 2^{r-1} ist, und daß mithin alle diejenigen Charakterensysteme, die der Bedingung des Satzes 100 Genüge leisten, wirklich unter den Geschlechtern vertreten sind. Wir bezeichnen die Anzahl der voneinander verschiedenen existierenden Geschlechter mit g und die Anzahl der Klassen des Hauptgeschlechtes mit f. Da nach § 66 alle Geschlechter die gleiche Anzahl von Klassen enthalten, so ist die Anzahl h sämtlicher Klassen des Körpers $h = gf$. Bezeichnen wir ferner die f Klassen des Hauptgeschlechtes mit $H_1, \ldots, H_f$, so können wir nach dem Satze 103 $H_1 = K_1^2, \ldots, H_f = K_f^2$ setzen, wo $K_1, \ldots, K_f$ gewisse f Klassen des Körpers bedeuten.

Es sei jetzt C eine beliebige Klasse des Körpers; da C^2 offenbar zum Hauptgeschlecht gehört, so ist $C^2 = K_a^2$, wo K_a eine ganz bestimmte der eben eingeführten Klassen $K_1, \ldots, K_f$ bedeutet. Es ist dann $\frac{C}{K_a}$, d. h. diejenige wieder ganz bestimmte Klasse A, für welche $C = AK_a$ wird, eine ambige Klasse, und es stellt also der Ausdruck AK, wenn A alle ambigen Klassen und K die Klassen $K_1, \ldots, K_f$ durchläuft, eine jede überhaupt vorhandene Idealklasse des Körpers dar, und auch jede nur auf eine Weise. Da nach Satz 108 die Anzahl der ambigen Klassen 2^{r-1} beträgt, so ergibt sich $h = 2^{r-1}f$, und es führt die Zusammenstellung dieser Gleichung mit der oben gefundenen $h = gf$ zu der Beziehung $g = 2^{r-1}$. Damit ist der Fundamentalsatz 100 vollständig bewiesen [Gauss (*1*)].

§ 79. Die transzendente Darstellung der Klassenanzahl und eine Anwendung darauf, daß der Grenzwert eines gewissen unendlichen Produktes positiv ist.

Der zweite Beweis für die Existenz der 2^{r-1} Geschlechter beruht auf transzendenter Grundlage; wir entwickeln der Reihe nach die folgenden Sätze:

Satz 109. Die Anzahl h der Idealklassen des quadratischen Körpers k mit der Diskriminante d bestimmt sich durch folgende Formel:

$$\varkappa h = L \prod_{s=1} \prod_{(p)} \frac{1}{1 - \left(\frac{d}{p}\right) p^{-s}}.$$

Hierin ist das Produkt rechter Hand über alle rationalen Primzahlen p zu erstrecken, und das Symbol $\left(\frac{d}{p}\right)$ hat die in § 61 festgesetzte Bedeutung. Für den Faktor $\varkappa$ gilt, je nachdem der Körper k imaginär oder reell, also d negativ oder positiv ist:

$$\varkappa = \frac{2\pi}{w\sqrt{|d|}} \quad \text{bez.} \quad \varkappa = \frac{2 \log \varepsilon}{\sqrt{|d|}}.$$

Dabei bedeutet w für $d = -3$ die Zahl 6, für $d = -4$ die Zahl 4, für jedes andere negative d die Zahl 2; andererseits verstehe man für einen reellen Körper k unter ε jetzt speziell diejenige seiner vier Grundeinheiten, welche > 1 ist, und unter $\log \varepsilon$ den reellen Wert des Logarithmus dieser Grundeinheit ε [Dirichlet (*8*, *9*)].

Beweis. Nach § 27 gilt, so lange s reell und > 1 ist:

$$\zeta(s) = \sum_{(\mathfrak{j})} \frac{1}{n(\mathfrak{j})^s} = \prod_{(\mathfrak{p})} \frac{1}{1 - n(\mathfrak{p})^{-s}},$$

wo das Produkt über alle Primideale $\mathfrak{p}$ des Körpers k zu erstrecken ist. Ordnen wir dieses Produkt nach den rationalen Primzahlen p, aus welchen die Primideale $\mathfrak{p}$ herstammen, so gehört, wie aus Satz 97 folgt, zu einer beliebigen rationalen Primzahl p in dem Produkte das Glied:

$$\frac{1}{(1-p^{-s})^2} \quad \text{oder} \quad \frac{1}{1-p^{-2s}} \quad \text{oder} \quad \frac{1}{1-p^{-s}},$$

je nachdem $\left(\frac{d}{p}\right) = +1, = -1, = 0$ ist. Wir schreiben diese drei Ausdrücke in der ihnen gemeinschaftlichen Form:

$$\frac{1}{1-p^{-s}} \frac{1}{1 - \left(\frac{d}{p}\right) p^{-s}}$$

und erhalten so:

$$\zeta(s) = \prod_{(p)} \frac{1}{1-p^{-s}} \prod_{(p)} \frac{1}{1 - \left(\frac{d}{p}\right) p^{-s}}.$$

wo die beiden Produkte rechter Hand über alle rationalen Primzahlen p zu erstrecken sind. Wegen

$$\underset{s=1}{L}\left\{(s-1)\prod_{(p)}\frac{1}{1-p^{-s}}\right\}=\underset{s-1}{L}\left\{(s-1)\sum_{(n)}\frac{1}{n^s}\right\}=1,$$

wo n alle positiven ganzen rationalen Zahlen durchläuft, wird dann:

$$\underset{s-1}{L}\{(s-1)\zeta(s)\}=\underset{s-1}{L}\prod_{(p)}\frac{1}{1-\left(\frac{d}{p}\right)p^{-s}}.$$

Die Richtigkeit unseres Satzes 109 folgt nun aus Satz 56, wenn wir den Wert von $\varkappa$ nach § 25 aufstellen. Zur Ermittelung von w ist zu berücksichtigen, daß der Körper $k\left(\sqrt{-3}\right)$ die 6 Einheitswurzeln ± 1, $\pm\frac{1\pm\sqrt{-3}}{2}$, der Körper $k\left(\sqrt{-1}\right)$ die 4 Einheitswurzeln ± 1, $\pm i$, dagegen ein jeder andere imaginäre quadratische Körper k nur die beiden Einheitswurzeln ± 1 enthält (vgl. § 62).

Die wichtigste Folgerung der eben bewiesenen Tatsache ist der Satz:

Satz 110. Bedeutet a eine beliebige ganze rationale positive oder negative Zahl, nur nicht eine Quadratzahl, so ist der Grenzwert

$$\underset{s-1}{L}\prod_{(p)}\frac{1}{1-\left(\frac{a}{p}\right)p^{-s}}$$

stets eine endliche und von 0 verschiedene Größe [Dirichlet (*8*, *9*)].

Beweis. Es sei $a=b^2m$, wo b^2 die größte in a aufgehende Quadratzahl sein soll; es sei ferner d die Diskriminante des durch $\sqrt{a}$ bestimmten quadratischen Körpers. Dann folgt für jede ungerade und nicht in b aufgehende rationale Primzahl p gewiß die Gleichung $\left(\frac{a}{p}\right)=\left(\frac{d}{p}\right)$. Die beiden unendlichen Produkte

$$\prod_{(p)}\frac{1}{1-\left(\frac{d}{p}\right)p^{-s}}\quad\text{und}\quad\prod_{(p)}\frac{1}{1-\left(\frac{a}{p}\right)p^{-s}}$$

können demnach nur in einer endlichen Anzahl von Faktoren voneinander abweichen. Da das erstere Produkt nach Satz 109 in der Grenze für $s=1$ endlich bleibt, so gilt daher dasselbe auch von dem zweiten Produkt.

§ 80. Das Vorhandensein unendlich vieler rationaler Primzahlen, nach denen gegebene Zahlen vorgeschriebene quadratische Restcharaktere erlangen.

Mit Hilfe des Satzes 110 beweisen wir der Reihe nach folgende Tatsachen: [Dirichlet (*9*), Kronecker (*10*)].

Satz 111. Bedeuten $a_1, a_2, \ldots, a_t$ irgend t ganze rationale, positive oder negative Zahlen von der Art, daß keine der 2^t-1 Zahlen

$a_1, a_2, \ldots, a_t, a_1a_2, \ldots, a_{t-1}a_t, \ldots, a_1a_2\ldots a_t$ eine Quadratzahl wird, und sind $c_1, c_2, \ldots, c_t$ nach Belieben vorgeschriebene Einheiten $+1$ oder -1, so gibt es stets unendlich viele rationale Primzahlen p, für die

$$\left(\frac{a_1}{p}\right)=c_1,\ \left(\frac{a_2}{p}\right)=c_2,\ \ldots,\ \left(\frac{a_t}{p}\right)=c_t$$

ist.

Beweis. Wir haben, solange $s>1$ ist:

$$\log\sum_{(n)}\frac{1}{n^s}=\sum_{(p)}\log\frac{1}{1-p^{-s}}=\sum_{(p)}\frac{1}{p^s}+S,$$

$$S=\frac{1}{2}\sum_{(p)}\frac{1}{p^{2s}}+\frac{1}{3}\sum_{(p)}\frac{1}{p^{3s}}+\cdots.$$

Da der Ausdruck S, wie in § 50 gezeigt worden ist, für $s=1$ endlich bleibt, so folgt, daß die über alle rationalen Primzahlen p erstreckte Summe

$$\sum_{(p)}\frac{1}{p^s} \tag{26}$$

bei Annäherung von s an 1 über alle Grenzen wächst. Ist ferner a eine beliebige ganze rationale Zahl, so gilt ähnlich für $s>1$ stets:

$$\log\prod_{(p)}\frac{1}{1-\left(\frac{a}{p}\right)p^{-s}}=\sum_{(p)}\left(\frac{a}{p}\right)\frac{1}{p^s}+S_a,$$

$$S_a=\frac{1}{2}\sum_{(p)}\left(\frac{a}{p}\right)^2\frac{1}{p^{2s}}+\frac{1}{3}\sum_{(p)}\left(\frac{a}{p}\right)^3\frac{1}{p^{3s}}+\cdots;$$

ist a nicht eine Quadratzahl, so bleibt nach Satz 110 $\log\prod_{(p)}\frac{1}{1-\left(\frac{a}{p}\right)p^{-s}}$ für $s=1$ endlich, und da das gleiche von dem Ausdruck S_a gilt, so folgt, daß dann auch die Summe

$$\sum_{(p)}\left(\frac{a}{p}\right)\frac{1}{p^s} \tag{27}$$

für $s=1$ sich einer endlichen Grenze nähert. Wir setzen nun in (27)

$$a=a_1^{u_1}a_2^{u_2}\ldots a_t^{u_t}$$

ein und geben jedem der t Exponenten $u_1, u_2, \ldots, u_t$ den Wert 0 oder 1, jedoch so, daß das Wertsystem $u_1=0, u_2=0, \ldots, u_t=0$ ausgeschlossen bleibt. Wird dann jede so aus (27) herzuleitende Summe noch mit dem entsprechenden Faktor $c_1^{u_1}c_2^{u_2}\ldots c_t^{u_t}$ multipliziert, und werden die hervorgehenden 2^t-1 Ausdrücke sämtlich zu (26) addiert, so entsteht:

$$\sum_{(p)}\left(1+c_1\left(\frac{a_1}{p}\right)\right)\left(1+c_2\left(\frac{a_2}{p}\right)\right)\cdots\left(1+c_t\left(\frac{a_t}{p}\right)\right)\frac{1}{p^s}. \tag{28}$$

Diese Summe wird, ebenso wie (26), bei Annäherung von s an 1 über alle

Grenzen wachsen. Sehen wir von den Gliedern ab, die den in $a_1 a_2 \dots a_t$ aufgehenden Primzahlen p entsprechen und die nur in endlicher Anzahl vorhanden sind, so ist im übrigen die Summe (28) gleich $2^t \sum_{(p')}' \frac{1}{p'^s}$, wo p' nur alle diejenigen Primzahlen p durchläuft, für welche die im Satze 111 verlangten Bedingungen sämtlich erfüllt sind. Da mithin auch diese letzte Summe für $s = 1$ über alle Grenzen wächst, so folgt, daß jene Primzahlen p' in unendlicher Anzahl vorhanden sein müssen. Damit ist Satz 111 bewiesen.

§ 81. Das Vorhandensein unendlich vieler Primideale mit vorgeschriebenen Charakteren in einem quadratischen Körper.

Satz 112. Sind

$$\chi_1(\mathfrak{j}) = \left(\frac{\pm n(\mathfrak{j}),\, m}{l_1}\right), \dots, \chi_r(\mathfrak{j}) = \left(\frac{\pm n(\mathfrak{j}),\, m}{l_r}\right)$$

die r Einzelcharaktere, welche das Geschlecht eines Ideals $\mathfrak{j}$ in k bestimmen, und bedeuten $c_1, \dots, c_r$ beliebig angenommene, der Bedingung $c_1 \dots c_r = +1$ genügende r Einheiten ± 1, so gibt es stets unendlich viele Primideale $\mathfrak{p}$ im Körper k, für welche

$$\chi_1(\mathfrak{p}) = c_1, \dots, \chi_r(\mathfrak{p}) = c_r$$

ist.

Beweis. In der Diskriminante d des Körpers seien die t rationalen Primzahlen $l_1, \dots, l_t$ enthalten. Es ist $t = r$ oder $= r+1$; in letzterem Falle sei $\left(\frac{-1,\, m}{l_t}\right) = -1$, und die Bedingung $\left(\frac{\pm n(\mathfrak{j}),\, m}{l_t}\right) = +1$ diene zur Bestimmung des Vorzeichens in $\pm n(\mathfrak{j})$. Zugleich schreiben wir in diesem Falle $c_t = c_{r+1} = +1$. Wir beweisen nun zunächst, daß es unendlich viele rationale Primzahlen p gibt, für welche

$$\left(\frac{p,\, m}{l_1}\right) = c_1, \dots, \left(\frac{p,\, m}{l_t}\right) = c_t$$

ist, und unterscheiden zu dem Zweck drei Fälle, je nachdem $m \equiv 1, \equiv 3$, oder $\equiv 2$ nach 4 ist.

Im ersten Falle gehen wir von den Forderungen

$$\left(\frac{-1}{p}\right) = +1, \left(\frac{l_1}{p}\right) = c_1, \dots, \left(\frac{l_t}{p}\right) = c_t$$

aus. Nach Satz 111 gibt es unendlich viele Primzahlen p, welche diesen Gleichungen genügen. Da die erste Gleichung auf $p \equiv 1$ nach 4 hinauskommt, so wird für diese Primzahlen p dann

$$\left(\frac{p,\, m}{l_i}\right) = \left(\frac{p}{l_i}\right) = \left(\frac{l_i}{p}\right) = c_i$$

für $i = 1, \dots, t$ gelten.

Im zweiten Falle sei unter den Primzahlen $l_1, \dots, l_t$ etwa l_z die Primzahl 2. Ist dann $c_z = +1$, so legen wir die Forderungen

$$\left(\frac{-1}{p}\right) = +1, \left(\frac{l_i}{p}\right) = c_i \qquad (i = 1, \dots, z-1, z+1, \dots, t)$$

zugrunde, und es folgt nach Satz 111, daß es unendlich viele diesen Gleichungen genügende Primzahlen p gibt. Wegen der ersten Gleichung wird $\left(\frac{p,\, m}{2}\right) = +1 = c_z$ und überdies $\left(\frac{p,\, m}{l_i}\right) = \left(\frac{p}{l_i}\right) = \left(\frac{l_i}{p}\right) = c_i$ für $i = 1, \dots, z-1, z+1, \dots, t$. Ist dagegen $c_z = -1$, so fordern wir:

$$\left(\frac{-1}{p}\right) = -1, \left(\frac{l_i}{p}\right) = (-1)^{\frac{l_i - 1}{2}} c_i, \quad (i = 1, \dots, z-1, z+1, \dots, t)$$

und die unendlich vielen, diesen Gleichungen genügenden Primzahlen p erfüllen zugleich die Bedingungen:

$$\left(\frac{p,\, m}{2}\right) = -1 = c_z \text{ und } \left(\frac{p,\, m}{l_i}\right) = \left(\frac{p}{l_i}\right) = (-1)^{\frac{l_i - 1}{2}} \left(\frac{l_i}{p}\right) = c_i$$

für $i = 1, \dots, z-1, z+1, \dots, t$.

Im dritten Falle endlich suchen wir wieder $l_z = 2$ heraus. Wir stellen die Forderungen:

$$\left(\frac{-1}{p}\right) = +1, \left(\frac{2}{p}\right) = c_z, \left(\frac{l_i}{p}\right) = c_i, \qquad (i = 1, \dots, z-1, z+1, \dots, t);$$

es existieren nach Satz 111 unendlich viele Primzahlen p, welche ihnen genügen, und für welche dann

$$\left(\frac{p,\, m}{2}\right) = (-1)^{\frac{p^2-1}{8} + \frac{p-1}{2}\frac{\frac{m}{2}-1}{2}} = (-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right) = c_z$$

und überdies $\left(\frac{p,\, m}{l_i}\right) = \left(\frac{p}{l_i}\right) = \left(\frac{l_i}{p}\right) = c_i$ für $i = 1, \dots, z-1, z+1, \dots, t$ wird.

Es bedeute nun p eine beliebige solche rationale Primzahl, daß

$$\left(\frac{p,\, m}{l_1}\right) = c_1, \dots, \left(\frac{p,\, m}{l_t}\right) = c_t$$

gilt. Nach Hilfssatz 14 ist dann

$$\prod_{(w)} \left(\frac{p,\, m}{w}\right) = \left(\frac{p,\, m}{p}\right)\left(\frac{p,\, m}{l_1}\right) \cdots \left(\frac{p,\, m}{l_t}\right) = +1,$$

und folglich

$$\left(\frac{m}{p}\right) c_1 \cdots c_t = \left(\frac{m}{p}\right) = +1;$$

also findet man p im Körper k in das Produkt zweier Primideale $\mathfrak{p}$ und $\mathfrak{p}'$ zerlegbar. Jedes dieser Primideale $\mathfrak{p}$ und $\mathfrak{p}'$ erfüllt die Bedingungen des zu beweisenden Satzes 112.

§ 82. Der transzendente Beweis für die Existenz der Geschlechter und für die übrigen in § 71 bis § 77 erlangten Resultate.

Der Satz 112 zeigt nicht nur die Existenz der 2^{r-1} Geschlechter von neuem, sondern er deckt zugleich eine andere tiefer liegende Tatsache auf:

Satz 113. Unter den Idealen eines beliebigen Geschlechtes im quadratischen Körper gibt es stets unendlich viele Primideale.

Hat man den Satz von der Existenz der 2^{r-1} Geschlechter auf dem zweiten transzendenten Wege unabhängig von den Sätzen 102, 103 und 108 festgestellt, so ist es leicht, nachträglich auch diese Sätze zu gewinnen. Man hat nämlich dazu nur noch die Kenntnis der Tatsache nötig, daß die Anzahl a der ambigen Klassen in k jedenfalls $\leqq 2^{r-1}$ ist. Diese Tatsache folgt aus Satz 106 über die Anzahl derjenigen ambigen Klassen, welche aus ambigen Idealen entspringen, in Verbindung mit den Schlüssen im zweiten und dritten Absatz des Beweises zu Satz 107; sie steht bei solcher Ableitung völlig unabhängig von Satz 102 da.

Es bezeichne dann, wie oben, f die Anzahl der Klassen des Hauptgeschlechtes, g die Anzahl der Geschlechter und ferner f' die Anzahl derjenigen unter den f Klassen des Hauptgeschlechtes, welche gleich Quadraten von Klassen sind. Es folgt wie in § 78, daß $gf = af'$ ist, und da nunmehr bereits $g = 2^{r-1}$ bewiesen, ferner $a \leqq 2^{r-1}$ sicher ist, und selbstverständlich $f' \leqq f$ besteht, so ergibt sich hieraus $f' = f$ und $a = 2^{r-1}$. Die erste Gleichung beweist den Satz 103, die zweite den Satz 108 und sodann den Satz 102 für $n = -1$. Aus Satz 103 und dem letzten Ergebnisse endlich folgt der Satz 102 vollständig. Denn die Zahl n darin ist wegen der für sie gestellten Bedingungen gleich der Norm eines Ideals $\mathfrak{h}$ des Hauptgeschlechtes, versehen mit einem Vorzeichen in der in § 65 festgesetzten Weise. Bedeutet dann $\mathfrak{k}$ ein solches Ideal, daß $\mathfrak{h} \sim \mathfrak{k}^2$ ist, so muß $\alpha = \frac{\mathfrak{h} \cdot n(\mathfrak{k})}{\mathfrak{k}^2}$ eine ganze oder gebrochene Zahl des Körpers k sein, und zwar ergibt sich $n(\alpha) = \pm n$, woraus der Satz 102 folgt, sobald man berücksichtigt, daß er für $n = -1$ gilt.

So sind durch die zuletzt entwickelte transzendente Methode die Resultate in § 71 bis § 78 gerade in umgekehrter Reihenfolge zum Nachweise gelangt, als sie auf dem zuerst eingeschlagenen rein arithmetischen Wege gefunden wurden.

§ 83. Die engere Fassung des Äquivalenz- und Klassenbegriffes.

Wenn wir den in § 24 dargelegten engeren Begriff der Äquivalenz zweier Ideale zugrunde legen, so erfahren die in den Kapiteln 17 und 18 aufgestellten Sätze nur einfache, leicht zu ermittelnde Modifikationen.

Zunächst ist klar, daß der engere Äquivalenzbegriff in einem imaginären Körper k unter allen Umständen und in einem reellen Körper k sicherlich

immer dann mit dem ursprünglichen Äquivalenzbegriffe zusammenfällt, wenn für den Körper die Norm der Grundeinheit $n(\varepsilon) = -1$ ist. Wenn aber k reell ist und $n(\varepsilon) = +1$ aufweist, so löst sich eine Idealklasse im Sinne der früheren Einteilung bei der neuen Einteilung regelmäßig in zwei Klassen auf; insbesondere entstehen aus der früheren Klasse der Hauptideale die zwei durch das Hauptideal (1) und durch das Hauptideal $(\sqrt{m})$ vertretenen Klassen der neuen Einteilung. Bezeichnet h' die Anzahl der Idealklassen bei Benutzung des engeren Äquivalenzbegriffes, so ist daher unter den gegenwärtig angenommenen Umständen $h' = 2h$ [Dedekind (*I*)].

§ 84. Der Fundamentalsatz für den neuen Klassen- und Geschlechtsbegriff.

Dem neuen Klassenbegriff entspricht ein neuer Geschlechtsbegriff: das Geschlecht eines Ideals $\mathfrak{j}$ im Körper $k(\sqrt{m})$ soll nämlich nunmehr in allen Fällen gleichmäßig durch die t Einheiten

$$\left(\frac{+n(\mathfrak{j}), m}{l_1}\right), \ldots, \left(\frac{+n(\mathfrak{j}), m}{l_t}\right)$$

charakterisiert werden, wo die Norm von $\mathfrak{j}$ im Unterschiede von der früheren Festsetzung stets das positive Vorzeichen erhält. Für einen imaginären Körper k stimmt dieser neue Geschlechtsbegriff mit dem alten völlig überein. Das Gleiche gilt für einen reellen Körper k, falls das Charakterensystem der Zahl -1 in k aus lauter positiven Einheiten besteht. Der letztere Umstand muß offenbar immer eintreten, wenn für k die Norm der Grundeinheit $= -1$ ist. Nun sei k reell und für k die Norm der Grundeinheit $= +1$, so sind zwei Fälle zu unterscheiden, je nachdem das Charakterensystem der Zahl -1 in k aus lauter positiven Einheiten besteht oder nicht.

Im ersteren Falle gehören die Ideale (1) und $\mathfrak{a} = (\sqrt{m})$ beide zum nämlichen Geschlechte, da sich

$$\left(\frac{n(\mathfrak{a}), m}{l_i}\right) = \left(\frac{+m, m}{l_i}\right) = \left(\frac{+m, m}{l_i}\right)\left(\frac{-1, m}{l_i}\right) = \left(\frac{-m, m}{l_i}\right) = +1$$

für $i = 1, \ldots, t$ ergibt. Die neuen Geschlechter umfassen also die nämlichen Ideale wie die alten, und die Zahl der Geschlechter ist wiederum $= 2^{t-1}$.

Im zweiten Falle gehören die beiden Idealklassen, welche durch das Ideal (1) und durch das Ideal $\mathfrak{a} = (\sqrt{m})$ repräsentiert werden, zu verschiedenen der neuen Geschlechter. Die Anzahl der neuen Geschlechter ist doppelt so groß, als die der alten; nun war für diesen Fall die Anzahl der Einzelcharaktere bei Zugrundelegung des ursprünglichen Geschlechtsbegriffs nur $= t - 1$ und die Anzahl der alten Geschlechter daher $= 2^{t-2}$; es ergibt sich somit die Anzahl der neuen Geschlechter, ebenso wie im ersten Falle, $= 2^{t-1}$. Da ferner in jedem Falle das Produkt

$$\left(\frac{-1, m}{l_1}\right) \cdots \left(\frac{-1, m}{l_t}\right) = +1$$

ist, so gilt der Fundamentalsatz 100 auch bei Zugrundelegung des neuen Klassenbegriffes mit dem entsprechenden Geschlechtsbegriffe, wenn nur darin t statt r gesetzt wird.

Die übrigen Tatsachen und Beweise der Kapitel 17 und 18 lassen sich ebenfalls ohne Schwierigkeiten umgestalten, und einige derselben erhalten bei Verwendung der neuen Begriffe sogar noch einen einfacheren Ausdruck.

19. Die Bestimmung der Anzahl der Idealklassen des quadratischen Körpers.

§ 85. Das Symbol $\left(\frac{a}{n}\right)$ für eine zusammengesetzte Zahl n.

Ein bemerkenswerter Ausdruck für die Anzahl h der Idealklassen der quadratischen Körpers k ergibt sich aus der Formel des Satzes 109, wenn wir die rechter Hand stehende Größe

$$L_{s=1} \prod_{(p)} \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}}$$

durch Rechnung in geschlossener Form auswerten. Zu dem Zwecke ist es nötig, das Symbol $\left(\frac{a}{n}\right)$ auch für den Fall zu definieren, daß n eine zusammengesetzte ganze rationale positive Zahl bedeutet. Ist $n = pq \dots w$, wo $p, q, \dots, w$ rationale gleiche oder verschiedene Primzahlen sind, so definieren wir:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)\cdots\left(\frac{a}{w}\right);$$

ferner soll $\left(\frac{a}{1}\right)$ stets $+1$ bedeuten. Dadurch wird für $s > 1$:

$$\prod_{(p)} \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}} = \sum_{(n)} \left(\frac{d}{n}\right)\frac{1}{n^s},$$

wo die Summe sich über alle ganzen rationalen positiven Zahlen n erstreckt. Die Berechnung des Grenzwertes dieser Summe für $s = 1$ führt zu einem geschlossenen Ausdruck für die Klassenanzahl h; wir sprechen das Resultat in dem jetzt folgenden Satze aus.

§ 86. Der geschlossene Ausdruck für die Anzahl der Idealklassen.

Satz 114. Die Anzahl h der Idealklassen des Körpers $k(\sqrt{m})$ ist:

$$h = -\frac{w}{2|d|}\sum_{(n)}\left(\frac{d}{n}\right)n \qquad \text{für } m < 0,$$

$$h = \frac{1}{2\log\varepsilon}\log\frac{\prod_{(b)}\left(e^{\frac{bi\pi}{d}} - e^{-\frac{bi\pi}{d}}\right)}{\prod_{(a)}\left(e^{\frac{ai\pi}{d}} - e^{-\frac{ai\pi}{d}}\right)} \qquad \text{für } m > 1,$$

wo die Summe $\sum_{(n)}$ über die $|d|$ ganzen rationalen Zahlen $n = 1, 2, \dots, |d|$, und wo die Produkte $\prod_{(a)}$, $\prod_{(b)}$ über alle diejenigen Zahlen a oder b unter diesen $|d|$ Zahlen zu erstrecken sind, welche der Bedingung $\left(\frac{d}{a}\right) = +1$ bezüglich $\left(\frac{d}{b}\right) = -1$ genügen [Dirichlet (8, 9) Weber (4)].

Beweis. Es seien n, n' Zahlen > 0. Wenn n und d einen gemeinsamen Teiler $\neq \pm 1$ besitzen, so ist $\left(\frac{d}{n}\right) = 0$. Ist dagegen n prim zu d, so wird, wie man leicht einsieht, $\left(\frac{d}{n}\right) = \prod_{(w)}\left(\frac{d,n}{w}\right)$, wo das Produkt über alle verschiedenen rationalen Primzahlen w zu erstrecken ist, die in n aufgehen. Nach Hilfssatz 14 stellt dann das Produkt $\prod_{(l)}\left(\frac{d,n}{l}\right)$ die nämliche Einheit dar, wenn l alle in d aufgehenden Primzahlen durchläuft. Ist nun $n' \equiv n$ nach d, so wird:

$$\prod_{(l)}\left(\frac{d,n}{l}\right) = \prod_{(l)}\left(\frac{d,n'}{l}\right),$$

und mit Rücksicht hierauf erhalten wir:

$$\left(\frac{d}{n}\right) = \left(\frac{d}{n'}\right), \tag{29}$$

wenn $n \equiv n'$ nach d ist.

Ferner ergibt sich

$$\left(\frac{d}{1}\right) + \left(\frac{d}{2}\right) + \cdots + \left(\frac{d}{|d|}\right) = 0, \tag{30}$$

indem wir eine Zahl b bestimmen, derart, daß $\left(\frac{d}{b}\right) = -1$ ist, und dann erwägen, daß die linke Seite von (30) mit Rücksicht auf (29) in die Gestalt

$$\left(\frac{d}{b}\right) + \left(\frac{d}{2b}\right) + \cdots + \left(\frac{d}{|d|b}\right) = -\left\{\left(\frac{d}{1}\right) + \left(\frac{d}{2}\right) + \cdots + \left(\frac{d}{|d|}\right)\right\}$$

gesetzt werden kann.

Durch Benutzung der Formel

$$\frac{1}{n^s} = \frac{1}{\Gamma(s)}\int_0^\infty e^{-nt}t^{s-1}\,dt$$

wird, wenn wir die Regel (29) berücksichtigen:

$$L_{s=1}\sum_{(n)}\left(\frac{d}{n}\right)\frac{1}{n^s} = L_{s=1}\int_0^\infty \frac{F(e^{-t})t^{s-1}}{1-e^{-|d|t}}\,dt,$$

wo zur Abkürzung

$$F(x) = \left(\frac{d}{1}\right)x + \left(\frac{d}{2}\right)x^2 + \cdots + \left(\frac{d}{|d|}\right)x^{|d|}$$

gesetzt ist. Wegen der Gleichung (30) enthält $F(x)$ den Faktor $1-x$; die in e^{-t} rationale Funktion $\frac{F(e^{-t})}{1-e^{-|d|t}}$ bleibt mithin für $t=0$ endlich. Aus diesem Grunde ist

$$\lim_{s=1}\int_0^\infty \frac{F(e^{-t})\,t^{s-1}}{1-e^{-|d|t}}\,dt=\int_0^\infty \frac{F(e^{-t})}{1-e^{-|d|t}}\,dt.$$

Wenn wir in dem letzteren Integral die neue Integrationsveränderliche $x=e^{-t}$ einführen, so erhält dasselbe die Gestalt:

$$\int_0^1 \frac{F(x)}{x(1-x^{|d|})}\,dx.$$

Nun haben wir die Zerlegung in Partialbrüche:

$$\frac{F(x)}{x(1-x^{|d|})}=-\frac{1}{|d|}\sum_{(n)}\frac{F\left(e^{\frac{2n i\pi}{|d|}}\right)}{x-e^{\frac{2n i\pi}{|d|}}},$$

wo die Summe über $n=1,2,\ldots,|d|$ zu erstrecken ist, und nach einem Satze von Gauss wird $F\left(e^{\frac{2n i\pi}{|d|}}\right)$, d. i.

$$\sum_{(n')}\left(\frac{d}{n'}\right)e^{\frac{2nn' i\pi}{|d|}}=\left(\frac{d}{n}\right)\sqrt{d};$$

n' durchläuft hier wiederum die Zahlen $1,2,\ldots,|d|$ und $\sqrt{d}$ ist bei positivem d positiv, bei negativem d positv imaginär zu nehmen (vgl. § 124). Da ferner

$$\int_0^1 \frac{dx}{x-e^{\frac{2n i\pi}{d}}}=\log\frac{e^{\frac{n i\pi}{|d|}}-e^{-\frac{n i\pi}{|d|}}}{i}-\frac{i\pi}{|d|}\left(n-\tfrac{1}{2}d\right)$$

$$(n=1,2,\ldots,|d|)$$

ist, wo für den Logarithmus der reelle Wert desselben zu nehmen ist, so folgt ohne Schwierigkeit das im Satze 114 angegebene Resultat.

Die Form dieses Resultates ist eine wesentlich verschiedene, je nachdem der Körper k imaginär oder reell ist. Im ersteren Falle kann h aus der angegebenen Formel ohne weiteres berechnet werden. Im zweiten Falle ist zuvor die Kenntnis der Grundeinheit ε erforderlich; der Quotient der beiden Produkte $\underset{(a)}{\Pi}$ und $\underset{(b)}{\Pi}$ ist, wie sich an einer späteren Stelle (vgl. § 121) zeigen wird, nichts anderes, als eine gewisse aus der Theorie der Kreisteilung für den quadratischen Körper k sich ergebende Einheit

Um ein Beispiel für den Fall eines imaginären Körpers zu nehmen, so erhält man, wenn $m=-p$ ist und p eine rationale positive Primzahl $\equiv 3$

nach 4 und überdies >3 bedeutet:

$$h=\frac{\Sigma b-\Sigma a}{p};$$

hierin bezeichnen Σa, Σb bezüglich die Summe der quadratischen Reste und die Summe der quadratischen Nichtreste nach p, die zwischen 0 und p liegen. Durch eine leichte Umformung kann in dem obigen Ausdrucke für h der Nenner p beseitigt werden; dadurch ergibt sich die Klassenanzahl h auch gleich dem Überschuß der Anzahl der zwsichen 0 und $\frac{p}{2}$ liegenden quadratischen Reste von p über die Anzahl der zwischen denselben Grenzen liegenden quadratischen Nichtreste oder gleich dem dritten Teil dieses Überschusses, je nachdem $p\equiv 7$ oder $\equiv 3$ nach 8 ist. Die erstere Anzahl übertrifft also stets die letztere Anzahl, eine auf rein arithmetischem Wege bisher nicht bewiesene Tatsache.

§ 87. Der Dirichletsche biquadratische Zahlkörper.

Eine nahe liegende Verallgemeinerung der bis hierher entwickelten Theorie des quadratischen Körpers betrifft folgendes Problem. Es werde statt des natürlichen aus allen rationalen Zahlen bestehenden Rationalitätsbereiches ein quadratischer Zahlkörper k als Rationalitätsbereich zugrunde gelegt; dann sollen die in bezug auf k relativ quadratischen Körper K untersucht werden, d. h. diejenigen biquadratischen Zahlkörper K, die den gegebenen Körper k als Unterkörper enthalten.

Wenn der Körper k durch die imaginäre Einheit $\sqrt{-1}$ bestimmt ist, so bezeichne ich K als einen **Dirichletschen biquadratischen Körper.** Für diesen Fall liegen umfassende Untersuchungen vor [Dirichlet (*10, 11, 12*), Eisenstein (*3, 6*), Bachmann (*1, 3*), Minnigerode (*1*), Hilbert (*5*)]. Nach der entsprechenden Einteilung der Idealklassen des Körpers K in Geschlechter und geeigneter Übertragung der Bezeichnungen gilt auch hier wiederum der Fundamentalsatz 100, und es sind die beiden in Kapitel 18 angewandten Beweismethoden dieses Satzes auch auf den Körper K übertragbar, so daß jener Fundamentalsatz für den Dirichletschen biquadratischen Körper sowohl eine reine arithmetische Begründung [Hilbert (*5*)] als auch einen Beweis mittelst der transzendenten Dirichletschen Methode [Dirichlet (*10, 11, 12*), Minnigerode (*1*)] zuläßt.

Von besonderem Interesse ist der Fall, daß der Dirichletsche biquadratische Körper K außer dem quadratischen Körper $k\left(\sqrt{-1}\right)$ noch zwei andere quadratische Körper $k\left(\sqrt{+m}\right)$ und $k\left(\sqrt{-m}\right)$ enthält. Für einen solchen **speziellen Dirichletschen Körper** K gilt die wiederum auf transzendentem und auch auf rein arithmetischem Wege zu beweisende Tatsache:

Satz 115. Die Anzahl der Idealklassen in einem speziellen Dirichletschen biquadratischen Körper $K(\sqrt{+m}, \sqrt{-m})$ ist gleich dem Produkt der Klassenanzahlen in den quadratischen Körpern $k(\sqrt{+m})$ und $k(\sqrt{-m})$ oder gleich der Hälfte dieses Produktes, je nachdem für die Grundeinheit des Körpers K die Relativnorm in bezug auf $k(\sqrt{-1})$ gleich $\pm i$ oder gleich ± 1 wird.

Dieses Resultat bezeichnet DIRICHLET als einen der schönsten Sätze der Theorie der imaginären Zahlen und als überraschend, weil durch dasselbe ein Zusammenhang zwischen denjenigen quadratischen Körpern aufgedeckt wird, die durch Quadratwurzeln aus entgegengesetzten reellen Zahlen bestimmt sind.

Bei dem rein arithmetischen Beweise dieses Satzes gelingt es zugleich in sehr einfacher Weise, und zwar durch bestimmte Bedingungen für die Geschlechtscharaktere, diejenigen Idealklassen des biquadratischen Körpers $K(\sqrt{+m}, \sqrt{-m})$ zu kennzeichnen, welche als Produkte aus einer Idealklasse von $k(\sqrt{+m})$ und einer Idealklasse von $k(\sqrt{-m})$ erhalten werden können [HILBERT (5)].

20. Die Zahlringe und Moduln des quadratischen Körpers.

§ 88. Die Zahlringe des quadratischen Körpers.

Die Theorie der Ringe und Moduln eines quadratischen Körpers erledigt sich rasch durch Spezialisierung der allgemeinen in Kapitel 9 entwickelten Sätze. Man findet leicht, daß jeder Ring r des Körpers k durch eine einzige Zahl von der Gestalt $\varrho = f\omega$ erzeugt werden kann, wo ω die in § 59 definierte Zahl bedeutet, die mit 1 zusammen eine Basis von k bildet, und wo f eine gewisse positive ganze Zahl, nämlich den Führer des Ringes r, bezeichnet. Ist insbesondere d negativ und außerdem < -4, so findet sich nach Satz 66 die Anzahl h_r der regulären Ringklassen des Ringes r durch die Formel

$$h_r = h f \prod_{(p)} \left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right)$$

ausgedrückt, wo das Produkt über alle in f enthaltenen voneinander verschiedenen rationalen Primzahlen p zu erstrecken ist [DEDEKIND (*I*, 3)].

§ 89. Ein Satz von den Modulklassen des quadratischen Körpers. Die binären quadratischen Formen.

Betreffs der Modulklassen endlich gilt im quadratischen Körper die folgende Tatsache:

Satz 116. In einer beliebigen Modulklasse des quadratischen Körpers k gibt es stets reguläre Ringideale [DEDEKIND (*I*)].

Beweis. Es sei $[\mu_1, \mu_2]$ ein beliebiger Modul des Körpers k, wobei also μ_1, μ_2 ganze Zahlen sind, und $\partial = f^2 d$ die Diskriminante der durch $[\mu_1, \mu_2]$ bestimmten Modulklasse; ferner bezeichne $\mathfrak{m} = (\mu_1, \mu_2)$ das durch die Zahlen μ_1, μ_2 bestimmte Ideal und $s\mathfrak{m} = \mathfrak{m}'$ das zu $\mathfrak{m}$ konjugierte Ideal. Nunmehr bestimme man eine durch $\mathfrak{m}'$ teilbare ganze Zahl α des Körpers k so, daß $\frac{\alpha}{\mathfrak{m}'}$ prim zu ∂ ausfällt. Setzen wir dann

$$\alpha_1 = \frac{\alpha\mu_1}{n(\mathfrak{m})}, \qquad \alpha_2 = \frac{\alpha\mu_2}{n(\mathfrak{m})},$$

so wird $[\alpha_1, \alpha_2]$ ein mit $[\mu_1, \mu_2]$ äquivalenter Modul, während zugleich das durch α_1, α_2 bestimmte Ideal $\mathfrak{a} = (\alpha_1, \alpha_2)$ prim zu ∂ ausfällt.

Ist nun ∂ eine gerade Zahl, so ziehen wir zunächst die drei ganzen Zahlen $\alpha_1, \alpha_2, \alpha_1 + \alpha_2$ in Betracht; darunter ist notwendig mindestens eine prim zu 2, denn anderenfalls müßten sich unter diesen drei Zahlen gewiß irgend zwei finden, die mit der Zahl 2 einen und den nämlichen idealen Primfaktor gemein haben, was dem widerspräche, daß das Ideal $\mathfrak{a}$ prim zu ∂ ist. Es sei etwa α_1 prim zu 2. Nunmehr bezeichne man die ungeraden in ∂ aufgehenden rationalen Primzahlen mit $p, q, \ldots, w$. Da $\mathfrak{a}$ prim zu p ist, so muß mindestens eine der drei Zahlen $\alpha_1, \alpha_1 + \alpha_2, \alpha_1 + 2\alpha_2$ prim zu p sein. Es sei $\alpha_1 + x\alpha_2$ prim zu p, ferner sei $\alpha_1 + y\alpha_2$ prim zu $q, \ldots$, wo $x, y, \ldots$ ganze rationale Zahlen bedeuten sollen. Dann folgt leicht die Existenz einer ganzen rationalen Zahl a von der Art, daß $\alpha_1 + a\alpha_2$ prim zu ∂ wird.

Setzen wir nun

$$b = \frac{|n(\alpha_1 + a\alpha_2)|}{n(\mathfrak{a})}, \qquad \beta = \frac{\alpha_2(\alpha_1' + a\alpha_2')}{n(\mathfrak{a})},$$

wo α_1', α_2' die zu α_1, α_2 konjugierten Zahlen bedeuten, so ist b eine ganze rationale positive und β eine ganze algebraische Zahl, und es wird der Modul $[\alpha_1, \alpha_2] = [\alpha_1 + a\alpha_2, \alpha_2]$ äquivalent dem Modul $[b, \beta]$. Zugleich ergibt sich wegen $(b, \beta) = \frac{\alpha_1' + a\alpha_2'}{\mathfrak{a}'}$ die Norm $n(b, \beta) = b$. Der Modul $[b, \beta]$ ist offenbar ein reguläres Ringideal in dem durch die Zahl β bestimmten Ringe $r = [\beta]$, und hiermit ist der Satz 116 vollständig bewiesen.

Wegen

$$\partial = \frac{1}{(n(b, \beta))^2}\begin{vmatrix} b, & \beta \\ b, & \beta' \end{vmatrix}^2 = \begin{vmatrix} 1, & \beta \\ 1, & \beta' \end{vmatrix}^2$$

stimmt die Diskriminante dieses Ringes r mit der Diskriminante der betrachteten Modulklasse überein. Der erhaltene Ring r ist zugleich der einzige, welcher mit $[\mu_1, \mu_2]$ äquivalente Moduln unter seinen regulären Ringidealen aufweist. Der Satz 116 zeigt, daß es im quadratischen Körper auf dasselbe hinauskommt, die Modulklassen oder die Klassen regulärer Ringideale zu betrachten.

Nach den allgemeinen Ausführungen in § 30 und § 35 entspricht einer jeden Modulklasse eines quadratischen Körpers $k(\sqrt{m})$ eine Klasse binärer

quadratischer Formen mit ganzzahligen Koeffizienten, und umgekehrt entspricht jeder solchen Formenklasse mit einer nichtquadratischen Diskriminante eine Modulklasse eines quadratischen Körpers, wobei die Modulklasse und die Formen stets gleiche Diskriminante besitzen. Danach ist durch die Untersuchungen in diesem Abschnitte zugleich die Theorie der quadratischen Formen mit vorgeschriebener Diskriminante ϑ vollständig erledigt.

§ 90. Die niedere und die höhere Theorie des quadratischen Zahlkörpers.

Die in diesem dritten Teile des Berichtes entwickelten und einheitlich dargestellten Untersuchungen machen die *niedere* Theorie des quadratischen Zahlkörpers aus; unter der *höheren* Theorie des quadratischen Zahlkörpers begreife ich die Darstellung derjenigen Eigenschaften dieses Körpers, zu deren naturgemäßer Herleitung die Benutzung gewisser Hilfskörper höheren Grades nötig ist. Ein Abschnitt dieser höheren Theorie findet in dem vierten Teil dieses Berichtes Platz. Die Theorie der zu einem imaginären quadratischen Körper gehörigen Klassenkörper sowie der dazu gehörigen relativ-Abelschen Körper erfordert jedoch zu ihrem Aufbau die Methode der komplexen Multiplikation der elliptischen Funktionen, und dies ist ein Gegenstand, welcher von der Aufnahme in diesen Bericht ausgeschlossen werden mußte.

Vierter Teil.

Der Kreiskörper.

21. Die Einheitswurzeln mit Primzahlexponent l und der durch sie bestimmte Kreiskörper.

§ 91. Der Grad des Kreiskörpers der l-ten Einheitswurzeln und die Zerlegung der Primzahl l in diesem Körper.

Es bedeute l eine ungerade rationale Primzahl, und es sei $\zeta = e^{\frac{2i\pi}{l}}$. Die Gleichung l-ten Grades

$$x^l - 1 = 0$$

besitzt die l Wurzeln

$$\zeta,\ \zeta^2,\ \ldots,\ \zeta^{l-1},\ \zeta^l = 1\,.$$

Diese Zahlen heißen **die l-ten Einheitswurzeln.** Der durch sie bestimmte Körper werde mit $k(\zeta)$ bezeichnet und der **Kreiskörper** der l-ten Einheitswurzeln genannt. Es gilt für ihn zunächst die folgende Tatsache:

Satz 117. Bedeutet l eine ungerade Primzahl, so besitzt der durch $\zeta = e^{\frac{2i\pi}{l}}$ bestimmte Kreiskörper $k(\zeta)$ der l-ten Einheitswurzeln den Grad $l-1$. Die Primzahl l gestattet in $k(\zeta)$ die Zerlegung $l = \mathfrak{l}^{l-1}$, wo $\mathfrak{l} = (1-\zeta)$ ein Primideal ersten Grades in $k(\zeta)$ ist.

Beweis. Die Zahl ζ genügt der Gleichung $l-1$-ten Grades

$$F(x) = \frac{x^l - 1}{x - 1} = x^{l-1} + x^{l-2} + \cdots + 1 = 0;$$

also ist der Körper $k(\zeta)$ höchstens vom Grade $l-1$. Da $\zeta, \zeta^2, \ldots, \zeta^{l-1}$ die $l-1$ Wurzeln dieser Gleichung $F(x) = 0$ sind, so gilt identisch in x die Gleichung:

$$x^{l-1} + x^{l-2} + \cdots + 1 = (x-\zeta)(x-\zeta^2)\ldots(x-\zeta^{l-1});$$

für $x = 1$ folgt hieraus:

$$l = (1-\zeta)(1-\zeta^2)\ldots(1-\zeta^{l-1}). \tag{31}$$

Es bedeute nun g eine beliebige durch l nicht teilbare ganze rationale Zahl > 1, und es sei dann g' eine positive ganze rationale Zahl von der Art, daß $gg' \equiv 1$ nach l ausfällt. Dann sind die Quotienten

$$\frac{1-\zeta^g}{1-\zeta} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{g-1}$$

und

$$\frac{1-\zeta}{1-\zeta^g} = \frac{1-\zeta^{gg'}}{1-\zeta^g} = \frac{1-(\zeta^g)^{g'}}{1-\zeta^g} = 1 + \zeta^g + \zeta^{2g} + \cdots + \zeta^{(g'-1)g}$$

beide ganze algebraische Zahlen, und es erweist sich somit

$$\varepsilon_g = \frac{1-\zeta^g}{1-\zeta}$$

als eine Einheit des Körpers $k(\zeta)$. Setzen wir noch $\lambda = 1-\zeta$ und $\mathfrak{l} = (\lambda)$, so erhält die Formel (31) die Gestalt

$$l = \lambda^{l-1}\varepsilon_2\varepsilon_3 \ldots \varepsilon_{l-1} = \mathfrak{l}^{l-1}. \tag{32}$$

Aus Satz 33 schließt man unmittelbar, daß eine rationale Primzahl in einem gegebenen Zahlkörper höchstens das Produkt so vieler Primideale sein kann, als der Grad des Körpers beträgt. In Anbetracht der Formel (32) muß mithin der Grad des Körpers $k(\zeta)$ mindestens $= l-1$ sein, also ist nach dem bereits oben Gefundenen dieser Grad genau $= l-1$. Andererseits kann aus dem nämlichen Grunde das Ideal $\mathfrak{l}$ im Körper $k(\zeta)$ nicht noch weiter in Faktoren zerfallen und es ist somit $\mathfrak{l}$ ein Primideal in $k(\zeta)$ [Dedekind (*I*)].

Das gewonnene Resultat besagt zugleich, daß die Funktion $F(x)$ im Bereich der rationalen Zahlen irreduzibel ist.

§ 92. Die Basis und die Diskriminante des Kreiskörpers der l-ten Einheitswurzeln.

Satz 118. In dem durch $\zeta = e^{\frac{2i\pi}{l}}$ bestimmten Kreiskörper $k(\zeta)$ der l-ten Einheitswurzeln bilden die Zahlen

$$1, \zeta, \zeta^2, \ldots, \zeta^{l-2}$$

eine Basis. Die Diskriminante des Kreiskörpers $k(\zeta)$ ist

$$d = (-1)^{\frac{l-1}{2}} l^{l-2}.$$

Beweis. Die Differente der Zahl ζ im Körper $k(\zeta)$ ist

$$\delta = (\zeta-\zeta^2)(\zeta-\zeta^3)\ldots(\zeta-\zeta^{l-1}) = \left[\frac{dF(x)}{dx}\right]_{x=\zeta}.$$

Aus

$$(x-1)F(x) = x^l - 1$$

folgt:

$$(x-1)\frac{dF(x)}{dx} + F(x) = l\,x^{l-1}, \quad \text{also} \quad \delta = -\frac{l\,\zeta^{l-1}}{1-\zeta};$$

nach der in § 3 (S. 71) gemachten Bemerkung ist dann die Diskriminante der Zahl ζ

$$d(\zeta) = (-1)^{\frac{(l-1)(l-2)}{2}} n(\delta) = (-1)^{\frac{l-1}{2}} l^{l-2}.$$

Da die Diskriminante $d(\lambda)$ der Zahl λ offenbar den nämlichen Wert $d(\zeta)$ hat, so lehrt die im Beweise zu Satz 5 bei Formel (1) S. 72 gemachte Bemerkung, daß eine jede ganze Zahl α des Körpers $k(\zeta)$ in der Gestalt

$$\alpha = \frac{a_0 + a_1\lambda + \ldots + a_{l-2}\lambda^{l-2}}{l^{l-2}} \tag{33}$$

mit ganzen rationalen Koeffizienten $a_0, a_1, \ldots, a_{l-2}$ dargestellt werden kann.

Dabei müssen dann die Zahlen $a_0, a_1, \ldots, a_{l-2}$ notwendig sämtlich durch den Nenner l^{l-2} teilbar sein. Um zunächst zu zeigen, daß sie ein erstes Mal durch l teilbar sind, nehmen wir an, es fände sich unter ihnen etwa a_g als erster nicht durch l teilbarer Koeffizient; aus $l^{l-2}\alpha \equiv 0$ nach l würde dann in Anbetracht von $l = \mathfrak{l}^{l-1}$ notwendig $a_g\lambda^g \equiv 0$ nach $\mathfrak{l}^{g+1}$, d. h. $a_g \equiv 0$ nach $\mathfrak{l}$ und also auch nach l folgen, was der Annahme widerspricht. Man kann mithin einen Faktor l in Zähler und Nenner des Ausdruckes (33) fortheben. Durch die geeignete Weiterführung des eben angewandten Verfahrens folgt schließlich, daß jede ganze Zahl α des Körpers $k(\zeta)$ bei ihren Darstellungen

$$\alpha = a_0 + a_1\lambda + \ldots + a_{l-2}\lambda^{l-2} = b_0 + b_1\zeta + \ldots + b_{l-2}\zeta^{l-2}$$

mit rationalen Koeffizienten $a_0, a_1, \ldots, a_{l-2}$, bzw. $b_0, b_1, \ldots b_{l-2}$ für diese lauter ganze rationale Zahlen bekommt.

Da somit die Potenzen $1, \zeta, \ldots, \zeta^{l-2}$ der Zahl ζ eine Basis des Körpers $k(\zeta)$ bilden, so folgt, daß die Diskriminante $d(\zeta)$ der Zahl ζ zugleich auch die Diskriminante des Körpers $k(\zeta)$ vorstellt.

§ 93. Die Zerlegung der von l verschiedenen rationalen Primzahlen im Kreiskörper der l-ten Einheitswurzeln.

Die Zerlegung der Primzahl l im Körper $k(\zeta)$ ist in Satz 117 ausgeführt. Für die Zerlegungen der übrigen rationalen Primzahlen im Körper $k(\zeta)$ gilt die folgende Regel:

Satz 119. Ist p eine von l verschiedene rationale Primzahl und f der kleinste positive Exponent, für welchen $p^f \equiv 1$ nach l ausfällt, und wird dann $l-1 = ef$ gesetzt, so findet im Kreiskörper $k(\zeta)$ die Zerlegung

$$p = \mathfrak{p}_1 \ldots \mathfrak{p}_e$$

statt, wo $\mathfrak{p}_1, \ldots, \mathfrak{p}_e$ voneinander verschiedene Primideale f-ten Grades in $k(\zeta)$ sind [Kummer (*5*, *6*)].

Beweis. Es sei $\alpha = a + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2}$ eine beliebige ganze Zahl des Kreiskörpers $k(\zeta)$; dann folgen die Kongruenzen

$$\begin{aligned}
\alpha^p &\equiv (a + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2})^p &&\equiv a + a_1\zeta^p + \ldots + a_{l-2}\zeta^{p(l-2)}, && (p)\\
\alpha^{p^2} &\equiv (a + a_1\zeta^p + \ldots + a_{l-2}\zeta^{p(l-2)})^p &&\equiv a + a_1\zeta^{p^2} + \ldots + a_{l-2}\zeta^{p^2(l-2)}, && (p)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\alpha^{p^{f-1}} &\equiv (a + a_1\zeta^{p^{f-1}} + \ldots + a_{l-2}\zeta^{p^{f-1}(l-2)})^p &&\equiv a + a_1\zeta^{p^f} + \ldots + a_{l-2}\zeta^{p^f(l-2)} \equiv \alpha, && (p).
\end{aligned}$$

Ist nun $\mathfrak{p}$ ein in p aufgehendes Primideal, so folgt aus der eben erhaltenen Kongruenz $\alpha^{p^f} \equiv \alpha$ nach p um so mehr $\alpha^{p^f} \equiv \alpha$ nach $\mathfrak{p}$, d. h. die Kongruenz

$$\xi^{p^f} - \xi \equiv 0, \qquad (\mathfrak{p}) \tag{34}$$

wird von einer jeden ganzen Zahl des Körpers $k(\zeta)$ erfüllt. Die Anzahl der nach $\mathfrak{p}$ einander inkongruenten Wurzeln dieser Kongruenz (34) ist daher gleich der Anzahl der vorhandenen nach $\mathfrak{p}$ inkongruenten ganzen Zahlen, d. h. $= n(\mathfrak{p}) = p^{f'}$, wenn mit f' der Grad des Primideals $\mathfrak{p}$ bezeichnet wird. Nun ist der Grad der Kongruenz (34) $p^{f'}$; nach Satz 26 folgt daher $p^{f'} \leqq p^f$, d. h. $f' \leqq f$.

Andererseits ist nach Satz 24, dem verallgemeinerten Fermatschen Satze, gewiß

$$\zeta^{p^{f'}-1} \equiv 1, \qquad (\mathfrak{p}). \tag{35}$$

Da nach Formel (31) für einen nicht durch l teilbaren Exponenten g die Zahl $1 - \zeta^g$ stets zu $\mathfrak{p}$ prim ist, so folgt aus der Kongruenz (35): $p^{f'} - 1 \equiv 0$ nach l, und damit $f' \geqq f$. Wir schließen nunmehr $f' = f$, d. h. jedes in p aufgehende Primideal hat den Grad f.

Da p nicht in der Diskriminante des Körpers $k(\zeta)$ aufgeht, so folgt nach Satz 31, daß p in lauter voneinander verschiedene Primideale zerfällt. Setzen wir etwa $p = \mathfrak{p}_1 \ldots \mathfrak{p}_{e'}$, so wird $n(p) = p^{l-1} = p^{e'f}$, d. h. $l - 1 = e'f$, $e' = e$. Damit ist der Beweis des Satzes 119 vollständig erbracht.

Zur wirklichen Aufstellung der Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_e$ wenden wir den Satz 33 an und berücksichtigen die im Anschluß daran auf S. 91 gemachte Bemerkung. Danach gilt identisch in x nach p eine Zerlegung

$$F(x) \equiv F_1(x) \ldots F_e(x), \qquad (p),$$

wo $F_1(x), \ldots, F_e(x)$ ganze nach p irreduzible und einander inkongruente Funktionen vom f-ten Grade in x mit ganzen rationalen Koeffizienten bedeuten. Nach Bestimmung dieser Funktionen erhalten wir die gewünschte Darstellung in den folgenden Formeln

$$\mathfrak{p}_1 = (p, F_1(\zeta)), \ldots, \mathfrak{p}_e = (p, F_e(\zeta)).$$

22. Die Einheitswurzeln für einen zusammengesetzten Wurzelexponenten m und der durch sie bestimmte Kreiskörper.

§ 94. Der Kreiskörper der m-ten Einheitswurzeln.

Es bedeute m eine beliebige positive ganze rationale Zahl, und es werde $\mathsf{Z} = \mathrm{e}^{\frac{2i\pi}{m}}$ gesetzt. Die Gleichung m-ten Grades

$$x^m - 1 = 0$$

besitzt die m Wurzeln

$$\mathsf{Z}, \mathsf{Z}^2, \ldots, \mathsf{Z}^{m-1}, \mathsf{Z}^m = 1.$$

Diese Zahlen heißen **die m-ten Einheitswurzeln;** der durch sie bestimmte Körper werde mit $k(\mathsf{Z})$ bezeichnet und der **Kreiskörper** der m-ten Einheitswurzeln genannt.

Setzt man, falls m durch mehr als eine Primzahl teilbar ist:

$$m = l_1^{h_1} l_2^{h_2} \ldots,$$

wo $l_1, l_2, \ldots$ verschiedene rationale Primzahlen seien, so kann man eine Partialbruchzerlegung vornehmen

$$\frac{1}{m} = \frac{a_1}{l_1^{h_1}} + \frac{a_2}{l_2^{h_2}} + \cdots,$$

wo $a_1, a_2, \ldots$ ganze rationale positive oder negative Zahlen bedeuten, und dann a_1 zu l_1, a_2 zu $l_2, \ldots$ prim ist. Die Benutzung dieser Zerlegung liefert

$$\mathsf{Z} = \mathsf{Z}_1^{a_1} \mathsf{Z}_2^{a_2} \ldots,$$

wenn $\mathsf{Z}_1 = \mathrm{e}^{\frac{2i\pi}{l_1^{h_1}}}$, $\mathsf{Z}_2 = \mathrm{e}^{\frac{2i\pi}{l_2^{h_2}}}, \ldots$ gesetzt wird; es entsteht also durch Zusammensetzung der Körper $k(\mathsf{Z}_1)$ der $l_1^{h_1}$-ten Einheitswurzeln, $k(\mathsf{Z}_2)$ der $l_2^{h_2}$-ten Einheitswurzeln, ... genau der Rationalitätsbereich $k(\mathsf{Z})$. Wir behandeln dementsprechend zunächst den einfacheren Fall $m = l^h$, wo in m nur eine Primzahl l aufgeht.

§ 95. Der Grad des Kreiskörpers der l^h-ten Einheitswurzeln und die Zerlegung der Primzahl l in diesem Körper.

Für den Kreiskörper der l^h-ten Einheitswurzeln gelten folgende Tatsachen:

Satz 120. Bedeutet l die Primzahl 2 oder eine ungerade Primzahl, so besitzt der durch $\mathsf{Z} = \mathrm{e}^{\frac{2i\pi}{l^h}}$ bestimmte Kreiskörper $k(\mathsf{Z})$ der l^h-ten Einheitswurzeln den Grad $l^{h-1}(l-1)$. Die Primzahl l gestattet in $k(\mathsf{Z})$ die Zerlegung $l = \mathfrak{L}^{l^{h-1}(l-1)}$, wo $\mathfrak{L}$ ein Primideal ersten Grades in $k(\mathsf{Z})$ ist.

Beweis. Z genügt der Gleichung vom $l^{h-1}(l-1)$-ten Grade:

$$F(x) = \frac{x^{l^h} - 1}{x^{l^{h-1}} - 1} = x^{l^{h-1}(l-1)} + x^{l^{h-1}(l-2)} + \cdots + 1 = 0.$$

Bedeutet g eine nicht durch l teilbare ganze rationale Zahl und dann g' eine ganze rationale Zahl von der Art, daß $gg' \equiv 1$ nach l^h ausfällt, so folgt ähnlich wie auf S. 195, daß sowohl

$$\mathsf{E}_g = \frac{1 - \mathsf{Z}^g}{1 - \mathsf{Z}},$$

als auch der reziproke Wert davon, nämlich:

$$\frac{1 - \mathsf{Z}}{1 - \mathsf{Z}^g} = \frac{1 - \mathsf{Z}^{gg'}}{1 - \mathsf{Z}^g}$$

ganze Zahlen sind; es ist daher E_g eine Einheit. Auf Grund dieses Umstandes können in der nämlichen Weise wie in § 91 die Gleichungen:

$$F(1) = l = \prod_{(g)} (1 - \mathsf{Z}^g) = \Lambda^{l^{h-1}(l-1)} \prod_{(g)} \mathsf{E}_g = \mathfrak{L}^{l^{h-1}(l-1)}$$

geschlossen werden, wo $\Lambda = 1 - Z$, $\mathfrak{L} = (\Lambda)$ gesetzt ist und in den Produkten g alle zu l primen Zahlen > 0 und $< l^h$ zu durchlaufen hat.

Durch dieselbe Überlegung wie in § 91 folgt hieraus, daß der Grad des Körpers $k(Z)$ mindestens $= l^{h-1}(l-1)$ ist, und damit zugleich, daß er genau diesen Wert hat.

§ 96. Die Basis und die Diskriminante des Kreiskörpers der l^h-ten Einheitswurzeln.

Satz 121. In dem durch $Z = e^{\frac{2i\pi}{l^h}}$ bestimmten Kreiskörper $k(Z)$ der l^h-ten Einheitswurzeln bilden die Zahlen

$$1,\ Z,\ Z^2,\ \ldots,\ Z^{l^{h-1}(l-1)-1}$$

eine Basis; die Diskriminante dieses Körpers ist

$$d = \pm l^{l^{h-1}(hl-h-1)},$$

wo für $l^h = 4$ oder $l = 3$ nach 4 das Vorzeichen $-$ und sonst das Vorzeichen $+$ gilt.

Satz 122. Ist p eine von l verschiedene rationale Primzahl und f der kleinste positive Exponent, für welchen $p^f \equiv 1$ nach l^h ausfällt, und wird $l^{h-1}(l-1) = ef$ gesetzt, so findet in $k(Z)$ die Zerlegung

$$p = \mathfrak{P}_1 \ldots \mathfrak{P}_e$$

statt, wo $\mathfrak{P}_1, \ldots, \mathfrak{P}_e$ voneinander verschiedene Primideale f-ten Grades in $k(Z)$ sind.

Die beiden Sätze 121 und 122 werden genau in der entsprechenden Weise bewiesen, wie die für den Körper $k(\zeta)$ aufgestellten Sätze 118 und 119.

§ 97. Der Kreiskörper der m-ten Einheitswurzeln. Der Grad, die Diskriminante und die Primideale dieses Körpers.

Jetzt sei m ein Produkt aus Potenzen verschiedener Primzahlen, etwa $m = l_1^{h_1} l_2^{h_2} \ldots$. Der nach § 94 definierte Kreiskörper $k(Z)$ der m-ten Einheitswurzeln entsteht dann, wie dort ausgeführt worden ist, durch Zusammensetzung der Kreiskörper $k(Z_1), k(Z_2), \ldots$ der $l_1^{h_1}$-ten, der $l_2^{h_2}$-ten, $\ldots$ Einheitswurzeln. Da die Diskriminanten der letzteren Kreiskörper zueinander prim sind, so folgt aus Satz 87 (§ 52) unmittelbar die Tatsache:

Satz 123. Der Grad des Körpers $k(Z)$ der $m = l_1^{h_1} l_2^{h_2} \ldots$-ten Einheitswurzeln ist:

$$\Phi(m) = l_1^{h_1-1}(l_1-1)\, l_2^{h_2-1}(l_2-1) \ldots.$$

Wenden wir die zweite Aussage in Satz 88 auf die Kreiskörper $k(Z_1)$, $k(Z_2), \ldots$ an und beachten den Satz 121, so folgt das weitere Resultat:

Satz 124. Der Kreiskörper $k(Z)$ der m-ten Einheitswurzeln besitzt die Basis:

$$1,\ Z,\ Z^2,\ \ldots,\ Z^{\Phi(m)-1}.$$

Die Diskriminante des Körpers $k(Z)$ der m-ten Einheitswurzeln ergibt sich durch die erste Aussage in Satz 88.

Endlich kann auf Grund des Satzes 88 unter Zuhilfenahme der Eigenschaften der Zerlegungs- und der Trägheitskörper die Zerlegung einer rationalen Primzahl p im Körper $k(Z)$ ausgeführt werden. Man erhält so den Satz:

Satz 125. Ist p eine in $m = l_1^{h_1} l_2^{h_2} \ldots$ nicht aufgehende rationale Primzahl und f der kleinste positive Exponent, für welchen $p^f \equiv 1$ nach m ausfällt, und wird dann $\Phi(m) = ef$ gesetzt, so findet im Kreiskörper $k(Z)$ der m-ten Einheitswurzeln die Zerlegung

$$p = \mathfrak{P}_1 \ldots \mathfrak{P}_e$$

statt, wo $\mathfrak{P}_1, \ldots, \mathfrak{P}_e$ voneinander verschiedene Primideale f-ten Grades in $k(Z)$ sind.

Ist ferner p^h eine Potenz von p, und wird $m^* = p^h m$ gesetzt, so findet im Körper $k(Z^*)$ der m^*-ten Einheitswurzeln die Zerlegung

$$p = \{\mathfrak{P}_1^* \ldots \mathfrak{P}_e^*\}^{p^{h-1}(p-1)}$$

statt, wo $\mathfrak{P}_1^*, \ldots, \mathfrak{P}_e^*$ voneinander verschiedene Primideale f-ten Grades in $k(Z^*)$ sind [Kummer (*15*), Dedekind (*5*), Weber (*4*)].

Zum Beweise des Satzes 125 nehmen wir der Kürze wegen $m = l_1^{h_1} l_2^{h_2}$ an und bezeichnen dann die Kreiskörper der $l_1^{h_1}$-ten, $l_2^{h_2}$-ten Einheitswurzeln mit $k^{(1)}$ bez. $k^{(2)}$. Ferner sei p eine von l_1, l_2 verschiedene rationale Primzahl und $\mathfrak{p}^{(1)}$, $\mathfrak{p}^{(2)}$ seien je ein idealer Primfaktor von p bez. in den Körpern $k^{(1)}, k^{(2)}$; wir bezeichnen in $k^{(1)}, k^{(2)}$ die Zerlegungskörper der Primideale $\mathfrak{p}^{(1)}$, $\mathfrak{p}^{(2)}$ bez. mit $k_z^{(1)}, k_z^{(2)}$. Es seien f_1, f_2 die kleinsten Exponenten, für welche $p^{f_1} \equiv 1$ nach $l_1^{h_1}$ bzw. $p^{f_2} \equiv 1$ nach $l_2^{h_2}$ ausfällt, und es möge

$$l_1^{h_1-1}(l_1-1) = e_1 f_1, \qquad l_2^{h_2-1}(l_2-1) = e_2 f_2$$

gesetzt werden: dann sind e_1, e_2 bez. die Grade der Körper $k_z^{(1)}, k_z^{(2)}$ und f_1, f_2 der Relativgrad von $k^{(1)}$ in bezug auf $k_z^{(1)}$ bez. der Relativgrad von $k^{(2)}$ in bezug auf $k_z^{(2)}$. Nach Satz 88 zerfällt die rationale Primzahl p in dem aus $k_z^{(1)}, k_z^{(2)}$ zusammengesetzten Körper $k_z^{(1,2)}$ in $e_1 e_2$ Ideale; diese sind daher sämtlich Primideale ersten Grades in $k_z^{(1,2)}$. Wir betrachten unter diesen insbesondere das Primideal $\mathfrak{p} = (\mathfrak{p}^{(1)}, \mathfrak{p}^{(2)})$ und bezeichnen mit $\mathfrak{P}$ einen Primfaktor von $\mathfrak{p}$ in dem aus $k^{(1)}, k^{(2)}$ zusammengesetzten Körper k; es sei k_z der Zerlegungskörper des Primideals $\mathfrak{P}$ in k. Es folgt zunächst aus der Definition der Zerlegungskörper, daß $k_z^{(1,2)}$ entweder mit k_z übereinstimmen oder in k_z als Unterkörper enthalten sein muß. Die Relativgruppe des aus $k^{(1)}$, $k_z^{(2)}$ zusammengesetzten Körpers in bezug auf $k_z^{(1,2)}$ ist zyklisch vom Grade f_1; die Relativgruppe des aus $k_z^{(1)}, k^{(2)}$ zusammengesetzten Körpers in bezug auf $k_z^{(1,2)}$ ist zyklisch vom Grade f_2. Wir entnehmen hieraus, daß, wenn f das kleinste gemeinsame Vielfache der Zahlen f_1, f_2 bedeutet, die Relativgruppe von k in bezug auf $k_z^{(1,2)}$ keine zyklische Untergruppe von höherem

als f-ten Grade enthalten kann. Da k als Trägheitskörper des Primideals $\mathfrak{P}$ eine zyklische Relativgruppe in bezug auf k_z besitzen muß und der Körper k_z den Körper $k_z^{(1,2)}$ enthält, so folgt, daß jene zyklische Relativgruppe von k in bezug auf k_z höchstens den Grad f hat.

Andrerseits stellen wir folgende Betrachtungen an. Die beiden Körper $k^{(1)}$ und k_z haben den Körper $k_z^{(1)}$, aber keinen Körper höheren Grades als gemeinsamen Unterkörper, da sonst $\mathfrak{p}^{(1)}$ in $k^{(1)}$ noch weiter zerlegbar sein müßte. Desgleichen haben die beiden Körper $k^{(2)}$ und k_z den Körper $k_z^{(2)}$ zum größten gemeinsamen Unterkörper. Wir legen nun $k_z^{(1,2)}$ als Rationalitätsbereich zugrunde; es ist dann k_z ein solcher Relativkörper in bezug auf $k_z^{(1,2)}$, der weder mit $k^{(1)}$, noch mit $k^{(2)}$ einen Relativkörper in bezug auf $k_z^{(1,2)}$ gemein hat. Hieraus schließen wir ohne Mühe, daß k_z höchstens vom Relativgrade $\frac{f_1 f_2}{f}$ in bezug auf $k_z^{(1,2)}$ sein kann. Der Körper k_z ist daher höchstens vom Grade $\frac{e_1 f_1 e_2 f_2}{f}$, d. h. die Relativgruppe von k in bezug auf k_z hat mindestens den Grad f. Dies zusammen mit der oben bewiesenen Tatsache zeigt, daß der Grad der Relativgruppe von k in bezug auf k_z gleich f sein muß, womit sich für den gegenwärtig betrachteten besonderen Fall die Aussage des Satzes 125 deckt.

Nach Satz 123 genügt $Z = e^{\frac{2i\pi}{m}}$ einer irreduziblen Gleichung $F(x) = 0$ vom $\Phi(m)$-ten Grade mit ganzen rationalen Koeffizienten, und nach dem Beweise zu Satz 87 bleibt diese Gleichung $F(x) = 0$ auch noch irreduzibel, wenn man als Rationalitätsbereich irgendeinen Körper zugrunde legt, dessen Diskriminante zu m prim ist [Kronecker (3, 21)].

Die Bildung der linken Seite $F(x)$ dieser Gleichung geschieht in folgender Weise. Wird für den Augenblick zur Abkürzung allgemein

$$x^m - 1 = [m]$$

und

$$\begin{aligned} \Pi_0 &= [m], \\ \Pi_1 &= \left[\frac{m}{l_1}\right]\left[\frac{m}{l_2}\right]\cdots, \\ \Pi_2 &= \left[\frac{m}{l_1 l_2}\right]\left[\frac{m}{l_1 l_3}\right]\cdots\left[\frac{m}{l_2 l_3}\right]\cdots, \\ \Pi_3 &= \left[\frac{m}{l_1 l_2 l_3}\right]\left[\frac{m}{l_1 l_2 l_4}\right]\cdots\left[\frac{m}{l_2 l_3 l_4}\right]\cdots, \\ &\cdots\cdots\cdots\cdots \end{aligned}$$

gesetzt, so ist:

$$F(x) = \frac{\Pi_0 \Pi_2 \Pi_4 \cdots}{\Pi_1 \Pi_3 \Pi_5 \cdots}.$$

[Dedekind (1), Bachmann (2)].

Ist a eine ganze rationale Zahl und p eine in $F(a)$ aufgehende zu m prime Primzahl, so hat mit Rücksicht auf Satz 125 p stets die Kongruenzeigenschaft $p \equiv 1$ nach m. Es gibt danach offenbar unendlich viele Primzahlen p mit dieser Kongruenzeigenschaft.

§ 98. Die Einheiten des Kreiskörpers $k(e^{\frac{2i\pi}{m}})$. Die Definition der Kreiseinheiten.

Es gelten folgende Tatsachen:

Satz 126. Wenn m eine Potenz einer Primzahl l ist und g eine nicht durch l teilbare Zahl bedeutet, so stellt in dem durch $Z = e^{\frac{2i\pi}{m}}$ bestimmten Kreiskörper der Ausdruck

$$\frac{1 - Z^g}{1 - Z}$$

stets eine Einheit dar.

Wenn die Zahl m verschiedene Primfaktoren enthält und g eine zu m prime Zahl bedeutet, so stellt in dem durch $Z = e^{\frac{2i\pi}{m}}$ bestimmten Kreiskörper der Ausdruck

$$1 - Z^g$$

stets eine Einheit dar.

Beweis. Der erste Teil dieses Satzes 126 ist bereits in den Beweisen der Sätze 117 und 120 festgestellt worden. Um den zweiten Teil zu beweisen, setzen wir $m = l_1^{h_1} l_2^{h_2} l_3^{h_3} \ldots$ und

$$\frac{g}{m} = \frac{a}{l_1^{h_1}} + \frac{b}{l_2^{h_2} l_3^{h_3} \ldots},$$

wo a eine zu l_1 und b eine zu $l_2, l_3, \ldots$ prime ganze rationale Zahl bezeichnet; dabei wird

$$1 - Z^g = 1 - e^{\frac{2i\pi g}{m}} = 1 - e^{\frac{2i\pi a}{l_1^{h_1}}} e^{\frac{2i\pi b}{l_2^{h_2} l_3^{h_3} \cdots}}. \tag{36}$$

Nun ist:

$$\prod_{(x)} \left(1 - e^{\frac{2i\pi x}{l_1^{h_1}}} e^{\frac{2i\pi b}{l_2^{h_2} l_3^{h_3} \cdots}}\right) = 1 - e^{\frac{2i\pi b l_1^{h_1}}{l_2^{h_2} l_3^{h_3} \cdots}},$$

wo das Produkt über $x = 0, 1, 2, \ldots, l_1^{h_1} - 1$ zu erstrecken ist, oder:

$$\prod_{(x')} \left(1 - e^{\frac{2i\pi x'}{l_1^{h_1}}} e^{\frac{2i\pi b}{l_2^{h_2} l_3^{h_3} \cdots}}\right) = \frac{1 - e^{\frac{2i\pi b l_1^{h_1}}{l_2^{h_2} l_3^{h_3} \cdots}}}{1 - e^{\frac{2i\pi b}{l_2^{h_2} l_3^{h_3} \cdots}}}, \tag{37}$$

wo das Produkt über $x' = 1, 2, \ldots, l_1^{h_1} - 1$ zu erstrecken ist.

Wir unterscheiden jetzt zwei Fälle, je nachdem die Anzahl der Primzahlen $l_1, l_2, \ldots$, die in m enthalten sind, zwei oder mehr als zwei beträgt. Im ersteren Falle ist die rechte Seite der Formel (37) nach dem bereits feststehenden ersten Teile des Satzes 126 eine Einheit. Im zweiten Falle können wir annehmen, der zu beweisende Satz 126 sei bereits für diejenigen Kreiskörper $k(e^{\frac{2i\pi}{m^*}})$ als richtig erkannt, bei welchen die Zahl m^* durch weniger

Primzahlen als m teilbar ist; es trifft dann dieser Satz für den Kreiskörper zu, der durch die $\frac{m}{l^{\lambda_l}}$-ten Einheitswurzeln bestimmt ist. Danach sind dann Zähler und Nenner des auf der rechten Seite von (37) stehenden Bruches für sich Einheiten. Der Ausdruck (36) ist ein Faktor des Produktes auf der linken Seite von (37) und daher gleichfalls in jedem Falle eine Einheit. Damit ist der Satz 126 vollständig bewiesen.

Von einer jeden beliebigen Einheit eines Kreiskörpers $k(e^{\frac{2i\pi}{m}})$ gilt die Tatsache, daß sie gleich dem Produkte aus einer Einheitswurzel und einer reellen Einheit ist. Die Einheitswurzel liegt dabei nicht notwendig immer in dem Körper $k(e^{\frac{2i\pi}{m}})$ selbst, sondern kann, wenn m verschiedene Primzahlen enthält, bei geradem m eine $2m$-te, bei ungeradem m eine $4m$-te Einheitswurzel sein [Kronecker (7)]. Wir sprechen insbesondere die folgende, schon von Kummer erkannte Tatsache aus:

Satz 127. Bezeichnet l eine ungerade Primzahl, und betrachten wir in dem durch $\zeta = e^{\frac{2i\pi}{l}}$ bestimmten Kreiskörper $k(\zeta)$ den durch $\zeta + \zeta^{-1}$ bestimmten reellen Unterkörper $k(\zeta + \zeta^{-1})$ vom Grade $\frac{l-1}{2}$, so ist ein beliebiges System von Grundeinheiten dieses reellen Körpers $k(\zeta + \zeta^{-1})$ stets auch für den Körper $k(\zeta)$ ein System von Grundeinheiten.

Beweis. Ist $\varepsilon(\zeta)$ eine beliebige Einheit in $k(\zeta)$, so ist $\frac{\varepsilon(\zeta)}{\varepsilon(\zeta^{-1})}$ eine solche Einheit in $k(\zeta)$, die selbst und deren Konjugierte sämtlich den absoluten Betrag 1 besitzen, und sie stellt daher nach Satz 48 eine Einheitswurzel dar; wir setzen $\frac{\varepsilon(\zeta)}{\varepsilon(\zeta^{-1})} = \pm\zeta^{2g}$, wo g eine ganze Zahl sei. Die Einheit $\eta(\zeta) = \varepsilon(\zeta)\zeta^{-g}$ besitzt dann die Eigenschaft:

$$\frac{\eta(\zeta)}{\eta(\zeta^{-1})} = \pm 1 . \tag{38}$$

In dieser Formel (38) kann rechter Hand nur das positive Vorzeichen gelten. Anderenfalls nämlich wäre $\eta(\zeta)$ eine rein imaginäre Einheit; dann setzen wir $\eta^2 = \vartheta$, so daß ϑ eine Einheit des reellen Unterkörpers $k(\zeta + \zeta^{-1})$ wird. Die Relativdifferente der Zahl $\eta = \sqrt{\vartheta}$ in bezug auf den reellen Unterkörper $k(\zeta + \zeta^{-1})$ ist 2η und mithin prim zu l. Demnach müßte auch die Relativdifferente des Körpers $k(\zeta)$ in bezug auf den Körper $k(\zeta + \zeta^{-1})$ prim zu l sein. Bedeutet nun $\mathfrak{l}^*$ ein beliebiges in l aufgehendes Primideal des reellen Körpers $k(\zeta + \zeta^{-1})$, so würde daher nach Satz 93 dieses Ideal nicht gleich dem Quadrate eines Primideals des Körpers $k(\zeta)$ sein. Da aber $\mathfrak{l}^*$ in l höchstens zur $\frac{l-1}{2}$-ten Potenz vorkommt, so fände sich diese letzte Folgerung in Widerspruch mit dem Satze 117 über die Zerlegung der Zahl l im Körper $k(\zeta)$; also gilt in der Tat auf der rechten Seite der Formel (38) das obere Vorzeichen. Aus $\eta(\zeta) = \eta(\zeta^{-1})$ folgt, daß die Zahl $\eta(\zeta)$ reell ist. Damit ist der Beweis des Satzes 127 erbracht.

Die in Satz 126 angegebenen Einheiten sind imaginär. Um reelle Einheiten zu erhalten, bilden wir, je nachdem m eine Potenz einer Primzahl ist oder verschiedene Primzahlen enthält, die Ausdrücke:

$$\mathsf{E}_g = \sqrt{\frac{(1-\mathsf{Z}^g)(1-\mathsf{Z}^{-g})}{(1-\mathsf{Z})(1-\mathsf{Z}^{-1})}}$$

bez.

$$\mathsf{E}_g = \sqrt{(1-\mathsf{Z}^g)(1-\mathsf{Z}^{-g})},$$

wo g eine zu m prime Zahl bedeute und der positive Wert der Quadratwurzel genommen werde. Diese Einheiten sollen kurz **Kreiseinheiten** genannt werden. Mit Rücksicht auf $1 - \mathsf{Z}^{-g} = -\mathsf{Z}^{-g}(1 - \mathsf{Z}^g)$ erkennt man, daß in dem ersteren Falle diese Einheiten im Körper $k(\mathsf{Z})$ selbst liegen, während sie im zweiten Falle als Produkte aus Einheiten des Körpers $k(\mathsf{Z})$ in $2m$-te bez. $4m$-te Einheitswurzeln erscheinen, je nachdem m gerade oder ungerade ist.

23. Der Kreiskörper in seiner Eigenschaft als Abelscher Körper.

§ 99. Die Gruppe des Kreiskörpers der m-ten Einheitswurzeln.

Der Kreiskörper der m-ten Einheitswurzeln ist bei jedem Werte von m, wie man leicht erkennt, ein Abelscher Körper, und zwar gelten die folgenden eingehenderen Sätze:

Satz 128. Bedeutet l eine ungerade Primzahl, so ist der durch $\mathsf{Z} = e^{\frac{2i\pi}{l^h}}$ bestimmte Kreiskörper ein zyklischer Körper.

Der durch $\mathsf{Z} = e^{\frac{i\pi}{2^h}}$ $(h \geqq 2)$ bestimmte Kreiskörper entsteht durch Zusammensetzung des imaginären quadratischen Körpers $k(i)$ und des reellen Körpers $k\left(e^{\frac{i\pi}{2^h}} + e^{-\frac{i\pi}{2^h}}\right)$. Der reelle Körper $k\left(e^{\frac{i\pi}{2^h}} + e^{-\frac{i\pi}{2^h}}\right)$ ist zyklisch vom Grade 2^{h-1}.

Beweis. Der erste Teil des Satzes 128 folgt, wenn wir die Substitution

$$s = (\mathsf{Z} : \mathsf{Z}^r)$$

(Ersetzung von Z durch Z^r) einführen, wo unter r eine Primitivzahl nach l^h verstanden werden soll. Offenbar sind dann alle Substitutionen der Gruppe des Körpers $k(\mathsf{Z})$ Potenzen von s.

Um den zweiten Teil des Satzes 128 zu beweisen, betrachten wir die Substitutionen

$$s = (\mathsf{Z} : \mathsf{Z}^5), \quad s' = (\mathsf{Z} : \mathsf{Z}^{-1}) = (i : -i).$$

Dann folgt leicht, daß die Potenzen von s und deren Produkte mit s' die sämtlichen Substitutionen des Körpers $k(\mathsf{Z})$ ausmachen.

Auf Grund des Satzes 128 ist auch für jede zusammengesetzte Zahl m die Gruppe des Kreiskörpers der m-ten Einheitswurzeln unmittelbar anzugeben.

Die Aufstellung des Zerlegungs-, des Trägheits- und des Verzweigungskörpers für ein gegebenes Primideal in $k\left(e^{\frac{2i\pi}{m}}\right)$ kann auf Grund der Bedeutung dieser Unterkörper mit Hilfe der in § 95, § 96 und § 97 bewiesenen Sätze über die Zerlegung einer rationalen Primzahl im Kreiskörper leicht bewirkt werden. So ergibt sich insbesondere das folgende Resultat:

Satz 129. Bedeutet l eine ungerade Primzahl, und betrachtet man den Kreiskörper $k(Z)$ der l^h-ten Einheitswurzeln, so ist für das in l enthaltene Primideal $\mathfrak{L} = (1 - Z)$ der Körper $k(Z)$ ein überstrichener Verzweigungskörper und der in ihm enthaltene Körper der l-ten Einheitswurzeln der Verzweigungskörper, während der Körper der rationalen Zahlen gleichzeitig die Rolle des Zerlegungs- und des Trägheitskörpers für $\mathfrak{L}$ übernimmt. Ist ferner $\mathfrak{P}$ ein von $\mathfrak{L}$ verschiedenes Primideal in $k(Z)$ vom Grade f, so ist für $\mathfrak{P}$ der Körper $k(Z)$ selbst der Trägheitskörper, während als Zerlegungskörper von $\mathfrak{P}$ derjenige Unterkörper $e = \frac{l^{h-1}(l-1)}{f}$-ten Grades von $k(Z)$ erscheint, der zu der Substitutionengruppe

$$s^e,\ s^{2e},\ s^{3e},\ \ldots,\ s^{fe}$$

gehört. Dabei bedeutet $s = (Z : Z^r)$ eine solche Substitution der Gruppe des Körpers $k(Z)$, welche mit ihren Potenzen diese Gruppe vollständig erzeugt.

§ 100. Der allgemeine Begriff des Kreiskörpers. Der Fundamentalsatz über die Abelschen Körper.

Wir erweitern nunmehr den Begriff des Kreiskörpers, wie er bisher in Betracht kam; wir bezeichnen als einen **Kreiskörper** schlechthin nicht nur einen jeden durch die Einheitswurzeln von irgendeinem Exponenten m bestimmten Körper $k\left(e^{\frac{2i\pi}{m}}\right)$, sondern auch einen jeden, irgendwie in einem solchen besonderen Kreiskörper $k\left(e^{\frac{2i\pi}{m}}\right)$ enthaltenen Unterkörper. Da jeder Körper $k\left(e^{\frac{2i\pi}{m}}\right)$ ein Abelscher Körper ist und ferner, wenn m und m' irgendwelche Exponenten bedeuten, der Körper der m-ten Einheitswurzeln und der Körper der m'-ten Einheitswurzeln beide zugleich in dem Körper der $m \cdot m'$-ten Einheitswurzeln als Unterkörper enthalten sind, so gelten für diesen erweiterten Begriff des Kreiskörpers allgemein die folgenden Tatsachen:

Satz 130. Jeder Kreiskörper ist ein Abelscher Körper. Jeder Unterkörper eines Kreiskörpers ist ein Kreiskörper. Jeder aus Kreiskörpern zusammengesetzte Körper ist wiederum ein Kreiskörper.

Es ist nun eine fundamentale Tatsache, daß die erste Aussage in diesem Satze 130 sich, wie folgt, umkehren läßt:

Satz 131. *Jeder Abelsche Zahlkörper im Bereiche der rationalen Zahlen ist ein Kreiskörper* [Kronecker (*2, 13*), Weber (*1*), Hilbert (*6*)].

Um den Beweis dieses fundamentalen Satzes vorzubereiten, erinnern wir daran, daß nach § 48 jeder Abelsche Körper sich aus solchen zyklischen Körpern zusammensetzen läßt, bei denen die Grade Primzahlen oder Primzahlpotenzen sind. Wir konstruieren nun folgende besonderen zyklischen Körper. Es bedeute u eine ungerade Primzahl und u^h eine Potenz derselben mit positivem Exponenten; dann ist der durch $e^{\frac{2i\pi}{u^h+1}}$ bestimmte Körper $k\left(e^{\frac{2i\pi}{u^h+1}}\right)$ ein zyklischer Körper vom $u^h(u-1)$-ten Grade. Der zyklische Unterkörper vom u^h-ten Grade dieses Körpers werde mit U_h bezeichnet. Ferner bestimmt die Zahl $e^{\frac{i\pi}{2^{h+1}}} + e^{\frac{-i\pi}{2^{h+1}}}$ einen reellen zyklischen Körper vom 2^h-ten Grade. Dieser Körper werde mit II_h bezeichnet. Endlich sei l^h eine Potenz einer beliebigen Primzahl $l (= 2 \text{ oder } \neq 2)$ und außerdem p eine Primzahl mit der Kongruenzeigenschaft $p \equiv 1$ nach l^h; dann besitzt der Kreiskörper $k\left(e^{\frac{2i\pi}{p}}\right)$ vom Grade $p - 1$ offenbar einen zyklischen Unterkörper vom Grade l^h. Dieser zyklische Körper l^h-ten Grades werde mit P_h bezeichnet. Die Körper U_h, II_h, P_h sind Kreiskörper bez. von den Graden $u^h, 2^h, l^h$; die Diskriminanten dieser Körper U_h, II_h, P_h sind infolge der Sätze 39 und 121 Potenzen bez. der Primzahlen $u, 2, p$. Daß es bei jeder Annahme von l^h Primzahlen p mit der Kongruenzeigenschaft $p \equiv 1$ nach l^h gibt, steht nach der letzten Bemerkung in § 97 fest, kommt jedoch hier nicht in Frage.

Wir werden in den folgenden Paragraphen zeigen, daß jeder Abelsche Körper als Unterkörper in einem solchen Körper enthalten ist, der durch Zusammensetzung aus $k(i)$ und geeigneten Körpern U_h, II_h, P_h entsteht. Zu diesem Nachweise ist eine Reihe von Hilfsbetrachtungen vorauszuschicken.

§ 101. Ein allgemeiner Hilfssatz über zyklische Körper.

Hilfssatz 15. Wenn ein zyklischer Körper C_h von einem Grade l^h, wo l eine beliebige Primzahl $(= 2 \text{ oder } \neq 2)$ ist, nicht den betreffenden Körper U_1 bez. II_1 als Unterkörper enthält, so entsteht durch Zusammensetzung von C_h mit dem durch $Z = e^{\frac{2i\pi}{l^h}}$ bestimmten Körper $k(Z)$ ein Körper $k(Z, C_h)$ vom Grade $l^{2h-1}(l-1)$, und es gibt dann stets in $k(Z)$ eine ganze Zahl $\varkappa$ mit folgenden Eigenschaften: der Körper $k(Z, C_h)$ ist auch durch die Zahlen Z und $\sqrt[l^h]{\varkappa}$ bestimmt; bezeichnet r eine beliebige nicht durch l teilbare ganze rationale Zahl, und wird aus der Gruppe des Körpers $k(Z)$ die Substitution

$$s = (Z : Z^r)$$

ins Auge gefaßt, so ist $\varkappa^{s-r}$ die l^h-te Potenz einer Zahl in $k(Z)$.

Beweis. Die erste Behauptung über den Grad von $k(Z, C_h)$ folgt unmittelbar daraus, daß $k(Z)$ und C_h außer dem Körper der rationalen Zahlen

keinen gemeinsamen Unterkörper haben. Es sei nun α eine den Körper C_h bestimmende ganze Zahl von der Art, daß auch keine Potenz von α in einem Unterkörper von C_h liegt; es sei ferner t eine solche Substitution der Gruppe von C_h, welche mit ihren Potenzen diese Gruppe erzeugt. Wir setzen, wenn a und b beliebige Exponenten sind:

$$K(\alpha^a, Z^b) = \alpha^a + Z^b \cdot (t\alpha)^a + Z^{2b} \cdot (t^2\alpha)^a + \cdots + Z^{(l^h-1)b} \cdot (t^{l^h-1}\alpha)^a .$$

Die Ausdrücke $K(\alpha, Z), K(\alpha^2, Z), \ldots, K(\alpha^{l^h-1}, Z)$ können nicht sämtlich verschwinden, da sonst wegen $K(\alpha^0, Z) = 0$ notwendig auch die Determinante

$$\begin{vmatrix} 1, & 1, & \ldots, & 1 \\ \alpha, & t\alpha, & \ldots, & t^{l^h-1}\alpha \\ \cdots & \cdots & \cdots & \cdots \\ \alpha^{l^h-1}, & (t\alpha)^{l^h-1}, & \ldots, & (t^{l^h-1}\alpha)^{l^h-1} \end{vmatrix}$$

verschwinden müßte und dann nach der Bemerkung auf S. 71 die Zahl α keine den Körper C_h bestimmende Zahl wäre. Es sei $\alpha^* = \alpha^a$ eine solche Potenz von α, für welche $K = K(\alpha^*, Z) + 0$ ausfällt. Vermöge $K(t\alpha^*, Z^b) = Z^{-b} K(\alpha^*, Z^b)$ folgt dann, daß die Zahl K^{l^h} und ferner alle Zahlen $\frac{K(\alpha^*, Z^b)}{K^b}$ Zahlen in dem Körper $k(Z)$ sind. Da

$$\alpha^* = \frac{1}{l^h}\{K(\alpha^*, Z) + K(\alpha^*, Z^2) + \cdots + K(\alpha^*, Z^{l^h})\}$$

wird und α^* ebenfalls eine den Körper C_h bestimmende Zahl ist, so sehen wir, daß der durch K und Z bestimmte Körper, dessen Grad höchstens $l^{2h-1}(l-1)$ ist, den Körper $k(Z, C_h)$ vom Grade $l^{2h-1}(l-1)$ enthält; der erstere Körper ist daher mit diesem letzteren Körper identisch, und die Zahl $\varkappa = K^{l^h}$ besitzt die im Hilfssatz 15 angegebene Eigenschaft.

Wir machen noch folgende Bemerkung. Der durch Z und $\sqrt[l^h]{\varkappa}$ bestimmte Körper ist, wie man leicht erkennt, relativ zyklisch vom Relativgrade l^h in bezug auf $k(Z)$ und besitzt daher einen einzigen Unterkörper, der $k(Z)$ enthält und relativ zyklisch vom Grade l in bezug auf $k(Z)$ ist. Bedeutet nun C_1 den Unterkörper l-ten Grades von C_h, so muß danach der aus $k(Z)$ und C_1 zusammengesetzte Körper mit dem durch Z und $\sqrt[l]{\varkappa}$ bestimmten Körper identisch sein.

§ 102. Von gewissen Primzahlen in der Diskriminante eines zyklischen Körpers vom Grade l^h.

Hilfssatz 16. Wenn C_h ein zyklischer Körper von einem Grade l^h ist, wo l eine beliebige Primzahl ($= 2$ oder $\neq 2$) ist, und wenn C_1 den Unterkörper l-ten Grades von C_h bezeichnet, so besitzen die etwaigen von l verschiedenen Primteiler p der Diskriminante von C_1 durchweg die Kongruenzeigenschaft $p \equiv 1$ nach l^h.

Beweis. Zunächst betrachten wir den Fall, daß l eine ungerade Primzahl und $h = 1$ ist. Wir nehmen an, es fände sich im Gegensatz zu unserer Behauptung eine rationale, in der Diskriminante von C_1 aufgehende Primzahl p, welche $\neq 1$ nach l ist. Es sei $\zeta = e^{\frac{2i\pi}{l}}$, ferner r eine Primitivzahl nach l, und man nehme aus der Gruppe des Körpers $k(\zeta)$ die Substitution $s = (\zeta : \zeta^r)$. Ist $\mathfrak{p}$ ein idealer Primfaktor von p im Körper $k(\zeta)$, so ist das Primideal $\mathfrak{p}$, wegen $p \neq 1$ nach l, nach Satz 119 von einem Grade $f > 1$; mithin ist nach Satz 129 der Zerlegungskörper des Primideals $\mathfrak{p}$ von einem Grade $e < l - 1$; die übrigen Primfaktoren von p sind dann

$$\mathfrak{p}' = s\mathfrak{p}, \ \ldots, \ \mathfrak{p}^{(e-1)} = s^{e-1}\mathfrak{p},$$

während $s^e\mathfrak{p} = \mathfrak{p}$, d. h.

$$\mathfrak{p}^{s^e-1} = 1 \tag{39}$$

wird. Desgleichen gelten auch für die zu $\mathfrak{p}$ konjugierten Primideale $\mathfrak{p}', \mathfrak{p}'', \ldots$ die entsprechenden Gleichungen

$$\mathfrak{p}'^{s^e-1} = 1, \qquad \mathfrak{p}''^{s^e-1} = 1, \ \ldots . \tag{40}$$

Nach Hilfssatz 15 gibt es eine ganze Zahl $\varkappa$ in $k(\zeta)$, so daß die beiden Zahlen ζ und $\sqrt[l]{\varkappa}$ den aus $k(\zeta)$ und C_1 zusammengesetzten Körper $k(\zeta, C_1)$ bestimmen, und für welche obendrein $\varkappa^{s-r}$ gleich der l-ten Potenz einer Zahl in $k(\zeta)$ wird. Da $s - r$ und $s^e - 1$ zwei ganzzahlige Funktionen von s sind, welche im Sinne der Kongruenz nach l keinen gemeinsamen Faktor haben, so gibt es drei ganzzahlige Funktionen $\varphi(s), \psi(s), \chi(s)$ der Veränderlichen s, so daß

$$1 = (s^e - 1)\varphi(s) + (s - r)\psi(s) + l\chi(s)$$

ist, und hieraus folgt

$$\varkappa = \varkappa^{(s^e-1)\varphi(s)+(s-r)\psi(s)+l\chi(s)} = \varkappa^{(s^e-1)\varphi(s)}\alpha^l,$$

wo α eine Zahl in $k(\zeta)$ ist. Wegen der vorhin bewiesenen Gleichungen (39) und (40) für die Primideale $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ läßt sich $\varkappa^{s^e-1}$ als eine solche ganze oder gebrochene Zahl schreiben, daß Zähler und Nenner keinen der Primfaktoren $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ enthalten und daher zu p prim sind; das gleiche gilt somit von der Zahl $\varkappa^{(s^e-1)\varphi(s)}$. Wir setzen $\varkappa^{(s^e-1)\varphi(s)} = \frac{\varrho}{a^l}$ in solcher Weise, daß ϱ eine ganze, zu p prime Zahl in $k(\zeta)$ und a eine ganze rationale Zahl bedeutet. Der Körper $k(\zeta, C_1)$ wird dann auch durch die beiden Zahlen ζ und $\sqrt[l]{\varrho}$ bestimmt. Die Relativdiskriminante der Zahl $\sqrt[l]{\varrho}$ in bezug auf $k(\zeta)$ ist $= \pm l^l \varrho^{l-1}$, und da ϱ zu p prim ist, so ist mithin auch die Relativdiskriminante von $k(\zeta, C_1)$ in bezug auf $k(\zeta)$ prim zu p. Da andererseits auch die Diskriminante von $k(\zeta)$ nicht durch p teilbar ist, so ist nach Satz 39 auch die Diskriminante von $k(\zeta, C_1)$ und folglich nach Satz 85 auch die Diskriminante des Körpers C_1 prim zu p, was unserer Annahme widerspricht.

In ähnlicher Weise erschließen wir die Richtigkeit des Hilfssatzes 16 bei ungeradem l, wenn der Exponent $h > 1$ angenommen wird. Es sei $Z = e^{\frac{2i\pi}{l^h}}$, ferner bezeichne r eine Primitivzahl nach l^h, und aus der Gruppe des Körpers $k(Z)$ sei $s = (Z : Z^r)$. Es sei p eine in der Diskriminante von C_1 aufgehende, von l verschiedene Primzahl und $\mathfrak{p}$ ein idealer Primfaktor von p in $k(Z)$. Nehmen wir $p \equiv 1$ nach l, aber $\not\equiv 1$ nach l^h an, so liegt das Primideal $\mathfrak{p}$ jedenfalls auch in dem Unterkörper $k(Z^l)$ des Körpers $k(Z)$, d. h. es ist $\mathfrak{p}^{s^{l^{h-2}(l-1)}-1} = 1$, und ebenso gelten für die zu $\mathfrak{p}$ in $k(Z)$ konjugierten Primideale $\mathfrak{p}', \mathfrak{p}'', \ldots$ die Gleichungen:

$$\mathfrak{p}'^{s^{l^{h-2}(l-1)}-1} = 1, \qquad \mathfrak{p}''^{s^{l^{h-2}(l-1)}-1} = 1, \ \ldots .$$

Da r Primitivzahl nach l^h ist, so wird $r^{l^{h-2}(l-1)} \not\equiv 1$ nach l^h, und mithin lassen sich drei ganzzahlige Funktionen $\varphi(s)$, $\psi(s)$, $\chi(s)$ der Variablen s derart bestimmen, daß

$$l^{h-1} = (s^{l^{h-2}(l-1)} - 1)\,\varphi(s) + (s - r)\,\psi(s) + l^h \chi(s)$$

ist; hieraus folgt alsdann, wenn $\varkappa$ eine nach Hilfssatz 15 bestimmte Zahl bedeutet,

$$\varkappa^{l^{h-1}} = \varkappa^{(s^{l^{h-2}(l-1)}-1)\varphi(s)} \alpha^{l^h},$$

wo α eine Zahl in $k(Z)$ ist. Wegen der vorhin bewiesenen Eigenschaft der Primideale $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ ist $\varkappa^{s^{l^{h-2}(l-1)}-1}$ und folglich auch $\varkappa^{(s^{l^{h-2}(l-1)}-1)\varphi(s)}$ eine Zahl, deren Zähler und Nenner zu p prim ausfallen. Wir können daher die letztere Zahl $= \frac{\varrho}{a^{l^h}}$ setzen in solcher Weise, daß ϱ eine ganze, zu p prime Zahl in $k(Z)$ und a eine ganze rationale Zahl bedeutet. Es ist dann $\sqrt[l]{\varkappa} = \frac{\alpha}{a}\sqrt[l^h]{\varrho}$, und daraus ergibt sich $\varrho = \sigma^{l^{h-1}}$, wo σ ebenfalls in $k(Z)$ liegt. Da der durch Z und $\sqrt[l]{\varkappa}$ bestimmte Körper, wie am Schlusse des § 101 bemerkt wurde, mit demjenigen Körper identisch ist, welcher durch Zusammensetzung aus $k(Z)$ und C_1 entsteht, und da die Relativdiskriminante der Zahl $\sqrt[l]{\sigma}$ in bezug auf $k(Z)$ den zu p primen Wert $\pm l^l \sigma^{l-1}$ besitzt, so ist die Relativdiskriminante des Körpers $k(Z, C_1)$ in bezug auf $k(Z)$ prim zu p. Andererseits ist die Diskriminante von $k(Z)$ ebenfalls nicht durch p teilbar, und folglich gilt das gleiche auch von der Diskriminante des Körpers $k(Z, C_1)$ und damit auch dann von der des Körpers C_1. Der letztere Umstand aber widerspricht unserer Annahme.

Um die Richtigkeit des Hilfssatzes 16 für $l = 2$ zu erkennen, machen wir zunächst die Annahme $h = 2$ und wenden dann auf den zyklischen Körper C_2 vom 4-ten Grade den Hilfssatz 15 an. Wir setzen $Z = e^{\frac{i\pi}{2}} = i$ und betrachten aus der Gruppe von $k(Z)$ die Substitution $s' = (i : -i)$. Es sei C_1 der quadratische Unterkörper von C_2, und wir nehmen an, es gebe eine in der Diskriminante von C_1 aufgehende ungerade Primzahl p, welche $\not\equiv 1$ nach 4 ist. Infolge der letzteren Eigenschaft ist p in $k(i)$ unzerlegbar. Ist nun die uns durch Hilfssatz 15 angewiesene Zahl $\varkappa$ durch p teilbar, so bilden wir die Zahl $\varrho = \varkappa^{s'-1}$. Da nach Hilfssatz 15 andererseits $\varkappa^{s'+1} = \alpha^4$ sein soll, wo α in $k(i)$ liegt, so folgt $\varkappa^2 = \varrho^{-1}\alpha^4$, d. h. $\sqrt{\varkappa} = \alpha\sqrt[4]{\varrho^{-1}}$. Infolgedessen ist ϱ das Quadrat einer Zahl in $k(i)$; wir können $\varrho = \frac{\tau^2}{\alpha^4}$ setzen in solcher Weise, daß τ eine ganze, zu p prime Zahl in $k(i)$ und a eine ganze rationale Zahl bedeutet. Da der Körper $k(i, C_1)$ mit dem Körper $k(i, \sqrt{\tau})$ übereinstimmt, und da andererseits die Relativdiskriminante der Zahl $\sqrt{\tau}$ in bezug auf $k(i)$ zu p prim ist, so ist auch die Relativdiskriminante des Körpers $k(i, C_1)$ in bezug auf $k(i)$ prim zu p, und hieraus folgt, daß die Diskriminante von C_1 nicht durch p teilbar ist, entgegen der Voraussetzung.

Ist im Falle $l = 2$ der Exponent $h > 2$, so setzen wir $Z = e^{\frac{i\pi}{2^{h-1}}}$. Nehmen wir dann an, es gäbe eine in der Diskriminante von C_1 aufgehende Primzahl $p \equiv 1$ nach 4 und $\not\equiv 1$ nach 2^h, und ist $\mathfrak{p}$ ein idealer Primfaktor von p in $k(Z)$, so bliebe $\mathfrak{p}$ ungeändert bei einer Substitution $s_*^{2^{h-3}}$, wo s_* entweder $= (Z : Z^5)$ oder $= (Z : Z^{-5})$ zu nehmen ist; folglich wäre $\mathfrak{p}^{s_*^{2^{h-3}}-1} \equiv 1$. Wegen $(\pm 5)^{2^{h-3}} \not\equiv 1$ nach 2^h würde, ähnlich wie oben, eine Gleichung von der Gestalt:

$$2^{h-1} = (s_*^{2^{h-3}} - 1)\,\varphi(s_*) + (s_* \mp 5)\,\psi(s_*) + 2^h \chi(s_*)$$

gelten, und aus dieser schließen wir, wie vorhin bei ungeradem l, auf einen Widerspruch mit der Annahme, wonach p in der Diskriminante von C_1 aufgeht. Damit ist der Hilfssatz 16 vollständig bewiesen.

Aus dem Hilfssatze 16 folgt ohne Schwierigkeit die weitere Tatsache:

Hilfssatz 17. Es sei C_h ein zyklischer Körper von einem Grade l^h, wo l eine beliebige Primzahl ($= 2$ oder $\neq 2$) ist; der Unterkörper l-ten Grades von C_h werde mit C_1 bezeichnet; die Diskriminante des Körpers C_1 enthalte die von l verschiedene Primzahl p: dann kann stets ein Abelscher Körper $C'_{h'}$ von einem gewissen Grade $l^{h'} \leqq l^h$ mit folgenden beiden Eigenschaften gefunden werden:

Erstens. Der aus $C'_{h'}$ und einem gewissen Kreiskörper P_h zusammengesetzte Körper enthält C_h als Unterkörper.

Zweitens. Die Diskriminante des Körpers $C'_{h'}$ enthält nur solche Primzahlen, die auch in der Diskriminante des Körpers C_h aufgehen, darunter aber nicht die Primzahl p.

Beweis. Nach Hilfssatz 16 besitzt die rationale Primzahl p die Kongruenzeigenschaft $p \equiv 1$ nach l^h; man konstruiere nach § 100 den zyklischen Kreiskörper P_h vom Grade l^h, dessen Diskriminante eine Potenz von p ist,

und betrachte den aus C_h und P_h zusammengesetzten Körper $k(C_h, P_h)$, dessen Grad $l^{h+h'}$ sei. In P_h gilt $p = \mathfrak{p}^{l^h}$, wo $\mathfrak{p}$ ein Primideal in P_h bedeutet. Es sei $\mathfrak{P}$ ein in $\mathfrak{p}$ aufgehendes Primideal des Körpers $k(C_h, P_h)$. Da das Primideal $\mathfrak{P}$ in der Gradzahl $l^{h+h'}$ des Körpers $k(C_h, P_h)$ nicht aufgeht, so ist dieser Körper $k(C_h, P_h)$ Verzweigungskörper des Primideals $\mathfrak{P}$ und als solcher nach Satz 81 relativ zyklisch, und zwar mindestens vom Relativgrade l^h, in bezug auf den Trägheitskörper des Primideals $\mathfrak{P}$, der $C'_{h'}$ heiße. Da ferner zyklische Körper von höherem als dem l^h-ten Grade in $k(C_h, P_h)$ nicht vorkommen können, so hat $k(C_h, P_h)$ genau den Relativgrad l^h in bezug auf $C'_{h'}$. Hieraus folgt, daß der Körper $C'_{h'}$ vom Grade $l^{h'}$ ist. Die Differente des Trägheitskörper $C'_{h'}$ ist nach Satz 76 nicht durch $\mathfrak{P}$ teilbar, und daher ist, mit Rücksicht auf Satz 68, die Diskriminante des Körpers $C'_{h'}$ nicht durch p teilbar. Andererseits enthält diese Diskriminante wegen Satz 39 nur solche rationale Primzahlen, welche in der Diskriminante von C_h aufgehen. Endlich folgt aus Satz 87, daß der aus $C'_{h'}$ und P_h zusammengesetzte Körper mit $k(C_h, P_h)$ übereinstimmt. Der Körper $C'_{h'}$ besitzt demnach alle im Hilfssatz 17 verlangten Eigenschaften.

§ 103. Der zyklische Körper vom Grade u, dessen Diskriminante nur u enthält, und die zyklischen Körper vom Grade u^h und 2^h, in denen U_1 bzw. Π_1 als Unterkörper enthalten ist.

Hilfssatz 18. Wenn die Diskriminante eines zyklischen Körpers C_1 von einem ungeraden Primzahlgrade u ausschließlich die Primzahl u enthält, so stimmt C_1 mit U_1 überein.

Beweis. Wir setzen $\zeta = e^{\frac{2i\pi}{u}}$ und $s = (\zeta : \zeta^r)$, wo r eine Primitivzahl nach u bedeute. Schreiben wir überdies $\lambda = 1 - \zeta$, so ist $\mathfrak{l} = (\lambda)$ ein Primideal in $k(\zeta)$, und es wird im Sinne der Idealtheorie $u = \mathfrak{l}^{u-1}$; endlich gilt die Kongruenz

$$s\lambda = 1 - \zeta^r \equiv r\lambda, \qquad (\mathfrak{l}^2).$$

Wir betrachten nun die uns durch Hilfssatz 15 angewiesene Zahl $\varkappa$. Da das Primideal $\mathfrak{l}$ in $k(\zeta)$ vom ersten Grade ist, so folgt, wenn $\varrho = \varkappa^{(s-1)(u-1)}$ gesetzt wird, in Anbetracht der Gleichung $s\mathfrak{l} = \mathfrak{l}$ und nach Satz 24 die Kongruenz $\varrho \equiv 1$ nach $\mathfrak{l}$, wobei eine Kongruenz zwischen gebrochenen Zahlen dann bestehen soll, wenn sie sich durch Multiplikation mit einer zum Modul teilerfremden ganzen Zahl in eine gewöhnliche Kongruenz verwandeln läßt. Da $r - 1$ zu u prim ist, so wird der aus C_1 und $k(\zeta)$ zusammengesetzte Körper auch durch ζ und $\sqrt[u]{\varrho}$ bestimmt sein. Wir setzen $\varrho \equiv 1 + a\lambda$ nach $\mathfrak{l}^2$, wo a eine ganze rationale Zahl bedeute; dann ist $\sigma = \varrho\zeta^a \equiv 1$ nach $\mathfrak{l}^2$.

Nunmehr führen wir den Nachweis dafür, daß die Kongruenz $\sigma \equiv 1$ nach $\mathfrak{l}^u$ besteht. Zu dem Zwecke nehmen wir an, es sei $\sigma \equiv 1 + a\lambda^e$ nach $\mathfrak{l}^{e+1}$,

wobei der Exponent $e < u$ ausfällt und a eine nicht durch u teilbare ganze rationale Zahl bedeutet.

Wir berücksichtigen, daß nach dem Hilfssatze 15 $\varkappa^{s-r}$ und folglich auch σ^{s-r} die u-te Potenz einer Zahl in $k(\zeta)$ ist; wir setzen $\sigma^{s-r} = \beta^u$, wo β eine Zahl des Körpers $k(\zeta)$ sei. Diese Gleichung liefert die Kongruenz $1 + a(r\lambda)^e - ar\lambda^e \equiv \beta^u$ nach $\mathfrak{l}^{e+1}$. Aus dieser folgt zunächst $\beta \equiv 1$ nach $\mathfrak{l}$, und dies liefert $\beta^u \equiv 1$ nach $\mathfrak{l}^u$. Hieraus würde endlich $ar^e \equiv ar$ nach $\mathfrak{l}$ folgen, was unmöglich ist, da r Primitivzahl nach u sein soll und $e > 1$ ist. Diese Betrachtung lehrt die Richtigkeit der Kongruenz $\sigma \equiv 1$ nach $\mathfrak{l}^u$.

Wir setzen nun $\sigma = \frac{\tau}{a^{u(u-1)}}$ in solcher Weise, daß τ eine ganze Zahl in $k(\zeta)$ und a eine ganze rationale Zahl bedeutet; es ist dann $\tau \equiv 1$ nach $\mathfrak{l}^u$. Nehmen wir nun an, der Körper C_1 sei von dem Körper U_1 verschieden, so entsteht durch Zusammensetzung aus $k(\zeta)$, U_1 und C_1 der durch $\sqrt[u]{\zeta}$ und $\sqrt[u]{\tau}$ bestimmte Körper $k(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$ vom Grade $u^2(u-1)$. Es ist andererseits $\xi = \frac{1 - \sqrt[u]{\tau}}{\lambda}$, wie die Gleichung $\frac{(\xi\lambda - 1)^u + \tau}{\lambda^u} = 0$ zeigt, eine ganze Zahl des Körpers $k(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$, und die Relativdiskriminante dieser Zahl in bezug auf $k(\sqrt[u]{\zeta})$ ist gleich $\varepsilon\tau^{u-1}$, wo ε eine Einheit ist. Da τ zu u prim ist, so ist mithin die Relativdiskriminante des Körpers $k(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$ in bezug auf den Körper $k(\sqrt[u]{\zeta})$ ebenfalls prim zu u. Bezeichnen wir daher mit $\mathfrak{L}^*$ einen idealen Primfaktor von $\mathfrak{l}$ im Körper $k(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$, so besitzt $\mathfrak{L}^*$ mit Rücksicht auf Satz 93 in diesem Körper einen Trägheitskörper T, welcher den Grad u hat. Die Diskriminante dieses Trägheitskörpers T ist prim zu u, und wegen Satz 85 müßte sie daher den Wert $+1$ oder -1 besitzen. Daß es aber einen zyklischen Körper vom Primzahlgrade u mit der Diskriminante ± 1 nicht gibt, folgt entweder direkt aus Satz 44 oder mittels Satz 94, wenn wir den in diesem Satze 94 mit k bezeichneten Körper gleich dem Körper der rationalen Zahlen nehmen und die Tatsache berücksichtigen, daß im Körper der rationalen Zahlen alle Ideale Hauptideale sind. Damit ist der Beweis für den Hilfssatz 18 erbracht.

Hilfssatz 19. Wenn ein zyklischer Körper C_h vom Grade l^h, wo l gleich einer ungeraden Primzahl u oder gleich 2 ist, den Körper U_1 bzw. Π_1 als Unterkörper enthält, so ist C_h Unterkörper eines solchen Körpers, welcher aus U_h bez. Π_h und aus einem gewissen zyklischen Körper $C'_{h'}$ von einem Grade $l^{h'} < l^h$ durch Zusammensetzung entsteht.

Beweis. Es sei $C_h + U_h$ bez. Π_h. Der größte sowohl in C_h als in U_h bez. Π_h enthaltene Unterkörper werde mit L_{h^*} bezeichnet; L_{h^*} habe den Grad l^{h^*}, wo h^* eine positive ganze rationale Zahl $< h$ bedeute. Es sei t eine solche Substitution aus der Gruppe des Körpers C_h, welche mit ihren Po-

tenzen diese Gruppe erzeugt, und z eine solche Substitution, welche die Gruppe des Körpers U_h bez. Π_h erzeugt. Setzen wir $t^* = t^{l^{h^*}}$ und $z^* = z^{l^{h^*}}$, so erzeugen t^* und z^* beide Male diejenigen Untergruppen vom Grade l^{h-h^*}, zu denen L_{h^*} als Unterkörper einerseits von C_h, andererseits von U_h bez. Π_h gehört. Der aus C_h und U_h bez. Π_h zusammengesetzte Körper K ist in bezug auf L_{h^*} vom Relativgrade l^{2h-2h^*} und daher überhaupt vom Grade l^{2h-h^*}.

Um die Gruppe G des Körpers K zu ermitteln, bezeichnen wir mit ϑ eine den Körper C_h und mit γ eine den Körper U_h bez. Π_h bestimmende Zahl und verstehen unter x, y unbestimmte Parameter. Die Größe $\Theta = x\vartheta + y\gamma$ genügt einer Gleichung vom l^{2h-h^*}-ten Grade, deren Koeffizienten ganzzahlige Funktionen von x und y sind, und welche in dem durch die Parameter x und y bestimmten Rationalitätsbereich irreduzibel ist. Die verschiedenen Wurzeln dieser Gleichung sind von der Gestalt

$$\Theta_{m\,n} = x\,t^m\,\vartheta + y\,z^n\,\gamma\,,$$

wo m, n gewisse Paare ganzer Zahlen bedeuten. Da einem bekannten Satze zufolge sowohl ϑ wie γ sich als rationale Funktionen von Θ ausdrücken lassen, wobei die Koeffizienten ganzzahlige Funktionen von x und y werden, so sind auch die Größen $\Theta_{m\,n}$ ebenso ausdrückbar; wir setzen

$$\Theta_{m\,n} = x\,t^m\,\vartheta + y\,z^n\,\gamma = \Phi_{m\,n}(\Theta)\,,$$

wobei $\Phi_{m\,n}$ eine rationale Funktion von Θ bedeutet, deren Koeffizienten ganzzahlige Funktionen von x, y sind. Es bezeichne nun A irgendeine Zahl in K oder überhaupt eine rationale Funktion von x, y, deren Koeffizienten in K liegen; dann wird A gleich einer rationalen Funktion $F(\Theta)$ der Größe Θ, deren Koeffizienten ganzzahlige Funktionen von x, y sind. Es drücken sich ferner die zu A konjugierten Größen in der Gestalt

$$S_{m\,n}\,\mathsf{A} = F(\Phi_{m\,n}(\Theta))$$

aus, und das System der betreffenden l^{2h-h^*} Substitutionen $S_{m\,n}$ bildet die Gruppe G des Körpers K. Wegen

$$S_{m\,n}\,\Theta = x\,S_{m\,n}\,\vartheta + y\,S_{m\,n}\,\gamma = x\,t^m\,\vartheta + y\,z^n\,\gamma$$

wird

$$S_{m\,n}\,\vartheta = t^m\,\vartheta\,, \qquad S_{m\,n}\,\gamma = z^n\,\gamma\,,$$

und hieraus folgt leicht:

$$S_{m\,n}\,S_{m'\,n'} = S_{m+m',\,n+n'}\,, \tag{41}$$

wenn allgemein die Festsetzung $S_{m\,n} = S_{m^*\,n^*}$ getroffen wird, falls $m \equiv m^*$ und $n \equiv n^*$ nach l^h ist. Aus (41) folgt die Vertauschbarkeit der Substitutionen der Gruppe G, d. h. der Körper K ist ein Abelscher Körper.

Es bezeichne r eine Primitivzahl nach l^h; da insbesondere $z^r\gamma$ eine zu γ konjugierte Zahl ist, so muß es jedenfalls eine Substitution in der Gruppe G geben, bei welcher der zweite Index $n \equiv r$ nach l^h ist. Wir setzen eine solche Substitution $S_{m\,r} = s$. Der Grad der aus s erzeugten zyklischen Gruppe ist l^h. Es kann ferner leicht erkannt werden, daß alle diejenigen Substitutionen der Gruppe G, bei denen der zweite Index $\equiv 0$ nach l^h ausfällt, für sich eine zyklische Untergruppe vom Grade l^{h-h^*} bilden. Es sei $s^* = S_{m^*\,0}$ eine erzeugende Substitution dieser zyklischen Gruppe. Die Gruppe G entsteht dann offenbar durch Zusammensetzung aus den l^h Potenzen von s und den l^{h-h^*} Potenzen von s^*. Zu der aus den Potenzen von s^* bestehenden Untergruppe gehört offenbar im Körper K der zyklische Unterkörper U_h bez. Π_h. Zu der aus s erzeugten Gruppe gehört in K ein gewisser zyklischer Unterkörper $C'_{h'}$ vom Grade l^{h-h^*}. Die beiden Körper U_h bez. Π_h und $C'_{h'}$ haben keinen gemeinsamen Unterkörper außer dem Körper der rationalen Zahlen, und der Körper K entsteht daher durch Zusammensetzung aus diesen beiden zyklischen Körpern. Damit ist der Hilfssatz 19 vollständig bewiesen.

§ 104. Beweis des Fundamentalsatzes über Abelsche Körper.

Wir beweisen nunmehr den Fundamentalsatz 131 in folgender Art. Zunächst ist in § 48 festgestellt worden, daß jeder Abelsche Körper sich aus zyklischen Körpern zusammensetzen läßt, deren Grade Primzahlen oder Primzahlpotenzen sind; es ist daher nur nötig, zu zeigen, daß jeder zyklische Körper C_h von einem Grade l^h, wo l eine Primzahl bezeichnet, ein Kreiskörper ist.

Um diesen Beweis zu führen, nehmen wir an, es sei bereits die Richtigkeit des Fundamentalsatzes 131 für alle diejenigen Abelschen Körper erkannt, deren Grad eine niedere Potenz von l als l^h ist.

Es werde nun der in C_h enthaltene Unterkörper vom l-ten Grade C_1 ins Auge gefaßt. Nehmen wir an, daß die Diskriminante von C_1 eine von l verschiedene rationale Primzahl p enthält, so ist nach Satz 39 auch die Diskriminante von C_h durch p teilbar. Ferner existiert nach Hilfssatz 17 ein Abelscher Körper $C'_{h'}$ vom Grade $l^{h'} \leqq l^h$ der Art, daß C_h Unterkörper des aus $C'_{h'}$ und dem Kreiskörper P_h zusammengesetzten Körpers wird. Ist dann $C'_{h'}$ ein zyklischer Körper von niederem als l^h-ten Grade oder aus mehreren solchen zyklischen Körpern zusammengesetzt, so erweist sich $C'_{h'}$ auf Grund unserer Annahme als Kreiskörper, und mithin ist auch C_h ein Kreiskörper. Es ist demnach nur noch der Fall in Betracht zu ziehen, daß $h' = h$ ausfällt und $C'_{h'} = C'_h$ ein zyklischer Körper vom Grade l^h ist. Wie der vorhin angewandte Hilfssatz 17 aussagt, enthält die Diskriminante von C'_h nur solche Primzahlen, welche in der Diskriminante von C_h aufgehen, aber nicht die Primzahl p; die Diskriminante von C'_h enthält also mindestens eine rationale Primzahl weniger als die Diskriminante von C_h.

Wir bezeichnen den Unterkörper l-ten Grades von C'_h mit C'_1. Geht dann in der Diskriminante von C'_1 noch eine von l verschiedene rationale Primzahl p'

auf, so können wir auf den Körper C'_h das nämliche Verfahren anwenden, das wir soeben für den ursprünglich vorgelegten Körper C_h dargelegt haben, und gelangen dann entweder zu der Einsicht, daß C'_h ein Kreiskörper ist, oder wir werden auf einen zyklischen Körper C''_h vom Grade l^h geführt, dessen Diskriminante wieder mindestens eine rationale Primzahl, nämlich die Primzahl p', weniger enthält als die Diskriminante des Körpers C'_h. Das so eingeleitete Verfahren führt nach einer gewissen Anzahl m sich folgender Anwendungen entweder auf einen Körper $C_{h^{(m)}}^{(m)}$, der sich auf Grund unserer Annahme bereits als Kreiskörper erweist, oder wir gelangen schließlich zu einem zyklischen Körper $C_h^{(m)}$ vom Grade l^h von der Art, daß der in $C_h^{(m)}$ enthaltene Unterkörper $C_1^{(m)}$ vom l-ten Grade eine Diskriminante besitzt, welche keine rationale Primzahl oder nur die Primzahl l enthält. Da es nach den Bemerkungen auf S. 213 einen zyklischen Körper l-ten Grades mit der Diskriminante ± 1 nicht gibt, so tritt notwendig der letztere Umstand ein.

Wir unterscheiden nunmehr zwei Fälle, je nachdem l eine ungerade Primzahl u oder gleich 2 ist.

Im *ersteren* Falle stimmt nach Hilfssatz 18 $C_1^{(m)}$ mit U_1 überein.

Im *zweiten* Falle $l = 2$ ist, wenn $h = 1$ ausfällt, der Körper $C_h^{(m)} = C_1^{(m)}$ entweder gleich $k(i)$ oder gleich $k(\sqrt{2}) = \Pi_1$ und mithin offenbar ein Kreiskörper. Für $h > 1$ erweist sich jedoch $C_1^{(m)}$ stets gleich $k(\sqrt{2}) = \Pi_1$. Ist nämlich $C_h^{(m)}$ ein reeller Körper, so ist offenbar auch $C_1^{(m)}$ reell, und daraus folgt die Behauptung. Ist jedoch $C_h^{(m)}$ ein imaginärer Körper, so bilden die sämtlichen reellen Zahlen desselben einen reellen Unterkörper vom Grade 2^{h-1}, und da $C_1^{(m)}$ notwendig in diesem reellen Körper enthalten ist, so ist $C_1^{(m)}$ ebenfalls reell und stimmt also mit Π_1 überein.

In den beiden oben unterschiedenen Fällen ist somit, wenn wir von $l = 2$, $h = 1$ absehen, stets der Körper $C_1^{(m)} = U_1$ bez. $= \Pi_1$. Nach Hilfssatz 19 ist infolgedessen $C_h^{(m)}$ Unterkörper eines Körpers, der sich aus U_h bez. Π_h und einem zyklischen Körper $C_{\bar{h}}$ vom Grade $l^{\bar{h}} < l^h$ zusammensetzt. Da nun der Fundamentalsatz 131 für zyklische Körper von der letzteren Beschaffenheit bereits als bewiesen angenommen worden ist, so erweist sich auch $C_h^{(m)}$ als Kreiskörper. Damit ist der Fundamentalsatz 131 vollständig bewiesen, und zugleich ist ersichtlich, in welcher Weise man alle Abelschen Körper von gegebener Gruppe und gegebener Diskriminante aufstellen kann.

24. Die Wurzelzahlen des Kreiskörpers der l-ten Einheitswurzeln.

§ 105. Die Definition und Existenz der Normalbasis.

Eine Basis eines Abelschen Körpers K von einem Grade M soll eine **Normalbasis** heißen, wenn sie aus einer ganzen Zahl N des Körpers K und den zu N konjugierten Zahlen $\mathsf{N}', \ldots, \mathsf{N}^{(M-1)}$ besteht. Es gilt der folgende Hilfssatz:

Hilfssatz 20. Wenn ein Abelscher Körper K eine Normalbasis besitzt, so besitzt auch jeder Unterkörper k des Körpers K eine Normalbasis.

Beweis. Es sei M der Grad von K, und es seien $t_1, \ldots, t_M$ die Substitutionen der Gruppe des Abelschen Körpers K; ferner sei N eine solche ganze Zahl in K, die mit ihren konjugierten zusammen eine Normalbasis von K liefert. Bilden dann $t_1, \ldots, t_r$ diejenige Untergruppe jener Gruppe von M Substitutionen, zu welcher der Unterkörper k von K gehört, so kann man dazu unter jenen M Substitutionen $t_1, \ldots, t_M$ solche $m = \frac{M}{r}$ Substitutionen $t'_1, \ldots, t'_m$ finden, daß die M Substitutionen $t_1, \ldots, t_M$, abgesehen von ihrer Reihenfolge, durch die Substitutionenprodukte

$$t'_1 t_1, \ldots, t'_1 t_r; \quad t'_2 t_1, \ldots, t'_2 t_r; \ \ldots; \quad t'_m t_1, \ldots, t'_m t_r$$

dargestellt werden. Ist α eine ganze Zahl in k, so gilt, da eine solche stets auch eine ganze Zahl in K ist, eine Gleichung

$$\alpha = a_{11} t'_1 t_1 \mathsf{N} + \cdots + a_{1r} t'_1 t_r \mathsf{N} + \cdots + a_{m1} t'_m t_1 \mathsf{N} + \cdots + a_{mr} t'_m t_r \mathsf{N},$$

wo $a_{11}, \ldots, a_{1r}, \ldots, a_{m1}, \ldots, a_{mr}$ ganze rationale Zahlen sind. Berücksichtigen wir, daß α bei Anwendung der einzelnen Substitutionen $t_1, \ldots, t_r$ ungeändert bleibt, und andererseits, daß zwischen den $M = mr$ Zahlen $t'_1 t_1 \mathsf{N}, \ldots, t'_1 t_r \mathsf{N}; \ \ldots; t'_m t_1 \mathsf{N}, \ldots, t'_m t_r \mathsf{N}$ keine lineare Relation mit ganzen rationalen nicht sämtlich verschwindenden Koeffizienten stattfinden kann, so folgt offenbar:

$$a_{11} = a_{12} = \cdots = a_{1r}, \ \ldots, \ a_{m1} = a_{m2} = \cdots = a_{mr},$$

d. h.: wenn

$$\nu = t_1 \mathsf{N} + t_2 \mathsf{N} + \cdots + t_r \mathsf{N}$$

gesetzt wird, so bilden die m Zahlen $t'_1 \nu, t'_2 \nu, \ldots, t'_m \nu$ eine Normalbasis des Körpers k.

Satz 132. Ein jeder Abelsche Körper K vom M-ten Grade, dessen Diskriminante D zu M prim ist, besitzt eine Normalbasis.

Beweis. Die verschiedenen rationalen Primzahlen in D seien $p, p', \ldots$. Da keine dieser Primzahlen in M aufgeht, so ist nach dem Beweise des Satzes 131 der Abelsche Körper K in demjenigen Kreiskörper als Unterkörper enthalten, welcher durch die Zahlen $\zeta = e^{\frac{2i\pi}{p}}, \zeta' = e^{\frac{2i\pi}{p'}}, \ldots$, d. h. welcher durch die Einheitswurzel $Z = e^{\frac{2i\pi}{pp'\cdots}}$ bestimmt ist. Für den Körper $k(\zeta)$ bilden nach Satz 118 die Zahlen $1, \zeta, \ldots, \zeta^{p-2}$ und folglich auch die Zahlen $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ eine Basis; die letztere Basis ist eine Normalbasis. Entsprechendes gilt für $k(\zeta'), \ldots$.

Man bilde nun das System der $(p-1)(p'-1)\ldots$ Zahlen $\zeta^h \zeta'^{h'} \ldots$, wo die Exponenten $h; h'; \ldots$ bez. die Zahlen

$$1, 2, \ldots, p-1; \qquad 1, 2, \ldots, p'-1; \ \ldots$$

unabhängig voneinander durchlaufen sollen; dann stellt dieses System von $\Phi(p\,p'\ldots)$ Zahlen nach Satz 88 eine Basis des Körpers $k(Z)$ dar, und diese Basis ist offenbar eine Normalbasis. Nach dem Hilfssatz 20 besitzt folglich auch der Abelsche Körper K eine Normalbasis. Damit ist der Satz 132 bewiesen.

§ 106. Der Abelsche Körper vom Primzahlgrade l und von der Diskriminante p^{l-1}. Die Wurzelzahlen dieses Körpers.

Die einfachsten und wichtigsten Abelschen Körper nächst den quadratischen Körpern sind diejenigen, bei welchen der Grad eine ungerade Primzahl l ist und die Diskriminante d nur eine einzige, und zwar von l verschiedene Primzahl p enthält. Es bedeute k einen solchen Körper. Nach Hilfssatz 16 besitzt die Primzahl p notwendig die Kongruenzeigenschaft $p \equiv 1$ nach l. Die Primzahl p wird im Körper k die l-te Potenz eines Primideales ersten Grades. Nach den Bemerkungen zu Satz 79 und mit Rücksicht darauf, daß k jedenfalls ein reeller Körper, also d positiv ist, ergibt sich $d = p^{l-1}$.

Es seien $1, t, t^2, \ldots, t^{l-1}$ die Substitutionen der Gruppe des Körpers k, und die Zahlen $v, tv, \ldots, t^{l-1}v$ mögen eine Normalbasis von k bilden (siehe Satz 132). Die Zahl v ist dann jedenfalls eine den Körper k bestimmende Zahl. Es werde $\zeta = e^{\frac{2i\pi}{l}}$ gesetzt; der Ausdruck

$$\Omega = v + \zeta \cdot tv + \zeta^2 \cdot t^2 v + \cdots + \zeta^{l-1} \cdot t^{l-1} v$$

soll eine **Wurzelzahl** des Körpers $k = k(v)$ heißen.

Jede solche Wurzelzahl Ω ist offenbar eine ganze Zahl des aus $k(v)$ und $k(\zeta)$ zusammengesetzten Körpers $k(v, \zeta)$. Das Studium der vorhandenen Normalbasen und Wurzelzahlen des Abelschen Körpers $k(v)$ gibt uns wichtige Aufschlüsse über die in p aufgehenden Primideale des Körpers $k(\zeta)$. Die Ausführungen dieses Kapitels erfahren nur leichte Abänderungen, wenn statt der ungeraden Primzahl l die Zahl 2 genommen wird.

§ 107. Die charakteristischen Eigenschaften der Wurzelzahlen.

Satz 133. Es sei ein Abelscher Körper k vom Grade l und mit der Diskriminante $d = p^{l-1}$ vorgelegt, wo l und p verschiedene ungerade Primzahlen bedeuten; ferner sei $v, tv, \ldots, t^{l-1}v$ eine Normalbasis dieses Körpers k. Wird dann $\zeta = e^{\frac{2i\pi}{l}}$, $\mathfrak{l} = (1-\zeta)$ und $s = (\zeta : \zeta^r)$ gesetzt, wo r eine Primitivzahl nach l bedeute, so besitzt die aus jener Normalbasis entspringende Wurzelzahl Ω des Körpers $k = k(v)$ die folgenden drei Eigenschaften:

Erstens. Die l-te Potenz der Wurzelzahl, $\omega = \Omega^l$, ist eine Zahl des Kreiskörpers $k(\zeta)$, und zudem wird ω^{s-r} gleich der l-ten Potenz einer Zahl des Körpers $k(\zeta)$.

Zweitens. Es gelten die sich gegenseitig bedingenden Kongruenzen

$$\Omega \equiv \pm 1, \quad (\mathfrak{l}), \quad \omega \equiv \pm 1, \quad (\mathfrak{l}^l).$$

Drittens. $n(\omega)$, die Norm der Zahl ω in $k(\zeta)$, ist $= p^{\frac{l(l-1)}{2}}$.

Beweis. Die Zahlen Ω^t und Ω^{s-r} sind solche Zahlen in $k(\zeta, v)$, welche beim Übergang von v in tv ungeändert bleiben. Sie sind deshalb Zahlen in $k(\zeta)$. Hieraus folgt die erste in Satz 133 angegebene Eigenschaft.

Da $v, tv, \ldots, t^{l-1}v$ Basiszahlen des Körpers $k(v)$ sind, so gilt insbesondere

$$1 = a_0 v + a_1 tv + \cdots + a_{l-1} t^{l-1} v$$

für bestimmte ganze rationale Zahlen $a_0, a_1, \ldots, a_{l-1}$. Die Anwendung der Substitution t auf diese Formel lehrt, daß $a_0 = a_1 = \cdots = a_{l-1}$ ist, und da die Koeffizienten $a_0, a_1, \ldots, a_{l-1}$ keinen gemeinsamen Teiler $\neq \pm 1$ haben können, so haben sie sämtlich den gleichen Wert ± 1, d. h. es ist $v + tv + \cdots + t^{l-1}v = \pm 1$. Aus dieser Formel folgt:

$$\begin{aligned}\Omega &= v + \zeta \cdot tv + \zeta^2 \cdot t^2 v + \cdots + \zeta^{l-1} \cdot t^{l-1} v \\ &\equiv v + tv + \cdots + t^{l-1} v \equiv \pm 1, \qquad (\mathfrak{l}).\end{aligned}$$

Mit Hilfe von $\omega \mp 1 = (\Omega \mp 1)(\zeta\Omega \mp 1) \ldots (\zeta^{l-1}\Omega \mp 1)$ erkennen wir die zweite Eigenschaft der Zahl ω.

Endlich folgt durch eine geeignete Anwendung des Multiplikationssatzes der Determinanten

$$\begin{vmatrix} v, & tv, & \ldots, & t^{l-1}v \\ t^{l-1}v, & v, & \ldots, & t^{l-2}v \\ \cdots & \cdots & \cdots & \cdots \\ tv, & t^2 v, & \ldots, & v \end{vmatrix} = (v + tv + \cdots + t^{l-1}v)\, n(\Omega) = \pm n(\Omega),$$

wo

$$n(\Omega) = (v + \zeta tv + \cdots + \zeta^{l-1} t^{l-1} v) \ldots (v + \zeta^{l-1} tv + \cdots + \zeta^{(l-1)^2} t^{l-1} v)$$

die Relativnorm von Ω in bezug auf den Körper $k(v)$ ist. Das Quadrat der Determinante linker Hand ist gleich der Diskriminante des Körpers $k(v)$, d. h. $= p^{l-1}$, und folglich ergibt sich

$$n(\omega) = (n(\Omega))^l = p^{l\left(\frac{l-1}{2}\right)}.$$

Damit ist der Satz 133 vollständig bewiesen.

Die drei in Satz 133 bewiesenen Eigenschaften einer Wurzelzahl Ω des Körpers $k(v)$ reichen umgekehrt völlig zur Charakterisierung einer solchen Zahl hin. Es gilt nämlich folgende Tatsache:

Satz 134. Es sei l eine ungerade Primzahl und $\zeta = e^{\frac{2i\pi}{l}}$, ferner p eine Primzahl $\equiv 1$ nach l; wenn dann ω eine solche Zahl des Kreiskörpers $k(\zeta)$

bedeutet, die nicht gleich der l-ten Potenz einer Zahl in $k(\zeta)$ wird, und welche die drei in Satz 133 angegebenen Eigenschaften besitzt, so ist $\Omega = \sqrt[l]{\omega}$ eine Wurzelzahl des Abelschen Körpers l-ten Grades von der Diskriminante p^{l-1}.

Beweis. Die Zahl $\Omega = \sqrt[l]{\omega}$ bestimmt einen relativ Galoisschen Körper vom Relativgrade l in bezug auf den Körper $k(\zeta)$. Es sei t diejenige Substitution der Relativgruppe, für welche $t\Omega = \zeta^{-1}\Omega$ wird. Mit Rücksicht auf die erste Eigenschaft der Zahl ω, die sich in der Formel $s\omega = \omega^r \alpha^l$ ausdrückt, wo α eine Zahl in $k(\zeta)$ bedeutet, ist der durch ζ und Ω bestimmte Körper vom $l(l-1)$-ten Grade ein Galoisscher Körper. Die Zahl α erfüllt die Bedingung

$$\omega^{1-r^{l-1}} = \alpha^{l\frac{s^{l-1}-r^{l-1}}{s-r}};$$

wir legen sie eindeutig fest durch die weitere Forderung

$$\omega^{\frac{1-r^{l-1}}{l}} = \alpha^{\frac{s^{l-1}-r^{l-1}}{s-r}}.$$

Wir wollen nun unter t und s zugleich diejenigen bestimmten Substitutionen der Gruppe dieses Galoisschen Körpers $k(\zeta, \Omega)$ verstehen, welche neben den für t und s schon festgesetzten Beziehungen noch $t\zeta = \zeta$ und $s\Omega = \Omega^r\alpha$ ergeben. Diese beiden Substitutionen s und t sind miteinander vertauschbar, da

$$st\Omega = \zeta^{-r}\Omega^r\alpha = ts\Omega$$

wird, d. h. der Körper $k(\zeta, \Omega)$ ist ein Abelscher Körper. Ferner wird die Untergruppe der Gruppe von $k(\zeta, \Omega)$, welche aus den Potenzen der Substitution s besteht, genau vom Grade $l-1$. Der zu dieser Untergruppe gehörige Unterkörper von $k(\zeta, \Omega)$ ist daher vom l-ten Grade; er ist wiederum ein Abelscher Körper; dieser Körper werde mit k bezeichnet.

Wir beweisen zunächst, daß die Diskriminante dieses Körpers k zu l prim ist. Da $\Omega \equiv \pm 1$ nach $\mathfrak{l} = (1-\zeta)$ ist, so stellt der Quotient $\frac{\Omega \mp 1}{1-\zeta}$ eine ganze Zahl dar. Wegen $t\Omega = \zeta^{-1}\Omega$ hat die Relativdifferente dieser ganzen Zahl in bezug auf den Körper $k(\zeta)$ den Wert $\varepsilon\Omega^{l-1}$, wo ε eine Einheit bedeutet, und daher ist die Relativdifferente des Körpers $k(\zeta, \Omega)$ in bezug auf den Körper $k(\zeta)$ prim zu l. Bedeutet $\mathfrak{L}$ ein in $\mathfrak{l}$ aufgehendes Primideal des Körpers $k(\zeta, \Omega)$, so kommt dieses nach Satz 93 in $\mathfrak{l}$ zu keiner höheren als der ersten Potenz vor, d. h. es ist $\mathfrak{l} = \mathfrak{L}^{l-1}\mathfrak{M}$, wo $\mathfrak{M}$ sich nicht mehr durch $\mathfrak{L}$ teilen läßt. Hieraus folgt nach § 39 und § 40, daß der Trägheitskörper des Primideals $\mathfrak{L}$ vom Grade l sein muß, und daher ist k selbst dieser Trägheitskörper. Nach Satz 76 ist die Differente des Körpers k nicht durch $\mathfrak{L}$ und folglich auf Grund des Satzes 68 auch die Diskriminante des Körpers k nicht durch l teilbar.

Wir setzen

$$\nu = \frac{\pm 1 + \Omega + s\Omega + s^2\Omega + \cdots + s^{l-2}\Omega}{l}, \tag{41}$$

wo das Vorzeichen das nämliche wie in den Kongruenzen $\Omega \equiv \pm 1$, $s\Omega \equiv \pm 1, \ldots$ nach $\mathfrak{l}$ ist; dann wird der Zähler dieses in gebrochener Form erscheinenden Ausdrucks (41) kongruent 0 nach $\mathfrak{l}$. Dieser Zähler stellt eine Zahl in k dar. Ist l in k Primideal, so muß daher dieser Zähler auch durch l teilbar sein, und es ist ν eine ganze Zahl. Anderenfalls haben wir im Körper k, da die Diskriminante von k nicht den Faktor l enthält, eine Zerlegung $l = \mathfrak{l}_1 \ldots \mathfrak{l}_l$, wo $\mathfrak{l}_1, \ldots, \mathfrak{l}_l$ voneinander verschiedene Primideale sind, und im Körper $k(\zeta, \Omega)$ gilt dann, wie man mit Hilfe von Satz 88 erkennt, die Zerlegung

$$\mathfrak{l} = (1-\zeta) = (\mathfrak{l}, \mathfrak{l}_1)(\mathfrak{l}, \mathfrak{l}_2) \ldots (\mathfrak{l}, \mathfrak{l}_l).$$

Da der Zähler des Ausdrucks rechter Hand in (41) durch das Ideal $(\mathfrak{l}, \mathfrak{l}_1)$ teilbar ist, so ist derselbe als eine ganze Zahl in k auch durch $\mathfrak{l}_1$ teilbar. Entsprechend folgt die Teilbarkeit jenes Zählers durch $\mathfrak{l}_2, \ldots, \mathfrak{l}_l$, und es ist derselbe also schließlich auch durch l teilbar, d. h. die durch (41) definierte Zahl ν ist auch jetzt eine ganze Zahl.

Durch Benutzung der Gleichung $t\Omega = \zeta^{-1}\Omega$ ergeben sich aus (41) die beiden Formeln:

$$\begin{aligned} &\nu + t\nu + t^2\nu + \cdots + t^{l-1}\nu = \pm 1, \\ &\nu + \zeta \cdot t\nu + \zeta^2 \cdot t^2\nu + \cdots + \zeta^{l-1} \cdot t^{l-1}\nu = \Omega. \end{aligned} \tag{42}$$

Eine Anwendung des Multiplikationssatzes der Determinanten, wie sie schon beim Beweise des Satzes 133 vorkam, ergibt dann

$$\mathsf{N} = \begin{vmatrix} \nu, & t\nu, \ldots, & t^{l-1}\nu \\ t^{l-1}\nu, & \nu, \ldots, & t^{l-2}\nu \\ \cdots & \cdots & \cdots \\ t\nu, & t^2\nu, \ldots, & \nu \end{vmatrix} = \pm\Omega \cdot s\Omega \ldots s^{l-2}\Omega,$$

und hieraus folgt vermittelst der dritten in Satz 133 ausgesprochenen Eigenschaft der Zahl ω die Gleichung

$$\mathsf{N}^l = \pm p^{\frac{l(l-1)}{2}}$$

und somit

$$\begin{vmatrix} \nu, & t\nu, \ldots, & t^{l-1}\nu \\ t^{l-1}\nu, & \nu, \ldots, & t^{l-2}\nu \\ \cdots & \cdots & \cdots \\ t\nu, & t^2\nu, \ldots, & \nu \end{vmatrix}^2 = p^{l-1}.$$

Wir beweisen nun, daß die Diskriminante des Körpers k notwendig $= p^{l-1}$ sein muß. In der Tat ist dieselbe wegen der letzten Gleichung ein positiver Teiler der Zahl p^{l-1}. Da sie nach Satz 44 oder nach Satz 94 nicht gleich 1 sein kann, so enthält sie die Primzahl p, und zwar nach den Bemerkungen zum Satze 79 notwendig in der $(l-1)$-ten Potenz. Aus der soeben bewiese-

nen Tatsache folgt, daß $\nu, t\nu, \ldots, t^{l-1}\nu$ eine Basis des Körpers k bilden; diese Basis ist offenbar eine Normalbasis. Die Zahl Ω ist wegen (42) die aus dieser Normalbasis entspringende Wurzelzahl des Körpers k.

§ 108. Die Zerlegung der l-ten Potenz einer Wurzelzahl im Körper der l-ten Einheitswurzeln.

Satz 135. Haben l, p, ζ, r, s die bisherige Bedeutung, und ist $k(\nu)$ ein Abelscher Körper l-ten Grades mit der Diskriminante $d = p^{l-1}$ und Ω eine Wurzelzahl des Körpers $k(\nu)$, so gestattet die Zahl $\omega = \Omega^l$ im Körper $k(\zeta)$ die Zerlegung

$$\omega = \mathfrak{p}^{r_0 + r_{-1}s + r_{-2}s^2 + \cdots + r_{-l+2}s^{l-2}},$$

wo $\mathfrak{p}$ ein bestimmtes in p aufgehendes Primideal des Körpers $k(\zeta)$ bedeutet, und wo allgemein r_{-i} die kleinste positive ganze rationale Zahl bedeutet, welche der $-i$-ten Potenz r^{-i} der Primitivzahl r nach l kongruent ist [Kummer (6, II)].

Beweis. Die Primzahl p zerfällt im Körper $k(\zeta)$ in $l-1$ voneinander verschiedene ideale Primfaktoren $\mathfrak{p}, s\mathfrak{p}, \ldots, s^{l-2}\mathfrak{p}$; die Zahl ω muß durch jedes dieser Primideale teilbar sein. Denn nach dem Beweise zu Satz 134 ist die Relativdifferente des Körpers $k(\zeta, \Omega)$ in bezug auf den Körper $k(\zeta)$ ein Teiler von $\Omega^l = \omega$; wäre nun ω etwa zu $\mathfrak{p}$ prim, so wäre also diese Relativdifferente und wegen Satz 41 auch die Differente und endlich wegen Satz 68 auch die Diskriminante von $k(\zeta, \Omega)$ prim zu $\mathfrak{p}$, was nicht sein kann, da sie die Diskriminante von $k(\nu)$ als Faktor enthält. Wegen $n(\omega) = p^{\frac{l(l-1)}{2}}$ sind $\mathfrak{p}, s\mathfrak{p}, \ldots, s^{l-2}\mathfrak{p}$ zugleich die einzigen in ω aufgehenden Primideale. Es sei $\mathfrak{p}$ ein solcher unter diesen Primfaktoren, welcher in der Zahl ω zu einer möglichst niedrigen Potenz vorkommt; dann haben wir

$$\omega = \mathfrak{p}^{a_0 + a_1 s + \cdots + a_{l-2}s^{l-2}},$$

wo $a_0, a_1, \ldots, a_{l-2}$ positive ganze rationale Zahlen bedeuten, unter welchen keine kleiner als a_0 ist. Die Bildung von $n(\omega)$ ergibt

$$a_0 + a_1 + \cdots + a_{l-2} = \frac{l(l-1)}{2}.$$

Da $a_0, a_1, \ldots, a_{l-2}$ sämtlich > 0 sind, können hiernach diese Zahlen nicht sämtlich durch l teilbar sein. Zufolge der ersten im Satze 133 bewiesenen Eigenschaft wird

$$\omega^{s-r} = \mathfrak{p}^{(s-r)(a_0 + a_1 s + \cdots + a_{l-2}s^{l-2})} = \alpha^l,$$

wo α eine Zahl in $k(\zeta)$ ist. Da die zu $\mathfrak{p}$ konjugierten Primideale sämtlich von $\mathfrak{p}$ und untereinander verschieden sind, so folgt hieraus, daß die ganzzahlige Funktion

$$(s-r)(a_0 + a_1 s + \cdots + a_{l-2}s^{l-2})$$

der Veränderlichen s, wenn man nach Ausführung der Multiplikation s^{l-1} durch 1 ersetzt, lauter durch l teilbare Koeffizienten erhalten muß, d. h. diese Funktion ist $\equiv a_{l-2}(s^{l-1} - 1)$ nach l. Daraus ist zunächst $a_{l-2} \not\equiv 0$ nach l ersichtlich, und wenn $a_{l-2} \equiv r^{m-l+2}$ nach l gesetzt wird, wo m eine der Zahlen $0, 1, \ldots, l-2$ bedeute, so folgt für jeden Index $i = 0, 1, \ldots, l-2$ die Kongruenz

$$a_i \equiv r^{m-i}, \qquad (l).$$

Wir setzen allgemein $a_i = r_{m-i} + lb_i$ so, daß $0 < r_{m-i} < l$ und b_i eine ganze rationale Zahl ist; dabei wird stets $b_i \geqq 0$. Da

$$r_m + r_{m-1} + \cdots + r_{m-l+2} = 1 + 2 + \cdots + (l-1) = \frac{l(l-1)}{2}$$

ist, so folgt $b_0 + b_1 + \cdots + b_{l-2} = 0$, und daraus geht notwendig

$$b_0 = 0, \quad b_1 = 0, \ldots, b_{l-2} = 0$$

hervor, d. h.

$$a_i = r_{m-i} \quad \text{für} \quad i = 0, 1, \ldots, l-2.$$

Unter den Zahlen $r_0, r_1, \ldots, r_{l-2}$ ist offenbar $r_0 = 1$ die kleinste, und da a_0 unter den Koeffizienten $a_0, a_1, \ldots, a_{l-2}$ möglichst klein sein sollte, so folgt $a_0 = r_0 = 1$, d. h. $m = 0$, und nunmehr allgemein $a_i = r_{-i}$, womit der Satz 135 bewiesen ist.

§ 109. Eine Äquivalenz für die Primideale ersten Grades des Körpers der l-ten Einheitswurzeln.

Aus den bisherigen Entwicklungen entnehmen wir eine wichtige Eigenschaft der in einer Primzahl $p \equiv 1$ nach l aufgehenden Primideale des Körpers der l-ten Einheitswurzeln. Es gilt nämlich die Tatsache:

Satz 136. Es sei l eine ungerade Primzahl und $\zeta = e^{\frac{2i\pi}{l}}$, ferner r eine positive Primitivzahl nach l und $s = (\zeta : \zeta^r)$; wenn dann $\mathfrak{p}$ ein beliebiges Primideal ersten Grades in dem Kreiskörper $k(\zeta)$ bedeutet, so besteht die Äquivalenz

$$\mathfrak{p}^{q_0 + q_{-1}s + q_{-2}s^2 + \cdots + q_{-l+2}s^{l-2}} \sim 1,$$

wo die Größen q_{-i} ganze rationale, durch das Gleichungssystem

$$q_{-i} = \frac{r\,r_{-i} - r_{-i+1}}{l} \qquad (i = 0, 1, \ldots, l-2)$$

bestimmte, nicht negative Zahlen sind. Dabei haben $r_0, r_{-1}, \ldots, r_{-l+2}$ dieselbe Bedeutung wie in Satz 135, und es ist außerdem $r_1 = r_{-l+2}$. [Kummer (6, II)].

Beweis. Es mögen p und ω dieselbe Bedeutung wie in Satz 133 haben. Nach Satz 133 ist ω^{s-r} die l-te Potenz einer Zahl $\varkappa$ in $k(\zeta)$. Wenn wir für ω

die in Satz 135 gegebene Darstellung durch $\mathfrak{p}$ einführen, so folgt

$$\mathfrak{p}^{(s-r)(r_0+r_{-1}s+\cdots+r_{-l+2}s^{l-2})}=\alpha^l,$$

und diese Gleichung zeigt, wenn wir daraus die Zerlegung von α selbst ermitteln, die Richtigkeit des Satzes 136.

Ist C eine beliebige Idealklasse des Kreiskörpers $k(\zeta)$ und $\mathfrak{j}$ ein Ideal in C, und bezeichnen wir mit sC, s^2C, ..., $s^{l-2}C$ bez. die durch $s\mathfrak{j}$, $s^2\mathfrak{j}$, ..., $s^{l-2}\mathfrak{j}$ bestimmten Idealklassen, so folgt mit Hilfe des Satzes 89 aus Satz 136 unmittelbar die Tatsache:

$$C^{q_0}(sC)^{q_{-1}}(s^2C)^{q_{-2}}\ldots(s^{l-2}C)^{q_{-l+2}}=1.$$

§ 110. Die Konstruktion sämtlicher Normalbasen und Wurzelzahlen.

Die Sätze 133, 134 und 135 ermöglichen zunächst die Konstruktion sämtlicher Wurzelzahlen des Abelschen Körpers $k(\nu)$. Es gilt nämlich die Tatsache:

Satz 137. Bezeichnen Ω und Ω^* für den Abelschen Körper k vom ungeraden Primzahlgrade l mit der Diskriminante p^{l-1} zwei verschiedene, aber zu derselben erzeugenden Substitution t der Gruppe dieses Körpers gehörende Wurzelzahlen, so ist stets $\Omega^*=\varepsilon\Omega$, wo ε eine Einheit des Körpers $k(\zeta)$ bedeutet, welche die Kongruenzeigenschaft $\varepsilon\equiv\pm 1$ nach $\mathfrak{l}=(1-\zeta)$ besitzt. Umgekehrt, wenn ε eine Einheit dieser Art in $k(\zeta)$ und Ω für k irgendeine Wurzelzahl bezeichnet, so ist $\Omega^*=\varepsilon\Omega$ stets wiederum eine Wurzelzahl jenes Abelschen Körpers k.

Beweis. Unter den Voraussetzungen in der ersten Aussage ist der Quotient $\varepsilon=\frac{\Omega^*}{\Omega}$ eine Zahl des aus k und $k(\zeta)$ zusammengesetzten Körpers, welche beim Übergang von ζ, ν zu $\zeta, t\nu$ ungeändert bleibt und daher im Körper $k(\zeta)$ liegt. Für $\omega=\Omega^l$ werde der im Satze 135 enthaltene Ausdruck angenommen. Ist dann etwa $s^{-a}\mathfrak{p}$, wo a eine der Zahlen $0, 1, 2, \ldots l-2$ bedeute, dasjenige unter den $l-1$ konjugierten, in p aufgehenden Primidealen des Körpers $k(\zeta)$, welches in $\omega^*=\Omega^{*l}$ nur zur ersten Potenz vorkommt, so hat man nach Satz 135 offenbar

$$\omega^*=\mathfrak{p}^{s^{-a}(r_0+r_{-1}s+\cdots+r_{-l+2}s^{l-2})},$$

und hieraus folgt, daß das Primideal $\mathfrak{p}$ in ω^* genau zur r_{-a}-ten Potenz vorkommt. Der Quotient $\frac{\omega^*}{\omega}$ kann daher in die Gestalt eines Bruches gebracht werden, dessen Zähler das Primideal $\mathfrak{p}$ in der $(r_{-a}-r_0)$-ten Potenz enthält, während der Nenner zu $\mathfrak{p}$ prim ist. Da wegen $\frac{\omega^*}{\omega}=\varepsilon^l$ der Exponent $r_{-a}-r_0$ durch l teilbar sein muß, so folgt $r_{-a}=r_0$, d. h. $a=0$. Wegen dieses Umstandes enthalten ω und ω^* die nämlichen Potenzen von Primidealen, und ε ist somit eine Einheit.

Die übrigen Behauptungen des Satzes 137 gehen unmittelbar aus den Sätzen 133 und 134 hervor.

Aus den zu t gehörenden Wurzelzahlen gewinnt man leicht nach Formel (41) die sämtlichen Normalbasen $\nu, t\nu, \ldots, t^{l-1}\nu$ des Abelschen Körpers k.

§ 111. Die Lagrangesche Normalbasis und die Lagrangesche Wurzelzahl.

Es sei wieder l eine ungerade Primzahl, $\zeta=e^{\frac{2i\pi}{l}}$, ferner p eine rationale Primzahl von der Form $lm+1$, es werde $Z=e^{\frac{2i\pi}{p}}$ gesetzt, und es bezeichne R eine Primitivzahl nach p. Endlich bedeute k den Abelschen Körper l-ten Grades mit der Diskriminante p^{l-1}.

Die $p-1$ Zahlen $Z, Z^2, \ldots, Z^{p-1}$ bilden eine Normalbasis des Körpers $k(Z)$; aus dem Beweise des Hilfssatzes 20 geht dann hervor, daß die l Zahlen

$$\begin{aligned}
\lambda_0 &= Z + Z^{R^l} + Z^{R^{2l}} + \cdots + Z^{R^{(m-1)l}}\\
\lambda_1 &= Z^R + Z^{R^{l+1}} + Z^{R^{1+2l}} + \cdots + Z^{R^{1+(m-1)l}},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\lambda_{l-1} &= Z^{R^{l-1}} + Z^{R^{2l-1}} + Z^{R^{3l-1}} + \cdots + Z^{R^{ml-1}}
\end{aligned}$$

eine Normalbasis des Körpers k bilden. Aus dieser Normalbasis entspringt die folgende Wurzelzahl dieses Körpers:

$$\begin{aligned}
\Lambda &= \lambda_0+\zeta\lambda_1+\zeta^2\lambda_2+\cdots+\zeta^{l-1}\lambda_{l-1},\\
&= Z+\zeta Z^R+\zeta^2 Z^{R^2}+\cdots+\zeta^{p-2}Z^{R^{p-2}}.
\end{aligned}$$

Diese besondere Normalbasis $\lambda_0, \lambda_1, \ldots, \lambda_{l-1}$ soll die **Lagrangesche Normalbasis** und die besondere Wurzelzahl Λ die **Lagrangesche Wurzelzahl** heißen.

§ 112. Die charakteristischen Eigenschaften der Lagrangeschen Wurzelzahl.

Die Lagrangesche Wurzelzahl Λ des Körpers k zeichnet sich vor den übrigen Wurzelzahlen von k durch folgende Eigenschaften aus:

Satz 138. Wenn die l-te Potenz Λ^l der Lagrangeschen Wurzelzahl Λ gemäß Satz 135 durch die Formel

$$\Lambda^l=\mathfrak{p}^{r_0+r_{-1}s+r_{-2}s^2+\cdots+r_{-l+2}s^{l-2}}$$

dargestellt wird, so ist $\mathfrak{p}$ das durch die Formel

$$\mathfrak{p}=(p,\ \zeta-R^{-m}),\quad\left(m=\frac{p-1}{l}\right)$$

bestimmte Primideal; die Zeichen sind im übrigen wie in Satz 135 zu verstehen. Die Lagrangesche Wurzelzahl Λ ist $\equiv -1$ nach $\mathfrak{l}$ und hat ferner die Eigenschaft, daß ihr absoluter Betrag $= |\sqrt{p}|$ ist.

Umgekehrt, wenn einer Wurzelzahl Ω die letzteren Eigenschaften zukommen und außerdem Ω^l gerade das soeben definierte Primideal $\mathfrak{p}$ zur ersten Potenz enthält, so ist $\Omega = \zeta^* \Lambda$, wo ζ^* eine l-te Einheitswurzel bedeutet.

Beweis. Wird $\mathfrak{P} = (1 - Z, \mathfrak{p})$ gesetzt, so erkennen wir mit Hilfe der Beziehungen $(1 - Z)^{p-1} = (p)$ und $(p, \mathfrak{p}^{p-1}) = \mathfrak{p}$, daß

$$\mathfrak{P}^{p-1} = (p, (1 - Z)^{p-2}\mathfrak{p}, \ldots, \mathfrak{p}^{p-1}) = \mathfrak{p}$$

wird; hieraus ist ersichtlich, daß $\mathfrak{P}$ in dem durch ζ und Z bestimmten Körper ein Primideal ist, und daß die Zahl $1-Z$ dieses Primideal $\mathfrak{P}$ nur zur ersten Potenz enthält. Setzen wir $Z = 1 + \Pi$ und berücksichtigen die Kongruenz $\zeta \equiv R^{-m}$ nach $\mathfrak{p}$ und die Gleichung $(1 + \Pi)^p = 1$, so wird:

$$\Lambda \equiv \sum_{(x)} R^{-mx}(1 + \Pi)^{R^x}, \qquad (\mathfrak{p})$$

$$\equiv \sum_{(X)}{}' \left\{ X^{-m} \sum_{(Y)}{}' \binom{X}{Y} \Pi^Y \right\}, \qquad (\mathfrak{p}),$$

wo die bezüglichen Summen über $x = 0, 1, 2, \ldots, p-2$; $X = 1, 2, \ldots, p-1$, $Y = 0, 1, 2, \ldots, X$ zu erstrecken sind. Aus der letzteren Formel gewinnen wir, wenn wir die Reihenfolge der Summationen umkehren, die Kongruenz:

$$\Lambda \equiv -\frac{\Pi^m}{m!}, \qquad (\mathfrak{P}^{m+1}). \tag{43}$$

Die Lagrangesche Wurzelzahl Λ enthält also genau die m-te Potenz von $\mathfrak{P}$ als Faktor, und folglich ist Λ^l nur durch die erste Potenz von $\mathfrak{p}$ teilbar.

Bezeichnen wir die zu Λ konjugiert imaginäre Zahl mit $\overline{\Lambda}$, so ist

$$\overline{\Lambda} = Z^{-1} + \zeta^{-1} Z^{-R} + \zeta^{-2} Z^{-R^2} + \cdots + \zeta^{-p+2} Z^{-R^{p-2}};$$

dann wird, wenn wir im Produkt $\Lambda\overline{\Lambda}$ immer die je $p-1$ mit gleicher Potenz von ζ multiplizierten Glieder zusammennehmen,

$$\begin{aligned}
\Lambda\overline{\Lambda} = {} & (1 + 1 + \cdots + 1) \\
& + \zeta \,(Z^{R-1} + Z^{R^2-R} + \cdots + Z^{R^{p-1}-R^{p-2}}) \\
& + \zeta^2 (Z^{R^2-1} + Z^{R^3-R} + \cdots + Z^{R^p - R^{p-2}}) \\
& \cdots\cdots\cdots\cdots\cdots\cdots \\
& + \zeta^{p-2}(Z^{R^{p-2}-1} + Z^{R^{p-1}-R} + \cdots + Z^{R^{2p-4}-R^{p-2}}) \\
= {} & p - 1 - (\zeta + \zeta^2 + \cdots + \zeta^{p-2}) = p.
\end{aligned}$$

Damit ist der erste Teil des Satzes 138 vollständig bewiesen.

Der zweite Teil ist wesentlich die Umkehrung des ersten; die Richtigkeit des zweiten Teiles folgt ohne Mühe aus den Sätzen 135 und 137, wenn man überdies den Satz 48 heranzieht; man hat dabei zu beachten, daß, wenn eine Zahl eines Abelschen Zahlkörpers den absoluten Betrag 1 hat, diese Eigenschaft stets auch den zu ihr konjugierten Zahlen zukommt.

In entsprechender Weise wie die Kongruenz (43) können wir die sämtlichen folgenden Kongruenzen ableiten [Jacobi (3)]:

$$s^{-i}\Lambda \equiv -\frac{\Pi^{r-im}}{(r-im)!}, \qquad \mathfrak{P}^{r-im+1} \tag{44}$$

für $i = 0, 1, 2, \ldots, l-2$. Berücksichtigen wir die Tatsache, daß $\Lambda \equiv -1$ nach $\mathfrak{l}$ und $|\Lambda| = |\sqrt{p}|$ ist, so entspringt aus diesen Kongruenzen (44) ein anderer Beweis der Sätze 135 und 136 [Kummer (6, 11)].

Die sämtlichen Sätze und Beweise in diesem Kapitel 24 gelten entsprechend auch für $l = 2$, nur daß dann die Diskriminante des Abelschen Körpers k den Wert $d = (-1)^{\frac{p-1}{2}} p$ bekommt.

Die Lagrangesche Wurzelzahl Λ des Körpers k ist eine ganze Zahl des aus $k(\zeta)$ und k zusammengesetzten Körpers, welche durch die in den Sätzen 133 und 138 aufgezählten Eigenschaften bis auf den Faktor ζ^* völlig bestimmt ist. Um endlich auch diesen Faktor ζ^* festzulegen, müßte man $\Lambda = |\sqrt{p}|\, e^{2i\pi\varphi}$ setzen derart, daß $0 \leqq \varphi < 1$ sei, und dann entscheiden, in welchem der l Intervalle

$$0 \leqq \varphi < \frac{1}{l}, \quad \frac{1}{l} \leqq \varphi < \frac{2}{l}, \quad \ldots, \quad \frac{l-1}{l} \leqq \varphi < 1$$

die betreffende Zahl φ gelegen ist. Aus dieser Frage entsteht in dem besonderen Falle, daß statt l die Primzahl 2 gewählt wird, das berühmte Problem der Bestimmung des Vorzeichens der Gaußschen Summen. Vgl. § 124. Für den Fall $l = 3$ werden wir auf eine von Kummer in Angriff genommene Aufgabe geführt [Kummer (2, 4)].

Die Zahlen der Lagrangeschen Normalbasis werden gewöhnlich „Perioden“ genannt. Die Literatur weist eine Reihe von Abhandlungen auf, welche sich mit diesen Perioden, sowie mit verwandten ganzen Zahlen von Kreiskörpern beschäftigen [Kummer (3, 17), Fuchs (1, 2), Schwering (1, 3, 4), Kronecker (17), Smith (1)]. In der Literatur finden sich noch Untersuchungen über besondere Kreiskörper [Berkenbusch (1), Eisenstein (10), Schwering (2), Weber (1, 2, 4), Wolfskehl (1)]. Auch sei hier erwähnt, daß, wenn die Primzahl $l < 100$ und nicht 29 oder 41 ist, der Kreiskörper $k(\zeta)$ stets eine solche Idealklasse enthält, deren Potenzen alle Klassen des Körpers liefern [Kummer (11, 13)].

25. Das Reziprozitätsgesetz für l-te Potenzreste zwischen einer rationalen Zahl und einer Zahl des Körpers der l-ten Einheitswurzeln.

§ 113. Der Potenzcharakter einer Zahl und das Symbol $\left\{\frac{\alpha}{\mathfrak{p}}\right\}$.

Es sei l eine ungerade Primzahl, $\zeta = e^{\frac{2i\pi}{l}}$, und $k(\zeta)$ bezeichne den durch ζ bestimmten Kreiskörper. Ist dann p eine rationale, von l verschiedene Primzahl und $\mathfrak{p}$ ein in p aufgehendes Primideal in $k(\zeta)$, und ist f der Grad von $\mathfrak{p}$, so gilt nach Satz 24 für jede nicht durch $\mathfrak{p}$ teilbare ganze Zahl α des Körpers $k(\zeta)$ die Kongruenz

$$\alpha^{p^f-1} - 1 \equiv 0, \qquad (\mathfrak{p}).$$

Da $p^f - 1$ nach Satz 119 durch l teilbar ist, so gestattet die linke Seite dieser Kongruenz die Zerlegung

$$\alpha^{p^f-1} - 1 = \prod_{(c)} \left(\alpha^{\frac{p^f-1}{l}} - \zeta^c\right),$$

wo das Produkt über die Werte $c = 0, 1, \ldots, l-1$ zu erstrecken ist. Hieraus folgt, daß für einen und jedenfalls auch nur einen Wert c die Kongruenz

$$\alpha^{\frac{p^f-1}{l}} \equiv \zeta^c, \qquad (\mathfrak{p})$$

erfüllt ist. Man nennt die hier auftretende Einheitswurzel ζ^c den **Potenzcharakter der Zahl α in Bezug auf das Primideal $\mathfrak{p}$** im Körper $k(\zeta)$ und bezeichnet diese Einheitswurzel ζ^c durch das **Symbol**

$$\left\{\frac{\alpha}{\mathfrak{p}}\right\},$$

so daß die Kongruenz

$$\alpha^{\frac{p^f-1}{l}} \equiv \left\{\frac{\alpha}{\mathfrak{p}}\right\}, \qquad (\mathfrak{p}) \tag{45}$$

gilt [Kummer (*10*)].

Sind α und β zwei durch $\mathfrak{p}$ nicht teilbare ganze Zahlen in $k(\zeta)$, so besteht, wie hieraus leicht ersichtlich, die Gleichung

$$\left\{\frac{\alpha\beta}{\mathfrak{p}}\right\} = \left\{\frac{\alpha}{\mathfrak{p}}\right\}\left\{\frac{\beta}{\mathfrak{p}}\right\}.$$

Wenn insbesondere die ganze Zahl α nach dem Primideal $\mathfrak{p}$ der l-ten Potenz einer ganzen Zahl in $k(\zeta)$ kongruent ist, so heißt α ein l-ter **Potenzrest nach dem Primideal $\mathfrak{p}$**. Es gilt die Tatsache:

Satz 139. Bedeutet $\mathfrak{p}$ ein von $\mathfrak{l} = (1-\zeta)$ verschiedenes Primideal und α eine ganze zu $\mathfrak{p}$ prime Zahl in $k(\zeta)$, so ist α dann und nur dann l-ter Potenzrest nach $\mathfrak{p}$, wenn $\left\{\frac{\alpha}{\mathfrak{p}}\right\} = 1$ ausfällt.

Beweis. Ist $\alpha \equiv \beta^l$ nach $\mathfrak{p}$, wo β wieder eine Zahl in $k(\zeta)$ bedeutet, so folgt $\alpha^{\frac{p^f-1}{l}} \equiv \beta^{p^f-1} \equiv 1$ nach $\mathfrak{p}$, d. h. $\left\{\frac{\alpha}{\mathfrak{p}}\right\} = 1$. Um die Umkehrung hiervon zu zeigen, bezeichnen wir mit ϱ eine Primitivzahl nach $\mathfrak{p}$ und setzen $\alpha \equiv \varrho^h$ nach $\mathfrak{p}$. Nehmen wir $\alpha^{\frac{p^f-1}{l}} \equiv \varrho^{\frac{h(p^f-1)}{l}} \equiv 1$ an, so folgt $\frac{h(p^f-1)}{l} \equiv 0$ nach $p^f - 1$, d. h. h ist durch l teilbar, und folglich ist α ein l-ter Potenzrest nach $\mathfrak{p}$, was zu beweisen war.

Für eine Primitivzahl ϱ nach $\mathfrak{p}$ ist der Potenzcharakter $\left\{\frac{\varrho}{\mathfrak{p}}\right\}$ sicherlich von 1 verschieden. Denn in der Reihe der Potenzen $\varrho, \varrho^2, \ldots$ ist ϱ^{p^f-1} die erste, welche $\equiv 1$ nach $\mathfrak{p}$ ausfällt, und also ist $\varrho^{\frac{p^f-1}{l}} \not\equiv 1$ nach $\mathfrak{p}$.

Es sei $\left\{\frac{\varrho}{\mathfrak{p}}\right\} = \zeta^g$; man bestimme eine zu $p^f - 1$ prime ganze rationale Zahl g^* derart, daß $gg^* \equiv 1$ nach l wird; dann ist offenbar $\varrho^* \equiv \varrho^{g^*}$ eine solche Primitivzahl nach $\mathfrak{p}$, für welche $\left\{\frac{\varrho^*}{\mathfrak{p}}\right\} = \zeta$ ausfällt. Ist nun α eine ganze, nicht durch $\mathfrak{p}$ teilbare Zahl in $k(\zeta)$, und hat man $\alpha \equiv \varrho^{*c}$ nach $\mathfrak{p}$, so besitzt α den Potenzcharakter ζ^c.

Hieraus ist leicht ersichtlich, daß das vollständige System der $p^f - 1$ einander nach $\mathfrak{p}$ inkongruenten Zahlen $1, \varrho^*, \varrho^{*2}, \ldots, \varrho^{*p^f-2}$ in l Teilsysteme zerfällt, von denen jedes $\frac{p^f-1}{l}$ Zahlen vom nämlichen Potenzcharakter enthält. Insbesondere gibt es genau $\frac{p^f-1}{l}$ einander inkongruente l-te Potenzreste nach $\mathfrak{p}$.

Ist $\mathfrak{b}$ ein beliebiges zu $\mathfrak{l}$ primes Ideal und α eine zu $\mathfrak{b}$ prime ganze Zahl in $k(\zeta)$, und wird $\mathfrak{b} = \mathfrak{p}\mathfrak{q}\ldots\mathfrak{w}$ gesetzt, wo $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{w}$ Primideale bedeuten, so werde das Symbol $\left\{\frac{\alpha}{\mathfrak{b}}\right\}$ durch die Gleichung

$$\left\{\frac{\alpha}{\mathfrak{b}}\right\} = \left\{\frac{\alpha}{\mathfrak{p}}\right\}\left\{\frac{\alpha}{\mathfrak{q}}\right\}\ldots\left\{\frac{\alpha}{\mathfrak{w}}\right\}$$

definiert.

§ 114. Ein Hilfssatz über den Potenzcharakter der l-ten Potenz der Lagrangeschen Wurzelzahl.

Es ist Eisenstein gelungen, dasjenige Reziprozitätsgesetz zu entdecken und zu beweisen, welches im Körper $k(\zeta)$ zwischen einer rationalen Zahl und einer beliebigen Zahl dieses Körpers besteht; dabei ist wieder $\zeta = e^{\frac{2i\pi}{l}}$ gesetzt, und l bedeutet eine ungerade Primzahl. Dieses Reziprozitätsgesetz ist zugleich ein bisher unentbehrliches Hilfsmittel zum Beweise des allgemeineren Kummerschen Reziprozitätsgesetzes (vgl. Kap. 31). Dem Beweise des Eisensteinschen Reziprozitätsgesetzes ist der folgende Hilfssatz vorauszuschicken:

Hilfssatz 21. Es sei $\zeta = e^{\frac{2i\pi}{l}}$; ferner bedeute p eine von l verschiedene rationale Primzahl von der Form $p = ml + 1$, R eine Primitivzahl nach p und $\mathfrak{p}$ das Primideal ersten Grades in $k(\zeta)$:

$$\mathfrak{p} = (p, \zeta - R^m);$$

es werde $Z = e^{\frac{2i\pi}{p}}$, die Lagrangesche Wurzelzahl

$$\Lambda = Z + \zeta Z^R + \zeta^2 Z^{R^2} + \cdots + \zeta^{p-2} Z^{R^{p-2}}$$

und $\pi = \Lambda^l$ gesetzt. Endlich bedeute q eine beliebige, von l und p verschiedene rationale Primzahl, $\mathfrak{q}$ ein in q aufgehendes Primideal des Körpers $k(\zeta)$ und g den Grad von $\mathfrak{q}$: dann drückt sich der Potenzcharakter der Zahl $\pi = \Lambda^l$ in bezug auf das Ideal $\mathfrak{q}$ durch die Formel aus

$$\left\{\frac{\pi}{\mathfrak{q}}\right\} = \left\{\frac{q}{\mathfrak{p}}\right\}^g.$$

Beweis. Durch g-maliges Erheben in die q-te Potenz folgt die Kongruenz

$$\Lambda^{q^g} \equiv Z^{q^g} + \zeta^{q^g} Z^{R\,q^g} + \zeta^{2\,q^g} Z^{R^2 q^g} + \cdots + \zeta^{(p-2)q^g} Z^{R^{p-2}q^g}, \quad (q). \tag{46}$$

Berücksichtigen wir, daß dem Satze 119 zufolge $q^g \equiv 1$ nach l ist, und setzen $q^g \equiv R^h$ nach p, so wird die rechte Seite der Kongruenz (46)

$$Z^{R^h} + \zeta Z^{R^{h+1}} + \zeta^2 Z^{R^{h+2}} + \cdots + \zeta^{p-2} Z^{R^{h+p-2}} = \zeta^{-h}\Lambda.$$

Hieraus folgt, da Λ wegen des Satzes 138 prim zu q ist, die Kongruenz

$$\Lambda^{q^g-1} \equiv \zeta^{-h}, \qquad (q),$$

und also ist auch gewiß

$$\Lambda^{q^g-1} = \pi^{\frac{q^g-1}{l}} \equiv \zeta^{-h}, \qquad (\mathfrak{q}),$$

d. h. es wird

$$\left\{\frac{\pi}{\mathfrak{q}}\right\} = \zeta^{-h}. \tag{47}$$

Andererseits entnimmt man aus den Kongruenzen $q^g \equiv R^h$ nach p und $R^m \equiv \zeta^{-1}$ nach $\mathfrak{p}$ die Beziehungen:

$$q^{\frac{g(p-1)}{l}} = q^{g\,m} \equiv R^{h\,m} \equiv \zeta^{-h}, \qquad (\mathfrak{p}),$$

d. h. es ist

$$\left\{\frac{q^g}{\mathfrak{p}}\right\} = \left\{\frac{q}{\mathfrak{p}}\right\}^g = \zeta^{-h}; \tag{48}$$

die Gleichungen (47) und (48) zusammen ergeben den Hilfssatz 21.

§ 115. Beweis des Reziprozitätsgesetzes im Körper $k(\zeta)$ zwischen einer rationalen und einer beliebigen Zahl.

Es bedeute $\mathfrak{l} = (1 - \zeta)$ das in l aufgehende Primideal des Körpers $k(\zeta)$. Eine ganze Zahl α des Körpers $k(\zeta)$ heiße **semiprimär**, wenn sie zu $\mathfrak{l}$ prim und nach $\mathfrak{l}^2$ einer ganzen rationalen Zahl kongruent ist. Eine ganze rationale, nicht durch l teilbare Zahl ist hiernach stets semiprimär. Eine beliebige ganze, nicht durch $\mathfrak{l}$ teilbare Zahl α des Körpers $k(\zeta)$ kann durch Multiplikation mit einer geeigneten Potenz der Einheitswurzel ζ stets in eine semiprimäre Zahl verwandelt werden. Ist nämlich

$$\alpha \equiv a + b(1 - \zeta), \qquad (\mathfrak{l}^2),$$

wo a und b ganze rationale Zahlen bedeuten, so ist

$$\zeta^{b^*} \cdot \alpha \equiv a, \qquad (\mathfrak{l}^2),$$

wenn b^* aus der Kongruenz $ab^* \equiv b$ nach l bestimmt wird. Die Zahl $\zeta^{b^*} \cdot \alpha$ ist mithin semiprimär.

Nach dieser Vorbemerkung läßt sich nunmehr das Eisensteinsche Reziprozitätsgesetz, wie folgt, aussprechen:

Satz 140. Wenn a eine beliebige ganze rationale, nicht durch die ungerade Primzahl l teilbare Zahl und α eine beliebige semiprimäre und zu a prime ganze Zahl des Körpers $k(\zeta)$ der l-ten Einheitswurzeln ist, so gilt in diesem Körper die Reziprozitätsgleichung

$$\left\{\frac{a}{\alpha}\right\} = \left\{\frac{\alpha}{a}\right\}.$$

[Eisenstein (2)].

Beweis. Wir verstehen unter r eine Primitivzahl nach l und schreiben $s = (\zeta : \zeta^r)$. Es werde zunächst angenommen, daß $a = q$ eine rationale Primzahl ist, und daß die Zahl α nur Primideale ersten Grades enthält. Es sei $\mathfrak{q}$ ein in q aufgehendes Primideal in $k(\zeta)$ und g der Grad von $\mathfrak{q}$, ferner sei p eine in der Norm $n(\alpha)$ vorkommende rationale Primzahl, und es mögen $\mathfrak{p}$ und π dazu die gleiche Bedeutung wie in Hilfssatz 21 haben. Ist nun s^u eine beliebige Potenz der Substitution s, und wenden wir den Hilfssatz 21 auf die Primideale $s^{-u}\mathfrak{q}$ und $\mathfrak{p}$ an, so ergibt sich:

$$\left\{\frac{\pi}{s^{-u}\mathfrak{q}}\right\} = \left\{\frac{q}{\mathfrak{p}}\right\}^g.$$

Unterwerfen wir diese Gleichung der Substitution s^u, so folgt:

$$\left\{\frac{s^u\pi}{\mathfrak{q}}\right\} = \left\{\frac{q}{s^u\mathfrak{p}}\right\}^g. \tag{49}$$

Die in der Norm $n(\alpha)$ vorkommenden, voneinander verschiedenen rationalen Primzahlen seien $p = ml + 1$, $p^* = m^*l + 1, \ldots$; ferner mögen $R, R^*, \ldots$ bez. Primitivzahlen nach $p, p^*, \ldots$ bedeuten; endlich werde

$$\mathfrak{p} = (p, \zeta - R^m), \qquad \mathfrak{p}^* = (p^*, \zeta - R^{*m^*}), \ \ldots$$

gesetzt, und es gestatte die Zahl α die Zerlegung

$$\alpha = \mathfrak{p}^{F(s)}\mathfrak{p}^{*F^*(s)}\ldots,$$

wo die Exponenten $F, F^*, \ldots$ ganzzahlige Funktionen in s vom Grade $l - 2$ mit lauter Koeffizienten, die $\geqq 0$ sind, bedeuten.

Bezeichnen dann $\Lambda, \Lambda^*, \ldots$ die bezüglichen, zu den Primzahlen $p, p^*, \ldots$ und deren Primitivzahlen $R, R^*, \ldots$ gehörigen Lagrangeschen Wurzelzahlen, und wird $\pi = \Lambda^l, \pi^* = \Lambda^{*l}, \ldots$ gesetzt, so gelten nach Satz 138 die Zerlegungen:

$$\pi = \mathfrak{p}^{r_0 + r_{-1}s + r_{-2}s^2 + \cdots + r_{-l+2}s^{l-2}},$$
$$\pi^* = \mathfrak{p}^{*r_0 + r_{-1}s + r_{-2}s^2 + \cdots + r_{-l+2}s^{l-2}},$$
$$\cdots\cdots\cdots\cdots$$

wo r_{-h} die kleinste positive ganze rationale Zahl bedeutet, welche der $-h$-ten Potenz r^{-h} der Primitivzahl r nach l kongruent ist. Der Quotient

$$\varepsilon = \frac{\alpha^{r_0 + r_{-1}s + r_{-2}s^2 + \cdots + r_{-l+2}s^{l-2}}}{\pi^{F(s)}\pi^{*F^*(s)}\ldots}$$

ist daher offenbar eine Einheit des Körpers $k(\zeta)$. Wir wollen beweisen, daß diese Einheit $\varepsilon = \pm 1$ ist. Zu dem Zwecke bilden wir den Ausdruck

$$|\varepsilon|^2 = \varepsilon^{1+s^{\frac{l-1}{2}}} = \frac{\alpha^{\left(1+s^{\frac{l-1}{2}}\right)(r_0 + r_{-1}s + \cdots + r_{-l+2}s^{l-2})}}{(|\pi|^2)^{F(s)}(|\pi^*|^2)^{F^*(s)}\ldots}.$$

Wegen der für $h = 0, 1, 2, \ldots, \frac{l-3}{2}$ gültigen Gleichung

$$r_{-h} + r_{-h-\frac{l-1}{2}} = l$$

wird der Zähler des Bruches rechter Hand

$$\alpha^{\left(1+s^{\frac{l-1}{2}}\right)(r_0 + r_{-1}s + \cdots + r_{-l+2}s^{l-2})} = \alpha^{l(1+s+\cdots+s^{l-2})} = (n(\alpha))^l.$$

Berücksichtigen wir, daß nach Satz 138 $|\pi|^2 = p^l, |\pi^*|^2 = p^{*l}, \ldots$ wird, so ergibt sich $|\varepsilon| = 1$. Nach Satz 48 ist folglich ε bis auf einen Faktor ± 1 eine Potenz der Einheitswurzel ζ. Da andererseits nach Satz 138 die Kongruenzen

$$\pi \equiv -1, \quad \pi^* \equiv -1, \ \ldots, \ (\mathfrak{l}^l)$$

bestehen, und daher $\pi, \pi^*, \ldots$ sämtlich semiprimäre Zahlen sind, so ist auch ε eine semiprimäre Zahl; mithin wird $\varepsilon = \pm 1$, und es folgt demnach:

$$\alpha^{r_0 + r_{-1}s + \cdots + r_{-l+2}s^{l-1}} = \pm \pi^{F(s)}\pi^{*F^*(s)}\ldots.$$

Diese Gleichung liefert unter Anwendung der Formel (49) die Reziprozitätsgleichung

$$\left\{\frac{\alpha^{r_0 + r_{-1}s + \cdots + r_{-l+2}s^{l-2}}}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{p}^{F(s)}\mathfrak{p}^{*F^*(s)}\ldots}\right\}^g = \left\{\frac{\mathfrak{q}}{\alpha}\right\}^g. \tag{50}$$

Berücksichtigen wir, daß

$$\left\{\frac{s\alpha}{\mathfrak{q}}\right\} = \left\{\frac{\alpha}{s^{-1}\mathfrak{q}}\right\}^r, \quad \left\{\frac{s^2\alpha}{\mathfrak{q}}\right\} = \left\{\frac{\alpha}{s^{-2}\mathfrak{q}}\right\}^{r^2}, \ \ldots, \ \left\{\frac{s^{l-2}\alpha}{\mathfrak{q}}\right\} = \left\{\frac{\alpha}{s^{-l+2}\mathfrak{q}}\right\}^{r^{l-2}}$$

ist, da ja die Symbole Potenzen von ζ darstellen, so folgt aus (50) die Gleichung

$$\left\{\frac{\alpha}{\mathfrak{q}^g}\right\} = \left\{\frac{\mathfrak{q}}{\alpha}\right\}^g \quad \text{oder} \quad \left\{\frac{\alpha}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\alpha}\right\};$$

damit ist der Satz 140 unter den zunächst gemachten Einschränkungen, daß α nur Primideale ersten Grades enthält und a eine Primzahl ist, bewiesen.

Um die erstere Einschränkung zu beseitigen, nehmen wir jetzt an, es sei α eine beliebige semiprimäre, zu q prime ganze Zahl in $k(\zeta)$, welche auch Primideale von höherem als erstem Grade enthalten kann. Wir bilden dann die Zahl

$$\beta = \alpha^{\prod_{(\varepsilon)}(1-\varepsilon^\varepsilon)},$$

wo das im Exponenten stehende Produkt über sämtliche von $l-1$ verschiedene Teiler e der Zahl $l-1$ zu erstrecken ist, und setzen

$$\beta = \frac{\mathfrak{j}}{\mathfrak{k}}$$

in solcher Weise, daß $\mathfrak{j}$ und $\mathfrak{k}$ zueinander prime Ideale bedeuten; dieselben enthalten dann, wie leicht ersichtlich, nur Primideale ersten Grades als Faktoren, und sie sind überdies nicht durch $\mathfrak{l}$ teilbar. Ist h die Anzahl der Idealklassen des Körpers $k(\zeta)$, so wird nach Satz 51 $\mathfrak{k}^h = (\varkappa)$, wo $\varkappa$ eine ganze Zahl in $k(\zeta)$ bedeutet; setzen wir $\gamma = \beta\varkappa^l$, so wird auch γ eine ganze Zahl in $k(\zeta)$, welche nur Primideale ersten Grades als Primfaktoren enthält, und überdies ist offenbar γ ebenso wie α semiprimär und zu q prim. Nach dem oben Bewiesenen ist daher

$$\left\{\frac{\gamma}{q}\right\} = \left\{\frac{q}{\gamma}\right\}. \tag{51}$$

Der einfacheren Darstellung halber wollen wir nun allgemein, wenn ϱ, σ zwei ganze zu q prime Zahlen in $k(\zeta)$ bedeuten,

$$\frac{\left\{\frac{\varrho}{q}\right\}}{\left\{\frac{\sigma}{q}\right\}} = \left\{\frac{\frac{\varrho}{\sigma}}{q}\right\} \quad \text{und} \quad \frac{\left\{\frac{q}{\varrho}\right\}}{\left\{\frac{q}{\sigma}\right\}} = \left\{\frac{q}{\frac{\varrho}{\sigma}}\right\}$$

schreiben, was zu keinem Widerspruche mit den bisherigen Festsetzungen führt; dann folgt wegen $\beta = \frac{\gamma}{\varkappa^l}$ aus (51) offenbar die Gleichung

$$\left\{\frac{\beta}{q}\right\} = \left\{\frac{q}{\beta}\right\}. \tag{52}$$

Berücksichtigen wir die Gleichungen

$$\left\{\frac{s^u\alpha}{q}\right\} = \left\{\frac{\alpha}{q}\right\}^{r^u} \quad \text{und} \quad \left\{\frac{q}{s^u\alpha}\right\} = \left\{\frac{q}{\alpha}\right\}^{r^u},$$

so erkennen wir aus (52), daß

$$\left\{\frac{\alpha}{q}\right\}^{\prod_{(\varepsilon)}(1-r^\varepsilon)} = \left\{\frac{q}{\alpha}\right\}^{\prod_{(\varepsilon)}(1-r^\varepsilon)}$$

wird. Wenn wir bedenken, daß das auf beiden Seiten als Exponent stehende

Produkt nicht durch l teilbar ist, so ergibt sich hieraus

$$\left\{\frac{\alpha}{q}\right\} = \left\{\frac{q}{\alpha}\right\}.$$

Wird endlich auch die ganze rationale durch l nicht teilbare Zahl a beliebig angenommen, nur so, daß a zu α prim ist, und wird $a = q\,q^* \ldots$ gesetzt, wo $q, q^*, \ldots$ rationale Primzahlen bedeuten, so folgt durch Multiplikation der Gleichungen

$$\left\{\frac{q}{\alpha}\right\} = \left\{\frac{\alpha}{q}\right\}, \quad \left\{\frac{q^*}{\alpha}\right\} = \left\{\frac{\alpha}{q^*}\right\}, \ldots$$

die Richtigkeit des Satzes 140 im allgemeinsten Falle.

26. Die Bestimmung der Anzahl der Idealklassen im Kreiskörper der m-ten Einheitswurzeln.

§ 116. Das Symbol $\left[\frac{a}{L}\right]$.

Um die in § 26 dargelegte transzendente Methode zur Bestimmung der Klassenanzahl eines Körpers auf den Fall des Kreiskörpers $k\left(e^{\frac{2i\pi}{m}}\right)$, wo m irgendeine ganze rationale Zahl bedeutet, anzuwenden, definieren wir zunächst die folgenden **Symbole**:

Es sei l^h eine Potenz einer ungeraden Primzahl l mit positivem Exponenten und r eine Primitivzahl nach l^h. Ist dann a eine nicht durch l teilbare ganze rationale Zahl und a' dazu ein solcher Exponent, daß die Kongruenz

$$r^{a'} \equiv a, \qquad (l^h)$$

gilt, so definieren wir

$$\left[\frac{a}{l^h}\right] = e^{\frac{2i\pi a'}{l^{h-1}(l-1)}}.$$

Ferner setzen wir

$$\left[\frac{a}{l^h}\right] = 0,$$

sobald a durch l teilbar ist. Sind a, b zwei beliebige ganze rationale Zahlen, so wird dann offenbar

$$\left[\frac{ab}{l^h}\right] = \left[\frac{a}{l^h}\right]\left[\frac{b}{l^h}\right].$$

Des weiteren setzen wir, wenn a eine ungerade Zahl bedeutet, zunächst

$$\left[\frac{a}{2^2}\right] = (-1)^{\frac{a-1}{2}};$$

ferner für ein $h > 2$, wenn a' eine solche ganze rationale Zahl zu a ist, daß die Kongruenz

$$5^{a'} \equiv \pm a, \qquad (2^h)$$

gilt,

$$\left[\frac{a}{2^h}\right] = e^{\frac{2i\pi a'}{2^{h-2}}}.$$

Bedeutet endlich a eine gerade Zahl, so setzen wir

$$\left[\frac{a}{2^2}\right] = 0, \qquad \left[\frac{a}{2^h}\right] = 0, \qquad (h > 2).$$

Sind a, b irgend zwei ganze rationale Zahlen, so gelten dann, wie man sieht, die Gleichungen

$$\left[\frac{ab}{2^h}\right] = \left[\frac{a}{2^h}\right]\left[\frac{b}{2^h}\right], \qquad (h > 1).$$

Durch diese Festsetzungen ist das Symbol $\left[\frac{a}{L}\right]$ vollständig für den Fall definiert, daß a eine beliebige ganze rationale Zahl und L eine höhere Potenz von 2 als die erste oder eine Potenz einer ungeraden Primzahl bedeutet, wobei im letzteren Falle irgendeine Primitivzahl r nach L von vornherein zugrunde zu legen ist.

Sind $l_1^{h_1}, l_2^{h_2}, \ldots$ irgendwelche fest gegebene Potenzen verschiedener ungerader Primzahlen und 2^{h^*} eine Potenz von 2, die größer als 2^2 ist, so setzen wir zur Abkürzung

$$\left[\frac{a}{u_1, u_2, \ldots}\right] = \left[\frac{a}{l_1^{h_1}}\right]^{u_1}\left[\frac{a}{l_2^{h_2}}\right]^{u_2}\cdots,$$

ferner

$$\left[\frac{a}{u;\, u_1, u_2, \ldots}\right] = \left[\frac{a}{2^2}\right]^{u}\left[\frac{a}{l_1^{h_1}}\right]^{u_1}\left[\frac{a}{l_2^{h_2}}\right]^{u_2}\cdots,$$

ferner

$$\left[\frac{a}{u, u^*; u_1, u_2, \ldots}\right] = \left[\frac{a}{2^2}\right]^{u}\left[\frac{a}{2^{h^*}}\right]^{u^*}\left[\frac{a}{l_1^{h_1}}\right]^{u_1}\left[\frac{a}{l_2^{h_2}}\right]^{u_2}\cdots;$$

darin soll a eine beliebige ganze rationale Zahl, und die Exponenten u, u^*; $u_1, u_2, \ldots$ sollen ganze rationale, nicht negative Zahlen vorstellen. Endlich setzen wir fest, daß das Zeichen $\left[\frac{a}{L}\right]^0$ stets den Wert 1 bedeuten soll, auch wenn $\left[\frac{a}{L}\right] = 0$ ist.

§ 117. Die Ausdrücke für die Klassenanzahl im Kreiskörper der m-ten Einheitswurzeln.

Es gilt der folgende Satz, dessen Beweis in § 118 gegeben werden wird:

Satz 141. Es sei m eine ganze rationale positive Zahl von der Gestalt

$$m = l_1^{h_1} l_2^{h_2} \ldots, \quad \text{oder} \quad = 2^2 l_1^{h_1} l_2^{h_2} \ldots, \quad \text{oder} \quad = 2^{h^*} l_1^{h_1} l_2^{h_2} \ldots$$
$$(h^* > 2,\ h_1 > 0,\ h_2 > 0, \ldots),$$

wo $l_1, l_2, \ldots$ voneinander verschiedene ungerade Primzahlen bedeuten. Es seien ferner $r_1, r_2, \ldots$ Primitivzahlen bez. nach $l_1^{h_1}, l_2^{h_2}, \ldots$ und mit ihrer Hilfe die betreffenden Symbole definiert. Dann kann die Klassenanzahl H des Kreiskörpers k der m-ten Einheitswurzeln auf folgende zwei Weisen ausgedrückt werden:

Der *erste* Ausdruck für H lautet:

$$H = \frac{1}{\varkappa} \prod_{(u_1, u_2, \ldots)} L_{s=1} \prod_{(p)} \frac{1}{1 - \left[\frac{p}{u_1, u_2, \ldots}\right] p^{-s}}$$

bez. entsteht aus dieser Formel, indem man $u_1, u_2, \ldots$ durch u; $u_1, u_2, \ldots$, bez. $u, u^*; u_1, u_2, \ldots$ ersetzt. Hierin ist dann das äußere Produkt Π über die Zahlen

$$\left.\begin{aligned} &u_1 = 0,\ 1,\ \ldots,\ l_1^{h_1-1}(l_1-1)-1, \\ &u_2 = 0,\ 1,\ \ldots,\ l_2^{h_2-1}(l_2-1)-1, \\ &\ldots\ldots\ldots\ldots\ldots \end{aligned}\right\} \tag{53}$$

ferner über

$$u = 0,\ 1$$

und über

$$u^* = 0,\ 1,\ \ldots,\ 2^{h^*-2}-1$$

zu erstrecken mit Ausschluß der einen Wertverbindung $u_1 = 0, u_2 = 0, \ldots$, bez. $u = 0$; $u_1 = 0, u_2 = 0, \ldots$, bez. $u = 0, u^* = 0$; $u_1 = 0, u_2 = 0, \ldots$; es besteht daher nur aus einer endlichen Anzahl von Faktoren. Jedes einzelne innere Produkt $\prod_{(p)}$ soll über alle rationalen Primzahlen p erstreckt werden und ist mithin ein unendliches Produkt. Die Größe $\varkappa$ ist die dem Körper k zugehörende Zahl des Satzes 56 (s. S. 115 vor § 26).

Der *zweite* Ausdruck für H ist ein Produkt aus zwei in Bruchform erscheinenden Faktoren und lautet:

$$H = \frac{\prod_{(u_1, u_2, \ldots)} \sum_{(n)} \left[\frac{n}{u_1, u_2, \ldots}\right] n}{(2m)^{\frac{1}{2}\varphi(m)-1}} \cdot \frac{\prod_{(u_1, u_2, \ldots)} \sum_{(n)} \left[\frac{n}{u_1, u_2, \ldots}\right] \log A_n}{R} \cdot 2^{\frac{1}{2}\varphi(m)-1}$$

bez. entsteht aus dieser Formel, indem man zum ersten Bruch rechts den Faktor $\frac{1}{2}$ hinzufügt und dann $u_1, u_2, \ldots$ durch $u; u_1, u_2, \ldots$ bez. $u, u^*; u_1, u_2, \ldots$ ersetzt. Hierin soll das Produkt Π im Zähler des ersten Bruches über alle diejenigen in (53) angegebenen Werte erstreckt werden, für welche im ersten Falle $u_1 + u_2 + \cdots$ bez. in den zwei anderen Fällen $u + u_1 + u_2 + \cdots$ eine ungerade Zahl ist, während das Produkt Π im Zähler des zweiten Bruches über alle diejenigen in (53) angegebenen Werte zu erstrecken ist, für welche im ersten Falle $u_1 + u_2 + \cdots$ bez. in den zwei anderen Fällen $u + u_1 + u_2 + \cdots$ eine gerade Zahl ist, mit Ausschluß immer der einen Wertverbindung $u_1 = 0, u_2 = 0, \ldots$, bez. $u = 0; u_1 = 0, u_2 = 0, \ldots$ bez. $u = 0, u^* = 0; u_1 = 0, u_2 = 0, \ldots$. Weiter ist jede einzelne Summe $\sum_{(n)}$ in dem ersten Bruche über alle ganzen rationalen positiven Zahlen $n = 1, 2, \ldots, m-1$, jede einzelne Summe $\sum_{(n)}$ in dem zweiten Bruche dagegen nur über alle diejenigen unter diesen Zahlen zu erstrecken, welche $< \frac{m}{2}$ sind.

Endlich bedeutet $\log A_n$ den reellen Wert des Logarithmus der Kreiskörperzahl

$$A_n = \sqrt{\left(1 - e^{\frac{2i\pi n}{m}}\right)\left(1 - e^{\frac{-2i\pi n}{m}}\right)}$$

und R den Regulator des Kreiskörpers [Kummer (*22*, *23*)].

Die zwei Brüche im zweiten Ausdrucke für H hat Kummer den **ersten** und den **zweiten Faktor der Klassenanzahl** genannt. Das Doppelte des ersten Faktors einerseits und andererseits der zweite Faktor der Klassenanzahl sind stets für sich ganze rationale Zahlen [Kronecker (*9*)].

Auf Grund des zweiten Ausdrucks für H hat Weber bewiesen, daß die Klassenanzahl des Kreiskörpers der 2^{h^*}-ten Einheitswurzeln stets eine ungerade Zahl ist [Weber (*I*, *4*)].

Der zweite Ausdruck für H gestattet noch weitere Umformungen. Im Falle, daß $m = l$ eine ungerade Primzahl ist, wird durch eine kleine Rechnung die Richtigkeit des folgenden Satzes erkannt:

Satz 142. Ist l eine ungerade Primzahl, so stellt sich die Klassenanzahl h des Kreiskörpers der l-ten Einheitswurzeln, wie folgt, dar:

$$h = \frac{\prod_{(u)} \sum_{(n)} n\, e^{\frac{2i\pi n' u}{l-1}}}{(2l)^{\frac{l-3}{2}}} \cdot \frac{\Delta}{R} 2^{\frac{l-3}{2}}.$$

Hierin ist das Produkt $\prod_{(u)}$ über die ungeraden Zahlen $u = 1, 3, 5, \ldots, l-2$ und jede einzelne Summe $\sum_{(n)}$ über die Zahlen $n = 1, 2, 3, \ldots, l-1$ zu erstrecken; ferner ist eine Primitivzahl r nach l zugrunde gelegt und man hat unter n' eine solche zu n gehörige ganze rationale Zahl zu verstehen, für welche $r^{n'} \equiv n$ nach l wird. Δ bedeutet die Determinante

$$(-1)^{\frac{(l-3)(l-5)}{8}} \begin{vmatrix} \log \varepsilon_1, & \log \varepsilon_2, & \ldots, & \log \varepsilon_{\frac{l-3}{2}} \\ \log \varepsilon_2, & \log \varepsilon_3, & \ldots, & \log \varepsilon_{\frac{l-1}{2}} \\ \ldots & \ldots & \ldots & \ldots \\ \log \varepsilon_{\frac{l-3}{2}}, & \log \varepsilon_{\frac{l-1}{2}}, & \ldots, & \log \varepsilon_{l-4} \end{vmatrix}$$

und dabei ist allgemein $\log \varepsilon_g$ der reelle Wert des Logarithmus der Einheit

$$\varepsilon_g = \sqrt{\frac{1 - \zeta^{r^g}}{1 - \zeta^{r^{g-1}}} \cdot \frac{1 - \zeta^{-r^g}}{1 - \zeta^{-r^{g-1}}}},$$

wo ζ für $e^{\frac{2i\pi}{l}}$ steht [Kummer (*7*, *11*), Dedekind (*1*)].

Die zwei Brüche hier in dem Ausdruck für h entstehen aus den zwei Brüchen in der oben gegebenen, auf den allgemeinen Fall bezüglichen

Formel und sind also der erste und der zweite Faktor der Klassenanzahl in dem früheren Sinne; im gegenwärtigen Falle sind beide Faktoren der Klassenanzahl für sich ganze rationale Zahlen. Der zweite Faktor stellt die Klassenanzahl des in $k(\zeta)$ enthaltenen reellen Unterkörpers vom $\frac{l-1}{2}$-ten Grade dar. KUMMER hat über diese zwei Faktoren noch weitere Sätze aufgestellt, welche ihre Teilbarkeit durch 2 betreffen [KUMMER (*25*)]. Der Versuch KRONECKERS, diese Sätze rein arithmetisch zu beweisen, weist einen Irrtum auf, und die von KRONECKER gegebene Verallgemeinerung ist nicht richtig [KRONECKER (*11*)]. Außerdem hat KUMMER noch nach einer anderen Richtung hin Untersuchungen über die Bedeutung und die Eigenschaften dieser zwei Faktoren angestellt [KUMMER (*13*)]. Man vergleiche ferner Kap. 36. Endlich hat KUMMER den Satz behauptet, daß die Klassenanzahl eines jeden in $k(\zeta)$ enthaltenen Unterkörpers in der Klassenanzahl h des Körpers $k(\zeta)$ aufgeht. Der von ihm versuchte Beweis hierfür ist jedoch nicht stichhaltig [KUMMER (7)].

§ 118. Die Ableitung der aufgestellten Ausdrücke für die Klassenanzahl des Kreiskörpers $k\left(e^{\frac{2i\pi}{m}}\right)$.

Um den Satz 141 zu beweisen, fassen wir sogleich den kompliziertesten Fall ins Auge, in welchem m durch 8 teilbar ist, und stellen den folgenden Hilfssatz auf:

Hilfssatz 22. Ist p eine beliebige rationale Primzahl und m eine durch 8 teilbare Zahl, so gilt unter Anwendung der in Satz 141 erklärten Bezeichnungen für reelle Werte $s > 1$ die Formel:

$$\prod_{(\mathfrak{P})} \{1 - n(\mathfrak{P})^{-s}\} = \prod_{(u, u^*; u_1, u_2, \ldots)} \left\{1 - \left[\frac{p}{u, u^*; u_1, u_2, \ldots}\right] p^{-s}\right\},$$

wo das Produkt linker Hand über alle verschiedenen Primideale $\mathfrak{P}$ des Kreiskörpers $k\left(e^{\frac{2i\pi}{m}}\right)$ zu erstrecken ist, welche in der Primzahl p enthalten sind, und wo das Produkt rechter Hand über alle in (53) angegebenen Wertsysteme $u, u^*; u_1, u_2, \ldots$ (das System $u = 0,\ u^* = 0;\ u_1 = 0, u_2 = 0, \ldots$ einbegriffen) genommen werden soll.

Beweis. Es sei zunächst p eine in m nicht aufgehende Primzahl; es sei l eine der ungeraden Primzahlen $l_1, l_2, \ldots$ und l^h die Potenz, zu der sie in m aufgeht, ferner r eine Primitivzahl nach l^h und $p \equiv r^{p'}$ nach l^h. Bedeutet e den größten gemeinsamen Teiler der beiden Zahlen p' und $l^{h-1}(l-1)$ und wird $l^{h-1}(l-1) = ef$ gesetzt, so ist das Symbol $\left[\frac{p}{l^h}\right]$ offenbar genau eine f-te und nicht eine niedere Einheitswurzel.

Wählen wir zunächst $l = l_1$ und setzen dementsprechend $h = h_1$, $e = e_1$, $l^{h_1-1}(l_1 - 1) = e_1 f_1$, so folgt aus dem eben angegebenen Umstande die Formel:

$$\prod_{(u_1)} \left\{1 - \left[\frac{p}{u, u^*; u_1, u_2, \ldots}\right] p^{-s}\right\} = \left\{1 - \left[\frac{p}{u, u^*; u_2, u_3, \ldots}\right]^{f_1} p^{-sf_1}\right\}^{e_1},$$

wo das Produkt über die in (53) bezeichneten Werte von u_1 zu erstrecken ist. Wählen wir ferner $l = l_2$ und setzen dementsprechend $h = h_2$, $e = e_2$, $l_2^{h_2-1}(l_2 - 1) = e_2 f_2$, so folgt, wenn f_{12} das kleinste gemeinsame Vielfache der Zahlen f_1, f_2 bezeichnet:

$$\prod_{(u_1, u_2)} \left\{1 - \left[\frac{p}{u, u^*; u_1, u_2, \ldots}\right] p^{-s}\right\} = \left\{1 - \left[\frac{p}{u, u^*; u_3, u_4, \ldots}\right]^{f_{12}} p^{-sf_{12}}\right\}^{\frac{e_1 e_2 f_1 f_2}{f_{12}}},$$

wo das Produkt sich über die in (53) bezeichneten Werte von u_1, u_2 erstreckt, und ebenso wird weiterhin, wenn $f_{12\ldots}$ das kleinste gemeinsame Vielfache der Zahlen $f_1, f_2, \ldots$ bezeichnet:

$$\prod_{(u_1, u_2, \ldots)} \left\{1 - \left[\frac{p}{u, u^*; u_1, u_2, \ldots}\right] p^{-s}\right\} = \left\{1 - \left[\frac{p}{u, u^*}\right]^{f_{12}\ldots} p^{-sf_{12}\ldots}\right\}^{\frac{e_1 e_2 \ldots f_1 f_2 \ldots}{f_{12}\ldots}},$$

wo das Produkt über alle in (53) bezeichneten Werte $u_1, u_2, \ldots$ zu erstrecken ist.

Es sei ferner $p \equiv \pm 5^{p'}$ nach 2^{h^*}, es bedeute e^* den größten gemeinsamen Teiler der Zahlen p' und 2^{h^*-2}, und es werde $2^{h^*-2} = e^* f^*$ gesetzt; dann ist offenbar $\left[\frac{p}{2^{h^*}}\right]$ genau eine f^*-te und nicht eine niedere Einheitswurzel. Wir erhalten infolgedessen, wenn $f^*_{12\ldots}$ das kleinste gemeinsame Vielfache der Zahlen $f^*, f_1, f_2, \ldots$ bezeichnet:

$$\prod_{(u^*; u_1, u_2, \ldots)} \left\{1 - \left[\frac{p}{u, u^*; u_1, u_2, \ldots}\right] p^{-s}\right\} = \left\{1 - \left[\frac{p}{2^2}\right]^{u f^*_{12}\ldots} p^{-s f^*_{12}\ldots}\right\}^{\frac{e^* e_1 e_2 \ldots f^* f_1 f_2 \ldots}{f^*_{12}\ldots}},$$

wo nun das Produkt auch über die in (53) bezeichneten Werte von u^* zu nehmen ist.

Endlich sei $\bar{e}$ der größte gemeinsame Teiler von $\frac{p-1}{2}$ und 2, und man setze $2 = \bar{e}\bar{f}$; aus der letzten Formel folgt dann, wenn F das kleinste gemeinsame

Vielfache der Zahlen $\bar{f}, f^*, f_1, f_2, \ldots$ bezeichnet und zur Abkürzung

$$E = \frac{\bar{e}\, e^* e_1 e_2 \cdots \bar{f} f^* f_1 f_2 \cdots}{F}$$

gesetzt wird,

$$\prod_{(u, u^*; u_1, u_2, \ldots)} \left\{1 - \left[\frac{p}{u, u^*; u_1, u_2, \ldots}\right] p^{-s}\right\} = \{1 - p^{-sF}\}^E, \tag{54}$$

wo das Produkt sich über alle in (53) bezeichneten Wertverbindungen $u, u^*; u_1, u_2, \ldots$ erstreckt. Man sieht sofort, daß F der kleinste positive Exponent mit der Kongruenzeigenschaft $p^F \equiv 1$ nach m ist. Da ferner $FE = \Phi(m)$ ist, so folgt aus (54) mit Rücksicht auf den Satz 125 die im Hilfssatz 22 aufgestellte Formel. Mit Hilfe der zweiten Aussage in Satz 125 erkennt man dann leicht die Gültigkeit dieser Formel auch in dem Falle, daß p eine in m enthaltene Primzahl ist.

Die Richtigkeit des ersten in Satz 141 aufgestellten Ausdruckes für H erkennen wir nun unmittelbar auf Grund des Satzes 56, wenn wir die zweite in § 27 gegebene Darstellung von $\zeta(s)$ und den eben bewiesenen Hilfssatz 22 anwenden.

Zur Ableitung des zweiten Ausdruckes für H formen wir zunächst das im ersten Ausdrucke hinter dem Limes-Zeichen stehende Produkt in eine unendliche Summe, wie folgt, um:

$$\prod_{(p)} \frac{1}{1 - \left[\frac{p}{u, u^*; u_1, u_2, \ldots}\right] p^{-s}} = \sum_{(n=1,2,3,\ldots)} \left[\frac{n}{u, u^*; u_1, u_2, \ldots}\right] \frac{1}{n^s}.$$

Die weitere Behandlung der rechts stehenden Summe geschieht dann am einfachsten, indem wir in derselben

$$\frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^\infty e^{-nt}\, t^{s-1}\, dt$$

einsetzen und dann in entsprechender Weise verfahren wie in § 86.

§ 119. Das Vorhandensein von unendlich vielen rationalen Primzahlen, welche nach einer gegebenen Zahl einen vorgeschriebenen, zu ihr primen Rest lassen.

Jeder der zwei in § 117 aufgestellten und soeben bewiesenen Ausdrücke für die Klassenanzahl H des Kreiskörpers der m-ten Einheitswurzeln gestattet eine wichtige Folgerung. Der erstere Ausdruck nämlich kann zum Nachweis der folgenden Tatsache dienen:

Satz 143. *Bedeuten m und n zwei zueinander prime ganze rationale Zahlen so gibt es stets unendlich viele rationale Primzahlen p mit der Kongruenzeigenschaft $p \equiv n$ nach m.* [Dirichlet (*5*, *6*), Dedekind (*1*)].

Beweis. Auch hier betrachten wir nur den kompliziertesten Fall, wo m durch 8 teilbar ist, und setzen, wie in § 117, $m = 2^{h^*} l_1^{h_1} l_2^{h_2} \ldots$. Jedes der dort betrachteten unendlichen Produkte

$$\prod_{(p)} \frac{1}{1 - \left[\frac{p}{u, u^*; u_1, u_2, \ldots}\right] p^{-s}}$$

mit Ausschluß desjenigen, welches der Wertverbindung $u = 0, u^* = 0; u_1 = 0, u_2 = 0, \ldots$ entspricht, konvergiert für $s = 1$ nach einem bestimmten Grenzwerte; aus der ersten in § 117 gegebenen Darstellung der Klassenanzahl H folgt, daß diese Grenzwerte sämtlich von 0 verschieden ausfallen; wir können daher die Logarithmen dieser Produkte verwenden, und es führen dann entsprechende einfache Betrachtungen, wie sie in § 80 angestellt worden sind, zu dem Resultate, daß für jedes betrachtete Wertsystem $u, u^*; u_1, u_2, \ldots$, immer von dem einen Systeme $u = 0, u^* = 0; u_1 = 0, u_2 = 0, \ldots$ abgesehen, die unendliche Summe

$$\sum_{(p)} \left[\frac{p}{u, u^*; u_1, u_2, \ldots}\right] \frac{1}{p^s}, \tag{55}$$

wo p alle rationalen Primzahlen durchläuft, in der Grenze für $s = 1$ stets endlich bleibt.

Da n zu m prim vorausgesetzt ist, so sind die Symbole

$$\left[\frac{n}{2^2}\right], \quad \left[\frac{n}{2^{h^*}}\right], \quad \left[\frac{n}{l_1^{h_1}}\right], \quad \left[\frac{n}{l_2^{h_2}}\right], \ldots$$

sämtlich von 0 verschieden. Wir multiplizieren den Ausdruck (55) mit

$$\frac{1}{\left[\frac{n}{2^2}\right]^u \left[\frac{n}{2^{h^*}}\right]^{u^*} \left[\frac{n}{l_1^{h_1}}\right]^{u_1} \left[\frac{n}{l_2^{h_2}}\right]^{u_2} \cdots},$$

lassen dann $u, u^*; u_1, u_2, \ldots$ alle in (53) angegebenen Werte durchlaufen, doch so, daß das eine System $u = 0, u^* = 0; u_1 = 0, u_2 = 0, \ldots$ ausgeschlossen wird, und addieren sämtliche so entstehenden Ausdrücke zu der unendlichen Summe (26) (siehe § 80, S. 183). Auf diese Weise geht der Ausdruck

$$\left.\begin{aligned} \sum_{(p)} (1 + P)\,&(1 + P^* + P^{*2} + \cdots + P^{*2^{h^*-2}-1}) \cdot \\ &(1 + P_1 + P_1^2 + \cdots + P_1^{l_1^{h_1-1}(l_1-1)-1}) \cdot \\ &(1 + P_2 + P_2^2 + \cdots + P_2^{l_2^{h_2-1}(l_2-1)-1}) \cdots \frac{1}{p^s}, \end{aligned}\right\} \tag{56}$$

hervor, wo zur Abkürzung

$$P = \frac{\left[\frac{p}{2^2}\right]}{\left[\frac{n}{2^2}\right]}, \quad P^* = \frac{\left[\frac{p}{2^{h^*}}\right]}{\left[\frac{n}{2^{h^*}}\right]}, \quad P_1 = \frac{\left[\frac{p}{l_1^{h_1}}\right]}{\left[\frac{n}{l_1^{h_1}}\right]}, \quad P_2 = \frac{\left[\frac{p}{l_2^{h_2}}\right]}{\left[\frac{n}{l_2^{h_2}}\right]}, \ldots$$

gesetzt ist. Sehen wir in dieser unendlichen Reihe (56) von denjenigen Gliedern ab, die den in m aufgehenden Primzahlen $2, l_1, l_2, \ldots$ entsprechen, und die nur in endlicher Anzahl vorhanden sind, so ist im übrigen diese Reihe gleich $\Phi(m)\,\Sigma\frac{1}{p^s}$, wo p nur alle diejenigen rationalen Primzahlen durchläuft, für welche die Werte $P, P^*, P_1, P_2, \ldots$ sämtlich gleich 1 werden, d. s. eben die Primzahlen, welche der im Satze 143 verlangten Kongruenzbedingung genügen.

Da die unendliche Summe (26) (s. S. 183) für $s = 1$ über alle Grenzen wächst, dagegen die hier betrachteten Reihen (55) für $s = 1$ sämtlich endlich bleiben, so folgt, daß auch der Wert der unendlichen Reihe (56) für $s = 1$ über alle Grenzen wächst, d. h. die Primzahlen mit der verlangten Kongruenzeigenschaft sind notwendig in unendlicher Anzahl vorhanden.

§ 120. Die Darstellung sämtlicher Einheiten des Kreiskörpers durch die Kreiseinheiten.

Der zweite der beiden in § 117 aufgestellten Ausdrücke kann zum Nachweise des folgenden Satzes dienen:

Satz 144. *Jede Einheit eines Abelschen Körpers ist eine Wurzel mit rationalem ganzzahligem Exponenten aus einem Produkt von Kreiseinheiten.*

Beweis. Fassen wir zunächst den Fall ins Auge, daß $m = l$ eine ungerade Primzahl ist. Nach der Formel im Satze 142 enthält der zweite Faktor der Klassenanzahl im Zähler eine gewisse Determinante Δ; jene Determinante Δ ist daher notwendig von 0 verschieden, und hieraus folgt mit Rücksicht auf die in § 20 und § 21 angestellten Betrachtungen, daß die in Satz 142 angegebenen $\frac{l-3}{2}$ Einheiten $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\frac{l-3}{2}}$ des Kreiskörpers $k\left(e^{\frac{2i\pi}{l}}\right)$ ein System von unabhängigen Einheiten bilden. Dieser Umstand lehrt die Richtigkeit des Satzes 144 für den besonderen Fall des Kreiskörpers $k\left(e^{\frac{2i\pi}{l}}\right)$, sowie auch für alle in diesem Körper enthaltenen Unterkörper (Kummer (*11*)).

Eine ähnliche Umformung des zweiten Faktors der Klassenanzahl, wie sie in Satz 142 gegeben wird, ist auch im Falle des Kreiskörpers der m-ten Einheitswurzeln möglich, wenn m eine beliebige zusammengesetzte Zahl ist; der betreffende Ausdruck ermöglicht dann auf Grund des Satzes 131 den allgemeinen Beweis des Satzes 144.

Ein reiches Zahlenmaterial, welches zu tieferen Untersuchungen in der Theorie der Kreiskörper von hohem Nutzen ist, bieten die von Reuschle berechneten Tafeln komplexer Primzahlen [Reuschle (*1*), Kummer (*24*), Kronecker (*12*)].

27. Anwendungen der Theorie des Kreiskörpers auf den quadratischen Körper.

§ 121. Die Erzeugung der Einheiten des reellen quadratischen Körpers aus Kreiseinheiten.

Indem wir gewisse in den vorangehenden Kapiteln abgeleitete Eigenschaften des Kreiskörpers der m-ten Einheitswurzeln für einen in ihm enthaltenen quadratischen Unterkörper verwerten, gelangen wir zu neuen Sätzen über den quadratischen Zahlkörper. Die Fruchtbarkeit dieser Methode wird noch erhöht, wenn wir sie mit denjenigen Wahrheiten in Verbindung bringen, welche im dritten Teil dieses Berichtes durch unmittelbare Betrachtung des quadratischen Körpers gewonnen worden sind.

Nach dem allgemeinen Satze 144 ist insbesondere eine jede Einheit eines reellen quadratischen Körpers $k\left(\sqrt{m}\right)$ eine Wurzel mit rationalem ganzzahligem Exponenten aus einem Produkte von Kreiseinheiten; es wird eine spezielle Einheit des Körpers $k\left(\sqrt{m}\right)$ einfach durch den folgenden Ausdruck

$$\frac{\prod\limits_{(b)}\left(e^{\frac{bi\pi}{d}} - e^{-\frac{bi\pi}{d}}\right)}{\prod\limits_{(a)}\left(e^{\frac{ai\pi}{d}} - e^{-\frac{ai\pi}{d}}\right)}$$

erhalten, wo d die Diskriminante des Körpers $k\left(\sqrt{m}\right)$ bedeutet, und wo die Produkte $\prod\limits_{(a)}, \prod\limits_{(b)}$ über alle diejenigen Zahlen a oder b der Reihe $1, 2, \ldots, |d|$ zu erstrecken sind, welche der Bedingung $\left(\frac{d}{a}\right) = +1$ bez. $\left(\frac{d}{b}\right) = -1$ genügen [Dirichlet (*7*)]. Vgl. § 86.

§ 122. Das Reziprozitätsgesetz für quadratische Reste.

Es sei l eine ungerade rationale Primzahl, r eine Primitivzahl nach l; ferner $\zeta = e^{\frac{2i\pi}{l}}$ und $s = (\zeta; \zeta^r)$. Zu der aus den $\frac{l-1}{2}$ Substitutionen $1, s^2, s^4, \ldots s^{l-3}$ gebildeten Untergruppe der Gruppe des Kreiskörpers $k(\zeta)$ gehört ein gewisser quadratischer Unterkörper k^* des Kreiskörpers $k(\zeta)$. Da die Diskriminante des Körpers $k(\zeta)$ nach Satz 118 gleich $(-1)^{\frac{l-1}{2}} l^{l-2}$ ist, so enthält nach Satz 39 die Diskriminante von k^* keine andere rationale Primzahl als l und besitzt daher wegen Satz 95 den Wert $d = (-1)^{\frac{l-1}{2}} l$.

Es sei p entweder die Primzahl 2 oder eine beliebige von l verschiedene ungerade rationale Primzahl. Indem wir die Zerlegung von p einerseits in dem Kreiskörper $k(\zeta)$ der l-ten Einheitswurzeln, andererseits direkt nach Satz 97 in dem quadratischen Unterkörper k^* ausführen und hernach die erhaltenen Resultate miteinander vergleichen, gelangen wir zu einem neuen

Beweise des Reziprozitätsgesetzes für quadratische Reste [KRONECKER (*15*)]. Wir verfahren dabei, wie folgt:

Ist f der kleinste positive Exponent, für welchen $p^f \equiv 1$ nach l ausfällt, und wird $e = \frac{l-1}{f}$ gesetzt, so zerlegt sich nach Satz 119 die Primzahl p im Körper $k(\zeta)$ in e Primideale $\mathfrak{P}, s\mathfrak{P}, \ldots, s^{e-1}\mathfrak{P}$, und es ist der gemeinsame Zerlegungskörper k_z dieser Primideale nach Satz 129 vom Grade e. Die rationale Primzahl p ist alsdann offenbar in dem quadratischen Körper k^* zerlegbar oder nicht zerlegbar, je nachdem der Körper k^* in k_z als Unterkörper enthalten ist oder nicht. Bedenken wir, daß der Körper $k(\zeta)$ nur den einen quadratischen Unterkörper k^* enthält, und ferner, daß ein Abelscher Körper dann und nur dann überhaupt einen quadratischen Unterkörper besitzt, wenn sein Grad gerade ist, so folgt, daß k^* dann und nur dann in k_z enthalten ist, wenn die Zahl e gerade ausfällt. Andererseits ist nach Satz 97 die Primzahl p in k^* zerlegbar oder nicht zerlegbar, je nachdem $\left(\frac{(-1)^{\frac{l-1}{2}} l}{p}\right) = +1$ oder $= -1$ ist. Ist nun e gerade, so folgt $p^{\frac{l-1}{2}} = p^{f \cdot \frac{e}{2}} \equiv 1$ nach l, d. h. $\left(\frac{p}{l}\right) = +1$; im anderen Falle wird $p^{\frac{l-1}{2}} = p^{\frac{f}{2} \cdot e} \equiv (-1)^e \equiv -1$ nach l, d. h. $\left(\frac{p}{l}\right) = -1$. Es ist mithin in jedem Falle

$$\left(\frac{p}{l}\right) = \left(\frac{(-1)^{\frac{l-1}{2}} l}{p}\right). \tag{57}$$

Wir nehmen zunächst p ungerade an; aus (57) folgt

$$\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = \left(\frac{(-1)^{\frac{l-1}{2}}}{p}\right) \tag{58}$$

und weiter, wenn wir p und l miteinander vertauschen,

$$\left(\frac{(-1)^{\frac{l-1}{2}}}{p}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{l}\right).$$

Die letztere Formel ergibt, wenn wir $l = 3$ nehmen,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \tag{59}$$

Die Verbindung der Gleichung (59) mit (58) liefert

$$\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2} \cdot \frac{p-1}{2}}. \tag{60}$$

Setzen wir in (57) $p = 2$, so folgt

$$\left(\frac{2}{l}\right) = \left(\frac{(-1)^{\frac{l-1}{2}} l}{2}\right) = (-1)^{\frac{l^2-1}{8}}. \tag{61}$$

Die Formeln (60), (59) und (61) enthalten das Reziprozitätsgesetz für quadratische Reste nebst den zugehörigen Ergänzungssätzen.

§ 123. Der imaginäre quadratische Körper mit einer Primzahldiskriminante.

Satz 145. Wenn l eine rationale Primzahl mit der Kongruenzeigenschaft $l \equiv 3$ nach 4 ist und p eine rationale Primzahl von der Gestalt $p = ml + 1$ bedeutet, so gilt für ein jedes in p aufgehende Primideal $\mathfrak{p}$ des imaginären quadratischen Körpers $k\left(\sqrt{-l}\right)$ die Äquivalenz

$$\mathfrak{p}^{\frac{\Sigma b - \Sigma a}{l}} \sim 1,$$

wo Σa die Summe der kleinsten positiven quadratischen Reste und Σb die Summe der kleinsten positiven quadratischen Nichtreste nach l bedeutet.

Setzt man ferner $p = \mathfrak{p}\mathfrak{p}'$ und

$$\mathfrak{p}^{\frac{\Sigma b - \Sigma a}{l}} = (\pi),$$

wobei π eine ganze Zahl des imaginären quadratischen Körpers $k\left(\sqrt{-l}\right)$ bedeutet, so gilt die Kongruenz

$$\pi \equiv \pm \frac{1}{\prod\limits_{(a)} (a\,m)!}, \qquad (\mathfrak{p}'),$$

wo das im Nenner stehende Produkt über alle kleinsten positiven quadratischen Reste a nach l zu erstrecken ist [JACOBI (*1, 2, 3, 4*), CAUCHY (*1*), EISENSTEIN (*4*)].

Beweis. Nach Satz 136 kann man, wenn $\mathfrak{P}$ ein Primideal ersten Grades in $k(\zeta)$ bedeutet, unter Benutzung der dort erklärten Bezeichnungen

$$\mathfrak{P}^{g_0 + g_{-1} s + g_{-2} s^2 + \cdots + g_{-l+2} s^{l-2}} = (\mathrm{A}) \tag{62}$$

setzen derart, daß A eine ganze Zahl in $k(\zeta)$ ist. Ist dann $p = ml + 1$ die durch $\mathfrak{P}$ teilbare rationale Primzahl und $p = \mathfrak{p}\mathfrak{p}'$ die Zerlegung dieser Primzahl in dem in $k(\zeta)$ enthaltenen quadratischen Unterkörper $k\left(\sqrt{-l}\right)$, so gehen andererseits diese zwei Primideale $\mathfrak{p}$ und $\mathfrak{p}'$ des Körpers $k\left(\sqrt{-l}\right)$ in der Gestalt hervor:

$$\mathfrak{p} = \mathfrak{P}^{1 + s^2 + s^4 + \cdots + s^{l-3}},$$
$$\mathfrak{p}' = s\mathfrak{p} = \mathfrak{P}^{s(1 + s^2 + s^4 + \cdots + s^{l-3})}.$$

Wenn wir die Gleichung (62) in die $(1+s^2+s^4+\cdots+s^{l-3})$-te symbolische Potenz erheben, so folgt

$$\mathfrak{p}^{q_0+q_{-2}+q_{-4}+\cdots+q_{-l+3}}\mathfrak{p}'^{q_{-1}+q_{-3}+q_{-5}+\cdots+q_{-l+2}}=(\alpha),$$

wo α eine Zahl in $k\left(\sqrt[l]{-l}\right)$ bedeutet. Wegen

$$q_{-1}+q_{-3}+\cdots+q_{-l+2}-q_0-q_{-2}-\cdots-q_{-l+3}=(r+1)\frac{\Sigma b-\Sigma a}{l}$$

folgt, wenn wir die Äquivalenz $\mathfrak{p}\,\mathfrak{p}'\sim 1$ berücksichtigen,

$$\mathfrak{p}^{(r+1)\frac{\Sigma b-\Sigma a}{l}}\sim 1. \tag{63}$$

Andererseits kann man nach Satz 135

$$\mathfrak{P}^{r_0+r_{-1}s+r_{-2}s^2+\cdots+r_{-l+2}s^{l-3}}=(\mathsf{B})$$

setzen, derart, daß B eine ganze Zahl in $k(\zeta)$ bedeutet. Wenn wir diese Gleichung in die $(1+s^2+s^4+\cdots+s^{l-3})$-te symbolische Potenz erheben, so folgt

$$\mathfrak{p}^{\Sigma b-\Sigma a}=\mathfrak{p}^{l\frac{\Sigma b-\Sigma a}{l}}\sim 1. \tag{64}$$

Da die Zahl $r+1$ nicht durch l teilbar ist, wenn wir von dem Falle $l=3$ absehen, der für sich ohne weiteres klar liegt, so folgt aus den beiden Äquivalenzen (63) und (64) die im ersten Teile des Satzes 145 behauptete Äquivalenz.

Der zweite Teil des Satzes 145 folgt durch eingehendere Betrachtung der in § 112 entwickelten Kongruenzeigenschaften (43), (44) der Lagrangeschen Wurzelzahl Λ.

Ein wesentlich verschiedener Beweis für den ersten Teil des Satzes 145 ergibt sich unmittelbar aus einer gegen den Schluß des § 86 gemachten Bemerkung über den Ausdruck der Klassenanzahl des Körpers $k\left(\sqrt[l]{-l}\right)$ für den Fall $l=3$ nach 4.

Durch eine bemerkenswerte Modifikation des Jacobischen Verfahrens gelingt es, die Aussagen des Satzes 145 auch auf den Fall zu erweitern, daß die Primzahl p nicht von der Gestalt $p=ml+1$ ist [Eisenstein (*11*), Stickelberger (*1*)].

§ 124. Die Bestimmung des Vorzeichens der Gaußschen Summe.

Es sei p eine ungerade rationale Primzahl, so können wir nach den Definitionen des § 111 und der in § 112 hinzugefügten Ausdehnung derselben auf den Fall $l=2$ die Lagrangesche Normalbasis und die Lagrangesche Wurzelzahl für den quadratischen Körper $k\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$ aufstellen. Es werde $\mathsf{Z}=e^{\frac{2i\pi}{p}}$ gesetzt, so besteht für diesen Körper die Lagrangesche Normalbasis aus den zwei Zahlen

$$\lambda_0=\sum_{(a)}\mathsf{Z}^a,\quad \lambda_1=\sum_{(b)}\mathsf{Z}^b,$$

und die Lagrangesche Wurzelzahl hat für ihn den Wert

$$\Lambda=\lambda_0-\lambda_1=\sum_{(a)}\mathsf{Z}^a-\sum_{(b)}\mathsf{Z}^b;$$

dabei durchlaufen a und b bez. die quadratischen Reste und Nichtreste nach p unter den Zahlen $1,2,\ldots,p-1$.

Das am Schlusse des § 112 charakterisierte Problem der vollständigen Ermittlung von Λ, nachdem Λ^l gefunden ist, kommt in dem vorliegenden Falle des quadratischen Körpers auf die Frage nach einem gewissen Vorzeichen $\pm$ hinaus und wird durch folgenden Satz erledigt:

Satz 146. Die Lagrangesche Wurzelzahl Λ des quadratischen Körpers mit der Primzahldiskriminante $(-1)^{\frac{p-1}{2}}p$ ist eine positiv reelle oder positiv rein imaginäre Zahl [Gauss (*2*), Kronecker (*4*)].

Beweis. Das Quadrat der in Frage stehenden Lagrangeschen Wurzelzahl Λ besitzt, weil Λ eine Zahl des quadratischen Körpers und nach Satz 138

$$|\Lambda|=|\sqrt{p}|$$

ist, jedenfalls den Wert $(-1)^{\frac{p-1}{2}}p$; man hat also

$$\Lambda=\pm\sqrt{(-1)^{\frac{p-1}{2}}p}. \tag{65}$$

An die Stelle der in § 112 mit $\mathfrak{p}$, $\mathfrak{P}$ bezeichneten Ideale treten im vorliegenden Falle $l=2$ bez. die Ideale (p) und $(1-\mathsf{Z})$; aus der Kongruenz (43) wird daher die Kongruenz

$$\Lambda\equiv\frac{(-1)^{\frac{p+1}{2}}}{\frac{p-1}{2}!}(1-\mathsf{Z})^{\frac{p-1}{2}},\qquad\left((1-\mathsf{Z})^{\frac{p+1}{2}}\right),$$

d. i.

$$\Lambda\equiv\tfrac{p-1}{2}!\,(1-\mathsf{Z})^{\frac{p-1}{2}},\qquad\left((1-\mathsf{Z})^{\frac{p+1}{2}}\right), \tag{66}$$

Wir betrachten andererseits den Ausdruck

$$\Delta=(\mathsf{Z}^{-1}-\mathsf{Z}^{+1})(\mathsf{Z}^{-2}-\mathsf{Z}^{+2})\ldots\left(\mathsf{Z}^{-\frac{p-1}{2}}-\mathsf{Z}^{+\frac{p-1}{2}}\right).$$

Da derselbe nur sein Vorzeichen ändert, wenn wir Z durch Z^R ersetzen, wobei R eine Primitivzahl nach p bedeuten soll, und da das Ideal (Δ) mit dem Ideal $(1-\mathsf{Z})^{\frac{p-1}{2}}$ übereinstimmt, so ist notwendig

$$\Delta=\pm\sqrt{(-1)^{\frac{p-1}{2}}p}.$$

Um das Vorzeichen hier zu bestimmen, bedenken wir, daß

$$Z^{-h} - Z^{+h} = -2i \sin\frac{2h\pi}{p}, \qquad \left(h = 1, 2, \ldots, \frac{p-1}{2}\right)$$

ist, und erhalten hieraus für Δ einen Wert von der Gestalt $(-i)^{\frac{p-1}{2}} P$, wo P eine positive Größe darstellt. Hieraus folgt, wenn wir fortan unter $\sqrt{(-1)^{\frac{p-1}{2}} p}$ denjenigen Wert dieser Quadratwurzel verstehen, welcher positiv reell oder positiv imaginär ist,

$$\Delta = (-1)^{\frac{p^2-1}{8}} \sqrt{(-1)^{\frac{p-1}{2}} p}. \tag{67}$$

Endlich lehrt die Gleichung

$$\Delta = Z^{-1-2-\cdots-\frac{p-1}{2}} (1 - Z^2)(1 - Z^4) \cdots (1 - Z^{p-1}),$$

daß

$$\Delta \equiv 2 \cdot 4 \cdot 6 \cdots (p-1)(1-Z)^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{2}} \tfrac{p-1}{2}! \, (1-Z)^{\frac{p-1}{2}}, \qquad \left((1-Z)^{\frac{p+1}{2}}\right)$$

ist, und hieraus folgt nach (66)

$$\Delta \equiv 2^{\frac{p-1}{2}} \Delta, \qquad \left((1-Z)^{\frac{p+1}{2}}\right).$$

Da

$$2^{\frac{p-1}{2}} = \left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}}, \qquad (p)$$

wird, so ergibt sich wegen (67)

$$\Delta = \sqrt{(-1)^{\frac{p-1}{2}} p}, \qquad \left((1-Z)^{\frac{p+1}{2}}\right),$$

und folglich ist wegen (65)

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

womit der Satz 146 bewiesen ist.

Über spezielle Abelsche Körper von höherem als dem zweiten Grade ist bisher wenig veröffentlicht worden; erwähnt seien die Eisensteinsche Abhandlung über kubische, aus der Kreisteilung entstehende Formen, welche als eine Einleitung in die Theorie der kubischen Abelschen Körper aufzufassen ist [Eisenstein (*10*)], ferner die Bachmannsche Arbeit über die aus zwei Quadratwurzeln zusammengesetzten komplexen Zahlen [Bachmann (*1*)], und die Weberschen Untersuchungen über Abelsche kubische und biquadratische Zahlkörper [Weber (*2, 4*)].

Fünfter Teil.

Der Kummersche Zahlkörper.

28. Die Zerlegung der Zahlen des Kreiskörpers im Kummerschen Körper.

§ 125. Die Definition des Kummerschen Körpers.

Es bezeichne l eine ungerade rationale Primzahl und $k(\zeta)$ den durch $\zeta = e^{\frac{2i\pi}{l}}$ bestimmten Kreiskörper. Ist dann μ eine solche ganze Zahl in $k(\zeta)$, welche nicht zugleich die l-te Potenz einer Zahl in $k(\zeta)$ wird, so erweist sich die Gleichung l-ten Grades

$$x^l - \mu = 0$$

als irreduzibel im Rationalitätsbereich $k(\zeta)$. Bedeutet $\mathsf{M} = \sqrt[l]{\mu}$ eine irgendwie in bestimmter Weise ausgewählte Wurzel dieser Gleichung, so sind

$$\zeta\mathsf{M}, \ \zeta^2\mathsf{M}, \ \ldots, \ \zeta^{l-1}\mathsf{M}$$

deren $l-1$ übrige Wurzeln. Den durch M und ζ bestimmten Körper $k(\mathsf{M}, \zeta)$ nenne ich einen **Kummerschen Körper**. Ein solcher Kummerscher Körper $k(\mathsf{M}, \zeta)$ ist vom Grade $l(l-1)$; er enthält den Kreiskörper $k(\zeta)$ als Unterkörper und ist in bezug auf $k(\zeta)$ ein relativ Abelscher Körper vom Relativgrade l. Durch die Operation der Vertauschung von M mit $\zeta\mathsf{M}$ in einer Zahl oder in einem Ideal dieses Kummerschen Körpers geht man zu der relativ konjugierten Zahl bezüglich dem relativ konjugierten Ideal über. Dieser Übergang werde durch Vorsetzen des Substitutionszeichens S angedeutet.

Man beweist leicht die Tatsachen:

Satz 147. Der durch $\mathsf{M} = \sqrt[l]{\mu}$ und ζ bestimmte Kummersche Körper ist im Bereiche der rationalen Zahlen dann und nur dann ein Galoisscher Körper, wenn unter den symbolischen Potenzen $\mu^{s-1}, \mu^{s-2}, \ldots, \mu^{s-l+1}$ eine die l-te Potenz einer Zahl in $k(\zeta)$ wird. Dabei ist $s = (\zeta : \zeta^r)$, worin r eine Primitivzahl nach l bedeutet.

Der Kummersche Körper $k(\mathsf{M}, \zeta)$ ist insbesondere dann und nur dann ein Abelscher Körper, wenn μ^{s-r} die l-te Potenz einer Zahl in $k(\zeta)$ wird.

Wenn der Kummersche Körper $k(\mathsf{M}, \zeta)$ ein Galoisscher oder insbesondere ein Abelscher Körper ist, so entsteht dieser Körper, wie man auf Grund der in § 38 entwickelten Begriffe ersieht, durch Zusammensetzung aus dem Kreiskörper $k(\zeta)$ und einem gewissen Körper l-ten Grades.

§ 126. Die Relativdiskriminante des Kummerschen Körpers.

Unsere erste Aufgabe ist die Ermittlung der Relativdiskriminante von $k(\mathsf{M},\zeta)$ in bezug auf $k(\zeta)$. Wir beweisen zunächst die folgende Tatsache:

Hilfssatz 23. Wenn ein Primideal $\mathfrak{p}$ des Kreiskörpers $k(\zeta)$ gleich der l-ten Potenz eines Primideals $\mathfrak{P}$ des Kummerschen Körpers $k(\mathsf{M},\zeta)$ wird und A eine ganze durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbare Zahl in $k(\mathsf{M},\zeta)$ ist, so enthalten die Relativdiskriminante der Zahl A und die Relativdiskriminante des Kummerschen Körpers $k(\mathsf{M},\zeta)$ in bezug auf $k(\zeta)$ genau die gleiche Potenz von $\mathfrak{p}$ als Faktor.

Beweis. Jede ganze Zahl des Kummerschen Körpers $k(\mathsf{M},\zeta)$ ist offenbar in der Gestalt

$$\Omega = \frac{\alpha+\alpha_1\mathsf{A}+\alpha_2\mathsf{A}^2+\cdots+\alpha_{l-1}\mathsf{A}^{l-1}}{\beta} \tag{68}$$

darstellbar, so daß $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{l-1}, \beta$ ganze Zahlen in $k(\zeta)$ sind. Ist dabei β durch $\mathfrak{p}$ teilbar, so folgt, daß auch der Zähler des rechter Hand stehenden Bruches kongruent 0 nach $\mathfrak{p}$ sein muß. Wegen $\mathsf{A}\equiv 0$ nach $\mathfrak{P}$ geht hieraus $\alpha\equiv 0$ nach $\mathfrak{P}$ und, da α in $k(\zeta)$ liegt, auch $\alpha\equiv 0$ nach $\mathfrak{p}$ hervor. Aus der letzten Kongruenz ergibt sich

$$\alpha_1\mathsf{A}+\alpha_2\mathsf{A}^2+\cdots+\alpha_{l-1}\mathsf{A}^{l-1}\equiv 0,\ (\mathfrak{p}),$$

und da $\mathsf{A}\not\equiv 0, \mathsf{A}^2\equiv 0, \mathsf{A}^3\equiv 0, \ldots, \mathsf{A}^{l-1}\equiv 0$ nach $\mathfrak{P}^2$ ist, so folgt $\alpha_1\equiv 0$ nach $\mathfrak{P}$ und daher auch nach $\mathfrak{p}$, also ist auch

$$\alpha_2\mathsf{A}^2+\cdots+\alpha_{l-1}\mathsf{A}^{l-1}\equiv 0,\ (\mathfrak{p}).$$

Wegen $\mathsf{A}^2\not\equiv 0, \mathsf{A}^3\equiv 0, \ldots, \mathsf{A}^{l-1}\equiv 0$ nach $\mathfrak{P}^3$ folgt $\alpha_2\equiv 0$ nach $\mathfrak{P}$ und daher auch nach $\mathfrak{p}$. Fahren wir so fort, so erkennen wir, daß notwendig alle Koeffizienten $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{l-1}$ durch $\mathfrak{p}$ teilbar sein müssen. Ist jetzt β' eine ganze Zahl in $k(\zeta)$, welche durch $\frac{\beta}{\mathfrak{p}}$ teilbar, aber nicht durch β teilbar ist, so werden die Zahlen $\alpha\beta', \alpha_1\beta', \ldots, \alpha_{l-1}\beta'$ sämtlich durch β teilbar. Wir setzen

$$\alpha'=\frac{\alpha\beta'}{\beta},\quad \alpha_1'=\frac{\alpha_1\beta'}{\beta},\quad \ldots,\quad \alpha_{l-1}'=\frac{\alpha_{l-1}\beta'}{\beta}$$

und erhalten dann

$$\Omega = \frac{\alpha'+\alpha_1'\mathsf{A}+\alpha_2'\mathsf{A}^2+\cdots+\alpha_{l-1}'\mathsf{A}^{l-1}}{\beta'}, \tag{69}$$

wo die im Nenner stehende Zahl β' jetzt einen Idealfaktor $\mathfrak{p}$ weniger enthält als β. Wenden wir die eben auf (68) angewandte Schlußweise nunmehr wiederum auf (69) an usf., so gelangen wir schließlich zu dem Resultat, daß jede ganze Zahl Ω des Körpers $k(\mathsf{M},\zeta)$ in der Gestalt

$$\Omega = \frac{\alpha+\bar\alpha_1\mathsf{A}+\bar\alpha_2\mathsf{A}^2+\cdots+\bar\alpha_{l-1}\mathsf{A}^{l-1}}{\bar\beta} \tag{70}$$

darstellbar ist derart, daß $\bar\alpha, \bar\alpha_1, \ldots, \bar\alpha_{l-1}, \bar\beta$ sämtlich ganze Zahlen in $k(\zeta)$ sind, und daß außerdem $\bar\beta$ zu $\mathfrak{p}$ prim ausfällt. Wir denken uns nun die $l(l-1)$ Zahlen einer Basis des Kummerschen Körpers $k(\mathsf{M},\zeta)$ gemäß (70) ausgedrückt und bilden aus diesen Zahlen und den zu ihnen relativ konjugierten Zahlen die l-reihige Matrix; es wird dann ersichtlich, daß die Relativdiskriminante des Kummerschen Körpers $k(\mathsf{M},\zeta)$ nach Multiplikation mit gewissen zu $\mathfrak{p}$ primen ganzen Zahlen $\bar\beta$ des Körpers $k(\zeta)$ durch die Relativdiskriminante der Zahl A teilbar werden muß, und hiermit ist der Hilfssatz 23 bewiesen.

Satz 148. Es werde $\lambda=1-\zeta$ und $\mathfrak{l}=(\lambda)$ gesetzt. Geht ein von $\mathfrak{l}$ verschiedenes Primideal $\mathfrak{p}$ des Kreiskörpers $k(\zeta)$ in der Zahl μ genau zur e-ten Potenz auf, so enthält, wenn der Exponent e zu l prim ist, die Relativdiskriminante des durch $\mathsf{M}=\sqrt[l]{\mu}$ und ζ bestimmten Kummerschen Körpers in bezug auf $k(\zeta)$ genau die Potenz $\mathfrak{p}^{l-1}$ von $\mathfrak{p}$ als Faktor. Ist dagegen der Exponent e ein Vielfaches von l, so fällt diese Relativdiskriminante prim zu $\mathfrak{p}$ aus.

Was das Primideal $\mathfrak{l}$ betrifft, so können wir zunächst den Umstand ausschließen, daß die Zahl μ durch $\mathfrak{l}$ teilbar ist und dabei $\mathfrak{l}$ genau in einer solchen Potenz enthält, deren Exponent ein Vielfaches von l ist; denn alsdann könnte die Zahl μ sofort durch eine zu $\mathfrak{l}$ prime Zahl μ^* ersetzt werden, so daß $k\left(\sqrt[l]{\mu^*},\zeta\right)$ derselbe Körper wie $k\left(\sqrt[l]{\mu},\zeta\right)$ ist. Unter Ausschluß des genannten Umstandes haben wir die zwei möglichen Fälle, daß μ genau eine Potenz von $\mathfrak{l}$ enthält, deren Exponent zu l prim ist, oder daß μ nicht durch $\mathfrak{l}$ teilbar ist. Im *ersteren* Falle ist die Relativdiskriminante von $k\left(\sqrt[l]{\mu},\zeta\right)$ in bezug auf $k(\zeta)$ genau durch die Potenz $\mathfrak{l}^{l-1}$ von $\mathfrak{l}$ teilbar. Im *zweiten* Falle sei m der höchste Exponent $\leq l$, für den es eine Zahl α in $k(\zeta)$ gibt, so daß $\mu\equiv\alpha^l$ nach $\mathfrak{l}^m$ ausfällt. Jene Relativdiskriminante ist dann im Falle $m=l$ zu $\mathfrak{l}$ prim; sie ist dagegen im Falle $m<l$ genau durch die Potenz $\mathfrak{l}^{(l-1)(l-m+1)}$ von $\mathfrak{l}$ teilbar.

Beweis. Gehen wir zunächst auf den ersten Teil des Satzes 148 ein. Es sei π eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare ganze Zahl in $k(\zeta)$, und weiter sei ν eine durch $\frac{\pi}{\mathfrak{p}}$ teilbare, aber zu $\mathfrak{p}$ prime ganze Zahl in $k(\zeta)$.

Ist der Exponent e der in μ enthaltenen Potenz von $\mathfrak{p}$ kein Vielfaches von l, so können wir zwei ganze rationale positive Zahlen a und b bestimmen, so daß $1=ae-bl$ ist. Dann ist $\mu^*=\frac{\mu^a\nu^{bl}}{\pi^{bl}}$ eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare ganze Zahl in $k(\zeta)$, und es erweist sich, wenn $\mathsf{M}^*=\sqrt[l]{\mu^*}$ gesetzt wird, $k(\mathsf{M}^*,\zeta)=k(\mathsf{M},\zeta)$, und wenn wir den gemeinsamen Idealteiler von $\mathfrak{p}$ und M^* im Körper $k(\mathsf{M},\zeta)$ mit $\mathfrak{P}$ bezeichnen,

$$\mathfrak{P}=S\mathfrak{P},\quad \mathfrak{p}=\mathfrak{P}^l.$$

Das Ideal $\mathfrak{P}$ ist also ein ambiges Primideal des Kummerschen Körpers $k(\mathsf{M},\zeta)$ in bezug auf den Unterkörper $k(\zeta)$; nach Satz 93 tritt dasselbe daher in der Relativdiskriminante von $k(\mathsf{M},\zeta)$ in bezug auf $k(\zeta)$ als Faktor auf.

Da ferner die Zahl M^* durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbar ist, und da die Relativdiskriminante der Zahl M^* in bezug auf $k(\zeta)$ den Wert $(-1)^{\frac{l-1}{2}} l^l \mu^{*l-1}$ hat, so ist nach Hilfssatz 23 das Ideal $\mathfrak{p}$ auch in der Relativdiskriminante des Körpers $k(\mathsf{M}, \zeta)$ genau zur $(l-1)$-ten Potenz enthalten.

Ist dagegen der Exponent e der in μ enthaltenen Potenz von $\mathfrak{p}$ ein Vielfaches von l, so ist $\mu^* = \frac{\mu \pi^e}{\pi^e}$ eine nicht durch $\mathfrak{p}$ teilbare ganze Zahl in $k(\zeta)$; da die Relativdiskriminante der Zahl $\mathsf{M}^* = \sqrt[l]{\mu^*}$ in bezug auf $k(\zeta)$ den Wert $(-1)^{\frac{l-1}{2}} l^l \mu^{*l-1}$ hat, so ist sie zu $\mathfrak{p}$ prim. Das gleiche gilt mithin von der Relativdiskriminante des Körpers $k(\mathsf{M}, \zeta)$ in bezug auf $k(\zeta)$.

Jetzt betrachten wir die Verhältnisse in betreff des Primfaktors $\mathfrak{l}$. Im Falle, daß derselbe in μ zu einem solchen Exponenten e erhoben aufgeht, der kein Vielfaches von l ist, verfahren wir in entsprechender Weise, wie im ersten Teil dieses Beweises bei Behandlung des Primideales $\mathfrak{p}$ verfahren wurde, indem wir an die Stelle von μ eine Zahl μ^* bringen, die durch $\mathfrak{l}$, aber nicht durch $\mathfrak{l}^2$ teilbar ist. Da die Relativdiskriminante der Zahl $\mathsf{M}^* = \sqrt[l]{\mu^*}$ den Wert $(-1)^{\frac{l-1}{2}} l^l \mu^{*l-1}$ hat, so ist, nach der Beschaffenheit von μ^*, dem Hilfssatze 23 zufolge die Relativdiskriminante des Körpers $k(\mathsf{M}, \zeta)$ in bezug auf $k(\zeta)$ genau durch $\mathfrak{l}^{n-1}$ teilbar.

An zweiter Stelle haben wir den Fall zu untersuchen, daß μ nicht durch $\mathfrak{l}$ teilbar ist. Der für diesen Fall in Satz 148 bezeichnete Exponent $m (\leqq l)$ sei zunächst $= l$; es gebe also eine ganze Zahl α in $k(\zeta)$ derart, daß $\mu \equiv \alpha^l$ nach $\mathfrak{l}^l$ ist; dabei wird dann $\frac{\mu - \alpha^l}{\lambda^l}$ eine ganze Zahl in $k(\zeta)$, und folglich besitzt die Gleichung l-ten Grades in x

$$\frac{(\lambda x - \alpha)^l + \mu}{\lambda^l} = 0$$

lauter ganze Koeffizienten. Da $x = \frac{\alpha - \mathsf{M}}{\lambda}$, wo $\mathsf{M} = \sqrt[l]{\mu}$ gesetzt ist, eine Wurzel dieser Gleichung ist, so erweist sich die Zahl $\Omega = \frac{\alpha - \mathsf{M}}{\lambda}$ des Körpers $k(\mathsf{M}, \zeta)$ als ganze Zahl. Die Relativdiskriminante dieser Zahl Ω ist gleich $\varepsilon \mu^{l-1}$, wo ε eine Einheit bedeutet, und folglich ist auch die Relativdiskriminante des Körpers $k(\mathsf{M}, \zeta)$ in bezug auf $k(\zeta)$ zu $\mathfrak{l}$ prim.

Zweitens sei $m < l$, so daß also μ nicht einer l-ten Potenz nach $\mathfrak{l}^l$ kongruent gesetzt werden kann; wir setzen $\mu \equiv \alpha^l + a\lambda^m$ nach $\mathfrak{l}^{m+1}$, wo α eine ganze Zahl in $k(\zeta)$, ferner m der im Satze erklärte Exponent ist und a eine ganze rationale, nicht durch l teilbare Zahl bedeutet. Wir betrachten nun das Ideal

$$\mathfrak{A} = (\lambda, \alpha - \mathsf{M}).$$

Die Zahl $\frac{\alpha - \mathsf{M}}{\lambda}$ ist sicher keine ganze Zahl, da ihre Relativnorm in bezug auf $k(\zeta)$, d. h. $\frac{\alpha^l - \mu}{\lambda^l}$, wegen $m < l$ eine gebrochene Zahl ist, also ist die Zahl $\alpha - \mathsf{M}$ nicht durch $\mathfrak{l}$ teilbar; mithin ist das Ideal $\mathfrak{A}$ von $\mathfrak{l}$ verschieden. Andererseits ist $\mathfrak{A}$ auch nicht $= 1$, da die Relativnorm der Zahl $\alpha - \mathsf{M}$ wegen

$$N_k(\alpha - \mathsf{M}) = \alpha^l - \mu \equiv -a\lambda^m, \quad ([^{m+1}]) \tag{71}$$

durch $\mathfrak{l}^m$ teilbar ist. Da sich $S\mathfrak{A} = \mathfrak{A}$ erweist, so ist $\mathfrak{A}$ ein ambiges Ideal, und da dasselbe ein Faktor von $\mathfrak{l}$ sein muß, so gehört unter den gegenwärtigen Umständen $\mathfrak{l}$ zur ersten von den drei in § 57 beim Beweise des Satzes 93 unterschiedenen Arten von Primidealen des Unterkörpers, d. h. wir haben $\mathfrak{l} = \mathfrak{L}^l$, wo $\mathfrak{L}$ ein Primideal und offenbar ersten Grades im Körper $k(\mathsf{M}, \zeta)$ bedeutet. Aus der Kongruenz (71) ergibt sich dann $\mathfrak{A} = \mathfrak{L}^m$.

Nunmehr bestimmen wir zwei ganze rationale positive Zahlen a und b, so daß $1 = am - bl$ wird, und setzen

$$\Omega = \frac{(\alpha - \mathsf{M})^a}{\lambda^b}.$$

Wegen $S\,\mathsf{M} = \zeta\,\mathsf{M}$ folgt

$$S\Omega = \frac{(\alpha - \mathsf{M} + \lambda \mathsf{M})^a}{\lambda^b},$$

und wir schließen aus diesem Ausdrucke, daß $\Omega - S\Omega$ genau durch die $(l - m + 1)$-te Potenz von $\mathfrak{L}$ teilbar ist. Da von jeder Differenz aus irgend zwei zu Ω relativ konjugierten Zahlen das gleiche gilt, so enthält die Relativdiskriminante der Zahl Ω in bezug auf $k(\zeta)$ genau die $(l-1)(l-m+1)$-te Potenz des Ideals $\mathfrak{l}$. Hieraus folgt, da Ω nur durch die erste Potenz von $\mathfrak{L}$ teilbar ist, nach Hilfssatz 23, daß auch die Relativdiskriminante des Körpers $k(\mathsf{M}, \zeta)$ in bezug auf $k(\zeta)$ genau durch die angegebene Potenz von $\mathfrak{l}$ teilbar sein muß.

Durch den eben bewiesenen Satz 148 ist die Relativdiskriminante des Kummerschen Körpers $k(\mathsf{M}, \zeta)$ in bezug auf den Körper $k(\zeta)$ völlig bestimmt, und nach Satz 39 kann man aus dieser Relativdiskriminante sogleich auch die Diskriminante des Kummerschen Körpers $k(\mathsf{M}, \zeta)$ finden.

§ 127. Das Symbol $\left\{\frac{\mu}{\mathfrak{w}}\right\}$.

Für die weiteren Entwicklungen ist es nötig, das in § 113 eingeführte Symbol $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ in folgender Weise zu verallgemeinern, so daß es auch in den Fällen eine Bedeutung hat, wo $\mathfrak{w}$ in μ aufgeht, und wo $\mathfrak{w} = \mathfrak{l}$ ist.

Es sei $\mathfrak{w}$ ein beliebiges Primideal in $k(\zeta)$ und μ eine beliebige ganze Zahl in $k(\zeta)$, welche nicht l-te Potenz einer ganzen Zahl in $k(\zeta)$ ist. Wenn dann die

Relativdiskriminante des durch $M = \sqrt[l]{\mu}$ und ζ bestimmten Kummerschen Körpers durch $\mathfrak{w}$ teilbar ist, so habe das **Symbol** $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ den Wert 0.

Ist dagegen die Relativdiskriminante dieses Körpers $k(M, \zeta)$ nicht durch $\mathfrak{w}$ teilbar, so kann man nach Satz 148 stets eine Zahl α in $k(\zeta)$ finden derart, daß $\mu^* = \alpha^l \mu$ eine ganze, nicht mehr durch $\mathfrak{w}$ teilbare Zahl in $k(\zeta)$ wird. Ist μ selbst zu $\mathfrak{w}$ prim, so erfüllt bereits $\alpha = 1$ diese Bedingung. Wir definieren dann, wenn $\mathfrak{w} \neq \mathfrak{l}$ ist, das fragliche **Symbol** durch die Formel

$$\left\{\frac{\mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^*}{\mathfrak{w}}\right\}.$$

Wenn aber $\mathfrak{w} = \mathfrak{l}$ ist, so kann, da die Relativdiskriminante von $k(M, \zeta)$ prim zu $\mathfrak{l}$ sein soll, nach dem Satze 148 die Zahl α überdies so gewählt werden, daß $\mu^* \equiv 1$ nach $\mathfrak{l}^l$ ausfällt. Ist dies geschehen, so gilt eine Kongruenz von der Gestalt

$$\mu^* \equiv 1 + a\lambda^l, \quad (\mathfrak{l}^{l+1}),$$

wo a eine bestimmte Zahl aus der Reihe $0, 1, 2, \ldots, l-1$ bedeutet. Ich definiere dann das **Symbol** $\left\{\frac{\mu}{\mathfrak{l}}\right\}$ durch die Gleichung

$$\left\{\frac{\mu}{\mathfrak{l}}\right\} = \zeta^a.$$

Ist μ die l-te Potenz einer ganzen Zahl in $k(\zeta)$ und $\mathfrak{w}$ ein beliebiges Primideal in $k(\zeta)$, so werde stets $\left\{\frac{\mu}{\mathfrak{w}}\right\} = 1$ genommen.

Auf diese Weise ist der Wert des Symbols $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ für jede ganze Zahl μ und für jedes Primideal $\mathfrak{w}$ in $k(\zeta)$ eindeutig festgelegt, und zwar wird dieser Wert entweder gleich 0 oder gleich einer bestimmten l-ten Einheitswurzel.

Ist endlich $\mathfrak{a}$ ein beliebiges Ideal des Körpers $k(\zeta)$ und hat man $\mathfrak{a} = \mathfrak{p}\mathfrak{q}\ldots\mathfrak{w}$, wo $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{w}$ Primideale in $k(\zeta)$ sind, so möge, wenn μ eine beliebige ganze Zahl in $k(\zeta)$ ist, das **Symbol** $\left\{\frac{\mu}{\mathfrak{a}}\right\}$ durch die folgende Gleichung definiert werden:

$$\left\{\frac{\mu}{\mathfrak{a}}\right\} = \left\{\frac{\mu}{\mathfrak{p}}\right\}\left\{\frac{\mu}{\mathfrak{q}}\right\}\cdots\left\{\frac{\mu}{\mathfrak{w}}\right\}.$$

Sind $\mathfrak{a}, \mathfrak{b}$ beliebige Ideale in $k(\zeta)$, so gilt dann offenbar die Gleichung:

$$\left\{\frac{\mu}{\mathfrak{a}\mathfrak{b}}\right\} = \left\{\frac{\mu}{\mathfrak{a}}\right\}\left\{\frac{\mu}{\mathfrak{b}}\right\}.$$

§ 128. Die Primideale des Kummerschen Körpers.

Es sei μ eine ganze Zahl in $k(\zeta)$, aber $M = \sqrt[l]{\mu}$ keine Zahl dieses Körpers. Die Aufgabe, die Primideale des Kreiskörpers $k(\zeta)$ in Primideale des Kummerschen Körpers $k(M, \zeta)$ zu zerlegen, wird durch folgenden Satz gelöst:

Satz 149. Ein beliebiges Primideal $\mathfrak{p}$ in $k(\zeta)$ ist in dem durch $M = \sqrt[l]{\mu}$ und ζ bestimmten Kummerschen Körper $k(M, \zeta)$ entweder gleich der l-ten

Potenz eines Primideals oder zerlegbar in l voneinander verschiedene Primideale oder selbst Primideal, je nachdem $\left\{\frac{\mu}{\mathfrak{p}}\right\} = 0$ oder $= 1$ oder gleich einer von 1 verschiedenen l-ten Einheitswurzel ausfällt.

Beweis. Der erste Teil dieses Satzes bezieht sich auf die in der Relativdiskriminante des Kummerschen Körpers $k(M, \zeta)$ aufgehenden Primideale; dieselben sind nach Satz 93 ambig. Hieraus oder aus dem Beweise des Satzes 148 ergibt sich für diese Primideale die Richtigkeit der Behauptung.

Wenn $\mathfrak{p}$ ein nicht in der Relativdiskriminante des Körpers $k(M, \zeta)$ aufgehendes Primideal ist, so möge μ^* eine durch $\mathfrak{p}$ nicht teilbare ganze Zahl von der Art sein, daß der Quotient $\frac{\mu^*}{\mu}$ gleich der l-ten Potenz einer Zahl in $k(\zeta)$ ist. Der Körper $k(M, \zeta)$ wird dann auch durch $M^* = \sqrt[l]{\mu^*}$ und ζ festgelegt.

Wir untersuchen zunächst den Fall, daß $\mathfrak{p} \neq \mathfrak{l}$ ist. Wenn dann $\left\{\frac{\mu^*}{\mathfrak{p}}\right\} = 1$ ausfällt, so ist nach Satz 139 die Zahl μ^* ein l-ter Potenzrest nach $\mathfrak{p}$. Wir bestimmen, was offenbar möglich ist, eine ganze Zahl α in $k(\zeta)$ derart, daß

$$\mu^* \equiv \alpha^l, \ (\mathfrak{p}) \quad \text{und} \quad \mu^* \not\equiv \alpha^l, \ (\mathfrak{p}^2)$$

wird; alsdann bilden wir die relativ konjugierte Ideale

$$\begin{aligned} \mathfrak{P} &= (\mathfrak{p}, M^* - \alpha), \\ S\mathfrak{P} &= (\mathfrak{p}, \zeta M^* - \alpha), \\ &\cdots\cdots\cdots \\ S^{l-1}\mathfrak{P} &= (\mathfrak{p}, \zeta^{l-1} M^* - \alpha) \end{aligned}$$

und erhalten leicht

$$\mathfrak{p} = \mathfrak{P} \cdot S\mathfrak{P} \cdots S^{l-1}\mathfrak{P}.$$

Wegen

$$(\mathfrak{P}, S\mathfrak{P}) = (\mathfrak{p}, M^* - \alpha, \zeta M^* - \alpha) = 1$$

ist $S\mathfrak{P}$ von $\mathfrak{P}$, und folglich sind alle l Primfaktoren $\mathfrak{P}, S\mathfrak{P}, \ldots, S^{l-1}\mathfrak{P}$ des Ideals $\mathfrak{p}$ untereinander verschieden. Das Primideal $\mathfrak{p}$ in $k(\zeta)$ gehört also zu der zweiten der drei im Beweise zu Satz 93 aufgezählten Arten von Primidealen des Unterkörpers: es zerfällt in $k(M, \zeta)$ in l voneinander verschiedene Primideale. Umgekehrt, wenn ein Primideal $\mathfrak{p}$ des Körpers $k(\zeta)$, wo jetzt $\mathfrak{p}$ auch $= \mathfrak{l}$ sein kann, in l voneinander verschiedene Primideale $\mathfrak{P}, S\mathfrak{P}, \ldots, S^{l-1}\mathfrak{P}$ des Körpers $k(M, \zeta)$ zerfällt, so wird, wenn p die durch $\mathfrak{p}$ teilbare rationale Primzahl und $N(\mathfrak{P}) = p^f$ die Norm von $\mathfrak{P}$ ist,

$$N(\mathfrak{p}) = N(\mathfrak{P})N(S\mathfrak{P}) \cdots N(S^{l-1}\mathfrak{P}) = p^{lf},$$

und mithin ist die Norm von $\mathfrak{p}$, im Körper $k(\zeta)$ genommen, $n(\mathfrak{p})$, ebenfalls gleich p^f. Die Gleichheit der Normen $N(\mathfrak{P})$ und $n(\mathfrak{p})$ läßt, wie in § 57, die Tatsache erkennen, daß eine jede ganze Zahl des Körpers $k(M, \zeta)$ einer ganzen Zahl

des Körpers $k(\zeta)$ nach $\mathfrak{P}$ kongruent gesetzt werden kann; setzen wir insbesondere $\mathsf{M}^* \equiv \alpha$ nach $\mathfrak{P}$, wo α in $k(\zeta)$ liegen soll, so folgt $\mathsf{M}^{*l} = \mu^* \equiv \alpha^l$ nach $\mathfrak{P}$, und da $\mu^* - \alpha^l$ eine Zahl in $k(\zeta)$ ist, so muß $\mu^* \equiv \alpha^l$ auch nach $\mathfrak{p}$ sein, d. h. es gilt $\left\{\frac{\mu^*}{\mathfrak{p}}\right\} = \left\{\frac{\mu}{\mathfrak{p}}\right\} = 1$. Damit ist zugleich für ein von $\mathfrak{l}$ verschiedenes Primideal $\mathfrak{p}$ der letzte Teil des Satzes 149 vollständig bewiesen.

Was endlich das Primideal $\mathfrak{l}$ anbetrifft, so gilt, falls die Relativdiskriminante des Körpers $k(\mathsf{M}, \zeta)$ in bezug auf $k(\zeta)$ durch $\mathfrak{l}$ nicht teilbar ist, für die Zahl μ^* dem Satze 148 gemäß eine Kongruenz von der Gestalt

$$\mu^* \equiv \alpha^l + a\lambda^l, \quad (\mathfrak{l}^{l+1}),$$

wo a eine ganze rationale Zahl bedeutet. Soll nun $\left\{\frac{\mu}{\mathfrak{l}}\right\} = 1$, d. h. a durch l teilbar sein, so folgt daraus eine Kongruenz von der Gestalt

$$\mu^* \equiv \alpha^l + a^*\lambda^{l+1}, \quad (\mathfrak{l}^{l+2}),$$

wo a^* wiederum eine ganze rationale Zahl bedeutet. Ist hierin a^* nicht durch l teilbar, so setzen wir $\mu^{**} = \mu^*$; ist dagegen a^* durch l teilbar, so setzen wir $\mu^{**} = (1+\lambda)^l\mu^* = (1-\lambda^2)^l\mu^*$, dann folgt

$$\mu^{**} \equiv \alpha^l + \lambda^{l+1}\alpha^l, \quad (\mathfrak{l}^{l+2}).$$

Demnach genügt die Zahl μ^{**} stets einer Kongruenz

$$\mu^{**} \equiv \alpha^l + a^{**}\lambda^{l+1}, \quad (\mathfrak{l}^{l+2}),$$

wo nun a^{**} eine ganze rationale, nicht durch l teilbare Zahl bedeutet, und hieraus folgt, wenn $\mathsf{M}^{**} = \sqrt[l]{\mu^{**}}$ und

$$\mathfrak{L} = \left(\lambda, \frac{\alpha - \mathsf{M}^{**}}{\lambda}\right)$$

gesetzt wird, für $\mathfrak{l}$ die Zerlegung

$$\mathfrak{l} = \mathfrak{L} \cdot S\mathfrak{L} \cdots S^{l-1}\mathfrak{L}.$$

Wegen

$$\left(\lambda, \frac{\alpha - \mathsf{M}^{**}}{\lambda}, \frac{\alpha - \zeta\mathsf{M}^{**}}{\lambda}\right) = 1$$

ist $S\mathfrak{L}$ von $\mathfrak{L}$ verschieden, und daher sind auch alle l Primideale $\mathfrak{L}, S\mathfrak{L}, \ldots, S^{l-1}\mathfrak{L}$ untereinander verschieden.

Umgekehrt, wenn $\mathfrak{l}$ eine Zerlegung dieser Art im Kummerschen Körper $k(\mathsf{M}, \zeta)$ gestattet, so stimmen nach einer oben gemachten und, wie dort erwähnt, auch für $\mathfrak{p} = \mathfrak{l}$ zutreffenden Bemerkung die Normen von $\mathfrak{L}$ in $k(\mathsf{M}, \zeta)$ und von $\mathfrak{l}$ in $k(\zeta)$ überein, und es muß daher jede ganze Zahl des Körpers $k(\mathsf{M}, \zeta)$ einer ganzen Zahl des Körpers $k(\zeta)$ nach $\mathfrak{L}$ kongruent sein. Da $\mathfrak{l}$ alsdann nach Satz 93 gewiß nicht in der Relativdiskriminante des Körpers $k(\mathsf{M}, \zeta)$ in bezug auf $k(\zeta)$ enthalten ist, so können wir nach Satz 148 $\mu^* \equiv \alpha^l$ nach $\mathfrak{l}^l$ setzen, und demgemäß ist $\frac{\alpha - \mathsf{M}^*}{\lambda}$ eine ganze Zahl. Da $\mathfrak{L}$ ein Primideal

ersten Grades in $k(\mathsf{M}, \zeta)$ wird, so können wir diese ganze Zahl kongruent a nach $\mathfrak{L}$ setzen, so daß a eine ganze rationale Zahl bedeutet; dann folgt, wenn N_k als Bezeichnung der Relativnorm in bezug auf $k(\zeta)$ dient, die Kongruenz

$$N_k\left(\frac{\alpha - \mathsf{M}^*}{\lambda} - a\right) \equiv 0, \qquad (\mathfrak{l}),$$

d. h.

$$(\alpha - a\lambda)^l - \mu^* \equiv 0, \qquad (\mathfrak{l}^{l+1});$$

es ist mithin $\left\{\frac{\mu^*}{\mathfrak{l}}\right\} = \left\{\frac{\mu}{\mathfrak{l}}\right\} = 1$. Diese Tatsachen beweisen auch für das Primideal $\mathfrak{l}$ den letzten Teil des Satzes 149.

Durch den Satz 149 haben wir ein einfaches Mittel erlangt, um die im Beweise des Satzes 93 aufgezählten drei Arten von Primidealen eines Körpers in Hinsicht auf einen relativ-zyklischen Oberkörper von einem Primzahlrelativgrade für den vorliegenden Fall der Körper $k(\mathsf{M}, \zeta)$ und $k(\zeta)$ zu unterscheiden.

29. Die Normenreste und Normennichtreste des Kummerschen Körpers.

§ 129. Die Definition der Normenreste und Normennichtreste.

Es sei, wie in § 125, μ eine Zahl des Kreiskörpers $k(\zeta)$, für welche $\mathsf{M} = \sqrt[l]{\mu}$ nicht in $k(\zeta)$ liegt, und es bedeute $k(\mathsf{M}, \zeta)$ den durch M und ζ bestimmten Kummerschen Körper; für eine Zahl A in $k(\mathsf{M}, \zeta)$ werde die Relativnorm in bezug auf $k(\zeta)$ mit $N_k(\mathsf{A})$ bezeichnet. Es sei $\mathfrak{w}$ ein beliebiges Primideal des Kreiskörpers $k(\zeta)$ und ν eine beliebige ganze Zahl in $k(\zeta)$. Wenn dann ν nach $\mathfrak{w}$ der Relativnorm einer ganzen Zahl des Körpers $k(\mathsf{M}, \zeta)$ kongruent ist, und wenn außerdem auch für jede höhere Potenz von $\mathfrak{w}$ stets eine solche ganze Zahl A im Körper $k(\mathsf{M}, \zeta)$ gefunden werden kann, daß $\nu \equiv N_k(\mathsf{A})$ nach jener Potenz von $\mathfrak{w}$ ausfällt, so nenne ich ν einen **Normenrest des Kummerschen Körpers $k(\mathsf{M}, \zeta)$ nach $\mathfrak{w}$**. In jedem anderen Falle nenne ich ν einen **Normennichtrest des Kummerschen Körpers $k(\mathsf{M}, \zeta)$ nach $\mathfrak{w}$**.

§ 130. Der Satz von der Anzahl der Normenreste. Die Verzweigungsideale.

Es gilt der folgende wichtige Satz:

Satz 150. *Wenn $\mathfrak{w}$ ein Primideal des Kreiskörpers $k(\zeta)$ ist, das nicht in der Relativdiskriminante des Kummerschen Körpers $k(\mathsf{M}, \zeta)$ aufgeht, so ist jede zu $\mathfrak{w}$ prime Zahl ν in $k(\zeta)$ Normenrest des Kummerschen Körpers $k(\mathsf{M}, \zeta)$ nach $\mathfrak{w}$.*

Wenn dagegen $\mathfrak{w}$ ein Primideal des Kreiskörpers $k(\zeta)$ ist, das in der Relativdiskriminante des Kummerschen Körpers $k(\mathsf{M}, \zeta)$ aufgeht, und e im Falle $\mathfrak{w} \neq \mathfrak{l}$ ein beliebiger positiver Exponent, im Falle $\mathfrak{w} = \mathfrak{l}$ ein beliebiger Exponent $> l$ ist, so sind von allen vorhandenen, zu $\mathfrak{w}$ primen und nach $\mathfrak{w}^e$ einander inkongruenten Zahlen in $k(\zeta)$ genau der l-te Teil Normenreste nach $\mathfrak{w}$.

Beweis. Es sei zunächst $\mathfrak{w}$ ein in der Relativdiskriminante des Körpers $k(\mathsf{M},\zeta)$ nicht aufgehendes und von $\mathfrak{l}$ verschiedenes Primideal des Kreiskörpers $k(\zeta)$; dann sind zwei Fälle zu unterscheiden, je nachdem $\mathfrak{w}$ in $k(\mathsf{M},\zeta)$ zerlegbar ist oder nicht. Im ersteren Falle sei $\mathfrak{W}$ ein in $\mathfrak{w}$ aufgehendes Primideal des Kummerschen Körpers $k(\mathsf{M},\zeta)$. Im Hinblick auf den Beweis zu Satz 148 können wir, ohne dadurch eine Beschränkung einzuführen, annehmen, es sei μ und mithin auch die Relativdiskriminante der Zahl $\mathsf{M} = \sqrt[l]{\mu}$ in bezug auf $k(\zeta)$ nicht durch $\mathfrak{W}$ teilbar; es gibt dann gewiß im Körper $k(\mathsf{M},\zeta)$ ein System von l ganzen Zahlen $\mathsf{A}_1, \ldots, \mathsf{A}_l$, für welche die l Kongruenzen

$$\left.\begin{aligned} &\mathsf{A}_1 + \mathsf{A}_2\mathsf{M} \quad + \cdots + \mathsf{A}_l\mathsf{M}^{l-1} \quad \equiv \nu,\\ &\mathsf{A}_1 + \mathsf{A}_2\zeta\mathsf{M} \quad + \cdots + \mathsf{A}_l(\zeta\mathsf{M})^{l-1} \quad \equiv 1,\\ &\mathsf{A}_1 + \mathsf{A}_2\zeta^2\mathsf{M} \quad + \cdots + \mathsf{A}_l(\zeta^2\mathsf{M})^{l-1} \quad \equiv 1,\\ &\quad\cdots\cdots\cdots\cdots\cdots\cdots\\ &\mathsf{A}_1 + \mathsf{A}_2\zeta^{l-1}\mathsf{M} + \cdots + \mathsf{A}_l(\zeta^{l-1}\mathsf{M})^{l-1} \equiv 1, \end{aligned}\right\} (\mathfrak{W})$$

erfüllt sind. Nun ist offenbar jede ganze Zahl des Körpers $k(\mathsf{M},\zeta)$ nach $\mathfrak{W}$ einer ganzen Zahl in $k(\zeta)$ kongruent; setzen wir

$$\mathsf{A}_1 \equiv \alpha_1, \qquad \mathsf{A}_2 \equiv \alpha_2, \ldots, \mathsf{A}_l \equiv \alpha_l, \qquad (\mathfrak{W}),$$

so daß $\alpha_1, \alpha_2, \ldots, \alpha_l$ ganze Zahlen in $k(\zeta)$ sind, und

$$\mathsf{A} = \alpha_1 + \alpha_2\mathsf{M} + \cdots + \alpha_l\mathsf{M}^{l-1},$$

so ergibt sich daher

$$\nu \equiv \mathsf{A}, \qquad 1 \equiv S\mathsf{A}, \ldots, 1 \equiv S^{l-1}\mathsf{A}, \qquad (\mathfrak{W}),$$

und durch Multiplikation folgt $\nu \equiv N_k(\mathsf{A})$ nach $\mathfrak{W}$ und daher auch nach $\mathfrak{w}$. Damit ist unter der gegenwärtigen Annahme über das Primideal $\mathfrak{w}$ der erste Teil des Satzes für den Fall $e = 1$ bewiesen. Um zu den Fällen $e > 1$ überzugehen, nehmen wir an, es sei $\nu \not\equiv N_k(\mathsf{A})$ nach $\mathfrak{w}^2$, und setzen dann

$$\frac{\nu}{N_k(\mathsf{A})} \equiv 1 + \omega, \qquad (\mathfrak{w}^2),$$

so daß dabei ω eine ganze, durch $\mathfrak{w}$, aber nicht durch $\mathfrak{w}^2$ teilbare Zahl in $k(\zeta)$ bedeutet. Die ganze Zahl $\mathsf{B} = \mathsf{A}(1 + l^*\omega)$, wobei l^* eine ganze rationale, der Kongruenz $ll^* \equiv 1$ nach $\mathfrak{w}$ genügende Zahl sein soll, erfüllt dann die Bedingung $\nu \equiv N_k(\mathsf{B})$ nach $\mathfrak{w}^2$. Durch die gehörige Fortsetzung des hier eingeschlagenen Verfahrens gelangen wir schließlich zu einer ganzen Zahl in $k(\mathsf{M},\zeta)$, deren Relativnorm in bezug auf $k(\zeta)$ der Zahl ν nach einer beliebig hohen Potenz $\mathfrak{w}^e$ kongruent ist.

Es sei andererseits $\mathfrak{w}$ im Körper $k(\mathsf{M},\zeta)$ nicht weiter zerlegbar; wir können es wiederum einrichten, daß μ nicht durch $\mathfrak{w}$ teilbar sei, und es ist dann nach Satz 149 μ jedenfalls kein l-ter Potenzrest nach $\mathfrak{w}$. Nach den

Folgerungen aus Satz 139 gibt es in $k(\zeta)$ genau $r = \frac{n(\mathfrak{w})-1}{l}$ zu $\mathfrak{w}$ prime l-te Potenzreste nach $\mathfrak{w}$; sind diese nach $\mathfrak{w}$ durch $\varrho_1, \ldots, \varrho_r$ vertreten, so fallen die $n(\mathfrak{w}) - 1$ Zahlen

$$\varrho_i\mu^g \qquad \begin{pmatrix} i = 1, 2, \ldots, r,\\ g = 0, 1, 2, \ldots, l-1 \end{pmatrix}$$

sämtlich nach $\mathfrak{w}$ untereinander inkongruent aus, da μ nicht l-ter Potenzrest nach $\mathfrak{w}$ ist, und es ist also jede zu $\mathfrak{w}$ prime Zahl in $k(\zeta)$ einer dieser Zahlen nach $\mathfrak{w}$ kongruent. Setzen wir $\varrho_1 \equiv \alpha_1^l, \ldots, \varrho_r \equiv \alpha_r^l$ nach $\mathfrak{w}$, so daß $\alpha_1, \ldots, \alpha_r$ ebenfalls Zahlen in $k(\zeta)$ sind, so folgt

$$\varrho_i\mu^g \equiv N_k(\alpha_i\mathsf{M}^g), \qquad (\mathfrak{w}),$$

und es ist also jede zu $\mathfrak{w}$ prime Zahl in $k(\zeta)$ der Norm einer geeigneten Zahl in $k(\mathsf{M},\zeta)$ nach $\mathfrak{w}$ kongruent; hieraus schließt man weiter, ähnlich wie im vorigen Falle, daß zu jeder zu $\mathfrak{w}$ primen ganzen Zahl ν in $k(\zeta)$ auch in bezug auf eine beliebig hohe Potenz $\mathfrak{w}^e$ von $\mathfrak{w}$ stets eine ganze Zahl des Körpers $k(\mathsf{M},\zeta)$ gefunden werden kann, deren Relativnorm nach $\mathfrak{w}^e$ der Zahl ν kongruent ist.

Wir wollen nun den ersten Teil des Satzes 150 auch für den Fall $\mathfrak{w} = \mathfrak{l}$ beweisen, dabei können wir μ zu $\mathfrak{l}$ prim annehmen; wir bezeichnen mit λ^m die höchste in $\mu^{l-1} - 1$ enthaltene Potenz von λ, wobei jedenfalls $m \geqq 1$ sein wird, und setzen

$$\mu^{l-1} \equiv 1 + a\lambda^m, \qquad (\mathfrak{l}^{m+1}),$$

wo a eine ganze rationale, zu l prime Zahl bedeuten soll. Ist dann a^* eine ganze rationale Zahl mit der Kongruenzeigenschaft $aa^* \equiv -1$ nach l, und setzen wir $\mu^* = \mu^{a^*(l-1)}$, so wird

$$\mu^* \equiv 1 - \lambda^m, \qquad (\mathfrak{l}^{m+1}). \tag{72}$$

Andererseits gelten die Kongruenzen

$$\left.\begin{aligned} &(1-\lambda^{g+1})^l \equiv 1 + \lambda^{l+g}\\ &(1-\lambda^{g+1})^{hl} \equiv 1 + h\lambda^{l+g} \end{aligned}\right\}, \qquad (\mathfrak{l}^{l+g+1}), \tag{73}$$

wo g eine jede positive ganze rationale Zahl und h eine jede positive ganze rationale zu l prime Zahl sein kann. Da die Relativdiskriminante des Körpers $k(\mathsf{M},\zeta)$ in bezug auf $k(\zeta)$ im gegenwärtig zu untersuchenden Falle den Faktor $\mathfrak{l}$ nicht enthalten soll, so ist nach Satz 148 notwendig $m \geqq l$.

Es sei zunächst $m = l$. Man entnimmt dann leicht aus den Kongruenzen (72) und (73), daß zu jeder beliebigen positiven ganzen rationalen Zahl g stets eine ganze Zahl α_g in $k(\zeta)$ gefunden werden kann derart, daß die Kongruenz

$$\mu^*\alpha_g^l \equiv 1 - \lambda^l + \lambda^{l+g}, \qquad (\mathfrak{l}^{l+g+1})$$

erfüllt wird. Setzen wir nun $M^* = \sqrt[l]{\mu^*}$ und ferner allgemein für jeden Wert von g:

$$\Omega_g = \frac{1 - \alpha_g M^*}{\lambda},$$

so wird jedesmal Ω_g eine ganze Zahl in $k(M, \zeta)$ und

$$N_k(\Omega_g) \equiv 1 - \lambda^g, \qquad ([^{g+1}).$$

Hieraus folgt unmittelbar, daß jede ganze Zahl ν in $k(\zeta)$, die der Kongruenz $\nu \equiv 1$ nach $\mathfrak{l}$ genügt, Normenrest des Körpers $k(M, \zeta)$ nach $\mathfrak{l}$ ist. Die Beschränkung, die hier in der Annahme $\nu \equiv 1$ nach $\mathfrak{l}$ liegt, wird leicht aufgehoben. Ist nämlich ν eine beliebige zu $\mathfrak{l}$ prime Zahl, und wird sie nach $\mathfrak{l}$ der ganzen rationalen Zahl a kongruent, so setzen wir $\nu^* = a^{*l}\nu$, wo a^* eine ganze rationale Zahl mit der Kongruenzeigenschaft $aa^* \equiv 1$ nach $\mathfrak{l}$ bedeute; dann wird offenbar $\nu^* \equiv 1$ nach $\mathfrak{l}$, und andererseits werden ν und ν^* gleichzeitig Normenrest oder Normennichtrest des Körpers $k(M, \zeta)$ nach $\mathfrak{l}$ sein.

Es sei zweitens in Formel (72) $m > l$ und mithin $\left\{\frac{\mu^*}{\mathfrak{l}}\right\} = 1$; dann können wir, wenn g eine beliebige positive ganze rationale Zahl ist, stets zwei ganze Zahlen α_g und α_{g+1} in $k(\zeta)$ konstruieren derart, daß

$$\left.\begin{aligned} \mu^* \alpha_g^l &\equiv 1 + \lambda^{l+1} + \lambda^{l+g+1}, \qquad ([^{l+g+2}), \\ \mu^* \alpha_{g+1}^l &\equiv 1 + \lambda^{l+1} + \lambda^{l+g+2}, \qquad ([^{l+g+3}) \end{aligned}\right\} \tag{74}$$

wird. Wir setzen gemäß dem Satze 149 $\mathfrak{l} = \mathfrak{L}\mathfrak{L}' \ldots \mathfrak{L}^{(l-1)}$, wo $\mathfrak{L}, \mathfrak{L}', \ldots, \mathfrak{L}^{(l-1)}$ voneinander verschiedene Primideale des Körpers $k(M, \zeta)$ bedeuten. Die beiden Zahlen

$$A_g = \frac{1 - \alpha_g M^*}{\lambda}, \qquad A_{g+1} = \frac{1 - \alpha_{g+1} M^*}{\lambda},$$

$M^* = \sqrt[l]{\mu^*}$ gesetzt, sind ganze Zahlen, und da $N_k(A_g) \equiv -\lambda$ nach $\mathfrak{l}^2$ wird, so enthält A_g eines der in $\mathfrak{l}$ aufgehenden Primideale, es sei dies etwa das Primideal $\mathfrak{L}$, zur ersten Potenz und die anderen in $\mathfrak{l}$ aufgehenden Primideale gar nicht. Aus den Formeln (74) folgt

$$\alpha_g^l \equiv \alpha_{g+1}^l, \qquad ([^{l+2}),$$

und wir können nun voraussetzen, daß α_{g+1} in der Reihe der Zahlen $\alpha_{g+1}, \zeta\alpha_{g+1}, \ldots, \zeta^{l-1}\alpha_{g+1}$ in solcher Weise gewählt sei, daß $\alpha_g \equiv \alpha_{g+1}$ nach $\mathfrak{l}^2$ und also $A_g \equiv A_{g+1}$ nach $\mathfrak{l}$ ausfällt. Wegen der letzteren Kongruenz ist auch die Zahl A_{g+1} durch $\mathfrak{L}$, aber durch keines der Primideale $\mathfrak{L}', \ldots, \mathfrak{L}^{(l-1)}$ teilbar und da auch $N_k(A_{g+1}) \equiv -\lambda$ nach $\mathfrak{l}^2$ ist, so ist A_{g+1} ebenfalls nur durch die erste Potenz von $\mathfrak{L}$ teilbar. Wir können mit Rücksicht auf das eben Bewiesene die gebrochene Zahl $\frac{A_g}{A_{g+1}}$ in der Form eines Bruches schreiben, dessen Zähler und Nenner zu $\mathfrak{l}$ prim sind. Setzen wir $\frac{A_g}{A_{g+1}} \equiv \Omega_g$ nach $\mathfrak{l}^{g+1}$ in solcher Weise,

daß Ω_g eine ganze Zahl in $k(M, \zeta)$ ist, so wird

$$N_k(\Omega_g) \equiv \frac{N_k(A_g)}{N_k(A_{g+1})} \equiv 1 + \lambda^g, \qquad ([^{g+1}).$$

Da eine solche Formel für jeden positiven Exponenten g möglich ist, so zeigt sich wie vorhin, daß jede zu $\mathfrak{l}$ prime Zahl Normenrest des Körpers $k(M, \zeta)$ ist.

Wir gehen jetzt zum Beweise der zweiten Hälfte von Satz 150 über. Es sei zunächst $\mathfrak{w}$ ein von $\mathfrak{l}$ verschiedenes, in der Relativdiskriminante des Körpers $k(M, \zeta)$ in bezug auf $k(\zeta)$ aufgehendes Primideal des Körpers $k(\zeta)$; wir haben dann nach Satz 149 $\mathfrak{w} = \mathfrak{W}^l$, wo $\mathfrak{W}$ ein Primideal in $k(M, \zeta)$ ist. Jede ganze Zahl des Körpers $k(M, \zeta)$ muß dann, wie schon mehrfach erwähnt wurde, einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{W}$ kongruent sein. Soll nun eine gegebene, zu $\mathfrak{w}$ prime ganze Zahl ν in $k(\zeta)$ nach $\mathfrak{w}$ kongruent der Relativnorm $N_k(A)$ einer ganzen Zahl A in $k(M, \zeta)$ sein, und setzen wir $A \equiv \alpha$ nach $\mathfrak{W}$, so folgt notwendig $\nu \equiv \alpha^l$ nach $\mathfrak{W}$, und daher auch nach $\mathfrak{w}$, d. h. ν ist l-ter Potenzrest nach $\mathfrak{w}$. Umgekehrt, wenn eine Zahl ν in $k(\zeta)$ ein l-ter Potenzrest nach $\mathfrak{w}$ ist, so ist ν offenbar auch kongruent einer Relativnorm $N_k(A)$ nach $\mathfrak{w}$. Wir entnehmen hieraus, daß die l-ten Potenzreste nach $\mathfrak{w}$ auch zugleich die sämtlichen Normenreste des Körpers $k(M, \zeta)$ nach $\mathfrak{w}$ liefern.

Es bleibt endlich die Behandlung des Falles übrig, daß $\mathfrak{w} = \mathfrak{l}$ ist und $\mathfrak{l}$ in der Relativdiskriminante des Körpers $k(M, \zeta)$ aufgeht. Wir haben in diesem Falle $\mathfrak{l} = \mathfrak{L}^l$, wo $\mathfrak{L}$ ein Primideal in $k(M, \zeta)$ ist, und können es im Hinblick auf Satz 148 stets einrichten, daß die Zahl μ entweder der Kongruenz

$$\mu \equiv \lambda, \qquad ([^2)$$

oder einer der folgenden Kongruenzen genügt:

$$\mu \equiv 1 + \lambda^m, \qquad ([^{m+1}),$$

wo m einen der Werte $1, 2, \ldots, l-1$ bedeutet. Wir wollen alsdann untersuchen, welche Zahlen in $k(\zeta)$ es in diesen zwei Fällen gibt, die kongruent der Relativnorm einer Zahl in $k(M, \zeta)$ nach $\mathfrak{l}^{l+1}$ bez. $\mathfrak{l}^l$ sind, und entnehmen hieraus leicht die Anzahl der nach jeder höheren Potenz von $\mathfrak{l}$ einander inkongruenten Normenreste.

Im Falle $\mu \equiv \lambda$ nach $\mathfrak{l}^2$ ist M durch $\mathfrak{L}$, aber nicht durch $\mathfrak{L}^2$ teilbar, und es gelten die Kongruenzen

$$\left.\begin{aligned} &N_k(1 + M) \equiv 1 + \lambda, && ([^2), \\ &N_k(1 + M) \equiv 1 + \lambda + \lambda^2 \varrho_1, && ([^{l+1}), \\ \text{d. i.} \quad &N_k(1 + M^2) \equiv 1 + \lambda^2, && ([^3), \\ &N_k(1 + M^2) \equiv 1 + \lambda^2 + \lambda^3 \varrho_2, && ([^{l+1}), \\ &\cdots\cdots\cdots

wo $\varrho_1, \varrho_2, \ldots, \varrho_{l-1}$ gewisse ganze Zahlen in $k(\zeta)$ bedeuten. Endlich ist

$$N_k(1+\lambda^t \mathsf{M}^g) \equiv 1, \qquad (\mathfrak{l}^{t+1}) \tag{76}$$

für $t = 1, 2, 3, \ldots$; $g = 0, 1, 2, \ldots, l-1$. Nun genügt offenbar jede zu $\mathfrak{L}$ prime ganze Zahl A des Körpers $k(\mathsf{M}, \zeta)$ einer Kongruenz von der Gestalt

$$\begin{aligned} \mathsf{A} \equiv a\,(1+\mathsf{M})^{a_1} \quad & (1+\mathsf{M}^2)^{a_2} \quad \ldots (1+\mathsf{M}^{l-1})^{a_{l-1}} \cdot \\ (1+\lambda\,\mathsf{M})^{a_1'} \quad & (1+\lambda\,\mathsf{M}^2)^{a_2'} \quad \ldots (1+\lambda\,\mathsf{M}^{l-1})^{a_{l-1}'} \cdot \\ & \ldots\ldots\ldots\ldots\ldots\ldots \\ (1+\lambda^t\mathsf{M})^{a_1^{(t)}} & (1+\lambda^t\mathsf{M}^2)^{a_2^{(t)}} \ldots (1+\lambda^t\mathsf{M}^{l-1})^{a_{l-1}^{(t)}}, \qquad (\mathfrak{l}^{t+1}), \end{aligned}$$

wo a eine bestimmte der Zahlen $1, 2, \ldots, l-1$ und die $(l+1)(l-1)$ Exponenten $a_1, a_2, \ldots, a_{l-1}^{(t)}$ bestimmte ganze rationale Zahlen aus der Reihe $0, 1, 2, \ldots, l-1$ sind. Wegen der Kongruenzen (75) und (76) folgt daher:

$$N_k(\mathsf{A}) \equiv a^l (1+\lambda+\lambda^2\varrho_1)^{a_1}(1+\lambda^2+\lambda^3\varrho_2)^{a_2}\ldots(1+\lambda^{l-1}+\lambda^l\varrho_{l-1})^{a_{l-1}}, \quad (\mathfrak{l}^{l+1}).$$

Der Ausdruck rechter Hand stellt, wenn a die Werte $1, 2, \ldots, l-1$ und die Exponenten $a_1, a_2, \ldots, a_{l-1}$ unabhängig voneinander je die Werte $0, 1, 2, \ldots, l-1$ durchlaufen, genau $(l-1)\,l^{l-1}$ Zahlen dar, und diese sind, wie leicht ersichtlich, alle einander inkongruent nach $\mathfrak{l}^{l+1}$. Nun ist jede zu $\mathfrak{l}$ prime Zahl in $k(\zeta)$, welche der Relativnorm $N_k(\mathsf{A})$ einer Zahl A in $k(\mathsf{M},\zeta)$ kongruent nach $\mathfrak{l}^{l+1}$ ist, notwendig einem Ausdruck dieser Gestalt nach $\mathfrak{l}^{l+1}$ kongruent, und umgekehrt ist auch jeder Ausdruck von dieser Gestalt, wie man aus (75) entnimmt, der Relativnorm einer Zahl in $k(\mathsf{M},\zeta)$ nach $\mathfrak{l}^{l+1}$ kongruent. Mit Hilfe der Kongruenzen (73) erkennt man, daß zwei nach $\mathfrak{l}^{l+1}$ kongruente, zu $\mathfrak{l}$ prime Zahlen in $k(\zeta)$ stets gleichzeitig Normenrest oder Normennichtrest nach $\mathfrak{l}$ sind. Die Anzahl der Normenreste nach $\mathfrak{l}$, welche zu $\mathfrak{l}$ prim und untereinander inkongruent nach $\mathfrak{l}^{l+1}$ sind, ist also genau gleich $(l-1)\,l^{l-1}$, d. i. gleich dem l-ten Teil der nach $\mathfrak{l}^{l+1}$ möglichen inkongruenten, zu $\mathfrak{l}$ primen Zahlen in $k(\zeta)$, und dieses Resultat kann sofort auf die Potenzen $\mathfrak{l}^e$ mit Exponenten $e > l+1$ ausgedehnt werden.

Von den übrigen möglichen Annahmen über μ werde hier der Kürze wegen nur die einfachste behandelt; es werde nämlich $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ zugrunde gelegt. Setzen wir dann $\Omega = \mathsf{M}-1$, so ist Ω eine durch $\mathfrak{L}$, aber nicht durch $\mathfrak{L}^2$ teilbare ganze Zahl in $k(\mathsf{M},\zeta)$, und wenn wir berücksichtigen, daß $N_k(\Omega) \equiv \lambda$ nach $\mathfrak{l}^2$ wird, so erkennen wir durch eine leichte Rechnung die Richtigkeit der Kongruenzen

$$\left.\begin{array}{lll} & N_k(1+\Omega) \equiv 1+\lambda, & (\mathfrak{l}^2), \\ \text{d. i.} & N_k(1+\Omega) \equiv 1+\lambda+\lambda^2\varrho_1, & (\mathfrak{l}^3), \\ & N_k(1+\Omega^2) \equiv 1+\lambda^2, & (\mathfrak{l}^3), \\ \text{d. i.} & N_k(1+\Omega^2) \equiv 1+\lambda^2+\lambda^3\varrho_2, & (\mathfrak{l}^4), \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ & N_k(1+\Omega^{l-2}) \equiv 1+\lambda^{l-2}, & (\mathfrak{l}^{l-1}), \\ \text{d. i.} & N_k(1+\Omega^{l-2}) \equiv 1+\lambda^{l-2}+\lambda^{l-1}\varrho_{l-2}, & (\mathfrak{l}^l), \end{array}\right| \tag{77}$$

wo $\varrho_1, \varrho_2, \ldots, \varrho_{l-2}$ gewisse ganze Zahlen in $k(\zeta)$ bedeuten. Wir haben ferner

$$N_k(1+\Omega^{l-1}) = 1+\Sigma_1+\Sigma_2+\Sigma_3+\cdots+\Sigma_{l-1}+N_k(\Omega^{l-1}),$$

wo zur Abkürzung

$$\begin{aligned} \Sigma_1 &= \Omega^{l-1} + (S\Omega)^{l-1} + \cdots + (S^{l-1}\Omega)^{l-1}, \\ \Sigma_2 &= \Omega^{l-1}(S\Omega)^{l-1} + \Omega^{l-1}(S^2\Omega)^{l-1} + \cdots + (S^{l-2}\Omega)^{l-1}(S^{l-1}\Omega)^{l-1}, \\ \Sigma_3 &= \Omega^{l-1}(S\Omega)^{l-1}(S^2\Omega)^{l-1} + \cdots + (S^{l-3}\Omega)^{l-1}(S^{l-2}\Omega)^{l-1}(S^{l-1}\Omega)^{l-1}, \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

gesetzt ist. Nun ergibt sich sofort $\Sigma_1 \equiv l$. Die einzelnen Summanden in den Ausdrücken für $\Sigma_2, \Sigma_3, \ldots, \Sigma_{l-1}$ sind sämtlich jedenfalls durch $\mathfrak{L}^l$ teilbar, sie lassen sich ferner in Aggregate von je l Summanden zusammenfassen, die aus einem beliebigen unter ihnen durch die Substitutionen $1, S, S^2, \ldots, S^{l-1}$ hervorgehen; setzen wir nun ein beliebiges Glied in der Gestalt $\lambda\Phi$ an, so bedeutet Φ eine ganze Zahl in $k(\mathsf{M},\zeta)$ und kann daher, wie aus dem Beweise des Hilfssatzes 23 hervorgeht, als ganze rationale Funktion von Ω und mithin auch von M dargestellt werden, deren Koeffizienten ganze oder gebrochene Zahlen in $k(\zeta)$ mit lauter zu $\mathfrak{l}$ primen Nennern sind. Setzen wir dementsprechend $\Phi = F(\mathsf{M})$, so läßt sich das betreffende Aggregat von l Summanden in die Form

$$\lambda\{F(\mathsf{M}) + F(\zeta\,\mathsf{M}) + F(\zeta^2\mathsf{M}) + \cdots + F(\zeta^{l-1}\mathsf{M})\}$$

bringen; die hier in der Klammer stehende Summe fällt, wie leicht ersichtlich, stets kongruent 0 nach l aus; danach müssen nun die Zahlen $\Sigma_2, \Sigma_3, \ldots, \Sigma_{l-1}$ sämtlich kongruent 0 nach $\mathfrak{l}^l$ sein, also wird

$$N_k(1+\Omega^{l-1}) \equiv 1+l+\lambda^{l-1} \equiv 1, \qquad (\mathfrak{l}^l). \tag{78}$$

Endlich ergeben sich leicht die Kongruenzen

$$N_k(1+\lambda^t\Omega^g) \equiv 1, \qquad (\mathfrak{l}^t) \tag{79}$$

für $t = 1, 2, 3, \ldots$; $g = 1, 2, 3, \ldots, l-1$.

Nun genügt offenbar jede zu $\mathfrak{L}$ prime ganze Zahl in $k(\mathsf{M},\zeta)$ einer Kongruenz von der Gestalt

$$\begin{aligned} \mathsf{A} \equiv a\,(1+\Omega)^{a_1} \quad & (1+\Omega^2)^{a_2} \quad \ldots (1+\Omega^{l-1})^{a_{l-1}} \cdot \\ (1+\lambda\,\Omega)^{a_1'} \quad & (1+\lambda\,\Omega^2)^{a_2'} \quad \ldots (1+\lambda\,\Omega^{l-1})^{a_{l-1}'} \cdot \\ & \ldots\ldots\ldots\ldots\ldots\ldots \\ (1+\lambda^{l-1}\Omega)^{a_1^{(l-1)}} & (1+\lambda^{l-1}\Omega^2)^{a_2^{(l-1)}} \ldots (1+\lambda^{l-1}\Omega^{l-1})^{a_{l-1}^{(l-1)}}, \qquad (\mathfrak{l}^l), \end{aligned}$$

wo a eine der Zahlen $1, 2, \ldots, l-1$, und wo die $l(l-1)$ Exponenten $a_1, a_2, \ldots, a_{l-1}^{(l-1)}$ bestimmte Zahlen aus der Reihe $0, 1, 2, \ldots, l-1$ sind. Wegen der vorhin aufgestellten Kongruenzen (77), (78), (79) folgt hieraus:

$$N_k(\mathsf{A}) \equiv a^l(1+\lambda+\lambda^2\varrho_1)^{a_1}(1+\lambda^2+\lambda^3\varrho_2)^{a_2}\ldots(1+\lambda^{l-2}+\lambda^{l-1}\varrho_{l-2}')^{a_{l-2}}, \quad (\mathfrak{l}^l).$$

Der hier rechts stehende Ausdruck stellt nun, wenn a die Werte 1, 2, ..., $l-1$, und wenn die Exponenten $a_1, a_2, \ldots, a_{l-2}$ unabhängig voneinander die Werte 0, 1, 2, ..., $l-1$ durchlaufen, $(l-1)\,l^{l-2}$ Zahlen dar, und diese sind sämtlich zu $\mathfrak{l}$ prim und einander inkongruent nach $\mathfrak{l}^l$. Mit Benutzung der Kongruenz $N_k(1+\lambda\,\mathsf{M}) \equiv 1+\lambda^l$ nach $\mathfrak{l}^{l+1}$ und weiter der Kongruenzen (73) schließen wir hieraus, daß genau der l-te Teil aller zu $\mathfrak{l}$ primen und nach $\mathfrak{l}^l$ einander inkongruenten Zahlen Normenreste des Körpers $k(\mathsf{M},\zeta)$ nach $\mathfrak{l}$ liefert, und übertragen dann dieses Resultat sogleich auf den Fall der Potenzen $\mathfrak{l}^e$ mit Exponenten $e = l+1$ bez. $e > l+1$.

Das nämliche Resultat ergibt sich durch entsprechende Rechnungen auch dann, wenn $\mu \equiv 1$ nach $\mathfrak{l}^2$ genommen wird, und damit ist der Satz 150 in allen Teilen bewiesen. Es sei jedoch bemerkt, daß wir es in unseren späteren Entwickelungen so einrichten können, daß der Satz 150 lediglich für den oben ausführlich bewiesenen Fall $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ zur Verwendung gelangt.

Der Satz 150 bringt eine neue, tief eingreifende Eigenschaft der in der Relativdiskriminante des Körpers $k(\mathsf{M},\zeta)$ in bezug auf $k(\zeta)$ aufgehenden Primideale $\mathfrak{w}$ zum Ausdruck. Diese Eigenschaft entspricht gewissermaßen dem bekannten Satze über die Verzweigungspunkte einer Riemannschen Fläche, wonach eine algebraische Funktion in der Umgebung eines Verzweigungspunktes l-ter Ordnung den Vollwinkel auf den l-ten Teil desselben konform abbildet. Infolgedessen nenne ich die in der Relativdiskriminante von $k(\mathsf{M},\zeta)$ in bezug auf $k(\zeta)$ aufgehenden Primideale $\mathfrak{w}$ auch **Verzweigungsideale** für den Körper $k(\mathsf{M},\zeta)$; es bedeuten hier also „Primfaktor der Relativdiskriminante“ und „Verzweigungsideal“ den nämlichen Begriff, und die Verzweigungsideale sind die l-ten Potenzen der ambigen Primideale.

§ 131. Das Symbol $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$.

Der Satz 150 weist uns auf die Möglichkeit hin, die nach einer Potenz $\mathfrak{w}^e$ $(e > l$ im Falle $\mathfrak{w} = \mathfrak{l})$ vorhandenen, einander inkongruenten Zahlen des Körpers $k(\zeta)$ in l Abteilungen zu sondern, die sämtlich gleich viele Zahlen enthalten, und von denen eine die Normenreste nach $\mathfrak{w}$ umfaßt. Um diese Sonderung in übersichtlicher Weise vornehmen zu können, führe ich ein neues Symbol $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$ ein, welches zwei beliebigen, von 0 verschiedenen ganzen Zahlen ν, μ des Körpers $k(\zeta)$ in bezug auf ein beliebiges Primideal $\mathfrak{w}$ in $k(\zeta)$ jedesmal eine bestimmte l-te Einheitswurzel zuweist, und zwar geschieht dies in folgender Weise:

Es sei zunächst $\mathfrak{w}$ ein von $\mathfrak{l}$ verschiedenes Primideal. Ist dann ν genau durch $\mathfrak{w}^b$ und μ genau durch $\mathfrak{w}^a$ teilbar, so bilde man die Zahl $\varkappa = \frac{\nu^a}{\mu^b}$

und bringe $\varkappa$ in die Gestalt eines Bruches $\frac{\varrho}{\sigma}$, dessen Zähler ϱ und Nenner σ nicht durch $\mathfrak{w}$ teilbar sind. Das **Symbol** $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$ werde dann durch die Formel

$$\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\} = \left\{\frac{\varkappa}{\mathfrak{w}}\right\} = \left\{\frac{\varrho}{\mathfrak{w}}\right\}\left\{\frac{\sigma}{\mathfrak{w}}\right\}^{-1}$$

definiert. Es ergeben sich hieraus unmittelbar für dieses Symbol die einfachen Regeln:

$$\left.\begin{aligned}\left\{\frac{\nu_1\nu_2,\mu}{\mathfrak{w}}\right\} &= \left\{\frac{\nu_1,\mu}{\mathfrak{w}}\right\}\left\{\frac{\nu_2,\mu}{\mathfrak{w}}\right\},\\ \left\{\frac{\nu,\mu_1\mu_2}{\mathfrak{w}}\right\} &= \left\{\frac{\nu,\mu_1}{\mathfrak{w}}\right\}\left\{\frac{\nu,\mu_2}{\mathfrak{w}}\right\},\\ \left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}\left\{\frac{\mu,\nu}{\mathfrak{w}}\right\} &= 1,\end{aligned}\right\} \tag{80}$$

wo ν, ν_1, ν_2, μ, μ_1, μ_2 beliebige von Null verschiedene ganze Zahlen in $k(\zeta)$ bedeuten können.

Um das neue Symbol für den Fall $\mathfrak{w} = \mathfrak{l}$ zu definieren, stellen wir folgende Überlegungen an:

Wenn eine beliebige ganze Zahl ω in $k(\zeta)$ vorgelegt ist, welche der Kongruenz $\omega \equiv 1$ nach $\mathfrak{l}$ genügt, und wenn wir setzen

$$\omega = c + c_1\zeta + \cdots + c_{l-2}\zeta^{l-2},$$

so daß $c, c_1, \ldots, c_{l-2}$ ganze rationale Zahlen sind, so genügen diese notwendig der Kongruenz

$$c + c_1 + \cdots + c_{l-2} \equiv 1, \qquad (l).$$

Setzen wir dann

$$\omega(x) = c + c_1 x + \cdots + c_{l-2}x^{l-2} - \frac{c + c_1 + \cdots + c_{l-2} - 1}{l}(1 + x + \cdots + x^{l-1}),$$

so stellt $\omega(x)$ eine ganzzahlige Funktion $(l-1)$-ten Grades dar, und es wird

$$\omega(1) = 1 \quad \text{und} \quad \omega(\zeta) = \omega.$$

Diese Funktion heiße die **zur ganzen Zahl ω gehörende Funktion.** Wir schreiben ferner

$$\left[\frac{\mathrm{d}^g \log \omega(\mathrm{e}^v)}{\mathrm{d}\,v^g}\right]_{v=0} = l^{(g)}(\omega), \qquad (g = 1, 2, \ldots, l-1), \tag{81}$$

welche Verbindungen von Kummer mit Vorteil zur Abkürzung gewisser Rechnungen eingeführt sind [Kummer (12)].

Wird die Zahl ω mit der Kongruenzeigenschaft $\omega \equiv 1$ nach $\mathfrak{l}$ auf irgendeine Weise in die Gestalt

$$\omega = a + a_1\zeta + \cdots + a_t\zeta^t$$

gebracht, wo $a, a_1, \ldots, a_t$ ganze rationale Zahlen bedeuten, so stellt

$$\overline{\omega}(x) = a + a_1 x + \cdots + a_t x^t$$

eine ganzzahlige Funktion t-ten Grades dar, welche im allgemeinen nicht der Gleichung $\overline{\omega}(1) = 1$, aber jedenfalls der Kongruenz

$$\overline{\omega}(1) \equiv 1, \qquad (l)$$

genüge leistet und also für $x = 1$ zu l prim ausfällt. Zwischen den Differentialquoten von $\log \overline{\omega}(e^v)$ für $v = 0$ und den soeben eingeführten Differentialquotienten (81) bestehen folgende Kongruenzen:

$$\left[\frac{d^g \log \overline{\omega}(e^v)}{d\, v^g}\right]_{v=0} \equiv l^{(g)}(\omega), \qquad (l), \qquad (g = 1, 2, \ldots, l-2),$$

$$\left[\frac{d^{l-1} \log \overline{\omega}(e^v)}{d\, v^{l-1}}\right]_{v=0} \equiv l^{(l-1)}(\omega) + \frac{1-\overline{\omega}(1)}{l}, \qquad (l).$$

Die Richtigkeit dieser Kongruenzen erkennen wir leicht wegen

$$\omega(x) = \overline{\omega}(x) + \frac{1-\overline{\omega}(1)}{l}(1 + x + \cdots + x^{l-1}) + O(x)(x^l - 1),$$

$$\omega(e^v) \equiv \overline{\omega}(e^v) + \frac{1-\overline{\omega}(1)}{l} v^{l-1}, \qquad (l);$$

in der ersten Formel bedeutet $O(x)$ eine bestimmte ganzzahlige Funktion von x, und die zweite Formel soll besagen, daß in den Entwicklungen der beiden Seiten dieser Kongruenz nach Potenzen von v die Koeffizienten von $1, v, v^2, \ldots, v^{l-1}$ nach l kongruent ausfallen.

Sind ν, μ irgend zwei ganze Zahlen in $k(\zeta)$ mit der Kongruenzeigenschaft $\nu \equiv 1$, $\mu \equiv 1$ nach $\mathfrak{l}$, so definieren wir das **Symbol** $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ wie folgt:

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = \zeta^{l^{(1)}(\nu) l^{(l-1)}(\mu) - l^{(2)}(\nu) l^{(l-2)}(\mu) + \cdots - l^{(l-1)}(\nu) l^{(1)}(\mu)}. \tag{82}$$

Aus dieser Definition ergeben sich unmittelbar die folgenden Regeln:

$$\left.\begin{aligned} \left\{\frac{\nu_1 \nu_2, \mu}{\mathfrak{l}}\right\} &= \left\{\frac{\nu_1, \mu}{\mathfrak{l}}\right\}\left\{\frac{\nu_2, \mu}{\mathfrak{l}}\right\}, \\ \left\{\frac{\nu, \mu_1 \mu_2}{\mathfrak{l}}\right\} &= \left\{\frac{\nu, \mu_1}{\mathfrak{l}}\right\}\left\{\frac{\nu, \mu_2}{\mathfrak{l}}\right\}, \\ \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}\left\{\frac{\mu, \nu}{\mathfrak{l}}\right\} &= 1, \end{aligned}\right\} \tag{83}$$

wo ν, ν_1, ν_2, μ, μ_1, μ_2 beliebige ganze Zahlen $\equiv 1$ nach $\mathfrak{l}$ in $k(\zeta)$ bedeuten können. Bezeichnet r eine Primitivzahl nach l und $s = (\zeta : \zeta^r)$ die entsprechende Substitution der Gruppe des Kreiskörpers $k(\zeta)$, so gilt, wie leicht ersichtlich ist, die weitere Formel

$$\left\{\frac{s\nu, s\mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}^r. \tag{84}$$

Sind ν, μ beliebige zu $\mathfrak{l}$ prime ganze Zahlen des Körpers $k(\zeta)$, so definiere ich das **Symbol** $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ durch die Formel

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu^{l-1}, \mu^{l-1}}{\mathfrak{l}}\right\}.$$

Für den Fall, daß eine der Zahlen ν, μ oder beide durch $\mathfrak{l}$ teilbar sind, vergleiche man die Bemerkungen gegen Schluß des § 133.

§ 132. Einige Hilfssätze über das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ und über Normenreste nach dem Primideal $\mathfrak{l}$.

Hilfssatz 24. Wenn ω eine ganze Zahl in $k(\zeta)$ mit der Kongruenzeigenschaft $\omega \equiv 1$ nach $\mathfrak{l}$ ist, so gilt für die Norm $n(\omega)$ von ω in $k(\zeta)$ die Kongruenz

$$l^{(l-1)}(\omega) \equiv \frac{1-n(\omega)}{l}, \qquad (l).$$

[Kummer (20)].

Beweis. Es bedeute $\omega(x)$ die zu ω gehörende Funktion, und es werde

$$F(x) = \prod_{(g)} \omega(1 + x(\zeta^g - 1))$$

gesetzt, wo das Produkt über die Werte $g = 0, 1, 2, \ldots, l-1$ zu erstrecken ist. Der Ausdruck $F(x)$ stellt eine ganzzahlige Funktion von x dar und die Koeffizienten aller durch x^l teilbaren Glieder dieser Funktion sind offenbar durch λ^l und folglich wegen der Rationalität der Koeffizienten auch durch l^2 teilbar. Durch Entwicklung nach Potenzen von x ergibt sich nun:

$$\left.\begin{aligned} \log \omega(1 + x(\xi - 1)) &= \frac{\xi - 1}{1!} x \left[\frac{d \log \omega(x)}{dx}\right]_{x=1} \\ &+ \frac{(\xi-1)^2}{2!} x^2 \left[\frac{d^2 \log \omega(x)}{dx^2}\right]_{x=1} + \cdots \\ \cdots &+ \frac{(\xi-1)^{l-1}}{l-1!} x^{l-1} \left[\frac{d^{l-1} \log \omega(x)}{dx^{l-1}}\right]_{x=1} + \cdots \end{aligned}\right\} \tag{85}$$

Setzen wir erstens in dieser Entwicklung der Reihe nach

$$\xi = 1, \ \zeta, \ \zeta^2, \ \ldots, \ \zeta^{l-1}$$

ein und addieren die betreffenden Formeln, so entsteht unter Berücksichtigung von

$$(\zeta - 1)^g + (\zeta^2 - 1)^g + \cdots + (\zeta^{l-1} - 1)^g = (-1)^g l, \qquad (g = 1, 2, \ldots, l-1)$$

die Gleichung:

$$\left.\begin{aligned} \log F(x) = l\Big\{ &- \frac{x}{1!}\left[\frac{d \log \omega(x)}{dx}\right]_{x=1} \\ &+ \frac{x^2}{2!}\left[\frac{d^2 \log \omega(x)}{dx^2}\right]_{x=1} - \cdots \\ \cdots &+ \frac{x^{l-1}}{l-1!}\left[\frac{d^{l-1} \log \omega(x)}{dx^{l-1}}\right]_{x=1}\Big\} + x^l G, \end{aligned}\right\} \tag{86}$$

wobei $x^l G$ das Aggregat der durch x^l teilbaren Glieder der Entwicklung andeutet.

Setzen wir zweitens in der Entwicklung (85) $\xi = e^v$ ein und bilden den $(l-1)$-ten Differentialquotienten nach v, so wird derselbe für $v = 0$:

$$\left.\begin{aligned}\left[\frac{d^{l-1}\log\omega(1+x(e^v-1))}{dv^{l-1}}\right]_{v=0} &= \frac{x}{1!}\left[\frac{d\log\omega(x)}{dx}\right]_{x=1}\\ &+\frac{2^{l-1}-2\cdot 1^{l-1}}{2!}x^2\left[\frac{d^2\log\omega(x)}{dx^2}\right]_{x=1}\\ &+\frac{3^{l-1}-3\cdot 2^{l-1}+3\cdot 1^{l-1}}{3!}x^3\left[\frac{d^3\log\omega(x)}{dx^3}\right]_{x=1}+\cdots\\ &+\frac{(l-1)^{l-1}-\cdots-(l-1)1^{l-1}}{l-1!}x^{l-1}\left[\frac{d^{l-1}\log\omega(x)}{dx^{l-1}}\right]_{x=1}\\ &\equiv \frac{x}{1!}\left[\frac{d\log\omega(x)}{dx}\right]_{x=1}-\frac{x^2}{2!}\left[\frac{d^2\log\omega(x)}{dx^2}\right]_{x=1}+\cdots\\ \cdots&-\frac{x^{l-1}}{l-1!}\left[\frac{d^{l-1}\log\omega(x)}{dx^{l-1}}\right]_{x=1},\qquad (l).\end{aligned}\right\}\tag{87}$$

Durch Vergleichung der beiden Formeln (86) und (87) ergibt sich

$$\log F(x) \equiv -l\left[\frac{d^{l-1}\log\omega(1+x(e^v-1))}{dv^{l-1}}\right]_{v=0},\qquad (l^2),$$

d. h. die Koeffizienten von x, x^2, …, x^{l-1} auf der linken Seite sind den entsprechenden Koeffizienten rechts nach l^2 kongruent, und wenn wir beide Seiten dieser Kongruenz in den Exponenten von e setzen, so erhalten wir zunächst in demselben Sinne, dann aber mit Rücksicht auf die zu Beginn dieses Beweises gemachte Bemerkung auch vollständig die Kongruenz der zwei ganzzahligen Funktionen:

$$F(x) \equiv 1 - l\left[\frac{d^{l-1}\log\omega(1+x(e^v-1))}{dv^{l-1}}\right]_{v=0},\qquad (l^2),$$

und folglich für $x = 1$:

$$n(\omega) \equiv 1 - l\cdot 1^{(l-1)}(\omega),\qquad (l^2),$$

womit der Hilfssatz 24 bewiesen ist.

Hilfssatz 25. Wenn die ganzen Zahlen ν, μ in $k(\zeta)$ die Kongruenzeigenschaften $\nu \equiv 1$ nach $\mathfrak{l}$ und $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ besitzen, und wenn außerdem ν kongruent der Relativnorm einer ganzen Zahl A des durch $\mathsf{M} = \sqrt[l]{\mu}$ bestimmten Kummerschen Körpers $k(\mathsf{M},\zeta)$ nach $\mathfrak{l}^l$ ist, so existiert eine ganzzahlige Funktion $f(x)$ vom $(l-1)$-ten Grade in x, derart, daß $f(1) > 0$ ist und die Kongruenzen

$$n(f(\zeta)) \equiv 1,\qquad (\mathfrak{l}^2)$$

und

$$\nu \equiv f(\mu),\qquad (\mathfrak{l}^l)$$

erfüllt sind. [Kummer (20)].

Beweis. Nach dem Beweise des Hilfssatzes 23 ist jede ganze Zahl A in $k(\mathsf{M},\zeta)$ in der Gestalt

$$\mathsf{A} = \frac{\gamma+\gamma_1(\mathsf{M}-1)+\cdots+\gamma_{l-1}(\mathsf{M}-1)^{l-1}}{\delta}$$

und folglich auch in der Gestalt

$$\mathsf{A} = \frac{\beta+\beta_1\mathsf{M}+\cdots+\beta_{l-1}\mathsf{M}^{l-1}}{\delta}$$

darstellbar, so daß γ, γ_1, …, γ_{l-1}, δ und β, β_1, …, β_{l-1} ganze Zahlen in $k(\zeta)$ sind und überdies δ zu $\mathfrak{l}$ prim ausfällt. Infolge des letzteren Umstandes können wir

$$\mathsf{A} \equiv \alpha + \alpha_1\mathsf{M}+\cdots+\alpha_{l-1}\mathsf{M}^{l-1},\qquad (\mathfrak{l}^l)$$

setzen in solcher Weise, daß α, α_1, …, α_{l-1} ganze Zahlen in $k(\zeta)$ sind. Es sei nun

$$\alpha \equiv a^*,\qquad \alpha_1 \equiv a_1^*,\ \ldots,\ \alpha_{l-1} \equiv a_{l-1}^*,\qquad (\mathfrak{l}),$$

wo a^*, a_1^*, …, a_{l-1}^* ganze rationale positive Zahlen bedeuten sollen; wir setzen

$$f^*(x) = a^* + a_1^*x+\cdots+a_{l-1}^*x^{l-1}.$$

Da in $k(\mathsf{M},\zeta)$ sich $\mathfrak{l} = \mathfrak{L}^l$ und $\mathsf{M} \equiv 1$ nach $\mathfrak{L}$ erweist, so folgt

$$\mathsf{A} \equiv \alpha+\alpha_1+\cdots+\alpha_{l-1} \equiv a^*+a_1^*+\cdots+a_{l-1}^*,\qquad (\mathfrak{L}).$$

Ist nun A die vorausgesetzte Zahl, für welche $N_k(\mathsf{A}) \equiv \nu$ nach $\mathfrak{l}^l$ wird, so erhalten wir weiter

$$\nu \equiv N_k(\mathsf{A}) \equiv a^*+a_1^*+\cdots+a_{l-1}^* \equiv 1,\qquad (\mathfrak{L}),$$

also auch

$$a^*+a_1^*+\cdots+a_{l-1}^* \equiv 1,\qquad (l).\tag{88}$$

Folglich ist $f^*(\zeta)$ eine Zahl in $k(\zeta)$ mit der Kongruenzeigenschaft $f^*(\zeta) \equiv 1$ nach $\mathfrak{l}$. Wir finden nun mit Rücksicht hierauf leicht eine ganze rationale positive Zahl b derart, daß die Norm der Zahl $f(\zeta) = f^*(\zeta) + lb$ im Körper $k(\zeta)$ der Kongruenz

$$n(f(\zeta)) \equiv 1,\qquad (\mathfrak{l}^2)\tag{89}$$

genügt; dann erfüllt die ganzzahlige Funktion

$$f(x) = f^*(x) + lb = a + a_1x+\cdots+a_{l-1}x^{l-1}$$

die Bedingungen des zu beweisenden Hilfssatzes 25. Denn es ist offenbar $\mathsf{A} = f(\mathsf{M}) + \lambda\mathsf{B}$, wo B eine ganze Zahl in $k(\mathsf{M},\zeta)$ bedeutet. Hieraus ergibt sich leicht durch eine ähnliche Betrachtung wie auf S. 263:

$$\nu \equiv N_k(\mathsf{A}) \equiv N_k(f(\mathsf{M})),\qquad (\mathfrak{l}^l).\tag{90}$$

Andererseits erkennen wir unter Berücksichtigung der Kongruenzen

$$a^l \equiv a,\quad a_1^l \equiv a_1,\ \ldots,\ a_{l-1}^l \equiv a_{l-1},\qquad (l),$$

daß identisch in x eine Gleichung

$$f(x)f(\zeta x)\dots f(\zeta^{l-1}x) = f(x^l) + lF(x^l) \tag{91}$$

gilt, wo $F(x^l)$ eine ganzzahlige Funktion von x^l bedeutet. Diese Gleichung liefert für $x = 1$ mit Rücksicht auf (89) die Kongruenz

$$f(1) \equiv f(1) + lF(1), \quad (l^2), \qquad \text{d. h.} \qquad F(1) \equiv 0, \quad (l).$$

Wenn in der Gleichung (91) $x = \mathsf{M}$ genommen wird, so ergibt sich

$$N_k(f(\mathsf{M})) = f(\mu) + lF(\mu)$$

und hieraus, da $F(\mu) \equiv F(1) \equiv 0$ nach l ausfällt,

$$N_k(f(\mathsf{M})) \equiv f(\mu), \qquad (l^l),$$

d. i. wegen (90)

$$\nu \equiv f(\mu), \qquad (l^l).$$

Damit und in Anbetracht von (89) ist der Hilfssatz 25 vollständig bewiesen.

Hilfssatz 26. Wenn ν, μ ganze Zahlen in $k(\zeta)$ mit den Kongruenzeigenschaften $\nu \equiv 1$ nach l und $\mu \equiv 1 + \lambda$ nach l^2 bedeuten, und wenn außerdem ν Normenrest des durch $\mathsf{M} = \sqrt[l]{\mu}$ bestimmten Kummerschen Körpers $k(\mathsf{M}, \zeta)$ nach l ist, so wird stets

$$\left\{\frac{\nu, \mu}{l}\right\} = 1.$$

[Kummer (20)].

Beweis. Aus der bekannten Lagrangeschen Formel für die Umkehrung einer Potenzreihe entnimmt man unmittelbar die folgende Identität:

$$\left[\frac{\mathrm{d}^{l-1}F(v)}{\mathrm{d}V^{l-1}}\right]_{V=0} = \left[\frac{\mathrm{d}^{l-2}\dfrac{\mathrm{d}F(v)}{\mathrm{d}v}(\varphi(v))^{l-1}}{\mathrm{d}v^{l-2}}\right]_{v=0}; \tag{92}$$

dabei stelle man sich unter $F(v)$ eine beliebige Potenzreihe von v, ferner unter $\varphi(v)$ eine Potenzreihe vor, deren konstantes Glied von 0 verschieden ist, und denke sich den Zusammenhang der Variabeln v und V durch die Gleichung $V\varphi(v) - v = 0$ vermittelt.

Es seien nun $\nu(x)$ und $\mu(x)$ die zu den Zahlen ν und μ gehörenden Funktionen. Da ν Normenrest des Körpers $k(\mathsf{M}, \zeta)$ nach l sein soll, so gibt es nach Hilfssatz 25 eine ganzzahlige Funktion $(l-1)$-ten Grades $f(x)$ derart, daß

$$n(f(\zeta)) \equiv 1, \qquad (l^2), \tag{93}$$

$$\nu \equiv f(\mu), \quad (l^l) \tag{94}$$

und $f(1) > 0$ wird.

Wir setzen nun

$$F(v) = \log f(\mu(\mathrm{e}^v)),$$
$$V = \log \mu(\mathrm{e}^v),$$
$$\varphi(v) = \frac{v}{\log \mu(\mathrm{e}^v)};$$

diese Funktionen werden nur an der Stelle $v = 0$ betrachtet werden, und es sollen die Logarithmen so genommen werden, daß sie für $v = 0$ reell sind.

Ersetzen wir die Zeichen $\omega, \overline{\omega}(x), v$ in der dritten Formelzeile auf S. 266 oben bez. durch $f(\zeta), f(x), V$, so wird aus derselben

$$\left[\frac{\mathrm{d}^{l-1}\log f(\mathrm{e}^V)}{\mathrm{d}V^{l-1}}\right]_{V=0} \equiv l^{(l-1)}(f(\zeta)) + \frac{1-f(1)}{l}, \qquad (l).$$

Aus Hilfssatz 24 ergibt sich unter Berücksichtigung von (93) die Kongruenz

$$l^{(l-1)}(f(\zeta)) \equiv 0, \qquad (l)$$

und folglich wird

$$\left[\frac{\mathrm{d}^{l-1}F(v)}{\mathrm{d}V^{l-1}}\right]_{V=0} = \left[\frac{\mathrm{d}^{l-1}\log f(\mathrm{e}^V)}{\mathrm{d}V^{l-1}}\right]_{V=0} \equiv \frac{1-f(1)}{l}, \qquad (l). \tag{95}$$

Andererseits gilt mit Rücksicht auf (94) die Kongruenz

$$f(\mu(\mathrm{e}^v)) \equiv \nu(\mathrm{e}^v) + \frac{f(1)-1}{l}v^{l-1}, \qquad (l),$$

welche so aufzufassen ist, daß in den Entwicklungen nach Potenzen von v die Koeffizienten von $1, v, \dots, v^{l-1}$ auf den beiden Seiten einander nach l kongruent sind, und hieraus ergibt sich die Entwicklung

$$\left.\begin{aligned}\frac{\mathrm{d}F(v)}{\mathrm{d}v} &\equiv l^{(1)}(\nu) + l^{(2)}(\nu)\frac{v}{1!} + l^{(3)}(\nu)\frac{v^2}{2!} + \dots \\ &\dots + \left(l^{(l-1)}(\nu) + \frac{1-f(1)}{l}\right)\frac{v^{l-2}}{(l-2)!}, \qquad (l),\end{aligned}\right\} \tag{96}$$

welche so aufzufassen ist, daß die Koeffizienten von $1, v, \dots, v^{l-2}$ auf den beiden Seiten einander nach l kongruent sind.

Endlich betrachten wir die Funktion $\varphi(v)$. Wegen $\mu \equiv 1 + \lambda$ nach l^2 wird $\varphi(v)$ eine Potenzreihe, deren konstantes Glied $\equiv -1$ nach l ist. Ferner folgt leicht

$$(\varphi(v))^l \equiv \varphi(v^l) \equiv \varphi(0) \equiv -1, \qquad (l)$$

in dem Sinne, daß die Koeffizienten von $1, v, \dots, v^{l-2}$ auf den beiden Seiten einander nach l kongruent sind. Es gilt daher weiter in demselben Sinne

$$-(\varphi(v))^{l-1} \equiv \frac{\log \mu(\mathrm{e}^v)}{v}, \qquad (l),$$

und es folgt hieraus endlich in eben demselben Sinne die Entwicklung

$$\left.\begin{aligned}-(\varphi(v))^{l-1} &\equiv l^{(1)}(\mu) + l^{(2)}(\mu)\frac{v}{2!} + l^{(3)}(\mu)\frac{v^2}{3!} + \dots \\ &\dots + l^{(l-1)}(\mu)\frac{v^{l-2}}{(l-1)!}, \qquad (l).\end{aligned}\right\} \tag{97}$$

Die Zusammenstellung der Kongruenz (95) und der beiden Entwicklungen (96), (97) mit (92) liefert, wegen $l^{(1)}(\mu) \equiv -1$ und $(l-g)!\,(g-1)! \equiv (-1)^g$ nach l für $g = 1, 2, \dots, l-1$, die folgende Kongruenz:

$$l^{(l-1)}(\nu)l^{(1)}(\mu) - l^{(l-2)}(\nu)l^{(2)}(\mu) + \dots - l^{(1)}(\nu)l^{(l-1)}(\mu) \equiv 0, \qquad (l),$$

d. i. nach der Definition (82) des Symbols $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ in § 131:

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = 1,$$

und hiermit ist der Hilfssatz 26 bewiesen.

§ 133. Das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ zur Unterscheidung zwischen Normenresten und Normennichtresten.

Wir sind jetzt in den Stand gesetzt, soweit die betreffenden Symbole bereits definiert sind, die Richtigkeit der folgenden Behauptung einzusehen:

Satz 151. Wenn ν, μ zwei beliebige ganze Zahlen in $k(\zeta)$ sind, nur daß $\sqrt[l]{\mu}$ nicht in $k(\zeta)$ liegt, und wenn $\mathfrak{w}$ ein beliebiges Primideal des Kreiskörpers $k(\zeta)$ bedeutet, so ist ν Normenrest oder Normennichtrest des durch $\mathsf{M} = \sqrt[l]{\mu}$ bestimmten Kummerschen Körpers $k(\mathsf{M}, \zeta)$ nach $\mathfrak{w}$, je nachdem

$$\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = 1 \quad \text{oder} \quad +1$$

ausfällt.

Beweis. Es sei zunächst das Primideal $\mathfrak{w}$ von $\mathfrak{l}$ verschieden und gehe nicht in der Relativdiskriminante des Körpers $k(\mathsf{M}, \zeta)$ auf. Ist μ^* eine ganze Zahl in $k(\zeta)$ derart, daß $\frac{\mu^*}{\mu}$ die l-te Potenz einer Zahl in $k(\zeta)$ ist, so gilt stets $\left\{\frac{\nu, \mu^*}{\mathfrak{w}}\right\} = \left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$; danach und mit Rücksicht auf Satz 148 können wir hier annehmen, daß μ nicht durch $\mathfrak{w}$ teilbar ist. Wir unterscheiden zwei Fälle, je nachdem $\mathfrak{w}$ im Körper $k(\mathsf{M}, \zeta)$ als Produkt von l Primidealen $\mathfrak{W}_1, \ldots, \mathfrak{W}_l$ darstellbar wird oder in $k(\mathsf{M}, \zeta)$ Primideal bleibt. Nach Satz 149 ist im ersteren Falle $\left\{\frac{\mu}{\mathfrak{w}}\right\} = 1$, im letzteren $\left\{\frac{\mu}{\mathfrak{w}}\right\} + 1$ und $+ 0$.

Im *ersteren* Falle bestimmen wir eine ganze Zahl A in $k(\mathsf{M}, \zeta)$, welche durch $\mathfrak{W}_1$, aber nicht durch $\mathfrak{W}_1^2$ und auch nicht durch eines der Primideale $\mathfrak{W}_2, \ldots, \mathfrak{W}_l$ teilbar ist; dann geht in der Relativnorm $\alpha = N_k(\mathsf{A})$ das Primideal $\mathfrak{w}$ genau zur ersten Potenz auf. Ist nun $\mathfrak{w}^b$ die in ν enthaltene Potenz von $\mathfrak{w}$, so läßt sich $\varkappa = \frac{\nu}{\alpha^b}$ als ein Bruch schreiben, dessen Zähler und Nenner zu $\mathfrak{w}$ prim sind, und folglich sind Zähler und Nenner dieses Bruches nach Satz 150 Normenreste des Körpers $k(\mathsf{M}, \zeta)$ nach $\mathfrak{w}$. Das gleiche gilt also auch von ν. Da nach der Definition in § 131

$$\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^b}{\mathfrak{w}}\right\}^{-1} = 1$$

ist, so erweist sich im ersteren Falle der Satz 151 als richtig.

Im *zweiten* Falle ist die Relativnorm einer ganzen Zahl A in $k(\mathsf{M}, \zeta)$ jedesmal genau durch eine solche Potenz von $\mathfrak{w}$ teilbar, deren Exponent

ein Vielfaches von l ist. Es sei wiederum $\mathfrak{w}^b$ die in ν enthaltene Potenz von $\mathfrak{w}$; ist dann b kein Vielfaches von l, so kann also ν nicht Normenrest nach $\mathfrak{w}$ sein; in diesem Falle wird andererseits $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^b}{\mathfrak{w}}\right\}^{-1} + 1$. Ist dagegen b ein Vielfaches von l, und bedeutet α eine ganze durch $\mathfrak{w}$, aber nicht durch $\mathfrak{w}^2$ teilbare Zahl in $k(\zeta)$, so setzen wir $\varkappa = \frac{\nu}{\alpha^b}$ und erkennen wie im ersteren Falle ν als Normenrest nach $\mathfrak{w}$; andererseits ist jetzt

$$\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^b}{\mathfrak{w}}\right\}^{-1} = 1.$$

Damit ist der Satz 151 auch für den zweiten Fall bewiesen.

Wir nehmen jetzt an, es sei die Relativdiskriminante des Körpers $k(\mathsf{M}, \zeta)$ durch das Primideal $\mathfrak{w}$ teilbar; $\mathfrak{w}$ soll dabei von $\mathfrak{l}$ verschieden sein. Es gehe $\mathfrak{w}$ in ν genau zur b-ten und in μ genau zur a-ten Potenz auf; dann ist a jedenfalls kein Vielfaches von l. Die Zahl $\varkappa = \frac{\nu^a}{\mu^b}$ läßt sich in die Gestalt eines Bruches $\frac{\varrho}{\sigma}$ setzen, dessen Zähler ϱ und dessen Nenner σ zu $\mathfrak{w}$ prim sind. Die Zahl $\varrho\sigma^{l-1}$ ist eine nicht durch $\mathfrak{w}$ teilbare ganze Zahl; nach dem Beweise des Satzes 150 auf S. 261 ist eine solche ganze Zahl dann und nur dann Normenrest des Körpers $k(\mathsf{M}, \zeta)$ nach $\mathfrak{w}$, wenn sie l-ter Potenzrest nach $\mathfrak{w}$ ist, d. i. hier, wenn $\left\{\frac{\varrho\sigma^{l-1}}{\mathfrak{w}}\right\} = 1$ und also $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = 1$ ist; damit ist für den gegenwärtigen Fall wiederum der Satz 151 als richtig erkannt.

Es sei endlich $\mathfrak{w} = \mathfrak{l}$. Wir fassen lediglich den Fall ins Auge, daß $\mu \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ ist: es ist dies der einzige Fall, für den wir die betreffenden Sätze späterhin brauchen werden; die anderen Fälle gestatten übrigens eine ähnliche Behandlung. Beim Beweise machen wir noch die nicht wesentlich einschränkende Annahme $\nu \equiv 1$ nach $\mathfrak{l}$. Wegen der Annahme $\mu \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ kann man laut Satz 150 genau l^{l-1} Normenreste ν^* des Körpers $k(\mathsf{M}, \zeta)$ nach $\mathfrak{l}$ bilden, welche kongruent 1 nach $\mathfrak{l}$ ausfallen und untereinander nach $\mathfrak{l}^{l+1}$ inkongruent sind. Andererseits muß ein jeder Normenrest ν^* von $k(\mathsf{M}, \zeta)$ nach $\mathfrak{l}$, für den man $\nu^* \equiv 1$ nach $\mathfrak{l}$ hat, laut Hilfssatz 26 die Bedingung $\left\{\frac{\nu^*, \mu}{\mathfrak{l}}\right\} = 1$ erfüllen. Wegen

$$\left.\begin{aligned} &1^{(1)}(\mu) \equiv -1, \\ &1^{(1)}(1-l) \equiv 0, \quad 1^{(2)}(1-l) \equiv 0, \ \ldots, \ 1^{(l-2)}(1-l) \equiv 0, \\ &1^{(l-1)}(1-l) \equiv \frac{1 - n(1-l)}{l} \equiv -1, \end{aligned}\right\} \qquad (l)$$

ergibt sich nach (82)

$$\left\{\frac{1-l, \mu}{\mathfrak{l}}\right\} = \zeta^{-1}. \qquad (98)$$

Es sei nun erstens α irgendeine ganze Zahl in $k(\zeta)$ mit der Kongruenzeigen-

schaft $\alpha \equiv 1$ nach $\mathfrak{l}$, und es werde $\left\{\frac{\alpha, \mu}{\mathfrak{l}}\right\} = \zeta^a$ gesetzt, wo a eine Zahl aus der Reihe $0, 1, 2, \ldots, l-1$ bedeuten soll; dann ist offenbar $\left\{\frac{\alpha(1-l)^s, \mu}{\mathfrak{l}}\right\} = 1$; dagegen fällt jedesmal $\left\{\frac{\alpha(1-l)^x, \mu}{\mathfrak{l}}\right\} \neq 1$ aus, wenn x eine von a verschiedene Zahl aus der Reihe $0, 1, 2, \ldots, l-1$ bedeutet. Wählen wir ferner eine ganze Zahl α' in $k(\zeta)$, welche ebenfalls kongruent 1 nach $\mathfrak{l}$, aber keiner der l Zahlen $\alpha, \alpha(1-l), \alpha(1-l)^2, \ldots, \alpha(1-l)^{l-1}$ nach $\mathfrak{l}^{l+1}$ kongruent ist, so sind auch die l Zahlen $\alpha', \alpha'(1-l), \alpha'(1-l)^2, \ldots, \alpha'(1-l)^{l-1}$ nach $\mathfrak{l}^{l+1}$ sämtlich untereinander inkongruent und zugleich keiner der ersteren l Zahlen kongruent; unter den letzteren l Zahlen gibt es wegen (98) offenbar eine und nur eine Zahl — es sei dies etwa $\alpha'(1-l)^{a'}$ — von der Art, daß $\left\{\frac{\alpha'(1-l)^{a'}, \mu}{\mathfrak{l}}\right\} = 1$ ist. Fahren wir in dieser Weise fort, so erkennen wir, daß die Anzahl der vorhandenen nach $\mathfrak{l}^{l+1}$ inkongruenten Zahlen ν, die kongruent 1 nach $\mathfrak{l}$ sind und der Bedingung $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = 1$ genügen, genau gleich l^{l-1} ist, und aus der Übereinstimmung dieser Anzahl mit der oben gefundenen für die Normenreste ν^* ist ersichtlich, daß umgekehrt auch jede Zahl ν mit diesen zwei Eigenschaften Normenrest des Körpers $k(\mathsf{M}, \zeta)$ nach $\mathfrak{l}$ ist.

Durch die bisherigen Überlegungen ist der Satz 151 in allen Teilen bewiesen; für den Fall $\mathfrak{w} = \mathfrak{l}$ allerdings nur soweit, als für die Zahlen ν, μ die Kongruenzeigenschaften $\nu \equiv 1$ nach $\mathfrak{l}$ und $\mu \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ erfüllt sind. Die ν betreffende Einschränkung ist offenbar leicht aufzuheben.

Aus dem Satze 151 folgt, bei Benutzung der ersten Formel in (80) und (83), die Formel

$$\left\{\frac{\nu\nu^*, \mu}{\mathfrak{w}}\right\} = \left\{\frac{\nu, \mu}{\mathfrak{w}}\right\},$$

wo $\mathfrak{w}$ ein beliebiges Primideal in $k(\zeta)$ bedeutet und ν^* ein Normenrest des Körpers $k(\mathsf{M}, \zeta)$ nach $\mathfrak{w}$ sein soll.

Um nun das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ auch für den Fall zu definieren, daß eine der beiden Zahlen ν, μ oder beide durch $\mathfrak{l}$ teilbar sind, braucht man nur die allgemeine Gültigkeit der Formeln

$$\left\{\frac{\nu\nu^*, \mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}, \qquad \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}\left\{\frac{\mu, \nu}{\mathfrak{l}}\right\} = 1$$

festzusetzen, wobei ν^* ein beliebiger Normenrest des Körpers $k(\sqrt[l]{\mu}, \zeta)$ nach $\mathfrak{l}$ bedeuten soll. Bei dieser Festsetzung folgt dann insbesondere

$$\left\{\frac{1 + a\lambda^l, \lambda}{\mathfrak{l}}\right\} = \left\{\frac{1 + a\lambda^l}{\mathfrak{l}}\right\} = \zeta^a.$$

Wir können überhaupt die Definition des **Symbols** $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ auf die Formeln

$$\left\{\frac{\alpha, \zeta}{\mathfrak{l}}\right\} = \zeta^{\frac{n(\alpha)-1}{l}}, \qquad \left\{\frac{\nu_1\nu_2, \mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu_1, \mu}{\mathfrak{l}}\right\}\left\{\frac{\nu_2, \mu}{\mathfrak{l}}\right\},$$

$$\left\{\frac{\nu^*, \mu}{\mathfrak{l}}\right\} = 1, \qquad \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}\left\{\frac{\mu, \nu}{\mathfrak{l}}\right\} = 1$$

gründen, wo α eine zu $\mathfrak{l}$ prime ganze Zahl in $k(\zeta)$, ν^* ein Normenrest des Körpers $k(\sqrt[l]{\mu}, \zeta)$ nach $\mathfrak{l}$ und ν, ν_1, ν_2, μ beliebige ganze Zahlen in $k(\zeta)$ sein sollen (vgl. § 166). Ich habe jedoch gegenwärtig die obige Definition (82) gewählt, welche unmittelbar an die Entwicklungen von Kummer anknüpft.

Schließlich sei hier bemerkt, daß nunmehr das zu Anfang des § 131 gesteckte Ziel erreicht ist; wenn nämlich $\mathfrak{w}^e$ eine beliebige Potenz eines Primideals $\mathfrak{w}$ bedeutet, wobei im Falle $\mathfrak{w} = \mathfrak{l}$ der Exponent $e > l$ sei, so kann offenbar ein vollständiges System zu $\mathfrak{w}$ primer und nach $\mathfrak{w}^e$ inkongruenter Zahlen ν in $k(\zeta)$ mit Rücksicht auf die Werte, die das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ annimmt, in l Abteilungen von gleich vielen Zahlen gesondert werden, von denen die eine Abteilung die sämtlichen im System befindlichen Normenreste des Kummerschen Körpers $k(\mathsf{M}, \zeta)$ nach $\mathfrak{w}$ darstellt.

30. Das Vorhandensein unendlich vieler Primideale mit vorgeschriebenen Potenzcharakteren im Kummerschen Körper.

§ 134. Der Grenzwert eines gewissen unendlichen Produktes.

Nachdem wir in § 128 die Primideale des Kummerschen Körpers sämtlich aufgestellt haben, sind wir imstande, diejenigen Untersuchungen für den Kummerschen Körper durchzuführen, welche den in § 79 und in § 80 für den quadratischen Körper behandelten Fragen entsprechen. Wir leiten vor allem die folgende wichtige Tatsache ab:

Hilfssatz 27. Bedeutet l eine ungerade rationale Primzahl und α in dem durch $\zeta = e^{\frac{2i\pi}{l}}$ bestimmten Kreiskörper $k(\zeta)$ eine beliebige ganze Zahl, nur nicht die l-te Potenz einer in $k(\zeta)$ liegenden Zahl, so ist der Grenzwert

$$\lim_{s=1} \prod_{(\mathfrak{p})} \prod_{(m)} \frac{1}{1 - \left\{\frac{\alpha}{\mathfrak{p}}\right\}^m n(\mathfrak{p})^{-s}}$$

stets eine endliche und von 0 verschiedene Größe; dabei soll das Produkt $\prod_{(\mathfrak{p})}$ über alle Primideale $\mathfrak{p}$ des Körpers $k(\zeta)$ und das Produkt $\prod_{(m)}$ über alle Exponenten m aus der Reihe $1, 2, \ldots, l-1$ erstreckt werden [Kummer (20)].

Beweis. Fassen wir den durch $\sqrt[l]{\alpha}$ und ζ bestimmten Kummerschen Körper $K = k(\sqrt[l]{\alpha}, \zeta)$ ins Auge und bezeichnen wir die dem Satze 56 gemäß gebildete Funktion $\zeta(s)$ für denselben mit $\zeta_K(s)$, so ist nach § 27

$$\zeta_K(s) = \prod_{(\mathfrak{P})} \frac{1}{1 - N(\mathfrak{P})^{-s}},$$

wo das Produkt über alle Primideale $\mathfrak{P}$ in K zu erstrecken ist und $N(\mathfrak{P})$ die in K genommene Norm von $\mathfrak{P}$ bedeutet. Ordnen wir dieses Produkt nach den Primidealen $\mathfrak{p}$ des Körpers $k(\zeta)$, aus welchen die Primideale $\mathfrak{P}$ herstammen,

so gehört, wie man aus Satz 149 schließt, zu einem beliebigen Primideal $\mathfrak{p}$ in dem Produkte das Glied

$$\frac{1}{(1-n(\mathfrak{p})^{-s})^t} \quad \text{oder} \quad \frac{1}{1-n(\mathfrak{p})^{-s}} \quad \text{oder} \quad \frac{1}{1-n(\mathfrak{p})^{-1}},$$

je nachdem $\left\{\frac{\alpha}{\mathfrak{p}}\right\} = 1$ oder $= 0$ oder $\neq 1$ und $\neq 0$ ausfällt. Wir schreiben diese drei Ausdrücke in der ihnen gemeinschaftlichen Form

$$\frac{1}{1-n(\mathfrak{p})^{-s}} \prod_{(m)} \frac{1}{1-\left\{\frac{\alpha}{\mathfrak{p}}\right\}^m n(\mathfrak{p})^{-s}}, \quad (m=1, 2, \ldots, l-1)$$

und erhalten so

$$\zeta_K(s) = \prod_{(\mathfrak{p})} \frac{1}{1-n(\mathfrak{p})^{-s}} \prod_{(\mathfrak{p})} \prod_{(m)} \frac{1}{1-\left\{\frac{\alpha}{\mathfrak{p}}\right\}^m n(\mathfrak{p})^{-s}}; \tag{99}$$

darin zeigt das Produkt $\prod_{(m)}$ an, daß der Exponent m jeden der Werte $1, 2, \ldots, l-1$ durchlaufen soll, und es sind die beiden Produkte $\prod_{(\mathfrak{p})}$ über alle Primideale $\mathfrak{p}$ in $k(\zeta)$ zu erstrecken. Nun stellt jeder der beiden Ausdrücke

$$\lim_{s=1} L(s-1) \prod_{(\mathfrak{p})} \frac{1}{1-n(\mathfrak{p})^{-s}}, \qquad \lim_{s=1} L(s-1)\,\zeta_K(s)$$

eine endliche und von 0 verschiedene Größe dar, wie wir erkennen, wenn wir den Satz 56 einmal auf den Kreiskörper $k(\zeta)$ und dann auf den Kummerschen Körper $K = k(\sqrt[l]{\alpha}, \zeta)$ anwenden. Durch Multiplikation der Gleichung (99) mit $s-1$ und Übergang zur Grenze für $s=1$ ergibt sich dann, daß auch der im Hilfssatz 27 angegebene Ausdruck eine endliche und von 0 verschiedene Größe besitzt.

§ 135. Primideale des Kreiskörpers $k(\zeta)$ mit vorgeschriebenen Potenzcharakteren.

Satz 152. Es seien $\alpha_1, \ldots, \alpha_t$ irgend t ganze Zahlen des Kreiskörpers $k(\zeta)$, welche die Bedingung erfüllen, daß das Produkt

$$\alpha_1^{m_1}\alpha_2^{m_2}\ldots\alpha_t^{m_t},$$

wenn man jeden der Exponenten $m_1, m_2, \ldots, m_t$ die Werte $0, 1, 2, \ldots, l-1$ durchlaufen läßt, jedoch das eine Wertsystem $m_1 = 0, m_2 = 0, \ldots, m_t = 0$ ausschließt, dabei niemals die l-te Potenz einer Zahl in $k(\zeta)$ wird; es seien ferner $\gamma_1, \gamma_2, \ldots, \gamma_t$ nach Belieben vorgeschriebene l-te Einheitswurzeln: dann gibt es im Kreiskörper $k(\zeta)$ stets unendlich viele Primideale $\mathfrak{p}$, für die jedesmal bei einem gewissen zu l primen Exponenten m

$$\left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m = \gamma_1, \quad \left\{\frac{\alpha_2}{\mathfrak{p}}\right\}^m = \gamma_2, \quad \ldots, \quad \left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m = \gamma_t$$

wird [Kummer (20)].

Beweis. Wir haben, so lange $s > 1$ ist,

$$\left.\begin{aligned} \log \sum_{(\mathfrak{j})} \frac{1}{n(\mathfrak{j})^s} &= \sum_{(\mathfrak{p})} \log \frac{1}{1-n(\mathfrak{p})^{-s}} = \sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} + S, \\ S &= \frac{1}{2}\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^{2s}} + \frac{1}{3}\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^{3s}} + \cdots, \end{aligned}\right\} \tag{100}$$

wo $\sum_{(\mathfrak{j})}$ über alle Ideale $\mathfrak{j}$ und $\sum_{(\mathfrak{p})}$ jedesmal über alle Primideale $\mathfrak{p}$ des Körpers $k(\zeta)$ zu erstrecken ist. Da der Ausdruck S, wie in § 50 gezeigt worden ist, für $s = 1$ endlich bleibt, so folgt aus (100), indem die linke Seite für $s = 1$ unendlich wird, daß die über alle Primideale $\mathfrak{p}$ des Körpers $k(\zeta)$ erstreckte Summe

$$\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s}$$

bei Annäherung von s an 1 über alle Grenzen wächst. Ist ferner α eine beliebige ganze Zahl in $k(\zeta)$, so gilt ähnlich für $s > 1$ stets

$$\left.\begin{aligned} \log \prod_{(\mathfrak{p})} \frac{1}{1-\left\{\frac{\alpha}{\mathfrak{p}}\right\} n(\mathfrak{p})^{-s}} &= \sum_{(\mathfrak{p})} \left\{\frac{\alpha}{\mathfrak{p}}\right\} \frac{1}{n(\mathfrak{p})^s} + S(\alpha), \\ S(\alpha) &= \frac{1}{2}\sum_{(\mathfrak{p})} \left\{\frac{\alpha}{\mathfrak{p}}\right\}^2 \frac{1}{n(\mathfrak{p})^{2s}} + \frac{1}{3}\sum_{(\mathfrak{p})} \left\{\frac{\alpha}{\mathfrak{p}}\right\}^3 \frac{1}{n(\mathfrak{p})^{3s}} + \cdots, \end{aligned}\right\} \tag{101}$$

und hier bleibt wiederum $S(\alpha)$ für $s = 1$ endlich. Es sei jetzt m eine der Zahlen $1, 2, \ldots, l-1$. Wir setzen in (101)

$$\alpha = \alpha_*^m = \alpha_1^{m u_1}\alpha_2^{m u_2}\ldots\alpha_t^{m u_t}$$

und multiplizieren die entstehende Gleichung noch mit dem Faktor $\gamma_1^{-u_1}\gamma_2^{-u_2}\ldots\gamma_t^{-u_t}$; wir erteilen dann jedem der t Exponenten $u_1, u_2, \ldots, u_t$ nacheinander alle die l Werte $0, 1, \ldots, l-1$, jedoch so, daß das eine Wertsystem $u_1 = 0, u_2 = 0, \ldots, u_t = 0$ ausgeschlossen bleibt. Werden die auf diese Weise hervorgehenden $l^t - 1$ Gleichungen sämtlich zu (100) addiert, so entsteht die Beziehung

$$\left.\begin{aligned} &\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} + S + \sum_{(u_1, \ldots, u_t)} \gamma_1^{-u_1}\ldots\gamma_t^{-u_t} \log \prod_{(\mathfrak{p})} \frac{1}{1-\left\{\frac{\alpha_1^{u_1}\cdots\alpha_t^{u_t}}{\mathfrak{p}}\right\}^m n(\mathfrak{p})^{-s}} \\ &= \sum_{(\mathfrak{p})} [1][2]\ldots[t] \frac{1}{n(\mathfrak{p})^s} + S + \sum_{(u_1, \ldots, u_t)} \gamma_1^{-u_1}\gamma_2^{-u_2}\ldots\gamma_t^{-u_t} S(\alpha_*^m), \end{aligned}\right\} \tag{102}$$

wo für den Augenblick

$$\begin{aligned} [1] &= 1 + \left(\gamma_1^{-1}\left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m\right) + \left(\gamma_1^{-1}\left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m\right)^2 + \cdots + \left(\gamma_1^{-1}\left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m\right)^{l-1}, \\ [2] &= 1 + \left(\gamma_2^{-1}\left\{\frac{\alpha_2}{\mathfrak{p}}\right\}^m\right) + \left(\gamma_2^{-1}\left\{\frac{\alpha_2}{\mathfrak{p}}\right\}^m\right)^2 + \cdots + \left(\gamma_2^{-1}\left\{\frac{\alpha_2}{\mathfrak{p}}\right\}^m\right)^{l-1}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ [t] &= 1 + \left(\gamma_t^{-1}\left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m\right) + \left(\gamma_t^{-1}\left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m\right)^2 + \cdots + \left(\gamma_t^{-1}\left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m\right)^{l-1} \end{aligned}$$

gesetzt ist; außerdem ist in $S(\alpha_*^m)$ für α_*^m der oben angegebene Ausdruck einzusetzen. Wenn wir nun in der ersten Summe rechter Hand in (102) von denjenigen Gliedern absehen — ihr Aggregat möge G_m heißen —, die den in $\alpha_1, \ldots, \alpha_t, \lambda$ aufgehenden Primidealen $\mathfrak{p}$ entsprechen und die nur in endlicher Anzahl vorhanden sind, so hat der übrige unendliche Teil dieser Summe offenbar den Wert $l^t \sum_{(\mathfrak{q})} \frac{1}{n(\mathfrak{q})^s}$, wo $\mathfrak{q}$ nur alle diejenigen unter den Primidealen $\mathfrak{p}$ des Körpers $k(\zeta)$ durchläuft, für welche die t Bedingungen

$$\left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m = \gamma_1, \ \ldots, \ \left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m = \gamma_t \tag{103}$$

sämtlich erfüllt sind. Bilden wir nun die Gleichungen (102) nacheinander für $m = 1, 2, \ldots, l-1$ und summieren die entstehenden Formeln, so erhalten wir

$$\left.\begin{aligned} &(l-1)\sum_{(\mathfrak{p})}\frac{1}{n(\mathfrak{p})^s} + (l-1)\,S \\ &+ \sum_{(u_1,\ldots,u_t)} \gamma_1^{-u_1}\cdots\gamma_t^{-u_t} \log \prod_{(\mathfrak{p})}\prod_{(m)} \frac{1}{1-\left\{\frac{\alpha_1^{u_1}\cdots\alpha_t^{u_t}}{\mathfrak{p}}\right\}^m n(\mathfrak{p})^{-s}} \\ &= l^t \sum_{(\mathfrak{r})}\frac{1}{n(\mathfrak{r})^s} + \sum_{(m)} G_m + (l-1)\,S + \sum_{(u_1,\ldots,u_t)} \gamma_1^{-u_1}\cdots\gamma_t^{-u_t} \sum_{(m)} S(\alpha_*^m); \end{aligned}\right| \tag{104}$$

hierbei hat in dem ersten Summenausdruck rechter Hand $\mathfrak{r}$ alle Primideale $\mathfrak{p}$ in $k(\zeta)$ zu durchlaufen, welche irgendeinem von den $l-1$ Bedingungssystemen genügen, die aus (103) entstehen, wenn man darin $m = 1, = 2, \ldots, = l-1$ einführt; für $\gamma_1 = 1, \ldots, \gamma_t = 1$ sind diese Bedingungssysteme identisch und die betreffenden Primideale $l-1$ mal zu nehmen. Gehen wir nun zur Grenze für $s = 1$ über, so wird die erste Summe Σ linker Hand in (104) nach den Ausführungen zu Beginn des Beweises über alle Grenzen wachsen, und die zweite Summe Σ linker Hand bleibt auf Grund von Hilfssatz 27 für $s = 1$ endlich. Da auch die Summen S und $S(\alpha_*^m)$ sämtlich endlich bleiben, so folgt dann, daß der Ausdruck $\sum \frac{1}{n(\mathfrak{r})^s}$ für $s = 1$ über alle Grenzen wächst, und also sind die betreffenden Primideale $\mathfrak{r}$ in unendlicher Anzahl vorhanden; diese Primideale $\mathfrak{r}$ erfüllen hinsichtlich ihrer Potenzcharaktere genau die Forderungen des Satzes 152.

31. Der reguläre Kreiskörper.

§ 136. Die Definition des regulären Kreiskörpers, der regulären Primzahl und des regulären Kummerschen Körpers.

Es bedeute l eine ungerade Primzahl und $k(\zeta)$ den durch $\zeta = e^{\frac{2i\pi}{l}}$ bestimmten Kreiskörper: dieser Kreiskörper $k(\zeta)$ heiße ein **regulärer Kreiskörper** und die Primzahl l **eine reguläre Primzahl,** wenn die Anzahl h der

Idealklassen des Körpers $k(\zeta)$ nicht durch l teilbar ist. Die weiteren Kapitel werden lediglich von regulären Kreiskörpern und von solchen Kummerschen Körpern handeln, welche aus regulären Kreiskörpern entspringen, und die ich daher **reguläre Kummersche Körper** nennen will; für dieselben können wir sofort folgende einfache Tatsache beweisen:

Satz 153. Es sei $k(\zeta)$ ein regulärer Kreiskörper und K ein aus $k(\zeta)$ entspringender Kummerscher Körper: wenn dann ein Ideal $\mathfrak{j}$ des Körpers $k(\zeta)$ in dem Körper K Hauptideal ist, so ist das Ideal $\mathfrak{j}$ auch in dem Kreiskörper $k(\zeta)$ selbst ein Hauptideal.

Beweis. Setzen wir $\mathfrak{j} = (\mathfrak{A})$, wo $\mathfrak{A}$ eine ganze Zahl in K bedeutet, so folgt, indem wir die Relativnorm bilden $\mathfrak{j}^l = (N_k(\mathfrak{A}))$, d. h. es gilt in $k(\zeta)$ die Äquivalenz $\mathfrak{j}^l \sim 1$. Andererseits ist auch $\mathfrak{j}^h \sim 1$, wobei h die Klassenanzahl von $k(\zeta)$ bedeutet. Bestimmen wir nun zwei ganze rationale positive Zahlen a und b, so daß $al - bh = 1$ wird, so folgt $\mathfrak{j}^{al-bh} \sim 1$, d. h. es ist $\mathfrak{j}$ in $k(\zeta)$ ein Hauptideal.

Es entsteht weiter die Aufgabe, ein Kriterium zu finden, durch welches sich auf leichte Weise ermitteln läßt, ob eine Primzahl l regulär ist. Es sollen zunächst zwei Hilfssätze entwickelt werden, die zu einem solchen Kriterium führen.

§ 137. Ein Hilfssatz über die Teilbarkeit des ersten Faktors der Klassenanzahl von $k\left(e^{\frac{2i\pi}{l}}\right)$ durch l.

Hilfssatz 28. Ist l eine ungerade Primzahl und $k(\zeta)$ der Kreiskörper der l-ten Einheitswurzeln, so ist der erste Faktor der Klassenanzahl von $k(\zeta)$ dann und nur dann durch l teilbar, wenn l im Zähler einer der ersten $l^* = \frac{l-3}{2}$ Bernoullischen Zahlen aufgeht [Kummer (8), Kronecker (5)].

Beweis. In Satz 142 ist die Klassenanzahl h des Körpers $k(\zeta)$ als Produkt von zwei Faktoren dargestellt; wir betrachten den dort angegebenen Ausdruck für den ersten Faktor dieser Klassenanzahl. Zur Abkürzung werde $Z = e^{\frac{2i\pi}{l-1}}$ gesetzt; ferner denken wir uns die zugrunde gelegte Primitivzahl r nach l speziell derart angenommen, daß $r^{\frac{l-1}{2}} + 1$ nur durch die erste Potenz von l teilbar ist. Es sei endlich, wie in § 108 und § 109, allgemein r_i der kleinste positive Rest von r^i nach l und $q_i = \frac{r r_i - r_{i+1}}{l}$.

Der erste Faktor der Klassenanzahl h stellt sich in Satz 142 als ein Bruch dar, dessen Nenner den Wert $(2l)^{l^*}$ hat, und dessen Zähler von der Gestalt

$$f(Z)\,f(Z^3)\,f(Z^5)\cdots f(Z^{l-2}) \tag{105}$$

ist, wo zur Abkürzung $f(x)$ die ganzzahlige Funktion

$$f(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_{l-2} x^{l-2}$$

bezeichnet. Wird ferner

$$g(x) = q_0 + q_1 x + q_2 x^2 + \cdots + q_{l-2} x^{l-2}$$

gesetzt, so ergibt sich leicht

$$(r\,\mathsf{Z} - 1) f(\mathsf{Z}) = l\,\mathsf{Z} \cdot g(\mathsf{Z}),$$

und da infolge der Wahl von r das Produkt

$$(r\,\mathsf{Z} - 1)(r\,\mathsf{Z}^3 - 1) \cdots (r\,\mathsf{Z}^{l-2} - 1) = (-1)^{\frac{l-1}{2}} \left(r^{\frac{l-1}{2}} + 1\right)$$

genau durch die erste Potenz von l teilbar ist, so folgt, daß der Zähler (105) des ersten Faktors von h nur dann durch $l^{\frac{l-1}{2}} = l^{l^*+1}$ teilbar ist, wenn die Zahl

$$g(\mathsf{Z})\, g(\mathsf{Z}^3)\, g(\mathsf{Z}^5) \cdots g(\mathsf{Z}^{l-2})$$

durch l teilbar ist. Nun ist $\mathfrak{L} = (l, \mathsf{Z} - r)$ ein in l aufgehendes Primideal des Körpers $k(\mathsf{Z})$, und da offenbar $\mathsf{Z} \equiv r$ nach $\mathfrak{L}$ ausfällt, so ist

$$g(\mathsf{Z})\, g(\mathsf{Z}^3) \cdots g(\mathsf{Z}^{l-2}) \equiv g(r)\, g(r^3) \cdots g(r^{l-2}), \qquad (\mathfrak{L});$$

folglich ist der erste Faktor der Klassenanzahl h nur dann durch l teilbar, wenn mindestens eine der $\frac{l-1}{2}$ Kongruenzen

$$g(r^{2t-1}) = q_0 + q_1 r^{2t-1} + q_2 r^{2(2t-1)} + \cdots + q_{l-2} r^{(l-2)(2t-1)} \equiv 0, \qquad (l)$$
$$\left(t = 1, 2, 3, \ldots, \frac{l-1}{2}\right)$$

erfüllt ist.

Es bedeute nun t eine der Zahlen $1, 2, 3, \ldots, \frac{l-1}{2}$. Erheben wir dann die Identität

$$r\, r_i = r_{i+1} + (r\, r_i - r_{i+1})$$

in die $(2t)$-te Potenz und bedenken, daß $r r_i - r_{i+1}$ durch l teilbar ist, so ergibt sich die Kongruenz

$$r^{2t} r_i^{2t} \equiv r_{i+1}^{2t} + 2t\,(r\, r_i - r_{i+1})\, r_{i+1}^{2t-1}, \qquad (l^2)$$

oder

$$2t\,(r\, r_i - r_{i+1})\, r_{i+1}^{2t-1} \equiv r^{2t} r_i^{2t} - r_{i+1}^{2t}, \qquad (l^2)$$

und da offenbar

$$(r\, r_i - r_{i+1})\, r_{i+1}^{2t-1} \equiv (r\, r_i - r_{i+1})\, r^{(i+1)(2t-1)}, \qquad (l^2)$$

ist, so folgt

$$2t\,(r\, r_i - r_{i+1})\, r^{(i+1)(2t-1)} \equiv r^{2t} r_i^{2t} - r_{i+1}^{2t}, \qquad (l^2).$$

Diese allgemeine Kongruenz ergibt bei Summation über die Werte $i = 0, 1, 2, \ldots, l-2$

$$2t\, l\, r^{2t-1} \sum_{(i)} q_i r^{i(2t-1)} \equiv r^{2t} \sum_{(i)} r_i^{2t} - \sum_{(i)} r_{i+1}^{2t}, \qquad (l^2).$$

Da nun

$$\sum_{(i)} r_i^{2t} = \sum_{(i)} r_{i+1}^{2t} = 1^{2t} + 2^{2t} + 3^{2t} + \cdots + (l-1)^{2t}$$

ist, so folgt, daß die Zahl $g(r^{2t-1})$ dann und nur dann durch l teilbar ist, wenn die Zahl

$$(r^{2t} - 1)(1^{2t} + 2^{2t} + 3^{2t} + \cdots + (l-1)^{2t}) \qquad (106)$$

durch l^2 teilbar ist. Wegen der über die Primitivzahl r gemachten Annahme ist nun der Ausdruck (106) für $t = \frac{l-1}{2}$ sicher nicht durch l^2 teilbar. Für $t = 1, 2, \ldots, \frac{l-3}{2}$ gilt auf Grund der Bernoullischen Summenformel jedesmal die Kongruenz

$$1^{2t} + 2^{2t} + 3^{2t} + \cdots + (l-1)^{2t} \equiv (-1)^{t+1} B_t\, l, \qquad (l^2),$$

wo B_t die t-te **Bernoullische Zahl** bedeutet, und somit erkennen wir, daß die Teilbarkeit wenigstens einer der Zahlen (106) für

$$t = 1, 2, \ldots, \frac{l-3}{2}$$

durch l^2 mit der Teilbarkeit wenigstens eines der Zähler der $\frac{l-3}{2}$ ersten Bernoullischen Zahlen durch l gleichbedeutend ist. Der Beweis des Hilfssatzes 28 ist dadurch erbracht.

§ 138. Ein Hilfssatz über die Einheiten des Kreiskörpers $k\left(e^{\frac{2i\pi}{l}}\right)$ für den Fall, daß l in den Zählern der ersten $\frac{l-3}{2}$ Bernoullischen Zahlen nicht aufgeht.

Hilfssatz 29. Wenn l eine ungerade Primzahl bedeutet, welche in den Zählern der ersten $l^* = \frac{l-3}{2}$ Bernoullischen Zahlen nicht aufgeht, so läßt sich aus den Kreiseinheiten des Körpers $k(\zeta)$ der l-ten Einheitswurzeln stets durch Bildung geeigneter Produkte und Quotienten ein System von solchen l^* Einheiten $\varepsilon_1, \ldots, \varepsilon_{l^*}$ ableiten, für welche l^* Kongruenzen von der Gestalt

$$\left.\begin{aligned} \varepsilon_1 &\equiv 1 + a_1 \lambda^2, && (l^3), \\ \varepsilon_2 &\equiv 1 + a_2 \lambda^4, && (l^5), \\ \varepsilon_3 &\equiv 1 + a_3 \lambda^6, && (l^7), \\ &\cdots\cdots\cdots\cdots \\ \varepsilon_{l^*} &\equiv 1 + a_{l^*} \lambda^{l-3}, && (l^{l-2}) \end{aligned}\right\} \qquad (107)$$

gelten, wo $a_1, a_2, \ldots, a_{l^*}$ ganze rationale, durch l nicht teilbare Zahlen bedeuten; dabei ist $\lambda = 1 - \zeta$, $\mathfrak{l} = (\lambda)$ gesetzt [Kummer (*12*)].

Beweis. Wir gehen aus von der Kreiseinheit (vgl. § 98)

$$\varepsilon = \sqrt{\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}}, \qquad (108)$$

wo r eine Primitivzahl nach l bezeichnet. Wir setzen dann $\eta = \varepsilon^{l-1}$ und

$$\varepsilon_t = \eta^{(r^2-s)(r^4-s)\cdots(r^{2t-2}-s)(r^{2t+2}-s)(r^{2t+4}-s)\cdots(r^{l-3}-s)} \qquad (109)$$

für $t = 1, 2, 3, \ldots, l^*$, wo $s = (\zeta : \zeta^r)$ im Exponenten symbolisch zu verstehen ist.

Die Einheit η ist als $(l-1)$-te Potenz einer ganzen Zahl in $k(\zeta)$ notwendig $\equiv 1$ nach $\mathfrak{l}$, und das gleiche gilt dann auch von jeder der Einheiten ε_t. Wir denken uns nun allgemein bei jedem Werte t die zur Einheit ε_t gehörende Funktion $\varepsilon_t(x)$ gemäß § 131 gebildet; dann gelten für die rationalen Zahlen

$$\mathfrak{l}^{(1)}(\varepsilon_t), \qquad \mathfrak{l}^{(2)}(\varepsilon_t), \ldots, \mathfrak{l}^{(l-2)}(\varepsilon_t),$$

d. h. für die Werte der ersten $l-2$ Differentialquotienten des Logarithmus von $\varepsilon_t(e^v)$ an der Stelle $v = 0$, die Kongruenzen:

$$\left.\begin{aligned} &\mathfrak{l}^{(u)}(\varepsilon_t) \equiv 0, && (l)\\ &(u = 1, 2, 3, \ldots, 2t-1, 2t+1, \ldots, l-3, l-2),\\ &\mathfrak{l}^{(2t)}(\varepsilon_t) \equiv (-1)^{t+1\cdot} \frac{B_t}{4t\,r^{2t}}, && (l)\\ &(t = 1, 2, \ldots, l^*). \end{aligned}\right\} \tag{110}$$

Um dies zu beweisen, bedenken wir, daß nach den Formeln S. 266 oben bei der Berechnung der ersten $l-2$ Differentialquotienten

$$\mathfrak{l}^{(1)}(\eta), \qquad \mathfrak{l}^{(2)}(\eta), \ldots, \mathfrak{l}^{(l-2)}(\eta)$$

in bezug auf die Zahl η an Stelle der zu η gehörenden Funktion direkt die folgende ganze Funktion

$$\tilde{\eta}(x) = \left(\frac{(1-x^r)(1-x^{-r})}{(1-x)(1-x^{-1})}\right)^{\frac{l-1}{2}}$$

genommen werden darf. Nun gilt bekanntlich die Entwicklung

$$\log \frac{e^v - 1}{v} = +\frac{1}{2}v + \frac{B_1}{2\cdot 2!}v^2 - \frac{B_2}{4\cdot 4!}v^4 + \frac{B_3}{6\cdot 6!}v^6 - \cdots,$$

wo $B_1, B_2, B_3, \ldots$ die Bernoullischen Zahlen bedeuten. Mit Benutzung dieser unendlichen Reihe folgt

$$\left.\begin{aligned} \log \tilde{\eta}(e^v) = (l-1)\Big\{&\log r + (r^2-1)\frac{B_1}{2\cdot 2!}v^2\\ &- (r^4-1)\frac{B_2}{4\cdot 4!}v^4 + (r^6-1)\frac{B_3}{6\cdot 6!}v^6 - \cdots\Big\}. \end{aligned}\right\} \tag{111}$$

Von derselben Verwendbarkeit wie $\tilde{\eta}(e^v)$ in bezug auf die Zahl η ist die Funktion $\tilde{\eta}(e^{rv})$ in bezug auf die Zahl $s\eta$, $\tilde{\eta}(e^{r^2v})$ in bezug auf $s^2\eta$ usf. Ersetzen wir dann nach Entwicklung des Ausdrucks (109) von ε_t darin η, $s\eta$, $s^2\eta, \ldots$ durch $\tilde{\eta}(e^v)$, $\tilde{\eta}(e^{rv})$, $\tilde{\eta}(e^{r^2v}), \ldots$, so entsteht eine Funktion $\tilde{\varepsilon}_t(e^v)$, welche nach den Ausführungen auf S. 266 bei Bildung von $\mathfrak{l}^{(1)}(\varepsilon_t), \mathfrak{l}^{(2)}(\varepsilon_t), \ldots, \mathfrak{l}^{(l-2)}(\varepsilon_t)$ die Stelle der Funktion $\varepsilon_t(e^v)$ vertreten kann. Aus (111) ergibt sich

$$\begin{aligned} \log \tilde{\varepsilon}_t(e^v) = (l-1)\Big\{&C + (-1)^t(r^2-r^{2t})(r^4-r^{2t})\cdots\\ &\cdots(r^{2t-2}-r^{2t})(r^{2t+2}-r^{2t})(r^{2t+4}-r^{2t})\cdots(r^{l-3}-r^{2t})(1-r^{2t})\frac{B_t}{2t\,(2t)!}v^{2t}\Big\}\\ &+ C_{l-1}v^{l-1} + C_{l+1}v^{l+1} + \cdots, \end{aligned}$$

wo $C, C_{l-1}, C_{l+1}, \ldots$ gewisse Konstanten bedeuten. Das ausführlich geschriebene Produkt in dem Koeffizienten von v^{2t} ist

$$(-1)^{l^*}\left[\frac{\mathrm{d}(x-1)(x-r^2)\cdots(x-r^{l-3})}{\mathrm{d}x}\right]_{x=r^{2t}},$$

und die hier zu differentiierende Funktion ist $\equiv x^{\frac{l-1}{2}} - 1$ nach l. Aus dieser Entwicklung folgt nun unmittelbar die Richtigkeit der Kongruenzen (110).

Da nach Voraussetzung die Zähler der ersten l^* Bernoullischen Zahlen $B_1, \ldots, B_{l^*}$ nicht durch l teilbar sein sollen, so sind nach (110) die l^* Differentialquotienten $\mathfrak{l}^{(2t)}(\varepsilon_t)$ für $t = 1, 2, \ldots, l^*$ sämtlich der Null inkongruent nach l. Aus dem letzteren Umstande schließen wir zunächst, daß keine der Einheiten $\varepsilon_1, \ldots, \varepsilon_{l^*}$ nach l der Zahl 1 kongruent ausfällt. Setzen wir daher

$$\left.\begin{aligned} \varepsilon_1 &\equiv 1 + a_1\lambda^{e_1}, && (\mathfrak{l}^{e_1+1}),\\ &\cdots\cdots\cdots\cdots\cdots\\ \varepsilon_{l^*} &\equiv 1 + a_{l^*}\lambda^{e_{l^*}}, && (\mathfrak{l}^{e_{l^*}+1}) \end{aligned}\right\} \tag{112}$$

mit solchen Exponenten $e_1, \ldots, e_{l^*}$, daß dabei $a_1, \ldots, a_{l^*}$ ganze rationale, nicht durch l teilbare Zahlen bedeuten, so sind diese Exponenten $e_1, \ldots, e_{l^*}$ sämtlich $< l-1$. Nun erhält man aus den Kongruenzen (112), da die Entwicklung eines Ausdruckes $(1 - e^v)^g$ nach Potenzen von v mit dem Gliede $(-1^g)v^g$ beginnt, für die Einheit ε_t die Kongruenzen

$$\begin{aligned} &\mathfrak{l}^{(1)}(\varepsilon_t) \equiv 0, \quad \mathfrak{l}^{(2)}(\varepsilon_t) \equiv 0, \ldots, \mathfrak{l}^{(e_t-1)}(\varepsilon_t) \equiv 0, && (l),\\ &\mathfrak{l}^{(e_t)}(\varepsilon_t) \equiv (-1)^{e_t} a_t \cdot e_t!, && (l), \end{aligned}$$

und da a_t nicht durch l teilbar sein soll, so ergibt sich mit Rücksicht auf die vorhin bemerkte Folgerung aus den Kongruenzen (110) $e_t = 2t$, womit der Hilfssatz 29 bewiesen ist.

§ 139. Ein Kriterium für die regulären Primzahlen.

Der folgende Satz liefert ein einfaches Kriterium für die regulären Primzahlen l:

Satz 154. Eine ungerade Primzahl l ist dann und nur dann regulär, wenn sie in den Zählern der ersten $l^* = \frac{l-3}{2}$ Bernoullischen Zahlen nicht aufgeht [Kummer (8)].

Beweis. Der Hilfssatz 28 zeigt, daß, wenn l im Zähler wenigstens einer der ersten l^* Bernoullischen Zahlen aufgeht, die Klassenanzahl h des Körpers $k(\zeta)$ jedenfalls durch l teilbar ist. Sind hingegen die Zähler der ersten l^* Bernoullischen Zahlen sämtlich zu l prim, so zeigt der nämliche Hilfssatz 28, daß der erste Faktor der Klassenanzahl zu l prim ist. Es bedarf also nur noch des Nachweises, daß auch der zweite Faktor der Klassenanzahl h nicht durch l teilbar ist, wenn die Zähler der ersten l^* Bernoullischen Zahlen sämtlich zu l prim sind. Diesen Nachweis führen wir in folgender Weise:

Es sei $\gamma_1, \ldots, \gamma_{l^*}$ ein System von reellen l^* Grundeinheiten des Körpers $k(\zeta)$, wie ein solches nach Satz 127 stets existiert; dann können wir setzen:

$$s^t \varepsilon = \gamma_1^{m_{1t}} \gamma_2^{m_{2t}} \cdots \gamma_{l^*}^{m_{l^*t}} \tag{113}$$

für $t = 0, 1, 2, \ldots, l^* - 1$, wo die Exponenten $m_{1t}, m_{2t}, \ldots, m_{l^*t}$ ganze rationale Zahlen sind und ε die in Formel (108) definierte Kreiseinheit bedeutet. Aus (113) erhalten wir:

$$\log|s^t \varepsilon| = m_{1t}\log|\gamma_1| + m_{2t}\log|\gamma_2| + \cdots + m_{l^*t}\log|\gamma_{l^*}| \tag{114}$$

für $t = 0, 1, 2, \ldots, l^* - 1$, wo unter den Logarithmen deren reelle Werte verstanden werden sollen. Andererseits bringen die Definitionsgleichungen (109) der Einheiten $\varepsilon_1, \ldots, \varepsilon_{l^*}$ ein Gleichungssystem von der Gestalt

$$\varepsilon_t = \varepsilon^{n_{1t}} (s\,\varepsilon)^{n_{2t}} \cdots (s^{l^*-1}\varepsilon)^{n_{l^*t}}, \qquad (t = 1, 2, \ldots, l^*) \tag{115}$$

mit sich. Von demselben gehen wir zu den Gleichungen

$$\log \varepsilon_t = n_{1t}\log|\varepsilon| + n_{2t}\log|s\,\varepsilon| + \cdots + n_{l^*t}\log|s^{l^*-1}\varepsilon| \tag{116}$$
$$(t = 1, 2, \ldots, l^*)$$

über, wo für die Logarithmen wieder die reellen Werte eintreten sollen, und vermöge (114) wird hieraus

$$\log \varepsilon_t = M_{1t}\log|\gamma_1| + M_{2t}\log|\gamma_2| + \cdots + M_{l^*t}\log|\gamma_{l^*}|, \tag{117}$$
$$(t = 1, 2, \ldots, l^*)$$

wo $M_{1t}, M_{2t}, \ldots, M_{l^*t}$ die bekannten bilinearen Verbindungen der $2l^{*2}$ ganzen rationalen Zahlen $n_{11}, n_{21}, \ldots, n_{l^*l^*}; m_{10}, m_{20}, \ldots, m_{l^*l^*-1}$ bedeuten. Aus den Gleichungssystemen (113) und (115) entspringen jedesmal $l^* - 1$ weitere Gleichungssysteme, wenn wir auf die darin vorkommenden Einheiten die Substitutionen $s, s^2, \ldots, s^{l^*-1}$ anwenden. Indem wir dann wieder die betreffenden Logarithmen nehmen, erhalten wir diejenigen Gleichungssysteme, die aus den Gleichungssystemen (114), (116) und (117) hervorgehen, wenn man auf die darin vorkommenden Einheiten der Reihe nach durchgehends die Substitution s, bez. $s^2, \ldots$, bez. s^{l^*-1} anwendet.

Setzen wir nun

$$R = \begin{vmatrix} \log|\gamma_1|, & \ldots, & \log|\gamma_{l^*}| \\ \log|s\gamma_1|, & \ldots, & \log|s\gamma_{l^*}| \\ \cdots & \cdots & \cdots \\ \log|s^{l^*-1}\gamma_1|, & \ldots, & \log|s^{l^*-1}\gamma_{l^*}| \end{vmatrix},$$

$$\Delta = \begin{vmatrix} \log|\varepsilon|, & \log|s\,\varepsilon|, \ldots, & \log|s^{l^*-1}\varepsilon| \\ \log|s\,\varepsilon|, & \log|s^2\varepsilon|, \ldots, & \log|s^{l^*}\varepsilon| \\ \cdots & \cdots & \cdots \\ \log|s^{l^*-1}\varepsilon|, & \log|s^{l^*}\varepsilon|, \ldots, & \log|s^{2l^*-2}\varepsilon| \end{vmatrix},$$

$$\bar{\Delta} = \begin{vmatrix} \log\varepsilon_1, & \log\varepsilon_2, & \ldots, & \log\varepsilon_{l^*} \\ \log s\varepsilon_1, & \log s\varepsilon_2, & \ldots, & \log s\varepsilon_{l^*} \\ \cdots & \cdots & \cdots & \cdots \\ \log s^{l^*-1}\varepsilon_1, & \log s^{l^*-1}\varepsilon_2, & \ldots, & \log s^{l^*-1}\varepsilon_{l^*} \end{vmatrix},$$

so ergibt eine Anwendung des Multiplikationssatzes der Determinanten

$$\left.\begin{aligned} \frac{\bar{\Delta}}{R} = \frac{\bar{\Delta}}{\Delta}\cdot\frac{\Delta}{R} = \begin{vmatrix} M_{11}, & M_{21}, & \ldots, & M_{l^*1} \\ M_{12}, & M_{22}, & \ldots, & M_{l^*2} \\ \cdots & \cdots & \cdots & \cdots \\ M_{1l^*}, & M_{2l^*}, & \ldots, & M_{l^*l^*} \end{vmatrix} \end{aligned}\right\}. \tag{118}$$

Die rechts stehende Determinante ist eine ganze rationale und überdies eine zu l prime Zahl. Wäre nämlich diese Determinante durch l teilbar, so würde man imstande sein, l^* ganze rationale Zahlen $N_1, \ldots, N_{l^*}$ zu finden, die nicht sämtlich durch l teilbar sind, während die aus ihnen gebildeten Ausdrücke

$$\sum_{(t)} N_t M_{1t}, \qquad \sum_{(t)} N_t M_{2t}, \ldots, \qquad \sum_{(t)} N_t M_{l^*t} \qquad (t = 1, 2, \ldots, l^*)$$

sämtlich durch l teilbar ausfallen. Durch Berücksichtigung dieses zweiten Umstandes ergibt sich aus (117) eine Gleichung von der Gestalt

$$N_1 \log \varepsilon_1 + N_2 \log \varepsilon_2 + \cdots + N_{l^*} \log \varepsilon_{l^*} = l \log \mathsf{E},$$

in welcher E eine gewisse positive Einheit des Körpers $k(\zeta)$ bezeichnet. Setzen wir beide Seiten in den Exponenten von e, so haben wir

$$\varepsilon_1^{N_1} \varepsilon_2^{N_2} \cdots \varepsilon_{l^*}^{N_{l^*}} = \mathsf{E}^l. \tag{119}$$

Es ist nun das Bestehen einer solchen Gleichung (119) unmöglich. Denn es würde zunächst $\mathsf{E} \equiv \mathsf{E}^l \equiv 1$ nach $\mathfrak{l}$ folgen; denken wir uns die zu E gehörende Funktion $\mathsf{E}(x)$ eingeführt und betrachten wir die Werte der ersten $l-2$ Differentialquotienten von $\log \mathsf{E}(e^v)$ an der Stelle $v = 0$, so würden aus (119) unter Verwendung von (110) die Kongruenzen

$$(-1)^{t+l^*} \frac{B_t}{4t^{2t}} N_t \equiv 0, \qquad (l), \qquad (t = 1, 2, \ldots, l^*)$$

folgen. Es sollen aber die Bernoullischen Zahlen $B_1, B_2, \ldots, B_{l^*}$ sämtlich zu l prim und andererseits die Zahlen $N_1, \ldots, N_{l^*}$ nicht sämtlich kongruent 0 nach l sein; wir erhalten damit einen Widerspruch.

Hiernach ist die Determinante rechts in (118) nicht durch l teilbar. Da andererseits ihre Faktoren $\frac{\bar{\Delta}}{\Delta}$ und $\frac{\Delta}{R}$ beide ebenfalls als ganze Zahlen erscheinen und $\frac{\Delta}{R}$ den zweiten Faktor der Klassenanzahl h darstellt, so ist auch der zweite Faktor der Klassenanzahl nicht durch l teilbar. Damit ist der Beweis des Satzes 154 vollständig erbracht.

Auf Grund des Satzes 154 findet sich aus den Werten der ersten 47 Bernoullischen Zahlen, daß außer den drei Primzahlen 37, 59, 67 die unterhalb 100 liegenden Primzahlen sämtlich regulär sind. Wie sich ferner durch Rechnung findet, sind die Klassenanzahlen h der Kreiskörper $k\left(e^{\frac{2i\pi}{l}}\right)$ für $l = 37, 59, 67$ nur durch die erste und nicht durch eine höhere Potenz von l teilbar [Kummer (*11*, *26*)].

§ 140. Ein besonderes System von unabhängigen Einheiten im regulären Kreiskörper.

Wir haben in § 139 die Mittel zur Aufstellung eines Systems von Einheiten des regulären Kreiskörpers gewonnen, welches für die weiteren Entwicklungen von Nutzen sein wird.

Satz 155. Ist l eine reguläre Primzahl, so gibt es im Kreiskörper der l-ten Einheitswurzeln stets ein System von $l^* = \frac{l-3}{2}$ unabhängigen Einheiten $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{l^*}$ von der Art, daß für dieselben die Kongruenzen

$$\begin{aligned} \bar{\varepsilon}_1 &\equiv 1 + \lambda^2, && (l^3), \\ \bar{\varepsilon}_2 &\equiv 1 + \lambda^4, && (l^5), \\ &\cdots\cdots\cdots \\ \bar{\varepsilon}_{l^*} &\equiv 1 + \lambda^{l-3}, && (l^{l-2}) \end{aligned}$$

erfüllt sind; dabei ist $\lambda = 1 - \zeta$, $l = (\lambda)$ gesetzt.

Beweis. Da der Kreiskörper $k(\zeta)$ regulär sein soll, so sind in Anbetracht von Satz 154 die Zähler der ersten l^* Bernoullischen Zahlen sämtlich zu l prim, und folglich gibt es nach Hilfssatz 29 l^* Einheiten $\varepsilon_1, \ldots, \varepsilon_{l^*}$, welche die in (107) ausgedrückten Kongruenzeigenschaften besitzen. Da dort die Koeffizienten $a_1, \ldots, a_{l^*}$ sämtlich zu l prim sind, so können wir l^* ganze rationale Zahlen $b_1, \ldots, b_{l^*}$ bestimmen derart, daß

$$a_1 b_1 \equiv 1, \ \ldots, \ a_{l^*} b_{l^*} \equiv 1, \qquad (l)$$

wird. Setzen wir dann

$$\bar{\varepsilon}_1 = \varepsilon_1^{b_1}, \ \ldots, \ \bar{\varepsilon}_{l^*} = \varepsilon_{l^*}^{b_{l^*}},$$

so erfüllen diese Einheiten $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{l^*}$ jedenfalls die in Satz 155 geforderten Kongruenzbedingungen.

Ferner bilden $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{l^*}$ ein System voneinander unabhängiger Einheiten, weil die in § 138 bestimmten Einheiten $\varepsilon_1, \ldots, \varepsilon_{l^*}$ ein solches waren. Um letzteres einzusehen, nehmen wir im Gegenteil an, daß eine Gleichung von der Gestalt

$$\varepsilon_1^{e_1} \cdots \varepsilon_{l^*}^{e_{l^*}} = 1 \qquad (120)$$

bestehe, wo die Exponenten $e_1, \ldots, e_{l^*}$ ganze rationale, nicht sämtlich verschwindende Zahlen sind; dann können wir weiter die Annahme machen, daß diese Exponenten $e_1, \ldots, e_{l^*}$ nicht sämtlich durch l teilbar seien, da im entgegengesetzten Falle offenbar sofort

$$\varepsilon_1^{\frac{e_1}{l}} \cdots \varepsilon_{l^*}^{\frac{e_{l^*}}{l}} = 1$$

folgen würde. Unter der Annahme, daß in (120) die Exponenten $e_1, \ldots, e_{l^*}$ nicht sämtlich durch l teilbar sind, ist aber (120) von der Gestalt der Gleichung (119), und daß eine solche Gleichung unmöglich ist, haben wir bereits in § 139 erkannt.

§ 141. Eine charakteristische Eigenschaft für die Einheiten eines regulären Kreiskörpers.

Satz 156. Wenn l eine reguläre Primzahl bedeutet und im Körper $k(\zeta)$ der l-ten Einheitswurzeln eine solche Einheit E vorliegt, welche einer ganzen rationalen Zahl nach l kongruent ist, so ist sie notwendig die l-te Potenz einer Einheit dieses Kreiskörpers [Kummer (δ)].

Beweis. Wir denken uns ein System von Einheiten $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{l^*}$ gemäß Satz 155 bestimmt; da dieselben ein System unabhängiger Einheiten bilden, so gibt es ganze rationale, nicht sämtlich verschwindende Exponenten $e, e_1, \ldots, e_{l^*}$, so daß

$$\mathsf{E}^e = \bar{\varepsilon}_1^{e_1} \cdots \bar{\varepsilon}_{l^*}^{e_{l^*}} \qquad (121)$$

wird, und wir können, wie sich sofort zeigt, noch annehmen, daß $e, e_1, \ldots, e_{l^*}$ nicht sämtlich durch l teilbar sind. Wäre dann e durch l teilbar, so hätte die Gleichung (121) die Gestalt (119), und daß eine Gleichung von dieser Gestalt nicht statthaben kann, haben wir bereits erkannt. Wäre andererseits e nicht durch l teilbar, so würde jedenfalls $\mathsf{E}^e \equiv 1$ nach $\mathfrak{l}$ und also $\equiv 1$ nach l sein; wir bilden dann für beide Seiten der Gleichung (121) die logarithmischen Differentialquotienten der zu ihnen gehörenden Funktionen. Da wegen $\mathsf{E}^e \equiv 1$ nach l die Zahlen $l^{(g)}(\mathsf{E}^e)$ für $g < l-1$ sämtlich kongruent 0 nach l sind, so folgt, wenn wir dies insbesondere für $g = 2, 4, \ldots, 2\,l^*$ in Anwendung bringen und die Werte der Zahlen $l^{(g)}(\bar{\varepsilon}_1), \ldots, l^{(g)}(\bar{\varepsilon}_{l^*})$ in Rücksicht auf (110) einsetzen, der Reihe nach $e_1 \equiv 0, \ldots, e_{l^*} \equiv 0$ nach l; es wird dann also $\mathsf{E}^e = \mathsf{H}^l$, wo H eine gewisse Einheit des Kreiskörpers bedeutet, während e nach Voraussetzung eine nicht durch l teilbare ganze rationale Zahl ist. Bestimmen wir nun zwei ganze rationale Zahlen a und b, so daß $ae + bl = 1$ wird, so folgt

$$\mathsf{E} = (\mathsf{H}^a \mathsf{E}^b)^l,$$

und hiermit ist der Beweis des Satzes 156 vollständig erbracht.

Ein wesentlich hiervon verschiedener Beweis des Satzes 156 beruht auf folgender Überlegung. Wäre E nicht die l-te Potenz einer Einheit in $k(\zeta)$, so könnte auch die Einheit $\mathsf{H} = \mathsf{E}^{1-s}$ nicht die l-te Potenz einer Einheit sein, wie leicht aus dem Umstande ersichtlich ist, daß $1 - s$ und $1 + s + \cdots + s^{l-2}$ zwei ganzzahlige Funktionen von s sind, die im Sinne der Kongruenz nach l keinen gemeinsamen Faktor haben. Nun wird aber, wenn wir E kongruent einer ganzen rationalen Zahl nach l annehmen, $\mathsf{H} \equiv 1$ nach $\mathfrak{l}^l$, und hieraus würde nach dem zweiten Teile von Satz 148 folgen, daß der Kummersche Körper $k(\sqrt[l]{\mathsf{H}}, \zeta)$ die Relativdiskriminante 1 in bezug auf $k(\zeta)$ besitzt. Da ferner dieser Kummersche Körper relativ-Abelsch vom Relativgrade l in bezug auf $k(\zeta)$ ist, so würde endlich aus Satz 94 folgen, daß die Anzahl der Idealklassen des Kreiskörpers $k(\zeta)$ durch l teilbar sein müßte, was der Annahme, daß $k(\zeta)$ ein regulärer Kreiskörper ist, widerspräche.