Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörpers.

Von

Philipp Furtwängler in Bonn.

Inhaltsübersicht.

§ 1.

Einleitung. Gang des Beweises.

In drei Mitteilungen, die in den Nachrichten von der Kgl. Gesellschaft der Wissenschaften in Göttingen erschienen sind*), habe ich allgemein den Nachweis geführt, daß zu jedem algebraischen Zahlkörper ein

*) Math.-physik. Klasse 1903, Heft 4 und Heft 5, 1904, Heft 3.

Klassenkörper existiert. Ich gebe im folgenden auf Wunsch der Redaktion dieser Zeitschrift eine zusammenfassende Bearbeitung dieser Entwicklungen, bei der einzelne Abschnitte wörtlich der genannten Stelle entnommen sind.

Die ersten Andeutungen über eine Theorie des Klassenkörpers finden sich wohl bei L. Kronecker, dem die Frage der „zu assoziierenden Gattungen" als ein „erstrebenswertes höchstes Ziel der Theorie der algebraischen Zahlen" erschien.*) Kronecker war durch die Beschäftigung mit der komplexen Multiplikation der elliptischen Funktionen, die für die imaginären quadratischen Bereiche $\sqrt{-n}$ die zu assoziierenden Gattungen liefert, zu der allgemeinen Fragestellung geführt. Er scheint auch über dieses spezielle Beispiel hinaus Einsicht in charakteristische Eigenschaften der zu assoziierenden Gattungen, d. h. des Klassenkörpers, gewonnen zu haben, hat jedoch keine bestimmten Angaben darüber gemacht.**) Den entscheidenden Schritt nach vorwärts hat dann D. Hilbert getan.***) Er hat, vorbereitet durch das Studium der Reziprozitätsgesetze in beliebigen algebraischen Zahlkörpern, das sowohl inhaltlich wie methodisch mit der Theorie des Klassenkörpers auf das engste zusammenhängt, die allgemeinen Eigenschaften des Klassenkörpers aufgedeckt und sie in dem einfachsten Falle, daß die Klassenzahl des Grundkörpers gleich 2 und der Grundkörper nebst sämtlichen konjugierten imaginär ist, bewiesen.

Der Klassenkörper eines beliebigen Grundkörpers k ist ein Oberkörper desselben, der folgende charakteristische Eigenschaften aufweist:

1. Seine Relativgruppe in bezug auf k ist zur Gruppe der Idealklassen in k holoedrisch isomorph, er ist also relativ-Abelsch in bezug auf k.

2. Er ist unverzweigt in bezug auf k, d. h. seine Relativdiskriminante ist gleich 1.

3. Alle Ideale des Grundkörpers werden im Klassenkörper Hauptideale, sie werden also durch wirkliche Zahlen des Klassenkörpers dargestellt.

4. Alle Primideale derselben Klasse des Grundkörpers werden im Klassenkörper gleichartig zerlegt oder genauer: Ist die Klassenzahl des Grundkörpers h und ist g der kleinste Exponent, für den die Äquivalenz

*) Grundzüge einer arithmetischen Theorie der algebraischen Größen, Journal für die reine und angew. Math. 92 (1882), p. 1; speziell sei auf p. 65—68 verwiesen.

**) Er sagt (l. c. p. 68), daß er zur aprioristischen Erkenntnis, nämlich zu einer von der analytischen Entstehung unabhängigen Auffassung der Natur jener den Gattungen $\sqrt{-n}$ assoziierten Gattungen gelangt sei und damit Gesichtspunkte für das Studium der allgemeinen Frage dieser Art der Assoziation gewonnen habe.

***) Über die Theorie der relativ-Abelschen Zahlkörper. Nachr. v. d. Kgl. Ges. d. Wiss. zu Göttingen, Math.-physik. Kl. 1898, p. 370; abgedruckt in Acta Math., Bd. 26.

$\mathfrak{p}^g \sim 1$ in k erfüllt ist, so zerfällt das Primideal $\mathfrak{p}$ aus k im Klassenkörper in $\frac{h}{g}$ verschiedene Primfaktoren.

Die beiden Eigenschaften 1. und 2. definieren den Klassenkörper vollständig und werden deshalb im folgenden zur Konstruktion desselben benutzt werden. Das Problem, das uns beschäftigen soll, läßt sich daher so formulieren:

Es sei ein beliebiger algebraischer Zahlkörper k mit der Klassenzahl h gegeben. Es soll dann ein relativ-Abelscher unverzweigter Oberkörper von k gefunden werden, dessen Relativgruppe mit der Gruppe der Idealklassen in k holoedrisch isomorph ist.

Der Gang der Untersuchung ist kurz folgender. Ebenso wie der Klassenkörper der Gesamtheit der Klassen in k entspricht, so entsprechen jeder Untergruppe der Klassengruppe bestimmte unverzweigte Körper in bezug auf k, die ebenfalls relativ-Abelsch sind, da jede Untergruppe einer Abelschen Gruppe selbst eine Abelsche Gruppe ist. Wie man daher die Klassenzahl h in Potenzen verschiedener Primzahlen zerlegen kann

$$h = l_1^{h_1} \cdot l_2^{h_2} \cdots,$$

so kann man den gesamten Klassenkörper dadurch aufbauen, daß man sukzessive unverzweigte relativ-Abelsche Körper von den Relativgraden $l_1^{h_1}, l_2^{h_2}, \cdots$ in bezug auf k konstruiert. Es genügt, die Konstruktion eines solchen Körpers zu zeigen, da sie für die übrigen analog verläuft. Man setzt daher $h = l^{h'} \cdot q$, wo l eine beliebige Primzahl bedeutet und $q \not\equiv 0(l)$ ist, und betrachtet nur die in der Klassengruppe von k enthaltene Untergruppe vom Grade $l^{h'}$, die alle q^{ten} Potenzen von Idealklassen enthält. Es läuft das auf dasselbe hinaus, als ob die Klassenzahl von k genau gleich $l^{h'}$ wäre, was wir um der einfachen Ausdrucksweise willen ohne Beschränkung der Allgemeinheit annehmen können.

Es sei also das Klassensystem von k in der Gestalt darstellbar:

$$(c)_k = c_1^{x_1} c_2^{x_2} \cdots c_e^{x_e} (x_i = 0, 1, \cdots, l^{h_i'} - 1), \quad h_1' + h_2' + \cdots + h_e' = h',$$

so daß die Klassengruppe in k genau e Basisklassen enthält. Es läßt sich dann der Klassenkörper von k durch Zusammensetzung von e Körpern erzeugen, die relativ zyklisch in bezug auf k von den Relativgraden $l^{h_1'}, \cdots, l^{h_e'}$ sind. Jeder dieser Körper besitzt einen Unterkörper vom Relativgrad l in bezug auf k, so daß im ganzen genau e unabhängige unverzweigte Körper vom Relativgrad l in bezug auf k existieren, die zuerst konstruiert werden müssen.

Ein relativzyklischer Körper vom Primzahlrelativgrad l läßt sich aber am einfachsten definieren, wenn der Grundkörper eine l^{te} Einheitswurzel enthält, da in diesem Falle der Oberkörper durch Adjunktion der Wurzel einer reinen Gleichung $x^l = \omega$ zu k erzeugt wird.

Wir machen daher zuerst die Voraussetzung, daß der Grundkörper k eine primitive l^{te} Einheitswurzel enthalte, und bestimmen unter dieser Voraussetzung e Zahlen $\omega_1, \cdots, \omega_e$ in k, die wir als singuläre Primärzahlen bezeichnen, so daß durch Adjunktion von $\sqrt[l]{\omega_1}, \cdots, \sqrt[l]{\omega_e}$ zu k e voneinander unabhängige unverzweigte Körper vom Relativgrad l in bezug auf k entstehen (§ 2 bis § 7). Um die Unverzweigtheit der entstehenden Körper zu beweisen, ist eine obere Grenze für die Anzahl ihrer ambigen Komplexe zu ermitteln, die sich gleich $e - 1$ ergibt, wenn e, wie oben angegeben, die Anzahl der Basisklassen der Klassengruppe von k bedeutet (§ 3 bis § 5). Auf dieser Grundlage ergibt sich, daß alle Primideale, von denen eine bestimmte singuläre Primärzahl ω l^{ter} Potenzrest ist, in einer Untergruppe der Klassengruppe vom Grade $l^{h'-1}$ liegen, wodurch der Zusammenhang der Zahlen ω mit der Klasseneinteilung der Ideale von k hervortritt (§ 6). Diese Tatsache führt in Verbindung mit einem Satze über gewisse Dirichletsche Reihen (§ 2) zum Nachweis der Unverzweigtheit der Körper $(\sqrt[l]{\omega}, k)$ (§ 7).

Um die unverzweigten Körper vom Relativgrad l zu konstruieren, wenn der Grundkörper k keine l^{te} Einheitswurzel ζ enthält (§ 9), adjungieren wir zu k eine solche und erhalten dadurch einen Körper $k' = (k, \zeta)$, dessen Klassensystem in der Form

$$(c)_k \cdot d$$

darstellbar ist, wo $(c)_k$ das System der Idealklassen von k bedeutet und d alle Klassen aus k', deren Relativnorm in bezug auf k in die Hauptklasse fällt, bezeichnet. Wir konstruieren nun in k' das System der e unabhängigen unverzweigten Körper vom Relativgrad l, die zu der Klassengruppe $(c)_k$ gehören. Es zeigt sich dann, daß jeder dieser Körper nicht nur in bezug auf k', sondern auch in bezug auf k relativ-Abelsch ist. Suchen wir daher diejenigen Unterkörper der konstruierten Körper auf, die zu der Relativgruppe von k' in bezug auf k gehören, so erhalten wir dadurch e unverzweigte unabhängige relativ-Abelsche Körper vom Relativgrad l in bezug auf k.

Eine besondere Behandlung erfordert der Fall $l = 2$, wenn der Körper k oder einer seiner konjugierten reell ist (§ 10). Man muß dann, um sämtliche unverzweigten relativquadratischen Körper in bezug auf den Grundkörper zu erhalten, einen schärferen Äquivalenzbegriff zugrunde legen, nach dem zwei Ideale nur dann äquivalent heißen, wenn ihr Quotient eine total positive Körperzahl ist.

Auf Grund der so geschilderten Entwicklungen gelingt dann der vollständige Aufbau des Klassenkörpers (§ 11).

Die letzten beiden Paragraphen bilden einen Anhang, der mit dem eigentlichen Existenzbeweis in keinem Zusammenhange steht. Im § 12 ist der Nachweis erbracht, daß die komplexe Multiplikation der elliptischen Funktionen für die imaginären quadratischen Körper den zugehörigen Klassenkörper liefert, wobei die Zerlegung der Primideale des Grundkörpers im Klassenkörper den springenden Punkt des Beweises bildet. Im letzten Paragraphen endlich ist aus der Existenz des Klassenkörpers auf Grund der Untersuchungen von H. Weber*) über Zahlengruppen in algebraischen Zahlkörpern gefolgert, daß in jeder Idealklasse eines solchen unendlich viele Primideale existieren.

Es sei hier zum Schluß noch diejenige Literatur angegeben, die für die folgenden Entwicklungen von Wichtigkeit ist, wobei in Klammern die Abkürzung angegeben ist, unter der die betreffende Abhandlung hier zitiert ist:

D. Hilbert, Über die Theorie der relativ-Abelschen Zahlkörper. Nachrichten von der Kgl. Gesellschaft der Wiss. in Göttingen 1898. (Hilbert, Rel. Abelsche Zahlk.)

D. Hilbert, Über die Theorie des relativquadratischen Zahlkörpers. Math. Ann. 51 (1898). (Hilbert, Rel. quadr. Zahlk.)

Ph. Furtwängler, Über das Reziprozitätsgesetz der l^{ten} Potenzreste in algebraischen Zahlkörpern, wenn l eine ungerade Primzahl bedeutet. Abhandlungen der Kgl. Ges. d. Wiss. zu Göttingen, math.-phys. Klasse. Neue Folge, Bd. II, Nr. 3 (1902). (Furtwängler, Reziprozitätsgesetz.)

Ein Auszug aus dieser Arbeit ist in den Math. Ann. 58 (1903), p. 1 erschienen.

D. Hilbert, Die Theorie der algebraischen Zahlkörper. Bericht, erstattet der Deutschen Mathematiker-Vereinigung. 189˙. (Hilbert, Algebr. Zahlk.)

§ 2.

Ein Hilfssatz transzendenter Natur.

Wir haben in diesem Paragraphen zunächst einen Satz über die Summe einer unendlichen Reihe zu entwickeln, der eine der Grundlagen der folgenden Ausführungen bildet.

Satz 1: *Es sei k ein algebraischer Zahlkörper mit der Klassenzahl $q \cdot l^h$, wo l eine beliebige Primzahl bedeutet und $q \not\equiv 0(l)$ ist. Es bezeichne ferner G_{l^h} die Gruppe, welche die q^{ten} Potenzen der Idealklassen aus k enthält, und $G_{l^{h-1}}$ eine Untergruppe von G_{l^h} vom Grade l^{h-1}. Läßt man dann $\mathfrak{w}^{(+)}$ alle Primideale durchlaufen, deren q^{te} Potenzen einer Klasse aus $G_{l^{h-1}}$ angehören, so gilt:*

$$(1) \qquad \sum_{(\mathfrak{w}^{(+)})} \frac{1}{n(\mathfrak{w}^{(+)})^s} \leqq \frac{1}{l} \log \frac{1}{s-1} + f(s), \qquad (s > 1),$$

*) Math. Ann. 49 (1897), p. 83.

wo $f(s)$ eine Funktion der reellen Veränderlichen s bedeutet, die endlich bleibt, wenn sich s der Grenze 1 nähert.

Beweis: Bedeutet C das System aller Klassen aus k, deren q^{te} Potenz in G_{lh-1} liegt, so läßt sich das System sämtlicher Klassen von k in der Gestalt:

$$(2)\qquad Cc^x, \quad (x = 0, 1, \cdots, l-1)$$

darstellen, wo c eine Klasse bedeutet, deren q^{te} Potenz nicht in G_{lh-1} liegt.

Bezeichnet man nun mit T die Anzahl aller Ideale einer bestimmten Klasse aus k, deren Normen $\leqq t$ sind, unter t eine reelle positive Größe verstanden, so gilt*):

$$(3)\qquad T = t\varkappa + Rt^{1-\frac{1}{m}},$$

wo $\varkappa$ eine nur vom Körper k und nicht von t abhängende Konstante und R eine derart von t abhängige Größe bedeutet, die für unendlich wachsendes t zwischen endlichen Grenzen bleibt. Aus (3) folgt:

$$(4)\qquad \sum_{(\mathfrak{j})} \frac{1}{n(\mathfrak{j})^s} = \sum_{(t)} \frac{\varkappa}{t^s} + f(s), \qquad (s > 1),$$

wo die Summe links über alle Ideale einer bestimmten Klasse aus k und die Summe rechts über alle Zahlen $t = 1, 2, \cdots, \infty$ zu erstrecken ist; $f(s)$ bedeutet eine Funktion der reellen Veränderlichen s, die endlich bleibt, wenn s gegen 1 konvergiert.

Ich ordne jetzt allen Klassen aus k l^{te} Einheitswurzeln zu, indem ich der Klasse $C_i c^{x_i}$ die Einheitswurzel ζ^{x_i} zuweise, wo C_i eine beliebige Klasse aus C bedeutet und ζ eine von 1 verschiedene l^{te} Einheitswurzel. Bei dieser Zuordnung entspricht dem Produkt zweier Klassen auch das Produkt der zugeordneten Einheitswurzeln. Bezeichne ich nun mit $\zeta_{\mathfrak{j}}$ diejenige Einheitswurzel, die der durch $\mathfrak{j}$ repräsentierten Idealklasse zugeordnet ist, so bleibt die Summe

$$(5)\qquad \sum_{(\mathfrak{j})} \sum_{(e)} \zeta_{\mathfrak{j}}^e \frac{1}{n(\mathfrak{j})^s} \; (e = 1, 2, \cdots, l-1), \qquad (s > 1),$$

in der $\mathfrak{j}$ alle Ideale der l Klassen $c_i = C_i c^{x_i}$, $c_i^2, \cdots, c_i^l$ $(x_i \not\equiv 0(l))$ durchläuft, stets endlich, wenn sich s der Grenze 1 nähert; dies folgt aus (4). Das gleiche gilt dann offenbar, wenn ich in (5) $\mathfrak{j}$ alle Ideale aus k durchlaufen lasse.

Andererseits ist, wenn $\mathfrak{w}$ alle Primideale aus k durchläuft:

$$(6)\qquad \log \sum_{(\mathfrak{j})} \sum_{(e)} \zeta_{\mathfrak{j}}^e \frac{1}{n(\mathfrak{j})^s} = \sum_{(\mathfrak{w})} \sum_{(e)} \zeta_{\mathfrak{w}}^e \frac{1}{n(\mathfrak{w})^s} + f_1(s), \; (e = 1, 2, \cdots, l-1), \; (s > 1).$$

*) Hilbert, Rel. quadr. Zahlk., § 22, p. 53.

Versteht man daher unter $\mathfrak{w}^{(+)}$ alle Primideale aus k, deren q^{te} Potenz in einer Klasse aus $G_{l^{h-1}}$ liegt, unter $\mathfrak{w}^{(-)}$ alle übrigen Primideale aus k, so folgt aus (5) und (6):

$$(7) \qquad (l-1)\sum_{(\mathfrak{w}^{(+)})} \frac{1}{n(\mathfrak{w}^{(+)})^s} - \sum_{(\mathfrak{w}^{(-)})} \frac{1}{n(\mathfrak{w}^{(-)})^s} \leqq f_2(s), \qquad (s > 1).$$

Ferner ist:

$$(8) \qquad \sum_{(\mathfrak{w}^{(+)})} \frac{1}{n(\mathfrak{w}^{(+)})^s} + \sum_{(\mathfrak{w}^{(-)})} \frac{1}{n(\mathfrak{w}^{(-)})^s} = \log\frac{1}{s-1} + f_3(s), \qquad (s > 1).$$

Durch Addition von (7) und (8) folgt die zu beweisende Ungleichung:

$$\sum_{(\mathfrak{w}^{(+)})} \frac{1}{n(\mathfrak{w}^{(+)})^s} \leqq \frac{1}{l}\log\frac{1}{s-1} + f(s), \qquad (s > 1).$$

Im vorstehenden bedeuten $f_i(s)$ Funktionen der reellen Veränderlichen s, die endlich bleiben, wenn s gegen 1 konvergiert.

§ 3.

Die singulären Primärzahlen.

Wir setzen in diesem und den folgenden Paragraphen von dem Grundkörper k voraus, daß er eine primitive l^{te} Einheitswurzel ζ enthalte, daß er also ein Oberkörper des Kreiskörpers der l^{ten} Einheitswurzeln und zwar vom Relativgrad m sei. Unter l verstehen wir eine ungerade Primzahl; es sei indessen gleich bemerkt, daß die folgenden Entwicklungen auch für den Fall $l = 2$ gelten, vorausgesetzt, daß der Körper k samt seinen sämtlichen konjugierten imaginär ist. Die Klassenzahl des Körpers k sei gleich $ql^{h'}$, wo $q \not\equiv 0(l)$ ist. Da uns im folgenden zunächst nur die Untergruppe der Klassengruppe vom Grade $l^{h'}$ interessiert, so wollen wir das System aller Klassen, deren q^{te} Potenz in die Hauptklasse fällt, mit 1 bezeichnen; wir drücken uns also so aus, als ob die Klassenzahl des Körpers k genau gleich $l^{h'}$ wäre. Eine Beschränkung liegt darin nicht. Die Klassengruppe von k möge e Basisklassen enthalten und dementsprechend das Klassensystem von k durch folgendes Schema dargestellt werden:

$$(1) \qquad c_1^{x_1} c_2^{x_2} \cdots c_e^{x_e} \quad (x_i = 0, 1, \cdots, l^{h_i} - 1), \quad h_1 + h_2 + \cdots + h_e = h'.$$

Ich bezeichne nun mit $\mathfrak{r}_1, \cdots, \mathfrak{r}_e$ Ideale aus den Klassen $c_1, \cdots, c_e$ und setze:

$$(2) \qquad \mathfrak{r}_1^{l^{h_1}} = (\varrho_1), \cdots, \mathfrak{r}_e^{l^{h_e}} = (\varrho_e),$$

wo $\varrho_1, \cdots, \varrho_e$ ganze Zahlen aus k bedeuten. Es sei ferner $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{m'-1}$ ein volles System von Grundeinheiten für k $\left(\text{also } m' = \frac{m(l-1)}{2}\right)$ und ε_m

eine in k liegende Einheitswurzel, deren l^{te} Wurzel nicht in k liegt. Wir setzen dann:

$$\varepsilon_{m'+1} = \varrho_1, \cdots, \varepsilon_{m'+e} = \varrho_e \tag{3}$$

und bestimmen ein System von $m' + e$ Primidealen $\mathfrak{q}$, das die Bedingungen:

$$\left(\frac{\varepsilon_i}{\mathfrak{q}_i}\right)_l \neq 1, \quad \left(\frac{\varepsilon_j}{\mathfrak{q}_i}\right)_l = 1, \quad (i \neq j), \quad (i, j = 1, 2, \cdots, m' + e) \tag{4}$$

befriedigt, was stets möglich ist.*)

Weiter wählen wir die Exponenten w so, daß

$$\begin{aligned} \mathfrak{q}_1 \mathfrak{r}_1^{w_1^{(1)}} \cdots \mathfrak{r}_e^{w_e^{(1)}} &= (\varkappa_1), \\ \cdots\cdots & \cdots\cdots \\ \mathfrak{q}_{m'+e} \mathfrak{r}_1^{w_1^{(m'+e)}} \cdots \mathfrak{r}_e^{w_e^{(m'+e)}} &= (\varkappa_{m'+e}) \end{aligned} \tag{5}$$

wird, wo $\varkappa_1, \cdots, \varkappa_{m'+e}$ ganze Zahlen aus k bedeuten. Bildet man dann das System der Zahlen:

$$\varepsilon_1^{u_1} \cdots \varepsilon_{m'+e}^{u_{m'+e}} \varkappa_1^{v_1} \cdots \varkappa_{m'+e}^{v_{m'+e}}, \quad (u, v = 0, 1, \cdots, l-1), \tag{6}$$

indem man die Exponenten v den Bedingungen:

$$\begin{aligned} v_1 w_1^{(1)} + \cdots + v_{m'+e} w_1^{(m'+e)} &\equiv 0(l), \\ \cdots\cdots & \cdots\cdots \\ v_1 w_e^{(1)} + \cdots + v_{m'+e} w_e^{(m'+e)} &\equiv 0(l), \end{aligned} \tag{7}$$

unterwirft, so erhält man dadurch sicher $l^{2m'+e}$ verschiedene Zahlen, die die Eigenschaft haben, daß sie die Ideale $\mathfrak{r}_1, \cdots, \mathfrak{r}_e$ nur in l^{ten} Potenzen als Faktoren enthalten.

Wir nennen jetzt nach D. Hilbert**) zwei Zahlen α, β aus k von *gleicher Art*, wenn sie eine Kongruenz:

$$\alpha \equiv \beta \gamma^l (\mathfrak{l}^l) \tag{8}$$

befriedigen, wo γ eine Zahl aus k bedeutet und $\mathfrak{l} = (1 - \zeta)$ ist. Die Primärzahlen in k, die zu $\mathfrak{l}$ prim und der l^{ten} Potenz einer Zahl aus k nach $\mathfrak{l}^l$ kongruent sind, bilden für sich eine Art. Die Gesamtheit der zu $\mathfrak{l}$ primen ganzen Zahlen in k liefert genau $l^{2m'}$ verschiedene Arten, wie leicht nachzuweisen ist.

Bedeutet nämlich α_i ein System von Zahlen, das die sämtlichen Arten der zu $\mathfrak{l}$ primen Zahlen repräsentiert, und β_k ein volles Restsystem von ganzen zu $\mathfrak{l}$ primen nach $\mathfrak{l}$ inkongruenten Zahlen, so bildet $\alpha_i \beta_k^l$ ein

---

*) Hilbert, Algebr. Zahlk., Satz 152, p. 426. $(-)_l$ bedeutet das l^{te} Potenzrestsymbol.

**) Rel. Abelsche Zahlk., p. 382.

volles Restsystem der zu $\mathfrak{l}$ primen nach $\mathfrak{l}^l$ inkongruenten Zahlen. Denn ist α eine beliebige ganze Zahl aus k, so gilt zunächst eine Kongruenz

$$\alpha \equiv \alpha_i \beta^l (\mathfrak{l}^l),$$

wo β eine ganze Zahl aus k bedeutet. Genügt diese der Kongruenz

$$\beta \equiv \beta_k (\mathfrak{l}),$$

so ist auch

$$\beta^l \equiv \beta_k^l (\mathfrak{l}^l),$$

folglich

$$\alpha \equiv \alpha_i \beta_k^l (\mathfrak{l}^l).$$

Wäre andererseits:

$$\alpha_i \beta_k^l \equiv \alpha_{i'} \beta_{k'}^l (\mathfrak{l}^l),$$

so müßte zunächst $i = i'$ sein, also auch

$$\beta_k^l \equiv \beta_{k'}^l (\mathfrak{l}^l)$$

und daher

$$\beta_k \equiv \beta_{k'} (\mathfrak{l}), \quad \text{also} \quad k = k'.$$

Da nun das System $\alpha_i \beta_k^l$ im ganzen $\varphi(\mathfrak{l}^l)$ Zahlen enthält und das System β_k $\varphi(\mathfrak{l})$ Zahlen, so bleiben für das System α_i $n(\mathfrak{l}^{l-1}) = l^{2m'}$ Zahlen, was nachzuweisen war.

Wie wir oben gesehen haben, enthält das System (6) sicher $l^{2m'+e}$ verschiedene Zahlen; es müssen daher notwendig unter diesen zwei Zahlen derselben Art ω_1 und ω_2 enthalten sein. Die Zahl $\omega = \omega_1 \omega_2^{l-1}$ ist dann eine Primärzahl von der Gestalt:

$$\omega = \varepsilon_1^{u_1} \cdot \cdot \cdot \varepsilon_{m'+1}^{u_{m'+1}} \varkappa_1^{v_1} \cdot \cdot \cdot \varkappa_{m'+1}^{v_{m'+1}} \alpha^l, \tag{9}$$

bei der nicht sämtliche Exponenten u und v durch l teilbar sind; α bedeutet eine Zahl aus k. Wir nennen ω kurz eine *singuläre Primärzahl*.

Es ist leicht einzusehen, daß man mit Hilfe des Systems (6) sogar e voneinander unabhängige singuläre Primärzahlen erhalten kann, was wir später (§ 7) benutzen werden. Vorläufig genügt uns aber die Existenz einer einzigen solchen Zahl ω, die einen relativzyklischen Körper $K(\sqrt[l]{\omega}, k)$ vom Relativgrad l in bezug auf k definiert. Die Untersuchung dieses Körpers K bildet den Inhalt der nächsten Paragraphen, und speziell der Nachweis, daß er unverzweigt in bezug auf k ist. Dies wird dann und nur dann der Fall sein, wenn die Exponenten v in (9) sämtlich Null sind.*) Um das zu beweisen, müssen wir in den nächsten Paragraphen zunächst die ambigen Komplexe in K betrachten und eine obere Grenze für ihre Anzahl ableiten.

---

*) Furtwängler, Reziprozitätsgesetz, p. 7, Satz 6.

§ 4.

Obere Grenze für die Anzahl der aus ambigen Idealen entspringenden ambigen Komplexe des Körpers $K(\sqrt[l]{\omega}, k)$, wo ω eine singuläre Primärzahl bedeutet.

Es sei ω eine singuläre Primärzahl, wie wir sie im vorigen Paragraphen ermittelt haben, von der Gestalt:

$$\omega = \varepsilon_1^{u_1} \cdots \varepsilon_{m'+e}^{u_{m'+e}} \varkappa_1^{v_1} \cdots \varkappa_{m'+e}^{v_{m'+e}} \tag{1}$$

und es mögen die Exponenten $v_{i_1}, v_{i_2}, \cdots, v_{i_t}$ die einzigen der Exponenten v sein, die nicht durch l teilbar sind. Es gilt dann, wie wir nachweisen wollen, folgender Satz:

Satz 2: *Ist die Anzahl aller ambigen Ideale des Körpers $K(\sqrt[l]{\omega}, k)$ gleich l^t, und machen die sämtlichen Einheiten in k, die Relativnormen von Einheiten in K sind, l^{v^*} Einheitenverbände aus, so gilt, wenn wir die Anzahl aller ambigen Komplexe, die aus ambigen Idealen entspringen, mit l^{a^*} bezeichnen, die Ungleichung:*

$$a^* \leqq t + v^* - m' - 1 + e_1. \tag{2}$$

*Die Zahl e_1 ist dadurch bestimmt, daß l^{e_1} Idealklassen aus k in K in die Hauptklasse übergehen.**)

Beweis: Bezeichnet man mit $\mathsf{H}_1, \cdots, \mathsf{H}_{m'}$ ein System relativer Grundeinheiten von K in bezug auf k**) und mit $\eta_1, \cdots, \eta_{m'}$ ihre Relativnormen in k, so ist jede Einheit ε in k, die Relativnorm einer Einheit in K ist, in der Form darstellbar***):

$$\varepsilon = \eta_1^{r_1} \cdots \eta_{m'}^{r_{m'}} \xi^l, \tag{3}$$

wo ξ eine Einheit aus k und $r_1, \cdots, r_{m'}$ irgend welche Zahlen $0, 1, \cdots, l-1$ bedeuten. Vorausgesetzt ist dabei, daß ω nicht das Produkt einer Einheit mit der l^{ten} Potenz einer Zahl aus k ist, was nach unserer Annahme über die Exponenten v zutrifft.

Da nun zusammen l^{v^*} Einheitenverbände, die Relativnormen von Einheiten aus K enthalten, existieren, so muß man unter den Einheiten $\eta_1, \cdots, \eta_{m'}$ v^* auswählen können, etwa $\eta_1, \eta_2, \cdots, \eta_{v^*}$, so daß jede Einheit ε in k, die Relativnorm einer Einheit in K ist, sich eindeutig in die Gestalt bringen läßt:

$$\varepsilon = \eta_1^{r_1} \cdots \eta_{v^*}^{r_{v^*}} \xi^l, \quad (r_1, \cdots, r_{v^*} = 0, 1, \cdots, l-1). \tag{4}$$

---

*) Über die Definition der Komplexe und speziell der ambigen Komplexe vgl. Hilbert, Rel. quadr. Zahlk., § 12, p. 22.

**) Hilbert, Algebr. Zahlk., § 55, p. 272.

***) Hilbert, Algebr. Zahlk., § 146, p. 448, Hilfssatz 32.

Wendet man dies auf die Einheiten $\eta_i (i = v^* + 1, \cdots, m')$ an, so ergibt sich:

$$\eta_i = \eta_1^{r_1^{(i)}} \cdots \eta_{v^*}^{r_{v^*}^{(i)}} (\xi^{(i)})^l, \quad (i = v^* + 1, \cdots, m'), \tag{5}$$

wo $\xi^{(i)}$ eine Einheit aus k ist und die Exponenten r bestimmte Werte $0, 1, \cdots, l-1$ haben. Daraus folgt, daß die $m' - v^*$ Ausdrücke:

$$\mathsf{H}_i' = \mathsf{H}_i \mathsf{H}_1^{-r_1^{(i)}} \cdots \mathsf{H}_{v^*}^{-r_{v^*}^{(i)}} (\xi^{(i)})^{-1}, \quad (i = v^* + 1, \cdots, m') \tag{6}$$

Einheiten in K mit der Relativnorm 1 sind und daß man deshalb:

$$\mathsf{H}_i' = \mathsf{M}_i^{(1-S)} \tag{7}$$

setzen kann, wo M_i eine ganze Zahl aus k und S die Substitution $\sqrt[l]{\omega} \mid \zeta \sqrt[l]{\omega}$ bedeutet. Die Ideale (M_i) und $(\mathsf{M}) = (\sqrt[l]{\omega})$ sind dann mit ihren relativ konjugierten Idealen identisch und darum Produkte aus den ambigen Primidealen in K, die wir mit $\mathfrak{D}_1, \cdots, \mathfrak{D}_t$ bezeichnen, und Idealen aus k:

$$\begin{aligned} \mathsf{M} &= \mathfrak{D}_1^{a_1} \cdots \mathfrak{D}_t^{a_t} \mathfrak{j}, \\ (\mathsf{M}_i) &= \mathfrak{D}_1^{a_1^{(i)}} \cdots \mathfrak{D}_t^{a_t^{(i)}} \mathfrak{j}^{(i)}, \quad (i = v^* + 1, \cdots, m'). \end{aligned} \tag{8}$$

Es ist nun zu untersuchen, wieviel voneinander unabhängige Beziehungen

$$(\mathsf{M})^b \cdot (\mathsf{M}_{v^*+1})^{b_{v^*+1}} \cdots (\mathsf{M}_{m'})^{b_{m'}} = \mathfrak{j}^* \tag{9}$$

bestehen können, wo die Exponenten b irgend welche Werte $0, 1, \cdots, l-1$ haben, die nicht sämtlich Null sind, und $\mathfrak{j}^*$ ein Ideal aus k ist. Es ist zunächst leicht zu erkennen, daß $\mathfrak{j}^*$ nicht Hauptideal in k sein kann, daß also keine Relation:

$$(\mathsf{M})^b (\mathsf{M}_{v^*+1})^{b_{v^*+1}} \cdots (\mathsf{M}_{m'})^{b_{m'}} = iE \tag{10}$$

gelten kann, wo i eine Zahl aus k und E eine Einheit aus K ist. Denn potenziert man (10) symbolisch mit $(1 - S)$, so ergibt sich:

$$\zeta^{-b} (\mathsf{H}_{v^*+1}')^{b_{v^*+1}} \cdots (\mathsf{H}_{m'}')^{b_{m'}} = E^{(1-S)} \tag{11}$$

und hieraus schließt man mit Hilfe der fundamentalen Eigenschaft des Systems relativer Grundeinheiten, daß $b = b_{v^*+1} = \cdots = b_{m'} = 0$ sein muß, wenn man noch beachtet, daß ω nicht das Produkt aus einer Einheit mit der l^{ten} Potenz einer Zahl aus k ist.

Da keine Relation (10) bestehen kann und andererseits das Ideal $\mathfrak{j}^*$ aus (9) in K Hauptideal ist, so können höchstens e_1 voneinander unabhängige Relationen (9) gelten, wenn l^{e_1} Idealklassen aus k in K in die Hauptklasse übergehen. Daraus ergibt sich die Richtigkeit der Ungleichung (2).

Die Ungleichung (2) gilt auch in dem Falle, daß ω eine Einheit aus k ist. Denn in diesem Falle sind die Einheiten $\omega, \eta_1, \cdots, \eta_{m'}$ Relativnormen von Einheiten aus K, und wir können als Repräsentanten der v^* unabhängigen Einheitenverbände, die Relativnormen von Einheiten aus K enthalten, etwa die Einheiten $\omega, \eta_1, \cdots, \eta_{v^*-1}$ wählen. Dadurch, daß man die übrigen $m' - v^* + 1$ Einheiten $\eta_{v^*}, \cdots, \eta_{m'}$ durch diese ausdrückt, gelangt man zu $m' - v^* + 1$ Relationen von der Art (8). Da jetzt wieder zwischen $\mathsf{M}_{v^*}, \mathsf{M}_{v^*+1}, \cdots, \mathsf{M}_{m'}$ höchstens e_1 Relationen von der Art (9) bestehen können, gilt auch jetzt die Ungleichung (2).

§ 5.

Obere Grenze für die Anzahl aller ambigen Komplexe in K.

Satz 3: *Ist a die Anzahl der unabhängigen ambigen Komplexe in K und e die Anzahl der Basisklassen der Klassengruppe von k, so gilt:*

(1) $$a \leqq e - 1.$$

Beweis: Ist l^v die Anzahl aller Einheiten, die Relativnormen von ganzen oder gebrochenen Zahlen aus K sind, so gibt es $v - v^*$ unabhängige Einheiten in k, die Relativnormen von gebrochenen Zahlen sind. Diese definieren $v - v^*$ ambige Idealklassen in K, die wir mit $A_1, \cdots, A_{v-v^*}$ bezeichnen. Der Weg, auf dem man dieselben erhält, ist genau derselbe wie in dem Beweise zu Satz 20 meiner Abhandlung über die Reziprozitätsgesetze.*) Bedeuten $\mathfrak{A}_1, \cdots, \mathfrak{A}_{v-v^*}$ diejenigen Ideale, welche die ambigen Klassen $A_1, \cdots, A_{v-v^*}$ definieren, und ist $\mathfrak{A}$ ein beliebiges Ideal eines ambigen Komplexes A aus K, so ist zu untersuchen, ob $\mathfrak{A}$ einem Produkt aus Potenzen von $\mathfrak{A}_1, \cdots, \mathfrak{A}_{v-v^*}$ mit Potenzen der a^* unabhängigen ambigen Ideale aus K und einem Ideal aus k äquivalent ist.

Es gilt:

(2) $$\mathfrak{A}^{(1-S)} = \Theta \mathfrak{j},$$

wo Θ eine Zahl aus k und $\mathfrak{j}$ ein Ideal aus k bedeutet. S bezeichnet eine erzeugende Substitution der Relativgruppe von K in bezug auf k.

Wir wollen nun zunächst sehen, welchen Bedingungen die Ideale $\mathfrak{j}$, die eine Beziehung (2) erfüllen, unterworfen sind. Wir stellen zu diesem Zweck die Klassen in k, deren l^{te} Potenz in k die Hauptklasse ergibt, in der Gestalt dar:

(3) $$(c_1^*)^{x_1} \cdots (c_e^*)^{x_e} \begin{pmatrix} x_1 = 0, 1, \cdots l-1 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x_e = 0, 1, \cdots l-1 \end{pmatrix},$$

indem wir:

(4) $$c_1^* = c_1^{l^{h_1}-1}, \cdots c_e^* = c_e^{l^{h_e}-1}$$

setzen. Gehört nun $\mathfrak{j}$ der Klasse c' an und ist:

---

*) Furtwängler, Reziprozitätsgesetz, p. 23.

$$c' = (c_1^*)^{x_1'} \cdots (c_e^*)^{x_e'}, \tag{5}$$

so kann man setzen:

$$\mathfrak{j} = \alpha\, \mathfrak{r}_1^{x_1' l^{h_1 - 1}} \cdots \mathfrak{r}_e^{x_e' l^{h_e - 1}}, \tag{6}$$

wo α eine Zahl aus k bedeutet. Andererseits ist nach (2)

$$\mathfrak{j}^l = N_k(\Theta^{-1}),$$

wenn N_k die Relativnorm in bezug auf k bedeutet; folglich

$$N_k(\Theta\alpha)^{-1} = \varepsilon' \varrho_1^{x_1'} \cdots \varrho_e^{x_e'}, \tag{7}$$

wenn ε' eine geeignete Einheit aus k bezeichnet.

Aus (7) folgt*):

$$\left(\frac{\varepsilon' \varrho_1^{x_1'} \cdots \varrho_e^{x_e'}}{\mathfrak{q}_{i_1}}\right) = 1, \cdots \left(\frac{\varepsilon' \varrho_1^{x_1'} \cdots \varrho_e^{x_e'}}{\mathfrak{q}_{i_t}}\right) = 1. \tag{8}$$

Unter den Indizes $i_1, \cdots i_t$ mögen nun aus der Reihe der Indizes $m' + 1, \cdots m' + e$ genau f vorkommen und zwar mögen dies die Indizes

$$m' + e^{(1)}, \cdots m' + e^{(f)} \tag{9}$$

sein. Es folgt dann, wenn man die Bedingungen (4) in § 3 beachtet, denen die $\mathfrak{q}$ genügen müssen, daß:

$$x'_{e^{(1)}} \equiv 0(l), \cdots x'_{e^{(f)}} \equiv 0(l) \tag{10}$$

sein muß; d. h. es gibt höchstens $e - f$ unabhängige Klassen in k, die in K der $(1-S)^{\text{ten}}$ Potenz einer Klasse gleich werden. Unter diesen sind e_1 Klassen, die in K in die Hauptklasse übergehen; geht aber $\mathfrak{j}$ in K in ein Hauptideal über, so folgt genau wie an der zitierten Stelle**), daß sich $\mathfrak{A}$ in der oben angegebenen Weise ausdrücken läßt. Es kann demnach in K höchstens $e - f - e_1$ unabhängige Klassen aus ambigen Komplexen geben, die sich nicht aus den Klassen $A_1, \cdots A_{v-v^*}$ und den aus den ambigen Idealen in K entspringenden Klassen zusammensetzen lassen. Es ist also

$$a \leqq a^* + v - v^* + e - f - e_1. \tag{11}$$

Alle Einheiten ε in k nun, die Relativnormen von Zahlen aus K sind, müssen die Bedingungen:

$$\left(\frac{\varepsilon}{\mathfrak{q}_{i_1}}\right) = 1, \cdots \left(\frac{\varepsilon}{\mathfrak{q}_{i_t}}\right) = 1 \tag{12}$$

befriedigen. Da unter den Indizes $i_1, \cdots i_t$ f Indizes aus der Reihe $m' + 1, \cdots, m' + e$ vorkommen, folgt aus (12)

$$v \leqq m' - t + f. \tag{13}$$

Addiert man jetzt endlich (2) des vorigen Paragraphen und (11) und (13) aus diesem Paragraphen, so ergibt sich $a \leqq e - 1$.

---

*) Furtwängler, Reziprozitätsgesetz, Satz 15, p. 16.

**) Furtwängler, Reziprozitätsgesetz, p. 24.

§ 6.

Für welche Primideale in k hat eine singuläre Primärzahl den Restcharakter 1?

Von ausschlaggebender Bedeutung für die folgenden Entwicklungen ist die Beziehung, welche die singulären Primärzahlen in K zur Einteilung der Ideale in Klassen besitzen. Es zeigt sich nämlich, daß eine bestimmte singuläre Primärzahl ω nur von solchen Primidealen l^{ter} Potenzrest sein kann, die einer bestimmten Untergruppe der Klassengruppe von K angehören. Die Entscheidung über die Frage, ob ω Rest oder Nichtrest eines gegebenen Primideals $\mathfrak{p}$ ist, hängt also davon ab, welcher Idealklasse $\mathfrak{p}$ angehört.

Um den angedeuteten Zusammenhang aufdecken zu können, müssen wir zunächst noch einige Festsetzungen treffen. Es sei P ein beliebiger ambiger Komplex in K, der nicht der Hauptkomplex ist, und es möge in K die Äquivalenz gelten:

$$P \sim Q^{(1-S)^p},$$

wo Q einen Komplex aus K bedeutet. Dagegen möge es keinen Komplex R in K geben, der die Äquivalenz:

$$P \sim R^{(1-S)^{p+1}}$$

befriedigt. Ich nenne dann kurz p den Exponenten des ambigen Komplexes P. Die Möglichkeit einer solchen Definition ist ersichtlich, wenn man bedenkt, daß nicht für beliebig hohe Werte von p eine Äquivalenz der angegebenen Art erfüllt sein kann, weil die $(1-S)^{\text{te}}$ symbolische Potenz eines Komplexes immer auch die l^{te} wirkliche Potenz eines Komplexes ist. Ich bestimme in K jetzt a unabhängige Komplexe in folgender Weise:

Ich wähle zunächst einen ambigen Komplex P_1 in K, dessen Exponent p_1 von keinem Exponenten eines anderen ambigen Komplexes übertroffen wird, darauf einen von P_1 unabhängigen ambigen Komplex P_2, dessen Exponent von keinem Exponenten eines von P_1 unabhängigen Komplexes übertroffen wird usf. Der letzte so auszuwählende Komplex ist mit P_a zu bezeichnen; er hat einen Exponenten p_a, der von keinem Exponenten eines ambigen Komplexes unterschritten wird.

Es gelten dann in K Äquivalenzen folgender Art:

$$P_i \sim Q_i^{(1-S)^{p_i}}, \ (i = 1, 2, \cdots a) \tag{1}$$

wo Q_i gewisse Komplexe aus K bedeuten, und die Exponenten p_i erfüllen die Bedingungen:

$$p_1 \geqq p_2 \cdots \geqq p_a.$$

Mit Hilfe der vorstehenden Festsetzungen können wir folgenden Satz aussprechen:

Satz 4: *Ist $\mathfrak{J}$ ein Ideal aus K und $\mathfrak{J}^{(1-S)}$ einem Idealquotienten von der Gestalt:*

(2) $$\mathfrak{j}\,\mathfrak{Q}_1^{F_1(S)} \cdots \mathfrak{Q}_a^{F_a(S)}$$

äquivalent, wo $F_1(S), \cdots F_a(S)$ ganze ganzzahlige Funktionen von S sind, so ist auch $\mathfrak{J}$ einem Idealquotienten dieser Gestalt äquivalent. Dabei bedeutet $\mathfrak{j}$ ein Ideal aus k, $\mathfrak{Q}_1, \cdots, \mathfrak{Q}_a$ Ideale aus Klassen in K, die resp. den Komplexen $Q_1, \cdots, Q_a$ angehören; diese sind, wie im vorstehenden erläutert ist, durch (1) *bestimmt.*

Beweis: Wir betrachten zunächst den Fall, daß für sämtliche Funktionen F gilt:

$$F_i(1) \equiv 0(l) \quad (i = 1, \cdots a).$$

Wir können dann auch annehmen, daß die sämtlichen Funktionen $F(S)$ durch $(1-S)$ teilbar seien; denn es gilt

(3) $$\mathfrak{Q}_i^l \sim \mathfrak{q}_i \mathfrak{Q}_i^{(1-S)\,G_i(S)},$$

wo $\mathfrak{q}_i$ die Relativnorm von $\mathfrak{Q}_i$ und $G_i(S)$ eine ganze, ganzzahlige Funktion von S bedeutet. Die Richtigkeit von (3) erkennt man leicht, wenn man die Funktion

$$l - (1 + S + \cdots S^{l-1})$$

nach Potenzen von $(1-S)$ entwickelt. Wir setzen daher jetzt:

$$F_i(S) = -(1-S)F'_i(S),$$

wo die Funktionen $F'_i(S)$ wieder ganze, ganzzahlige Funktionen von S sind.

Bezeichnet man dann den Ausdruck:

$$\mathfrak{Q}_1^{F'_1(S)} \cdots \mathfrak{Q}_a^{F'_a(S)}$$

mit $\mathfrak{J}'$, so gilt offenbar:

$$(\mathfrak{J}\mathfrak{J}')^{(1-S)} \sim \mathfrak{j}$$

d. h. $\mathfrak{J}\mathfrak{J}'$ gehört einem ambigen Komplex an, woraus sich ohne weiteres die Richtigkeit unserer Behauptung in dem betrachteten Falle ergibt.

Wir nehmen zweitens an, daß nicht sämtliche Funktionen $F_i(1)$ durch l teilbar sind und zwar sei F_b die erste unter den nicht teilbaren; ich setze dann wieder voraus, daß sämtliche Funktionen $F_1(S), \cdots F_{b-1}(S)$ durch $(1-S)$ teilbar sind, was nach (3) gestattet ist. Ich potenziere jetzt die vorausgesetzte Äquivalenz:

$$\mathfrak{J}^{(1-S)} \sim \mathfrak{j}\,\mathfrak{Q}_1^{F_1(S)} \cdots \mathfrak{Q}_{b-1}^{F_{b-1}(S)} \mathfrak{Q}_b^{F_b(S)} \cdots \mathfrak{Q}_a^{F_a(S)}$$

symbolisch mit $(1-S)^{p_b}$. Ich erhalte dadurch eine Äquivalenz von folgender Gestalt:

(4) $$(\mathfrak{J}\mathfrak{J}')^{(1-S)^{p_b+1}} \sim \mathfrak{j}_1 \mathfrak{A}_b^{c_b} \mathfrak{A}_{b+1}^{c_{b+1}} \cdots \mathfrak{A}_a^{c_a},$$

wo $\mathfrak{j}_1$ ein Ideal aus k, $\mathfrak{J}'$ einen leicht angebbaren Idealquotienten aus K und $\mathfrak{A}_b, \mathfrak{A}_{b+1}, \cdots, \mathfrak{A}_a$ Ideale aus Klassen der ambigen Komplexe $P_b, \cdots, P_a$ bedeuten. Da der Exponent c_b wegen $F_b(1) \not\equiv 0\,(l)$ nicht durch l teilbar ist, so steht die Äquivalenz (4) in Widerspruch mit unserer Festsetzung über die Auswahl der Komplexe P_i. Denn sie lehrt, daß es einen von den Komplexen $P_1, \cdots, P_{b-1}$ unabhängigen ambigen Komplex gibt, dessen Exponent größer als p_b ist. Der angenommene zweite Fall ist deshalb unmöglich; hiermit ist unser Satz vollständig bewiesen.

Satz 5: *Ist* $\mathfrak{p}$ *ein Primideal aus* k *mit der Eigenschaft* $\left(\frac{\omega}{\mathfrak{p}}\right)_l = 1$, *so gehört* $\mathfrak{p}$ *einer durch* ω *völlig bestimmten Untergruppe der Klassengruppe von* k *an, deren Grad den Betrag* l^{h-1} *nicht übersteigt.*

Beweis: Ich bezeichne die Klassen in k, in die die Relativnormen von $\mathfrak{Q}_1, \cdots, \mathfrak{Q}_a$ hineinfallen, mit $c_1, \cdots, c_a$. Bezeichne ich dann die kleinste Gruppe, der diese Klassen und außerdem sämtliche l^{ten} Potenzen von Klassen in k angehören, mit G, so hat G höchstens den Grad l^{h-1}. Denn da $a \leqq e-1$ ist, so können höchstens $e-1$ Basisklassen von k durch Produkte aus Potenzen von $c_1, \cdots, c_a$ dargestellt werden; es muß daher sicher eine Basisklasse in G fehlen und der Grad von G ist daher höchstens l^{h-1}. Das Primideal $\mathfrak{p}$ gehört aber, wie leicht einzusehen ist, zu einer Klasse aus G. Denn wegen $\left(\frac{\omega}{\mathfrak{p}}\right)_l = 1$ ist $\mathfrak{p}$ in $K(\sqrt[l]{\omega}, k)$ zerlegbar. Ist $\mathfrak{P}$ ein Primfaktor von $\mathfrak{p}$, so gibt es sicher einen Exponenten b, so daß die Äquivalenz

$$\mathfrak{P}^{q_1(1-S)^b} \sim 1 \tag{5}$$

in K gilt, wo $q_1 \not\equiv 0(l)$ ist. Daraus folgt nach Satz 4, daß $\mathfrak{P}^{q_1}$ einem Ausdruck von der Gestalt (2) äquivalent ist, woraus man sofort erkennt, daß $\mathfrak{p}$ zu einer Klasse der Gruppe G gehört. Von der Gruppe G, die durch ω vollständig bestimmt ist, wollen wir sagen, daß sie zu ω gehört.

Der Grad der Gruppe G ist genau gleich l^{h-1}. Die Richtigkeit dieser Tatsache wird sich aber erst im nächsten Paragraphen ergeben. Ich trage diesem Umstande dadurch Rechnung, daß ich jede Gruppe, die G enthält und deren Grad nicht größer als l^{h-1} ist, als zu ω gehörig bezeichne.

§ 7.

Die Unverzweigtheit der Körper K.

Wir können nunmehr zu dem Nachweis übergehen, daß in bezug auf den gegebenen Grundkörper k genau e voneinander unabhängige *unverzweigte* Körper vom Relativgrade l existieren. Wir beweisen zu diesem Zweck zunächst, daß sicher *ein* solcher Körper existiert.

Ist der in den vorigen Paragraphen betrachtete Körper $K(\sqrt[l]{\omega}, k)$ nicht unverzweigt in bezug auf k, so wähle man ein zweites System von Primidealen $\mathfrak{q}'_1, \cdots, \mathfrak{q}'_{m'+e}$, das ebenfalls die Bedingungen (4) in § 3 befriedigt. Man gelangt dadurch zu einer primären Zahl ω', die von ω verschieden ist. Ist jetzt der Köper $K(\sqrt[l]{\omega'}, k)$ unverzweigt in bezug auf k, so ist unsere Behauptung bewiesen; ist er verzweigt, so schließen wir aus Satz 5, daß zu ω' eine Untergruppe G' gehört, die von G verschieden sein muß. Wäre nämlich $G = G'$, so würde man dadurch zu einem Widerspruche mit Satz 1 kommen. Denn bezeichnet man alle Primideale, für die

$$\left(\frac{\omega}{\mathfrak{p}}\right)_l = 1,$$

mit $\mathfrak{p}$, und diejenigen, für die

$$\left(\frac{\omega}{\mathfrak{p}'}\right)_l \neq 1, \quad \left(\frac{\omega'}{\mathfrak{p}'}\right)_l = 1, \text{ mit } \mathfrak{p}',$$

so gilt bekanntlich:

$$\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} = \frac{l}{l^2} \log \frac{1}{s-1} + f(s) \qquad (s>1)$$

$$\sum_{(\mathfrak{p}')} \frac{1}{n(\mathfrak{p}')^s} = \frac{l-1}{l^2} \log \frac{1}{s-1} + f'(s) \qquad (s>1)$$

$$(1) \qquad \sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} + \sum_{(\mathfrak{p}')} \frac{1}{n(\mathfrak{p}')^s} = \frac{2l-1}{l^2} \log \frac{1}{s-1} + f(s) + f'(s). \qquad (s>1)$$

$f(s)$ und $f'(s)$ haben die bekannte Bedeutung. Da die Primideale $\mathfrak{p}$ sämtlich von den Primidealen $\mathfrak{p}'$ verschieden sind und beide Arten zu Klassen aus der Gruppe $G = G'$ gehören, so involviert Gleichung (1) einen Widerspruch gegen Satz 1, weil

$$(2) \qquad \frac{2l-1}{l^2} > \frac{1}{l}, \text{ wenn } l > 1 \text{ ist.}$$

Wir können nun den begonnenen Prozeß beliebig fortsetzen, indem wir immer neue Systeme von Primidealen $\mathfrak{q}$ mit den Eigenschaften (4) in § 3 wählen. Ich behaupte, daß wir dadurch sicher zu einer primären Zahl ω_1 gelangen müssen, welche einen unverzweigten Körper $K(\sqrt[l]{\omega_1}, k)$ in bezug auf k definiert. Denn wäre dies nicht der Fall, so müßten, da nur eine endliche Anzahl Untergruppen der Gruppe der Klassen von k existieren, sicher in der Reihe der erhaltenen primären Zahlen zwei auftreten, zu denen dieselbe Untergruppe der Klassengruppe von k gehört. Dies ist nach den eben gegebenen Ausführungen unmöglich und daher unsere Behauptung bewiesen.

Wir haben jetzt noch zu zeigen, daß genau e voneinander unabhängige unverzweigte relativzyklische Körper vom Relativgrad l in bezug auf k existieren.

Wir nennen ein System von Körpern unabhängig, wenn keiner in dem aus der Gesamtheit der übrigen Körper zusammengesetzten Körper enthalten ist.

Wir haben im vorhergehenden gesehen, daß es in bezug auf k einen unverzweigten Körper $K_1\left(\sqrt[l]{\omega_1}, k\right)$ gibt. Es sei:

$$\omega_1 = \varepsilon_1^{u_1} \cdots \varepsilon_{m'+e}^{u_{m'+e}},$$

wo $\varepsilon_1, \cdots, \varepsilon_{m'+e}$ die früher angegebene Bedeutung haben und es sei der Exponent u_{i_1} von Null verschieden. Es gibt nun in dem früher betrachteten System von Zahlen (6) in § 3 $l^{2m'+e}$ verschiedene Zahlen und deshalb auch, wenn $e \geqq 2$ ist, sicher zwei Zahlen derselben Art, für die der Exponent von ε_{i_1} denselben Wert hat. Der Quotient dieser beiden Zahlen liefert dann eine primäre Zahl $\omega^{(i_1)}$, für die der Exponent von ε_{i_1} Null ist, und die deshalb sicher einen von K_1 unabhängigen Relativkörper in bezug auf k definiert. Ist dieser unverzweigt, so ist der zweite der gesuchten e Körper gefunden; ist er verzweigt, so wiederholen wir die Betrachtungen der ersten Hälfte dieses Paragraphen, indem wir jetzt aber nur solche primäre Zahlen heranziehen, für die der Exponent von ε_{i_1} Null ist.

Wir kommen dadurch sicher zu einer primären Zahl ω_2, die einen von K_1 unabhängigen unverzweigten Körper $K_2\left(\sqrt[l]{\omega_2}, k\right)$ definiert. Dies Verfahren können wir fortsetzen, wenn $e \geqq 3$ ist.

Ist nämlich in dem Ausdruck für ω_2 der Exponent von ε_{i_2} von Null verschieden, so bestimmen wir in der geschilderten Weise eine primäre Zahl ω_3, die einen unverzweigten Körper $K\left(\sqrt[l]{\omega_3}, k\right)$ in bezug auf k definiert und bei der die Exponenten von ε_{i_1} und ε_{i_2} Null sind; K_3 ist dann von K_2 und K_1 unabhängig. So können wir offenbar fortfahren, bis wir e unabhängige, in bezug auf k unverzweigte Körper vom Relativgrad l erhalten haben, da das Zahlensystem (6) in § 3 $l^{2m'+e}$ verschiedene Zahlen enthält.

Wir haben jetzt noch nachzuweisen, daß es nicht mehr derartige unabhängige Körper gibt. Wir müssen zu diesem Zweck die Untergruppen der Klassengruppe von k vom Grade l^{h-1} und ihre Zusammengehörigkeit mit den im vorigen betrachteten primären Zahlen ω etwas näher untersuchen.

Die Klassengruppe von k war:

$$\text{(3)} \qquad c_1^{x_1} \cdots c_e^{x_e} \; (x_i = 0, 1, \cdots, l^{h_i} - 1), \qquad h_1 + h_2 + \cdots + h_e = h'.$$

Jede Untergruppe von k vom Grade l^{h-1} läßt sich dann durch eine bestimmte Kongruenz

$$(4) \qquad f_1 x_1 + \cdots + f_e x_e \equiv 0\,(l)$$

charakterisieren, wo die $f_1, \cdots, f_e$ feste ganze rationale Zahlen bedeuten, die nicht sämtlich durch l teilbar sind; d. h. man erhält alle Klassen der Untergruppe und jede nur einmal, wenn man die Exponenten $x_1, \cdots, x_e$ in (3) alle Werte durchlaufen läßt, welche der Kongruenz (4) genügen. Man erkennt dies leicht, wenn man bedenkt, daß die Untergruppe als Abelsche Gruppe selbst eine Basis besitzt, und dann die Klassen dieser Basis durch $c_1, \cdots, c_e$ darstellt.

Eine leichte Abzählung vermittelst (4) lehrt dann, daß es $\frac{l^e-1}{l-1}$ verschiedene Untergruppen vom Grade l^{h-1} in der Klassengruppe gibt; andererseits folgt aus der Existenz der Zahlen $\omega_1, \cdots, \omega_e$, daß es mindestens $\frac{l^e-1}{l-1}$ verschiedene unverzweigte Körper vom Relativgrade l in bezug auf k gibt. Da nun aber zu zwei verschiedenen Körpern nicht zwei gleiche Untergruppen gehören können, weil man sonst in der zu Anfang dieses Paragraphen ausgeführten Weise zu einem Widerspruch mit Satz 1 kommen würde, so lassen sich die verschiedenen unverzweigten Körper und die Untergruppen eindeutig zuordnen. Daraus folgt zugleich, daß weiter keine unverzweigten relativzyklischen Körper vom Relativgrad l in bezug auf k existieren können und daß zu jedem solchen Körper eine Untergruppe der Klassengruppe von k gehört, die genau den Grad l^{h-1} hat.

§ 8.

Die genaue Anzahl der ambigen Komplexe und die Einheiten in den Körpern K.

Satz 6: *Die Anzahl der unabhängigen ambigen Komplexe in*

$$K_j(\sqrt[l]{\omega_j}, k) \qquad (j = 1, 2, \cdots, e)$$

ist gleich $e-1$.

Beweis: Wir werden im folgenden den Index j immer fortlassen, da die Ausführungen gleichmäßig für die e Körper $K_1, \cdots, K_e$ gelten, und die in den vorigen Paragraphen gebrauchten Bezeichnungen anwenden. Es mögen $Q_1, \cdots, Q_a$ die durch (1) in § 6 definierten Komplexe aus K sein und $A_1, \cdots, A_a$ mögen Idealklassen aus den Komplexen $Q_1, \cdots, Q_a$ sein. Es sind dann sämtliche Idealklassen aus K in der Gestalt darstellbar:

$$(1) \qquad c A_1^{F_1(S)} \cdots A_a^{F_a(S)},$$

wo c eine Klasse aus k und $F_1(S), \cdots, F_a(S)$ ganze, ganzzahlige Funktionen von S bedeuten. S ist die Substitution, durch die $\sqrt[l]{\omega}$ in $\zeta\sqrt[l]{\omega}$ übergeführt wird. Bezeichnet man nun die Klassen in k, in welche die Relativnormen der Ideale aus $A_1, \cdots, A_a$ hineinfallen, mit $c_1, \cdots, c_a$, so muß die Gruppe der Klassen in k, die $c_1, \cdots, c_a$ und außerdem sämtliche l^{ten} Potenzen von Klassen enthält, vom Grade l^{h-1} sein.

Wäre aber $a < e - 1$, so wäre dies offenbar unmöglich; es ist also notwendig

$$a \geqq e - 1$$

und folglich wegen Satz 3:

$$a = e - 1. \tag{2}$$

Auch die Anzahlen v und v^* lassen sich jetzt leicht bestimmen, wie folgender Satz lehrt:

Satz 7: *Haben v, v^*, e, e_1 und m' dieselbe Bedeutung wie in den Sätzen 2 und 3, so gilt*

$$v^* = m' - e_1 + 1, \tag{3}$$

$$v = m' \tag{4}$$

oder in Worten:

Jede Einheit in k ist Relativnorm einer Zahl aus $K(\sqrt[l]{\omega}, k)$, dagegen sind nur $l^{m'-e_1+1}$ Einheiten Relativnormen von Einheiten aus K.

Beweis: Aus den Ungleichungen (2) in § 4 und (11) in § 5 folgt, wenn man beachtet, daß a^*, t und f den Wert Null haben, und $a = e - 1$ ist:

$$v^* \geqq m' + 1 - e_1, \tag{5}$$

$$v \geqq v^* + e_1 - 1, \tag{6}$$

also auch

$$v \geqq m'.$$

Da v nicht größer als m' sein kann, muß $v = m'$ sein. Aus (6) folgt dann:

$$v^* \leqq m' + 1 - e_1,$$

also wegen (5)

$$v^* = m' - e_1 + 1.$$

Aus der letzten Gleichung schließt man noch, daß e_1 mindestens den Wert 1 haben muß, d. h. *daß es sicher eine Klasse in k geben muß, die in k nicht Hauptklasse ist, aber in K in die Hauptklasse übergeht.*

§ 9.

Konstruktion des unverzweigten Körpers vom Relativgrad l, wenn der Grundkörper keine l^{te} Einheitswurzel enthält.

Wir haben in den vorhergehenden Paragraphen immer vorausgesetzt, daß der Grundkörper k eine l^{te} Einheitswurzel enthalte. Von dieser beschränkenden Voraussetzung haben wir uns jetzt zu befreien, indem wir folgenden Satz beweisen:

Satz 8: *Es sei k ein beliebiger algebraischer Zahlkörper mit der Klassenzahl $ql^{h'}$, wo l eine ungerade Primzahl bedeutet und q zu l prim ist. Ist dann das System der q^{ten} Potenzen der Idealklassen aus k in der Gestalt darstellbar:*

$$(c)_k = c_1^{x_1} \cdots c_e^{x_e} \quad (x_i = 0, 1, \cdots, l^{h_i} - 1), \quad h_1 + \cdots + h_e = h',$$

so existieren in bezug auf k genau e unabhängige unverzweigte relativzyklische Körper vom Relativgrad l. Dasselbe gilt für $l = 2$, wenn der Körper K samt seinen konjugierten imaginär ist.

Beweis: Ich erinnere zunächst daran, daß wir wieder das System aller Klassen, deren q^{te} Potenz in die Hauptklasse fällt, mit 1 bezeichnen und in diesem Sinne die Äquivalenz $\mathfrak{a} \sim 1$ verstehen. Ist dann l^{h_i} der kleinste Exponent, für den die Äquivalenz

$$\mathfrak{b}^{l^{h_i}} \sim 1$$

gilt, so soll l^{h_i} der zum Ideal $\mathfrak{b}$ oder zu der betreffenden Idealklasse gehörige Exponent heißen. Ferner sei noch auf folgende Bezeichnungsweise hingewiesen, die weiterhin benutzt wird. Ist K ein beliebiger Oberkörper von k nnd fallen die Relativnormen der Ideale aus einer Klasse C in K in die Klasse c in k, so werde ich kurz c die Relativnorm von C nennen und schreiben:

$$C = N_k^K(\mathfrak{c}).$$

Wenn die Deutlichkeit nicht darunter leidet, kann bei N der obere oder der untere Index fortbleiben.

Ich adjungiere jetzt zu dem Körper k die l^{te} Einheitswurzel ζ und bezeichne den Körper (k, ζ) mit k', dessen Relativgrad l' in bezug auf k als Faktor von $l - 1$ zu l prim ist. Aus dieser Tatsache folgt leicht, daß jede Idealklasse aus k' in der Form cC darstellbar ist, wo c eine Klasse aus k bedeutet und C eine solche Klasse aus k', die der Bedingung:

$$N_k^{k'}(C) = 1 \tag{2}$$

genügt. Das gesamte Klassensystem von k' ist also in der Gestalt:

$$(c)_k\, C \tag{3}$$

darstellbar, wo C eine beliebige Klasse mit der Eigenschaft (2) bedeutet.

Zwischen den Klassen $c_1, \cdots, c_e$ kann in k' keine Äquivalenz von der Gestalt:

$$c_1^{a_1} \cdots c_e^{a_e} \sim C_i B^l \tag{4}$$

bestehen, wo C_i eine beliebige Klasse aus dem System C, und B eine beliebige Klasse aus k' bedeutet, außer wenn sämtliche a_i durch l teilbar sind. Die Unmöglichkeit von (4) erkennt man, wenn man auf beiden Seiten die Relativnorm in bezug auf k bildet. Es folgt daher aus § 7, daß e unabhängige primäre Zahlen $\omega_1, \cdots, \omega_e$ in k' existieren, welche unverzweigte relativzyklische Körper vom Relativgrad l in bezug auf k' definieren und respektive zu den durch die Kongruenzen:

$$x_i \equiv 0\,(l)$$

definierten Untergruppen der Klassengruppe von k' gehören. Ich betrachte jetzt den Körper $\left(k', \sqrt[l]{\omega_1}\right)$ und will zunächst zeigen, daß er in bezug auf k relativ-Abelsch ist. Bezeichnet man die erzeugende Substitution der Relativgruppe von k' in bezug auf k mit

$$s = \zeta \,|\, \zeta^r,$$

so gilt:

$$s^{l'} = 1, \quad r^{l'} \equiv 1\,(l). \tag{5}$$

Da nun die Untergruppe der Klassengruppe von k', zu der ω_1 gehört, gegenüber s invariant ist, so muß dasselbe von dem Körper $\left(k', \sqrt[l]{\omega_1}\right)$ gelten, d. h. es muß eine Beziehung:

$$s\,\omega_1 = \omega_1^a \beta^l \tag{6}$$

bestehen, wo a eine rationale ganze Zahl und β eine Zahl aus k' bedeutet. Um zu zeigen, daß $\left(k', \sqrt[l]{\omega_1}\right)$ in bezug auf k relativ-Abelsch ist, hat man nachzuweisen, daß die Kongruenz:

$$a \equiv r\,(l) \tag{7}$$

gilt. Wir setzen zu diesem Zweck:

$$l' = p_1^{q_1} r_1 = p_2^{q_2} r_2 = \cdots, \tag{8}$$

wo $p_1^{q_1}, p_2^{q_2}, \cdots$ die verschiedenen in l' aufgehenden Primzahlpotenzen bedeuten, und beweisen, daß die Kongruenzen

$$\begin{aligned} a^{r_1} &\equiv r^{r_1}\,(l), \\ a^{r_2} &\equiv r^{r_2}\,(l), \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \end{aligned} \tag{9}$$

gelten. Aus der Gesamtheit derselben folgt leicht die Richtigkeit von (7). Denn da die Zahlen $r_1, r_2, \cdots$ nicht sämtlich einen gemeinsamen Teiler haben, so läßt sich die Gleichung:

$$y_1 r_1 + y_2 r_2 + \cdots = 1$$

durch ganze rationale y erfüllen und es folgt dann aus (9)

$$a^{y_1 r_1 + y_2 r_2 + \cdots} \equiv r^{y_1 r_1 + y_2 r_2 + \cdots}\,(l),$$

d. h.

$$a \equiv r\,(l).$$

Es genügt, von den Kongruenzen (9) die Richtigkeit der ersten nachzuweisen, da der Beweis für die übrigen sich analog gestaltet. Zu diesem Nachweis müssen wir uns ein Primideal $\mathfrak{P}_1$ in k' verschaffen, das folgende beiden Eigenschaften besitzt: 1) es muß in einer Idealklasse liegen, die der Bedingung $x_1 \not\equiv 0\,(l)$ genügt, wo x_1 den Exponenten von c_1 in der Klassengruppe von k' bedeutet; 2) es muß $s'\mathfrak{P}_1 = \mathfrak{P}_1$ sein, wenn wir mit s' die Substitution s^{r_1} bezeichnen. Haben wir ein solches Primideal gefunden, so ist die Richtigkeit der Kongruenz:

$$a^{r_1} \equiv r^{r_1}\,(l) \tag{10}$$

in folgender Weise einzusehen. Nach den Annahmen über $\mathfrak{P}_1$ gilt:

$$\left(\frac{\omega_1}{\mathfrak{P}_1}\right)_l = \zeta^* \neq 1 \tag{11}$$

und folglich, wenn wir die Substitution s' auf (11) anwenden:

$$\left(\frac{\omega_1^{a^{r_1}}}{\mathfrak{P}_1}\right)_l = (\zeta^*)^{r^{r_1}}. \tag{12}$$

Daraus ergibt sich die Gültigkeit von (10).

Wir haben also jetzt nur noch, um den Beweis vollständig zu machen, zu zeigen, daß ein Primideal $\mathfrak{P}_1$ in k' mit den oben angegebenen Eigenschaften existiert. Wir betrachten zu diesem Zweck den Oberkörper k_1 von k, der zu der Gruppe $\left(s^{p_1^{q_1}}\right)^x$ $(x = 0, 1, \cdots, r_1 - 1)$ gehört. Derselbe ist relativzyklisch in bezug auf k vom Relativgrad $p_1^{q_1}$ und besitzt einen Unterkörper Uk_1, der relativzyklisch vom Relativgrad p_1 in bezug auf k ist. Ich behaupte nun, daß es in einer Klasse von k, die der Bedingung $x_1 \not\equiv 0\,(l)$ genügt, ein Primideal gibt, das in Uk_1 und folglich dann auch in k_1 Primideal bleibt. Bezeichnet nämlich $\mathfrak{P}_i$ ein beliebiges Primideal aus Uk_1, so gilt

$$\sum \frac{1}{n(\mathfrak{P}_i)^s} = \log\frac{1}{s-1} + f_1(s) \qquad (s > 1)$$

und daher

$$\sum \frac{1}{n(\mathfrak{p}_i)^s} = \frac{1}{p_1}\cdot\log\frac{1}{s-1} + f_2(s), \qquad (s > 1)$$

wenn

$$\mathfrak{p}_i = N_k^{Uk_1}(\mathfrak{P}_i)$$

gesetzt wird. Bezeichne ich andererseits alle Primideale in k, die in einer Klasse mit $x_1 \not\equiv 0\,(l)$ liegen, mit $\mathfrak{q}_i$, so folgt aus Satz 1:

$$\sum \frac{1}{n(\mathfrak{q}_i)^s} \geqq \frac{l-1}{l}\log\frac{1}{s-1} + f_3(s) \qquad (s > 1).$$

Die Funktionen $f(s)$ bleiben endlich, wenn sich s der Grenze 1 nähert. Da $\frac{l-1}{l} > \frac{1}{p_1}$ ist, so ergibt sich somit, daß unendlichviele Primideale aus einer Klasse, die der Bedingung $x_1 \not\equiv 0\,(l)$ genügt, in Uk_1 und deshalb in k_1 Primideale bleiben. Ist $\mathfrak{p}_1$ ein solches Primideal und $\mathfrak{P}_1$ ein Primfaktor desselben in k', so erfüllt $\mathfrak{P}_1$ die beiden oben angegebenen Bedingungen.

Wir haben damit bewiesen, daß der Körper $(k', \sqrt[l]{\omega_1})$ in bezug auf k relativ Abelsch vom Relativgrad $l'l$ ist. Die Relativgruppe besitzt deshalb eine ausgezeichnete Untergruppe vom Grade l', zu der der Körper K_1 gehören möge. K_1 ist dann relativzyklisch vom Relativgrad l in bezug auf k und unverzweigt, wie sich leicht zeigen läßt. Ginge nämlich das Primideal $\mathfrak{p}$ aus k in der Relativdiskriminante von K_1 in bezug auf k auf, so müßte $\mathfrak{p}$ in K_1 in l gleiche Primfaktoren zerfallen. Wenn man dann $\mathfrak{p}$ in $(k', \sqrt[l]{\omega_1})$ zerlegt, so müßten sich die Primfaktoren in Systeme von je l gleichen anordnen lassen. Daraus würde folgen, daß es ein Primideal $\mathfrak{P}$ in k' geben müßte, das in $(k', \sqrt[l]{\omega_1})$ in l gleiche Primfaktoren zerfällt, was unmöglich ist. Es ist also K_1 in bezug auf k unverzweigt.

Verfährt man jetzt in derselben Weise mit $(k', \sqrt[l]{\omega_2})$, $(k', \sqrt[l]{\omega_3})$, $\cdots$, wie wir es eben mit $(k', \sqrt[l]{\omega_1})$ getan haben, so erhält man die Körper $K_2, K_3, \cdots$. Das System der Körper

$$K_1, K_2, \cdots, K_e$$

liefert dann e unverzweigte unabhängige relativzyklische Körper vom Relativgrad l in bezug auf k, womit unser Satz bewiesen ist.

§ 10.

Konstruktion der unverzweigten relativquadratischen Körper, wenn unter den konjugierten Körpern des Grundkörpers k reelle vorhanden sind.

Die bisherigen Entwicklungen bezogen sich auf den Fall, daß l eine ungerade Primzahl ist; sie gelten, wie bereits erwähnt ist, auch für $l=2$, wenn noch die weitere Voraussetzung erfüllt ist, daß der Grundkörper nebst allen konjugierten imaginär ist. Ist das nicht der Fall, so sind besondere Entwicklungen nötig, die in diesem Paragraphen gegeben werden sollen. Es genügt jetzt, wenn man alle unverzweigten relativquadratischen Körper erhalten will, nicht mehr der gewöhnliche Äquivalenzbegriff, sondern es ist der von D. Hilbert*) eingeführte schärfere Äquivalenzbegriff zugrunde zu legen, nach dem zwei Ideale nur dann äquivalent heißen, wenn ihr Quotient als total positive**) Körperzahl darstellbar ist.

*) Rel. Abelsche Zahlk., § 5.

**) Eine Körperzahl heißt total positiv, wenn ihre sämtlichen konjugierten Zahlen, soweit sie reell sind, positiv sind.

Es sei noch bemerkt, daß im folgenden, wenn von den zu k konjugierten Körpern die Rede ist, immer der Körper k einbegriffen ist.

Wir nehmen an, daß der Grad des Körpers k gleich m sei und daß sich unter den konjugierten Körpern s reelle befinden. Wir haben dann zunächst noch eine für k charakteristische Zahl p zu definieren, wobei wir festsetzen, daß die zu einer Zahl α aus k konjugierte Zahl, die in dem mit k konjugierten Körper $k^{(i)}$ liegt, mit $\alpha^{(i)}$ bezeichnet werden soll.

Es sei ε_1^* eine Einheit aus k, unter deren konjugierten sich wenigstens eine negative befindet und zwar sei dies $\varepsilon_1^{*(z_1)}$ in $k^{(z_1)}$; es sei dann ε_2^* eine solche Einheit, daß $\varepsilon_2^{*(z_1)}$ positiv und $\varepsilon_2^{*(z_2)}$ negativ ist; weiter sei ε_3^* eine solche Einheit, daß $\varepsilon_3^{*(z_1)}$ und $\varepsilon_3^{*(z_2)}$ positiv sind und $\varepsilon_3^{*(z_3)}$ negativ usw. Die letzte auf solche Weise zu wählende Einheit sei ε_p^*; es folgt dann, daß jede Einheit ε in k, deren konjugierte in $k^{(z_1)}, \cdots, k^{(z_p)}$ positiv sind, auch in den noch übrigen reellen Körpern $k^{(z_{p+1})}, \cdots, k^{(z_s)}$ positive konjugierte Einheiten hat. Die Zahl p läßt sich auch in folgender Weise charakterisieren. Die Anzahl der Grundeinheiten von k ist $m'-1$, wo $m' = \frac{m+s}{2}$ ist. Nimmt man zu diesen noch eine Einheitswurzel aus k hinzu, deren Quadratwurzel nicht in k liegt, so erhält man $2^{m'}$ Einheitenverbände in k, unter denen sich mindestens $2^{m'-s}$ Verbände von total positiven Einheiten finden. Ist $s-p=p'>0$, so wird diese Minimalzahl überschritten und es gibt in k genau $2^{m'-p}$ Verbände von total positiven Einheiten.

Aus den im vorstehenden für den Körper k gemachten Annahmen, die keine Beschränkung enthalten, folgt, daß man zu jeder Zahl α in k eine Einheit ε so bestimmen kann, daß die Zahlen $(\varepsilon\alpha)^{(z_1)}, \cdots, (\varepsilon\alpha)^{(z_p)}$ positiv werden. Daraus folgt, daß zwischen den Klassenzahlen 2^h und $2^{h'}$ von k, von denen die erste im engeren, die zweite im weiteren Sinne verstanden sei, die Beziehung besteht:

$$2^h = 2^{h'} \cdot 2^{p'}, \quad p' = s - p.$$

Es möge nun das Klassensystem von k, wenn der engere Äquivalenzbegriff zugrunde gelegt wird, in der Gestalt:

$$c_1^{x_1} \cdots c_e^{x_e} d_1^{y_1} \cdots d_{e'}^{y_{e'}} \; (x_i = 0, 1, \cdots, 2^{h_i}-1;\; y_i = 0, 1); \; h_1 + \cdots + h_e + e' = h,$$

darstellbar sein, wo $d_1, \cdots, d_{e'}$ solche Klassen bedeuten, die bei Zugrundelegung des weiteren Äquivalenzbegriffes in die Hauptklasse fallen. Die Erhöhung der Klassenzahl in k bei der schärferen Fassung des Äquivalenzbegriffes kommt also dadurch zustande, daß erstens e' neue Basisklassen zur Klassengruppe hinzutreten und daß zweitens $e'' = p' - e'$ Basisklassen in k eine Verdoppelung ihres Exponenten erfahren. Die Bezeichnung der Klassen möge so gewählt sein, daß dies die Klassen $c_1, \cdots, c_{e''}$ sind.

Wir behaupten jetzt, daß genau $e+e'$ unabhängige unverzweigte relativ-quadratische Körper in bezug auf k existieren.

Zum Beweise bezeichnen wir die Grundeinheiten in k, zu denen noch eine Einheitswurzel, deren Quadratwurzel nicht in k liegt, hinzugenommen ist, mit $\varepsilon_1, \cdots, \varepsilon_{m'}$, wo $m' = \frac{m+s}{2}$ ist. Die Gesamtheit der Einheitenverbände ist dann in der Gestalt:

(1) $$\varepsilon_1^{u_1} \cdots \varepsilon_{m'}^{u_{m'}} \xi^2$$

darstellbar, wo ξ alle Einheiten aus k durchläuft; wir wollen uns dabei die Bezeichnung so gewählt denken, daß $\varepsilon_{p+1}, \cdots, \varepsilon_{m'}$ total positive Einheiten sind. Wir bezeichnen ferner mit $\mathfrak{r}_1, \cdots, \mathfrak{r}_e$ Ideale aus den Klassen $c_1, \cdots, c_e$ und setzen

$$\mathfrak{r}_1^{2^{h_1-1}} = \varrho_1, \cdots, \mathfrak{r}_{e''}^{2^{h_{e''}-1}} = \varrho_{e''}, \quad \mathfrak{r}_{e''+1}^{2^{h_{e''}+1}} = \varrho_{e''+1}, \cdots, \mathfrak{r}_e^{2^{h_e}} = \varrho_e,$$

wo die Größen $\varrho_1, \cdots, \varrho_e$ Zahlen aus k bedeuten, die nicht Quadrate von Zahlen sind. Wir schreiben nun:

$$\varepsilon_{m'+1} = \varrho_1, \cdots, \varepsilon_{m'+e} = \varrho_e$$

und bestimmen $m'+e-p$ Primideale $\mathfrak{q}_i$ derart, daß:

$$\left(\frac{\varepsilon_i}{\mathfrak{q}_i}\right)_2 = -1, \quad \left(\frac{\varepsilon_j}{\mathfrak{q}_i}\right)_2 = 1, \quad \begin{pmatrix} i = p+1, \cdots, m'+e; & \\ j = 1, 2, \cdots, m'+e; & i \neq j \end{pmatrix}.$$

Man wähle darauf die Exponenten w so, daß

$$\mathfrak{q}_{p+1} \mathfrak{r}_1^{w_{p+1}^{(1)}} \cdots \mathfrak{r}_e^{w_{p+1}^{(e)}} = (\varkappa_{p+1}),$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$\mathfrak{q}_{m'+e} \mathfrak{r}_1^{w_{m'+e}^{(1)}} \cdots \mathfrak{r}_e^{w_{m'+e}^{(e)}} = (\varkappa_{m'+e})$$

wird, wo $\varkappa_{p+1}, \cdots, \varkappa_{m'+e}$ Zahlen aus k bedeuten. Bildet man jetzt das System von Zahlen

(2) $$\omega = \varepsilon_1^{u_1} \cdots \varepsilon_{m'+e}^{u_{m'+e}} \varkappa_{p+1}^{v_{p+1}} \cdots \varkappa_{m'+e}^{v_{m'+e}},$$

indem man die v den bekannten e Bedingungen unterwirft, damit kein Faktor der Ideale $\mathfrak{r}_1, \cdots, \mathfrak{r}_e$ in der Relativdiskriminante von $(k, \sqrt{\omega})$ in bezug auf k aufgeht, so enthält dasselbe im ganzen $2^{2m'+e-p}$ Zahlen. Da nun im ganzen nur $2^{2m'-s}$ Arten von Zahlen in k existieren, so gibt es $e+p'$ unabhängige primäre Zahlen von der Gestalt (2).*) Wir bezeichnen mit:

*) Primär nennen wir eine zu 2 prime Zahl, wenn sie dem Quadrat einer Zahl aus k nach dem Modul 4 kongruent ist; dagegen fordern wir nicht, daß sie total positiv sei, wie D. Hilbert für die Aufstellung der Reziprozitätsgesetze im Körper k definiert hat. In diesem Sinne sind auch seine Ausführungen auf p. 378 der Rel. Abelschen Zahlk., speziell Satz 9, zu berichtigen, da an dieser Stelle ebenfalls die obige Definition der primären Zahl anzuwenden ist.

$$\omega_1 = \varepsilon_1^{u_1} \cdots \varepsilon_{m'+e}^{u_{m'+e}} \varkappa_{p+1}^{v_{p+1}} \cdots \varkappa_{m'+e}^{v_{m'+e}}$$

eine solche und untersuchen jetzt den Körper $K_1 = (k, \sqrt{\omega_1})$. Es mögen die Exponenten $v_{i_1}, \cdots, v_{i_t}$ von Null verschieden sein, ferner möge ω_1 in n der reellen Körper $k^{(z_1)}, \cdots, k^{(z_s)}$ negativ werden und es mögen l^{e_1} Idealklassen aus k in weiterem Sinne in K in die Hauptklasse (in weiterem Sinne) übergehen.*) Haben dann a^*, a, v^*, v dieselbe Bedeutung wie früher, so gilt die Ungleichung:

$$a^* \leqq t - m' + v^* + n + e_1 - 1. \tag{3}$$

Man erhält dieselbe, wenn man zunächst in analoger Weise, wie es D. Hilbert**) für ungerades l ausgeführt hat, ein System von $\frac{m+s}{2} - n$ relativen Grundeinheiten von K_1 in bezug auf k konstruiert und dann ebenso wie in § 4 verfährt.

Um eine Ungleichung für a, die Anzahl der unabhängigen ambigen Komplexe in K_1, zu gewinnen (bei ihrer Definition werde der weitere Äquivalenzbegriff zugrunde gelegt), bezeichnen wir die Anzahl negativer unter den Zahlen:

$$\omega_1^{(z_1)}, \omega_1^{(z_2)}, \cdots, \omega_1^{(z_p)}$$

mit n_1; die Anzahl negativer unter den Zahlen:

$$\omega_1^{(z_{p+1})}, \cdots, \omega_1^{(z_s)}$$

ist dann $n - n_1$. Sind ferner unter den Indizes $i_1, \cdots, i_t$ f aus der Reihe $m' + 1, \cdots, m' + e$ vorhanden, so gilt:

$$a \leqq a^* + v - v^* + e - f - e_1. \tag{4}$$

Die Überlegungen zur Ableitung dieser Ungleichung sind völlig analog denen in § 5.

Jede Zahl α nun, die Relativnorm einer Zahl aus K_1 ist, muß die Bedingungen***):

$$\left(\frac{\alpha, \omega_1}{1^{(z_i)}}\right) = 1, \quad (i = 1, 2, \cdots, s)$$

erfüllen. Denn ist $\omega_1^{(z_i)}$ positiv, so ist das Vorzeichensymbol selbstverständlich positiv; ist aber $\omega_1^{(z_i)}$ negativ, so folgt aus:

$$\alpha^{(z_i)} = \left(\alpha_1 + \alpha_2 \sqrt{\omega_1^{(z_i)}}\right)\left(\alpha_1 - \alpha_2 \sqrt{\omega_1^{(z_i)}}\right) = \alpha_1^2 - \alpha_2^2 \omega_1^{(z_i)},$$

---

*) Für die Konstruktion der ersten e unverzweigten relativquadratischen Körper genügt der weitere Äquivalenzbegriff.

**) Algebr. Zahlk., § 55, p. 572.

***) Vgl. Hilbert, Rel. Abelsche Zahlk., § 6, p. 376.

daß $\alpha^{(z_i)}$ positiv ist; es ist also auch in diesem Falle das Vorzeichensymbol gleich $+1$. Beachtet man dies, so ergibt sich:

$$v \leqq m' - t + f - n_1. \tag{5}$$

Addiert man jetzt die Ungleichungen (3), (4) und (5), so folgt:

$$a \leqq e - 1 + n - n_1. \tag{6}$$

Um jetzt sämtliche Ideale aus K_1 darzustellen, definiert man in analoger Weise wie in § 6 die Ideale $\mathfrak{Q}_1, \mathfrak{Q}_2, \cdots, \mathfrak{Q}_a$ in K_1 und zeigt wie dort, daß für jedes Ideal $\mathfrak{J}$ in K_1 eine Relation gilt:

$$\mathfrak{J}^q = A\,\mathfrak{j}\,\mathfrak{Q}_1^{F_1(S_1)} \cdots \mathfrak{Q}_a^{F_a(S_1)}, \tag{7}$$

wo A eine Zahl aus K_1, $\mathfrak{j}$ ein Ideal aus k, q einen ungeraden Exponenten und S_1 die Substitution $\sqrt{\omega_1} \mid -\sqrt{\omega_1}$ bedeutet.

Ist nun $e > 0$, so kann man offenbar, da $e + p'$ unabhängige primäre Zahlen ω zur Verfügung stehen, ω_1 so wählen, daß die sämtlichen Zahlen $\omega_1^{(z_p+1)}, \cdots, \omega_1^{(z_s)}$ positiv werden. Es ist dann $n = n_1$ und folglich:

$$a \leqq e - 1.$$

Aus der letzten Ungleichung schließt man mit Hilfe von (7), daß alle Primideale $\mathfrak{p}$ in k mit der Eigenschaft $\left(\frac{\omega_1}{\mathfrak{p}}\right)_2 = 1$ in einer Untergruppe vom Grade 2^{h-1} (oder $2^{h'-1}$ bei Zugrundelegung des weiteren Äquivalenzbegriffes) der Klassengruppe von k liegen, die durch eine Kongruenz:

$$a_1 x_1 + \cdots + a_e x_e \equiv 0\,(2)$$

definiert wird. Daraus schließt man in bekannter Weise die Unverzweigtheit von K_1. In gleicher Weise wie K_1 kann man noch $e-1$ unabhängige unverzweigte relativquadratische Körper $K_1, \cdots, K_e$ konstruieren durch Benutzung der primären Zahlen $\omega_2, \cdots, \omega_e$, die ebenso wie ω_1 die Eigenschaft haben, daß ihre konjugierten in den Körpern $k^{(z_p+1)}, \cdots, k^{(z_s)}$ sämtlich positiv sind.

Wir haben jetzt noch p' unabhängige primäre Zahlen aus (2) zur Verfügung und wollen zeigen, daß man mit ihrer Hilfe noch genau e' unabhängige unverzweigte relativquadratische Körper in bezug auf k konstruieren kann. Ich wähle zu diesem Zweck eine Zahl δ_1 aus der Klasse d_1' des Klassensystems $d_1^{y_1} \cdots d_{e'}^{y_{e'}}$, die nicht Hauptklasse im engeren Sinne ist, und normiere δ_1 durch Multiplikation mit einer Einheit so, daß die zu δ_1 konjugierten Zahlen in den Körpern $k^{(z_1)}, \cdots, k^{(z_p)}$ positiv sind. Es muß dann unter den Zahlen:

$$\delta_1^{(z_p+1)}, \cdots, \delta_1^{(z_s)} \tag{8}$$

sicher eine negative sein; man kann ohne Beschränkung der Allgemeinheit annehmen, daß die erste unter ihnen negativ sei. Ferner wollen wir noch voraussetzen, daß die Klasse d_1' so gewählt sei, daß unter den Zahlen (8) möglichst wenige negative vorkommen.

Unter den p' unabhängigen primären Zahlen aus (2), die noch zur Verfügung stehen, gibt es nun keine einzige mehr, deren sämtliche konjugierte in den Körpern $k^{(z_p+1)}, \cdots, k^{(z_s)}$ positiv wären. Denn sonst könnte man noch einen unabhängigen Körper von der Art der Körper $K_1, \cdots, K_e$ konstruieren, was unmöglich ist. Denn es existieren in der Klassengruppe von k im weiteren Sinne nur $2^e - 1$ Untergruppen vom Grade $2^{h'-1}$, denen die $2^e - 1$ konstruierten unverzweigten Körper eindeutig zugeordnet sind. Es folgt daraus, daß man stets eine primäre Zahl ω_{e+1} von der Gestalt (2) angeben kann, so daß $\omega_{e+1}^{(z_p+1)}$ negativ und $\omega_{e+1}^{(z_p+2)}, \cdots, \omega_{e+1}^{(z_s)}$ positiv ausfallen. Wir untersuchen jetzt den Körper $K_{e+1} = \left(k, \sqrt{\omega_{e+1}}\right)$ und behaupten, daß die Anzahl der ambigen Komplexe in ihm größer als $e - 1$ ist. Wäre sie nämlich gleich oder kleiner als $e - 1$, so würde folgen, daß der Körper K_{e+1} zu einer Untergruppe der Klassengruppe von k gehört, zu der bereits ein unverzweigter Körper konstruiert ist, was unmöglich ist. Es gilt also für K_{e+1}:

$$a \geqq e,$$

andererseits folgt aus (6), da $n - n_1 = 1$ ist,

$$a \leqq e,$$

es ist also die Anzahl der ambigen Komplexe genau gleich e. Daraus schließt man, daß

$$v = m' - t + f - n_1 \tag{9}$$

ist; denn nach (4) ist v nicht kleiner und nach (5) nicht größer als die rechte Seite von (9). Die Ideale in K_{e+1} lassen sich nun wieder in der Form darstellen:

$$\mathfrak{J}^q = A\, \mathfrak{j}\, \mathfrak{Q}_1^{F_1(S_1)} \;.\;.\;.\; \mathfrak{Q}_e^{F_e(S_1)}, \tag{10}$$

wo die Bezeichnungen die analoge Bedeutung wie in (7) haben. Die Ideale $\mathfrak{Q}_1, \cdots, \mathfrak{Q}_e$ kann man sich so gewählt denken, daß ihre Relativnormen resp. in die Klassen $c_1, \cdots, c_e$ fallen. Ich behaupte jetzt, daß die Relativnormen von Zahlen aus K_{e+1} nicht in die Klasse d'_1 fallen können. Ist nämlich α die Relativnorm einer beliebigen Zahl A aus k, so gilt zunächst für jeden Index i:

$$\left(\frac{\alpha, \omega_{e+1}}{1^{(i)}}\right) = 1 \cdot \tag{11}$$

Um unsere Behauptung zu beweisen, normieren wir α, d. h. wir verwandeln α durch Multiplikation mit einer geeignet gewählten Einheit ξ_α aus k in eine Zahl, deren konjugierte in den Körpern $k^{(z_1)}, \cdots, k^{(z_p)}$ positiv sind. Wir wollen zeigen, daß wir dies stets mit Hilfe einer Einheit bewerkstelligen können, die selbst Relativnorm einer Zahl aus K_{e+1} ist.

Bedeuten nämlich $k^{(y_1)}, \cdots, k^{(y_{n_1})}$ diejenigen unter den Körpern $k^{(z_1)}, \cdots, k^{(z_p)}$, in denen die zu ω_{e+1} konjugierten Zahlen negativ werden, so ist zunächst klar, daß alle Einheiten ξ, welche die Bedingungen:

$$(12) \qquad \left(\frac{\xi}{\mathfrak{q}_{i_1}}\right) = 1, \cdots, \left(\frac{\xi}{\mathfrak{q}_{i_t}}\right) = 1$$

$$(13) \qquad \left(\frac{\xi, \omega_{e+1}}{\mathfrak{l}^{(y_1)}}\right) = 1, \cdots, \left(\frac{\xi, \omega_{e+1}}{\mathfrak{l}^{(y_{n_1})}}\right) = 1$$

befriedigen, Relativnormen von Zahlen aus K_{e+1} sind. Denn alle Einheiten, welche diese Eigenschaft haben, müssen (12) und (13) erfüllen. Es kann daher höchstens $m' - t + f - n_1$ unabhängige Einheitenverbände geben, deren Einheiten Relativnormen von Zahlen aus K_{e+1} sind; daraus folgt in Verbindung mit (9), daß alle Einheiten, welche die Bedingungen (12) und (13) erfüllen, Relativnormen von Zahlen aus K_{e+1} sind.

Es mögen nun unter den Zahlen $\alpha^{(z_1)}, \cdots, \alpha^{(z_p)}$ im ganzen n' negative vorhanden sein, die mit:

$$(14) \qquad \alpha^{(x_1)}, \cdots, \alpha^{(x_{n'})}$$

bezeichnet seien. Die gesuchte Einheit ξ_α hat dann außer den Bedingungen (12) und (13) noch die weiteren:

$$(15) \qquad \xi_\alpha^{(x_1)}, \cdots, \xi_\alpha^{(x_{n'})} \text{ negativ}$$

zu erfüllen. Um die Einheit ξ_α bequemer darstellen zu können, wollen wir noch über die Einheiten $\varepsilon_1, \cdots, \varepsilon_p$ in (1) eine besondere Verfügung treffen. Wir wollen uns ε_i so gewählt denken, daß

$$-1, \left(\frac{\varepsilon_i}{\mathfrak{q}_j}\right) = 1; \qquad \varepsilon_i^{(z_i)} < 0,\ \varepsilon_i^{(z_j)} > 0 \qquad \left(\begin{matrix} i, j = 1, 2, \cdots, p \\ j \neq i \end{matrix}\right).$$

Daß diese Wahl, durch die die Ideale $\mathfrak{q}_i$ nicht weiter berührt werden, stets möglich ist, erkennt man leicht, wenn man bedenkt, daß die Vorzeichenanordnungen, die sich durch die Reihen:

$$\varepsilon^{(z_1)}, \cdots, \varepsilon^{(z_p)}$$

ergeben, wenn man ε alle Einheiten des Systems:

$$\varepsilon_1^{u_1} \cdot \varepsilon_2^{u_2} \cdots \varepsilon_p^{u_p}, \quad (u = 0, 1)$$

durchlaufen läßt, alle überhaupt möglichen sind. Setzt man jetzt:

$$\xi_\alpha = \varepsilon_{x_1} \cdot \varepsilon_{x_2} \cdots \varepsilon_{x_{n'}},$$

so ist ξ_α eine Einheit der gewünschten Art. Denn sie befriedigt die Bedingungen (12) und (15). Daß sie auch (13) befriedigt, folgt daraus, daß alle Indizes $x_1, \cdots, x_{n'}$ von den Indizes $y_1, \cdots, y_{n_1}$ verschieden sind. Denn aus (11) und (14) folgt, daß:

$$\omega^{(x_1)}, \cdots, \omega^{(x_{n'})} \qquad \omega = \omega_{e+1}$$

positiv sind. Damit ist unsere Behauptung bewiesen, daß sich α mit Hilfe einer Einheit normieren läßt, die Relativnorm einer Zahl aus K_{e+1} ist. Ich kann daher direkt annehmen, daß α normiert sei. Fiele nun α in die Klasse d_1', so wäre α mit δ_1 im engeren Sinne äquivalent und folglich $\alpha^{(z_p+1)}$ negativ. Da auch $\omega_{e+1}^{(z_p+1)}$ negativ ist, so widerspricht dies der Relation:

$$\left(\frac{\alpha,\, \omega_{e+1}}{\mathfrak{l}^{(z_p+1)}}\right) = 1 \cdot$$

Damit ist gezeigt, daß α nicht in der Klasse d_1' liegen kann, und deshalb folgt aus (10), daß alle Relativnormen von Idealen aus K_{e+1} in einer Untergruppe der Klassengruppe von k vom Grade 2^{h-1} liegen. Daraus schließt man in bekannter Weise, daß K_{e+1} unverzweigt in bezug auf k ist.

Ist $e' > 1$, so kann man noch einen weiteren unverzweigten relativquadratischen Körper in bezug auf k konstruieren. Wir nehmen zu diesem Zweck an, daß K_{e+1} zu der durch die Kongruenz:

$$y_1 \equiv 0\,(2)$$

definierten Untergruppe der Klassengruppe von k gehört, was offenbar durch nachträgliche Abänderung der Bezeichnung der Klassen d stets erreicht werden kann. Es sei nun δ_2 eine Zahl aus einer Klasse d_2' des Systems $d_2^{y_2} \cdots d_{e'}^{y_{e'}}$, die nicht Hauptklasse im engeren Sinne ist, und zwar sei δ_2 normiert. Es muß dann unter den Zahlen:

$$(16) \qquad \delta_2^{(z_p+2)}, \ldots, \delta_2^{(z_s)}$$

eine negative sein. Denn wären alle Zahlen (16) positiv, so müßten auch alle Zahlen $\delta_1^{(z_p+2)}, \ldots, \delta_1^{(z_s)}$ positiv sein, weil δ_1 so gewählt sein sollte, daß unter den Zahlen (8) möglichst wenige negative vorkommen. Es wäre dann δ_2 mit δ_1 äquivalent, was der Wahl der Klasse d_2' widerspricht. Wir nehmen deshalb an, die erste der Zahlen (16) sei negativ, und setzen außerdem voraus, daß die Klasse d_2' so gewählt sei, daß sich unter den Zahlen (16) möglichst wenige negative befinden. Wir wählen dann unter den $p'-1$ noch zur Verfügung stehenden unabhängigen primären Zahlen aus (21) eine solche ω_{e+2} aus, daß $\omega_{e+2}^{(z_p+2)}$ negativ und $\omega_{e+2}^{(z_p+3)}, \ldots, \omega_{e+2}^{(z_s)}$ positiv ausfallen. Durch Multiplikation mit einer geeigneten Potenz von ω_{e+1} können wir es offenbar auch noch erreichen, daß $\omega_{e+2}^{(z_p+1)}$ positiv wird. Wir wollen also voraussetzen, daß unter den Zahlen:

$$\omega_{e+2}^{(z_p+1)},\ \omega_{e+2}^{(z_p+2)}, \ldots, \omega_{e+2}^{(z_s)}$$

nur die zweite negativ sei. Es lassen sich dann für ω_{e+2} die ganz analogen Überlegungen durchführen wie für ω_{e+1}, womit die Existenz eines zweiten unabhängigen unverzweigten relativquadratischen Körpers in bezug auf k bewiesen ist. Den angegebenen Konstruktionsprozeß kann man offenbar fortsetzen und zu den Körpern $K_1, \cdots, K_e$ noch weitere e' Körper $K_{e+1}, \cdots, K_{e+e'}$ konstruieren, so daß damit im ganzen $e + e'$ unabhängige unverzweigte relativquadratische Körper in bezug auf k gewonnen sind, deren Existenz wir beweisen wollten.

§ 11.

Der Aufbau des Klassenkörpers.

Wir haben jetzt durch die Entwicklungen der vorstehenden Paragraphen die Bausteine gewonnen, aus denen wir den vollständigen Klassenkörper aufbauen können.

Es sei die Klassenzahl h von k gleich $l_1^{h_1'} \cdots l_i^{h_i'}$, wo $l_1, \cdots, l_i$ verschiedene Primzahlen sind; bei der Klassenzahlbestimmung ist der schärfere Äquivalenzbegriff zugrunde zu legen, nach dem zwei Ideale nur dann äquivalent heißen, wenn ihr Quotient eine total positive Körperzahl ist. Wir konstruieren dann, wie bereits in der Einleitung angegeben, unverzweigte relativ-Abelsche Körper in bezug auf k von den resp. Relativgraden $l_1^{h_1'}, \cdots, l_i^{h_i'}$. Durch Zusammensetzung dieser Körper entsteht dann der vollständige Klassenkörper. Es genügt, wenn wir hier die Konstruktion eines solchen Körpers angeben. Wir setzen deshalb $h = l_1^{h_1'} \cdot q$, wo q zu l_1 prim sei, und verstehen unter l_1 eine beliebige Primzahl.

Es sei wieder das System der q^{ten} Potenzen der Idealklassen von k in der Gestalt darstellbar:

$$(c)_k = c_1^{x_1} \cdots c_e^{x_e}, \ \left(x_i = 0, 1, \cdots, l_1^{h_i''} - 1\right), \ h_1'' + \cdots + h_e'' = h_1',$$

und es werde wieder, wie früher schon, um der einfacheren Ausdrucksweise willen, das System aller Klassen, deren q^{te} Potenz in die Hauptklasse fällt, mit 1 bezeichnet. Es möge nun $K_1^{(1)}$ derjenige unverzweigte Körper vom Relativgrad l_1 in bezug auf k sein, der zu der durch die Kongruenz $x_1 \equiv 0 (l_1)$ definierten Untergruppe der Klassengruppe von k gehört. Ist jetzt $h_1'' > 1$, also $c_1^{l_1} \neq 1$ in k, so ist in $K_1^{(1)}$ die Äquivalenz $c_1 \sim C^{l_1}$, wo C eine beliebige Klasse aus $K_1^{(1)}$ bedeutet, unmöglich. Denn aus der Annahme, daß $K_1^{(1)}$ zu der genannten Untergruppe gehört, folgt, daß

$$N_k(C) \sim c^{l_1} c_2^{a_2} \cdots c_e^{a_e} \quad \text{in} \quad k,$$

wo c eine Klasse aus k und $a_2, \cdots, a_e$ ganze rationale Zahlen bedeuten. Es müßte also auch gelten:

$$c_1^{l_1} \sim N_k(C^{l_1}) \sim c^{l_1} c_2^{a_2 l_1} \cdots c_e^{a_e l_1} \quad \text{in} \quad k,$$

und hieraus würde folgen, daß

$$c_1^{b_1 l_1} c_2^{b_2 l_1} \cdots c_e^{b_e l_1} \sim 1 \quad \text{in} \quad k,$$

wo $b_1, \cdots, b_e$ wieder ganze rationale Zahlen bedeuten, von denen die erste nicht durch l_1 teilbar ist. Da die letzte Äquivalenz unmöglich ist, wenn $c_1^{l_1} \not\sim 1$ in k, so ist auch die Äquivalenz $c_1 \sim C^{l_1}$ in $K_1^{(1)}$ unmöglich.

Führen wir den Begriff des *Klassenverbandes* ein als eines Systems von Klassen, das durch Multiplikation einer fest gegebenen Klasse mit den l_1^{ten} Potenzen aller Klassen des Körpers entsteht, und nennen Hauptklassenverband denjenigen, der die l_1^{ten} Potenzen aller Klassen enthält, so können wir die vorstehenden Entwicklungen dahin zusammenfassen, daß c_1 einen vom Hauptverbande verschiedenen Klassenverband in $K_1^{(1)}$ definiert. Es existiert dann, wie aus den Entwicklungen der vorigen Paragraphen folgt, in bezug auf $K_1^{(1)}$ ein unverzweigter relativzyklischer Körper $K_1^{(2)}$ vom Relativgrad l_1, der zu der durch die Bedingung „Exponent von c_1 durch l_1 teilbar" definierten Untergruppe der Klassengruppe von $K_1^{(1)}$ gehört. Bezeichnet man jetzt die erzeugende Substitution der Relativgruppe von $K_1^{(1)}$ in bezug auf k mit S_1, so folgt aus dem Umstande, daß die genannte Bedingung gegenüber S_1 invariant ist, daß $K_1^{(2)}$ ein relativ-Galoisscher Körper vom Relativgrad l_1^2 in bezug auf k ist. Daß er auch relativ-Abelsch ist, folgt aus der Darstellung der Substitutionen seiner Relativgruppe, die die Vertauschbarkeit derselben ohne weiteres erkennen läßt. Daß er endlich relativzyklisch sein muß, folgt aus dem Umstande, daß er nur einen relativzyklischen Unterkörper vom Relativgrad l_1 in bezug auf k besitzt. Denn unter den Abelschen Gruppen vom Grade l_1^2 besitzt nur die zyklische die Eigenschaft, daß sie nur *eine* Untergruppe vom Grade l_1 besitzt. Ist nämlich eine Abelsche Gruppe vom Grade l_1^2 nicht zyklisch, so ist sie in der Gestalt

$$S_1^{x_1} S_2^{x_2} \, (x_i = 0, 1, \cdots, l_1 - 1)$$

darstellbar und besitzt daher mehr als eine Untergruppe vom Grade l_1.

Daß $K_1^{(2)}$ nur einen Unterkörper vom Relativgrad l_1 in bezug auf k, nämlich den Körper $K_1^{(1)}$, besitzt, ist nach der Konstruktion der Körper beinahe selbstverständlich. Besäße nämlich $K_1^{(2)}$ noch einen zweiten Unterkörper K_1', so wäre dieser unverzweigt vom Relativgrad l_1 in bezug auf k und gehörte daher zu einer bestimmten Untergruppe der Klassengruppe von k, die von der durch die Bedingung $x_1 \equiv 0(l_1)$ definierten Untergruppe verschieden wäre. $K_1^{(2)}$ würde dann durch Zusammensetzung zweier in bezug auf k unverzweigter Körper vom Relativgrad l_1 entstehen, nämlich der Körper $K_1^{(1)}$ und K_1'. Das ist unmöglich, wie aus folgender

Überlegung hervorgeht. Das Klassensystem des Körpers $K_1^{(1)}$ läßt sich nach § 6 in der Gestalt schreiben:

$$C_2^{F_2(S_1)} \cdots C_e^{F_e(S_1)}(c)_k C^{l_1},$$

wo $C_2, \cdots, C_e$ Klassen aus $K_1^{(1)}$ bedeuten, deren Relativnormen in k in die Klassen $c_2, \cdots, c_e$ fallen; $(c)_k$ bedeutet das Klassensystem aus k, und C eine beliebige Klasse aus $K_1^{(1)}$. $F_2(S_1), \cdots, F_e(S_1)$ sind ganze ganzzahlige Funktionen von S_1 vom Grade $l_1 - 2$. Die Körper $K_2^{(1)}, \cdots, K_e^{(1)}$ nun, die unverzweigt vom Relativgrad l_1 in bezug auf k sind und zu den Untergruppen $x_2 \equiv 0(l_1), \cdots, x_e \equiv 0(l_1)$ resp. gehören, sind natürlich auch in bezug auf $K_1^{(1)}$ unverzweigt und gehören in $K_1^{(1)}$ resp. zu den durch folgende Bedingungen definierten $e-1$ Untergruppen der Klassengruppe von $K_1^{(1)}$:

$$F_2(1) \equiv 0(l_1), \cdots, F_e(1) \equiv 0(l_1).$$

Denn die Relativnormen aller Klassen aus $K_1^{(1)}$, die z. B. der Bedingung $F_2(1) \equiv 0(l_1)$ entsprechen, liefern in k die durch die Bedingung $x_2 \equiv 0(l_1)$ charakterisierte Untergruppe der Klassengruppe von k, und analog für die übrigen Indizes. Daraus folgt, daß K_1' in dem Körper $(K_1^{(1)}, K_2^{(1)}, \cdots, K_e^{(1)})$ nicht enthalten sein kann, weil K_1' in bezug auf $K_1^{(1)}$ zu der durch die Bedingung „Exponent von c_1 durch l_1 teilbar" definierten Untergruppe der Klassengruppe von $K_1^{(1)}$ gehört. Damit ist gezeigt, daß $K_1^{(2)}$ relativzyklisch vom Relativgrad l_1^2 in bezug auf k ist.

Ist h_1'' auch größer als 2, also $c_1^{l_1^2} \neq 1$ in k, so kann man das Verfahren fortsetzen, und es gelingt auf dem angegebenen Wege, einen relativzyklischen Körper vom Relativgrad $l_1^{h_1''}$ in bezug auf k zu konstruieren. In analoger Weise konstruiert man die unverzweigten relativzyklischen Körper $K_2^{(h_2'')}, \cdots, K_e^{(h_e'')}$ in bezug auf k, die resp. die Relativgrade $l_1^{h_2''}, \cdots, l_1^{h_e''}$ besitzen, indem man mit den Klassen $c_2, \cdots, c_e$ ebenso operiert wie oben mit c_1. Durch Zusammensetzung der e Körper entsteht ein unverzweigter relativ-Abelscher Körper vom Relativgrad $l_1^{h_1'}$ in bezug auf k.

In entsprechender Weise erhält man unverzweigte, relativ-Abelsche Körper von den Relativgraden $l_2^{h_2'}, \cdots, l_i^{h_i'}$ in bezug auf k. Durch Zusammensetzung aller dieser Körper erhält man einen unverzweigten relativ-Abelschen Körper vom Relativgrad h in bezug auf k, dessen Relativgruppe offenbar seiner Entstehungsweise nach mit der Klassengruppe von k holoedrisch isomorph ist. Wir haben damit folgenden fundamentalen Satz bewiesen:

Satz 9: Es sei k ein beliebiger algebraischer Zahlkörper, dessen Klassenzahl gleich h ist, wenn wir zwei Ideale als äqui-

valent betrachten, deren Quotient als total positive Körperzahl dargestellt werden kann. Es existiert dann in bezug auf k ein unverzweigter relativ-Abelscher Körper vom Relativgrad h, dessen Relativgruppe mit der Gruppe der Idealklassen in k holoedrisch isomorph ist. Dieser Körper heiße der Klassenkörper von k.

§ 12.

Zusammenhang mit der komplexen Multiplikation der elliptischen Funktionen.

Ist der Grundkörper k ein imaginärer quadratischer Körper, so liefert die Theorie der komplexen Multiplikation der elliptischen Funktionen einen Relativkörper $\overline{K}$ in bezug auf k, dessen Relativgruppe ebenfalls mit der Gruppe der Idealklassen von k holoedrisch isomorph ist.*) Es soll im folgenden kurz gezeigt werden, daß dieser Körper $\overline{K}$, den wir als Klassenkörper der komplexen Multiplikation bezeichnen, identisch ist mit dem arithmetisch konstruierten Klassenkörper K in bezug auf k. Die Eigenschaft von $\overline{K}$, auf die wir uns bei dem Identitätsbeweise stützen, ist folgende: Ist $\mathfrak{p}$ ein Primideal aus k, das nicht in der Relativdiskriminante von $\overline{K}$ aufgeht, und ist g der niedrigste Exponent, für den die Äquivalenz:

$$(1) \qquad \mathfrak{p}^g \sim 1$$

in k gilt, so zerfällt $\mathfrak{p}$ in $\overline{K}$ in $\frac{h}{g}$ verschiedene Primfaktoren, wenn mit h die Klassenzahl von k bezeichnet wird.**)

Wir können wieder ohne Beschränkung der Allgemeinheit annehmen, daß die Klassenzahl von k gleich $l^{h'}$ sei, wo l eine Primzahl bedeutet; denn man kann, wie auch bei der Konstruktion des Klassenkörpers ausgeführt wurde, die einzelnen Untergruppen der Klassengruppe von k, deren Grade Potenzen verschiedener Primzahlen sind, für sich betrachten. Es sei also das Klassensystem von k in der Gestalt darstellbar:

$$c_1^{x_1} c_2^{x_2} \cdots c_e^{x_e} \quad (x_i = 1, 2, \cdots, l^{h_i})$$

und dementsprechend das Klassensystem von $k' = (k, \zeta)$ in der Gestalt:

$$c_1^{x_1} c_2^{x_2} \cdots c_e^{x_e}\, d,$$

wo d das System von Klassen bedeutet, deren Relativnormen in k in die Hauptklasse fallen. Es bedeute wie oben K den arithmetischen Klassen-

*) Vgl. H. Weber, Elliptische Funktionen und algebraische Zahlen, Braunschweig 1891, III. Teil.

**) H. Weber, l. c., p. 444 u. 445.

körper und $\overline{K}$ den Klassenkörper der komplexen Multiplikation und es sei:

$$(K, \zeta) = K', \quad (\overline{K}, \zeta) = \overline{K}'.$$

Die Körper K' und $\overline{K}'$ setzen sich dann jeder aus e relativzyklischen Körpern in bezug auf k' zusammen, deren Relativgrade $l^{h_1}, \cdots, l^{h_e}$ sind. Wir nehmen an, daß die Bezeichnung der Klassen c so gewählt sei, daß $h_1 \geqq h_2 \cdots \geqq h_e$ sei. Es gibt dann in K' e unabhängige relativzyklische Körper vom Relativgrad l in bezug auf k', die durch Adjunktion von $\sqrt[l]{\omega_1}, \cdots, \sqrt[l]{\omega_e}$ erzeugt werden mögen, und zwar möge ω_i zu der durch die Kongruenz $x_i \equiv 0\,(l)$ definierten Untergruppe der Klassengruppe von k' gehören. Ebenso enthält $\overline{K}'$ e unabhängige relativzyklische Körper vom Relativgrad l in bezug auf k', die durch Adjunktion von $\sqrt[l]{\overline{\omega}_1}, \cdots, \sqrt[l]{\overline{\omega}_e}$ erzeugt werden mögen, und zwar möge die Bezeichnung so gewählt sein, daß $(\sqrt[l]{\overline{\omega}_i}, k')$ als Unterkörper in einem in $\overline{K}'$ enthaltenen relativzyklischen Körper vom Relativgrad l^{h_i} liegt.

Es möge jetzt $h_1 = h_2 = \cdots = h_{e'}$ sein und $h_{e'+1} < h_{e'}$. Ich fasse dann ein Primideal $\mathfrak{p}$ aus k' ins Auge mit den Eigenschaften:

(1) $$\left(\frac{\omega_1}{\mathfrak{p}}\right)_l = 1, \cdots, \left(\frac{\omega_{e'}}{\mathfrak{p}}\right)_l = 1,$$

wobei die Primideale, die in der Relativdiskriminante von $\overline{K}$ in bezug auf k aufgehen, ausgeschlossen bleiben. Es gilt dann offenbar:

$$\mathfrak{p}^{l^{h_1-1}} \sim 1 \text{ in } k',$$

wo diese Äquivalenz wieder die Bedeutung haben soll, daß $\mathfrak{p}^{l^{h_1-1}}$ in einer Klasse des Systems d liegt. Denn $\mathfrak{p}$ liegt nach (1) in einer Klasse, die der durch die Kongruenzen:

$$x_1 \equiv 0, \cdots, x_{e'} \equiv 0\,(l)$$

definierten Untergruppe der Klassengruppe von k' angehört. Es zerfällt daher $\mathfrak{p}$ in $\overline{K}'$ in mindestens l^{h-h_1+1} verschiedene Primfaktoren; daraus folgt, daß auch

(2) $$\left(\frac{\overline{\omega}_1}{\mathfrak{p}}\right)_l = 1, \cdots, \left(\frac{\overline{\omega}_{e'}}{\mathfrak{p}}\right)_l = 1$$

sein muß. Wenn aber die Gleichungen (1) für alle Primideale aus k' (mit Ausnahme einer endlichen Anzahl) die Gleichungen (2) zur Folge haben, so muß:

$$K_1' = (k', \sqrt[l]{\omega_1}, \cdots, \sqrt[l]{\omega_{e'}}) = (k', \sqrt[l]{\overline{\omega}_1}, \cdots, \sqrt[l]{\overline{\omega}_{e'}})$$

sein.*) Operiert man jetzt mit K_1' so weiter, wie wir eben mit k' operiert haben, so ergibt sich dadurch die Identität von K' mit $\overline{K}'$. Daß dann auch K und $\overline{K}$ identisch sind, ergibt sich wieder daraus, daß

*) Furtwängler, Reziprozitätsgesetz, Satz 26, p. 28.

diese Körper zu derselben Untergruppe der Relativgruppe von K' in bezug auf k gehören. Hiermit ist folgender Satz bewiesen:

Satz 10: *Ist k ein beliebiger imaginärer quadratischer Körper, so ist der auf arithmetischem Wege zu k konstruierte Klassenkörper identisch mit dem zu k gehörigen Klassenkörper aus der Theorie der komplexen Multiplikation der elliptischen Funktionen. Der letzte ist daher unverzweigt in bezug auf k.*

§ 13.

Existenz von unendlich vielen Primidealen in jeder Klasse eines Zahlkörpers.

Auf Grund des Existenzbeweises für den Klassenkörper eines beliebigen Zahlkörpers k kann man den Nachweis führen, daß in jeder Idealklasse von k unendlich viel Primideale liegen. Wir zeigen es zunächst für die Hauptklasse von K. Ist K der Klassenkörper von k und h die Klassenzahl von k, so zerfallen nur solche Primideale aus k in K in h verschiedene Primfaktoren, die in k in der Hauptklasse liegen. Ist $\mathfrak{P}_i$ ein beliebiges Primideal aus K, so gilt:

$$(1)\qquad \sum_{(\mathfrak{P}_i)} \frac{1}{n(\mathfrak{P}_i)^s} = \log \frac{1}{s-1} + f(s) \qquad (s > 1).$$

Daraus folgt, wenn man mit $\mathfrak{p}_i$ ein beliebiges Primideal der Hauptklasse in k bezeichnet:

$$(2)\qquad \sum_{(\mathfrak{p}_i)} \frac{1}{n(\mathfrak{p}_i)^s} \geqq \frac{1}{h} \log \frac{1}{s-1} + f_1(s) \qquad (s > 1).$$

$f(s)$ und $f_1(s)$ bedeuten Funktionen der reellen Veränderlichen s, die für $s = 1$ endlich bleiben. Aus (2) folgt sofort unsere Behauptung.

Daß auch in jeder Klasse von k unendlich viele Primideale liegen, folgt durch einen ganz analogen Beweis, wie ihn Herr H. Weber in seinen Untersuchungen über Zahlengruppen in algebraischen Körpern (Zweite Abhandlung, § 1) gegeben hat.*) Wir können auf Grund der Weberschen Entwickelungen, da alle wesentlichen Voraussetzungen hier erfüllt sind, ohne weiteres folgendes Theorem aussprechen:

Satz 11: *Durchläuft $\mathfrak{p}_i$ alle Primideale einer bestimmten Idealklasse des Körpers k, dessen Klassenzahl gleich h ist, so gilt:*

$$\sum_{(\mathfrak{p}_i)} \frac{1}{n(\mathfrak{p}_i)^s} = \frac{1}{h} \log \frac{1}{s-1} + f(s), \qquad (s > 1)$$

wo $f(s)$ eine Funktion der reellen Veränderlichen s bedeutet, die endlich bleibt, wenn sich s der 1 nähert. In jeder Idealklasse von k liegen daher unendlich viele Primideale.

*) H. Weber, Über Zahlengruppen in algebraischen Körpern. Math. Ann. 49 (1897), p. 83.