§ 142. Der Begriff der primären Zahl im regulären Kreiskörper.

Eine ganze Zahl α des regulären Kreiskörpers $k(\zeta)$ heißt **primär**, wenn sie *erstens* semiprimär ist (s. S. 230), und wenn sie *zweitens* die Eigenschaft besitzt, daß ihr Produkt mit der konjugiert imaginären Zahl, also mit $s^{\frac{l-1}{2}}\alpha$, einer ganzen rationalen Zahl nach $l=\mathfrak{l}^{l-1}$ kongruent wird. Eine primäre Zahl ist also stets zu $\mathfrak{l}$ prim und hat die Kongruenzen

$$\alpha \equiv a, \qquad (\mathfrak{l}^2),$$

$$\alpha \cdot s^{\frac{l-1}{2}}\alpha \equiv b, \qquad (\mathfrak{l}^{l-1})$$

so zu erfüllen, daß a und b ganze rationale Zahlen sind [Kummer (*12*)]. Es gilt die Tatsache:

Satz 157. In einem regulären Kreiskörper $k(\zeta)$ kann eine beliebige zu $\mathfrak{l}$ prime ganze Zahl α stets durch Multiplikation mit einer Einheit in eine primäre Zahl verwandelt werden [Kummer (*12*)].

Beweis. Bilden wir aus α die Zahl $\beta = \alpha \cdot s^{\frac{l-1}{2}}\alpha$, so ist dieselbe offenbar eine Zahl in dem Unterkörper vom Grade $\frac{l-1}{2}$ des Körpers $k(\zeta)$ und genügt daher einer Kongruenz $\beta \equiv a$ nach $\mathfrak{l}^2$, wo a eine ganze rationale, nicht durch l teilbare Zahl bedeutet. Es seien $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{l^*}$ die l^* in § 140 bestimmten Einheiten. Ist nun etwa $\beta \equiv a + a_1\lambda^2$ nach $\mathfrak{l}^4$, wo a_1 eine ganze rationale Zahl bedeute, so bestimme man eine ganze rationale Zahl u_1 so, daß $2au_1 + a_1 \equiv 0$ nach l wird; dann ist notwendig

$$\beta\varepsilon_1^{2u_1} \equiv a, \qquad (\mathfrak{l}^4).$$

Ist ferner etwa $\beta\varepsilon_1^{2u_1} \equiv a + a_2\lambda^4$ nach $\mathfrak{l}^6$, wo a_2 wieder eine ganze rationale Zahl bedeute, so bestimme man eine ganze rationale Zahl u_2 derart, daß $2au_2 + a_2 \equiv 0$ nach l wird; dann ist

$$\beta\varepsilon_1^{2u_1}\varepsilon_2^{2u_2} \equiv a, \qquad (\mathfrak{l}^6).$$

Fahren wir in der begonnenen Weise fort und setzen am Ende

$$\varepsilon = \varepsilon_1^{u_1}\varepsilon_2^{u_2}\cdots\varepsilon_{l^*}^{u_{l^*}},$$

so wird $\beta\varepsilon^2 \equiv a$ nach $\mathfrak{l}^{l-1}$. Ist andererseits ζ^* eine solche Potenz von ζ, daß $\zeta^*\alpha$ semiprimär wird, so ist offenbar $\zeta^*\varepsilon\alpha$ eine primäre Zahl.

Eine reelle primäre Zahl ist stets einer ganzen rationalen Zahl nach $l=\mathfrak{l}^{l-1}$ kongruent. Aus Satz 156 folgt leicht, daß eine primäre Einheit in $k(\zeta)$ stets die l-te Potenz einer Einheit in $k(\zeta)$ ist.

Wir erörtern noch kurz einen Hilfssatz über primäre Zahlen, welcher uns später von Nutzen sein wird.

Hilfssatz 30. Wenn ν, μ zwei primäre Zahlen des regulären Kreiskörpers $k(\zeta)$ sind, so ist stets

$$\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\} = 1.$$

Beweis. Wir dürfen annehmen, daß die Zahlen ν, μ beide $\equiv 1$ nach $\mathfrak{l}$ ausfallen, da sonst ihre $(l-1)$-ten Potenzen sicher dieser Bedingung genügen und wir mit Rücksicht auf $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu^{l-1},\mu^{l-1}}{\mathfrak{l}}\right\}$ (vgl. S. 266) diese an Stelle der Zahlen ν, μ selbst betrachten können. Nach (83) ist

$$\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}\left\{\frac{\nu,s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu,\mu\cdot s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\},$$

und da bei unserer Annahme $\mu\cdot s^{\frac{l-1}{2}}\mu \equiv 1$ nach $\mathfrak{l}^{l-1}$ und $\nu \equiv 1$ nach $\mathfrak{l}^2$ ausfällt, so folgt aus der allgemeinen Definition (82) des Symbols $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$ in § 131 unmittelbar $\left\{\frac{\nu,\mu\cdot s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\} = 1$, und daher wird

$$\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}\left\{\frac{\nu,s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\} = 1.$$

Entsprechend beweisen wir, daß

$$\left\{\frac{\nu,s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\}\left\{\frac{s^{\frac{l-1}{2}}\nu,s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\} = 1$$

ist. Aus Formel (84) ergibt sich ferner:

$$\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}\left\{\frac{s^{\frac{l-1}{2}}\nu,s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\} = 1.$$

Die drei letzten Gleichungen zusammengenommen liefern:

$$\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}^2 = 1, \quad \text{d. h.} \quad \left\{\frac{\nu,\mu}{\mathfrak{l}}\right\} = 1,$$

und damit ist der Hilfssatz 30 bewiesen.

32. Die ambigen Idealklassen und die Geschlechter im regulären Kummerschen Körper.

§ 143. Der Begriff der Einheitenschar im regulären Kreiskörper.

Es sei l eine reguläre ungerade Primzahl, und in dem durch $\zeta = e^{\frac{2i\pi}{l}}$ bestimmten regulären Kreiskörper $k(\zeta)$ sei ein solches System E von Einheiten vorgelegt, in welchem die l-ten Potenzen aller Einheiten des Körpers $k(\zeta)$ enthalten sind, und welchem überdies die Eigenschaft zukommt, daß das Produkt und der Quotient von irgend zwei Einheiten des Systems stets

wieder dem Systeme angehört. Ein solches System E nenne ich eine **Einheitenschar des Kreiskörpers** $k(\zeta)$. Man kann in einer jeden Einheitenschar E stets eine gewisse Anzahl m von Einheiten $\varepsilon_1, \ldots, \varepsilon_m$ bestimmen von der Art, daß man jede Einheit der Einheitenschar und jede nur einmal erhält, wenn man in dem Ausdruck

$$\varepsilon_1^{u_1} \varepsilon_2^{u_2} \cdots \varepsilon_m^{u_m} \xi^l$$

einem jeden der Exponenten $u_1, \ldots, u_m$ unabhängig von den übrigen alle Werte $0, 1, \ldots, l-1$ erteilt und für ξ eine jede Einheit in $k(\zeta)$ einsetzt. Ein System von Einheiten $\varepsilon_1, \ldots, \varepsilon_m$ dieser Beschaffenheit nenne ich eine **Basis der Einheitenschar** E. Es ist klar, daß für die Einheiten $\varepsilon_1, \ldots, \varepsilon_m$ einer Basis von E niemals eine Relation von der Gestalt

$$\varepsilon_1^{e_1} \cdots \varepsilon_m^{e_m} = \varepsilon^l$$

stattfinden kann, wo $e_1, \ldots, e_m$ ganze rationale, nicht sämtlich durch l teilbare Exponenten sind und ε eine Einheit in $k(\zeta)$ bedeutet. Es läßt sich leicht zeigen, daß für eine jede andere Basis der Einheitenschar E die Anzahl m der Einheiten, aus denen sie besteht, die gleiche sein muß. Diese Zahl m ist daher für die Einheitenschar E eine vollkommen bestimmte; sie heiße der **Grad der Einheitenschar.**

Enthält insbesondere eine Einheitenschar nur die l-ten Potenzen der Einheiten in $k(\zeta)$, so ist sie die möglichst wenig Einheiten umfassende Einheitenschar, und ihr Grad 0. Ferner bildet die Gesamtheit aller Einheiten des Körpers $k(\zeta)$ eine Einheitenschar; aus dem Umstande, daß nach Satz 127 jede Einheit in $k(\zeta)$ das Produkt einer l-ten Einheitswurzel und einer reellen Einheit ist, und aus den Entwicklungen beim Beweise des Satzes 157 entnehmen wir sofort, daß die in § 140 mit $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{\frac{l-3}{2}}$ bezeichneten Einheiten mit der Einheitswurzel ζ zusammen eine Basis dieser umfassendsten Einheitenschar sind. Die aus allen Einheiten des Körpers $k(\zeta)$ bestehende Einheitenschar besitzt folglich den Grad $m = \frac{l-1}{2}$; sie ist offenbar die einzige Einheitenschar vom Grade $\frac{l-1}{2}$, und es kann überhaupt keine Einheitenschar von höherem als dem $\frac{l-1}{2}$-ten Grade geben.

Wie man ferner leicht erkennt, bilden die Relativnormen aller Einheiten eines aus $k(\zeta)$ entspringenden Kummerschen Körpers $k(\sqrt[l]{\mu}, \zeta)$ für den Kreiskörper $k(\zeta)$ eine Einheitenschar; endlich ist auch die Gesamtheit aller derjenigen Einheiten in $k(\zeta)$ eine Einheitenschar, welche gleich Relativnormen, sei es von Einheiten, sei es von gebrochenen Zahlen des Kummerschen Körpers $k(\sqrt[l]{\mu}, \zeta)$ sind.

§ 144. Die ambigen Ideale und die ambigen Idealklassen eines regulären Kummerschen Körpers.

Es sei $k(\zeta)$ ein regulärer Kreiskörper, und μ eine ganze Zahl in $k(\zeta)$, welche nicht gleich der l-ten Potenz einer Zahl in $k(\zeta)$ ist; der durch $\mathsf{M} = \sqrt[l]{\mu}$ und ζ bestimmte reguläre Kummersche Körper $k(\mathsf{M}, \zeta)$ werde mit K bezeichnet. Wir suchen nunmehr die Theorie dieses Körpers mittelst der entsprechenden Begriffe und Methoden zu fördern, wie sie in den Kapiteln 17 bis 18 in der Theorie des quadratischen Körpers angewandt worden sind.

Die Relativgruppe von K in bezug auf $k(\zeta)$ wird durch die Potenzen der Substitution $S = (\mathsf{M}:\zeta\,\mathsf{M})$ gebildet; es werde gemäß § 57 ein Ideal $\mathfrak{A}$ des Körpers K ein **ambiges Ideal** genannt, wenn $\mathfrak{A}$ bei Anwendung der Operation S ungeändert bleibt, d. h. $S\mathfrak{A} = \mathfrak{A}$ ist, und wenn außerdem $\mathfrak{A}$ kein von 1 verschiedenes Ideal des Körpers $k(\zeta)$ als Faktor enthält. Nach Satz 93 sind die l in der Relativdiskriminante von K aufgehenden Primideale sämtlich ambig, und es gibt außer diesen auch keine anderen ambigen Primideale. Ist sodann $\mathfrak{A}$ ein beliebiges ambiges Ideal in K, so schließen wir aus $\mathfrak{A} = S\mathfrak{A}$ leicht (vgl. § 73), daß auch jedes in $\mathfrak{A}$ aufgehende Primideal des Körpers K ambig sein muß, und daraus folgt dann, daß die Anzahl aller vorhandenen ambigen Ideale l^h beträgt.

Ist $\mathfrak{C}$ ein Ideal aus einer Klasse C des Kummerschen Körpers K, so werde die durch das relativ konjugierte Ideal $S\mathfrak{C}$ bestimmte Idealklasse mit SC bezeichnet. Die Klassen $SC, S^2C, \ldots, S^{l-1}C$ sollen die zu C **relativ konjugierten Klassen** heißen. Ist ferner $F(S)$ eine beliebige ganzzahlige Funktion vom $(l-1)$-ten Grade in S, nämlich

$$F(S) = a + a_1 S + a_2 S^2 + \cdots + a_{l-1} S^{l-1},$$

wo $a, a_1, \ldots, a_{l-1}$ ganze rationale Zahlen sind, so werde die durch den Ausdruck

$$C^a (SC)^{a_1} (S^2C)^{a_2} \cdots (S^{l-1}C)^{a_{l-1}}$$

bestimmte Klasse die **$F(S)$-te symbolische Potenz** der Klasse C genannt und mit

$$C^{a + a_1 S + a_2 S^2 + \cdots + a_{l-1} S^{l-1}} = C^{F(S)}$$

bezeichnet. Endlich heiße eine Idealklasse A des Kummerschen Körpers K eine **ambige Klasse** wenn $A = SA$, d. h., wenn ihre $(1-S)$-te symbolische Potenz $A^{1-S} = 1$ wird. Die l-te Potenz einer beliebigen ambigen Klasse A ist stets eine solche Klasse, welche unter ihren Idealen in $k(\zeta)$ liegende Ideale enthält. Dies ergibt sich unmittelbar, wenn wir berücksichtigen, daß wir

$$A^l = A^{1 + S + S^2 + \cdots + S^{l-1}}$$

als Folge von $A = SA$ haben und daß andererseits die Relativnorm eines beliebigen Ideals in K stets notwendig ein Ideal in $k(\zeta)$ ist.

§ 145. Der Begriff der Klassenschar im regulären Kummerschen Körper.

Es sei in dem regulären Kummerschen Körper K ein solches System von Klassen vorgelegt, daß in der l-ten Potenz einer jeden dieser Klassen stets Ideale des Körpers $k(\zeta)$ vorkommen, und überdies sollen insbesondere alle diejenigen Klassen, in welchen Ideale des Körpers $k(\zeta)$ vorkommen, dem Systeme angehören; endlich sollen das Produkt und der Quotient von irgend zwei Klassen des Systems stets wiederum dem Systeme angehören. Ein solches System von Klassen nenne ich eine **Klassenschar des Kummerschen Körpers.** In einer vorgelegten Klassenschar kann man stets eine gewisse Anzahl n von Klassen $C_1, \ldots, C_n$ bestimmen von der Beschaffenheit, daß man jede Klasse der Klassenschar und jede nur einmal erhält, wenn man in dem Ausdruck

$$C_1^{u_1} C_2^{u_2} \cdots C_n^{u_n} c$$

einem jeden der Exponenten $u_1, u_2, \ldots, u_n$ unabhängig von den anderen alle Werte $0, 1, \ldots, l-1$ erteilt, und für c eine jede solche Klasse setzt, welche unter ihren Idealen in $k(\zeta)$ liegende Ideale enthält. Die Klassen $C_1, C_2, \ldots, C_n$ mögen dann eine **Basis der Klassenschar** heißen. Es läßt sich leicht zeigen, daß für eine jede andere Basis der Klassenschar die Anzahl n der Klassen, aus welchen die Schar besteht, die gleiche sein muß. Diese Zahl n heiße der **Grad der Klassenschar.**

Enthalten insbesondere alle Klassen einer Schar Ideale des Körpers $k(\zeta)$, so ist die Schar vom Grade 0. Des weiteren ist beispielsweise die Gesamtheit aller derjenigen Klassen in K, in welchen, sei es ambige Ideale in K, sei es Produkte aus ambigen Idealen in K mit Idealen des Körpers $k(\zeta)$ vorkommen, eine Klassenschar. Ferner bildet die Gesamtheit aller ambigen Klassen des Kummerschen Körpers eine Klassenschar.

§ 146. Zwei allgemeine Hilfssätze über die relativen Grundeinheiten eines relativ-zyklischen Körpers von ungeradem Primzahlgrade.

Bevor wir die Untersuchungen des vorigen Paragraphen fortsetzen, leiten wir zwei Hilfssätze ab, die sich an den Satz 91 in § 55 anschließen und wie folgt lauten:

Hilfssatz 31. Es sei der Relativgrad l eines relativ zyklischen Körpers K in bezug auf einen Unterkörper k eine ungerade Primzahl, ferner sei S eine von der identischen verschiedene Substitution der Relativgruppe von K in bezug auf k und $\mathsf{H}_1, \ldots, \mathsf{H}_{r+1}$ ein System von relativen Grundeinheiten des Körpers K in bezug auf k, dann gilt für eine beliebige Einheit E in K jedesmal eine Gleichung von der Gestalt

$$\mathsf{E}^f = \mathsf{H}_1^{F_1(S)} \cdots \mathsf{H}_{r+1}^{F_{r+1}(S)} [\varepsilon],$$

wo f ein ganzer rationaler, nicht durch l teilbarer Exponent ist, $F_1(S), \ldots, F_{r+1}(S)$ ganzzahlige Funktionen vom $(l-2)$-ten Grade in S bezeichnen und $[\varepsilon]$ eine Einheit bedeutet, deren l-te Potenz in k liegt.

Beweis. Aus dem Beweise des Satzes 91 geht hervor, daß die Einheiten

$$\mathsf{H}_1, \ldots, \mathsf{H}_{r+1}, S\mathsf{H}_1, \ldots, S\mathsf{H}_{r+1}, \ldots, S^{l-2}\mathsf{H}_1, \ldots, S^{l-2}\mathsf{H}_{r+1}$$

unter Hinzufügung von r Grundeinheiten des Körpers k voneinander unabhängig sind, und da die Anzahl dieser Einheiten insgesamt $l(r+1)-1$ beträgt, so gibt es, wenn E eine beliebig angenommene Einheit in K bedeutet, für E gewiß Relationen von der Gestalt

$$\mathsf{E}^{G(S)} = \mathsf{H}_1^{G_1(S)} \cdots \mathsf{H}_{r+1}^{G_{r+1}(S)} [\varepsilon], \tag{122}$$

wo $G(S), G_1(S), \ldots, G_{r+1}(S)$ ganzzahlige Funktionen vom $(l-2)$-ten Grade in S sind, unter denen die erste nicht identisch verschwindet, und wo $[\varepsilon]$ eine solche Einheit in K bedeutet, daß $[\varepsilon]^l$ in k liegt. Aus den unendlich vielen vorhandenen Relationen dieser Art denken wir uns eine solche ausgewählt, bei welcher die ganze Funktion $G(\zeta)$ durch eine möglichst niedrige Potenz von $1-\zeta$ teilbar ist. Wir nehmen an, es treffe dies eben für die Relation (122) zu; wir setzen zunächst voraus, es sei dabei $G(\zeta)$ noch mindestens einmal durch $1-\zeta$ teilbar. Nach der Definition der Grundeinheiten in § 55 müssen dann

$$G_1(\zeta), \ldots, G_{r+1}(\zeta)$$

sämtlich ebenfalls durch $1-\zeta$ teilbar sein. Erheben wir die Gleichung (122) in die $(1-S^2)(1-S^3)\ldots(1-S^{l-1})$-te symbolische Potenz und setzen

$$G(\zeta) = (1-\zeta)\, G^*(\zeta),$$
$$G_1(\zeta) = (1-\zeta)\, G_1^*(\zeta), \cdots, G_{r+1}(\zeta) = (1-\zeta) G_{r+1}^*(\zeta),$$

so folgt leicht, indem wir berücksichtigen, daß die $(1+S+S^2+\cdots+S^{l-1})$-te symbolische Potenz einer Einheit in K stets eine Einheit in k wird,

$$\mathsf{E}^{lG^*(S)} = \mathsf{H}^{lG_1^*(S)} \cdots \mathsf{H}_{r+1}^{lG_{r+1}^*(S)} [\varepsilon], \tag{123}$$

wo $[\varepsilon]$ wieder eine Einheit in k oder die l-te Wurzel aus einer Einheit in k bedeutet. Wegen der Gleichung (123) ist eine l-te Wurzel aus dieser Zahl $[\varepsilon]$ sicherlich eine Zahl in K, also, wie leicht ersichtlich, ebenfalls eine solche Einheit in K, deren l-te Potenz in k liegt, und die wiederum mit $[\varepsilon]$ zu bezeichnen ist; aus (123) schließen wir daher:

$$\mathsf{E}^{G^*(S)} = \mathsf{H}_1^{G_1^*(S)} \cdots \mathsf{H}_{r+1}^{G_{r+1}^*(S)} [\varepsilon],$$

wo wiederum $[\varepsilon]$ eine Einheit in K bedeutet, deren l-te Potenz in k liegt. Diese Gleichung ist von der nämlichen Gestalt wie (122), nur daß hier $G^*(\zeta)$ durch eine niedrigere Potenz von $1-\zeta$ teilbar wäre als oben $G(\zeta)$.

Dadurch erhalten wir einen Widerspruch mit unserer Annahme, wonach die zugrunde gelegte Relation (122) bereits eine solche war, in der $G(\zeta)$ eine möglichst niedrige Potenz von $1-\zeta$ enthielt; wir sehen also, daß unter dieser Voraussetzung in (122) $G(\zeta)$ nicht durch $1-\zeta$ teilbar sein kann.

Setzen wir

$$f = G(\zeta)\,G(\zeta^2)\cdots G(\zeta^{l-1}),$$

so wird f eine ganze rationale, nicht durch l teilbare Zahl, und es gibt offenbar zwei ganzzahlige Funktionen $H(S)$, $M(S)$, so daß die Gleichung

$$f = H(S)\,G(S) + M(S)\,(1 + S + S^2 + \cdots + S^{l-1})$$

identisch in S erfüllt ist. Erheben wir (122) in die $H(S)$-te symbolische Potenz, so folgt daraus sofort eine Formel von der im Hilfssatz 31 verlangten Beschaffenheit.

Hilfssatz 32. Es mögen dieselben Bezeichnungen wie in Hilfssatz 31 gelten, und überdies bilden wir die Relativnormen der $r+1$ relativen Grundeinheiten des relativ-zyklischen Körpers K, nämlich

$$\eta_1 = N_k(\mathsf{H}_1),\ \ldots,\ \eta_{r+1} = N_k(\mathsf{H}_{r+1}):$$

dann läßt sich jede Einheit ε in k, welche die Relativnorm einer Einheit E des Körpers K ist, in der Gestalt

$$\varepsilon = \eta_1^{u_1}\cdots\eta_{r+1}^{u_{r+1}}[\varepsilon]^l$$

darstellen, wo $u_1, \ldots, u_{r+1}$ ganze rationale Exponenten sind und $[\varepsilon]$ eine Einheit in K ist.

Beweis. Nach Hilfssatz 31 haben wir für E eine Gleichung

$$\mathsf{E}^f = \mathsf{H}_1^{F_1(S)}\cdots\mathsf{H}_{r+1}^{F_{r+1}(S)}[\varepsilon],$$

wo die Zeichen die dort angegebene Bedeutung besitzen. Indem wir von beiden Seiten dieser Gleichung die Relativnorm in bezug auf k bilden, ergibt sich

$$\varepsilon^f = \eta_1^{F_1(1)}\cdots\eta_{r+1}^{F_{r+1}(1)}[\varepsilon]^l. \tag{124}$$

Bestimmen wir nun zwei ganze rationale Zahlen a, b, so daß

$$1 = af + bl$$

wird, und erheben dann die Gleichung (124) in die a-te Potenz, so entsteht eine Formel von der im Hilfssatz 32 behaupteten Art.

§ 147. Die durch ambige Ideale bestimmten Idealklassen.

Es sei $K = k(\sqrt[l]{\mu}, \zeta)$ ein regulärer Kummerscher Körper; wir nehmen aus seiner Relativgruppe die Substitution $S = (\sqrt[l]{\mu} : \zeta\sqrt[l]{\mu})$. Da ein beliebiges ambiges Ideal $\mathfrak{A}$ des Körpers K vermöge seiner Eigenschaft $\mathfrak{A} = S\mathfrak{A}$ stets eine ambige Klasse bestimmt, so haben wir, um zur Kenntnis der ambigen

Klassen zu gelangen, vor allem die aus den ambigen Idealen entspringende Klassenschar zu untersuchen. Wir beweisen die wichtige Tatsache:

Satz 158. *Es sei t die Anzahl der verschiedenen Primideale, welche in der Relativdiskriminante des regulären Kummerschen Zahlkörpers $K = k(\sqrt[l]{\mu}, \zeta)$ vom Relativgrade l aufgehen; ferner mögen die Relativnormen aller Einheiten von K für $k(\zeta)$ eine Einheitenschar vom Grade m bilden: betrachten wir dann alle diejenigen Klassen, in welchen sei es ambige Ideale des Körpers K, sei es Produkte von ambigen Idealen in K mit Idealen in $k(\zeta)$ vorkommen, so bilden diese eine Klassenschar vom Grade*

$$t + m - \frac{l+1}{2}.$$

Beweis. Wir setzen im folgenden zunächst voraus, daß die Zahl μ nicht von der Gestalt $\varepsilon\alpha^l$ sei, wo ε eine Einheit und α eine Zahl in $k(\zeta)$ bedeuten soll. Es ist dann jede Einheit $[\varepsilon]$ des Körpers $K = k(\sqrt[l]{\mu}, \zeta)$, deren l-te Potenz in $k(\zeta)$ liegt, notwendig selbst in $k(\zeta)$ gelegen. Nunmehr mögen $\mathsf{H}_1, \ldots, \mathsf{H}_{\frac{l-1}{2}}$ ein System von relativen Grundeinheiten des Körpers K in bezug auf $k(\zeta)$ und

$$\eta_1 = N_k(\mathsf{H}_1),\ \ldots,\ \eta_{\frac{l-1}{2}} = N_k(\mathsf{H}_{\frac{l-1}{2}})$$

deren Relativnormen bedeuten.

Wir nehmen *erstens* an, daß der äußerste Fall $m = \frac{l-1}{2}$ eintritt. Aus Hilfssatz 32 schließen wir dann, daß die Einheiten $\eta_1, \ldots, \eta_{\frac{l-1}{2}}$ eine Basis derjenigen Einheitenschar bilden, welche aus den Relativnormen aller Einheiten in K besteht. Andererseits fassen wir die t ambigen Primideale $\mathfrak{L}_1, \ldots, \mathfrak{L}_t$ des Körpers K ins Auge; dieselben bestimmen t ambige Idealklassen, die wir bez. $L_1, \ldots, L_t$ nennen wollen. Um für die aus diesen Klassen entspringende Klassenschar den Grad zu bestimmen, setzen wir

$$\mathsf{M} = \sqrt[l]{\mu} = \mathfrak{L}_1^{a_1}\cdots\mathfrak{L}_t^{a_t}\mathfrak{j}, \tag{125}$$

wo $a_1, \ldots, a_t$ gewisse ganze rationale Exponenten bedeuten, und wo $\mathfrak{j}$ ein Ideal in $k(\zeta)$ ist. Wegen der zu Anfang getroffenen Voraussetzung über μ ist wenigstens einer der Exponenten $a_1, \ldots, a_t$ nicht durch l teilbar; es sei etwa a_t prim zu l. Wir entnehmen aus der Gleichung (125), daß

$$c = L_1^{a_1}\cdots L_t^{a_t}$$

eine solche Klasse ist, die Ideale des Körpers $k(\zeta)$ enthält; da L_t^l ebenfalls eine Klasse dieser Art ist, so folgt hieraus sofort, daß die Klasse L_t sich als Produkt von Potenzen der Klassen $L_1, \ldots, L_{t-1}$ und einer Klasse darstellen läßt, die Ideale des Körpers $k(\zeta)$ enthält.

Wir beweisen jetzt, daß aus den Idealklassen $L_1, \ldots, L_{l-1}$ allein keine Klasse von der Gestalt

$$c' = L_1^{a_1} \cdots L_{l-1}^{a_{l-1}} \tag{126}$$

hervorgehen kann, welche Ideale des Körpers $k(\zeta)$ enthält, während $a_1', \ldots, a_{l-1}'$ ganze rationale, nicht sämtlich durch l teilbare Exponenten sind. In der Tat, auf Grund der Relation (126) würden wir eine Gleichung

$$\mathsf{M}' = \mathfrak{L}_1^{a_1} \cdots \mathfrak{L}_{l-1}^{a_{l-1}} \mathfrak{j}' \tag{127}$$

aufstellen können, so daß $\mathfrak{j}'$ ein Ideal des Körpers $k(\zeta)$ und M' eine ganze Zahl des Körpers K ist; hieraus schließen wir dann, daß $\mathsf{E} = \mathsf{M}'^{1-S}$ eine Einheit in K sein müßte. Auf diese Einheit E wenden wir den Hilfssatz 31 an und erhalten so eine Gleichung von der Gestalt

$$\mathsf{E}^f = \mathsf{H}_1^{F_1(S)} \cdots \mathsf{H}_{\frac{l-1}{2}}^{F_{\frac{l-1}{2}}(S)} \varepsilon, \tag{128}$$

wo f eine ganze rationale, nicht durch l teilbare Zahl, $F_1(S), \ldots, F_{\frac{l-1}{2}}(S)$ ganzzahlige Funktionen von S und ε eine Einheit in $k(\zeta)$ bedeuten. Da offenbar $N_k(\mathsf{E}) = 1$ ist, so ergibt sich durch Bildung der Relativnorm auf beiden Seiten von (128) die Gleichung

$$1 = \eta_1^{F_1(1)} \cdots \eta_{\frac{l-1}{2}}^{F_{\frac{l-1}{2}}(1)} \varepsilon^l.$$

Da $\eta_1, \ldots, \eta_{\frac{l-1}{2}}$ eine Basis einer Einheitenschar bilden sollen, so müssen die ganzen rationalen Zahlen $F_1(1), \ldots, F_{\frac{l-1}{2}}(1)$ sämtlich durch l und demnach die ganzen Zahlen $F_1(\zeta), \ldots, F_{\frac{l-1}{2}}(\zeta)$ sämtlich durch $1-\zeta$ teilbar sein. Setzen wir

$$F_1(\zeta) = (1-\zeta) F_1^*(\zeta), \ \ldots, \ F_{\frac{l-1}{2}}(\zeta) = (1-\zeta) F_{\frac{l-1}{2}}^*(\zeta)$$

und

$$\mathsf{H} = \mathsf{H}_1^{F_1^*(S)} \cdots \mathsf{H}_{\frac{l-1}{2}}^{F_{\frac{l-1}{2}}^*(S)},$$

so wird

$$\mathsf{E}^f = \mathsf{H}^{1-S} \varepsilon^*,$$

wo ε^* wieder eine Einheit in $k(\zeta)$ bedeutet. Durch Bildung der Relativnorm folgt aus letzterer Gleichung $1 = \varepsilon^{*l}$, d. h. ε^* ist eine l-te Einheitswurzel, etwa $= \zeta^\varrho$. Berücksichtigen wir $\mathsf{M}^{1-S} = \zeta^{-1}$, so haben wir

$$\{\mathsf{M}'^f \mathsf{M}^\varrho \mathsf{H}^{-1}\}^{1-S} = 1,$$

d. h. der Ausdruck $\mathsf{M}'^f \mathsf{M}^\varrho \mathsf{H}^{-1}$ stellt eine Zahl in $k(\zeta)$ dar. Da nun M' wegen

(127) das Ideal $\mathfrak{L}_t$ nicht oder zu einem durch l teilbaren Exponenten erhoben enthält, M dagegen das Ideal $\mathfrak{L}_t$ in einer Potenz enthält, deren Exponent a_t nicht durch l teilbar ist, so zeigt die Zerlegung dieser Zahl in Primideale des Körpers $k(\zeta)$ erstens, daß g durch l teilbar sein muß; dann zeigt sie weiter, da f zu l prim ist, daß die Exponenten $a_1', \ldots, a_{l-1}'$ sämtlich durch l teilbar sein müßten, was der Voraussetzung widerspricht. Daraus folgt, daß zwischen den Klassen $L_1, \ldots, L_{l-1}$ eine Relation wie (126) nicht bestehen kann, d. h. die Klassen $L_1, \ldots, L_{l-1}$ bilden unter der gegenwärtigen Annahme, die wesentlich auf $m = \frac{l-1}{2}$ hinauskommt, für die aus allen ambigen Idealen entspringende Klassenschar eine Basis; der Grad dieser Klassenschar ist daher gleich $t-1$, wie es unserem Satze 158 für $m = \frac{l-1}{2}$ entspricht.

Wir nehmen *zweitens* $m = \frac{l-3}{2}$ an; dann muß zwischen den Einheiten $\eta_1, \ldots, \eta_{\frac{l-1}{2}}$ eine Relation von der Gestalt $\eta_1^{e_1} \cdots \eta_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}} = \eta^l$ bestehen, wo die Exponenten $e_1, \ldots, e_{\frac{l-1}{2}}$ ganze rationale, nicht sämtlich durch l teilbare Zahlen sind und η eine Einheit in $k(\zeta)$ bedeutet. Ist etwa $e_{\frac{l-1}{2}}$ nicht durch l teilbar, so sind, wie man aus Hilfssatz 32 schließt, notwendig $\eta_1, \ldots, \eta_{\frac{l-3}{2}}$ eine Basis der aus den Relativnormen aller Einheiten in K gebildeten Einheitenschar. Wir bilden nun die Einheit

$$\mathsf{E} = \mathsf{H}_1^{e_1} \cdots \mathsf{H}_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}} \eta^{-1}. \tag{129}$$

Da diese die Relativnorm 1 besitzt, so gibt es nach Satz 90 (S. 149) eine ganze Zahl Λ in K von der Beschaffenheit, daß $\mathsf{E} = \Lambda^{1-S}$ wird. Wir bestimmen nun, was jedenfalls möglich ist, eine ganze rationale positive Zahl r in der Weise, daß in dem Produkt $\mathsf{M}' = \Lambda \mathsf{M}'$ das Primideal $\mathfrak{L}_t$ zu einem durch l teilbaren Exponenten erhoben vorkommt. Es dürfen dann in M' nicht auch die Faktoren $\mathfrak{L}_1, \ldots, \mathfrak{L}_{t-1}$ sämtlich in solchen Potenzen, deren Exponenten durch l teilbar sind, vorkommen, da man sonst unter Benutzung von Satz 153 (S. 279) $\mathsf{M}' = \Theta\alpha$ hätte in der Art, daß Θ eine Einheit in K und α eine ganze Zahl in $k(\zeta)$ bedeutet; dann aber würde $\Theta^{1-S} = \mathsf{E}\zeta^{-r}$ folgen, und dies widerspräche mit Rücksicht auf (129), da $e_{\frac{l-1}{2}}$ zu l prim ist, der Definition der relativen Grundeinheiten $\mathsf{H}_1, \ldots, \mathsf{H}_{\frac{l-1}{2}}$ nach § 55. Es komme nun in M' etwa das ambige Primideal $\mathfrak{L}_{t-1}$ zu einem nicht durch l teilbaren Exponenten erhoben vor. Dann entnehmen wir aus diesem Umstande die Tatsache, daß

die Klasse L_{l-1} sich als Produkt von Potenzen der Klassen $L_1, \ldots, L_{l-2}$ und einer solchen Klasse darstellen läßt, die Ideale des Körpers $k(\zeta)$ enthält.

Wir beweisen jetzt, daß aus den Idealklassen $L_1, \ldots, L_{l-2}$ keine Klasse

$$c'' = L_1^{a_1''} \cdots L_{l-2}^{a_{l-2}''} \tag{130}$$

hervorgehen kann, welche Ideale in $k(\zeta)$ enthält, während die Exponenten $a_1'', \ldots, a_{l-2}''$ ganze rationale, nicht sämtlich durch l teilbare Zahlen sind. In der Tat, eine Relation (130) hätte eine Gleichung von der Gestalt

$$\mathsf{M}'' = \mathfrak{Q}_1^{a_1''} \cdots \mathfrak{Q}_{l-2}^{a_{l-2}''} \mathfrak{j}'' \tag{131}$$

zur Folge von der Art, daß M'' eine ganze Zahl in K und $\mathfrak{j}''$ ein Ideal in $k(\zeta)$ ist; hieraus schließen wir dann, daß $\mathsf{E}' = \mathsf{M}''^{1-S}$ eine Einheit in K sein müßte. Wir wenden für diese Einheit E' den Hilfssatz 31 an und erhalten so eine Gleichung

$$\mathsf{E}'^{f'} = \mathsf{H}_1^{F_1(S)} \cdots \mathsf{H}_{\frac{l-1}{2}}^{F_{\frac{l-1}{2}}(S)} \varepsilon, \tag{132}$$

wo f' eine ganze rationale, nicht durch l teilbare Zahl,

$$F_1(S), \ldots, F_{\frac{l-1}{2}}(S)$$

ganzzahlige Funktionen von S sind und ε eine Einheit in $k(\zeta)$ ist. Wir bestimmen nun einen ganzen rationalen Exponenten u in der Weise, daß die ganze Zahl $F'_{\frac{l-1}{2}}(1) + ue_{\frac{l-1}{2}}$ durch l teilbar wird; mit Rücksicht auf $N_k(\mathsf{E}') = 1$ erhalten wir aus (132) durch Bildung der Relativnorm in bezug auf $k(\zeta)$ die Gleichung:

$$1 = \eta_1^{F_1'(1)+ue_1} \cdots \eta_{\frac{l-3}{2}}^{F'_{\frac{l-3}{2}}(1)+ue_{\frac{l-3}{2}}} \varepsilon'^{l}, \tag{133}$$

wo ε' wiederum eine Einheit in $k(\zeta)$ ist. Da die Einheiten $\eta_1, \ldots, \eta_{\frac{l-3}{2}}$ eine Basis einer Einheitenschar sind, so folgt aus (133), daß die Exponenten $F_1'(1) + ue_1, \ldots, F'_{\frac{l-3}{2}}(1) + ue_{\frac{l-3}{2}}$ sämtlich durch l, d. h. die Zahlen $F_1'(\zeta) + ue_1, \ldots, F'_{\frac{l-3}{2}}(\zeta) + ue_{\frac{l-3}{2}}$ sämtlich durch $1-\zeta$ teilbar sein müssen. Setzen wir

$$F_1'(\zeta) + ue_1 = (1-\zeta) F_1^*(\zeta), \ldots, F_{\frac{l-1}{2}}'(\zeta) + ue_{\frac{l-1}{2}} = (1-\zeta) F^*_{\frac{l-1}{2}}(\zeta)$$

und

$$\mathsf{H}' = \mathsf{H}_1^{F_1^*} \cdots \mathsf{H}_{\frac{l-1}{2}}^{F^*_{\frac{l-1}{2}}},$$

so folgt aus (132)

$$\mathsf{E}'^{f'} \mathsf{E}^u = \mathsf{H}'^{1-S} \varepsilon'^{*},$$

wo E die durch (129) festgelegte Einheit in K und ε'^* wieder eine Einheit in $k(\zeta)$ bedeutet; durch Bildung der Relativnorm erhalten wir $1 = \varepsilon'^{*l}$, d. h. ε'^* ist eine l-te Einheitswurzel, etwa gleich $\zeta^{g'}$. Alsdann wird, wenn wir die Gleichungen

$$\mathsf{M}^{1-S} = \zeta^{-1}, \quad \mathsf{M}'^{1-S} = \mathsf{E}\zeta^{-r}, \quad \mathsf{M}''^{1-S} = \mathsf{E}'$$

berücksichtigen,

$$\{\mathsf{M}''^{f'} \mathsf{M}'^{u} \mathsf{M}^{g'-ur} \mathsf{H}'^{-1}\}^{1-S} = 1,$$

d. h. der Ausdruck $\mathsf{M}''^{f'} \mathsf{M}'^{u} \mathsf{M}^{g'-ur} \mathsf{H}'^{-1}$ stellt eine Zahl in $k(\zeta)$ dar. Beachten wir, daß $\mathfrak{Q}_l', \mathfrak{Q}_{l-1}', \mathfrak{Q}_{l-2}', \ldots, \mathfrak{Q}_1'$ in $k(\zeta)$ Primideale sind, so schließen wir daraus zunächst, daß $g' - ur$ durch l teilbar sein muß; sodann ersehen wir, da M' nach Voraussetzung das Ideal $\mathfrak{Q}_{l-1}$ zu einer Potenz erhoben enthält, deren Exponent nicht durch l teilbar ist, dagegen in der Zahl M'' wegen (131) das Ideal $\mathfrak{Q}_{l-1}$ sicher zu einem durch l teilbaren Exponenten erhoben vorkommt, daß notwendigerweise auch u durch l teilbar sein muß, und endlich müßten dann, da f' zu l prim ist, die Exponenten $a_1'', \ldots, a_{l-2}''$ sämtlich durch l teilbar sein, was unserer Voraussetzung über dieselben widerspricht. Damit ist gezeigt, daß zwischen den Klassen $L_1, \ldots, L_{l-2}$ eine Relation wie (130) nicht bestehen kann, d. h. die Klassen $L_1, \ldots, L_{l-2}$ bilden unter der gegenwärtigen Annahme $m = \frac{l-3}{2}$ für die aus allen ambigen Idealen entspringende Klassenschar eine Basis; der Grad dieser Klassenschar ist daher gleich $l-2$, wie es unserem Satz 158 entspricht.

Wenn wir *drittens* $m = \frac{l-5}{2}$ annehmen, so besteht zwischen den Einheiten $\eta_1, \ldots, \eta_{\frac{l-1}{2}}$ nicht nur, wie im vorigen Falle, *eine* Relation von der Gestalt $\eta_1^{e_1} \cdots \eta_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}} = \eta^l$, wo η eine Einheit in $k(\zeta)$ und einer der Exponenten $e_1, \ldots, e_{\frac{l-1}{2}}$, etwa wieder $e_{\frac{l-1}{2}}$, nicht durch l teilbar ist, sondern es besteht alsdann noch eine zweite Relation von der Gestalt $\eta_1^{e_1'} \cdots \eta_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}} = \eta'^l$, wo η' wieder eine Einheit in $k(\zeta)$ ist, und wo einer der Exponenten $e_1', \ldots, e'_{\frac{l-3}{2}}$, etwa $e'_{\frac{l-3}{2}}$, nicht durch l teilbar ist. Wir bilden die Einheiten

$$\left.\begin{aligned} \mathsf{E} &= \mathsf{H}_1^{e_1} \cdots \mathsf{H}_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}} \eta^{-1}, \\ \mathsf{E}' &= \mathsf{H}_1^{e_1'} \cdots \mathsf{H}_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}} \eta'^{-1}. \end{aligned}\right| \tag{134}$$

Da die Relativnormen der Einheiten E und E' gleich 1 sind, so können wir

nach Satz 90 (S. 149) $\mathsf{E} = A^{1-S}$ und $\mathsf{E}' = A'^{1-S}$ setzen, wobei A und A' ganze Zahlen in K bedeuten. Bestimmen wir dann zunächst, wie im vorigen Falle, eine ganze rationale positive Zahl r derart, daß $\mathsf{M}' = A\,\mathsf{M}^r$ den Faktor $\mathfrak{L}_t$ zu einem durch l teilbaren Exponenten erhoben enthält, so kommt, wie die dortigen Überlegungen zeigen, in M' mindestens eines der ambigen Primideale $\mathfrak{L}_1, \ldots, \mathfrak{L}_{t-1}$ zu einer Potenz erhoben vor, deren Exponent nicht durch l teilbar ist; es treffe dies etwa für $\mathfrak{L}_{t-1}$ zu. Wir bestimmen dann zwei ganze rationale positive Zahlen r' und r'' so, daß die Zahl $\mathsf{M}'' = A'\,\mathsf{M}'^{r'}\,\mathsf{M}^{r''}$ die beiden Faktoren $\mathfrak{L}_t$ und $\mathfrak{L}_{t-1}$ zu Exponenten erhoben enthält, die durch l teilbar sind. Alsdann können in dieser Zahl M'' die Faktoren $\mathfrak{L}_1, \ldots, \mathfrak{L}_{t-2}$ nicht sämtlich zu solchen Potenzen erhoben vorkommen, deren Exponenten durch l teilbar sind. Denn wäre dies der Fall, so könnten wir unter Benutzung von Satz 153 $\mathsf{M}'' = \Theta'\alpha'$ setzen, so daß Θ' eine Einheit in K und α' eine ganze Zahl in $k(\zeta)$ ist. Berücksichtigen wir dann die Gleichungen $\mathsf{M}^{1-S} = \zeta^{-1}$, $A^{1-S} = \mathsf{E}$, $A'^{1-S} = \mathsf{E}'$, so wäre

$$\Theta'^{1-S} = \mathsf{E}'\mathsf{E}'^{r}\,\zeta^{-(rr'+r'')};$$

wegen (134) würde hieraus folgen:

$$\Theta'^{1-S} = \mathsf{H}_1^{e_1+r'e_1} \cdots \mathsf{H}_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}+r'e_{\frac{l-3}{2}}} \mathsf{H}_{\frac{l-1}{2}}^{r'e_{\frac{l-1}{2}}}\,\varepsilon, \tag{135}$$

wo ε eine gewisse Einheit in $k(\zeta)$ bedeutet; diese Relation widerspräche aber der Definition der relativen Grundeinheiten nach § 55; denn da jede der beiden Zahlen $e_{\frac{l-1}{2}}, e'_{\frac{l-3}{2}}$ zu l prim ist, so sind die Exponenten von $\mathsf{H}_{\frac{l-3}{2}}, \mathsf{H}_{\frac{l-1}{2}}$ in (135) sicher niemals beide zugleich durch l teilbar. Kommt nun in M'' etwa $\mathfrak{L}_{t-2}$ zu einem nicht durch l teilbaren Exponenten erhoben vor, so entnehmen wir aus diesem Umstande, daß die Klasse L_{t-2} sich als Produkt von Potenzen der Klassen $L_1, \ldots, L_{t-3}$ und einer solchen Klasse darstellen läßt, die Ideale des Körpers $k(\zeta)$ enthält.

Durch die entsprechenden Überlegungen wie im vorigen Falle $m = \frac{l-3}{2}$ kann man nun unter der gegenwärtigen Annahme $m = \frac{l-5}{2}$ beweisen, daß aus den Idealklassen $L_1, \ldots, L_{t-3}$ keine Klasse

$$\mathfrak{c}''' = L_1^{a'''_1} \cdots L_{t-3}^{a'''_{t-3}}$$

hervorgehen kann, welche Ideale in $k(\zeta)$ enthält, während die Exponenten $a'''_1, \ldots, a'''_{t-3}$ ganze rationale, nicht sämtlich durch l teilbare Zahlen sind. Wir ersehen dann, daß bei der gegenwärtigen Annahme $L_1, \ldots, L_{t-3}$ eine Basis der aus den ambigen Idealen entspringenden Klassenschar bilden; der Grad dieser Klassenschar beträgt folglich $t-3$, wie es dem Satz 158 entspricht.

Durch die geeignete Weiterführung des oben geschilderten Verfahrens gelangen wir zum vollständigen Beweise des Satzes 158.

Wir hatten oben den Fall ausgeschlossen, daß der Kummersche Körper K durch eine Zahl $\sqrt[l]{\varepsilon}$ bestimmt werden kann, wo ε eine Einheit in $k(\zeta)$ bedeutet; wir haben daher diesen Fall jetzt noch besonders zu behandeln. Die Relativdiskriminante des Körpers $K = k(\sqrt[l]{\varepsilon}, \zeta)$ kann alsdann nach Satz 148 keine anderen Primfaktoren als $\mathfrak{l}$ enthalten; nach Satz 94 und Satz 153 muß sie den Faktor $\mathfrak{l}$ wirklich enthalten. Wir haben dann in K eine Zerlegung $\mathfrak{l} = \mathfrak{L}^l$, und es ist $\mathfrak{L}$ das einzige ambige Primideal des Körpers K. Es seien wieder $\eta_1, \ldots, \eta_{\frac{l-1}{2}}$ bez. die Relativnormen der $\frac{l-1}{2}$ relativen Grundeinheiten $\mathsf{H}_1, \ldots, \mathsf{H}_{\frac{l-1}{2}}$. Da der Grad einer Einheitenschar in $k(\zeta)$ stets $\leqq \frac{l-1}{2}$ ist, so besteht sicher eine Relation von der Gestalt:

$$\eta_1^{e_1} \cdots \eta_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}}\,\varepsilon^{e_{\frac{l+1}{2}}} = \eta^l, \tag{136}$$

wo $e_1, \ldots, e_{\frac{l-1}{2}}, e_{\frac{l+1}{2}}$ ganze rationale, nicht sämtlich durch l teilbare Exponenten sind, und wo η eine Einheit in $k(\zeta)$ bedeutet. Setzen wir

$$\mathsf{H} = \mathsf{H}_1^{e_1} \cdots \mathsf{H}_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}} \left(\sqrt[l]{\varepsilon}\right)^{e_{\frac{l+1}{2}}} \eta^{-1}, \tag{137}$$

so ist $N_k(\mathsf{H}) = 1$ und folglich nach Satz 90 $\mathsf{H} = A^{1-S}$, wo A eine geeignete ganze Zahl in K bedeutet; wir können dann $A = \mathfrak{L}^a\mathfrak{j}$ setzen, wo $\mathfrak{L}^a$ eine Potenz des ambigen Primideals $\mathfrak{L}$ und $\mathfrak{j}$ ein Ideal in $k(\zeta)$ bedeutet. Der Exponent a ist dann sicher nicht durch l teilbar; denn sonst wäre wegen $\mathfrak{L}^l = \mathfrak{l} = 1 - \zeta$ und mit Rücksicht auf Satz 153 $A = \Theta\alpha$ in solcher Weise, daß Θ eine Einheit in K und α eine Zahl in $k(\zeta)$ bezeichnet; hieraus aber würden wir $\mathsf{H} = \Theta^{1-S}$ entnehmen und dadurch mit Rücksicht auf (137) in einen Widerspruch mit der Definition der relativen Grundeinheiten in § 55 geraten. Aus der Gleichung $A = \mathfrak{L}^a\mathfrak{j}$ schließen wir $\mathfrak{j}^t \sim 1$, daraus $\mathfrak{j} \sim 1$, $\mathfrak{L}^a \sim 1$ und, da a zu l prim ist, $\mathfrak{L} \sim 1$, d. h. das einzige im gegenwärtigen Fall vorhandene ambige Ideal $\mathfrak{L}$ ist ein Hauptideal; der Grad der aus den ambigen Idealen entspringenden Klassenschar ist mithin gleich 0.

Wir nehmen nun an, von den Exponenten $e_1, \ldots, e_{\frac{l-1}{2}}$ sei etwa $e_{\frac{l-1}{2}}$ prim zu l, und beweisen dann, daß keine Relation

$$\eta_1^{e_1} \cdots \eta_{\frac{l-3}{2}}^{e_{\frac{l-3}{2}}}\,\varepsilon^{e'_{\frac{l+1}{2}}} = \eta'^l \tag{138}$$

bestehen kann von der Art, daß $e'_1, \ldots, e'_{\frac{l-3}{2}}, e'_{\frac{l+1}{2}}$ ganze rationale, nicht sämtlich durch l teilbare Exponenten sind und η' eine Einheit in $k(\zeta)$ bedeutet. In der Tat, würde eine solche Relation (138) gelten, so hätten wir in

$$H' = H_1^{e'_1} \cdots H_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}} \left(\sqrt[l]{\varepsilon}\right)^{e'_{\frac{l+1}{2}}} \eta'^{-1}$$

eine Einheit mit der Relativnorm 1. Wir setzen unter Benutzung des Satzes 90 $H' = A'^{1-S}$, wo A' eine geeignete ganze Zahl in K bedeutet, und bestimmen dann einen solchen ganzen rationalen positiven Exponenten r, daß in $A'A^r$ das Primideal $\mathfrak{L}$ zu einem durch l teilbaren Exponenten vorkommt. Nunmehr können wir mit Rücksicht auf Satz 153 $A'A^r = \Theta'\alpha'$ setzen in solcher Weise, daß Θ' eine Einheit in K und α' eine ganze Zahl in $k(\zeta)$ bedeutet; dann wird $\Theta'^{1-S} = H'H'$, d. h. die Einheit

$$H_1^{e'_1 + re_1} \cdots H_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}} + re_{\frac{l-3}{2}}} H_{\frac{l-1}{2}}^{re_{\frac{l-1}{2}}} \left(\sqrt[l]{\varepsilon}\right)^{e'_{\frac{l+1}{2}} + re_{\frac{l+1}{2}}} \eta'^{-1} \eta^{-r}$$

wäre die symbolische $(1 - S)$-te Potenz einer Einheit in K, und diese Folgerung steht mit der Definition der relativen Grundeinheiten aus dem schon mehrfach erörterten Grunde in Widerspruch. Damit ist gezeigt, daß eine Relation wie (138) nicht statthaben kann; mit Rücksicht auf (136) und auf den Umstand, daß $e_{\frac{l-1}{2}}$ zu l prim ist, bilden nunmehr $\eta_1, \ldots, \eta_{\frac{l-3}{2}}, \varepsilon$ eine Basis der aus den Relativnormen aller Einheiten in K gebildeten Einheitenschar; es folgt also, daß der Grad m dieser Schar gleich $\frac{l-1}{2}$ ist und somit jede Einheit in $k(\zeta)$ die Relativnorm einer Einheit in K ist. Es ist demnach

$$t + m - \frac{l+1}{2} = 0$$

und damit der Satz 158 auch in diesem Falle bestätigt.

§ 148. Die sämtlichen ambigen Idealklassen.

Der Satz 158 hat eine merkwürdige Beziehung aufgedeckt, die zwischen der aus den ambigen Idealen entspringenden Klassenschar und derjenigen Einheitenschar stattfindet, die aus den Relativnormen sämtlicher Einheiten in K gebildet wird. Eine ebenso wichtige Beziehung herrscht zwischen der aus allen ambigen Klassen gebildeten Klassenschar und einer gewissen Einheitenschar in $k(\zeta)$. Wir sprechen folgenden Satz aus:

Satz 159. *Es sei t die Anzahl der Primideale, die in der Relativdiskriminante des regulären Kummerschen Körpers K vom Relativgrade l aufgehen; ferner mögen alle diejenigen Einheiten in $k(\zeta)$, welche gleich Relativnormen sei es von Einheiten, sei es von gebrochenen Zahlen des Körpers K sind, eine Einheitenschar vom Grade n bilden: dann besitzt die aus sämtlichen ambigen Klassen bestehende Klassenschar den Grad $t + n - \frac{l+1}{2}$.*

Beweis. Es habe m die Bedeutung wie in Satz 158. Fällt *erstens* $n = m$ aus, so stimmt die jetzt in Frage kommende Einheitenschar mit der in Satz 158 behandelten Einheitenschar überein, d. h. wenn eine Einheit in $k(\zeta)$ gleich der Relativnorm einer gebrochenen Zahl in K ist, so ist sie stets auch gleich der Relativnorm einer Einheit in K. Wir beweisen nun, daß in diesem Falle die Klassenschar, die aus den ambigen Idealen entspringt, die Schar sämtlicher ambigen Klassen darstellt. In der Tat, wenn A eine beliebige ambige Klasse in K und $\mathfrak{A}$ ein Ideal aus A ist, so können wir $\mathfrak{A}^{1-S} = \mathsf{A}$ setzen in solcher Weise, daß A eine geeignete ganze oder gebrochene Zahl in K bedeutet, und die Relativnorm $N_k(\mathsf{A})$ wird dann offenbar gleich einer Einheit ϑ des Körpers $k(\zeta)$. Da dann unter der gegenwärtigen Annahme $n = m$ nach dem soeben bemerkten auch eine Einheit H in K gefunden werden kann derart, daß $N_k(\mathsf{H}) = \vartheta$ wird, so haben wir $N_k(\mathsf{A}^{-1}\mathsf{H}) = 1$ und folglich nach Satz 90 $\mathsf{A}^{-1}\mathsf{H} = \mathsf{B}^{1-S}$ oder $\mathsf{A}\mathsf{B}^{1-S} = \mathsf{H}$, wo B eine geeignete ganze Zahl in K ist. Wegen $\mathsf{A} = \mathfrak{A}^{1-S}$ wird $(\mathfrak{A}\mathsf{B})^{1-S} = 1$, d. h. es ist $\mathfrak{A}\mathsf{B}$ gleich dem Produkte aus einem ambigen Ideal und einem Ideal in $k(\zeta)$, und es entsteht also die Klasse A durch Multiplikation einer Klasse, die ein ambiges Ideal enthält, mit einer Klasse, die Ideale in $k(\zeta)$ enthält. Damit ist unsere Behauptung bewiesen und der Grad der aus sämtlichen ambigen Klassen gebildeten Klassenschar ist nunmehr mit Rücksicht auf Satz 158 gleich

$$t + m - \frac{l+1}{2},$$

wie es im vorliegenden Falle $n = m$ dem Satz 159 entspricht.

Es sei *zweitens* $n = m + 1$; dann kommt in $k(\zeta)$ eine Einheit ϑ vor, die zwar nicht die Relativnorm einer Einheit in K, aber doch die Relativnorm einer gebrochenen Zahl A in K ist, und es muß sich jede andere Einheit ϑ' von der nämlichen Natur durch die Einheit ϑ solcher Gestalt $\vartheta' = \vartheta^a \eta$ ausdrücken lassen, daß a ein ganzer rationaler Exponent und η die Relativnorm einer Einheit in K ist. Wir setzen

$$\mathsf{A} = \mathfrak{P}_1^{G_1(S)} \cdots \mathfrak{P}_r^{G_r(S)},$$

wo $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ voneinander verschiedene Primideale in K bedeuten sollen, von denen keine zwei zueinander relativ konjugiert sind, und wo $G_1(S), \ldots, G_r(S)$ ganzzahlige Funktionen vom $(l-1)$-ten Grade in S sind. Wegen $N_k(\mathsf{A}) = \vartheta$ folgt

$$(\mathfrak{P}_1^{G_1(S)} \cdots \mathfrak{P}_r^{G_r(S)})^{1+S+\cdots+S^{l-1}} = 1,$$

und hieraus entnehmen wir leicht, daß die Funktionen $G_1(S), \ldots, G_r(S)$

sämtlich durch $1-S$ teilbar sein müssen. Setzen wir

$$G_1(S) = (1-S)\,G_1^*(S),\ \ldots,\ G_r(S) = (1-S)\,G_r^*(S)$$

und

$$\mathfrak{P}_1^{G_1^*(S)} \ldots \mathfrak{P}_r^{G_r^*(S)} = \mathfrak{A}\,\alpha,$$

wo $\mathfrak{A}$ ein Ideal in K und α eine ganze oder gebrochene Zahl in $k(\zeta)$ ist, so wird $\mathsf{A} = \mathfrak{A}^{1-S}$. Hieraus folgt zunächst, daß $\mathfrak{A}$ eine ambige Klasse bestimmt. Diese ambige Klasse, sie heiße A, enthält kein Ideal, welches das Produkt eines ambigen Ideals mit einem Ideal des Körpers $k(\zeta)$ wäre. In der Tat, wäre dies der Fall, so könnten wir $\mathfrak{A} = \Gamma\mathfrak{Q}\mathfrak{j}$ setzen so, daß Γ eine ganze oder gebrochene Zahl in K, ferner $\mathfrak{Q}$ ein ambiges Ideal in K und $\mathfrak{j}$ ein Ideal in $k(\zeta)$ bedeutet; dann aber wäre $\mathfrak{A}^{1-S} = \Gamma^{1-S}$, d. h. $\mathsf{A} = \mathsf{H}\Gamma^{1-S}$, wo H eine Einheit in K ist. Hieraus würde $N_k(\mathsf{A}) = N_k(\mathsf{H}) = \vartheta$ folgen, was der vorausgesetzten Beschaffenheit der Einheit ϑ widerspricht.

Wir wollen nun für die gegenwärtige Annahme $n = m+1$ den Nachweis führen, daß jede überhaupt vorhandene ambige Klasse A' in der Gestalt $A' = A^a Lc$ dargestellt werden kann, wo A^a eine Potenz der soeben bestimmten Klasse A bedeutet, wo ferner L eine Klasse mit ambigem Ideal und c eine solche Klasse bedeutet, die unter ihren Idealen Ideale des Körpers $k(\zeta)$ enthält. Zu dem Zwecke nehmen wir aus A' ein beliebiges Ideal $\mathfrak{A}'$; dann können wir $\mathfrak{A}'^{1-S} = \mathsf{A}'$ setzen in solcher Weise, daß A' eine geeignete ganze oder gebrochene Zahl in K wird. Es ist sodann $N_k(\mathsf{A}') = \vartheta'$ eine Einheit in $k(\zeta)$; wir setzen unserer Voraussetzung entsprechend $N_k(\mathsf{A}') = \vartheta^a\eta$, wo ϑ, a, η die oben erklärte Bedeutung haben sollen. Es sei A die oben betrachtete Zahl für welche $\vartheta = N_k(\mathsf{A})$ ist; es sei ferner $\eta = N_k(\mathsf{H})$, wo H eine Einheit in K bedeute. Aus diesen Gleichungen ergibt sich $N_k(\mathsf{A}'^{-1}\mathsf{A}^a\mathsf{H}) = 1$, und daher wird nach Satz 90 $\mathsf{A}'^{-1}\mathsf{A}^a\mathsf{H} = \Gamma^{1-S}$, wo Γ eine geeignete ganze Zahl in K ist; hieraus entnehmen wir $(\mathfrak{A}'^{-1}\mathfrak{A}^a\Gamma^{-1})^{1-S} = 1$. Die letztere Gleichung zeigt, daß $\mathfrak{A}'^{-1}\mathfrak{A}^a\Gamma^{-1}$ nach Multiplikation mit einer geeigneten ganzen Zahl des Körpers $k(\zeta)$ das Produkt eines ambigen Ideals $\mathfrak{Q}$ in ein Ideal $\mathfrak{j}$ des Körpers $k(\zeta)$ wird; wir haben somit $\mathfrak{A}' \sim \mathfrak{A}^a\mathfrak{Q}\mathfrak{j}$. Es geht daraus in dem vorliegenden Falle $n = m+1$ hervor, daß der Grad der aus sämtlichen ambigen Klassen bestehenden Klassenschar $t + m + 1 - \frac{l+1}{2}$ beträgt, und dies ist die Aussage des Satzes 159 für diesen Fall.

Nehmen wir *drittens* $n = m+2$ an, so existiert in $k(\zeta)$ außer der Einheit ϑ noch eine Einheit ϑ', welche die Relativnorm einer gebrochenen Zahl A' in K ist, und für die dennoch keine Darstellung von der Gestalt $\vartheta' = \vartheta^a\eta$ möglich ist, wo ϑ^a eine Potenz der oben eingeführten Einheit ϑ und η die Relativnorm einer Einheit in K bedeuten soll. Wir setzen

$$\mathsf{A}' = \mathfrak{P}_1'^{G_1'(S)} \ldots \mathfrak{P}_{r'}'^{G_{r'}'(S)},$$

wo $\mathfrak{P}_1', \ldots, \mathfrak{P}_{r'}'$ solche Primideale in K bedeuten sollen, von denen keine

zwei einander gleich oder relativ konjugiert sind, und wo $G_1'(S), \ldots, G_{r'}'(S)$ ganzzahlige Funktionen vom $(l-1)$-ten Grade in S sind. Wegen $N_k(\mathsf{A}') = \vartheta'$ folgt

$$(\mathfrak{P}_1'^{G_1'(S)} \ldots \mathfrak{P}_{r'}'^{G_{r'}'(S)})^{1+S+\cdots+S^{l-1}} = 1,$$

und hieraus entnehmen wir leicht, daß die Funktionen $G_1'(S), \ldots, G_{r'}'(S)$ sämtlich durch $1-S$ teilbar sein müssen. Setzen wir

$$G_1'(S) = (1-S)\,G_1'^*(S),\ \ldots,\ G_{r'}'(S) = (1-S)\,G_{r'}'^*(S)$$

und

$$\mathfrak{P}_1'^{G_1'^*(S)} \ldots \mathfrak{P}_{r'}'^{G_{r'}'^*(S)} = \mathfrak{A}'\alpha',$$

so daß $\mathfrak{A}'$ ein Ideal in K und α' eine ganze oder gebrochene Zahl in $k(\zeta)$ ist, so wird $\mathsf{A}' = \mathfrak{A}'^{1-S}$. Das Ideal $\mathfrak{A}'$ bestimmt daher eine ambige Klasse A'. Diese Klasse ist nicht in der Gestalt $A' = A^a Lc$ darstellbar, wo A^a eine Potenz der Klasse A, L eine Klasse mit einem ambigen Ideal und c eine Klasse mit Idealen in $k(\zeta)$ bedeutet. In der Tat, eine solche Darstellung der Klasse A' hätte für das Ideal $\mathfrak{A}'$ eine Darstellung $\mathfrak{A}' = \Gamma'\mathfrak{A}^a\mathfrak{Q}\mathfrak{j}$ zur Folge, wo Γ' eine Zahl in K, ferner $\mathfrak{Q}$ ein ambiges Ideal und $\mathfrak{j}$ ein Ideal in $k(\zeta)$ bedeuten soll; dann aber wäre $\mathfrak{A}'^{1-S} = \Gamma'^{1-S}\mathfrak{Q}^{a(1-S)} = \Gamma'^{1-S}\mathsf{A}^a$, d. h. $\mathsf{A}' = \mathsf{H}\Gamma'^{1-S}\mathsf{A}^a$, wo H eine Einheit in K ist. Durch Bildung der Relativnorm ergäbe sich nunmehr $N_k(\mathsf{A}') = \vartheta' = \vartheta^a N_k(\mathsf{H})$, und das Vorhandensein einer solchen Relation haben wir oben ausgeschlossen.

Bei der gegenwärtigen Annahme $n = m+2$ muß jede Einheit ϑ'' in $k(\zeta)$, welche die Relativnorm einer Zahl in K ist, in der Gestalt $\vartheta'' = \vartheta'^{a'}\vartheta^a\eta$ darstellbar sein, so daß a', a ganze rationale Exponenten sind und η die Relativnorm einer Einheit in K bedeutet. Indem wir diesen Umstand berücksichtigen, können wir durch ähnliche Überlegungen, wie im vorigen Falle $n = m+1$, zeigen, daß überhaupt jede vorhandene ambige Klasse A'' in der Gestalt $A'^{a'}A^a Lc$ sich darstellen läßt, wo A', A die eben bestimmten ambigen Klassen sind und L eine Klasse mit ambigem Ideal, c eine Klasse mit Idealen in $k(\zeta)$ ist. Daraus geht dann hervor, daß der Grad der aus allen ambigen Klassen bestehenden Klassenschar genau $t + m + 2 - \frac{l+1}{2}$ beträgt, wie es der Satz 159 für den Fall $n = m+2$ aussagt.

Durch Fortsetzung der eingeleiteten Schlußweise erhalten wir den vollständigen Beweis des Satzes 159.

§ 149. Das Charakterensystem einer Zahl und eines Ideals im regulären Kummerschen Körper.

Es handelt sich nun darum, diejenige Einteilung der Idealklassen eines aus dem regulären Kreiskörper $k(\zeta)$ entspringenden Kummerschen Körpers $K = k(\sqrt[l]{\mu}, \zeta)$ zu erörtern, welche der Einteilung der Klassen eines quadra-

tischen Körpers in Geschlechter entspricht. Wir bezeichnen die verschiedenen in der Relativdiskriminante des Körpers K aufgehenden Primideale des Körpers $k(\zeta)$, deren Anzahl t sei, mit $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$. Zu einer beliebigen ganzen Zahl $\nu(\neq 0)$ in $k(\zeta)$ gehören dann bestimmte Werte der t einzelnen Symbole

$$\left\{\frac{\nu, \mu}{\mathfrak{l}_1}\right\}, \ldots, \left\{\frac{\nu, \mu}{\mathfrak{l}_t}\right\}; \tag{139}$$

diese Symbole bedeuten l-te Einheitswurzeln gemäß ihrer Definition in § 131. Diese t Einheitswurzeln (139) sollen das **Charakterensystem der Zahl** ν im Kummerschen Körper K heißen. Um auch einem jeden Ideal $\mathfrak{J}$ des Kummerschen Körpers K in bestimmter Weise ein Charakterensystem zuzuordnen, bilden wir die Relativnorm $N_k(\mathfrak{J}) = \mathfrak{j}$. Ferner bezeichnen wir mit h die Anzahl der Idealklassen in $k(\zeta)$ und bestimmen eine ganze rationale positive Zahl h^* derart, daß $hh^* \equiv 1$ nach l wird. Dann ist $\mathfrak{j}^{hh^*}$ sicher ein Hauptideal in $k(\zeta)$; wir setzen $\mathfrak{j}^{hh^*} = (\nu)$, wo ν eine ganze Zahl in $k(\zeta)$ sein soll. Nunmehr verstehen wir unter ξ_1 eine Einheit in $k(\zeta)$. Haben dann für jede beliebige Einheit ξ_1 alle t Symbole

$$\left\{\frac{\xi_1, \mu}{\mathfrak{l}_1}\right\}, \ldots, \left\{\frac{\xi_1, \mu}{\mathfrak{l}_t}\right\}$$

durchweg den Wert 1, so setzen wir $r = t$ und bezeichnen die r Einheitswurzeln

$$\left\{\frac{\nu, \mu}{\mathfrak{l}_1}\right\}, \ldots, \left\{\frac{\nu, \mu}{\mathfrak{l}_r}\right\}$$

als das **Charakterensystem des Ideals** $\mathfrak{J}$; dasselbe ist dann durch das Ideal $\mathfrak{J}$ völlig eindeutig bestimmt.

Es sei andererseits eine spezielle Einheit ε_1 in $k(\zeta)$ vorhanden, für welche wenigstens eines der t Symbole

$$\left\{\frac{\varepsilon_1, \mu}{\mathfrak{l}_1}\right\}, \ldots, \left\{\frac{\varepsilon_1, \mu}{\mathfrak{l}_t}\right\}$$

von 1 verschieden ausfällt; dann können wir, ohne damit eine Beschränkung einzuführen, annehmen, es sei etwa $\left\{\frac{\varepsilon_1, \mu}{\mathfrak{l}_t}\right\} = \zeta$. Wir betrachten nun alle diejenigen Einheiten ξ_2 in $k(\zeta)$, für welche $\left\{\frac{\xi_2, \mu}{\mathfrak{l}_t}\right\} = 1$ wird. Es sei unter diesen weiter eine solche Einheit $\xi_2 = \varepsilon_2$ vorhanden, für welche wenigstens eines der $t-1$ Symbole

$$\left\{\frac{\varepsilon_2, \mu}{\mathfrak{l}_1}\right\}, \ldots, \left\{\frac{\varepsilon_2, \mu}{\mathfrak{l}_{t-1}}\right\}$$

von 1 verschieden ausfällt; dann können wir annehmen, es sei etwa $\left\{\frac{\varepsilon_2, \mu}{\mathfrak{l}_{t-1}}\right\} = \zeta$. Wir betrachten nunmehr alle diejenigen Einheiten ξ_3, für welche sowohl $\left\{\frac{\xi_3, \mu}{\mathfrak{l}_t}\right\} = 1$ als auch $\left\{\frac{\xi_3, \mu}{\mathfrak{l}_{t-1}}\right\} = 1$ wird, und sehen nach, ob unter diesen

eine Einheit $\xi_3 = \varepsilon_3$ vorhanden, für welche wenigstens eines der $t-2$ Symbole

$$\left\{\frac{\varepsilon_3, \mu}{\mathfrak{l}_1}\right\}, \ldots, \left\{\frac{\varepsilon_3, \mu}{\mathfrak{l}_{t-2}}\right\}$$

von 1 verschieden ausfällt. Fahren wir in der geeigneten Weise fort, so erhalten wir schließlich eine gewisse Anzahl r^* und dazu ein System von r^* Einheiten $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r^*}$ des Körpers $k(\zeta)$ von der Art, daß bei geeigneter Anordnung der Primideale $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ die Gleichungen

$$\left.\begin{aligned}
&\left\{\frac{\varepsilon_1, \mu}{\mathfrak{l}_t}\right\} = \zeta, \\
&\left\{\frac{\varepsilon_2, \mu}{\mathfrak{l}_t}\right\} = 1, \quad \left\{\frac{\varepsilon_2, \mu}{\mathfrak{l}_{t-1}}\right\} = \zeta \\
&\left\{\frac{\varepsilon_3, \mu}{\mathfrak{l}_t}\right\} = 1, \quad \left\{\frac{\varepsilon_3, \mu}{\mathfrak{l}_{t-1}}\right\} = 1, \quad \left\{\frac{\varepsilon_3, \mu}{\mathfrak{l}_{t-2}}\right\} = \zeta, \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
&\left\{\frac{\varepsilon_{r^*}, \mu}{\mathfrak{l}_t}\right\} = 1, \quad \left\{\frac{\varepsilon_{r^*}, \mu}{\mathfrak{l}_{t-1}}\right\} = 1, \quad \left\{\frac{\varepsilon_{r^*}, \mu}{\mathfrak{l}_{t-2}}\right\} = 1, \ldots, \left\{\frac{\varepsilon_{r^*}, \mu}{\mathfrak{l}_{t-r^*+1}}\right\} = \zeta
\end{aligned}\right| \tag{140}$$

gelten, und daß außerdem für eine jede solche Einheit ξ, die den r^* Gleichungen

$$\left\{\frac{\xi, \mu}{\mathfrak{l}_t}\right\} = 1, \quad \left\{\frac{\xi, \mu}{\mathfrak{l}_{t-1}}\right\} = 1, \ldots, \left\{\frac{\xi, \mu}{\mathfrak{l}_{t-r^*+1}}\right\} = 1$$

genügt, notwendig auch die $r = t - r^*$ Symbole

$$\left\{\frac{\xi, \mu}{\mathfrak{l}_1}\right\}, \ldots, \left\{\frac{\xi, \mu}{\mathfrak{l}_r}\right\}$$

sämtlich den Wert 1 besitzen.

Wir multiplizieren nunmehr die vorhin aus dem Ideal $\mathfrak{J}$ gebildete Zahl ν des Körpers $k(\zeta)$ derart mit Potenzen der Einheiten $\varepsilon_1, \ldots, \varepsilon_{r^*}$, daß das entstehende Produkt $\bar{\nu}$ den Gleichungen

$$\left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_t}\right\} = 1, \quad \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_{t-1}}\right\} = 1, \ldots, \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_{t-r^*+1}}\right\} = 1$$

genügt; dann bezeichne ich die $r = t - r^*$ Einheiten

$$\chi_1(\mathfrak{J}) = \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_1}\right\}, \ldots, \chi_r(\mathfrak{J}) = \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_r}\right\}$$

als das **Charakterensystem des Ideals** $\mathfrak{J}$. Dasselbe ist durch das Ideal $\mathfrak{J}$ völlig eindeutig bestimmt. In § 151 wird gezeigt werden, daß stets $r^* < t$ und mithin $r \geqq 1$ wird.

§ 150. Das Charakterensystem einer Idealklasse und der Begriff des Geschlechtes.

Mit Rücksicht auf den Satz 151 und die dazu auf S. 274 angefügten Bemerkungen erkennen wir sofort die Tatsache:

Satz 160. Die Ideale ein und derselben Klasse eines regulären Kummerschen Körpers besitzen sämtlich dasselbe Charakterensystem.

Auf diese Weise ist überhaupt einer jeden Idealklasse ein bestimmtes Charakterensystem zuzuordnen. Wir rechnen, ähnlich wie es in § 66 für den quadratischen Körper geschehen ist, 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 Einheiten 1 besteht. Da das Charakterensystem der Hauptklasse offenbar von der letzteren Eigenschaft ist, so gehört insbesondere die Hauptklasse stets zum Hauptgeschlecht. Aus der ersten Formel in (80) und in (83) auf S. 265 und S. 266 entnehmen wir leicht die folgenden Tatsachen: Wenn G und G' zwei beliebige Geschlechter sind und jede Klasse in G mit jeder Klasse in G' multipliziert wird, so bilden sämtliche solche Produkte wiederum ein Geschlecht; dieses werde das **Produkt der Geschlechter** G und G' genannt. Das Charakterensystem desselben erhalten wir durch Multiplikation der entsprechenden Charaktere der beiden Geschlechter G und G'.

Aus der eben aufgestellten Definition der Geschlechter leuchtet ferner ein, daß die zu einer Klasse C relativ konjugierten Klassen $SC, \ldots, S^{l-1}C$ zu demselben Geschlechte wie C selbst gehören, und hieraus folgt, daß die $(1-S)$-te symbolische Potenz C^{1-S} einer jeden Klasse C stets zum Hauptgeschlecht gehört. Endlich ist offenbar, daß jedes Geschlecht des Kummerschen Körpers gleichviel Klassen enthält.

§ 151. Obere Grenze für den Grad der aus sämtlichen ambigen Klassen bestehenden Klassenschar.

Es entsteht, entsprechend wie in der Theorie des quadratischen Körpers, die wichtige Frage, ob ein System von r beliebig vorgelegten l-ten Einheitswurzeln stets das Charakterensystem für ein Geschlecht des Kummerschen Körpers sein kann. Diese Frage findet erst in Kapitel 34 ihre vollständige Erledigung. In diesem und in den nächsten Paragraphen werden lediglich einige für das Spätere notwendige Hilfssätze bewiesen.

Hilfssatz 33. Wenn t und n die Bedeutung wie in Satz 159 haben und r die Anzahl der Charaktere ist, welche das Geschlecht einer Klasse des Kummerschen Körpers bestimmen, so ist stets

$$t + n - \frac{l+1}{2} \leqq r - 1.$$

Beweis. Es seien $\varepsilon_1, \ldots, \varepsilon_{r^*}$ diejenigen besonderen r^* Einheiten des Körpers $k(\zeta)$, welche in § 149 eingeführt worden sind. Es ist dann $r = t - r^*$. Ferner mögen $\vartheta_1, \ldots, \vartheta_n$ eine Basis für diejenige Einheitenschar in $k(\zeta)$ bilden, welche aus allen Einheiten in $k(\zeta)$ besteht, die Relativnormen von Zahlen in K sind. Wir nehmen nun an, es gäbe zwischen den $r^* + n$ Einheiten

$\varepsilon_1, \ldots, \varepsilon_{r^*}, \vartheta_1, \ldots, \vartheta_n$ eine Relation von der Gestalt

$$\varepsilon_1^{a_1} \cdots \varepsilon_{r^*}^{a_{r^*}} \vartheta_1^{b_1} \cdots \vartheta_n^{b_n} = \varepsilon^l, \tag{141}$$

so daß die Exponenten $a_1, \ldots, a_{r^*}, b_1, \ldots, b_n$ ganze rationale, nicht sämtlich durch l teilbare Zahlen sind und ε eine geeignete Einheit in $k(\zeta)$ vorstellt; dann müßte für $u = 1, 2, \ldots, t$ stets

$$\left\{\frac{\varepsilon_1^{a_1} \cdots \varepsilon_{r^*}^{a_{r^*}} \vartheta_1^{b_1} \cdots \vartheta_n^{b_n}, \mu}{\mathfrak{l}_u}\right\} = 1$$

ausfallen, und wenn wir berücksichtigen, daß die Einheiten $\vartheta_1, \ldots, \vartheta_n$ sämtlich Relativnormen von Zahlen in K sind und daher stets $\left\{\frac{\vartheta_v, \mu}{\mathfrak{l}_u}\right\} = 1$ für $u = 1, 2, \ldots, t$, und $v = 1, 2, \ldots, n$ sein muß, so ergibt sich auch

$$\left\{\frac{\varepsilon_1^{a_1} \cdots \varepsilon_{r^*}^{a_{r^*}}, \mu}{\mathfrak{l}_u}\right\} = 1$$

für $u = 1, 2, \ldots, t$. Wegen der Formeln (140) für die Einheiten $\varepsilon_1, \ldots, \varepsilon_{r^*}$ ist dies nur möglich, wenn die Exponenten $a_1, \ldots, a_{r^*}$ sämtlich durch l teilbar sind, und die Relation (141) würde somit die Gestalt

$$\vartheta_1^{b_1} \cdots \vartheta_n^{b_n} = \varepsilon^{*l}$$

annehmen, wo ε^* wiederum eine Einheit in $k(\zeta)$ bedeutet. Das Bestehen einer solchen Relation ist aber, da $\vartheta_1, \ldots, \vartheta_n$ die Basis einer Einheitenschar in $k(\zeta)$ bilden, nur möglich, falls die Exponenten $b_1, \ldots, b_n$ sämtlich durch l teilbar sind. Daraus folgt, daß eine Relation von der Gestalt (141), wie wir sie annahmen, nicht statthaben kann, d. h. die Einheiten $\varepsilon_1, \ldots, \varepsilon_{r^*}, \vartheta_1, \ldots, \vartheta_n$ bilden eine Basis einer Einheitenschar; es ist der Grad dieser Einheitenschar $r^* + n$, und da der Grad einer Einheitenschar höchstens $\frac{l-1}{2}$ sein kann, so haben wir $r^* + n \leqq \frac{l-1}{2}$; hiermit deckt sich die Aussage des Hilfssatzes 33. Da $t + n - \frac{l+1}{2} \geqq 0$ ist, so folgt insbesondere, daß stets $r^* < t$, also $r \geqq 1$ ausfällt.

§ 152. Die Komplexe des regulären Kummerschen Körpers.

Es sei h die Anzahl der Idealklassen des regulären Kreiskörpers $k(\zeta)$: dann gibt es in dem Kummerschen Körper $K = k(\sqrt[l]{\mu}, \zeta)$ genau h voneinander verschiedene Idealklassen, welche unter ihren Idealen Ideale des Kreiskörpers $k(\zeta)$ enthalten. In der Tat, jede Klasse in $k(\zeta)$ liefert offenbar eine Klasse in K von der fraglichen Art; würden nun zwei verschiedene Klassen c_1, c_2 in $k(\zeta)$ Ideale enthalten, die in K einander äquivalent sind, so würde ein Ideal $\mathfrak{j}$ in $k(\zeta)$ aus der Klasse $\frac{c_1}{c_2}$ stets zu einem Hauptideal im Körper K werden müssen.

Nach Satz 153 wäre dann aber $\mathfrak{j}$ auch ein Hauptideal in $k(\zeta)$, und dies ist gegen die Annahme $c_1 \neq c_2$.

Ist nun C eine beliebige Klasse in K und sind $c_1, \ldots, c_h$ diejenigen h Klassen in K, welche Ideale in $k(\zeta)$ enthalten, so nenne ich das System der h Klassen $c_1 C, \ldots, c_h C$ einen **Komplex**. Der Komplex, welcher aus den h Klassen $c_1, \ldots, c_h$ besteht, heiße der **Hauptkomplex** und werde mit 1 bezeichnet. Die h Klassen eines beliebigen Komplexes P gehören offenbar sämtlich zu dem nämlichen Geschlecht; ich bezeichne dieses Geschlecht als das **Geschlecht des Komplexes P**.

Wenn eine Klasse eines Komplexes P ambig ist, so sind sämtliche Klassen dieses Komplexes ambig; den Komplex P nenne ich dann einen **ambigen Komplex**.

Wenn P und P' zwei ambige Komplexe sind und jede Klasse in P mit jeder Klasse in P' multipliziert wird, so bilden sämtliche solche Produkte wiederum einen Komplex; dieser werde das **Produkt der Komplexe** P, P' genannt und mit PP' bezeichnet. Wenn C eine Klasse in P ist, so werde derjenige Komplex, zu welchem die relativ konjugierte Klasse SC gehört, mit SP bezeichnet; ferner nenne ich denjenigen Komplex Q, der nach der Multiplikation mit SP den Komplex P ergibt, die **symbolische $(1-S)$-te Potenz des Komplexes P** und bezeichne ihn mit $Q = P^{1-S}$.

Wenn insbesondere die symbolische $(1-S)$-te Potenz eines Komplexes P den Hauptkomplex 1 liefert, so ist P ein ambiger Komplex. In der Tat, wenn C eine Klasse in P ist, so folgt aus $P^{1-S} = 1$ offenbar $C^{1-S} = c$, wo c eine der h Idealklassen $c_1, \ldots, c_h$ ist. Bilden wir auf beiden Seiten der letzten Gleichung die Relativnorm, so erhalten wir $1 = c^l$, und da andererseits auch $c^h = 1$ ist, so folgt $c = 1$, d. h. $C^{1-S} = 1$; mithin ist C eine ambige Klasse und daher P ein ambiger Komplex.

§ 153. Obere Grenze für die Anzahl der Geschlechter in einem regulären Kummerschen Körper.

Hilfssatz 34. Wenn t und n die Bedeutung wie in Satz 159 haben und g die Anzahl der Geschlechter des regulären Kummerschen Körpers K bezeichnet, so fällt stets $g \leqq l^{t+n-\frac{l+1}{2}}$ aus.

Beweis. Wenn g die Anzahl der Geschlechter in dem Kummerschen Körper K ist, so zerfallen, wie man unmittelbar aus der Definition des Geschlechtes eines Komplexes ersieht, auch die Komplexe genau in g Geschlechter. Bezeichnen wir daher mit f die Anzahl der Komplexe vom Hauptgeschlecht, so ist die Anzahl aller überhaupt vorhandenen Komplexe, welche M heiße, genau $M = fg$.

Wir wollen nun die Anzahl a der ambigen Komplexe ermitteln. Zu dem Zwecke bedenken wir, daß nach Satz 159 der Grad der aus allen ambigen Klassen bestehenden Klassenschar gleich $t + n - \frac{l+1}{2}$ ist. Es sei $A_1, \ldots, A_{t+n-\frac{l+1}{2}}$ eine Basis dieser Klassenschar, dann stellt der Ausdruck

$$A_1^{u_1} \cdots A_{t+n-\frac{l+1}{2}}^{u_{t+n-\frac{l+1}{2}}},$$

wenn die Exponenten $u_1, \ldots, u_{t+n-\frac{l+1}{2}}$ unabhängig voneinander die Werte $0, 1, \ldots, l-1$ durchlaufen, lauter ambige Klassen dar, welche in verschiedenen Komplexen liegen, und es werden somit durch diese Klassen genau $l^{t+n-\frac{l+1}{2}}$ Komplexe bestimmt. Jede vorhandene ambige Klasse A ist in der Gestalt

$$A = A_1^{a_1} \cdots A_{t+n-\frac{l+1}{2}}^{a_{t+n-\frac{l+1}{2}}} c$$

darstellbar, wo $a_1, \ldots, a_{t+n-\frac{l+1}{2}}$ ganze rationale Exponenten sind und c eine Klasse in $k(\zeta)$ bedeutet. Berücksichtigen wir nun, daß die l-ten Potenzen der ambigen Klassen $A_1, \ldots, A_{t+n-\frac{l+1}{2}}$ Klassen sind, welche Ideale des Körpers $k(\zeta)$ enthalten, so folgt, daß A notwendig einem der oben bestimmten $l^{t+n-\frac{l+1}{2}}$ Komplexe angehören muß, und mithin ist die gesuchte Anzahl $a = l^{t+n-\frac{l+1}{2}}$.

Aus den Definitionen in § 150 und § 152 geht unmittelbar hervor, daß die symbolische $(1-S)$-te Potenz eines beliebigen Komplexes stets ein Komplex des Hauptgeschlechtes ist. Wir fassen nun diejenigen Komplexe des Hauptgeschlechtes ins Auge, welche $(1-S)$-te symbolische Potenzen von Komplexen sind; ihre Anzahl sei f'; wir bezeichnen sie mit $P_1, \ldots, P_{f'}$, und wir mögen $P_1 = G_1^{1-S}, \ldots, P_{f'} = G_{f'}^{1-S}$ haben, wo $G_1, \ldots, G_{f'}$ gewisse Komplexe bedeuten. Ist jetzt P ein beliebiger Komplex, so ist P^{1-S} notwendig ein bestimmter der f' Komplexe $P_1, \ldots, P_{f'}$; es sei etwa $P^{1-S} = P_v$. Dann folgt $P^{1-S} = G_v^{1-S}$, d. h. $(PG_v^{-1})^{1-S} = 1$, und somit ist PG_v^{-1} ein bestimmter ambiger Komplex A; es wird $P = AG_v$, und folglich stellt der Ausdruck AG_v alle Komplexe dar, sobald A alle ambigen Komplexe und G_v die f' Komplexe $G_1, \ldots, G_{f'}$ durchläuft. Auch ist klar, daß diese Darstellung für jeden Komplex nur auf eine Weise möglich ist; es ist daher die Anzahl aller überhaupt vorhandenen Komplexe $M = af'$. Die Zusammenstellung dieser

Gleichung mit der vorhin gefundenen $M = gf$ liefert $af' = gf$, und wegen $f' \leqq f$ folgt hieraus $g \leqq a$, d. h. $g \leqq l^{t+n-\frac{l+1}{2}}$, und hiermit ist der Hilfssatz 34 bewiesen.

Aus den beiden Hilfssätzen 33 und 34 folgt sofort die weitere Tatsache:

Hilfssatz 35. Wenn in einem regulären Kummerschen Körper r die Anzahl der Charaktere ist, welche das Geschlecht einer Klasse bestimmen, so ist die Anzahl der Geschlechter jenes Körpers $g \leqq l^{r-1}$.

33. Das Reziprozitätsgesetz für l-te Potenzreste im regulären Kreiskörper.

§ 154. Das Reziprozitätsgesetz für l-te Potenzreste und die Ergänzungssätze.

Die bisher dargelegte Theorie des Kummerschen Körpers liefert uns die Hilfsmittel zum Beweise gewisser fundamentaler Gesetze über l-te Potenzreste im regulären Kreiskörper, welche den Reziprozitätsgesetzen für quadratische Reste im Gebiete der rationalen Zahlen entsprechen, und welche das in § 115 entwickelte Eisensteinsche Reziprozitätsgesetz (Satz 140) zwischen einer beliebigen Zahl in $k(\zeta)$ und einer rationalen Zahl als besonderen Fall enthalten. Um diese Gesetze für l-te Potenzreste in ihrer einfachsten Gestalt aussprechen zu können, verallgemeinern wir das in § 113 und § 127 definierte Symbol $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ in folgender Weise:

Es sei h die Anzahl der Idealklassen in $k(\zeta)$; dann bestimmen wir eine ganze rationale positive Zahl h^* so, daß $hh^* \equiv 1$ nach l wird. Bedeutet dann $\mathfrak{p}$ ein beliebiges, von $\mathfrak{l}$ verschiedenes Primideal in $k(\zeta)$, so ist stets $\mathfrak{p}^{hh^*}$ ein Hauptideal in $k(\zeta)$; wir setzen $\mathfrak{p}^{hh^*} = (\pi)$, so daß π eine ganze Zahl in $k(\zeta)$ ist, und nehmen hierin, was dem Satze 157 zufolge geschehen kann, die Zahl π primär an. Eine solche ganze Zahl π heiße eine **Primärzahl von** $\mathfrak{p}$. Es hat dann, da jede primäre Einheit in $k(\zeta)$ zufolge einer Bemerkung auf S. 288 die l-te Potenz einer Einheit in $k(\zeta)$ ist, π in bezug auf jedes von $\mathfrak{p}$ verschiedene Primideal einen völlig bestimmten Potenzcharakter. Bedeutet nun $\mathfrak{q}$ ein beliebiges, von $\mathfrak{l}$ und von $\mathfrak{p}$ verschiedenes Primideal in $k(\zeta)$, so wird das **Symbol** $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}$ durch die Formel

$$\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = \left\{\frac{\pi}{\mathfrak{q}}\right\}$$

definiert. Das Symbol $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}$ ist somit eine durch die zwei Primideale $\mathfrak{p}$ und $\mathfrak{q}$ eindeutig bestimmte l-te Einheitswurzel. Mit Benutzung dieses Symbols sprechen wir folgende Tatsache aus:

Satz 161. *Sind $\mathfrak{p}$ und $\mathfrak{q}$ voneinander und von dem Primideal $\mathfrak{l}$ verschiedene Primideale des regulären Kreiskörpers $k(\zeta)$, so gilt die Regel*

$$\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}.$$

das sogenannte Reziprozitätsgesetz für l-te Potenzreste. Außerdem gelten, wenn ξ eine beliebige Einheit in $k(\zeta)$ und π eine Primärzahl von dem Primideal $\mathfrak{p}$ bedeutet, die Regeln

$$\left\{\frac{\xi}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \xi}{\mathfrak{l}}\right\}, \quad \left\{\frac{\lambda}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \lambda}{\mathfrak{l}}\right\},$$

die beiden sogenannten Ergänzungssätze zum Reziprozitätsgesetz für l-te Potenzreste [Kummer (*10, 12, 18, 19, 20, 21*)].

Wir führen den Nachweis dieses Fundamentalsatzes in den folgenden Paragraphen § 155 bis § 161 des gegenwärtigen Kapitels durch schrittweises Vorgehen, indem wir für besondere reguläre Kummersche Körper die im vorigen Kapitel gefundenen Sätze und Hilfssätze zur Anwendung bringen.

§ 155. Die Primideale erster und zweiter Art im regulären Kreiskörper.

Es ist für die folgenden Entwicklungen von Nutzen, zwei Arten von Primidealen in $k(\zeta)$ zu unterscheiden: ein solches von $\mathfrak{l}$ verschiedenes Primideal $\mathfrak{p}$ in $k(\zeta)$, nach welchem nicht jede vorhandene Einheit in $k(\zeta)$ l-ter Potenzrest ist, möge ein **Primideal erster Art** heißen; dagegen möge jedes von $\mathfrak{l}$ verschiedene Primideal $\mathfrak{q}$ in $k(\zeta)$, nach welchem alle Einheiten in $k(\zeta)$ l-te Potenzreste sind, ein **Primideal zweiter Art** heißen [Kummer (*20*)]. Wir beweisen zunächst folgende Hilfssätze:

Hilfssatz 36. Wenn ξ und ε beliebige Einheiten des regulären Kreiskörpers $k(\zeta)$ sind und $\lambda = 1 - \zeta$, $\mathfrak{l} = (\lambda)$ gesetzt wird, so gelten stets die Gleichungen

$$\left\{\frac{\xi, \varepsilon}{\mathfrak{l}}\right\} = 1, \quad \left\{\frac{\lambda, \varepsilon}{\mathfrak{l}}\right\} = 1.$$

Beweis. Wenn ε die l-te Potenz einer Einheit in $k(\zeta)$ ist, so leuchtet die Richtigkeit der aufgestellten Gleichungen von selbst ein. Andernfalls definiert $\sqrt[l]{\varepsilon}$ einen Kummerschen Körper $k(\sqrt[l]{\varepsilon}, \zeta)$, und zwar einen solchen, für welchen die Betrachtungen am Schluß des § 147 zutreffen. Es sind daher alle Einheiten in $k(\zeta)$ und zudem auch die Zahl λ Relativnormen von Zahlen in $k(\sqrt[l]{\varepsilon}, \zeta)$, und hieraus ergibt sich wegen Satz 151 die Richtigkeit der Gleichungen des Hilfssatzes 36.

Will man hier den Satz 151 für $\mathfrak{w} = \mathfrak{l}$ nur in dem auf S. 273 bis S. 274 ausführlich behandelten Fall anwenden, wo die betreffende Zahl $\mu \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ ist, so mache man die letzten Schlüsse zunächst, indem man ζ^{l-1} für die Einheit ε nimmt; dann folgt $\left\{\frac{\xi, \zeta}{\mathfrak{l}}\right\} = 1$ und $\left\{\frac{\lambda, \zeta}{\mathfrak{l}}\right\} = 1$. Weiter bestimme man, wenn ε eine beliebige Einheit in $k(\zeta)$ bedeutet, eine solche l-te Einheitswurzel ζ^*, daß $\zeta^* \varepsilon^{l-1} \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ ausfällt. Nimmt man dann im oben

dargelegten Beweise $\zeta^* \varepsilon^{l-1}$ an Stelle der Einheit ε, so folgt unter Benutzung der zweiten Formel in (83) (S. 266) $\left\{\frac{\xi, \varepsilon}{l}\right\} = 1$ und in gleicher Weise $\left\{\frac{\lambda, \varepsilon}{l}\right\} = 1$.

Hilfssatz 37. Wenn $\mathfrak{p}$ ein Primideal erster Art und π eine Primärzahl von $\mathfrak{p}$ ist, so gibt es in $k(\zeta)$ stets wenigstens eine Einheit ε, für welche

$$\left\{\frac{\varepsilon, \pi}{l}\right\} \neq 1$$

ausfällt; ist dagegen ein Primideal $\mathfrak{q}$ zweiter Art vorgelegt und bedeutet $\varkappa$ eine Primärzahl von $\mathfrak{q}$, so gilt für jede Einheit ξ in $k(\zeta)$ die Gleichung

$$\left\{\frac{\xi, \varkappa}{l}\right\} = 1.$$

Beweis. Um die erste Aussage dieses Hilfssatzes zu beweisen, nehmen wir an, es gelte im Gegenteil für jede Einheit ξ in $k(\zeta)$ die Gleichung

$$\left\{\frac{\xi, \pi}{l}\right\} = 1.$$

Wir setzen $\pi \equiv a + b\lambda^e$ nach $\mathfrak{l}^{e+1}$, wobei a und b ganze rationale Zahlen sein sollen und e den größten Exponent $\leqq l-1$ bedeutet, für den jener Ansatz möglich ist. Da π eine primäre Zahl ist, so muß notwendig $e > 1$ und $\pi \cdot s^{\frac{l-1}{2}} \pi$ einer ganzen rationalen Zahl nach l kongruent sein; hierbei bedeutet $s^{\frac{l-1}{2}}$ die Substitution $(\zeta : \zeta^{-1})$ aus der Gruppe des Kreiskörpers $k(\zeta)$. Da $s^{\frac{l-1}{2}} \lambda \equiv -\lambda$ nach $\mathfrak{l}^2$ ist, so wird

$$\pi \cdot s^{\frac{l-1}{2}} \pi \equiv (a + b\lambda^e)(a + b(-\lambda)^e), \qquad (\mathfrak{l}^{e+1}),$$

und hieraus folgt, daß im Falle $e < l-1$ der Exponent e notwendig ungerade sein muß.

Wir haben nun beim Beweise des Hilfssatzes 29 gefunden, daß die $l^* = \frac{l-3}{2}$ dort mit $\varepsilon_1, \ldots, \varepsilon_{l^*}$ bezeichneten Einheiten des Kreiskörpers $k(\zeta)$ die Bedingungen

$$\left.\begin{aligned} &l^{(u)}(\varepsilon_t) \equiv 0, \quad (l), \quad (u + 2t) \\ &l^{(2t)}(\varepsilon_t) \not\equiv 0, \quad (l) \end{aligned}\right\} \quad \begin{pmatrix} t = 1, 2, \cdots, l^*; \\ u = 1, 2, \cdots, l-2 \end{pmatrix}$$

erfüllen. Setzen wir in der ersten Gleichung dieses Beweises der Reihe nach für ξ die Werte $\varepsilon_1, \ldots, \varepsilon_{l^*}$ ein, so entspringen zufolge der Definition (82) des Symbols $\left\{\frac{\nu, \mu}{l}\right\}$ auf S. 266 und ihrer auf S. 266 gegebenen Ausdehnung die Kongruenzen

$$l^{(l-2)}(\pi^{l-1}) \equiv 0, \; l^{(l-4)}(\pi^{l-1}) \equiv 0, \; l^{(l-6)}(\pi^{l-1}) \equiv 0, \cdots, \; l^{(3)}(\pi^{l-1}) \equiv 0, \quad (l);$$

und diese lassen erkennen, daß in der Kongruenz $\pi \equiv a + b\lambda^e$ nach $\mathfrak{l}^{e+1}$ der Exponent e keinen der Werte $l-2, l-4, l-6, \ldots, 3$ haben darf. Stellen

wir damit die oben gefundenen Bedingungen für e zusammen, so folgt, daß $e = l-1$ sein muß. Da nun $\lambda^{l-1} \equiv -l$ nach $\mathfrak{l}^l$ wird, so ergibt sich $\pi \equiv a - bl$ nach $\mathfrak{l}^l$, und folglich genügt die Norm von π der Kongruenz

$$n(\pi) \equiv (a - bl)^{l-1} \equiv \pi^{l-1}, \quad (\mathfrak{l}^l).$$

Andererseits entnehmen wir aus der Definition des Symbols auf S. 266 unter Berücksichtigung des Hilfssatzes 24

$$\left\{\frac{\zeta, \pi}{l}\right\} = \zeta^{\frac{1-n(\pi)}{l}},$$

und da das Symbol linker Hand den Wert 1 haben soll, so folgt $n(\pi) \equiv 1$ nach l^2, d. h. $\pi^{l-1} \equiv 1$ nach $\mathfrak{l}^l$ oder $\pi \equiv \pi^l$ nach $\mathfrak{l}^l$. Nach Satz 148 besitzt infolge der letzteren Kongruenz der durch $\sqrt[l]{\pi}$ bestimmte Kummersche Körper $k(\sqrt[l]{\pi}, \zeta)$ eine zu l prime Relativdiskriminante, und es ist mithin $\mathfrak{p}$ das einzige in der Relativdiskriminante von $k(\sqrt[l]{\pi}, \zeta)$ aufgehende Primideal. Setzen wir $\mathfrak{p} = \mathfrak{P}^l$, so ist $\mathfrak{P}$ das einzige ambige Primideal dieses Körpers. Aus $\sqrt[l]{\pi} = \mathfrak{P}^{hh^*} = \mathfrak{P}\mathfrak{p}^{\frac{hh^*-1}{l}}$ folgt, daß $\mathfrak{P}$ einem Ideal des Körpers $k(\zeta)$ äquivalent ist. Die aus allen ambigen Idealen entspringende Klassenschar hat also für den Kummerschen Körper $k(\sqrt[l]{\pi}, \zeta)$ den Grad 0. Da die Anzahl t der ambigen Ideale für diesen Körper 1 ist, so folgt nach Satz 158, wenn m die dort festgesetzte Bedeutung für diesen Körper hat, $1 + m - \frac{l+1}{2} = 0$, d. h. $m = \frac{l-1}{2}$. Es ist folglich jede Einheit ξ in $k(\zeta)$ die Relativnorm einer Einheit in $k(\sqrt[l]{\pi}, \zeta)$, und mithin wird nach Satz 151 stets $\left\{\frac{\xi, \pi}{\mathfrak{p}}\right\} = 1$ und also, da $\left\{\frac{\xi, \pi}{\mathfrak{p}}\right\} = \left\{\frac{\xi^{hh^*}}{\mathfrak{p}}\right\} = \left\{\frac{\xi}{\mathfrak{p}}\right\}$ ist, auch $\left\{\frac{\xi}{\mathfrak{p}}\right\} = 1$, entgegen unserer Annahme, wonach das Primideal $\mathfrak{p}$ von der ersten Art sein sollte.

Um die zweite Aussage des Hilfssatzes 37 zu beweisen, betrachten wir ähnlich wie im Beweise des Hilfssatzes 36 den Kummerschen Körper $k(\sqrt[l]{\xi}, \zeta)$, wo ξ eine beliebige Einheit in $k(\zeta)$, nur nicht die l-te Potenz einer Einheit in $k(\zeta)$, sein soll. Wie am Schlusse des § 147 bewiesen wurde, ist jede Einheit in $k(\zeta)$ die Relativnorm einer Einheit in $k(\sqrt[l]{\xi}, \zeta)$ und daher haben die beiden in Satz 158 und in Satz 159 bezeichneten Einheitenscharen für diesen Körper den gemeinsamen Grad

$$m = n = \frac{l-1}{2}.$$

Da ferner für ihn $t = 1$ ist, so folgt aus Hilfssatz 34 $g \leqq 1$; mithin ist $g = 1$, d. h. alle Idealklassen des Körpers $k(\sqrt[l]{\xi}, \zeta)$ gehören zum Hauptgeschlecht. Da $\mathfrak{q}$ ein Primideal zweiter Art sein soll, so ist $\left\{\frac{\xi}{\mathfrak{q}}\right\} = 1$, und mithin zerfällt nach Satz 149 $\mathfrak{q}$ in l voneinander verschiedene Primideale des Körpers $k(\sqrt[l]{\xi}, \zeta)$;

es sei $\mathfrak{L}$ einer dieser Primfaktoren von $\mathfrak{q}$. Das Charakterensystem einer Zahl $\alpha(+0)$ des Körpers $k(\zeta)$ in $k(\sqrt[l]{\xi}, \zeta)$ besteht aus dem einen Charakter $\left\{\frac{\alpha, \xi}{\mathfrak{l}}\right\}$; derselbe fällt nach Hilfssatz 36 stets gleich 1 aus, wenn man für α eine Einheit in $k(\zeta)$ nimmt. Der Charakter des Primideals $\mathfrak{L}$ in $k(\sqrt[l]{\xi}, \zeta)$ hat daher den Wert $\left\{\frac{\alpha, \xi}{\mathfrak{l}}\right\}$, und dieser muß wegen der vorhin bewiesenen Tatsache gleich 1 sein. Damit ist der Hilfssatz 37 vollständig bewiesen.

Will man wiederum Satz 151 für $\mathfrak{w} = \mathfrak{l}$ nur in dem Falle eines Körpers $k(\sqrt[l]{\mu}, \zeta)$, für den $\mu \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ ist, als bewiesen annehmen, so gilt auch die Einteilung der Geschlechter und insbesondere der Hilfssatz 34 nur für diesen Fall. Wir müssen dann zum Beweise der zweiten Aussage des Hilfssatzes 37 erst $\xi = \zeta^{*l-1}$ und dann $\xi = \zeta^* \varepsilon^{l-1}$ wählen, wobei ε eine beliebige Einheit in $k(\zeta)$ und ζ^* dazu eine solche l-te Einheitswurzel bedeute, daß $\zeta^* \varepsilon^{l-1} \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ wird. Durch Verbindung der beiden sich dabei ergebenden Resultate erkennen wir dann die vollständige Richtigkeit der zweiten Aussage des Hilfssatzes 37.

§ 156. Hilfssätze über Primideale erster Art im regulären Kreiskörper.

Wir beweisen der Reihe nach folgende Hilfssätze über Primideale erster Art im Körper $k(\zeta)$:

Hilfssatz 38. Es sei $\mathfrak{p}$ ein Primideal erster Art im regulären Kreiskörper $k(\zeta)$ und π eine Primärzahl von $\mathfrak{p}$. Wenn es dann eine Einheit ε in $k(\zeta)$ gibt, so daß

$$\left\{\frac{\pi, \varepsilon}{\mathfrak{l}}\right\} \neq 1, \quad \left\{\frac{\varepsilon}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \varepsilon}{\mathfrak{l}}\right\}$$

statthat, so gilt für jede beliebige Einheit ξ in $k(\zeta)$ die Gleichung:

$$\left\{\frac{\xi}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \xi}{\mathfrak{l}}\right\}.$$

Beweis. Der durch $\sqrt[l]{\pi}$ bestimmte Kummersche Körper $k(\sqrt[l]{\pi}, \zeta)$ besitzt, weil $\mathfrak{p}$ ein Primideal erster Art ist, nach dem Beweise des Hilfssatzes 37 zwei ambige Primideale $\mathfrak{L}$ und $\mathfrak{P}$, nämlich diejenigen, deren l-te Potenzen $\mathfrak{l}$ bez. $\mathfrak{p}$ sind. Da das ambige Primideal $\mathfrak{P}$ offenbar Hauptideal in $k(\sqrt[l]{\pi}, \zeta)$ ist, so beträgt für diesen Körper der Grad der aus den ambigen Idealen entspringenden Klassenschar 0 oder 1, je nachdem $\mathfrak{L}$ Hauptideal ist oder nicht. Wegen des Satzes 158 besitzt daher, wenn m die dort erklärte Bedeutung für den Körper $k(\sqrt[l]{\pi}, \zeta)$ hat, die Zahl $2 + m - \frac{l+1}{2}$ den Wert 0 der 1, d. h. es ist $m = \frac{l-3}{2}$ oder $m = \frac{l-1}{2}$. Da die Einheit ε infolge der Voraussetzung

$\left\{\frac{\varepsilon, \pi}{\mathfrak{l}}\right\} \neq 1$ mit Rücksicht auf Satz 151 sicher nicht die Relativnorm einer Einheit des Körpers $k(\sqrt[l]{\pi}, \zeta)$ ist, so haben wir notwendigerweise $m = \frac{l-3}{2}$, und es ist sodann jede Einheit ξ in $k(\zeta)$ in der Gestalt $\xi = \varepsilon^a \vartheta$ darstellbar, wo a ein ganzer rationaler Exponent und ϑ eine solche Einheit bedeutet, die sich als Relativnorm einer Einheit in $k(\sqrt[l]{\pi}, \zeta)$ erweist. Aus dem letzteren Grunde ist wegen Satz 151

$$\left\{\frac{\vartheta, \pi}{\mathfrak{l}}\right\} = 1, \quad \left\{\frac{\vartheta, \pi}{\mathfrak{p}}\right\} = \left\{\frac{\vartheta}{\mathfrak{p}}\right\} = 1$$

und also auch $\left\{\frac{\pi, \vartheta}{\mathfrak{l}}\right\} = \left\{\frac{\vartheta}{\mathfrak{p}}\right\}$; hieraus folgt unter Benutzung der zweiten Formel in (83) (S. 266) auch $\left\{\frac{\pi, \xi}{\mathfrak{l}}\right\} = \left\{\frac{\xi}{\mathfrak{p}}\right\}$, und damit ist der Beweis für den Hilfssatz 38 erbracht.

Soll Satz 151 für $\mathfrak{w} = \mathfrak{l}$ nur in dem Falle eines Körpers $k(\sqrt[l]{\mu}, \zeta)$, für den $\mu \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ ist, angewandt werden, so bestimme man eine l-te Einheitswurzel ζ^* derart, daß $\zeta^* \pi^{l-1} \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ wird, und dann betrachte man, indem man im übrigen wie in dem oben dargelegten Beweise verfährt, an Stelle des Körpers $k(\sqrt[l]{\pi}, \zeta)$ den Körper $k(\sqrt[l]{\zeta^* \pi^{l-1}}, \zeta)$. Wenn man schließlich noch den Hilfssatz 36 zuzieht, folgt dann der Hilfssatz 38 vollständig.

Hilfssatz 39. Wenn $\mathfrak{p}$, $\mathfrak{p}^*$ zwei Primideale erster Art in $k(\zeta)$ und π, π^* Primärzahlen bez. von $\mathfrak{p}$, $\mathfrak{p}^*$ sind, wenn ferner für jede beliebige Einheit ξ in $k(\zeta)$

$$\left\{\frac{\xi}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \xi}{\mathfrak{l}}\right\}, \quad \left\{\frac{\xi}{\mathfrak{p}^*}\right\} = \left\{\frac{\pi^*, \xi}{\mathfrak{l}}\right\}$$

wird, so ist

$$\left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\} = \left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\}.$$

Beweis. Da $\mathfrak{p}^*$ ein Primideal erster Art ist, so können wir eine Einheit ε in $k(\zeta)$ derart bestimmen, daß $\left\{\frac{\varepsilon \pi}{\mathfrak{p}^*}\right\} = 1$ wird. Wir betrachten nun den Kummerschen Körper $k(\sqrt[l]{\varepsilon \pi}, \zeta)$. Da die Relativdiskriminante dieses Körpers nur die beiden Primfaktoren $\mathfrak{l}$ und $\mathfrak{p}$ enthält, so besteht das Charakterensystem einer Zahl $\alpha(+0)$ in $k(\zeta)$ für diesen Körper aus den zwei Charakteren $\left\{\frac{\alpha, \varepsilon\pi}{\mathfrak{l}}\right\}$ und $\left\{\frac{\alpha, \varepsilon\pi}{\mathfrak{p}}\right\} = \left\{\frac{\alpha}{\mathfrak{p}}\right\}$. Wegen $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\} = 1$ ist $\mathfrak{p}^*$ in $k(\sqrt[l]{\varepsilon\pi}, \zeta)$ weiter zerlegbar; es sei $\mathfrak{P}^*$ ein Primfaktor von $\mathfrak{p}^*$ in diesem Körper. Um das Charakterensystem von $\mathfrak{P}^*$ zu bilden, bedenken wir, daß $\mathfrak{p}$ ein Primideal erster Art ist; es läßt sich dann eine Einheit ε^* in $k(\zeta)$ bestimmen, für welche $\left\{\frac{\varepsilon^* \pi^*}{\mathfrak{p}}\right\} = 1$ wird und es besteht das Charakterensystem von $\mathfrak{P}^*$ aus dem einen Charakter $\left\{\frac{\varepsilon^* \pi^*, \varepsilon\pi}{\mathfrak{l}}\right\}$. Wir entnehmen mithin aus dem Hilfssatz 35 $g \leqq 1$ für den Kör-

per $k(\sqrt[l]{\varepsilon\pi}, \zeta)$, d. h. in diesem Körper gehört jede Idealklasse dem Hauptgeschlecht an, und der zuletzt genannte Charakter besitzt daher den Wert 1. Wir haben nun $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\} = 1$, d. h. wegen der Formel auf S. 228

$$\left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\} = \left\{\frac{\varepsilon}{\mathfrak{p}^*}\right\}^{-1}; \tag{142}$$

ferner $\left\{\frac{\varepsilon^*\pi^*}{\mathfrak{p}}\right\} = 1$, d. h.

$$\left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\} = \left\{\frac{\varepsilon^*}{\mathfrak{p}}\right\}^{-1}, \tag{143}$$

und endlich $\left\{\frac{\varepsilon^*\pi^*, \varepsilon\pi}{\mathfrak{l}}\right\} = 1$ oder mit Benutzung von (83), (S. 266)

$$\left\{\frac{\varepsilon^*, \varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\varepsilon^*, \pi}{\mathfrak{l}}\right\}\left\{\frac{\pi^*, \varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\pi^*, \pi}{\mathfrak{l}}\right\} = 1.$$

Da nach Hilfssatz 36 $\left\{\frac{\varepsilon^*, \varepsilon}{\mathfrak{l}}\right\} = 1$ und nach Hilfssatz 30 $\left\{\frac{\pi^*, \pi}{\mathfrak{l}}\right\} = 1$ ist, so geht letztere Formel in

$$\left\{\frac{\pi, \varepsilon^*}{\mathfrak{l}}\right\} = \left\{\frac{\pi^*, \varepsilon}{\mathfrak{l}}\right\} \tag{144}$$

über. Da wegen der von uns gemachten Voraussetzung

$$\left\{\frac{\pi, \varepsilon^*}{\mathfrak{l}}\right\} = \left\{\frac{\varepsilon^*}{\mathfrak{p}}\right\} \quad \text{und} \quad \left\{\frac{\pi^*, \varepsilon}{\mathfrak{l}}\right\} = \left\{\frac{\varepsilon}{\mathfrak{p}^*}\right\}$$

ist, so folgt aus (144) $\left\{\frac{\varepsilon^*}{\mathfrak{p}}\right\} = \left\{\frac{\varepsilon}{\mathfrak{p}^*}\right\}$, und diese Gleichung liefert mit Benutzung der Formeln (142), (143) die im Hilfssatz 39 behauptete Gleichung.

Will man wiederum den Satz 151 für $\mathfrak{w} = \mathfrak{l}$ nur in dem Falle eines Körpers $k(\sqrt[l]{\mu}, \zeta)$ anwenden, für den $\mu \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ ausfällt, so wähle man im obigen Beweise die Einheit ε derart, daß man außer $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\} = 1$ noch bei einem geeigneten, zu l primen Exponenten a $(\varepsilon\pi)^a \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ hat. Eine Bestimmung der Einheit ε in dieser Weise ist, wie man leicht sieht, sicher stets dann möglich, wenn $\left\{\frac{\zeta}{\mathfrak{p}^*}\right\} = 1$ ist. Ist aber $\left\{\frac{\zeta}{\mathfrak{p}^*}\right\} \neq 1$ und zugleich $\left\{\frac{\pi}{\mathfrak{p}^*}\right\} \neq 1$, so kann jene Bedingung ebenfalls erfüllt werden, indem man für ε eine geeignete Potenz von ζ nimmt. Ob die fragliche Bedingung sich erfüllen läßt, bleibt also nur dann zweifelhaft, wenn gleichzeitig $\left\{\frac{\zeta}{\mathfrak{p}^*}\right\} \neq 1$ und $\left\{\frac{\pi}{\mathfrak{p}^*}\right\} = 1$ ausfällt. In diesem Falle vertauschen wir bei dem obigen Beweise die Rollen von $\mathfrak{p}, \pi$ einerseits und $\mathfrak{p}^*, \pi^*$ andererseits; dann bleibt offenbar nur noch der Fall unerledigt, daß zugleich $\left\{\frac{\zeta}{\mathfrak{p}^*}\right\} \neq 1$, $\left\{\frac{\zeta}{\mathfrak{p}}\right\} \neq 1$ und $\left\{\frac{\pi}{\mathfrak{p}^*}\right\} = 1$, $\left\{\frac{\pi^*}{\mathfrak{p}}\right\} = 1$ ausfällt. In diesem Falle erkennt man aber aus den letzten zwei Beziehungen die Behauptung des Hilfssatzes 39 ohne weiteres als richtig.

Hilfssatz 40. Wenn $\mathfrak{p}$ ein Primideal erster Art in $k(\zeta)$ ist und π eine Primärzahl von $\mathfrak{p}$ bedeutet, und wenn für jede beliebige Einheit ξ in $k(\zeta)$ die Gleichung

$$\left\{\frac{\xi}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \xi}{\mathfrak{l}}\right\}$$

besteht, wenn ferner $\mathfrak{p}^*$ ein solches von $\mathfrak{p}$ verschiedenes Primideal erster Art ist, daß

$$\left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\} = \left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\} + 1$$

ausfällt, so gibt es stets eine Einheit ε in $k(\zeta)$ von der Art, daß

$$\left\{\frac{\varepsilon}{\mathfrak{p}^*}\right\} = \left\{\frac{\pi^*, \varepsilon}{\mathfrak{l}}\right\} + 1$$

wird, wobei π^* eine Primärzahl von $\mathfrak{p}^*$ bezeichnet.

Beweis. Wir verfahren zuvörderst genau wie beim Beweise des vorigen Hilfssatzes und gelangen so unter Einführung gewisser Einheiten ε und ε^* wieder zu den drei Formeln (142), (143), (144). Nun ist wegen der Voraussetzung des Hilfssatzes 40 $\left\{\frac{\varepsilon^*}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \varepsilon^*}{\mathfrak{l}}\right\}$; hieraus und wegen $\left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\} = \left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\} + 1$ folgt in Verbindung mit den drei genannten Formeln die Richtigkeit des Hilfssatzes 40.

Soll Satz 151 nur für den Fall $\mu \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ zur Anwendung gelangen, so hat man im vorstehenden Beweise nur nötig, die Einheit ε so zu bestimmen, daß außer der Gleichung $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\} = 1$ noch die Kongruenz $(\varepsilon\pi)^a \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ bei einem zu l primen Exponenten a erfüllt wird; es ist eine solche Bestimmung von ε hier stets möglich.

§ 157. Ein besonderer Fall des Reziprozitätsgesetzes für zwei Primideale.

Satz 162. Wenn $\mathfrak{p}$ und $\mathfrak{q}$ irgend zwei beliebige Primideale eines regulären Kreiskörpers sind, für welche $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1$ gilt, so ist stets auch $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = 1$.

Beweis. Es seien $\pi, \varkappa$ Primärzahlen bez. von $\mathfrak{p}, \mathfrak{q}$. Wir betrachten den Kummerschen Körper $k(\sqrt[l]{\pi}, \zeta)$ und unterscheiden zwei Fälle, je nachdem $\mathfrak{p}$ ein Primideal erster oder zweiter Art ist.

Im ersten Falle enthält die Relativdiskriminante von $k(\sqrt[l]{\pi}, \zeta)$ die zwei Primideale $\mathfrak{l}$ und $\mathfrak{p}$, und es gibt nach Hilfssatz 37 eine Einheit ε in $k(\zeta)$, für welche der Charakter $\left\{\frac{\varepsilon, \pi}{\mathfrak{l}}\right\} + 1$ ausfällt. Das Charakterensystem eines Ideals in $k(\sqrt[l]{\pi}, \zeta)$ besteht daher nur aus einem Charakter, d. h. es ist $r = 1$ und nach Hilfssatz 35 auch $g = 1$. Wegen $\left\{\frac{\pi}{\mathfrak{q}}\right\} = 1$ ist $\mathfrak{q}$ in $k(\sqrt[l]{\pi}, \zeta)$ weiter zerlegbar;

es sei $\mathfrak{Q}$ ein Primfaktor von $\mathfrak{q}$ in diesem Körper. Da $\pi, \varkappa$ primär sind, so fällt nach Hilfssatz 30 (S. 289) $\left\{\frac{\varkappa,\pi}{l}\right\}=1$ aus, und da $\mathfrak{Q}$ zum Hauptgeschlecht gehört, so ist auch $\left\{\frac{\varkappa,\pi}{\mathfrak{p}}\right\}=\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}=1$, wie es der Satz 162 behauptet.

Wenn $\mathfrak{p}$ ein Primideal zweiter Art ist, so gilt nach Hilfssatz 37 für jede Einheit ξ in $k(\zeta)$ die Gleichung $\left\{\frac{\xi,\pi}{l}\right\}=1$, und folglich enthält, wie im Beweise des Hilfssatzes 37 gezeigt worden ist, die Relativdiskriminante von $k(\sqrt[l]{\pi},\zeta)$ nur das eine Primideal $\mathfrak{p}$. Es ist daher wiederum $r=1$ und $g=1$. Wegen $\left\{\frac{\pi}{\mathfrak{q}}\right\}=1$ ist $\mathfrak{q}$ in $k(\sqrt[l]{\pi},\zeta)$ weiter zerlegbar. Es sei $\mathfrak{Q}$ ein Primfaktor von $\mathfrak{q}$ in diesem Körper. Da $\mathfrak{Q}$ zum Hauptgeschlecht gehört, und mit Rücksicht auf $\left\{\frac{\xi,\pi}{l}\right\}=1$ ist $\left\{\frac{\varkappa,\pi}{\mathfrak{p}}\right\}=\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}=1$, und damit ist der Satz 162 vollständig bewiesen.

Soll wiederum Satz 151 und dementsprechend auch Hilfssatz 35 für $\mathfrak{w}=\mathfrak{l}$ nur in dem Fall eines Körpers $k(\sqrt[l]{\mu},\zeta)$, für den $\mu=1+\lambda$ nach $\mathfrak{l}^2$ ist, angewandt werden, so ist zum Beweise des Satzes 162 im ersten der beiden vorhin unterschiedenen Fälle der folgende Zusatz erforderlich.

Wenn $\mathfrak{p}$ ein beliebiges Primideal und π eine Primärzahl von $\mathfrak{p}$ ist, so erkennen wir aus der Definition des Symbols $\left\{\frac{\nu,\mu}{l}\right\}$ auf S. 266 und mit Rücksicht auf Hilfssatz 24 (S. 267) die Richtigkeit der Gleichung

$$\left\{\frac{\pi,\zeta}{l}\right\}=\zeta^{\frac{n(\mathfrak{p})-1}{l}}=\left\{\frac{\zeta}{\mathfrak{p}}\right\}. \tag{145}$$

Ist nun das Primideal $\mathfrak{q}$ von der Beschaffenheit, daß $\left\{\frac{\zeta}{\mathfrak{q}}\right\}=1$ ausfällt, so bestimmen wir eine l-te Einheitswurzel ζ^* derart, daß $\zeta^*\pi^{l-1}\equiv 1+\lambda$ nach $\mathfrak{l}^2$ ausfällt, und fassen statt des Kummerschen Körpers $k(\sqrt[l]{\pi},\zeta)$ den Körper $k(\sqrt[l]{\zeta^*\pi^{l-1}},\zeta)$ ins Auge. Wir wenden dann die oben dargelegte Schlußweise an. Da

$$\left\{\frac{\varkappa,\zeta^*\pi^{l-1}}{l}\right\}=\left\{\frac{\varkappa,\zeta^*}{l}\right\}\left\{\frac{\varkappa,\pi}{l}\right\}^{l-1}$$

wird und, wie oben, $\left\{\frac{\varkappa,\pi}{l}\right\}=1$ ist, andererseits mit Rücksicht auf die in (145) angegebene Tatsache $\left\{\frac{\varkappa,\zeta}{l}\right\}=\left\{\frac{\zeta}{\mathfrak{q}}\right\}=1$ ausfällt, so folgt $\left\{\frac{\varkappa,\zeta^*\pi^{l-1}}{l}\right\}=1$, und deshalb schließen wir $\left\{\frac{\varkappa,\zeta^*\pi^{l-1}}{\mathfrak{p}}\right\}=1$, d. h. $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}=1$.

Es sei andererseits $\left\{\frac{\zeta}{\mathfrak{q}}\right\}\neq 1$. Da $\mathfrak{p}$ ein Primideal erster Art ist, so gibt es sicher eine Einheit ε_1, für welche $\left\{\frac{\varepsilon_1}{\mathfrak{p}}\right\}\neq 1$ ist, und ferner nach Hilfssatz 37 (S. 314) sicher eine Einheit ε_2, für welche $\left\{\frac{\varepsilon_2,\pi}{l}\right\}\neq 1$ ausfällt. Auch können

wir diese Einheiten $\varepsilon_1, \varepsilon_2$ überdies beide so wählen, daß sie $\equiv 1+\lambda$ nach $\mathfrak{l}^2$ sind. Wir entnehmen hieraus weiter die Existenz einer Einheit ε, für welche $\left\{\frac{\varepsilon}{\mathfrak{p}}\right\}\neq 1$ sowie $\left\{\frac{\varepsilon,\pi}{l}\right\}\neq 1$ ausfällt und überdies die Kongruenzeigenschaft $\varepsilon\equiv 1+\lambda$ nach $\mathfrak{l}^2$ erfüllt ist. In der Tat, wenn diese Bedingungen weder für $\varepsilon=\varepsilon_1$ noch für $\varepsilon=\varepsilon_2$ zutreffen, so ist gleichzeitig $\left\{\frac{\varepsilon_1,\pi}{l}\right\}=1$ und $\left\{\frac{\varepsilon_2}{\mathfrak{p}}\right\}=1$, und dann würde $\varepsilon=(\varepsilon_1\varepsilon_2)^{\frac{l+1}{2}}$ eine Einheit von der verlangten Beschaffenheit sein. Wir bestimmen nun eine solche Potenz $\eta=\varepsilon^a$ der Einheit ε, daß $\left\{\frac{\eta\varkappa}{\mathfrak{p}}\right\}=1$ wird. Wäre nun $\left\{\frac{\varkappa}{\mathfrak{p}}\right\}\neq 1$, so fiele der Exponent a gewiß zu l prim aus, und folglich wäre $\left\{\frac{\eta,\pi}{l}\right\}\neq 1$. Es ist außerdem, da $\varkappa$ eine primäre Zahl darstellt, ersichtlich, daß eine gewisse Potenz von $\eta\varkappa$ mit einem zu l primen Exponenten der Zahl $1+\lambda$ nach $\mathfrak{l}^2$ kongruent wird. Aus (145) und Hilfssatz 36 (S. 313) folgt noch $\left\{\frac{\zeta,\eta\varkappa}{l}\right\}\neq 1$. Der Kummersche Körper $k(\sqrt[l]{\eta\varkappa},\zeta)$ besitzt deshalb nur ein Geschlecht. Wegen $\left\{\frac{\eta\varkappa}{\mathfrak{p}}\right\}=1$ ist $\mathfrak{p}$ in diesem Körper weiter zerlegbar; ist $\mathfrak{P}$ ein in $\mathfrak{p}$ aufgehender Primfaktor dieses Körpers, so findet man den Charakter von $\mathfrak{P}$ gleich dem Symbol

$$\left\{\frac{\zeta^*\pi,\eta\varkappa}{\mathfrak{q}}\right\}=\left\{\frac{\zeta^*\pi}{\mathfrak{q}}\right\},$$

wenn ζ^* eine solche l-te Einheitswurzel bedeutet, daß $\left\{\frac{\zeta^*\pi,\eta\varkappa}{l}\right\}=1$ ausfällt. Wegen der letzten Gleichung, und da $\left\{\frac{\zeta,\eta}{l}\right\}=1$ ist, folgt $\left\{\frac{\zeta^*,\varkappa}{l}\right\}\left\{\frac{\pi,\eta}{l}\right\}=1$, und wegen $\left\{\frac{\pi,\eta}{l}\right\}\neq 1$ ist also auch $\left\{\frac{\zeta^*,\varkappa}{l}\right\}\neq 1$, d. i. mit Rücksicht auf (145) $\left\{\frac{\zeta^*}{\mathfrak{q}}\right\}\neq 1$; somit ist $\zeta^*\neq 1$. Da aber jener eine Charakter des Primideals $\mathfrak{P}$ gleich 1 sein muß, so folgt wegen $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=1$ notwendig auch $\left\{\frac{\zeta^*}{\mathfrak{q}}\right\}=1$, und dies stünde im Widerspruch mit der eben gezogenen Folgerung.

§ 158. Das Vorhandensein gewisser Hilfsprimideale, für welche das Reziprozitätsgesetz gilt.

Auf Grund der Sätze 152, 140 und 162 erkennen wir leicht die Existenz gewisser Primideale, die in § 159 und § 160 zur Verwendung kommen werden. Es gelten folgende Tatsachen:

Hilfssatz 41. Wenn $\mathfrak{p}$ ein beliebiges Primideal des regulären Kreiskörpers $k(\zeta)$ bedeutet, so gibt es stets ein Primideal $\mathfrak{r}$ in $k(\zeta)$, welches den Bedingungen

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\}\neq 1, \qquad \left\{\frac{\mathfrak{p}}{\mathfrak{r}}\right\}=\left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\}\neq 1$$

genügt.

Beweis. Es sei h die Klassenanzahl von $k(\zeta)$ und, wie in § 149 und § 154, h^* eine positive ganze rationale Zahl, so daß $hh^* \equiv 1$ nach l wird. Es sei p die rationale, durch $\mathfrak{p}$ teilbare Primzahl und $\pi = \mathfrak{p}^{hh^*}$ eine Primärzahl von $\mathfrak{p}$; ferner seien $\mathfrak{p}', \mathfrak{p}'', \ldots$ die untereinander und von $\mathfrak{p}$ verschiedenen, zu $\mathfrak{p}$ konjugierten Primideale in $k(\zeta)$ und $\pi' = \mathfrak{p}'^{hh^*}, \pi'' = \mathfrak{p}''^{hh^*}$ die betreffenden zu π konjugierten Zahlen in $k(\zeta)$; sie sind Primärzahlen bez. von $\mathfrak{p}', \mathfrak{p}'', \ldots$. Wir haben dann $p = \mathfrak{p}\mathfrak{p}'\mathfrak{p}'' \ldots$; da ferner $\frac{p^{hh^*}}{\pi\pi'\pi'' \ldots}$ eine Einheit in $k(\zeta)$ sein muß und überdies primär ausfällt, so stellt nach Satz 156 (s. auch S. 287) dieser Quotient die l-te Potenz einer Einheit ε in $k(\zeta)$ dar, es ist also

$$p^{hh^*} = \varepsilon^l \pi\pi'\pi'' \ldots .$$

Nunmehr wenden wir den Satz 152 (S. 276) an, indem wir dort

$$\alpha_1 = \zeta, \quad \alpha_2 = \pi, \quad \alpha_3 = \pi', \quad \alpha_4 = \pi'', \quad \alpha_5 = \pi''', \ldots,$$
$$\gamma_1 = \zeta, \quad \gamma_2 = \zeta, \quad \gamma_3 = 1, \quad \gamma_4 = 1, \quad \gamma_5 = 1, \ldots$$

nehmen. Da ζ nicht die l-te Potenz einer Einheit in $k(\zeta)$ ist und $\pi, \pi', \pi'', \ldots$ Potenzen von Primidealen sind, deren Exponenten zu l prim ausfallen, so sind die Voraussetzungen des Satzes 152 erfüllt, und es gibt daher nach diesem Satze in $k(\zeta)$ ein Primideal $\mathfrak{r}$, für welches bei irgendeinem geeigneten, zu l primen Exponenten m

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\}^m = \zeta, \qquad \left\{\frac{\pi}{\mathfrak{r}}\right\}^m = \zeta, \qquad \left\{\frac{\pi'}{\mathfrak{r}}\right\}^m = 1, \qquad \left\{\frac{\pi''}{\mathfrak{r}}\right\}^m = 1, \ldots,$$

d. h.

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\} = \zeta^*, \qquad \left\{\frac{\pi}{\mathfrak{r}}\right\} = \zeta^*, \qquad \left\{\frac{\pi'}{\mathfrak{r}}\right\} = 1, \qquad \left\{\frac{\pi''}{\mathfrak{r}}\right\} = 1, \ldots \tag{146}$$

wird, wo ζ^* eine von 1 verschiedene l-te Einheitswurzel darstellt. Aus (146) erhalten wir $\left\{\frac{p^{hh^*}}{\mathfrak{r}}\right\} = \left\{\frac{\varepsilon^{-l} p^{hh^*}}{\mathfrak{r}}\right\} = \left\{\frac{\pi\pi'\pi'' \ldots}{\mathfrak{r}}\right\} = \zeta^*$, und folglich wird wegen Satz 140 (S. 231) auch $\left\{\frac{\varrho}{p^{hh^*}}\right\} = \zeta^*$, wo ϱ eine Primärzahl von $\mathfrak{r}$ bedeuten soll. Da nun wegen (146) nach Satz 162 (S. 319) $\left\{\frac{\varrho}{\pi'}\right\} = 1, \left\{\frac{\varrho}{\pi''}\right\} = 1, \ldots$ sein muß und

$$\left\{\frac{\varrho}{p^{hh^*}}\right\} = \left\{\frac{\varrho}{\pi}\right\}\left\{\frac{\varrho}{\pi'}\right\}\left\{\frac{\varrho}{\pi''}\right\} \ldots$$

ist, so erhalten wir $\left\{\frac{\varrho}{\pi}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\} = \zeta^*$; damit ist gezeigt, daß das Primideal $\mathfrak{r}$ alle Bedingungen des Hilfssatzes 41 erfüllt.

Hilfssatz 42. Wenn $\mathfrak{p}$ ein beliebiges Primideal des regulären Kreiskörpers $k(\zeta)$ und π eine Primärzahl von $\mathfrak{p}$ bedeutet, wenn ferner ε eine beliebige Einheit in $k(\zeta)$, nur nicht die l-te Potenz einer Einheit in $k(\zeta)$ ist, so gibt es ein Primideal $\mathfrak{r}$ in $k(\zeta)$, das den Bedingungen

$$\left\{\frac{\varepsilon\pi}{\mathfrak{r}}\right\} = 1, \qquad \left\{\frac{\mathfrak{p}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\} \neq 1$$

genügt.

Beweis. Es mögen $\pi, \pi', \pi'', \ldots$ für $\mathfrak{p}$ die Bedeutung wie im vorigen Hilfssatz 41 haben; wir nehmen in Satz 152 (S. 276)

$$\alpha_1 = \varepsilon\pi, \quad \alpha_2 = \pi, \quad \alpha_3 = \pi', \quad \alpha_4 = \pi'', \quad \alpha_5 = \pi''', \ldots,$$
$$\gamma_1 = 1, \quad \gamma_2 = \zeta, \quad \gamma_3 = 1, \quad \gamma_4 = 1, \quad \gamma_5 = 1, \ldots;$$

die Zahlen $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \ldots$ genügen wiederum, wie man leicht einsieht, der Voraussetzung des Satzes 152; es führt die entsprechende Schlußweise wie in Hilfssatz 41 zu einem Primideal $\mathfrak{r}$ von der hier verlangten Beschaffenheit.

§ 159. Beweis des ersten Ergänzungssatzes zum Reziprozitätsgesetz.

Um den ersten Ergänzungssatz für ein Primideal $\mathfrak{p}$ der ersten Art zu beweisen, wenden wir den Hilfssatz 41 an; diesem zufolge läßt sich ein Primideal $\mathfrak{r}$ bestimmen, für welches

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\} \neq 1 \quad \text{und} \quad \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\} = \left\{\frac{\mathfrak{p}}{\mathfrak{r}}\right\} \neq 1$$

wird, und das also gewiß ein Primideal erster Art ist. Nach Gleichung (145) haben wir für das Primideal $\mathfrak{r}$ die Gleichung

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\} = \zeta^{\frac{n(\mathfrak{r})-1}{l}} = \left\{\frac{\varrho, \zeta}{l}\right\},$$

wo ϱ eine Primärzahl von $\mathfrak{r}$ bedeuten soll. Da $\left\{\frac{\zeta}{\mathfrak{r}}\right\} \neq 1$ ausfällt, so besteht nach Hilfssatz 38 (S. 316) auch für jede andere Einheit ξ in $k(\zeta)$ die Gleichung

$$\left\{\frac{\xi}{\mathfrak{r}}\right\} = \left\{\frac{\varrho, \xi}{l}\right\}$$

und demnach treffen die sämtlichen Bedingungen des Hilfssatzes 40 (S. 319) zu, wenn wir an Stelle der dort mit $\mathfrak{p}$ bez. $\mathfrak{p}^*$ bezeichneten Primideale die beiden Primideale $\mathfrak{r}$ bez. $\mathfrak{p}$ nehmen. Nach jenem Hilfssatze gibt es somit eine Einheit ε in $k(\zeta)$ derart, daß $\left\{\frac{\varepsilon}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \varepsilon}{l}\right\} \neq 1$ wird, wobei π eine Primärzahl von $\mathfrak{p}$ bedeuten soll. Infolge dieser Tatsache ist nach Hilfssatz 38 (S. 316) auch für jede andere Einheit ξ in $k(\zeta)$ die Gleichung $\left\{\frac{\xi}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \xi}{l}\right\}$ erfüllt, wie es der erste Ergänzungssatz behauptet.

Des weiteren bedeute $\mathfrak{q}$ ein Primideal zweiter Art in $k(\zeta)$. Dann ist nach der Definition eines solchen Primideals für jede Einheit ξ in $k(\zeta)$ stets $\left\{\frac{\xi}{\mathfrak{q}}\right\} = 1$, und wenn $\varkappa$ eine Primärzahl von $\mathfrak{q}$ bezeichnet, so ist nach Hilfssatz 37 (S. 314) stets auch $\left\{\frac{\varkappa, \xi}{l}\right\} = 1$. Es gilt daher in der Tat wiederum der erste Ergänzungssatz $\left\{\frac{\xi}{\mathfrak{q}}\right\} = \left\{\frac{\varkappa, \xi}{l}\right\}$.

§ 160. Beweis des Reziprozitätsgesetzes zwischen zwei beliebigen Primidealen.

Nachdem der erste Ergänzungssatz in § 159 bewiesen worden ist, folgt aus Hilfssatz 39 (S. 317) sofort die Richtigkeit des Reziprozitätsgesetzes für zwei beliebige Primideale erster Art.

Es sei *zweitens* ein Primideal $\mathfrak{p}$ erster Art und ein Primideal $\mathfrak{q}$ zweiter Art vorgelegt; π und $\varkappa$ seien Primärzahlen von $\mathfrak{p}$ und $\mathfrak{q}$. Im Falle, daß $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}=1$ ausfällt, folgt aus Satz 162 (S. 319) $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=1$ und mithin die Richtigkeit des Reziprozitätsgesetzes für $\mathfrak{p}$ und $\mathfrak{q}$. Wir nehmen jetzt an, es sei $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}=\left\{\frac{\varkappa}{\mathfrak{p}}\right\}\neq 1$. Da $\mathfrak{p}$ von der ersten Art ist, so gibt es eine Einheit ε, so daß $\left\{\frac{\varepsilon\varkappa}{\mathfrak{p}}\right\}=1$ ausfällt, und es kann hierbei stets, wie aus einer Betrachtung am Schlusse des Beweises von Hilfssatz 39 (S. 317) hervorgeht, die Einheit ε zugleich so bestimmt werden, daß eine gewisse Potenz von $\varepsilon\varkappa$ mit einem zu l primen Exponenten $\equiv 1+\lambda$ nach $\mathfrak{l}^2$ wird. Wir betrachten den Kummerschen Körper $k(\sqrt[l]{\varepsilon\varkappa},\zeta)$. Nach Satz 148 (S. 251) enthält die Relativdiskriminante dieses Körpers in bezug auf $k(\zeta)$ die zwei Primfaktoren $\mathfrak{l}$ und $\mathfrak{q}$. Da $\mathfrak{q}$ ein Primideal zweiter Art ist, so gelten wegen der Hilfssätze 36 und 37 für jede Einheit ξ in $k(\zeta)$ die Gleichungen

$$\left\{\frac{\xi,\varepsilon\varkappa}{\mathfrak{l}}\right\}=\left\{\frac{\xi,\varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\xi,\varkappa}{\mathfrak{l}}\right\}=1,\qquad \left\{\frac{\xi}{\mathfrak{q}}\right\}=1,$$

und demgemäß ist die Anzahl r der Charaktere, welche das Geschlecht eines Ideals in $k(\sqrt[l]{\varepsilon\varkappa},\zeta)$ bestimmen, gleich 2. Nach Hilfssatz 35 (S. 312) ist dann in $k(\sqrt[l]{\varepsilon\varkappa},\zeta)$ die Anzahl der Geschlechter $g\leq l$. Wir bestimmen nun nach Hilfssatz 42 (S. 322) ein Primideal $\mathfrak{r}$ in $k(\zeta)$ von der Beschaffenheit, daß

$$\left\{\frac{\varepsilon\varkappa}{\mathfrak{r}}\right\}=1,\qquad \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}\neq 1$$

wird. Wegen der ersteren Gleichung ist $\mathfrak{r}$ in $k(\sqrt[l]{\varepsilon\varkappa},\zeta)$ weiter zerlegbar. Es sei $\mathfrak{R}$ ein Primfaktor von $\mathfrak{r}$ in diesem Körper und ϱ eine Primärzahl von $\mathfrak{r}$. Dann besteht das Charakterensystem des Ideals $\mathfrak{R}$ in $k(\sqrt[l]{\varepsilon\varkappa},\zeta)$ aus den beiden Charakteren

$$\left\{\frac{\varrho,\varepsilon\varkappa}{\mathfrak{l}}\right\},\qquad \left\{\frac{\varrho,\varepsilon\varkappa}{\mathfrak{q}}\right\}=\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}. \tag{147}$$

Da der zweite Charakter $\neq 1$ ist, so bestimmen die Ideale $\mathfrak{R},\mathfrak{R}^2,\ldots,\mathfrak{R}^l$ lauter voneinander verschiedene Geschlechter, und es gibt, wie die oben gefundene obere Grenze für die Anzahl der Geschlechter zeigt, außer diesen keine weiteren Geschlechter. Mit Benutzung des in § 159 bewiesenen ersten

Ergänzungssatzes ergibt sich

$$\left\{\frac{\varrho,\varepsilon\varkappa}{\mathfrak{l}}\right\}\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=\left\{\frac{\varrho,\varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=\left\{\frac{\varepsilon}{\mathfrak{r}}\right\}\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=\left\{\frac{\varepsilon}{\mathfrak{r}}\right\}\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}=\left\{\frac{\varepsilon\varkappa}{\mathfrak{r}}\right\}=1,$$

d. h. das Produkt der beiden Charaktere (147) ist gleich 1. Da jedes beliebige Ideal in $k(\sqrt[l]{\varepsilon\varkappa},\zeta)$ notwendig einem jener l Geschlechter angehören muß, so folgt hieraus, daß für jedes Ideal in $k(\sqrt[l]{\varepsilon\varkappa},\zeta)$ das Produkt seiner beiden Charaktere stets gleich 1 ist. Wegen $\left\{\frac{\varepsilon\varkappa}{\mathfrak{p}}\right\}=1$ ist $\mathfrak{p}$ in $k(\sqrt[l]{\varepsilon\varkappa},\zeta)$ weiter zerlegbar; bezeichnet $\mathfrak{P}$ einen Primfaktor von $\mathfrak{p}$ in diesem Körper, so sind die beiden Charaktere für $\mathfrak{P}$ durch die Symbole

$$\left\{\frac{\pi,\varepsilon\varkappa}{\mathfrak{l}}\right\},\qquad \left\{\frac{\pi,\varepsilon\varkappa}{\mathfrak{q}}\right\}=\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}$$

gegeben, und es folgt somit unter Benutzung des in § 159 bewiesenen Ergänzungssatzes notwendig

$$\left\{\frac{\pi,\varepsilon\varkappa}{\mathfrak{l}}\right\}\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=\left\{\frac{\pi,\varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=\left\{\frac{\varepsilon}{\mathfrak{p}}\right\}\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=1$$

oder

$$\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=\left\{\frac{\varepsilon}{\mathfrak{p}}\right\}^{-1}=\left\{\frac{\varkappa}{\mathfrak{p}}\right\}=\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\},$$

d. h. es gilt das Reziprozitätsgesetz für die beiden Primideale $\mathfrak{p}$ und $\mathfrak{q}$.

Es seien *drittens* zwei Primideale $\mathfrak{q}$ und $\mathfrak{q}^*$ der zweiten Art vorgelegt; $\varkappa,\varkappa^*$ seien Primärzahlen von $\mathfrak{q}$ bez. $\mathfrak{q}^*$. Wir betrachten den Kummerschen Körper $k(\sqrt[l]{\varkappa\varkappa^*},\zeta)$. Die Zahlen $\varkappa$ und $\varkappa^*$ sind, wie sich im Beweise des Hilfssatzes 37 herausgestellt hat, l-ten Potenzen von gewissen ganzen Zahlen in $k(\zeta)$ nach $\mathfrak{l}'$ kongruent; das gleiche gilt daher von $\varkappa\varkappa^*$, und folglich ist nach Satz 148 (S. 251) die Relativdiskriminante des Körpers $k(\sqrt[l]{\varkappa\varkappa^*},\zeta)$ nicht durch $\mathfrak{l}$ teilbar. Diese Relativdiskriminante enthält somit nur die beiden Primfaktoren $\mathfrak{q}$ und $\mathfrak{q}^*$. Nun ist für jede Einheit ξ in $k(\zeta)$

$$\left\{\frac{\xi,\varkappa\varkappa^*}{\mathfrak{q}}\right\}=\left\{\frac{\xi}{\mathfrak{q}}\right\}=1,\qquad \left\{\frac{\xi,\varkappa\varkappa^*}{\mathfrak{q}^*}\right\}=\left\{\frac{\xi}{\mathfrak{q}^*}\right\}=1,$$

und dementsprechend ist die Anzahl r der Charaktere, welche das Geschlecht eines Ideals in $k(\sqrt[l]{\varkappa\varkappa^*},\zeta)$ bestimmen, $=2$. Nach Hilfssatz 35 (S. 312) ist dann in $k(\sqrt[l]{\varkappa\varkappa^*},\zeta)$ die Anzahl der Geschlechter $g\leqq l$. Ferner läßt sich nach Satz 152 (S. 276) jedenfalls ein Primideal $\mathfrak{r}$ in $k(\zeta)$ bestimmen derart, daß

$$\left\{\frac{\varkappa\varkappa^*}{\mathfrak{r}}\right\}=1,\qquad \left\{\frac{\zeta}{\mathfrak{r}}\right\}\neq 1,\qquad \left\{\frac{\varkappa}{\mathfrak{r}}\right\}\neq 1$$

ausfällt. Wegen der ersten Gleichung ist $\mathfrak{r}$ in $k(\sqrt[l]{\varkappa\varkappa^*},\zeta)$ weiter zerlegbar; es sei $\mathfrak{R}$ ein Primfaktor von $\mathfrak{r}$ in diesem Körper und ϱ eine Primärzahl von $\mathfrak{r}$.

Dann besteht das Charakterensystem des Ideals $\mathfrak{R}$ in $k(\sqrt[l]{\varkappa\varkappa^*}, \zeta)$ aus den beiden Charakteren

$$\left.\begin{aligned}\left\{\frac{\varrho\cdot\varkappa\varkappa^*}{\mathfrak{q}}\right\} &= \left\{\frac{\varrho}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\},\\ \left\{\frac{\varrho\cdot\varkappa\varkappa^*}{\mathfrak{q}^*}\right\} &= \left\{\frac{\varrho}{\mathfrak{q}^*}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}^*}\right\}.\end{aligned}\right| \tag{148}$$

Da der erste Charakter wegen $\left\{\frac{\varkappa}{\mathfrak{r}}\right\} + 1$ dem Satze 162 (S. 319) gemäß notwendig ebenfalls verschieden von 1 ist, so bestimmen die Ideale $\mathfrak{R}, \mathfrak{R}^2, \cdots, \mathfrak{R}^l$ lauter voneinander verschiedene Geschlechter, und es gibt, wie bereits gezeigt worden ist, auch hier nicht mehr als l Geschlechter. Wegen $\left\{\frac{\zeta}{\mathfrak{r}}\right\} + 1$ ist $\mathfrak{r}$ ein Primideal erster Art; es gilt daher nach dem vorigen einerseits für die Primideale $\mathfrak{r}, \mathfrak{q}$, andererseits für die Primideale $\mathfrak{r}, \mathfrak{q}^*$ das Reziprozitätsgesetz, und das Produkt der beiden Charaktere (148) wird folglich

$$\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}\left\{\frac{\mathfrak{r}}{\mathfrak{q}^*}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}\left\{\frac{\mathfrak{q}^*}{\mathfrak{r}}\right\} = \left\{\frac{\varkappa\varkappa^*}{\mathfrak{r}}\right\} = 1. \tag{149}$$

Da jedes beliebige Ideal in $k(\sqrt[l]{\varkappa\varkappa^*}, \zeta)$ einem jener l Geschlechter angehören muß, so folgt aus (149), daß für jedes Ideal das Produkt seiner beiden Charaktere gleich 1 sein muß. Nun ist das Ideal $\mathfrak{q}$ gleich der l-ten Potenz eines Primideals $\mathfrak{Q}$ in $k(\sqrt[l]{\varkappa\varkappa^*}, \zeta)$. Die beiden Charaktere von $\mathfrak{Q}$ in diesem Körper sind alsdann

$$\left\{\frac{\varkappa, \varkappa\varkappa^*}{\mathfrak{q}}\right\} = \left\{\frac{\varkappa^*, \varkappa\varkappa^*}{\mathfrak{q}}\right\}^{-1} = \left\{\frac{\varkappa^*}{\mathfrak{q}}\right\}^{-1} = \left\{\frac{\mathfrak{q}^*}{\mathfrak{q}}\right\}^{-1},$$

$$\left\{\frac{\varkappa, \varkappa\varkappa^*}{\mathfrak{q}^*}\right\} = \left\{\frac{\varkappa}{\mathfrak{q}^*}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{q}^*}\right\},$$

und da ihr Produkt gleich 1 sein soll, so erhalten wir

$$\left\{\frac{\mathfrak{q}^*}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{q}^*}\right\}.$$

Hiermit ist das Reziprozitätsgesetz für zwei Primideale der zweiten Art bewiesen, und nunmehr ist der Beweis des Reziprozitätsgesetzes für zwei beliebige Primideale vollständig erbracht.

§ 161. Beweis des zweiten Ergänzungssatzes zum Reziprozitätsgesetz.

Es sei zunächst $\mathfrak{p}$ ein Primideal erster Art und π eine Primärzahl von $\mathfrak{p}$. Wir bestimmen eine Einheit ε in $k(\zeta)$ derart, daß $\left\{\frac{\varepsilon\lambda}{\mathfrak{p}}\right\} = 1$ wird, und betrachten dann den durch $\sqrt[l]{\varepsilon\lambda}$ und ζ bestimmten Kummerschen Körper. Wegen $\left\{\frac{\varepsilon\lambda}{\mathfrak{p}}\right\} = 1$ ist $\mathfrak{p}$ in diesem Körper weiter zerlegbar; es sei $\mathfrak{P}$ ein Primfaktor von $\mathfrak{p}$ in diesem Körper. Wir erkennen, daß das Charakterensystem des Ideals $\mathfrak{P}$ aus dem

einen Charakter $\left\{\frac{\pi, \varepsilon\lambda}{\mathfrak{l}}\right\}$ besteht, und da somit nach Hilfssatz 35 (S. 312) auch nur ein Geschlecht, nämlich das Hauptgeschlecht, vorhanden ist, so muß dieser Charakter den Wert 1 besitzen. Hieraus, und da nach § 159 $\left\{\frac{\varepsilon}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \varepsilon}{\mathfrak{l}}\right\}$ ist, folgt sofort die Gleichung $\left\{\frac{\lambda}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \lambda}{\mathfrak{l}}\right\}$.

Des weiteren sei ein Primideal $\mathfrak{q}$ der zweiten Art vorgelegt, und es bezeichne $\varkappa$ eine Primärzahl von $\mathfrak{q}$; dann sind zwei Fälle zu unterscheiden, je nachdem $\left\{\frac{\lambda}{\mathfrak{q}}\right\} = 1$ oder $+1$ ausfällt. Im ersteren Falle lehrt die Betrachtung des Kummerschen Körpers $k(\sqrt[l]{\lambda}, \zeta)$, daß auch $\left\{\frac{\varkappa, \lambda}{\mathfrak{l}}\right\} = 1$ ist. Im zweiten Falle bestimme man nach Satz 152 (S. 276) ein Primideal $\mathfrak{p}$, für welches $\left\{\frac{\zeta}{\mathfrak{p}}\right\} = \left\{\frac{\varkappa}{\mathfrak{p}}\right\}^{-1} + 1$ ausfällt. Dann ist $\mathfrak{p}$ gewiß ein Primideal erster Art, und es folgt nach Satz 162 (S. 319), wenn π eine Primärzahl von $\mathfrak{p}$ bedeutet, $\left\{\frac{\pi}{\mathfrak{q}}\right\} + 1$; mithin läßt sich gewiß eine ganze rationale Zahl a so bestimmen, daß $\left\{\frac{\lambda\pi^a}{\mathfrak{q}}\right\} = 1$ ausfällt. Betrachten wir den Körper $k(\sqrt[l]{\lambda\pi^a}, \zeta)$, so besteht für diesen, weil $\left\{\frac{\zeta, \lambda\pi^a}{\mathfrak{p}}\right\} = \left\{\frac{\zeta}{\mathfrak{p}}\right\}^a + 1$ ist, das Charakterensystem eines Ideals wiederum nur aus einem Charakter und dieser ist stets gleich 1. Wenden wir die letztere Tatsache auf einen Primfaktor $\mathfrak{Q}$ von $\mathfrak{q}$ in diesem Körper an, so folgt $\left\{\frac{\zeta\varkappa, \lambda\pi^a}{\mathfrak{l}}\right\} = \left\{\frac{\zeta}{\mathfrak{p}}\right\}^{-a}\left\{\frac{\varkappa, \lambda}{\mathfrak{l}}\right\} = 1$, und berücksichtigen wir die Gleichung $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}$, so entsteht $\left\{\frac{\lambda}{\mathfrak{q}}\right\} = \left\{\frac{\varkappa, \lambda}{\mathfrak{l}}\right\}$.

Das Reziprozitätsgesetz für l-te Potenzreste ist zuerst von Kummer bewiesen worden. Der hier dargelegte neue Beweis desselben unterscheidet sich von den Kummerschen Beweisen vor allem darin, daß Kummer zunächst den ersten Ergänzungssatz, und zwar unter einem erheblichen Aufwande von Rechnung, durch eine kunstvolle Erweiterung der Formeln der Kreisteilung gewinnt und dann erst auf Grund der errechneten Formeln das Reziprozitätsgesetz zwischen zwei Primidealen ableitet, während die obige Entwicklung die Beweisgründe für das Reziprozitätsgesetz und seine beiden Ergänzungssätze aus gemeinsamer Quelle schöpft.

Von besonderen Reziprozitätsgesetzen, zu deren Behandlung die Formeln der Kreisteilung ausreichen, sind das Reziprozitätsgesetz für biquadratische Reste [Gauss (*3*), Eisenstein (*8*, *9*)], das Reziprozitätsgesetz für kubische Reste [Eisenstein (*5*, *7*), Jacobi (*1*)], ferner für bikubische Reste [Gmeiner (*1*, *2*, *3*)] und die auf 5-te, 8-te, 12-te Potenzreste bezüglichen Untersuchungen von Jacobi zu nennen [Jacobi (*4*)].

Auch sei endlich noch erwähnt, daß Eisenstein ohne Beweis ein Reziprozitätsgesetz für l-te Potenzreste aufgestellt und dabei auch den Fall in Betracht gezogen hat, daß die Klassenanzahl des Kreiskörpers der l-ten Einheitswurzeln durch l teilbar ist [Eisenstein (*1*, *12*)].

34. Die Anzahl der vorhandenen Geschlechter im regulären Kummerschen Körper.

§ 162. Ein Satz über das Symbol $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$.

Die wichtigste Aufgabe in der Theorie der Geschlechter eines Kummerschen Körpers betrifft die Ermittlung der Anzahl der wirklich vorhandenen Geschlechter. Wir beweisen hier zunächst einen Satz, welcher dem Hilfssatz 14 (S. 171) aus der Theorie des quadratischen Körpers entspricht.

Satz 163. Wenn ν und μ zwei beliebige ganze Zahlen ($+0$) eines regulären Kreiskörpers $k(\zeta)$ bedeuten, so ist stets

$$\prod_{(\mathfrak{w})}\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}=1,$$

wenn das Produkt linker Hand über sämtliche Primideale $\mathfrak{w}$ in $k(\zeta)$ erstreckt wird.

Beweis. Es sei h die Anzahl der Idealklassen in $k(\zeta)$ und h^* eine ganze rationale positive Zahl mit der Kongruenzeigenschaft $hh^*\equiv 1$ nach l. Wir setzen $\nu=\mathfrak{l}^a\mathfrak{p}_1\mathfrak{p}_2\cdots$ und $\mu=\mathfrak{l}^b\mathfrak{q}_1\mathfrak{q}_2\cdots$, so daß a und b ganze rationale Exponenten und $\mathfrak{p}_1,\mathfrak{p}_2,\ldots,\mathfrak{q}_1,\mathfrak{q}_2,\ldots$ gewisse von $\mathfrak{l}$ verschiedene Primideale in $k(\zeta)$ sind. Bedeuten ferner $\pi_1,\pi_2,\ldots,\varkappa_1,\varkappa_2,\ldots$ Primärzahlen der Prim-Ideale bez. $\mathfrak{p}_1,\mathfrak{p}_2,\ldots,\mathfrak{q}_1,\mathfrak{q}_2,\ldots$, und zwar derart, daß

$$\pi_1=\mathfrak{p}_1^{hh^*},\quad \pi_2=\mathfrak{p}_2^{hh^*},\ \ldots,\quad \varkappa_1=\mathfrak{q}_1^{hh^*},\quad \varkappa_2=\mathfrak{q}_2^{hh^*},\ \ldots$$

gilt, und wird noch $\lambda=1-\zeta$ gesetzt, so bestehen zwei Gleichungen von der Gestalt:

$$\nu^{hh^*}=\varepsilon\lambda^{ahh^*}\pi_1\pi_2\ldots,\qquad \mu^{hh^*}=\eta\lambda^{bhh^*}\varkappa_1\varkappa_2\ldots, \tag{150}$$

worin ε und η Einheiten in $k(\zeta)$ sind. Wenn $\mathfrak{w}$ ein beliebiges Primideal bedeutet, so ist allgemein

$$\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}=\left\{\frac{\nu^{hh^*},\mu^{hh^*}}{\mathfrak{w}}\right\}. \tag{151}$$

Es seien nun $\mathfrak{p},\mathfrak{q}$ zwei voneinander und von $\mathfrak{l}$ verschiedene Primideale in $k(\zeta)$ und $\pi,\varkappa$ bez. Primärzahlen von $\mathfrak{p},\mathfrak{q}$; ferner seien ε,η beliebige Einheiten in $k(\zeta)$. Aus Hilfssatz 36 (S. 313) und aus Satz 161 (S. 312) folgen dann leicht die Formeln

$$\left.\begin{aligned}\left\{\frac{\varepsilon,\eta}{\mathfrak{l}}\right\}&=1,&\qquad\left\{\frac{\varepsilon,\lambda}{\mathfrak{l}}\right\}&=1,\\ \left\{\frac{\varepsilon,\pi}{\mathfrak{l}}\right\}\left\{\frac{\varepsilon,\pi}{\mathfrak{p}}\right\}&=1,&\qquad\left\{\frac{\pi,\varkappa}{\mathfrak{p}}\right\}\left\{\frac{\pi,\varkappa}{\mathfrak{q}}\right\}&=1.\end{aligned}\right\} \tag{152}$$

Ist $\mathfrak{w}$ ein von $\mathfrak{l}$ verschiedenes Primideal, welches nicht in μ aufgeht, so ist nach Satz 148 (S. 251) die Relativdiskriminante des Kummerschen Körpers $k(\sqrt[l]{\mu},\zeta)$ zu $\mathfrak{w}$ prim; fällt dann $\mathfrak{w}$ auch zu ν prim aus, so ist nach Satz 150 (S. 257) die Zahl ν Normenrest des Kummerschen Körpers $k(\sqrt[l]{\mu},\zeta)$, und daher gilt nach

Satz 151 (S. 272) die Gleichung $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}=1$. Mit Rücksicht hierauf gilt wegen (152) der Satz für den Fall, daß eine jede der Zahlen ν,μ sei es eine Einheit, sei es eine beliebige Potenz von λ, sei es eine Primärzahl eines von $\mathfrak{l}$ verschiedenen Primideals vorstellt; wegen (150) und (151) und auf Grund der Regeln (80) (S. 265) und (83) (S. 266) gilt sodann der Satz 163 allgemein.

§ 163. Der Fundamentalsatz über die Geschlechter eines regulären Kummerschen Körpers.

Wir sind jetzt imstande, für den regulären Kummerschen Körper denjenigen Satz aufzustellen und zu beweisen, welcher dem fundamentalen Satz 100 (S. 168) in der Theorie des quadratischen Körpers entspricht. Dieser Satz lautet:

Satz 164. *Es sei r die Anzahl der Charaktere, welche ein Geschlecht im regulären Kummerschen Körper $K=k(\sqrt[l]{\mu},\zeta)$ bestimmen; ist dann ein System von r beliebigen l-ten Einheitswurzeln vorgelegt, so ist dieses System dann und nur dann das Charakterensystem eines Geschlechtes in K, wenn das Produkt der sämtlichen r Einheitswurzeln gleich 1 ist. Die Anzahl der in K vorhandenen Geschlechter ist daher gleich l^{r-1}.*

Beweis. Es sei h die Klassenanzahl des regulären Kreiskörpers $k(\zeta)$ und h^* eine ganze rationale positive Zahl mit der Kongruenzeigenschaft $hh^*\equiv 1$ nach l; ferner seien $\mathfrak{l}_1,\ldots,\mathfrak{l}_r$ die r gemäß § 149 ausgewählten Primfaktoren der Relativdiskriminante von K. Es bedeute nun A irgendeine Idealklasse in K, $\mathfrak{J}$ ein zu $\mathfrak{l}=(1-\zeta)$ und zur Relativdiskriminante von K primes Ideal der Klasse A und $\bar{\nu}=(N_k(\mathfrak{J}))^{hh^*}$ die nach der Vorschrift in § 149 (S. 306) aus $\mathfrak{J}$ gebildete und mit einem gewissen Einheitsfaktor versehene ganze Zahl in $k(\zeta)$, so daß

$$\chi_1(\mathfrak{J})=\left\{\frac{\bar{\nu},\mu}{\mathfrak{l}_1}\right\},\ \ldots,\ \chi_r(\mathfrak{J})=\left\{\frac{\bar{\nu},\mu}{\mathfrak{l}_r}\right\}$$

die r Einzelcharaktere sind, welche das Geschlecht von $\mathfrak{J}$ bestimmen. Es sei $\mathfrak{p}$ ein Ideal des Kreiskörpers $k(\zeta)$, wofern es ein solches gibt, welches in $\bar{\nu}$ zu einem nicht durch l teilbaren Exponenten vorkommt; dabei ist $\mathfrak{p}$ sicher von $\mathfrak{l}$ verschieden und prim zur Relativdiskriminante von K. Da $N_k(\mathfrak{J})$ die Relativnorm eines Ideals ist, so muß $\mathfrak{p}$ im Körper K zerlegbar sein. Es gilt mithin nach Satz 149 (S. 254) für jedes solche Primideal $\mathfrak{p}$ die Gleichung $\left\{\frac{\mu}{\mathfrak{p}}\right\}=1$, und daher ist auch stets $\left\{\frac{\bar{\nu},\mu}{\mathfrak{p}}\right\}=1$. Mit Rücksicht auf Satz 163 (S. 328) folgt daher

$$\prod_{(\mathfrak{w})}\left\{\frac{\bar{\nu},\mu}{\mathfrak{w}}\right\}=1, \tag{153}$$

wenn $\mathfrak{w}$ alle in der Relativdiskriminante von K enthaltenen, von $\mathfrak{l}$ verschiede-

nen Primideale und außerdem das Primideal $\mathfrak{l}$ durchläuft. Ferner ist, wenn $\mathfrak{l}_{r+1}, \mathfrak{l}_{r+2}, \ldots, \mathfrak{l}_t$ die außer $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_r$ in der Relativdiskriminante aufgehenden Primideale bedeuten, nach § 149

$$\left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_{r+1}}\right\} = 1, \qquad \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_{r+2}}\right\} = 1, \ \ldots, \ \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_t}\right\} = 1. \tag{154}$$

Kommt nun in der Relativdiskriminante des Körpers K das Primideal $\mathfrak{l}$ vor, so ist wegen (153) schon hiermit bewiesen, daß das Produkt sämtlicher r Charaktere gleich 1 ist. Kommt andererseits das Primideal $\mathfrak{l}$ in jener Relativdiskriminante nicht vor, so ist nach Satz 150 (S. 257) die Zahl $\bar{\nu}$ Normenrest des Körpers K nach $\mathfrak{l}$, und folglich ist nach Satz 151 (S. 272) $\left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}}\right\} = 1$; damit erkennen wir aus (153) und (154) auch in diesem Falle den einen Teil der Aussage des Satzes 164 als richtig.

Den Beweis für den anderen Teil der Aussage des Satzes 164 führen wir der Kürze wegen nur in dem Fall, daß die Relativdiskriminante des Körpers K den Primfaktor $\mathfrak{l}$ nicht enthält. Es seien dann wiederum $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ die t in der Relativdiskriminante von K aufgehenden Primideale des Körpers $k(\zeta)$, und $\lambda_1, \ldots, \lambda_t$ seien bezüglich Primärzahlen von $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$; ferner gehe allgemein $\mathfrak{l}_i$ in μ genau e_i mal auf, und es sei e_i^* dann eine ganze rationale Zahl mit der Kongruenzeigenschaft $e_i e_i^* \equiv 1$ nach l. Endlich mögen $\gamma_1, \ldots, \gamma_r$ beliebig gewählte r der Bedingung $\gamma_1 \ldots \gamma_r = 1$ genügende l-te Einheitswurzeln sein; nach Satz 152 (S. 276) gibt es dann stets in $k(\zeta)$ ein Primideal $\mathfrak{p}$, das in μ nicht aufgeht und überdies die Forderungen

$$\left\{\frac{\lambda_1}{\mathfrak{p}}\right\}^m = \gamma_1^{e_1^*}, \qquad \left\{\frac{\lambda_2}{\mathfrak{p}}\right\}^m = \gamma_2^{e_2^*}, \ \ldots, \ \left\{\frac{\lambda_r}{\mathfrak{p}}\right\}^m = \gamma_r^{e_r^*}, \tag{155}$$

$$\left\{\frac{\lambda_{r+1}}{\mathfrak{p}}\right\}^m = 1, \qquad \left\{\frac{\lambda_{r+2}}{\mathfrak{p}}\right\}^m = 1, \ \ldots, \ \left\{\frac{\lambda_t}{\mathfrak{p}}\right\}^m = 1 \tag{156}$$

für irgendeinen Exponenten m aus der Reihe $1, 2, \ldots, l-1$ erfüllt. Ist π eine Primärzahl von $\mathfrak{p}$, so folgt wegen (155) mit Benutzung von Satz 161 (S. 312)

$$\left\{\frac{\pi^m, \mu}{\mathfrak{l}_i}\right\} = \left\{\frac{\pi, \mu}{\mathfrak{l}_i}\right\}^m = \left\{\frac{\pi}{\mathfrak{l}_i}\right\}^{m e_i} = \left\{\frac{\lambda_i}{\mathfrak{p}}\right\}^{m e_i} = \gamma_i, \qquad (i = 1, 2, \ldots, r). \tag{157}$$

Ferner ergibt sich wegen (156) in ähnlicher Weise

$$\left\{\frac{\pi, \mu}{\mathfrak{l}_i}\right\} = \left\{\frac{\pi}{\mathfrak{l}_i}\right\}^{e_i} = \left\{\frac{\lambda_i}{\mathfrak{p}}\right\}^{e_i} = 1, \qquad (i = r+1, r+2, \ldots, t). \tag{158}$$

Da $\gamma_1 \cdots \gamma_r = 1$ ist, so ist wegen (157) und (158)

$$\prod_{(\mathfrak{w})} \left\{\frac{\pi, \mu}{\mathfrak{w}}\right\} = 1, \tag{159}$$

wenn hierin $\mathfrak{w}$ alle Primideale $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ durchläuft. Bedeutet nun $\mathfrak{m}$ ein von $\mathfrak{p}, \mathfrak{l}_1, \ldots, \mathfrak{l}_t$ verschiedenes Primideal in $k(\zeta)$, so ist gemäß Satz 150

(S. 257) die Zahl π Normenrest des Kummerschen Körpers K nach $\mathfrak{m}$ und folglich nach Satz 151 (S. 272) stets $\left\{\frac{\pi, \mu}{\mathfrak{m}}\right\} = 1$. Mit Rücksicht auf diesen Umstand und wegen (159) lehrt der Satz 163 (S. 328), daß auch $\left\{\frac{\pi, \mu}{\mathfrak{p}}\right\} = 1$, d. h. $\left\{\frac{\mu}{\mathfrak{p}}\right\} = 1$ sein muß. Infolge der letzteren Gleichung zerfällt das Primideal $\mathfrak{p}$ nach Satz 149 (S. 254) im Körper K in l Primideale. Ist $\mathfrak{P}$ eines derselben, so hat, wenn wir (157) und (158) berücksichtigen, das Ideal $\mathfrak{P}^m$ offenbar die vorgeschriebenen Einheitswurzeln $\gamma_1, \ldots, \gamma_r$ als Charaktere, und damit ist der Satz 164 für den hier betrachteten Fall vollständig bewiesen.

Geht $\mathfrak{l}$ in der Relativdiskriminante von K auf, so hat man, um den Satz 164 zu beweisen, an den vorstehenden Ausführungen eine geeignete Abänderung anzubringen, die man leicht aus der Analogie mit den entsprechenden Betrachtungen für den quadratischen Körper (vgl. S. 184 bis 185) ersieht.

Kummer hat seinen Untersuchungen einen gewissen Zahlring im Körper $K = k(\sqrt[l]{\mu}, \zeta)$, nicht die Gesamtheit der ganzen Zahlen dieses Körpers zugrunde gelegt. Der Begriff des Geschlechtes bedarf dann einer gewissen veränderten Fassung. Es ist Kummers großes Verdienst, für den von ihm ausgewählten Zahlring diejenige Tatsache aufgestellt und bewiesen zu haben, die für den Körper K selbst sich in dem Satze 164 ausdrückt [Kummer (*20*)]. Außer dem von Kummer behandelten Ringe sind noch unendlich viele andere Ringe in K vorhanden, deren Theorie mit entsprechendem Erfolge zu entwickeln sein würde.

§ 164. Die Klassen des Hauptgeschlechtes in einem regulären Kummerschen Körper.

Wir heben in diesem und dem nächsten Paragraphen einige wichtige Folgerungen hervor, die aus dem Fundamentalsatz 164 für den Kummerschen Körper $K = k(\sqrt[l]{\mu}, \zeta)$ sich ergeben, und die den in § 71 und § 72 oder in § 82 für den quadratischen Körper entwickelten Sätzen entsprechen.

Satz 165. Die Anzahl g der Geschlechter in einem regulären Kummerschen Körper ist gleich der Anzahl seiner ambigen Komplexe.

Beweis. Wenn t und n die Bedeutung wie in Satz 159 (S. 302) haben, und wenn wir berücksichtigen, daß nach Satz 164 (S. 329) $g = l^{r-1}$ ist, so folgt aus Hilfssatz 34 (S. 310) $r - 1 \leqq t + n - \frac{l+1}{2}$, und da nach Hilfssatz 33 (S. 308) andererseits $t + n - \frac{l+1}{2} \leqq r - 1$ sein muß, so folgt

$$r - 1 = t + n - \frac{l+1}{2}.$$

Die im Beweise (S. 311) zu Hilfssatz 34 bestimmte Anzahl a der ambigen Komplexe ist mithin $= l^{r-1}$; wir haben daher $a = g$.

Satz 166. *Jeder Komplex des Hauptgeschlechtes in einem regulären Kummerschen Körper K ist die $(1-S)$-te symbolische Potenz eines Komplexes in K, d. h. jede Klasse des Hauptgeschlechtes in einem regulären Kummerschen Körper K ist gleich dem Produkt aus der $(1-S)$-ten symbolischen Potenz einer Klasse und aus einer solchen Klasse, welche Ideale des Kreiskörpers $k(\zeta)$ enthält.*

Beweis. In dem Beweise (S. 312) zu Hilfssatz 34 ist die Gleichung $af' = gf$ abgeleitet; hierbei bedeutet a die Anzahl der ambigen Komplexe, f' die Anzahl derjenigen Komplexe, welche gleich $(1-S)$-ten symbolischen Potenzen von Komplexen sind, ferner bedeutet g die Anzahl der Geschlechter und f die Anzahl der Komplexe des Hauptgeschlechtes. Da nach Satz 165 $a = g$ ist, so folgt $f' = f$, und damit ist bewiesen, daß jeder Komplex des Hauptgeschlechtes die $(1-S)$-te symbolische Potenz eines Komplexes ist.

§ 165. Der Satz von den Relativnormen der Zahlen eines regulären Kummerschen Körpers.

Satz 167. *Wenn ν, μ zwei ganze Zahlen des regulären Kreiskörpers $k(\zeta)$ bedeuten, von denen μ nicht die l-te Potenz einer ganzen Zahl in $k(\zeta)$ ist, und welche für jedes Primideal $\mathfrak{w}$ in $k(\zeta)$ die Bedingung*

$$\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = 1,$$

erfüllen, so ist die Zahl ν stets gleich der Relativnorm einer ganzen oder gebrochenen Zahl $\mathfrak{A}$ des Kummerschen Körpers $K = k(\sqrt[l]{\mu}, \zeta)$.

Beweis. Wir beweisen diesen Satz zunächst für den Fall, daß ν eine Einheit in $k(\zeta)$ ist. Es mögen wiederum t und n für den Kummerschen Körper $K = k(\sqrt[l]{\mu}, \zeta)$ die Bedeutung wie in Satz 159 (S. 302) haben; im Beweise zu Satz 165 ist gezeigt worden, daß $r - 1 = t + n - \frac{l+1}{2}$ sein muß, d. h. es ist $n = \frac{l-1}{2} - t + r$. Andererseits betrachten wir die $r^* = t - r$ Einheiten $\varepsilon_1, \ldots, \varepsilon_{r^*}$, die in § 149 (S. 307) bestimmt worden sind. Wegen der Gleichungen (140) (S. 307) kann ein Produkt aus Potenzen dieser r^* Einheiten nur dann die l-te Potenz einer Einheit in $k(\zeta)$ sein, wenn die Potenzexponenten sämtlich durch l teilbar sind. Es müssen sich daher, da die Gesamtheit aller Einheiten in $k(\zeta)$ eine Schar vom Grade $\frac{l-1}{2}$ bildet, weiter $\frac{l-1}{2} - r^*$ Einheiten $\varepsilon_{r^*+1}, \varepsilon_{r^*+2}, \ldots, \varepsilon_{\frac{l-1}{2}}$ in $k(\zeta)$ bestimmen lassen, so daß überhaupt jede Einheit ξ in $k(\zeta)$ sich in der Gestalt

$$\xi = \varepsilon_1^{x_1} \varepsilon_2^{x_2} \cdots \varepsilon_{\frac{l-1}{2}}^{x_{\frac{l-1}{2}}} \cdot \varepsilon^l$$

darstellen läßt, wobei $x_1, x_2, \ldots, x_{\frac{l-1}{2}}$ ganze rationale Exponenten sind und ε eine geeignete Einheit in $k(\zeta)$ bedeutet. Setzen wir nun allgemein

$$\left\{\frac{\varepsilon_u, \mu}{\mathfrak{l}_{l-v+1}}\right\} = \zeta^{e_{uv}}, \qquad \left(u = 1, 2, \ldots, \frac{l-1}{2};\ v = 1, 2, \ldots, r^*\right),$$

so liefern die r^* Gleichungen

$$\left\{\frac{\xi, \mu}{\mathfrak{l}_l}\right\} = 1, \quad \left\{\frac{\xi, \mu}{\mathfrak{l}_{l-1}}\right\} = 1, \ldots, \left\{\frac{\xi, \mu}{\mathfrak{l}_{l-r^*+1}}\right\} = 1 \tag{160}$$

für die Exponenten $x_1, x_2, \ldots, x_{\frac{l-1}{2}}$ die r^* linearen Kongruenzen

$$\left.\begin{aligned} e_{11} x_1 + e_{21} x_2 + \cdots + e_{\frac{l-1}{2}, 1}\, x_{\frac{l-1}{2}} &\equiv 0, \\ \cdots\cdots\cdots\

pers $k(\zeta)$ ins Auge. Wir setzen $\lambda = 1 - \zeta$ und $\mathfrak{l} = (\lambda)$. Kommt das Primideal $\mathfrak{l}$ des Körpers $k(\zeta)$ in ν zu einer Potenz erhoben vor, deren Exponent b nicht durch l teilbar ist, und geht außerdem $\mathfrak{l}$ in der Relativdiskriminante des Körpers K nicht auf, so haben wir auf Grund der Angaben am Schlusse von § 133 auf S. 274

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = \left\{\frac{\lambda^b, \mu}{\mathfrak{l}}\right\} = \left\{\frac{\mu}{\mathfrak{l}}\right\}^{-b},$$

und mit Rücksicht auf die hieraus zu entnehmende Gleichung

$$\left\{\frac{\mu}{\mathfrak{l}}\right\} = 1$$

ist $\mathfrak{l}$ nach Satz 149 (S. 254) in K als Produkt von l Primfaktoren darstellbar. Bedeutet $\mathfrak{L}$ einen derselben, so haben wir $\mathfrak{l} = N_k(\mathfrak{L})$.

Es sei ferner $\mathfrak{p}$ ein von $\mathfrak{l}$ verschiedenes Primideal des Kreiskörpers $k(\zeta)$, und es komme $\mathfrak{p}$ in ν zu einer Potenz erhoben vor, deren Exponent b nicht durch l teilbar ist; dagegen sei der Exponent a, zu dem $\mathfrak{p}$ in μ aufgeht, durch l teilbar: dann ist nach der Definition des Symbols

$$\left\{\frac{\nu, \mu}{\mathfrak{p}}\right\} = \left\{\frac{\mu^b}{\mathfrak{p}}\right\}^{-1},$$

und hieraus folgt wegen der Voraussetzung des Satzes 167 $\left\{\frac{\mu}{\mathfrak{p}}\right\} = 1$; nach Satz 149 (S. 254) ist also $\mathfrak{p}$ in K als Produkt von l Primidealen darstellbar. Ist $\mathfrak{P}$ eines dieser l Primideale, so wird $\mathfrak{p} = N_k(\mathfrak{P})$.

Endlich sind die in der Relativdiskriminante von K aufgehenden Primideale des Körpers $k(\zeta)$ stets l-te Potenzen von Primidealen in K und daher ebenfalls Relativnormen von Idealen in K. Aus allen diesen Umständen zusammengenommen folgt, daß ν die Relativnorm eines Ideals $\mathfrak{H}$ in K sein muß, d. h. es ist $\nu = N_k(\mathfrak{H})$.

Wegen der Voraussetzung des Satzes 167 gehört ferner $\mathfrak{H}$ dem Hauptgeschlecht in K an, und wir können daher nach Satz 166 (S. 332)

$$\mathfrak{H} \sim \mathfrak{j}\,\mathfrak{J}^{1-s}$$

setzen, in solcher Weise, daß $\mathfrak{j}$ ein Ideal in $k(\zeta)$ und $\mathfrak{J}$ ein Ideal in K bedeutet. Ist h die Anzahl der Idealklassen in $k(\zeta)$, so haben wir $\mathfrak{j}^h \sim 1$, und folglich muß $\mathsf{A} = \left(\frac{\mathfrak{H}}{\mathfrak{J}^{1-s}}\right)^h$ eine ganze oder gebrochene Zahl des Körpers K sein; die Relativnorm dieser Zahl $N_k(\mathsf{A})$ ist offenbar $= \varepsilon \nu^h$, wo ε eine Einheit in $k(\zeta)$ bedeutet. Aus der letzten Gleichung folgt nach Satz 151 (S. 272), daß für jedes beliebige Primideal $\mathfrak{w}$ in $k(\zeta)$ notwendig $\left\{\frac{\varepsilon \nu^h, \mu}{\mathfrak{w}}\right\} = 1$ und daher auch $\left\{\frac{\varepsilon, \mu}{\mathfrak{w}}\right\} = 1$ sein muß. Es ist nun im ersten Teile des gegenwärtigen Beweises gezeigt worden, daß unter diesen Umständen ε stets gleich der Relativnorm einer Zahl in K sein muß, wir setzen $\varepsilon = N_k(\mathsf{H})$, wo H eine Zahl in K ist. Bedeuten dann b und e zwei ganze rationale Zahlen von der Art, daß $bh + el = 1$ ist, so folgt

$$\nu = N_k(\mathsf{A}^b \mathsf{H}^{-b} \nu^e),$$

und hiermit ist der Beweis für den Satz 167 vollständig erbracht.

In diesem Beweise können wir die Anwendung des Satzes 151 beidemal auf den Fall $\mathfrak{w} \neq \mathfrak{l}$ beschränken, da dann nach Satz 163 (S. 328) die behaupteten Tatsachen auch für $\mathfrak{w} = \mathfrak{l}$ folgen.

Damit ist es dann gelungen, alle diejenigen Eigenschaften auf den regulären Kummerschen Körper zu übertragen, welche für den quadratischen Körper bereits von Gauss aufgestellt und bewiesen worden sind.

35. Neue Begründung der Theorie des regulären Kummerschen Körpers.

§ 166. Die wesentlichen Eigenschaften der Einheiten des regulären Kreiskörpers.

Wir haben gesehen, eine wie wichtige Rolle das besondere Symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ in der Theorie des Kummerschen Körpers spielt. Was die Definition dieses Symbols in § 131 (S. 266) und die Ableitung seiner Eigenschaften in § 131 bis § 133 betrifft, so knüpften wir in der dortigen Darstellung an die von Kummer eingeführten logarithmischen Differentialquotienten der zu einer Zahl $\omega \equiv 1$ nach $\mathfrak{l}$ gehörenden Funktion $\omega(x)$ an. Die in § 131 bis § 133 für das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ im Kummerschen Körper ausgeführten Rechnungen entsprechen übrigens genau denjenigen Betrachtungen, welche in § 64 für das Symbol $\left(\frac{n, m}{2}\right)$ im quadratischen Körper angestellt worden sind. Obwohl es nun bereits gelang, die von Kummer ersonnenen rechnerischen Hilfsmittel auf ein geringes Maß zu bringen, so erscheint es mir doch noch, vor allem auch im Hinblick auf eine künftige Erweiterung der Theorie, notwendig zu untersuchen, ob nicht eine Begründung der Theorie des Kummerschen Körpers ganz ohne jene Rechnungen möglich ist. Ich gebe in diesem Kapitel den Weg hierzu kurz an.

Zunächst können leicht ohne Rechnung und ohne Heranziehung der Bernoullischen Zahlen die späterhin wesentlichen Eigenschaften der Einheiten des regulären Kreiskörpers $k(\zeta)$ abgeleitet werden. Für Satz 156 erinnern wir uns des zweiten auf S. 287 mitgeteilten Beweises.

Wir können dann aus diesem Satz 156 den Satz 155 (S. 286) wie folgt ableiten. Wir wollen unter $\varepsilon_1, \ldots, \varepsilon_{l^*}$ irgendein System von l^* reellen Grundeinheiten des Körpers $k(\zeta)$ verstehen; wir bestimmen dann positive Exponenten $e_1, \ldots, e_{l^*}$ und gewisse ganze rationale, zu l prime Zahlen $a_1, \ldots, a_{l^*}$,

$b_1, \ldots, b_{l^*}$ derart, daß die Kongruenzen

$$\begin{aligned} \varepsilon_1 &\equiv a_1 + b_1 \lambda^{e_1}, \qquad ([e_1+1]),\\ &\cdots\cdots\cdots\cdots\\ \varepsilon_{l^*} &\equiv a_{l^*} + b_{l^*} \lambda^{e_{l^*}}, \qquad ([l^{e_{l^*}+1}]) \end{aligned}$$

gültig sind. Wir nehmen an, es habe unter den Exponenten $e_1, \ldots, e_{l^*}$ etwa e_1 den niedrigsten vorkommenden Wert. Dann können wir, wie leicht ersichtlich ist, die l^*-1 Einheiten $\varepsilon_2, \ldots, \varepsilon_{l^*}$ derart mit Potenzen von ε_1 multiplizieren, daß für die l^*-1 entstehenden Produkte $\varepsilon'_2, \ldots, \varepsilon'_{l^*}$ die Kongruenzen

$$\begin{aligned} \varepsilon'_2 = \varepsilon_2 \varepsilon_1^{f_2} &\equiv a'_2 + b'_2 \lambda^{e'_2}, \qquad ([e'_2+1]),\\ &\cdots\cdots\cdots\cdots\\ \varepsilon'_{l^*} = \varepsilon_{l^*} \varepsilon_1^{f_{l^*}} &\equiv a'_{l^*} + b'_{l^*} \lambda^{e'_{l^*}}, \qquad ([l^{e'_{l^*}+1}]) \end{aligned}$$

bestehen, wo $a'_2, \ldots, a'_{l^*}, b'_2, \ldots, b'_{l^*}$ ganze rationale, zu l prime Zahlen bedeuten, und wo nun die Exponenten $e'_2, \ldots, e'_{l^*}$ sämtlich größer als e_1 sind. Die Einheiten $\varepsilon_1, \varepsilon'_2, \varepsilon'_3, \ldots, \varepsilon'_{l^*}$ bilden wiederum ein System von Grundeinheiten in $k(\zeta)$. Nun möge unter den Exponenten $e'_2, \ldots, e'_{l^*}$ etwa e'_2 den niedrigsten vorkommenden Wert haben; dann ist es weiter möglich, die Einheiten $\varepsilon'_3, \ldots, \varepsilon'_{l^*}$ derart mit Potenzen von ε'_2 zu multiplizieren, daß für die l^*-2 entstehenden Produkte $\varepsilon''_3, \ldots, \varepsilon''_{l^*}$ die Kongruenzen

$$\begin{aligned} \varepsilon''_3 = \varepsilon'_3 \varepsilon_2'^{f'_3} &\equiv a''_3 + b''_3 \lambda^{e''_3}, \qquad ([l^{e''_3+1}]),\\ &\cdots\cdots\cdots\cdots\\ \varepsilon''_{l^*} = \varepsilon'_{l^*} \varepsilon_2'^{f'_{l^*}} &\equiv a''_{l^*} + b''_{l^*} \lambda^{e''_{l^*}}, \qquad ([l^{e''_{l^*}+1}]) \end{aligned}$$

gelten, wo $a''_3, \ldots, a''_{l^*}, b''_3, \ldots, b''_{l^*}$ ganze rationale, zu l prime Zahlen bedeuten und nunmehr die Exponenten $e''_3, \ldots, e''_{l^*}$ sämtlich größer als e'_2 sind. Die Einheiten $\varepsilon_1, \varepsilon'_2, \varepsilon''_3, \varepsilon''_4, \ldots, \varepsilon''_{l^*}$ bilden offenbar wiederum ein System von Grundeinheiten in $k(\zeta)$. Indem wir in geeigneter Weise fortfahren, gelangen wir zu einem System von Grundeinheiten $\varepsilon_1, \varepsilon'_2, \ldots, \varepsilon''^{(l^*-1)}_{l^*}$ in $k(\zeta)$, die den Kongruenzen

$$\begin{aligned} \varepsilon_1 &\equiv a_1 + b_1 \lambda^{e_1}, \qquad ([e_1+1]),\\ \varepsilon'_2 &\equiv a'_2 + b'_2 \lambda^{e'_2}, \qquad ([e'_2+1]),\\ \varepsilon''_3 &\equiv a''_3 + b''_3 \lambda^{e''_3}, \qquad ([l^{e''_3+1}]),\\ &\cdots\cdots\cdots\cdots\\ \varepsilon''^{(l^*-1)}_{l^*} &\equiv a''^{(l^*-1)}_{l^*} + b''^{(l^*-1)}_{l^*} \lambda^{e''^{(l^*-1)}_{l^*}}, \qquad ([l^{e''^{(l^*-1)}_{l^*}+1}]) \end{aligned}$$

genügen, wo $a_1, \ldots, a''^{(l^*-1)}_{l^*}, b_1, \ldots, b''^{(l^*-1)}_{l^*}$ ganze rationale, zu l prime Zahlen sind, während für die Exponenten $e_1, \ldots, e''^{(l^*-1)}_{l^*}$ die Kette von Ungleichungen

$$e_1 < e'_2 < e''_3 < \cdots < e''^{(l^*-1)}_{l^*} \tag{162}$$

gilt. Da die betrachteten Einheiten sämtlich reell sind, so fallen die Exponenten $e_1, e'_2, e''_3, \ldots, e''^{(l^*-1)}_{l^*}$ gerade aus. Wäre nun

$$e''^{(l^*-1)}_{l^*} \geqq l-1,$$

so würde nach Satz 156 $\varepsilon''^{(l^*-1)}_{l^*}$ die l-te Potenz einer Einheit η in $k(\zeta)$ sein. Drücken wir dann η durch die Einheiten $\zeta, \varepsilon_1, \varepsilon'_2, \ldots, \varepsilon''^{(l^*-1)}_{l^*}$ aus in der Gestalt

$$\eta = \zeta^u \varepsilon_1^{u_1} \varepsilon_2'^{u_2} \cdots (\varepsilon''^{(l^*-1)}_{l^*})^{u_{l^*}},$$

wo $u, u_1, u_2, \ldots, u_{l^*}$ ganze rationale Exponenten sind, und erheben diese Gleichung in die l-te Potenz, so erhalten wir eine Relation zwischen den l^* Einheiten $\varepsilon_1, \varepsilon'_2, \ldots, \varepsilon''^{(l^*-1)}_{l^*}$ mit Exponenten, die nicht sämtlich Null sind; dies widerspricht der Tatsache, daß $\varepsilon_1, \varepsilon'_2, \ldots, \varepsilon''^{(l^*-1)}_{l^*}$ ein System von Grundeinheiten in $k(\zeta)$ bilden. Es ist daher

$$e''^{(l^*-1)}_{l^*} < l-1.$$

Hieraus folgt mit Rücksicht auf die Ungleichungen (162), daß notwendigerweise

$$e_1 = 2, \quad e'_2 = 4, \quad e''_3 = 6, \ldots, e''^{(l^*-1)}_{l^*} = l-3$$

sein muß, und diese Tatsache läßt unmittelbar auf das Vorhandensein von solchen Einheiten $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{l^*}$ schließen, die von der im Satze 155 (S. 286) verlangten Beschaffenheit sind.

Der Satz 157 (S. 288) folgt wie in § 142 aus Satz 155.

§ 167. Beweis einer Eigenschaft für die Primärzahlen von Primidealen der zweiten Art.

Wir legen die in § 131 (S. 264) gegebene Definition des Symbols $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ für ein Primideal $\mathfrak{w} \neq \mathfrak{l}$ zugrunde, sehen jedoch vorläufig von einer Definition des Symbols $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ ab; wir benutzen dementsprechend die Sätze 150 (S. 257), 151 (S. 272) ebenfalls nur für $\mathfrak{w} \neq \mathfrak{l}$. Die Sätze 158 (S. 295), 159 (S. 302) folgen dann unmittelbar in der dort dargelegten Weise für den Kummerschen Körper $k(\sqrt[l]{\mu}, \zeta)$, sobald wir die einschränkende Annahme machen, daß die Relativdiskriminante von $k(\sqrt[l]{\mu}, \zeta)$ in bezug auf $k(\zeta)$ zu $\mathfrak{l}$ prim sei. Unter derselben Einschränkung gelangen wir ohne Gebrauch des Symbols $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ zu dem Begriff des Charakters eines Ideals in $k(\sqrt[l]{\mu}, \zeta)$, zu der Einteilung der Idealklassen eines Kummerschen Körpers in Geschlechter, sowie zu der Gültigkeit der Hilfssätze 33 (S. 308), 34 (S. 310), 35 (S. 312) und beweisen dann zunächst folgenden Hilfssatz:

Hilfssatz 43. Eine jede Primärzahl $\varkappa$ eines Primideals $\mathfrak{q}$ der zweiten Art ist der l-ten Potenz einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{l}^l$ kongruent.

Beweis. Es seien $\varepsilon_1, \ldots, \varepsilon_{l^*}$ die in § 166 bestimmten und dort mit $\varepsilon_1, \ldots, \varepsilon_{l^*}^{(l^*-1)}$ bezeichneten $l^* = \frac{l-3}{2}$ Grundeinheiten des Körpers $k(\zeta)$; es seien ferner $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ von $\mathfrak{l}$ verschiedene Primideale in $k(\zeta)$ von der Beschaffenheit, daß

$$\left.\begin{array}{llll} \left\{\frac{\zeta}{\mathfrak{p}}\right\} = \zeta^*, & \left\{\frac{\varepsilon_1}{\mathfrak{p}}\right\} = 1, & \left\{\frac{\varepsilon_2}{\mathfrak{p}}\right\} = 1, \ \ldots, & \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}}\right\} = 1, \\ \left\{\frac{\zeta}{\mathfrak{p}_1}\right\} = 1, & \left\{\frac{\varepsilon_1}{\mathfrak{p}_1}\right\} = \zeta_1, & \left\{\frac{\varepsilon_2}{\mathfrak{p}_1}\right\} = 1, \ \ldots, & \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}_1}\right\} = 1, \\ \cdots\cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots \\ \left\{\frac{\zeta}{\mathfrak{p}_{l^*}}\right\} = 1, & \left\{\frac{\varepsilon_1}{\mathfrak{p}_{l^*}}\right\} = 1, & \left\{\frac{\varepsilon_2}{\mathfrak{p}_{l^*}}\right\} = 1, \ \ldots, & \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}_{l^*}}\right\} = \zeta_{l^*} \end{array}\right\} \quad (163)$$

ausfällt, wo $\zeta^*, \zeta_1, \ldots, \zeta_{l^*}$ irgendwelche von 1 verschiedene l-te Einheitswurzeln bedeuten. Die Existenz solcher Primideale folgt aus Satz 152 (S. 276); wenn wir auf den Beweis dieses Satzes zurückgreifen, sehen wir, daß nicht bloß die Anzahl, sondern die Summe der reziproken Normen aller Primideale $\mathfrak{r}$ von der dort angegebenen Beschaffenheit unendlich war, und wegen dieses Umstandes dürfen wir, wie aus den Betrachtungen beim Beweise des Satzes 83 (S. 143) ersichtlich ist, gegenwärtig annehmen, daß die Primideale $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ obenein sämtlich vom ersten Grade sind. Ferner können wir voraussetzen, daß die durch $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ teilbaren rationalen Primzahlen sämtlich voneinander verschieden ausfallen. Es seien $\pi, \pi_1, \ldots, \pi_{l^*}$ Primärzahlen bez. von $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$.

Wir behandeln nun die Annahme, es gäbe l^*+1 ganze, nicht sämtlich durch l teilbare Exponenten $u, u_1, \ldots, u_{l^*}$, für welche der Ausdruck $\alpha = \pi^u \pi_1^{u_1} \cdots \pi_{l^*}^{u_{l^*}}$ der l-ten Potenz einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{l}^l$ kongruent wird. Nach Satz 148 (S. 251) besitzt dann die Relativdiskriminante des Kummerschen Körpers $k(\sqrt[l]{\alpha}, \zeta)$ eine gewisse Anzahl t der Primideale $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$, aber nicht das Primideal $\mathfrak{l}$ als Faktor. Andererseits folgt aus (163) unter Berücksichtigung des Satzes 151 (S. 272), daß der Grad m der Schar derjenigen Einheiten in $k(\zeta)$, welche Relativnormen von Einheiten in $k(\sqrt[l]{\alpha}, \zeta)$ sind, höchstens den Wert $\frac{l-1}{2} - t$ hat; somit würde für den Kummerschen Körper $k(\sqrt[l]{\alpha}, \zeta)$

$$m \leqq \frac{l-1}{2} - t, \quad \text{d. h.} \quad t + m - \frac{l+1}{2} < 0$$

ausfallen, was nach Satz 158 (S. 295) nicht sein kann. Damit ist die oben versuchte Annahme als unmöglich erkannt, d. h. für Exponenten $u, u_1, \ldots, u_{l^*}$, die nicht sämtlich durch l teilbar sind, ist der Ausdruck $\pi^u \pi_1^{u_1} \ldots \pi_{l^*}^{u_{l^*}}$ niemals der l-ten Potenz einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{l}^l$ kongruent.

Es sei $\varkappa$ eine Primärzahl des Primideals $\mathfrak{q}$. Aus dem Beweise des Satzes 157 (S. 288) entnehmen wir, daß es genau $\frac{(l-1)\cdot l^{l-3}}{h^*}$ nach $\mathfrak{l}^{l-1}$ und also $(l-1)l^{l^*+1}$

nach $\mathfrak{l}^l$ inkongruente primäre Zahlen in $k(\zeta)$ gibt; andererseits ist die l-te Potenz einer zu $\mathfrak{l}$ primen Zahl in $k(\zeta)$ stets der l-ten Potenz einer der $l-1$ Zahlen $1, 2, \ldots, l-1$ nach $\mathfrak{l}^l$ kongruent. Aus der vorhin gefundenen Tatsache folgt daher, daß es stets möglich sein muß, die Exponenten $u, u_1, \ldots, u_{l^*}$ derart zu bestimmen, daß der Ausdruck $\mu = \pi^u \pi_1^{u_1} \cdots \pi_{l^*}^{u_{l^*}} \varkappa$ der l-ten Potenz einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{l}^l$ kongruent wird; wir setzen, wenn $u, u_1, \ldots, u_{l^*}$ solcher Art bestimmt sind, $\alpha = \pi^u \pi_1^{u_1} \cdots \pi_{l^*}^{u_{l^*}}$, so daß $\mu = \alpha\varkappa$ wird, und behandeln nun die Annahme, daß eine gewisse *positive* Anzahl a von diesen Exponenten $u, u_1, \ldots, u_{l^*}$ zu l prim, die übrigen $\frac{l-1}{2} - a$ aber durch l teilbar seien. Es wäre dann wegen (163) für den Kummerschen Körper $k(\sqrt[l]{\mu}, \zeta)$, indem wir für ihn die Bezeichnungen des § 149 benutzen, $t = a+1, r^* = a, r = t - r^* = 1$, und folglich sind nach Hilfssatz 35 (S. 312) in diesem Körper $k(\sqrt[l]{\mu}, \zeta)$ alle Idealklassen vom Hauptgeschlecht. Hieraus ergibt sich unmittelbar folgende Tatsache: wenn $\mathfrak{r}$ irgendein Primideal in $k(\zeta)$ mit der Eigenschaft $\left\{\frac{\mu}{\mathfrak{r}}\right\} = 1$ ist und ϱ eine Primärzahl von $\mathfrak{r}$ bedeutet, so muß bei geeigneter Wahl der Einheit ξ das Charakterensystem der Zahl $\xi\varrho$ im Körper $k(\sqrt[l]{\mu}, \zeta)$ aus lauter Einheiten 1 bestehen; es ist also insbesondere

$$\left\{\frac{\xi\varrho, \mu}{\mathfrak{q}}\right\} = \left\{\frac{\xi\varrho}{\mathfrak{q}}\right\} = 1,$$

und da $\mathfrak{q}$ ein Primideal zweiter Art sein soll, so ist auch $\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} = 1$.

Wir bezeichnen jetzt die zu $\mathfrak{q}$ konjugierten und von $\mathfrak{q}$ verschiedenen Primideale mit $\mathfrak{q}', \mathfrak{q}'', \ldots$ und diejenigen Substitutionen aus der Gruppe von $k(\zeta)$, welche $\mathfrak{q}$ in $\mathfrak{q}', \mathfrak{q}'', \ldots$ überführen, bez. mit $s', s'', \ldots$. Haben dann h, h^* die Bedeutung wie in § 149, und ist q die durch $\mathfrak{q}$ teilbare ganze rationale Primzahl, so ergibt sich (ähnlich wie in § 158) mit Rücksicht auf die Bemerkung hinter dem Satze 157 (S. 288)

$$\varkappa(s'\varkappa)(s''\varkappa)\cdots = \varepsilon^l q^{hh^*},$$

wo ε eine Einheit in $k(\zeta)$ ist. Wegen unserer Annahme über die Exponenten $u, u_1, \ldots, u_{l^*}$, und da die Primideale $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ vom ersten Grade und ferner die durch sie teilbaren rationalen Primzahlen unter sich verschieden sind, können wir aus dem Satz 152 (S. 276) schließen, daß es in $k(\zeta)$ ein Primideal $\mathfrak{r}$ gibt mit den Eigenschaften

$$\left.\begin{array}{ll} \left\{\frac{\alpha}{\mathfrak{r}}\right\} = \zeta^{*-1}, & \left\{\frac{\varkappa}{\mathfrak{r}}\right\} = \zeta^*, \\ \left\{\frac{s'\alpha}{\mathfrak{r}}\right\} = 1, & \left\{\frac{s'\varkappa}{\mathfrak{r}}\right\} = 1, \\ \left\{\frac{s''\alpha}{\mathfrak{r}}\right\} = 1, & \left\{\frac{s''\varkappa}{\mathfrak{r}}\right\} = 1, \\ \cdots\cdots\cdots & \cdots\cdots\cdots \end{array}\right\} \quad (164)$$

wo ζ^* irgendeine von 1 verschiedene l-te Einheitswurzel bedeutet. Diese Gleichungen (164) ergeben sofort

$$\left\{\frac{\mu}{\mathfrak{r}}\right\}=1,\quad \left\{\frac{s'\mu}{\mathfrak{r}}\right\}=1,\quad \left\{\frac{s''\mu}{\mathfrak{r}}\right\}=1,\ \ldots, \tag{165}$$

$$\left\{\frac{\varkappa\cdot s'\varkappa\cdot s''\varkappa\cdot\cdots}{\mathfrak{r}}\right\}=\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}=\zeta^*; \tag{166}$$

aus der ersten von den Gleichungen (165) folgt nach dem zuvor Bewiesenen $\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=1$, und in gleicher Weise liefern die weiteren Gleichungen (165) die Beziehungen $\left\{\frac{\mathfrak{r}}{\mathfrak{q}'}\right\}=1$, $\left\{\frac{\mathfrak{r}}{\mathfrak{q}''}\right\}=1,\ldots$; durch Multiplikation wird hieraus $\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=1$, was wegen Satz 140 (S. 231) der Gleichung (166) widerspricht. Unsere augenblicklich behandelte Annahme über die Exponenten $u, u_1, \ldots, u_{l^*}$ ist daher unzutreffend, d. h. diese Exponenten, wie sie oben bestimmt wurden, müssen sämtlich durch l teilbar sein, und α ist mithin gleich der l-ten Potenz einer ganzen Zahl in $k(\zeta)$; hieraus ergibt sich, daß $\varkappa$ kongruent der l-ten Potenz einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{l}^l$ ausfällt, womit der Hilfssatz 43 bewiesen ist.

§ 168. Beweis des Reziprozitätsgesetzes für die Fälle, daß eines der beiden Primideale von der zweiten Art ist.

Wir gelangen jetzt schrittweise, wie folgt, zu einzelnen Teilen des Reziprozitätsgesetzes für l-te Potenzreste:

Hilfssatz 44. Es sei $\mathfrak{q}$ ein Primideal zweiter Art und $\mathfrak{r}$ ein Primideal erster oder zweiter Art in $k(\zeta)$: wenn dann $\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}=1$ ist, so wird auch $\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=1$.

Beweis. Es seien $\varkappa, \varrho$ Primärzahlen der Primideale $\mathfrak{q}$ bez. $\mathfrak{r}$. Mit Rücksicht auf Hilfssatz 43 (S. 337) besitzt die Relativdiskriminante des Körpers $k(\sqrt[l]{\varkappa}, \zeta)$ nach Satz 148 (S. 251) nur den einen Primfaktor $\mathfrak{q}$, und daher gehören wegen des Hilfssatzes 35 (S. 312) in diesem Körper alle Ideale dem Hauptgeschlechte an. Wegen $\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}=1$ ist $\mathfrak{r}$ im Körper $k(\sqrt[l]{\varkappa}, \zeta)$ das Produkt von l Primidealen; für den Charakter irgendeines dieser Primideale erhalten wir den Wert

$$\left\{\frac{\varrho,\varkappa}{\mathfrak{q}}\right\}=\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=1,$$

und damit ist der Hilfssatz 44 bewiesen.

Hilfssatz 45. Wenn $\mathfrak{q}, \bar{\mathfrak{q}}$ irgend zwei Primideale zweiter Art in $k(\zeta)$ sind, so ist stets $\left\{\frac{\mathfrak{q}}{\bar{\mathfrak{q}}}\right\}=\left\{\frac{\bar{\mathfrak{q}}}{\mathfrak{q}}\right\}$.

Beweis. Im Falle $\left\{\frac{\mathfrak{q}}{\bar{\mathfrak{q}}}\right\}=1$ folgt die Richtigkeit der Behauptung unmittelbar aus Hilfssatz 44. Wir betrachten nunmehr den Fall $\left\{\frac{\mathfrak{q}}{\bar{\mathfrak{q}}}\right\}+1$. Es

seien $\varkappa, \bar{\varkappa}$ Primärzahlen bez. von $\mathfrak{q}, \bar{\mathfrak{q}}$; ferner seien $\mathfrak{q}', \mathfrak{q}'', \ldots$ die von $\mathfrak{q}$ verschiedenen, zu $\mathfrak{q}$ konjugierten Primideale und $\varkappa', \varkappa'', \ldots$ bez. die betreffenden zu $\varkappa$ konjugierten Primärzahlen von $\mathfrak{q}', \mathfrak{q}'', \ldots$; andererseits seien $\bar{\mathfrak{q}}', \bar{\mathfrak{q}}'', \ldots$ die von $\bar{\mathfrak{q}}$ verschiedenen, zu $\bar{\mathfrak{q}}$ konjugierten Primideale und $\bar{\varkappa}', \bar{\varkappa}'', \ldots$ bez. die betreffenden zu $\bar{\varkappa}$ konjugierten Primärzahlen von $\bar{\mathfrak{q}}', \bar{\mathfrak{q}}'', \ldots$. Endlich sei q die durch $\mathfrak{q}$ teilbare rationale Primzahl; man hat dann $\varkappa\varkappa'\varkappa''\cdots=\varepsilon^l q^{hh^*}$, wo ε eine Einheit in $k(\zeta)$ ist. Nach Satz 152 (S. 276) gibt es ein Primideal $\mathfrak{r}$, für welches

$$\left\{\frac{\varkappa}{\mathfrak{r}}\right\}=\zeta^*,\quad \left\{\frac{\varkappa'}{\mathfrak{r}}\right\}=1,\quad \left\{\frac{\varkappa''}{\mathfrak{r}}\right\}=1,\ \ldots, \tag{167}$$

$$\left\{\frac{\bar{\varkappa}}{\mathfrak{r}}\right\}=\zeta^*,\quad \left\{\frac{\bar{\varkappa}'}{\mathfrak{r}}\right\}=1,\quad \left\{\frac{\bar{\varkappa}''}{\mathfrak{r}}\right\}=1,\ \ldots, \tag{168}$$

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\}=1,\quad \left\{\frac{\varepsilon_1}{\mathfrak{r}}\right\}=1,\quad \left\{\frac{\varepsilon_2}{\mathfrak{r}}\right\}=1,\ \ldots,\ \left\{\frac{\varepsilon_{l^*}}{\mathfrak{r}}\right\}=1 \tag{169}$$

wird, wo ζ^* irgendeine von 1 verschiedene Einheitswurzel bedeutet, und wo $\varepsilon_1, \ldots, \varepsilon_{l^*}$ die l^* in § 166 bestimmten und dort mit $\varepsilon_1, \varepsilon_2', \ldots, \varepsilon_{l^*}^{(l^*-1)}$ bezeichneten Einheiten in $k(\zeta)$ sind. Aus (167) folgt

$$\left\{\frac{\varkappa\varkappa'\varkappa''\cdots}{\mathfrak{r}}\right\}=\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}=\zeta^*,$$

und daher ist, wenn ϱ eine Primärzahl von $\mathfrak{r}$ bedeutet, nach Satz 140 (S. 231) auch

$$\left\{\frac{\varrho}{\mathfrak{q}}\right\}=\left\{\frac{\varrho}{\mathfrak{q}}\right\}\left\{\frac{\varrho}{\mathfrak{q}'}\right\}\left\{\frac{\varrho}{\mathfrak{q}''}\right\}\cdots=\zeta^*. \tag{170}$$

Andererseits ist wegen (167) nach Hilfssatz 44

$$\left\{\frac{\varrho}{\mathfrak{q}'}\right\}=1,\quad \left\{\frac{\varrho}{\mathfrak{q}''}\right\}=1,\ \ldots;$$

und daher folgt aus (170) $\left\{\frac{\varrho}{\mathfrak{q}}\right\}=\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=\zeta^*$, es ist also

$$\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}=\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}+1. \tag{171}$$

In gleicher Weise leiten wir aus (168) die Beziehung her:

$$\left\{\frac{\bar{\mathfrak{q}}}{\mathfrak{r}}\right\}=\left\{\frac{\mathfrak{r}}{\bar{\mathfrak{q}}}\right\}+1. \tag{172}$$

Wir bestimmen nun die Potenz ϱ^e von ϱ so, daß $\left\{\frac{\varkappa\varrho^e}{\bar{\mathfrak{q}}}\right\}=1$ wird, und betrachten dann den Kummerschen Körper $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$. Da $\mathfrak{q}$ nach Voraussetzung und $\mathfrak{r}$ wegen (169) Primideale zweiter Art sind, so folgt vermittelst des Hilfssatzes 43, daß die Relativdiskriminante dieses Körpers nur die beiden Primideale $\mathfrak{q}, \mathfrak{r}$ enthält. Nach Hilfssatz 35 (S. 312) gibt es daher in $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$ höchstens l Geschlechter. Das Primideal $\mathfrak{r}$ ist die l-te Potenz eines Prim-

ideals $\mathfrak{R}$ in $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$. Die beiden Charaktere von $\mathfrak{R}$ in diesem Körper sind

$$\left\{\frac{\varrho, \varkappa\varrho^e}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}, \qquad \left\{\frac{\varrho, \varkappa\varrho^e}{\mathfrak{r}}\right\} = \left\{\frac{\varkappa}{\mathfrak{r}}\right\}^{-1} = \left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}^{-1},$$

und hieraus ergeben sich die Charaktere von $\mathfrak{R}^2, \mathfrak{R}^3, \ldots, \mathfrak{R}^l$. Wegen (171) bestimmen die l Ideale $\mathfrak{R}, \mathfrak{R}^2, \ldots, \mathfrak{R}^l$ l verschiedene Geschlechter, und wegen der nämlichen Formel (171) ist zugleich für dieselben stets das Produkt ihrer beiden Charaktere gleich 1. Die letztere Tatsache gilt folglich für jedes beliebige Ideal in $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$. Da $\left\{\frac{\varkappa\varrho^e}{\mathfrak{q}}\right\} = 1$ ist, so wird $\bar{\mathfrak{q}}$ in $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$ weiter zerlegbar; die Charaktere eines Primfaktors von $\bar{\mathfrak{q}}$ sind

$$\left\{\frac{\bar{\varkappa}, \varkappa\varrho^e}{\mathfrak{q}}\right\} = \left\{\frac{\bar{\varkappa}}{\mathfrak{q}}\right\}, \qquad \left\{\frac{\bar{\varkappa}, \varkappa\varrho^e}{\mathfrak{r}}\right\} = \left\{\frac{\bar{\varkappa}}{\mathfrak{r}}\right\}^e,$$

und es ist daher das Produkt $\left\{\frac{\bar{\varkappa}}{\mathfrak{q}}\right\}\left\{\frac{\bar{\varkappa}}{\mathfrak{r}}\right\}^e = 1$. Da andererseits

$$\left\{\frac{\varkappa\varrho^e}{\bar{\mathfrak{q}}}\right\} = \left\{\frac{\mathfrak{q}}{\bar{\mathfrak{q}}}\right\}\left\{\frac{\mathfrak{r}}{\bar{\mathfrak{q}}}\right\}^e = 1$$

sein soll, so folgt unter Heranziehung von (172) $\left\{\frac{\bar{\mathfrak{q}}}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\bar{\mathfrak{q}}}\right\}$.

Hilfssatz 46. Es sei $\mathfrak{p}$ ein Primideal der ersten Art und $\mathfrak{q}$ ein Primideal der zweiten Art in $k(\zeta)$; wenn dann $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1$ ausfällt, so wird auch $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = 1$.

Beweis. Es seien $\pi, \varkappa$ Primärzahlen bez. von $\mathfrak{p}, \mathfrak{q}$. Wir nehmen an, es wäre $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} \neq 1$. Nach Satz 152 (S. 276) gibt es ein von $\mathfrak{p}$ und $\mathfrak{q}$ verschiedenes Primideal $\mathfrak{r}$, für welches

$$\left\{\frac{\pi}{\mathfrak{r}}\right\} \neq 1, \quad \left\{\frac{\varkappa}{\mathfrak{r}}\right\} \neq 1, \tag{173}$$

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\} = 1, \quad \left\{\frac{\varepsilon_1}{\mathfrak{r}}\right\} = 1, \ldots, \left\{\frac{\varepsilon_{l^*}}{\mathfrak{r}}\right\} = 1 \tag{174}$$

ausfällt, wo $\varepsilon_1, \ldots, \varepsilon_{l^*}$ die in § 166 bestimmten und dort mit $\varepsilon_1, \ldots, \varepsilon_{l^*}^{(l^*-1)}$ bezeichneten Einheiten sind. Wegen (174) ist $\mathfrak{r}$ ein Primideal zweiter Art. Bedeutet ϱ eine Primärzahl von $\mathfrak{r}$, so fällt $\left\{\frac{\varrho}{\mathfrak{p}}\right\} \neq 1$ aus; denn aus $\left\{\frac{\varrho}{\mathfrak{p}}\right\} = 1$ würde nach Hilfssatz 44 (S. 340) $\left\{\frac{\pi}{\mathfrak{r}}\right\} = 1$ folgen, was der ersten Gleichung in (173) widerspräche. Wir können daher eine Potenz ϱ^e von ϱ bestimmen derart, daß $\left\{\frac{\varkappa\varrho^e}{\mathfrak{p}}\right\} = 1$ wird.

Da $\mathfrak{r}, \mathfrak{q}$ Primideale zweiter Art sind, so folgt mit Rücksicht auf Hilfssatz 43 (S. 337) nach Satz 148 (S. 251), daß die Relativdiskriminante des Körpers $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$ nur die beiden Primideale $\mathfrak{q}, \mathfrak{r}$ als Faktoren enthält. Nun ist nach (173) $\left\{\frac{\varkappa}{\mathfrak{r}}\right\} \neq 1$ und nach Hilfssatz 45 (S. 340)

$$\left\{\frac{\varkappa}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\},$$

und daraus folgt, wie im Beweise des Hilfssatzes 45, daß für jedes Ideal in $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$ das Produkt der beiden Charaktere gleich 1 sein muß. Wegen $\left\{\frac{\varkappa\varrho^e}{\mathfrak{p}}\right\} = 1$ wird $\mathfrak{p}$ in $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$ weiter zerlegbar; ein jeder Primfaktor von $\mathfrak{p}$ besitzt als seine beiden Charaktere

$$\left\{\frac{\pi, \varkappa\varrho^e}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}, \quad \left\{\frac{\pi, \varkappa\varrho^e}{\mathfrak{r}}\right\} = \left\{\frac{\pi}{\mathfrak{r}}\right\}^e.$$

Da der erste Charakter nach Voraussetzung gleich 1 ist, so würde nach dem eben Bewiesenen auch $\left\{\frac{\pi}{\mathfrak{r}}\right\} = 1$ folgen, was nach (173) nicht zutrifft. Dadurch ist unsere Annahme $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} \neq 1$ widerlegt.

Hilfssatz 47. Wenn $\mathfrak{q}$ ein Primideal zweiter Art und $\mathfrak{p}$ ein Primideal erster Art ist, so folgt stets $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = \left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}$.

Beweis. Wir verfahren genau wie im Beweise des Hilfssatzes 45, indem wir statt des Primideals $\bar{\mathfrak{q}}$ nunmehr das Primideal $\mathfrak{p}$ einsetzen und demgemäß im Verlauf des Beweises behufs Ableitung der (172) entsprechenden Beziehung statt des Hilfssatzes 44 den Hilfssatz 46 heranziehen.

§ 169. Ein Hilfssatz über das Produkt $\prod'\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$, worin $\mathfrak{w}$ alle von $\mathfrak{l}$ verschiedenen Primideale durchläuft.

Wir sind nunmehr imstande, den folgenden Hilfssatz abzuleiten:

Hilfssatz 48. Wenn ν, μ zu $\mathfrak{l}$ prime ganze Zahlen sind und überdies μ der l-ten Potenz einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{l}^l$ kongruent wird, so ist stets

$$\prod_{(\mathfrak{w})}'\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = 1,$$

wo das Produkt über alle von $\mathfrak{l}$ verschiedenen Primideale $\mathfrak{w}$ in $k(\zeta)$ erstreckt werden soll.

Beweis. Unter der über μ gemachten Voraussetzung können wir offenbar μ gleich einem Produkt aus lauter Primärzahlen von Primidealen, dividiert durch die l-te Potenz einer ganzen Zahl in $k(\zeta)$, setzen. Ist ν insbesondere gleich einer Primärzahl $\varkappa$ eines Primideals $\mathfrak{q}$ zweiter Art, so folgt alsdann die Richtigkeit der Behauptung sofort aus den Hilfssätzen 45 und 47, d. h. es ist unter der über μ gemachten Voraussetzung stets

$$\prod_{(\mathfrak{w})}'\left\{\frac{\varkappa, \mu}{\mathfrak{w}}\right\} = 1. \tag{175}$$

Nunmehr betrachten wir den Kummerschen Körper $k(\sqrt[l]{\mu}, \zeta)$. Wenn r die Anzahl der Charaktere bezeichnet, die das Geschlecht einer Klasse in diesem Körper bestimmen, so gibt es nach Hilfssatz 35 (S. 312) höchstens l^{r-1} Geschlechter in diesem Körper. Sind nun $\gamma_1, \ldots, \gamma_r$ irgend r solche l-te

Einheitswurzeln, deren Produkt gleich 1 ist, so können wir genau wie beim Beweise des Satzes 164 (S. 329) nachweisen, daß es stets Ideale in $k(\sqrt[l]{\mu}, \zeta)$ gibt, deren Charaktere mit $\gamma_1, \ldots, \gamma_r$ übereinstimmen. Dabei ist nur zu den Bedingungen (155), (156), denen das dort mit $\mathfrak{p}$ bezeichnete Primideal genügen soll, noch das Bedingungssystem

$$\left\{\frac{\zeta}{\mathfrak{p}}\right\} = 1, \quad \left\{\frac{\varepsilon_1}{\mathfrak{p}}\right\} = 1, \ldots, \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}}\right\} = 1$$

hinzuzunehmen, wo $\varepsilon_1, \ldots, \varepsilon_{l^*}$ die in § 166 bestimmten und dort mit $\varepsilon_1, \ldots, \varepsilon_{l^*}^{(l^*-1)}$ bezeichneten Einheiten sind. Auf diese Weise wird nämlich erreicht, daß $\mathfrak{p}$ obenein noch ein Primideal zweiter Art wird, und wegen dieses Umstandes dürfen wir mit Rücksicht auf die Hilfssätze 45 und 47 das Reziprozitätsgesetz in der nämlichen Weise anwenden, wie dies beim Beweise des Satzes 164 geschehen ist. Statt des dort benutzten Satzes 163 ziehen wir hier die Formel (175) heran. Zugleich folgt, daß in $k(\sqrt[l]{\mu}, \zeta)$ wirklich l^{r-1} Geschlechter vorhanden sind, und damit zugleich, daß für jedes derselben das Produkt der r Charaktere stets gleich 1 sein muß. Diese Tatsache bringen wir nun zur Anwendung, um den Hilfssatz 48 für den Fall zu beweisen, daß ν eine Einheit ist, und weiter für den Fall, daß ν eine Primärzahl eines Primideals erster Art ist.

Es seien wiederum $\varepsilon_1, \ldots, \varepsilon_{l^*}$ die soeben erwähnten l^* Einheiten; ferner $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$, wie in § 149, die t in der Relativdiskriminante von $k(\sqrt[l]{\mu}, \zeta)$ aufgehenden verschiedenen Primideale, und es mögen darunter $\mathfrak{l}_t, \mathfrak{l}_{t-1}, \ldots, \mathfrak{l}_{r+1}$ wie in § 149 ausgewählt sein; ferner seien $\lambda_{r+1}, \ldots, \lambda_t$ Primärzahlen bez. von $\mathfrak{l}_{r+1}, \ldots, \mathfrak{l}_t$; endlich sei ξ eine beliebige Einheit in $k(\zeta)$. Nach Satz 152 (S. 276) gibt es ein Primideal $\mathfrak{q}$, für welches bei einem gewissen zu l primen Exponenten m

$$\left\{\frac{\zeta}{\mathfrak{q}}\right\} = 1, \quad \left\{\frac{\varepsilon_1}{\mathfrak{q}}\right\} = 1, \ldots, \left\{\frac{\varepsilon_{l^*}}{\mathfrak{q}}\right\} = 1, \quad \left\{\frac{\mu}{\mathfrak{q}}\right\} = 1, \tag{176}$$

$$\left\{\frac{\lambda_{r+1}}{\mathfrak{q}}\right\} = \left\{\frac{\xi}{\mathfrak{l}_{r+1}}\right\}^m, \quad \left\{\frac{\lambda_{r+2}}{\mathfrak{q}}\right\} = \left\{\frac{\xi}{\mathfrak{l}_{r+2}}\right\}^m, \ldots, \left\{\frac{\lambda_t}{\mathfrak{q}}\right\} = \left\{\frac{\xi}{\mathfrak{l}_t}\right\}^m \tag{177}$$

wird. Es sei $\varkappa$ eine Primärzahl von $\mathfrak{q}$. Wegen der Gleichung $\left\{\frac{\mu}{\mathfrak{q}}\right\} = 1$ zerfällt $\mathfrak{q}$ im Körper $k(\sqrt[l]{\mu}, \zeta)$, und wegen der übrigen Gleichungen (176) ist $\mathfrak{q}$ ein Primideal zweiter Art. Die r Charaktere eines Primfaktors von $\mathfrak{q}$ haben, da, wie man aus (177) und durch die Hilfssätze 45 und 47 erkennt,

$$\left\{\frac{\xi^{-m}\varkappa, \mu}{\mathfrak{l}_{r+1}}\right\} = 1, \ldots, \left\{\frac{\xi^{-m}\varkappa, \mu}{\mathfrak{l}_t}\right\} = 1 \tag{178}$$

ist, folgende Werte:

$$\left\{\frac{\xi^{-m}\varkappa, \mu}{\mathfrak{l}_1}\right\}, \quad \left\{\frac{\xi^{-m}\varkappa, \mu}{\mathfrak{l}_2}\right\}, \ldots, \left\{\frac{\xi^{-m}\varkappa, \mu}{\mathfrak{l}_r}\right\}.$$

Nun muß nach dem oben Bewiesenen das Produkt derselben gleich 1 sein; dies liefert mit Rücksicht auf (178) und auf die letzte Gleichung in (176) die Beziehung

$$\prod_{(\mathfrak{w})}{}' \left\{\frac{\xi^{-m}\varkappa, \mu}{\mathfrak{w}}\right\} = 1,$$

wo das Produkt über alle von $\mathfrak{l}$ verschiedenen Primideale $\mathfrak{w}$ zu erstrecken ist; daraus folgt dann weiter mit Hilfe von (175)

$$\prod_{(\mathfrak{w})}{}' \left\{\frac{\xi^{-m}, \mu}{\mathfrak{w}}\right\} = 1, \quad \text{d. h.} \quad \prod_{(\mathfrak{w})}{}' \left\{\frac{\xi, \mu}{\mathfrak{w}}\right\} = 1; \tag{179}$$

der Hilfssatz 48 gilt also auch in dem Falle, daß ν eine beliebige Einheit in $k(\zeta)$ vorstellt.

Nunmehr sei $\mathfrak{p}$ irgendein Primideal der ersten Art, welches die Bedingung $\left\{\frac{\mu}{\mathfrak{p}}\right\} = 1$ erfüllt und folglich in $k(\sqrt[l]{\mu}, \zeta)$ zerlegbar ist. Die r Charaktere eines beliebigen Primfaktors von $\mathfrak{p}$ sind, wenn π eine Primärzahl von $\mathfrak{p}$ und ξ eine geeignete Einheit in $k(\zeta)$ bedeutet,

$$\left\{\frac{\xi\pi, \mu}{\mathfrak{l}_1}\right\}, \quad \left\{\frac{\xi\pi, \mu}{\mathfrak{l}_2}\right\}, \ldots, \left\{\frac{\xi\pi, \mu}{\mathfrak{l}_r}\right\}.$$

Da das Produkt derselben gleich 1 sein muß, so folgt wie vorhin:

$$\prod_{(\mathfrak{w})}{}' \left\{\frac{\xi\pi, \mu}{\mathfrak{w}}\right\} = 1$$

und hieraus wegen (179):

$$\prod_{(\mathfrak{w})}{}' \left\{\frac{\pi, \mu}{\mathfrak{w}}\right\} = 1.$$

Ist endlich $\mathfrak{p}$ ein solches, zu μ primes Primideal erster Art, für welches $\left\{\frac{\mu}{\mathfrak{p}}\right\} + 1$ ist, so bestimme man ein Primideal zweiter Art $\mathfrak{q}$ derart, daß $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} + 1$ ist; dann ist nach Hilfssatz 44 auch $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} + 1$. Bedeutet $\varkappa$ eine Primärzahl von $\mathfrak{q}$ und $\varkappa^e$ eine solche Potenz von $\varkappa$, daß $\left\{\frac{\mu\varkappa^e}{\mathfrak{p}}\right\} = 1$ wird, so ist nach dem soeben Bewiesenen

$$\prod_{(\mathfrak{w})}{}' \left\{\frac{\pi, \mu\varkappa^e}{\mathfrak{w}}\right\} = 1,$$

und da auf Grund des Hilfssatzes 47 auch

$$\prod_{(\mathfrak{w})}{}' \left\{\frac{\pi, \varkappa}{\mathfrak{w}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}^{-1} \left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1$$

ausfällt, so folgt weiter

$$\prod_{(\mathfrak{w})}{}' \left\{\frac{\pi, \mu}{\mathfrak{w}}\right\} = 1; \tag{180}$$

der Hilfssatz 48 gilt also auch dann, wenn ν eine Primärzahl eines beliebigen Primideals erster Art ist. Aus (175), (179), (180) folgt die allgemeine Gültigkeit des Hilfssatzes 48.

§ 170. Das Symbol $\{\nu, \mu\}$ und das Reziprozitätsgesetz zwischen zwei beliebigen Primidealen.

Wir gelangen jetzt in überraschend einfacher Weise zu der am Anfang dieses Kapitels in Aussicht gestellten neuen Begründung der Theorie des regulären Kummerschen Körpers. Setzen wir, wenn ν und μ ganze Zahlen in $k(\zeta)$ bedeuten,

$$\{\nu, \mu\} = \Big(\prod_{(\mathfrak{w})}{}' \Big\{\frac{\nu, \mu}{\mathfrak{w}}\Big\}\Big)^{-1}, \tag{181}$$

wo das Produkt $\prod'_{(\mathfrak{w})}$ wiederum über alle von $\mathfrak{l}$ verschiedenen Primideale $\mathfrak{w}$ in $k(\zeta)$ zu erstrecken ist, so stellt das **Symbol** $\{\nu, \mu\}$ eine l-te Einheitswurzel dar, die durch die Zahlen ν, μ völlig bestimmt ist, und es folgen aus (80) (S. 265) sofort die Formeln

$$\left.\begin{aligned} \{\nu_1\ \nu_2, \mu\} &= \{\nu_1, \mu\}\{\nu_2, \mu\}, \\ \{\nu, \mu_1\ \mu_2\} &= \{\nu, \mu_1\}\{\nu, \mu_2\}, \\ \{\nu, \mu\}\{\mu, \nu\} &= 1, \end{aligned}\right\} \tag{182}$$

in denen $\nu, \nu_1, \nu_2, \mu, \mu_1, \mu_2$ beliebige ganze Zahlen in $k(\zeta)$ bedeuten. Bezeichnet ferner r eine Primitivzahl nach l und $s = (\zeta : \zeta^r)$ die betreffende Substitution der Gruppe von $k(\zeta)$, so folgt

$$\{s\,\nu, s\,\mu\} = \{\nu, \mu\}^r. \tag{183}$$

Ferner ergibt sich die Tatsache:

Hilfssatz 49. Wenn ν, μ zwei primäre Zahlen des Körpers $k(\zeta)$ sind, so hat das Symbol $\{\nu, \mu\}$ stets den Wert 1.

Beweis. Zunächst folgt, wenn a irgendeine ganze rationale, zu l und zu ν prime Zahl ist, mit Rücksicht auf Satz 140 (S. 231) die Gleichung

$$\{\nu, a\} = \Big\{\frac{\nu}{a}\Big\}^{-1}\Big\{\frac{a}{\nu}\Big\} = 1. \tag{184}$$

Da μ eine primäre Zahl sein soll, so ist $\mu \cdot s^{\frac{l-1}{2}}\mu$ einer ganzen rationalen Zahl nach $\mathfrak{l}^{l-1}$ kongruent. Infolgedessen können wir dann auch nach $\mathfrak{l}^l$ eine ganze rationale Zahl a bestimmen, derart, daß die Kongruenz

$$a \cdot \mu \cdot s^{\frac{l-1}{2}}\mu \equiv 1, \qquad (\mathfrak{l}^l)$$

besteht, und außerdem wieder a prim zu ν wählen. Nun ergibt sich bei Anwendung des Hilfssatzes 48

$$\{\nu, a\}\{\nu, \mu\}\{\nu, s^{\frac{l-1}{2}}\mu\} = \{\nu, a \cdot \mu \cdot s^{\frac{l-1}{2}}\mu\} = 1,$$

und folglich wird wegen (184) auch

$$\{\nu, \mu\}\{\nu, s^{\frac{l-1}{2}}\mu\} = 1.$$

Entsprechend beweisen wir

$$\{\nu, s^{\frac{l-1}{2}}\mu\}\{s^{\frac{l-1}{2}}\nu, s^{\frac{l-1}{2}}\mu\} = 1.$$

Aus Formel (183) ergibt sich ferner

$$\{\nu, \mu\}\{s^{\frac{l-1}{2}}\nu, s^{\frac{l-1}{2}}\mu\} = 1.$$

Die drei letzten Gleichungen zusammengenommen liefern

$$\{\nu, \mu\}^2 = 1, \quad \text{d. h.} \quad \{\nu, \mu\} = 1,$$

und damit ist der Hilfssatz 49 bewiesen.

Wählen wir insbesondere ν, μ als Primärzahlen von zwei beliebigen Primidealen $\mathfrak{p}, \mathfrak{q}$ in $k(\zeta)$, so ist die Aussage des Hilfssatzes 49 mit dem allgemeinen Reziprozitätsgesetze 161 (S. 312) für diese Primideale $\mathfrak{p}, \mathfrak{q}$ gleichbedeutend.

§ 171. Übereinstimmung des Symbols $\{\nu, \mu\}$ mit dem Symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$.

Wir schließen aus Satz 151 (S. 272), wobei nur der Fall $\mathfrak{w} + \mathfrak{l}$ dieses Satzes zur Anwendung kommt, daß $\{\nu, \mu\}$ stets den Wert 1 besitzt, sobald ν die Relativnorm einer ganzen Zahl des Körpers $k(\sqrt[l]{\mu}, \zeta)$ ist; und endlich gelingt jetzt auch der Nachweis dafür, daß $\{\alpha, \mu\}$ stets den Wert 1 hat, sobald die ganze Zahl α Normenrest des Körpers $k(\sqrt[l]{\mu}, \zeta)$ nach $\mathfrak{l}$ ist. In der Tat, nehmen wir der Kürze wegen an, daß beide Zahlen α, μ zu $\mathfrak{l}$ prim sind, und setzen wir $\alpha \equiv N_k(\mathsf{A})$ nach $\mathfrak{l}^l$, wo $N_k(\mathsf{A})$ die Relativnorm einer ganzen Zahl A in $k(\sqrt[l]{\mu}, \zeta)$ bedeuten soll, so ist die Zahl $\alpha \cdot (N_k(\mathsf{A}))^{l-1}$ offenbar der l-ten Potenz einer ganzen Zahl nach $\mathfrak{l}^l$ kongruent; daher wird unter Benutzung der Formeln (182) sowie mit Rücksicht auf die vorausgeschickten Bemerkungen und den Hilfssatz 48:

$$\{\alpha \cdot (N_k(\mathsf{A}))^{l-1}, \mu\} = \{\alpha, \mu\}\{N_k(\mathsf{A}), \mu\}^{l-1} = \{\alpha, \mu\} = 1,$$

wie behauptet wurde. Wenn eine der Zahlen α, μ oder beide durch $\mathfrak{l}$ teilbar sind, so gelingt der Nachweis dieser Formel ebenfalls ohne Mühe vermöge der nämlichen Hilfsmittel.

Ist μ eine ganze, zu $\mathfrak{l}$ prime Zahl in $k(\zeta)$, so folgt aus (181) leicht die Gleichung

$$\{\zeta, \mu\} = \zeta^{\frac{1-n(\mu)}{l}};$$

demnach erfüllt der Ausdruck $\{\nu, \mu\}$ sämtliche Forderungen, die für das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ am Schluß des § 133 aufgestellt worden sind; es ist somit,

wenn wir die dort auf S. 274 unten angegebene Definition des Symbols $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ zugrunde legen,

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

in dieser Gleichung erkennen wir dann den Satz 163 (S. 328) wieder.

Sind insbesondere die beiden Zahlen ν, μ zu $\mathfrak{l}$ prim und $\bar{\nu}, \bar{\mu}$ ganze Zahlen in $k(\zeta)$, die mit den ersteren durch die Kongruenzen

$$\nu \equiv \bar{\nu}, \qquad \mu \equiv \bar{\mu}, \qquad (\mathfrak{l}^l)$$

verknüpft sind, so erhalten wir durch Benutzung des Hilfssatzes 48 leicht

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = \left\{\frac{\bar{\nu}, \bar{\mu}}{\mathfrak{l}}\right\}.$$

Hieraus und in Ansehung der Formeln (182) entnehmen wir folgende Tatsache: Wenn die beiden Zahlen ν, μ zu $\mathfrak{l}$ prim sind und

$$\nu \equiv a^l (1+\lambda)^{m_1} (1+\lambda^2)^{m_2} \cdots (1+\lambda^{l-1})^{m_{l-1}}, \qquad (\mathfrak{l}^l),$$
$$\mu \equiv b^l (1+\lambda)^{m_1} (1+\lambda^2)^{m_2} \cdots (1+\lambda^{l-1})^{m_{l-1}}, \qquad (\mathfrak{l}^l)$$

gesetzt wird, wo a, b und die Exponenten

$$n_1, \quad n_2, \quad \ldots, \quad n_{l-1}; \qquad m_1, \quad m_2, \quad \ldots, \quad m_{l-1}$$

ganze rationale Zahlen sind, so besteht eine Gleichung von der Gestalt

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = \zeta^{L(n_1, \ldots, n_{l-1}; m_1, \ldots, m_{l-1})};$$

dabei ist L eine homogene bilineare Funktion der beiden Reihen von Veränderlichen $n_1, \ldots, n_{l-1}; m_1, \ldots, m_{l-1}$, und die Koeffizienten von L sind ganze rationale Zahlen, die nur von der Primzahl l abhängen, und die man bei gegebenem Werte der Primzahl l etwa durch besondere Annahmen der Zahlen ν, μ leicht berechnen kann.

Nachdem nun das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ definiert und seine wichtigsten Eigenschaften abgeleitet worden sind, dürfen wir die in diesem Kapitel bisher festgehaltene Einschränkung auf Kummersche Körper mit einer zu $\mathfrak{l}$ primen Relativdiskriminante fallen lassen; es gelangen dann, genau wie oben, die Sätze 164 (S. 329), 165 (S. 331), 166 (S. 332) und vor allem der Fundamentalsatz 167 (S. 332) zum Nachweise. Mit Hilfe dieses Satzes 167 und geeigneter Benutzung des Satzes 152 (S. 276) läßt sich dann auch zeigen, daß, wenn ν, μ zwei beliebige ganze Zahlen in $k(\zeta)$ mit der Eigenschaft $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = 1$ sind und μ nicht gleich der l-ten Potenz einer ganzen Zahl in $k(\zeta)$ ausfällt, die Zahl ν stets Normenrest des Kummerschen Körpers $k(\sqrt[l]{\mu}, \zeta)$ nach $\mathfrak{l}$ sein muß. Damit ist dann der Satz 151 (S. 272) für den Fall $\mathfrak{w} = \mathfrak{l}$ nachträglich als richtig erkannt, und es folgt hieraus auch die Gültigkeit des Satzes 150 (S. 257) für $\mathfrak{w} = \mathfrak{l}$. Bei der hier dargelegten Begründungsart der Theorie des

Kummerschen Körpers erscheinen also die Sätze 150 und 151 für $\mathfrak{w} = \mathfrak{l}$ im Gegensatz zu dem früheren Aufbau als die Schlußsteine des ganzen Gebäudes.

36. Die Diophantische Gleichung $\alpha^m + \beta^m + \gamma^m = 0$.

§ 172. Die Unmöglichkeit der Diophantischen Gleichung $\alpha^l + \beta^l + \gamma^l = 0$ für reguläre Primzahlexponenten l.

Fermat hat die Behauptung aufgestellt, daß die Gleichung

$$a^m + b^m + c^m = 0$$

in ganzen rationalen, von Null verschiedenen Zahlen a, b, c für keinen ganzzahligen Exponenten $m > 2$ lösbar ist. Wenngleich schon aus der Literatur vor Kummer vereinzelte Resultate über diese Gleichung von Fermat bemerkenswert sind [Abel (*1*), Cauchy (*1, 2*), Dirichlet (*1, 2, 3*), Lamé (*1, 2, 3*), Lebesgue (*1, 2, 3*)], so ist es doch erst Kummer auf Grund der Theorie der Ideale des regulären Kreiskörpers gelungen, den Beweis der Fermatschen Behauptung für sehr umfangreiche Klassen von Exponenten m vollständig zu führen. Die wichtigste von Kummer bewiesene Tatsache ist die folgende:

Satz 168. Wenn l eine reguläre Primzahl bedeutet und α, β, γ irgendwelche ganze Zahlen des Kreiskörpers der l-ten Einheitswurzeln sind, von denen keine verschwindet, so besteht niemals die Gleichung

$$\alpha^l + \beta^l + \gamma^l = 0. \qquad (185)$$

[Kummer (*1, 9, 11*)].

Beweis. Es sei $\zeta = e^{\frac{2i\pi}{l}}$, $\lambda = 1 - \zeta$, $\mathfrak{l} = (\lambda)$. Wir nehmen im Gegensatz zu der Behauptung an, die Gleichung (185) besäße eine Lösung in ganzen Zahlen α, β, γ des Körpers $k(\zeta)$, und unterscheiden dann die zwei Fälle, daß keine der drei ganzen Zahlen α, β, γ durch $\mathfrak{l}$ teilbar ist, oder daß mindestens eine unter ihnen durch $\mathfrak{l}$ teilbar ist.

Im *ersten* Falle sind jedenfalls für den Exponenten l die Werte 3 und 5 ausgeschlossen. In der Tat, für $l = 3$ wäre jede der drei Zahlen $\alpha, \beta, \gamma \equiv \pm 1$ nach $\mathfrak{l}$ und folglich jede der drei Potenzen $\alpha^3, \beta^3, \gamma^3 \equiv \pm 1$ nach $\mathfrak{l}^3$; hieraus würde folgen, daß die Summe dieser drei Potenzen $\equiv \pm 1$ oder $\equiv \pm 3$ nach $\mathfrak{l}^3$ ausfiele, was mit dem Bestehen der Gleichung (185) nicht verträglich ist. Auf einen ähnlichen Widerspruch gelangen wir für $l = 5$, wenn wir berücksichtigen, daß in diesem Falle jede der drei Zahlen $\alpha, \beta, \gamma \equiv \pm 1, \pm 2$ nach $\mathfrak{l}$ und folglich jede der drei Potenzen $\alpha^5, \beta^5, \gamma^5 \equiv \pm 1, \pm 32$ nach $\mathfrak{l}^5$ sein müßte.

Es sei also $l \geqq 7$. Gilt die Gleichung (185) für die drei Zahlen α, β, γ, so ist offenbar auch $\alpha^{*l} + \beta^{*l} + \gamma^{*l} = 0$, wenn $\alpha^*, \beta^*, \gamma^*$ bezüglich die Produkte von α, β, γ mit irgendwelchen l-ten Einheitswurzeln bedeuten. Wegen dieses Umstandes dürfen wir von vornherein annehmen, daß die drei der

Gleichung (185) genügenden Zahlen α, β, γ semiprimär sind. Wir bringen nun die Gleichung (185) in die Gestalt

$$(\alpha+\beta)(\alpha+\zeta\beta)(\alpha+\zeta^2\beta)\cdots(\alpha+\zeta^{l-1}\beta) = -\gamma^l. \qquad (186)$$

Würden hier zwei der l Faktoren linker Hand, z. B. $\alpha+\zeta^u\beta$ und $\alpha+\zeta^{u+v}\beta$, einen Faktor gemein haben, so müßte dieser auch in $(\zeta^v-1)\alpha$ und in $(1-\zeta^v)\beta$ aufgehen, und da $\frac{1-\zeta^v}{1-\zeta}$ eine Einheit ist und $\mathfrak{l}$ nicht in γ aufgeht, so müßte dieser gemeinsame Faktor notwendig ein gemeinsamer Faktor der Zahlen α und β sein. Da jeder Primfaktor, der nur in *einem* der l Faktoren linker Hand von (186) aufgeht, wegen eben dieser Gleichung offenbar zu einem durch l teilbaren Exponenten darin vorkommen muß, so folgt, daß die l Faktoren der linken Seite von (186) die folgende Zerlegung gestatten:

$$\begin{aligned}
\alpha+\beta &= \mathfrak{j}^l\mathfrak{a},\\
\alpha+\zeta\beta &= \mathfrak{j}_1^l\mathfrak{a},\\
\alpha+\zeta^2\beta &= \mathfrak{j}_2^l\mathfrak{a},\\
&\cdots\cdots\cdots\\
\alpha+\zeta^{l-1}\beta &= \mathfrak{j}_{l-1}^l\mathfrak{a};
\end{aligned}$$

darin bedeutet $\mathfrak{a}$ den größten gemeinsamen Idealteiler der Zahlen α, β, und $\mathfrak{j}, \mathfrak{j}_1, \mathfrak{j}_2, \ldots, \mathfrak{j}_{l-1}$ sind gewisse Ideale in $k(\zeta)$. Da insbesondere $\alpha+\zeta^{l-1}\beta$ zu $\mathfrak{l}$ prim ist, so können wir eine l-te Einheitswurzel ζ^* bestimmen derart, daß $\zeta^*(\alpha+\zeta^{l-1}\beta)$ semiprimär wird; wir setzen

$$\mu = \frac{\alpha}{\zeta^*(\alpha+\zeta^{l-1}\beta)}, \qquad \varrho = \frac{\beta}{\zeta^*(\alpha+\zeta^{l-1}\beta)}.$$

Es ergibt sich dann

$$\left.\begin{aligned}
\mu+\varrho &= \left(\frac{\mathfrak{i}}{\mathfrak{j}_{l-1}}\right)^l,\\
\mu+\zeta\varrho &= \left(\frac{\mathfrak{i}_1}{\mathfrak{j}_{l-1}}\right)^l,\\
&\cdots\cdots\cdots\\
\mu+\zeta^{l-2}\varrho &= \left(\frac{\mathfrak{j}_{l-2}}{\mathfrak{j}_{l-1}}\right)^l,
\end{aligned}\right| \qquad (187)$$

d. h. es ist

$$\left(\frac{\mathfrak{i}}{\mathfrak{j}_{l-1}}\right)^l \sim 1, \quad \left(\frac{\mathfrak{i}_1}{\mathfrak{j}_{l-1}}\right)^l \sim 1, \ \ldots, \ \left(\frac{\mathfrak{j}_{l-2}}{\mathfrak{j}_{l-1}}\right)^l \sim 1,$$

und ferner wird

$$\mu+\zeta^{l-1}\varrho = \zeta^{s-1}. \qquad (188)$$

Bedeutet h die Anzahl der Idealklassen in $k(\zeta)$, so ist andererseits

$$\left(\frac{\mathfrak{i}}{\mathfrak{j}_{l-1}}\right)^h \sim 1, \quad \left(\frac{\mathfrak{i}_1}{\mathfrak{j}_{l-1}}\right)^h \sim 1, \ \ldots, \ \left(\frac{\mathfrak{j}_{l-2}}{\mathfrak{j}_{l-1}}\right)^h \sim 1,$$

und da h zu l prim ist, so folgt hieraus weiter

$$\frac{\mathfrak{i}}{\mathfrak{j}_{l-1}} \sim 1, \quad \frac{\mathfrak{i}_1}{\mathfrak{j}_{l-1}} \sim 1, \ \ldots, \ \frac{\mathfrak{j}_{l-2}}{\mathfrak{j}_{l-1}} \sim 1.$$

Die Gleichungen (187) können infolgedessen und mit Rücksicht auf Satz 127 (S. 204) in der Gestalt

$$\mu+\zeta^u\varrho = \zeta^{e_u}\varepsilon_u\alpha_u^l, \qquad (u=0,1,2,\ldots,l-2) \qquad (189)$$

geschrieben werden, wo die e_u gewisse ganzzahlige Exponenten, die ε_u geeignete *reelle* Einheiten des Kreiskörpers $k(\zeta)$ und die α_u gewisse ganze oder gebrochene Zahlen mit zu $\mathfrak{l}$ primen Zählern und Nennern in $k(\zeta)$ bedeuten. Da die l-te Potenz der Zahl α_u jedesmal kongruent einer gewissen ganzen rationalen Zahl a_u nach $\mathfrak{l}^l$ ist, so erhalten wir aus den Gleichungen (189) die Kongruenzen

$$\mu+\zeta^u\varrho \equiv \zeta^{e_u}\varepsilon_u a_u, \qquad (\mathfrak{l}^l), \quad (u=0,1,2,\ldots,l-2). \qquad (190)$$

Auf diese Kongruenzen wenden wir die Substitution $(\zeta:\zeta^{-1})$ an und bezeichnen die bei dieser Substitution aus μ und ϱ hervorgehenden Zahlen mit μ' und ϱ'; dann entsteht

$$\mu'+\zeta^{-u}\varrho' \equiv \zeta^{-e_u}\varepsilon_u a_u, \qquad (\mathfrak{l}^l), \quad (u=0,1,2,\ldots,l-2). \qquad (191)$$

Aus (190) und (191) folgt

$$\mu+\zeta^u\varrho \equiv \zeta^{2e_u}\mu'+\zeta^{2e_u-u}\varrho', \quad (\mathfrak{l}^l), \quad (u=0,1,2,\ldots,l-2). \qquad (192)$$

Setzen wir $\mu \equiv m$, $\varrho \equiv r$ nach $\mathfrak{l}^2$, wo m und r ganze rationale Zahlen bedeuten sollen, so folgt aus (192)

$$m+\zeta^u r \equiv \zeta^{2e_u}m+\zeta^{2e_u-u}r, \qquad (\mathfrak{l}^2), \qquad (193)$$

und wegen der allgemeinen Beziehung $\zeta^g \equiv 1-g\lambda$ nach $\mathfrak{l}^2$ liefert (193) die Kongruenz:

$$2e_u(m+r) \equiv 2ru, \qquad (l).$$

Andererseits folgt aus der Gleichung (188) $m+r \equiv 1$ nach l, und daher haben wir

$$e_u \equiv ru, \qquad (l), \quad (u=0,1,2,\ldots,l-2).$$

Nehmen wir nun unter Berücksichtigung dieser Beziehung speziell die Kongruenzen (192) für $u=0,1,2,3$, so folgt aus diesen durch Elimination der Zahlen $\mu, \varrho, \mu', \varrho'$ notwendig

$$\begin{vmatrix}
1, & 1, & 1, & 1\\
1, & \zeta, & \zeta^{2r}, & \zeta^{2r-1}\\
1, & (\zeta)^2, & (\zeta^{2r})^2, & (\zeta^{2r-1})^2\\
1, & (\zeta)^3, & (\zeta^{2r})^3, & (\zeta^{2r-1})^3
\end{vmatrix} \equiv 0, \qquad (\mathfrak{l}^l),$$

d. i.

$$(1-\zeta)(1-\zeta^{2r})(1-\zeta^{2r-1})(\zeta-\zeta^{2r})(\zeta-\zeta^{2r-1})(\zeta^{2r}-\zeta^{2r-1}) \equiv 0, \quad (\mathfrak{l}^l). \qquad (194)$$

Hier ist auf der linken Seite keiner der Faktoren gleich 0, denn sonst müßte entweder $r \equiv 0$ oder $r \equiv 1$ oder $r \equiv \frac{1}{2}$ nach l sein. Wäre $r \equiv 0$ nach l, so

würde $\beta \equiv 0$ nach $\mathfrak{l}$ folgen; wäre $r \equiv 1$ nach l, so würde $\varrho \equiv 1$ nach $\mathfrak{l}$, d. h. $\beta \equiv \alpha + \beta$ oder $\alpha \equiv 0$ nach $\mathfrak{l}$ folgen; beides läuft unserer Annahme über die Zahlen α, β, γ zuwider. Wäre $r \equiv \frac{1}{2}$ nach l, so würde $\varrho \equiv \frac{1}{2}$ nach $\mathfrak{l}$, d. h. $2\beta \equiv \alpha + \beta$ oder $\alpha \equiv \beta$ nach $\mathfrak{l}$ folgen. Da aber α, β, γ in der Gleichung (185) symmetrisch auftreten, so würde die gleiche Schlußweise auch zu der Kongruenz $\alpha \equiv \gamma$ nach $\mathfrak{l}$ führen, und dann wäre $\alpha^l + \beta^l + \gamma^l \equiv 3\alpha \equiv 0$, d. h. $\alpha \equiv 0$ nach $\mathfrak{l}$, was wiederum unserer Annahme über α, β, γ widerspricht. Jeder Faktor auf der linken Seite der Kongruenz (194) ist demnach durch $\mathfrak{l}$, aber nicht durch $\mathfrak{l}^2$ teilbar, daher ist mit Rücksicht auf die Annahme $l \geq 7$ diese Kongruenz (194) unmöglich.

Wir nehmen nunmehr *zweitens* an, es sei in der Gleichung (185) eine der drei Zahlen α, β, γ, etwa γ, durch $\mathfrak{l}$ teilbar, und zwar gehe in γ genau die m-te Potenz von $\mathfrak{l}$ auf. Wird dann γ durch $\lambda^m \delta$ ersetzt, so daß δ eine zu $\mathfrak{l}$ prime ganze Zahl in $k(\zeta)$ bedeutet, so ist die aus (185) entstehende Gleichung von der Gestalt

$$\alpha^l + \beta^l = \varepsilon \lambda^{lm} \delta^l; \tag{195}$$

hierin ist $\varepsilon = -1$. Es soll jetzt gezeigt werden, daß überhaupt eine Gleichung von dieser Gestalt (195) nicht möglich ist, wenn in derselben α, β, δ zu $\mathfrak{l}$ prime ganze Zahlen und ε irgendeine Einheit des Kreiskörpers $k(\zeta)$ sein sollen. Zu dem Zwecke nehmen wir wiederum die Zahlen α, β semiprimär an und bedenken dann zunächst, daß α^l, β^l ganzen rationalen Zahlen nach $\mathfrak{l}^{l+1}$ kongruent werden und daher wegen (195) auch $\varepsilon\lambda^{ml}\delta^l$ einer ganzen rationalen Zahl nach $\mathfrak{l}^{l+1}$ kongruent sein muß; infolgedessen ist notwendig $m > 1$. Ferner erkennen wir durch eine ähnliche Überlegung wie in dem vorher behandelten Falle und in Berücksichtigung des Umstandes, daß $\alpha + \beta$ semiprimär ist, die Gültigkeit der folgenden Gleichungen:

$$\left.\begin{aligned} \alpha + \beta &= \lambda^{l(m-1)+1} \mathfrak{j}^l \mathfrak{a}, \\ \alpha + \zeta\beta &= \lambda \mathfrak{j}_1^l \mathfrak{a}, \\ &\cdots\cdots\cdots\cdots \\ \alpha + \zeta^{l-1}\beta &= \lambda \mathfrak{j}_{l-1}^l \mathfrak{a}, \end{aligned}\right\} \tag{196}$$

wo $\mathfrak{j}, \mathfrak{j}_1, \ldots, \mathfrak{j}_{l-1}, \mathfrak{a}$ zu $\mathfrak{l}$ prime Ideale in $k(\zeta)$ sind. Ist insbesondere $l = 3$, so fällt die Klassenanzahl h des Körpers $k(\zeta)$ gleich 1 aus, und es ist daher jedes Ideal in $k(\zeta)$ ein Hauptideal. Setzen wir in diesem Falle $\mathfrak{a} = (\varkappa)$, wo $\varkappa$ eine ganze Zahl in $k(\zeta)$ bedeute, und dann

$$\mu = \frac{\alpha}{\varkappa}, \qquad \varrho = \frac{\beta}{\varkappa},$$

so gehen die Gleichungen (196) über in

$$\left.\begin{aligned} \mu + \varrho &= \lambda^{3(m-1)+1} \mathfrak{j}^3, \\ \mu + \zeta\varrho &= \lambda \mathfrak{j}_1^3, \\ \mu + \zeta^2\varrho &= \lambda \mathfrak{j}_2^3. \end{aligned}\right\} \tag{197}$$

Im Falle $l > 3$ bilden wir die Zahlen

$$\mu = \frac{\alpha\lambda}{\alpha + \zeta^{l-1}\beta}, \qquad \varrho = \frac{\beta\lambda}{\alpha + \zeta^{l-1}\beta};$$

dieselben lassen sich auch in der Gestalt von Brüchen schreiben, deren Zähler und Nenner zu $\mathfrak{l}$ prim sind. Aus den drei ersten und der letzten der Gleichungen (196) entnehmen wir die Gleichungen

$$\left.\begin{aligned} \mu + \varrho &= \lambda^{l(m-1)+1} \left(\frac{\mathfrak{j}}{\mathfrak{j}_{l-1}}\right)^l, \\ \mu + \zeta\varrho &= \lambda \left(\frac{\mathfrak{j}_1}{\mathfrak{j}_{l-1}}\right)^l, \\ \mu + \zeta^2\varrho &= \lambda \left(\frac{\mathfrak{j}_2}{\mathfrak{j}_{l-1}}\right)^l. \end{aligned}\right\} \tag{198}$$

Wie in dem zuerst behandelten Falle schließen wir hieraus wiederum

$$\frac{\mathfrak{j}}{\mathfrak{j}_{l-1}} \sim 1, \quad \frac{\mathfrak{j}_1}{\mathfrak{j}_{l-1}} \sim 1, \quad \frac{\mathfrak{j}_2}{\mathfrak{j}_{l-1}} \sim 1,$$

und infolgedessen können wir die Gleichungen (198) in der Gestalt

$$\left.\begin{aligned} \mu + \varrho &= \frac{\varepsilon^* \lambda^{l(m-1)+1} \gamma^{*l}}{\nu}, \\ \mu + \zeta\varrho &= \frac{\lambda \alpha^{*l}}{\nu}, \\ \mu + \zeta^2\varrho &= \frac{\varepsilon\lambda \beta^{*l}}{\nu} \end{aligned}\right\} \tag{199}$$

schreiben, so daß $\nu, \alpha^*, \beta^*, \gamma^*$ ganze, zu $\mathfrak{l}$ prime Zahlen und ε und ε^* Einheiten in $k(\zeta)$ bedeuten. Wegen (197) besteht ein Gleichungssystem wie (199) auch für $l = 3$. Durch Elimination von μ, ϱ folgt daher für $l = 3$ sowie für $l > 3$ eine Gleichung von der Gestalt:

$$\alpha^{*l} + \eta\beta^{*l} = \eta^* \lambda^{l(m-1)} \gamma^{*l}, \tag{200}$$

wo η und $\eta^*\left(= -\frac{(1-\zeta)}{(1-\zeta^2)}\varepsilon \text{ und } = \frac{\zeta(1-\zeta)}{(1-\zeta^2)}\varepsilon^*\right)$ Einheiten in $k(\zeta)$ sind. Da α^{*l}, β^{*l} ganzen rationalen Zahlen nach $\mathfrak{l}^l$ kongruent sind und, wie vorhin bewiesen, $m > 1$ ausfällt, so folgt in Anbetracht dieser Gleichung (200), daß auch η einer ganzen rationalen Zahl nach $\mathfrak{l}^l$ kongruent sein muß, und daher ist nach Satz 156 (S. 287) η die l-te Potenz einer Einheit in $k(\zeta)$. Schreiben wir nun in der Gleichung (200) $\beta^*\eta^{-\frac{1}{l}}$ an Stelle von β^*, so nimmt diese Gleichung die Gestalt von (195) an, nur daß der Exponent m jetzt um 1 kleiner geworden ist. Die wiederholte Anwendung des nämlichen Verfahrens auf die Gleichung (200) würde notwendig zu einer Gleichung von der Form (195) mit $m = 1$ und dadurch auf einen Widerspruch führen. Damit ist der Satz 168 vollständig bewiesen.

§ 173. Weitere Untersuchungen über die Unmöglichkeit der Diophantischen Gleichung $\alpha^m + \beta^m + \gamma^m = 0$.

Der Beweis der Unlösbarkeit der Gleichung $\alpha^l + \beta^l + \gamma^l = 0$ in ganzen Zahlen α, β, γ des Kreiskörpers der l-ten Einheitswurzeln ist von KUMMER noch in dem Falle erbracht worden, daß l eine Primzahl ist, die in der Klassenanzahl h des Kreiskörpers $k\left(e^{\frac{2i\pi}{l}}\right)$ zur ersten, aber nicht zu einer höheren Potenz aufgeht, wenn außerdem die Einheiten noch gewisse Bedingungen erfüllen [KUMMER (*16*)]. Unter Berücksichtigung der Bemerkung auf S. 285 läßt sich insbesondere zeigen, daß die Fermatsche Behauptung für jeden Exponenten $m \leqq 100$ richtig ist. Die Aufgabe, die Fermatsche Behauptung allgemein als richtig zu erweisen, harrt jedoch noch ihrer Lösung.

Es bleibt noch übrig, die Gleichung $\alpha^m + \beta^m + \gamma^m = 0$ für den Fall zu behandeln, daß der Exponent m eine Potenz von 2 ist. Die Gleichung $a^2 + b^2 = c^2$ besitzt bekanntlich unendlich viele Lösungen in ganzen rationalen Zahlen a, b, c. Weiter gilt jedoch der Satz:

Satz 169. Wenn α, β, γ ganze Zahlen des durch $i = \sqrt{-1}$ bestimmten quadratischen Körpers sind, von denen keine verschwindet, so gilt niemals die Gleichung

$$\alpha^4 + \beta^4 = \gamma^2. \tag{201}$$

Beweis. Wir nehmen im Gegenteil an, daß es drei solche ganze Zahlen α, β, γ gebe, welche diese Gleichung erfüllen. Es werde $\lambda = 1 + i$ und $\mathfrak{l} = (\lambda)$ gesetzt. Zunächst sehen wir dann leicht ein, daß notwendig eine der beiden Zahlen α, β durch λ teilbar sein muß. In der Tat, nehmen wir an, daß α und β prim zu λ wären, und berücksichtigen wir, daß eine zu λ prime ganze Zahl in $k(i)$ stets $\equiv 1$ oder i nach $\mathfrak{l}^2$, ihre zweite Potenz dann $\equiv \pm 1$ nach $\mathfrak{l}^4$ und ihre vierte notwendig $\equiv 1$ nach $\mathfrak{l}^6$ sein muß, so folgt $\alpha^4 + \beta^4 \equiv 2$ nach $\mathfrak{l}^6$. Hiernach müßte γ notwendig durch $\mathfrak{l}$ und durch keine höhere Potenz von $\mathfrak{l}$ teilbar sein. Setzen wir aber dementsprechend $\gamma = \lambda + \lambda^2\gamma'$, wo γ' wiederum eine ganze Zahl in $k(i)$ bedeute, so finden wir $\gamma^2 \equiv 2i$ nach $\mathfrak{l}^4$ und daher stets $\gamma^2 \not\equiv \alpha^4 + \beta^4$ nach $\mathfrak{l}^4$, womit unsere Annahme widerlegt ist. Der Fall, daß beide Zahlen α und β durch $\mathfrak{l}$ teilbar sind, kann offenbar sofort ausgeschlossen werden, da dann γ durch $\mathfrak{l}^2$ teilbar und somit das Fortheben der Potenz λ^4 auf beiden Seiten der Gleichung (201) möglich wäre.

Es bleibt also nur die Annahme übrig, daß die eine der Zahlen α, β, etwa die Zahl α, durch $\mathfrak{l}$ teilbar, die Zahlen β und γ dann aber zu $\mathfrak{l}$ prim sind. Wir setzen demgemäß $\alpha = \lambda^m\alpha^*$, wo α^* eine zu λ prime Zahl bedeute, und legen dann unserer Betrachtung sogleich die allgemeinere Gleichung

$$\beta^4 - \gamma^2 = \varepsilon\,\lambda^{4m}\alpha^{*4} \tag{202}$$

zugrunde, wo ε eine beliebige Einheit in $k(i)$ bedeute. Wir entnehmen aus

dieser Gleichung (202), indem wir nötigenfalls γ mit $-\gamma$ vertauschen, zwei Gleichungen von der Gestalt:

$$\left.\begin{aligned} \beta^2 + \gamma &= \eta\,\lambda^{4m-2}\alpha'^4, \\ \beta^2 - \gamma &= \vartheta\,\lambda^2\beta'^4, \end{aligned}\right\} \tag{203}$$

wobei η, ϑ Einheiten und α', β' ganze, zu $\mathfrak{l}$ prime Zahlen in $k(i)$ bedeuten. Wenn man die beiden Gleichungen (203) addiert und das Resultat durch $\vartheta\lambda^2$ dividiert, so entsteht eine Gleichung

$$\beta'^4 - \vartheta'\beta^2 = \eta'\lambda^{4m-4}\alpha'^4, \tag{204}$$

wo ϑ', η' Einheiten in $k(i)$ sind. Im Falle $m = 1$ wäre diese Gleichung sicher unmöglich, weil die Zahlen $\beta', \vartheta', \beta, \eta', \alpha'$ sämtlich $\equiv 1$ nach $\mathfrak{l}$ ausfallen. Es ist daher notwendig $m > 1$. Dann aber folgt aus dieser Gleichung (204), wenn sie als Kongruenz nach $\mathfrak{l}^2$ aufgefaßt wird, zunächst $\vartheta' \equiv 1$ nach $\mathfrak{l}^2$; es ist daher $\vartheta' = \pm 1$. Setzen wir, je nachdem hier das positive oder das negative Vorzeichen gilt, $\beta = \gamma'$ bez. $\beta = i\gamma'$, so nimmt die Gleichung (204) die Gestalt der Gleichung (202) an, nur daß jetzt m einen um 1 kleineren Wert hat. Die gehörige Wiederholung des angegebenen Verfahrens führt auf einen Widerspruch.

Aus der Fermatschen Behauptung für den Fall $l = 3$ läßt sich sofort die Tatsache ableiten, daß es keine andere kubische Gleichung mit rationalen Koeffizienten gibt, deren Diskriminante gleich 1 ist, außer den zwei folgenden:

$$x^3 - x \pm \tfrac{1}{3} = 0$$

und denjenigen, die durch die Transformation $x = x' + a$, wo a eine rationale Zahl ist, aus jenen Gleichungen hervorgehen [KRONECKER (*8*)].

Die allgemeine Fermatsche Behauptung läßt sich nach HURWITZ in der Fassung aussprechen, daß der Ausdruck $\sqrt[m]{1 - x^m}$ für eine positive, echt gebrochene rationale Zahl x und einen ganzen rationalen Exponenten $m > 2$ stets eine irrationale Zahl darstellt.

Literaturverzeichnis.

(Die hinter jeder einzelnen Abhandlung in eckiger Klammer beigefügten Zahlen bezeichnen die Seiten des Berichtes, auf denen die Abhandlung genannt ist.)

Abel, N. H. (*1*): Extraits de quelques lettres à Holmboe. Werke **2**, 254. [349]

Arndt, F. (*1*): Bemerkungen über die Verwandlung der irrationalen Quadratwurzel in einen Kettenbruch. J. Math. **31** (1846). [161]

Bachmann, P. (*1*): Zur Theorie der komplexen Zahlen. J. Math. **67** (1867). [191, 248]; (*2*): Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie. Leipzig **1872**. [202]; (*3*): Ergänzung einer Untersuchung von Dirichlet. Math. Ann. **16** (1880) [191]

Berkenbusch, H. (*1*): Über die aus den 8-ten Wurzeln der Einheit entspringenden Zahlen. Inauguraldissertation. Marburg 1891. [227]

Cauchy, A. L. (*1*): Mémoire sur la théorie des nombres. Comptes Rendus **1840** [245, 349]; (*2*): Mémoire sur diverses propositions relatives à la théorie des nombres. (Drei Noten.) Comptes Rendus **1847**. [349]

Cayley, A. (*1*): Tables des formes quadratiques binaires pour les déterminants négatifs depuis $D = -1$ jusqu'à $D = -100$, pour les déterminants positifs non carrés depuis $D = 2$ jusqu'à $D = 99$ et pour les treize déterminants négatifs irréguliers qui se trouvent dans le premier millier. Werke **5**, 141 (1862). [161]

Dedekind, R. (*1*): Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet, 2. bis 4. Aufl. Braunschweig 1871—1894. Supplement **11** [69, 71, 73, 75, 83, 102, 110, 111, 112, 113, 117, 119, 120, 121, 128, 157, 160, 187, 192, 196, 237, 240] und Supplement **7** [202]; (*2*): Sur la théorie des nombres entiers algébriques. Paris 1877. Abdruck aus Bull. des sciences math. et astron. s. 1 t. XI und s. 2 t. I. [69]; (*3*): Über die Anzahl der Idealklassen in den verschiedenen Ordnungen eines endlichen Körpers. Braunschweig 1877. [122, 128, 192]; (*4*): Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. Abh. K. Ges. Wiss. Göttingen **1878**. [92]; (*5*): Sur la théorie des nombres complexes idéaux. Comptes rendus **90** (1880). [201]; (*6*): Über die Diskriminanten endlicher Körper. Abh. K. Ges. Wiss. Göttingen **1882**. [83, 85, 123, 128]; (*7*): Über einen arithmetischen Satz von Gauss. Mitt. dtsch. math. Ges. Prag **1892** und: Über die Begründung der Idealtheorie. Nachr. K. Ges. Wiss. Göttingen **1895**. [76]; (*8*): Zur Theorie der Ideale. Nachr. K. Ges. Wiss. Göttingen **1894**. [146]; (*9*): Über eine Erweiterung des Symbols (a, b) in der Theorie der Moduln. Nachr. K. Ges. Wiss. Göttingen **1895**. [128] — (*3*) bis (*6*) siehe auch Dedekind, gesammelte Werke I, Braunschweig (1930); (*7*) bis (*9*) Werke II, (1931).

Lejeune Dirichlet, G. (*1*): Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré. Werke **1**, 1 (1825). [349]; (*2*): Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré. Werke **1**, 21 (1825), (1828). [349]; (*3*): Démonstration du théorème de Fermat pour le cas des 14ièmes puissances.

Werke **1**, 189 (1832). [349]; (*4*): Einige neue Sätze über unbestimmte Gleichungen. Werke **1**, 219 (1834). [161]; (*5*): Beweis eines Satzes über die arithmetische Progression. Werke **1**, 307 (1837). [240]; (*6*): Beweis des Satzes, daß jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Faktor sind, unendlich viele Primzahlen enthält. Werke **1**, 313 (1837). [240]; (*7*): Sur la manière de résoudre l'équation $t^2 - pu^2 = 1$ au moyen des fonctions circulaires. Werke **1**, 343. [112, 243]; (*8*): Sur l'usage des séries infinies dans la théorie des nombres. Werke **1**, 357 (1838). [112, 181, 182, 189]; (*9*): Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres. Werke **1**, 411 (1839), (1840). [181, 182, 189]; (*10*): Untersuchungen über die Theorie der komplexen Zahlen. Werke **1**, 503 (1841). [191]; (*11*): Untersuchungen über die Theorie der komplexen Zahlen. Werke **1**, 509 (1841). [191]; (*12*): Recherches sur les formes quadratiques à coefficients et à indéterminées complexes. Werke **1**, 533 (1842). [191]; (*13*): Sur la théorie des nombres. Werke **1**, 619 (1840). [102]; (*14*): Einige Resultate von Untersuchungen über eine Klasse homogener Funktionen des dritten und der höheren Grade. Werke **1**, 625 (1841). [102]; (*15*): Sur un théorème relatif aux séries. J. Math. **53** (1857). [116]; (*16*): Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen. Werke **1**, 633 (1842) und: Zur Theorie der komplexen Einheiten. Werke **1**, 639 (1846). [102]

Eisenstein, G. (*1*): Über eine neue Gattung zahlentheoretischer Funktionen. Ber. K. Akad. Wiss. Berlin **1850**. [327]; (*2*): Beweis der allgemeinsten Reziprozitätsgesetze zwischen reellen und komplexen Zahlen. Ber. K. Akad. Wiss. Berlin **1850**. [231]; (*3*): Über die Anzahl der quadratischen Formen, welche in der Theorie der komplexen Zahlen zu einer reellen Determinante gehören. J. Math. **27** (1844). [191]; (*4*): Beiträge zur Kreisteilung. J. Math. **27** (1844). [245]; (*5*): Beweis des Reziprozitätsgesetzes für die kubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten komplexen Zahlen. J. Math. **27** (1844). [327]; (*6*): Über die Anzahl der quadratischen Formen in den verschiedenen komplexen Theorien. J. Math. **27** (1844). [191]; (*7*): Nachtrag zum kubischen Reziprozitätssatze für die aus dritten Wurzeln der Einheit zusammengesetzten komplexen Zahlen. Kriterien des kubischen Charakters der Zahl 3 und ihrer Teiler. J. Math. **28** (1844). [327]; (*8*): Loi de reciprocité. Nouvelle démonstration du théorème fondamental sur les résidus quadratiques dans la théorie des nombres complexes. Démonstration du théorème fondamental sur les résidus biquadratiques qui comprend comme cas particulier le théorème fondamental. J. Math. **28** (1844). [327]; (*9*): Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste. J. Math. **28** (1844). [327]; (*10*): Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreisteilung ihre Entstehung verdanken. J. Math. **28** u. **29** (1844), (1845). [227, 248]; (*11*): Zur Theorie der quadratischen Zerfällung der Primzahlen $8n + 3$, $7n + 2$ und $7n + 4$. J. Math. **37** (1848). [246]; (*12*): Über ein einfaches Mittel zur Auffindung der höheren Reziprozitätsgesetze und der mit ihnen zu verbindenden Ergänzungssätze. J. Math. **39** (1850). [327]

Frobenius, G. (*1*): Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. Ber. K. Akad. Wiss. Berlin **1896**. [143]

Fuchs, L. (*1*): Über die Perioden, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist. J. Math. **61** (1862). [227]; (*2*): Über die aus Einheitswurzeln gebildeten komplexen Zahlen von periodischem Verhalten, insbesondere die Bestimmung der Klassenanzahl derselben. J. Math. **65** (1864). [227]

Gauss, C. F. (*1*): Disquisitiones arithmeticae. Werke **1** (1801). [161, 168, 169, 175, 180]; (*2*): Summatio quarundam serierum singularium. Werke **2**, 11. [247]; (*3*): Theoria residuorum biquadraticorum, commentatio prima et secunda. Werke **2**, 65 u. 93. [327]

Gmeiner, J. A. (*1*): Die Ergänzungssätze zum bikubischen Reziprozitätsgesetze. Ber. K. Akad. Wiss. Wien **1891**. [327]; (*2*): Das allgemeine bikubische Reziprozitätsgesetz. Ber. Akad. Wiss. Wien **1892**. [327]; (*3*): Die bikubische Reziprozität zwischen einer reellen und einer zweigliedrigen regulären Zahl. Monatsh. Math. Phys. **3** (1892). [327]

Hensel, K. (*1*): Arithmetische Untersuchungen über Diskriminanten und ihre außerwesentlichen Teiler. Inaugural-Dissert. Berlin **1884**. [91, 92]; (*2*): Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor. J. Math. **101** u. **103** (1887), (1888). [91, 92]; (*3*): Über Gattungen, welche durch Komposition aus zwei anderen Gattungen entstehen. J. Math. **105** (1889). [146]; (*4*): Untersuchung der Fundamentalgleichung einer Gattung für eine reelle Primzahl als Modul und Bestimmung der Teiler ihrer Diskriminante. J. Math. **113** (1894). [85, 90]; (*5*): Arithmetische Untersuchungen über die gemeinsamen außerwesentlichen Diskriminantenteiler einer Gattung. J. Math. **113** (1894). [91, 92]

Hermite, Ch. (*1*): Sur la théorie des formes quadratiques ternaires indéfinies. J. Math. **47** (1854). [100]; (*2*): Extrait d'une lettre de M. Ch. Hermite à M. Borchardt sur le nombre limité d'irrationalités aux quelles se réduisent les racines des équations à coefficients entiers complexes d'un degré et d'un discriminant donnés. J. Math. **53** (1857). [100]

Hilbert, D. (*2*): Zwei neue Beweise für die Zerlegbarkeit der Zahlen eines Körpers in Primideale. Jber. Dtsch. Mathem.-Verein. **3** (1893). [79, 129]; (*3*): Über die Zerlegung der Ideale eines Zahlkörpers in Primideale. Math. Ann. **44** (1894). [79, 129, 131]; (*4*): Grundzüge einer Theorie des Galoisschen Zahlkörpers. Nachr. K. Ges. Wiss. Göttingen **1894**. [95, 131]; (*5*): Über den Dirichletschen biquadratischen Zahlkörper. Math. Ann. **45** (1894). [191, 192]; (*6*): Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper. Nachr. K. Ges. Wiss. Göttingen **1896**. [206]

Hurwitz, A. (*1*): Über die Theorie der Ideale. Nachr. K. Ges. Wiss. Göttingen 1894. [76]; (*2*): Über einen Fundamentalsatz der arithmetischen Theorie der algebraischen Größen. Nachr. K. Ges. Wiss. Göttingen **1895**. [76]; (*3*): Zur Theorie der algebraischen Zahlen. Nachr. K. Ges. Wiss. Göttingen **1895**. [79]; (*4*): Die unimodularen Substitutionen in einem algebraischen Zahlkörper. Nachr. K. Ges. Wiss. Göttingen **1895**. [111]

Jacobi, C. G. J. (*1*): De residuis cubicis commentatio numerosa. Werke **6**, 233 (1827) [245, 327]; (*2*): Observatio arithmetica de numero classium divisorum quadraticorum formae $y^2 + Az^2$ designante A numerum primum formae $4n + 3$. Werke **6**, 240 (1832) [245]; (*3*): Über die Kreisteilung und ihre Anwendung auf die Zahlentheorie. Werke **6**, 254 (1837) [227, 245]; (*4*): Über die komplexen Primzahlen, welche in der Theorie der Reste der 5ten, 8ten und 12ten Potenzen zu betrachten sind. Werke **6**, 275 (1839) [245, 327].

Kronecker, L. (*1*): De unitatibus complexis. Dissertatio inauguralis. Berolini 1845. Werke **1**, 5 (1845). [149]; (*2*): Über die algebraisch auflösbaren Gleichungen. Ber. K. Akad. Wiss. Berlin **1853**. [206]; (*3*): Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$. Werke **1**, 75 (1854). [202]; (*4*): Sur une formule de Gauss. J. de Math. **1856**. [247]; (*5*): Démonstration d'une théorème de M. Kummer. Werke 1, 93 (1856). [279]; (*6*): Zwei Sätze über Gleichungen mit ganzzahligen Koeffizienten. Werke **1**, 103 (1857). [108]; (*7*): Über komplexe Einheiten. Werke **1**, 109 (1857). [204];

(*8*): Über kubische Gleichungen mit rationalen Koeffizienten. Werke **1**, 119 (1859). [354]; (*9*): Über die Klassenanzahl der aus Wurzeln der Einheit gebildeten komplexen Zahlen. Werke **1**, 123 (1863). [237]; (*10*): Über den Gebrauch der Dirichletschen Methoden in der Theorie der quadratischen Formen. Ber. K. Akad. Wiss. Berlin **1864**. [182]; (*11*): Auseinandersetzung einiger Eigenschaften der Klassenanzahl idealer komplexer Zahlen. Werke **1**, 271 (1870). [118, 238]; (*12*): Bemerkungen über Reuschles Tafeln komplexer Primzahlen. Ber. K. Akad. Wiss. Berlin **1875**. [242]; (*13*): Über Abelsche Gleichungen. Ber. K. Akad. Wiss. Berlin **1877**. [206]; (*14*): Über die Irreduktibilität von Gleichungen. Ber. K. Akad. Wiss. Berlin **1880**. [142, 144]; (*15*): Über die Potenzreste gewisser komplexer Zahlen. Ber. K. Akad. Wiss. Berlin **1880**. [244]; (*16*): Grundzüge einer arithmetischen Theorie der algebraischen Größen. J. Math. **92** (1882). [69, 71, 73, 77, 85, 90, 92, 110]; (*17*): Zur Theorie der Abelschen Gleichungen. Bemerkungen zum vorangehenden Aufsatz des Herrn Schwering. J. Math. **93** (1882). [227]; (*18*): Sur les unités complexes. (Drei Noten.) Comptes rendus **96** (1883); vgl. auch J. Molk: Sur les unités complexes. Bull. sciences math. astron. **1883**. [102]; (*19*): Zur Theorie der Formen höherer Stufen. Ber. K. Akad. Wiss. Berlin **1883**. [76]; (*20*): Additions au mémoire sur les unités complexes. Comptes rendus **99** (1884). [102]; (*21*): Ein Satz über Diskriminanten-Formen. J. Math. **100** (1886). [202]

Kummer, E. (*1*): De aequatione $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ per numeros integros resolvenda. J. Math. **17** (1837). [349]; (*2*): Eine Aufgabe, betreffend die Theorie der kubischen Reste. J. Math. **23** (1842). [227]; (*3*): Über die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreisteilung entstehen. J. Math. **30** (1846). [227]; (*4*): De residuis cubicis disquisitiones nonnullae analyticae. J. Math. **32** (1846). [227]; (*5*): Zur Theorie der komplexen Zahlen. J. Math. **35** (1847). [73, 197]; (*6*): Über die Zerlegung der aus Wurzeln der Einheit gebildeten komplexen Zahlen in ihre Primfaktoren. J. Math **35** (1847). [73, 149, 197, 222, 223, 227]; (*7*): Bestimmung der Anzahl nicht äquivalenter Klassen für die aus λ-ten Wurzeln der Einheit gebildeten komplexen Zahlen und die idealen Faktoren derselben. J. Math. **40** (1850). [237, 238]; (*8*): Zwei besondere Untersuchungen über die Klassenanzahl und über die Einheiten der aus λ-ten Wurzeln der Einheit gebildeten komplexen Zahlen. J. Math. **40** (1850). [279, 283, 287]; (*9*): Allgemeiner Beweis des Fermatschen Satzes, daß die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten $\frac{1}{4}(\lambda - 3)$ Bernoullischen Zahlen als Faktoren nicht vorkommen. J. Math. **40** (1850). [349]; (*10*): Über allgemeine Reziprozitätsgesetze für beliebig hohe Potenzreste. Ber. K. Akad. Wiss. Berlin **1850**. [228, 313]; (*11*): Mémoire sur la théorie des nombres complexes composés de racines de l'unité et des nombres entiers. J. de Math. **16** (1851). [222, 223, 227, 237, 285, 349]; (*12*): Über die Ergänzungssätze zu den allgemeinen Reziprozitätsgesetzen. J. Math. **44** (1851). [265, 281, 288, 313]; (*13*): Über die Irregularität der Determinanten. Ber. K. Akad. Wiss. Berlin **1853**. [227, 238]; (*14*): Über eine besondere Art aus komplexen Einheiten gebildeter Ausdrücke. J. Math. **50** (1854). [154]; (*15*): Theorie der idealen Primfaktoren der komplexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist. Abh. K. Akad. Wiss. Berlin **1856**. [201]; (*16*): Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten komplexen Zahlen für den Fall, daß die Klassenanzahl durch λ teilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermatschen Lehrsatzes. Abh. K. Akad. Wiss. Berlin **1857**. [354]; (*17*): Über die den Gaußschen Perioden der Kreisteilung entsprechenden Kongruenzwurzeln. J. Math. **53** (1856).

[227]; (*18*): Über die allgemeinen Reziprozitätsgesetze der Potenzreste. Ber. K. Akad. Wiss. Berlin **1858**. [313]; (*19*): Über die Ergänzungssätze zu den allgemeinen Reziprozitätsgesetzen. J. Math. **56** (1858). [313]; (*20*): Über die allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist. Abh. K. Akad. Wiss. Berlin **1859**. [154, 267, 268, 275, 276, 313, 331]; (*21*): Zwei neue Beweise der allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist. Abh. K. Akad. Wiss. Berlin **1861**. Abgedruckt im J. Math. **100**. [154, 313]; (*22*): Über die Klassenanzahl der aus n-ten Einheitswurzeln gebildeten komplexen Zahlen. Ber. K. Akad. Wiss. Berlin **1861**. [237]; (*23*): Über die Klassenanzahl der aus zusammengesetzten Einheitswurzeln gebildeten idealen komplexen Zahlen. Ber. K. Akad. Wiss. Berlin **1863**. [237]; (*24*): Über die einfachste Darstellung der aus Einheitswurzeln gebildeten komplexen Zahlen, welche durch Multiplikation mit Einheiten bewirkt werden kann. Ber. K. Akad. Wiss. Berlin **1870**. [242]; (*25*): Über eine Eigenschaft der Einheiten der aus den Wurzeln der Gleichung $x^\lambda = 1$ gebildeten komplexen Zahlen und über den zweiten Faktor der Klassenzahl. Ber. K. Akad. Wiss. Berlin **1870**. [238]; (*26*): Über diejenigen Primzahlen λ, für welche die Klassenzahl der aus λ-ten Einheitswurzeln gebildeten komplexen Zahlen durch λ teilbar ist. Ber. K. Akad. Wiss. Berlin **1874**. [285]

Lagrange, J. L. (*1*): Sur la solution des problèmes indéterminés du second degré. Werke **2**, 375 (1868). [173, 175]

Lamé, G. (*1*): Mémoire d'analyse indéterminée démontrant que l'équation $x^7 + y^7 = z^7$ est impossible en nombres entiers. J. de Math. **1840**. [349]; (*2*): Mémoire sur la résolution, en nombres complexes, de l'équation $A^5 + B^5 + C^5 = 0$. J. de Math. **1847**. [349]; (*3*): Mémoire sur la résolution, en nombres complexes, de l'équation $A^n + B^n + C^n = 0$. J. de Math. **1847**. [349]

Lebesgue, V. A. (*1*): Démonstration de l'impossibilité de résoudre l'équation $x^7 + y^7 + z^7 = 0$ en nombres entiers. J. de Math. **1840**. [349]; (*2*): Addition à la note sur l'équation $x^7 + y^7 + z^7 = 0$. J. de Math. **1840**. [349]; (*3*): Théorèmes nouveaux sur l'équation indéterminée $x^5 + y^5 = az^5$. J. de Math. **1843**. [349]

Legendre, A. (*1*): Essai sur la théorie des nombres **1798**. [161, 175]

Mertens, F. (*1*): Über einen algebraischen Satz. Ber. K. Akad. Wiss. Wien **1892**. [76]

Minnigerode, C. (*1*): Über die Verteilung der quadratischen Formen mit komplexen Koeffizienten und Veränderlichen in Geschlechter. Nachr. K. Ges. Wiss. Göttingen **1873**. [191]

Minkowski, H. (*1*): Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen. J. Math. **107** (1891). [100, 101, 110]; (*2*): Théorèmes arithmétiques. Extrait d'une lettre à M. Hermite. Comptes rendus. **92** (1891). [100, 101]; (3): Geometrie der Zahlen. Leipzig 1896. [98, 100, 101, 102, 108, 109, 110]; (*4*): Généralisation de la théorie des fractions continues. Ann. l'école normale **1896**. [109]

Reuschle, C. G. (*1*): Tafeln komplexer Primzahlen, welche aus Wurzeln der Einheit gebildet sind. Berlin 1875. [242]

Schering, E. (*1*): Zahlentheoretische Bemerkung. Auszug aus einem Brief an Herrn Kronecker. J. Math. **100** (1887). [118]; (*2*): Die Fundamentalklassen der zusammensetzbaren arithmetischen Formen. Abh. K. Ges. Wiss. Göttingen **1869**. [118]

Schwering, K. (*1*): Zur Theorie der arithmetischen Funktionen, welche von Jacobi $\psi(\alpha)$ genannt werden. J. Math. **93** (1882). [227]; (*2*): Untersuchung über die fünften Potenzreste und die aus fünften Einheitswurzeln gebildeten ganzen Zahlen. Z. Math. Phys. **27** (1882). [227]: (*3*): Über gewisse trinomische komplexe Zahlen. Acta Math. **10** (1887). [227]; (*4*): Eine Eigenschaft der Primzahl 107. Acta Math. **11** (1887). [227]

Serret, J. A. (*1*): Handbuch der höheren Algebra **2**, Teil 3. Deutsch von G. Wertheim. Leipzig 1879. [85]

Smith, H. (*1*): Report on the theory of numbers. Werke. [227]

Stickelberger, L. (1): Über eine Verallgemeinerung der Kreisteilung. Math. Ann. **37** (1890). [246]

Tano, F. (*1*): Sur quelques théorèmes de Dirichlet. J. Math. **105**. [161]

Weber, H. (*1*): Theorie der Abelschen Zahlkörper. Acta Math. **8** u. **9** (1886), (1887). [206, 227, 237]; (*2*): Über Abelsche Zahlkörper dritten und vierten Grades. Sitzungsber. Ges. Naturwiss. Marburg **1892**. [227, 248]; (*3*): Zahlentheoretische Untersuchungen aus dem Gebiete der elliptischen Funktionen. Nachr. K. Ges. Wiss. Göttingen **1893**. (Drei Mitteilungen.); (*4*): Lehrbuch der Algebra 2. Braunschweig 1896. [189, 201, 227, 237, 248].

Wolfskehl, P. (*1*): Beweis, daß der zweite Faktor der Klassenanzahl für die aus den elften und dreizehnten Einheitswurzeln gebildeten Zahlen gleich eins ist. J. Math. **99** (1885). [227].

Verzeichnis der Sätze und Hilfssätze.

Die Sätze mit fettgedruckten Nummern sind im Text durch kursiven Druck ausgezeichnet.

	Seite		Seite		Seite
Satz 1	69	Satz 43	100	Satz 85	144
„ 2	70	„ **44**	100	„ 86	145
„ 3	70	„ **45**	100	„ 87	145
„ 4	70	„ 46	102	„ 88	146
„ 5	71	„ **47**	102	„ 89	146
„ 6	73	„ 48	108	„ 90	149
„ **7**	75	„ 49	110	„ 91	150
„ 8	76	„ 50	110	„ 92	152
„ 9	76	„ 51	110	„ 93	154
„ 10	76	„ **52**	111	„ **94**	155
„ 11	76	„ 53	111	„ 95	157
„ 12	77	„ **54**	115	„ 96	158
„ 13	78	„ 55	116	„ 97	160
„ 14	79	„ **56**	116	„ 98	162
„ 15	79	„ 57	118	„ 99	167
„ 16	79	„ 58	120	„ **100**	168
„ 17	79	„ 59	120	„ **101**	169
„ 18	80	„ 60	122	„ 102	173
„ 19	80	„ 61	122	„ 103	175
„ 20	80	„ 62	122	„ 104	175
„ 21	82	„ 63	123	„ 105	176
„ 22	82	„ 64	126	„ 106	177
„ 23	82	„ 65	126	„ 107	178
„ 24	82	„ 66	128	„ 108	179
„ 25	82	„ 67	130	„ 109	181
„ 26	83	„ 68	131	„ 110	182
„ 27	83	„ 69	132	„ 111	182
„ 28	83	„ **70**	134	„ 112	184
„ 29	83	„ 71	135	„ 113	186
„ 30	84	„ 72	135	„ 114	188
„ **31**	85	„ 73	136	„ 115	192
„ 32	86	„ 74	136	„ 116	192
„ 33	88	„ 75	136	„ 117	195
„ 34	88	„ 76	139	„ 118	196
„ 35	89	„ 77	139	„ 119	197
„ 36	90	„ 78	139	„ 120	199
„ **37**	90	„ 79	140	„ 121	200
„ 38	95	„ 80	140	„ 122	200
„ 39	95	„ 81	142	„ 123	200
„ **40**	97	„ **82**	142	„ 124	200
„ 41	98	„ 83	143	„ 125	201
„ 42	99	„ 84	144	„ 126	203

	Seite		Seite		Seite
Satz 127	204	Satz 142	237	Satz 157	288
„ 128	205	„ **143**	240	„ **158**	295
„ 129	206	„ **144**	242	„ **159**	302
„ 130	206	„ 145	245	„ 160	307
„ **131**	206	„ 146	247	„ **161**	312
„ 132	217	„ **147**	249	„ 162	319
„ 133	218	„ 148	251	„ 163	328
„ 134	219	„ 149	254	„ **164**	329
„ 135	222	„ **150**	257	„ 165	331
„ 136	223	„ 151	272	„ **166**	332
„ 137	224	„ 152	276	„ **167**	332
„ 138	225	„ 153	279	„ 168	349
„ 139	228	„ 154	283	„ 169	354
„ 140	231	„ 155	286		
„ 141	235	„ 156	287		

	Seite		Seite		Seite
Hilfssatz 1	75	Hilfssatz 18	212	Hilfssatz 35	312
„ 2	75	„ 19	213	„ 36	313
„ 3	86	„ 20	217	„ 37	314
„ 4	87	„ 21	230	„ 38	316
„ 5	87	„ 22	238	„ 39	317
„ 6	98	„ 23	250	„ 40	319
„ 7	99	„ 24	267	„ 41	321
„ 8	100	„ 25	268	„ 42	322
„ 9	104	„ 26	270	„ 43	337
„ 10	113	„ 27	275	„ 44	340
„ 11	130	„ 28	279	„ 45	340
„ 12	146	„ 29	281	„ 46	342
„ 13	168	„ 30	289	„ 47	343
„ 14	171	„ 31	292	„ 48	343
„ 15	207	„ 32	294	„ 49	346
„ 16	208	„ 33	308		
„ 17	211	„ 34	310		

8. Über die Theorie der relativquadratischen Zahlkörper.

[Jahresbericht der Deutschen Mathematiker-Vereinigung. Bd. 6. S. 88—94 (1899).]

In der Theorie der relativ Abelschen Zahlkörper nehmen zunächst die Körper vom *zweiten* Relativgrade unser Interesse in Anspruch.

Es sei ein beliebiger Zahlkörper k vom Grade n als Rationalitätsbereich zugrunde gelegt; unsere Aufgabe ist es dann, die Theorie der relativquadratischen Zahlkörper $K\left(\sqrt{\mu}\right)$, d. h. derjenigen Körper zu begründen, die durch die Quadratwurzel aus einer beliebigen ganzen Zahl μ des Körpers k bestimmt sind. Die „disquisitiones arithmeticae“ von Gauss sind als der einfachste Fall in jenem Problem enthalten. Wir können unseren Gegenstand auch als die Theorie der quadratischen Gleichungen oder Formen bezeichnen, deren Koeffizienten Zahlen des vorgelegten Rationalitätsbereiches k sind.

Für unsere Theorie ist vor allem die Erkenntnis notwendig, daß auch in dem beliebigen Zahlkörper k ein Reziprozitätsgesetz für quadratische Reste besteht. Das quadratische Reziprozitätsgesetz im Bereiche der rationalen Zahlen lautet bekanntlich:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

wo p, q beliebige ungerade rationale positive Primzahlen bedeuten. Aber diese Form des Reziprozitätsgesetzes ist, sobald wir den Zweck der Verallgemeinerung desselben vor Augen haben, aus mannigfachen Gründen — ich hebe nur die unübersichtliche Form der auftretenden Exponenten, den Mangel an Einheitlichkeit und die Ausnahmestellung der Zahl 2 hervor — eine unvollkommene. Nun spielt bekanntlich der Begriff der „primären“ Zahlen in der bisherigen Fassung der höheren Reziprozitätsgesetze eine sehr wichtige Rolle. Doch für unser allgemeineres Problem werden wir von der Benutzung dieses Begriffes eine Beseitigung der angedeuteten Mißstände nicht erwarten dürfen; denn wir müssen bedenken, daß im Körper k die Zahl 2 im allgemeinen als Produkt von gewissen Potenzen von Primidealen zerlegt werden kann, und daß demgemäß die Definition des Begriffes „primär“

eine Unterscheidung der verschiedenen Möglichkeiten dieser Zerlegung und die Einführung mannigfacher willkürlicher Annahmen nötig machen würde. Auch ist die Fassung, welche Kummer seinen allgemeinen Reziprozitätsgesetzen gegeben hat, schon deshalb für uns nicht verwendbar, weil wir bei ihrer Annahme dem Körper k die beschränkende Bedingung auferlegen müßten, daß seine Klassenanzahl ungerade ist; es wird sich aber zeigen, daß uns der Fall einer durch 2 teilbaren Klassenanzahl zu den schönsten und wertvollsten Resultaten führt.

Aus den angegebenen Gründen erscheint mir die Einführung eines neuen Symbols $\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$ in die Zahlentheorie nötig, welches in unserem Falle der Theorie eines relativquadratischen Körpers, wie folgt, zu definieren ist. Sind ν, μ ganze Zahlen in k, dabei μ nicht Quadratzahl, und ist $\mathfrak{w}$ ein beliebiges Primideal in k, so bezeichne jenes Symbol den Wert

$$\left(\frac{\nu,\mu}{\mathfrak{w}}\right) = +1, \tag{1}$$

sobald die Zahl ν mit der Relativnorm einer ganzen Zahl des durch $\sqrt{\mu}$ bestimmten relativquadratischen Körpers $K\left(\sqrt{\mu}\right)$ nach dem Primideal $\mathfrak{w}$ kongruent ist, und sobald außerdem auch für jede höhere Potenz von $\mathfrak{w}$ eine ganze Zahl in $K\left(\sqrt{\mu}\right)$ existiert, deren Relativnorm der Zahl ν nach jener Potenz von $\mathfrak{w}$ kongruent ist; in jedem anderen Falle setzen wir

$$\left(\frac{\nu,\mu}{\mathfrak{w}}\right) = -1. \tag{2}$$

Diejenigen ganzen Zahlen ν, für welche die Gleichung (1) gilt, sollen *Normenreste*[1] des Körpers $K\left(\sqrt{\mu}\right)$ nach $\mathfrak{w}$, diejenigen Zahlen, für welche die Gleichung (2) gilt, *Normennichtreste* des Körpers $K\left(\sqrt{\mu}\right)$ nach $\mathfrak{w}$ heißen. Wenn μ das Quadrat einer Zahl in k ist, möge die Gleichung (1) gelten. Der Bildung der Begriffe „Normenrest“ und „Normennichtrest“ entspricht in der Funktionentheorie gewissermaßen die Unterscheidung, ob eine algebraische Funktion einer Variablen an einer Stelle nach ganzen oder nach gebrochenen Potenzen der Variablen entwickelt werden kann.

Die ersten Sätze für das eben definierte Symbol sind in den Formeln enthalten:

$$\left(\frac{\nu,\mu}{\mathfrak{w}}\right) = \left(\frac{\mu,\nu}{\mathfrak{w}}\right),$$

$$\left(\frac{\nu\nu',\mu}{\mathfrak{w}}\right) = \left(\frac{\nu,\mu}{\mathfrak{w}}\right)\left(\frac{\nu',\mu}{\mathfrak{w}}\right),$$

$$\left(\frac{\nu,\mu\mu'}{\mathfrak{w}}\right) = \left(\frac{\nu,\mu}{\mathfrak{w}}\right)\left(\frac{\nu,\mu'}{\mathfrak{w}}\right);$$

[1] Vgl. meinen Bericht über die Theorie der Zahlkörper. (Dieser Band, Abh. 7, S. 161/162 und 257.)

die wichtigste Eigenschaft unseres Symbols spricht sich in dem folgenden Satze aus:

Wenn $\mathfrak{w}$ ein Primideal des Körpers k ist, das nicht in der Relativdiskriminante des Körpers $K\left(\sqrt{\mu}\right)$ aufgeht, so ist jede zu $\mathfrak{w}$ prime Zahl in k Normenrest des Körpers $K\left(\sqrt{\mu}\right)$ nach $\mathfrak{w}$. Wenn dagegen $\mathfrak{w}$ ein Primideal des Körpers k ist, das in der Relativdiskriminante des Körpers $K\left(\sqrt{\mu}\right)$ aufgeht, so sind bei genügend hohem Exponenten e von allen vorhandenen zu $\mathfrak{w}$ primen und nach $\mathfrak{w}^e$ einander inkongruenten Zahlen in k genau die Hälfte Normenreste nach $\mathfrak{w}$.

Diese Tatsache entspricht dem bekannten Satze über die Verzweigungspunkte einer Riemannschen Fläche, wonach eine algebraische Funktion in der Umgebung eines einfachen Verzweigungspunktes den Vollwinkel auf die Hälfte desselben konform abbildet.

Mit Benutzung des eben definierten Symboles drückt sich das allgemeinste Reziprozitätsgesetz für quadratische Reste durch die Formel aus:

$$\prod_{(\mathfrak{w})}\left(\frac{\nu,\mu}{\mathfrak{w}}\right)=[\nu,\mu][\nu',\mu']\cdots[\nu^{(n-1)},\mu^{(n-1)}]. \tag{3}$$

Hierin bedeuten ν, μ zwei beliebige ganze Zahlen des Körpers k. Das Produkt linker Hand ist über alle Primideale $\mathfrak{w}$ des Körpers k zu erstrecken; da dem vorigen Satz zufolge das Symbol $\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$ nur für eine endliche Anzahl von Primidealen $\mathfrak{w}$ den Wert -1 haben kann, so kommt bei der Bestimmung des Wertes des Produktes nur eine endliche Anzahl von Faktoren in Betracht. Auf der rechten Seite der Formel (3) bedeuten $\nu', \mu'; \ldots; \nu^{(n-1)}, \mu^{(n-1)}$ die zu ν, μ konjugierten Zahlen bzw. in den zu k konjugierten Körpern $k'; \ldots; k^{(n-1)}$; das Zeichen $[\nu, \mu]$ bedeutet den Wert -1, wenn der Körper k reell und zugleich jede der beiden Zahlen ν, μ negativ ist; in jedem anderen Falle bezeichnet $[\nu, \mu]$ den Wert $+1$. Entsprechend bedeutet $[\nu', \mu']$ den Wert -1, wenn k' reell und zugleich jede der beiden Zahlen ν', μ' negativ ausfällt, in jedem anderen Falle dagegen soll $[\nu', \mu']$ den Wert $+1$ haben, usf.

Sind beispielsweise k und alle zu k konjugierten Körper imaginär, so lautet das Reziprozitätsgesetz

$$\prod_{(\mathfrak{w})}\left(\frac{\nu,\mu}{\mathfrak{w}}\right)=+1. \tag{4}$$

Im Falle, daß k den Körper der rationalen Zahlen bedeutet, erhalten wir

$$\prod_{(w)}\left(\frac{n,m}{w}\right)=[n,m], \tag{5}$$

wo n, m zwei beliebige ganze rationale Zahlen sind, ferner w alle rationalen Primzahlen durchläuft und $[n, m]$ den Wert $+1$ oder -1 bezeichnet, je

nachdem wenigstens eine der Zahlen m, n positiv ausfällt oder beide negativ sind[1].

Die einfachsten Fälle des quadratischen Reziprozitätsgesetzes erhalten wir aus unseren Formeln (3), (4), indem wir für ν, μ Einheiten oder unzerlegbare Zahlen des Körpers k einsetzen. Insbesondere folgen aus (5) die bekannten Formeln des gewöhnlichen quadratischen Reziprozitätsgesetzes, indem wir für n, m die Zahlen -1, 2 oder beliebige ungerade Primzahlen p, q wählen[1].

Es sei insbesondere der Körper k nebst seinen sämtlichen Konjugierten imaginär und habe überdies die Klassenanzahl $h = 1$. Bedeuten dann $\pi, \varkappa$, $\pi', \varkappa'$ irgendwelche Primzahlen in k, die zu 2 prim sind und nach dem Modul 4 den Kongruenzen

$$\pi \equiv \pi', \qquad \varkappa \equiv \varkappa', \tag{4}$$

genügen, so gelten, wie wir aus (4) leicht erkennen, folgende spezielle Gesetze:

$$\left(\frac{\pi}{\varkappa}\right)\left(\frac{\varkappa}{\pi}\right)=\left(\frac{\pi'}{\varkappa'}\right)\left(\frac{\varkappa'}{\pi'}\right),$$

und ferner wird, falls wenigstens eine der Primzahlen $\pi, \varkappa$ dem Quadrat einer ganzen Zahl in k nach dem Modul 4 kongruent ist:

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

In den beiden letzten Formeln bedeutet allgemein das Symbol $\left(\frac{\nu}{\mu}\right)$ den Wert $+1$ oder -1, je nachdem ν dem Quadrat einer ganzen Zahl in k nach μ kongruent ist oder nicht. Die beiden letzteren Gesetze können leicht auf die mannigfaltigste Weise durch numerische Beispiele bestätigt werden.

Es ist überaus bemerkenswert, daß bei Anwendung unseres Symbols eine einzige Gleichung von so einfacher Bauart, wie es die Formel (3) ist, das quadratische Reziprozitätsgesetz für einen beliebigen Zahlkörper in vollster Allgemeinheit zum Ausdruck bringt: die Formel (3) gilt, gleichviel ob der zugrunde gelegte Körper k ein Galoisscher ist oder irgendeinen oder gar keinen Affekt hat; die Formel (3) nimmt Rücksicht auf die vielen möglichen Fälle, je nach der Realität des Körpers k und seiner Konjugierten; sie gilt, wie auch immer die Zerlegung der Zahl 2 im Körper k ausfallen möge; sie enthält alle Ergänzungssätze; durch sie erscheint die exklusive Stellung der Zahl 2 und der in 2 aufgehenden Primideale beseitigt; vor allem endlich gilt die nämliche Formel (3) unabhängig davon, ob die Klassenanzahl des Körpers k ungerade oder durch irgendeine Potenz der Zahl 2 teilbar ist.

Das Reziprozitätsgesetz in der Fassung (3) erinnert an den Cauchyschen Integralsatz in der Funktionentheorie, demzufolge ein komplexes Integral,

[1] Vgl. l. c. § 64 und § 69. (Dieser Band S. 161 und 169.)

um alle einzelnen Singularitäten einer Funktion geführt, insgesamt stets den Wert 0 ergibt. Einer der bekannten Beweise des gewöhnlichen quadratischen Reziprozitätsgesetzes weist auch auf einen inneren Zusammenhang zwischen jenem zahlentheoretischen Gesetze und CAUCHYS funktionentheoretischem Fundamentalsatz hin.

Doch das Reziprozitätsgesetz (3) bildet nur den ersten wichtigen Schritt zur Begründung unserer Theorie der relativquadratischen Zahlkörper. Unsere weitere Aufgabe ist die Aufstellung aller relativquadratischen Körper und die Untersuchung ihrer Eigenschaften. Der Einfachheit halber sei fortan der zugrunde gelegte Rationalitätsbereich k nebst sämtlichen Konjugierten imaginär. Da wir die Relativkörper durch ihre Relativdiskriminanten festlegen wollen, so ist offenbar die einfachste Frage diejenige nach den relativquadratischen Körpern mit der Relativdiskriminante 1. Nach einem in meinem Berichte über die Theorie der algebraischen Zahlkörper bewiesenen Satze[1] kann es einen solchen Relativkörper niemals geben, falls die Klassenanzahl des Köpers k ungerade ist; wir wählen daher den Körper k so, daß seine Klassenanzahl gerade, und zwar der Einfachheit halber gleich 2 sei. In der Tat gelingt dann der Nachweis der Existenz eines Relativkörpers K mit der Relativdiskriminante 1. Dieser Körper werde der *Klassenkörper*[2] von k genannt. Der Klassenkörper K besitzt folgende fundamentalen Eigenschaften:

1. Der Klassenkörper K hat in bezug auf k die Relativdiskriminante 1.

2. Die Klassenanzahl des Klassenkörpers K ist ungerade.

3a) Diejenigen Primideale in k, welche in k Hauptideale sind, zerfallen in K in das Produkt zweier Primideale.

3b) Diejenigen Primideale in k, welche in k nicht Hauptideale sind, bleiben in K Primideale; sie werden jedoch in K Hauptideale.

Von diesen vier Eigenschaften 1, 2, 3a, 3b definiert bei unserer Annahme über den Körper k jede für sich in eindeutiger Weise den Klassenkörper K; wir haben somit die Sätze:

1. Es gibt außer K keinen anderen relativquadratischen Körper mit der Relativdiskriminante 1 in bezug auf k.

2. Wenn ein zu k relativquadratischer Körper eine ungerade Klassenanzahl hat, so stimmt derselbe mit dem Klassenkörper K überein.

3. Wenn alle Primideale in k, die in k Hauptideale sind, in einem relativquadratischen Körper zerfallen, oder wenn alle Primideale in k, die in k nicht Hauptideale sind, in einem relativquadratischen Körper Primideale bleiben, so folgt jedesmal, daß dieser relativquadratische Körper kein anderer als der Klassenkörper K ist.

[1] Satz 94 (dieser Band S. 155).

[2] Vgl. H. WEBER: Über Zahlengruppen in algebraischen Körpern. Drei Abhandlungen. Math. Ann. **48, 49, 50.** (1897, 1897, 1898).

Diese Gesetze für den Klassenkörper K sind einer weiten Verallgemeinerung fähig; sie lassen eine wunderbare Harmonie erkennen und erschließen, wie mir scheint, ein an neuen arithmetischen Wahrheiten reiches Gebiet.

Auch eine Theorie der Geschlechter läßt sich in unserem relativquadratischen Körper aufstellen; aus dieser fließen dann die Bedingungen für die Auflösbarkeit ternärer diophantischer Gleichungen, deren Koeffizienten Zahlen des beliebigen Rationalitätsbereiches k sind.

Wir haben uns in diesem Vortrage auf die Untersuchung relativ Abelscher Körper vom *zweiten* Grad beschränkt. Diese Beschränkung ist jedoch nur eine vorläufige, und da die von mir bei den Beweisen der Sätze angewandten Schlüsse sämtlich der Verallgemeinerung fähig sind, so steht zu hoffen, daß die Schwierigkeiten nicht unüberwindliche sein werden, die die Begründung einer allgemeinen Theorie der relativ Abelschen Körper bietet. Die oben in der Theorie des relativquadratischen Körpers auftretenden, in der Unterscheidung zwischen reellen und imaginären Körpern beruhenden Schwierigkeiten fallen in der Theorie der Abelschen Körper von ungeradem Relativgrade sogar gänzlich fort, und die höheren Reziprozitätsgesetze erhalten deshalb einen noch einfacheren Ausdruck als das quadratische Reziprozitätsgesetz (3), indem dann in dieser Formel an Stelle der rechten Seite stets die Zahl 1 tritt.

Die Theorie der relativ Abelschen Körper enthält als besonders einfachen Fall die Theorie derjenigen Zahlkörper, die die komplexe Multiplikation der elliptischen Funktionen liefert. Da H. WEBER[1] für diese Körper die Eigenschaften 3a und 3b bewiesen hat, so werden wir hieraus schließen, daß den nämlichen Zahlkörpern das volle System der oben angedeuteten arithmetischen Eigenschaften zukommt; es ist dann nicht schwer, den Nachweis dafür zu erbringen, daß die Abelschen Gleichungen im Bereiche eines quadratischen imaginären Körpers durch die Transformationsgleichungen elliptischer Funktionen mit singulären Moduln erschöpft werden — und dies hieße, den „liebsten Jugendtraum" KRONECKERS verwirklichen, der diesen Gelehrten noch bis an seinen Lebensabend lebhaft beschäftigt hat.

[1] Vgl. Elliptische Funktionen und algebraische Zahlen (Braunschweig 1891), sowie die zweite und dritte der vorhin genannten Abhandlungen über Zahlengruppen.

9. Über die Theorie des relativquadratischen Zahlkörpers.

[Mathematische Annalen Bd. 51, S. 1—127 (1899).]

Einleitung.

Es sei ein beliebiger Zahlkörper k zugrunde gelegt; der Grad dieses Körpers k heiße m und die $m-1$ zu k konjugierten Zahlkörper mögen mit $k', k'', \ldots, k^{(m-1)}$ bezeichnet werden. Die Anzahl der Idealklassen des Körpers k werde h genannt.

Bezeichnet μ irgendeine ganze Zahl in k, die nicht gleich dem Quadrat einer Zahl in k ist, so bestimmt $\sqrt{\mu}$ zusammen mit den Zahlen des Körpers k einen Körper vom Grade $2m$, welcher relativ quadratisch in bezug auf den Körper k ist und mit $K(\sqrt{\mu})$ oder auch kurz mit K bezeichnet wird. Es entsteht die Aufgabe, die Theorie der relativquadratischen Zahlkörper aufzustellen und zu begründen. Dieses Problem erscheint mir als eine naturgemäße Verallgemeinerung desjenigen Problems, das den Gegenstand der „disquisitiones arithmeticae" von Gauss bildet.

Die Theorie des relativquadratischen Körpers führte mich zur Entdeckung eines allgemeinen Reziprozitätsgesetzes für quadratische Reste, welches das gewöhnliche Reziprozitätsgesetz zwischen rationalen Primzahlen nur als ein vereinzeltes Glied in einer Kette der wunderbarsten und mannigfaltigsten Zahlenbeziehungen erscheinen läßt.

Die Methoden, welche ich im folgenden zur Untersuchung der relativquadratischen Körper angewandt habe, sind bei gehöriger Verallgemeinerung auch in der Theorie der relativ-Abelschen Körper von beliebigem Relativgrade mit gleichem Erfolge verwendbar und führen dann insbesondere zu den allgemeinsten Reziprozitätsgesetzen für beliebig hohe Potenzreste innerhalb eines beliebigen algebraischen Zahlenbereiches[1].

Wenn man den in der vorliegenden Arbeit dargelegten Beweis des allgemeinen Reziprozitätsgesetzes für quadratische Reste auf die von Kummer behandelte Theorie der l-ten Potenzreste im Körper der l-ten Einheitswurzeln überträgt, so entsteht ein neuer Beweis des Kummerschen Reziprozitätsgesetzes für l-te Potenzreste, welcher sich sowohl von den Kummerschen wie von meinen bisher gegebenen Beweisen wesentlich dadurch unterscheidet, daß darin das besondere aus der Kreisteilung herstammende Eisensteinsche Reziprozitätsgesetz *nicht* zur Verwendung gelangt.

[1] Vgl. das von der K. Gesellschaft der Wiss. zu Göttingen für das Jahr 1891 gestellte Preisthema.

Unter den Anwendungen meiner Theorie nenne ich hier die Aufstellung der Kriterien dafür, daß eine quadratische diophantische Gleichung mit beliebigen algebraischen Koeffizienten in dem durch diese Koeffizienten bestimmten Rationalitätsbereiche lösbar ist.

Die vorliegende Arbeit zerfällt in *zwei Abschnitte*. Der *erste* Abschnitt behandelt die *allgemeinen Definitionen und vorbereitenden Sätze* in der Theorie der relativquadratischen Körper für einen *beliebigen* Grundkörper k, der *zweite* Abschnitt entwickelt *vollständig* die Theorie des relativquadratischen Körpers in bezug auf einen solchen Grundkörper k, der nebst seinen sämtlichen konjugierten Körpern *imaginär* ist und überdies eine *ungerade Klassenanzahl* h besitzt. Was den Fall eines beliebigen Grundkörpers k betrifft, so gedenke ich die wichtigsten Sätze der entsprechenden Theorie demnächst in den Göttinger Nachrichten mit einer kurzen Angabe der Beweise zu veröffentlichen[1].

I. Allgemeine Definitionen und vorbereitende Sätze.

§ 1. Quadratische Reste und Nichtreste im Grundkörper k und das Symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)$.

Definition 1. Es sei $\mathfrak{p}$ ein in der Zahl 2 nicht aufgehendes Primideal des Körpers k und α eine beliebige zu $\mathfrak{p}$ prime ganze Zahl in k: dann heiße α in k *quadratischer Rest* nach $\mathfrak{p}$, wenn α kongruent dem Quadrat einer ganzen Zahl in k nach $\mathfrak{p}$ wird, d. h. wenn die Kongruenz

$$\xi^2 \equiv \alpha, \qquad (\mathfrak{p})$$

durch eine ganze Zahl ξ des Körpers k befriedigt werden kann; im anderen Falle heiße α *quadratischer Nichtrest* nach $\mathfrak{p}$. Wir definieren jetzt das *Symbol* $\left(\frac{\alpha}{\mathfrak{p}}\right)$, indem wir, wenn α in k quadratischer Rest nach $\mathfrak{p}$ ist,

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = +1$$

und im anderen Fall

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = -1$$

setzen.

[1] Vgl. meinen in der Mathematiker-Vereinigung zu Braunschweig 1897 gehaltenen Vortrag „Über die Theorie der relativquadratischen Zahlkörper". (Dieser Band Abh. 8, S. 364—369.)

Satz 1. Wenn $\mathfrak{p}$ ein beliebiges nicht in 2 aufgehendes Primideal des Körpers k und α eine zu $\mathfrak{p}$ prime ganze Zahl in k ist, so gilt nach dem Modul $\mathfrak{p}$ die Kongruenz

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right), \quad (\mathfrak{p}),$$

worin $n(\mathfrak{p})$ die Norm des Primideals $\mathfrak{p}$ im Körper k bedeutet.

Beweis. Ist $\alpha \equiv \beta^2$ nach $\mathfrak{p}$, wo β wieder eine ganze Zahl in k bedeutet, so folgt nach dem Fermatschen Satze[1] sofort

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv \beta^{n(\mathfrak{p})-1} \equiv +1, \quad (\mathfrak{p}).$$

Wir nehmen andererseits an, es sei α quadratischer Nichtrest nach $\mathfrak{p}$; bezeichnen wir dann mit ϱ eine Primitivzahl nach $\mathfrak{p}$ im Körper k und setzen $\alpha \equiv \varrho^a$ nach $\mathfrak{p}$, so muß hierin offenbar der Exponent a eine ungerade Zahl sein. Nach dem Fermatschen Satze ist aber

$$\varrho^{n(\mathfrak{p})-1} \equiv +1, \quad (\mathfrak{p}),$$

und folglich

$$\varrho^{\frac{n(\mathfrak{p})-1}{2}} \equiv \pm 1, \quad (\mathfrak{p}). \tag{1}$$

Da in der Reihe der Potenzen $\varrho, \varrho^2, \varrho^3, \ldots$ die Potenz $\varrho^{n(\mathfrak{p})-1}$ die erste sein soll, welche $\equiv +1$ nach $\mathfrak{p}$ wird, so gilt notwendig auf der rechten Seite der Kongruenz (1) das negative Vorzeichen und demzufolge wird

$$\alpha^{\frac{n(\mathfrak{p})-1}{2}} \equiv \varrho^{a\frac{n(\mathfrak{p})-1}{2}} \equiv -1, \quad (\mathfrak{p}).$$

Aus dem eben bewiesenen Satze 1 folgen leicht die weiteren Tatsachen:

Satz 2. Wenn α, β irgend zwei zu dem Primideal $\mathfrak{p}$ prime ganze Zahlen in k sind, so gilt stets die Gleichung

$$\left(\frac{\alpha\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right).$$

Ein vollständiges System von $n(\mathfrak{p}) - 1$ zu $\mathfrak{p}$ primen und einander nach $\mathfrak{p}$ inkongruenten Zahlen zerfällt in zwei Teilsysteme, von denen das eine aus den $\frac{n(\mathfrak{p})-1}{2}$ quadratischen Resten nach $\mathfrak{p}$, das andere aus den $\frac{n(\mathfrak{p})-1}{2}$ quadratischen Nichtresten nach $\mathfrak{p}$ besteht.

§ 2. Die Begriffe Relativnorm, Relativdifferente und Relativdiskriminante.

Definition 2. Jede Zahl A des Körpers $K(\sqrt{\mu})$ kann in die Gestalt

$$\mathsf{A} = \alpha + \beta\sqrt{\mu}$$

gebracht werden, wo α, β ganze oder gebrochene Zahlen des Körpers k sind;

[1] Vgl. meinen der Deutschen Mathematiker-Vereinigung erstatteten Bericht „Die Theorie der algebraischen Zahlkörper". 1897, Satz 22 (dieser Band S. 82) und Satz 24 (dieser Band S. 82). Ich werde in der vorliegenden Abhandlung diesen Bericht von mir kurz mit „Algebraische Zahlkörper" zitieren. (Dieser Band Abh. 7, S. 63—363.)

ist dies geschehen, so heiße die Zahl

$$S\mathsf{A} = \alpha - \beta\sqrt{\mu},$$

die vermöge der Substitution

$$S = (\sqrt{\mu} : -\sqrt{\mu})$$

aus A entspringende oder zu A *relativkonjugierte Zahl* in $K(\sqrt{\mu})$. Die Zahl

$$\mathsf{A} - S\mathsf{A}$$

heiße die *Relativdifferente der Zahl* A im Körper $K(\sqrt{\mu})$. Der größte gemeinsame Teiler der Relativdifferenten aller *ganzen* Zahlen $\Omega_1, \Omega_2, \ldots$ des Körpers $K(\sqrt{\mu})$, d. h. das Ideal

$$\mathfrak{D} = (\Omega_1 - S\Omega_1, \Omega_2 - S\Omega_2, \ldots)$$

heiße die *Relativdifferente des Körpers* $K(\sqrt{\mu})$ in bezug auf den Körper k.

Das Produkt einer Zahl A des Körpers K mit der relativkonjugierten Zahl $S\mathsf{A}$ heißt die *Relativnorm der Zahl* A und wird mit $N(\mathsf{A})$ bezeichnet; es ist also

$$N(\mathsf{A}) = \mathsf{A} \cdot S\mathsf{A}.$$

Die Relativnorm $N(\mathsf{A})$ einer Zahl A in K ist stets eine Zahl in k.

Ist $\mathfrak{J} = (\mathsf{i}_1, \mathsf{i}_2, \ldots)$ ein beliebiges Ideal der Körpers K und wendet man auf sämtliche ganze Zahlen $\mathsf{i}_1, \mathsf{i}_2, \ldots$ dieses Ideals die Substitution S an, so heißt das so entstehende Ideal das zu $\mathfrak{J}$ *relativkonjugierte Ideal* und wird mit $S\mathfrak{J}$ bezeichnet; es ist also

$$S\mathfrak{J} = (S\mathsf{i}_1, S\mathsf{i}_2, \ldots).$$

Das Produkt eines Ideals $\mathfrak{J}$ des Körpers K mit dem relativkonjugierten Ideal $S\mathfrak{J}$ heißt die *Relativnorm des Ideals* $\mathfrak{J}$ und wird mit $N(\mathfrak{J})$ bezeichnet; es ist also

$$N(\mathfrak{J}) = \mathfrak{J} \cdot S\mathfrak{J}.$$

Die Relativnorm eines Ideals $\mathfrak{J}$ in K ist stets ein Ideal in k.

Das Quadrat der Relativdifferente einer Zahl A des Körpers K d. h. die Zahl $(\mathsf{A} - S\mathsf{A})^2$ heißt die *Relativdiskriminante der Zahl* A. Die Relativdiskriminante einer Zahl A in K ist stets eine Zahl in k.

Das Quadrat der Relativdifferente des Körpers K

$$\mathfrak{d} = \mathfrak{D}^2 = (\Omega_1 - S\Omega_1, \Omega_2 - S\Omega_2, \ldots)^2$$

heißt die *Relativdiskriminante des Körpers* K. Da die Relativdifferente $\mathfrak{D}$ des Körpers K ein solches Ideal des Körpers K ist, das seinem relativ konjugierten Ideale gleich wird, so ist die Relativdiskriminante $\mathfrak{d}$ auch gleich der Relativnorm der Relativdifferente $\mathfrak{D}$ des Körpers K; es ist daher die Relativdiskriminante $\mathfrak{d}$ stets ein Ideal in k.

§ 3. Das ambige Ideal.

Definition 3. Ein Ideal $\mathfrak{A}$ des Körpers K heißt ein *ambiges Ideal,* wenn dasselbe bei der Operation S ungeändert bleibt, d. h. wenn

$$S\mathfrak{A} = \mathfrak{A}$$

ist und wenn außerdem $\mathfrak{A}$ kein von 1 verschiedenes Ideal des Körpers k als Faktor enthält. Insbesondere heißt ein Primideal des Körpers K ein *ambiges Primideal,* wenn dasselbe bei Anwendung der Substitution S ungeändert bleibt und nicht zugleich im Körper k liegt. Jedes ambige Ideal ist ein Produkt von ambigen Primidealen. Das Quadrat eines ambigen Primideals ist gleich der Relativnorm desselben und stellt im Körper k selbst ein Primideal dar.

Satz 3[1]. Die Relativdifferente $\mathfrak{D}$ des relativquadratischen Körpers K enthält alle und nur diejenigen Primideale, welche ambig sind.

§ 4. Die Primfaktoren der Relativdiskriminante.

Unsere nächste Aufgabe ist es, die Primfaktoren der Relativdiskriminante $\mathfrak{d}$ des Körpers $K(\sqrt{\mu})$ wirklich zu ermitteln. Diese Aufgabe wird durch den folgenden Satz gelöst:

Satz 4. Es sei $\mathfrak{p}$ ein zu 2 primes Primideal des Körpers k; geht dann $\mathfrak{p}$ in der Zahl μ genau zur a-ten Potenz auf, so enthält, wenn der Exponent a ungerade ist, die Relativdiskriminante $\mathfrak{d}$ des Körpers $K(\sqrt{\mu})$ stets den Faktor $\mathfrak{p}$. Ist dagegen der Exponent a gerade, so fällt die Relativdiskriminante $\mathfrak{d}$ prim zu $\mathfrak{p}$ aus.

Es sei $\mathfrak{l}$ ein Primideal des Körpers k, welches in 2 aufgeht, und zwar genau zur l-ten Potenz; ferner gehe $\mathfrak{l}$ in μ genau zur a-ten Potenz auf: so ist die Relativdiskriminante des Körpers $K(\sqrt{\mu})$ stets dann und nur dann zu $\mathfrak{l}$ prim, wenn im Körper k eine ganze Zahl α vorhanden ist, die der Kongruenz

$$\mu \equiv \alpha^2, \qquad (\mathfrak{l}^{2l+a}) \tag{1}$$

genügt.

Beweis. Gehen wir zunächst auf den ersten Teil des Satzes 4 ein. Es sei π eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare ganze Zahl in k, und weiter sei ν eine durch $\frac{\pi}{\mathfrak{p}}$ teilbare, aber zu $\mathfrak{p}$ prime ganze Zahl in k.

Ist der Exponent a ungerade, so stellt $\mu^* = \frac{\mu \cdot \nu^{a-1}}{\pi^{a-1}}$ eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare ganze Zahl in k dar von der Art, daß die Zahl $\sqrt{\mu^*}$ im Körper $K(\sqrt{\mu})$ liegt und wenn wir den gemeinsamen Idealteiler von $\mathfrak{p}$ und $\sqrt{\mu^*}$ mit $\mathfrak{P}$ bezeichnen, so ist

$$\mathfrak{P} = S\,\mathfrak{P}, \qquad \mathfrak{p} = \mathfrak{P}^2.$$

[1] Vgl. „Algebraische Zahlkörper" Satz 93 (dieser Band S. 154), woselbst dieser Satz allgemein für relativzyklische Körper von einem Primzahlgrade aufgestellt und bewiesen worden ist.

Das Ideal $\mathfrak{P}$ ist also ein ambiges Primideal und nach Satz 3 tritt dasselbe daher in der Relativdifferente $\mathfrak{D}$ des Körpers $K(\sqrt{\mu})$ als Faktor auf; es ist also die Relativdiskriminante $\mathfrak{d}$ durch $\mathfrak{p}$ teilbar.

Ist dagegen der Exponent a gerade, so stellt $\mu^* = \frac{\mu \nu^a}{\pi^a}$ eine zu $\mathfrak{p}$ prime ganze Zahl in k dar, von der Art, daß $\sqrt{\mu^*}$ in $K(\sqrt{\mu})$ liegt; da die Relativdiskriminante der Zahl $\sqrt{\mu^*}$ den Wert $2^2\mu^*$ hat, so ist sie zu $\mathfrak{p}$ prim. Das gleiche gilt mithin von der Relativdiskriminante $\mathfrak{d}$ des Körpers $K(\sqrt{\mu})$.

Jetzt betrachten wir die Verhältnisse in betreff des Primfaktors $\mathfrak{l}$. Ist die Kongruenz (1) erfüllt, so muß $\mathfrak{l}$ in der Zahl α^2 genau zur a-ten Potenz aufgehen und mithin ist der Exponent a eine gerade Zahl. Es sei nun λ eine durch $\mathfrak{l}$, aber nicht durch $\mathfrak{l}^2$ teilbare ganze Zahl in k und weiter sei ν eine durch $\frac{\lambda}{\mathfrak{l}}$ teilbare, aber zu $\mathfrak{l}$ prime ganze Zahl in k: der Ausdruck

$$\Omega = \left(\frac{\nu}{\lambda}\right)^{l+\frac{a}{2}}(\alpha + \sqrt{\mu})$$

stellt dann eine ganze Zahl in $K(\sqrt{\mu})$ dar, da die beiden Ausdrücke

$$\Omega + S\Omega = \left(\frac{\nu}{\lambda}\right)^{l+\frac{a}{2}} \cdot 2\alpha,$$

$$\Omega \cdot S\Omega = \left(\frac{\nu}{\lambda}\right)^{2l+a}(\alpha^2 - \mu)$$

offenbar ganze Zahlen in k sind. Andererseits hat die Relativdiskriminante der Zahl Ω den Wert

$$(\Omega - S\Omega)^2 = \left(\frac{\nu}{\lambda}\right)^{2l+a} \cdot 2^2\mu$$

und ist mithin prim zu $\mathfrak{l}$; das gleiche gilt also für die Relativdiskriminante des Körpers $K(\sqrt{\mu})$.

Setzen wir umgekehrt voraus, die Relativdiskriminante $\mathfrak{d}$ des Körpers $K(\sqrt{\mu})$ sei prim zu $\mathfrak{l}$, so folgt wegen

$$\begin{aligned}\mathfrak{d} &= (\Omega_1 - S\Omega_1, \quad \Omega_2 - S\Omega_2, \quad \ldots)^2 \\ &= ([\Omega_1 - S\Omega_1]^2, \ [\Omega_2 - S\Omega_2]^2, \ldots),\end{aligned}$$

daß dann notwendig im Körper $K(\sqrt{\mu})$ eine ganze Zahl Ω existieren muß, deren Relativdiskriminante $[\Omega - S\Omega]^2$ zu $\mathfrak{l}$ prim ausfällt; wir setzen

$$\Omega = \frac{\alpha^* + \beta^*\sqrt{\mu}}{\gamma^*},$$

wo $\alpha^*, \beta^*, \gamma^*$ ganze Zahlen in k bezeichnen, die bez. genau durch die a^*-te, b^*-te, c^*-te Potenz von $\mathfrak{l}$ aufgehen mögen. Da nun $[\Omega - S\Omega]^2 = \frac{2^2\beta^{*2}\mu}{\gamma^{*2}}$ eine zu $\mathfrak{l}$ prime ganze Zahl sein soll, so folgt

$$2l + 2b^* + a = 2c^*, \tag{2}$$

und da andererseits die Relativnorm $N(\Omega) = \frac{\alpha^{*2} - \beta^{*2}\mu}{\gamma^{*2}}$ eine ganze Zahl ist, so müssen entweder beide der Zahlen α^{*2} und $\beta^{*2}\mu$ genau durch die gleiche Potenz von $\mathfrak{l}$ aufgehen oder es müßte jede dieser beiden Zahlen mindestens durch $\mathfrak{l}^{2c^*}$ teilbar sein. Das letztere ist nicht der Fall, weil wegen der eben abgeleiteten Gleichung (2) jedenfalls $2b^* + a < 2c^*$ ausfällt und daher $\beta^{*2}\mu$ sicher nicht durch $\mathfrak{l}^{2c^*}$ teilbar sein kann. Es ist daher notwendigerweise $2a^* = 2b^* + a$ und mithin wegen (2) auch $2l + 2a^* = 2c^*$ oder $l + a^* = c^*$. Aus $2a^* = 2b^* + a$ folgt ferner $a^* \geqq b^*$ und aus $l + a^* = c^*$ folgt $c^* > a^*$; mithin ist auch $c^* > b^*$. Da $\frac{\alpha^{*2} - \beta^{*2}\mu}{\gamma^{*2}}$ eine ganze Zahl sein soll, so haben wir die Kongruenz

$$\mu \equiv \left(\frac{\alpha^*}{\beta^*}\right)^2, \qquad (\mathfrak{l}^{2c^*-2b^*}).$$

Wegen $a^* \geqq b^*$ läßt sich der Bruch $\frac{\alpha^*}{\beta^*}$ in der Gestalt eines Bruches schreiben, dessen Nenner zu $\mathfrak{l}$ prim ausfällt, und es ist somit $\frac{\alpha^*}{\beta^*}$ notwendig einer gewissen ganzen Zahl α des Körpers k nach $\mathfrak{l}^{2c^*-2b^*}$ kongruent, so daß auch die Kongruenz

$$\mu \equiv \alpha^2, \qquad (\mathfrak{l}^{2c^*-2b^*})$$

gilt. Hierdurch ist mit Rücksicht auf die aus (2) folgende Gleichung $2c^* - 2b^* = 2l + a$ die Richtigkeit des Satzes 4 vollständig gezeigt.

Aus diesem Satze 4 entnehmen wir leicht die folgende besondere Tatsache:

Satz 5. Wenn μ eine beliebige zu 2 prime ganze Zahl in k bedeutet, die nicht das Quadrat einer Zahl in k wird, so ist die Relativdiskriminante des Körpers $K(\sqrt{\mu})$ stets dann und nur dann zu 2 prim, wenn μ dem Quadrat einer ganzen Zahl in k nach dem Modul 2^2 kongruent wird.

§ 5. Die Zerlegung der Primideale des Grundkörpers k im relativquadratischen Körper K.

Die Frage, wie die Primideale des relativquadratischen Körpers K durch Zerlegung aus den Primidealen des Körpers k entstehen, erledigt sich in den folgenden Sätzen:

Satz 6. Ein Primideal $\mathfrak{p}$ des Körpers k ist stets dann und nur dann im Körper K gleich dem Quadrat eines Primideals $\mathfrak{P}$, wenn $\mathfrak{p}$ in der Relativdiskriminante des Körpers K aufgeht.

Beweis. Aus $\mathfrak{p} = \mathfrak{P}^2$ folgt $\mathfrak{p} = (S\mathfrak{P})^2$ und mithin $\mathfrak{P} = S\mathfrak{P}$, d. h. $\mathfrak{P}$ ist ein ambiges Primideal des Körpers K und als solches nach Satz 3 in der Relativdifferente des Körpers K enthalten, d. h. $\mathfrak{p}$ geht geht dann in der Relativdiskriminante auf.

Wenn wir umgekehrt annehmen, daß $\mathfrak{p}$ in der Relativdiskriminante des Körpers K aufgehe und mit $\mathfrak{P}$ einen in $\mathfrak{p}$ aufgehenden Primfaktor des Körpers K bezeichnen, so geht offenbar $\mathfrak{P}$ in der Relativdifferente des Körpers K auf und ist mithin nach Satz 3 ein ambiges Ideal, d. h. es ist nach Definition 3 $\mathfrak{P} = S\mathfrak{P}$ und $\mathfrak{p} \neq \mathfrak{P}$. Wegen dieser Beziehungen ist auch $\mathfrak{p}^2 \neq \mathfrak{P} \cdot S\mathfrak{P}$, und hieraus folgt $\mathfrak{p} = \mathfrak{P} \cdot S\mathfrak{P} = \mathfrak{P}^2$. Damit ist der Beweis für den Satz 6 erbracht.

Satz 7. Wenn $\mathfrak{p}$ ein Primideal des Körpers k bedeutet, welches weder in 2 noch in μ aufgeht, so ist $\mathfrak{p}$ im Körper $K(\sqrt{\mu})$ in zwei voneinander verschiedene Primideale weiter zerlegbar oder unzerlegbar, je nachdem μ im Körper k quadratischer Rest oder Nichtrest nach $\mathfrak{p}$ ist.

Beweis. Es sei μ in k quadratischer Rest nach $\mathfrak{p}$ und demgemäß etwa α eine ganze Zahl in k so, daß die Kongruenz

$$\mu \equiv \alpha^2, \qquad (\mathfrak{p})$$

gilt; alsdann bilden wir die zu einander relativkonjugierten Ideale des Körpers $K(\sqrt{\mu})$

$$\mathfrak{P} = (\mathfrak{p}, \alpha - \sqrt{\mu}),$$
$$S\mathfrak{P} = (\mathfrak{p}, \alpha + \sqrt{\mu})$$

und erhalten leicht

$$\mathfrak{p} = \mathfrak{P} \cdot S\mathfrak{P}.$$

Wegen

$$(\mathfrak{p}, \alpha - \sqrt{\mu}, \alpha + \sqrt{\mu}) = 1$$

sind $\mathfrak{P}$ und $S\mathfrak{P}$ von einander verschieden.

Es sei umgekehrt das Primideal $\mathfrak{p}$ des Körpers K in zwei Primideale $\mathfrak{P}$ und $S\mathfrak{P}$ zerlegbar: dann gelten, wenn allgemein N die Norm im Körper $K(\sqrt{\mu})$ und n die Norm im Körper k bezeichnet, die Gleichungen

$$N(\mathfrak{p}) = N(\mathfrak{P}) \cdot N(S\mathfrak{P}) = (N(\mathfrak{P}))^2,$$
$$N(\mathfrak{p}) = (n(\mathfrak{p}))^2$$

und mithin ist

$$N(\mathfrak{P}) = n(\mathfrak{p}).$$

Die Gleichheit dieser Normen $N(\mathfrak{P})$ und $n(\mathfrak{p})$ läßt die Tatsache erkennen, daß eine jede ganze Zahl des Körpers $K(\sqrt{\mu})$ einer ganzen Zahl des Körpers k nach $\mathfrak{P}$ kongruent gesetzt werden kann, da ja irgend $n(\mathfrak{p})$ nach $\mathfrak{p}$ einander inkongruente Zahlen zugleich auch in $K(\sqrt{\mu})$ nach $\mathfrak{P}$ ein volles Restsystem bilden müssen; setzen wir insbesondere $\sqrt{\mu} \equiv \alpha$ nach $\mathfrak{P}$, wo α in k liegen soll, so folgt $\mu \equiv \alpha^2$ nach $\mathfrak{P}$, und da $\mu - \alpha^2$ eine Zahl in k ist, so muß $\mu \equiv \alpha^2$ auch nach $\mathfrak{p}$ gelten, d. h. es ist μ quadratischer Rest nach $\mathfrak{p}$. Damit ist der Satz 7 vollständig bewiesen.

Satz 8. Es sei $\mathfrak{l}$ ein in 2 enthaltenes Primideal des Körpers k, und zwar gehe $\mathfrak{l}$ genau zur l-ten Potenz in 2 auf; ferner sei μ eine zu $\mathfrak{l}$ prime ganze Zahl in k, welche dem Quadrat einer ganzen Zahl in k nach $\mathfrak{l}^{2l}$ kongruent ausfällt, so daß nach Satz 4 das Primideal $\mathfrak{l}$ nicht in der Relativdiskriminante des Kör-

pers $K(\sqrt{\mu})$ vorkommt: dann ist $\mathfrak{l}$ im Körper $K(\sqrt{\mu})$ in zwei voneinander verschiedene Primideale weiter zerlegbar oder unzerlegbar, je nachdem μ dem Quadrat einer ganzen Zahl in k nach $\mathfrak{l}^{2l+1}$ kongruent ausfällt oder nicht.

Beweis. Ist $\mathfrak{l}$ in $K(\sqrt{\mu})$ weiter zerlegbar und bedeutet $\mathfrak{L}$ einen Primfaktor von $\mathfrak{l}$, so schließen wir aus der Gleichheit der Norm $N(\mathfrak{L})$ in $K(\sqrt{\mu})$ mit der Norm $n(\mathfrak{l})$ in k, wie im Beweise des Satzes 7, daß jede ganze Zahl in $K(\sqrt{\mu})$ einer ganzen Zahl in k nach $\mathfrak{L}$ kongruent sein muß. Nach Voraussetzung gibt es eine ganze Zahl α in k, so daß $\mu \equiv \alpha^2$ nach $\mathfrak{l}^{2l}$ ausfällt; ist dann λ irgendeine durch $\mathfrak{l}$, aber nicht durch $\mathfrak{l}^2$ teilbare ganze Zahl in k und weiter ν eine durch $\frac{\lambda}{\mathfrak{l}}$ teilbare, aber zu $\mathfrak{l}$ prime ganze Zahl in k, so stellt, wie wir dem Beweise des Satzes 4 entnehmen, der Ausdruck $\frac{\nu^l(\alpha+\sqrt{\mu})}{\lambda^l}$ eine ganze Zahl in $K(\sqrt{\mu})$ dar. Es gibt also nach dem vorhin Bewiesenen eine ganze Zahl β in k, für welche

$$\frac{\nu^l(\alpha+\sqrt{\mu})}{\lambda^l} \equiv \beta, \qquad (\mathfrak{L})$$

wird. Aus dieser Kongruenz schließen wir

$$\sqrt{\mu} \equiv -\alpha + \frac{\beta\lambda^l}{\nu^l}, \qquad (\mathfrak{l}^l\,\mathfrak{L}).$$

Mit Rücksicht auf den Umstand, daß ν zu $\mathfrak{l}$ prim ist, können wir in dieser Kongruenz den rechts stehenden Ausdruck durch eine ganze Zahl γ des Körpers k ersetzen und erhalten dann

$$\sqrt{\mu} \equiv \gamma \quad \text{oder} \quad \sqrt{\mu} - \gamma \equiv 0, \qquad (\mathfrak{l}^l\,\mathfrak{L}). \tag{1}$$

Da ferner $-\gamma \equiv +\gamma$ nach dem Modul 2 und folglich auch nach $\mathfrak{l}^l$ ausfällt, so gilt auch die Kongruenz

$$\sqrt{\mu} + \gamma \equiv 0, \qquad (\mathfrak{l}^l) \tag{2}$$

und durch Multiplikation erhalten wir schließlich aus den beiden Kongruenzen (1) und (2):

$$\mu - \gamma^2 \equiv 0, \qquad (\mathfrak{l}^{2l}\,\mathfrak{L}).$$

Da die linke Seite dieser Kongruenz eine ganze Zahl in k ist, so folgt auch

$$\mu - \gamma^2 = 0 \quad \text{oder} \quad \mu \equiv \gamma^2, \qquad (\mathfrak{l}^{2l+1})$$

womit eine Aussage des Satzes 8 bewiesen ist.

Nehmen wir nun umgekehrt an, es sei $\mu \equiv \alpha^2$ nach $\mathfrak{l}^{2l+1}$, wobei α eine ganze Zahl in k ist, so erkennen wir leicht die Richtigkeit der Gleichung

$$\mathfrak{l} = \left(\mathfrak{l}, \frac{\nu^l[\alpha+\sqrt{\mu}]}{\lambda^l}\right)\left(\mathfrak{l}, \frac{\nu^l[\alpha-\sqrt{\mu}]}{\lambda^l}\right)$$

und hier sind die beiden Primideale rechter Hand wegen

$$\left(\mathfrak{l}, \frac{\nu^l[\alpha+\sqrt{\mu}]}{\lambda^l}, \frac{\nu^l[\alpha-\sqrt{\mu}]}{\lambda^l}\right) = 1$$

in der Tat voneinander verschieden; damit ist der Satz 8 vollständig bewiesen.

§ 6. Das Symbol $\left(\frac{\mu}{\mathfrak{a}}\right)$.

Definition 4. Wir erweitern nunmehr die Bedeutung des in Definition 1 erklärten *Symbols* in folgender Weise:

Ist $\mathfrak{w}$ irgendein Primideal in k, so setzen wir

$$\left(\frac{\mu}{\mathfrak{w}}\right) = +1 \quad \text{oder} \quad = -1 \quad \text{oder} \quad = 0,$$

je nachdem $\mathfrak{w}$ im Körper $K(\sqrt{\mu})$ in zwei voneinander verschiedene Primideale weiter zerlegbar oder nicht zerlegbar oder gleich dem Quadrat eines Primideals wird. Ist μ das Quadrat einer Zahl in k, so setzen wir stets

$$\left(\frac{\mu}{\mathfrak{w}}\right) = +1.$$

Es ist nach den Sätzen 6, 7, 8 leicht möglich, in allen Fällen den Wert des Symbols $\left(\frac{\mu}{\mathfrak{w}}\right)$ zu berechnen und wir erkennen aus Satz 7 im Falle, daß $\mathfrak{w}$ zu 2 und μ prim ausfällt, die volle Übereinstimmung mit der Definition 1. Was insbesondere den Fall anbetrifft, daß $\mathfrak{w}$ gleich einem in 2 aufgehenden Primideal $\mathfrak{l}$ des Körpers k ist, so bestimmen wir zunächst die höchste Potenz von $\mathfrak{l}$, welche in μ aufgeht. Ist der Exponent a dieser Potenz ungerade, so haben wir gewiß $\left(\frac{\mu}{\mathfrak{l}}\right) = 0$; ist a dagegen gerade, so bestimmen wir, wenn λ eine durch $\mathfrak{l}$, aber nicht durch $\mathfrak{l}^2$ teilbare Zahl bedeutet, eine ganze zu $\mathfrak{l}$ prime Zahl μ^* in k der Art, daß

$$\mu = \lambda^a \mu^*, \qquad (\mathfrak{l}^{2l+a+1}).$$

Ist hier μ^* nicht dem Quadrat einer ganzen Zahl in k nach $\mathfrak{l}^{2l}$ kongruent, so haben wir mit Rücksicht auf die Sätze 4 und 6 ebenfalls $\left(\frac{\mu}{\mathfrak{l}}\right) = 0$; im anderen Fall unterscheiden wir, ob μ^* dem Quadrat einer ganzen Zahl in k auch nach $\mathfrak{l}^{2l+1}$ kongruent ausfällt oder nicht, und haben wegen Satz 8 dementsprechend $\left(\frac{\mu}{\mathfrak{l}}\right) = +1$ oder $= -1$.

Definition 5. Ist $\mathfrak{a}$ ein beliebiges Ideal des Körpers k und hat man $\mathfrak{a} = \mathfrak{p}\mathfrak{q}\ldots\mathfrak{w}$, wo $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{w}$ Primideale in k sind, so möge, wenn μ eine beliebige ganze Zahl in k 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, so gilt dann offenbar die Gleichung

$$\left(\frac{\mu}{\mathfrak{a}\mathfrak{b}}\right) = \left(\frac{\mu}{\mathfrak{a}}\right)\left(\frac{\mu}{\mathfrak{b}}\right).$$

Das Symbol $\left(\frac{\mu}{\mathfrak{a}}\right)$ ist durch diese Festsetzungen stets definiert, sobald μ irgendeine ganze Zahl in k und $\mathfrak{a}$ irgendein Ideal in k bedeutet. Das Symbol $\left(\frac{\mu}{\mathfrak{a}}\right)$ ist nur der Werte $+1, -1, 0$ fähig.

§ 7. Normenreste und Normennichtreste des Körpers K und das Symbol $\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$.

Definition 6. *Es sei* $\mathfrak{w}$ *irgendein Primideal in* k, *und es seien* ν, μ *beliebige ganze Zahlen in* k, *nur daß* μ *nicht gleich dem Quadrat einer Zahl in* k *ausfällt: wenn dann* ν *nach* $\mathfrak{w}$ *der Relativnorm einer ganzen Zahl des Körpers* $K(\sqrt{\mu})$ *kongruent ist und wenn außerdem auch für jede höhere Potenz von* $\mathfrak{w}$ *stets eine solche ganze Zahl* A *im Körper* $K(\sqrt{\mu})$ *gefunden werden kann, daß* $\nu \equiv N(\mathsf{A})$ *nach jener Potenz von* $\mathfrak{w}$ *ausfällt, so nenne ich* ν *einen Normenrest des Körpers* $K(\sqrt{\mu})$ *nach* $\mathfrak{w}$. *In jedem anderen Falle nenne ich* ν *einen Normennichtrest des Körpers* $K(\sqrt{\mu})$ *nach* $\mathfrak{w}$.

Ich definiere das Symbol $\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$, *indem ich*

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = +1 \quad \text{oder} \quad = -1$$

setze, je nachdem ν *Normenrest oder Normennichtrest nach* $\mathfrak{w}$ *ist. Fällt* μ *gleich dem Quadrat einer ganzen Zahl in* k *aus, so werde stets*

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = +1$$

gesetzt.

Das neue Symbol $\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$ ist durch diese Festsetzungen in jedem Falle definiert, sobald ν, μ irgend zwei ganze Zahlen des Körpers k und $\mathfrak{w}$ irgendein Primideal des Körpers k bedeuten. Das Symbol $\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$ ist nur der beiden Werte $+1$ oder -1 fähig.

§ 8. Eigenschaften des Symbols $\left(\frac{\nu, \mu}{\mathfrak{p}}\right)$.

In den folgenden Sätzen entwickeln wir einige Eigenschaften des Symbols $\left(\frac{\nu, \mu}{\mathfrak{p}}\right)$ für den Fall, daß $\mathfrak{p}$ ein nicht in 2 aufgehendes Primideal bedeutet.

Satz 9. Wenn ν, μ irgend beliebige ganze Zahlen in k bedeuten und $\mathfrak{p}$ ein Primideal des Körpers k ist, das zu 2 und zu ν prim ausfällt, aber in μ genau zur ersten Potenz aufgeht, so gilt stets die Gleichung

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\nu}{\mathfrak{p}}\right).$$

Beweis. Ist $\left(\frac{\nu}{\mathfrak{p}}\right) = +1$, so gibt es nach Definition 1 eine ganze Zahl α in k, für welche $\nu \equiv \alpha^2$ nach $\mathfrak{p}$ wird. Um zu zeigen, daß dann die Kongruenz $\nu \equiv \xi^2$ auch nach jeder beliebigen Potenz von $\mathfrak{p}$ durch geeignete Wahl von ξ lösbar ist, setzen wir

$$\frac{\nu}{\alpha^2} \equiv 1 + 2\omega, \qquad (\mathfrak{p}^2),$$

so daß dabei ω eine ganze durch $\mathfrak{p}$ teilbare Zahl in k bedeutet. Die ganze Zahl $\alpha' = \alpha(1+\omega)$, erfüllt dann die Bedingung

$$\nu \equiv \alpha'^2, \qquad (\mathfrak{p}^2).$$

Durch gehörige Fortsetzung dieses Verfahrens erkennen wir, daß für jeden Exponenten e eine ganze Zahl $\alpha^{(e-1)}$ existiert, so daß

$$\nu \equiv (\alpha^{(e-1)})^2, \qquad (\mathfrak{p}^e)$$

ausfällt. Setzen wir $\mathsf{A} \equiv \alpha^{(e-1)}$, so folgt

$$\nu \equiv N(\mathsf{A}), \qquad (\mathfrak{p}^e),$$

d. h. es hat unter der obigen Annahme das Symbol $\left(\frac{\nu, \mu}{\mathfrak{p}}\right)$ den Wert $+1$.

Machen wir umgekehrt die Annahme $\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = +1$, so gibt es nach Definition 6 eine ganze Zahl A in $K(\sqrt{\mu})$, für welche $\nu \equiv N(\mathsf{A})$ nach $\mathfrak{p}$ wird. Da nach Satz 4 das Primideal $\mathfrak{p}$ in der Relativdiskriminante des Körpers $K(\sqrt{\mu})$ aufgeht, so ist nach Satz 6 das Primideal $\mathfrak{p}$ gleich dem Quadrat eines Primideals $\mathfrak{P}$ im Körper $K(\sqrt{\mu})$. Aus der Gleichung $\mathfrak{p} = \mathfrak{P}^2$ folgt die Gleichheit der Normen $n(\mathfrak{p})$ in k und $N(\mathfrak{P})$ in $K(\sqrt{\mu})$ und wie im Beweise des Satzes 7 schließen wir dann auch hier, daß jede ganze Zahl des Körpers $K(\sqrt{\mu})$ einer ganzen Zahl des Körpers k nach $\mathfrak{P}$ kongruent sein muß. Setzen wir insbesondere $\mathsf{A} \equiv \alpha$ nach $\mathfrak{P}$, wo α eine ganze Zahl in k ist, so folgt

$$\nu \equiv N(\mathsf{A}) \equiv \alpha^2, \qquad (\mathfrak{P})$$

und daher ist auch $\nu \equiv \alpha^2$ nach $\mathfrak{p}$, d. h. unter der gegenwärtigen Annahme erhalten wir $\left(\frac{\nu}{\mathfrak{p}}\right) = +1$; hiermit und durch das vorhin Bewiesene wird der Satz 9 vollständig als richtig erkannt.

Satz 10. Wenn ν, μ zwei beliebige ganze Zahlen in k bedeuten und $\mathfrak{p}$ ein weder in ν noch in μ noch in 2 aufgehendes Primideal in k ist, so gilt stets die Gleichung

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = +1.$$

Beweis. Nach Satz 4 geht $\mathfrak{p}$ nicht in der Relativdiskriminante des Körpers $K(\sqrt{\mu})$ auf; wir haben demgemäß nur zwei Annahmen zu behandeln, je nachdem $\mathfrak{p}$ in zwei voneinander verschiedene Primideale des Körpers $K(\sqrt{\mu})$ zerlegbar ist oder in $K(\sqrt{\mu})$ unzerlegbar bleibt.

Wir nehmen zunächst $\mathfrak{p}$ als zerlegbar an, und zwar sei $\mathfrak{p} = \mathfrak{P} \cdot S\mathfrak{P}$, wo $\mathfrak{P}$ ein Primideal des Körpers $K(\sqrt{\mu})$ bedeutet. Es gibt dann gewiß in $K(\sqrt{\mu})$ ein System von zwei ganzen Zahlen, $\mathsf{A}_1, \mathsf{A}_2$, für welche die beiden in $\mathsf{A}_1, \mathsf{A}_2$ linearen Kongruenzen

$$\left.\begin{aligned} \mathsf{A}_1 + \mathsf{A}_2\sqrt{\mu} &\equiv \nu \\ \mathsf{A}_1 - \mathsf{A}_2\sqrt{\mu} &\equiv 1, \end{aligned}\right\} \qquad (\mathfrak{P}) \qquad (1)$$

erfüllt sind. Nun können wir wegen der Gleichheit der Normen $n(\mathfrak{p})$ und $N(\mathfrak{P})$, wie im Beweise zu Satz 7 und zu Satz 9, jede ganze Zahl in $K(\sqrt{\mu})$ einer ganzen Zahl des Körpers k nach $\mathfrak{P}$ kongruent setzen; es sei demgemäß

$$\mathsf{A}_1 = \alpha_1, \quad \mathsf{A}_2 \equiv \alpha_2, \qquad (\mathfrak{P}), \tag{2}$$

wo α_1, α_2 ganze Zahlen in k sind. Wenn wir dann zur Abkürzung

$$\mathsf{A} = \alpha_1 + \alpha_2\sqrt{\mu}$$

setzen, so folgt wegen (2) durch Multiplikation der Kongruenzen (1) die Kongruenz

$$\nu \equiv N(\mathsf{A}), \qquad (\mathfrak{P})$$

und da beide Seiten dieser Kongruenz ganze Zahlen in k sind, so gilt sie auch nach dem Modul $\mathfrak{p}$. Um zu beweisen, daß die Kongruenz $\nu \equiv N(\Xi)$ durch geeignete Wahl der ganzen Zahl Ξ in $K(\sqrt{\mu})$ auch nach jeder Potenz $\mathfrak{p}^e$ des Primideals $\mathfrak{p}$ lösbar ist, zeigen wir, wie im Beweise zu Satz 9, die Existenz einer Zahl ξ, welche der Kongruenz

$$\frac{\nu}{N(\mathsf{A})} \equiv \xi^2, \qquad (\mathfrak{p}^e)$$

genügt; dann ist offenbar $\nu \equiv N(\xi\mathsf{A})$ nach $\mathfrak{p}^e$.

Es sei andererseits $\mathfrak{p}$ im Körper $K(\sqrt{\mu})$ nicht weiter zerlegbar und somit nach Satz 7 die Zahl μ quadratischer Nichtrest nach $\mathfrak{p}$. Nach Satz 2 gibt es in k genau $f = \frac{n(\mathfrak{p})-1}{2}$ quadratische Reste nach $\mathfrak{p}$; es seien diese durch die Quadratzahlen $\alpha_1^2, \alpha_2^2, \ldots, \alpha_f^2$ vertreten. Wir unterscheiden nun zwei Fälle, je nachdem die Zahl -1 quadratischer Rest oder Nichtrest nach $\mathfrak{p}$ ist.

Im ersteren Falle sind wegen unserer Annahme über μ die $n(\mathfrak{p})-1$ Zahlen

$$\alpha_1^2, \alpha_2^2, \ldots, \alpha_f^2, \quad -\alpha_1^2\mu, -\alpha_2^2\mu, \ldots, -\alpha_f^2\mu \tag{3}$$

sämtlich nach $\mathfrak{p}$ untereinander inkongruent. Es ist daher jede zu $\mathfrak{p}$ prime ganze Zahl in k einer der Zahlen (3) nach $\mathfrak{p}$ kongruent. Die Zahlen (3) sind bez. die Relativnormen der Zahlen

$$\alpha_1, \alpha_2, \ldots, \alpha_f, \quad \alpha_1\sqrt{\mu}, \alpha_2\sqrt{\mu}, \ldots, \alpha_f\sqrt{\mu}$$

und es ist mithin jede zu $\mathfrak{p}$ prime Zahl in k der Relativnorm einer geeigneten ganzen Zahl in $K(\sqrt{\mu})$ nach $\mathfrak{p}$ kongruent.

Ist -1 quadratischer Nichtrest nach $\mathfrak{p}$, so wird $-\mu$ quadratischer Rest nach $\mathfrak{p}$; es sei $-\mu \equiv \beta^2$ nach $\mathfrak{p}$, wo β eine ganze Zahl in k bedeutet. In der Reihe der ganzen rationalen positiven Zahlen

$$1, 2, 3, \ldots, n(\mathfrak{p})-1$$

ist die letzte Zahl Nichtrest nach $\mathfrak{p}$; es sei r die erste Zahl dieser Reihe, auf welche ein Nichtrest des Primideals $\mathfrak{p}$ folgt. Wir setzen $r \equiv \alpha^2$ nach $\mathfrak{p}$, wo α eine ganze Zahl in k bedeutet: dann ist die ganze Zahl $\alpha^2\beta^2 - \mu$ wegen

$$\alpha^2\beta^2 - \mu = r\beta^2 + \beta^2 \equiv (r+1)\beta^2, \qquad (\mathfrak{p})$$

sicher quadratischer Nichtrest nach $\mathfrak{p}$, und es fallen folglich die $n(\mathfrak{p})-1$ Zahlen

$$\alpha_1^2, \alpha_2^2, \ldots, \alpha_f^2, \quad \alpha_1^2(\alpha^2\beta^2-\mu), \alpha_2^2(\alpha^2\beta^2-\mu), \ldots, \alpha_f^2(\alpha^2\beta^2-\mu) \tag{4}$$

sämtlich untereinander inkongruent nach $\mathfrak{p}$ aus. In diesem Falle ist also jede zu $\mathfrak{p}$ prime Zahl in k einer der Zahlen (4) nach $\mathfrak{p}$ kongruent. Die Zahlen (4) sind aber bez. die Relativnormen der Zahlen

$$\alpha_1, \alpha_2, \ldots, \alpha_f, \quad \alpha_1(\alpha\beta+\sqrt{\mu}), \alpha_2(\alpha\beta+\sqrt{\mu}), \ldots, \alpha_f(\alpha\beta+\sqrt{\mu}),$$

und es ist mithin jede zu $\mathfrak{p}$ prime ganze Zahl in k der Relativnorm einer ganzen Zahl in $K(\sqrt{\mu})$ kongruent. Hieraus schließt man weiter, wie im ersten Teil dieses Beweises, daß zu jeder nicht durch $\mathfrak{p}$ teilbaren Zahl ν des Körpers k auch für eine beliebig hohe Potenz $\mathfrak{p}^e$ des Primideals $\mathfrak{p}$ stets eine ganze Zahl in $K(\sqrt{\mu})$ gefunden werden kann, deren Relativnorm der Zahl ν nach $\mathfrak{p}^e$ kongruent ist. Damit ist Satz 10 in allen Fällen bewiesen.

Satz 11. Wenn ν, μ zwei beliebige ganze Zahlen in k bedeuten und $\mathfrak{p}$ ein Primideal des Körpers k ist, das zu 2 und zu μ prim ausfällt, aber in ν genau zur ersten Potenz aufgeht, so gilt stets die Gleichung

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\mu}{\mathfrak{p}}\right).$$

Beweis. Ist $\left(\frac{\mu}{\mathfrak{p}}\right) = +1$, so wird nach Satz 7 das Primideal $\mathfrak{p}$ des Körpers k in zwei voneinander verschiedene Primideale $\mathfrak{P}$ und $S\mathfrak{P}$ des Körpers $K(\sqrt{\mu})$ weiter zerlegbar. Wir bestimmen eine ganze Zahl A in $K(\sqrt{\mu})$, welche durch $\mathfrak{P}$, aber weder durch $\mathfrak{P}^2$ noch durch $S\mathfrak{P}$ teilbar ist; dann geht die Relativnorm $\alpha = N(\mathsf{A})$ der Zahl A genau durch die erste Potenz von $\mathfrak{p}$ auf. Es sei ϱ eine durch $\frac{\alpha}{\mathfrak{p}}$ teilbare, aber zu $\mathfrak{p}$ prime ganze Zahl in k, dann ist $\frac{\nu\varrho^2}{\alpha}$ eine ganze zu $\mathfrak{p}$ prime Zahl und daher zufolge des Satzes 10 Normenrest des Körpers $K(\sqrt{\mu})$ nach $\mathfrak{p}$. Bedeutet $\mathfrak{p}^e$ eine beliebige Potenz von $\mathfrak{p}$ und setzen wir

$$\frac{\nu\varrho^2}{\alpha} \equiv N(\mathsf{P}), \qquad (\mathfrak{p}^e),$$

wo P eine ganze Zahl in $K(\sqrt{\mu})$ bedeutet, und bestimmen dann ϱ^* als ganze Zahl in k, so daß $\varrho\varrho^* \equiv 1$ nach $\mathfrak{p}^e$ ausfällt, so wird offenbar

$$\nu \equiv N(\varrho^*\mathsf{P}\mathsf{A}), \qquad (\mathfrak{p}^e)$$

d. h. es ist ν Normenrest des Körpers $K(\sqrt{\mu})$ nach $\mathfrak{p}$.

Umgekehrt, wenn ν Normenrest des Körpers $K(\sqrt{\mu})$ ist und etwa $\nu \equiv N(\Omega)$ nach $\mathfrak{p}^2$ ausfällt, wo Ω eine ganze Zahl in $K(\sqrt{\mu})$ ist, so geht $N(\Omega)$ wegen der über ν gemachten Annahme nur durch die erste Potenz von $\mathfrak{p}$ auf; wir haben daher offenbar

$$\mathfrak{p} = (\mathfrak{p}, \Omega)\cdot(\mathfrak{p}, S\Omega),$$

d. h. $\mathfrak{p}$ zerfällt in $K(\sqrt{\mu})$ in ein Produkt von zwei Idealen und mithin ist nach Satz 7 $\left(\frac{\mu}{\mathfrak{p}}\right) = +1$. Damit ist der Satz 11 vollständig bewiesen.

Satz 12. Es sei $\mathfrak{p}$ ein zu 2 primes Primideal des Körpers k, ferner seien ν, μ, ν^*, μ^* vier ganze Zahlen in k von der Beschaffenheit, daß $\frac{\mu}{\mu^*}$ das Quadrat einer ganzen oder gebrochenen Zahl in k und $\frac{\nu}{\nu^*}$ die Relativnorm einer ganzen oder gebrochenen Zahl des Körpers $K(\sqrt{\mu})$ wird: dann gilt stets die Gleichung

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\nu^*, \mu^*}{\mathfrak{p}}\right).$$

Beweis. Zunächst bemerken wir, daß wegen der Definition 6 des Symbols $\left(\frac{\nu, \mu}{\mathfrak{p}}\right)$ offenbar stets die Gleichung

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\nu, \mu^*}{\mathfrak{p}}\right) \tag{5}$$

gilt, da offenbar der durch $\sqrt{\mu^*}$ bestimmte relativquadratische Körper mit dem Körper $K(\sqrt{\mu})$ übereinstimmt.

Ferner wollen wir beweisen, daß, wenn γ die Relativnorm $N(\Gamma)$ einer ganzen Zahl Γ des Körpers $K(\sqrt{\mu})$ ist, stets

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\gamma\nu, \mu}{\mathfrak{p}}\right) \tag{6}$$

ausfällt.

In der Tat, wenn ν Normenrest des Körpers $K(\sqrt{\mu})$ nach $\mathfrak{p}$ ist, so wird offenbar auch $\gamma\nu$ Normenrest dieses Körpers nach $\mathfrak{p}$. Die umgekehrte Annahme, daß $\gamma\nu$ Normenrest des Körpers $K(\sqrt{\mu})$ nach $\mathfrak{p}$ ist, behandeln wir in folgender Weise: Es gehe ν genau durch die b-te Potenz von $\mathfrak{p}$ und γ genau durch die c-te Potenz von $\mathfrak{p}$ auf; es sei ferner Ω eine ganze Zahl in $K(\sqrt{\mu})$, so daß die Kongruenz

$$\nu\gamma \equiv N(\Omega), \qquad (\mathfrak{p}^{c+e}) \tag{7}$$

gilt, wobei e einen beliebigen Exponenten der größer als b ist, bedeutet. Wir unterscheiden nun drei Fälle, je nachdem $\mathfrak{p}$ im Körper $K(\sqrt{\mu})$ Primideal bleibt oder in zwei gleiche oder in zwei voneinander verschiedene Primideale des Körpers $K(\sqrt{\mu})$ weiter zerlegbar ist.

Im ersten Falle muß wegen $\gamma = N(\Gamma)$ der Exponent c gerade sein und $\mathfrak{p}$ in Γ genau zur $\frac{c}{2}$-ten Potenz aufgehen; ferner erkennen wir aus (7), daß Ω genau durch die $\frac{c+b}{2}$-te Potenz von $\mathfrak{p}$ teilbar sein muß. Nun sei α eine durch $\frac{\gamma}{\mathfrak{p}^c}$ teilbare, aber zu $\mathfrak{p}$ prime ganze Zahl in k. Dann ist $\mathsf{A} = \frac{\alpha\Omega}{\Gamma}$ gewiß eine ganze Zahl in $K(\sqrt{\mu})$ und wir erhalten $\alpha^2\nu \equiv N(\mathsf{A})$ nach $\mathfrak{p}^e$. Bestimmen wir noch eine ganze Zahl α^* in k, so daß $\alpha\alpha^* \equiv 1$ nach $\mathfrak{p}^e$ ausfällt, so folgt $\nu \equiv N(\alpha^*\mathsf{A})$ nach $\mathfrak{p}^e$, d. h. ν ist Normenrest des Körpers $K(\sqrt{\mu})$ nach $\mathfrak{p}$.

Im zweiten Falle setzen wir $\mathfrak{p} = \mathfrak{P}^2$, so daß $\mathfrak{P}$ ein Primideal in $K(\sqrt{\mu})$ bedeutet. Wegen $\gamma = N(\Gamma)$ geht in Γ genau die c-te Potenz von $\mathfrak{P}$ auf und wegen der Kongruenz (7) geht in Ω genau die $(c+b)$-te Potenz von $\mathfrak{P}$ auf. Wir bestimmen nun eine Zahl α in k wie im ersten Falle, und gelangen dann durch die entsprechenden Schlüsse wiederum zu dem Resultat, daß ν Normenrest des Körpers $K(\sqrt{\mu})$ nach $\mathfrak{p}$ sein muß.

Im dritten Falle endlich setzen wir $\mathfrak{p} = \mathfrak{P} \cdot S\mathfrak{P}$, wo $\mathfrak{P}$ ein Primideal des Körpers $K(\sqrt{\mu})$ bedeutet, welches von seinem relativkonjugierten Primideale $S\mathfrak{P}$ verschieden ausfällt. Nun gehe in Γ das Primideal $\mathfrak{P}$ genau zur C-ten und das Primideal $S\mathfrak{P}$ genau zur C'-ten Potenz auf; ferner gehe in Ω das Primideal $\mathfrak{P}$ genau zur U-ten und $S\mathfrak{P}$ genau zur U'-ten Potenz auf; es ist dann $c = C + C'$ und $c + b = U + U'$, und folglich

$$U + U' \geqq C + C'. \tag{8}$$

Wir bilden jetzt in $K(\sqrt{\mu})$ eine ganze Zahl A, die genau durch die C-te Potenz von $\mathfrak{P}$ und durch die U-te Potenz von $S\mathfrak{P}$ teilbar ist, und endlich eine ganze Zahl α in k, die durch $\frac{\Gamma \cdot S\mathsf{A}}{\mathfrak{P}^{U+C}\, S\mathfrak{P}^{C+C'}}$ teilbar ist, aber zu $\mathfrak{p}$ prim ausfällt. Wegen der Ungleichung (8) ist dann $\mathsf{B} = \frac{\alpha\Omega\,\mathsf{A}}{\Gamma \cdot S\mathsf{A}}$ gewiß eine ganze Zahl in $K(\sqrt{\mu})$ und wir erhalten $\alpha^2\nu \equiv N(\mathsf{B})$ nach $\mathfrak{p}^e$. Bestimmen wir also noch eine ganze Zahl α^* in k, so daß $\alpha\alpha^* \equiv 1$ nach $\mathfrak{p}^e$ ausfällt, so folgt $\nu \equiv N(\alpha^*\mathsf{B})$ nach $\mathfrak{p}^e$, d. h. ν ist Normenrest des Körpers $K(\sqrt{\mu})$ nach $\mathfrak{p}$. Damit ist die Richtigkeit der in Formel (6) ausgesprochenen Behauptung in allen Fällen als richtig erkannt.

Wegen der über $\frac{\nu}{\nu^*}$ gemachten Voraussetzung dürfen wir $\frac{\nu}{\nu^*} = \frac{\gamma^*}{\gamma}$ oder $\nu\gamma = \nu^*\gamma^*$ setzen, wobei γ, γ^* Relativnormen gewisser ganzer Zahlen in $K(\sqrt{\mu^*})$ bedeuten. Mit Hilfe der eben bewiesenen Formel (6) erhalten wir

$$\left(\frac{\nu, \mu^*}{\mathfrak{p}}\right) = \left(\frac{\gamma\nu, \mu^*}{\mathfrak{p}}\right) \quad \text{und} \quad \left(\frac{\nu^*, \mu^*}{\mathfrak{p}}\right) = \left(\frac{\gamma^*\nu^*, \mu^*}{\mathfrak{p}}\right);$$

mithin ist auch

$$\left(\frac{\nu, \mu^*}{\mathfrak{p}}\right) = \left(\frac{\nu^*, \mu^*}{\mathfrak{p}}\right).$$

Die letztere Formel und die Formel (5) zusammen zeigen die Richtigkeit des Satzes 12.

§ 9. Die allgemeinen Grundformeln für das Symbol $\left(\frac{\nu, \mu}{\mathfrak{p}}\right)$.

Aus den in § 8 entwickelten Eigenschaften des Symbols $\left(\frac{\nu, \mu}{\mathfrak{p}}\right)$ können wir ein System von Grundformeln für dieses Symbol herleiten unter der Voraussetzung, daß dabei $\mathfrak{p}$ ein in 2 nicht aufgehendes Primideal bedeutet.

Satz 13. *Es sei $\mathfrak{p}$ ein zu 2 primes Primideal des Körpers k und ν, μ seien zwei beliebige ganze Zahlen in k; geht das Primideal $\mathfrak{p}$ in diesen Zahlen ν, μ genau zur b-ten, bez. a-ten Potenz auf, so bilde man die Zahl $\frac{\nu^a}{\mu^b}$ und bringe die-*

selbe in die Gestalt eines Bruches $\frac{\varrho}{\sigma}$, dessen Zähler ϱ und dessen Nenner σ nicht durch $\mathfrak{p}$ teilbar sind: dann gilt stets die Gleichung

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{(-1)^{a\,b}\,\varrho\,\sigma}{\mathfrak{p}}\right).$$

Beweis. Die Sätze 9, 10, 11 zeigen unmittelbar, daß der Satz 13 für $a = 1, b = 0$, für $a = 0, b = 0$ und für $a = 0, b = 1$ gilt. Im Falle $a = 1$, $b = 1$ haben wir $\frac{\nu}{\mu} = \frac{\varrho}{\sigma}$ zu setzen; da nun

$$\frac{\nu}{-\varrho\,\sigma} = -\frac{\mu}{\sigma^2}$$

die Relativnorm der Zahl $\sqrt{\frac{\mu}{\sigma}}$ ist, so ergibt sich nach Satz 12

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{-\varrho\,\sigma, \mu}{\mathfrak{p}}\right),$$

und da andererseits nach Satz 9

$$\left(\frac{-\varrho\,\sigma, \mu}{\mathfrak{p}}\right) = \left(\frac{-\varrho\,\sigma}{\mathfrak{p}}\right)$$

ist, so folgt auch für diesen Fall die Richtigkeit des Satzes 13.

Sind nun a, b beliebige ganze rationale nicht negative Exponenten, so möge a^* den Wert 0 oder 1 bedeuten, je nachdem a gerade oder ungerade ausfällt, und entsprechend möge b^* den Wert 0 oder 1 bedeuten, je nachdem b gerade oder ungerade ausfällt. Wir bestimmen jetzt im Körper k eine ganze Zahl ν^*, in der genau die b^*-te Potenz von $\mathfrak{p}$ aufgeht, und eine Zahl μ^*, in der genau die a^*-te Potenz von $\mathfrak{p}$ aufgeht von der Beschaffenheit, daß $\frac{\nu}{\nu^*}$ und $\frac{\mu}{\mu^*}$ Quadrate von Zahlen in k sind; dann setzen wir $\frac{\nu^{*a^*}}{\mu^{*b^*}}$ gleich einem Bruche $\frac{\varrho^*}{\sigma^*}$, dessen Zähler ϱ^* und dessen Nenner σ^* ganze zu $\mathfrak{p}$ prime Zahlen in k sind, und erkennen leicht, daß in der Zahlenreihe

$$\varrho^*\sigma^*, \quad \frac{\varrho^*}{\sigma^*}, \quad \frac{\nu^{*a^*}}{\mu^{*b^*}}, \quad \frac{\nu^{*a}}{\mu^{*b}}, \quad \frac{\nu^a}{\mu^b}, \quad \frac{\varrho}{\sigma}, \quad \varrho\,\sigma$$

jede Zahl durch die darauffolgende dividiert, gleich dem Quadrat einer Zahl des Körpers k wird; wir schließen hieraus, daß auch der Quotient der ersten Zahl $\varrho^*\sigma^*$ und der letzten $\varrho\sigma$ in jener Reihe gleich dem Quadrat einer gewissen Zahl $\varkappa$ des Körpers k sein muß. Da andererseits diese Zahlen beide zu $\mathfrak{p}$ prim sind, so läßt sich notwendig auch $\varkappa$ in die Gestalt eines Bruches $\frac{\psi}{\psi^*}$ setzen, dessen Zähler ψ und dessen Nenner ψ^* ganze zu $\mathfrak{p}$ prime Zahlen in k sind. Wir erhalten mithin $\psi^{*2}\varrho^*\sigma^* = \psi^2\varrho\sigma$ und folglich ist $\left(\frac{\varrho^*\sigma^*}{\mathfrak{p}}\right) = \left(\frac{\varrho\,\sigma}{\mathfrak{p}}\right)$; da ferner $(-1)^{a\,b} = (-1)^{a^*b^*}$ ausfällt, so ist auch

$$\left(\frac{(-1)^{a^*b^*}\varrho^*\sigma^*}{\mathfrak{p}}\right) = \left(\frac{(-1)^{a\,b}\varrho\,\sigma}{\mathfrak{p}}\right). \tag{1}$$

Weiter ist nach Satz 12

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\nu^*, \mu^*}{\mathfrak{p}}\right), \tag{2}$$

und da nach dem ersten Teil des gegenwärtigen Beweises der Satz 13 auf die Zahlen ν^*, μ^* angewandt werden darf, so gilt die Gleichung

$$\left(\frac{\nu^*, \mu^*}{\mathfrak{p}}\right) = \left(\frac{(-1)^{a^*b^*}\,\varrho^*\,\sigma^*}{\mathfrak{p}}\right). \tag{3}$$

Aus den Formeln (1), (2), (3) folgt die Richtigkeit des Satzes 13 allgemein.

Aus Satz 13 ergeben sich für das Symbol $\left(\frac{\nu, \mu}{\mathfrak{p}}\right)$ eine Reihe von wichtigen Formeln, die wir in folgendem Satze zusammenstellen:

Satz 14. *Wenn $\nu, \nu_1, \nu_2, \mu, \mu_1, \mu_2$ beliebige ganze Zahlen des Körpers k sind, so gelten in bezug auf irgendein zu 2 primes Primideal $\mathfrak{p}$ des Körpers k stets die Formeln:*

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\mu, \nu}{\mathfrak{p}}\right),$$

$$\left(\frac{\nu_1\nu_2, \mu}{\mathfrak{p}}\right) = \left(\frac{\nu_1, \mu}{\mathfrak{p}}\right)\left(\frac{\nu_2, \mu}{\mathfrak{p}}\right),$$

$$\left(\frac{\nu, \mu_1\mu_2}{\mathfrak{p}}\right) = \left(\frac{\nu, \mu_1}{\mathfrak{p}}\right)\left(\frac{\nu, \mu_2}{\mathfrak{p}}\right).$$

Beweis. Die erste Formel folgt unmittelbar aus Satz 13.

Um die zweite Formel zu beweisen, nehmen wir an, es gehe das Primideal $\mathfrak{p}$ in ν_1, ν_2, μ bez. genau zur b_1-ten, b_2-ten, a-ten Potenz auf, und setzen dann

$$\frac{\nu_1^a}{\mu^{b_1}} = \frac{\varrho_1}{\sigma_1}, \qquad \frac{\nu_2^a}{\mu^{b_2}} = \frac{\varrho_2}{\sigma_2},$$

so daß $\varrho_1, \sigma_1, \varrho_2, \sigma_2$ ganze zu $\mathfrak{p}$ prime Zahlen in k sind. Nach Satz 13 erhalten wir

$$\left(\frac{\nu_1, \mu}{\mathfrak{p}}\right) = \left(\frac{(-1)^{a\,b_1}\,\varrho_1\,\sigma_1}{\mathfrak{p}}\right),$$

$$\left(\frac{\nu_2, \mu}{\mathfrak{p}}\right) = \left(\frac{(-1)^{a\,b_2}\,\varrho_2\,\sigma_2}{\mathfrak{p}}\right),$$

$$\left(\frac{\nu_1\nu_2, \mu}{\mathfrak{p}}\right) = \left(\frac{(-1)^{a(b_1+b_2)}\,\varrho_1\,\varrho_2\,\sigma_1\,\sigma_2}{\mathfrak{p}}\right)$$

und diese Gleichungen zeigen die Richtigkeit der zweiten Formel.

Die dritte Formel ist eine unmittelbare Folge der ersten und zweiten.

Im Lauf der gegenwärtigen Untersuchung werden wir erkennen, daß die Formeln des Satzes 14 auch für jedes in 2 aufgehende Primideal des Körpers k gültig sind.

§ 10. Die Anzahl der Normenreste nach einem nicht in 2 aufgehenden Primideal.

Satz 15. Wenn $\mathfrak{p}$ ein zu 2 primes Primideal des Körpers k ist, das nicht in der Relativdiskriminante des relativquadratischen Körpers $K(\sqrt{\mu})$ aufgeht, so ist jede zu $\mathfrak{p}$ prime Zahl ν Normenrest des Körpers $K(\sqrt{\mu})$ nach $\mathfrak{p}$.

Wenn dagegen $\mathfrak{p}$ ein zu 2 primes Primideal des Körpers k ist, das in der Relativdiskriminante des Körpers $K(\sqrt{\mu})$ aufgeht und wenn e ein beliebiger positiver Exponent bedeutet, so sind von allen vorhandenen zu $\mathfrak{p}$ primen und nach $\mathfrak{p}^e$ einander inkongruenten Zahlen in k genau die Hälfte Normenreste des Körpers $K(\sqrt{\mu})$.

Beweis. Es gehe $\mathfrak{p}$ in μ genau zur a-ten Potenz auf. Soll zunächst $\mathfrak{p}$ zur Relativdiskriminante des Körpers $K(\sqrt{\mu})$ prim ausfallen, so muß nach Satz 4 a eine gerade Zahl sein; da ferner nach Voraussetzung ν zu $\mathfrak{p}$ prim ist, so können wir bei Anwendung des Satzes 13 zur Bestimmung des Symbols $\left(\frac{\nu, \mu}{\mathfrak{p}}\right)$ einfach $\varrho = \nu^a$ und $\sigma = 1$ setzen und erhalten dann

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\nu^a}{\mathfrak{p}}\right) = +1,$$

womit der erste Teil des Satzes 15 bewiesen ist.

Soll andererseits $\mathfrak{p}$ in der Relativdiskriminante des Körpers $K(\sqrt{\mu})$ aufgehen, so ist nach Satz 4 der Exponent a eine ungerade Zahl; mithin haben wir nach Satz 13

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\nu^a}{\mathfrak{p}}\right) = \left(\frac{\nu}{\mathfrak{p}}\right),$$

woraus leicht mit Rücksicht auf Satz 2 der zweite Teil des Satzes 15 zu entnehmen ist.

An späterer Stelle werden wir erkennen, daß dieser Satz 15 ebenso wie Satz 14 auch für jedes in 2 aufgehende Primideal gilt; doch bietet der Nachweis hierfür erheblich größere Schwierigkeiten. Wir werden dann auf die Bedeutung hinweisen, die diesem Satz 15 und seiner Verallgemeinerung auf beliebige Primideale für unsere Theorie zukommt.

§ 11. Die Einheitenverbände des Körpers k.

Definition 7. Wenn ε eine Einheit des Körpers k ist, so heißt das System aller Einheiten von der Form $\varepsilon\xi^2$ wo ξ alle Einheiten des Körpers k durchläuft, ein *Verband von Einheiten* oder ein *Einheitenverband* des Körpers k. Der durch die Einheit $\varepsilon = 1$ bestimmte Einheitenverband, d. h. derjenige Verband, welcher die Quadrate aller Einheiten des Körpers enthält, heiße der *Hauptverband* und werde mit 1 bezeichnet. Wenn V, V' zwei beliebige Verbände von Einheiten in k sind und jede Einheit in V mit jeder Einheit in V' multipliziert wird, so bilden sämtliche solche Produkte wiederum einen Verband von Einheiten in k; dieser werde das *Produkt der Verbände* V und V' genannt und mit VV' bezeichnet. Wenn eine Anzahl von Verbänden in k vorgelegt ist, von denen keiner der Hauptverband ist und keiner durch Multiplikation aus den anderen erhalten werden kann, so heißen dieselben von einander *unabhängig*.

Es mögen die r Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ ein volles System von Grundeinheiten[1] des Körpers k bilden. Ferner sei ζ eine Einheitswurzel, welche in k vorkommt, während $\sqrt{\zeta}$ nicht in k liegt; wir setzen $\varepsilon_{r+1} = \zeta$ und erkennen dann leicht, daß $\varepsilon_1, \ldots, \varepsilon_{r+1}$ ein System von $r+1$ Einheiten bilden derart, daß überhaupt jede Einheit ε in k auf eine und nur auf eine Weise sich in der Gestalt

$$\varepsilon = \varepsilon_1^{u_1} \varepsilon_2^{u_2} \cdots \varepsilon_{r+1}^{u_{r+1}} \xi^2$$

darstellen läßt, wo die Exponenten $u_1, u_2, \ldots, u_{r+1}$ nur die Werte 0 oder 1 annehmen und ξ eine geeignete Einheit in k bedeutet. Es bestimmen also offenbar die Einheiten $\varepsilon_1, \ldots, \varepsilon_{r+1}$ ein System von $r+1$ unabhängigen Verbänden in k, durch deren Multiplikation überhaupt jeder in k vorhandene Verband erhalten werden kann. Der Körper k besitzt, wie wir hieraus schließen, im ganzen genau 2^{r+1} verschiedene Einheitenverbände.

§ 12. Die Komplexe des relativquadratischen Körpers K.

Definition 8. Ist $\mathfrak{C}$ ein Ideal aus einer Idealklasse C des in bezug auf k relativquadratischen Körpers K, so werde die durch das relativkonjugierte Ideal $S\mathfrak{C}$ bestimmte Idealklasse mit SC bezeichnet und die zu C *relativkonjugierte Klasse* genannt. Eine Idealklasse A des Körpers $K(\sqrt{\mu})$ heiße eine *ambige Klasse*, wenn sie ihrer relativkonjugierten Klasse SA gleich wird, wenn also

$$A = SA$$

ist.

Insbesondere ist offenbar jede Klasse des Körpers K ambig, welche ein ambiges Ideal des Körpers K enthält; doch kann es, wie später gezeigt werden wird, sehr wohl ambige Klassen in K geben, welche kein ambiges Ideal enthalten.

Das Quadrat einer ambigen Klasse A ist stets eine solche Klasse in K, welche unter ihren Idealen sicher auch in k liegende Ideale enthält; dies folgt leicht aus der Gleichung $A^2 = A \cdot SA$.

Definition 9. *Ist C eine beliebige Klasse in K, so nenne ich das System aller Klassen von der Form cC, wo c die Klassen des Körpers k durchläuft, einen Komplex des Körpers K. Der Komplex der aus den sämtlichen Klassen c in k besteht, heiße der Hauptkomplex des Körpers K und werde mit 1 bezeichnet.*

Wenn P und P' zwei beliebige Komplexe sind und jede Klasse in P mit jeder Klasse in P' multipliziert wird, so bilden sämtliche solche Produkte

[1] Vgl. „Algebraische Zahlkörper", dieser Band S. 102 und S. 108.

wiederum einen Komplex; dieser werde das *Produkt der Komplexe* P und P' genannt und mit PP' bezeichnet.

Wenn C eine Klasse im Komplexe P ist, so werde derjenige Komplex, zu welchem die relativkonjugierte Klasse SC gehört, der zu P *relativkonjugierte Komplex* genannt und mit SP bezeichnet.

Jeder Komplex, der mit dem ihm relativkonjugierten Komplexe übereinstimmt, heißt ein *ambiger Komplex*. Wenn P ein ambiger Komplex ist, so folgt aus $P = SP$ die Gleichung

$$P^2 = P \cdot SP = 1\,,$$

d. h. das Quadrat jedes ambigen Komplexes ist der Hauptkomplex. Umgekehrt, wenn das Quadrat eines Komplexes P den Hauptkomplex 1 liefert, so ist P ein ambiger Komplex. In der Tat folgt, da $P \cdot SP$ stets gleich 1 ausfällt, aus $P^2 = 1$ die Gleichung $P = SP$.

Jeder Komplex P, der eine ambige Klasse A enthält, ist ein ambiger Komplex; ein solcher Komplex werde ein aus der ambigen Klasse A entspringender Komplex genannt. Enthält insbesondere die ambige Klasse A ein ambiges Ideal $\mathfrak{A}$, so heißt P ein aus dem ambigen Ideal $\mathfrak{A}$ entspringender Komplex.

Wenn eine Anzahl von Komplexen des Körpers K vorgelegt ist, unter denen keiner der Hauptkomplex 1 ist und keiner durch Multiplikation aus den übrigen hergeleitet werden kann, so heißen diese Komplexe voneinander *unabhängig*.

§ 13. Primideale des Körpers k mit vorgeschriebenen quadratischen Charakteren.

Ein sehr wichtiges Hilfsmittel für die weitere Entwicklung der Theorie der relativquadratischen Körper gewinnen wir durch die Erörterung der Frage, ob es stets im Körper k Primideale gibt, nach denen irgendwelche gegebene Zahlen vorgeschriebene quadratische Charaktere besitzen. Wir führen die Untersuchung dieser Frage in folgender Weise:

Satz 16. (Hilfssatz). Es bedeute α irgendeine ganze Zahl in k, welche nicht das Quadrat einer Zahl in k ist, und man setze

$$f(s) = \sum_{(\mathfrak{p})}{}' \left(\frac{\alpha}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{p})^s}, \qquad (s > 1)\,,$$

wo die Summe rechter Hand über sämtliche Primideale $\mathfrak{p}$ des Körpers k zu erstrecken ist: dann nähert sich die Funktion $f(s)$ der reellen Veränderlichen s, wenn s nach 1 abnimmt, einer endlichen Grenze.

Beweis. Wir fassen den Körper k vom Grade m und ferner den durch $\sqrt{\alpha}$ bestimmten relativquadratischen Körper $K(\sqrt{\alpha})$ vom Grade $2m$ ins Auge und bilden bez. die Funktionen

$$\zeta_k(s) = \prod_{(\mathfrak{p})} \frac{1}{1 - n(\mathfrak{p})^{-s}}, \qquad \zeta_K(s) = \prod_{(\mathfrak{P})} \frac{1}{1 - N(\mathfrak{P})^{-s}},$$

wobei das erste Produkt über alle Primideale $\mathfrak{p}$ in k und das zweite Produkt über alle Primideale $\mathfrak{P}$ in $K(\sqrt{\alpha})$ zu erstrecken ist, und wo ferner $n(\mathfrak{p})$ die Norm von $\mathfrak{p}$ in k und $N(\mathfrak{P})$ die Norm von $\mathfrak{P}$ in $K(\sqrt{\alpha})$ bedeutet. Es ist bekannt, daß diese unendlichen Produkte für $s > 1$ konvergieren und daß die Grenzausdrücke

$$\lim_{s=1} \{(s-1)\,\zeta_k(s)\}\,, \qquad \lim_{s=1} \{(s-1)\,\zeta_K(s)\}$$

endliche und von 0 verschiedene Werte darstellen[1]; hieraus folgt, daß auch der Ausdruck

$$\lim_{s=1} \frac{\zeta_K(s)}{\zeta_k(s)} \tag{1}$$

einen endlichen von 0 verschiedenen Wert besitzt. Ordnen wir nun das Produkt

$$\zeta_K(s) = \prod_{(\mathfrak{P})} \frac{1}{1 - N(\mathfrak{P})^{-s}} \tag{2}$$

nach den Primidealen $\mathfrak{p}$ des Körpers k, aus welchen die Primideale $\mathfrak{P}$ herstammen, so gehört, wenn wir Definition 4 berücksichtigen, zu einem beliebigen Primideale $\mathfrak{p}$ in dem Produkt (2) das Glied

$$\frac{1}{(1 - n(\mathfrak{p})^{-s})^2} \quad \text{oder} \quad \frac{1}{1 - n(\mathfrak{p})^{-s}} \quad \text{oder} \quad \frac{1}{1 - n(\mathfrak{p})^{-2s}}, \tag{3}$$

je nachdem

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = +1 \quad \text{oder} \quad = 0 \quad \text{oder} \quad = -1$$

ausfällt. Wir können daher die drei Ausdrücke (3) in der gemeinschaftlichen Form

$$\frac{1}{1 - n(\mathfrak{p})^{-s}} \cdot \frac{1}{1 - \left(\frac{\alpha}{\mathfrak{p}}\right) n(\mathfrak{p})^{-s}}$$

schreiben und erhalten so

$$\zeta_K(s) = \prod_{(\mathfrak{p})} \frac{1}{1 - n(\mathfrak{p})^{-s}} \prod_{(\mathfrak{p})} \frac{1}{1 - \left(\frac{\alpha}{\mathfrak{p}}\right) n(\mathfrak{p})^{-s}} = \zeta_k(s) \prod_{(\mathfrak{p})} \frac{1}{1 - \left(\frac{\alpha}{\mathfrak{p}}\right) n(\mathfrak{p})^{-s}}$$

und da der Grenzwert (1) endlich und von 0 verschieden ausfällt, so folgt das gleiche für den Grenzwert

$$\lim_{s=1} \prod_{(\mathfrak{p})} \frac{1}{1 - \left(\frac{\alpha}{\mathfrak{p}}\right) n(\mathfrak{p})^{-s}},$$

und hieraus schließen wir, indem wir in bekannter Weise zum Logarithmus übergehen, daß der Ausdruck

$$\lim_{s=1} \sum_{(\mathfrak{p})} \left(\frac{\alpha}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{p})^s}$$

einen endlichen Wert besitzt, wie es Satz 16 behauptet.

[1] Vgl. „Algebraische Zahlkörper" § 26, dieser Band S. 116.

Satz 17. (Hilfssatz). Es seien $\alpha_1, \ldots, \alpha_z$ irgend z ganze Zahlen in k, welche die Bedingung erfüllen, daß kein aus denselben zu bildendes Produkt gleich dem Quadrat einer Zahl in k wird; es seien ferner $c_1, \ldots, c_z$ nach Belieben vorgeschriebene Einheiten ± 1: dann gilt eine Gleichung von der Gestalt

$$\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} = \frac{1}{2^z} \log \frac{1}{s-1} + f(s), \qquad (s > 1);$$

hierbei ist die Summe linker Hand über alle diejenigen Primideale $\mathfrak{p}$ des Körpers k zu erstrecken, die den Bedingungen

$$\left(\frac{\alpha_1}{\mathfrak{p}}\right) = c_1, \ \left(\frac{\alpha_2}{\mathfrak{p}}\right) = c_2, \ \ldots, \ \left(\frac{\alpha_z}{\mathfrak{p}}\right) = c_z$$

genügen und rechter Hand bedeutet $f(s)$ eine Funktion der reellen Veränderlichen s, welche sich für $s = 1$ einem endlichen Grenzwert nähert.

Beweis. Wir haben

$$\left.\begin{aligned} \log \zeta_k(s) &= \sum_{(\mathfrak{p})} \log \frac{1}{1 - n(\mathfrak{p})^{-s}} \\ &= \sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} + \varphi(s), \end{aligned}\right\} \qquad (s > 1),$$

wobei die Summen über alle Primideale $\mathfrak{p}$ in k zu erstrecken sind und $\varphi(s)$ eine für $s = 1$ endlich bleibende Funktion der reellen Veränderlichen s bedeutet. Da andererseits der Ausdruck $(s-1)\zeta_k(s)$ für $s = 1$ endlich und von 0 verschieden bleibt, so folgt, daß in der Gleichung

$$\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} = \log \frac{1}{s-1} + \psi(s), \qquad (s > 1), \tag{4}$$

$\psi(s)$ wiederum eine für $s = 1$ endlich bleibende Funktion von s bedeutet.

Wir setzen nun in der über alle Primideale $\mathfrak{p}$ zu erstreckenden Summe

$$\sum_{(\mathfrak{p})} \left(\frac{\alpha}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{p})^s}, \qquad (s > 1) \tag{5}$$

den Wert $\alpha = \alpha_1^{u_1} \alpha_2^{u_2} \ldots \alpha_z^{u_z}$ ein und multiplizieren die so entstehende Gleichung mit dem Faktor $c_1^{u_1} c_2^{u_2} \ldots c_z^{u_z}$. Wir erteilen dann jedem der z Exponenten $u_1, u_2, \ldots, u_z$ nacheinander die Werte 0, 1, jedoch so, daß das eine Wertsystem $u_1 = 0, u_2 = 0, \ldots, u_z = 0$ ausgeschlossen wird. Nach Satz 16 bleiben die sämtlichen $2^z - 1$ aus (5) in dieser Weise entstehenden Ausdrücke für $s = 1$ endlich. Werden dieselben zu (4) addiert, so erhalten wir daher eine Gleichung von der Form

$$\sum_{(\mathfrak{p})} \left\{1 + c_1\left(\frac{\alpha_1}{\mathfrak{p}}\right)\right\}\left\{1 + c_2\left(\frac{\alpha_2}{\mathfrak{p}}\right)\right\} \cdots \left\{1 + c_z\left(\frac{\alpha_z}{\mathfrak{p}}\right)\right\} \frac{1}{n(\mathfrak{p})^s}$$
$$= \log \frac{1}{s-1} + \chi(s), \tag{6}$$

wo $\chi(s)$ wiederum eine für $s = 1$ endlich bleibende Funktion bedeutet.

Die Richtigkeit des Satzes 17 folgt unmittelbar aus dieser Beziehung (6), wenn wir bedenken, daß der Ausdruck

$$\left\{1 + c_1\left(\frac{\alpha_1}{\mathfrak{p}}\right)\right\}\left\{1 + c_2\left(\frac{\alpha_2}{\mathfrak{p}}\right)\right\} \cdots \left\{1 + c_z\left(\frac{\alpha_z}{\mathfrak{p}}\right)\right\}$$

für alle diejenigen Primideale $\mathfrak{p}$, die den Bedingungen des Satzes 17 genügen, den Wert 2^z besitzt und daß dieser Ausdruck für alle anderen Primideale $\mathfrak{p}$ des Körpers k verschwindet, abgesehen von den endlich vielen Primidealen, die in $\alpha_1 \alpha_2 \ldots \alpha_z$ aufgehen.

Aus der soeben bewiesenen Gleichung des Satzes 17 folgt, indem wir bedenken, daß $\log \frac{1}{s-1}$ für $s = 1$ über alle Grenzen wächst, sofort die folgende Tatsache:

Satz 18. *Es seien $\alpha_1, \alpha_2, \ldots, \alpha_z$ irgend z ganze Zahlen in k, welche die Bedingung erfüllen, daß kein aus denselben zu bildendes Produkt gleich dem Quadrat einer Zahl in k wird: es seien ferner $c_1, c_2, \ldots, c_z$ nach Belieben vorgeschriebene Einheiten ± 1: dann gibt es im Körper k stets unendlich viele Primideale $\mathfrak{p}$, die den Bedingungen*

$$\left(\frac{\alpha_1}{\mathfrak{p}}\right) = c_1, \left(\frac{\alpha_2}{\mathfrak{p}}\right) = c_2, \ldots, \left(\frac{\alpha_z}{\mathfrak{p}}\right) = c_z$$

genügen.

II. Die Theorie der relativquadratischen Körper für einen Grundkörper mit lauter imaginären Konjugierten und von ungerader Klassenanzahl.

Um die weiteren Sätze der Theorie der relativquadratischen Zahlkörper in möglichst leicht faßlicher Weise auszudrücken und ihre Beweise in naturgemäßer Stufenfolge entwickeln zu können, beschränke ich mich fortan in der gegenwärtigen Arbeit auf die Untersuchung eines besonderen Falles, indem ich durchweg folgende zwei Annahmen über den zugrunde gelegten Körper k mache:

1. *Der Körper k vom m-ten Grade sei nebst allen konjugierten Körpern $k', \ldots, k^{(m-1)}$ imaginär.*
2. *Die Anzahl h der Idealklassen im Körper k sei ungerade.*

§ 14. Die relativen Grundeinheiten des Körpers K.

Infolge der ersteren der beiden soeben gemachten Annahmen ist die Anzahl der Einheiten, welche ein volles System von Grundeinheiten in k bilden, gleich $\frac{m}{2} - 1$; es sei $\varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}-1}$ ein volles System von Grundeinheiten in k. Wir beweisen zunächst folgende Tatsache:

Satz 19. (Hilfssatz.) Im relativquadratischen Körper $K(\sqrt{\mu})$ lassen sich stets $\frac{m}{2}$ Einheiten $\mathsf{H}_1, \ldots, \mathsf{H}_{\frac{m}{2}}$ finden, so daß für irgendeine Einheit E in

$K(\sqrt{\mu})$ jedes Mal eine Gleichung von der Gestalt

$$\mathsf{E}^u = \mathsf{H}_1^{U_1} \cdots \mathsf{H}_{\frac{m}{2}}^{U_{\frac{m}{2}}} [\xi]$$

besteht, wo der Exponent u eine ungerade Zahl und die Exponenten $U_1, \ldots, U_{\frac{m}{2}}$ irgendwelche ganze rationale Werte oder den Wert 0 haben können; endlich bedeutet $[\xi]$ eine Einheit des Körpers k oder eine solche Einheit in $K(\sqrt{\mu})$, deren Quadrat eine Einheit in k wird, so daß $[\xi]$ im allgemeinen eine Einheit in k sein muß und nur dann die Wurzel aus einer Einheit in k darstellen kann, wenn μ eine Einheit in k oder das Produkt einer solchen in das Quadrat einer Zahl des Körpers k ist.

Die Einheiten $\mathsf{H}_1, \ldots, \mathsf{H}_{\frac{m}{2}}$ sind in dem Sinne voneinander unabhängig, daß zwischen ihnen keine Relation von der Gestalt

$$\mathsf{H}_1^{U_1} \cdots \mathsf{H}_{\frac{m}{2}}^{U_{\frac{m}{2}}} [\xi] = 1$$

mit ganzen rationalen Exponenten $U_1, \ldots, U_{\frac{m}{2}}$ besteht, es sei denn, daß diese Exponenten sämtlich verschwinden und $[\xi] = 1$ ist.

Beweis. Im Körper $K(\sqrt{\mu})$ gibt es ein volles System von $m-1$ Grundeinheiten $\mathsf{H}_1, \ldots, \mathsf{H}_{m-1}$. Wir betrachten die Gesamtheit der $\frac{3m}{2} - 2$ Einheiten

$$\mathsf{H}_1, \ldots, \mathsf{H}_{m-1}, \quad \varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}-1}.$$

Sobald $\frac{m}{2} - 1 > 0$ ist, besteht zwischen diesen Einheiten jedenfalls eine Relation von der Gestalt

$$\mathsf{H}_1^{A_1} \cdots \mathsf{H}_{m-1}^{A_{m-1}} \varepsilon_1^{a_1} \cdots \varepsilon_{\frac{m}{2}-1}^{a_{\frac{m}{2}-1}} = 1, \tag{1}$$

wo $A_1, \ldots, A_{m-1}$, $a_1, \ldots, a_{\frac{m}{2}-1}$ ganze rationale Exponenten und $A_1, \ldots, A_{m-1}$ nicht sämtlich Null sind. Wir setzen

$$A_1 = 2^e A_1', \ldots, A_{m-1} = 2^e A_{m-1}';$$

dabei bedeute 2^e die höchste in den sämtlichen Zahlen $A_1, \ldots, A_{m-1}$ aufgehende Potenz von 2 und es sei etwa A_{m-1}' eine ungerade Zahl. Setzen wir ferner zur Abkürzung

$$\varepsilon = \varepsilon_1^{-a_1} \cdots \varepsilon_{\frac{m}{2}-1}^{-a_{\frac{m}{2}-1}},$$

so erhalten wir aus der Relation (1) die folgende Gleichung

$$\mathsf{H}_1^{A_1'} \cdots \mathsf{H}_{m-1}^{A_{m-1}'} = \sqrt[2^e]{\varepsilon}. \tag{2}$$

Da hier die rechte Seite eine gewisse 2^e-te Wurzel aus einer Einheit ε in k bedeutet und wegen dieser Relation (2) zugleich eine Einheit in K sein soll, so steht rechter Hand entweder eine Einheit in k oder die Quadratwurzel aus einer Einheit in k; wir schreiben demgemäß die Relation (2) in der Gestalt

$$\mathsf{H}_1^{A_1'} \cdots \mathsf{H}_{m-1}^{A_{m-1}'} = [\xi],$$

und hieraus folgt

$$\mathsf{H}_{m-1}^{A_{m-1}'} = \mathsf{H}_1^{-A_1'} \cdots \mathsf{H}_{m-2}^{-A_{m-2}'} [\xi], \tag{3}$$

wo $[\xi]$ die im Satze 19 erklärte Bedeutung hat.

Nunmehr schalten wir die Einheit H_{m-1} aus dem ursprünglichen System von Grundeinheiten aus und betrachten nur die Gesamtheit der $\frac{3m}{2} - 3$ Einheiten

$$\mathsf{H}_1, \ldots, \mathsf{H}_{m-2}, \quad \varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}-1}.$$

Falls noch $\frac{m}{2} - 2 > 0$ ausfällt, besteht zwischen diesen Einheiten eine Relation von der Gestalt

$$\mathsf{H}_1^{B_1} \cdots \mathsf{H}_{m-2}^{B_{m-2}} \varepsilon_1^{b_1} \cdots \varepsilon_{\frac{m}{2}-1}^{b_{\frac{m}{2}-1}} = 1, \tag{4}$$

wo $B_1, \ldots, B_{m-2}, b_1, \ldots, b_{\frac{m}{2}-1}$ ganze rationale Exponenten und $B_1, \ldots, B_{m-2}$ nicht sämtlich Null sind. Wir setzen

$$B_1 = 2^f B_1', \ldots, B_{m-2} = 2^f B_{m-2}';$$

dabei bedeute 2^f die höchste in den sämtlichen Zahlen $B_1, \ldots, B_{m-2}$ aufgehende Potenz von 2 und es sei etwa B_{m-2}' eine ungerade Zahl. Setzen wir ferner zur Abkürzung

$$\bar{\varepsilon} = \varepsilon_1^{-b_1} \cdots \varepsilon_{\frac{m}{2}-1}^{-b_{\frac{m}{2}-1}},$$

so erhalten wir aus der Relation (4) die folgende Gleichung

$$\mathsf{H}_1^{B_1'} \cdots \mathsf{H}_{m-2}^{B_{m-2}'} = \sqrt[2^f]{\bar{\varepsilon}}$$

und hieraus schließen wir, wie vorhin, die Gleichung

$$\mathsf{H}_{m-2}^{B_{m-2}'} = \mathsf{H}_1^{-B_1'} \cdots \mathsf{H}_{m-3}^{-B_{m-3}'} [\xi], \tag{5}$$

wo $[\xi]$ wiederum die im Satze 19 erklärte Bedeutung hat. Wir betrachten nun das Einheitensystem $\mathsf{H}_1, \ldots, \mathsf{H}_{m-3}, \varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}-1}$. Es läßt sich dann das beschriebene Verfahren offenbar so lange fortsetzen, bis von den ursprünglichen Grundeinheiten $\mathsf{H}_1, \ldots, \mathsf{H}_{m-1}$ nur $\frac{m}{2}$ Einheiten, etwa die Einheiten $\mathsf{H}_1, \ldots, \mathsf{H}_{\frac{m}{2}}$, übrig bleiben; wir erkennen leicht, daß diese Einheiten dann die im Satze 19 verlangte Eigenschaft besitzen. Denn da $\mathsf{H}_1, \ldots, \mathsf{H}_{m-1}$ ein System von Grundeinheiten des Körpers K darstellen, so ist überhaupt jede Einheit E in K in der Gestalt

$$\mathsf{E} = \mathsf{H}_1^{U_1} \cdots \mathsf{H}_{m-1}^{U_{m-1}} \mathsf{Z} \tag{6}$$

darstellbar, wo $U_1, \ldots, U_{m-1}$ ganze rationale Exponenten und Z eine Einheitswurzel bezeichnet. Nun ist Z offenbar entweder eine in k liegende Einheitswurzel oder die Quadratwurzel aus einer in k liegenden Einheitswurzel, multipliziert in eine Einheitswurzel Z* mit ungeradem Wurzelexponenten u^*; wir dürfen daher $Z = [\xi] Z^*$ setzen, wo $[\xi]$ die im Satze 19 erklärte Bedeutung hat. Wenn wir dann die Gleichung (6) in die $u = u^* A'^{u_{m-1}}_{m-1} B'^{\ldots}_{m-2} \ldots$-te Potenz erheben, so folgt, bei Benutzung der Gleichungen (3), (5) und der späteren analogen, eine Relation, welche, da u ungerade ausfällt, die Richtigkeit des Satzes 19 erkennen läßt.

Definition 10. Die Einheiten $\mathsf{H}_1, \ldots, \mathsf{H}_{\frac{m}{2}}$, welche die Eigenschaft des Satzes 19 besitzen, nenne ich ein System von *relativen Grundeinheiten des Körpers* $K(\sqrt{\mu})$ in bezug auf k.

Satz 20. (Hilfssatz.) Wenn $\mathsf{H}_1, \ldots, \mathsf{H}_{\frac{m}{2}}$ ein System von relativen Grundeinheiten des Körpers K bilden und deren Relativnormen bez. mit

$$\eta_1 = N(\mathsf{H}_1), \ldots, \eta_{\frac{m}{2}} = N(\mathsf{H}_{\frac{m}{2}})$$

bezeichnet werden, so läßt sich jede Einheit ε in k, welche die Relativnorm irgendeiner Einheit E des Körpers K ist, in der Gestalt

$$\varepsilon = \eta_1^{u_1} \cdots \eta_{\frac{m}{2}}^{u_{\frac{m}{2}}} N([\xi])$$

darstellen, wo die Exponenten $u_1, \ldots, u_{\frac{m}{2}}$ gewisse Werte 0, 1 haben und $[\xi]$ eine Einheit in k oder eine in K liegende Quadratwurzel aus einer Einheit in k bezeichnet.

Beweis. Nach dem Satze 19 gilt für die Einheit E eine Gleichung

$$\mathsf{E}^u = \mathsf{H}_1^{U_1} \cdots \mathsf{H}_{\frac{m}{2}}^{U_{\frac{m}{2}}} [\xi],$$

wo die Bezeichnungen wie im Satz 19 zu verstehen sind. Indem wir von beiden Seiten dieser Gleichung die Relativnorm bilden, ergibt sich

$$\varepsilon^u = \eta_1^{U_1} \cdots \eta_{\frac{m}{2}}^{U_{\frac{m}{2}}} N([\xi])$$

und hieraus folgt

$$\varepsilon = \eta_1^{u_1} \cdots \eta_{\frac{m}{2}}^{u_{\frac{m}{2}}} N([\xi^*]),$$

wenn allgemein $u_i = 0$ oder $= 1$ genommen wird, je nachdem U_i gerade oder ungerade ausfällt und wo ferner

$$[\xi^*] = \eta_1^{\frac{U_1 - u_1}{2}} \cdots \eta_{\frac{m}{2}}^{\frac{U_{\frac{m}{2}} - u_{\frac{m}{2}}}{2}} \varepsilon^{\frac{1-u}{2}} [\xi]$$

gesetzt ist; damit ist Satz 20 bewiesen.

§ 15. Die Anzahl der aus ambigen Idealen entspringenden ambigen Komplexe in K.

Satz 21. Ein ambiger Komplex P des relativquadratischen Körpers K enthält lauter ambige Klassen. Die Anzahl der ambigen Klassen in K ist genau gleich der h-fachen Anzahl der ambigen Komplexe.

Beweis. Wenn C irgendeine Klasse des ambigen Komplexes P ist, so folgt aus $P = SP$ offenbar $C = c \cdot SC$, wo c eine der h Klassen des Körpers k bedeutet. Bilden wir auf beiden Seiten der letzten Gleichung die Relativnorm, so erhalten wir leicht $1 = c^2$ und da andererseits auch $c^h = 1$ ist, wobei die Klassenanzahl h eine ungerade Zahl sein soll, so folgt $c = 1$, d. h. es wird $C = SC$; mithin ist C eine ambige Klasse. Soll andererseits $C = cC$ sein, wo c eine Klasse in k ist, so folgt ebenso $c = 1$ und damit ergibt sich die zweite Aussage des Satzes 21.

Satz 22. Wenn die Anzahl aller ambigen Ideale des Körpers $K(\sqrt{\mu})$ gleich 2^t ist und wenn diejenigen Einheiten in k, welche Relativnormen von Einheiten in $K(\sqrt{\mu})$ sind, zusammengenommen 2^{v^*} Einheitenverbände in k ausmachen: dann ist die Anzahl derjenigen ambigen Komplexe des Körpers $K(\sqrt{\mu})$, welche aus ambigen Idealen entspringen, genau gleich 2^{a^*}, wo a^* den Wert

$$a^* = t + v^* - \frac{m}{2} - 1$$

hat.

Beweis. Wir nehmen im folgenden zunächst an, daß die Zahl μ nicht das Produkt einer Einheit in das Quadrat einer Zahl des Körpers k sei; es ist dann jeder Ausdruck $[\xi]$ notwendig eine in k gelegene Einheit ξ.

Nunmehr mögen, wie in Satz 20, $\mathsf{H}_1, \ldots, \mathsf{H}_{\frac{m}{2}}$ ein System von relativen Grundeinheiten des Körpers $K(\sqrt{\mu})$ und

$$\eta_1 = N(\mathsf{H}_1), \ldots, \eta_{\frac{m}{2}} = N(\mathsf{H}_{\frac{m}{2}})$$

deren Relativnormen bedeuten. Nach Satz 20 läßt sich bei unserer Annahme jede Einheit ε in k, welche die Relativnorm einer Einheit in $K(\sqrt{\mu})$ ist, in der Gestalt

$$\varepsilon = \eta_1^{u_1} \cdots \eta_{\frac{m}{2}}^{u_{\frac{m}{2}}} \xi^2$$

darstellen, wo die Exponenten $u_1, \ldots, u_{\frac{m}{2}}$ gewisse Werte 0, 1 haben und ξ eine Einheit in k bedeutet. Da nun die Anzahl der Verbände von Einheiten in k, die Relativnormen von Einheiten in $K(\sqrt{\mu})$ sind, nach Voraussetzung 2^{v^*} betragen soll, so muß es möglich sein, unter den $\frac{m}{2}$ Einheiten $\eta_1, \ldots, \eta_{\frac{m}{2}}$ gewisse v^* auszuwählen — es seien hierfür die Einheiten $\eta_1, \ldots, \eta_{v^*}$ geeignet — derart, daß jede Einheit ε in k, welche die Relativnorm einer Einheit in $K(\sqrt{\mu})$

ist, sich auf eine und nur auf eine Weise in der Gestalt

$$\varepsilon = \eta_1^{u_1} \cdots \eta_{v^*}^{u_{v^*}} \xi^2$$

darstellen läßt, wo die Exponenten $u_1, \ldots, u_{v^*}$ wiederum gewisse Werte 0, 1 haben und ξ eine Einheit in k bedeutet.

Wir stellen insbesondere die Einheiten $\eta_{v^*+1}, \ldots, \eta_{\frac{m}{2}}$ auf diese Weise dar und setzen demgemäß

$$\eta_i = \eta_1^{u_1^{(i)}} \cdots \eta_{v^*}^{u_{v^*}^{(i)}} (\xi^{(i)})^2, \qquad \left(i = v^*+1, v^*+2, \ldots, \frac{m}{2}\right),$$

wo $u_1^{(i)}, \ldots, u_{v^*}^{(i)}$ gewisse Werte 0, 1 haben und $\xi^{(i)}$ Einheiten in k sind. Die $\frac{m}{2} - v^*$ Ausdrücke

$$\mathsf{H}_i' = \mathsf{H}_i \mathsf{H}_1^{-u_1^{(i)}} \cdots \mathsf{H}_{v^*}^{-u_{v^*}^{(i)}} (\xi^{(i)})^{-1}, \qquad \left(i = v^*+1, v^*+2, \ldots, \frac{m}{2}\right) \tag{1}$$

sind dann offenbar Einheiten in $K(\sqrt{\mu})$, deren Relativnormen gleich 1 ausfallen, und folglich erfüllen die $\frac{m}{2} - v^*$ ganzen Zahlen

$$\mathsf{M}_1 = 1 + \mathsf{H}'_{v^*+1}, \ldots, \mathsf{M}_{\frac{m}{2}-v^*} = 1 + \mathsf{H}'_{\frac{m}{2}}$$

bez. die Gleichungen

$$\mathsf{M}_1 = \mathsf{H}'_{v^*+1} \cdot S\mathsf{M}_1, \ldots, \mathsf{M}_{\frac{m}{2}-v^*} = \mathsf{H}'_{\frac{m}{2}} \cdot S\mathsf{M}_{\frac{m}{2}-v^*}. \tag{2}$$

Wir setzen noch $\mathsf{M} = \sqrt{\mu}$ und betrachten dann die durch

$$\mathsf{M}, \mathsf{M}_1, \ldots, \mathsf{M}_{\frac{m}{2}-v^*}$$

bestimmten Hauptideale

$$(\mathsf{M}) = \mathfrak{M}, (\mathsf{M}_1) = \mathfrak{M}_1, \ldots, (\mathsf{M}_{\frac{m}{2}-v^*}) = \mathfrak{M}_{\frac{m}{2}-v^*}.$$

Da wegen (2) diese Hauptideale je ihren relativkonjugierten Idealen gleich ausfallen und mithin Produkte ambiger Ideale mit Idealen in k sein müssen, so können wir wegen Definition 3 setzen:

$$\begin{aligned}
\mathfrak{M} &= \mathfrak{D}_1^{a_1} \cdots \mathfrak{D}_t^{a_t} \mathfrak{j}, \\
\mathfrak{M}_1 &= \mathfrak{D}_1^{a_1^{(1)}} \cdots \mathfrak{D}_t^{a_t^{(1)}} \mathfrak{j}^{(1)}, \\
&\cdots\cdots\cdots\cdots\cdots \\
\mathfrak{M}_{\frac{m}{2}-v^*} &= \mathfrak{D}_1^{a_1^{(\frac{m}{2}-v^*)}} \cdots \mathfrak{D}_t^{a_t^{(\frac{m}{2}-v^*)}} \mathfrak{j}^{(\frac{m}{2}-v^*)},
\end{aligned} \tag{3}$$

wo $\mathfrak{D}_1, \ldots, \mathfrak{D}_t$ die t ambigen Primideale des Körpers $K(\sqrt{\mu})$, ferner $\mathfrak{j}, \mathfrak{j}^{(1)}, \ldots, \mathfrak{j}^{(\frac{m}{2}-v^*)}$ Ideale in k und $a_1, a_2, \ldots, a_t^{(\frac{m}{2}-v^*)}$ gewisse Exponenten 0, 1 bedeuten.

Wir wollen nun beweisen, daß zwischen den Idealen

$$\mathfrak{M}, \mathfrak{M}_1, \ldots, \mathfrak{M}_{\frac{m}{2}-v^*}$$

keine Relation von der Gestalt

$$\mathfrak{M}^e \mathfrak{M}_1^{e_1} \cdots \mathfrak{M}_{\frac{m}{2}-v^*}^{e_{\frac{m}{2}}-v^*} = \mathfrak{j}^* \tag{4}$$

stattfinden kann, wo die Exponenten $e, e_1, \ldots, e_{\frac{m}{2}-v^*}$ irgendwelche Werte 0, 1 haben und $\mathfrak{j}^*$ ein Ideal in k bedeutet, es sei denn, daß diese Exponenten sämtlich gleich 0 sind und $\mathfrak{j}^* = 1$ wird.

Zu dem Zwecke erheben wir die Relation (4) in die h-te Potenz und setzen $\mathfrak{j}^h = (\iota)$, wo ι eine ganze Zahl in k bedeutet; wir erhalten dann eine Relation von der Gestalt

$$\mathsf{M}^{eh} \mathsf{M}_1^{e_1 h} \cdots \mathsf{M}_{\frac{m}{2}-v^*}^{e_{\frac{m}{2}}-v^*{}^h} = \iota \mathsf{E},$$

wo E eine Einheit des Körpers $K(\sqrt{\mu})$ ist. Wenden wir auf diese Relation die Substitution S an und dividieren sie dann durch die so entstehende neue Relation, so folgt

$$\left(\frac{\mathsf{M}}{S\mathsf{M}}\right)^{eh} \left(\frac{\mathsf{M}_1}{S\mathsf{M}_1}\right)^{e_1 h} \cdots \left(\frac{\mathsf{M}_{\frac{m}{2}-v^*}}{S\mathsf{M}_{\frac{m}{2}-v^*}}\right)^{e_{\frac{m}{2}}-v^*{}^h} = \frac{\mathsf{E}}{S\mathsf{E}}$$

oder vermöge (2)

$$(-1)^{eh} \mathsf{H}_{v^*+1}'^{e_1 h} \cdots \mathsf{H}_{\frac{m}{2}}'^{e_{\frac{m}{2}}-v^*{}^h} = \frac{\mathsf{E}}{S\mathsf{E}}.$$

Wir schreiben diese Relation in der Gestalt

$$\mathsf{H}_{v^*+1}'^{e_1 h} \cdots \mathsf{H}_{\frac{m}{2}}'^{e_{\frac{m}{2}}-v^*{}^h} = \mathsf{E}^2 \xi, \tag{5}$$

wo $\xi = \frac{(-1)^{eh}}{N(\mathsf{E})}$ eine Einheit in k bezeichnet.

Nach Satz 19 gibt es für jede Einheit E einen ungeraden Exponenten u, so daß

$$\mathsf{E}^u = \mathsf{H}_1^{U_1} \cdots \mathsf{H}_{\frac{m}{2}}^{U_{\frac{m}{2}}} \xi' \tag{6}$$

wird, wo die Exponenten $U_1, \ldots, U_{\frac{m}{2}}$ gewisse ganze rationale Werte haben und ξ' eine Einheit in k ist; aus (5) und (6) folgt mit Rücksicht auf (1) eine Gleichung von der Gestalt

$$\mathsf{H}_1^{E_1} \cdots \mathsf{H}_{v^*}^{E_{v^*}} \mathsf{H}_{v^*+1}^{e_1 hu - 2U_{v^*+1}} \cdots \mathsf{H}_{\frac{m}{2}}^{e_{\frac{m}{2}}-v^*{}^{hu} - 2U_{\frac{m}{2}}} \xi'' = 1, \tag{7}$$

wo $E_1, \ldots, E_{v^*}$ gewisse ganze rationale Exponenten sind und ξ'' wiederum eine Einheit in k bedeutet. Da h und u ungerade Zahlen sind, so würde, wenn unter den Zahlen $e_1, \ldots, e_{\frac{m}{2}-v^*}$ auch nur eine gleich 1 ausfiele, notwendig der betreffende Exponent in der Reihe

$$e_1 hu - 2U_{v^*+1}, \ldots, e_{\frac{m}{2}-v^*} hu - 2U_{\frac{m}{2}}$$

ungerade und daher gewiß von 0 verschieden sein; dann aber widerspräche die Relation (7) der zweiten Aussage des Satzes 19. Hiermit ist gezeigt, daß in der Relation (4) die Exponenten $e_1, \ldots, e_{\frac{m}{2}-v^*}$ notwendig sämtlich gleich 0 sind.

Nunmehr erkennen wir leicht, daß in (4) auch der Exponent e verschwinden muß. Würde e nämlich den Wert 1 haben können, so wäre $\mathfrak{M} = \sqrt{\mu}$ ein Ideal $\mathfrak{j}$ in k und folglich $\mu = \mathfrak{j}^2$; das Erheben zur h-ten Potenz würde $\mu^h = \mathfrak{j}^{2h}$ liefern und, wenn $\mathfrak{j}^h = (\iota)$ gesetzt wird, wo ι eine ganze Zahl in k bedeutet, so würde $\mu^h = \varepsilon\iota^2$ oder $\mu = \varepsilon\alpha^2$ folgen, wo ε eine Einheit in k und $\alpha = \frac{\iota}{\mu^{\frac{h-1}{2}}}$ eine gewisse Zahl in k bedeutet. Diese Annahme ist jedoch zu Anfang unseres Beweises vorläufig ausgeschlossen. Hiermit ist in der Tat bewiesen, daß eine Relation von der Gestalt (4) nicht stattfinden kann; es sei denn, daß die Exponenten $e, e_1, \ldots, e_{\frac{m}{2}-v^*}$ sämtlich gleich 0 sind.

Nunmehr kehren wir zu den Gleichungen (3) zurück und wählen unter den t ambigen Primidealen $\mathfrak{D}_1, \ldots, \mathfrak{D}_t$ solche $\frac{m}{2} - v^* + 1$ aus — es seien dazu etwa $\mathfrak{D}_1, \ldots, \mathfrak{D}_{\frac{m}{2}-v^*+1}$ geeignet —, welche sich vermöge dieser Gleichungen (3) durch die Ideale $\mathfrak{M}, \mathfrak{M}_1, \ldots, \mathfrak{M}_{\frac{m}{2}-v^*}$, durch die übrigen ambigen Primideale $\mathfrak{D}_{\frac{m}{2}-v^*+2}, \ldots, \mathfrak{D}_t$ und gewisse Ideale $\mathfrak{m}^{(i)}$ des Körpers k, wie folgt, ausdrücken lassen:

$$\mathfrak{D}_i = \mathfrak{M}^{b^{(i)}}\mathfrak{M}_1^{b_1^{(i)}} \cdots \mathfrak{M}_{\frac{m}{2}-v^*}^{b_{\frac{m}{2}-v^*}^{(i)}} \mathfrak{D}_{\frac{m}{2}-v^*+2}^{d_{\frac{m}{2}-v^*+2}^{(i)}} \cdots \mathfrak{D}_t^{d_t^{(i)}} \mathfrak{m}^{(i)}, \tag{8}$$

$$\left(i = 1, 2, \ldots, \frac{m}{2} - v^* + 1\right),$$

wo die Exponenten $b^{(i)}, b_1^{(i)}, \ldots, b_{\frac{m}{2}-v^*}^{(i)}, d_{\frac{m}{2}-v^*+2}^{(i)}, \ldots, d_t^{(i)}$ gewisse Werte 0, 1 haben. Daß dies möglich sein muß, erkennen wir, wenn wir die vorhin bewiesene Tatsache benutzen, derzufolge eine Relation von der Gestalt (4) nicht stattfinden kann, es sei denn, daß sämtliche Exponenten $e, e_1, \ldots, e_{\frac{m}{2}-v^*}$ verschwinden. Überdies haben wir dabei den Umstand zu berücksichtigen, daß die Quadrate der ambigen Primideale $\mathfrak{D}_1, \ldots, \mathfrak{D}_t$ und ebenso die Quadrate der Ideale

$$\mathfrak{M}, \mathfrak{M}_1, \ldots, \mathfrak{M}_{\frac{m}{2}-v^*}$$

Ideale in k werden.

Da die Ideale $\mathfrak{M}, \mathfrak{M}_1, \ldots, \mathfrak{M}_{\frac{m}{2}-v^*}$ Hauptideale sind, so zeigen die Gleichungen (8) unmittelbar, daß die durch $\mathfrak{D}_1, \ldots, \mathfrak{D}_{\frac{m}{2}-v^*+1}$ bestimmten ambigen Komplexe gewisse Produkte derjenigen Komplexe sind, die durch die Ideale $\mathfrak{D}_{\frac{m}{2}-v^*+2}, \ldots, \mathfrak{D}_t$ bestimmt sind. Die Anzahl der voneinander unabhängigen,

aus ambigen Idealen entspringenden Komplexe ist also sicher nicht größer als $a^* = t + v^* - \frac{m}{2} - 1$ und die Anzahl aller überhaupt aus ambigen Idealen entspringenden Komplexe ist demnach nicht größer als 2^{a^*}.

Wir beweisen jetzt, daß die aus den a^* ambigen Primidealen $\mathfrak{D}_{\frac{m}{2}-v^*+2}, \ldots, \mathfrak{D}_t$ entspringenden a^* Komplexe wirklich voneinander unabhängig sind. In der Tat, würde einer dieser Komplexe, etwa der aus $\mathfrak{D}_{\frac{m}{2}-v^*+2}$ entspringende Komplex, sich durch die übrigen ausdrücken lassen, so müßte eine Äquivalenz von der Gestalt

$$\mathfrak{D}_{\frac{m}{2}-v^*+2} \sim \mathfrak{D}_{\frac{m}{2}-v^*+3}^{e_{\frac{m}{2}-v^*+3}} \cdots \mathfrak{D}_t^{e_t}\mathfrak{j}$$

statthaben, worin $e_{\frac{m}{2}-v^*+3}, \ldots, e_t$ gewisse Exponenten 0, 1 bedeuten und $\mathfrak{j}$ ein Ideal in k ist. Verstehen wir unter $\mathfrak{j}'$ ein Ideal in k, für welches in k die Äquivalenz $\mathfrak{j}'\mathfrak{D}_{\frac{m}{2}-v^*+2}^2 \sim \mathfrak{j}$ gilt, so folgt die weitere Äquivalenz

$$\mathfrak{D}_{\frac{m}{2}-v^*+2}\mathfrak{D}_{\frac{m}{2}-v^*+3}^{e_{\frac{m}{2}-v^*+3}} \cdots \mathfrak{D}_t^{e_t}\mathfrak{j}' \sim 1;$$

wir können demnach

$$\mathfrak{D}_{\frac{m}{2}-v^*+2}\mathfrak{D}_{\frac{m}{2}-v^*+3}^{e_{\frac{m}{2}-v^*+3}} \cdots \mathfrak{D}_t^{e_t}\mathfrak{j}' = (\mathsf{A}) \tag{9}$$

setzen, wobei A eine ganze Zahl des Körpers K bedeuten soll.

Da der Gleichung (9) zufolge das Hauptideal (A) seinem relativ konjugierten Ideale gleich sein muß, so findet eine Gleichung von der Gestalt

$$\mathsf{A} = \mathsf{E} \cdot S\mathsf{A} \tag{10}$$

statt, wo E eine Einheit in K bedeutet. Nun wenden wir den Satz 19 auf die Einheit E an; es sei demgemäß u ein ungerader Exponent, so daß

$$\mathsf{E}^u = \mathsf{H}_1^{U_1} \cdots \mathsf{H}_{\frac{m}{2}}^{U_{\frac{m}{2}}} \xi$$

wird, wo die Exponenten $U_1, \ldots, U_{\frac{m}{2}}$ gewisse ganze rationale Werte haben und ξ eine Einheit in k ist. Wegen (1) können wir auch setzen

$$\mathsf{E}^u = \mathsf{H}_1^{U_1} \cdots \mathsf{H}_{v^*}^{U_{v^*}} \mathsf{H}'^{U_{v^*+1}}_{v^*+1} \cdots \mathsf{H}'^{U_{\frac{m}{2}}}_{\frac{m}{2}} \xi', \tag{11}$$

wo $\mathsf{H}'_{v^*+1}, \ldots, \mathsf{H}'_{\frac{m}{2}}$ die in (1) bestimmten Einheiten, $U'_1, \ldots, U'_{v^*}$ gewisse ganze rationale Exponenten sind und ξ' wiederum eine Einheit in k bedeutet. Wenn wir hierin auf beiden Seiten die Relativnorm bilden und berücksichtigen, daß wegen (10) $N(\mathsf{E}) = 1$ wird und daß auch die Relativnormen der Einheiten (1) den Wert 1 haben, so ergibt sich leicht

$$1 = \eta_1^{U_1} \cdots \eta_{v^*}^{U_{v^*}} \xi'^2;$$

da die durch $\eta_1, \ldots, \eta_{v^*}$ bestimmten Einheitenverbände in k voneinander unabhängig sein sollen, so folgt hieraus, daß die Exponenten $U_1', \ldots, U_{v^*}'$ sämtlich gerade sind. Wir setzen nun in Formel (11) die Werte

$$\mathsf{E} = \frac{\mathsf{A}}{S\mathsf{A}},$$

$$\mathsf{H}_1^{U_1'} = \left(\frac{\mathsf{H}_1}{S\mathsf{H}_1}\eta_1\right)^{\frac{1}{2}U_1'}, \ldots, \mathsf{H}_{v^*}^{U_{v^*}'} = \left(\frac{\mathsf{H}_{v^*}}{S\mathsf{H}_{v^*}}\eta_{v^*}\right)^{\frac{1}{2}U_{v^*}'},$$

$$\mathsf{H}'_{v^*+1} = \frac{\mathsf{M}_1}{S\mathsf{M}_1}, \ldots, \mathsf{H}'_{\frac{m}{2}} = \frac{\mathsf{M}_{\frac{m}{2}-v^*}}{S\mathsf{M}_{\frac{m}{2}-v^*}}$$

ein und erhalten dann, wenn zur Abkürzung

$$\mathsf{B} = \mathsf{A}^{-u}\mathsf{H}_1^{\frac{1}{2}U_1'} \ldots \mathsf{H}_{v^*}^{\frac{1}{2}U_{v^*}'} \cdot \mathsf{M}_1^{U_{v^*+1}} \ldots \mathsf{M}_{\frac{m}{2}-v^*}^{U_{\frac{m}{2}}} \tag{12}$$

gesetzt wird, aus (11) die Gleichung

$$\frac{\mathsf{B}}{S\mathsf{B}} = \xi'', \tag{13}$$

wo ξ'' wiederum eine Einheit in k bezeichnet. Wir bilden die Relativnorm von (13) und erhalten so $\xi''^2 = 1$; wir setzen $\xi'' = (-1)^a$, wo a einen der Werte 0, 1 bedeute. Demgemäß können wir (13) in die Gestalt

$$\frac{\mathsf{B}(\sqrt{\mu})^a}{S\{\mathsf{B}(\sqrt{\mu})^a\}} = 1 \quad \text{oder} \quad \mathsf{B}(\sqrt{\mu})^a = S\{\mathsf{B}(\sqrt{\mu})^a\}$$

bringen, d. h. $\mathsf{B}(\sqrt{\mu})^a$ ist eine Zahl in k. Indem wir die Werte (9) und (12) für die Zahlen A und B benutzen und bedenken, daß u eine ungerade Zahl ist, leiten wir aus der zuletzt gefundenen Tatsache leicht eine Relation von der Gestalt

$$\mathfrak{D}_{\frac{m}{2}-v^*+2} = \mathfrak{M}^b \mathfrak{M}_1^{b_1} \ldots \mathfrak{M}_{\frac{m}{2}-v^*}^{b_{\frac{m}{2}-v^*}} \mathfrak{D}_{\frac{m}{2}-v^*+3}^{d_{\frac{m}{2}-v^*+3}} \ldots \mathfrak{D}_t^{d_t}\mathfrak{m} \tag{14}$$

ab, worin $b, b_1, \ldots, b_{\frac{m}{2}-v^*}, d_{\frac{m}{2}-v^*+3}, \ldots, d_t$ gewisse Werte 0, 1 bedeuten und $\mathfrak{m}$ ein Ideal in k ist. Setzen wir diesen Wert für $\mathfrak{D}_{\frac{m}{2}-v^*+2}$ in die rechten Seiten der Formeln (8) ein und fügen wir den so entstehenden $\frac{m}{2} - v^* + 1$ Gleichungen noch die Gleichung (14) hinzu, so erhalten wir ein System von $\frac{m}{2} - v^* + 2$ Gleichungen von der Gestalt

$$\mathfrak{D}_i = \mathfrak{M}^{B^{(i)}} \mathfrak{M}_1^{B_1^{(i)}} \ldots \mathfrak{M}_{\frac{m}{2}-v^*}^{B_{\frac{m}{2}-v^*}^{(i)}} \mathfrak{D}_{\frac{m}{2}-v^*+3}^{D_{\frac{m}{2}-v^*+3}^{(i)}} \ldots \mathfrak{D}_t^{D_t^{(i)}} \mathfrak{n}^{(i)}, \tag{15}$$

$$\left(i = 1, 2, \ldots, \frac{m}{2} - v^* + 2\right),$$

worin

$$B^{(i)}, B_1^{(i)}, \ldots, B_{\frac{m}{2}-v^*}^{(i)}, D_{\frac{m}{2}-v^*+3}^{(i)}, \ldots, D_t^{(i)}$$

gewisse Exponenten 0, 1 und $\mathfrak{n}^{(i)}$ wiederum gewisse Ideale in k sind. Das Bestehen dieser Gleichungen (15) ist aber unmöglich. In der That, bestimmen wir $\frac{m}{2} - v^* + 2$ ganze rationale Zahlen

$$a^{(1)}, \ldots, a^{\left(\frac{m}{2}-v^*+2\right)},$$

die nicht sämtlich gerade sind, derart daß nach dem Modul 2 die $\frac{m}{2} - v^* + 1$ Kongruenzen

$$\sum_{(i)} a^{(i)} B^{(i)} \equiv 0, \sum_{(i)} a^{(i)} B_1^{(i)} \equiv 0, \ldots, \sum_{(i)} a^{(i)} B_{\frac{m}{2}-v^*}^{(i)} \equiv 0, \quad (2),$$

$$\left(i = 1, 2, \ldots, \frac{m}{2} - v^* + 2\right)$$

gelten, so ergibt sich, indem wir (15) in die $a^{(i)}$-te Potenz erheben und die so für $i = 1, 2, \ldots, \frac{m}{2} - v^* + 2$ entstehenden Gleichungen miteinander multiplizieren, eine Gleichung von der Gestalt:

$$\mathfrak{D}_1^{a^{(1)}} \ldots \mathfrak{D}_{\frac{m}{2}-v^*+2}^{a^{\left(\frac{m}{2}-v^*+2\right)}} = \mathfrak{D}_{\frac{m}{2}-v^*+3}^{E^{\left(\frac{m}{2}-v^*+3\right)}} \ldots \mathfrak{D}_t^{E^{(t)}} \mathfrak{n}, \tag{16}$$

wo die Exponenten $E^{\left(\frac{m}{2}-v^*+3\right)}, \ldots, E^{(t)}$ gewisse Werte 0, 1 bedeuten und $\mathfrak{n}$ ein Ideal in k ist. Diese Gleichung (16) ist unmöglich, weil ihre linke Seite wenigstens einen der Primfaktoren $\mathfrak{D}_1, \ldots, \mathfrak{D}_{\frac{m}{2}-v^*+2}$ zu einer ungeraden Potenz erhoben enthält, rechts dagegen diese Primfaktoren nur in $\mathfrak{n}$ und also sämtlich zu einer geraden Potenz vorkommen. Wir müssen daher unsere ursprüngliche Annahme verwerfen, wonach der aus $\mathfrak{D}_{\frac{m}{2}-v^*+2}$ entspringende Komplex sich durch die aus $\mathfrak{D}_{\frac{m}{2}-v^*+3}, \ldots, \mathfrak{D}_t$ entspringenden Komplexe sollte ausdrücken lassen; mithin haben wir gezeigt, daß es in $K(\sqrt{\mu})$ genau 2^{a^*} Komplexe von der Art gibt, wie es Satz 22 behauptet.

In dem soeben geführten Beweise für Satz 22 wurde zu Anfang der Fall ausgeschlossen, daß μ gleich dem Produkt einer Einheit in das Quadrat einer Zahl des Körpers k ausfällt; es lassen sich jedoch ohne Schwierigkeit die Abänderungen auffinden, welche in diesem speziellen Falle an dem eben mitgeteilten Beweise anzubringen sind.

Da die Anzahl der aus ambigen Idealen entspringenden Komplexe mindestens gleich 1 ist, so folgt insbesondere aus dem Satze 22 die Ungleichung

$$t + v^* - \frac{m}{2} > 0.$$

§ 16. Die Anzahl aller ambigen Komplexe in K.

Satz 23. Wenn die Anzahl aller ambigen Ideale des Körpers $K(\sqrt{\mu})$ gleich 2^t ist und wenn diejenigen Einheiten in k, welche Relativnormen von Einheiten oder von gebrochenen Zahlen des Körpers $K(\sqrt{\mu})$ sind, zusammen

genau 2^v Einheitenverbände in k ausmachen: dann ist die Anzahl aller ambigen Komplexe des Körpers $K(\sqrt{\mu})$ genau 2^a, wo a die Zahl

$$a = t + v - \frac{m}{2} - 1$$

bedeutet.

Beweis. Wir machen über die Zahl μ zunächst wieder die nämliche Annahme wie zu Beginn des Beweises von Satz 22 und benutzen durchweg die dort angewandte Bezeichnungsweise. Da die Anzahl der Verbände von Einheiten in k, welche Relativnormen irgendwelcher Zahlen in K sind, 2^v betragen soll, so muß es möglich sein, zu den im vorigen Beweise bestimmten Einheiten $\eta_1, \ldots, \eta_{v^*}$ gewisse $v - v^*$ Einheiten $\vartheta_1, \ldots, \vartheta_{v-v^*}$ von folgenden Eigenschaften hinzuzufügen: die Einheiten $\vartheta_1, \ldots, \vartheta_{v-v^*}$ sind Relativnormen von gewissen gebrochenen Zahlen $\Theta_1, \ldots, \Theta_{v-v^*}$ des Körpers K, so daß die Gleichungen

$$\vartheta_1 = N(\Theta_1), \ldots, \vartheta_{v-v^*} = N(\Theta_{v-v^*}) \tag{1}$$

bestehen, und überdies soll jede Einheit ε in k, welche Relativnorm einer Einheit oder einer gebrochenen Zahl in K ist, auf eine und nur auf eine Weise in der Gestalt

$$\varepsilon = \eta_1^{e_1} \cdots \eta_{v^*}^{e_{v^*}} \vartheta_1^{f_1} \cdots \vartheta_{v-v^*}^{f_{v-v^*}} \xi^2$$

darstellbar sein, wo die Exponenten $e_1, \ldots, e_{v^*}, f_1, \ldots, f_{v-v^*}$ gewisse Werte 0, 1 haben und ξ eine Einheit in k bedeutet. Es sind dann die aus $\eta_1, \ldots, \eta_{v^*}$, $\vartheta_1, \ldots, \vartheta_{v-v^*}$ entspringenden Einheitenverbände voneinander unabhängig.

Wir setzen nun

$$\Theta_i = \frac{\mathfrak{A}_i}{\mathfrak{B}_i}, \qquad (i = 1, 2, \ldots, v - v^*),$$

wo $\mathfrak{A}_i$ und $\mathfrak{B}_i$ je zwei zueinander prime Ideale des Körpers K seien; dann folgt wegen (1) $\mathfrak{B}_i = S\mathfrak{A}_i$ und hieraus

$$\Theta_i = \frac{\mathfrak{A}_i}{S\mathfrak{A}_i}, \qquad (i = 1, 2, \ldots, v - v^*) \tag{2}$$

und aus dieser Gleichung (2) wiederum schließen wir $\mathfrak{A}_i \sim S\mathfrak{A}_i$ d. h. die durch die Ideale $\mathfrak{A}_i$ bestimmten Komplexe sind sämtlich ambig.

Wir wollen nun beweisen, daß diese $v - v^*$ durch die Ideale $\mathfrak{A}_i$ bestimmten Komplexe zusammen mit den im Beweise zu Satz 22 gefundenen aus den ambigen Idealen $\mathfrak{D}_{\frac{m}{2}-v^*+2}, \ldots, \mathfrak{D}_t$ entspringenden

$$a^* = t + v^* - \frac{m}{2} - 1$$

ambigen Komplexen ein System voneinander unabhängiger Komplexe bilden und daß ferner überhaupt jeder ambige Komplex des Körpers K ein Produkt von denjenigen

$$a = v - v^* + a^* = t + v - \frac{m}{2} - 1$$

ambigen Komplexen ist, die aus den Idealen $\mathfrak{A}_1, \ldots, \mathfrak{A}_{v-v^*}, \mathfrak{D}_{\frac{m}{2}-v^*+2}, \ldots, \mathfrak{D}_t$ entspringen.

In der Tat, nehmen wir an, es seien diese Komplexe nicht voneinander unabhängig, so müßte für die betreffenden Ideale eine Relation von der Gestalt

$$\mathfrak{A}_1^{a_1} \cdots \mathfrak{A}_{v-v^*}^{a_{v-v^*}} \mathfrak{D}_{\frac{m}{2}-v^*+2}^{e_1} \cdots \mathfrak{D}_t^{e_{a^*}} \cdot \mathfrak{j} = \Theta \tag{3}$$

gelten, worin die Exponenten $a_1, \ldots, a_{v-v^*}, e_1, \ldots, e_{a^*}$ gewisse Werte 0, 1, jedoch nicht sämtlich den Wert 0 haben, ferner $\mathfrak{j}$ ein Ideal in k und Θ eine ganze Zahl in K bedeutet. Aus (3) folgt leicht wegen (2) die Gleichung

$$\frac{\Theta}{S\Theta} = \Theta_1^{a_1} \cdots \Theta_{v-v^*}^{a_{v-v^*}} \mathsf{H}, \tag{4}$$

wo H eine gewisse Einheit in $K(\sqrt{\mu})$ ist. Indem wir von beiden Seiten der Formel (4) die Relativnorm bilden, erhalten wir mit Rücksicht auf (1)

$$N(\mathsf{H}) = \vartheta_1^{-a_1} \cdots \vartheta_{v-v^*}^{-a_{v-v^*}}$$

und hieraus ersehen wir, daß die Einheit

$$\vartheta = \vartheta_1^{-a_1} \cdots \vartheta_{v-v^*}^{-a_{v-v^*}} \tag{5}$$

die Relativnorm einer Einheit in K ist. Wir dürfen folglich

$$\vartheta = \eta_1^{b_1} \cdots \eta_{v^*}^{b_{v^*}} \xi^2 \tag{6}$$

setzen, wo $b_1, \ldots, b_{v^*}$ gewisse Werte 0, 1 haben und ξ eine Einheit in k bedeutet. Aus (5) und (6) erhalten wir die Gleichung

$$\eta_1^{b_1} \cdots \eta_{v^*}^{b_{v^*}} \vartheta_1^{a_1} \cdots \vartheta_{v-v^*}^{a_{v-v^*}} \xi^2 = 1.$$

Wegen der Unabhängigkeit der durch $\eta_1, \ldots, \eta_{v^*}, \vartheta_1, \ldots, \vartheta_{v-v^*}$ bestimmten Einheitenverbände ist diese Gleichung nur möglich, wenn sämtliche Exponenten $b_1, \ldots, b_{v^*}, a_1, \ldots, a_{v-v^*}$ gerade und also gleich 0 sind. Hierdurch erhält die Relation (3) die Gestalt

$$\mathfrak{D}_{\frac{m}{2}-v^*+2}^{e_1} \cdots \mathfrak{D}_t^{e_{a^*}} \mathfrak{j} = \Theta$$

und diese Relation erfordert wegen der Unabhängigkeit der aus $\mathfrak{D}_{\frac{m}{2}-v^*+2}, \ldots, \mathfrak{D}_t$ entspringenden Komplexe, daß auch sämtliche Exponenten $e_1, \ldots, e_{a^*}$ gleich 0 sind — eine Folgerung, die unserer ursprünglichen Annahme über die Exponenten in der Relation (3) widerspricht.

Es bleibt noch übrig, den Nachweis dafür zu führen, daß jeder ambige Komplex A als Produkt von solchen Komplexen dargestellt werden kann, die aus den Idealen $\mathfrak{A}_1, \ldots, \mathfrak{A}_{v-v^*}, \mathfrak{D}_{\frac{m}{2}-v^*+2}, \ldots, \mathfrak{D}_t$ entspringen. Ist $\mathfrak{A}$ ein beliebiges Ideal des Komplexes A, so gilt wegen Satz 21 eine Gleichung von der Gestalt

$$\frac{S\mathfrak{A}}{\mathfrak{A}} = \Theta, \tag{7}$$

wo Θ eine Zahl in K bedeutet. Indem wir auf beiden Seiten dieser Gleichung (7) die Relativnorm bilden, erkennen wir, daß die Relativnorm der Zahl Θ eine Einheit ϑ in k wird; wir können demgemäß

$$\vartheta = N(\Theta) = \eta_1^{e_1} \cdots \eta_{v^*}^{e_{v^*}} \vartheta_1'^{f_1} \cdots \vartheta_{v-v^*}'^{f_{v-v^*}} \xi^z$$

setzen, wo die Exponenten $e_1, \ldots, e_{v^*}, f_1, \ldots, f_{v-v^*}$ gewisse Werte 0, 1 haben und ξ eine Einheit in k bedeutet. Wir entnehmen hieraus für die Zahl

$$\Theta' = \pm \Theta \mathsf{H}_1^{-e_1} \cdots \mathsf{H}_{v^*}^{-e_{v^*}} \Theta_1'^{-f_1} \cdots \Theta_{v-v^*}'^{-f_{v-v^*}} \xi^{-1},$$

wo das Vorzeichen so angenommen werde, daß jedenfalls $\Theta' \neq -1$ ist, die Gleichung

$$N(\Theta') = 1.$$

Wegen dieser Gleichung haben wir

$$\Theta' = \frac{\Theta' + 1}{S(\Theta' + 1)}. \tag{8}$$

Nunmehr entsteht aus der Gleichung

$$\pm \Theta' \Theta^{-1} \mathsf{H}_1^{e_1} \cdots \mathsf{H}_{v^*}^{e_{v^*}} \Theta_1'^{f_1} \cdots \Theta_{v-v^*}'^{f_{v-v^*}} \xi = 1$$

vermöge (2), (7), (8) die Gleichung für Ideale

$$\frac{(\Theta' + 1)\, \mathfrak{A}\, \mathfrak{A}_1'^{f_1} \cdots \mathfrak{A}_{v-v^*}'^{f_{v-v^*}}}{S(\Theta' + 1)\, S\mathfrak{A}\, S\mathfrak{A}_1'^{f_1} \cdots S\mathfrak{A}_{v-v^*}'^{f_{v-v^*}}} = 1,$$

und wenn daher zur Abkürzung

$$\mathfrak{D} = (\Theta' + 1)\, \mathfrak{A}\, \mathfrak{A}_1'^{f_1} \cdots \mathfrak{A}_{v-v^*}'^{f_{v-v^*}} \tag{9}$$

gesetzt wird, so erhalten wir schließlich

$$\mathfrak{D} = S\mathfrak{D},$$

d. h. $\mathfrak{D}$ ist ein Produkt eines gewissen ambigen Ideals in ein Ideal des Körpers k und folglich zeigt die Gleichung (9), daß $\mathfrak{A}$ einem Produkt von gewissen Idealen aus der Reihe $\mathfrak{A}_1, \ldots, \mathfrak{A}_{v-v^*}, \mathfrak{D}_1, \ldots, \mathfrak{D}_t$ in ein Ideal des Körpers k äquivalent ist. Da die ambigen Ideale $\mathfrak{D}_1, \ldots, \mathfrak{D}_{\frac{w}{2}-v^*+1}$ als gewisse Produkte aus den Idealen $\mathfrak{D}_{\frac{w}{2}-v^*+2}, \ldots, \mathfrak{D}_t$ darstellbar sind, so ist hiermit der Beweis des Satzes 23 vollständig geführt. Wird angenommen, daß μ gleich dem Produkt einer Einheit in das Quadrat einer Zahl in k ist, so sind geringe Abänderungen dieses Beweises nötig.

§ 17. Das Charakterensystem einer Zahl und eines Ideals im Körper K.

Wir erörtern nunmehr die Einteilung der Idealklassen des relativquadratischen Körpers $K(\sqrt{\mu})$ in Geschlechter. Zu dem Zwecke bezeichnen wir die t in der Relativdiskriminante des Körpers $K(\sqrt{\mu})$ aufgehenden Primideale

des Körpers k mit $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ und machen für die folgenden Definitionen und Beweise in § 17 bis § 19 *die vorläufige Annahme, daß diese Primideale* $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ *sämtlich zu* 2 *prim sind*, oder, was nach Satz 5 im wesentlichen auf das nämliche hinauskommt, daß die Zahl μ zu 2 prim ist und zugleich dem Quadrat einer ganzen Zahl in k nach 2^2 kongruent ausfällt. Erst im Laufe der weiteren Untersuchung werden wir diese Einschränkung aufheben.

Definition 11. Zu einer beliebigen ganzen von 0 verschiedenen Zahl ν des Körpers k gehören bestimmte Werte der t einzelnen Symbole

$$\left(\frac{\nu, \mu}{\mathfrak{d}_1}\right), \ldots, \left(\frac{\nu, \mu}{\mathfrak{d}_t}\right),$$

welche gemäß der Definition 6 gewisse t Einheiten ± 1 bedeuten; diese Einheiten sollen das *Charakterensystem der Zahl* ν *im Körper* $K(\sqrt{\mu})$ heißen.

Um auch einem jeden Ideal $\mathfrak{J}$ des Körpers $K(\sqrt{\mu})$ in bestimmter Weise ein Charakterensystem zuzuordnen, bilden wir die Relativnorm $N(\mathfrak{J}) = \mathfrak{j}$ und dann ihre h-te Potenz $\mathfrak{j}^h = (\nu)$, wo ν eine ganze Zahl in k sein soll. Nunmehr verstehen wir unter ξ_1 eine Einheit in k. Haben dann für jede beliebige Einheit ξ_1 alle t Symbole

$$\left(\frac{\xi_1, \mu}{\mathfrak{d}_1}\right), \ldots, \left(\frac{\xi_1, \mu}{\mathfrak{d}_t}\right)$$

durchweg den Wert $+1$, so setzen wir $r = t$ und bezeichnen die r Einheitswurzeln

$$\left(\frac{\nu, \mu}{\mathfrak{d}_1}\right), \ldots, \left(\frac{\nu, \mu}{\mathfrak{d}_r}\right)$$

als das *Charakterensystem des Ideals* $\mathfrak{J}$; dasselbe ist dann durch das Ideal $\mathfrak{J}$ völlig eindeutig bestimmt.

Es sei andererseits eine spezielle Einheit ε_1 in k vorhanden, für welche wenigstens eines der t Symbole

$$\left(\frac{\varepsilon_1, \mu}{\mathfrak{d}_1}\right), \ldots, \left(\frac{\varepsilon_1, \mu}{\mathfrak{d}_t}\right)$$

gleich -1 wird; dann können wir, ohne damit eine Beschränkung einzuführen, annehmen, es sei etwa $\left(\frac{\varepsilon_1, \mu}{\mathfrak{d}_t}\right) = -1$. Wir betrachten nun alle diejenigen Einheiten ξ_2 in k, für welche $\left(\frac{\xi_2, \mu}{\mathfrak{d}_t}\right) = +1$ wird. Es sei unter diesen wieder eine solche Einheit $\xi_2 = \varepsilon_2$ vorhanden, für welche wenigstens eines der $t-1$ Symbole

$$\left(\frac{\varepsilon_2, \mu}{\mathfrak{d}_1}\right), \ldots, \left(\frac{\varepsilon_2, \mu}{\mathfrak{d}_{t-1}}\right)$$

gleich -1 wird; dann können wir annehmen, es sei etwa $\left(\frac{\varepsilon_2, \mu}{\mathfrak{d}_{t-1}}\right) = -1$. Wir betrachten ferner alle diejenigen Einheiten ξ_3, für welche sowohl $\left(\frac{\xi_3, \mu}{\mathfrak{d}_t}\right) = +1$ als auch $\left(\frac{\xi_3, \mu}{\mathfrak{d}_{t-1}}\right) = +1$ wird, und sehen nach, ob unter diesen eine Einheit

$\xi_3 = \varepsilon_3$ vorhanden ist, für welche wenigstens eines der $t-2$ Symbole

$$\left(\frac{\varepsilon_3, \mu}{\mathfrak{d}_1}\right), \ldots, \left(\frac{\varepsilon_3, \mu}{\mathfrak{d}_{t-2}}\right)$$

gleich -1 wird. Fahren wir in der begonnenen Weise fort, so erhalten wir schließlich eine gewisse Anzahl r^* und dazu ein System von r^* Einheiten $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r^*}$ des Körpers k, von der Art, daß bei geeigneter Anordnung der Primideale $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ die Gleichungen

$$\left.\begin{aligned}
&\left(\frac{\varepsilon_1, \mu}{\mathfrak{d}_t}\right) = -1, \\
&\left(\frac{\varepsilon_2, \mu}{\mathfrak{d}_t}\right) = +1, \left(\frac{\varepsilon_2, \mu}{\mathfrak{d}_{t-1}}\right) = -1, \\
&\left(\frac{\varepsilon_3, \mu}{\mathfrak{d}_t}\right) = +1, \left(\frac{\varepsilon_3, \mu}{\mathfrak{d}_{t-1}}\right) = +1, \left(\frac{\varepsilon_3, \mu}{\mathfrak{d}_{t-2}}\right) = -1, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&\left(\frac{\varepsilon_{r^*}, \mu}{\mathfrak{d}_t}\right) = +1, \left(\frac{\varepsilon_{r^*}, \mu}{\mathfrak{d}_{t-1}}\right) = +1, \left(\frac{\varepsilon_{r^*}, \mu}{\mathfrak{d}_{t-2}}\right) = +1, \ldots, \left(\frac{\varepsilon_{r^*}, \mu}{\mathfrak{d}_{t-r^*+1}}\right) = -1
\end{aligned}\right\} \quad (1)$$

gelten und daß außerdem für eine jede solche Einheit ξ, die den r^* Gleichungen

$$\left(\frac{\xi, \mu}{\mathfrak{d}_t}\right) = +1, \left(\frac{\xi, \mu}{\mathfrak{d}_{t-1}}\right) = +1, \ldots, \left(\frac{\xi, \mu}{\mathfrak{d}_{t-r^*+1}}\right) = +1$$

genügt, notwendig auch die $t - r^*$ Symbole

$$\left(\frac{\xi, \mu}{\mathfrak{d}_1}\right), \ldots, \left(\frac{\xi, \mu}{\mathfrak{d}_{t-r^*}}\right)$$

sämtlich den Wert $+1$ besitzen.

Wir können nunmehr mit Rücksicht auf die zweite Formel in Satz 14 die vorhin aus dem Ideal $\mathfrak{J}$ gebildete Zahl ν des Körpers k derart mit gewissen der Einheiten $\varepsilon_1, \ldots, \varepsilon_{r^*}$ multiplizieren, daß das entstehende Produkt $\bar{\nu}$ den Gleichungen

$$\left(\frac{\bar{\nu}, \mu}{\mathfrak{d}_t}\right) = +1, \left(\frac{\bar{\nu}, \mu}{\mathfrak{d}_{t-1}}\right) = +1, \ldots, \left(\frac{\bar{\nu}, \mu}{\mathfrak{d}_{t-r^*+1}}\right) = +1$$

genügt; ist $\bar{\nu}$ derart bestimmt, so bezeichne ich die $r = t - r^*$ Einheiten ± 1

$$\left(\frac{\bar{\nu}, \mu}{\mathfrak{d}_1}\right), \ldots, \left(\frac{\bar{\nu}, \mu}{\mathfrak{d}_r}\right)$$

als das *Charakterensystem des Ideals* $\mathfrak{J}$. Dasselbe ist durch das Ideal $\mathfrak{J}$ völlig eindeutig bestimmt. In § 19 wird gezeigt werden, daß stets $r^* < t$ und mithin $r \geqq 1$ wird.

§ 18. Der Begriff des Geschlechtes.

Wir erkennen sofort die Tatsache, daß die Ideale ein und derselben Klasse des Körpers $K(\sqrt{\mu})$ sämtlich dasselbe Charakterensystem besitzen. Hierdurch ist überhaupt einer jeden Idealklasse des Körpers $K(\sqrt{\mu})$ ein bestimmtes Charakterensystem zugeordnet.

Definition 12. Alle diejenigen Idealklassen, denen ein und dasselbe Charakterensystem zugeordnet ist, deren Ideale also sämtlich ein und dasselbe Charakterensystem besitzen, fassen wir zu einem *Geschlecht* zusammen und definieren insbesondere das *Hauptgeschlecht* als die Gesamtheit aller derjenigen Klassen, deren Charakterensystem aus lauter Einheiten $+1$ besteht. Da das Charakterensystem der Hauptklasse offenbar von der letzteren Eigenschaft ist, so gehört insbesondere die Hauptklasse stets zum Hauptgeschlecht.

Aus der zweiten Formel des Satzes 14 entnehmen wir leicht die folgenden Tatsachen: Wenn G und G' zwei beliebige Geschlechter sind und die Klassen in G mit den Klassen in G' multipliziert werden, so bilden sämtliche solche Produkte wiederum ein Geschlecht; dieses werde das *Produkt der Geschlechter* G und G' genannt. Das Charakterensystem desselben erhalten wir durch Multiplikation der entsprechenden Charaktere der beiden Geschlechter G und G'.

Jedes Geschlecht des Körpers K enthält gleich viel Klassen, nämlich so viel Klassen als das Hauptgeschlecht. Die zu irgendeiner Klasse C relativ konjugierte Klasse SC gehört zu demselben Geschlechte wie C selbst. Das Quadrat einer jeden Klasse C gehört stets zum Hauptgeschlecht.

Die h Klassen eines beliebigen Komplexes P gehören offenbar sämtlich zu dem nämlichen Geschlecht; ich bezeichne dieses Geschlecht als das *Geschlecht des Komplexes* P.

§ 19. Obere Grenze für die Anzahl der Geschlechter in K.

Es entsteht die wichtige Frage, ob ein System von r beliebig vorgelegten Einheiten ± 1 stets das Charakterensystem für ein Geschlecht in K sein kann. Wir beweisen zunächst einige zur Beantwortung dieser Frage notwendige Hilfssätze.

Satz 24. (Hilfssatz.) Wenn t und v die Bedeutung wie in Satz 23 haben und r wie in § 17 die Anzahl der Charaktere ist, welche das Geschlecht einer Idealklasse in K bestimmen, so ist stets

$$t + v - \frac{m}{2} \leqq r.$$

Beweis. Im Beweise zu Satz 22 und Satz 23 sind v^* Einheiten $\eta_1, \ldots, \eta_{v^*}$ und $v - v^*$ Einheiten $\vartheta_1, \ldots, \vartheta_{v-v^*}$ mit gewissen dort entwickelten Eigenschaften aufgestellt worden. Es seien ferner $\varepsilon_1, \ldots, \varepsilon_{r^*}$ diejenigen besonderen r^* Einheiten des Körpers k, die in § 17 eingeführt worden sind; dann ist $r = t - r^*$. Wir beweisen zunächst, daß die $r^* + v$ aus

$$\varepsilon_1, \ldots, \varepsilon_{r^*}, \quad \eta_1, \ldots, \eta_{v^*}, \quad \vartheta_1, \ldots, \vartheta_{v-v^*}$$

entspringenden Einheitenverbände voneinander unabhängig sind. In der Tat, nehmen wir an, es gäbe zwischen den genannten $r^* + v$ Einheiten eine Relation von der Gestalt

$$\varepsilon_1^{a_1} \ldots \varepsilon_{r^*}^{a_{r^*}} \eta_1^{b_1} \ldots \eta_{v^*}^{b_{v^*}} \vartheta_1^{c_1} \ldots \vartheta_{v-v^*}^{c_{v-v^*}} = \xi^z, \quad (1)$$

so daß die Exponenten $a_1, \ldots, a_{r^*}, b_1, \ldots, b_{v^*}, c_1, \ldots, c_{v-v^*}$ gewisse Werte 0, 1, jedoch nicht sämtlich den Wert 0 haben und ξ eine geeignete Einheit in k vorstellt: dann müßte für jedes Primideal $\mathfrak{w}$ des Körpers k

$$\left(\frac{\varepsilon_1^{a_1} \cdots \varepsilon_{r^*}^{a_{r^*}} \eta_1^{b_1} \cdots \eta_{v^*}^{b_{v^*}} \vartheta_1^{c_1} \cdots \vartheta_{v-v^*}^{c_{v-v^*}}, \mu}{\mathfrak{w}}\right) = +1$$

ausfallen, und wenn wir berücksichtigen, daß die Einheiten

$$\eta_1, \ldots, \eta_{v^*}, \quad \vartheta_1, \ldots, \vartheta_{v-v^*}$$

sämtlich Relativnormen von Zahlen in K sind und daher auch stets

$$\left(\frac{\eta_x, \mu}{\mathfrak{w}}\right) = +1, \quad \left(\frac{\vartheta_y, \mu}{\mathfrak{w}}\right) = +1$$
$$(x = 1, 2, \ldots, v^*;\ y = 1, 2, \ldots, v - v^*)$$

sein muß, so ergibt sich

$$\left(\frac{\varepsilon_1^{a_1} \cdots \varepsilon_{r^*}^{a_{r^*}}, \mu}{\mathfrak{w}}\right) = +1.$$

Hierin setzen wir der Reihe nach für $\mathfrak{w}$ jedes der r^* in der Relativdiskriminante von K aufgehenden Primideale $\mathfrak{d}_{t-r^*+1}, \ldots, \mathfrak{d}_t$ ein und erhalten so die Gleichungen

$$\left(\frac{\varepsilon_1^{a_1} \cdots \varepsilon_{r^*}^{a_{r^*}}, \mu}{\mathfrak{d}_i}\right) = +1, \qquad (i = t - r^* + 1, \ldots, t). \tag{2}$$

Wegen des in § 17 aufgestellten Systems von Formeln (1) für die Einheiten $\varepsilon_1, \ldots, \varepsilon_{r^*}$ können diese Gleichungen (2) nur bestehen, wenn die Exponenten $a_1, \ldots, a_{r^*}$ sämtlich gerade und also gleich 0 sind. Die Relation (1) erhält dann die Gestalt

$$\eta_1^{b_1} \cdots \eta_{v^*}^{b_{v^*}} \vartheta_1^{c_1} \cdots \vartheta_{v-v^*}^{c_{v-v^*}} = \xi^2.$$

Das Bestehen dieser Relation ist aber, da nach § 16 die durch $\eta_1, \ldots, \eta_{v^*}$, $\vartheta_1, \ldots, \vartheta_{v-v^*}$ bestimmten Einheitenverbände voneinander unabhängig sind, nur möglich, falls die Exponenten $b_1, \ldots, b_{v^*}, c_1, \ldots, c_{v-v^*}$ sämtlich gerade und also gleich 0 sind. Daraus folgt, daß eine Relation von der Gestalt (1), wie wir sie annahmen, nicht statthaben kann, d. h. die aus den Einheiten $\varepsilon_1, \ldots, \varepsilon_{r^*}, \eta_1, \ldots, \eta_{v^*}, \vartheta_1, \ldots, \vartheta_{v-v^*}$ entspringenden Verbände sind voneinander unabhängig; durch Multiplikation erhalten wir also aus diesen Verbänden genau 2^{r^*+v} voneinander verschiedene Einheitenverbände in k, und da es im ganzen in k nach § 11 nur $2^{\frac{m}{2}}$ Einheitenverbände gibt, so haben wir $r^* + v \leqq \frac{m}{2}$. Hiermit deckt sich die Aussage des Satzes 24.

Da nach der Bemerkung am Schluß von § 15 stets $t + v^* - \frac{m}{2} > 0$ und also um so mehr $t + v - \frac{m}{2} > 0$ ausfällt, so folgt aus Satz 24 insbesondere $r \geqq 1$ und also $r^* < t$.

Satz 25. (Hilfssatz.) Die Anzahl g der verschiedenen Geschlechter im Körper $K(\sqrt{\mu})$ ist kleiner oder höchstens gleich der Anzahl A der ambigen Komplexe des Körpers $K(\sqrt{\mu})$.

Beweis. Wenn g die Anzahl der Geschlechter ist, in welche sich die Ideale oder die Idealklassen des Körpers K einteilen, so zerfallen zufolge der letzten Bemerkung in § 18 auch die Komplexe des Körpers K genau in g Geschlechter. Bezeichnen wir daher mit f die Anzahl der Komplexe vom Hauptgeschlecht, so ist die Anzahl aller überhaupt vorhandenen Komplexe, welche M heiße, genau

$$M = gf.$$

Wie bereits in § 18 bemerkt worden ist, gehört das Quadrat einer beliebigen Klasse C stets zum Hauptgeschlecht, und daher ist auch das Quadrat eines beliebigen Komplexes stets ein Komplex des Hauptgeschlechtes. Wir fassen nun diejenigen Komplexe des Hauptgeschlechtes ins Auge, welche Quadrate von Komplexen sind; ihre Anzahl sei f', und wir bezeichnen sie mit $P_1, \ldots, P_{f'}$, so daß $P_1 = Q_1^2, \ldots, P_{f'} = Q_{f'}^2$ wird, wo $Q_1, \ldots, Q_{f'}$ gewisse Komplexe bedeuten. Es fällt offenbar $f' \leqq f$ aus. Ist jetzt P ein beliebiger Komplex, so wird P^2 notwendig ein bestimmter der f' Komplexe $P_1, \ldots, P_{f'}$; es sei etwa $P^2 = P_i$. Dann folgt $P^2 = Q_i^2$, d. h. $(PQ_i^{-1})^2 = 1$ und nach § 12 ist aus diesem Grunde PQ_i^{-1} ein ambiger Komplex A; es wird $P = AQ_i$, und folglich stellt der Ausdruck AQ_i überhaupt alle Komplexe dar, sobald A alle ambigen Komplexe und Q_i die f' Komplexe $Q_1, \ldots, Q_{f'}$ durchläuft. Auch ist klar, daß diese Darstellung für jeden Komplex nur auf eine Weise möglich ist; es ist daher die Anzahl aller überhaupt vorhandenen Komplexe

$$M = \mathrm{A}f'.$$

Die Zusammenstellung dieser Gleichung mit der vorhin gefundenen $M = gf$ liefert $gf = \mathrm{A}f'$, und wegen $f' \leqq f$ folgt hieraus $g \leqq \mathrm{A}$, womit der Satz 25 bewiesen ist.

Nunmehr sind wir imstande, die folgende Tatsache zu beweisen, welche für unsere späteren Entwicklungen von besonderer Bedeutung ist:

Satz 26. (Hilfssatz.) Wenn im Körper K die Anzahl der Charaktere, welche das Geschlecht einer Klasse bestimmen, gleich r ist, so genügt die Anzahl g der Geschlechter jenes Körpers stets der Bedingung

$$g \leqq 2^{r-1}.$$

Beweis. Nach Satz 23 ist die Anzahl A aller ambigen Komplexe in K

$$\mathrm{A} = 2^a = 2^{t+v-\frac{m}{2}-1}.$$

Nach Satz 24 gilt die Ungleichung

$$t + v - \frac{m}{2} \leqq r;$$

mithin ist auch

$$\mathrm{A} \leqq 2^{r-1}$$

und daraus folgt, vermöge Satz 25, die Richtigkeit des Satzes 26.

§ 20. Das primäre Primideal $\mathfrak{p}$ und das Symbol $\left(\frac{\mathfrak{j}}{\mathfrak{p}}\right)$.

Es ist für die folgenden Entwicklungen von Nutzen, eine gewisse Art von Primidealen in k besonders zu benennen.

Definition 13. Ein solches zu 2 primes Primideal des Körpers k, nach welchem jede Einheit in k quadratischer Rest ist, möge ein *primäres Primideal* heißen; dagegen möge jedes solche Primideal *nichtprimär* genannt werden, nach welchem wenigstens eine Einheit in k quadratischer Nichtrest ist.

Wir führen für primäre Primideale noch ein neues Symbol ein.

Definition 14. Es sei $\mathfrak{p}$ ein primäres Primideal und $\mathfrak{j}$ ein beliebiges Ideal in k, es werde $\mathfrak{j}^h = (\iota)$ gesetzt, wo ι eine ganze Zahl in k bedeutet; dieselbe ist bis auf eine Einheit als Faktor eindeutig durch das Ideal $\mathfrak{j}$ bestimmt. Das Symbol $\left(\frac{\iota}{\mathfrak{p}}\right)$ ist folglich ein durch $\mathfrak{p}$ und $\mathfrak{j}$ völlig bestimmter Wert $+1$ oder -1 oder 0; dieser Wert werde mit $\left(\frac{\mathfrak{j}}{\mathfrak{p}}\right)$ bezeichnet, so daß das neue Symbol $\left(\frac{\mathfrak{j}}{\mathfrak{p}}\right)$ durch die Gleichung

$$\left(\frac{\mathfrak{j}}{\mathfrak{p}}\right) = \left(\frac{\iota}{\mathfrak{p}}\right)$$

definiert ist.

Sind $\mathfrak{j}_1$, $\mathfrak{j}_2$ irgend zwei zu $\mathfrak{p}$ prime Ideale in k, so gilt offenbar stets die Gleichung

$$\left(\frac{\mathfrak{j}_1\mathfrak{j}_2}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{j}_1}{\mathfrak{p}}\right)\left(\frac{\mathfrak{j}_2}{\mathfrak{p}}\right).$$

Ist η eine ganze Zahl in k und $\mathfrak{h} = (\eta)$ das durch η dargestellte Hauptideal, so ist offenbar

$$\left(\frac{\eta}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{h}}{\mathfrak{p}}\right);$$

denn da h ungerade ist, so haben beide Seiten dieser Gleichung den Wert $\left(\frac{\eta^h}{\mathfrak{p}}\right)$.

In § 21 werden wir gewisse Systeme von $\frac{m}{2}$ nichtprimären Primidealen des Körpers k untersuchen und in § 23 die wichtigste Eigenschaft der primären Primideale beweisen.

§ 21. Ein System von $\frac{m}{2}$ nichtprimären Primidealen des Körpers k.

Es sei, wie zu Beginn von § 14, $\varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}-1}$ ein volles System von Grundeinheiten in k; ferner sei $\varepsilon_{\frac{m}{2}} = \zeta$ eine wie in § 11 bestimmte Einheitswurzel in k, so daß nach § 11 jede beliebige Einheit ε des Körpers k sich auf eine und nur auf eine Weise in der Gestalt

$$\varepsilon = \varepsilon_1^{e_1}\varepsilon_2^{e_2}\cdots\varepsilon_{\frac{m}{2}}^{e_{\frac{m}{2}}}\xi^2$$

darstellen läßt, wo $e_1, \ldots, e_{\frac{m}{2}}$ gewisse Werte 0, 1 haben und ξ eine Einheit in k bedeutet. Es sind dann die aus $\varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}}$ entspringenden Verbände des Körpers k voneinander unabhängig und diese $\frac{m}{2}$ Verbände liefern durch Multiplikation die sämtlichen $2^{\frac{m}{2}}$ Einheitenverbände des Körpers k.

Satz 27[1]. *Die Relativdiskriminante eines relativquadratischen Körpers $K(\sqrt{\mu})$ in bezug auf k ist stets von 1 verschieden.*

Beweis. Zufolge der Bemerkung am Ende des § 15 gilt bei Benutzung der in Satz 22 erklärten Bezeichnungen die Ungleichung

$$t + v^* - \frac{m}{2} > 0.$$

Da die Anzahl sämtlicher Einheitenverbände im Körper k genau $2^{\frac{m}{2}}$ beträgt, so ist notwendig $\frac{m}{2} \geqq v^*$ und mithin erhalten wir $t > 0$. Diese Folgerung stimmt mit der Aussage des Satzes 27 überein.

Satz 28. Wenn eine Einheit ε des Körpers k kongruent dem Quadrat einer ganzen Zahl nach 2^2 ausfällt, so ist sie das Quadrat einer Einheit in k.

Beweis. Nehmen wir im Gegenteil an, es wäre ε nicht das Quadrat einer Zahl in k, so würde $\sqrt{\varepsilon}$ einen relativquadratischen Körper bestimmen; wegen der Sätze 4 und 5 besäße dieser Körper die Relativdiskriminante 1 und, da dies nach Satz 27 nicht sein kann, so ist die Annahme, von der wir ausgingen, unzutreffend.

Die Gültigkeit der Sätze 27 und 28 ist wesentlich durch die beiden besonderen Annahmen bedingt, welche wir im Anfange dieses Abschnittes II (S. 393) für den Körper k gemacht haben. Wenn also etwa k^* ein Zahlkörper ist, der entweder selbst reell ist, bez. einen reellen konjugierten Körper besitzt oder dessen Klassenanzahl gerade ausfällt, so kann es sehr wohl einen relativquadratischen Körper K^* geben, der in bezug auf k^* die Relativdiskriminante 1 besitzt, und es ist die Aufstellung und Untersuchung aller solcher relativquadratischen Körper K^* sogar die wichtigste und schwierigste Aufgabe, die sich bei der Ausdehnung unserer Theorie auf beliebige Grundkörper k^* bietet.

Satz 29. Es sei $\varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}}$ das zu Beginn dieses § 21 aufgestellte System von Einheiten in k; es seien ferner $\mathfrak{q}_1, \ldots, \mathfrak{q}_{\frac{m}{2}}$ solche zu 2 prime Primideale des Körpers k, für welche allemal

$$\left(\frac{\varepsilon_i}{\mathfrak{q}_i}\right) = -1, \quad \left(\frac{\varepsilon_k}{\mathfrak{q}_i}\right) = +1, \quad (i \neq k),$$

$$\left(i, k = 1, 2, \ldots, \frac{m}{2}\right)$$

[1] Vgl. „Algebraische Zahlkörper“ Satz 94 (dieser Band S. 155), sowie die daselbst zu diesem Satze gemachte Bemerkung.

ausfällt; endlich setzen wir

$$\mathfrak{q}_1^h = (\varkappa_1), \ldots, \mathfrak{q}_{\frac{m}{2}}^h = \left(\varkappa_{\frac{m}{2}}\right),$$

so daß $\varkappa_1, \ldots, \varkappa_{\frac{m}{2}}$ gewisse ganze Zahlen des Körpers k bedeuten: dann gilt für jede beliebige zu 2 prime ganze Zahl ω in k nach dem Modul 2^2 eine Kongruenz von der Gestalt

$$\omega \equiv \varepsilon_1^{u_1} \cdots \varepsilon_{\frac{m}{2}}^{u_{\frac{m}{2}}} \varkappa_1^{v_1} \cdots \varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}} \alpha^2, \qquad (2^2),$$

worin die Exponenten $u_1, \ldots, u_{\frac{m}{2}}, v_1, \ldots, v_{\frac{m}{2}}$ gewisse Werte 0, 1 haben und α eine geeignete ganze Zahl in k ist.

Beweis. Wir behandeln zunächst die Annahme, es gäbe m Exponenten $u_1, \ldots, u_{\frac{m}{2}}, v_1, \ldots, v_{\frac{m}{2}}$, die gewisse Werte 0, 1 haben, aber nicht sämtlich gleich 0 sind, derart, daß die vermöge dieser Exponenten gebildete Zahl

$$\mu = \varepsilon_1^{u_1} \cdots \varepsilon_{\frac{m}{2}}^{u_{\frac{m}{2}}} \varkappa_1^{v_1} \cdots \varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}} \qquad (1)$$

dem Quadrat einer ganzen Zahl in k nach dem Modul 2^2 kongruent werde. Die Zahl $\sqrt{\mu}$ bestimmt, wie leicht ersichtlich, einen relativquadratischen Körper $K(\sqrt{\mu})$ in bezug auf k. Zufolge des Satzes 5 ist die Relativdiskriminante dieses Körpers $K(\sqrt{\mu})$ prim zu 2 und nach Satz 4 besitzt sie diejenigen von den Primidealen $\mathfrak{q}_1, \ldots, \mathfrak{q}_{\frac{m}{2}}$ zu Faktoren, für welche in (1) die betreffenden Exponenten $v_1, \ldots, v_{\frac{m}{2}}$ gleich 1 werden. Wegen Satz 27 ist die Anzahl t dieser Primideale mindestens gleich 1; es seien etwa die t Primideale $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ diejenigen, die in der Relativdiskriminante des Körpers $K(\sqrt{\mu})$ als Faktoren enthalten sind.

Ist nun ε irgendeine Einheit in k, die gleich der Relativnorm einer Einheit in $K(\sqrt{\mu})$ gesetzt werden kann, und bringen wir ε in die Gestalt

$$\varepsilon = \varepsilon_1^{e_1} \cdots \varepsilon_{\frac{m}{2}}^{e_{\frac{m}{2}}} \xi^2,$$

wo die Exponenten $e_1, \ldots, e_{\frac{m}{2}}$ gewisse Werte 0, 1 haben und ξ eine Einheit in k bedeutet, so folgt aus Definition 6 unmittelbar

$$\left(\frac{\varepsilon, \mu}{\mathfrak{q}_i}\right) = +1$$

für $i = 1, 2, \ldots, t$ und, da nach Satz 9 mit Rücksicht auf unsere über $\mathfrak{q}_1, \ldots, \mathfrak{q}_{\frac{m}{2}}$ gemachten Voraussetzungen

$$\left(\frac{\varepsilon, \mu}{\mathfrak{q}_i}\right) = \left(\frac{\varepsilon}{\mathfrak{q}_i}\right) = (-1)^{e_i}, \qquad (i = 1, 2, \ldots, t)$$

ausfällt, so folgt notwendig

$$e_1 = 0, e_2 = 0, \ldots, e_t = 0,$$

d. h. die Einheit ε muß ein Produkt aus gewissen von den $\frac{m}{2} - t$ Einheiten $\varepsilon_{t+1}, \varepsilon_{t+2}, \ldots, \varepsilon_{\frac{m}{2}}$ in das Quadrat einer Einheit des Körpers k sein. Die sämtlichen Einheiten in k, welche Relativnormen von Einheiten in $K(\sqrt{\mu})$ sind, machen also höchstens $2^{\frac{m}{2}-t}$ Verbände in k aus; somit würde unter Anwendung der in Satz 22 erklärten Bezeichnungsweise

$$v^* \leqq \frac{m}{2} - t \quad \text{oder} \quad t + v^* - \frac{m}{2} \leqq 0$$

sein müssen, was der Bemerkung am Schluß von § 15 widerspricht. Unsere vorhin versuchte Annahme ist also unzutreffend, d. h. es ist keine Zahl μ von der Gestalt (1) nach 2^2 dem Quadrat einer ganzen Zahl in k kongruent, es sei denn, daß die Exponenten

$$u_1, \ldots, u_{\frac{m}{2}}, \quad v_1, \ldots, v_{\frac{m}{2}}$$

sämtlich gleich 0 sind.

Wir verstehen nun unter $\alpha_1, \alpha_2, \ldots, \alpha_{\varphi(2)}$ ein volles System von $\varphi(2)$ ganzen nach dem Modul 2 einander inkongruenten und zu 2 primen Zahlen in k. Dann stellt der Ausdruck

$$\varepsilon_1^{u_1} \cdots \varepsilon_{\frac{m}{2}}^{u_{\frac{m}{2}}} \varkappa_1^{v_1} \cdots \varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}} \alpha_i^2 \qquad (2)$$

$$\left(u_1, \ldots, u_{\frac{m}{2}}, v_1, \ldots, v_{\frac{m}{2}} = 0, 1; \qquad i = 1, 2, 3, \ldots, \varphi(2)\right)$$

ein System von $2^m \varphi(2)$ Zahlen dar, welche untereinander nach 2^2 inkongruent sind. In der Tat, wären zwei von diesen $2^m \varphi(2)$ Zahlen (2) nach 2^2 kongruent, wäre etwa

$$\varepsilon_1^{u_1} \cdots \varepsilon_{\frac{m}{2}}^{u_{\frac{m}{2}}} \varkappa_1^{v_1} \cdots \varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}} \alpha_i^2 \equiv \varepsilon_1^{u'_1} \cdots \varepsilon_{\frac{m}{2}}^{u'_{\frac{m}{2}}} \varkappa_1^{v'_1} \cdots \varkappa_{\frac{m}{2}}^{v'_{\frac{m}{2}}} \alpha_{i'}^2, \qquad (2^2),$$

so würde, da $\alpha_i, \alpha_{i'}$ zu 2 prim sind, aus dem vorhin Bewiesenen sofort folgen, daß die Exponenten $u_1, \ldots, u_{\frac{m}{2}}, v_1, \ldots, v_{\frac{m}{2}}$ sämtlich bez. mit den Exponenten $u'_1, \ldots, u'_{\frac{m}{2}}, v'_1, \ldots, v'_{\frac{m}{2}}$ übereinstimmen, und es wäre mithin

$$\alpha_i^2 \equiv \alpha_{i'}^2, \qquad (2^2). \qquad (3)$$

Betrachten wir jetzt ein in der Zahl 2 als Faktor enthaltenes Primideal $\mathfrak{l}$ und nehmen an, es gehe dasselbe in 2 genau zur l-ten Potenz auf, so folgt aus (3)

$$(\alpha_i - \alpha_{i'})(\alpha_i + \alpha_{i'}) \equiv 0, \qquad (\mathfrak{l}^{2l});$$

es ist mithin entweder $\alpha_i - \alpha_{i'}$ oder $\alpha_i + \alpha_{i'}$ durch $\mathfrak{l}^l$ teilbar, und da offenbar

$$\alpha_i - \alpha_{i'} \equiv \alpha_i + \alpha_{i'}, \qquad (2)$$

ist, so folgt in jedem Falle

$$\alpha_i \equiv \alpha_{i'}, \qquad (\mathfrak{l}^l).$$

Die nämliche Betrachtung gilt für jedes in 2 aufgehende Primideal und daher erhalten wir

$$\alpha_i \equiv \alpha_{i'}, \qquad (2)$$

und schließen hieraus

$$\alpha_i = \alpha_{i'},$$

d. h. die beiden ganzen Zahlen des Systems (2) waren nicht voneinander verschieden. Bezeichnen wir die verschiedenen in 2 aufgehenden Primideale des Körpers k mit $\mathfrak{l}_1, \ldots, \mathfrak{l}_s$, so haben wir[1]

$$\varphi(2) = 2^m \left(1 - \frac{1}{n(\mathfrak{l}_1)}\right) \cdots \left(1 - \frac{1}{n(\mathfrak{l}_s)}\right),$$

$$\varphi(2^2) = 2^{2m} \left(1 - \frac{1}{n(\mathfrak{l}_1)}\right) \cdots \left(1 - \frac{1}{n(\mathfrak{l}_s)}\right);$$

es ist somit $2^m \varphi(2) = \varphi(2^2)$ und die Zahlen von der Gestalt (2), deren Anzahl $\varphi(2^2)$ ist, bilden folglich ein volles System von Resten nach dem Modul 2^2, die zu 2 prim sind; dies ist die Aussage des Satzes 29.

§ 22. Die unendliche Reihe $\sum_{(\mathfrak{w})} \left(\frac{\mathfrak{w}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{w})^s}$.

Ehe wir näher die Natur der primären Primideale ergründen, entwickeln wir einige Sätze, die sich an die Überlegungen in § 13 anschließen.

Satz 30. (Hilfssatz.) Die reellen Veränderlichen $x_1, \ldots, x_m$ mögen als rechtwinklige Koordinaten eines m-dimensionalen Raumes betrachtet werden und es sei in diesem Raume eine endliche Anzahl von $(m-1)$-dimensionalen Flächenscharen durch Gleichungen von der Gestalt

$$f_1(x_1, \ldots, x_m, \tau) = 0, \qquad f_2(x_1, \ldots, x_m, \tau) = 0, \ldots$$

gegeben, wo $f_1, f_2, \ldots$ analytische Funktionen der Argumente $x_1, \ldots, x_m, \tau$ bedeuten, die in der Umgebung des Parameterwertes $\tau = 0$ sich regulär verhalten; diese Flächen mögen, wenn wir dem Parameter τ einen festen positiven Wert oder den Wert 0 erteilen, einen bestimmten ganz im Endlichen gelegenen Teil R_τ des m-dimensionalen Raumes abgrenzen. Nunmehr wählen wir für den Parameter τ einen positiven Wert und fixieren in dem m-dimensionalen Raume alle Punkte, deren Koordinaten von der Form

$$x_1 = u_1 \tau, \; x_2 = u_2 \tau, \ldots, \; x_m = u_m \tau$$

sind, wo $u_1, u_2, \ldots, u_m$ sämtliche ganze rationale Zahlen durchlaufen: dann wird die Anzahl T aller derjenigen solchen Punkte, die in jenem Raume R_τ liegen, durch die Formel

$$T = \frac{J}{\tau^m} + \frac{M}{\tau^{m-1}}$$

dargestellt, wo J den Inhalt des für $\tau = 0$ sich ergebenden Raumes R_0 und M

[1] Vgl. „Algebraische Zahlkörper" Satz 23 (dieser Band Abh. 7 S. 82).

eine von τ abhängige Größe bezeichnet, welche stets zwischen endlichen Grenzen bleibt, sobald τ gegen 0 konvergiert.

Dieser Hilfssatz ist eine Erweiterung desjenigen Satzes, welchen bereits H. Minkowski[1] und H. Weber[2] aufgestellt und bewiesen haben, und man erkennt ohne Schwierigkeit die Abänderungen, welche diese Beweise verlangen, wenn man die Richtigkeit der soeben von mir aufgestellten Erweiterung einsehen will.

Satz 31. Ist $\mathfrak{p}$ ein bestimmtes primäres Primideal, so stellt die über sämtliche Primideale $\mathfrak{w}$ des Körpers k zu erstreckende unendliche Summe

$$\sum_{(\mathfrak{w})} \left(\frac{\mathfrak{w}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{w})^s}, \qquad (s > 1)$$

eine solche Funktion der reellen Veränderlichen s dar, welche stets unterhalb einer *positiven* endlichen Grenze bleibt, wenn die reelle Veränderliche s sich der Grenze 1 nähert.

Beweis. Aus den m konjugierten Körpern $k, k', \ldots, k^{(m-1)}$ wählen wir irgend solche $\frac{m}{2} - 1$ Körper aus, von denen keine zwei zu einander konjugiert imaginär sind, und bezeichnen diese mit $k_1, k_2, \ldots, k_{\frac{m}{2}-1}$. Ist ferner α irgendeine von 0 verschiedene Zahl in k, so bezeichnen wir die zu α konjugierten in $k_1, \ldots, k_{\frac{m}{2}-1}$ liegenden Zahlen bez. mit $\alpha_1, \ldots, \alpha_{\frac{m}{2}-1}$ und nennen die $\frac{m}{2} - 1$ reellen Logarithmen

$$\begin{aligned} l_1(\alpha) &= 2 \log |\alpha_1|, \\ l_2(\alpha) &= 2 \log |\alpha_2|, \\ &\cdots\cdots\cdots \\ l_{\frac{m}{2}-1}(\alpha) &= 2 \log |\alpha_{\frac{m}{2}-1}| \end{aligned}$$

kurz die Logarithmen zur Zahl α. Endlich bezeichnen wir mit $\varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}-1}$ ein System von $\frac{m}{2} - 1$ Grundeinheiten in k und berechnen dann aus den Gleichungen

$$\begin{aligned} l_1(\alpha) - \frac{2}{m} \log n(\alpha) &= e_1(\alpha) l_1(\varepsilon_1) + \cdots + e_{\frac{m}{2}-1}(\alpha) l_1\left(\varepsilon_{\frac{m}{2}-1}\right), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ l_{\frac{m}{2}-1}(\alpha) - \frac{2}{m} \log n(\alpha) &= e_1(\alpha) l_{\frac{m}{2}-1}(\varepsilon_1) + \cdots + e_{\frac{m}{2}-1}(\alpha) l_{\frac{m}{2}-1}\left(\varepsilon_{\frac{m}{2}-1}\right) \end{aligned}$$

[1] Geometrie der Zahlen, Teubner 1896, S. 62.

[2] Über einen in der Zahlentheorie angewandten Satz der Integralrechnung, Nachr. Ges. Wiss. Göttingen 1896, S. 275. H. Weber hat diesen Satz hernach in seinen Untersuchungen „Über Zahlengruppen in algebraischen Körpern" zweite Abhandlung Math. Ann. 49, S. 83 (1897) auf ein dem meinigen verwandtes Problem der Zahlentheorie angewandt.

$\frac{m}{2}-1$ reelle Größen $e_1(\alpha), \ldots, e_{\frac{m}{2}-1}(\alpha)$; diese $\frac{m}{2}-1$ Größen mögen kurz die Exponenten zur Zahl α heißen. Es ist klar, daß jede Zahl α durch Multiplikation mit ganzen Potenzen von $\varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}-1}$ auf eine und nur auf eine Weise in eine solche Zahl α^* verwandelt werden kann, zu der die Exponenten $e_1, \ldots, e_{\frac{m}{2}-1}$ den Bedingungen

$$0 \leqq e_1 < 1,\ 0 \leqq e_2 < 1, \ldots, 0 \leqq e_{\frac{m}{2}-1} < 1$$

genügen. Umgekehrt sehen wir leicht, daß zwei Einheiten, deren Exponenten bez. einander gleich sind, sich nur um einen Faktor unterscheiden können, welcher eine Einheitswurzel ist. Die Anzahl aller in k liegenden Einheitswurzeln werde mit w bezeichnet.

Es sei nun C eine beliebige Idealklasse in k und $\mathfrak{a}$ ein zu $\mathfrak{p}$ primes Ideal der zu C reziproken Klasse C^{-1}; ferner bestimmen wir ein volles System von quadratischen Resten nach $\mathfrak{p}$, etwa $\varrho, \varrho', \varrho'', \ldots$, und zwar derart, daß diese $\frac{n(\mathfrak{p})-1}{2}$ Zahlen $\varrho, \varrho', \varrho'', \ldots$ sämtlich durch $\mathfrak{a}$ teilbar sind: dann läßt sich offenbar jede durch $\mathfrak{a}$ teilbare ganze Zahl in k, welche quadratischer Rest nach $\mathfrak{p}$ ist, in einer der $\frac{n(\mathfrak{p})-1}{2}$ Formen

$$\left.\begin{array}{l} u_1\varkappa^{(1)} + \cdots + u_m\varkappa^{(m)} + \varrho\ , \\ u_1\varkappa^{(1)} + \cdots + u_m\varkappa^{(m)} + \varrho'\ , \\ u_1\varkappa^{(1)} + \cdots + u_m\varkappa^{(m)} + \varrho''\ , \\ \cdots\cdots\cdots\cdots \end{array}\right| \tag{1}$$

darstellen, wo $u_1, \ldots, u_m$ gewisse ganze rationale Zahlen und $\varkappa^{(1)}, \ldots, \varkappa^{(m)}$ die Basiszahlen des Ideals $\mathfrak{p}\mathfrak{a}$ bedeuten. Es sei ferner α irgendein durch $\mathfrak{a}$ teilbarer quadratischer Rest nach $\mathfrak{p}$; da $\mathfrak{p}$ ein primäres Primideal sein soll, so besitzt jede Zahl α^*, die durch Multiplikation der Zahl α mit einer beliebigen Einheit entspringt, die gleiche Eigenschaft und ist mithin ebenfalls in einer jener Formen (1) darstellbar.

Indem wir diese Tatsachen zusammen nehmen, erkennen wir folgendes: das w-fache der Anzahl $F(t)$ aller durch $\mathfrak{a}$ teilbaren Hauptideale $\mathfrak{h}$, deren Normen die reelle positive Zahl t nicht überschreiten und für welche $\left(\frac{\mathfrak{h}}{\mathfrak{p}}\right) = +1$ ausfällt, ist gleich der Anzahl T der verschiedenen Systeme von rationalen ganzzahligen Werten $u_1, \ldots, u_m$, für welche die Ungleichungen

$$\left.\begin{array}{r} n(u_1\varkappa^{(1)} + \cdots + u_m\varkappa^{(m)} + \varrho) \leqq t \\ 0 \leqq e_1(u_1\varkappa^{(1)} + \cdots + u_m\varkappa^{(m)} + \varrho) < 1\ , \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ 0 \leqq e_{\frac{m}{2}-1}(u_1\varkappa^{(1)} + \cdots + u_m\varkappa^{(m)} + \varrho) < 1 \end{array}\right| \tag{2}$$

erfüllt sind, vermehrt um die entsprechenden Anzahlen $T', T'', \ldots$, wo allgemein $T^{(s)}$ die Anzahl der verschiedenen rationalen ganzzahligen Wertsysteme $u_1, \ldots, u_m$ bedeutet, für welche die Ungleichungen

$$\begin{array}{r} n(u_1\varkappa^{(1)} + \cdots + u_m\varkappa^{(m)} + \varrho^{(s)}) \leqq t\ , \\ 0 \leqq e_1(u_1\varkappa^{(1)} + \cdots + u_m\varkappa^{(m)} + \varrho^{(s)}) < 1\ , \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ 0 \leqq e_{\frac{m}{2}-1}(u_1\varkappa^{(1)} + \cdots + u_m\varkappa^{(m)} + \varrho^{(s)}) < 1 \end{array}$$

erfüllt sind; es ist also

$$w\,F(t) = T + T' + T'' + \cdots .$$

Um zunächst die Anzahl T abzuschätzen, setzen wir in den Ungleichungen (2)

$$u_1 = \frac{x_1}{\tau}, \ldots, u_m = \frac{x_m}{\tau}, \tau = t^{-\frac{1}{m}}$$

ein; dieselben gehen dadurch in die folgenden Ungleichungen über:

$$\left.\begin{array}{r} n(x_1\varkappa^{(1)} + \cdots + x_m\varkappa^{(m)} + \varrho\tau) \leqq 1, \\ 0 \leqq e_1 < 1\ , \\ \cdots\cdots \\ 0 \leqq e_{\frac{m}{2}-1} < 1\ , \end{array}\right| \tag{3}$$

wo die Größen $e_1, \ldots, e_{\frac{m}{2}-1}$ durch die Gleichungen

$$\left.\begin{array}{r} e_1 l_1(\varepsilon_1) + \cdots + e_{\frac{m}{2}-1} l_1\left(\varepsilon_{\frac{m}{2}-1}\right) \\ = 2\log|x_1\varkappa_1^{(1)} + \cdots + x_m\varkappa_1^{(m)} + \varrho_1\tau| \\ - \frac{2}{m}\log n(x_1\varkappa^{(1)} + \cdots + x_m\varkappa^{(m)} + \varrho\tau)\ , \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ e_1 l_{\frac{m}{2}-1}(\varepsilon_1) + \cdots + e_{\frac{m}{2}-1} l_{\frac{m}{2}-1}\left(\varepsilon_{\frac{m}{2}-1}\right) \\ = 2\log|x_1\varkappa_{\frac{m}{2}-1}^{(1)} + \cdots + x_m\varkappa_{\frac{m}{2}-1}^{(m)} + \varrho_{\frac{m}{2}-1}\tau| \\ - \frac{2}{m}\log n(x_1\varkappa^{(1)} + \cdots + x_m\varkappa^{(m)} + \varrho\tau) \end{array}\right| \tag{4}$$

als Funktionen von $x_1, \ldots, x_m, \tau$ zu bestimmen sind; hierin bedeuten $\varkappa_1^{(i)}, \ldots, \varkappa_{\frac{m}{2}-1}^{(i)}, \varrho_1, \ldots, \varrho_{\frac{m}{2}-1}$ die zu $\varkappa^{(i)}$, ϱ konjugierten und bez. in den Körpern $k_1, \ldots, k_{\frac{m}{2}-1}$ gelegenen Zahlen. Die Anzahl T ist mithin gleich der Anzahl aller Punkte mit den Koordinaten

$$x_1 = u_1\tau, \ldots, x_m = u_m\tau,$$

die in den durch die Ungleichungen (3) charakterisierten Teil des $x_1 \ldots x_m$-Raumes fallen. Dieser Raumteil liegt ganz im Endlichen und wird durch eine

endliche Anzahl analytischer Flächen begrenzt. Die Gleichungen dieser Flächen enthalten noch einen Parameter τ, und da ihre linken Seiten für $\tau = 0$ im fraglichen Gebiete sich regulär verhalten, so sind alle Voraussetzungen des Satzes 30 erfüllt. Wir bezeichnen mit J den Inhalt dieses Raumteiles für $\tau = 0$, d. h. den Inhalt desjenigen Raumteiles, der durch die Ungleichungen

$$\begin{gathered} n(x_1 \varkappa^{(1)} + \cdots + x_m \varkappa^{(m)}) \leqq 1, \\ 0 \leqq e_1 < 1, \\ \cdots\cdots \\ 0 \leqq e_{\frac{m}{2}-1} < 1 \end{gathered}$$

charakterisiert ist, wo jetzt die Größen $e_1, \ldots, e_{\frac{m}{2}-1}$ aus den Gleichungen

$$\begin{aligned} e_1 l_1(\varepsilon_1) + \cdots + e_{\frac{m}{2}-1} l_1\left(\varepsilon_{\frac{m}{2}-1}\right) &= 2\log\left| x_1 \varkappa_1^{(1)} + \cdots + x_m \varkappa_1^{(m)}\right| \\ &\quad - \frac{2}{m}\log n(x_1 \varkappa^{(1)} + \cdots + x_m \varkappa^{(m)}), \\ \cdots\cdots\cdots\

ist, so erhalten wir weiter

$$\sum_{(t)} \frac{\Phi(t) - \Phi(t-1)}{t^s} = \sum_{(t)} \Phi(t) \frac{s\vartheta}{t^{s+1}}, \qquad (0 < \vartheta < 1),$$

und wegen (7) und (8) folgt hieraus

$$\sum_{(\mathfrak{h})} \left(\frac{\mathfrak{h}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{h})^s} = \sum_{(t)} \frac{s\vartheta D}{t^{s+\frac{1}{m}}}, \qquad (s > 1). \tag{9}$$

Da nach dem vorhin Bewiesenen D für unendlich wachsende t zwischen endlichen Grenzen bleibt und der Wert der unendlichen Reihe

$$\sum_{(t)} \frac{1}{t^{s+\frac{1}{m}}}$$

für $s = 1$ gegen eine endliche Grenze konvergiert, so folgt aus (9), daß auch die unendliche Summe

$$\sum_{(\mathfrak{h})} \left(\frac{\mathfrak{h}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{h})^s}, \qquad (s > 1) \tag{10}$$

eine Funktion von s darstellt, welche für $s = 1$ gegen eine endliche Grenze konvergiert.

Setzen wir in (10) $\mathfrak{h} = \mathfrak{a}\mathfrak{j}$, so gehört das zu $\mathfrak{p}$ prime Ideal $\mathfrak{j}$ der Klasse C an und wir erhalten mit Rücksicht auf die Gleichung

$$\left(\frac{\mathfrak{h}}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{a}}{\mathfrak{p}}\right)\left(\frac{\mathfrak{j}}{\mathfrak{p}}\right)$$

aus der zuletzt bewiesenen Tatsache das Resultat, daß die über alle zu $\mathfrak{p}$ primen Ideale $\mathfrak{j}$ der Klasse C zu erstreckende unendliche Summe

$$\sum_{(\mathfrak{j})} \left(\frac{\mathfrak{j}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{j})^s}, \qquad (s > 1) \tag{11}$$

ebenfalls eine Funktion von s darstellt, welche für $s = 1$ gegen eine endliche Grenze konvergiert. Bilden wir die dem Ausdrucke (11) entsprechenden unendlichen Summen unter Benutzung der h verschiedenen Klassen des Körpers k und addieren alle so entstehenden h unendlichen Summen, so erkennen wir, daß auch die über alle zu $\mathfrak{p}$ primen Ideale $\mathfrak{j}$ des Körpers k erstreckte unendliche Summe

$$\sum_{(\mathfrak{j})} \left(\frac{\mathfrak{j}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{j})^s}, \qquad (s > 1) \tag{12}$$

für $s = 1$ gegen einen endlichen Grenzwert konvergiert.

Nun ist

$$\sum_{(\mathfrak{j})} \left(\frac{\mathfrak{j}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{j})^s} = \prod_{(\mathfrak{w})} \frac{1}{1 - \left(\frac{\mathfrak{w}}{\mathfrak{p}}\right) n(\mathfrak{w})^{-s}},$$

wenn das Produkt $\prod_{(\mathfrak{w})}$ über alle Primideale $\mathfrak{w}$ des Körpers k erstreckt wird und folglich erhalten wir

$$\log \sum_{(\mathfrak{j})} \left(\frac{\mathfrak{j}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{j})^s} = \sum_{(\mathfrak{w})} \left(\frac{\mathfrak{w}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{w})^s} + f(s), \qquad (s > 1), \tag{13}$$

wobei die Summe $\sum_{(\mathfrak{w})}$ ebenfalls über alle Primideale $\mathfrak{w}$ des Körpers k zu erstrecken ist und wo $f(s)$ eine Größe darstellt, die für $s = 1$ gegen einen endlichen Grenzwert konvergiert. Da (12) für $s = 1$ gegen einen endlichen Grenzwert konvergiert, so muß notwendig (13) für $s = 1$ entweder ebenfalls gegen einen endlichen Grenzwert konvergieren oder negativ über alle Grenzen wachsen; in beiden Fällen ersehen wir mithin die Richtigkeit des zu beweisenden Satzes 31.

§ 23. Eine Eigenschaft primärer Primideale.

Durch die beiden Sätze 29 und 31 gelangen wir zu folgendem wichtigen Satze über primäre Primideale:

Satz 32. Wenn $\mathfrak{p}$ ein primäres Primideal ist, so ist es stets möglich, in k eine ganze Zahl π zu finden, so daß das Ideal (π) gleich $\mathfrak{p}^h$ wird und überdies die Zahl π nach dem Modul 2^2 eine Kongruenz von der Gestalt

$$\pi \equiv \alpha^2, \qquad (2^2)$$

erfüllt, wo α eine geeignete ganze Zahl des Körpers k ist.

Beweis. Es sei $\varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}}$ das zu Beginn von § 21 aufgestellte System von Einheiten in k; es seien ferner $\mathfrak{q}_1, \ldots, \mathfrak{q}_{\frac{m}{2}}$, wie in Satz 29, solche zu 2 prime Primideale des Körpers k, für welche allemal

$$\left(\frac{\varepsilon_i}{\mathfrak{q}_i}\right) = -1, \qquad \left(\frac{\varepsilon_k}{\mathfrak{q}_i}\right) = +1, \qquad (i \neq k), \qquad \left(i, k = 1, 2, \ldots, \frac{m}{2}\right)$$

ausfällt. Die Existenz solcher Primideale folgt aus Satz 18. Wir setzen dann

$$\mathfrak{p}^h = (\pi^*), \ \mathfrak{q}_1^h = (\varkappa_1), \ \ldots, \ \mathfrak{q}_{\frac{m}{2}}^h = (\varkappa_{\frac{m}{2}}),$$

so daß $\pi^*, \varkappa_1, \ldots, \varkappa_{\frac{m}{2}}$ gewisse ganze Zahlen des Körpers k bedeuten. Wenden wir nun den Satz 29 insbesondere auf die ganze Zahl π^* an, so ergibt sich, daß π^* einer Kongruenz von der Gestalt

$$\pi^* \equiv \varepsilon \varkappa_1^{v_1} \cdots \varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}} \alpha^2, \qquad (2^2) \tag{1}$$

genügt, wo ε eine geeignete Einheit in k, ferner $v_1, \ldots, v_{\frac{m}{2}}$ gewisse Exponenten 0, 1 und α eine geeignete ganze Zahl in k bedeutet. Hätten in diesem Ausdrucke (1) rechter Hand die Exponenten $v_1, \ldots, v_{\frac{m}{2}}$ sämtlich den Wert 0, so wäre bereits $\pi = \pi^* \varepsilon$ eine Zahl von der Art, wie sie Satz 32 verlangt. Wir

nehmen also an, die Anzahl e derjenigen unter den Exponenten $v_1, \ldots, v_{\frac{m}{2}}$, welche gleich 1 ausfallen, sei größer als 0.

Setzen wir

$$\mu = \pi^* \varepsilon \varkappa_1^{v_1} \cdots \varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}},$$

so besitzt nach Satz 5 der relativquadratische Körper $K(\sqrt{\mu})$ eine zu 2 prime Relativdiskriminante. Für diesen Fall ist der Satz 26 von uns bereits bewiesen worden. Indem wir die in Definition 11 gebrauchten Bezeichnungen beibehalten, haben wir offenbar

$$t = e + 1, \quad r^* = e, \quad r = t - r^* = 1,$$

und nach dem Satze 26 ist folglich die Anzahl g der Geschlechter des Körpers $K(\sqrt{\mu})$ höchstens gleich 1 und also gleich 1, d. h. alle Idealklassen des Körpers $K(\sqrt{\mu})$ sind vom Hauptgeschlecht.

Aus der eben bewiesenen Tatsache ziehen wir folgende Schlüsse: es sei $\mathfrak{r}$ irgendein zu 2 primes Primideal in k mit der Eigenschaft

$$\left(\frac{\mu}{\mathfrak{r}}\right) = +1,$$

so daß $\mathfrak{r}$ nach Satz 7 in $K(\sqrt{\mu})$ in das Produkt zweier Primideale $\mathfrak{R}$, $S\mathfrak{R}$ zerfällt. Soll nun $\mathfrak{R}$ zum Hauptgeschlechte gehören, so muß das Charakterensystem dieses Primideals im Körper $K(\sqrt{\mu})$ aus lauter Einheiten $+1$ bestehen; es muß also das Charakterensystem einer Zahl $\xi\varrho$, wobei ξ eine geeignete Einheit in k und ϱ eine ganze Zahl in k mit der Eigenschaft $\mathfrak{r}^h = (\varrho)$ bedeutet, aus lauter Einheiten $+1$ bestehen. Wir bilden insbesondere den Charakter der Zahl $\xi\varrho$ in bezug auf das in der Relativdiskriminante von $K(\sqrt{\mu})$ aufgehende Primideal $\mathfrak{p}$ und erhalten dadurch

$$\left(\frac{\xi\varrho, \mu}{\mathfrak{p}}\right) = \left(\frac{\xi\varrho}{\mathfrak{p}}\right) = +1,$$

und wenn wir berücksichtigen, daß $\mathfrak{p}$ ein primäres Primideal ist, so wird

$$\left(\frac{\xi\varrho}{\mathfrak{p}}\right) = \left(\frac{\varrho}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{r}}{\mathfrak{p}}\right) = +1,$$

d. h. jedes Primideal $\mathfrak{r}$, für welches $\left(\frac{\mu}{\mathfrak{r}}\right) = +1$ ausfällt, besitzt auch die Eigenschaft $\left(\frac{\mathfrak{r}}{\mathfrak{p}}\right) = +1$.

Wir bestimmen nun an Stelle der Primideale $\mathfrak{q}_1, \ldots, \mathfrak{q}_{\frac{m}{2}}$ irgend $\frac{m}{2}$ andere Primideale $\mathfrak{q}_1', \ldots, \mathfrak{q}_{\frac{m}{2}}'$ mit den entsprechenden Eigenschaften

$$\left(\frac{\varepsilon_i}{\mathfrak{q}_i'}\right) = -1, \qquad \left(\frac{\varepsilon_k}{\mathfrak{q}_i'}\right) = +1, \qquad (i \neq k),$$
$$\left(i, k = 1, 2, \ldots, \frac{m}{2}\right)$$

und setzen wiederum $\mathfrak{q}_1'^h = (\varkappa_1'), \ldots, \mathfrak{q}_{\frac{m}{2}}'^h = (\varkappa_{\frac{m}{2}}')$, wo $\varkappa_1', \ldots, \varkappa_{\frac{m}{2}}'$ ganze Zahlen in k sind; sodann denken wir uns die sämtlichen Schlußfolgerungen dieses Beweises für das neue System von Primidealen $\mathfrak{q}_1', \ldots, \mathfrak{q}_{\frac{m}{2}}'$ wiederholt. Auf diese Weise gelangen wir zu einem Ausdruck

$$\mu' = \pi^* \varepsilon' \varkappa_1'^{v_1'} \cdots \varkappa_{\frac{m}{2}}'^{v_{\frac{m}{2}}'} \equiv \alpha'^2, \qquad (2^2),$$

in dem ε' eine gewisse Einheit und $v_1', \ldots, v_{\frac{m}{2}}'$ gewisse Exponenten 0, 1 bedeuten. Hätten hier die Exponenten $v_1', \ldots, v_{\frac{m}{2}}'$ sämtlich den Wert 0, so wäre wiederum $\pi = \pi^* \varepsilon'$ eine Zahl von der Art, wie sie Satz 32 verlangt; wir nehmen also an, daß diese Exponenten $v_1', \ldots, v_{\frac{m}{2}}'$ nicht sämtlich gleich 0 ausfallen und folgern dann wie vorhin, daß jedes Primideal $\mathfrak{r}$, für welches $\left(\frac{\mu'}{\mathfrak{r}}\right) = +1$ ist, auch die Eigenschaft $\left(\frac{\mathfrak{r}}{\mathfrak{p}}\right) = +1$ besitzt.

Wir bezeichnen nun kurz mit $\mathfrak{r}_\mu$ alle diejenigen Primideale in k, für welche

$$\left(\frac{\mu}{\mathfrak{r}_\mu}\right) = +1$$

ist und mit $\mathfrak{r}_{\mu\mu'}$ alle diejenigen Primideale in k, für welche zugleich

$$\left(\frac{\mu}{\mathfrak{r}_{\mu\mu'}}\right) = -1 \quad \text{und} \quad \left(\frac{\mu'}{\mathfrak{r}_{\mu\mu'}}\right) = +1$$

ausfällt, ferner mit $\mathfrak{r}_\mathfrak{p}^{(+)}, \mathfrak{r}_\mathfrak{p}^{(-)}$ diejenigen Primideale, für welche

$$\left(\frac{\mathfrak{r}_\mathfrak{p}^{(+)}}{\mathfrak{p}}\right) = +1 \quad \text{bez.} \quad \left(\frac{\mathfrak{r}_\mathfrak{p}^{(-)}}{\mathfrak{p}}\right) = -1$$

wird. Da die Zahlen μ, μ' sicher nicht Quadrate von ganzen Zahlen in k sind und bei unseren Annahmen das nämliche auch für das Produkt $\mu\mu'$ gilt, so folgen aus Satz 17 die Gleichungen

$$\left.\begin{aligned} \sum_{(\mathfrak{r}_\mu)} \frac{1}{n(\mathfrak{r}_\mu)^s} &= \frac{1}{2} \log \frac{1}{s-1} + f_\mu(s), \qquad (s > 1), \\ \sum_{(\mathfrak{r}_{\mu\mu'})} \frac{1}{n(\mathfrak{r}_{\mu\mu'})^s} &= \frac{1}{4} \log \frac{1}{s-1} + f_{\mu\mu'}(s), \qquad (s > 1); \end{aligned}\right\} \qquad (2)$$

hier sind die unendlichen Summen über alle Primideale $\mathfrak{r}_\mu$ bez. $\mathfrak{r}_{\mu\mu'}$ zu erstrecken und $f_\mu(s), f_{\mu\mu'}(s)$ bedeuten Funktionen der reellen Veränderlichen s, welche stets zwischen endlichen Grenzen bleiben, wenn s sich dem Werte 1 nähert.

Die Primideale $\mathfrak{r}_\mu$ sind offenbar sämtlich von den Primidealen $\mathfrak{r}_{\mu\mu'}$ verschieden und da nach dem vorhin Bewiesenen die Primideale $\mathfrak{r}_\mu$, $\mathfrak{r}_{\mu\mu'}$ sämtlich unter den Primidealen $\mathfrak{r}_\mathfrak{p}^{(+)}$ vorkommen, so haben wir

$$\sum_{(\mathfrak{r}_\mathfrak{p}^{(+)})} \frac{1}{n(\mathfrak{r}_\mathfrak{p}^{(+)})^s} \geqq \sum_{(\mathfrak{r}_\mu)} \frac{1}{n(\mathfrak{r}_\mu)^s} + \sum_{(\mathfrak{r}_{\mu\mu'})} \frac{1}{n(\mathfrak{r}_{\mu\mu'})^s}$$

und folglich wegen (2)

$$\sum_{(\mathfrak{r}_\mathfrak{p}^{(+)})} \frac{1}{n(\mathfrak{r}_\mathfrak{p}^{(+)})^s} \geqq \frac{3}{4} \log \frac{1}{s-1} + f_\mu(s) + f_{\mu\mu'}(s); \tag{3}$$

hier sind die unendlichen Summen wiederum über alle Primideale mit den betreffenden Eigenschaften zu erstrecken.

Die Primideale $\mathfrak{r}_\mathfrak{p}^{(+)}, \mathfrak{r}_\mathfrak{p}^{(-)}$ erschöpfen offenbar, wenn man von dem einen Primideale $\mathfrak{p}$ absieht, die sämtlichen Primideale $\mathfrak{w}$ in k und es ist daher

$$\sum_{(\mathfrak{r}_\mathfrak{p}^{(+)})} \frac{1}{n(\mathfrak{r}_\mathfrak{p}^{(+)})^s} + \sum_{(\mathfrak{r}_\mathfrak{p}^{(-)})} \frac{1}{n(\mathfrak{r}_\mathfrak{p}^{(-)})^s} = -\frac{1}{n(\mathfrak{p})^s} + \sum_{(\mathfrak{w})} \frac{1}{n(\mathfrak{w})^s} = \log \frac{1}{s-1} + f(s), \tag{4}$$

wo die Summe $\sum_{(\mathfrak{w})}$ über sämtliche Primideale $\mathfrak{w}$ in k erstreckt werden soll und $f(s)$ wiederum eine für $s = 1$ zwischen endlichen Grenzen bleibende Größe bezeichnet. Aus (3) und (4) zusammen folgt die Ungleichung

$$\sum_{(\mathfrak{r}_\mathfrak{p}^{(+)})} \frac{1}{n(\mathfrak{r}_\mathfrak{p}^{(+)})^s} - \sum_{(\mathfrak{r}_\mathfrak{p}^{(-)})} \frac{1}{n(\mathfrak{r}_\mathfrak{p}^{(-)})^s} \geqq \frac{1}{2} \log \frac{1}{s-1} + 2 f_\mu(s) + 2 f_{\mu\mu'}(s) - f(s). \tag{5}$$

Wegen

$$\sum_{(\mathfrak{r}_\mathfrak{p}^{(+)})} \frac{1}{n(\mathfrak{r}_\mathfrak{p}^{(+)})^s} - \sum_{(\mathfrak{r}_\mathfrak{p}^{(-)})} \frac{1}{n(\mathfrak{r}_\mathfrak{p}^{(-)})^s} = \sum_{(\mathfrak{w})} \left(\frac{\mathfrak{w}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{w})^s}$$

enthält die Ungleichung (5) unmittelbar einen Widerspruch gegen den Satz 31 und mithin sind unsere Annahmen zu verwerfen, d. h. es müssen die Exponenten $v_1, \ldots, v_{m-\varrho}$ in der Kongruenz (1) oder das zweitemal die Exponenten $v_1', \ldots, v_{m-\varrho}'$ in der entsprechenden Kongruenz sämtlich 0 sein; dann ist aber, wie bereits hervorgehoben wurde, $\pi = \pi^* \varepsilon$ bez. $\pi = \pi^* \varepsilon'$ eine Zahl von der Art, wie sie der Satz 32 verlangt und damit haben wir die Richtigkeit dieses Satzes erkannt.

Auch die Umkehrung des Satzes 32 ist gültig, wie der folgende Satz zeigt:

Satz 33. Wenn π eine ganze Zahl in k bedeutet, welche dem Quadrat einer ganzen Zahl in k nach 2^2 kongruent ausfällt, und wenn überdies (π) gleich $\mathfrak{p}^h$ ist, wo $\mathfrak{p}$ ein Primideal in k bedeutet, so ist dieses Primideal $\mathfrak{p}$ stets primär.

Beweis. Wir betrachten den Körper $K(\sqrt{\pi})$: Wegen Satz 4 und 5 besitzt die Relativdiskriminante dieses Körpers nur den einen Primfaktor $\mathfrak{p}$. Mit Hilfe von Satz 22, nach der Bemerkung am Schluß von § 15, und bei Anwendung der Bezeichnungsweise dieses Satzes 22 für den Körper $K(\sqrt{\pi})$ erhalten wir wegen $t = 1$ die Ungleichung

$$1 + v^* - \frac{m}{2} > 0 \quad \text{d. h.} \quad v^* \geqq \frac{m}{2}.$$

Da andererseits v^* nach § 11 nicht größer als $\frac{m}{2}$ sein kann, so haben wir $v^* = \frac{m}{2}$;

es ist mithin jede Einheit ξ in k die Relativnorm einer Einheit des Körpers $K(\sqrt{\pi})$ und hieraus folgt nach Satz 9

$$\left(\frac{\xi, \pi}{\mathfrak{p}}\right) = \left(\frac{\xi}{\mathfrak{p}}\right) = +1,$$

d. h. $\mathfrak{p}$ ist ein primäres Primideal.

§ 24. Zwei besondere Fälle des Reziprozitätsgesetzes für quadratische Reste im Körper k.

Auf Grund des Satzes 32 können wir folgende neue Definition aufstellen:

Definition 15. Wenn $\mathfrak{p}$ ein primäres Primideal in k ist und $\mathfrak{p}^h = (\pi)$ wird, wo π eine solche ganze Zahl in k bedeutet, die dem Quadrat einer ganzen Zahl in k nach dem Modul 2^2 kongruent ausfällt, so nenne ich π eine *Primärzahl des primären Primideals* $\mathfrak{p}$. Wegen Satz 28 ist die Primärzahl π durch das primäre Primideal $\mathfrak{p}$ bis auf das Quadrat einer Einheit in k bestimmt.

Satz 34. Es sei $\mathfrak{p}$ ein primäres Primideal in k und $\mathfrak{r}$ ein beliebiges Primideal in k; ferner sei π eine Primärzahl von $\mathfrak{p}$ und ϱ irgendeine ganze Zahl in k, so daß $(\varrho) = \mathfrak{r}^h$ wird: wenn dann $\left(\frac{\pi}{\mathfrak{r}}\right) = +1$ ist, so fällt auch $\left(\frac{\varrho}{\mathfrak{p}}\right) = +1$ aus.

Beweis. Mit Rücksicht auf Definition 15 und wegen Satz 4 und 5 besitzt die Relativdiskriminante des Körpers $K(\sqrt{\pi})$ nur den einen Primfaktor $\mathfrak{p}$, und daher ist wegen Satz 26 in diesem Relativkörper die Anzahl der Geschlechter gleich 1, d. h. es gehören alle Ideale des Körpers $K(\sqrt{\pi})$ dem Hauptgeschlechte an. Wegen der Annahme $\left(\frac{\pi}{\mathfrak{r}}\right) = +1$ ist nach Satz 7 $\mathfrak{r}$ in $K(\sqrt{\pi})$ in das Produkt zweier Primideale zerlegbar; für den Charakter eines jeden dieser beiden Primideale erhalten wir den Wert

$$\left(\frac{\varrho, \pi}{\mathfrak{p}}\right) = \left(\frac{\varrho}{\mathfrak{p}}\right) = +1,$$

womit der Satz 34 bewiesen ist.

Satz 35. Wenn $\mathfrak{p}, \mathfrak{p}^*$ zwei primäre Primideale in k und π, π^* bez. Primärzahlen von $\mathfrak{p}, \mathfrak{p}^*$ sind, so gilt die Gleichung

$$\left(\frac{\pi}{\mathfrak{p}^*}\right) = \left(\frac{\pi^*}{\mathfrak{p}}\right).$$

Beweis. Im Falle $\left(\frac{\pi}{\mathfrak{p}^*}\right) = +1$ folgt die Richtigkeit dieses Satzes unmittelbar aus dem Satze 34. Nehmen wir andererseits $\left(\frac{\pi}{\mathfrak{p}^*}\right) = -1$ an, so muß notwendig auch $\left(\frac{\pi^*}{\mathfrak{p}}\right) = -1$ sein; denn wäre $\left(\frac{\pi^*}{\mathfrak{p}}\right) = +1$, so würde aus dem nämlichen Satze 34 die Gleichung $\left(\frac{\pi}{\mathfrak{p}^*}\right) = +1$ folgen, was der Annahme widerspricht.

§ 25. Das Produkt $\prod_{(\mathfrak{w})}'\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$ für ein zu 2 primes ν und bei gewissen Annahmen über μ.

Wir sind jetzt imstande, einen weiteren wichtigen Bestandteil des Reziprozitätsgesetzes für quadratische Reste im Körper k abzuleiten.

Satz 36. *Wenn ν, μ zu 2 prime ganze Zahlen in k sind und überdies die Zahl μ dem Quadrat einer ganzen Zahl in k nach dem Modul 2^2 kongruent wird, so ist stets*

$$\prod_{(\mathfrak{w})}'\left(\frac{\nu,\mu}{\mathfrak{w}}\right)=+1,$$

wo das Produkt über sämtliche zu 2 primen Primideale $\mathfrak{w}$ des Körpers k erstreckt werden soll.

Beweis. Wir nehmen *erstens* ν gleich einer Zahl $\varkappa$ des Körpers k an, die von der Beschaffenheit ist, daß das Ideal $(\varkappa)$ die h-te Potenz eines nichtprimären Primideals $\mathfrak{q}$ in k wird; die Zahl μ dagegen sei ein Produkt von lauter Potenzen primärer Primideale. Bedeuten $\mathfrak{d}_1,\ldots,\mathfrak{d}_t$ diejenigen unter diesen Primfaktoren von μ, die in μ zu einer ungeraden Potenz aufgehen, so finden wir, wenn bez. $\delta_1,\ldots,\delta_t$ Primärzahlen von $\mathfrak{d}_1,\ldots,\mathfrak{d}_t$ bezeichnen, bei Anwendung des Satzes 28 leicht die Gleichung

$$\mu^h=\delta_1\cdots\delta_t\alpha^2, \tag{1}$$

wo α eine geeignete ganze Zahl in k bedeutet. Wir betrachten den Körper $K(\sqrt{\mu})$; nach Satz 4 sind $\mathfrak{d}_1,\ldots,\mathfrak{d}_t$ die in der Relativdiskriminante von $K(\sqrt{\mu})$ aufgehenden Primideale. Da diese t Primideale sämtlich primär sein sollen und mithin für jede Einheit ξ stets

$$\left(\frac{\xi,\mu}{\mathfrak{d}_i}\right)=\left(\frac{\xi}{\mathfrak{d}_i}\right)=+1,\qquad (i=1,2,\ldots,t)$$

ausfällt, so ist $r=t$ die Anzahl der Charaktere, welche das Geschlecht einer Klasse in diesem Körper $K(\sqrt{\mu})$ bestimmen; es gibt daher nach Satz 26 in $K(\sqrt{\mu})$ höchstens 2^{t-1} Geschlechter.

Wir weisen nun nach, daß im Körper $K(\sqrt{\mu})$ wirklich 2^{t-1} Geschlechter vorhanden sind. Zu dem Zwecke bezeichnen wir mit $c_1,\ldots,c_t$ irgend t solche Einheiten ±1, deren Produkt gleich $+1$ ist, und bestimmen dann ein Primideal $\mathfrak{p}$ in k, welches den Bedingungen

$$\left(\frac{\varepsilon_1}{\mathfrak{p}}\right)=+1,\ldots,\left(\frac{\varepsilon_{m-\frac{s}{2}}}{\mathfrak{p}}\right)=+1, \tag{2}$$

$$\left(\frac{\delta_1}{\mathfrak{p}}\right)=c_1,\ldots,\left(\frac{\delta_t}{\mathfrak{p}}\right)=c_t \tag{3}$$

genügt, wobei $\varepsilon_1,\ldots,\varepsilon_{m-\frac{s}{2}}$ das zu Beginn von § 21 aufgestellte System von Einheiten in k bedeuten soll; nach Satz 18 gibt es sicher Primideale $\mathfrak{p}$ von der verlangten Beschaffenheit. Wegen (2) ist $\mathfrak{p}$ ein primäres Primideal; es sei π eine Primärzahl von $\mathfrak{p}$. Nach Satz 35 folgen aus den Gleichungen (3) die Gleichungen

$$\left(\frac{\pi}{\mathfrak{d}_1}\right)=c_1,\ldots,\left(\frac{\pi}{\mathfrak{d}_t}\right)=c_t. \tag{4}$$

Wenn wir die Gleichungen (3) miteinander multiplizieren, erhalten wir wegen (1) und wegen $c_1\ldots c_t=+1$ die Gleichung

$$\left(\frac{\delta_1\cdots\delta_t}{\mathfrak{p}}\right)=\left(\frac{\mu}{\mathfrak{p}}\right)=+1,$$

d. h. $\mathfrak{p}$ zerfällt im Körper $K(\sqrt{\mu})$ in zwei Primfaktoren. Die Charaktere eines jeden dieser Primfaktoren stimmen wegen (4) mit $c_1,\ldots,c_t$ überein. Die Anzahl der möglichen Systeme von Einheiten $c_1,\ldots,c_t$ mit der Bedingung $c_1\ldots c_t=+1$ ist offenbar 2^{t-1}; es existieren daher wirklich so viele Geschlechter, und da es nach dem vorhin Bewiesenen eine größere Anzahl von Geschlechtern nicht geben kann, so erkennen wir hieraus die Tatsache, daß das Charakterensystem $c_1,\ldots,c_t$ eines jeden Geschlechts im Körper $K(\sqrt{\mu})$ notwendig die Bedingung $c_1\ldots c_t=+1$ erfüllen muß.

Um aus dieser Tatsache unter den an erster Stelle gemachten Annahmen den Satz 36 abzuleiten, nehmen wir zunächst an, es sei $\left(\frac{\mu}{\mathfrak{q}}\right)=+1$. Dann zerfällt $\mathfrak{q}$ in $K(\sqrt{\mu})$ in zwei Primfactoren; das Charakterensystem eines jeden dieser Primfaktoren ist

$$\left(\frac{\varkappa,\mu}{\mathfrak{d}_1}\right)=\left(\frac{\varkappa}{\mathfrak{d}_1}\right),\ldots,\left(\frac{\varkappa,\mu}{\mathfrak{d}_t}\right)=\left(\frac{\varkappa}{\mathfrak{d}_t}\right).$$

Da das Produkt dieser Charaktere nach dem vorhin Bewiesenen gleich $+1$ sein soll, so folgt wegen

$$\left(\frac{\varkappa,\mu}{\mathfrak{q}}\right)=\left(\frac{\mu}{\mathfrak{q}}\right)=+1$$

notwendig die Gleichung

$$\prod_{(\mathfrak{w})}'\left(\frac{\varkappa,\mu}{\mathfrak{w}}\right)=+1,$$

wenn das Produkt über alle zu 2 primen Primideale $\mathfrak{w}$ des Körpers k erstreckt wird; diese Gleichung zeigt unmittelbar die Richtigkeit der Behauptung.

Ist dagegen $\left(\frac{\mu}{\mathfrak{q}}\right)=-1$, so bestimme man ein von den Primidealen $\mathfrak{d}_1,\ldots,\mathfrak{d}_t$ verschiedenes primäres Primideal $\mathfrak{p}$ von der Art, daß $\left(\frac{\varkappa}{\mathfrak{p}}\right)=-1$ ausfällt; nach Satz 18 ist dies stets möglich. Bezeichnet π eine Primärzahl von $\mathfrak{p}$, so muß notwendig auch $\left(\frac{\pi}{\mathfrak{q}}\right)=-1$ ausfallen, weil im entgegengesetzten Falle aus Satz 34 $\left(\frac{\varkappa}{\mathfrak{p}}\right)=+1$ folgen würde. Nunmehr ist $\left(\frac{\mu\pi}{\mathfrak{q}}\right)=+1$, und wenn wir daher in der voranstehenden Betrachtung an Stelle von μ jetzt $\mu\pi$

nehmen, so geht aus derselben die Gleichung

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varkappa, \mu\pi}{\mathfrak{w}}\right) = +1$$

hervor. Es ist aber

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varkappa, \pi}{\mathfrak{w}}\right) = \left(\frac{\varkappa}{\mathfrak{p}}\right)\left(\frac{\pi}{\mathfrak{q}}\right) = +1$$

und folglich

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varkappa, \mu}{\mathfrak{w}}\right) = +1; \tag{5}$$

damit ist die Behauptung des Satzes 36 unter den an erster Stelle gemachten Annahmen als richtig erkannt.

Wenden wir die Formel (5) insbesondere auf den Fall an, daß μ eine Primärzahl π eines primären Primideals $\mathfrak{p}$ ist, so erhalten wir die Gleichung

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varkappa, \pi}{\mathfrak{w}}\right) = \left(\frac{\varkappa}{\mathfrak{p}}\right)\left(\frac{\pi}{\mathfrak{q}}\right) = +1; \tag{6}$$

es ist folglich stets

$$\left(\frac{\varkappa}{\mathfrak{p}}\right) = \left(\frac{\pi}{\mathfrak{q}}\right). \tag{7}$$

Wir behandeln *zweitens* den Fall, daß ν eine Primärzahl π eines primären Primideals $\mathfrak{p}$ sei, während die Zahl μ beliebige primäre oder nichtprimäre Primideale enthalten möge. Setzen wir $(\mu) = \mathfrak{r}_1\mathfrak{r}_2\ldots$, wo $\mathfrak{r}_1, \mathfrak{r}_2, \ldots$ Primideale sind, und bezeichnen $\varrho_1, \varrho_2, \ldots$ ganze Zahlen in k, so daß

$$(\varrho_1) = \mathfrak{r}_1^{\mathfrak{h}}, \qquad (\varrho_2) = \mathfrak{r}_2^{\mathfrak{h}}, \ldots$$

ausfällt, so wird

$$\mu^{\mathfrak{h}} = \eta\,\varrho_1\varrho_2\ldots,$$

wobei η eine Einheit in k sein muß. Bei Anwendung der dritten Formel des Satzes 14 erhalten wir

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \mu}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \mu^{\mathfrak{h}}}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \eta}{\mathfrak{w}}\right)\prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \varrho_1}{\mathfrak{w}}\right)\prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \varrho_2}{\mathfrak{w}}\right)\cdots. \tag{8}$$

Andererseits ist mit Rücksicht auf Satz 13

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \eta}{\mathfrak{w}}\right) = \left(\frac{\eta}{\mathfrak{p}}\right) = +1. \tag{9}$$

Ferner gelten die Gleichungen

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \varrho_i}{\mathfrak{w}}\right) = \left(\frac{\varrho_i}{\mathfrak{p}}\right)\left(\frac{\pi}{\mathfrak{r}_i}\right) = +1, \quad (i = 1, 2, \ldots), \tag{10}$$

wie wir für ein primäres $\mathfrak{r}_i$ aus Satz 35 und für ein nichtprimäres $\mathfrak{r}_i$ aus Formel (6) schließen. Nunmehr führt die Gleichung (8) in Verbindung mit (9) und (10) zu der Gleichung

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \mu}{\mathfrak{w}}\right) = +1, \tag{11}$$

und diese lehrt die Richtigkeit des Satzes 36 für den an zweiter Stelle behandelten Fall.

Wir nehmen *drittens* an, es sei ν gleich einer Einheit ε in k, während μ beliebige primäre oder nichtprimäre Primideale enthalten möge. Wir betrachten den Relativkörper $K(\sqrt{\mu})$. Bedeuten, wie in unserem ersten Falle, $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ diejenigen unter den Primfaktoren von μ, die in μ zu einer ungeraden Potenz aufgehen, und sind $\delta_1, \ldots, \delta_t$ solche ganze Zahlen in k, daß

$$(\delta_1) = \mathfrak{d}_1^{\mathfrak{h}}, \ldots, (\delta_t) = \mathfrak{d}_t^{\mathfrak{h}}$$

wird, so finden wir eine Gleichung von der Gestalt

$$\mu^{\mathfrak{h}} = \eta\,\delta_1\cdots\delta_t\,\alpha^2, \tag{12}$$

wo η eine Einheit in k und α eine ganze Zahl in k bezeichnet. Nach Satz 4 sind $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ die in der Relativdiskriminante des Körpers $K(\sqrt{\mu})$ aufgehenden Primideale. Wir bezeichnen mit r die Anzahl der Charaktere, die das Geschlecht einer Klasse in $K(\sqrt{\mu})$ bestimmen, und es seien unter den Primidealen $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ die Primideale $\mathfrak{d}_t, \mathfrak{d}_{t-1}, \ldots, \mathfrak{d}_{r+1}$ nach der in Definition 11 gemachten Vorschrift ausgewählt. Dann beweisen wir folgende Tatsache: wenn $c_1, \ldots, c_r$ irgend r Einheiten ± 1 sind, deren Produkt $c_1 \ldots c_r = +1$ ausfällt, so gibt es im Körper $K(\sqrt{\mu})$ stets Ideale, deren Charaktere mit $c_1, \ldots, c_r$ übereinstimmen. In der Tat nach Satz 18 gibt es in k sicher ein Primideal $\mathfrak{p}$, welches den Gleichungen

$$\left(\frac{\varepsilon_1}{\mathfrak{p}}\right) = +1, \ldots, \left(\frac{\varepsilon_{\frac{m}{2}}}{\mathfrak{p}}\right) = +1, \tag{13}$$

$$\left.\begin{aligned}\left(\frac{\delta_1}{\mathfrak{p}}\right) &= c_1, \ldots, \left(\frac{\delta_r}{\mathfrak{p}}\right) = c_r,\\ \left(\frac{\delta_{r+1}}{\mathfrak{p}}\right) &= +1, \ldots, \left(\frac{\delta_t}{\mathfrak{p}}\right) = +1\end{aligned}\right\} \tag{14}$$

genügt. Wegen (13) ist $\mathfrak{p}$ ein primäres Primideal; es sei π eine Primärzahl von $\mathfrak{p}$. Vermöge des Satzes 35 bez. der Relation (7) folgen aus (14) die Gleichungen

$$\left(\frac{\pi}{\mathfrak{d}_1}\right) = c_1, \ldots, \left(\frac{\pi}{\mathfrak{d}_r}\right) = c_r, \qquad \left(\frac{\pi}{\mathfrak{d}_{r+1}}\right) = 1, \ldots, \left(\frac{\pi}{\mathfrak{d}_t}\right) = +1. \tag{15}$$

Da $c_1 \ldots c_r = +1$ sein soll, so erhalten wir aus (14)

$$\left(\frac{\delta_1 \cdots \delta_t}{\mathfrak{p}}\right) = +1$$

und folglich ist wegen (12)

$$\left(\frac{\mu^{\mathfrak{h}}}{\mathfrak{p}}\right) = \left(\frac{\mu}{\mathfrak{p}}\right) = +1,$$

d. h. $\mathfrak{p}$ zerfällt in $K(\sqrt{\mu})$ in zwei Primfaktoren. Die Charaktere eines jeden dieser Primfaktoren stimmen wegen (15) mit $c_1, \ldots, c_r$ überein.

Da die Anzahl der Systeme von je r Einheiten $c_1, \ldots, c_r$ mit der Bedingung $c_1 \ldots c_r = +1$ gleich 2^{r-1} ist und andererseits nach Satz 26 im Körper $K(\sqrt{\mu})$ nicht mehr als 2^{r-1} Geschlechter existieren können, so schließen wir, wie in unserem ersten Falle, daß das Charakterensystem $c_1, \ldots, c_r$ eines jeden in $K(\sqrt{\mu})$ vorhandenen Geschlechtes notwendig die Bedingung $c_1 \ldots c_r = +1$ erfüllen muß.

Um aus dieser Tatsache im gegenwärtigen dritten Falle den Satz 36 zu beweisen, sei $\mathfrak{p}$ ein Primideal, welches den Bedingungen

$$\left(\frac{\mu}{\mathfrak{p}}\right) = +1, \tag{16}$$

$$\left(\frac{\varepsilon_1}{\mathfrak{p}}\right) = +1, \left(\frac{\varepsilon_2}{\mathfrak{p}}\right) = +1, \ldots, \left(\frac{\varepsilon_m}{\mathfrak{p}}\right) = +1, \tag{17}$$

$$\left(\frac{\delta_{r+1}}{\mathfrak{p}}\right) = \left(\frac{\varepsilon}{\mathfrak{d}_{r+1}}\right), \left(\frac{\delta_{r+2}}{\mathfrak{p}}\right) = \left(\frac{\varepsilon}{\mathfrak{d}_{r+2}}\right), \ldots, \left(\frac{\delta_t}{\mathfrak{p}}\right) = \left(\frac{\varepsilon}{\mathfrak{d}_t}\right) \tag{18}$$

genügt. Wegen der Gleichung (16) zerfällt $\mathfrak{p}$ im Körper $K(\sqrt{\mu})$ in zwei Primfaktoren und wegen der Gleichungen (17) ist $\mathfrak{p}$ ein primäres Primideal; es sei π eine Primärzahl von $\mathfrak{p}$. Wegen (18) erhalten wir unter Benutzung des Satzes 35 bez. der Relation (7) die Gleichungen

$$\left(\frac{\varepsilon\pi, \mu}{\mathfrak{d}_i}\right) = \left(\frac{\varepsilon\pi}{\mathfrak{d}_i}\right) = \left(\frac{\varepsilon}{\mathfrak{d}_i}\right)\left(\frac{\pi}{\mathfrak{d}_i}\right) = +1 \qquad (i = r+1, r+2, \ldots, t), \tag{19}$$

und daher haben die r Charaktere eines Primfaktors von $\mathfrak{p}$ folgende Werte

$$\left(\frac{\varepsilon\pi, \mu}{\mathfrak{d}_1}\right), \left(\frac{\varepsilon\pi, \mu}{\mathfrak{d}_2}\right), \ldots, \left(\frac{\varepsilon\pi, \mu}{\mathfrak{d}_r}\right).$$

Nun muß nach dem vorhin Bewiesenen das Produkt dieser Charaktere gleich $+1$ sein; dies liefert mit Rücksicht auf (16) und (19) die Beziehung

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varepsilon\pi, \mu}{\mathfrak{w}}\right) = +1,$$

und da wegen der an zweiter Stelle bewiesenen Tatsache

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \mu}{\mathfrak{w}}\right) = +1$$

sein muß, so folgt auch die Gleichung

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varepsilon, \mu}{\mathfrak{w}}\right) = +1, \tag{20}$$

womit der Satz 36 unter den an dritter Stelle gemachten Annahmen als richtig erkannt ist. Das Produkt $\prod'_{(\mathfrak{w})}$ ist hier wie auch im folgenden stets über alle zu 2 primen Primideale $\mathfrak{w}$ des Körpers k zu erstrecken.

Wir machen *viertens* die Annahme, daß ν die h-te Potenz eines nichtprimären Primideals $\mathfrak{q}$ sei, und setzen $(\varkappa) = \mathfrak{q}^h$, wo $\varkappa$ eine ganze Zahl in k bedeutet; die Zahl μ enthalte jedoch beliebig viele primäre oder nicht primäre Primideale

als Faktoren. Wir betrachten den Körper $K(\sqrt{\mu})$, wenden für ihn die Bezeichnungen wie im vorigen Falle an und entnehmen aus der Behandlung dieses dritten Falles die Tatsache, daß das Produkt der r Charaktere eines Geschlechtes in $K(\sqrt{\mu})$ gleich $+1$ sein muß. Es sei zunächst $\left(\frac{\mu}{\mathfrak{q}}\right) = +1$; dann zerfällt $\mathfrak{q}$ im Körper $K(\sqrt{\mu})$ in zwei Primfaktoren. Die r Charaktere eines jeden dieser Primfaktoren von $\mathfrak{q}$ sind, wenn ξ eine geeignete Einheit in k bedeutet, und im übrigen die Bezeichnungsweise, die im dritten Falle benutzt wurde, beibehalten wird:

$$\left(\frac{\xi\varkappa, \mu}{\mathfrak{d}_1}\right), \left(\frac{\xi\varkappa, \mu}{\mathfrak{d}_2}\right), \ldots, \left(\frac{\xi\varkappa, \mu}{\mathfrak{d}_r}\right), \tag{21}$$

während überdies die Gleichungen

$$\left(\frac{\xi\varkappa, \mu}{\mathfrak{d}_{r+1}}\right) = +1, \left(\frac{\xi\varkappa, \mu}{\mathfrak{d}_{r+2}}\right) = +1, \ldots, \left(\frac{\xi\varkappa, \mu}{\mathfrak{d}_t}\right) = +1 \tag{22}$$

gelten. Durch Multiplikation dieser Gleichungen (21), (22) folgt leicht

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\xi\varkappa, \mu}{\mathfrak{w}}\right) = \left(\frac{\mu}{\mathfrak{q}}\right) = +1$$

und vermöge der im dritten Falle bewiesenen Relation (20) schließen wir hieraus

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varkappa, \mu}{\mathfrak{w}}\right) = +1. \tag{23}$$

Fällt andererseits $\left(\frac{\mu}{\mathfrak{q}}\right) = -1$ aus, so bestimmen wir ein primäres Primideal $\mathfrak{p}$ von der Art, daß $\left(\frac{\varkappa}{\mathfrak{p}}\right) = -1$ ausfällt. Bezeichnet π eine Primärzahl von $\mathfrak{p}$, so erhalten wir wegen (7) $\left(\frac{\pi}{\mathfrak{q}}\right) = -1$, und folglich wird $\left(\frac{\pi\mu}{\mathfrak{q}}\right) = +1$. Nach der eben bewiesenen Formel (23) folgt mithin, wenn wir jetzt $\pi\mu$ an Stelle von μ nehmen,

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varkappa, \pi\mu}{\mathfrak{w}}\right) = +1$$

und hieraus wiederum mit Hinzuziehung von (11)

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varkappa, \mu}{\mathfrak{w}}\right) = +1; \tag{24}$$

damit ist der Satz 36 auch unter der vierten Annahme bewiesen.

Wir beweisen endlich den Satz 36 allgemein. Zu dem Zwecke setzen wir

$$\mathfrak{p}^h = \varepsilon\varrho_1\varrho_2 \ldots,$$

wo ε eine Einheit in k und $\varrho_1, \varrho_2, \ldots$, sei es Primärzahlen von primären Primidealen, sei es solche ganze Zahlen in k bedeuten, die h-te Potenzen von nichtprimären Primidealen darstellen. Dann entnehmen wir aus (20), (11), (24) die

zu beweisende Gleichung

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu,\mu}{\mathfrak{w}}\right)=\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^h,\mu}{\mathfrak{w}}\right)=+1.$$

Der Satz 36 enthält bereits wesentliche Bestandteile des quadratischen Reziprozitätsgesetzes zwischen den zu 2 primen Zahlen im Körper k. Wir fassen einige wichtige Folgerungen des Satzes 36 in nachstehendem Satze zusammen:

Satz 37. Bedeuten ν, μ, ν^*, μ^* irgendwelche ganze Zahlen in k, die zu 2 prim sind und nach dem Modul 2^2 den Kongruenzen

$$\nu\equiv\nu^*,\quad \mu\equiv\mu^*, \qquad (2^2)$$

genügen, und fällt überdies ν zu μ und ν^* zu μ^* prim aus, so gilt stets die Formel

$$\left(\frac{\nu}{\mu}\right)\left(\frac{\mu}{\nu}\right)=\left(\frac{\nu^*}{\mu^*}\right)\left(\frac{\mu^*}{\nu^*}\right).$$

Bedeuten ν, μ irgendwelche zueinander und zu 2 prime ganze Zahlen in k, von denen wenigstens eine dem Quadrat einer ganzen Zahl in k nach 2^2 kongruent ausfällt, so gilt stets die Formel

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

Beweis. Unter den zuerst gemachten Annahmen haben wir nach Satz 36

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu\,\nu^*,\mu}{\mathfrak{w}}\right)=\prod_{(\mathfrak{w})}{}'\left(\frac{\nu,\mu}{\mathfrak{w}}\right)\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*,\mu}{\mathfrak{w}}\right)=+1,$$

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*,\mu\,\mu^*}{\mathfrak{w}}\right)=\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*,\mu}{\mathfrak{w}}\right)\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*,\mu^*}{\mathfrak{w}}\right)=+1$$

und mithin

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu,\mu}{\mathfrak{w}}\right)=\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*,\mu^*}{\mathfrak{w}}\right);$$

hieraus entnehmen wir leicht die erste Aussage des Satzes 37. Die zweite Aussage folgt unmittelbar durch Anwendung des Satzes 36.

Die Formeln des Satzes 37 können auf die mannigfaltigste Weise durch numerische Beispiele bestätigt werden.

§ 26. Das primäre Ideal und seine Eigenschaften.

Wir erweitern die Definition 13 in folgender Weise:

Definition 16. Ein solches zu 2 primes Ideal $\mathfrak{a}$ des Körpers k, in bezug auf das für jede Einheit ξ in k

$$\left(\frac{\xi}{\mathfrak{a}}\right)=+1$$

ausfällt, heiße ein *primäres Ideal*; dagegen mögen diejenigen Ideale *nicht-*

primär genannt werden, in bezug auf die jene Gleichung nicht für jede Einheit ξ erfüllt ist.

Auf Grund des Satzes 36 gelingt es nun, den Satz 32 in folgender Weise zu verallgemeinern:

Satz 38. Es sei $\mathfrak{a}$ ein beliebiges primäres Ideal in k: dann ist es stets möglich, in k eine ganze Zahl α zu finden, so daß das Ideal (α) gleich $\mathfrak{a}^h$ wird, und überdies die Zahl α nach dem Modul 2^2 dem Quadrat einer ganzen Zahl des Körpers k kongruent ausfällt.

Beweis. Es sei α^* irgendeine ganze Zahl in k, so daß $(\alpha^*)=\mathfrak{a}^h$ wird. Bezeichnen ferner $\mathfrak{q}_1,\ldots,\mathfrak{q}_{\frac{m}{2}}, \varkappa_1,\ldots,\varkappa_{\frac{m}{2}}$ die $\frac{m}{2}$ Ideale bez. ganze Zahlen, wie in Satz 29, so ist nach dem dort Bewiesenen jede ganze zu 2 prime Zahl nach dem Modul 2^2 in einer gewissen Gestalt (vgl. S. 414) darstellbar; wir dürfen danach insbesondere

$$\alpha^*=\varepsilon^*\varkappa_1^{v_1}\cdots\varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}}\beta^2, \qquad (2^2) \qquad (1)$$

setzen, wo ε^* eine geeignete Einheit in k, ferner $v_1,\ldots,v_{\frac{m}{2}}$ gewisse Exponenten 0, 1 und β eine geeignete ganze Zahl in k bedeutet. Da wegen (1) die Zahl

$$\alpha^*\varepsilon^*\varkappa_1^{v_1}\cdots\varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}}$$

kongruent dem Quadrat einer ganzen Zahl in k nach dem Modul 2^2 ausfällt, so ist nach dem Satze 36 für jede Einheit ξ in k

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\xi,\alpha^*\varepsilon^*\varkappa_1^{v_1}\cdots\varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}}}{\mathfrak{w}}\right)=+1$$

und folglich

$$\left(\frac{\xi}{\alpha^*\varkappa_1^{v_1}\cdots\varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}}}\right)=\left(\frac{\xi}{\mathfrak{a}}\right)\left(\frac{\xi}{\mathfrak{q}_1}\right)^{v_1}\cdots\left(\frac{\xi}{\mathfrak{q}_{\frac{m}{2}}}\right)^{v_{\frac{m}{2}}}=+1;$$

da nach Voraussetzung $\left(\frac{\xi}{\mathfrak{a}}\right)=+1$ sein soll, so entnehmen wir hieraus, daß für jede Einheit ξ in k die Gleichung

$$\left(\frac{\xi}{\mathfrak{q}_1}\right)^{v_1}\cdots\left(\frac{\xi}{\mathfrak{q}_{\frac{m}{2}}}\right)^{v_{\frac{m}{2}}}=+1$$

bestehen muß. Indem wir hierin der Reihe nach für ξ die in § 21 aufgestellten Einheiten $\varepsilon_1,\ldots,\varepsilon_{\frac{m}{2}}$ einsetzen, schließen wir aus den Formeln S. 413, daß die Exponenten $v_1,\ldots,v_{\frac{m}{2}}$ sämtlich gleich 0 sind, und daher ist wegen (1) $\alpha=\alpha^*\varepsilon^*$ eine ganze Zahl in k von der im Satze 38 verlangten Beschaffenheit.

Die Umkehrung des Satzes 38 stellt eine Verallgemeinerung des Satzes 33 dar und lautet wie folgt:

Satz 39. Wenn $\mathfrak{a}$ ein zu 2 primes Ideal in k und α eine ganze Zahl in k von der Beschaffenheit ist, daß das Ideal (α) gleich $\mathfrak{a}^h$ wird und überdies die Zahl α nach dem Modul 2^2 dem Quadrat einer ganzen Zahl des Körpers k kongruent ausfällt, so ist $\mathfrak{a}$ ein primäres Ideal in k.

Den Beweis dieses Satzes gewinnen wir aus Satz 36, wenn wir in der Gleichung dieses Satzes 36 für ν eine beliebige Einheit ξ in k und für μ die Zahl α nehmen.

§ 27. Beispiele für die Sätze 32, 33, 38, 39.

Die Sätze 32, 33 entsprechen dem bekannten Satze aus der Theorie der rationalen Zahlen, demzufolge -1 quadratischer Rest oder Nichtrest nach einer rationalen positiven Primzahl ist, je nachdem diese von der Form $4n+1$ oder $4n+3$ ausfällt. Zur Erläuterung und Bestätigung der genannten Sätze 32, 33 wie der allgemeineren Sätze 38, 39 mögen folgende Beispiele dienen:

Beispiel 1. Der quadratische Körper $k(\sqrt{-7})$ hat die Klassenanzahl $h=1$; er besitzt zwei Einheitenverbände, nämlich diejenigen, die durch die Einheiten $+1$ und -1 bestimmt sind. Die Zahlen

$$3, \quad \sqrt{-7}, \quad 2+\sqrt{-7}, \quad 4+\sqrt{-7}, \quad 1+2\sqrt{-7}$$

sind Primzahlen mit den Normen bez.

$$3^2, \quad 7, \quad 11, \quad 23, \quad 29.$$

Nun gelten die Kongruenzen:

$$-1 \equiv (\sqrt{-7})^2, \quad (3) \quad \text{und} \quad -1 \equiv 12^2, \quad (1+2\sqrt{-7});$$

also haben wir im Körper $k(\sqrt{-7})$

$$\left(\frac{-1}{3}\right) = +1 \quad \text{und} \quad \left(\frac{-1}{1+2\sqrt{-7}}\right) = +1,$$

d. h. die Primideale (3) und $(1+2\sqrt{-7})$ sind primär. Dagegen finden wir mittels Satz 1

$$\left(\frac{-1}{\sqrt{-7}}\right) = (-1)^{\frac{7-1}{2}} = -1, \quad \left(\frac{-1}{2+\sqrt{-7}}\right) = (-1)^{\frac{11-1}{2}} = -1,$$

$$\left(\frac{-1}{4+\sqrt{-7}}\right) = (-1)^{\frac{23-1}{2}} = -1;$$

d. h. die Primideale $(\sqrt{-7})$, $(2+\sqrt{-7})$, $(4+\sqrt{-7})$ sind nichtprimär. In Übereinstimmung mit dem Satze 32 haben wir in der Tat

$$-3 \equiv 1^2, \quad (2^2) \quad \text{und} \quad -1-2\sqrt{-7} \equiv 1^2, \quad (2^2),$$

d. h. -3 und $-1-2\sqrt{-7}$ sind Primärzahlen der Primideale (3) bez. $(1+2\sqrt{-7})$. Dagegen ist von den sechs Zahlen

$$\pm\sqrt{-7}, \quad \pm(2+\sqrt{-7}), \quad \pm(4+\sqrt{-7})$$

keine dem Quadrat einer ganzen Zahl in $k(\sqrt{-7})$ nach dem Modul 2^2 kongruent, womit Satz 33 bestätigt wird.

Nach Definition 16 sind die Ideale

$$(\sqrt{-7})(2+\sqrt{-7}) = (-7+2\sqrt{-7}),$$
$$(\sqrt{-7})(4+\sqrt{-7}) = (-7+4\sqrt{-7})$$

primär; in der Tat gelten in Bestätigung des Satzes 38 nach dem Modul 2^2 die Kongruenzen

$$-(-7+2\sqrt{-7}) \equiv 1^2, \quad (2^2),$$
$$-7+4\sqrt{-7} \equiv 1^2, \quad (2^2).$$

Beispiel 2. Der biquadratische Körper $k(\sqrt{-1}, \sqrt{5})$ hat die Klassenanzahl $h=1$; wir setzen $i=\sqrt{-1}$ und $\vartheta=\frac{1+\sqrt{5}}{2}$, so daß $i^2+1=0$ und $\vartheta^2-\vartheta-1=0$ wird. Der Körper $k(i,\vartheta)$ besitzt 4 Einheitenverbände, nämlich diejenigen, die durch die Einheiten $1, i, \vartheta, i\vartheta$ bestimmt sind.

Die Zahlen

$$i+\vartheta, \quad 3+2i, \quad 2i+\vartheta, \quad 1-2\vartheta+i\vartheta, \quad 1+2i+2\vartheta, \quad 3i+\vartheta \qquad (1)$$

sind Primzahlen mit den Normen bez.

$$5, \quad 13^2, \quad 29, \quad 41, \quad 89, \quad 109.$$

Wir finden nun leicht mittels Satz 1 im Körper $k(i,\vartheta)$ die Gleichungen

$$\left(\frac{i}{i+\vartheta}\right) = i^{\frac{5-1}{2}} = -1, \qquad \left(\frac{\vartheta}{i+\vartheta}\right) = \left(\frac{-i}{i+\vartheta}\right) = -1,$$

$$\left(\frac{i}{3+2i}\right) = +1, \qquad \left(\frac{\vartheta}{3+2i}\right) = +1,$$

$$\left(\frac{i}{2i+\vartheta}\right) = -1, \qquad \left(\frac{\vartheta}{2i+\vartheta}\right) = +1,$$

$$\left(\frac{i}{1-2\vartheta+i\vartheta}\right) = +1, \qquad \left(\frac{\vartheta}{1-2\vartheta+i\vartheta}\right) = -1,$$

$$\left(\frac{i}{1+2i+2\vartheta}\right) = +1, \qquad \left(\frac{\vartheta}{1+2i+2\vartheta}\right) = +1,$$

$$\left(\frac{i}{3i+\vartheta}\right) = -1, \qquad \left(\frac{\vartheta}{3i+\vartheta}\right) = -1.$$

Dem Satze 33 zufolge darf daher keine der vier Primzahlen $i+\vartheta$, $2i+\vartheta$, $1-2\vartheta+i\vartheta$, $3i+\vartheta$ nach dem Modul 2^2 einem Ausdrucke von der Gestalt $i^u\vartheta^v\alpha^2$ kongruent sein, wo u, v gewisse Werte 0, 1 haben dürfen und α irgendeine ganze Zahl in $k(i,\vartheta)$ bedeutet; dagegen muß nach Satz 32 jede

der beiden übrigen Zahlen aus der Reihe (1) einer solchen Kongruenz genügen. In der Tat ist

$$3+2i\equiv\vartheta(1-i-\vartheta)^2,\ (2^2)\ \text{und}\ 1+2i+2\vartheta\equiv(1+\vartheta+i\vartheta)^2,\ (2^2).$$

Aus der obigen Tabelle erkennen wir ferner, daß die Ideale

$$(i+\vartheta)(3i+\vartheta) = (-2+\vartheta+4i\vartheta),$$
$$(i+\vartheta)(2i+\vartheta)(1-2\vartheta+i\vartheta) = (-6-5i-2\vartheta-3i\vartheta)$$

primär sind; in der Tat gelten in Bestätigung der Sätze 38 und 39 die Kongruenzen:

$$-2+\vartheta+4i\vartheta\equiv-(1-\vartheta)^2,\qquad(2^2),$$
$$-6-5i-2\vartheta-3i\vartheta\equiv-i(1+i-\vartheta)^2,\qquad(2^2).$$

Beispiel 3. Der biquadratische Körper $k\left(\sqrt{1+4\sqrt{-1}}\right)$ hat die Klassenanzahl $h=1$; wir setzen $i=\sqrt{-1}$ und $\vartheta=\frac{1+\sqrt{1+4i}}{2}$, so daß $\vartheta^2-\vartheta-i=0$ wird. Der Körper $k(\sqrt{\vartheta})$ besitzt 4 Einheitenverbände, nämlich diejenigen, die durch die Einheiten $1, i, \vartheta, i\vartheta$ bestimmt sind.

Durch Zerlegung der Zahl 5 erhalten wir in $k(\sqrt{\vartheta})$ die drei Primzahlen

$$2+i,\quad 1+\vartheta,\quad 2-\vartheta; \tag{2}$$

das Produkt der beiden letzteren ist gleich $2-i$, und das Produkt aller drei Primzahlen ist gleich 5. Wir finden leicht in diesem Körper $k(\vartheta)$:

$$\left(\frac{i}{2+i}\right)=i^{\frac{5^2-1}{2}}=+1,\quad \left(\frac{i}{1+\vartheta}\right)=i^{\frac{5-1}{2}}=-1,\quad \left(\frac{i}{2-\vartheta}\right)=-1, \tag{3}$$

und

$$\left(\frac{\vartheta}{2+i}\right)=-1,\qquad \left(\frac{\vartheta}{1+\vartheta}\right)=+1,\qquad \left(\frac{\vartheta}{2-\vartheta}\right)=-1, \tag{4}$$

und in der Tat ist keine der drei Primzahlen (2) nach dem Modul 2^2 einem Ausdruck von der Gestalt $i^u\vartheta^v\alpha^2$ kongruent, wo u, v gewisse Werte 0, 1 haben und α irgendeine ganze Zahl in $k(\vartheta)$ bedeutet. Dagegen ist $5\equiv1^2$ nach 2^2, und wegen (3), (4) haben wir

$$\left(\frac{i}{5}\right)=\left(\frac{i}{2+i}\right)\left(\frac{i}{1+\vartheta}\right)\left(\frac{i}{2-\vartheta}\right)=+1,$$
$$\left(\frac{\vartheta}{5}\right)=\left(\frac{\vartheta}{2+i}\right)\left(\frac{\vartheta}{1+\vartheta}\right)\left(\frac{\vartheta}{2-\vartheta}\right)=+1,$$

d. h. das Ideal (5) ist in Übereinstimmung mit Satz 39 primär.

Die Zahl 37 ist in $k(\vartheta)$ gleich dem Produkt der drei Primzahlen

$$6+i,\qquad -3+\vartheta,\qquad 2+\vartheta.$$

Wir finden leicht

$$\left(\frac{i}{6+i}\right)=+1,\quad \left(\frac{i}{3-\vartheta}\right)=-1,\quad \left(\frac{i}{2+\vartheta}\right)=-1 \tag{5}$$

und

$$\left(\frac{\vartheta}{6+i}\right)=-1,\quad \left(\frac{\vartheta}{3-\vartheta}\right)=+1,\quad \left(\frac{\vartheta}{2+\vartheta}\right)=-1. \tag{6}$$

Die Primfaktoren von 37 sind ebenso wie diejenigen von 5 sämtlich nichtprimär; dagegen ist das Ideal (37) primär. Ferner sind wegen (3), (4), (5), (6) die Ideale

$$((2+i)(6+i)),\quad ((1+\vartheta)(3-\vartheta)),\quad ((2-\vartheta)(2+\vartheta))$$

primär; in der Tat gelten in Übereinstimmung mit Satz 38 die Kongruenzen

$$(2+i)(6+i)\equiv(2+i)^2,\qquad(2^2),$$
$$-(1+\vartheta)(3-\vartheta)\equiv(1-\vartheta)^2,\qquad(2^2),$$
$$-(2-\vartheta)(2+\vartheta)\equiv\vartheta^2,\qquad(2^2).$$

Die Zahlen 3 und 7 sind in $k(\vartheta)$ unzerlegbar, und da $-3\equiv1^2$ und $-7\equiv1^2$ nach dem Modul 2^2 ausfällt, so müssen nach Satz 33 (3) und (7) primäre Primideale mit den Primärzahlen -3 und -7 sein. In der Tat sind die Einheiten i, ϑ beide in $k(\vartheta)$ quadratische Reste nach den Moduln (3) und (7); denn wir haben

$$\left(\frac{i}{3}\right)=i^{\frac{3^4-1}{2}}=+1\quad\text{und}\quad\left(\frac{i}{7}\right)=i^{\frac{7^4-1}{2}}=+1$$

sowie ferner

$$\vartheta\equiv(1-\vartheta+i\vartheta)^2,\ (3)\quad\text{und}\quad\vartheta\equiv(1+3i-3\vartheta-i\vartheta)^2,\ (7).$$

Beispiel 4. Der biquadratische Körper $k(\sqrt[4]{-2})$ hat die Klassenanzahl $h=1$; wir setzen $\vartheta=\sqrt[4]{-2}$, so daß $\vartheta^4+2=0$ wird. Der Körper $k(\vartheta)$ besitzt 4 Einheitenverbände, nämlich diejenigen, die durch die Einheiten 1, $-1, \varepsilon, -\varepsilon$ bestimmt sind, wobei zur Abkürzung

$$\varepsilon=1-\vartheta^2+\vartheta^3$$

gesetzt ist.

Die Zahlen

$$\left.\begin{array}{lll} 1-\vartheta, & 1+\vartheta, & 1+\vartheta-2\vartheta^2+2\vartheta^3, \\ & 1+\vartheta+2\vartheta^2+\vartheta^3, & 1+2\vartheta-\vartheta^2 \end{array}\right\} \tag{7}$$

sind Primzahlen ersten Grades in $k(\vartheta)$ mit den Normen bez.

$$\begin{array}{lll} 3, & 3, & 19, \\ & 59, & 73; \end{array}$$

wir schließen hieraus mittels Satz 1

$$\left.\begin{array}{lll} \left(\frac{-1}{1-\vartheta}\right)=-1, & \left(\frac{-1}{1+\vartheta}\right)=-1, & \left(\frac{-1}{1+\vartheta-2\vartheta^2+2\vartheta^3}\right)=-1, \\ \left(\frac{-1}{1+\vartheta+2\vartheta^2+\vartheta^3}\right)=-1, & \left(\frac{-1}{1+2\vartheta-\vartheta^2}\right)=+1. & \end{array}\right\} \tag{8}$$

Die Zahl ϑ genügt nach den Primzahlen in (7) bez. den Kongruenzen

$$\begin{array}{llll} \vartheta\equiv1, & \vartheta\equiv-1, & \vartheta\equiv-5, & \\ & \vartheta\equiv6, & \vartheta\equiv-31 & \end{array}$$

und daher gelten für ε bez. nach jenen Primzahlen die Kongruenzen

$$\varepsilon \equiv 1, \quad \varepsilon \equiv -1, \quad \varepsilon \equiv 3,$$
$$\varepsilon \equiv 4, \quad \varepsilon \equiv -18.$$

Da nun im Bereiche der rationalen Zahlen 1 quadratischer Rest nach 3, -1 Nichtrest nach 3, 3 Nichtrest nach 19, 4 Rest nach 59 und -18 Rest nach 73 ist, so haben wir im Körper $k(\vartheta)$ die Gleichungen

$$\left.\begin{aligned} \left(\frac{\varepsilon}{1-\vartheta}\right) = +1, \quad \left(\frac{\varepsilon}{1+\vartheta}\right) = -1, \quad \left(\frac{\varepsilon}{1+\vartheta-2\vartheta^2+2\vartheta^3}\right) = -1, \\ \left(\frac{\varepsilon}{1+\vartheta+2\vartheta^2+\vartheta^3}\right) = +1, \quad \left(\frac{\varepsilon}{1+2\vartheta-\vartheta^2}\right) = +1. \end{aligned}\right\} \quad (9)$$

Wegen (8), (9) ist von den fünf Primzahlen in (7) nur die letzte primär, und in der Tat gilt in Bestätigung des Satzes 32 nach dem Modul 2^2 die Kongruenz

$$-(1+2\vartheta-\vartheta^2) \equiv (1+\vartheta+\vartheta^2+\vartheta^3)^2, \quad (2^2),$$

so daß $-1-2\vartheta+\vartheta^2$ eine Primärzahl des Primideals $(1+2\vartheta-\vartheta^2)$ wird.

Die Zahlen

$$1-2\vartheta+2\vartheta^2, \quad 1-4\vartheta^2+2\vartheta^3$$

sind Primzahlen zweiten Grades in $k(\vartheta)$ mit den Normen bez.

$$7^2, \quad 31^2.$$

Zunächst ergibt sich

$$\left(\frac{-1}{1-2\vartheta+2\vartheta^2}\right) = (-1)^{\frac{7^2-1}{2}} = +1.$$

Ferner finden wir mit Benutzung der Kongruenz

$$\vartheta^2 \equiv \vartheta + 3, \quad (1-2\vartheta+2\vartheta^2)$$

leicht, daß ε quadratischer Nichtrest nach $1-2\vartheta+2\vartheta^2$ ist, d. h. wir haben

$$\left(\frac{\varepsilon}{1-2\vartheta+2\vartheta^2}\right) = -1,$$

und die Primzahl $1-2\vartheta+2\vartheta^2$ ist mithin nichtprimär. Dagegen gilt die Kongruenz

$$-1+4\vartheta^2-2\vartheta^3 \equiv (1+\vartheta^2+\vartheta^3)^2, \quad (2^2).$$

Nach Satz 33 muß mithin $(1-4\vartheta^2+2\vartheta^3)$ ein primäres Primideal sein. In der Tat haben wir

$$\left(\frac{-1}{1-4\vartheta^2+2\vartheta^3}\right) = (-1)^{\frac{31^2-1}{2}} = +1$$

und überdies gilt die Kongruenz

$$\varepsilon \equiv (3-2\vartheta)^2, \quad (1-4\vartheta^2+2\vartheta^3).$$

Endlich sind wegen (8), (9) die Ideale

$$((1+\vartheta)(1+\vartheta-2\vartheta^2+2\vartheta^3)), \quad ((1-\vartheta)(1+\vartheta+2\vartheta^2+\vartheta^3))$$

primär und in Bestätigung des Satzes 38 finden wir in der Tat

$$-(1+\vartheta)(1+\vartheta-2\vartheta^2+2\vartheta^3) \equiv (1+\vartheta+\vartheta^2+\vartheta^3)^2, \quad (2^2),$$
$$-\varepsilon(1-\vartheta)(1+\vartheta+2\vartheta^2+\vartheta^3) \equiv \varepsilon^2, \quad (2^2).$$

Die Zahl 5 ist in $k(\vartheta)$ unzerlegbar und wegen $5 \equiv 1^2$ nach 2^2 ist mithin dem Satze 33 zufolge (5) ein primäres Primideal; in der Tat ist ε quadratischer Rest nach 5 wegen der Kongruenz

$$\varepsilon \equiv (1+2\vartheta+\vartheta^2+\vartheta^3)^2, \quad (5).$$

Beispiel 5. Der durch die 5-ten Einheitswurzeln bestimmte Körper ist ein biquadratischer zyklischer Körper mit der Klassenanzahl $h=1$; es sei ϑ eine von 1 verschiedene 5-te Einheitswurzel, so daß

$$\vartheta^4+\vartheta^3+\vartheta^2+\vartheta+1=0$$

wird. Der Körper $k(\vartheta)$ besitzt 4 Einheitenverbände, nämlich diejenigen, welche durch die Einheiten $+1, -1, 1+\vartheta, -1-\vartheta$ bestimmt sind.

Die Zahlen

$$\left.\begin{aligned} 1+2\vartheta^2, \quad 2-\vartheta^2, \quad 3+2\vartheta+\vartheta^2, \\ 3+\vartheta, \quad 3+4\vartheta^2, \quad 1+5\vartheta^2 \end{aligned}\right\} \quad (10)$$

sind Primzahlen ersten Grades in $k(\vartheta)$ mit den Normen bez.

$$11, \quad 31, \quad 41,$$
$$61, \quad 181, \quad 521;$$

wir schließen hieraus mittels Satz 1 leicht

$$\left.\begin{aligned} \left(\frac{-1}{1+2\vartheta^2}\right) = -1, \quad \left(\frac{-1}{2-\vartheta^2}\right) = -1, \quad \left(\frac{-1}{3+2\vartheta+\vartheta^2}\right) = +1, \\ \left(\frac{-1}{3+\vartheta}\right) = +1, \quad \left(\frac{-1}{3+4\vartheta^2}\right) = +1, \quad \left(\frac{-1}{1+5\vartheta^2}\right) = +1. \end{aligned}\right\} \quad (11)$$

Die Einheit $1+\vartheta$ genügt nach den Primzahlen (10) bez. den Kongruenzen

$$1+\vartheta \equiv 5, \quad \equiv 9, \quad \equiv 11,$$
$$\equiv -2, \quad \equiv 43, \quad \equiv 26.$$

Da nun im Bereich der rationalen Zahlen 5 quadratischer Rest nach 11, 9 quadratischer Rest nach 31, 11 Nichtrest nach 41, -2 Nichtrest nach 61, 43 Rest nach 181, und 26 Rest nach 521 ist, so haben wir im Körper $k(\vartheta)$ die Gleichungen

$$\left.\begin{aligned} \left(\frac{1+\vartheta}{1+2\vartheta^2}\right) = +1, \quad \left(\frac{1+\vartheta}{2-\vartheta^2}\right) = +1, \quad \left(\frac{1+\vartheta}{3+2\vartheta+\vartheta^2}\right) = -1, \\ \left(\frac{1+\vartheta}{3+\vartheta}\right) = -1, \quad \left(\frac{1+\vartheta}{3+4\vartheta^2}\right) = +1, \quad \left(\frac{1+\vartheta}{1+5\vartheta^2}\right) = +1, \end{aligned}\right\} \quad (12)$$

Wegen (11), (12) sind von den sechs Primzahlen in (10) nur die zwei letzten primär, und in der Tat gelten in Bestätigung der Sätze 32 und 33 nach dem

Modul 2^2 die Kongruenzen

$$3 + 4\vartheta^2 \equiv -1, \qquad (2^2),$$
$$1 + 5\vartheta^2 \equiv -\frac{\vartheta^4}{1+\vartheta}, \qquad (2^2),$$

so daß

$$-3 - 4\vartheta^2 \quad \text{und} \quad -(1+\vartheta)(1+5\vartheta^2) = -1 - \vartheta - 5\vartheta^2 - 5\vartheta^3$$

Primärzahlen der betreffenden beiden Primideale werden.

Aus den Gleichungen (11), (12) entnehmen wir leicht die Gleichungen

$$\left(\frac{-1}{(1+2\vartheta^2)(2-\vartheta^2)}\right) = +1, \quad \left(\frac{-1}{(3+2\vartheta+\vartheta^2)(3+\vartheta)}\right) = +1,$$
$$\left(\frac{1+\vartheta}{(1+2\vartheta^2)(2-\vartheta^2)}\right) = +1, \quad \left(\frac{1+\vartheta}{(3+2\vartheta+\vartheta^2)(3+\vartheta)}\right) = +1.$$

Die Zahlen $(1+2\vartheta^2)(2-\vartheta^2)$ und $(3+2\vartheta+\vartheta^2)(3+\vartheta)$ müssen daher dem Satze 38 zufolge dem Produkte einer Einheit in das Quadrat einer ganzen Zahl des Körpers $k(\vartheta)$ nach dem Modul 2^2 kongruent ausfallen; in der Tat gelten die Kongruenzen:

$$(1+2\vartheta^2)(2-\vartheta^2) \equiv 2\vartheta + \vartheta^2 + 2\vartheta^3 \equiv (1+\vartheta)(1+\vartheta^4)^2, \quad (2^2),$$
$$(3+2\vartheta+\vartheta^2)(3+\vartheta) \equiv -\vartheta^4 \quad , \quad (2^2).$$

Beispiel 6. Der durch eine Wurzel ϑ der Gleichung

$$\vartheta^4 + \vartheta + 1 = 0$$

bestimmte Körper ist ein biquadratischer Körper ohne quadratischen Unterkörper; er hat die Klassenanzahl $h = 1$ und besitzt 4 Einheitenverbände, nämlich diejenigen, die durch die Einheiten $+1, -1, \vartheta, -\vartheta$ bestimmt sind.

Für die Zahlen 3, 5 gelten in $k(\vartheta)$ die Zerlegungen

$$3 = (1-\vartheta)(2+\vartheta+\vartheta^2+\vartheta^3),$$
$$5 = (1+\vartheta+\vartheta^2+\vartheta^3)(2-4\vartheta+2\vartheta^2-\vartheta^3),$$

worin beidemal der erste Faktor auf der rechten Seite eine Primzahl ersten Grades und der zweite Faktor eine Primzahl dritten Grades ist. Mit Hilfe des Satzes 1 erhalten wir darnach leicht

$$\left.\begin{aligned} &\left(\frac{-1}{1-\vartheta}\right) = -1, \quad \left(\frac{-1}{2+\vartheta+\vartheta^2+\vartheta^3}\right) = (-1)^{\frac{3^3-1}{2}} = -1, \\ &\left(\frac{-1}{1+\vartheta+\vartheta^2+\vartheta^3}\right) = +1, \quad \left(\frac{-1}{2-4\vartheta+2\vartheta^2-\vartheta^3}\right) = (-1)^{\frac{5^3-1}{2}} = +1. \end{aligned}\right\} \quad (13)$$

Andererseits findet man aus den Kongruenzen

$$\vartheta \equiv 1, \quad (1-\vartheta) \quad \text{und} \quad \vartheta \equiv -2, \quad (1+\vartheta+\vartheta^2+\vartheta^3)$$

die Gleichungen

$$\left(\frac{\vartheta}{1-\vartheta}\right) = +1, \quad \left(\frac{\vartheta}{1+\vartheta+\vartheta^2+\vartheta^3}\right) = -1. \qquad (14)$$

Wegen $-3 \equiv 1^2$ und $5 \equiv 1^2$ nach 2^2 sind (3), (5) nach Satz 39 primäre Ideale und mithin folgt

$$\left(\frac{\vartheta}{3}\right) = \left(\frac{\vartheta}{1-\vartheta}\right)\left(\frac{\vartheta}{2+\vartheta+\vartheta^2+\vartheta^3}\right) = +1,$$
$$\left(\frac{\vartheta}{5}\right) = \left(\frac{\vartheta}{1+\vartheta+\vartheta^2+\vartheta^3}\right)\left(\frac{\vartheta}{2-4\vartheta+2\vartheta^2-\vartheta^3}\right) = +1;$$

hieraus entnehmen wir mit Rücksicht auf (14), daß notwendig

$$\left(\frac{\vartheta}{2+\vartheta+\vartheta^2+\vartheta^3}\right) = +1 \quad \text{und} \quad \left(\frac{\vartheta}{2-4\vartheta+2\vartheta^2-\vartheta^3}\right) = -1 \qquad (15)$$

sein muß. In der Tat wird die erstere Gleichung durch die Kongruenz

$$\vartheta \equiv (\vartheta - \vartheta^2)^2, \qquad (2+\vartheta+\vartheta^2+\vartheta^3)$$

bestätigt. Um die letztere Gleichung zu bestätigen, berücksichtigen wir, daß wegen

$$\vartheta^3 \equiv 2(1-\vartheta)^2, \qquad (2-4\vartheta+2\vartheta^2-\vartheta^3)$$
$$\left(\frac{\vartheta}{2-4\vartheta+2\vartheta^2-\vartheta^3}\right) = \left(\frac{2}{2-4\vartheta+2\vartheta^2-\vartheta^3}\right)$$

und wegen

$$2^{\frac{5^3-1}{2}} \equiv -1, \qquad (5)$$

nach Satz 1

$$\left(\frac{2}{2-4\vartheta+2\vartheta^2-\vartheta^3}\right) = -1$$

ausfällt

Die Zahl 7 ist in $k(\vartheta)$ unzerlegbar und wegen $-7 \equiv 1^2$ nach 2^2 muß demnach ϑ nach 7 quadratischer Rest in $k(\vartheta)$ sein; in der Tat finden wir

$$\vartheta \equiv (\vartheta + \vartheta^2 + 3\vartheta^3)^2, \qquad (7).$$

Die Zahlen $2-\vartheta$, $2-\vartheta^2$ sind Primzahlen ersten Grades in $k(\vartheta)$ mit den Normen 19 bez. 23. Wir erhalten leicht

$$\left(\frac{-1}{2-\vartheta}\right) = -1, \quad \left(\frac{\vartheta}{2-\vartheta}\right) = -1$$
$$\left(\frac{-1}{2-\vartheta^2}\right) = -1, \quad \left(\frac{\vartheta}{2-\vartheta^2}\right) = +1.$$

Hieraus und aus (13), (14), (15) entnehmen wir die Gleichungen

$$\left(\frac{-1}{(1-\vartheta)(2-\vartheta)(2-4\vartheta+2\vartheta^2-\vartheta^3)}\right) = +1, \quad \left(\frac{-1}{(1-\vartheta)(2-\vartheta^2)}\right) = +1.$$

Dem Satze 38 zufolge muß daher jedes der beiden betreffenden Primzahlprodukte nach Multiplikation mit einer geeigneten Einheit dem Quadrat einer ganzen Zahl in $k(\vartheta)$ nach dem Modul 2^2 kongruent werden; in der Tat ist

$$-(1-\vartheta)(2-\vartheta)(2-4\vartheta+2\vartheta^2-\vartheta^3) \equiv (1-\vartheta)^2 \quad , \quad (2^2)$$
$$-\vartheta(1-\vartheta)(2-\vartheta^2) \equiv (\vartheta+\vartheta^2+\vartheta^3)^2, \quad (2^2).$$

Beispiel 7. Der durch die 7-ten Einheitswurzeln bestimmte Körper ist ein Abelscher Körper 6-ten Grades mit der Klassenanzahl $h = 1$; derselbe läßt sich aus einem quadratischen und einem kubischen Körper zusammensetzen. Verstehen wir unter ϑ eine von 1 verschiedene 7-te Einheitswurzel und setzen

$$\zeta = \vartheta + \vartheta^2 + \vartheta^4 \quad \text{und} \quad \eta = \vartheta + \vartheta^6,$$

so wird

$$\zeta^2 + \zeta + 2 = 0 \quad \text{und} \quad \eta^3 + \eta^2 - 2\eta - 1 = 0.$$

Der Körper $k(\vartheta)$ besitzt 8 Einheitenverbände, nämlich diejenigen, welche durch die Einheiten $+1$, -1, $+\eta$, $-\eta$, $2-\eta^2$, $-2+\eta^2$, $\eta(2-\eta^2)$, $-\eta(2-\eta^2)$ bestimmt sind.

Die Zahlen

$$1 - \vartheta + 2\vartheta^3, \qquad 1 + 3\vartheta + \vartheta^2 + \vartheta^3 \tag{16}$$

sind Primzahlen ersten Grades in $k(\vartheta)$ mit den Normen bez.

$$113, \qquad 197.$$

Da überdies nach jenen Primzahlen bez. die Kongruenzen

$$\left.\begin{aligned} \eta &\equiv 9, \\ 2-\eta^2 &\equiv 34, \end{aligned}\right\} \qquad \left.\begin{aligned} \eta &\equiv -39 \\ 2-\eta^2 &\equiv 57 \end{aligned}\right\}$$

gelten, so finden wir leicht

$$\left(\frac{-1}{1-\vartheta+2\vartheta^3}\right) = +1, \quad \left(\frac{\eta}{1-\vartheta+2\vartheta^3}\right) = +1, \quad \left(\frac{2-\eta^2}{1-\vartheta+2\vartheta^3}\right) = -1,$$

$$\left(\frac{-1}{1+3\vartheta+\vartheta^2+\vartheta^3}\right) = +1, \quad \left(\frac{\eta}{1+3\vartheta+\vartheta^2+\vartheta^3}\right) = +1, \quad \left(\frac{2-\eta^2}{1+3\vartheta+\vartheta^2+\vartheta^3}\right) = -1.$$

Nach Definition 16 ist also das Produkt der beiden Primzahlen in (16) ein primäres Ideal des Körpers $k(\vartheta)$, und in der Tat gilt in Bestätigung der Sätze 38 und 39 nach dem Modul (2^2) die Kongruenz

$$(1 - \vartheta + 2\vartheta^3)(1 + 3\vartheta + \vartheta^2 + \vartheta^3) \equiv (2 - \eta^2)\vartheta^2.$$

Die Zahl 37 gestattet die Zerlegung

$$37 = (1 - 4\zeta)(5 + 4\zeta),$$

wobei die beiden Faktoren rechter Hand Primzahlen dritten Grades in $k(\vartheta)$ sind. Da dieselben nach dem Modul 2^2 kongruent 1^2 ausfallen, so stellen sie nach Satz 33 primäre Primideale dar. In Übereinstimmung damit finden wir

$$\left(\frac{-1}{1-4\zeta}\right) = +1,$$

$$\eta \equiv (14 + 17\eta + 19\eta^2)^2, \qquad (37),$$

$$-2 + \eta^2 \equiv (19\eta + 2\eta^2)^2, \qquad (37).$$

Die Zahl 3 ist Primzahl in $k(\vartheta)$ und wegen $-3 \equiv 1^2$ nach 2^2 ist das Ideal (3) nach Satz 33 ein primäres Primideal. In der Tat haben wir

$$\left(\frac{-1}{3}\right) = (-1)^{\frac{3^6-1}{2}} = +1,$$

$$\eta \equiv (\eta - \eta^2)^2, \qquad (3),$$

$$-2 + \eta^2 \equiv (1 + \eta - \eta^2)^2, \qquad (3).$$

Die angeführten Beispiele lassen erkennen, welche reiche Mannigfaltigkeit an arithmetischen Wahrheiten insbesondere in den Sätzen 32, 33, 38, 39 enthalten ist — und doch bilden diese Sätze nur Bestandteile des *ersten* Ergänzungssatzes zu dem später von mir zu entwickelnden allgemeinen Reziprozitätsgesetze für quadratische Reste. Der vollständige erste Ergänzungssatz wird erst im Satz 53 (§ 36) zum Ausdruck kommen. Endlich erinnern wir daran, daß wir des leichteren Verständnisses wegen in dem zweiten Abschnitte der vorliegenden Abhandlung durchweg über den Grundkörper k die auf Seite 27 angegebenen besonderen Annahmen gemacht haben; wir müssen es uns daher auch an dieser Stelle versagen, mitzuteilen, wie der erste Ergänzungssatz lautet und wie tief derselbe das Wesen des Begriffes der Idealklasse berührt, falls der zugrunde gelegte Körper k eine *gerade* Klassenanzahl aufweist.

§ 28. Das Produkt $\prod_{(\mathfrak{w})}' \left(\frac{\nu, \mu}{\mathfrak{w}}\right)$ für ein beliebiges ν und bei gewissen Annahmen über μ.

Für die späteren Entwicklungen ist es erforderlich, den Satz 36 in folgender Weise zu erweitern:

Satz 40. Es seien $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ die sämtlichen von einander verschiedenen Primfaktoren der Zahl 2 und es gehe $\mathfrak{l}_1$ genau zur l_1-ten, $\mathfrak{l}_2$ genau zur l_2-ten, $\ldots$, $\mathfrak{l}_z$ genau zur l_z-ten Potenz in 2 auf, so daß

$$2 = \mathfrak{l}_1^{l_1}\mathfrak{l}_2^{l_2}\cdots\mathfrak{l}_z^{l_z}$$

wird; wenn dann ν eine beliebige ganze Zahl und μ eine solche ganze Zahl in k bedeutet, die zu 2 prim ist und dem Quadrat einer ganzen Zahl in k nach $\mathfrak{l}_1^{2l_1+1}\mathfrak{l}_2^{2l_2+1}\cdots\mathfrak{l}_z^{2l_z+1}$ kongruent ist, so fällt stets

$$\prod_{(\mathfrak{w})}' \left(\frac{\nu, \mu}{\mathfrak{w}}\right) = +1$$

aus, wo das Produkt über alle zu 2 primen Primideale $\mathfrak{w}$ des Körpers k erstreckt werden soll.

Beweis. Wir setzen

$$\nu = \pi\,\mathfrak{l}_1^{e_1}\cdots\mathfrak{l}_z^{e_z},$$

so daß $e_1, \ldots, e_z$ gewisse ganze rationale Exponenten und $\mathfrak{n}$ ein zu 2 primes Ideal bedeutet. Nach Satz 8 sind die Ideale $\mathfrak{l}_1, \ldots, \mathfrak{l}_z$ sämtlich im Körper $K(\sqrt{\mu})$ weiter zerlegbar; es seien $\mathfrak{L}_1, \ldots, \mathfrak{L}_z$ bez. je ein Primfaktor von $\mathfrak{l}_1, \ldots, \mathfrak{l}_z$ in $K(\sqrt{\mu})$; endlich sei A eine durch das Ideal $\mathfrak{L}_1^{e_1} \ldots \mathfrak{L}_z^{e_z}$ teilbare ganze Zahl des Körpers $K(\sqrt{\mu})$ von der Art, daß der Quotient $\frac{\mathsf{A}}{\mathfrak{L}_1^{e_1} \ldots \mathfrak{L}_z^{e_z}}$ zu 2 prim ausfällt. Die Relativnorm α der Zahl A erhält dann die Gestalt

$$\alpha = N(\mathsf{A}) = \mathfrak{a}\, \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_z^{e_z},$$

wo $\mathfrak{a}$ ein zu 2 primes Ideal des Körpers k bedeutet, und es läßt sich infolgedessen der Quotient $\frac{\nu}{\alpha}$ als ein Bruch $\frac{\varrho}{\sigma}$ darstellen, dessen Zähler ϱ und dessen Nenner σ ganze zu 2 prime Zahlen sind. Wegen der Definition 6 ist für jedes Primideal $\mathfrak{w}$

$$\left(\frac{N(\mathsf{A}), \mu}{\mathfrak{w}}\right) = +1$$

und mithin auch

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\alpha, \mu}{\mathfrak{w}}\right) = +1,$$

wo Π' über alle zu 2 primen Primideale $\mathfrak{w}$ in k erstreckt werden soll. Berücksichtigen wir ferner, daß nach Satz 36 die Gleichungen

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\sigma, \mu}{\mathfrak{w}}\right) = +1, \qquad \prod_{(\mathfrak{w})}{}' \left(\frac{\varrho, \mu}{\mathfrak{w}}\right) = +1$$

gelten, so erhalten wir mit Rücksicht auf die zweite Formel in Satz 14

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu\sigma, \mu}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\alpha\, \varrho, \mu}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\alpha, \mu}{\mathfrak{w}}\right) = +1,$$

wie der zu beweisende Satz 40 behauptet.

§ 29. Der Fundamentalsatz über die Anzahl der Geschlechter in einem relativquadratischen Körper.

In § 19 haben wir für den Fall, daß die Relativdiskriminante des Körpers $K(\sqrt{\mu})$ zu 2 prim ist, den Satz 26 bewiesen und dadurch eine obere Grenze für die Anzahl der Geschlechter in $K(\sqrt{\mu})$ aufgestellt. Wir sind nunmehr imstande, unter der nämlichen Einschränkung das folgende wichtige Theorem zu beweisen:

Satz 41. *Es sei r die Anzahl der Charaktere, welche ein Geschlecht des relativquadratischen Körpers $K(\sqrt{\mu})$ bestimmen; ist dann ein System von r beliebigen Einheiten ± 1 vorgelegt, so wird dieses System dann und nur dann das Charakterensystem eines Geschlechtes in $K(\sqrt{\mu})$, wenn das Produkt der sämtlichen r Einheiten gleich $+1$ ist. Die Anzahl g der in $K(\sqrt{\mu})$ vorhandenen Geschlechter ist daher gleich 2^{r-1}.*

Beweis. Es seien $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ die t in der Relativdiskriminante von $K(\sqrt{\mu})$ aufgehenden Primideale des Körpers $K(\sqrt{\mu})$ und man setze

$$\mathfrak{d}_1^h = (\delta_1), \ldots, \mathfrak{d}_t^h = (\delta_t),$$

wo $\delta_1, \ldots, \delta_t$ gewisse ganze Zahlen in k bedeuten. Es ist offenbar

$$\delta_1 \cdots \delta_t = \varepsilon\, \alpha^2\, \mu, \tag{1}$$

wo ε eine Einheit und α eine gewisse ganze Zahl in k bedeutet. Ferner wähle man nach der Vorschrift des § 17 von diesen t Primidealen gewisse $r = t - r^*$ aus; es seien dies etwa die Primideale $\mathfrak{d}_1, \ldots, \mathfrak{d}_r$. Endlich mögen $c_1, \ldots, c_r$ beliebige r Einheiten ± 1 bedeuten, die der Bedingung

$$c_1 \cdots c_r = +1 \tag{2}$$

genügen. Wegen Satz 18 gibt es in k gewiß ein primäres Primideal $\mathfrak{p}$, für welches

$$\left(\frac{\delta_1}{\mathfrak{p}}\right) = c_1, \ldots, \left(\frac{\delta_r}{\mathfrak{p}}\right) = c_r, \qquad \left(\frac{\delta_{r+1}}{\mathfrak{p}}\right) = +1, \ldots, \left(\frac{\delta_t}{\mathfrak{p}}\right) = +1 \tag{3}$$

ausfällt. Es sei π eine Primärzahl von $\mathfrak{p}$; dann ist nach Satz 37

$$\left(\frac{\pi}{\mathfrak{d}_i}\right) = \left(\frac{\delta_i}{\mathfrak{p}}\right), \qquad (i = 1, 2, \ldots, t).$$

Wegen (1), (2), (3) haben wir

$$\left(\frac{\delta_1 \cdots \delta_t}{\mathfrak{p}}\right) = \left(\frac{\varepsilon\, \alpha^2 \mu}{\mathfrak{p}}\right) = \left(\frac{\mu}{\mathfrak{p}}\right) = +1,$$

d. h. $\mathfrak{p}$ zerfällt in $K(\sqrt{\mu})$ in zwei Primfaktoren. Ein jeder derselben hat wegen

$$\left(\frac{\pi, \mu}{\mathfrak{d}_{r+1}}\right) = \left(\frac{\pi}{\mathfrak{d}_{r+1}}\right) = +1, \ldots, \qquad \left(\frac{\pi, \mu}{\mathfrak{d}_t}\right) = \left(\frac{\pi}{\mathfrak{d}_t}\right) = +1$$

im Körper $K(\sqrt{\mu})$ die Charaktere

$$\left(\frac{\pi, \mu}{\mathfrak{d}_1}\right) = \left(\frac{\pi}{\mathfrak{d}_1}\right) = c_1, \ldots, \qquad \left(\frac{\pi, \mu}{\mathfrak{d}_r}\right) = \left(\frac{\pi}{\mathfrak{d}_r}\right) = c_r.$$

Es lassen sich nun die Einheiten $c_1, \ldots, c_r$ offenbar auf 2^{r-1} Weisen so bestimmen, daß die Bedingung $c_1 \ldots c_r = +1$ erfüllt ist. Nach dem eben Bewiesenen gehört zu jedem solchen Systeme von r Einheiten wirklich ein Geschlecht in $K(\sqrt{\mu})$, und da die Anzahl g der Geschlechter von $K(\sqrt{\mu})$ nach Satz 26 auch nicht größer sein kann als 2^{r-1}, so ist der Satz 41 hiermit für den Fall bewiesen, daß die Relativdiskriminante des Körpers $K(\sqrt{\mu})$ zu 2 prim ausfällt. Den allgemeinen Nachweis des Satzes 41 werden wir erst in § 41 führen.

§ 30. Ein gewisses System von $\frac{m}{2} + z$ zu 2 primen Primidealen des Körpers k.

Wir leiten jetzt einen Satz ab, der im folgenden Paragraphen gebraucht werden wird und der eine Erweiterung des Satzes 29 ist. Dieser Satz lautet:

Satz 42. Es mögen $\varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}}, \mathfrak{q}_1, \ldots, \mathfrak{q}_{\frac{m}{2}}, \varkappa_1, \ldots, \varkappa_{\frac{m}{2}}$ die Bedeutung wie in Satz 29 haben; ferner werde

$$2 = \mathfrak{l}_1^{l_1} \ldots \mathfrak{l}_z^{l_z}$$

gesetzt, wo $\mathfrak{l}_1, \ldots, \mathfrak{l}_z$ die voneinander verschiedenen Primfaktoren der Zahl 2 in k und $l_1, \ldots, l_z$ die Potenzexponenten bedeuten, zu denen bez. jene Primideale in der Zahl 2 aufgehen. Es werde

$$\mathfrak{l}_1^h = (\lambda_1), \ldots, \mathfrak{l}_z^h = (\lambda_z)$$

gesetzt, wo $\lambda_1, \ldots, \lambda_z$ gewisse ganze Zahlen in k sind; endlich seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_z$ solche primäre Primideale, daß allemal

$$\left(\frac{\lambda_i}{\mathfrak{p}_i}\right) = -1, \quad \left(\frac{\lambda_k}{\mathfrak{p}_i}\right) = +1, \quad (i \neq k) \qquad (i, k = 1, 2, \ldots, z)$$

ausfällt, und es seien $\pi_1, \ldots, \pi_z$ bez. Primärzahlen der primären Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_z$: dann gilt für jede beliebige zu 2 prime ganze Zahl ω in k eine Kongruenz von der Gestalt

$$\omega \equiv \varepsilon_1^{u_1} \cdots \varepsilon_{\frac{m}{2}}^{u_{\frac{m}{2}}} \varkappa_1^{v_1} \cdots \varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}} \pi_1^{w_1} \cdots \pi_z^{w_z} \alpha^2, \qquad (\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}),$$

wo die Exponenten $u_1, \ldots, u_{\frac{m}{2}}, v_1, \ldots, v_{\frac{m}{2}}, w_1, \ldots, w_z$ gewisse Werte 0, 1 haben und α eine geeignete ganze Zahl in k bedeutet.

Beweis. Wir behandeln zunächst die Annahme, es gäbe $m+z$ Exponenten $u_1, \ldots, u_{\frac{m}{2}}, v_1, \ldots, v_{\frac{m}{2}}, w_1, \ldots, w_z$, die gewisse Werte 0,1 haben, aber nicht sämtlich gleich 0 sind, derart, daß die vermöge dieser Exponenten gebildete Zahl

$$\mu = \varepsilon_1^{u_1} \cdots \varepsilon_{\frac{m}{2}}^{u_{\frac{m}{2}}} \varkappa_1^{v_1} \cdots \varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}} \pi_1^{w_1} \cdots \pi_z^{w_z} \qquad (1)$$

dem Quadrat einer gewissen ganzen Zahl in k nach $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$ kongruent werde. Die Zahl $\sqrt{\mu}$ bestimmt dann offenbar einen relativquadratischen Körper $K(\sqrt{\mu})$, und zufolge des Satzes 5 ist die Relativdiskriminante dieses Körpers $K(\sqrt{\mu})$ prim zu 2. Aus dem Beweise zu Satz 29 schließen wir, daß die Exponenten $u_1, \ldots, u_{\frac{m}{2}}, v_1, \ldots, v_{\frac{m}{2}}$ im Ausdruck (1) sämtlich gleich 0 sind. Die Relativdiskriminante von $K(\sqrt{\mu})$ besitzt demnach mit Rücksicht auf Satz 4 keines der Primideale $\mathfrak{l}_1, \ldots, \mathfrak{l}_z, \mathfrak{q}_1, \ldots, \mathfrak{q}_{\frac{m}{2}}$ als Faktor, sondern enthält lediglich diejenigen unter den Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_z$, für welche in (1) bez. die Exponenten $w_1, \ldots, w_z$ gleich 1 ausfallen; es seien dies etwa die t Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. Infolge unserer Annahme ist dann notwendig $t > 0$.

Wir dürfen nunmehr Satz 41 anwenden, da derselbe in § 29 für den hier zutreffenden Fall bewiesen worden ist. Nach diesem Satze gibt es, da hier $r = t$ ausfällt, im Körper $K(\sqrt{\mu})$ genau 2^{t-1} Geschlechter und das Produkt

der sämtlichen Charaktere ist für jedes Geschlecht gleich $+1$. Da μ dem Quadrat einer ganzen Zahl in k nach dem Modul $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$ kongruent sein soll, so zerfällt insbesondere das Primideal $\mathfrak{l}_1$ im Körper $K(\sqrt{\mu})$ in zwei Primfaktoren. Die Charaktere eines jeden dieser Primfaktoren sind offenbar

$$\left(\frac{\lambda_1, \mu}{\mathfrak{p}_1}\right), \ldots, \left(\frac{\lambda_1, \mu}{\mathfrak{p}_t}\right)$$

und da das Produkt derselben gleich $+1$ sein soll, so würden wir

$$\left(\frac{\lambda_1}{\mathfrak{p}_1}\right) \cdots \left(\frac{\lambda_1}{\mathfrak{p}_t}\right) = +1$$

erhalten. Diese Folgerung widerspricht den Voraussetzungen, die wir im Satze 42 über die Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_z$ getroffen haben, und demnach ist unsere zu Anfang dieses Beweises gemachte Annahme zu verwerfen, d. h. irgendein Ausdruck von der Gestalt (1) kann nur dann kongruent dem Quadrat einer ganzen Zahl in k nach dem Modul $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$ sein, wenn sämtliche Exponenten $u_1, \ldots, u_{\frac{m}{2}}, v_1, \ldots, v_{\frac{m}{2}}, w_1, \ldots, w_z$ gleich 0 sind.

Wir setzen nun zur Abkürzung

$$L_1 = n(\mathfrak{l}_1)^{l_1}(n(\mathfrak{l}_1) - 1)$$

und verstehen unter

$$\alpha_1^{(1)}, \ldots, \alpha_1^{(L_1)}$$

ein volles System von ganzen zu $\mathfrak{l}_1$ primen und nach $\mathfrak{l}_1^{l_1+1}$ einander inkongruenten Zahlen in k, die überdies sämtlich kongruent 1 nach dem Modul $\mathfrak{l}_2^{l_2+1}\mathfrak{l}_3^{l_3+1} \ldots \mathfrak{l}_z^{l_z+1}$ sein sollen. Da allgemein

$$\alpha_1^{(i)} \not\equiv -\alpha_1^{(i)}, \qquad (\mathfrak{l}_1^{l_1+1}), \qquad (i = 1, 2, \ldots, L_1)$$

ist, so können wir annehmen, es sei etwa stets

$$-\alpha_1^{(i)} \equiv \alpha_1^{\left(\frac{L_1}{2}+i\right)}, \qquad (\mathfrak{l}_1^{l_1+1}), \qquad \left(i = 1, 2, \ldots, \frac{L_1}{2}\right).$$

Die $\frac{L_1}{2}$ Zahlen $\alpha_1^{(1)}, \ldots, \alpha_1^{\left(\frac{L_1}{2}\right)}$ haben dann offenbar die Eigenschaft, daß weder die Differenz noch die Summe von irgend zwei derselben durch $\mathfrak{l}_1^{l_1+1}$ teilbar wird. Ferner setzen wir zur Abkürzung

$$L_2 = n(\mathfrak{l}_2)^{l_2}(n(\mathfrak{l}_2) - 1),$$
$$\cdots\cdots\cdots\cdots$$
$$L_z = n(\mathfrak{l}_z)^{l_z}(n(\mathfrak{l}_z) - 1)$$

und bilden in der entsprechenden Weise wie oben zunächst das System von $\frac{L_2}{2}$ ganzen, zu $\mathfrak{l}_2$ primen Zahlen

$$\alpha_2^{(1)}, \ldots, \alpha_2^{\left(\frac{L_2}{2}\right)},$$

die sämtlich kongruent 1 nach $\mathfrak{l}_1^{l_1+1}\mathfrak{l}_3^{l_3+1} \ldots \mathfrak{l}_z^{l_z+1}$ sind und die Eigenschaft

haben, daß weder die Differenz noch die Summe von irgend zwei derselben durch $\mathfrak{l}_2^{l_2+1}$ teilbar wird usf.; endlich bilden wir ein System von $\frac{L_z}{2}$ ganzen, zu $\mathfrak{l}_z$ primen Zahlen

$$\alpha_z^{(1)}, \ldots, \alpha_z^{\left(\frac{L_z}{2}\right)},$$

die sämtlich kongruent 1 nach $\mathfrak{l}_1^{l_1+1}\,\mathfrak{l}_2^{l_2+1}\ldots\mathfrak{l}_{z-1}^{l_{z-1}+1}$ sind und die Eigenschaft haben, daß weder die Differenz noch die Summe von irgend zwei derselben durch $\mathfrak{l}_z^{l_z+1}$ teilbar wird.

Der Ausdruck

$$\varepsilon_1^{u_1}\cdots\varepsilon_{\frac{m}{2}}^{u_{\frac{m}{2}}}\varkappa_1^{v_1}\cdots\varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}}\pi_1^{w_1}\cdots\pi_z^{w_z}(\alpha_1^{(i_1)})^2\cdots(\alpha_z^{(i_z)})^2, \tag{2}$$

$$\left(\begin{array}{c} u_1, \ldots, u_{\frac{m}{2}}, v_1, \ldots, v_{\frac{m}{2}};\quad w_1, \ldots, w_z = 0, 1, \\ i_1 = 1, 2, \ldots, \frac{L_1}{2}, \ldots,\quad i_z = 1, 2, \ldots, \frac{L_z}{2} \end{array}\right)$$

stellt ein System von $2^m L_1 \ldots L_z$ ganzen Zahlen in k dar; diese sind sämtlich zu 2 prim und nach $\mathfrak{l}_1^{2l_1+1}\ldots\mathfrak{l}_z^{2l_z+1}$ einander inkongruent. In der Tat wären zwei Zahlen von der Gestalt (2) einander nach $\mathfrak{l}_1^{2l_1+1}\ldots\mathfrak{l}_z^{2l_z+1}$ kongruent, wäre etwa

$$\left.\begin{array}{c} \varepsilon_1^{u_1}\cdots\varepsilon_{\frac{m}{2}}^{u_{\frac{m}{2}}}\varkappa_1^{v_1}\cdots\varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}}\pi_1^{w_1}\cdots\pi_z^{w_z}(\alpha_1^{(i_1)})^2\cdots(\alpha_z^{(i_z)})^2 \\ \equiv \varepsilon_1^{u_1'}\cdots\varepsilon_{\frac{m}{2}}^{u_{\frac{m}{2}}'}\varkappa_1^{v_1'}\cdots\varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}'}\pi_1^{w_1'}\cdots\pi_z^{w_z'}(\alpha_1^{(i_1')})^2\cdots(\alpha_z^{(i_z')})^2, \\ (\mathfrak{l}_1^{2l_1+1}\mathfrak{l}_2^{2l_2+1}\ldots\mathfrak{l}_z^{2l_z+1}), \end{array}\right\} \tag{3}$$

so würde, da die Zahlen $\alpha_1^{(i)}, \ldots, \alpha_z^{(i)}$ sämtlich zu 2 prim sind, aus dem vorhin Bewiesenen sofort folgen, daß die Exponenten $u_1, \ldots, u_{\frac{m}{2}}, v_1, \ldots, v_{\frac{m}{2}}$, $w_1, \ldots, w_z$ bez. mit den Exponenten $u_1', \ldots, u_{\frac{m}{2}}', v_1', \ldots, v_{\frac{m}{2}}', w_1', \ldots, w_z'$ übereinstimmen und es wäre mithin

$$(\alpha_1^{(i_1)})^2\cdots(\alpha_z^{(i_z)})^2 \equiv (\alpha_1^{(i_1')})^2\cdots(\alpha_z^{(i_z')})^2, \qquad (\mathfrak{l}_1^{2l_1+1}\ldots\mathfrak{l}_z^{2l_z+1}).$$

Aus dieser Kongruenz entnehmen wir der Reihe nach die z Kongruenzen

$$\begin{array}{ll} (\alpha_1^{(i_1)})^2 \equiv (\alpha_1^{(i_1')})^2, & (\mathfrak{l}_1^{2l_1+1}), \\ \cdots\cdots\cdots\cdots & \\ (\alpha_z^{(i_z)})^2 \equiv (\alpha_z^{(i_z')})^2, & (\mathfrak{l}_z^{2l_z+1}). \end{array}$$

Aus der ersten Kongruenz folgt leicht, daß entweder $\alpha_1^{(i_1)} - \alpha_1^{(i_1')}$ oder $\alpha_1^{(i_1)} + \alpha_1^{(i_1')}$ durch $\mathfrak{l}_1^{l_1+1}$ teilbar sein muß, und deswegen ist notwendigerweise $i_1 = i_1'$. Ebenso schließen wir $i_2 = i_2', \ldots, i_z = i_z'$, d. h. die beiden Ausdrücke auf der linken und rechten Seite der Kongruenz (3) waren nicht voneinander verschieden.

Nun gibt es für den Modul $\mathfrak{l}_1^{2l_1+1}\ldots\mathfrak{l}_z^{2l_z+1}$ genau

$$n(\mathfrak{l}_1)^{2l_1}\cdots n(\mathfrak{l}_z)^{2l_z}(n(\mathfrak{l}_1)-1)\cdots(n(\mathfrak{l}_z)-1) = 2^m L_1\cdots L_z$$

zu 2 prime und untereinander inkongruente Zahlen und mithin bilden die ganzen Zahlen in (2) ein volles Restsystem der genannten Art nach $\mathfrak{l}_1^{2l_1+1}\ldots\mathfrak{l}_z^{2l_z+1}$; dies ist die Aussage des Satzes 42.

§ 31. Eine Eigenschaft gewisser besonderer Ideale des Körpers k.

Wir setzen nunmehr die in § 23 und in § 26 angestellten Untersuchungen über primäre Ideale des Körpers k fort und gelangen zu folgenden Sätzen:

Satz 43. Es sei $\mathfrak{a}$ ein beliebiges zu 2 primes Ideal in k von solcher Beschaffenheit, daß die Gleichungen

$$\left(\frac{\varepsilon_1}{\mathfrak{a}}\right) = +1, \ldots, \left(\frac{\varepsilon_{\frac{m}{2}}}{\mathfrak{a}}\right) = +1,$$
$$\left(\frac{\lambda_1}{\mathfrak{a}}\right) = +1, \ldots, \left(\frac{\lambda_z}{\mathfrak{a}}\right) = +1$$

gelten: dann ist es stets möglich, in k eine ganze Zahl α zu finden, so daß das Ideal (α) gleich $\mathfrak{a}^h$ wird, und überdies die Zahl α nach dem Modul $\mathfrak{l}_1^{2l_1+1}\ldots\mathfrak{l}_z^{2l_z+1}$ dem Quadrat einer ganzen Zahl des Körpers k kongruent wird; hierbei haben $\varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}}, \mathfrak{l}_1, \ldots, \mathfrak{l}_z, l_1, \ldots, l_z, \lambda_1, \ldots, \lambda_z$ die Bedeutung wie in Satz 42.

Beweis. Es sei α^* irgendeine ganze Zahl in k, so daß $(\alpha^*) = \mathfrak{a}^h$ wird. Bezeichnen ferner $\mathfrak{q}_1, \ldots, \mathfrak{q}_{\frac{m}{2}}, \mathfrak{p}_1, \ldots, \mathfrak{p}_z, \varkappa_1, \ldots, \varkappa_{\frac{m}{2}}, \pi_1, \ldots, \pi_z$ dieselben Ideale bez. ganzen Zahlen des Körpers k wie in Satz 42, so ist nach dem dort Bewiesenen jede ganze zu 2 prime Zahl nach dem Modul $\mathfrak{l}_1^{2l_1+1}\ldots\mathfrak{l}_z^{2l_z+1}$ in der Gestalt darstellbar, wie im Satze 42 angegeben worden ist; wir dürfen also insbesondere

$$\alpha^* \equiv \varepsilon^*\varkappa_1^{v_1}\cdots\varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}}\pi_1^{w_1}\cdots\pi_z^{w_z}\beta^2, \qquad (\mathfrak{l}_1^{2l_1+1}\ldots\mathfrak{l}_z^{2l_z+1}) \tag{1}$$

setzen, wo ε^* eine geeignete Einheit in k, $v_1, \ldots, v_{\frac{m}{2}}, w_1, \ldots, w_z$ gewisse Exponenten 0, 1 und β eine geeignete ganze Zahl in k bedeutet. Da hiernach die Zahl

$$\mu = \alpha^*\varepsilon^*\varkappa_1^{v_1}\cdots\varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}}\pi_1^{w_1}\cdots\pi_z^{w_z}$$

dem Quadrat einer ganzen Zahl in k nach dem Modul $\mathfrak{l}_1^{2l_1+1}\ldots\mathfrak{l}_z^{2l_z+1}$ kongruent ausfällt, so erhalten wir nach Satz 40 die Gleichungen

$$\left.\begin{array}{l} \prod_{(\mathfrak{w})}{}'\left(\frac{\varepsilon_1, \mu}{\mathfrak{w}}\right) = +1, \ldots, \prod_{(\mathfrak{w})}{}'\left(\frac{\varepsilon_{\frac{m}{2}}, \mu}{\mathfrak{w}}\right) = +1, \\ \prod_{(\mathfrak{w})}{}'\left(\frac{\lambda_1, \mu}{\mathfrak{w}}\right) = +1, \ldots, \prod_{(\mathfrak{w})}{}'\left(\frac{\lambda_z, \mu}{\mathfrak{w}}\right) = +1, \end{array}\right\} \tag{2}$$

wo das Produkt Π' stets über alle zu 2 primen Primideale $\mathfrak{w}$ des Körpers k erstreckt werden soll. Aus den Gleichungen (2) folgt leicht

$$\left(\frac{\varepsilon_i}{\alpha^* \varkappa_1^{v_1} \cdots \varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}} \pi_1^{w_1} \cdots \pi_z^{w_z}}\right) = \left(\frac{\varepsilon_i}{\mathfrak{a}}\right)\left(\frac{\varepsilon_i}{\mathfrak{q}_1}\right)^{v_1} \cdots \left(\frac{\varepsilon_i}{\mathfrak{q}_{\frac{m}{2}}}\right)^{v_{\frac{m}{2}}} \left(\frac{\varepsilon_i}{\mathfrak{p}_1}\right)^{w_1} \cdots \left(\frac{\varepsilon_i}{\mathfrak{p}_z}\right)^{w_z} = +1, \quad (3)$$

$$\left(i = 1, 2, \ldots, \frac{m}{2}\right),$$

$$\left(\frac{\lambda_k}{\alpha^* \varkappa_1^{v_1} \cdots \varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}} \pi_1^{w_1} \cdots \pi_z^{w_z}}\right) = \left(\frac{\lambda_k}{\mathfrak{a}}\right)\left(\frac{\lambda_k}{\mathfrak{q}_1}\right)^{v_1} \cdots \left(\frac{\lambda_k}{\mathfrak{q}_{\frac{m}{2}}}\right)^{v_{\frac{m}{2}}} \left(\frac{\lambda_k}{\mathfrak{p}_1}\right)^{w_1} \cdots \left(\frac{\lambda_k}{\mathfrak{p}_z}\right)^{w_z} = +1, \quad (4)$$

$$(k = 1, 2, \ldots, z).$$

Indem wir die Voraussetzungen des Satzes 43 benutzen, schließen wir aus (3), (4) der Reihe nach, daß die Exponenten $v_1, \ldots, v_{\frac{m}{2}}, w_1, \ldots, w_z$ sämtlich gleich 0 sind; folglich ist wegen (1) die Zahl $\alpha = \varepsilon^* \alpha^*$ von der im Satze 43 verlangten Art.

Die Umkehrung des Satzes 43 lautet wie folgt:

Satz 44. Wenn α eine zu 2 prime ganze Zahl in k ist, die dem Quadrat einer ganzen Zahl in k nach $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$ kongruent ausfällt, so gelten die Gleichungen

$$\left(\frac{\varepsilon_1}{\alpha}\right) = +1, \ldots, \left(\frac{\varepsilon_{\frac{m}{2}}}{\alpha}\right) = +1,$$
$$\left(\frac{\lambda_1}{\alpha}\right) = +1, \ldots, \left(\frac{\lambda_z}{\alpha}\right) = +1;$$

dabei haben $\varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}}, \mathfrak{l}_1, \ldots, \mathfrak{l}_z, l_1, \ldots, l_z, \lambda_1, \ldots, \lambda_z$ die Bedeutung wie in Satz 42.

Den Beweis dieses Satzes gewinnen wir unmittelbar aus Satz 40, indem wir in der Gleichung dieses Satzes 40 für ν der Reihe nach die Zahlen $\varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}}, \lambda_1, \ldots, \lambda_z$ und für μ jedesmal die Zahl α nehmen.

Die Sätze 43 und 44 bilden einen wesentlichen Bestandteil des *zweiten* Ergänzungssatzes zu dem später aufzustellenden allgemeinen Reziprozitätsgesetze für quadratische Reste. Es ist eine lohnende Aufgabe, für die Sätze 43 und 44 numerische Beispiele in ähnlicher Weise zu berechnen wie dies in § 27 für die entsprechenden Aussagen des ersten Ergänzungssatzes geschah. Wegen der vielen möglichen Arten der Zerlegung der Zahl 2 in verschiedenen Körpern k weisen die Aussagen des zweiten Ergänzungssatzes sogar eine noch größere Mannigfaltigkeit an einzelnen arithmetischen Wahrheiten auf als bei Erörterung des ersten Ergänzungssatzes zutage traten.

§ 32. Das Symbol $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ für irgendwelche zu 2 primen Zahlen ν, μ.

Wir sind nunmehr imstande, diejenigen Sätze aufzustellen und zu beweisen, welche den Sätzen 14, 15 entsprechen, wenn man für $\mathfrak{w}$ ein in 2 aufgehendes Primideal des Körpers k nimmt. Um dieses Ziel zu erreichen, führen wir ein neues Symbol $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ ein; dieses Symbol dient uns jedoch nur zum vorübergehenden Gebrauch, da dasselbe sich später als gleichbedeutend mit dem Symbol $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ herausstellen wird.

Definition 17. Es seien ν, μ irgendwelche zu 2 prime ganze Zahlen in k; ferner sei $\mathfrak{l}$ ein in der Zahl 2 aufgehendes Primideal des Körpers k, und wir setzen $2 = \mathfrak{l}^l \mathfrak{L}$, wo l einen positiven Potenzexponenten und $\mathfrak{L}$ ein zu $\mathfrak{l}$ primes Ideal des Körpers k bedeutet: dann werde das neue Symbol $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ durch die Gleichung

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu^*}{\mathfrak{w}}\right)$$

definiert; hierin ist $\prod'$ über alle zu 2 primen Primideale $\mathfrak{w}$ zu erstrecken, und μ^* soll eine solche zu 2 prime ganze Zahl in k bedeuten, die den Kongruenzen

$$\mu^* \equiv \mu, \quad (\mathfrak{l}^{2l}),$$
$$\mu^* \equiv \alpha^2, \quad (\mathfrak{L}^2)$$

genügt, wo α irgendeine zu $\mathfrak{L}$ prime ganze Zahl in k sein soll.

In der Tat ist das Symbol $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ durch diese Festsetzung eindeutig bestimmt. Ist nämlich μ_0^* eine ganze Zahl in k, welche den Kongruenzen

$$\mu_0^* \equiv \mu, \quad (\mathfrak{l}^{2l}),$$
$$\mu_0^* \equiv \alpha_0^2, \quad (\mathfrak{L}^2)$$

genügt, wobei α_0 irgendeine zu $\mathfrak{L}$ prime und von α verschiedene ganze Zahl in k darstellt, so bestimme man zwei ganze Zahlen ξ, ξ_0 in k, die den Kongruenzen

$$\left.\begin{aligned} \xi \xi_0 \mu &\equiv 1, \quad (\mathfrak{l}^{2l}), \\ \xi \alpha &\equiv 1, \\ \xi_0 \alpha_0 &\equiv 1, \end{aligned}\right\} \quad (\mathfrak{L}^2)$$

genügen: dann erfüllt die Zahl $\zeta = \xi^2 \xi_0^2 \mu^* \mu_0^*$ die Kongruenz $\zeta \equiv 1$ nach 2^2, und folglich erhalten wir nach Satz 36

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \zeta}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu^* \mu_0^*}{\mathfrak{w}}\right) = +1;$$

mithin ist

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu^*}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu_0^*}{\mathfrak{w}}\right),$$

wo das Produkt $\prod'$ stets über sämtliche zu 2 primen Primideale $\mathfrak{w}$ in k zu erstrecken ist.

Wenn wir die beiden letzten Formeln des Satzes 14 heranziehen, so erhalten wir unmittelbar aus der Definition 17 des Symbols $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ zwei entsprechende Formeln für dieses neue Symbol; wir drücken diese Tatsache in dem folgenden Satze aus:

Satz 45. (Hilfssatz.) Wenn $\nu, \nu_1, \nu_2, \mu, \mu_1, \mu_2$ beliebige zu 2 prime ganze Zahlen des Körpers k sind, so gelten in bezug auf ein jedes in 2 aufgehende Primideal $\mathfrak{l}$ die Formeln

$$\left(\frac{\nu_1 \nu_2, \mu}{\mathfrak{l}}\right) = \left(\frac{\nu_1, \mu}{\mathfrak{l}}\right)\left(\frac{\nu_2, \mu}{\mathfrak{l}}\right),$$

$$\left(\frac{\nu, \mu_1 \mu_2}{\mathfrak{l}}\right) = \left(\frac{\nu, \mu_1}{\mathfrak{l}}\right)\left(\frac{\nu, \mu_2}{\mathfrak{l}}\right).$$

§ 33. Die Übereinstimmung der beiden Symbole $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ und $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ für irgendwelche zu 2 prime Zahlen ν, μ.

Um die Übereinstimmung der beiden Symbole $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ und $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ miteinander zu erkennen, bedienen wir uns der folgenden Entwicklungen:

Satz 46. (Hilfssatz.) Es sei wie in Definition 17 $\mathfrak{l}$ ein Primfaktor von 2 im Körper k und es gehe $\mathfrak{l}$ in 2 genau zur l-ten Potenz auf; ferner sei ϱ eine ganze oder gebrochene Zahl in k, für die eine Kongruenz

$$\varrho \equiv \alpha^2, \qquad (\mathfrak{l}^{2l+1})$$

gilt, wobei α eine ganze zu 2 prime Zahl in k bedeutet: dann kann stets auch für jede Potenz $\mathfrak{l}^L$ mit höherem Exponenten L eine ganze Zahl α_L in k gefunden werden, welche der Kongruenz

$$\varrho \equiv \alpha_L^2, \qquad (\mathfrak{l}^L)$$

genügt.

Beweis. Nehmen wir an, es sei für die Potenz $\mathfrak{l}^{2l+a}$ $(a \geqq 1)$ eine Zahl α_{2l+a} von der verlangten Beschaffenheit bereits gefunden, so gelangen wir zu einer Zahl α_{2l+a+1} für die Potenz $\mathfrak{l}^{2l+a+1}$ auf diese Weise. Wir wählen zunächst eine ganze Zahl λ in k, welche durch $\mathfrak{l}$, aber nicht durch $\mathfrak{l}^2$ teilbar ist, und setzen

$$\alpha_{2l+a+1} = \alpha_{2l+a} + 2\lambda^a \xi,$$

worin ξ noch eine zu bestimmende ganze Zahl in k sei. Aus der Kongruenz

$$\varrho \equiv \alpha_{2l+a+1}^2 = \alpha_{2l+a}^2 + 4\alpha_{2l+a}\lambda^a \xi + 4\lambda^{2a}\xi^2, \qquad (\mathfrak{l}^{2l+a+1})$$

erhalten wir

$$\varrho \equiv \alpha_{2l+a}^2 + 4\alpha_{2l+a}\lambda^a \xi, \qquad (\mathfrak{l}^{2l+a+1})$$

und bestimmen wir sodann ξ aus der Kongruenz

$$\xi \equiv \frac{\varrho - \alpha_{2l+a}^2}{4\alpha_{2l+a}\lambda^a}, \qquad (\mathfrak{l}),$$

so ist α_{2l+a+1} eine Zahl von der verlangten Beschaffenheit; damit haben wir den Beweis für den Satz 46 erbracht.

Satz 47. (Hilfssatz.) Es sei $\mathfrak{l}$ ein Primfaktor von 2 in k und es gehe $\mathfrak{l}$ in 2 genau zur l-ten Potenz auf: wenn dann $\nu_1, \nu_2, \mu_1, \mu_2$ irgendwelche zu 2 prime ganze Zahlen in k sind, derart, daß die Brüche $\frac{\nu_1}{\nu_2}$ und $\frac{\mu_1}{\mu_2}$ den Quadraten gewisser ganzen Zahlen in k nach $\mathfrak{l}^{2l+1}$ kongruent ausfallen, so ist stets

$$\left(\frac{\nu_1, \mu_1}{\mathfrak{l}}\right) = \left(\frac{\nu_2, \mu_2}{\mathfrak{l}}\right).$$

Beweis. Wir nehmen an, es sei μ_1 nicht das Quadrat einer Zahl in k und ν_1 im Körper $K(\sqrt{\mu_1})$ Normenrest nach $\mathfrak{l}$; wir verstehen dann unter L irgendeinen Exponenten und unter A eine solche ganze Zahl in $K(\sqrt{\mu_1})$, daß $\nu_1 \equiv N(\mathsf{A})$ nach $\mathfrak{l}^L$ wird. Da $\frac{\nu_1}{\nu_2}$ und mithin auch $\frac{\nu_2}{\nu_1}$ dem Quadrat einer ganzen Zahl in k nach $\mathfrak{l}^{2l+1}$ kongruent ist, so muß nach Satz 46 auch für jeden beliebigen Exponenten L eine ganze Zahl α_L in k existieren, deren Quadrat dem Bruche $\frac{\nu_2}{\nu_1}$ kongruent nach $\mathfrak{l}^L$ ausfällt; wir haben somit

$$\nu_2 \equiv \alpha_L^2 \nu_1 \equiv N(\alpha_L \mathsf{A}), \qquad (\mathfrak{l}^L), \tag{1}$$

d. h. ν_2 ist im Körper $K(\sqrt{\mu_1})$ Normenrest nach $\mathfrak{l}$.

Wir setzen nun

$$\alpha_L \mathsf{A} = \frac{\alpha + \beta\sqrt{\mu_1}}{\gamma}; \tag{2}$$

hierin seien α, β, γ gewisse ganze Zahlen in k und es gehe $\mathfrak{l}$ in γ genau zur c-ten Potenz auf. Wegen der über $\frac{\mu_1}{\mu_2}$ gemachten Voraussetzung können wir nach Satz 46 eine Zahl β_L finden, so daß

$$\frac{\mu_1}{\mu_2} \equiv \beta_L^2, \quad \text{d. h.} \quad \mu_1 \equiv \mu_2 \beta_L^2, \qquad (\mathfrak{l}^{L+2c}) \tag{3}$$

ausfällt. Aus (1), (2), (3) erhalten wir dann

$$\nu_2 \gamma^2 \equiv \alpha^2 - \beta^2 \mu_1 \equiv \alpha^2 - \beta^2 \beta_L^2 \mu_2, \qquad (\mathfrak{l}^{L+2c}). \tag{4}$$

Stellt nun δ irgendeine zu $\mathfrak{l}$ prime und durch $\frac{\gamma}{\mathfrak{l}^c}$ teilbare Zahl in k dar, so ist

$$\mathsf{A}^* = \frac{\delta(\alpha + \beta\beta_L\sqrt{\mu_2})}{\gamma}$$

gewiß eine ganze Zahl in $K(\sqrt{\mu_2})$, da offenbar Summe und Produkt dieser Zahl A^* und ihrer relativkonjugierten Zahl $S\mathsf{A}^*$ ganze Zahlen in k sind. Bei Benutzung von (4) folgt

$$N(\mathsf{A}^*) \equiv \delta^2 \nu_2, \qquad (\mathfrak{l}^L),$$

und da δ zu $\mathfrak{l}$ prim ist, so erweist sich mithin ν_2 als Normenrest des Körpers $K(\sqrt{\mu_2})$ nach $\mathfrak{l}$.

Wir haben also bewiesen, daß allemal, wenn $\left(\frac{\nu_1, \mu_1}{\mathfrak{l}}\right) = +1$ ist, auch $\left(\frac{\nu_2, \mu_2}{\mathfrak{l}}\right) = +1$ sein muß. Da nun aus denselben Gründen umgekehrt aus $\left(\frac{\nu_2, \mu_2}{\mathfrak{l}}\right) = +1$, wenn μ_2 nicht das Quadrat einer Zahl in k ist, allemal auch $\left(\frac{\nu_1, \mu_1}{\mathfrak{l}}\right) = +1$ gefolgert werden kann, so ist damit die Richtigkeit des Satzes 47 für den Fall gezeigt, daß keine der beiden Zahlen μ_1, μ_2 das Quadrat einer Zahl in k ist.

Nehmen wir an, es sei eine jener beiden Zahlen, etwa die Zahl μ_2, dagegen nicht μ_1 das Quadrat einer ganzen Zahl in k, so ist nach Definition 6 $\left(\frac{\nu_2, \mu_2}{\mathfrak{l}}\right) = +1$, und die Voraussetzung des zu beweisenden Satzes 47 fordert dann, daß μ_1 kongruent dem Quadrat einer ganzen Zahl in k nach $\mathfrak{l}^{2l+1}$ sein muß; wir wollen im folgenden den Nachweis dafür führen, daß in diesem Falle auch stets $\left(\frac{\nu_1, \mu_1}{\mathfrak{l}}\right) = +1$ ausfällt.

Zu dem Zwecke bezeichnen wir wie in Satz 40 mit $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ die sämtlichen voneinander verschiedenen in 2 aufgehenden Primideale, und es möge ferner allgemein $\mathfrak{l}_i$ genau zur l_i-ten Potenz in 2 aufgehen, so daß

$$2 = \mathfrak{l}_1^{l_1} \mathfrak{l}_2^{l_2} \ldots \mathfrak{l}_z^{l_z}$$

wird; wir nehmen $\mathfrak{l} = \mathfrak{l}_1$ und setzen $l = l_1$. Sodann bestimmen wir eine ganze Zahl μ_1^* in k, welche den Kongruenzen

$$\left.\begin{aligned} \mu_1^* &\equiv \mu_1, \qquad (\mathfrak{l}_1^{2l_1+1}), \\ \mu_1^* &\equiv 1, \qquad (\mathfrak{l}_2^{2l_2} \ldots \mathfrak{l}_z^{2l_z}) \end{aligned}\right\} \tag{5}$$

genügt und, nachdem dies geschehen, ein Primideal $\mathfrak{p}$ in k, für welches die Gleichungen

$$\left.\begin{aligned} \left(\frac{\varepsilon_1}{\mathfrak{p}}\right) &= \left(\frac{\varepsilon_1}{\mu_1^*}\right), \ldots, \left(\frac{\varepsilon_{\frac{m}{2}}}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_{\frac{m}{2}}}{\mu_1^*}\right), \\ \left(\frac{\lambda_1}{\mathfrak{p}}\right) &= \left(\frac{\lambda_1}{\mu_1^*}\right), \ldots, \left(\frac{\lambda_z}{\mathfrak{p}}\right) = \left(\frac{\lambda_z}{\mu_1^*}\right) \end{aligned}\right\} \tag{6}$$

gelten; hierbei sollen $\varepsilon_1, \ldots, \varepsilon_{\frac{m}{2}}, \lambda_1, \ldots, \lambda_z$ die Bedeutung wie in Satz 42 haben. Da wegen (6)

$$\left(\frac{\varepsilon_1}{\mathfrak{p}\mu_1^*}\right) = +1, \ldots, \left(\frac{\varepsilon_{\frac{m}{2}}}{\mathfrak{p}\mu_1^*}\right) = +1,$$
$$\left(\frac{\lambda_1}{\mathfrak{p}\mu_1^*}\right) = +1, \ldots, \left(\frac{\lambda_z}{\mathfrak{p}\mu_1^*}\right) = +1$$

wird, so können wir nach Satz 43 eine ganze Zahl α derart bestimmen, daß das

Ideal (α) gleich $\mathfrak{p}^h \mu_1^{*h}$ ist und überdies die Zahl α dem Quadrat einer ganzen Zahl in k nach $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$ kongruent ausfällt. Wir setzen $\pi = \frac{\alpha}{\mu_1^{*h}}$ und haben dann $(\pi) = \mathfrak{p}^h$.

Nunmehr bestimmen wir in k ein Primideal $\mathfrak{q}$, für welches die Gleichungen

$$\left(\frac{\varepsilon_1}{\mathfrak{q}}\right) = \left(\frac{\varepsilon_1}{\nu_1}\right), \ldots, \left(\frac{\varepsilon_{\frac{m}{2}}}{\mathfrak{q}}\right) = \left(\frac{\varepsilon_{\frac{m}{2}}}{\nu_1}\right),$$
$$\left(\frac{\lambda_1}{\mathfrak{q}}\right) = \left(\frac{\lambda_1}{\nu_1}\right), \ldots, \left(\frac{\lambda_z}{\mathfrak{q}}\right) = \left(\frac{\lambda_z}{\nu_1}\right),$$
$$\left(\frac{\pi}{\mathfrak{q}}\right) = +1 \tag{7}$$

gelten. Indem wir wie vorhin verfahren, können wir nach Satz 43 eine ganze Zahl β derart bestimmen, daß das Ideal $(\beta) = \mathfrak{q}^h \nu_1^h$ wird und überdies die Zahl β dem Quadrat einer ganzen Zahl in k nach dem Modul $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$ kongruent ausfällt; wir setzen $\varkappa = \frac{\beta}{\nu_1^h}$ und haben dann $(\varkappa) = \mathfrak{q}^h$.

Indem wir die Beschaffenheit der Zahlen α, β berücksichtigen und den Satz 47 für den oben bereits behandelten Fall anwenden, erhalten wir

$$\left(\frac{\nu_1, \mu_1}{\mathfrak{l}}\right) = \left(\frac{\varkappa, \pi}{\mathfrak{l}}\right). \tag{8}$$

Wir betrachten jetzt den Körper $K(\sqrt{\pi})$ und werden beweisen, daß $\varkappa$ gleich der Relativnorm einer solchen Zahl dieses Körpers $K(\sqrt{\pi})$ ist, deren Nenner prim zu 2 ausfällt. Wegen der Kongruenzen (5) ist μ_1^* und folglich auch π gewiß dem Quadrat einer ganzen Zahl in k nach dem Modul 2^2 kongruent; infolgedessen enthält die Relativdiskriminante des Körpers $K(\sqrt{\pi})$ nach Satz 4 und 5 nur den einen Primfaktor $\mathfrak{p}$. Wenn wir die am Schlusse von § 15 gemachte Bemerkung auf diesen Körper $K(\sqrt{\pi})$ anwenden und demgemäß $t = 1$ nehmen, so wird aus der dort aufgestellten Ungleichung die folgende

$$v^* > \frac{m}{2} - 1,$$

und da v^* offenbar nicht größer als $\frac{m}{2}$ sein kann, so ist hier notwendig $v^* = \frac{m}{2}$, d. h. jede Einheit in k ist die Relativnorm einer Einheit in $K(\sqrt{\pi})$. Die im Satze 23 mit v bezeichnete Anzahl hat ihrer Bedeutung nach mindestens den Wert v^* und ist daher ebenfalls gleich $\frac{m}{2}$; der Satz 23 lehrt dann, daß die Anzahl aller ambigen Komplexe im Körper $K(\sqrt{\pi})$ gleich 1 ist, d. h. im Körper $K(\sqrt{\pi})$ ist der einzige ambige Komplex der Hauptkomplex.

Aus der soeben festgestellten Tatsache erkennen wir leicht, daß die Klassenanzahl H des Körpers $K(\sqrt{\pi})$ notwendig ungerade ausfallen muß. Im entgegengesetzten Falle gäbe es nämlich in $K(\sqrt{\pi})$ ein Ideal $\mathfrak{J}$, so daß

$$\mathfrak{J} \not\sim 1, \qquad \mathfrak{J}^2 \sim 1$$

wäre. Dieses Ideal $\mathfrak{J}$ könnte nun nicht dem Hauptkomplex angehören; denn wäre $\mathfrak{J}$ einem Ideale $\mathfrak{j}$ in k äquivalent, so müßte

$$\mathfrak{J}^h \sim \mathfrak{j}^h \sim 1$$

sein und aus dieser Äquivalenz würde, da h eine ungerade Zahl ist, sofort $\mathfrak{J} \sim 1$ folgen, was nicht der Fall sein sollte. Andererseits ist, wenn $N(\mathfrak{J}) = \mathfrak{J} \cdot S\mathfrak{J} = \mathfrak{n}$ gesetzt wird, $\mathfrak{n} \cdot \mathfrak{J} \sim S\mathfrak{J}$ und mithin würde das Ideal $\mathfrak{J}$ im Körper $K(\sqrt{\pi})$ einen ambigen Komplex bestimmen, welcher von dem Hauptkomplexe verschieden wäre; dies widerspräche der vorhin bewiesenen Tatsache.

Wegen der Gleichung (7) zerfällt das Ideal $\mathfrak{q}$ im Körper $K(\sqrt{\pi})$; es sei $\mathfrak{Q}$ einer der beiden Primfaktoren von $\mathfrak{q}$. Setzen wir $\mathfrak{Q}^{hH} = (\mathsf{A})$, so daß A eine ganze Zahl des Körpers $K(\sqrt{\pi})$ bezeichnet, so folgt, daß das Hauptideal $\mathfrak{q}^{hH}$ gleich der Relativnorm des Hauptideals (A) wird, und mithin ist

$$\varepsilon \varkappa^H = N(\mathsf{A}),$$

wenn ε eine geeignete Einheit in k bezeichnet. Da aber nach dem vorhin Bewiesenen eine jede Einheit in k die Relativnorm einer Einheit in $K(\sqrt{\pi})$ ist, so ist auch $\varkappa^H$ die Relativnorm einer ganzen Zahl A^* in $K(\sqrt{\pi})$; folglich ist $\varkappa$ die Relativnorm der Zahl $\frac{\mathsf{A}^*}{\varkappa^{\frac{H-1}{2}}}$, und der Nenner dieses Bruches fällt prim zu 2 aus. Hieraus folgt leicht nach Definition 6 $\left(\frac{\varkappa, \pi}{\mathfrak{l}}\right) = +1$ und mithin wegen (8) auch $\left(\frac{\nu_1, \mu_1}{\mathfrak{l}}\right) = +1$; hiermit ist der Beweis für den Satz 47 im gegenwärtigen Falle erbracht.

Nehmen wir endlich an, es sei jede der beiden Zahlen μ_1, μ_2 das Quadrat einer ganzen Zahl in k, so ergibt sich nach der Definition 6 für die beiden Symbole $\left(\frac{\nu_1, \mu_1}{\mathfrak{l}}\right), \left(\frac{\nu_2, \mu_2}{\mathfrak{l}}\right)$ stets der Wert $+1$ und damit ist der Satz 47 vollständig bewiesen.

Satz 48. (Hilfssatz.) Es sei $\mathfrak{l}$ ein in 2 aufgehendes Primideal und ferner seien ν, μ beliebige zu 2 prime ganze Zahlen in k: wenn dann $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$ ausfällt, so ist auch stets $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$.

Beweis. Wir bezeichnen wie in Satz 40 mit $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ die z voneinander verschiedenen in 2 aufgehenden Primideale und es möge allgemein $\mathfrak{l}_i$ genau zur l_i-ten Potenz in 2 aufgehen, so daß

$$2 = \mathfrak{l}_1^{l_1} \mathfrak{l}_2^{l_2} \ldots \mathfrak{l}_z^{l_z}$$

wird. Nehmen wir sodann $\mathfrak{l} = \mathfrak{l}_1$ und setzen $l = l_1, \mathfrak{L} = \mathfrak{l}_2^{l_2} \ldots \mathfrak{l}_z^{l_z}$, so haben wir

$$2 = \mathfrak{l}^l \mathfrak{L},$$

wo $\mathfrak{L}$ ein durch $\mathfrak{l}$ nicht teilbares Ideal bedeutet.

Es sei nun μ^* eine ganze den Kongruenzen

$$\mu^* \equiv \mu, \qquad (\mathfrak{l}^{2l+1}),$$
$$\mu^* \equiv 1, \qquad (\mathfrak{L}^2)$$

genügende Zahl des Körpers k; wir bestimmen dann zunächst ein Primideal $\mathfrak{p}$ in k derart, daß die Gleichungen

$$\left(\frac{\varepsilon_1}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_1}{\mu^*}\right), \ldots, \left(\frac{\varepsilon_{m-\frac{m}{2}}}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_{m-\frac{m}{2}}}{\mu^*}\right),$$
$$\left(\frac{\lambda_1}{\mathfrak{p}}\right) = \left(\frac{\lambda_1}{\mu^*}\right), \ldots, \left(\frac{\lambda_z}{\mathfrak{p}}\right) = \left(\frac{\lambda_z}{\mu^*}\right)$$

gelten; hierbei sollen $\varepsilon_1, \ldots, \varepsilon_{m-\frac{m}{2}}, \lambda_1, \ldots, \lambda_z$ die Bedeutung wie in Satz 42 haben. Da folglich

$$\left(\frac{\varepsilon_1}{\mathfrak{p}\,\mu^*}\right) = +1, \ldots, \left(\frac{\varepsilon_{m-\frac{m}{2}}}{\mathfrak{p}\,\mu^*}\right) = +1,$$
$$\left(\frac{\lambda_1}{\mathfrak{p}\,\mu^*}\right) = +1, \ldots, \left(\frac{\lambda_z}{\mathfrak{p}\,\mu^*}\right) = +1$$

wird, so können wir nach Satz 43 eine ganze Zahl α derart bestimmen, daß das Ideal (α) gleich $\mathfrak{p}^h \mu^{*h}$ wird und überdies die Zahl α dem Quadrat einer ganzen Zahl in k nach dem Modul $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$ kongruent ausfällt; wir setzen $\pi = \frac{\alpha}{\mu^{*h}}$ und haben dann $(\pi) = \mathfrak{p}^h$.

Andererseits bestimmen wir ein Primideal $\mathfrak{q}$ derart, daß die Gleichungen

$$\left(\frac{\varepsilon_1}{\mathfrak{q}}\right) = \left(\frac{\varepsilon_1}{\nu}\right), \ldots, \left(\frac{\varepsilon_{m-\frac{m}{2}}}{\mathfrak{q}}\right) = \left(\frac{\varepsilon_{m-\frac{m}{2}}}{\nu}\right),$$
$$\left(\frac{\lambda_1}{\mathfrak{q}}\right) = \left(\frac{\lambda_1}{\nu}\right), \ldots, \left(\frac{\lambda_z}{\mathfrak{q}}\right) = \left(\frac{\lambda_z}{\nu}\right),$$
$$\left(\frac{\pi}{\mathfrak{q}}\right) = +1 \qquad (1)$$

gelten. Indem wir wie vorhin verfahren, können wir nach Satz 43 eine ganze Zahl β derart bestimmen, daß das Ideal (β) gleich $\mathfrak{q}^h \nu^h$ wird und überdies die Zahl β dem Quadrat einer ganzen Zahl in k nach dem Modul $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$ kongruent ausfällt; wir setzen $\varkappa = \frac{\beta}{\nu^h}$ und haben dann $(\varkappa) = \mathfrak{q}^h$.

Zufolge Satz 40 haben wir

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu, \alpha}{\mathfrak{w}}\right) = +1, \quad \prod_{(\mathfrak{w})}{}'\left(\frac{\beta, \pi}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \beta}{\mathfrak{w}}\right) = +1,$$

wo die Produkte Π' über sämtliche zu 2 primen Primideale $\mathfrak{w}$ des Körpers k erstreckt werden sollen; mit Rücksicht auf die Definition 17 ergibt sich hieraus

$$\left(\frac{\nu, \alpha}{\mathfrak{l}}\right) = +1, \quad \left(\frac{\beta, \pi}{\mathfrak{l}}\right) = +1,$$

und folglich bei Benutzung der Formeln des Satzes 45

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \left(\frac{\nu, \mu^*}{\mathfrak{l}}\right) = \left(\frac{\nu, \mu^{*h}}{\mathfrak{l}}\right) = \left(\frac{\nu, \pi}{\mathfrak{l}}\right)$$

und

$$\left(\frac{\nu, \pi}{\mathfrak{l}}\right) = \left(\frac{\nu^h, \pi}{\mathfrak{l}}\right) = \left(\frac{\varkappa, \pi}{\mathfrak{l}}\right).$$

Somit erhalten wir schließlich

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \left(\frac{\varkappa, \pi}{\mathfrak{l}}\right)$$

und infolge der Voraussetzung des Satzes 48 ist daher

$$\left(\frac{\varkappa, \pi}{\mathfrak{l}}\right) = +1. \tag{2}$$

Da μ^* und folglich auch die Zahl π dem Quadrat einer ganzen Zahl in k nach dem Modul $\mathfrak{L}^2$ kongruent ist, so nimmt mit Rücksicht auf die Definition 17 die Gleichung (2) die Gestalt

$$\left(\frac{\varkappa, \pi}{\mathfrak{l}}\right) = \left(\frac{\pi}{\mathfrak{q}}\right)\left(\frac{\varkappa}{\mathfrak{p}}\right) = +1$$

an, und hieraus schließen wir wegen (1), daß notwendig

$$\left(\frac{\varkappa}{\mathfrak{p}}\right) = +1 \tag{3}$$

ausfallen muß.

Wir betrachten jetzt den Körper $K(\sqrt{\pi})$ und werden beweisen, daß $\varkappa$ stets gleich der Relativnorm einer solchen Zahl dieses Körpers $K(\sqrt{\pi})$ ist, deren Nenner prim zu 2 ausfällt. Zu dem Zwecke unterscheiden wir folgende drei Fälle:

Erstens nehmen wir an, es sei das Primideal $\mathfrak{p}$ primär und π eine Primärzahl von $\mathfrak{p}$. Die Relativdiskriminante des Körpers $K(\sqrt{\pi})$ enthält dann nur den einen Primfaktor $\mathfrak{p}$, und wir können in diesem Falle genau wie im zweiten Teile des Beweises zu Satz 47 zeigen, daß $\varkappa$ die Relativnorm einer Zahl des Körpers $K(\sqrt{\pi})$ ist, deren Nenner zu 2 prim ausfällt.

Nehmen wir *zweitens* an, es sei $\mathfrak{p}$ ein primäres Primideal; dagegen sei π nicht eine Primärzahl von $\mathfrak{p}$, sondern es sei vielmehr $\pi = \varepsilon\pi^*$, wobei π^* eine Primärzahl von $\mathfrak{p}$ und ε eine Einheit in k bedeutet, welche nicht gleich dem Quadrat einer Einheit in k ausfällt. Die Relativdiskriminante des Körpers $K(\sqrt{\pi})$ enthält, da π dem Quadrat einer ganzen Zahl in k nach $\mathfrak{L}^2$ kongruent ist, wegen Satz 4 lediglich die beiden Primideale $\mathfrak{l}$ und $\mathfrak{p}$. Setzen wir in Satz 23 $t = 2$ ein, so folgt aus demselben wegen $v \leqq \frac{m}{2}$ die Ungleichung $a \leqq 1$, d. h. die Anzahl $\mathrm{A} = 2^a$ aller ambigen Komplexe des Körpers $K(\sqrt{\pi})$ ist höchstens gleich 2.

Es sei nun $\mathfrak{J}$ irgendein Ideal in $K(\sqrt{\pi})$ und $\mathfrak{j} = N(\mathfrak{J})$ die Relativnorm von $\mathfrak{J}$; wir setzen ferner $\mathfrak{j}^h = (\iota)$, wo ι eine ganze Zahl in k bedeutet: fällt dann $\left(\frac{\iota}{\mathfrak{p}}\right) = +1$ aus, so bezeichnen wir denjenigen Komplex des Körpers $K(\sqrt{\pi})$, zu welchem $\mathfrak{J}$ gehört, als einen Komplex des Hauptgeschlechtes in $K(\sqrt{\pi})$. Wir können leicht beweisen, daß nicht sämtliche Komplexe in $K(\sqrt{\pi})$ Komplexe des Hauptgeschlechtes sind. Es sei nämlich $\mathfrak{r}$ ein Primideal in k, für welches

$$\left(\frac{\pi}{\mathfrak{r}}\right) = +1 \quad \text{und} \quad \left(\frac{\pi^*}{\mathfrak{r}}\right) = -1$$

ausfällt. Wegen der ersteren Gleichung ist $\mathfrak{r}$ in $K(\sqrt{\pi})$ weiter zerlegbar; es bedeute $\mathfrak{R}$ einen Primfaktor von $\mathfrak{r}$ in $K(\sqrt{\pi})$. Wird $\mathfrak{r}^h = (\varrho)$ gesetzt, wo ϱ eine ganze Zahl in k darstellt, so erhalten wir nach Satz 37

$$\left(\frac{\varrho}{\mathfrak{p}}\right) = \left(\frac{\pi^*}{\mathfrak{r}}\right) = -1,$$

und diese Gleichung zeigt, daß der durch $\mathfrak{R}$ bestimmte Komplex in $K(\sqrt{\pi})$ nicht ein Komplex des Hauptgeschlechtes ist.

Wir bezeichnen nun mit f' die Anzahl derjenigen Komplexe in $K(\sqrt{\pi})$, welche Quadrate von Komplexen in $K(\sqrt{\pi})$ sind, und mit f die Anzahl aller Komplexe des Hauptgeschlechtes in $K(\sqrt{\pi})$; dann erkennen wir genau wie im Beweise zu Satz 25 die Richtigkeit der Gleichung

$$\mathrm{A}\, f' = 2\, f. \tag{4}$$

Aus dieser Gleichung folgt wegen $\mathrm{A} \leqq 2$ die Ungleichung $f \leqq f'$. Da ferner jedes Quadrat eines Komplexes notwendig ein Komplex des Hauptgeschlechtes sein muß, so ist auch $f' \leqq f$ und mithin haben wir $f = f'$, d. h. jeder Komplex des Hauptgeschlechtes ist gleich dem Quadrat eines Komplexes. Aus $f = f'$ folgt ferner wegen (4) zugleich $\mathrm{A} = 2$ und $a = 1$; mit Rücksicht auf Satz 23 entnehmen wir hieraus $v = \frac{m}{2}$, d. h. jede Einheit des Körpers k ist gleich der Relativnorm einer ganzen oder gebrochenen Zahl des Körpers $K(\sqrt{\pi})$.

Um nun zu zeigen, daß $\varkappa$ gleich der Relativnorm einer Zahl in $K(\sqrt{\pi})$ ist, bedenken wir, daß wegen (1) das Primideal $\mathfrak{q}$ in $K(\sqrt{\pi})$ weiter zerlegbar ist; die Gleichung (3) zeigt sodann, daß jedes in $\mathfrak{q}$ enthaltene Primideal $\mathfrak{Q}$ des Körpers $K(\sqrt{\pi})$ einem Komplex des Hauptgeschlechtes angehört, und da nach dem vorhin Bewiesenen jeder solche Komplex gleich dem Quadrat eines Komplexes ist, so genügt das Ideal $\mathfrak{Q}$ einer Gleichung von der Gestalt

$$\mathfrak{Q} = \mathfrak{J}^2 \mathrm{A}\, \mathfrak{j},$$

wobei $\mathfrak{J}$ ein Ideal in $K(\sqrt{\pi})$, A eine Zahl in $K(\sqrt{\pi})$ und $\mathfrak{j}$ ein Ideal in k bedeutet. Bilden wir nun auf beiden Seiten dieser Gleichung die Relativnorm und erheben sie dann in die h-te Potenz, so entsteht eine Gleichung von der Gestalt

$$(\varkappa) = N(\mathrm{A})\{N(\mathfrak{J}) \cdot \mathfrak{j}\}^{2h} = N(\mathrm{A})(\gamma)^2,$$

wobei γ eine geeignete ganze Zahl in k ist und aus dieser Gleichung entnehmen wir die Gleichung

$$\xi\varkappa = N(\gamma\mathfrak{A}),$$

wo ξ eine Einheit in k bedeutet. Da nach dem vorhin Bewiesenen jede Einheit in k die Relativnorm einer Zahl in $K(\sqrt{\pi})$ ist, so zeigt die letzte Gleichung, daß auch $\varkappa$ die Relativnorm einer gewissen Zahl in $K(\sqrt{\pi})$ sein muß. Durch eine einfache Betrachtung erkennen wir sodann, daß $\varkappa$ sich jedenfalls auch als Relativnorm einer solchen Zahl muß darstellen lassen, deren Nenner zu 2 prim ist.

Wir nehmen *drittens* an, es wäre $\mathfrak{p}$ ein nichtprimäres Primideal in k und ζ eine Einheit, für welche $\left(\frac{\zeta}{\mathfrak{p}}\right) = -1$ wird. In diesem Falle kann ζ sicher nicht die Relativnorm einer ganzen oder gebrochenen Zahl in $K(\sqrt{\pi})$ sein; es ist mithin die in Satz 23 mit v bezeichnete Anzahl hier $\leqq \frac{m}{2} - 1$. Da π dem Quadrat einer ganzen Zahl in k nach dem Modul $\mathfrak{Q}^2$ kongruent wird, so ist die Relativdiskriminante des Körpers $K(\sqrt{\pi})$ nach Satz 4 prim zu $\mathfrak{Q}$ und enthält daher wiederum nur die beiden Primfaktoren $\mathfrak{p}$ und $\mathfrak{l}$. Setzen wir in Satz 23 $t = 2$ ein, so folgt aus demselben wegen $v \leqq \frac{m}{2} - 1$ die Ungleichung $a \leqq 0$, d. h. es ist $a = 0$ und $v = \frac{m}{2} - 1$. Es machen nun die Gesamtheit aller Einheiten ξ, für welche $\left(\frac{\xi}{\mathfrak{p}}\right) = +1$ ausfällt, offenbar genau $2^{\frac{m}{2}-1}$ Einheitenverbände des Körpers k aus und da diejenigen $2^{\frac{m}{2}-1}$ Verbände von Einheiten η, für welche $\left(\frac{\eta}{\mathfrak{p}}\right) = -1$ ausfällt, gewiß nicht Einheiten enthalten dürfen, die Relativnormen von Zahlen sind, so folgt, daß alle Einheiten ξ mit der Eigenschaft $\left(\frac{\xi}{\mathfrak{p}}\right) = +1$ notwendig Relativnormen von Zahlen des Körpers $K(\sqrt{\pi})$ sind.

Aus der Gleichung $a = 0$ folgt ferner, daß im Körper $K(\sqrt{\pi})$ der einzige ambige Komplex der Hauptkomplex ist und hieraus schließen wir, wie im zweiten Teil des Beweises zu Satz 47, daß die Klassenanzahl H des Körpers $K(\sqrt{\pi})$ notwendig ungerade sein muß. Auch erkennen wir, wie dort, daß, wenn ε eine geeignete Einheit in k bezeichnet, die Zahl $\varepsilon\varkappa^H$ gleich der Relativnorm einer gewissen ganzen Zahl in $K(\sqrt{\pi})$ sein muß. Infolgedessen besteht die Gleichung

$$\left(\frac{\varepsilon\varkappa^H}{\mathfrak{p}}\right) = +1;$$

wegen (3) muß hiernach auch $\left(\frac{\varepsilon}{\mathfrak{p}}\right) = +1$ sein, und nach dem Vorigen ist mithin ε die Relativnorm einer Zahl in $K(\sqrt{\pi})$. Hieraus schließen wir, daß auch $\varkappa^H$ die Relativnorm einer Zahl in $K(\sqrt{\pi})$ sein muß und folglich ist $\varkappa$ die Relativnorm einer Zahl in $K(\sqrt{\pi})$ und insbesondere auch einer solchen Zahl, deren Nenner zu 2 prim ist.

In allen drei soeben behandelten Fällen ist mithin nach Definition 6 gewiß

$$\left(\frac{\varkappa, \pi}{\mathfrak{l}}\right) = +1.$$

Wir hatten nun zu Beginn des Beweises $\alpha = \pi\mu^{*h}$ und sodann $\beta = \varkappa\nu^h$ als ganze Zahlen in k derart bestimmt, daß sie Quadraten ganzer Zahlen in k nach $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$ kongruent ausfielen. Da ferner $\mu^* \equiv \mu$ nach $\mathfrak{l}^{2l+1}$ ist, so folgt nach Satz 47

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \left(\frac{\varkappa, \pi}{\mathfrak{l}}\right) = +1;$$

damit ist der Satz 48 vollständig bewiesen.

Satz 49. (Hilfssatz.) Es sei $\mathfrak{l}$ ein in 2 aufgehendes Primideal und ferner seien ν, μ beliebige zu 2 prime ganze Zahlen in k: wenn dann $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$ ausfällt, so ist auch stets $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$.

Beweis. Wir wenden die am Anfang des Beweises zu Satz 48 erläuterten Bezeichnungen an und bestimmen eine ganze Zahl μ^*, welche den Kongruenzen

$$\mu^* \equiv \mu, \quad (\mathfrak{l}_1^{2l_1+1}),$$
$$\mu^* \equiv 1, \quad (\mathfrak{l}_2^{2l_2+1}\mathfrak{l}_3^{2l_3+1} \ldots \mathfrak{l}_z^{2l_z+1})$$

genügt und nicht zugleich das Quadrat einer ganzen Zahl in k ist; dann haben wir wegen Satz 47

$$\left(\frac{\nu, \mu^*}{\mathfrak{l}_1}\right) = \left(\frac{\nu, \mu}{\mathfrak{l}_1}\right) = +1,$$
$$\left(\frac{\nu, \mu^*}{\mathfrak{l}_i}\right) = \left(\frac{\nu, 1}{\mathfrak{l}_i}\right) = +1, \quad (i = 2, 3, \ldots, z);$$

infolgedessen gibt es gewisse ganze Zahlen $\mathfrak{A}_1, \ldots, \mathfrak{A}_z$ im Körper $K(\sqrt{\mu^*})$ derart, daß

$$\nu \equiv N(\mathfrak{A}_1), \quad (\mathfrak{l}_1^{2l_1}),$$
$$\ldots\ldots\ldots\ldots$$
$$\nu \equiv N(\mathfrak{A}_z), \quad (\mathfrak{l}_z^{2l_z})$$

ausfällt. Wenn wir daher eine ganze Zahl $\mathfrak{A}$ in $K(\sqrt{\mu^*})$ bestimmen, die zugleich den z Kongruenzen

$$\mathfrak{A} \equiv \mathfrak{A}_1, \quad (\mathfrak{l}_1^{2l_1}),$$
$$\ldots\ldots\ldots$$
$$\mathfrak{A} \equiv \mathfrak{A}_z, \quad (\mathfrak{l}_z^{2l_z})$$

genügt, so wird auch

$$\nu = N(\mathfrak{A}), \qquad (\mathfrak{l}_1^{2l_1}\mathfrak{l}_2^{2l_2} \ldots \mathfrak{l}_z^{2l_z})$$

und vermöge des Satzes 36 schließen wir hieraus leicht

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu, \mu^*}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{N(\mathfrak{A}), \mu^*}{\mathfrak{w}}\right),$$

wo die Produkte Π' über alle zu 2 primen Primideale $\mathfrak{w}$ in k zu erstrecken sind; nach der Definition 17 ist das Produkt linker Hand gleich $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$. Da nun nach Definition 6 sämtliche Faktoren des Produktes rechter Hand den Wert $+1$ haben, so folgt $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$, womit der Satz 49 vollständig bewiesen ist. Die beiden Sätze 48 und 49 zusammengenommen ergeben das folgende Resultat:

Satz 50. (Hilfssatz.) Wenn $\mathfrak{l}$ irgendein in 2 aufgehendes Primideal und ferner ν, μ irgendwelche zu 2 prime ganze Zahlen in k bedeuten, dann gilt stets die Gleichung

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \left(\frac{\nu, \mu}{\mathfrak{l}}\right).$$

§ 34. Die Eigenschaften des Symbols $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ für irgendwelche zu 2 prime ganze Zahlen ν, μ.

Mit Hilfe des Satzes 50 können wir die wichtige Tatsache beweisen, daß die in Satz 14 aufgestellten Formeln auch für jedes in 2 aufgehende Primideal $\mathfrak{l}$ gültig sind. Wir sprechen den Satz aus:

Satz 51. Wenn $\nu, \nu_1, \nu_2, \mu, \mu_1, \mu_2$ beliebige zu 2 prime ganze Zahlen in k sind, so gelten in bezug auf jedes in 2 aufgehende Primideal $\mathfrak{l}$ des Körpers k die Formeln

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \left(\frac{\mu, \nu}{\mathfrak{l}}\right),$$

$$\left(\frac{\nu_1 \nu_2, \mu}{\mathfrak{l}}\right) = \left(\frac{\nu_1, \mu}{\mathfrak{l}}\right)\left(\frac{\nu_2, \mu}{\mathfrak{l}}\right),$$

$$\left(\frac{\nu, \mu_1 \mu_2}{\mathfrak{l}}\right) = \left(\frac{\nu, \mu_1}{\mathfrak{l}}\right)\left(\frac{\nu, \mu_2}{\mathfrak{l}}\right).$$

Beweis. Es mögen $\mathfrak{l}$ und $\mathfrak{L}$ die Bedeutung wie in Definition 17 haben. Um die erste Formel des Satzes 51 zu beweisen, bestimmen wir zwei ganze Zahlen ν^*, μ^* in k von der Art, daß

$$\left.\begin{aligned} \nu^* &\equiv \nu \\ \mu^* &\equiv \mu \end{aligned}\right\}, \qquad (\mathfrak{l}^{2l+1})$$

$$\left.\begin{aligned} \nu^* &\equiv 1 \\ \mu^* &\equiv 1 \end{aligned}\right\}, \qquad (\mathfrak{L}^2)$$

wird. Nach Satz 47 ist dann

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \left(\frac{\nu^*, \mu}{\mathfrak{l}}\right), \quad \left(\frac{\mu, \nu}{\mathfrak{l}}\right) = \left(\frac{\mu^*, \nu}{\mathfrak{l}}\right)$$

und folglich wegen Satz 50 auch

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \left(\frac{\nu^*, \mu}{\mathfrak{l}}\right), \quad \left(\frac{\mu, \nu}{\mathfrak{l}}\right) = \left(\frac{\mu^*, \nu}{\mathfrak{l}}\right). \qquad (1)$$

Nun ist nach Definition 17

$$\left(\frac{\nu^*, \mu}{\mathfrak{l}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*, \mu^*}{\mathfrak{w}}\right), \quad \left(\frac{\mu^*, \nu}{\mathfrak{l}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\mu^*, \nu^*}{\mathfrak{w}}\right), \qquad (2)$$

und da nach der ersten Formel in Satz 14 für jedes zu 2 prime Primideal $\mathfrak{w}$

$$\left(\frac{\nu^*, \mu^*}{\mathfrak{w}}\right) = \left(\frac{\mu^*, \nu^*}{\mathfrak{w}}\right)$$

ausfällt, so folgt aus (2) auch

$$\left(\frac{\nu^*, \mu}{\mathfrak{l}}\right) = \left(\frac{\mu^*, \nu}{\mathfrak{l}}\right)$$

und daher wegen (1) auch

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

diese Gleichung lehrt mit Rücksicht auf Satz 50 die Richtigkeit der ersten Formeln des zu beweisenden Satzes 51.

Die beiden letzten Formeln des Satzes 51 folgen unmittelbar aus den Sätzen 45 und 50.

§ 35. Das Produkt $\prod_{(\mathfrak{w})}\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$ für irgendwelche zu 2 prime Zahlen ν, μ.

Wir sind nunmehr imstande, einen Satz zu beweisen, der eine wesentliche Verallgemeinerung des Satzes 36 darstellt.

Satz 52. *Wenn ν, μ irgendwelche zu 2 prime ganze Zahlen in k sind, so ist stets*

$$\prod_{(\mathfrak{w})}\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = +1,$$

wo das Produkt über sämtliche Primideale $\mathfrak{w}$ des Körpers k erstreckt werden soll.

Beweis. Wir wenden die in Satz 40 erläuterten Bezeichnungen an und bestimmen z ganze Zahlen $\mu_1, \mu_2, \ldots, \mu_z$ in k, so daß die Kongruenzen

$$\left.\begin{aligned} &\mu_1 \equiv \mu, \ \mu_2 \equiv 1, \ \ldots, \mu_z \equiv 1, \quad (\mathfrak{l}_1^{2l_1}), \\ &\mu_1 \equiv 1, \ \mu_2 \equiv \mu, \ \ldots, \mu_z \equiv 1, \quad (\mathfrak{l}_2^{2l_2}), \\ &\qquad \ldots\ldots\ldots\ldots\ldots\ldots \\ &\mu_1 \equiv 1, \ \mu_2 \equiv 1, \ \ldots, \mu_z \equiv \mu, \quad (\mathfrak{l}_z^{2l_z}) \end{aligned}\right\} \qquad (1)$$

gelten; dann genügt offenbar das Produkt dieser z Zahlen der Kongruenz

$$\mu_1 \mu_2 \cdots \mu_z \equiv \mu, \qquad (\mathfrak{L}^2). \qquad (2)$$

Die Definition 17 liefert mit Rücksicht auf die Kongruenzen (1) die Gleichungen

$$\left(\frac{\nu, \mu}{\mathfrak{l}_i}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\nu, \mu_i}{\mathfrak{w}}\right), \quad (i = 1, 2, \ldots, z)$$

und wegen Satz 50 folgt hieraus das weitere System von z Gleichungen

$$\left(\frac{\nu, \mu}{\mathfrak{l}_i}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\nu, \mu_i}{\mathfrak{w}}\right), \quad (i = 1, 2, \ldots, z); \tag{3}$$

dabei ist das Produkt Π' über alle zu 2 primen Primideale $\mathfrak{w}$ in k zu erstrecken. Multiplizieren wir die z Gleichungen (3) miteinander, so entsteht die Gleichung

$$\left(\frac{\nu, \mu}{\mathfrak{l}_1}\right)\left(\frac{\nu, \mu}{\mathfrak{l}_2}\right) \cdots \left(\frac{\nu, \mu}{\mathfrak{l}_z}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\nu, \mu_1 \mu_2 \cdots \mu_z}{\mathfrak{w}}\right)$$

und durch Multiplikation mit $\prod_{(\mathfrak{w})}{}'\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$ erhalten wir hieraus die Gleichung

$$\prod_{(\mathfrak{w})}\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\nu, \mu\, \mu_1 \mu_2 \cdots \mu_z}{\mathfrak{w}}\right), \tag{4}$$

wo rechter Hand das Produkt Π' über alle zu 2 primen Primideale $\mathfrak{w}$, dagegen linker Hand das Produkt Π über sämtliche Primideale $\mathfrak{w}$ in k genommen werden soll. Nun wird wegen der Kongruenz (2) die Zahl $\mu\, \mu_1\, \mu_2 \ldots \mu_z$ dem Quadrat einer ganzen Zahl in k kongruent nach 2^2 und folglich ist gemäß Satz 36 die rechte Seite von (4) gleich $+1$; damit ist der Beweis für Satz 52 erbracht.

§ 36. Der erste Ergänzungssatz und das allgemeine Reziprozitätsgesetz für quadratische Reste.

Wir heben einige besonders wichtige Folgerungen des Satzes 52 hervor.

Satz 53. *Es seien $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ die in 2 aufgehenden Primideale des Körpers k und ε bedeute irgendeine Einheit in k; ferner sei $\mathfrak{p}$ ein zu 2 primes Primideal und π eine ganze Zahl in k, so daß $(\pi) = \mathfrak{p}^h$ ausfällt: dann gilt stets die Gleichung*

$$\left(\frac{\varepsilon}{\mathfrak{p}}\right) = \left(\frac{\varepsilon, \pi}{\mathfrak{l}_1}\right)\left(\frac{\varepsilon, \pi}{\mathfrak{l}_2}\right) \cdots \left(\frac{\varepsilon, \pi}{\mathfrak{l}_z}\right).$$

Dieser Satz 53 heiße der *erste Ergänzungssatz zum allgemeinen Reziprozitätsgesetze für quadratische Reste im Körper k*.

Satz 54. *Es seien $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ die in 2 aufgehenden Primideale des Körpers k; ferner seien $\mathfrak{p}, \mathfrak{q}$ irgend zwei zu 2 prime Primideale und $\pi, \varkappa$ ganze Zahlen in k, so daß $(\pi) = \mathfrak{p}^h$, $(\varkappa) = \mathfrak{q}^h$ wird: dann gilt die Gleichung*

$$\left(\frac{\pi}{\mathfrak{q}}\right)\left(\frac{\varkappa}{\mathfrak{p}}\right) = \left(\frac{\pi, \varkappa}{\mathfrak{l}_1}\right)\left(\frac{\pi, \varkappa}{\mathfrak{l}_2}\right) \cdots \left(\frac{\pi, \varkappa}{\mathfrak{l}_z}\right).$$

Der Satz 54 heiße das *allgemeine Reziprozitätsgesetz für quadratische Reste im Körper k*.

Wir können die Sätze 53 und 54 unmittelbar aus Satz 52 herleiten, indem wir in Satz 52 zunächst $\nu = \varepsilon, \mu = \pi$ und dann $\nu = \pi, \mu = \varkappa$ wählen.

§ 37. Das Symbol $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ für beliebige ganze Zahlen ν, μ.

Wir dehnen nunmehr die Bedeutung des in Definition 17 eingeführten Symbols $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ auf den Fall aus, daß ν, μ beliebige ganze Zahlen in k sind; das so verallgemeinerte Symbol wird sich wiederum als gleichbedeutend mit dem allgemeinen Symbol $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ erweisen.

Definition 18. Es seien wie bisher $\mathfrak{l}_1 = \mathfrak{l}, \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ die voneinander verschiedenen Primfaktoren von 2 und es gehe das Primideal $\mathfrak{l}_1 = \mathfrak{l}$ genau zur $l_1 = l$-ten, ferner gehen die Primideale $\mathfrak{l}_2, \ldots, \mathfrak{l}_z$ bez. zur $l_2, \ldots, l_z$-ten Potenz in 2 auf; endlich seien ν, μ beliebige ganze Zahlen in k und es gehe in μ genau die a-te Potenz von $\mathfrak{l}$ auf: dann wird das Symbol $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ durch die Gleichung

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\nu, \mu^*}{\mathfrak{w}}\right)$$

definiert; hierin ist das Produkt $\prod_{(\mathfrak{w})}{}'$ über alle zu 2 primen Primideale $\mathfrak{w}$ zu erstrecken und μ^* soll eine solche ganze Zahl sein, die den Kongruenzen

$$\mu^* \equiv \mu, \qquad (\mathfrak{l}^{2l+1+a}),$$
$$\mu^* \equiv \alpha^2, \qquad (\mathfrak{l}_2^{2l_2+1} \ldots \mathfrak{l}_z^{2l_z+1})$$

genügt, wo α irgendeine ganze zu $\mathfrak{l}_2, \mathfrak{l}_3, \ldots, \mathfrak{l}_z$ prime Zahl in k bedeutet.

Wir zeigen wie in § 32, indem wir statt des dort benutzten Satzes 36 nunmehr den Satz 40 anwenden, daß das Symbol $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ durch die getroffenen Festsetzungen eindeutig bestimmt ist.

Aus der Definition 18 entnehmen wir leicht mit Benutzung der beiden letzten Formeln in Satz 14 die folgende dem Satz 45 entsprechende Tatsache:

Satz 55. (Hilfssatz). Wenn $\nu, \nu_1, \nu_2, \mu, \mu_1, \mu_2$ beliebige ganze Zahlen in k sind, so gelten in bezug auf ein jedes in 2 aufgehende Primideal $\mathfrak{l}$ die Formeln

$$\left(\frac{\nu_1 \nu_2, \mu}{\mathfrak{l}}\right) = \left(\frac{\nu_1, \mu}{\mathfrak{l}}\right)\left(\frac{\nu_2, \mu}{\mathfrak{l}}\right),$$
$$\left(\frac{\nu, \mu_1 \mu_2}{\mathfrak{l}}\right) = \left(\frac{\nu, \mu_1}{\mathfrak{l}}\right)\left(\frac{\nu, \mu_2}{\mathfrak{l}}\right).$$

§ 38. Die Übereinstimmung der beiden Symbole $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ und $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ für beliebige ganze Zahlen ν, μ.

Um die Übereinstimmung der beiden Symbole $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ und $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ für beliebige ganze Zahlen ν, μ zu erkennen, bedienen wir uns der folgenden Entwicklungen:

Satz 56. (Hilfssatz). Es sei $\mathfrak{l}$ ein Primfaktor von 2 im Körper k und es gehe $\mathfrak{l}$ in 2 genau zur l-ten Potenz auf; ferner seien $\nu_1, \nu_2, \mu_1, \mu_2$ ganze Zahlen in k und es gehe in diesen Zahlen das Primideal $\mathfrak{l}$ bez. genau zur b_1, b_2, a_1, a_2-ten

Potenz auf, wobei $b_2 \leqq b_1$, $a_2 \leqq a_1$ ausfallen möge: wenn es dann in k gewisse ganze Zahlen α, β gibt, für welche die Kongruenzen

$$\nu_1 \equiv \alpha^2 \nu_2, \qquad (\mathfrak{l}^{2l+1+b_1}),$$
$$\mu_1 \equiv \beta^2 \mu_2, \qquad (\mathfrak{l}^{2l+1+a_1})$$

gelten, so ist stets

$$\left(\frac{\nu_1, \mu_1}{\mathfrak{l}}\right) = \left(\frac{\nu_2, \mu_2}{\mathfrak{l}}\right).$$

Den Beweis dieses Hilfssatzes führen wir leicht, indem wir uns der nämlichen Schlüsse wie beim Beweise des entsprechenden Satzes 47 bedienen.

Satz 57. (Hilfssatz.) Es sei $\mathfrak{l}$ ein in 2 aufgehendes Primideal des Körpers k und ferner seien ν, μ beliebige ganze Zahlen ($\neq 0$) in k: wenn dann $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$ ausfällt, so ist auch stets $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$.

Beweis. Wir benutzen die in Definition 18 erläuterten Bezeichnungen. Es sind zwei Fälle gesondert zu behandeln, je nachdem der Exponent a, zu dem $\mathfrak{l}$ in μ aufgeht, gerade oder ungerade ausfällt.

Im *ersteren* Falle bezeichnen wir mit $\bar{\lambda}$ irgendeine durch $\mathfrak{l}^{\frac{a}{2}}$, aber durch keine höhere Potenz von $\mathfrak{l}$ teilbare und zu $\mathfrak{l}_2, \mathfrak{l}_3, \ldots, \mathfrak{l}_z$ prime ganze Zahl in k und bestimmen dann eine ganze Zahl μ^* in k derart, daß sie die Kongruenzen

$$\bar{\lambda}^2 \mu^* \equiv \mu, \qquad (\mathfrak{l}^{2l+1+a}),$$
$$\mu^* \equiv 1, \qquad (\mathfrak{l}_2^{2l_2+1} \mathfrak{l}_3^{2l_3+1} \ldots \mathfrak{l}_z^{2l_z+1}) \tag{1}$$

erfüllt und nicht zugleich das Quadrat einer Zahl in k ist; es ist dann μ^* eine zu 2 prime Zahl und nach Definition 18 wird

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \bar{\lambda}^2 \mu^*}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu^*}{\mathfrak{w}}\right),$$

wo die Produkte $\prod_{(\mathfrak{w})}{}'$ über alle zu 2 primen Primideale $\mathfrak{w}$ in k zu erstrecken sind. Wegen der Voraussetzung des Satzes 57 haben wir mithin

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu^*}{\mathfrak{w}}\right) = +1. \tag{2}$$

Wir wollen nun aus (2) beweisen, daß der Exponent b, zu dem $\mathfrak{l}$ in ν aufgeht, sicher dann gerade ausfallen muß, wenn das Ideal $\mathfrak{l}$ des Körpers k auch in $K(\sqrt{\mu^*})$ Primideal bleibt. Zu dem Zwecke nehmen wir an, es bliebe $\mathfrak{l}$ in $K(\sqrt{\mu^*})$ Primideal. Wir bestimmen sodann ein Primideal $\mathfrak{p}$, für welches die Gleichungen

$$\left(\frac{\varepsilon_1}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_1}{\mu^*}\right), \ldots, \left(\frac{\varepsilon_m}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_m}{\mu^*}\right), \tag{3}$$
$$\left(\frac{\lambda_1}{\mathfrak{p}}\right) = \left(\frac{\lambda_1}{\mu^*}\right), \ldots, \left(\frac{\lambda_z}{\mathfrak{p}}\right) = \left(\frac{\lambda_z}{\mu^*}\right) \tag{4}$$

erfüllt sind, wobei $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m$, $\lambda_1, \lambda_2, \ldots, \lambda_z$ die in Satz 42 erklärte Bedeutung haben mögen. Da $\mathfrak{l}$ im Körper $K(\sqrt{\mu^*})$ unzerlegbar sein soll, so ist nach Satz 4 und 6 μ^* kongruent dem Quadrat einer ganzen Zahl in k nach dem Modul $\mathfrak{l}_1^{2l}$ und folglich wegen (1) auch nach 2^2; mithin gelten nach Satz 39 die Gleichungen

$$\left(\frac{\varepsilon_1}{\mu^*}\right) = +1, \ldots, \left(\frac{\varepsilon_m}{\mu^*}\right) = +1$$

und wegen (3) ist daher $\mathfrak{p}$ ein primäres Primideal. Bezeichnet π eine Primärzahl von $\mathfrak{p}$, so ist, wie man aus (3), (4) vermöge Satz 43 unter Hinzuziehung von Satz 28 erkennt, $\pi\mu^*$ dem Quadrat einer ganzen Zahl in k nach $\mathfrak{l}_1^{2l_1+1} \mathfrak{l}_2^{2l_2+1} \ldots \mathfrak{l}_z^{2l_z+1}$ kongruent; es ist folglich wegen (1) π gewiß dem Quadrat einer ganzen Zahl in k nach $\mathfrak{l}_2^{2l_2+1} \ldots \mathfrak{l}_z^{2l_z+1}$ kongruent und nach Satz 8 zerfällt daher jedes der Primideale $\mathfrak{l}_2, \mathfrak{l}_3, \ldots, \mathfrak{l}_z$ im Körper $K(\sqrt{\pi})$ in zwei Primfaktoren. Im Beweise zu Satz 34 ist gezeigt worden, daß alle Ideale des Körpers $K(\sqrt{\pi})$ dem Hauptgeschlechte angehören. Die Charaktere der in $\mathfrak{l}_2, \mathfrak{l}_3, \ldots, \mathfrak{l}_z$ enthaltenen Primfaktoren des Körpers $K(\sqrt{\pi})$ müssen somit sämtlich $+1$ sein, d. h. es gelten die Gleichungen

$$\left(\frac{\lambda_2}{\mathfrak{p}}\right) = +1, \left(\frac{\lambda_3}{\mathfrak{p}}\right) = +1, \ldots, \left(\frac{\lambda_z}{\mathfrak{p}}\right) = +1.$$

Würde nun auch $\left(\frac{\lambda_1}{\mathfrak{p}}\right) = +1$ ausfallen, so müßte nach Satz 43 die Primärzahl π und folglich auch die Zahl μ^* kongruent dem Quadrat einer ganzen Zahl in k nach $\mathfrak{l}_1^{2l_1+1} \mathfrak{l}_2^{2l_2+1} \ldots \mathfrak{l}_z^{2l_z+1}$ sein und dann zerfiele nach Satz 8 das Primideal $\mathfrak{l} = \mathfrak{l}_1$ im Körper $K(\sqrt{\mu^*})$ in zwei Primfaktoren, was unserer Annahme entgegen ist. Es ist mithin notwendigerweise

$$\left(\frac{\lambda_1}{\mathfrak{p}}\right) = -1. \tag{5}$$

Nunmehr setzen wir

$$(\nu) = \mathfrak{n}\, \mathfrak{l}^b \mathfrak{l}_0^{b_2} \ldots \mathfrak{l}_z^{b_z},$$

so daß $\mathfrak{n}$ prim zu 2 ist und $b_2, \ldots, b_z$ gewisse ganze rationale Exponenten bedeuten; es folgt dann

$$\nu^h \equiv \nu^* \lambda_1^b \lambda_2^{b_2} \lambda_3^{b_3} \ldots \lambda_z^{b_z},$$

wobei ν^* eine zu 2 prime ganze Zahl in k darstellt. Nach Satz 40 haben wir

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\nu^h, \pi\mu^*}{\mathfrak{w}}\right) = +1.$$

Ferner ist mit Rücksicht auf (2)

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\nu^h, \pi\mu^*}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu^h, \pi}{\mathfrak{w}}\right) \prod_{(\mathfrak{w})}{}' \left(\frac{\nu^h, \mu^*}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu^h, \pi}{\mathfrak{w}}\right);$$

es wird daher

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\nu^h, \pi}{\mathfrak{w}}\right) = +1. \tag{6}$$

Andererseits erhalten wir, da nach Satz 36

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*, \pi}{\mathfrak{w}}\right) = +1$$

ausfällt, die Gleichung

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^h, \pi}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*, \pi}{\mathfrak{w}}\right) \prod_{(\mathfrak{w})}{}'\left(\frac{\lambda_1, \pi}{\mathfrak{w}}\right)^b \prod_{(\mathfrak{w})}{}'\left(\frac{\lambda_2, \pi}{\mathfrak{w}}\right)^{b_2} \cdots \prod_{(\mathfrak{w})}{}'\left(\frac{\lambda_z, \pi}{\mathfrak{w}}\right)^{b_z}$$
$$= \prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*, \pi}{\mathfrak{w}}\right) \cdot \left(\frac{\lambda_1}{\mathfrak{p}}\right)^b \left(\frac{\lambda_2}{\mathfrak{p}}\right)^{b_2} \cdots \left(\frac{\lambda_z}{\mathfrak{p}}\right)^{b_z} = \left(\frac{\lambda_1}{\mathfrak{p}}\right)^b;$$

wegen (5) und (6) entnehmen wir hieraus

$$(-1)^b = +1,$$

d. h. b ist eine gerade Zahl.

Damit ist unsere Behauptung bewiesen und es muß mithin entweder das Primideal $\mathfrak{l}$ des Körpers k in $K(\sqrt{\mu^*})$ weiter zerlegbar sein oder der Exponent b, zu dem $\mathfrak{l}$ in ν aufgeht, gerade ausfallen. In beiden Fällen aber kann, wie leicht ersichtlich, eine ganze Zahl A im Körper $K(\sqrt{\mu^*})$ gefunden werden, derart, daß $\frac{\nu}{N(\mathsf{A})}$ gleich einem Bruche $\frac{\varrho}{\sigma}$ wird, dessen Zähler ϱ und dessen Nenner σ zu 2 prim ausfallen, und aus (2) schließen wir dann

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varrho\,\sigma, \mu^*}{\mathfrak{w}}\right) = +1.$$

Diese Gleichung erhält mit Rücksicht auf die Definition 17 die Gestalt

$$\left(\frac{\varrho\,\sigma, \mu^*}{\mathfrak{l}}\right) = +1$$

und folglich ist nach Satz 50 auch

$$\left(\frac{\varrho\sigma, \mu^*}{\mathfrak{l}}\right) = +1,$$

d. h. $\varrho\sigma$ ist Normenrest im Körper $K(\sqrt{\mu^*})$ nach $\mathfrak{l}$ und folglich ist wegen Satz 56 auch $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$. Damit ist der Satz 57 in dem Falle bewiesen, daß der Exponent a gerade ausfällt.

Wir machen *zweitens* die Annahme, daß der Exponent a ungerade ist und benutzen wiederum die Bezeichnungen wie in Satz 42. Wir bestimmen dann eine ganze zu 2 prime Zahl μ^* in k, für welche die Kongruenzen

$$\lambda_1^a \mu^* \equiv \mu^h, \qquad (\mathfrak{l}^{2l+1+ah}),$$
$$\lambda_1^a \mu^* \equiv 1\ , \qquad (\mathfrak{l}_0^{2l_0+1}\mathfrak{l}_3^{2l_3+1} \ldots \mathfrak{l}_z^{2l_z+1})$$

bestehen. Es sei ferner $\mathfrak{p}$ ein Primideal in k, welches den Bedingungen

$$\left(\frac{\varepsilon_1}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_1}{\mu^*}\right), \ldots, \left(\frac{\varepsilon_m}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_m}{\mu^*}\right),$$
$$\left(\frac{\lambda_1}{\mathfrak{p}}\right) = \left(\frac{\lambda_1}{\mu^*}\right), \ldots, \left(\frac{\lambda_z}{\mathfrak{p}}\right) = \left(\frac{\lambda_z}{\mu^*}\right)$$

genügt. Mit Rücksicht auf Satz 43 gibt es dann in k eine ganze Zahl π^* derart, daß das Hauptideal (π^*) gleich $\mathfrak{p}^h$ wird und das Produkt $\pi^*\mu^*$ kongruent dem Quadrat einer ganzen Zahl in k nach $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$ ausfällt. Ferner läßt sich, wie leicht mit Rücksicht auf Satz 4, 6 und 8 ersichtlich ist, im Körper $K(\sqrt{\lambda_1\mu^*})$ gewiß eine Zahl A finden, so daß $\frac{\nu}{N(\mathsf{A})}$ gleich einem Bruche $\frac{\varrho}{\sigma}$ wird, dessen Zähler ϱ und dessen Nenner σ zu 2 prim ausfallen. Endlich werde ein Primideal $\mathfrak{q}$ in k bestimmt, welches den Bedingungen

$$\left(\frac{\varepsilon_1}{\mathfrak{q}}\right) = \left(\frac{\varepsilon_1}{\varrho\,\sigma}\right), \ldots, \left(\frac{\varepsilon_m}{\mathfrak{q}}\right) = \left(\frac{\varepsilon_m}{\varrho\,\sigma}\right),$$
$$\left(\frac{\lambda_1}{\mathfrak{q}}\right) = \left(\frac{\lambda_1}{\varrho\,\sigma}\right), \ldots, \left(\frac{\lambda_z}{\mathfrak{q}}\right) = \left(\frac{\lambda_z}{\varrho\,\sigma}\right),$$
$$\left(\frac{\lambda_1\pi^*}{\mathfrak{q}}\right) = +1 \tag{7}$$

genügt. Mit Rücksicht auf Satz 43 gibt es dann in k eine ganze Zahl $\varkappa$ derart, daß $(\varkappa) = \mathfrak{q}^h$ und zugleich $\varkappa\varrho\sigma$ kongruent dem Quadrat einer ganzen Zahl in k nach $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$ ausfällt.

Wir haben nun auf Grund von Definition 18

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\nu, \lambda_1^a\mu^*}{\mathfrak{w}}\right),$$

ferner ist

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu, \lambda_1^a\mu^*}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\varrho\,\sigma, \lambda_1^a\mu^*}{\mathfrak{w}}\right).$$

Endlich folgt bei Anwendung der Sätze 36 und 40

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varrho\,\sigma, \lambda_1^a\mu^*}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\varkappa, \lambda_1\pi^*}{\mathfrak{w}}\right),$$

und wegen der Voraussetzung des Satzes 57 haben wir mithin

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varkappa, \lambda_1\pi^*}{\mathfrak{w}}\right) = +1,$$

d. h. es ist

$$\left(\frac{\varkappa}{\mathfrak{p}}\right)\left(\frac{\lambda_1\pi^*}{\mathfrak{q}}\right) = +1$$

und wegen (7) wird also auch

$$\left(\frac{\varkappa}{\mathfrak{p}}\right) = +1. \tag{8}$$

Wir betrachten nunmehr den Körper $K(\sqrt{\lambda_1\pi^*})$ und bedienen uns dann zum Beweise des Satzes 57 der nämlichen Schlußweise, welche wir beim Beweise des Satzes 48 angewandt haben. Aus (7) folgt, daß das Primideal $\mathfrak{q}$ des Körpers k in $K(\sqrt{\lambda_1\pi^*})$ stets weiter zerlegbar ist. Wir unterscheiden ferner im

folgenden zwei Fälle, je nachdem $\mathfrak{p}$ ein nichtprimäres oder ein primäres Primideal ist.

Im ersteren Falle erweist sich durch eine ähnliche Betrachtung, wie sie im dritten Teile des Beweises zu Satz 48 (S. 462) angestellt wurde, die Klassenanzahl des Körpers $K(\sqrt{\lambda_1 \pi^*})$ als ungerade und es folgt hieraus mit Hinzuziehung von (8) wie in dem eben genannten Beweise, daß $\varkappa$ die Relativnorm einer Zahl in $K(\sqrt{\lambda_1 \pi^*})$ ist.

Im zweiten Falle verteilen wir ähnlich wie im zweiten Teile des Beweises zu Satz 48 (S. 460—462) die Komplexe des Körpers $K(\sqrt{\lambda_1 \pi^*})$ in zwei Geschlechter und zeigen dann, wie dort, daß jeder Komplex des Hauptgeschlechtes gleich dem Quadrat eines Komplexes wird. Berücksichtigen wir, daß wegen (8) jedes durch Zerlegung von $\mathfrak{q}$ entstehende Primideal in $K(\sqrt{\lambda_1 \pi^*})$ dem Hauptgeschlechte angehört, so folgt wiederum, daß $\varkappa$ die Relativnorm einer Zahl in $K(\sqrt{\lambda_1 \pi^*})$ ist.

In beiden vorhin unterschiedenen Fällen erhalten wir mithin

$$\left(\frac{\varkappa, \lambda_1 \pi^*}{\mathfrak{l}}\right) = +1$$

und da die Zahlen $\pi^* \mu^*$ und $\varkappa \varrho \sigma$ Quadraten von ganzen Zahlen in k nach $\mathfrak{l}^{2l+1}$ kongruent ausfallen, so folgt auf Grund des Satzes 56 schließlich auch

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1.$$

Hiermit ist Satz 57 bewiesen.

Satz 58. (Hilfssatz.) Es sei $\mathfrak{l}$ ein in 2 aufgehendes Primideal in k und ferner seien ν, μ beliebige ganze Zahlen $\neq 0$ in k: wenn dann $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$ ausfällt, so ist auch stets $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$.

Beweis. Wir benutzen die in Definition 18 erläuterten Bezeichnungen und bestimmen eine ganze Zahl μ^*, welche den Kongruenzen

$$\begin{aligned} \mu^* &\equiv \mu, \qquad (\mathfrak{l}_1^{2l_1+1+a}), \\ \mu^* &\equiv 1, \qquad (\mathfrak{l}_2^{2l_2+1} \ldots \mathfrak{l}_z^{2l_z+1}) \end{aligned}$$

genügt und nicht zugleich das Quadrat einer ganzen Zahl in k ist; dann haben wir nach Satz 56

$$\left.\begin{aligned} \left(\frac{\nu, \mu^*}{\mathfrak{l}_1}\right) = \left(\frac{\nu, \mu}{\mathfrak{l}_1}\right) &= +1, \\ \left(\frac{\nu, \mu^*}{\mathfrak{l}_i}\right) = \left(\frac{\nu, 1}{\mathfrak{l}_i}\right) &= +1, \qquad (i = 2, 3, \ldots z). \end{aligned}\right\} \tag{9}$$

Es mögen nun in der Zahl ν die Primideale $\mathfrak{l}_1, \ldots, \mathfrak{l}_z$ bez. genau zur $b_1, \ldots, b_z$-ten Potenz aufgehen; infolge der Gleichungen (9) gibt es gewisse

Zahlen $\mathfrak{A}_1, \ldots, \mathfrak{A}_z$ im Körper $K(\sqrt{\mu^*})$ derart, daß

$$\begin{aligned} \nu &\equiv N(\mathfrak{A}_1), \qquad (\mathfrak{l}_1^{2l_1+1+b_1}), \\ &\ldots\ldots\ldots\ldots \\ \nu &\equiv N(\mathfrak{A}_z), \qquad (\mathfrak{l}_z^{2l_z+1+b_z}) \end{aligned}$$

ausfällt. Wenn wir ähnlich wie im Beweise zu Satz 49 aus den Zahlen $\mathfrak{A}_1, \ldots, \mathfrak{A}_z$ eine Zahl $\mathfrak{A}$ konstruieren und dann in entsprechender Weise wie am genannten Ort verfahren, so erkennen wir ohne Schwierigkeit die Richtigkeit des Satzes 58.

Die beiden Sätze 57 und 58 zusammen genommen ergeben das Resultat:

Satz 59. (Hilfssatz). Wenn $\mathfrak{l}$ irgendein in 2 aufgehendes Primideal und ferner ν, μ beliebige ganze Zahlen $\neq 0$ in k bedeuten, dann gilt stets die Gleichung

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \left(\frac{\nu, \mu}{\mathfrak{l}}\right).$$

Mit Hilfe des Satzes 59 können wir leicht die in Satz 51 für das Symbol $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ aufgestellten drei Formeln auch in dem Falle als richtig nachweisen, daß ν, μ beliebige ganze Zahlen in k sind. Das Schlußverfahren zum Beweise der ersten Formel entspricht demjenigen, das zum Beweise der ersten Formel des Satzes 51 angewandt worden ist. Die Richtigkeit der beiden letzten Formeln folgt unmittelbar aus Satz 55 und 59. Wir erkennen hiernach, *daß die für das Symbol* $\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$ *in Satz* 14 *aufgestellten Formeln allgemein für beliebige ganze Zahlen* ν, μ *in* k *und in bezug auf jedes beliebige Primideal* $\mathfrak{w}$ *in* k *gültig sind.*

§ 39. Das Produkt $\prod_{(\mathfrak{w})} \left(\frac{\nu, \mu}{\mathfrak{w}}\right)$ für beliebige ganze Zahlen ν, μ.

Wir sind nunmehr imstande, einen Satz auszusprechen und zu beweisen, der als die weiteste Verallgemeinerung der Sätze 36, 40 und 52 anzusehen ist und der zugleich, wie mir scheint, das Reziprozitätsgesetz für quadratische Reste im Körper k auf die einfachste und vollständigste Weise zum Ausdruck bringt. Dieser Satz lautet:

Satz 60. *Wenn* ν, μ *beliebige ganze Zahlen* $\neq 0$ *in* k *sind, so ist stets*

$$\prod_{(\mathfrak{w})} \left(\frac{\nu, \mu}{\mathfrak{w}}\right) = +1,$$

wo das Produkt über sämtliche Primideale $\mathfrak{w}$ *in* k *erstreckt werden soll.*

Zum Beweise dieses Satzes gelangen wir durch eine entsprechende Schlußweise, wie sie zum Beweise des Satzes 52 angewandt worden ist.

Wir heben endlich noch eine besondere Folgerung des Satzes 60 hervor.

Satz 61. *Es seien* $\mathfrak{l}_1 (= \mathfrak{l}), \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ *die in* 2 *aufgehenden Primideale des Körpers* k, *und* λ *bedeute eine ganze Zahl in* k *derart, daß das Ideal* (λ) *die* h*-te Potenz von* $\mathfrak{l}$ *wird; ferner sei* $\mathfrak{p}$ *ein zu* 2 *primes Primideal und* π *eine ganze Zahl in* k,

so daß $(\pi) = \mathfrak{p}^h$ *ausfällt: dann gilt die Gleichung*

$$\left(\frac{\lambda}{\mathfrak{p}}\right) = \left(\frac{\lambda, \pi}{\mathfrak{l}_1}\right)\left(\frac{\lambda, \pi}{\mathfrak{l}_2}\right) \cdots \left(\frac{\lambda, \pi}{\mathfrak{l}_s}\right).$$

Zum Beweise des Satzes 61 setze man in 60 $\nu = \lambda, \mu = \pi$ ein.

Der Satz 61 heiße der *zweite Ergänzungssatz zum allgemeinen Reziprozitätsgesetze für die quadratischen Reste im Körper* k.

§ 40. Die Anzahl der Normenreste nach einem in 2 aufgehenden Primideal.

Es gelingt jetzt, die Aussagen des Satzes 15 auf die Primfaktoren der Zahl 2 auszudehnen. Wir sprechen den folgenden Satz aus:

Satz 62. *Es sei* $\mathfrak{l}$ *ein Primfaktor von* 2 *und zwar gehe* $\mathfrak{l}$ *genau zur* l*-ten Potenz in* 2 *auf: wenn dann die Relativdiskriminante des Körpers* $K(\sqrt{\mu})$ *nicht durch* $\mathfrak{l}$ *teilbar ist, so ist jede zu* $\mathfrak{l}$ *prime ganze Zahl* ν *in* k *Normenrest des Körpers* $K(\sqrt{\mu})$ *nach* $\mathfrak{l}$.

Wenn dagegen die Relativdiskriminante des Körpers $K(\sqrt{\mu})$ *den Faktor* $\mathfrak{l}$ *enthält und* L *einen beliebigen Exponenten größer als* $2l$ *bedeutet, so sind von allen vorhandenen zu* $\mathfrak{l}$ *primen und nach* $\mathfrak{l}^L$ *inkongruenten Zahlen* ν *in* k *genau die Hälfte Normenreste des Körpers* $K(\sqrt{\mu})$ *nach* $\mathfrak{l}$.

Beweis. Wenn $\mathfrak{l}$ nicht in der Relativdiskriminante von $K(\sqrt{\mu})$ aufgeht, so können wir mit Rücksicht auf Satz 4 und 6 annehmen, daß μ kongruent dem Quadrat einer ganzen zu $\mathfrak{l}$ primen Zahl nach $\mathfrak{l}^{2l}$ ausfällt. Eine gemäß Definition 17 zu μ bestimmte Zahl μ^* wird dann kongruent dem Quadrat einer ganzen Zahl in k nach dem Modul 2^2 und folglich erhalten wir nach Satz 36 $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$ und mithin nach Satz 50 auch $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$; damit ist die erste Aussage des Satzes 62 als richtig erkannt.

Und um die zweite Aussage des Satzes 62 zu beweisen, nehmen wir zunächst μ prim zu 2 an; es sei μ^* eine gemäß Definition 17 zu μ bestimmte ganze Zahl in k. Wir haben in Satz 29 gewisse $\frac{m}{2}$ Primideale $\mathfrak{q}_1, \ldots, \mathfrak{q}_{\frac{m}{2}}$ aufgestellt und aus diesen gewisse ganze Zahlen $\varkappa_1, \ldots, \varkappa_{\frac{m}{2}}$ abgeleitet, so daß dann nach diesem Satze jede zu 2 prime ganze Zahl des Körpers k nach dem Modul 2^2 in der dort angegebenen Gestalt darstellbar ist; wir setzen somit insbesondere

$$\mu^* \equiv \varepsilon_1^{u_1} \cdots \varepsilon_{\frac{m}{2}}^{u_{\frac{m}{2}}} \varkappa_1^{v_1} \cdots \varkappa_{\frac{m}{2}}^{v_{\frac{m}{2}}} \beta^2, \qquad (2^2),$$

worin die Exponenten $u_1, \ldots, u_{\frac{m}{2}}$, $v_1, \ldots, v_{\frac{m}{2}}$ gewisse Werte 0, 1 haben und β eine geeignete ganze Zahl in k bedeutet.

Wir unterscheiden im folgenden zwei Fälle, je nachdem die Exponenten $v_1, \ldots, v_{\frac{m}{2}}$ sämtlich gleich 0 sind oder mindestens einer dieser Exponenten

$v_1, \ldots, v_{\frac{m}{2}}$ von 0 verschieden ausfällt. Im ersten Falle können die Exponenten $u_1, \ldots, u_{\frac{m}{2}}$ nicht ebenfalls sämtlich verschwinden, da sonst $\mu^* \equiv \mu \equiv \beta^2$ nach dem Modul $\mathfrak{l}^{2l}$ und mithin der Voraussetzung entgegen die Relativdiskriminante von $K(\sqrt{\mu})$ prim zu $\mathfrak{l}$ wäre. Ist also etwa $u_i = 1$, so wird mit Berücksichtigung der Sätze 50 und 36

$$\left(\frac{\varkappa_i, \mu}{\mathfrak{l}}\right) = \left(\frac{\varkappa_i, \mu}{\mathfrak{l}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\varkappa_i, \mu^*}{\mathfrak{w}}\right) = \left(\frac{\varepsilon_i}{\mathfrak{q}_i}\right) = -1.$$

Im zweiten Falle sei etwa $v_i = 1$; dann schließen wir auf die nämliche Weise

$$\left(\frac{\varepsilon_i, \mu}{\mathfrak{l}}\right) = \left(\frac{\varepsilon_i, \mu}{\mathfrak{l}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\varepsilon_i, \mu^*}{\mathfrak{w}}\right) = \left(\frac{\varepsilon_i}{\mathfrak{q}_i}\right) = -1.$$

Nehmen wir im ersten Falle $\nu = \varkappa_i$, im zweiten $\nu = \varepsilon_i$, so ist gezeigt, daß es im Körper k stets eine Zahl ν gibt, welche Normennichtrest des Körpers $K(\sqrt{\mu})$ nach $\mathfrak{l}$ wird.

Wegen $L > 2l$ sind nach Satz 47 zwei nach $\mathfrak{l}^L$ kongruente zu $\mathfrak{l}$ prime ganze Zahlen in k stets gleichzeitig Normenreste oder Normennichtreste nach $\mathfrak{l}$. Wir bezeichnen nun mit $\nu_1, \nu_2, \ldots, \nu_s$ ein System ganzer Zahlen in k von folgender Beschaffenheit: die Zahlen $\nu_1, \ldots, \nu_s$ sollen nach $\mathfrak{l}^L$ untereinander inkongruente und zu $\mathfrak{l}$ prime Normenreste nach $\mathfrak{l}$ sein; endlich soll jede zu $\mathfrak{l}$ prime Zahl, welche Normenrest nach $\mathfrak{l}$ ist, einer jener Zahlen $\nu_1, \ldots, \nu_s$ nach $\mathfrak{l}^L$ kongruent sein. Ist nun ν ein zu $\mathfrak{l}$ primer Normennichtrest nach $\mathfrak{l}$, so sind die Zahlen $\nu\nu_1, \nu\nu_2, \ldots, \nu\nu_s$ wegen der zweiten Formel in Satz 51 sämtlich Normennichtreste nach $\mathfrak{l}$ und wir können leicht zeigen, daß jeder beliebige zu $\mathfrak{l}$ prime Normennichtrest nach $\mathfrak{l}$ einer dieser s Zahlen nach $\mathfrak{l}^L$ kongruent ausfällt. In der Tat bestimmen wir eine ganze Zahl ν^*, so daß $\nu\nu^* \equiv 1$ nach $\mathfrak{l}^L$ ausfällt, so folgt wegen $L > 2l$ mit Rücksicht auf Satz 47 die Gleichung

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \left(\frac{\nu^*, \mu}{\mathfrak{l}}\right) = -1;$$

es ist folglich auch ν^* Normennichtrest nach $\mathfrak{l}$. Bedeutet nun ν' irgendeinen beliebigen Normennichtrest nach $\mathfrak{l}$, so ist $\nu'\nu^*$ Normenrest nach $\mathfrak{l}$ und folglich einer der Zahlen $\nu_1, \ldots, \nu_s$ nach $\mathfrak{l}^L$ kongruent; es sei etwa $\nu'\nu^* \equiv \nu_i$ nach $\mathfrak{l}^L$; dann ist $\nu\nu'\nu^* \equiv \nu' \equiv \nu\nu_i$ nach $\mathfrak{l}^L$.

Aus dieser Betrachtung ergibt sich unmittelbar die Richtigkeit der zweiten Aussage des Satzes 62 für den Fall, daß μ zu 2 prim ist. Der vollständige Nachweis dieser zweiten Aussage gelingt leicht durch ein ähnliches Schlußverfahren unter Heranziehung von Satz 56.

Die in den beiden Sätzen 15 und 62 ausgesprochene Tatsache entspricht gewissermaßen dem bekannten Satze über die Verzweigungspunkte einer Riemannschen Fläche, wonach eine algebraische Funktion in der Umgebung

eines einfachen Verzweigungspunktes den Vollwinkel auf die Hälfte desselben konform abbildet. Infolgedessen nenne ich die in der Relativdiskriminante von $K(\sqrt{\mu})$ aufgehenden Primideale $\mathfrak{d}$ des Körpers k auch *Verzweigungsideale* für den Körper $K(\sqrt{\mu})$. Die Verzweigungsideale sind die Quadrate oder die Relativnormen der ambigen Primideale des Körpers $K(\sqrt{\mu})$.

§ 41. Beweis des Fundamentalsatzes über die Geschlechter in einem beliebigen relativquadratischen Körper.

In § 17 bis § 19, sowie in § 29 hatten wir die vorläufige Annahme gemacht, daß die Relativdiskriminante des zu untersuchenden Körpers K zu 2 prim ausfällt. Da wir erkannt haben, daß alle wesentlichen Eigenschaften des Symbols $\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$ auch für die in 2 enthaltenen Primideale $\mathfrak{w}$ des Körpers k gültig sind, so kann nunmehr jene vorläufige Annahme beseitigt werden.

Wir bezeichnen wie bisher mit $\mathfrak{l}_1, \ldots, \mathfrak{l}_z$ die voneinander verschiedenen Primfaktoren der Zahl 2 und setzen

$$2 = \mathfrak{l}_1^{l_1} \ldots \mathfrak{l}_z^{l_z}.$$

Zunächst lassen sich die Definitionen 11 und 12 der Begriffe „Charakterensystem" und „Geschlecht" unmittelbar auf den Fall ausdehnen, daß die Relativdiskriminante von K Faktoren aus der Reihe der Primideale $\mathfrak{l}_1, \ldots, \mathfrak{l}_z$ enthält; wir haben hierbei nur die Bemerkung am Schluß des § 38 zu berücksichtigen.

Desgleichen können wir die Beweise der Sätze 24, 25, 26 sofort auf den gegenwärtigen allgemeinen Fall übertragen, und es gilt demnach insbesondere auch der Satz 26 für jeden beliebigen relativquadratischen Körper $K(\sqrt{\mu})$.

Endlich entsteht die Aufgabe, den fundamentalen Satz 41 auch in dem Falle zu beweisen, daß die Relativdiskriminante des Körpers $K(\sqrt{\mu})$ Primfaktoren der Zahl 2 enthält. Um diesen Beweis zu entwickeln, behalten wir die in § 29 festgesetzten Bezeichnungen bei; es ist hierbei nur zu beachten, daß im gegenwärtigen Falle unter den Primidealen $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ auch solche vorkommen, die in der Zahl 2 aufgehen.

Es seien $\mathfrak{l}_1, \ldots, \mathfrak{l}_{z^*}$ diejenigen Primfaktoren von 2, die unter den r Idealen $\mathfrak{d}_1, \ldots, \mathfrak{d}_r$ vorkommen; wir setzen etwa

$$\mathfrak{l}_1 = \mathfrak{d}_{r-z^*+1}, \ldots, \mathfrak{l}_{z^*} = \mathfrak{d}_r,$$

so daß die $r - z^*$ Primideale $\mathfrak{d}_1, \ldots, \mathfrak{d}_{r-z^*}$ zu 2 prim sind. Es mögen nun $c_1, \ldots, c_r$ irgend beliebige r der Bedingung $c_1 \ldots c_r = +1$ genügende Einheiten ± 1 sein. Wegen Satz 62 kann man gewiß z^* ganze zu 2 prime Zahlen $\nu_1, \ldots, \nu_{z^*}$ finden, so daß

$$\left(\frac{\nu_1, \mu}{\mathfrak{l}_1}\right) = c_{r-z^*+1}, \ldots, \left(\frac{\nu_{z^*}, \mu}{\mathfrak{l}_{z^*}}\right) = c_r$$

wird. Bestimmen wir nun eine ganze Zahl ν derart, daß

$$\begin{aligned}
&\nu \equiv \nu_1, && (\mathfrak{l}_1^{2l_1+1}),\\
&\ldots\ldots\ldots\ldots\\
&\nu \equiv \nu_{z^*}, && (\mathfrak{l}_{z^*}^{2l_{z^*}+1}),\\
&\nu \equiv 1, && (\mathfrak{l}_{z^*+1}^{2l_{z^*+1}+1}),\\
&\ldots\ldots\ldots\ldots\\
&\nu \equiv 1, && (\mathfrak{l}_z^{2l_z+1})
\end{aligned}$$

ausfällt, so genügt ν nach Satz 56 den Bedingungen

$$\left.\begin{aligned}
&\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = c_{r-z^*+1}, \ldots, \left(\frac{\nu, \mu}{\mathfrak{l}_{z^*}}\right) = c_r,\\
&\left(\frac{\nu, \mu}{\mathfrak{l}_{z^*+1}}\right) = +1, \quad \ldots, \left(\frac{\nu, \mu}{\mathfrak{l}_z}\right) = +1.
\end{aligned}\right\} \tag{1}$$

Nunmehr bezeichnen wir mit $\mathfrak{d}_{r+1}, \ldots, \mathfrak{d}_{t^*}$ diejenigen unter den $t - r$ Primidealen $\mathfrak{d}_{r+1}, \ldots \mathfrak{d}_t$, die zu 2 prim sind und bestimmen dann ein Primideal $\mathfrak{p}$, für welches bei Benutzung der Bezeichnungen von § 31 die Gleichungen

$$\left.\begin{aligned}
&\left(\frac{\varepsilon_1}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_1}{\nu}\right), \ldots, \left(\frac{\varepsilon_m^{\frac{m}{2}}}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_m^{\frac{m}{2}}}{\nu}\right),\\
&\left(\frac{\lambda_1}{\mathfrak{p}}\right) = \left(\frac{\lambda_1}{\nu}\right), \ldots, \left(\frac{\lambda_z}{\mathfrak{p}}\right) = \left(\frac{\lambda_z}{\nu}\right),
\end{aligned}\right\} \tag{2}$$

$$\left.\begin{aligned}
&\left(\frac{\delta_1}{\mathfrak{p}}\right) = c_1\left(\frac{\nu}{\mathfrak{d}_1}\right)\left(\frac{\delta_1}{\nu}\right), \ldots, \left(\frac{\delta_{r-z^*}}{\mathfrak{p}}\right) = c_{r-z^*}\left(\frac{\nu}{\mathfrak{d}_{r-z^*}}\right)\left(\frac{\delta_{r-z^*}}{\nu}\right),\\
&\left(\frac{\delta_{r+1}}{\mathfrak{p}}\right) = \left(\frac{\nu}{\mathfrak{d}_{r+1}}\right)\left(\frac{\delta_{r+1}}{\nu}\right), \ldots, \left(\frac{\delta_{t^*}}{\mathfrak{p}}\right) = \left(\frac{\nu}{\mathfrak{d}_{t^*}}\right)\left(\frac{\delta_{t^*}}{\nu}\right)
\end{aligned}\right\} \tag{3}$$

gelten. Wegen (2) läßt sich nach Satz 43 eine ganze Zahl π bestimmen, so daß $(\pi) = \mathfrak{p}^h$ und überdies die Zahl $\pi\nu$ kongruent dem Quadrat einer ganzen Zahl in k nach $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$ wird. Infolgedessen schließen wir aus Satz 56 mit Rücksicht auf (1)

$$\left.\begin{aligned}
&\left(\frac{\pi, \mu}{\mathfrak{l}_1}\right) = \left(\frac{\nu, \mu}{\mathfrak{l}_1}\right) = c_{r-z^*+1}, \ldots, \left(\frac{\pi, \mu}{\mathfrak{l}_{z^*}}\right) = \left(\frac{\nu, \mu}{\mathfrak{l}_{z^*}}\right) = c_r,\\
&\left(\frac{\pi, \mu}{\mathfrak{l}_{z^*+1}}\right) = \left(\frac{\nu, \mu}{\mathfrak{l}_{z^*+1}}\right) = +1, \quad \ldots, \left(\frac{\pi, \mu}{\mathfrak{l}_z}\right) = \left(\frac{\nu, \mu}{\mathfrak{l}_z}\right) = +1.
\end{aligned}\right\} \tag{4}$$

Andererseits folgt aus Satz 40, wenn wir die erste Formel des Satzes 14 berücksichtigen,

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\pi\nu, \delta_i}{\mathfrak{w}}\right) = +1, \qquad (i = 1, 2, \ldots, r - z^*, r+1, \ldots, t^*)$$

und wegen (3) haben wir daher

$$\left(\frac{\pi}{\mathfrak{d}_i}\right)\left(\frac{\nu}{\mathfrak{d}_i}\right)\left(\frac{\delta_i}{\mathfrak{p}}\right)\left(\frac{\delta_i}{\nu}\right) = \left(\frac{\pi}{\mathfrak{d}_i}\right)c_i = +1, \qquad (i = 1, 2, \ldots, r - z^*),$$

$$\left(\frac{\pi}{\mathfrak{d}_i}\right)\left(\frac{\nu}{\mathfrak{d}_i}\right)\left(\frac{\delta_i}{\mathfrak{p}}\right)\left(\frac{\delta_i}{\nu}\right) = \left(\frac{\pi}{\mathfrak{d}_i}\right) = +1, \qquad (i = r+1, \ldots, t^*),$$

d. h. es gelten die Gleichungen

$$\left.\begin{aligned}\left(\frac{\pi}{\mathfrak{d}_i}\right)=\left(\frac{\pi,\mu}{\mathfrak{d}_i}\right)&=c_i, \qquad (i=1,2,\ldots,r-z^*),\\ \left(\frac{\pi}{\mathfrak{d}_i}\right)=\left(\frac{\pi,\mu}{\mathfrak{d}_i}\right)&=+1, \qquad (i=r+1,\ldots,t^*).\end{aligned}\right\} \tag{5}$$

Da $\mathfrak{d}_1,\ldots,\mathfrak{d}_{r-z^*},\mathfrak{d}_{r+1},\ldots,\mathfrak{d}_{t^*}$ die sämtlichen zu 2 primen Teiler der Relativdiskriminante von $K(\sqrt{\mu})$ sind, so können wir

$$\mu^h=\gamma\,\alpha^2\,\delta_1\cdots\delta_{r-z^*}\,\delta_{r+1}\cdots\delta_{t^*}$$

setzen, wo γ eine ganze Zahl in k ist, deren Primfaktoren sämtlich in 2 aufgehen, und wo α irgendeine bestimmte ganze Zahl in k bedeutet. Nach Satz 60 ist

$$\prod_{(\mathfrak{w})}\left(\frac{\pi,\mu}{\mathfrak{w}}\right)=\left(\frac{\mu}{\mathfrak{p}}\right)\left(\frac{\pi,\mu}{\mathfrak{d}_1}\right)\cdots\left(\frac{\pi,\mu}{\mathfrak{d}_{r-z^*}}\right)\left(\frac{\pi,\mu}{\mathfrak{d}_{r+1}}\right)\cdots\left(\frac{\pi,\mu}{\mathfrak{d}_{t^*}}\right)\left(\frac{\pi,\mu}{\mathfrak{l}_1}\right)\cdots\left(\frac{\pi,\mu}{\mathfrak{l}_r}\right)=+1$$

und folglich erhalten wir wegen (4), (5)

$$\left(\frac{\mu}{\mathfrak{p}}\right)c_1\cdots c_r=+1;$$

da nun $c_1\ldots c_r=+1$ angenommen worden ist, so ergibt sich auch $\left(\frac{\mu}{\mathfrak{p}}\right)=+1$, d. h. $\mathfrak{p}$ zerfällt in $K(\sqrt{\mu})$ in zwei Primfaktoren. Mit Rücksicht auf (4), (5) haben die Charaktere eines jeden dieser Primfaktoren die Werte

$$\left(\frac{\pi,\mu}{\mathfrak{d}_1}\right)=c_1,\ldots,\left(\frac{\pi,\mu}{\mathfrak{d}_r}\right)=c_r.$$

Hieraus schließen wir genau wie bei dem in § 29 entwickelten Beweise die Richtigkeit des Satzes 41 im allgemeinen Falle.

Wir haben damit die wichtigste Frage nach der Anzahl der Geschlechter in einem beliebigen relativquadratischen Körper $K(\sqrt{\mu})$ vollständig erledigt.

§ 42. Die Klassen des Hauptgeschlechtes.

Wir heben in diesem und in den folgenden Paragraphen einige Folgerungen hervor, die sich aus dem Satze 41 ergeben.

Satz 63. Die Anzahl g der Geschlechter in einem relativquadratischen Körper ist gleich der Anzahl A seiner ambigen Komplexe.

Beweis. Wenn t und v die Bedeutung wie in Satz 23 haben und wenn wir berücksichtigen, daß nach Satz 41 $g=2^{r-1}$ ist, so folgt aus den Sätzen 23 und 25

$$r\leqq t+v-\frac{m}{2}$$

und da andererseits nach Satz 24

$$t+v-\frac{m}{2}\leqq r$$

sein muß, so erhalten wir

$$r=t+v-\frac{m}{2};$$

nach Satz 23 ist mithin die Anzahl der ambigen Komplexe

$$\mathrm{A}=2^a=2^{r-1}=g.$$

Satz 64. *Jeder Komplex des Hauptgeschlechtes in einem relativquadratischen Körper K ist das Quadrat eines Komplexes in K, d. h. jede Klasse des Hauptgeschlechtes in einem relativquadratischen Körper K ist gleich dem Produkt aus dem Quadrat einer Klasse und aus einer solchen Klasse, welche Ideale des Grundkörpers k enthält.*

Beweis. In dem Beweise zu Satz 25 ist die Gleichung $\mathrm{A}f'=gf$ abgeleitet worden; hierbei haben A und g die Bedeutung wie in Satz 63; ferner bedeutet f' die Anzahl derjenigen Komplexe, welche gleich Quadraten von Komplexen sind und f die Anzahl der Komplexe des Hauptgeschlechtes. Da nach Satz 63 $\mathrm{A}=g$ ist, so folgt $f'=f$ und damit ist bewiesen, daß jeder Komplex des Hauptgeschlechtes das Quadrat eines Komplexes ist.

§ 43. Der Satz von den Relativnormen eines relativquadratischen Körpers.

Satz 65. *Wenn ν,μ irgend zwei beliebige ganze Zahlen $\neq 0$ des Körpers k bedeuten, von denen μ nicht das Quadrat einer Zahl in k ist, und welche für jedes Primideal $\mathfrak{w}$ in k die Bedingung*

$$\left(\frac{\nu,\mu}{\mathfrak{w}}\right)=+1$$

erfüllen, so ist die Zahl ν stets gleich der Relativnorm einer ganzen oder gebrochenen Zahl des Körpers $K(\sqrt{\mu})$.

Beweis. Wir beweisen diesen Satz zunächst für den Fall, daß ν eine Einheit in k ist. Es mögen t und v die Bedeutung wie in Satz 23 haben; im Beweise zu Satz 63 ist gezeigt worden, daß $r=t+v-\frac{m}{2}$ sein muß: d. h. es ist $v=\frac{m}{2}-t+r$. Die Anzahl der Einheitenverbände in k, soweit sie aus Einheiten, die Relativnormen sind, entspringen, beträgt also $2^{\frac{m}{2}-t+r}$.

Andererseits betrachten wir die $r^*=t-r$ Einheiten $\varepsilon_1,\ldots,\varepsilon_{r^*}$, die in § 17 bestimmt worden sind. Aus den Gleichungen (1) in § 17 erkennen wir leicht, daß die r^* aus $\varepsilon_1,\ldots,\varepsilon_{r^*}$ entspringenden Einheitenverbände voneinander unabhängig sind. Es müssen sich daher $\frac{m}{2}-r^*$ solche Einheitenverbände finden lassen, die mit jenen zusammen ein System von $\frac{m}{2}$ unabhängigen Einheitenverbänden bilden. Sind $\varepsilon_{r^*+1},\ldots,\varepsilon_{\frac{m}{2}}$ Einheiten bez. aus diesen $\frac{m}{2}-r^*$ Einheitenverbänden, so läßt sich offenbar jede beliebige Einheit ξ des Körpers k in der Gestalt

$$\xi=\varepsilon_1^{u_1}\cdots\varepsilon_{\frac{m}{2}}^{u_{\frac{m}{2}}}\varepsilon^2$$

darstellen, wo $u_1,\ldots,u_{\frac{m}{2}}$ gewisse Exponenten 0, 1 und ε eine geeignete Einheit in k bedeutet. Betrachtet man nun die r^* Gleichungen

$$\left(\frac{\xi,\mu}{\mathfrak{d}_t}\right)=+1,\left(\frac{\xi,\mu}{\mathfrak{d}_{t-1}}\right)=+1,\ldots,\left(\frac{\xi,\mu}{\mathfrak{d}_{t-r^*+1}}\right)=+1, \tag{1}$$

so liefern sie für die Exponenten $u_1, u_2, \ldots, u_{\frac{m}{2}}$ gewisse r^* lineare Kongruenzen nach dem Modul 2, die, wie man leicht erkennt, voneinander unabhängig sind; es folgt somit, daß alle diejenigen Einheiten ξ, die den Bedingungen (1) genügen, insgesamt

$$2^{\frac{m}{2}-r^*} = 2^{\frac{m}{2}-t+r}$$

Einheitenverbände ausmachen.

Wir haben zu Beginn dieses Beweises festgestellt, daß die Anzahl der Einheitenverbände, soweit sie aus Einheiten, die Relativnormen sind, entspringen, in gleicher Anzahl vorhanden sind. Da ferner jede Einheit in k, welche die Relativnorm einer Einheit oder einer gebrochenen Zahl von $K(\sqrt{\mu})$ ist, offenbar Normenrest nach I sein und daher notwendig den Gleichungen (1) genügen muß, so ist jeder Verband der zu Anfang behandelten Einheiten auch unter den Verbänden enthalten, deren Einheiten ξ den Gleichungen (1) genügen; da die Anzahlen beider Systeme von Einheitenverbänden die gleiche ist, so sind die beiden Systeme miteinander identisch. Die vorgelegte Einheit ν genügt nach Voraussetzung den Bedingungen (1) und ist mithin nach dem eben Bewiesenen die Relativnorm einer Einheit oder einer gebrochenen Zahl in $K(\sqrt{\mu})$.

Es sei jetzt ν eine beliebige Zahl in $K(\sqrt{\mu})$, welche die Voraussetzung des Satzes 65 erfüllt. Sind dann $\mathfrak{n}_1, \mathfrak{n}_2, \ldots$ die höchsten in ν aufgehenden Potenzen von Primidealen des Körpers k, so muß es wegen der Voraussetzung des Satzes 65 gewiß ganze Zahlen $\mathsf{A}_1, \mathsf{A}_2, \ldots$ in $K(\sqrt{\mu})$ geben von der Art, daß die Kongruenzen gelten

$$\begin{aligned} \nu &\equiv N(\mathsf{A}_1), \qquad (\mathfrak{n}_1^2), \\ \nu &\equiv N(\mathsf{A}_2), \qquad (\mathfrak{n}_2^2), \\ &\cdots\cdots\cdots \end{aligned}$$

Bezeichnet also A eine ganze Zahl in $K(\sqrt{\mu})$, die kongruent A_1 nach $\mathfrak{n}_1^2$, kongruent A_2 nach $\mathfrak{n}_2^2$, usf. ausfällt, so erhalten wir

$$\nu \equiv N(\mathsf{A}), \qquad (\nu^2). \tag{2}$$

Betrachten wir nun in $K(\sqrt{\mu})$ das Ideal

$$\mathfrak{H} = (\nu, \mathsf{A}),$$

so ergibt sich wegen (2)

$$\mathfrak{H} \cdot S\mathfrak{H} = (\nu, \mathsf{A})(\nu, S\mathsf{A}) = (\nu^2, \nu\mathsf{A}, \nu S\mathsf{A}, \mathsf{A}S\mathsf{A}) = (\nu)$$

und hieraus folgt, daß ν die Relativnorm des Ideals $\mathfrak{H}$ in $K(\sqrt{\mu})$ sein muß.

Wegen der Voraussetzung des Satzes 65 gehört $\mathfrak{H}$ notwendig dem Hauptgeschlecht von $K(\sqrt{\mu})$ an und wir können daher nach Satz 64

$$\mathfrak{H} \sim \mathfrak{j}\mathfrak{J}^2$$

setzen in solcher Weise, daß $\mathfrak{j}$ ein Ideal in k und $\mathfrak{J}$ ein Ideal in $K(\sqrt{\mu})$ bedeutet. Wegen $\mathfrak{j}^h \sim 1$ muß $\mathsf{B} = \left(\frac{\mathfrak{H}}{\mathfrak{J}^2}\right)^h$ eine ganze oder gebrochene Zahl des Körpers K sein; die Relativnorm $N(\mathsf{B})$ dieser Zahl ist offenbar von der Gestalt $\frac{\varepsilon \nu^h}{\alpha^2}$, wo ε eine Einheit in k und α eine ganze Zahl in k bedeutet. Aus der letzten Gleichung folgt, daß für jedes beliebige Primideal $\mathfrak{w}$ notwendig $\left(\frac{\varepsilon \nu^h \alpha^2, \mu}{\mathfrak{w}}\right) = +1$ und daher auch $\left(\frac{\varepsilon, \mu}{\mathfrak{w}}\right) = +1$ sein muß. Es ist nun im ersten Teil des gegenwärtigen Beweises gezeigt worden, daß unter diesen Umständen ε stets gleich der Relativnorm einer Zahl in $K(\sqrt{\mu})$ sein muß; wir setzen $\varepsilon = N(\Gamma)$, wo Γ eine Zahl in $K(\sqrt{\mu})$ ist. Es folgt dann

$$\nu = N\left(\frac{\mathsf{B} \cdot \alpha}{\Gamma \cdot \nu^{\frac{h-1}{2}}}\right),$$

und hiermit ist der Beweis für Satz 65 vollständig erbracht.

§ 44. Die ternäre quadratische Diophantische Gleichung im Körper k.

Den Inhalt des Satzes 65 können wir auch auf folgende Weisen aussprechen:

Satz 66. Wenn ν, μ beliebige ganze Zahlen $+0$ in k bedeuten, so ist die Diophantische Gleichung

$$\nu\xi^2 + \mu\eta^2 = 1$$

in ganzen oder gebrochenen Zahlen ξ, η des Körpers k stets dann lösbar, wenn für jedes Primideal $\mathfrak{w}$ in k die Bedingung

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = 1$$

erfüllt ist.

Satz 67. *Wenn ν, μ irgend zwei beliebige ganze Zahlen des Körpers k bedeuten, so ist die Diophantische Gleichung*

$$\nu\xi^2 + \mu\eta^2 = 1$$

in ganzen oder gebrochenen Zahlen ξ, η des Körpers k stets dann lösbar, wenn die Kongruenz

$$\nu\xi^2 + \mu\eta^2 \equiv 1$$

nach jedem Primideal des Körpers k und nach jeder Potenz eines solchen in ganzen Zahlen ξ, η des Körpers k lösbar ist.

Beweis. Falls μ das Quadrat einer ganzen Zahl in k ist, wird jener Diophantischen Gleichung durch $\xi = 0, \eta = \frac{1}{\sqrt{\mu}}$ genügt. Es sei nun μ nicht das Quadrat einer ganzen Zahl in k. Es sei ferner $\mathfrak{w}$ ein Primideal in k und $\mathfrak{w}^L$ eine beliebige Potenz von $\mathfrak{w}$; endlich seien ξ, η ganze Zahlen in k, die der im Satze 67 aufgestellten Kongruenz nach $\mathfrak{w}^L$ genügen. Da offenbar ξ, η nicht beide zugleich durch $\mathfrak{w}$ teilbar sein können, so dürfen wir annehmen, daß etwa ξ zu $\mathfrak{w}$ prim ausfiele: dann ist wegen

$$\nu \equiv N\left(\frac{1 + \eta\sqrt{\mu}}{\xi}\right), \qquad (\mathfrak{w}^L)$$

die Zahl ν Normenrest des Körpers $K(\sqrt{\mu})$ nach $\mathfrak{w}$ und folglich erfüllen die

Zahlen ν, μ die Bedingungen des Satzes 65. Nach diesem Satze 65 ist daher ν die Relativnorm einer gewissen Zahl A des Körpers $K(\sqrt{\mu})$; setzen wir $A = \frac{\alpha + \beta\sqrt{\mu}}{\gamma}$, wo α, β, γ ganze Zahlen in k sind, so folgt

$$\nu = \frac{\alpha^2 - \mu\beta^2}{\gamma^2}$$

und mithin erfüllen die Zahlen $\xi = \frac{\gamma}{\alpha}$, $\eta = \frac{\beta}{\alpha}$ die vorgelegte Gleichung. Damit ist der Satz 67 bewiesen.

Ist irgendeine ternäre homogene quadratische Diophantische Gleichung mit beliebigen in k liegenden Koeffizienten vorgelegt, so entsteht die Frage nach den Bedingungen, unter denen diese Gleichung durch geeignete ganze Zahlen des Körpers k gelöst werden kann. Auch diese Frage findet, wie leicht zu sehen, auf Grund der Sätze 66 und 67 ihre vollständige Beantwortung.

Verzeichnis der Sätze und Definitionen.

	Seite		Seite		Seite
Satz 1	372	Satz 24	409	Satz 47	455
„ 2	372	„ 25	411	„ 48	458
„ 3	374	„ 26	411	„ 49	463
„ 4	374	„ 27	413	„ 50	464
„ 5	376	„ 28	413	„ 51	464
„ 6	376	„ 29	413	„ 52	465
„ 7	377	„ 30	416	„ 53	466
„ 8	377	„ 31	417	„ 54	466
„ 9	380	„ 32	423	„ 55	467
„ 10	381	„ 33	426	„ 56	467
„ 11	383	„ 34	427	„ 57	468
„ 12	384	„ 35	427	„ 58	472
„ 13	385	„ 36	428	„ 59	473
„ 14	387	„ 37	434	„ 60	473
„ 15	388	„ 38	435	„ 61	473
„ 16	390	„ 39	436	„ 62	474
„ 17	392	„ 40	445	„ 63	478
„ 18	393	„ 41	446	„ 64	479
„ 19	393	„ 42	448	„ 65	479
„ 20	396	„ 43	451	„ 66	481
„ 21	397	„ 44	452	„ 67	481
„ 22	397	„ 45	454		
„ 23	403	„ 46	454		

Definition 1	371	Definition 7	388	Definition 13	412
„ 2	372	„ 8	389	„ 14	412
„ 3	374	„ 9	389	„ 15	427
„ 4	379	„ 10	396	„ 16	434
„ 5	379	„ 11	407	„ 17	453
„ 6	380	„ 12	409	„ 18	467

10. Über die Theorie der relativ-Abelschen Zahlkörper[1].

[Acta Mathematica Bd. 26, S. 99—132 (1902).]

§ 1.

In der Theorie der relativ-Abelschen Zahlkörper nehmen zunächst die Körper vom *zweiten* Relativgrade unser Interesse in Anspruch.

Es sei ein beliebiger Zahlkörper k vom Grade n als Rationalitätsbereich zugrunde gelegt; unsere Aufgabe ist es dann, die Theorie der relativquadratischen Zahlkörper $K(\sqrt{\mu})$, d. h. derjenigen Körper zu begründen, die durch die Quadratwurzel aus einer beliebigen ganzen Zahl μ des Körpers k bestimmt sind. Die „disquisitiones arithmeticae" von Gauss sind als der einfachste Fall in jenem Problem enthalten. Wir können unsern Gegenstand auch als die Theorie der quadratischen Gleichungen oder Formen bezeichnen, deren Koeffizienten Zahlen des vorgelegten Rationalitätsbereiches k sind.

Die Theorie des relativquadratischen Körpers führte mich zur Entdeckung eines allgemeinen Reziprozitätsgesetzes für quadratische Reste, welches das gewöhnliche Reziprozitätsgesetz zwischen rationalen Primzahlen nur als ein vereinzeltes Glied in einer Kette sehr interessanter und mannigfaltiger Zahlenbeziehungen erscheinen läßt.

In meiner Abhandlung *Über die Theorie des relativquadratischen Zahlkörpers*[2] habe ich die Theorie der quadratischen Relativkörper innerhalb eines algebraischen Grundkörpers k vollständig für den Fall entwickelt, daß der Grundkörper k nebst seinen sämtlichen konjugierten Körpern imaginär ist und überdies eine ungerade Klassenanzahl besitzt. Die wichtigsten der in der genannten Abhandlung aufgestellten Sätze sind das Reziprozitätsgesetz für quadratische Reste in k und der Satz, demzufolge in einem relativquadrati-

[1] Mit geringen Änderungen abgedruckt aus den Nachrichten der K. Ges. der Wiss. zu Göttingen 1898.

Inzwischen sind folgende auf diesen Gegenstand bezügliche Inaugural-Dissertationen in Göttingen erschienen: *Das quadratische Reziprozitätsgesetz im quadratischen Zahlkörper mit der Klassenzahl* 1. von H. Dörrie 1898, *Tafel der Klassenzahlen für kubische Zahlkörper* von L. W. Reid 1899, *Das allgemeine quadratische Reziprozitätsgesetz in ausgewählten Kreiskörpern der 2^k-ten Einheitswurzeln* von K. S. Hilbert 1900, *Quadratische Reziprozitätsgesetze in algebraischen Zahlkörpern* von G. Rückle 1901. Insbesondere die letzte Dissertation enthält zahlreiche und interessante Beispiele zu der hier entwickelten Theorie.

[2] Math. Ann. 51, 1—127 (1899). Dieser Band Abh. 9, S. 370—482.

schen Körper in bezug auf k stets die Hälfte aller denkbaren Charakterensysteme wirklich durch Geschlechter vertreten sind. Ich habe in jener Abhandlung zu zeigen versucht, welch ein Reichtum an arithmetischen Wahrheiten in diesen Sätzen enthalten ist; dennoch offenbart sich die volle Bedeutung der genannten Sätze erst, wenn wir ihre Gültigkeit auf *beliebige* algebraische Grundkörper k ausdehnen. In einem auf der Mathematiker-Vereinigung zu Braunschweig gehaltenen Vortrage[1] habe ich einige kurze Bemerkungen über den Fall gemacht, daß der Grundkörper k reell ist, bzw. reelle konjugierte Körper aufweist oder die Klassenanzahl 2 besitzt. In der gegenwärtigen Arbeit beabsichtige ich, die wichtigsten Sätze aus der Theorie der quadratischen Relativkörper innerhalb eines beliebigen Grundkörpers k aufzustellen und zugleich die Abänderungen anzugeben, welche die Beweise in meiner zu Anfang genannten Abhandlung erfahren müssen, wenn man für den Grundkörper k die dort gemachten beschränkenden Annahmen beseitigen will.

Endlich habe ich im letzten Paragraph (§ 16) der gegenwärtigen Arbeit für relativ-Abelsche Zahlkörper von beliebigem Relativgrade und mit der Relativdiskriminante 1 eine Reihe von allgemeinen Sätzen vermutungsweise aufgestellt; es sind dies Sätze von wunderbarer Einfachheit und kristallener Schönheit, deren vollständiger Beweis und gehörige Verallgemeinerung auf den Fall einer beliebigen Relativdiskriminante mir als das Endziel der rein arithmetischen Theorie der relativ-Abelschen Zahlkörper erscheint.

§ 2.

Es sei k ein beliebiger Zahlkörper; der Grad dieses Körpers k heiße m und die $m-1$ zu k konjugierten Zahlkörper mögen mit $k', k'', \ldots, k^{(m-1)}$ bezeichnet werden. Die Anzahl der Idealklassen des Körpers k werde h genannt. Wir übertragen das bekannte Symbol aus der Theorie der rationalen Zahlen auf den hier zu behandelnden Fall, wie folgt[2]:

Es sei $\mathfrak{p}$ ein in 2 nicht aufgehendes Primideal des Körpers k und α eine beliebige zu $\mathfrak{p}$ prime ganze Zahl in k: dann bedeute das Symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)$ den Wert $+1$ oder -1, je nachdem α dem Quadrat einer ganzen Zahl in k nach $\mathfrak{p}$ kongruent ist oder nicht. Ist ferner $\mathfrak{a}$ ein beliebiges zu 2 primes Ideal in k und hat man $\mathfrak{a} = \mathfrak{p}\mathfrak{q}\ldots\mathfrak{w}$, wo $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{w}$ Primideale in k sind und ist α eine zu $\mathfrak{a}$ prime ganze Zahl in k, so möge das Symbol $\left(\frac{\alpha}{\mathfrak{a}}\right)$ durch die folgende Gleichung definiert werden:

$$\left(\frac{\alpha}{\mathfrak{a}}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\alpha}{\mathfrak{q}}\right)\cdots\left(\frac{\alpha}{\mathfrak{w}}\right).$$

[1] Jber. Mathematiker-Vereinigung 4, 88—94 (1897). Dieser Band Abh. 8, S. 364—369.
[2] Vgl. meine Abhandlung *Über die Theorie des relativquadratischen Zahlkörpers*, Definition 1 und 5. Dieser Band S. 371 und 379.

Sind $\mathfrak{a}$, $\mathfrak{b}$ beliebige zu 2 prime Ideale in k und α eine zu $\mathfrak{a}\mathfrak{b}$ prime ganze Zahl in k, so gilt offenbar die Gleichung

$$\left(\frac{\alpha}{\mathfrak{a}\mathfrak{b}}\right) = \left(\frac{\alpha}{\mathfrak{a}}\right)\left(\frac{\alpha}{\mathfrak{b}}\right).$$

Bezeichnet μ irgendeine ganze Zahl in k, die nicht gleich dem Quadrat einer Zahl in k ist, so bestimmt $\sqrt{\mu}$ zusammen mit den Zahlen des Körpers k einen Körper vom Grade $2m$, welcher relativquadratisch in bezug auf den Körper k ist und mit $K\left(\sqrt{\mu}\right)$ oder auch kurz mit K bezeichnet werde. Sind in bezug auf k mehrere relativquadratische Körper vorgelegt, so heißen dieselben *voneinander unabhängig*, sobald keiner derselben als Unterkörper in demjenigen Körper enthalten ist, der aus den übrigen durch Zusammensetzung entsteht.

Ein relativquadratischer Körper K heiße *unverzweigt* in bezug auf k, wenn die Relativdiskriminante von K in bezug auf k gleich 1 ausfällt oder, was das nämliche bedeutet, wenn es in k kein Primideal gibt, das gleich dem Quadrat eines Primideals in K wird.

§ 3.

Wir machen zunächst über den zugrunde gelegten Körper k solche zwei Annahmen, unter denen die Theorie des relativquadratischen Körpers bereits in meiner Abhandlung ausführlich entwickelt worden ist; es sind dies folgende Annahmen:

1. Der Körper k vom m-ten Grade sei nebst allen konjugierten Körpern $k', k'', \ldots, k^{(m-1)}$ imaginär.

2. Die Anzahl h der Idealklassen im Körper k sei gleich 1.

Wegen der späteren Ausführungen wiederholen wir hier die hauptsächlichsten in Frage kommenden Definitionen und Resultate in einer Fassung, die von der in meiner Abhandlung gegebenen Darstellung ein wenig abweicht.

Definition 1. Ein solches zu 2 primes Ideal $\mathfrak{a}$ des Körpers k, in bezug auf das für jede Einheit ξ in k

$$\left(\frac{\xi}{\mathfrak{a}}\right) = +1$$

ausfällt, heiße ein *primäres Ideal*.

Definition 2. Eine solche zu 2 prime ganze Zahl α des Körpers k, welche kongruent dem Quadrat einer ganzen Zahl in k nach dem Modul 2^2 ausfällt, heiße eine *primäre Zahl* des Körpers k.

Wir können dann den wesentlichen Inhalt des *ersten* Ergänzungssatzes zum Reziprozitätsgesetz wie folgt aussprechen:

Satz 1. Wenn $\mathfrak{a}$ ein primäres Ideal in k ist, so gibt es stets eine primäre Zahl α, so daß $\mathfrak{a} = (\alpha)$ wird, und umgekehrt: wenn α eine primäre Zahl in k ist, so ist das Ideal $\mathfrak{a} = (\alpha)$ stets ein primäres Ideal.

Wir zerlegen nun die Zahl 2 im Körper k in Primideale wie folgt:

$$2 = \mathfrak{l}_1^{l_1}\mathfrak{l}_2^{l_2}\cdots\mathfrak{l}_z^{l_z},$$

wo $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ die voneinander verschiedenen Primfaktoren der Zahl 2 in k und $l_1, l_2, \ldots, l_z$ die Potenzexponenten bedeuten, zu denen bez. jene Primideale in der Zahl 2 aufgehen.

Definition 3. Ein solches zu 2 primes Ideal $\mathfrak{a}$ des Körpers k, in bezug auf das nicht nur für jede Einheit ξ in k, sondern auch für jede in 2 aufgehende ganze Zahl λ des Körpers k

$$\left(\frac{\xi}{\mathfrak{a}}\right) = +1, \qquad \left(\frac{\lambda}{\mathfrak{a}}\right) = +1$$

ausfällt, heiße ein *hyperprimäres Ideal*.

Definition 4. Eine solche zu 2 prime Zahl α des Körpers k, welche kongruent dem Quadrat einer ganzen Zahl in k nach dem Modul $\mathfrak{l}_1^{2l_1+1}\mathfrak{l}_2^{2l_2+1}\ldots\mathfrak{l}_z^{2l_z+1}$ ausfällt, heiße eine *hyperprimäre Zahl* des Körpers k.

Wir können dann den wesentlichen Inhalt des *zweiten* Ergänzungssatzes zum Reziprozitätsgesetz wie folgt aussprechen:

Satz 2. Wenn $\mathfrak{a}$ ein hyperprimäres Ideal in k ist, so gibt es stets eine hyperprimäre Zahl α, so daß $\mathfrak{a} = (\alpha)$ wird, und umgekehrt: wenn α eine hyperprimäre Zahl in k ist, so ist das Ideal $\mathfrak{a} = (\alpha)$ stets ein hyperprimäres Ideal.

Der wesentliche Inhalt des allgemeinen Reziprozitätsgesetzes für quadratische Reste im Körper k lautet wie folgt:

Satz 3. Wenn ν, μ, ν', μ' irgendwelche zu zwei prime ganze Zahlen in k sind derart, daß die beiden Produkte $\nu\nu'$ und $\mu\mu'$ primär ausfallen und ν zu μ, ν' zu μ' prim ist, so ist stets

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

Wenn die Klassenanzahl h des Körpers k nicht gleich 1, sondern eine beliebige ungerade Zahl ist, so wird nur eine geringfügige und aus meiner Abhandlung leicht zu entnehmende Abänderung im Ausdrucke der Sätze 1 bis 3 notwendig.

Satz 4. Jede Einheit in k, welche primär (eine primäre Zahl) ist, ist das Quadrat einer Einheit in k.

Satz 5. Es gibt in bezug auf k keinen relativquadratischen unverzweigten Körper.

Die beiden letzten Sätze gelten unverändert für den Fall, daß die Klassenanzahl h des Körpers k eine beliebige ungerade Zahl ist.

§ 4.

Wir legen nunmehr für den Körper k folgende Annahmen zugrunde:

1. Unter den m konjugierten Körpern $k, k', k'', \ldots, k^{(m-1)}$ gebe es eine beliebige Anzahl $s\,(>0)$ reeller Körper; seien dies die Körper $k, k', k'', \ldots, k^{(s-1)}$.

2. Die Anzahl h der Idealklassen im Körper k sei gleich 1.

Bei diesen Annahmen wird die Definition 1 des primären Ideals unverändert beibehalten, dagegen wird es nötig, den Begriff einer primären Zahl enger zu fassen.

Definition 5. Eine Zahl α des Körpers k heißt *total positiv in* k, falls die s zu α konjugierten bez. in $k, k', \ldots, k^{(s-1)}$ gelegenen Zahlen sämtlich positiv sind. Wenn eine zu 2 prime Zahl α des Körpers k kongruent dem Quadrat einer ganzen Zahl in k nach dem Modul 2^2 ausfällt und wenn außerdem α total positiv in k ist, so heiße α eine *primäre Zahl* des Körpers k.

Bei Anwendung der so festgesetzten Bezeichnungsweise gilt der erste Ergänzungssatz 1 und das allgemeine Reziprozitätsgesetz 3 wiederum genau in der früheren Fassung und, wenn man in entsprechender Weise den Begriff der hyperprimären Zahl enger faßt, so bleibt auch der zweite Ergänzungssatz 2 in der früheren Fassung gültig.

§ 5.

Wir erörtern ferner die Frage, ob es unter den in § 4 für den Körper k zugrunde gelegten Annahmen relativquadratische unverzweigte Körper in bezug auf k gibt. Zu dem Zwecke setzen wir zunächst allgemein fest, daß, wenn ε irgendeine Einheit in k bedeutet, stets $\varepsilon', \varepsilon'', \ldots, \varepsilon^{(s-1)}$ die zu ε konjugierten bez. in $k', k'', \ldots, k^{(s-1)}$ gelegenen Einheiten bezeichnen sollen.

Nunmehr nehmen wir $\varepsilon_1 = -1$: wie die Einheit ε_1 fallen offenbar alle zu ε_1 konjugierten Einheiten negativ aus. Ferner möge es in k eine Einheit ε_2 geben, welche in k positiv ist, während mindestens eine der konjugierten Einheiten $\varepsilon_2', \ldots, \varepsilon_2^{(s-1)}$ negativ ausfällt; es sei etwa die in k' gelegene Einheit ε_2' negativ. Sodann möge es in k eine Einheit ε_3 geben, welche positiv ist und für welche auch ε_3' positiv wird, während mindestens eine der konjugierten Einheiten $\varepsilon_3'', \varepsilon_3''', \ldots, \varepsilon_3^{(s-1)}$ negativ ausfällt; es sei etwa die in k'' gelegene Einheit ε_3'' negativ. In dieser Weise fahren wir fort; wir mögen schließlich eine Einheit $\varepsilon_p (p \leqq s)$ erhalten von der Beschaffenheit, daß $\varepsilon_p, \varepsilon_p', \varepsilon_p'', \ldots, \varepsilon_p^{(p-2)}$ sämtlich positiv sind, dagegen $\varepsilon_p^{(p-1)}$ negativ ausfällt und nun soll das eingeschlagene Verfahren sein Ende erreicht haben, d. h. wenn irgendeine Einheit ε in k nebst ihren $p-1$ konjugierten Einheiten $\varepsilon', \varepsilon'', \ldots, \varepsilon^{(p-1)}$ positiv ausfällt, so sei nunmehr auch stets jede der übrigen $s-p$ konjugierten Einheiten $\varepsilon^{(p)}, \ldots, \varepsilon^{(s-1)}$ positiv.

Die Zahl $s-p$ erhält eine besonders einfache Bedeutung, wenn wir dem Äquivalenz- und Klassenbegriff eine engere Fassung erteilen als bisher geschehen ist. Wir wollen nämlich fortan zwei Ideale $\mathfrak{j}, \mathfrak{f}$ des Körpers k nur dann als äquivalent bezeichnen, wenn $\frac{\mathfrak{j}}{\mathfrak{f}} = \alpha$ gesetzt werden kann, so daß α eine ganze oder gebrochene Zahl in k ist, die selbst nebst den sämtlichen bez. in

$k', k'', \ldots, k^{(s-1)}$ gelegenen zu α konjugierten Zahlen $\alpha', \alpha'', \ldots, \alpha^{(s-1)}$ positiv ausfällt, d. h., die total positiv in k ist. Rechnen wir alle solchen Ideale des Körpers k, die in diesem engeren Sinne untereinander äquivalent sind, zu einer Klasse, so besitzt der Körper k, wie leicht ersichtlich ist, genau $\bar{h} = 2^{s-p}$ Idealklassen.

Nach diesen Vorbereitungen findet die oben aufgeworfene Frage nach den unverzweigten Körpern in bezug auf k in folgender Weise ihre Beantwortung:

Satz 6. Für den Körper k gibt es ein System von $s - p$ unabhängigen relativquadratischen unverzweigten Körpern in bezug auf k. Durch Zusammensetzung dieser $s - p$ Körper entsteht ein Körper Kk vom Relativgrade $\bar{h} = 2^{s-p}$ in bezug auf k, der sämtliche unverzweigten Körper in bezug auf k als Unterkörper enthält und der *Klassenkörper* von k heißen möge. Die Anzahl H der Idealklassen dieses Körpers Kk ist, auch wenn wir den Klassenbegriff in der vorhin (für k) angegebenen engeren Fassung nehmen, stets eine ungerade Zahl[1].

Eine der merkwürdigsten Eigenschaften des Klassenkörpers Kk besteht darin, daß die Primideale des Körpers k, welche einer und der nämlichen Idealklasse von k im engeren Sinne angehören, im Klassenkörper Kk stets die nämliche Zerlegung in Primideale dieses Körpers Kk erfahren, d. h. so daß die Anzahl der verschiedenen Primideale und ihre Grade die gleichen sind; die Zerlegung eines Primideals $\mathfrak{p}$ des Körpers k im Körper Kk hängt somit nur von der Klasse ab, der das Primideal $\mathfrak{p}$ im Körper k angehört.

§ 6.

Um die genannten Tatsachen zu beweisen und unter den in § 4 gemachten Annahmen die Theorie des relativquadratischen Körpers in bezug auf k vollständig aufzubauen, bedürfen wir eines Symbols, welches ich bereits in meinem in Braunschweig gehaltenen Vortrage erklärt habe.

Definition 6. Es sei $\mathfrak{w}$ irgendein Primideal in k, und es seien ν, μ beliebige ganze Zahlen in k, nur daß μ nicht gleich dem Quadrat einer Zahl in k ausfällt; wenn dann ν nach $\mathfrak{w}$ der Relativnorm einer ganzen Zahl des Körpers $K\left(\sqrt{\mu}\right)$ kongruent ist und wenn außerdem auch für jede höhere Potenz von $\mathfrak{w}$ stets eine solche ganze Zahl A im Körper $K\left(\sqrt{\mu}\right)$ gefunden werden kann, daß $\nu \equiv N(A)$ nach jener Potenz von $\mathfrak{w}$ ausfällt, so setze ich

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = +1;$$

[1] Für $k = 1$, $\bar{h} = 2$ und $\bar{h} = 4$ wurde diese letzte Behauptung von PH. FURTWÄNGLER bewiesen. Nachrichten der K. Ges. d. Wiss. Göttingen **1906**, S. 417—434. [Anm. d. Herausgeber.]

in jedem anderen Falle dagegen

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = -1.$$

Fällt μ gleich dem Quadrat einer ganzen Zahl ($\neq 0$) in k aus, so werde stets

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = +1$$

gesetzt. Ferner definieren wir noch die s Symbole

$$\left(\frac{\nu, \mu}{1}\right), \left(\frac{\nu, \mu}{1'}\right), \ldots, \left(\frac{\nu, \mu}{1^{(s-1)}}\right);$$

wir setzen stets

$$\left(\frac{\nu, \mu}{1}\right) = +1,$$

wenn wenigstens eine der beiden Zahlen ν, μ positiv ausfällt; dagegen setzen wir

$$\left(\frac{\nu, \mu}{1}\right) = -1,$$

wenn jede der beiden Zahlen ν, μ negativ ausfällt. Ferner bezeichnen wir allgemein die in $k^{(i)}$ gelegenen zu ν, μ konjugierten Zahlen bez. mit $\nu^{(i)}, \mu^{(i)}$ und setzen

$$\left(\frac{\nu, \mu}{1'}\right) = \left(\frac{\nu', \mu'}{1}\right), \quad \left(\frac{\nu, \mu}{1''}\right) = \left(\frac{\nu'', \mu''}{1}\right), \ldots, \left(\frac{\nu, \mu}{1^{(s-1)}}\right) = \left(\frac{\nu^{(s-1)}, \mu^{(s-1)}}{1}\right).$$

Ist nun ein bestimmter relativquadratischer Körper $K\left(\sqrt{\mu}\right)$ in bezug auf k vorgelegt, so wird eine naturgemäße Definition des Geschlechtsbegriffes aus der Definition 12 meiner Abhandlung gewonnen, wenn man sich des verallgemeinerten Symbols $\left(\frac{\nu, \mu}{\omega}\right)$ bedient, wo ω die in der Relativdiskriminante von $K\left(\sqrt{\mu}\right)$ aufgehenden Primideale und überdies diejenigen Zeichen $1^{(i)}$ durchläuft, wofür die in $k^{(i)}$ gelegene zu μ konjugierte Zahl $\mu^{(i)}$ negativ ausfällt. Es gelingt dann ohne erhebliche Schwierigkeit die ganze in meiner Abhandlung entwickelte Theorie der relativquadratischen Körper auf den hier in Rede stehenden Fall, daß der Körper k die in § 4 gemachten Annahmen erfüllt, auszudehnen.

Das Reziprozitätsgesetz für quadratische Reste im Körper k erhält mit Benutzung des erweiterten Symbols $\left(\frac{\nu, \mu}{\omega}\right)$ die folgende einfache Fassung:

Satz 7. Wenn ν, μ beliebige ganze Zahlen $\neq 0$ in k sind, so ist stets

$$\prod_{(\omega)} \left(\frac{\nu, \mu}{\omega}\right) = +1,$$

wo das Produkt über sämtliche Primideale $\omega = \mathfrak{w}$ in k und über die s Zeichen $\omega = 1, 1', 1'', \ldots, 1^{(s-1)}$ erstreckt werden soll.

Auch die Sätze 41, 64, 65, 67 in meiner Abhandlung lassen sich mit Hilfe des erweiterten Symbols $\left(\frac{\nu, \mu}{\omega}\right)$ unmittelbar auf den Fall des hier betrachteten Grundkörpers k übertragen.

Wenn die in ursprünglichem Sinne verstandene Klassenzahl h des Körpers k nicht 1, sondern irgendeine ungerade Zahl ist, so bedürfen die Sätze in § 4 bis § 6 nur einer geringen und aus meiner Abhandlung leicht zu entnehmenden Abänderung.

§ 7.

Wenn für den Körper k insbesondere $s - p = 0$ ausfällt, so wird $\overline{h} = 1$ und Satz 6 lehrt dann, daß es keinen unverzweigten Körper in bezug auf k gibt. Wir wollen den nächst einfachen Fall $s - p = 1, \overline{h} = 2$ betrachten und vor allem die am Schluß von § 5 angedeuteten Gesetze der Zerlegung der Primideale in k näher erörtern. Es mögen daher fortan für den Grundkörper k folgende speziellere Annahmen gelten:

1. Unter den m konjugierten Körpern $k, k', k'', \ldots, k^{(m-1)}$ gebe es eine beliebige Anzahl s (> 0) reelle Körper; es seien dies die Körper $k, k', k'', \ldots, k^{(s-1)}$.

2. Die Anzahl h der Idealklassen des Körpers k, im ursprünglichen weiteren Sinne verstanden, sei gleich 1; die Anzahl $\overline{h}$ der Idealklassen des Körpers k, im engeren Sinne verstanden, sei gleich 2.

Unter diesen Annahmen ist der in § 5 erwähnte Klassenkörper Kk relativquadratisch und besitzt folgende Eigenschaften:

Satz 8a. Der Klassenkörper Kk hat in bezug auf k die Relativdiskriminante 1; d. h. er ist unverzweigt in bezug auf k.

Satz 8b. Die Klassenanzahl $\overline{H}$ des Klassenkörpers Kk, in engerem Sinne verstanden, ist ungerade.

Satz 8c. Diejenigen Primideale in k, welche in k Hauptideale im engeren Sinne sind, zerfallen in Kk in das Produkt zweier Primideale. Diejenigen Primideale in k, welche in k nicht Hauptideale im engeren Sinne sind, bleiben in Kk Primideale.

Von diesen drei Eigenschaften 8a, 8b, 8c charakterisiert jede für sich allein bei unseren Annahmen über den Körper k in eindeutiger Weise den Klassenkörper Kk.

Zum Beweise der Existenz des Klassenkörpers Kk ist es erforderlich zu zeigen, daß es unter den hier gemachten Annahmen stets eine Einheit ε in k gibt, die kongruent dem Quadrat einer ganzen Zahl nach dem Modul 2^2 ausfällt, ohne daß sie das Quadrat einer Einheit in k wird. Der verlangte Klassenkörper Kk ist dann der Körper $K\left(\sqrt{\varepsilon}\right)$. Der Beweis für die Existenz einer solchen Einheit ε läßt sich durch eine ähnliche Schlußweise führen, wie sie im § 9 beim Beweise der Sätze 9a, 9b, 9c angewandt werden wird.

§ 8.

Im weiteren Verlaufe dieser Untersuchung wollen wir für einige andere Fälle die Gesetze der Zerlegung der Primideale des Grundkörpers k im Klassenkörper Kk genau erörtern und die Beweise der aufgestellten Behauptungen erbringen. Es mögen in diesem Paragraphen für die Grundkörper k folgende spezielle Annahmen gelten:

1. Unter den m konjugierten Körpern $k, k', k'', \ldots, k^{(m-1)}$ gebe es eine beliebige Anzahl s reeller Körper.

2. Die Anzahl h der Idealklassen des Körpers k, im ursprünglichen weiteren Sinne, stimme mit der im engeren Sinne verstandenen Klassenanzahl $\overline{h}$ überein und sei gleich 2.

Unter diesen Annahmen ist der Klassenkörper Kk relativquadratisch und besitzt folgende Eigenschaften:

Satz 9a. Der Klassenkörper Kk ist unverzweigt in bezug auf k, d. h. er hat die Relativdiskriminante 1 in bezug auf k.

Satz 9b. Die Klassenanzahl H und $\overline{H}$ des Klassenkörpers Kk, im weiteren sowie im engeren Sinne verstanden, sind ungerade ($H = \overline{H}$).

Satz 9c. Diejenigen Primideale in k, welche in k Hauptideale sind, zerfallen in Kk in das Produkt zweier Primideale. Diejenigen Primideale in k, welche in k nicht Hauptideale sind, bleiben in Kk Primideale; sie werden jedoch in Kk Hauptideale.

Von diesen drei Eigenschaften 9a, 9b, 9c charakterisiert jede für sich allein bei unseren Annahmen über den Körper k in eindeutiger Weise den Klassenkörper Kk; wir haben somit die Sätze:

Satz 10a. Es gibt außer Kk keinen anderen relativquadratischen Körper, der in bezug auf k unverzweigt ist.

Satz 10b. Wenn ein zu k relativquadratischer Körper eine ungerade Klassenzahl hat, so stimmt derselbe mit dem Klassenkörper Kk überein.

Satz 10c. Wenn alle Primideale in k, die in k Hauptideale sind, in einem relativquadratischen Körper zerfallen, oder wenn alle Primideale in k, die in k nicht Hauptideale sind, in einem relativquadratischen Körper Primideale bleiben, so folgt jedesmal, daß dieser relativquadratische Körper kein anderer als der Klassenkörper Kk ist.

§ 9.

Um die Existenz des Klassenkörpers Kk und sodann die Sätze 9a, 9b, 9c zu beweisen, machen wir der Kürze halber die Annahme, daß der Grundkörper k und seine sämtlichen konjugierten Körper imaginär sind und nennen dann wie in § 3 eine ganze Zahl in k primär, wenn sie zu 2 prim ist und dem Quadrat einer ganzen Zahl in k nach dem Modul 2^2 kongruent ausfällt.

Wir bestimmen jetzt ein System von Grundeinheiten in k und bezeichnen dieselben mit $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\frac{m}{2}-1}$; ferner sei $\mathfrak{r}$ ein zu 2 primes Primideal des Körpers k, welches nicht der Hauptklasse in k angehört, und es werde $\mathfrak{r}^2 = (\varrho)$ gesetzt, wo ϱ eine gewisse ganze Zahl in k bedeutet. Fügen wir sodann den obigen $\frac{m}{2} - 1$ Einheiten noch folgende Zahlen hinzu

$$\varepsilon_{\frac{m}{2}} = -1, \qquad \varepsilon_{\frac{m}{2}+1} = \varrho,$$

so bilden die $\frac{m}{2} + 1$ Zahlen $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\frac{m}{2}+1}$ ein System von Zahlen dieser Beschaffenheit: jede ganze Zahl ξ in k, welche das Quadrat eines Ideals in k ist, läßt sich in der Gestalt

$$\xi = \varepsilon_1^{x_1} \varepsilon_2^{x_2} \cdots \varepsilon_{\frac{m}{2}+1}^{x_{\frac{m}{2}+1}} \alpha^2$$

darstellen, wo die Exponenten $x_1, x_2, \ldots, x_{\frac{m}{2}+1}$ gewisse Werte 0, 1 haben und α eine ganze oder gebrochene Zahl in k bedeutet.

Endlich bestimmen wir mit Hinblick auf Satz 18 meiner Abhandlung ein System von Primidealen $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_{\frac{m}{2}+1}$ in k, die zu 2 prim sind, so daß

$$\left(\frac{\varepsilon_i}{\mathfrak{q}_i}\right) = -1, \quad \left(\frac{\varepsilon_j}{\mathfrak{q}_i}\right) = +1, \quad (i \neq j) \qquad \left(i, j = 1, 2, \ldots, \frac{m}{2}+1\right) \tag{1}$$

ausfällt und zu diesen solche Exponenten $w_1, \ldots, w_{\frac{m}{2}+1}$ mit Werten 0, 1, daß die Produkte

$$\mathfrak{q}_1 \mathfrak{r}^{w_1}, \mathfrak{q}_2 \mathfrak{r}^{w_2}, \ldots, \mathfrak{q}_{\frac{m}{2}+1} \mathfrak{r}^{w_{\frac{m}{2}+1}}$$

Hauptideale in k werden; es sei etwa

$$\mathfrak{q}_1 \mathfrak{r}^{w_1} = (\varkappa_1), \ldots, \mathfrak{q}_{\frac{m}{2}+1} \mathfrak{r}^{w_{\frac{m}{2}+1}} = \left(\varkappa_{\frac{m}{2}+1}\right),$$

wo $\varkappa_1, \ldots, \varkappa_{\frac{m}{2}+1}$ gewisse ganze Zahlen in k sind.

Nach diesen Vorbereitungen betrachten wir den Ausdruck

$$\varepsilon_1^{u_1} \cdots \varepsilon_{\frac{m}{2}+1}^{u_{\frac{m}{2}+1}} \varkappa_1^{v_1} \cdots \varkappa_{\frac{m}{2}+1}^{v_{\frac{m}{2}+1}}; \tag{2}$$

derselbe stellt, wenn man rechter Hand für die Exponenten $u_1, \ldots, u_{\frac{m}{2}+1}$ beliebige Werte 0, 1 und für die Exponenten $v_1, \ldots, v_{\frac{m}{2}+1}$ irgendwelche der Kongruenzbedingung

$$v_1 w_1 + v_2 w_2 + \cdots + v_{\frac{m}{2}+1} w_{\frac{m}{2}+1} \equiv 0, \tag{3}$$

genügende Werte 0, 1 nimmt, im Ganzen 2^{m+1} Zahlen dar. Rechnet man jetzt allgemein zwei ganze zu 2 prime Zahlen ω_1, ω_2 in k zu derselben Art, wenn ihr Produkt $\omega_1 \omega_2$ eine primäre Zahl ist, so lehrt die Betrachtung am Schlusse von § 21 meiner Abhandlung, daß es im Körper k genau 2^m verschiedene Arten von Zahlen gibt und es müssen also unter den Zahlen von der Gestalt (2) notwendig wenigstens zwei Zahlen vorhanden sein, die derselben Art angehören. Das Produkt zweier solcher Zahlen ist eine primäre Zahl von der Gestalt

$$\omega = \varepsilon_1^{u_1} \cdots \varepsilon_{\frac{m}{2}+1}^{u_{\frac{m}{2}+1}} \varkappa_1^{v_1} \cdots \varkappa_{\frac{m}{2}+1}^{v_{\frac{m}{2}+1}} \alpha^2, \tag{4}$$

wo die Exponenten $u_1, \ldots, u_{\frac{m}{2}+1}$, $v_1, \ldots, v_{\frac{m}{2}+1}$ gewisse Werte 0, 1 haben, aber nicht sämtlich gleich 0 sind und α eine ganze Zahl in k bedeutet.

Wenn in dem Ausdrucke (4) für die Zahl ω die Exponenten $v_1, \ldots, v_{\frac{m}{2}+1}$ sämtlich sich gleich 0 herausstellten, so wäre nach Satz 4 und 5 meiner Abhandlung der Körper $K\left(\sqrt{\omega}\right)$ ein in bezug auf k unverzweigter relativquadratischer Körper und somit der verlangte Beweis für die Existenz des Klassenkörpers mit der Eigenschaft 9a erbracht.

Wir nehmen nun im Gegenteil an, es habe wenigstens einer der Exponenten $v_1, \ldots, v_{\frac{m}{2}+1}$ den Wert 1, und zwar sei t deren genaue Anzahl; es sei etwa $v_{i_1} = 1, v_{i_2} = 1, \ldots, v_{i_t} = 1$, wo die Indizes $i_1, i_2, \ldots, i_t$ gewisse t Zahlen der Reihe $1, 2, \ldots, \frac{m}{2}+1$ bedeuten. Bei dieser Annahme müssen die t Primideale $\mathfrak{q}_{i_1}, \mathfrak{q}_{i_2}, \ldots, \mathfrak{q}_{i_t}$ in der Relativdiskriminante des Körpers $K\left(\sqrt{\omega}\right)$ aufgehen; wegen der Bedingung (3) und da ω primär ist, folgt ferner, daß es außer diesen t Primidealen kein weiteres gibt, welches in der Relativdiskriminante von $K\left(\sqrt{\omega}\right)$ enthalten wäre. Die genannten t Primideale des Körpers k werden bez. die Quadrate gewisser t ambiger Primideale des Körpers $K\left(\sqrt{\omega}\right)$, und die Anzahl aller ambigen Ideale des Körpers $K\left(\sqrt{\omega}\right)$, fällt daher genau gleich 2^t aus. Auch die weiteren Bezeichnungen des Satzes 22 in § 15 meiner Abhandlung benutzen wir: es möge der Körper k genau 2^{e^*} Einheitenverbände besitzen, die aus Relativnormen von Einheiten in $K\left(\sqrt{\omega}\right)$ entspringen, und es sei 2^{a^*} die Anzahl der ambigen Klassen, in denen ambige Ideale des Körpers $K\left(\sqrt{\omega}\right)$ enthalten sind.

Was das Verhalten der Ideale des Körpers k im Körper $K(\sqrt{\omega})$ betrifft, so sind hier die folgenden zwei Fälle möglich:

I. Die Ideale des Körpers k, welche in k nicht Hauptideale sind, werden in $K(\sqrt{\omega})$ Hauptideale.

II. Die Ideale des Körpers k, welche in k nicht Hauptideale sind, werden auch in $K(\sqrt{\omega})$ nicht Hauptideale.

Indem wir das Verfahren, welches ich in meiner Abhandlung beim Beweise des Satzes 22 angewendet habe, auf den Körper $K(\sqrt{\omega})$ übertragen, finden wir leicht im Falle I die Gleichung

$$a^* = t + v^* - \frac{m}{2} \tag{5}$$

und im Falle II die Gleichung

$$a^* = t + v^* - \frac{m}{2} - 1. \tag{6}$$

§ 10.

Wir wollen ferner für die Zahl v^* eine obere von t und m abhängige Grenze ableiten. Zu dem Zweck mögen $x_1, \ldots, x_{\frac{m}{2}}$ irgendwelche Exponenten 0, 1 bedeuten; soll dann die Einheit

$$\varepsilon = \varepsilon_1^{x_1} \cdots \varepsilon_{\frac{m}{2}}^{x_{\frac{m}{2}}}$$

die Relativnorm einer Einheit in $K(\sqrt{\omega})$ sein, so müssen notwendig die t Bedingungen

$$\left(\frac{\varepsilon}{\mathfrak{q}_{i_1}}\right) = +1, \ \ldots, \ \left(\frac{\varepsilon}{\mathfrak{q}_{i_t}}\right) = +1 \tag{7}$$

erfüllt sein.

Wir stellen nun der Reihe nach folgende Hilfssätze auf, welche für beide Fälle I, II gelten:

Hilfssatz 1. Jede Einheit ε des Körpers k, die den Bedingungen (7) genügt, ist notwendig die Relativnorm einer Einheit des Relativkörpers $K(\sqrt{\omega})$.

Zum Beweise dieses Hilfssatzes unterscheiden wir, ob unter den Indizes $i_1, \ldots, i_t$ die Zahl $\frac{m}{2}+1$ vorkommt oder nicht. Im ersteren Falle sei $i_t = \frac{m}{2}+1$. Wir schließen dann aus (7) mit Rücksicht auf (1), daß gewiß die Gleichungen

$$x_{i_1} = 0, \ \ldots, \ x_{i_{t-1}} = 0$$

bestehen müssen, und hieraus entnehmen wir, daß die Anzahl v^* der voneinander unabhängigen Einheitenverbände, welche aus den Relativnormen von Einheiten in $K(\sqrt{\omega})$ entspringen, höchstens gleich $\frac{m}{2} - t + 1$ ist.

Kommt andererseits unter den Indizes $i_1, \ldots, i_t$ die Zahl $\frac{m}{2}+1$ nicht vor, so schließen wir auf die nämliche Weise

$$x_{i_1} = 0, \ \ldots, \ x_{i_t} = 0$$

und mithin ist die Anzahl v^* der voneinander unabhängigen Einheitenverbände, welche aus den Relativnormen von Einheiten in $K(\sqrt{\omega})$ entspringen, in diesem Falle höchstens gleich $\frac{m}{2} - t$.

Wir erkennen leicht, daß im Falle I unter den Indizes $i_1, \ldots, i_t$ die Zahl $\frac{m}{2}+1$ nicht vorkommen kann. Wäre nämlich im Gegenteil das Primideal $\mathfrak{q}_{\frac{m}{2}+1}$ in der Relativdiskriminante des Körpers $K(\sqrt{\omega})$ enthalten und bezeichnet P die ganze Zahl in $K(\sqrt{\omega})$, welche das Ideal $\mathfrak{r}$ darstellt, so muß die Relativnorm dieser Zahl P gleich einer Zahl in k von der Gestalt $\varepsilon\varrho$ werden, wo ε eine Einheit in k bezeichnet und $\varrho = \varepsilon_{\frac{m}{2}+1}$ die früher festgesetzte Bedeutung hat. Die hieraus folgende Bedingungsgleichung

$$\left(\frac{\varepsilon\varrho}{\mathfrak{q}_{\frac{m}{2}+1}}\right) = \left(\frac{\varepsilon\,\varepsilon_{\frac{m}{2}+1}}{\mathfrak{q}_{\frac{m}{2}+1}}\right)$$

steht im Widerspruch mit der in (1) getroffenen Festsetzung für das Primideal $\mathfrak{q}_{\frac{m}{2}+1}$.

Die bisherigen Überlegungen führen im Falle I zu der Ungleichung

$$v^* \leqq \frac{m}{2} - t \tag{8}$$

und im Falle II zu der Ungleichung

$$v^* \leqq \frac{m}{2} - t + 1. \tag{9}$$

Die Gleichungen (5), (6) und die Ungleichungen (8), (9) zeigen, daß in beiden Fällen I und II die Ungleichung $a^* \leqq 0$ gilt und da gewiß auch $a^* \geqq 0$ sein muß, so folgt notwendig $a^* = 0$, d. h. es ist im Falle I

$$v^* = \frac{m}{2} - t. \tag{10}$$

und im Falle II

$$v^* = \frac{m}{2} - t + 1. \tag{11}$$

Nunmehr können wir auch einsehen, daß im Falle II das Primideal $\mathfrak{q}_{\frac{m}{2}+1}$ in der Relativdiskriminante des Körpers $K(\sqrt{\omega})$ vorkommen muß. Wäre nämlich im Gegenteil die Zahl $\frac{m}{2}+1$ unter den Indizes $i_1, \ldots, i_t$ nicht enthalten,

so müßte, wie die vorhin angestellte Überlegung zeigt, die Ungleichung (8) gelten, was der Gleichung (11) widerspricht.

Wir sehen mit Rücksicht hierauf, daß die Einheiten ε in k, welche den Bedingungen (7) genügen, im Falle I genau $\frac{m}{2}-t$ und im Falle II genau $\frac{m}{2}-t+1$ voneinander unabhängige Einheitenverbände ausmachen. Da diese Zahl wegen (10), (11) in beiden Fällen I, II gleich v^* ausfällt, so liefern jene Einheiten ε im ganzen 2^{v^*} Einheitenverbände; dieselben müssen daher mit denjenigen Einheitenverbänden übereinstimmen, deren Einheiten Relativnormen von Einheiten in $K(\sqrt{\omega})$ sind, d. h. in beiden Fällen I, II ist jede Einheit ε in k, die den Bedingungen (7) genügt, notwendig die Relativnorm einer Einheit in $K(\sqrt{\omega})$ und damit ist Hilfssatz 1 bewiesen.

Hilfssatz 2. Wenn $\mathfrak{J}$ ein Ideal in $K(\sqrt{\omega})$ ist, dessen Quadrat einem Ideal in k äquivalent ausfällt, so ist auch $\mathfrak{J}$ stets einem Ideal in k äquivalent.

Beim Beweise verstehen wir unter S die Relativsubstitution $(\sqrt{\omega}: -\sqrt{\omega})$ und unter N die Relativnorm einer Zahl oder eines Ideals in $K(\sqrt{\omega})$. Da die Relativnorm des Ideals $\mathfrak{J}$

$$N(\mathfrak{J}) = \mathfrak{J} . S\mathfrak{J}$$

jedenfalls ein Ideal in k ist und nach Voraussetzung $\mathfrak{J}^2$ einem Ideal in k äquivalent sein soll, so folgt, daß auch der Idealquotient $\frac{\mathfrak{J}}{S\mathfrak{J}}$ einem Ideal $\mathfrak{j}$ in k äquivalent sein muß.

Im Falle I ist $\mathfrak{j}$ gewiß in $K(\sqrt{\omega})$ ein Hauptideal. Wir beweisen andererseits, daß im Falle II das Ideal $\mathfrak{j}$ im Körper k Hauptideal ist. Wäre nämlich $\mathfrak{j}$ in k nicht Hauptideal, so wäre $\mathfrak{j}\mathfrak{r} \sim 1$, wo $\mathfrak{r}$ die früher festgesetzte Bedeutung hat; setzen wir dann

$$\frac{\mathfrak{J}}{S\mathfrak{J}}\mathfrak{r} = A,$$

wo A eine gebrochene Zahl in $K(\sqrt{\omega})$ ist, so folgt offenbar, indem wir auf beiden Seiten die Relativnorm bilden,

$$\varepsilon\varrho = N(A), \tag{12}$$

wo ε eine Einheit und $\varrho = \varepsilon_{\frac{m}{2}+1}$ die früher bestimmte Zahl in k bezeichnet. Da das Primideal $\mathfrak{q}_{\frac{m}{2}+1}$ im Falle II in der Relativdiskriminante von $K(\sqrt{\omega})$ vorkommt, so erhalten wir wegen (12) die Gleichung

$$\left(\frac{\varepsilon\,\varepsilon_{\frac{m}{2}+1}}{\mathfrak{q}_{\frac{m}{2}+1}}\right) = +1,$$

und diese widerspricht der in (1) getroffenen Festsetzung für das Primideal $\mathfrak{q}_{\frac{m}{2}+1}$.

Wir haben somit erkannt, daß in beiden Fällen I, II der Idealquotient $\frac{\mathfrak{J}}{S\mathfrak{J}}$ in $K(\sqrt{\omega})$ äquivalent 1 ausfällt; wir setzen demgemäß

$$\frac{\mathfrak{J}}{S\mathfrak{J}} = A, \tag{13}$$

wo A eine ganze oder gebrochene Zahl in $K(\sqrt{\omega})$ ist. Bilden wir dann die Relativnorm

$$\varepsilon = N(A), \tag{14}$$

so ist ε eine Einheit in k, die den Bedingungen (7) genügen muß und diese Einheit ε wird daher nach dem oben bewiesenen Hilfssatz 1 gleich der Relativnorm einer Einheit in $K(\sqrt{\omega})$; wir setzen

$$\varepsilon = N(E^{-1}), \tag{15}$$

wo E eine Einheit in $K(\sqrt{\omega})$ ist. Aus (14) und (15) folgt

$$N(AE) = 1. \tag{16}$$

Setzen wir

$$B = 1 + S(AE),$$

(bez. $B = 1$, wenn etwa $AE = -1$ ist), so wird wegen (16)

$$\frac{SB}{B} = EA \qquad (\text{bez.} = 1),$$

und hieraus entnehmen wir mit Rücksicht auf (13) die Gleichung für Ideale

$$\frac{S(B\mathfrak{J})}{B\mathfrak{J}} = 1,$$

d. h. $B\mathfrak{J}$ ist das Produkt eines ambigen Ideals des Körpers $K(\sqrt{\omega})$ in ein Ideal des Körpers k. Da nun für beide Fälle I, II früher die Gleichung $a^* = 0$ bewiesen worden ist und folglich alle ambigen Ideale in $K(\sqrt{\omega})$ Hauptideale sind, so folgt, daß auch das Ideal $\mathfrak{J}$ einem Ideal des Körpers k äquivalent sein muß. Hiermit ist der Beweis für den Hilfssatz 2 erbracht.

Hilfssatz 3. Wenn $\mathfrak{J}$ irgendein Ideal in $K(\sqrt{\omega})$ ist, so gibt es stets einen ungeraden Exponenten u, so daß $\mathfrak{J}^u$ einem Ideal in k äquivalent ist.

In der Tat, ist H die Klassenanzahl des Körpers $K(\sqrt{\omega})$ und setzen wir $H = 2^a u$, wo a einen gewissen Exponenten und u eine ungerade Zahl bedeutet, so folgt, daß $\mathfrak{J}^{2^a u} \sim 1$ sein muß und hieraus schließen wir mit Rücksicht auf Hilfssatz 2 der Reihe nach, daß die Ideale $\mathfrak{J}^{2^{a-1}u}, \mathfrak{J}^{2^{a-2}u}, \ldots, \mathfrak{J}^{2u}, \mathfrak{J}^u$ gewissen Idealen in k äquivalent ausfallen.

Hilfssatz 4. Wenn $\mathfrak{p}$ ein Primideal des Körpers k bedeutet, für welches

$$\left(\frac{\omega}{\mathfrak{p}}\right) = +1 \tag{17}$$

ausfällt, so ist $\mathfrak{p}$ stets im Körper k ein Hauptideal.

Zum Beweise bedenken wir, daß wegen der Voraussetzung (17) das Primideal $\mathfrak{p}$ im Körper $K\left(\sqrt{\omega}\right)$ zerlegbar sein muß; wir setzen

$$\mathfrak{p} = \mathfrak{P} \cdot S\mathfrak{P},$$

wo $\mathfrak{P}$, $S\mathfrak{P}$ zueinander relativkonjugierte Ideale in $K\left(\sqrt{\omega}\right)$ sind und verstehen dann mit Rücksicht auf Hilfssatz 3 unter u einen solchen ungeraden Potenzexponenten, daß $\mathfrak{P}^u$ einem Ideal $\mathfrak{j}$ in k äquivalent wird. Hieraus folgt offenbar

$$\mathfrak{p}^u \sim \mathfrak{j}^2 \sim 1, \quad \text{d. h.} \quad \mathfrak{p} \sim 1.$$

§ 11.

Der gewünschte Nachweis für die Existenz der Klassenkörper mit den Eigenschaften 9a, 9b, 9c gelingt mittelst der folgenden Schlüsse. Wir wählen an Stelle der in § 9 bestimmten den Bedingungen (1) genügenden Primideale $\mathfrak{q}_1, \ldots, \mathfrak{q}_{\frac{m}{2}+1}$ irgend $\frac{m}{2}+1$ andere zu 2 prime Primideale $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{\frac{m}{2}+1}$ mit den entsprechenden Eigenschaften

$$\left(\frac{\varepsilon_i}{\mathfrak{q}'_i}\right) = -1, \qquad \left(\frac{\varepsilon_j}{\mathfrak{q}'_i}\right) = +1, \qquad (i \neq j) \qquad \left(i, j = 1, 2, \ldots, \frac{m}{2}+1\right)$$

und wählen wiederum die Exponenten $w'_1, \ldots, w'_{\frac{m}{2}+1}$ in geeigneter Weise so, daß

$$\mathfrak{q}'_1 \mathfrak{r}^{w'_1} = (\varkappa'_1), \ \ldots, \ \mathfrak{q}'_{\frac{m}{2}+1} \mathfrak{r}^{w'_{\frac{m}{2}+1}} = \left(\varkappa'_{\frac{m}{2}+1}\right)$$

und darin $\varkappa'_1, \ldots, \varkappa'_{\frac{m}{2}+1}$ ganze Zahlen in k sind; sodann denken wir uns die sämtlichen Schlußfolgerungen in § 9 bis § 10 für das neue System von Primidealen $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{\frac{m}{2}+1}$ wiederholt. Auf diese Weise gelangen wir zu einem Ausdruck

$$\omega' = \varepsilon' \varkappa_1'^{v'_1} \cdots \varkappa_{\frac{m}{2}+1}'^{v'_{\frac{m}{2}+1}}, \tag{18}$$

in dem ε' eine gewisse Einheit in k und $v'_1, \ldots, v'_{\frac{m}{2}+1}$ gewisse Exponenten 0, 1 bedeuten; falls wir wie vorhin annehmen, daß die Exponenten $v'_1, \ldots, v'_{\frac{m}{2}+1}$ nicht sämtlich gleich 0 ausfallen, folgern wir wiederum für den Körper $K\left(\sqrt{\omega}\right)$

die Gültigkeit der Hilfssätze 1 bis 4, und entsprechend dem Hilfssatz 4 ist mithin jedes Primideal $\mathfrak{p}$ des Körpers k, für welches

$$\left(\frac{\omega'}{\mathfrak{p}}\right) = +1$$

ausfällt, stets notwendig ein Hauptideal des Körpers k.

Wir bezeichnen nun kurz mit $\mathfrak{w}_\omega$ alle diejenigen Primideale in k, für welche

$$\left(\frac{\omega}{\mathfrak{w}_\omega}\right) = +1$$

ist, und mit $\mathfrak{w}_{\omega\omega'}$ diejenigen Primideale in k für welche zugleich

$$\left(\frac{\omega}{\mathfrak{w}_{\omega\omega'}}\right) = -1 \quad \text{und} \quad \left(\frac{\omega'}{\mathfrak{w}_{\omega\omega'}}\right) = +1$$

ausfällt, ferner mit $\mathfrak{w}^{(+)}$ diejenigen Primideale des Körpers k, welche Hauptideale in k sind, dagegen mit $\mathfrak{w}^{(-)}$ diejenigen Primideale des Körpers k, welche nicht Hauptideale in k sind.

Da die Zahlen ω, ω' sicher nicht Quadrate von ganzen Zahlen in k sind und bei unseren Annahmen wegen der Verschiedenheit der Primideale $\mathfrak{q}_1, \ldots, \mathfrak{q}_{\frac{m}{2}+1}, \mathfrak{q}'_1, \ldots, \mathfrak{q}'_{\frac{m}{2}+1}$ das Nämliche auch für das Produkt $\omega\omega'$ gilt, so folgen aus Satz 17 meiner Abhandlung die Gleichungen

$$\left.\begin{aligned} \sum_{(\mathfrak{w}_\omega)} \frac{1}{n(\mathfrak{w}_\omega)^s} &= \frac{1}{2} \log \frac{1}{s-1} + f_\omega(s), \quad (s>1) \\ \sum_{(\mathfrak{w}_{\omega\omega'})} \frac{1}{n(\mathfrak{w}_{\omega\omega'})^s} &= \frac{1}{4} \log \frac{1}{s-1} + f_{\omega\omega'}(s); \quad (s>1) \end{aligned}\right\} \tag{19}$$

hier sind die unendlichen Summen über alle Primideale $\mathfrak{w}_\omega$ bez. $\mathfrak{w}_{\omega\omega'}$ zu erstrecken und $f_\omega(s)$, $f_{\omega\omega'}(s)$ bedeuten Funktionen der reellen Veränderlichen s, welche stets zwischen endlichen Grenzen bleiben, wenn s sich dem Werte 1 nähert; n bezeichnet stets die Norm im Körper k.

Die Primideale $\mathfrak{w}_\omega$ sind offenbar sämtlich von den Primidealen $\mathfrak{w}_{\omega\omega'}$ verschieden und da nach dem vorhin Bewiesenen die Primideale $\mathfrak{w}_\omega$, $\mathfrak{w}_{\omega\omega'}$ sämtlich unter den Primidealen $\mathfrak{w}^{(+)}$ vorkommen, so haben wir

$$\sum_{(\mathfrak{w}^{(+)})} \frac{1}{n(\mathfrak{w}^{(+)})^s} \geqq \sum_{(\mathfrak{w}_\omega)} \frac{1}{n(\mathfrak{w}_\omega)^s} + \sum_{(\mathfrak{w}_{\omega\omega'})} \frac{1}{n(\mathfrak{w}_{\omega\omega'})^s} \qquad (s>1)$$

und folglich wegen (19)

$$\sum_{(\mathfrak{w}^{(+)})} \frac{1}{n(\mathfrak{w}^{(+)})^s} \geqq \frac{3}{4} \log \frac{1}{s-1} + f_\omega(s) + f_{\omega\omega'}(s); \tag{20}$$

hier sind die unendlichen Summen wiederum über alle Primideale mit den betreffenden Eigenschaften zu erstrecken.

Die Primideale $\mathfrak{w}^{(+)}$, $\mathfrak{w}^{(-)}$ erschöpfen offenbar die sämtlichen Primideale $\mathfrak{w}$ in k, und es ist daher

$$\sum_{(\mathfrak{w}^{(+)})} \frac{1}{n(\mathfrak{w}^{(+)})^s} + \sum_{(\mathfrak{w}^{(-)})} \frac{1}{n(\mathfrak{w}^{(-)})^s} = \sum_{(\mathfrak{w})} \frac{1}{n(\mathfrak{w})^s} = \log \frac{1}{s-1} + f(s), \tag{21}$$

wo die Summe $\sum_{(\mathfrak{w})}$ über sämtliche Primideale $\mathfrak{w}$ in k erstreckt werden soll und $f(s)$ wiederum eine für Werte $s > 1$, die sich dem Werte 1 nähern, zwischen endlichen Grenzen bleibende Größe bezeichnet. Aus (20) und (21) zusammen folgt die Ungleichung

$$\sum_{(\mathfrak{w}^{(+)})} \frac{1}{n(\mathfrak{w}^{(+)})^s} - \sum_{(\mathfrak{w}^{(-)})} \frac{1}{n(\mathfrak{w}^{(-)})^s} \geqq \frac{1}{2} \log \frac{1}{s-1} + 2f_{\omega}(s) + 2f_{\omega\omega'}(s) - f(s). \tag{22}$$

Nunmehr stellen wir folgenden Hilfssatz über die Ideale des Körpers k auf:

Hilfssatz 5. Wenn in dem Ausdrucke

$$\sum_{(\mathfrak{w}^{(+)})} \frac{1}{n(\mathfrak{w}^{(+)})^s} - \sum_{(\mathfrak{w}^{(-)})} \frac{1}{n(\mathfrak{w}^{(-)})^s} \qquad (s > 1)$$

die erste Summe über alle Primideale $\mathfrak{w}^{(+)}$ und die zweite Summe über alle Primideale $\mathfrak{w}^{(-)}$ erstreckt wird, so stellt dieselbe eine solche Funktion der reellen Veränderlichen s dar, welche stets unterhalb einer *positiven* endlichen Grenze bleibt, wenn die reelle Veränderliche s sich der Grenze 1 nähert.

Der Beweis dieses Satzes wird durch die nämliche Schlußweise geführt, wie sie beim Beweise des Satzes 31 in meiner Abhandlung angewandt worden ist.

Wir erkennen, daß die Ungleichung (22) unmittelbar einen Widerspruch gegen den Hilfssatz 5 enthält, und mithin ist unsere ursprüngliche Annahme zu verwerfen, d. h. es müssen in der Gleichung (4) die Exponenten $v_1, \ldots, v_{\frac{m}{2}+1}$ oder das zweitemal in der entsprechenden Gleichung (18) die Exponenten $v_1', \ldots, v_{\frac{m}{2}+1}'$ sämtlich 0 sein; in der Zahl ω bez. ω' haben wir also eine Zahl des Körpers k, welche als Ideal das Quadrat eines Ideals in k darstellt, die überdies kongruent dem Quadrat einer Zahl in k nach dem Modul 2^2 wird und doch nicht das Quadrat einer Zahl in k ist.

Der Körper $K\left(\sqrt{\omega}\right)$ bez. $K\left(\sqrt{\omega'}\right)$ ist der gesuchte Klassenkörper Kk zum Grundkörper k, da er die in Satz 9a ausgesprochene Eigenschaft besitzt. Damit ist die schwierigste Aufgabe in der hier erörterten Theorie gelöst.

§ 12.

Der Beweis für den Satz 9b sowie für die zweite Aussage des Satzes 9c ist aus den bisherigen Entwicklungen leicht zu entnehmen. Nicht so einfach gelingt der Nachweis für die erste Aussage des Satzes 9c, wonach jedes Primideal des Körpers k, das in k der Hauptklasse angehört, im Klassenkörper Kk, der jetzt $K\left(\sqrt{\omega}\right)$ ist, weiter zerlegbar sein muß. Wir führen diesen Nachweis in folgender Weise:

Nach dem in § 11 Bewiesenen ist die Zahl ω von der Gestalt (4):

$$\omega = \varepsilon_1^{u_1} \varepsilon_2^{u_2} \cdots \varepsilon_{\frac{m}{2}+1}^{u_{\frac{m}{2}+1}},$$

wo die Exponenten $u_1, \ldots, u_{\frac{m}{2}+1}$ gewisse Werte 0, 1 haben, aber nicht sämtlich gleich 0 sind: es sei etwa $u_i = 1$; dann bezeichnen wir die Zahlen $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{i-1}, \varepsilon_{i+1}, \ldots, \varepsilon_{\frac{m}{2}}, \varepsilon_{\frac{m}{2}+1}$ bez. mit $\varepsilon_1^*, \ldots, \varepsilon_{\frac{m}{2}}^*$ und bestimmen $\frac{m}{2}$ von r verschiedene Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_{\frac{m}{2}}$ in k derart, daß

$$\left(\frac{\varepsilon_k^*}{\mathfrak{p}_k}\right) = -1, \quad \left(\frac{\varepsilon_k^*}{\mathfrak{p}_k}\right) = +1, \qquad (h \neq k)$$
$$\left(h, k = 1, 2, \ldots, \frac{m}{2}\right)$$
$$\left(\frac{\omega}{\mathfrak{p}_h}\right) = +1, \qquad \left(h = 1, 2, \ldots, \frac{m}{2}\right) \tag{23}$$

wird. Wegen (23) sind nach der zweiten Aussage des Satzes 9c diese Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_{\frac{m}{2}}$ sämtlich Hauptideale in k; wir setzen

$$\mathfrak{p}_1 = (\pi_1), \ldots, \mathfrak{p}_{\frac{m}{2}} = \left(\pi_{\frac{m}{2}}\right),$$

wo $\pi_1, \ldots, \pi_{\frac{m}{2}}$ ganze Zahlen in k bedeuten. Nunmehr wollen wir zeigen, daß ein Ausdruck von der Gestalt

$$\omega^* = \varepsilon_1^{*u_1^*} \cdots \varepsilon_{\frac{m}{2}}^{*u_{\frac{m}{2}}^*} \pi_1^{v_1} \cdots \pi_{\frac{m}{2}}^{v_{\frac{m}{2}}}, \tag{24}$$
$$\left(u_1^*, \ldots, u_{\frac{m}{2}}^*, v_1, \ldots, v_{\frac{m}{2}} = 0, 1\right)$$

nur dann eine primäre Zahl in k darstellen kann, wenn die Exponenten $u_1^*, \ldots, u_{\frac{m}{2}}^*, v_1, \ldots, v_{\frac{m}{2}}$ sämtlich den Wert 0 haben. In der Tat, wäre ω^* primär und wenigstens einer dieser Exponenten gleich 1, so beweisen wir wie oben durch Hilfssatz 4, daß alle Primideale in k, welche in $K\left(\sqrt{\omega^*}\right)$ zerlegbar werden, in k Hauptideale sind, d. h. es müßten dann alle Primideale $\mathfrak{w}$, nach welchen ω^* quadratischer Rest ist, Hauptideale in k sein. Die Tatsache, daß zugleich auch alle Primideale $\mathfrak{w}$, nach denen ω quadratischer Rest ist, Hauptideale in k sind, führt uns wie früher in § 11 auf einen Widerspruch.

Aus der soeben erkannten Tatsache, daß der Ausdruck (24) außer der Zahl 1 niemals eine primäre Zahl darstellen kann, ziehen wir leicht durch ein ähnliches Schlußverfahren, wie wir es früher angewandt haben, diese Folgerung: wenn $\varkappa$ eine beliebige zu 2 prime ganze Zahl in k ist, so läßt sich stets ein System von Exponenten $u_1^*, \ldots, u_{\frac{m}{2}}^*, v_1, \ldots, v_{\frac{m}{2}}$ finden, derart, daß der Ausdruck

$$\varkappa\, \varepsilon_1^{*u_1^*} \cdots \varepsilon_{\frac{m}{2}}^{*u_{\frac{m}{2}}^*} \pi_1^{v_1} \cdots \pi_{\frac{m}{2}}^{v_{\frac{m}{2}}} \tag{25}$$

eine primäre Zahl in k darstellt.

Es sei nun $\mathfrak{q}$ irgendein Primideal der Hauptklasse in k; wir setzen $\mathfrak{q} = (\varkappa)$, wo $\varkappa$ eine ganze Zahl in k bedeutet und nehmen entgegen der zu beweisenden Behauptung an, es sei $\mathfrak{q}$ in $K\left(\sqrt{\omega}\right)$ unzerlegbar. Wir bilden für die Zahl $\varkappa$ den Ausdruck (25) und bezeichnen denselben mit α. Endlich bestimmen wir in k ein von $\mathfrak{r}$ verschiedenes Primideal $\bar{\mathfrak{r}}$, welches in k nicht Hauptideal ist, und eine Zahl σ in k, so daß $\sigma = \mathfrak{r}\bar{\mathfrak{r}}$ wird; wir setzen $\bar{\omega} = \frac{\omega\sigma^2}{\varrho^2}$ oder $\bar{\omega} = \omega$, je nachdem ω den Faktor $\mathfrak{r}^2$ enthält oder nicht.

Da nach Satz 9b der Körper $K\left(\sqrt{\omega}\right)$ eine ungerade Klassenanzahl besitzt, so gilt mit Rücksicht darauf, daß α primär ist, nach dem in meiner Abhandlung für diesen Fall bewiesenen quadratischen Reziprozitätsgesetz die Formel

$$\left\{\frac{\alpha}{\sqrt{\bar{\omega}}}\right\} = \left\{\frac{\sqrt{\bar{\omega}}}{\alpha}\right\}; \tag{26}$$

hierbei habe die geschwungene Klammer für den Körper $K\left(\sqrt{\omega}\right)$ die entsprechende Bedeutung des quadratischen Restcharakters, wie die gewöhnliche Klammer für den Körper k. Das Hauptideal $\sqrt{\bar{\omega}}$ im Körper $K\left(\sqrt{\omega}\right)$ ist entweder gleich 1 oder gleich dem Primideal $\bar{\mathfrak{r}}$. Fällt nun $\left(\frac{\alpha}{\bar{\mathfrak{r}}}\right) = +1$ aus, so ist gewiß auch $\left\{\frac{\alpha}{\bar{\mathfrak{r}}}\right\} = +1$. Ist $\left(\frac{\alpha}{\bar{\mathfrak{r}}}\right) = -1$, so wird wegen $\left(\frac{\omega}{\bar{\mathfrak{r}}}\right) = -1$ notwendig $\left(\frac{\alpha\omega}{\bar{\mathfrak{r}}}\right) = +1$ und um so mehr $\left\{\frac{\alpha\omega}{\bar{\mathfrak{r}}}\right\} = +1$. Andererseits ist wegen $\omega = \left(\sqrt{\omega}\right)^2$ notwendig $\left\{\frac{\omega}{\bar{\mathfrak{r}}}\right\} = +1$ und folglich auch $\left\{\frac{\alpha}{\bar{\mathfrak{r}}}\right\} = +1$. Wir haben also in jedem Falle gewiß $\left\{\frac{\alpha}{\sqrt{\bar{\omega}}}\right\} = +1$ und wegen (26) folgt hieraus

$$\left\{\frac{\sqrt{\bar{\omega}}}{\alpha}\right\} = +1. \tag{27}$$

Wenn A irgendeine ganze zu $\mathfrak{q}$ prime Zahl in $K\left(\sqrt{\omega}\right)$ bedeutet, so gelten nach dem Primideal $\mathfrak{q}$ des Körpers k, das auch in $K\left(\sqrt{\omega}\right)$ Primideal bleiben

sollte, folgende Kongruenzen

$$\left\{\frac{A}{\mathfrak{q}}\right\} \equiv A^{\frac{n(\mathfrak{q})^2-1}{2}}, \quad (\mathfrak{q})$$

$$\left(\frac{NA}{\mathfrak{q}}\right) \equiv (NA)^{\frac{n(\mathfrak{q})-1}{2}}, \quad (\mathfrak{q})$$

und da

$$SA \equiv A^{n(\mathfrak{q})}, \quad NA = A^{n(\mathfrak{q})+1}, \quad (\mathfrak{q})$$

ausfällt, so wird mithin

$$\left\{\frac{A}{\mathfrak{q}}\right\} = \left(\frac{NA}{\mathfrak{q}}\right).$$

Nehmen wir insbesondere $A = \sqrt{\bar{\omega}}$, so erhalten wir

$$\left\{\frac{\sqrt{\bar{\omega}}}{\varkappa}\right\} = \left(\frac{-\bar{\omega}}{\varkappa}\right). \tag{28}$$

Andererseits ist wegen (23) allgemein das Primideal $\mathfrak{p}_h$ in $K\left(\sqrt{\omega}\right)$ zerlegbar; wir setzen

$$\mathfrak{p}_h = \mathfrak{P}_h \cdot S\mathfrak{P}_h, \qquad \left(h = 1, 2, \ldots, \frac{m}{2}\right)$$

wo $\mathfrak{P}_h$ ein Primideal in $K\left(\sqrt{\omega}\right)$ bedeutet. Da

$$\left\{\frac{\sqrt{\bar{\omega}}}{\mathfrak{p}_h}\right\} = \left\{\frac{\sqrt{\bar{\omega}}}{\mathfrak{P}_h}\right\}\left\{\frac{\sqrt{\bar{\omega}}}{S\mathfrak{P}_h}\right\}, \qquad \left\{\frac{\sqrt{\bar{\omega}}}{\mathfrak{P}_h}\right\} = \left\{\frac{-\sqrt{\bar{\omega}}}{S\mathfrak{P}_h}\right\}$$

wird, so haben wir

$$\left\{\frac{\sqrt{\bar{\omega}}}{\mathfrak{p}_h}\right\} = \left\{\frac{-1}{\mathfrak{P}_h}\right\} = \left(\frac{-1}{\mathfrak{p}_h}\right). \tag{29}$$

Wegen (27), (28), (29) ist mit Rücksicht auf die Bedeutung von α

$$\left(\frac{-\bar{\omega}}{\varkappa}\right)\left(\frac{-1}{\pi_1}\right)^{v_1} \cdots \left(\frac{-1}{\pi_{\frac{m}{2}}}\right)^{v_{\frac{m}{2}}} = +1$$

und folglich

$$\left(\frac{-1}{\alpha}\right)\left(\frac{\bar{\omega}}{\varkappa}\right) = +1. \tag{30}$$

Da die Zahl α primär ist, d. h. dem Quadrat einer ganzen Zahl in k kongruent nach 2^2 ausfällt, so folgt leicht, daß $n(\alpha) \equiv 1$ nach 2^2 und mithin

$$\left(\frac{-1}{\alpha}\right) = (-1)^{\frac{n(\alpha)-1}{2}} = +1$$

sein muß; wir erhalten mithin aus (30) die Gleichung

$$\left(\frac{\bar{\omega}}{\varkappa}\right) = +1 \quad \text{und somit auch} \quad \left(\frac{\omega}{\varkappa}\right) = +1,$$

welche der Annahme widerspricht, wonach $\mathfrak{q}$ in k unzerlegbar sein sollte;

diese Annahme ist somit als unzutreffend erkannt, d. h. jedes Primideal des Körpers k, welches der Hauptklasse in k angehört, zerfällt in $K\left(\sqrt{\omega}\right)$ in das Produkt zweier Primideale, wie Satz 9c in seinem ersten Teile aussagt.

§ 13.

Wir erörtern jetzt die Reziprozitätsgesetze für quadratische Reste im Körper k unter den besonderen Annahmen $h = \overline{h} = 2$, wie sie in § 8 über den Körper k gemacht worden sind. Der erste Ergänzungssatz läßt sich wieder genau wie früher in der Form des Satzes 1 aussprechen, sobald wir dem Begriff „primäres Ideal" die folgende engere Fassung geben: wir nennen in dem zugrunde gelegten Körper k ein zu 2 primes Ideal $\mathfrak{a}$ dann *primär*, wenn für dasselbe

$$\left(\frac{\xi}{\mathfrak{a}}\right) = +1$$

ausfällt — nicht nur für alle Einheiten ξ, sondern auch für diejenigen ganzen Zahlen ξ in k, die Quadrate von Idealen sind, d. h. wenn

$$\left(\frac{\varepsilon_1}{\mathfrak{a}}\right) = +1, \qquad \left(\frac{\varepsilon_2}{\mathfrak{a}}\right) = +1, \ldots, \left(\frac{\varepsilon_m^{\frac{2^m}{2}+1}}{\mathfrak{a}}\right) = +1$$

wird. Indem wir in entsprechender Weise den Begriff eines hyperprimären Ideals in dem zugrunde liegenden Körper k enger fassen, gilt auch der zweite Ergänzungssatz in der früher aufgestellten Form des Satzes 2 und ebenso auch das allgemeine Reziprozitätsgesetz in der Fassung des Satzes 3.

Um den Beweis für diese Reziprozitätsgesetze zu führen, bedenken wir, daß der Klassenkörper $K\left(\sqrt{\omega}\right)$ eine ungerade Klassenanzahl hat. Für einen solchen Körper habe ich das Reziprozitätsgesetz in meiner Abhandlung bereits bewiesen. Aus diesem Reziprozitätsgesetz für den Körper $K\left(\sqrt{\omega}\right)$ gewinnen wir sodann ohne Schwierigkeit durch ein geeignetes Schlußverfahren die eben genannten Reziprozitätsgesetze für den Körper k.

In meiner Abhandlung habe ich unter den in § 3 der vorliegenden Arbeit gemachten Annahmen gezeigt, wie die Idealklassen eines beliebigen in bezug auf k relativquadratischen Körpers in Geschlechter einzuteilen sind. Unter der gegenwärtigen Annahme $h = \overline{h} = 2$, die wir im § 8 für den Körper k gemacht haben, teilen wir die Idealklassen eines beliebigen relativquadratischen Körpers $K\left(\sqrt{\mu}\right)$ in bezug auf k auf folgende Weise in Geschlechter ein. Es sei $\mathfrak{J}$ ein beliebiges Ideal des relativquadratischen Körpers $K\left(\sqrt{\mu}\right)$. Wir definieren zunächst wie in dem Falle, den meine Abhandlung betrifft, das Charakterensystem einer Zahl des Körpers k. Sodann verstehen wir unter $\mathfrak{r}$ ein bestimmtes zu 2 primes Ideal, welches nicht der Hauptklasse in k angehört, und wählen dann den Exponenten $u = 0, 1$ derart, daß im Körper k das Produkt der Relativnorm von $\mathfrak{J}$ dem Ideal $\mathfrak{r}^u$ äquivalent wird: es sei etwa

$$N(\mathfrak{J})\,\mathfrak{r}^u = (\iota),$$

wo ι eine geeignete ganze Zahl in k bedeutet. Endlich bilden wir das Charakterensystem für die Zahl ι und fügen diesem noch die Einheit $(-1)^u$ hinzu. Das so erhaltene System von Einheiten ± 1 heiße das Charakterensystem des Ideals $\mathfrak{J}$. Alle Ideale, die dasselbe Charakterensystem besitzen, bilden ein Geschlecht. *Es gilt wiederum der Fundamentalsatz, daß stets genau die Hälfte aller möglichen Charakterensysteme wirklich durch Geschlechter in $K\left(\sqrt{\mu}\right)$ aertreten sind.*

Wenn für einen Körper k der Wert der Klassenanzahl h im ursprünglichen Sinne und der Klassenanzahl $\overline{h}$ im engeren Sinne zusammenfallen und nicht gleich 2, sondern das Doppelte irgendeiner ungeraden Zahl sind, so bedürfen die in § 8 bis § 13 ausgesprochenen Sätze nur einer geringen und aus meiner Abhandlung leicht zu entnehmenden Abänderung.

§ 14.

Es möge endlich kurz die Annahme behandelt werden, daß der Grundkörper k die Klassenanzahl $h = \overline{h} = 4$ besitzt; wir haben dann zwei Fälle zu unterscheiden:

A. Es gibt eine Klasse C in k derart, daß $C, C^2, C^3, C^4 = 1$ die 4 Klassen des Körpers k darstellen.

B. Es gibt zwei Klassen C_1, C_2 in k derart, daß C_1, C_2, $C_1 C_2 = C_3$, $C_1^2 = C_2^2 = 1$ die 4 Klassen des Körpers k darstellen.

Im Falle A. ist der Klassenkörper Kk des Körpers k relativzyklisch vom Relativgrade 4 in bezug auf k und weist folgende fundamentale Eigenschaften auf:

Satz 11a. Der Klassenkörper Kk hat in bezug auf k die Relativdiskriminante 1.

Satz 11b. Die Klassenzahl H, $\overline{H}$ des Klassenkörpers Kk im ursprünglichen bez. im engeren Sinne ist eine ungerade Zahl. Der Klassenkörper Kk besitzt einen und nur einen relativquadratischen Unterkörper UKk. Die Klassenanzahl von UKk ist das Doppelte einer ungeraden Zahl.

Satz 11c. Diejenigen Primideale in k, welche in k Hauptideale sind, d. h. der Klasse 1 angehören, zerfallen in Kk in das Produkt von 4 Primidealen. Diejenigen Primideale in k, welche der Klasse C^2 angehören, zerfallen in UKk in das Produkt zweier solcher Primideale, die im Körper Kk unzerlegbar bleiben. Diejenigen Primideale in k, welche der Klasse C oder C^3 angehören, bleiben in Kk unzerlegbar; sämtliche Ideale in k werden in Kk Hauptideale.

Von diesen 3 Eigenschaften 11a, 11b, 11c charakterisiert jede für sich allein bei unserer Annahme über den Körper k in eindeutiger Weise den Klassenkörper Kk; wir haben somit insbesondere folgende Sätze:

Satz 12a. Wenn ein relativquadratischer Körper die Relativdiskriminante 1 in bezug auf k besitzt, so stimmt derselbe mit UKk überein. Wenn ein relativ-Abelscher Körper vom Relativgrade 4 in bezug auf k die Relativdiskriminante 1 besitzt, so stimmt er mit Kk überein.

Satz 12b. Wenn ein relativquadratischer Körper in bezug auf k eine Klassenanzahl besitzt, die das Doppelte einer ungeraden Zahl ist, so stimmt dieser Körper mit UKk überein.

Satz 12c. Wenn ein relativ-Abelscher Körper vom Relativgrade 4 in bezug auf k eine ungerade Klassenanzahl besitzt, so stimmt er mit Kk überein.

Im Falle B. ist der Klassenkörper Kk des Körpers k relativ-Abelsch vom Relativgrade 4 und weist folgende fundamentale Eigenschaften auf:

Satz 13a. Der Klassenkörper Kk hat in bezug auf k die Relativdiskriminante 1.

Satz 13b[1]. Die Klassenanzahl des Körpers Kk ist ungerade. Der Klassenkörper Kk besitzt drei relativquadratische Unterkörper UKk_1, UKk_2, UKk_3 in bezug auf k. Die Klassenanzahl eines jeden dieser drei Unterkörper ist gleich dem Doppelten einer ungeraden Zahl.

Satz 13c[1]. Diejenigen Primideale in k, welche in k Hauptideale sind, d. h. der Klasse 1 angehören, zerfallen in Kk in das Produkt von vier Primidealen. Diejenigen Primideale in k, welche der Klasse C_1 angehören, zerfallen in einem jener drei Unterkörper, etwa in UKk_1, in das Produkt von zwei Primidealen und sind in jedem der beiden anderen Unterkörper, also in UKk_2, UKk_3 unzerlegbar. Diejenigen Primideale in k, welche der Klasse C_2 bez. C_3 angehören, zerfallen etwa in UKk_2 bez. UKk_3 in das Produkt von zwei Primidealen und sind in UKk_1, UKk_3 bez. in UKk_1, UKk_2 unzerlegbar. *Sämtliche Ideale des Körpers k werden in jedem der drei relativquadratischen Körper UKk_1, UKk_2, UKk_3 Hauptideale.*

Von diesen Eigenschaften charakterisiert[1] wiederum jede für sich vollständig den Klassenkörper Kk und die drei Unterkörper UKk_1, UKk_2, UKk_3.

Die eben aufgestellten Sätze 11a, 11b, 11c, 12a, 12b, 12c, 13a, 13b, 13c bestätigen, wie wir leicht erkennen, unter der gegenwärtigen Annahme $h = \overline{h} = 4$ sowohl im Falle A. wie im Falle B. die Gültigkeit der weiter unten in § 16 aufgestellten allgemeinen Sätze 14 und 15.

Zum Beweise der Sätze 11, 12, 13 ist vor allem nötig, zu zeigen, daß für den Grundkörper k bei der gemachten Annahme stets wenigstens ein relativquadratischer Körper mit der Relativdiskriminante 1 existiert. Sodann hat man in bezug auf diesen noch einen weiteren relativquadratischen Körper mit der

[1] Die beiden Vermutungen von Satz 13b und der letzte Satz von 13c wurden durch die weitere Entwicklung der Theorie nicht allgemein bestätigt. Der letzte Satz von 13c gilt immer dann, wenn 13b eintrifft. [Anm. d. Herausgeber.]

Relativdiskriminante 1 zu konstruieren, was auf Grund des schon bewiesenen Satzes 9a stets möglich ist.

Wenn für einen Körper k der gemeinsame Wert der Klassenanzahl h im ursprünglichen Sinne und der Klassenanzahl $\overline{h}$ im engeren Sinne nicht gleich 4, sondern das Vierfache irgendeiner ungeraden Zahl ist, so bedürfen die hier ausgesprochenen Sätze nur einer geringen und aus meiner Abhandlung leicht zu entnehmenden Abänderung.

§ 15.

Die im vorstehenden bewiesenen und im folgenden Paragraph (§ 16) allgemein ausgesprochenen Sätze zeigen, daß für die vollständige Untersuchung der arithmetischen Eigenschaften eines beliebig vorgelegten Grundkörpers k vor allem die Kenntnis des zu k gehörigen Klassenkörpers Kk erforderlich ist. Unsere Entwicklungen setzen uns nun in den Stand, in jedem besonderen Falle auf arithmetischem Wege den Klassenkörper Kk wirklich zu finden. Im folgenden wollen wir auf eine transzendente Bestimmungsweise des Klassenkörpers hinweisen, die der bekannten von DIRICHLET ersonnenen Methode der transzendenten Bestimmung der Klassenanzahl entspricht.

Wir machen für den Grundkörper k die besondere Annahme $h = \overline{h} = 2$ und bezeichnen mit $\varkappa$ die in meinem Berichte *Über die Theorie der algebraischen Zahlkörper*[1] im § 25 definierte, dem Körper k eigentümliche Zahl; ferner mögen H die Klassenanzahl des Klassenkörpers Kk und K die entsprechend definierte Zahl für den Klassenkörper Kk bezeichnen: dann gilt die folgende Formel

$$\lim_{s=1}\left\{\sum_{(\mathfrak{j}^{(+)})}\frac{1}{n(\mathfrak{j}^{(+)})^s}-\sum_{(\mathfrak{j}^{(-)})}\frac{1}{n(\mathfrak{j}^{(-)})^s}\right\}=\frac{H\mathsf{K}}{h\varkappa},\qquad (s>1) \tag{31}$$

worin die Summe $\sum_{(\mathfrak{j}^{(+)})}$ über alle Hauptideale $\mathfrak{j}^{(+)}$ in k und die Summe $\sum_{(\mathfrak{j}^{(-)})}$ über alle diejenigen Ideale $\mathfrak{j}^{(-)}$ erstreckt werden soll, die nicht Hauptideale in k sind. Der Ausdruck K enthält in gewisser Weise die Logarithmen der Einheiten des Klassenkörpers Kk, so daß durch denselben die erwünschte Bestimmung des Klassenkörpers ermöglicht ist.

Zum Beweise der Formel (31) betrachten wir das Produkt

$$\zeta(s)=\prod_{(\mathfrak{w})}\frac{1}{1-n(\mathfrak{w})^{-s}}, \tag{32}$$

in welchem $\mathfrak{w}$ alle Primideale des Körpers k durchläuft; dasselbe konvergiert für reelle Werte von $s > 1$ und es ist

$$\lim_{s=1}\{(s-1)\zeta(s)\}=h\varkappa. \tag{33}$$

[1] Vgl. Jber. der Deutschen Mathematiker-Vereinigung 4, 229 (1894—95). Dieser Band S. 115.

Das entsprechende Produkt für den Körper Kk lautet

$$Z(s) = \prod_{(\mathfrak{W})} \frac{1}{1 - nN(\mathfrak{W})^{-s}}, \qquad (s > 1)$$

wo rechter Hand $\mathfrak{W}$ alle Primideale von Kk durchläuft und nN die Norm der Relativnorm von $\mathfrak{W}$ in k, d. h. die Norm in Kk bedeutet. Es ist dann

$$\lim_{s=1} \{(s-1)Z(s)\} = H\mathsf{K}. \qquad (34)$$

Wir unterscheiden nun unter den Primidealen $\mathfrak{W}$ diejenigen, die durch Zerlegung irgendeines Primideals in k entstehen, und diejenigen, die Primideale in k sind. Wegen Satz 9c fällt für die ersteren $N(\mathfrak{W})$ gleich einem Primideal $\mathfrak{w}^{(+)}$ der Hauptklasse in k aus; für die letzteren dagegen ist $N(\mathfrak{W})$ gleich dem Quadrat eines Primideals $\mathfrak{w}^{(-)}$ in k, welches nicht der Hauptklasse in k angehört. Mit Rücksicht hierauf wird

$$Z(s) = \prod_{(\mathfrak{w}^{(+)})} \frac{1}{(1 - n(\mathfrak{w}^{(+)})^{-s})^2} \prod_{(\mathfrak{w}^{(-)})} \frac{1}{1 - n(\mathfrak{w}^{(-)})^{-2s}}$$

und hieraus folgt wegen (32)

$$\frac{Z(s)}{\zeta(s)} = \prod_{(\mathfrak{w}^{(+)})} \frac{1}{1 - n(\mathfrak{w}^{(+)})^{-s}} \prod_{(\mathfrak{w}^{(-)})} \frac{1}{1 + n(\mathfrak{w}^{(-)})^{-s}} = \sum_{(\mathfrak{j}^{(+)})} \frac{1}{n(\mathfrak{j}^{(+)})^s} - \sum_{(\mathfrak{j}^{(-)})} \frac{1}{n(\mathfrak{j}^{(-)})^s};$$

diese Gleichung liefert, wenn wir zur Grenze $s = 1$ übergehen, mit Rücksicht auf (33), (34) den verlangten Beweis der Formel (31).

§ 16.

Es sei endlich k ein völlig beliebiger Zahlkörper. Wir treffen folgende Festsetzungen, in denen gar keine beschränkende Annahme für k liegt:

1. Unter den m konjugierten Körpern $k, k', k'', \ldots, k^{(m-1)}$ gebe es eine beliebige Anzahl s reeller Körper.

2. Die Anzahl der Idealklassen des Körpers k, im engeren Sinne verstanden, sei eine beliebige Zahl $\bar{h}$.

Ein in bezug auf k relativ-Abelscher Körper K heiße *unverzweigt*, wenn die Relativdiskriminante von K in bezug auf k gleich 1 ausfällt, oder, was das nämliche bedeutet, wenn es in k kein Primideal gibt, das durch das Quadrat eines Primideals in K teilbar wird. Wir stellen dann folgende Theoreme auf, die im vorstehenden für gewisse besondere Fälle bewiesen worden sind, deren vollständiger Beweis jedoch, wie ich überzeugt bin, auf Grund der von mir angegebenen Methoden gelingen muß:

Satz 14. *Es gibt in bezug auf k stets einen völlig bestimmten relativ-Abelschen unverzweigten Körper Kk vom Relativgrade $\bar{h}$; dieser Körper Kk heiße der Klassenkörper von k. Der Klassenkörper Kk enthält sämtliche in bezug auf k relativ-Abelschen unverzweigten Körper als Unterkörper.*

Die Relativgruppe des Klassenkörpers Kk ist mit derjenigen Abelschen Gruppe holoedrisch isomorph, die durch die Zusammensetzung der Idealklassen in k bestimmt wird[1].

Diejenigen Primideale $\mathfrak{p}$ des Körpers k, welche der nämlichen Idealklasse von k, im engeren Sinne verstanden, angehören, erfahren im Klassenkörper Kk eine Zerlegung in Primideale der nämlichen Anzahl und der nämlichen Grade, so daß die weitere Zerlegung eines Primideals $\mathfrak{p}$ des Körpers k im Körper K nur von der Klasse abhängt, der das Primideal $\mathfrak{p}$ im Körper k angehört.

Definition 7. Eine ganze Zahl A des Klassenkörpers Kk heiße eine *Ambige* dieses Körpers Kk, wenn sie die beiden folgenden Bedingungen erfüllt:

a) Die ganze Zahl A sei total positiv (vgl. Definition 5); d. h. das durch A dargestellte Ideal gehöre auch im engeren Sinne der Hauptklasse in k an.

b) Jede zu A relativkonjugierte Zahl soll sich von A nur um einen Faktor unterscheiden, welcher eine Einheit in Kk ist.

Eine Ambige heiße eine *Primambige*, wenn sie nicht eine Einheit ist und sich nicht als ein Produkt von zwei Ambigen darstellen läßt, von denen keine eine Einheit ist.

Satz 15. *Jede Ambige des Klassenkörpers Kk stellt ein Ideal des Grundkörpers k dar und umgekehrt jedes Ideal des Grundkörpers k läßt sich durch eine Ambige des Klassenkörpers Kk darstellen; diese ist abgesehen von einem Einheitsfaktor durch jenes Ideal bestimmt.*

Jede Ambige des Klassenkörpers Kk ist mithin auf eine und nur auf eine Weise in ein Produkt von Primambigen zerlegbar, wenn man dabei von der Willkür der auftretenden Einheitsfaktoren absieht.

Die in diesem Satze aufgestellte Eigenschaft kommt unter allen relativ-Abelschen Körpern in bezug auf k allein dem Klassenkörper Kk zu[2].

Das allgemeinste Reziprozitätsgesetz für quadratische Reste drückt sich auch in dem beliebigen Körper k durch die Formel des Satzes 7 aus. Auch das Reziprozitätsgesetz für höhere Potenzreste gestattet eine ebenso einfache und allgemeingültige Fassung[3].

Endlich sei noch bemerkt, daß die zugehörige Verallgemeinerung dieser Entwicklungen zur Begründung einer Theorie der „Ringklassenkörper" führt, d. h. solcher relativ-Abelscher Körper in bezug auf k, die zu den Idealklassen eines Ringes in k in einem entsprechenden engen Zusammenhange stehen, wie der hier behandelte Klassenkörper Kk zu den gewöhnlichen Idealklassen des Körpers k.

[1] Man vergleiche hierzu die Untersuchungen von H. Weber *Über Zahlengruppen in algebraischen Körpern*, Math. Ann. 48, 433 und 49, 83.

[2] In speziellen Fällen auch schon einem echten Unterkörper von Kk. [Anm. d. Her.]

[3] Vgl. die Preisaufgabe der K. Ges. d. Wiss. zu Göttingen für das Jahr 1901. Math. Ann. 51, 159. Die preisgekrönte Arbeit von Furtwängler erscheint demnächst in den Abhandlungen der K. Ges. d. Wiss. zu Göttingen, math. phys. Kl. (Neue Folge II, Nr. 3. 1902.)

11. Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem)[1].

Dem Andenken an Hermann Minkowski gewidmet.

[Mathematische Annalen Bd. 67, S. 281—300 (1909)].

Theorem. *Jede positive ganze Zahl läßt sich als Summe von n-ten Potenzen positiver ganzer Zahlen darstellen, so daß deren Anzahl unterhalb einer Schranke liegt, die nur durch den Exponenten n bedingt ist, dagegen nicht von der darzustellenden Zahl abhängt.*

Dieses Theorem ist allgemein von Waring[2] vermutungsweise ausgesprochen worden; der Beweis für dasselbe gelang jedoch bisher nur in besonderen Fällen, nämlich für

$$n = 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 10.$$

Die Mathematiker, denen wir diese Beweise und zugleich auch scharfsinnige Untersuchungen über die Reduktion der Anzahl der zur Darstellung zu verwendenden Potenzen verdanken, sind J. Liouville ($n = 4$), Maillet[3] ($n = 3$, $n = 5$, $n = 8$), Fleck[4] ($n = 6$), Landau[5] ($n = 3$, $n = 4$), I. Schur ($n = 10$), Hurwitz[6] ($n = 8$), Wieferich[7] ($n = 3$, $n = 4$, $n = 5$, $n = 7$).

Der allgemeine Beweis des Theorems, den ich im folgenden geben werde, gelingt mittels einer *neuartigen Anwendung der Analysis auf die Zahlentheorie*. Während man nämlich sonst in der analytischen Zahlentheorie von arithmetischen Formeln ausgehend durch Grenzübergang zu Integralrelationen für arithmetische Größen gelangt — ich erinnere an die Bestimmung der Klassenanzahlen — oder, wie in der Primzahltheorie, asymptotische Ausdrücke mittels transzendenter Funktionen sucht, so werde ich gegenwärtig umgekehrt von einer gewissen Integralformel ausgehen und aus ihr schließlich eine rein arithmetische Relation gewinnen.

Um diesen Gedanken deutlich hervortreten zu lassen, schicke ich dem Beweise des Theorems zunächst zwei Sätze voraus.

Satz I[1]. *Es sei m eine beliebige positive ganze Zahl, dann gilt identisch in den 5 Variabeln $x_1, \ldots, x_5$ die Integralformel*

$$(x_1^2 + \cdots + x_5^2)^m = C \int_{(S)} \cdots \int (t_1 x_1 + \cdots + t_5 x_5)^{2m}\, dt_1 \cdots dt_5; \qquad (1)$$

dabei bedeutet C eine gewisse durch m bestimmte positive Konstante, nämlich

$$\frac{(2m+1)\,(2m+3)\,(2m+5)}{8\pi^2},$$

und das 5-fache Integral rechts ist über die Kugel S

$$t_1^2 + \cdots + t_5^2 \leqq 1 \qquad (2)$$

zu erstrecken.

Zum Beweise verstehen wir unter $x_1, \ldots, x_5$ irgend welche reellen Größen und bestimmen dann eine orthogonale Substitution der 5 Variabeln $t_1, \ldots, t_5$ in $t_1', \ldots, t_5'$

$$\begin{aligned} t_1' &= \alpha_{11} t_1 + \cdots + \alpha_{51} t_5, \\ &\cdots\cdots\cdots\cdots \\ t_5' &= \alpha_{15} t_1 + \cdots + \alpha_{55} t_5, \end{aligned} \qquad (3)$$

[1] Mit einigen Veränderungen und Zusätzen abgedruckt aus den Nachr. Ges. Wiss. Göttingen, Math.-phys. Kl. **1909**, Sitzg. 6. Februar. S. 17—36.

[2] Meditationes algebricae, ed. III. Cambridge 1782, S. 349—350.

[3] Congrès de Bordeaux 1895. — J. de Mathém., Ser. 5, **2** (1896). — C. r. Acad. Sci. Paris **145** (1907). — Bull. Soc. math. France **36** (1908).

[4] Sitzgsber. Berl. math. Ges. **1906**. — Math. Annalen **64** (1907).

[5] Rendiconti Circ. mat. Palermo **23** (1907). — Math. Annalen **66** (1908).

[6] Math. Annalen **65** (1908).

[7] Math. Annalen **66, 67** (1908—09) (3 Abhandlungen).

[1] In meiner ursprünglichen Veröffentlichung (Nachr. Ges. Wiss. Göttingen, Math.-phys. Kl. **1909**) habe ich mich hier eines gewissen 25-fachen Integrals bedient; daß man dasselbe für den vorliegenden Zweck durch das obige 5-fache Integral ersetzen kann, ist eine sehr dankenswerte, mir von verschiedenen Seiten (F. Hausdorff, J. Kürschák u.a.) gemachte Bemerkung. Der dort von mir formulierte und bewiesene Satz I über das 25-fache Integral beansprucht jedoch deshalb ein selbständiges Interesse, weil er in engster Beziehung zu der schönen Theorie der orthogonalen Invarianten von A. Hurwitz steht (vgl. dessen Abhandlung „Über die Erzeugung der Invarianten durch Integration", Nachr. Ges. Wiss. Göttingen, Math.-phys. Kl. **1897**) und in einfachster Weise den Grundgedanken zum Ausdruck bringt, mittels dessen diesem Forscher der Nachweis für die Endlichkeit des vollen Systems orthogonaler Invarianten gelungen ist.

[Es handelt sich dort um die Formel

$$(x_1^2 + \cdots + x_5^2)^m = C \int_{(T)} \cdots \int (t_{11} x_1 + \cdots + t_{15} x_5)^{2m}\, dt_{11} dt_{12} \cdots dt_{22} dt_{23} \cdots dt_{45} dt_{55},$$

wobei das 25-fache Integral rechts über denjenigen 25-dimensionalen ganz im Endlichen gelegenen Bereich T zu erstrecken ist, der dadurch bestimmt ist, daß seine Punkte $t_{\varkappa\lambda}$ von einem Punkte $o_{\varkappa\lambda}$ des durch die 15 Orthogonalitätsrelationen

$$\begin{aligned} o_{\varkappa 1}^2 + \cdots + o_{\varkappa 5}^2 &= 1, \\ o_{\varkappa 1} o_{\lambda 1} + \cdots + o_{\varkappa 5} o_{\lambda 5} &= 0 \qquad (\varkappa \neq \lambda) \\ (\varkappa, \lambda &= 1, \ldots, 5) \end{aligned}$$

definierten 10-dimensionalen Bereiches Ω eine Entfernung

$$\sum_{\varkappa,\lambda} (t_{\varkappa\lambda} - o_{\varkappa\lambda})^2 \leqq 1$$

besitzen. (Anm. d. Her.)]

in welcher

$$\alpha_{11}=\frac{x_1}{\sqrt{x_1^2+\cdots+x_5^2}},\ \ldots,\ \alpha_{51}=\frac{x_5}{\sqrt{x_1^2+\cdots+x_5^2}} \tag{4}$$

wird. Da die Kugel S bei Anwendung dieser Substitution (3) unverändert bleibt, so geht das Integral der Formel (1) nach Einführung der Integrationsvariabeln $t_1', \ldots, t_5'$ über in

$$(x_1^2+\cdots+x_5^2)^m \int_{(S)} \cdots \int t_1'^{2m}\, dt_1' \cdots dt_5';$$

hierin ist offenbar das 5-fache Integral eine von $x_1, \ldots, x_5$ unabhängige positive Zahl; setzen wir dieselbe gleich $\frac{1}{C}$, so folgt die Formel (1) des Satzes I.

Satz II. *Es sei wiederum m eine beliebige positive ganze Zahl, dann gilt identisch in den 5 Variabeln $x_1, \ldots, x_5$ eine Formel von der Gestalt*

$$(x_1^2+\cdots+x_5^2)^m=\sum_{h=1,\ldots,M} r_h (a_{1h}x_1+\cdots+a_{5h}x_5)^{2m}; \tag{5}$$

dabei ist zur Abkürzung

$$M=\frac{(2m+1)\,(2m+2)\,(2m+3)\,(2m+4)}{1\cdot 2\cdot 3\cdot 4}$$

gesetzt, ferner bedeuten $r_1, \ldots, r_M$ gewisse positive rationale, durch m bestimmte Zahlen und $a_{1h}, \ldots, a_{5h}$ gewisse ganze, ebenfalls nur durch m bestimmte Zahlen.

Der Beweis gründet sich auf die in Satz I aufgestellte Integralformel; von der letzteren ausgehend werden wir durch eine Reihe von Schritten schließlich zu der in Satz II behaupteten arithmetischen Identität gelangen.

Der *erste* Schritt besteht in der Approximation des 5-fachen Integrales

$$C\int_{(S)} \cdots \int (t_1x_1+\cdots+t_5x_5)^{2m}\, dt_1 \cdots dt_5$$

durch eine endliche Summe. Wir denken uns zu dem Zwecke den 5-dimensionalen Raum der Variabeln t_h in 5-dimensionale Würfel von der Kantenlänge ε zerlegt. Da der Bereich S ganz im Endlichen gelegen ist, so fällt nur eine endliche Anzahl $H^{(\varepsilon)}$ dieser Würfel ins Innere von S. Bilden wir sodann für den Mittelpunkt eines jeden dieser Würfel den linearen Ausdruck

$$t_1x_1+\cdots+t_5x_5,$$

multiplizieren denselben mit dem Inhalt ε^5 des Würfels sowie mit dem positiven Werte von $\sqrt[2m]{C}$, so entsteht aus dem Integral eine Summe von der Gestalt

$$\sum_{h=1,\ldots,H^{(\varepsilon)}} \{P_h^{(\varepsilon)}(x)\}^{2m}, \tag{6}$$

wo die $P_h^{(\varepsilon)}$ gewisse $H^{(\varepsilon)}$ lineare Funktionen von $x_1, \ldots, x_5$ bedeuten, deren Koeffizienten noch von ε abhängen; zugleich gilt die Limesgleichung

$$C\int_{(S)} \cdots \int (t_1x_1+\cdots+t_5x_5)^{2m}\, dt_1\, dt_2 \cdots dt_5 = \mathop{\mathrm{L}}_{\varepsilon=0} \sum_{h=1,\ldots,H^{(\varepsilon)}} \{P_h^{(\varepsilon)}(x)\}^{2m}.$$

Nach der Integralformel des Satzes I ist mithin auch

$$(x_1^2+\cdots+x_5^2)^m=\mathop{\mathrm{L}}_{\varepsilon=0} \sum_{h=1,\ldots,H^{(\varepsilon)}} \{P_h^{(\varepsilon)}(x)\}^{2m}. \tag{7}$$

Der *zweite* wesentliche Schritt beruht darauf, daß wir hier in der Summe rechts die Anzahl $H^{(\varepsilon)}$, die ja mit verschwindendem ε notwendig über alle Grenzen wächst, auf eine feste, von ε unabhängige Zahl reduzieren. Dies gelingt in folgender Weise. Wir bedenken, daß es nur M linear unabhängige Formen $2m$-ten Grades von 5 Variabeln gibt und daß daher gewiß zwischen den ersten $M+1$ Formen $2m$-ten Grades

$$\{P_h^{(\varepsilon)}(x)\}^{2m}, \qquad (h=1, \ldots, M+1)$$

eine lineare Identität von der Gestalt

$$c_1 P_1^{(\varepsilon)2m}+c_2 P_2^{(\varepsilon)2m}+\cdots+c_{M+1} P_{M+1}^{(\varepsilon)2m}=0$$

bestehen muß, wo die $c_1, \ldots, c_{M+1}$ reelle Konstante bedeuten, von denen einige positiv und einige negativ ausfallen müssen. Indem wir diese Identität durch den größten unter den positiven Koeffizienten dividieren, entsteht eine Identität von der Gestalt

$$c_1' P_1^{(\varepsilon)2m}+c_2' P_2^{(\varepsilon)2m}+\cdots+c_{M+1}' P_{M+1}^{(\varepsilon)2m}=0,$$

wo gewiß einer unter den Koeffizienten $c_1', \ldots, c_{M+1}'$ den Wert $+1$ besitzt und zugleich alle übrigen Koeffizienten $\leqq 1$ ausfallen. Subtrahieren wir diese Identität von der Summe (6), so hebt sich offenbar eine der $2m$-ten Potenzen fort, und wir erhalten eine Summe über nur $H^{(\varepsilon)}-1$ Summanden, von denen keiner negativ wird, da ja die zu den $P_h^{(\varepsilon)2m}$ hinzutretenden konstanten Faktoren sämtlich positiv ausfallen, wenn sie nicht insbesondere verschwinden. Indem wir diese konstanten Faktoren in die $2m$-te Potenz hineinziehen, gelangen wir zu einer Formel von der Gestalt

$$\sum_{h=1,\ldots,H^{(\varepsilon)}} \{P_h^{(\varepsilon)}(x)\}^{2m}=\sum_{h=1,\ldots,H^{(\varepsilon)}-1} \{P_h'^{(\varepsilon)}(x)\}^{2m},$$

worin die $P_h'^{(\varepsilon)}$ wieder Linearformen der Variabeln $x_1, \ldots, x_5$ bedeuten und die Anzahl der Summanden rechts gegenüber der ursprünglichen Summe links gewiß um 1 vermindert ist.

Das dadurch eingeleitete Reduktionsverfahren können wir fortsetzen, bis schließlich die Zahl der Summanden auf M herabkommt; alsdann erhalten wir eine Formel von der Gestalt:

$$\sum_{h=1,\ldots,H^{(\varepsilon)}} \{P_h^{(\varepsilon)}(x)\}^{2m}=\sum_{h=1,\ldots,M} \{Q_h^{(\varepsilon)}(x)\}^{2m}, \tag{8}$$

wo wiederum die

$$Q_h^{(\varepsilon)}(x)=q_{h1}^{(\varepsilon)}x_1+\cdots+q_{h5}^{(\varepsilon)}x_5 \qquad (h=1, \ldots, M)$$

Linearformen der Variabeln $x_1, \ldots, x_5$ bedeuten, deren Koeffizienten $q_{hk}^{(\varepsilon)}$ wesentlich noch von ε abhängen.

Der *nächste* Schritt besteht in der Ausführung des Grenzüberganges zu $\varepsilon = 0$; dieser erfolgt leicht in der aus (7) und (8) entstehenden Formel

$$(x_1^2 + \cdots + x_5^2)^m = \mathop{\mathrm{L}}_{\varepsilon=0} \sum_{h=1,\ldots,M} \{Q_h^{(\varepsilon)}(x)\}^{2m}. \tag{9}$$

Zunächst ist nämlich klar, daß sämtliche Koeffizienten der Formen $Q_h^{(\varepsilon)}$ unterhalb endlicher von ε unabhängiger Grenzen bleiben, sobald ε gegen 0 konvergiert; dies folgt aus den Limesgleichungen

$$1 = \mathop{\mathrm{L}}_{\varepsilon=0} (q_{1k}^{(\varepsilon)2m} + q_{2k}^{(\varepsilon)2m} + \cdots + q_{Mk}^{(\varepsilon)2m}),$$

wie sie durch Vergleichung der Koeffizienten von x_k^{2m} in (9) entstehen. Wegen des Umstandes, daß hiernach insbesondere $q_{11}^{(\varepsilon)}$ für alle ε unterhalb einer endlichen Grenze bleibt, können wir für ε eine gegen 0 konvergierende Folge von positiven Werten $\varepsilon_1, \varepsilon_2, \cdots$ finden, derart, daß der Limes

$$\mathop{\mathrm{L}}_{r=\infty} q_{11}^{(\varepsilon_r)} = q_{11}$$

existiert. Da ferner, wie gezeigt, auch $q_{21}^{(\varepsilon_r)}$ unterhalb einer endlichen Grenze bleibt, so läßt sich wiederum aus jener Folge von Werten $\varepsilon_1, \varepsilon_2, \ldots$ eine Folge $\varepsilon_1', \varepsilon_2', \ldots$ herausgreifen, so daß auch der Limes

$$\mathop{\mathrm{L}}_{r=\infty} q_{21}^{(\varepsilon_r')} = q_{21}$$

existiert. So fortfahrend erhalten wir schließlich nach $5M$-maliger Anwendung dieses Verfahrens eine gegen 0 konvergierende Folge $\bar{\varepsilon}_1, \bar{\varepsilon}_2, \ldots$ derart, daß zugleich die sämtlichen Limesgleichungen

$$\mathop{\mathrm{L}}_{r=\infty} q_{hk}^{(\bar{\varepsilon}_r)} = q_{hk} \qquad (h = 1, \ldots, M,\ k = 1, \ldots, 5)$$

statthaben. Setzen wir sodann

$$Q_h(x) = q_{h1}x_1 + \cdots + q_{h5}x_5 \qquad (h = 1, \ldots, M),$$

so gilt wegen (9) identisch in den Variabeln $x_1, \ldots, x_5$ die Formel

$$(x_1^2 + \cdots + x_5^2)^m = \sum_{h=1,\ldots,M} Q_h^{2m}(x). \tag{10}$$

Diese Formel unterscheidet sich von der in Satz II behaupteten noch wesentlich dadurch, daß die Koeffizienten der Linearformen Q_h keineswegs rationale Zahlen sind.

Der *letzte* entscheidende Schritt meiner Beweisführung wird darin bestehen, von der Formel (10) den Übergang zu einer Formel zu ermöglichen, in welcher alle auftretenden Zahlenkoeffizienten rational sind. Zu dem Zwecke verschaffen wir uns zunächst M Linearformen

$$G_h(x) = a_{h1}x_1 + \cdots + a_{h5}x_5 \qquad (h = 1, \ldots, M)$$

mit ganzzahligen Koeffizienten a_{hk}, derart, daß zwischen ihren $2m$-ten Potenzen keine lineare Relation mit konstanten Koeffizienten stattfindet. Dies

ist gewiß möglich, da die Determinante

$$A = \begin{vmatrix} a_{11}^{2m} & a_{21}^{2m} & \cdots & a_{M1}^{2m} \\ a_{11}^{2m-1}a_{12} & a_{21}^{2m-1}a_{22} & \cdots & a_{M1}^{2m-1}a_{M2} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ a_{15}^{2m} & a_{25}^{2m} & \cdots & a_{M5}^{2m} \end{vmatrix}$$

offenbar nicht identisch in allen Argumenten a_{hk} Null ist und zur Erfüllung unserer Forderung nur nötig wird, die a_{hk} als ganze rationale Zahlen so zu bestimmen, daß A von Null verschieden ausfällt.

Nun sei in Formel (10) etwa Q_1 eine Linearform, deren Koeffizienten jedenfalls nicht sämtlich verschwinden, so daß

$$q_{11}^2 + \cdots + q_{15}^2$$

eine positive von Null verschiedene Zahl wird. Setzen wir dann zur Abkürzung

$$\alpha_h = \sqrt{\frac{q_{11}^2 + \cdots + q_{15}^2}{a_{h1}^2 + \cdots + a_{h5}^2}} \qquad (h = 1, \ldots, M),$$

so haben die M Linearformen

$$\alpha_1 G_1, \ldots, \alpha_M G_M$$

sämtlich die nämliche Quadratsumme ihrer Koeffizienten wie Q_1; es gibt daher gewiß eine orthogonale Transformation der Variabeln $x_1, \ldots, x_5$, welche Q_1 in $\alpha_1 G_1$, ferner je eine solche orthogonale Transformation, die Q_1 in $\alpha_2 G_2, \ldots$, bzw. in $\alpha_M G_M$ überführt. Wenden wir diese M orthogonalen Transformationen sämtlich der Reihe nach auf die Formel (10) an, addieren die so entstehenden M Formeln und dividieren durch M, so wird, wenn wir noch

$$\varrho_1 = \frac{\alpha_1^{2m}}{M}, \ \ldots, \ \varrho_M = \frac{\alpha_M^{2m}}{M}$$

setzen:

$$(x_1^2 + \cdots + x_5^2)^m = \sum_{h=1,\ldots,M} \varrho_h G_h^{2m}(x) + \sum_{h=1,\ldots,M(M-1)} S_h^{2m}(x), \tag{11}$$

wo die S_h gewisse $M(M-1)$ Linearformen der $x_1, \ldots, x_5$ sind, wie sie aus den $Q_2, \ldots, Q_M$ durch jene orthogonalen Transformationen nach Hineinziehung des Faktors $\frac{1}{\sqrt[2m]{M}}$ entstehen. Wir betrachten nun dasjenige System von M linearen Gleichungen für die M Unbekannten $u_1, \ldots, u_M$, welches aus der Identität

$$\sum_{h=1,\ldots,M} u_h G_h^{2m}(x) = (x_1^2 + \cdots + x_5^2)^m - \sum_{h=1,\ldots,M(M-1)} S_h^{2m}(x)$$

entspringt, wenn man die nämlichen Potenzen und Produkte von Potenzen der Variabeln $x_1, \ldots, x_5$ auf beiden Seiten gleich setzt. Da die Determinante dieses Gleichungssystems bis auf einen Zahlenfaktor die von Null verschiedene

Zahl A ist, so sind dessen Lösungen eindeutig bestimmt; sie lauten wegen (11):

$$u_1 = \varrho_1, \ \ldots, \ u_M = \varrho_M$$

und sind folglich sämtlich *positive* Größen. Da nun die Lösungen eines linearen Gleichungssystems mit einer von Null verschiedenen Determinante stetige Funktionen der rechten Seiten der Gleichungen sind, so folgt, daß, wenn wir die Koeffizienten der Linearformen S_h innerhalb eines gewissen genügend kleinen Spielraumes irgendwie abändern, die Lösungen $u_1, \ldots, u_M$ des abgeänderten Gleichungssystemes ebenfalls noch sämtlich *positive* Zahlen bleiben. Wählen wir dabei die Koeffizienten innerhalb jenes Spielraums als rationale Zahlen, so müssen überdies die Lösungen $u_1, \ldots, u_M$, da ja die Koeffizienten von G_h sämtlich ganze rationale Zahlen sind, ebenfalls rational ausfallen. Bezeichnen S_h' die an Stelle der S_h tretenden Formen mit rationalen Koeffizienten und seien die betreffenden positiven rationalen Lösungen

$$u_1 = r_1, \ \ldots, \ u_M = r_M,$$

so gewinnen wir die Identität

$$(x_1^2 + \cdots + x_5^2)^m = \sum_{h=1,\ldots,M} r_h G_h^{2m}(x) + \sum_{h=1,\ldots,M(M-1)} S_h'^{2m}(x)$$

oder, indem wir noch die in den Koeffizienten von S_h' auftretenden Nenner herausziehen und die neu entstehenden Formen mit $G_{M+1}, \ldots, G_{M^2}$ bezeichnen,

$$(x_1^2 + \cdots + x_5^2)^m = \sum_{h=1,\ldots,M^2} r_h G_h^{2m}(x), \tag{12}$$

wo $r_1, \ldots, r_{M^2}$ nun positive rationale Zahlen und die Koeffizienten der G_h sämtlich ganze Zahlen sind.

Schließlich können wir noch auf diese Formel (12) ein analoges Reduktionsverfahren anwenden wie dasjenige, welches uns oben zu der Formel (8) führte. Wir bedenken, daß zwischen den Linearformen $G_1, \ldots, G_{M+1}$ eine Identität von der Gestalt

$$c_1 G_1^{2m}(x) + \cdots + c_{M+1} G_{M+1}^{2m}(x) = 0 \tag{13}$$

bestehen muß, wo $c_1, \ldots, c_{M+1}$ jetzt rationale Zahlen sind, bestimmen alsdann eine rationale Zahl c derart, daß unter den Zahlen

$$\frac{c c_1}{r_1}, \ \ldots, \ \frac{c c_{M+1}}{r_{M+1}}$$

eine gleich 1 und die übrigen $\leqq 1$ werden. Subtrahieren wir nun die mit c multiplizierte Identität (13) von der rechten Seite der Formel (12), so wird in der rechts entstehenden Summe einer der Koeffizienten Null, ohne daß einer der übrigen negativ ausfällt, so daß die neu entstandene Formel rechts gewiß einen Summanden weniger aufweist. Fahren wir in dieser Weise fort, so gelangen wir schließlich zu einer Formel, die alle in Satz II verlangten Eigenschaften besitzt. Damit ist der Beweis des Satzes II vollendet.

Es sei noch bemerkt, daß, wenn wir in der vorstehenden Überlegung an Stelle von Q_1 nicht eine beliebige der M Linearformen $Q_1, \ldots, Q_M$, sondern eine solche unter diesen M Formen nehmen, für die die Quadratsumme der Koeffizienten am größten ausfällt, es leicht wegen der Identität (10) gelingt, für die betreffende Quadratsumme

$$q_{11}^2 + \cdots + q_{15}^2$$

eine untere nur durch m bedingte Schranke zu bestimmen, und daß aus dieser unteren Schranke wiederum ohne wesentliche Schwierigkeit eine obere Schranke σ für denjenigen Spielraum abzuleiten ist, innerhalb dessen die Koeffizienten der Formen S_h abgeändert werden dürfen, ohne daß die betreffenden Lösungen $u_1, \ldots, u_M$ negativ werden. Durch die Kenntnis von σ aber ist es schließlich auch möglich, für die absoluten Werte der Zähler und Nenner der in der Formel des Satzes II auftretenden rationalen Zahlen r_h und für die absoluten Werte der ganzen Zahlen a_{kh} eine obere Schranke aufzufinden, die nur durch m bedingt ist.

Die Formel des Satzes II bildet den Kernpunkt für den Beweis unseres Theorems. Sie läßt nämlich sofort aus der Gültigkeit des Waringschen Theorems für die m-ten Potenzen auf seine Gültigkeit für die $2m$-ten Potenzen schließen[1]. Denn bezeichnen wir etwa den nur von m abhängigen Generalnenner der in Formel (5) rechts auftretenden rationalen Zahlen r_h mit E, nehmen $x_5 = 0$ und beachten, daß jede Zahl sich als Summe von 4 Quadraten darstellen läßt, so lehrt Formel (5) sofort, daß jede durch E teilbare positive ganze Zahl sich als Summe einer Anzahl von $2m$-ten Potenzen darstellen läßt, die unterhalb einer nur von m abhängigen Schranke liegt, vorausgesetzt, daß der Waringsche Satz für die m-ten Potenzen gilt. Da jede positive ganze Zahl sich in der Form $H \cdot E + K$ darstellen läßt, wo H und K positiv ganz sind und $K < E$ ist, so folgt hieraus, da ja die Zahl K eine Summe von höchstens $E - 1$ Zahlen 1^{2m} ist, das Waringsche Theorem für die $2m$-ten Potenzen.

Wir sehen somit, daß durch das Vorangehende das Waringsche Theorem gewiß für alle unendlich vielen Exponenten der Form $m = 2^r$ bewiesen ist, da es für $m = 2$ gilt. Um es allgemein für beliebige Exponenten zu beweisen, müssen wir der Reihe nach folgende 5 Hilfssätze entwickeln.

Hilfssatz 1. *Zu jedem Exponenten m gehören eine gewisse Anzahl N positiver rationaler Zahlen*

$$r_1, \ r_2, \ \ldots, \ r_N,$$

sowie zwei positive ganze Zahlen a, A von folgender Eigenschaft:

Es seien x und G beliebige positive ganze Zahlen und Γ eine beliebige reelle

[1] Vgl. A. Hurwitz: Math. Annalen 65, 424—427 (1908).

positive Zahl, es sei ferner X eine positive ganze Zahl, die der Ungleichung

$$X < \Gamma^2 x^2 \tag{14}$$

genügt; dann können zu diesen Größen x, G, Γ, X stets N ganze Zahlen ($\leqq 0$)

$$X_1,\ X_2,\ \ldots,\ X_N,$$

deren absolute Beträge den Ungleichungen

$$|X_h| < A\Gamma x \qquad (h = 1, \ldots, N)$$

genügen, derart gefunden werden, daß die Gleichung

$$(G^2x^2 + X)^m = \sum_{h=1,\ldots,N} r_h (aGx + X_h)^{2m}$$

statthat.

Zum Beweise gestalten wir die Formel des Satzes II in folgender Weise um. Zunächst bedenken wir, daß auf der rechten Seite dieser Formel möglicherweise eine oder mehrere der zur $2m$-ten Potenz erhobenen Linearformen lauter verschwindende Koeffizienten haben könnten. Lassen wir diese Potenzen weg, so mögen etwa $N \leqq M$ Summanden rechts übrig bleiben, so daß unsere Formel wie folgt lautet

$$(x_1^2 + \cdots + x_5^2)^m = \sum_{h=1,\ldots,N} r_h (a_{1h}x_1 + \cdots + a_{5h}x_5)^{2m}. \tag{15}$$

Hierin dürfen wir annehmen, daß jede der mit x_1 multiplizierten Zahlen a_{1h} von Null verschieden ist, da andernfalls die Anwendung einer geeigneten orthogonalen Transformation mit rationalen Koeffizienten unsere Formel in eine solche umwandeln würde, in der die jenen Koeffizienten entsprechenden Koeffizienten sämtlich von Null verschieden sind. Endlich setzen wir in unserer Formel (15) für $x_1, x_2, \ldots, x_5$ bzw. die Größen $Gx, x_1, \ldots, x_4$ ein, ferner sei

$$a = |a_{11}a_{12}\cdots a_{1N}|$$

$$\frac{a\,a_{2h}}{a_{1h}} = a'_{1h},\ \frac{a\,a_{3h}}{a_{1h}} = a'_{2h},\ \ldots,\ \frac{a\,a_{5h}}{a_{1h}} = a'_{4h},$$

so daß $a'_{1h}, \ldots, a'_{4h}$ wiederum ganze Zahlen werden. Wir erhalten so die Formel

$$(G^2x^2 + x_1^2 + \cdots + x_4^2)^m = \sum_{h=1,\ldots,N} r_h (aGx + a'_{1h}x_1 + \cdots + a'_{4h}x_4)^{2m}, \tag{16}$$

wo die r_h, wie leicht ersichtlich, eine nicht wesentlich veränderte Bedeutung haben.

Bezeichnen wir nun mit A den größten Wert, den eine der N Zahlen

$$|a'_{1h}| + \cdots + |a'_{4h}| \qquad (h = 1, \ldots, N)$$

annimmt, so folgt Hilfssatz 1 unmittelbar durch folgende Überlegung. Stellen wir die ganze Zahl X als Summe von 4 Quadratzahlen dar und setzen

$$X = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

so folgt aus (14)

$$|x_h| < \Gamma x \qquad (h = 1, \ldots, 4).$$

Nehmen wir daher

$$X_h = a'_{1h}x_1 + \cdots + a'_{4h}x_4,$$

so wird

$$|X_h| \leqq (|a'_{1h}| + \cdots + |a'_{4h}|)\,\Gamma x < A\Gamma x.$$

Hilfssatz 2. *Zu jedem Exponenten m gehören wie in Hilfssatz 1 eine gewisse Anzahl N positiver rationaler Zahlen*

$$r_1,\ r_2,\ \ldots,\ r_N,$$

sowie zwei positive ganze Zahlen a, A von folgender Eigenschaft:

Es seien x, G, Γ Zahlen wie in Hilfssatz 1, es sei ferner X eine positive ganze Zahl, die der Ungleichung

$$X < \Gamma^2 x^2 \tag{17}$$

genügt, dann können zu diesen Größen x, G, Γ, X stets N ganze Zahlen ($\leqq 0$)

$$X_1,\ X_2,\ \ldots,\ X_N,$$

deren absolute Beträge den Ungleichungen

$$|X_h| < A\Gamma x \qquad (h = 1, \ldots, N)$$

genügen, derart gefunden werden, daß die Gleichung

$$x\,(G^2x^2 + X)^m = \frac{1}{G} \sum_{h=1,\ldots,N} r_h (aGx + X_h)^{2m+1}$$

statthat.

Durch Differentiation von (16) nach x entsteht eine Formel von der Gestalt

$$x(G^2x^2 + x_1^2 + \cdots + x_4^2)^{m-1} = \frac{1}{G} \sum_{h=1,\ldots,N} r_h (aGx + a'_{1h}x_1 + \cdots + a'_{4h}x_4)^{2m-1},$$

wo die r_h eine nicht wesentlich veränderte Bedeutung haben. Ersetzen wir hierin m durch $m+1$ und wenden dann die vorige Überlegung auf *diese* Formel statt auf (16) an, so ergibt sich der Beweis des Hilfssatzes 2.

Aus den eben bewiesenen Hilfssätzen 1 und 2 leiten wir jetzt zwei weitere Hilfssätze 3 und 4 ab, in denen gewisse Gleichungen behauptet werden, die sich von den am Schlusse der Hilfssätze 1 und 2 aufgestellten hauptsächlich dadurch unterscheiden, daß auf ihrer linken Seite an Stelle der positiven Zahlen X gewisse Zahlen Y treten, für die auch negative Werte zulässig sind.

Hilfssatz 3. *Zu jedem Exponenten m gehören eine gewisse Anzahl N positiver rationaler Zahlen*

$$r_1,\ r_2,\ \ldots,\ r_N,$$

ferner eine reelle, stets positive Funktion $\varphi(\varkappa)$ der reellen Variabeln $\varkappa$ und endlich eine Funktion $F(K, \varkappa)$ der ganzzahligen Variabeln K und der reellen Variabeln $\varkappa$, die durchweg positive ganzzahlige Werte hat und bei festgehaltenem $\varkappa$ mit unendlich wachsendem K selbst, ohne je abzunehmen, über alle Grenzen wächst; diese zu m zugehörigen Größen r_h, φ, F sind von folgender Beschaffenheit:

Es sei x eine beliebige positive ganze Zahl und K eine beliebige positive Zahl > 16, ferner $\varkappa$ eine reelle, der Ungleichung

$$1 \leqq \varkappa < \frac{1}{2}\sqrt{K} - 1 \tag{18}$$

genügende Größe; es werde endlich

$$\varkappa' = \varphi(\varkappa), \quad K' = F(K, \varkappa) \tag{19}$$

gesetzt; wenn dann Y eine beliebige ganze Zahl ($\gtrless 0$) ist, deren absoluter Betrag der Ungleichung

$$|Y| < \varkappa\sqrt{K}x^2 \tag{20}$$

genügt, so können zu diesen Größen $x, K, \varkappa, Y$ stets N ganze Zahlen $Y'_1, \ldots, Y'_N$ ($\gtrless 0$), deren absolute Beträge die Ungleichungen

$$|Y'_h| < \varkappa'\sqrt{K'}x \tag{21}$$

befriedigen, derart gefunden werden, daß die Gleichung

$$(Kx^2 + Y)^m = \sum_{h=1,\ldots,N} r_h (K'x + Y'_h)^{2m}$$

stattfindet.

Zum Beweise bestimmen wir zunächst eine positive ganze Zahl G durch die Ungleichungen

$$(G + \varkappa)^2 < K \leqq (G + \varkappa + 1)^2; \tag{22}$$

dann wird

$$K - G^2 > \varkappa(2G + \varkappa) \geqq 2\varkappa\sqrt{K} - \varkappa(\varkappa + 2),$$

und da wegen (18)

$$\sqrt{K} > \varkappa + 2$$

ist, so haben wir demnach auch

$$K - G^2 > \varkappa\sqrt{K}. \tag{23}$$

Andererseits ist mit Rücksicht auf (22)

$$K - G^2 \leqq (\varkappa + 1)(2G + \varkappa + 1) < 2(\varkappa + 1)\sqrt{K} \leqq 4\varkappa\sqrt{K},$$

d. h.

$$K - G^2 < 4\varkappa\sqrt{K}. \tag{24}$$

Setzen wir nun

$$X = (K - G^2)x^2 + Y, \tag{25}$$

so gilt wegen (23), (24) infolge der Voraussetzung (20) unseres zu beweisenden Hilfssatzes

$$0 < X < 5\varkappa\sqrt{K}x^2.$$

Wir wenden jetzt den Hilfssatz 1 auf die Zahlen x, G, X an; setzen wir noch darin

$$\Gamma = \sqrt[4]{5\varkappa}\sqrt[4]{K},$$

so wird zugleich auch der Bedingung (14) dieses Hilfssatzes 1 genügt, und derselbe lehrt das Bestehen einer Gleichung von der Gestalt

$$(G^2x^2 + X)^m = \sum_{h=1,\ldots,N} r_h (aGx + Y'_h)^{2m}, \tag{26}$$

wo Y'_h (d. h. die X_h in Hilfssatz 1) ganze den Ungleichungen

$$|Y'_h| < A\sqrt[4]{5\varkappa}\sqrt[4]{K}x \tag{27}$$

genügende Zahlen sind. Setzen wir

$$\varphi(\varkappa) = \frac{A}{\sqrt{a}}\sqrt{10\varkappa}, \quad F(K, \varkappa) = aG,$$

so erfüllen diese Funktionen alle Bedingungen des zu beweisenden Hilfssatzes. Denn wegen (19) wird dann notwendig

$$\varkappa' = \frac{A}{\sqrt{a}}\sqrt{10\varkappa}, \quad K' = aG,$$

und es geht (26) wegen (25) in die zum Schluß des Hilfssatzes 3 behauptete Gleichung über. Endlich ist wegen (18), (22)

$$(2\varkappa + 2)^2 < K \leqq (G + \varkappa + 1)^2,$$

folglich

$$\varkappa + 1 < G,$$

und demnach

$$A\sqrt[4]{5\varkappa}\sqrt[4]{K} \leqq A\sqrt[4]{5\varkappa}\sqrt{G + \varkappa + 1} < A\sqrt{10\varkappa}\sqrt{G},$$

d. h.

$$A\sqrt[4]{5\varkappa}\sqrt[4]{K} < \varkappa'\sqrt{K'}.$$

Wegen dieser Ungleichung geht aus (27) die Ungleichung (21) des Hilfssatzes 3 hervor; dieser Hilfssatz 3 ist mithin vollständig bewiesen.

Hilfssatz 4. *Zu jedem Exponenten m gehören wie in Hilfssatz 3 eine gewisse Anzahl N positiver rationaler Zahlen*

$$r_1, r_2, \ldots, r_N,$$

ferner eine reelle, stets positive Funktion $\varphi(\varkappa)$ der reellen Variabeln $\varkappa$ und endlich eine Funktion $F(K, \varkappa)$ der ganzzahligen Variabeln K und der reellen Variabeln $\varkappa$, die durchweg positive ganzzahlige Werte hat und bei festgehaltenem $\varkappa$ mit unendlich wachsendem K selbst, ohne je abzunehmen, über alle Grenzen

wächst; diese zu m zugehörigen Größen r_h, φ, F sind von folgender Beschaffenheit:

Es seien $x, K, \varkappa$ Zahlen, die denselben Bedingungen wie in Hilfssatz 3 genügen; es werde endlich, wie dort

$$\varkappa' = \varphi(\varkappa), \quad K' = F(K, \varkappa)$$

gesetzt; wenn dann Y eine beliebige ganze Zahl ($\gtreqless 0$) ist, deren absoluter Betrag der Ungleichung

$$|Y| < \varkappa \sqrt{K}\, x^2$$

genügt, so können zu diesen Größen $x, K, \varkappa, Y$ stets N ganze Zahlen $Y'_1, \ldots, Y'_N$ ($\gtreqless 0$), deren absolute Beträge die Ungleichungen

$$|Y'_h| < \varkappa' \sqrt{K'}\, x$$

befriedigen, derart gefunden werden, daß die Gleichung

$$x(Kx^2 + Y)^m = \frac{1}{K'} \sum_{h=1,\ldots,N} r_h (K'x + Y'_h)^{2m+1}$$

stattfindet.

Der Beweis folgt, indem wir die zum Beweis des Hilfssatzes 3 vorhin angewandten Schlußfolgerungen, statt auf Hilfssatz 1, nunmehr auf Hilfssatz 2 beziehen.

Hilfssatz 5. *Zu jedem Exponenten n gehören zwei ganze Zahlen p, q, so daß*

$$n = p + q \tag{28}$$

und

$$0 \leqq p < q \tag{29}$$

ist, ferner eine positive ganze Zahl K und eine gewisse Anzahl N^* positiver rationaler Zahlen

$$k_1,\ k_2,\ \ldots,\ k_{N^*}$$

von folgender Beschaffenheit:

Ist x eine beliebige positive ganze Zahl, Y irgend eine ganze Zahl ($\gtreqless 0$), deren absoluter Betrag der Ungleichung

$$|Y| < \sqrt{K}\, x^q$$

genügt, so gibt es zu diesen Zahlen x, Y stets gewisse N^* positive ganze Zahlen

$$P_1,\ P_2,\ \ldots,\ P_{N^*}$$

derart, daß die Gleichung

$$x^p(Kx^q + Y) = \sum_{h=1,2,\ldots,N^*} k_h P_h^n$$

statthat.

Zum Beweise entwickeln wir den Exponenten n im dyadischen Zahlsystem wie folgt

$$\begin{aligned} n &= 2^g + e_1 2^{g-1} + e_2 2^{g-2} + \cdots + e_{g-1} 2 + e_g \\ &= 1 e_1 e_2 \cdots e_{g-1} e_g, \end{aligned}$$

so daß g ein ganzer Exponent ist und $e_1, e_2, \ldots, e_g$ gewisse Werte Null oder Eins werden. Nun definieren wir $g+1$ Zahlen $n_0, n_1, n_2, \ldots, n_g$ durch folgende Gleichungen

$$\begin{aligned} n_0 &= 1, \\ n_1 &= 2 + e_1 \\ &= 1 e_1, \\ n_2 &= 2^2 + e_1 2 + e_2 \\ &= 1 e_1 e_2, \\ n_3 &= 2^3 + e_1 2^2 + e_2 2 + e_3 \\ &= 1 e_1 e_2 e_3, \\ &\cdots\cdots\cdots\cdots \\ n_g &= 2^g + e_1 2^{g-1} + \cdots + e_{g-1} 2 + e_g \\ &= 1 e_1 e_2 \cdots e_{g-1} e_g = n, \end{aligned}$$

so daß allgemein

$$n_{h+1} = 2n_h + e_{h+1}$$

wird. Ferner setzen wir

$$\begin{aligned} p_0 &= e_1 2^{g-1} + e_2 2^{g-2} + \cdots + e_g \\ &= e_1 e_2 \cdots e_g, \\ p_1 &= e_2 2^{g-2} + e_3 2^{g-3} + \cdots + e_g \\ &= e_2 e_3 \cdots e_g, \\ p_2 &= e_3 2^{g-3} + \cdots + e_g \\ &= e_3 \cdots e_g, \\ &\cdots\cdots\cdots \\ p_{g-1} &= e_g, \\ p_g &= 0, \end{aligned}$$

so daß allgemein

$$p_{h-1} - p_h = e_h 2^{g-h}$$

wird. Endlich sei noch

$$\begin{aligned} p &= n - 2^g = e_1 2^{g-1} + e_2 2^{g-2} + \cdots + e_g = p_0, \\ q &= 2^g, \end{aligned}$$

so daß die Bedingungen (28), (29) erfüllt sind.

Nunmehr wenden wir die Hilfssätze 3 bzw. 4 im ganzen g-mal an und gelangen so zu den Gleichungen

$$\left.\begin{aligned} x^{p_0}(Kx^{2^g} + Y) &= \frac{1}{K'^{e_1}} \sum_{h=1,\ldots,N_1} r_h^{(1)} x^{p_1} (K' x^{2^{g-1}} + Y_h'^{(1)})^{n_1}, \\ x^{p_1}(K_1 x^{2^{g-1}} + Y_1)^{n_1} &= \frac{1}{K_1'^{e_2}} \sum_{h=1,\ldots,N_2} r_h^{(2)} x^{p_2} (K_1' x^{2^{g-2}} + Y_h'^{(2)})^{n_2}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x^{p_{g-2}}(K_{g-2} x^{2^2} + Y_{g-2})^{n_{g-2}} &= \frac{1}{K_{g-2}'^{e_{g-1}}} \sum_{h=1,\ldots,N_{g-1}} r_h^{(g-1)} x^{p_{g-1}} (K_{g-2}' x^2 + Y_h'^{(g-1)})^{n_{g-1}}, \\ x^{p_{g-1}}(K_{g-1} x^2 + Y_{g-1})^{n_{g-1}} &= \frac{1}{K_{g-1}'^{e_g}} \sum_{h=1,\ldots,N_g} r_h^{(g)} (K_{g-1}' x + Y_h'^{(g)})^n. \end{aligned}\right| \tag{30}$$

Dabei ist jede dieser Gleichungen so zu verstehen, daß ihre linke Seite, sobald dort Y_s eine ganze, der Bedingung

$$|Y_s| < \varkappa_s \sqrt[n]{K_s}\, x^{\varrho^{g-s}}$$

genügende Zahl ist, sich in Gestalt der rechts stehenden Summe darstellen läßt, so daß die $Y_h'^{(s+1)}$ passend gewählte, den Ungleichungen

$$|Y_h'^{(s+1)}| < \varkappa_s' \sqrt[n]{K_s'}\, x^{\varrho^{g-s-1}} \tag{31}$$

genügende ganze Zahlen bedeuten. Die Größen $r_h^{(s)}, \varkappa_s, \varkappa_s', K_s, K_s'$ haben hierbei die in Hilfssatz 3 und 4 angegebene Bedeutung; es ist demnach (der untere Index 0 ist stets zu unterdrücken)

$$\left.\begin{aligned} \varkappa_s' &= \varphi_s(\varkappa_s), \\ K_s' &= F_s(K_s, \varkappa_s), \end{aligned} \qquad (s = 0, 1, \ldots, g-1)\right\} \tag{32}$$

wo φ, F die in den Hilfssätzen 3 und 4 auftretenden Funktionen sind. Überdies ist zu beachten, daß allgemein $\varkappa_s$ den Ungleichungen

$$1 \leqq \varkappa_s < \frac{1}{2}\sqrt[n]{K_s} - 1 \tag{33}$$

genügen muß, wodurch auch zugleich $K_s > 16$ wird.

Um nun zum Beweise des Hilfssatzes 5 zu gelangen, muß es möglich sein, die auf den rechten Seiten einer jeden der Formeln (30) stehenden Summanden als linke Seiten der nächstfolgenden Formel zu nehmen, damit sich schließlich die linke Seite der ersten Formel als Summe von Größen ergibt, die die Gestalt der rechten Seite der letzten Formel haben. Um diese Möglichkeit darzutun, setzen wir allgemein

$$K_s = K_{s-1}' \qquad (s = 1, \ldots, g-1) \tag{34}$$

und brauchen dann nur noch zu bewirken, daß die Bedingungen

$$\varkappa' < \varkappa_1,\ \varkappa_1' < \varkappa_2,\ \ldots,\ \varkappa_{g-2}' < \varkappa_{g-1} \tag{35}$$

erfüllt sind.

Wählen wir nun bei der erstmaligen Anwendung des Hilfssatzes 3 bzw. 4 $\varkappa = 1$, so ist dadurch wegen (32)

$$\varkappa' = \varphi(1)$$

bestimmt, während uns die Wahl von K noch freisteht. Da die in den Hilfssätzen auftretende Funktion $F(K, \varkappa)$ bei festem $\varkappa$ mit K zugleich, ohne je abzunehmen, über alle Grenzen wächst und wegen (32), (34)

$$K_1 = F(K, \varkappa) = F(K, 1)$$

ist, so können wir K so groß wählen, daß

$$\frac{1}{2}\sqrt[n]{K_1} - 1 > \varkappa' + 1$$

wird, und dann bleibt diese Ungleichung auch erfüllt, wenn wir K noch vergrößern. Nun setzen wir

$$\varkappa_1 = \varkappa' + 1$$

und genügen damit der ersten der Bedingungen (35) und der Bedingung (33) für $s = 1$. Nach dieser Verfügung über $\varkappa_1$ bestimmt sich $\varkappa_1'$ wegen (32) aus der Gleichung

$$\varkappa_1' = \varphi_1(\varkappa_1).$$

Da nun wiederum die Funktion $F_1(K_1, \varkappa_1)$ bei festem $\varkappa_1$ mit K_1 zugleich, ohne je abzunehmen, über alle Grenzen wächst und wegen (32), (34)

$$K_2 = F_1(K_1, \varkappa_1)$$

ist, so können wir K weiter so groß wählen, daß

$$\frac{1}{2}\sqrt[n]{K_2} - 1 > \varkappa_1' + 1$$

wird, und dann bleibt diese Ungleichung auch erfüllt, wenn wir K noch vergrößern. Nun setzen wir

$$\varkappa_2 = \varkappa_1' + 1$$

und genügen damit der zweiten der Bedingungen (35) und der Bedingung (33) für $s = 2$. In derselben Weise fahren wir fort, bis wir zu der Gleichung

$$\varkappa_{g-1} = \varkappa_{g-2}' + 1$$

gelangen.

Schließlich machen wir K noch so groß, daß

$$\sqrt[n]{K_{g-1}'} > \varkappa_{g-1}'$$

wird; da wegen (31) für $s = g-1$

$$|Y_h'^{(g)}| < \varkappa_{g-1}' \sqrt[n]{K_{g-1}'}\, x,$$

und folglich jetzt

$$|Y_h'^{(g)}| < K_{g-1}'\, x$$

ist, so werden die auf der rechten Seite der letzten Formel in (30) zur n-ten Potenz erhobenen ganzen Zahlen positiv.

Führen wir nun die Substitutionen der linken Seiten der Formeln (30) in den rechten Seiten der jedesmal vorangehenden Formel aus, so entsteht eine Formel von der Gestalt

$$x^p(Kx^q + Y) = \sum_{h=1,\ldots,N^*} k_h (K_{g-1}' x + Y_h'^{(g)})^n,$$

wobei rechts

$$N^* = N_1 N_2 \cdots N_g$$

Summanden stehen und die k_h positive rationale Zahlen sind. Damit ist Hilfssatz 5 bewiesen.

Aus Hilfssatz 5 vermögen wir nun das anfangs aufgestellte Theorem über die Darstellbarkeit der ganzen Zahlen durch n-te Potenzen folgendermaßen abzuleiten.

Wir verstehen unter x eine beliebige positive ganze Zahl $\geqq 2^n$, ferner unter Y_1, Y_2 irgend zwei ganze, den Ungleichungen

$$\left.\begin{aligned} 0 \leqq Y_1 &< \sqrt[n]{K}\, x^q, \\ 0 \leqq Y_2 &< \sqrt[n]{K}\,(x+1)^q \end{aligned}\right\} \tag{36}$$

genügende Zahlen. Dann gelten nach Hilfssatz 5 die Gleichungen

$$x^p[Kx^q - Y_1] = \sum_{h=1,2,\ldots,N^*} k_h P_h^n,$$

$$(x+1)^p[K(x+1)^q + Y_2] = \sum_{h=1,2,\ldots,N^*} k_h Q_h^n$$

und nach Addition

$$x^p[Kx^q - Y_1] + (x+1)^p[K(x+1)^q + Y_2] = \sum_{h=1,2,\ldots,N^*} k_h (P_h^n + Q_h^n), \tag{37}$$

wo die P_h und Q_h gewisse $2N^*$ ganze positive Zahlen sind. Die linke Seite der Formel (37) hat die Gestalt

$$K[x^n + (x+1)^n] + Z,$$

wenn

$$Z = (x+1)^p Y_2 - x^p Y_1$$

gesetzt wird.

Wir überzeugen uns nun davon, daß der Ausdruck

$$(x+1)^p Y_2 - x^p Y_1$$

bei geeigneter, den Ungleichungen (36) entsprechender Wahl von Y_1, Y_2 jede ganze Zahl Z darzustellen vermag, die den Ungleichungen

$$0 \leqq Z \leqq x^n$$

genügt. In der Tat, da die Zahlen $(x+1)^p$ und x^p relativ prim sind, so besitzt erstlich für jedes ganzzahlige Z die diophantische Gleichung

$$Z = (x+1)^p Y_2 - x^p Y_1$$

ganzzahlige Lösungen Y_1, Y_2; nun ist aber zugleich mit Y_1, Y_2 auch

$$Y_1 - T(x+1)^p,$$
$$Y_2 - Tx^p$$

für jedes ganzzahlige T eine Lösung, und daraus wird ersichtlich, daß wir Y_1 der Ungleichung

$$0 \leqq Y_1 < (x+1)^p$$

entsprechend annehmen dürfen. Da $p < q$ ist, so wird $(x+1)^p < x^q$, sobald nur x hinreichend groß, etwa $\geqq 2^n$ gewählt wird; wir haben dann

$$0 \leqq Y_1 < x^q.$$

Mit Rücksicht auf die Ungleichung $Y_1 < (x+1)^p$ folgt ferner

$$Y_2 = \frac{x^p Y_1 + Z}{(x+1)^p} < x^p + \frac{x^n}{(x+1)^p} < x^p + x^q,$$

wenn

$$0 \leqq Z \leqq x^n$$

vorausgesetzt wird, und demnach haben wir mit Rücksicht auf $q > p$, und da Y_2 nicht negativ werden kann,

$$0 \leqq Y_2 < (x+1)^q.$$

Den Ungleichungen (36) ist damit genügt, da ja $K > 16$ ist.

Durch Zusammenfassung des Bisherigen erkennen wir, daß jede in dem durch die Ungleichungen

$$K[x^n + (x+1)^n] \leqq U \leqq K[x^n + (x+1)^n] + x^n$$

bestimmten Intervalle J_x gelegene ganze Zahl U sich in der Gestalt

$$\sum_{h=1,\ldots,N^*} k_h (P_h^n + Q_h^n)$$

darstellen läßt. Von einem hinreichend großen x an greifen nun diese Intervalle J_x übereinander derart, daß die größte Zahl von J_x größer als die kleinste von J_{x+1} ist; in der Tat haben wir gewiß

$$K[x^n + (x+1)^n] + x^n > K[(x+1)^n + (x+2)^n],$$

sobald

$$x > \frac{2\sqrt[n]{K}}{\sqrt[n]{K+1} - \sqrt[n]{K}}$$

genommen wird.

Es lassen sich also alle ganzen Zahlen U, die eine gewisse Größe S überschreiten, in der Gestalt

$$\sum_{h=1,\ldots,N^*} k_h (P_h^n + Q_h^n)$$

darstellen, wo P_h, Q_h gewisse $2N^*$ positive ganze Zahlen bedeuten.

Bezeichnen wir den Generalnenner der rationalen Zahlen k_h mit E, so folgt aus dieser Darstellung nach Multiplikation mit E, daß gewiß jede oberhalb der Größe ES gelegene und durch E teilbare ganze Zahl sich als Summe von n-ten Potenzen positiver ganzer Zahlen darstellen läßt, so daß deren Anzahl unterhalb einer Schranke liegt, die nur von n abhängt. Folglich gilt dies auch für *jede* durch E teilbare und daher auch für jede nicht durch E teilbare ganze Zahl, auf Grund der nämlichen Betrachtung, die oben nach Schluß des Beweises zu Satz II angestellt worden ist. Damit ist das anfangs aufgestellte Theorem, wie es von Waring vermutet worden ist, vollständig bewiesen.

Zum Schluß sei noch bemerkt, daß man durch das vorstehende Beweisverfahren auch zugleich eine obere Schranke für die Anzahl der zur Darstellung einer beliebigen Zahl nötigen n-ten Potenzen wirklich finden kann; dazu ist erforderlich, die am Schluß des Beweises von Satz II gemachte Bemerkung zu berücksichtigen und die in dem soeben vollendeten Beweisverfahren auftretenden Größen so weit abzuschätzen, daß die fragliche Schranke schließlich durch n ausdrückbar ist.

Zu Hilberts algebraisch-zahlentheoretischen Arbeiten.

Von Helmut Hasse.

Hilberts Arbeiten zur algebraischen Zahlentheorie stehen nicht nur rein zeitlich, sondern auch inhaltlich betrachtet an der Wende zweier Jahrhunderte. Sie heben einerseits mit klarem, aufs Große gerichtetem Blick die den Arbeiten der Zahlentheoretiker des alten Jahrhunderts zugrunde liegenden Probleme in großer Allgemeinheit heraus, behandeln sie in dieser Allgemeinheit mit großenteils neuartigen Methoden, die den früheren an Eleganz und Einfachheit weit überlegen sind, und werden so andrerseits richtungweisend für die im neuen Jahrhundert einsetzende Entwicklung, die in den von Hilbert überall mit bewundernswerter Weitsicht vorgezeichneten Bahnen zu einer abschließenden Behandlung dieses Problemkreises geführt hat.

Es handelt sich dabei vornehmlich um das Problem des *Reziprozitätsgesetzes*, das man als im Brennpunkt dieser Entwicklung stehend bezeichnen muß. Um dieses Problem in der ihm vorschwebenden Allgemeinheit angreifen zu können, mußte Hilbert zunächst eine genügend breite Grundlage in der allgemeinen Theorie der algebraischen Zahlkörper legen, deren Fundamentalsatz, von der eindeutigen Primidealzerlegung, einige Zeit vor dem Einsetzen seines Schaffens durch die grundlegenden Arbeiten Dedekinds und Kroneckers bewiesen war. Nachdem er zunächst, in 2 und 3, den Elementen der Theorie, die er zu meistern gedenkt, durch eine elegante Wendung des Beweises dieses Fundamentalsatzes seinen Stempel aufgedrückt hat, wendet sich Hilbert in 4 zu einem eingehenden Studium der Galoisschen Zahlkörper. Das Prinzip dieser Untersuchung, deren Methoden und Ergebnisse für die ganze weitere Entwicklung der Theorie nicht nur des Reziprozitätsgesetzes, sondern weit darüber hinaus von der allergrößten Bedeutung geworden sind, ist die Abbildung der arithmetischen Eigenschaften (Primidealzerlegung, Restklassen nach Primidealpotenzen, Diskriminante) eines Galoisschen Körpers in seine Galoissche Gruppe.

Nunmehr wendet sich Hilbert seinem eigentlichen Problem, dem Reziprozitätsgesetz, zu. An die klassischen Untersuchungen von Gauss und Dirichlet anknüpfend, beginnt er mit der Verallgemeinerung des quadratischen Reziprozitätsgesetzes vom rationalen Zahlkörper R auf den sog. Gaußschen Zahlkörper $k = R(\sqrt{-1})$ der ganzen komplexen Zahlen als Grundkörper. Ebenso wie das Reziprozitätsgesetz in R in der Theorie der quadratischen

Zahlkörper $R(\sqrt{d})$ über R wurzelt, wurzelt das Reziprozitätsgesetz in k in der Theorie der relativ-quadratischen Zahlkörper $k(\sqrt{\partial})$ über k. In dieser körpertheoretischen Art der Darstellung und Deutung des Reziprozitätsgesetzes liegt hier der entscheidende Fortschritt Hilberts, nicht in dem Resultat, das ja schon auf Gauss und Dirichlet zurückgeht.

Des weiteren wendet sich Hilbert dem Reziprozitätsgesetz der l-ten Potenzreste für einen höheren Primzahlexponenten l zu, das als Grundkörper naturgemäß den l-ten Kreiskörper k_l (Körper der l-ten Einheitswurzeln) erfordert. Hilbert beginnt mit dem Studium des allgemeinen m-ten Kreiskörpers k_m für sich. Er entwickelt in 6 einen neuen, auf seine Theorie des Galoisschen Körpers gestützten Beweis des zuerst von Kronecker bewiesenen Fundamentalsatzes, daß jeder Abelsche Zahlkörper Teilkörper eines solchen Kreiskörpers k_m ist.

Für die Behandlung des Reziprozitätsgesetzes der l-ten Potenzreste hatte Hilbert an die Arbeiten Kummers anzuknüpfen, in denen die körpertheoretische Verwurzelung jenes Gesetzes in der Theorie der sog. Kummerschen Körper $k_l(\sqrt[l]{\mu})$ bereits hervortrat. Hilbert gibt hier neue, von den umständlichen und wenig durchsichtigen Rechnungen Kummers freie Beweise. Auch setzt er das Reziprozitätsgesetz hier erstmalig in die elegante Form der Produktformel für das nach ihm benannte Normenrestsymbol. All dies geschieht in dem umfangreichen fünften und letzten Teil des sog. Zahlberichts 7.

In diesem Bericht hat Hilbert alles zur damaligen Zeit in der Theorie der algebraischen Zahlkörper erreichte Wissen gesammelt und zu einer einheitlichen, von großen Gesichtspunkten getragenen Theorie zusammengestellt. Die Resultate seines bisherigen Wirkens auf diesem Gebiete (2—6) sind darin verarbeitet, und überdies sind neben den vorhandenen Ergebnissen anderer Forscher eine große Menge eigener Erkenntnisse hier erstmalig ausgesprochen und gleich in den großen Zusammenhang eingeordnet. Das Werk ist noch heute der gegebene Ausgangspunkt für jeden, der in die Geheimnisse der Theorie der algebraischen Zahlkörper eindringen und der modernen zahlentheoretischen Forschung auf ihre Höhen folgen will.

Wegen dieser grundlegenden Bedeutung des Zahlberichts als Handbuch für das Studium wird er vielfach als der Gipfel der Hilbertschen Leistung auf zahlentheoretischem Gebiet angesehen. Es muß hier klar gesagt werden, daß das keineswegs den Tatsachen entspricht. Von der neuartigen, in 4 entwickelten Theorie des Galoisschen Zahlkörpers abgesehen, handelt es sich ja im Zahlbericht, wie in den in ihm verarbeiteten früheren Arbeiten im wesentlichen um die Durchdringung älterer Resultate mit neuen, eleganten, weittragenden Methoden. Hilberts eigentliche neuen Resultate dagegen setzen jetzt erst ein; sie erwachsen auf dem Boden, den der Zahlbericht geebnet hat, und führen von dort in neue ungeahnte Höhen.

Noch einmal wendet sich HILBERT jetzt, in 8, 9, dem quadratischen Reziprozitätsgesetz zu, nun aber nicht mehr mit der früheren Beschränkung auf den speziellen Gaußschen Grundkörper $k = R(\sqrt{-1})$, sondern für einen allgemeinen algebraischen Zahlkörper k als Grundkörper. Dieser Schritt ist von entscheidender Wichtigkeit, und charakteristisch für die Hilbertsche aufs allgemeine gerichtete Denkweise. Während man bisher zwar die Bedeutung der algebraischen Zahlentheorie für das Reziprozitätsgesetz erkannt hatte, hatte man sich doch durchweg auf die Betrachtung der gerade erforderlichen algebraischen Zahlkörper beschränkt, im Falle des Reziprozitätsgesetzes der l-ten Potenzreste also des l-ten Kreiskörpers als Grundkörper und der Kummerschen Körper $k_l(\sqrt[l]{\mu})$ über ihm[1]. HILBERTS Schritt zu allgemeinen algebraischen Grundkörpern k bedeutet als neue Zielsetzung das Studium der Theorie der allgemeinen algebraischen Zahlkörper, der algebraischen und arithmetischen Gesetzlichkeiten in und über ihnen, *um ihrer selbst willen*, während die klassische Zahlentheorie nur den rationalen Zahlkörper um seiner selbst willen studiert hatte. So entwickelt denn HILBERT jetzt das quadratische Reziprozitätsgesetz im Rahmen einer allgemeinen Theorie der relativ-quadratischen Zahlkörper $k(\sqrt{\mu})$ über einem algebraischen Zahlkörper k, den er allerdings zunächst der wesentlichen Beschränkung unterwerfen muß, daß seine Klassenzahl ungerade ist, ebenso wie ja auch die Kummerschen, im fünften Teil des Zahlberichts behandelten Untersuchungen nur für solche l-te Kreiskörper durchgeführt werden konnten, deren Klassenzahl zu l prim ist („reguläre" Kreiskörper).

Den Gipfel von HILBERTS zahlentheoretischer Leistung hat man ohne Frage in der letzten seiner Arbeiten zur algebraischen Zahlentheorie, in 10, zu sehen, wenn auch — oder vielleicht gerade weil — diese Arbeit einen mehr programmatischen Charakter hat. Hier weist HILBERT zunächst auf, wie man in der Theorie der relativ-quadratischen Zahlkörper die Beschränkung auf Grundkörper ungerader Klassenzahl loswerden kann. Den Schlüssel dazu findet er in der Theorie der *Klassenkörper* eines algebraischen Zahlkörpers, das sind bei HILBERT die unverzweigten relativ-Abelschen Körper. Mit bewundernswertem Weitblick stellt er am Schluß jener Arbeit, wennschon lediglich im Besitz der Theorie des Relativgrades 2, ganz allgemein für diese Klassenkörper den Komplex derjenigen Sätze hin, die man heute als Hauptsätze der Klassenkörpertheorie (im unverzweigten Fall) bezeichnet. Zudem spricht er am Schluß des § 1 sowie durch die Wahl des Titels klar aus, daß

[1] Das gilt sinngemäß auch für HILBERTS Untersuchung 5. Denn die zugrunde liegende Gaußsche Untersuchung zielte auf mehr als bloß das *quadratische* Reziprozitätsgesetz in $R(\sqrt{-1})$, vielmehr auf das *biquadratische* Reziprozitätsgesetz in $R(\sqrt{-1})$, und dafür ist der 4-te Kreiskörper $R(\sqrt{-1})$ naturgemäß erforderlich.

auch die letzte Beschränkung, auf den unverzweigten Fall, in seinen Augen nur eine vorläufige ist, und daß seine programmatisch skizzierte Theorie eine Theorie der allgemeinen relativ-Abelschen Zahlkörper über einem beliebigen algebraischen Zahlkörper anstrebt.

Das neue Jahrhundert hat dieses in seinem Weitblick wie in seinem Wesen großartige Hilbertsche Programm restlos durchführen können, und insbesondere nahezu alle von HILBERT vermuteten Einzeltatsachen bestätigt.

Über die Einzelheiten dieser Entwicklung der Theorie der relativ-Abelschen Zahlkörper ist, in Fortsetzung des Hilbertschen Zahlberichts, ebenfalls im Jahresbericht der Deutschen Mathematiker-Vereinigung, zunächst in kleinerem Rahmen von FUETER[1], später ausführlich von HASSE[2], mit genauen Literaturangaben berichtet worden. Hier mögen nur die Hauptzüge der Entwicklung und die gewonnenen Hauptsätze angeführt werden.

1. Zunächst hat FURTWÄNGLER in unmittelbarer Fortsetzung des Hilbertschen Werks den von HILBERT skizzierten Fall der unverzweigten relativ-Abelschen Körper allgemein durchgeführt und zum Abschluß gebracht. Ferner hat dann TAKAGI, unter Heranziehung von H. WEBERS tiefgreifenden Ansätzen, auch den allgemeinen Fall der relativ-Abelschen Körper beliebiger Relativdiskriminante erledigt.

Die Hauptsätze der so gewonnenen Theorie lauten:

Definition des Klassenkörpers. *Ein algebraischer Körper K über k heißt Klassenkörper zur Idealgruppe H aus k, wenn von den Primidealen aus k alle und nur die zu H gehörigen in K in verschiedene Primideale vom Relativgrade 1 zerfallen.*

Dabei bedeutet „Idealgruppe" irgendeine solche Gruppe von Idealen, die für ein geeignetes ganzes Ideal $\mathfrak{f}$*

1. alle Hauptideale (α) mit $\alpha \equiv 1 \bmod \mathfrak{f}$ enthält,

2. für keinen echten Teiler $\mathfrak{f}_0$ von $\mathfrak{f}$ alle Hauptideale (α) mit $\alpha \equiv 1 \bmod \mathfrak{f}_0$ enthält,

3. nur aus zu $\mathfrak{f}$ primen Idealen besteht.

Das durch diese Forderungen eindeutig bestimmte $\mathfrak{f}$ heißt der „Führer" von H.

[1] Die Klassenkörper der komplexen Multiplikation und ihr Einfluß auf die Entwicklung der Zahlentheorie. Jber. dtsch. Math.-Ver. **20** (1911).

[2] Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil I: Klassenkörpertheorie. Jber. dtsch. Math.-Ver. **35** (1926). Teil Ia: Beweise zu Teil I. Jber. dtsch. Math.-Ver. **36** (1927). Teil II: Reziprozitätsgesetz. Erg.Bd. **6** (1930) zum Jber. dtsch. Math.-Ver.

* In $\mathfrak{f}$ sind dabei, den reellen konjugierten zu k entsprechend, „unendliche Primstellen" als Faktoren zuzulassen, für die die Kongruenz durch die Vorzeichengleichheit der betreffenden reellen konjugierten erklärt ist.

Existenzsatz. *Zu jeder Idealgruppe H in k existiert ein Klassenkörper K über k.*

Isomorphiesatz. *K ist relativ-Abelsch über k, und die Galoissche Relativgruppe von K ist isomorph zur Gruppe der Idealklassen nach der Idealgruppe H als Hauptklasse.*

Die Idealklasseneinteilung hat dabei naturgemäß nur innerhalb der Gruppe aller zu $\mathfrak{f}$ primen Ideale zu erfolgen.

Zerlegungssatz für die Nichtteiler des Führers. *Ist, für ein nicht im Führer $\mathfrak{f}$ von H aufgehendes Primideal $\mathfrak{p}$, $\mathfrak{p}^f$ die früheste Potenz, die in H enthalten ist, so zerfällt $\mathfrak{p}$ in K in verschiedene Primidealfaktoren vom Relativgrade f.*

Diskriminantensatz. *Die Relativdiskriminante von K über k enthält genau diejenigen Primideale, die im Führer $\mathfrak{f}$ von H aufgehen.*

Beide Sätze sind als Spezialfälle in dem folgenden Satz enthalten:

Allgemeiner Zerlegungssatz. *Hat, für ein beliebiges Primideal $\mathfrak{p}$, H innerhalb der engsten H enthaltenden Idealgruppe H_0 von nicht durch $\mathfrak{p}$ teilbarem Führer den Index e, und ist $\mathfrak{p}^f$ als früheste Potenz in H_0 enthalten, so zerfällt $\mathfrak{p}$ in K in e-te Potenzen verschiedener Primideale vom Relativgrade f.*

Anordnungs- und Eindeutigkeitssatz. *Ist K Klassenkörper zu H, K' Klassenkörper zu H', so bedingen sich die Relationen $K' \geqq K$ und $H' \leqq H$ gegenseitig.*

Insbesondere bestimmen sich also eine Idealgruppe H und ihr Klassenkörper K gegenseitig eindeutig.

Die Relation $H' \leqq H$ ist dabei derart zu verstehen, daß H' bei Beschränkung auf die zum Führer $\mathfrak{f}$ von H (aber nicht notwendig sogar zum Führer $\mathfrak{f}'$ von H') primen Ideale Teilmenge von H wird.

Umkehrsatz. *Jeder relativ-Abelsche Körper K über k ist Klassenkörper zu einer Idealgruppe H aus k.*

Der Sinn dieser Sätze ist dieser: Durch die Klassenkörperbeziehung wird eine umkehrbar eindeutige Abbildung des Systems aller relativ-Abelschen Körper K über k auf das System aller Idealgruppen H aus k geliefert, bei der jedem körpertheoretischen Sachverhalt ein bestimmtes Äquivalent für die Idealgruppen entspricht. Man beherrscht so durch das System der Idealgruppen *in* k völlig das System der relativ-Abelschen Körper *über* k.

Insbesondere geht der Umkehrsatz für den Spezialfall des rationalen Zahlkörpers R als Grundkörper k in den oben erwähnten, von Hilbert in 6 behandelten Kroneckerschen Fundamentalsatz über, so wie überhaupt die von Hilbert im vierten Teil des Zahlberichts behandelte Theorie des allgemeinen m-ten Kreiskörpers, von den allgemeinen Sätzen der Klassenkörpertheorie aus gesehen, einfach als Theorie des Klassenkörpers zur Restklasseneinteilung mod. m in R erscheint.

Ferner ergibt sich aus dem Existenzsatz die wichtige Aussage:

Allgemeiner Satz von der arithmetischen Progression. *In jeder Idealklasse nach jeder Idealgruppe H in k existieren unendlich viele Primideale.*

2. Sowohl Furtwängler, von der Theorie der unverzweigten relativ-Abelschen Zahlkörper ausgehend, als auch Takagi, von der Theorie der allgemeinen relativ-Abelschen Zahlkörper ausgehend, haben dann ferner das Reziprozitätsgesetz in einem allgemeinen (die erforderlichen Einheitswurzeln enthaltenden) algebraischen Zahlkörper k behandelt, und zwar beide im wesentlichen nur für Primzahlexponenten l. Gerade hatte Furtwängler begonnen, in gleicher Weise auch den Fall höherer Exponenten mit Erfolg zu behandeln, als Artin mit einem neuen, grundlegenden Satz hervortrat, der sich zunächst in Form einer Ergänzung zu den obigen Hauptsätzen der Klassenkörpertheorie darbietet, der aber andrerseits gerade den Mechanismus darstellt, durch den das Reziprozitätsgesetz mit diesen Sätzen verkettet ist, und den Artin daher schlechthin das allgemeine Reziprozitätsgesetz genannt hat. Dieses Artinsche Reziprozitätsgesetz ist eine Ergänzung zu dem Isomorphiesatz der Klassenkörpertheorie. Es lautet:

Artinsches Reziprozitätsgesetz. *Der Isomorphismus zwischen der Idealklassengruppe nach H und der Galoisschen Relativgruppe von K wird dargestellt, wenn man jedem zum Führer von H primen Primideal $\mathfrak{p}$ von k diejenige Substitution σ der Galoisschen Relativgruppe von K zuordnet, für die gilt:*

$$\sigma A \equiv A^{N(\mathfrak{p})} \bmod \mathfrak{p} \quad \textit{für jedes ganze } A \textit{ aus } K.$$

Es gilt also:

Die Substitution σ hängt nur von der Klasse nach H ab, der $\mathfrak{p}$ angehört, und der Multiplikation der Klassen entspricht dabei die Multiplikation der Substitutionen.

Die Existenz und eindeutige Bestimmtheit einer solchen Substitution σ ist in der von Hilbert in 4, unabhängig von Dedekind und Frobenius, entwickelten Theorie der Galoisschen Körper enthalten; σ ist eine gewisse Erzeugende der zu $\mathfrak{p}$ für K gehörigen Zerlegungsgruppe. Nach Frobenius, der die Zuordnung dieser Substitution σ zu $\mathfrak{p}$ zuerst (auf die Verteilung der $\mathfrak{p}$ bei gegebenem σ hin) untersucht hat, nennt man σ die zu $\mathfrak{p}$ für K gehörige „Frobenius-Substitution". Das Artinsche Reziprozitätsgesetz hat dann insbesondere zur Aufstellung des allgemeinen Reziprozitätsgesetzes der Potenzreste für beliebige Exponenten m in der klassischen Form geführt:

Definition des m-ten Potenzrestsymbols. *Für ein zum Führer von $k(\sqrt[m]{\alpha})$ primes Primideal $\mathfrak{p}$ ist $\left(\frac{\alpha}{\mathfrak{p}}\right)$ derjenige Einheitswurzelfaktor, den die Zahl $\sqrt[m]{\alpha}$ bei Anwendung der zu $\mathfrak{p}$ für $k(\sqrt[m]{\alpha})$ gehörigen Frobenius-Substitution σ bekommt.*

Für ein zum Führer von $k(\sqrt[m]{\alpha})$ (bis auf evtl. m-te Potenzen) primes zusammen-

gesetztes Ideal $\mathfrak{b} = \prod \mathfrak{p}^{\nu}$ *ist*

$$\left(\frac{\alpha}{\mathfrak{b}}\right) = \prod \left(\frac{\alpha}{\mathfrak{p}}\right)^{\nu}.$$

Diese Definition ist sachlich etwas allgemeiner als die in den Arbeiten von HILBERT, FURTWÄNGLER, TAKAGI und ARTIN benutzte, führt aber in den dortigen Spezialfällen ($\mathfrak{b}$ prim zu m) ohne weiteres auf die dort zugrunde gelegte Definition mittels des verallgemeinerten Eulerschen Kriteriums zurück.

Aus seinem Reziprozitätsgesetz folgerte ARTIN durch Anwendung auf die speziellen relativ-Abelschen Körper $k(\sqrt[m]{\alpha})$ unmittelbar:

Das Reziprozitätsgesetz der Potenzreste (1. Form). *Das m-te Potenzrestsymbol* $\left(\frac{\alpha}{\mathfrak{b}}\right)$ *hängt nur von der Klasse ab, der das Ideal* $\mathfrak{b}$ *bei der zu* $k(\sqrt[m]{\alpha})$ *gehörigen Klasseneinteilung angehört.*

Mittels eines Furtwänglerschen Schlußverfahrens leitete ferner HASSE die folgende Tatsache von der klassischen Gestalt des Reziprozitätsgesetzes her:

Das Reziprozitätsgesetz der Potenzreste (2. Form). *Es ist*

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

wenn die Führer von $k(\sqrt[m]{\alpha})$ *und* $k(\sqrt[m]{\beta})$ *zueinander prim sind.*

3. Weiter konnte HASSE auch die elegante Hilbertsche Formulierung des Reziprozitätsgesetzes als Produkttheorem für das Normenrestsymbol in der jetzt erreichten Allgemeinheit geben:

Das Reziprozitätsgesetz als Produkttheorem für das Normenrestsymbol. *Für beliebige* $\beta \neq 0$ *aus k und beliebige relativ-Abelsche Körper K über k ist stets das über alle Primstellen* $\mathfrak{p}$ *von K erstreckte Produkt*

$$\prod_{\mathfrak{p}} \left(\frac{\beta, K}{\mathfrak{p}}\right) = 1.$$

Dabei ist das Symbol $\left(\frac{\beta, K}{\mathfrak{p}}\right)$ als Element der Galoisschen Relativgruppe von K derart erklärt, daß insbesondere gilt:

$\left(\frac{\beta, K}{\mathfrak{p}}\right) = 1$ dann und nur dann, wenn β für jede noch so hohe Potenz von $\mathfrak{p}$ der Norm einer Zahl aus K nach $\mathfrak{p}$ kongruent ist.

Die exakte Definition des Symbols wird, ähnlich wie für das Potenzrestsymbol, durch Zurückführung auf eine FROBENIUS-Substitution gegeben, welche hier allerdings etwas komplizierter ist:

$\left(\frac{\beta, K}{\mathfrak{p}}\right)$ ist die FROBENIUS-Substitution zu $\mathfrak{q}$ für K, wenn $\mathfrak{q}$ aus β durch den Mechanismus bestimmt wird:

$$\beta_0 \equiv \beta \bmod \mathfrak{f}_{\mathfrak{p}}, \quad \beta_0 \equiv 1 \bmod \frac{\mathfrak{f}}{\mathfrak{f}_{\mathfrak{p}}} \qquad (\mathfrak{f} \text{ der Führer von } K, \ \mathfrak{f}_{\mathfrak{p}} \text{ der } \mathfrak{p}\text{-Bestandteil von } \mathfrak{f})$$

und

$$\beta_0 = \mathfrak{p}^b \mathfrak{q} \quad \text{mit einem Primideal } \mathfrak{q} \neq \mathfrak{p}.$$

$\mathfrak{q}$ existiert nach dem allgemeinen Satz von der arithmetischen Progression.

Für den Fall, daß K *zyklisch* über k ist, gilt auch für dieses allgemeine Normenrestsymbol die von HILBERT in seinen Spezialfällen festgestellte Tatsache:

Normensatz. *Dann und nur dann ist β Norm einer Zahl aus K, wenn* $\left(\frac{\beta, K}{\mathfrak{p}}\right) = 1$ *für alle Primstellen* $\mathfrak{p}$ *von K ist.*

Dagegen verliert dieser Satz im allgemeinen seine Gültigkeit, wenn K nicht mehr zyklisch über k ist.

Auf Grund dieses Normensatzes konnte HASSE neuerdings grundlegende Anwendungen der Klassenkörpertheorie auf die Strukturtheorie der einfachen Systeme hyperkomplexer Zahlen über einem algebraischen Zahlkörper k geben. Zufolge dieser Anwendungen und mittels der allgemeinen Begriffsbildungen von E. NOETHER scheint diese Theorie nunmehr rückwärts für die noch offenen großen Probleme in der Theorie der algebraischen Zahlkörper, nämlich die Verallgemeinerung der Klassenkörpertheorie auf allgemeine relativ-Galoissche Zahlkörper, den Zugang zu liefern. Doch ist diese Entwicklung noch zu jung, als daß hier schon darüber berichtet werden könnte.

4. Von den von HILBERT am Schluß von 10 skizzierten Klassenkörpergesetzlichkeiten hat ein Satz auch noch nach fertigem Vorliegen der Furtwängler-Takagischen Theorie und des Artinschen Reziprozitätsgesetzes eine Zeitlang hartnäckig allen Beweisversuchen getrotzt. Es war dies die folgende Tatsache:

Hauptidealsatz. *Im absoluten (d. i. größten unverzweigten) Klassenkörper K zu einem algebraischen Zahlkörper k werden alle Ideale von k zu Hauptidealen.*

Auch diese Tatsache, die wegen ihrer bevorzugten Stellung in dem Hilbertschen Programm zu den am weitesten bekannten Eigenschaften des Klassenkörpers gehört, konnte aber schließlich bewiesen werden, und zwar durch FURTWÄNGLER, nachdem zuvor ARTIN mittels seines Reziprozitätsgesetzes eine Reduktion auf eine rein gruppentheoretische Frage gegeben hatte. Diese Artinsche Reduktion beruht auf dem Gedanken, die Idealklassen des Klassenkörpers K, um deren Studium es sich handelt, durch das Artinsche Reziprozitätsgesetz auf die Substitutionen der Galoisschen Relativgruppe des absoluten Klassenkörpers K' von K, also des zweiten absoluten Klassenkörpers zu k, abzubilden. Dieser Körper K' ist über k nicht mehr Abelsch, sondern nur noch metabelsch. Daher überschreitet der Hauptidealsatz die eigentliche Theorie der relativ-Abelschen Körper, reicht vielmehr in die Theorie der relativ-metabelschen Körper hinein. Bei dem auch heute noch unvollkommenen Stand der Einsicht in ihn — man kann ihn nach FURTWÄNGLER zwar durch kunstvolle Rechnungen bestätigen, aber nicht innerlich verstehen — muß man dem wissenschaftlichen Instinkt HILBERTS, der diesen Satz, lediglich auf fast triviale Spezialfälle gestützt, vorausgesehen hat, staunende Bewunderung zollen.

Verzeichnis der Begriffsnamen.

Die dem Begriffsnamen beigefügten Seitenzahlen bezeichnen diejenigen Stellen, wo die Begriffsnamen definiert werden; in Abh. 7 (S. 63—363) sind dieselben auf der betreffenden Seite fett gedruckt.

Abelscher Körper 141.
Äquivalent (zwei Ideale zueinander) 109.
— (zwei Ideale zueinander, im engeren Sinne) 112, 487.
— (zwei Moduln zueinander) 128.
Algebraische Zahl 69.
Ambige 509.
Ambige Idealklasse 38, 176.
— Klasse 291, 389.
Ambiger Komplex 310, 390.
Ambiges Ideal 9, 37, 154, 176, 291, 374.
— Primideal 154, 374.

Basis der Einheitenschar 290.
— des Ideals 6, 74.
— der Klassenschar 292.
— des Körpers 73.
— des Rings 121.
— des Ringideals 122.
Bereich s. Rationalitäts-, Integritätsbereich.
Bernoullische Zahl 281.

Charaktere der Klasse 119.
Charakterensystem des Ideals 31, 167, 306, 307, 407.
— der Zahl 31, 166, 306, 407, 408.

Dichtigkeit 143.
Differente des Körpers 90.
— der Zahl 71.
Dirichletscher biquadratischer Körper 24, 191.
— Körper, spezieller 24, 47, 191.
Diskriminante 84.
— der Form 120.
— der Modulklasse 128.
— des Rings 121.
— der Zahl 71.

Einheit 102.
Einheitenschar des Kreiskörpers 290.
Einheiten, System von unabhängigen 109.
Einheitenverband 388.
Einheitsform 78.
—, rationale 78.
Einheitswurzeln (bei Primzahlexponent) 195.
— (bei zusammengesetztem Exponent) 198.
Eisensteinsches Reziprozitätsgesetz 231.
Elemente 90.
Engere Fassung des Äquivalenz- und Klassenbegriffs 112, 487.

Faktor der Klassenanzahl des Kreiskörpers, erster, zweiter 237.
Form des Körpers 77.
—, primitive 120.
—, zerlegbare 119.
—, —, des Körpers 120.
—, — (zu einer Ringklasse gehörig) 128.
Form, zerlegbare (eines Moduls) 128.
—, zusammengesetzte 121.
Formenklasse 120.
— (eines Moduls) 128.
Formen, konjugierte 77.
Führer des Rings 122.
Fundamentalform 85.
Fundamentalgleichung 85.
Funktion, zur ganzen Zahl gehörende 265.
—, ganzzahlige 85.

Galoisscher Körper 129.
Ganze algebraische Zahl 70.
— Zahl 70.
Ganzzahlige Funktion 85.
Gebrochene Zahl 109.
Geschlecht 31, 167, 308, 409, 505.
— der Hauptart (im speziellen Dirichletschen Körper) 49.
— des Komplexes 310, 409.
Grad d. Einheitenschar 290.
— der Klassenschar 292.
— des Körpers 69.
— des Primideals 80.
Grundeinheiten, System von 108.
—, System von relativen 150, 396.
Grundideal des Körpers 21, 90.
Grundklassen, System von 119.
Gruppe des Galoisschen Körpers 129.

Hauptgeschlecht 32, 167, 308, 409.
Hauptideal 6, 74.
Hauptklasse 110.
Hauptkomplex 310, 389.
Hauptringklasse 127.
Hauptverband 388.
Hyperprimär 486.

Ideal 6, 73.
—, ambiges 9, 37, 154, 176, 291, 374.
—, hyperprimäres 486.
—, invariantes 130.
—, konjugiertes 81.
—, primäres 434, 485.
—, relativ konjugiertes 93, 373.
— des Ringes 121.
Idealklasse 109.
—, ambige 176.
Idealklassen im engeren Sinne 487, 488.
—, voneinander unabhängige 177.
Inhalt 78.
Inhaltsgleich 78.
Inkongruent 74.
Integritätsbereich 121.
Invariantes Ideal 130.

Klasse s. auch Idealklasse.
—, ambige 291, 389.
—, reziproke 110.
Klassenbegriff, engere Fassung des 112.
Klassenkörper des Körpers 156, 368, 488.
Klassen, relativ konjugierte 291, 389.
Klassenschar des Kummerschen Körpers 292.
Koeffizienten der Form 119.
Komplex 310, 389.
—, ambiger 310, 390.
—, relativ konjugierter 390.
Kongruent 6, 7, 74.
Konjugierte Formen 77.
Konjugiertes Ideal 81.
Konjugierte Körper 69.
— Zahlen 70.
Körper 69.
—, Abelscher 141.
—, den Körper bestimmende Zahl 69.
—, Dirichletscher biquadratischer 24, 191.
—, Dirichletscher, spezieller 24, 47, 191.
—, Galoisscher 129.
—, konjugierte 69.
—, Kummerscher 249.
—, —, regulärer 279.
—, relativ Abelscher 141.
—, — Galoisscher 141.
—, — konjugierte 93, 373.
—, — quadratischer 370.
—, — zyklischer 141.
—, zyklischer 141.
Körperideal, zugeordnetes 126.
Kreiseinheiten 205.
Kreiskörper (der Einheitswurzeln mit Primzahlexponent) 195.
— (der Einheitswurzeln mit zusammengesetztem Exponenten) 198.
— (im weiteren Sinn) 53, 206.
—, regulärer 278.
Kummerscher Körper 249.
— —, regulärer 279.

Lagrangesche Normalbasis 225.
— Wurzelzahl 225.
Logarithmen zur Form 103.
— zur Zahl 103.

Modul 128.
Modulklasse 128.

Nichtprimär 412, 434.
Nichtrest 371.
Normalbasis 216.
—, Lagrangesche 225.
Norm der Form 78.
— des Ideals 79.
— der Zahl 71.
— eines Ringideals 127.
Normennichtrest 162, 257, 365, 380.
Normenrest 162, 257, 365, 380.

Oberkörper 92.

Partialdiskriminante 21, 26.
Partialgrundideal 21.
Partialnorm eines Ideals 15, 31.
— einer Zahl 15, 28.
Potenzcharakter der Zahl in bezug auf das Primideal 228.
Potenzrest nach dem Primideal 228.
Potenz, symbolische (einer Zahl) 149.
—, — (einer Klasse) 291.
—, — (eines Komplexes) 310.
Prim 75.
Primambige 509.
Primär 288, 412, 434, 485, 504.
Primärzahl von einem Primideal 312, 427.
Primform 78.
Primfunktion nach einer Primzahl 86.
Primideal 7, 75.
—, ambiges 154, 374.
— erster Art 313.
—, nichtprimäres 412.
—, primäres 412.
— zweiter Art 313.
Primitive Form 120.
Primitivzahl nach dem Primideal 83.
Primzahl, reguläre 278.
Produkt der Idealklassen 110.
— der Geschlechter 308, 409.

Produkt der Komplexe 310, 390.
— zweier Ideale 7, 74.
— — Ringideale 126.
— — Verbände 389.

Quadratischer Nichtrest 371.
— Rest 371.

Rationale Einheitsform 78.
Rationalitätsbereich, Zahlkörper, Körper 69.
Regulärer Kreiskörper 276.
— Kummerscher Körper 279.
Reguläre Primzahl 278.
Reguläres Ringideal 126.
Regulator des Körpers 108.
Relativ Abelscher Körper 141.
Relativdifferente des Körpers 94, 373.
— der Zahl 94, 373.
Relativdiskriminante des Körpers 95, 373.
— der Zahl 94, 373.
Relative Grundeinheiten 150, 396.
Relativ Galoisscher Körper 141.
Relativgrad 93.
Relativgruppe 141.
Relativkörper 92.
Relativ konjugiertes Ideal 93, 373.
— konjugierte Klassen 291, 389.
— — Komplexe 390.
— — Körper 93.
— — Zahlen 93, 373.
—quadratischer Körper 370.
— zyklisch 141.
Relativnorm des Ideals 93, 373.
— der Zahl 93, 373.
Reziproke Klasse 110.
Reziprozitätsgesetz 43—46, 169, 231, 312, 366, 466, 473, 474, 485, 486, 489.
Ring 121.
Ringideal 121, 127.
— im engeren Sinne 127.
—, reguläres 126.
Ringklasse 127.
Ringklassenkörper 509.

Semiprimär 230.
Spezieller Dirichletscher Körper 24, 47, 191.
Symbol $\left[\frac{d}{\tau}\right]$ 28.
— $\left[\frac{\sigma}{\lambda : \delta}\right]$ 28.
— $\left(\frac{a}{w}\right)$ 160.
— $\left(\frac{n, m}{w}\right)$ 162.
— $\left\{\frac{\alpha}{\mathfrak{p}}\right\}$ 226.
— $\left[\frac{a}{L}\right]$ 234.
— $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ 254.
— $\left\{\frac{\mu}{\mathfrak{l}}\right\}$ 254.
— $\left\{\frac{\mu}{\mathfrak{a}}\right\}$ 254.
— $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ 265.
— $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ 266, 274.
— $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}$ 312.
— $\{\nu, \mu\}$ 346.
— $\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$ 365, 380, 488.
— $[\nu, \mu]$ 366.
— $\left(\frac{\alpha}{\mathfrak{p}}\right)$ 371, 484.
— $\left(\frac{\mu}{\mathfrak{a}}\right)$ 379, 484.
— $\left(\frac{\mathfrak{j}}{\mathfrak{p}}\right)$ 412.
— $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ 453, 467.
Symbole $\left(\frac{\nu, \mu}{\mathfrak{l}}\right), \left(\frac{\nu, \mu}{\mathfrak{l}'}\right), \ldots$ 489.
Symbolische Potenz einer Klasse 291.
— — eines Komplexes 310.
— — einer Zahl 149.
System von Grundeinheiten 108.
— von Grundklassen 119.
— von relativen Grundeinheiten 150, 396.
— von unabhängigen Einheiten 109.

Teilbar (eine Form durch eine andere) 78.
— (ein Ideal durch ein anderes) 7, 74.
— (eine Zahl durch eine andere) 70.
— nach einer Primzahl (eine ganzzahlige Funktion durch eine andere) 85.
Total positiv 487.
Trägheitsgruppe des Primideals 14, 132.
Trägheitskörper des Primideals 15, 132.

Überstrichene Verzweigungsgruppe des Primideals 18, 19, 136, 137.
Überstrichener Verzweigungskörper des Primideals 18, 19, 136, 137.
Unabhängige Einheiten 109.
— Einheitenverbände 389.
— Idealklassen 176.
— Komplexe 390.
— relativquadratische Körper 485.
Untergruppe, den Unterkörper bestimmende 132.
Unterkörper 92.
—, zur Untergruppe gehöriger 131.
Unverzweigter Relativkörper 485, 508.

Verband von Einheiten 388.
Verzweigungsgruppe des Primideals 17, 135.
— des Primideals, einmal, zweimal usw. überstrichene 18, 19, 136, 137.
Verzweigungsideale 264.
Verzweigungskörper des Primideals 17, 135.
— des Primideals, einmal, zweimal usw. überstrichener 18, 19, 136, 137.

Wurzelzahl 218.
—, Lagrangesche 225.

Zahl, algebraische 69.
—, den Körper bestimmende 69.
—, ganze 70.
—, — algebraische 70.
—, hyperprimäre 486.
—, primäre 485, 487.
—, total positive 487.
Zahlbruch 112.
Zahlen, konjugierte 70.
—, relativ konjugierte 93, 373.
Zahlkörper 69.
Zahlring 121.
Zerlegbare Form 119.
Zerlegbare Form des Körpers 120.
— — (eines Moduls) 128.
— — (zu einer Ringklasse gehörig) 128.
Zerlegungsgruppe des Primideals 14, 132.
Zerlegungskörper des Primideals 15, 132.
Zugeordnetes Körperideal 126.
Zusammengesetzte Form 121.
Zyklischer Körper 141.

東京圖書館

Druck von Oscar Brandstetter in Leipzig.

* **Grundzüge der theoretischen Logik.** Von Geheimrat Professor Dr. **David Hilbert,** Göttingen, und **W. Ackermann,** Göttingen. („Grundlehren der mathematischen Wissenschaften", Band XXVII.) VIII, 120 Seiten. 1928. RM 7.60; gebunden RM 8.80

Ein sehr schönes Geschenk ist dieses Buch für jeden denkenden Leser, dem die Logik nicht gleichgültig ist; denn eindringlicher als irgendein anderes Werk von so knappem Umfang zeigt es, was die Logik seit Aristoteles, nach einem dogmatischen Schlummer von mehr als zwei Jahrtausenden, in den letzten anderthalb Menschenaltern an Methoden, Resultaten und Problemen gewonnen hat. Durch diesen fast beispiellosen Aufstieg ist sie eine der interessantesten philosophischen Disziplinen geworden und die einzige philosophische Disziplin, die heute so durchgearbeitet ist, daß sie als eine strenge Wissenschaft vom Range der Mathematik bezeichnet werden darf. . . . Das vorliegende Buch ist der ausgearbeitete Inhalt von Vorlesungen, die Hilbert in drei Semestern in Göttingen gehalten hat.

Das Buch ist ungemein übersichtlich, in vier Kapiteln aufgebaut. 1. Der Aussagenkalkül. 2. Der Prädikaten- und Klassenkalkül. 3. Der engere (d. i. auf „Individuen" als Argumentwerte eingeschränkte) Funktionenkalkül. 4. Der erweiterte (d. i. auf Aussagen, Prädikate, Prädikate von Prädikaten usw. als Argumentwerte ausgedehnte) Funktionenkalkül. . . . *„Deutsche Literaturzeitung."*

Vorlesungen über anschauliche Geometrie. Von Geheimrat Professor Dr. **David Hilbert,** Göttingen. Bearbeitet von Dr. **Stefan Cohn-Vossen,** Köln. („Grundlehren der mathematischen Wissenschaften", Band XXXVII.) Mit etwa 340 Abbildungen. Etwa 360 Seiten. Erscheint im Sommer 1932.

Die Geometrie appelliert in gleicher Weise an den Verstand wie an Einbildungskraft und Vorstellungsvermögen. Sie ist geeignet, von einem größeren Kreis als den eigentlichen Berufsmathematikern erfaßt zu werden und seine Freude an dem Wesen der Mathematik ohne ein zu beschwerliches Studium zu mehren. Die Hilbertschen Vorlesungen sind denn auch von dem Wunsch getragen, neben der Darstellung des Aufbaus dieser schönen Wissenschaft einem weiteren Kreis das Verständnis für sie näherzubringen. Ohne populäre Oberflächlichkeit sind die Ergebnisse und Tatsachen der Geometrie so elementar wie möglich auf Grund der Anschauung dargestellt. Das Verständnis wird besonders erleichtert durch die außerordentlich große Zahl gut und klar durchgearbeiteter Figuren, die sehr leicht vom Leser noch durch Modelle zu vervollkommnen sind. Berücksichtigt man, wie sehr die Geometrie ausgezeichnet ist durch ihre nahen und unmittelbaren Beziehungen zu fast allen naturwissenschaftlichen Betätigungen des menschlichen Geistes, wie sie hineingreift in das praktische Leben, in die Technik ebenso wie in die tiefsten philosophischen Probleme, so wird es klar, daß die Hilbertschen Vorlesungen für einen sehr, sehr großen Kreis von ungemeiner Bedeutung sein werden.

* **Methoden der mathematischen Physik.** Von **R. Courant,** ord. Professor der Mathematik an der Universität Göttingen, und Geheimrat Professor Dr. **David Hilbert,** Göttingen. Erster Band. Zweite, verbesserte Auflage. („Grundlehren der mathematischen Wissenschaften", Band XII.) Mit 26 Abbildungen. XIV, 469 Seiten. 1931. RM 29.20; gebunden RM 30.80

* **Vorlesungen über die Zahlentheorie der Quaternionen.** Von Professor Dr. **Adolf Hurwitz,** Zürich. IV, 74 Seiten. 1919. RM 4.—

* **Niels Henrik Abel.** Eine Schilderung seines Lebens und seiner Arbeit. Von **C. A. Bjerknes.** Umgearbeitete und gekürzte Ausgabe aus Anlaß von Abels 100jährigem Todestag von Dr. V. Bjerknes, Professor an der Universität Oslo. Ins Deutsche übertragen von Else Wegener-Köppen. Mit einem Bildnis. V, 136 Seiten. 1930. RM 6.60; gebunden RM 7.80

* *Auf alle vor dem 1. Juli 1931 erschienenen Bücher wird ein Notnachlaß von 10% gewährt.*

圖書館藏

* **Aus Carl Friedrich Gauss Werken.** Herausgegeben von der **Gesellschaft der Wissenschaften** zu Göttingen.

I. **Disquisitiones Arithmeticae.** Zweiter Abdruck. 478 Seiten. 1870. Kart. RM 48.—

II. **Höhere Arithmetik.** Zweiter Abdruck. 528 Seiten. 1876. Kart. RM 53.—
Nachtrag zum ersten Abdruck des zweiten Bandes. Seite 493—528. 1876. Kart. RM 3.80

III. **Analysis.** Zweiter Abdruck. 499 Seiten. 1876. Kart. RM 50.—

IV. **Wahrscheinlichkeitsrechnung und Geometrie.** Zweiter Abdruck. 492 Seiten. 1880. Kart. RM 50.—

VIII. **Arithmetik. Analysis, Wahrscheinlichkeitsrechnung, Geometrie.** (Nachträge zu Band I—IV.) 458 Seiten. 1900. Kart. RM 46.—

X. Abteilung 1. **Nachlaß und Briefwechsel zur reinen Mathematik.** (Nachträge zu Band I—IV und VIII.) **Tagebuch.** 586 Seiten. 1917. Kart. RM 59.—

X. Abteilung 2. **Abhandlungen über Gauss' wissenschaftliche Tätigkeit auf den Gebieten der reinen Mathematik.**
Abhandlung 1 und 5: Über Gauss' zahlentheoretische Arbeiten. Von Paul Bachmann. — Gauss und die Variationsrechnung. Von Oscar Bolza. 75 und 95 Seiten. 1922. RM 17.—
Abhandlung 4: Gauss als Geometer. Von Paul Staeckel. 123 Seiten. 1923. RM 12.50
Abhandlung 6: Gauss als Zahlenrechner. Von Philipp Maennchen. 76 Seiten. 1930. RM 8.40

---

* **Materialien für eine wissenschaftliche Biographie von Gauss.** Gesammelt von **F. Klein, M. Brendel** und **L. Schlesinger.**

Heft I: **Über Gauss' zahlentheoretische Arbeiten.** Von P. Bachmann in Weimar. III, 54 Seiten. 1911. RM 2.80

Heft IV: **C. F. Gauss als Zahlenrechner.** Von A. Galle in Potsdam.
Heft V: **C. F. Gauss als Geometer.** Von P. Stäckel in Heidelberg. II, 142 Seiten. 1918. RM 7.20

Heft VI: **Die Wechselwirkung zwischen Zahlenrechnen und Zahlentheorie bei C. F. Gauss.** Von Ph. Maennchen in Gießen. II, 47 Seiten. 1918. RM 2.40

Heft VIII: **Zahlbegriff und Algebra bei Gauss.** Von A. Fraenkel in Marburg a. d. Lahn. Mit einem Anhang von A. Ostrowski in Göttingen: Zum ersten und vierten Gausschen Beweise des Fundamentalsatzes der Algebra. 59 Seiten. 1920. RM 3.—

Georg Cantor, Gesammelte Abhandlungen mathematischen und philosophischen Inhalts mit erläuternden Anmerkungen sowie mit Ergänzungen aus dem Briefwechsel Cantor-Dedekind. Herausgegeben von **Ernst Zermelo** nebst einem Lebenslauf Cantors von Adolf Fraenkel. Mit einem Bildnis. VII, 486 Seiten. 1932. RM 48.—

---

* **Moderne Algebra.** Unter Benutzung von Vorlesungen von E. Artin und E. Noether von Dr. **B. L. van der Waerden,** o. Prof. an der Universität Leipzig.
Erster Teil: VIII, 243 Seiten. 1930. RM 15.60; gebunden RM 17.20
Zweiter Teil: VII, 216 Seiten. 1931. RM 15.—; gebunden RM 16.60
(„Grundlehren der mathematischen Wissenschaften", Band XXXIII und XXXIV.)

---

* **Die Theorie der Gruppen von endlicher Ordnung.** Mit Anwendungen auf algebraische Zahlen und Gleichungen sowie auf die Kristallographie. Von **Andreas Speiser,** ord. Professor der Mathematik an der Universität Zürich. Zweite Auflage. („Grundlehren der mathematischen Wissenschaften", Band V.) Mit 38 Textabbildungen. IX, 251 Seiten. 1927. RM 15.—; gebunden RM 16.50

** Auf alle vor dem 1. Juli 1931 erschienenen Bücher wird ein Notnachlaß von 10% gewährt.*

書庫

* **Grundzüge der theoretischen Logik.** Von Geheimrat Professor Dr. **David Hilbert,** Göttingen, und **W. Ackermann,** Göttingen. („Grundlehren der mathematischen Wissenschaften", Band XXVII.) VIII, 120 Seiten. 1928. RM 7.60; gebunden RM 8.80

Ein sehr schönes Geschenk ist dieses Buch für jeden denkenden Leser, dem die Logik nicht gleichgültig ist; denn eindringlicher als irgendein anderes Werk von so knappem Umfang zeigt es, was die Logik seit Aristoteles, nach einem dogmatischen Schlummer von mehr als zwei Jahrtausenden, in den letzten anderthalb Menschenaltern an Methoden, Resultaten und Problemen gewonnen hat. Durch diesen fast beispiellosen Aufstieg ist sie eine der interessantesten philosophischen Disziplinen geworden und die einzige philosophische Disziplin, die heute so durchgearbeitet ist, daß sie als eine strenge Wissenschaft vom Range der Mathematik bezeichnet werden darf. . . . Das vorliegende Buch ist der ausgearbeitete Inhalt von Vorlesungen, die Hilbert in drei Semestern in Göttingen gehalten hat.

Das Buch ist ungemein übersichtlich, in vier Kapiteln aufgebaut. 1. Der Aussagenkalkül. 2. Der Prädikaten- und Klassenkalkül. 3. Der engere (d. i. auf „Individuen" als Argumentwerte eingeschränkte) Funktionenkalkül. 4. Der erweiterte (d. i. auf Aussagen, Prädikate, Prädikate von Prädikaten usw. als Argumentwerte ausgedehnte) Funktionenkalkül. . . . *„Deutsche Literaturzeitung."*

Vorlesungen über anschauliche Geometrie. Von Geheimrat Professor Dr. **David Hilbert,** Göttingen. Bearbeitet von Dr. **Stefan Cohn-Vossen,** Köln. („Grundlehren der mathematischen Wissenschaften", Band XXXVII.) Mit etwa 340 Abbildungen. Etwa 360 Seiten. Erscheint im Sommer 1932.

Die Geometrie appelliert in gleicher Weise an den Verstand wie an Einbildungskraft und Vorstellungsvermögen. Sie ist geeignet, von einem größeren Kreis als den eigentlichen Berufsmathematikern erfaßt zu werden und seine Freude an dem Wesen der Mathematik ohne ein zu beschwerliches Studium zu mehren. Die Hilbertschen Vorlesungen sind denn auch von dem Wunsch getragen, neben der Darstellung des Aufbaus dieser schönen Wissenschaft einem weiteren Kreis das Verständnis für sie näherzubringen. Ohne populäre Oberflächlichkeit sind die Ergebnisse und Tatsachen der Geometrie so elementar wie möglich auf Grund der Anschauung dargestellt. Das Verständnis wird besonders erleichtert durch die außerordentlich große Zahl gut und klar durchgearbeiteter Figuren, die sehr leicht vom Leser noch durch Modelle zu vervollkommnen sind. Berücksichtigt man, wie sehr die Geometrie ausgezeichnet ist durch ihre nahen und unmittelbaren Beziehungen zu fast allen naturwissenschaftlichen Betätigungen des menschlichen Geistes, wie sie hineingreift in das praktische Leben, in die Technik ebenso wie in die tiefsten philosophischen Probleme, so wird es klar, daß die Hilbertschen Vorlesungen für einen sehr, sehr großen Kreis von ungemeiner Bedeutung sein werden.

---

* **Methoden der mathematischen Physik.** Von **R. Courant,** ord. Professor der Mathematik an der Universität Göttingen, und Geheimrat Professor Dr. **David Hilbert,** Göttingen. Erster Band. Zweite, verbesserte Auflage. („Grundlehren der mathematischen Wissenschaften", Band XII.) Mit 26 Abbildungen. XIV, 469 Seiten. 1931. RM 29.20; gebunden RM 30.80

---

* **Vorlesungen über die Zahlentheorie der Quaternionen.** Von Professor Dr. **Adolf Hurwitz,** Zürich. IV, 74 Seiten. 1919. RM 4.—

---

* **Niels Henrik Abel.** Eine Schilderung seines Lebens und seiner Arbeit. Von **C. A. Bjerknes.** Umgearbeitete und gekürzte Ausgabe aus Anlaß von Abels 100jährigem Todestag von Dr. V. Bjerknes, Professor an der Universität Oslo. Ins Deutsche übertragen von Else Wegener-Köppen. Mit einem Bildnis. V, 136 Seiten. 1930. RM 6.60; gebunden RM 7.80

---

* *Auf alle vor dem 1. Juli 1931 erschienenen Bücher wird ein Notnachlaß von 10% gewährt.*