

Abelsche Gleichungen in algebraischen Zahlkörpern.

Autor(en): **Fueter, Rud.**

Objektyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **17 (1944-1945)**

PDF erstellt am: **27.09.2024**

Persistenter Link: <https://doi.org/10.5169/seals-16332>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Abelsche Gleichungen in algebraischen Zahlkörpern

(Erste Mitteilung)

Von RUD. FUETER, Zürich

Einleitung

Im folgenden gebe ich eine neue Darstellung des Beweises eines grundlegenden Satzes der Klassenkörpertheorie: Ist K ein zum algebraischen Zahlkörper k Abelscher Körper vom Primzahlrelativgrad l , so existieren in K nur $l^{h(\mathfrak{f})-1}$ Geschlechter, falls $l^{h(\mathfrak{f})}$ die Klassenzahl des Strahles der Normenreste (mod. \mathfrak{f}) in k ist, und \mathfrak{f} ein geeignetes Ideal von k ist. Der Begriff des Geschlechtes, wie er von mir für den Bereich der quadratisch-imaginären Zahlkörper eingeführt wurde¹⁾, und wie er nachher von *Takagi* allgemein verwendet wurde²⁾, scheint mir von besonderer Einfachheit zu sein; benutzt er doch keine Symbole, und stützt er sich doch nur auf allgemeine zahlentheoretische Begriffe. Inhaltlich kann man sogar das Wort Geschlecht weglassen und nur von der Gruppe verschiedener Idealklassen von k sprechen, die *Relativnormen von Klassen von K* sind. Der folgende Beweis benutzt statt des Symboles des Normenrestes, das eigentlich zu andern Fragen gehört, den Begriff des Systems der (relativen) *Grundkomplexe*, der dem Begriff des Systems der (relativen) *Grundeinheiten* entspricht und tief im Wesen der Frage verankert ist. Setzt man die Existenz der beiden Systeme voraus (ihre Beweise sind ganz analog), so ist der zu beweisende Satz über die Geschlechter fast selbstverständlich. Überträgt man ihn etwa auf einen absolut Abelschen Körper vom Primzahlgrade l , so werden die Grundkomplexe zu Idealklassen, und die Theorie ist analog und noch einfacher als im klassischen Fall $l = 2$ des quadratischen Körpers³⁾. Der Beweis, daß die $l^{h(\mathfrak{f})-1}$ -Geschlechter wirklich existieren, wird am einfachsten mit „transzendenten“ Mitteln⁴⁾ geführt. Ich sehe nicht ein, warum diese Methode gegenüber einer „arithmetischen“ Methode weniger dem Wesen der Zahlentheorie entsprechen soll. Schließlich benutzt auch die Berechnung der Klassenzahl oder die Aufstellung der Einheiten transzendente Mittel.

¹⁾ *Rud. Fueter*, Abelsche Gleichungen in quadratisch-imaginären Zahlkörpern. *Math. Ann.* Bd. LXXV (1913), p. 231 u. ff.

²⁾ *T. Takagi*, Über eine Theorie des relativ Abelschen Zahlkörpers. *Journ. of the Coll. of sc. Tokyo Imp. University*, Vol. XLI, art. 9 (1920).

³⁾ Siehe etwa *D. Hilbert*, Die Theorie der algebraischen Zahlkörper. *Ber. D. Math. Ver.* IV. Bd. (1897), p. 286 u. ff.

⁴⁾ *Hilbert*, a. a. O. p. 314.

In weitem Mitteilungen hoffe ich, die Folgerungen aus dem hier bewiesenen Satze zu ziehen. Die erneute Beschäftigung mit der Frage der Theorie der Klassenkörper verdanke ich der anregenden Durcharbeit dieses Gebietes, wie sie Herr Speiser veranlaßt hat, und wozu ihm die *Stiftung für wissenschaftliche Forschung an der Universität Zürich* Mittel zur Verfügung gestellt hat. Ich spreche auch meinerseits der genannten Stiftung hierfür herzlichen Dank aus.

1. Der Strahl der Relativnormen

Es sei K ein zyklischer Körper über k vom Grade l , l eine ungerade Primzahl⁵⁾. Wir setzen voraus, k enthalte die l te Einheitswurzel nicht⁶⁾. Die Relativdiskriminante von K zu k sei \mathfrak{f}^{l-1} . \mathfrak{f} ist dann die l te Potenz eines Ideals \mathfrak{F} von K : $\mathfrak{f} = \mathfrak{F}^l$. Die Gruppe von K/k sei durch S gegeben, wo also $S^l = 1$ die Einheitssubstitution ist. Jede ganze Zahl Ω von K genügt dann einer Kongruenz:

$$\Omega \equiv S\Omega \pmod{\mathfrak{F}} .$$

\mathfrak{F} enthält alle zu l teilerfremden Primideale in erster Potenz, dagegen die in l enthaltenen Primideale, falls solche auftreten, in $(1+v)$ ter Potenz, wo $v \geq 1$ ist. Es sollen in \mathfrak{F} u von einander verschiedene Primideale \mathfrak{Q}_h aufgehen. Wir setzen:

$$\mathfrak{F} = \prod_{h=1}^u \mathfrak{Q}_h^{1+v_h} , \quad v_h \geq 0 ,$$

und v_h ist dann und nur dann $= 0$, wenn \mathfrak{Q}_h zu l teilerfremd ist. \mathfrak{Q}_h^l ist ein Primideal von k . Wir setzen $\mathfrak{Q}_h^l = \mathfrak{I}_h$; also wird:

$$\mathfrak{f} = \prod_{h=1}^u \mathfrak{I}_h^{1+v_h} .$$

Wir bilden mit dem Führer \mathfrak{f} den Strahl $k(\mathfrak{f})$ der Normenreste $(\text{mod. } \mathfrak{f})$ in k . Ist α eine Strahlzahl von $k(\mathfrak{f})$, so muß es eine Zahl A in K geben, so daß

$$\alpha \equiv N(A) \pmod{\mathfrak{f}}$$

wird. Wir wollen von jetzt an Zahlen von K oder k , deren Zähler und Nenner zu \mathfrak{F} teilerfremd gemacht werden können, *erlaubte Zahlen* nennen. α und A sind dann solche erlaubten Zahlen.

⁵⁾ Der Fall $l = 2$ wird ebenso behandelt, nur muß der engere Äquivalenzbegriff eingeführt werden.

⁶⁾ Diese Annahme geschieht nur, um Fallunterschiede zu vermeiden. Tritt die l . Einheitswurzel auf, so ist der Satz über die Grundeinheiten etwas anders. Siehe *Takagi*, a. a. O. p. 39.

1. Satz: Die Faktorgruppe der Gruppe aller Kongruenzklassen (mod. \mathfrak{f}) in k zur Gruppe der in $k(\mathfrak{f})$ liegenden Kongruenzklassen ist vom Typus:

$$(l, l, \dots, l), \quad u \text{ mal } l.$$

Beweis: \mathfrak{Q}_h hat in K dieselbe absolute Norm wie \mathfrak{I}_h in k . Daher ist jede erlaubte Zahl A von K einer Zahl von k (mod. \mathfrak{Q}_h) kongruent:

$$A \equiv SA \equiv \alpha \pmod{\mathfrak{Q}_h}, \quad N(A) \equiv \alpha^l \pmod{\mathfrak{Q}_h}.$$

Ist \mathfrak{I}_h zu (l) teilerfremd, also $v_h = 0$, so gilt auch:

$$N(A) \equiv \alpha^l \pmod{\mathfrak{I}_h}.$$

$k(\mathfrak{f})$ ist (mod. \mathfrak{I}_h) der Strahl der l -ten Potenzreste, dessen Gruppe zur Gruppe aller Kongruenzklassen den Index l hat.

Ist dagegen \mathfrak{I}_h in (l) enthalten, also $v_h \geq 1$, so setze man:

$$A = \alpha + A_h,$$

wo A_h genau durch \mathfrak{Q}_h^r teilbar ist. Man darf r zu l teilerfremd annehmen. Wäre nämlich r durch l teilbar, so gäbe es eine Zahl λ von k , für die A_h/λ erlaubt und einer Zahl α^* von k (mod. \mathfrak{Q}_h) kongruent ist; d. h.:

$$A_h \equiv \alpha^* \lambda \pmod{\mathfrak{Q}_h^{1+r}}, \quad A \equiv \alpha + \alpha^* \lambda \pmod{\mathfrak{Q}_h^{r+1}}.$$

Ist A eine genau durch \mathfrak{Q}_h teilbare Zahl, so ist genau

$$A \equiv SA \pmod{\mathfrak{Q}_h^{1+v_h}}, \quad A^r \equiv SA^r \pmod{\mathfrak{Q}_h^{v_h+r}}, \quad A^{r(1-S)} \equiv 1 \pmod{\mathfrak{Q}_h^{v_h}}.$$

Nun ist A_h/A^r eine erlaubte Zahl. Daher wird:

$$\frac{A_h}{A^r} \equiv S \frac{A_h}{A^r} \pmod{\mathfrak{Q}_h^{1+v_h}}, \quad A_h \equiv SA_h A^{r(1-S)} \equiv SA_h \pmod{\mathfrak{Q}_h^{v_h+r}}.$$

Die Differenten von A_h , die die Ableitung der Gleichung von A_h :

$$A_h^l - \lambda_1 A_h^{l-1} + \dots - \lambda_l = 0$$

ist, ist somit genau durch $\mathfrak{Q}_h^{(l-1)(v_h+r)}$ teilbar:

$$l A_h^{l-1} - (l-1) \lambda_1 A_h^{l-2} + \dots + \lambda_{l-1} \equiv 0 \pmod{\mathfrak{Q}_h^{(v_h+r)(l-1)}}.$$

Da r zu l teilerfremd ist, ist jeder Summand durch eine andere Potenz von \mathfrak{L}_h teilbar. Jeder muß wenigstens durch den Modul teilbar sein. Ist λ_n genau durch $\mathfrak{L}_h^{x_n}$ teilbar, so muß daher, falls (l) genau durch \mathfrak{L}_h^σ teilbar ist:

$$\sigma l + r(l-1) \geq (l-1)(v_h + r) \quad \text{oder} \quad v_h \leq \frac{l\sigma}{l-1}; \quad (\text{a})$$

$$lx_n + (l-1-n)r \geq (l-1)(v_h + r), \quad \text{oder} \quad lx_n \geq (l-1)v_h + r, \\ n = 1, 2, \dots, l-1,$$

sein. Ist $r \geq v_h + 1$, so ist jedes λ_n , $n = 1, 2, \dots, l-1$, durch $\lambda_h^{v_h+1}$ teilbar. Da auch die Norm λ_l dieser Bedingung genügt, so muß:

$$N(A) = N(\alpha + A_h) = \alpha^l + \alpha^{l-1}\lambda_1 + \dots + \lambda_l \equiv \alpha^l \pmod{\mathfrak{L}_h^{v_h+1}}$$

sein.

Gilt für zwei erlaubte Zahlen B_1 und B_2 : $B_1 \equiv B_2 \pmod{\mathfrak{L}_h^{v_h+1}}$, so folgt somit

$$N(B_1) \equiv N(B_2) \pmod{\mathfrak{L}_h^{v_h+1}}.$$

Ist umgekehrt diese Bedingung erfüllt und setzt man $A = B_1/B_2$, so ist A erlaubt und $N(A) \equiv 1 \pmod{\mathfrak{L}_h^{v_h+1}}$. Wir fragen, wie viele $(\text{mod. } \mathfrak{L}_h^{v_h+1})$ inkongruente solche A es gibt und beweisen zunächst, daß $A = 1 + A^*$, wo A^* wenigstens durch $\mathfrak{L}_h^{v_h}$ teilbar ist. $A = \alpha + A_h$ ist eine der oben behandelten Zahlen; A_h erzeugt die Ungleichungen (a), in denen wenigstens einmal das Gleichheitszeichen gilt. Ist v_h durch l teilbar, so kann dies nur für $v_h = \frac{\sigma l}{l-1}$ eintreten. Nun muß:

$$N(A) \equiv 1 \equiv \alpha^l \pmod{\mathfrak{L}_h}$$

sein. Setzt man $\alpha = 1 + \lambda$, so sei λ genau durch \mathfrak{L}_h^s teilbar, wo $s > 0$ sein muß. Wir beweisen, daß stets $r \geq v_h$, $ls \geq v_h$ ist. Wäre $r < v_h$, also $lv_h + 1 > v_h(l-1) + r > rl$, so folgt aus (a):

$$N(A) \equiv 1 \equiv (1 + \lambda)^l + \lambda_l \pmod{\mathfrak{L}_h^{v_h(l-1)+r}}.$$

Daher muß $(1 + \lambda)^l - 1$ genau durch \mathfrak{L}_h^r teilbar sein, was, wie man leicht sieht, bei den gemachten Annahmen unmöglich ist. Also muß $r \geq v_h$ sein. Für $r > v_h$ ist nach dem bereits bewiesenen:

$$N(A) \equiv (1 + \lambda)^l \pmod{\mathfrak{L}_h^{v_h+1}},$$

was sofort zu $s = \frac{\sigma}{l-1}$, $v_h = \frac{l\sigma}{l-1}$, $ls = v_h$ führt. Ist $r = v_h$ (also v_h zu l teilerfremd), so folgt aus (a):

$$N(A) \equiv 1 \equiv (1 + \lambda)^l \pmod{\mathfrak{I}_h^{v_h}},$$

woraus, da $s \neq \frac{\sigma}{l-1}$ ist, $sl \geq v_h$ wird. Die Behauptung ist in allen Fällen bewiesen. Nimmt man jetzt die oben definierte Zahl A und bildet $A^* = A^{1-s}$, so ist $N(A^*) = 1$ und $A^* = 1 + A_h$, wo A_h genau durch $\mathfrak{Q}_h^{v_h}$ teilbar ist. In (a) tritt für zu l teilerfremdes v_h wenigstens einmal das Gleichheitszeichen auf; es ist $x_1 = v_h$, $x_n \geq v_h + 1$, $n = 2, 3, \dots, l-1$ und:

$$N(A^*) = 1 \equiv 1 + \lambda_1 + \lambda_l \pmod{\mathfrak{I}_h^{v_h+1}}.$$

Dies gilt auch, wenn v_h durch l teilbar ist. Jedes weitere zu A^* (mod. $\mathfrak{Q}_h^{v_h+1}$) inkongruente A kann $= 1 + \varrho A_h$ gesetzt werden, wo ϱ in k liegt. Dann ist:

$$N(A) \equiv 1 \equiv 1 + \varrho \lambda_1 + \varrho^l \lambda_l \pmod{\mathfrak{I}_h^{v_h+1}}.$$

Aus beiden Kongruenzen folgt $\varrho \equiv 0$ oder $\varrho^{l-1} \equiv 1 \pmod{\mathfrak{I}_h}$. Letztere hat nur die $l-1$ inkongruenten Lösungen $1, 2, \dots, l-1$. Daher gibt es genau l (mod. $\mathfrak{Q}_h^{v_h+1}$) inkongruente A , für die $N(A) \equiv 1 \pmod{\mathfrak{I}_h^{v_h+1}}$ ist. Der Index der Gruppe der Normenreste zur Gruppe aller Kongruenzklassen ist l . Daraus folgt der Satz.

Aus der Definition folgt ohne weiteres:

2. Satz: Die Normen aller Ideale einer Idealklasse von K zu k liegen in derselben Strahlklasse von $k(\mathfrak{f})$.

2. Die ambigen Komplexe

Im folgenden behandeln wir von allen Abelschen Gruppen nur die zur Primzahl l gehörenden Untergruppen. Unter Gruppe verstehen wir also stets nur diese Untergruppe. Ist \mathfrak{f} eine Idealklasse von k , so gehört sie zu einer Potenz von l . Die Klassenzahl selbst sei l^h . Sind genau e der r Grundeinheiten von k Nichtnormenreste (mod. \mathfrak{f}), $0 \leq e \leq r$, so ist der Index der Gruppe aller Einheiten zur Gruppe aller Einheiten, die Normenreste sind, gleich l^e . Die e genannten Grundeinheiten können nicht Norm einer Zahl von K sein.

Die Hauptklasse von k ergibt in $k(\mathfrak{f})$ l^{u-e} verschiedene Strahlklassen, und die Klassenzahl von $k(\mathfrak{f})$ ist $l^{h(\mathfrak{f})}$, wo $h(\mathfrak{f}) = h + u - e$ ist.

Jedes Ideal i von k wird durch zwei Zahlen von k gegeben $i = (\alpha, \rho)$ und enthält alle Zahlen $\xi\alpha + \eta\rho$, wo ξ, η alle ganzen Zahlen von k durchlaufen. Setzt man statt ξ, η beliebige ganze Zahlen von $K : \mathcal{E}, H$, so erhält man das Ideal i in K . Letzteres liegt in einer Klasse von K , die wir aber stets ebenfalls mit \mathfrak{f} bezeichnen. \mathfrak{f} ist also entweder eine Klasse von k , die nur Ideale von k enthält, oder eine Klasse von K , die wenigstens ein Ideal i von k in K enthält. Enthält die Klasse \mathfrak{R} von K die Ideale $\mathfrak{A}, \mathfrak{B}, \dots$, so bilden auch alle Ideale $S^v\mathfrak{A}, S^v\mathfrak{B}, \dots$ eine Klasse, die man mit $S^v\mathfrak{R} = \mathfrak{R}^{S^v}$ bezeichnet. Sicherlich muß $\mathfrak{f} = S\mathfrak{f}$ sein.

Es sei jetzt \mathfrak{R} eine feste Klasse von K . Wir bilden die Menge aller Klassen $\mathfrak{f}\mathfrak{R}$, wo \mathfrak{f} alle verschiedenen Klassen von k in K durchläuft. Diese Menge heißt der Komplex \mathfrak{C} , der durch \mathfrak{R} erzeugt wird. Erzeugen \mathfrak{R}_1 und \mathfrak{R}_2 die Komplexe \mathfrak{C}_1 und \mathfrak{C}_2 , so heißt der durch $\mathfrak{R}_1\mathfrak{R}_2$ erzeugte Komplex das Produkt $\mathfrak{C}_1\mathfrak{C}_2$ der beiden Komplexe. Der durch die Hauptklasse von K erzeugte Komplex heißt der Einheitskomplex und wird mit 1 bezeichnet. Die Komplexe bilden eine endliche Abelsche Gruppe. Jeder Komplex enthält so viele Klassen, als es in K verschiedene Klassen \mathfrak{f} gibt. Der Komplex, der durch $S^v\mathfrak{R}$ erzeugt wird, wird mit $S^v\mathfrak{C}$ bezeichnet, falls \mathfrak{C} der von \mathfrak{R} erzeugte Komplex ist. Ist $f(S)$ irgend ein Polynom von S mit ganzen rationalen Koeffizienten:

$$f(S) = n_0 + n_1S + n_2S^2 + \dots,$$

so versteht man unter $\mathfrak{C}^{f(S)}$ die $f(S)$ te symbolische Potenz:

$$\mathfrak{C}^{f(S)} = \mathfrak{C}^{n_0} (S\mathfrak{C})^{n_1} (S^2\mathfrak{C})^{n_2} \dots$$

Man sieht, daß stets $\mathfrak{C}^{1+S+\dots+S^{l-1}} = 1$ ist, da $\mathfrak{R}^{1+S+\dots+S^{l-1}} = \mathfrak{f}$ ist.

Ein Komplex heißt ambig, wenn $\mathfrak{C}^{1-S} = 1$ ist. Es ist dann $\mathfrak{C}^{1+S+\dots+S^{l-1}} = \mathfrak{C}^l = 1$. Erzeugt \mathfrak{R} den ambigen Komplex \mathfrak{C} , so muß daher $\mathfrak{R}^{1-S} = \mathfrak{f}$ sein, wo \mathfrak{f} in K genommen ist.

Die erste Aufgabe wird sein, die Zahl der ambigen Komplexe zu bestimmen. Dazu machen wir folgende Hilfsbetrachtungen. Es sei \mathfrak{f} eine von der Hauptklasse in k verschiedene Klasse, die in K Hauptklasse werde. Dann ist das Ideal i der Klasse \mathfrak{f} von k in K Hauptideal $= (N)$, seine Relativnorm zu k also in k (und sogar in $k(\mathfrak{f})$) Hauptideal, oder

$$\mathfrak{f}^{1+S+\dots+S^{l-1}} = \mathfrak{f}^l = 1 ;$$

wegen $i = Si$ muß N^{1-S} eine relative Grundeinheit von K zu k sein. Umgekehrt gebe es genau c relative Grundeinheiten in K , deren Normen

zu k eins, und die nicht die $(1 - S)$ te symbolische Potenz einer Einheit von K sind, dagegen die $(1 - S)$ te symbolische Potenz einer zu \mathfrak{f} teilerfremden ganzen Zahl N . Dann ist (N) Ideal einer Klasse \mathfrak{f} , die in K Hauptideal wird. Daher gibt es genau l^c Klassen \mathfrak{f} in k , die in K Hauptideal werden, und deren l te Potenz in k Hauptklasse ist. Ihre Gruppe ist vom Typus (l, l, \dots, l) (c mal l).

1. *Hilfssatz*: Die l^h Klassen von k bilden in K genau l^{h-c} verschiedene Klassen.

Somit enthält der Einheitskomplex und damit auch jeder Komplex genau l^{h-c} verschiedene Klassen, und es muß $0 \leq c \leq r + 1$ sein.

Es gebe weiter genau d relative Grundeinheiten⁷⁾, deren Norm zu k eins ist, die nicht die $(1 - S)$ te symbolische Potenz einer Einheit sind, und die die $(1 - S)$ te symbolische Potenz einer ganzen Zahl Φ von K sind, die mit \mathfrak{F} einen nicht in k liegenden Teiler gemein habe. Dann gibt es l^d unabhängige Klassen in \mathfrak{R} , für die $\mathfrak{R}^{1-S} = 1$ ist, und die lauter verschiedene Komplexe erzeugen. Dabei ist

$$1 \leq c + d \leq r + 1 .$$

Damit ist für alle Grundeinheiten, deren Norm zu k eins ist, die Möglichkeit erschöpft, und es gibt genau $r + 1 - c - d$ unabhängige Grundeinheiten in k , die Relativnorm einer Einheit von K und somit Normenreste (mod. \mathfrak{f}) sind. Daher werden

$$r - (r + 1 - c - d) = c + d - 1 \text{ unabhängige Grundeinheiten in } k$$

nicht Norm einer Einheit in K sein.

Ist jetzt \mathfrak{R} eine von der Hauptklasse verschiedene ambige Klasse:

$$\mathfrak{R}^{1-S} = 1 ,$$

so ist $\mathfrak{R}^l = \mathfrak{R}^{1+S+\dots+S^{l-1}} = \mathfrak{f}$. Es sei \mathfrak{J} ein zu \mathfrak{F} teilerfremdes Ideal von \mathfrak{R} . Dann ist $\mathfrak{J}^{1-S} = (A)$ Hauptideal in K , also $N(A) = \varepsilon$, wo ε eine Einheit von k ist. Hier haben wir zwei Fälle zu unterscheiden:

a) Die Einheit ε ist Norm einer Einheit E von K . Dann ist $N(AE^{-1}) = 1$, und es muß $AE^{-1} = N^{S-1}$ sein, wo N ganz ist. Also ist:

$$\mathfrak{J}(N) = S(\mathfrak{J}(N)) = i\mathfrak{F}^* ,$$

⁷⁾ Siehe *Hilbert*, a. a. O. p. 272 und 446, u. ff. *Takagi*, a. a. O. p. 35 und 39.

wo i in k liegt und \mathfrak{F}^* nur Primideale von \mathfrak{F} als Faktor enthält, aber keinen in k liegenden Teiler besitzt. Die Anzahl der inäquivalenten Ideale $i \in \mathfrak{F}^*$ ist aber $l^{h-c-d+u}$. Denn nach dem 1. Hilfssatz gibt es l^{h-c} inäquivalente Ideale i in K und alle Primideale \mathfrak{Q}_h bilden l^u Klassen, von denen genau l^d einer der Klassen von k äquivalent sind. Es bleiben somit noch l^{u-d} von den Klassen \mathfrak{f} unabhängige Klassen der \mathfrak{F}^* . \mathfrak{A} muß somit einer dieser $l^{h+u-c-d}$ Klassen angehören.

b) Die Einheit ε ist nicht Norm einer Einheit von K . Sie ist wegen $N(A) = \varepsilon$ sicherlich Normenrest (mod. \mathfrak{f}) in k , liegt also in $k(\mathfrak{f})$. Wir nehmen an, es gebe e^* Grundeinheiten in k , die nicht Norm einer Einheit von K , aber Norm einer (gebrochenen) Zahl von K und somit Normenreste (mod. \mathfrak{f}) sind. Sie müssen von den e Grundeinheiten in k , die es nicht sind, verschieden sein. Es gibt also l^{e+e^*} unabhängige Einheiten in k , die nicht Normen von Einheiten von K sind. Nach obigem ist daher:

$$e + e^* \leq c + d - 1. \quad (1)$$

Nach der Definition von e^* gibt es im Falle b) genau l^{e^*} Klassen \mathfrak{A} , für die $\mathfrak{A}^{1-S} = 1$ ist. Zusammenfassend lautet das Ergebnis:

2. Hilfssatz: Es gibt $l^{h+u-c-d+e^*}$ verschiedene Klassen \mathfrak{A} in K , für die

$$\mathfrak{A}^{1-S} = 1$$

ist.

Jetzt können wir berechnen, wie viele verschiedene Klassen \mathfrak{A} es geben muß, für die

$$\mathfrak{A}^{1-S} = \mathfrak{f}$$

ist. Ihre Zahl ergibt zugleich die Zahl der ambigen Komplexe. Ist nämlich \mathfrak{A}^* eine weitere Klasse, für die $\mathfrak{A}^{*1-S} = \mathfrak{f}$ ist, muß $(\mathfrak{A}^* \mathfrak{A}^{-1})^{1-S} = 1$ sein, und somit \mathfrak{A}^* das Produkt aus \mathfrak{A} und einer der $l^{h+u-c-d+e^*}$ verschiedenen ambigen Klassen sein. Es gibt daher genau $l^{h+u-c-d+e^*}$ verschiedene Klassen \mathfrak{A} , für die $\mathfrak{A}^{1-S} = \mathfrak{f}$ ist. Es sei l^s die Anzahl der verschiedenen Klassen \mathfrak{f} in K , die die $(1-S)$ te symbolische Potenz einer Klasse \mathfrak{A} von K sind. Diese \mathfrak{f} können nicht beliebig sein, sondern wegen Satz 2 und wegen $\mathfrak{f} = S\mathfrak{f}$ muß:

$$\mathfrak{f}^{1+s+\dots+s^{l-1}} = \mathfrak{f}^l = 1$$

die Hauptstrahlklasse von $k(\mathfrak{f})$ sein; d. h. die l te Potenz aller Ideale dieser \mathfrak{f} muß in der Hauptstrahlklasse von $k(\mathfrak{f})$ liegen. Wir sagen dafür kurz \mathfrak{f}^l muß in der Hauptstrahlklasse von $k(\mathfrak{f})$ liegen. l^s ist somit höchstens

die Zahl der verschiedenen Klassen \mathfrak{f} in K , deren l te Potenzen in der Hauptstrahlklasse von $k(\mathfrak{f})$ liegen. Um s abzuschätzen, nehmen wir an, es sei l^{s^*} die Zahl aller Klassen \mathfrak{f} in k , deren l te Potenzen in der Hauptstrahlklasse von $k(\mathfrak{f})$ liegen. Sie bilden eine Gruppe vom Typus (l, l, \dots, l) (l^{s^*} mal). Unter ihnen befinden sich die l^c Klassen von k , die in K in die Hauptklasse fallen. Daher gibt es höchstens l^{s^*-c} verschiedene Klassen \mathfrak{f} in K , die die $(1 - S)$ te symbolische Potenz einer Klasse \mathfrak{R} von K werden können, und es muß:

$$s \leq s^* - c . \quad (2)$$

Die Zahl aller Klassen \mathfrak{R} , deren $(1 - S)$ te symbolische Potenz eine Klasse \mathfrak{f} in K ist, wird deshalb $l^{h+s+u-c-d+e^*}$. Von diesen liegen nach Hilfssatz 1 je l^{h-c} im selben Komplex, der ambig sein muß, und die Zahl der ambigen Komplexe ist $l^a = l^{s+u+e^*-d}$. Wegen (1) und (2) ist: $a \leq s^* + u - e - 1$.

3. Satz: *Ist l^a die Anzahl der verschiedenen ambigen Komplexe, so ist:*

$$a = s + u + e^* - d \leq s^* + u - e - 1 .$$

Dabei ist: l^s die Zahl der Klassen von k in K , die die $(1 - S)$ te symbolische Potenz einer Klasse von K sind; l^{s^} die Zahl der Klassen von k , deren l te Potenz in die Hauptstrahlklasse von $k(\mathfrak{f})$ fallen; u die Zahl der verschiedenen in \mathfrak{f} aufgehenden Primideale; e die Zahl der unabhängigen Grundeinheiten von k , die nicht in $k(\mathfrak{f})$ liegen; e^* die Zahl der unabhängigen Grundeinheiten in k , die nicht Norm einer Einheit, dagegen Norm einer gebrochenen Zahl von K sind;*

3. Die (relativen) Grundkomplexe

Unter einem Polynom $f(S)$ verstehen wir im folgenden stets eine ganze rationale Funktion von S mit ganzen rationalen Koeffizienten.

3. Hilfssatz: *Genügt der Komplex \mathfrak{C} der Bedingung $\mathfrak{C}^{f(S)} = 1$, wo $f(S)$ ein Polynom und $f(1)$ zu l teilerfremd ist, so ist auch $\mathfrak{C} = 1$.*

Es sei ζ die l te Einheitswurzel $e^{\frac{2\pi i}{l}}$ und $k(\zeta)$ der Körper von ζ . $f(\zeta)$ ist eine ganze zu l teilerfremde Zahl von $k(\zeta)$. Ist q ihre Norm, so ist q ganz und nicht durch l teilbar. Ferner gibt es eine ganze Zahl $g(\zeta)$ von $k(\zeta)$, für die

$$f(\zeta) g(\zeta) = q$$

ist. Da ζ der im rationalen irreduzibeln Gleichung $S^{l-1} + \dots + S + 1 = 0$ genügt, so muß:

$$f(S) g(S) \equiv q + h(S) (1 + S + \dots + S^{l-1})$$

identisch in S sein, wo $h(S)$ wieder ein Polynom ist. Somit wird:

$$\mathfrak{C}^{f(S) g(S)} = \mathfrak{C}^q = 1 ,$$

da $\mathfrak{C}^{1+S+\dots+S^{l-1}} = 1$ ist. Nun gehört \mathfrak{C} zu einer Potenz von l , also ist $\mathfrak{C} = 1$.

4. Hilfssatz: Die l te Potenz eines Komplexes ist stets die $(1 - S)$ te symbolische Potenz eines Komplexes.

Man entwickle $1 + S + \dots + S^{l-1}$ nach Potenzen von $S - 1$:

$$1 + S + \dots + S^{l-1} \equiv l + f(S) (S - 1) ,$$

wo $f(S)$ ein Polynom ist. Daher ist für jeden Komplex \mathfrak{C} :

$$\mathfrak{C}^{l+(S-1)f(S)} = 1 , \quad \text{oder} \quad \mathfrak{C}^l = (\mathfrak{C}^{f(S)})^{1-S} .$$

5. Hilfssatz: Ist $f(S)$ ein Polynom und $f(1)$ durch l teilbar, so gibt es zu jedem Komplex \mathfrak{C} einen Komplex \mathfrak{C}^ , so daß:*

$$\mathfrak{C}^{f(S)} = \mathfrak{C}^{*1-S} .$$

Es ist $f(S) = f(1) + (1 - S) g(S)$, wo $g(S)$ ein Polynom und $f(1)$ durch l teilbar ist. Nach Hilfssatz 4 ist $\mathfrak{C}^{f(1)} = \mathfrak{C}^{1-S}$, also:

$$\mathfrak{C}^{f(S)} = \mathfrak{C}^{*1-S} , \quad \text{wo} \quad \mathfrak{C}^* = \mathfrak{C}^l \mathfrak{C}^{g(S)} \quad \text{ist.}$$

6. Hilfssatz: Zu jedem von 1 verschiedenen Komplex \mathfrak{C} gibt es ein und nur eine natürliche Zahl $n + 1$, für die

$$\mathfrak{C}^{(1-S)^{n+1}} = 1 , \quad \mathfrak{C}^{(1-S)^n} \neq 1$$

ist. $\mathfrak{C}^{(1-S)^n}$ ist ein von 1 verschiedener ambiger Komplex.

Wir nennen n den Index von \mathfrak{C} , und $\mathfrak{C}^{(1-S)^n}$ den zu \mathfrak{C} gehörigen ambigen Komplex.

Beweis: Man bilde alle Komplexe:

$$\mathfrak{C}^{(1-S)^m}, \quad m = 0, 1, 2, \dots (\mathfrak{C} \neq 1).$$

Da es nur endlich viele Komplexe gibt, muß es ein kleinstes $m = n + 1 > 0$ geben, für das der Komplexe $\mathfrak{C}^{(1-S)^{n+1}}$ schon unter den vorhergehenden auftritt. Es sei etwa $\mathfrak{C}^{(1-S)^{n+1}} = \mathfrak{C}^{(1-S)^m}$, $m \leq n$. Dann muß:

$$\mathfrak{C}^{f(S) (1-S)^m} = 1$$

sein, wo $f(S) = 1 - (1 - S)^{n-m+1}$ ein Polynom und $f(1) = 1$ ist. Daher ist nach Hilfssatz 3 auch

$$\mathfrak{C}^{(1-S)^m} = 1,$$

was $m = 0$ bedingt, da $n + 1$ die kleinste Zahl vorausgesetzt wurde, die einen frühern Komplex ergibt. Somit ist

$$\mathfrak{C}^{(1-S)^{n+1}} = 1,$$

und $\mathfrak{C}^{(1-S)^n} = \mathfrak{C}^*$ darf nicht eins sein nach Voraussetzung. Zudem ist \mathfrak{C}^* ambig wegen $\mathfrak{C}^{*(1-S)} = 1$.

7. Hilfssatz: Durchläuft $f(S)$ alle möglichen Polynome, und ist $\mathfrak{C} \neq 1$ ein Komplex, so finden sich unter $\mathfrak{C}^{f(S)}$ genau l verschiedene ambige Komplexe.

Ist $\mathfrak{C}^{f(S)}$ ambig und $\neq 1$, so muß:

$$\mathfrak{C}^{f(S) (1-S)} = 1$$

sein. Ist $f(1)$ zu l teilerfremd, so muß nach Hilfssatz 3 auch $\mathfrak{C}^{1-S} = 1$ werden, also \mathfrak{C} ambig sein. Somit ist $\mathfrak{C}^{f(S)} = \mathfrak{C}^{f(1)}$, und da $\mathfrak{C}^l = 1$ sein muß, gibt es die l ambigen Komplexe $1, \mathfrak{C}, \mathfrak{C}^2, \dots, \mathfrak{C}^{l-1}$.

Ist dagegen $f(1)$ durch l teilbar, und ζ wieder die l te Einheitswurzel, so ist entweder $f(\zeta) = 0$ oder $\neq 0$. Im erstern Falle wäre identisch:

$$f(S) \equiv g(S) (1 + S + \dots + S^{l-1}), \quad \mathfrak{C}^{f(S)} = 1 \quad \text{gegen Annahme.}$$

Im zweiten Falle ist $f(\zeta)$ durch eine größte Potenz von $(1 - \zeta)$, etwa $(1 - \zeta)^\nu$, $\nu > 0$, teilbar, so daß $f^*(\zeta) = f(\zeta)/(1 - \zeta)^\nu$ ganz und zu l teilerfremd ist. Dann besteht wieder eine Identität

$$f(S) \equiv (1 - S)^\nu f^*(S) + g(S) (1 + S + \dots + S^{l-1}),$$

wo $g(S)$ ein Polynom und $f^*(1) \not\equiv 0 \pmod{l}$ ist. Daher wird:

$$\mathfrak{C}^{f(S)} = \mathfrak{C}^{f^*(S) (1-S)^\nu}.$$

Da $\mathfrak{C}^{f(S)}$ ambig und $\neq 1$ sein soll, so muß nach Hilfssatz 3 auch $\mathfrak{C}^{(1-S)^\nu}$ ambig sein, d. h.

$$\mathfrak{C}^{(1-S)^\nu+1} = 1$$

werden. $\nu = n$ ist der Index von \mathfrak{C} , also von $f(S)$ unabhängig. Ist \mathfrak{C}^* der zu \mathfrak{C} gehörende ambige Komplex, so ist für jeden ambigen Komplex der Form $\mathfrak{C}^{f(S)}$:

$$\mathfrak{C}^{f(S)} = \mathfrak{C}^{*f^*(1)};$$

es gibt daher nur die l ambigen Komplexe $1, \mathfrak{C}^*, \mathfrak{C}^{*2}, \dots, \mathfrak{C}^{*(l-1)}$.

Wir nennen im folgenden ein Polynom der Form:

$$g(S) \equiv d_0 + d_1(1 - S) + d_2(1 - S)^2 + \dots + d_n(1 - S)^n, \quad 0 \leq d_h \leq l - 1,$$

wo d_h eine der Zahlen $0, 1, 2, \dots, l - 1$ ist, $h = 0, 1, 2, \dots, n$, ein *kanonisches Polynom vom Grade n* .

8. Hilfssatz: Ist \mathfrak{C} ein Komplex und $f(S)$ ein gegebenes Polynom, so gibt es stets ein kanonisches Polynom $g(S)$, für das:

$$\mathfrak{C}^{f(S)} = \mathfrak{C}^{g(S)},$$

wird, wo der Grad von $g(S)$ der Index von \mathfrak{C} , und $f(1) \equiv g(1) \pmod{l}$ ist.

Denn zunächst ist, falls ζ wieder die l te Einheitswurzel ist, $f(\zeta) \equiv d_0 \pmod{1 - \zeta}$, wo $0 \leq d_0 < l$ angenommen werden darf. Gilt:

$$f(\zeta) \equiv d_0 + d_1(1 - \zeta) + \dots + d_r(1 - \zeta)^r \pmod{(1 - \zeta)^{r+1}},$$

$$0 \leq d_h < l, \quad h = 0, 1, \dots, r,$$

so ist $(f(\zeta) - d_0 - \dots - d_r(1 - \zeta)^r) / (1 - \zeta)^{r+1}$ ganz und einer Zahl $d_{r+1} \pmod{1 - \zeta}$, $0 \leq d_{r+1} < l$, kongruent, d. h. auch

$$f(\zeta) \equiv d_0 + \dots + d_r(1 - \zeta)^r + d_{r+1}(1 - \zeta)^{r+1} \pmod{(1 - \zeta)^{r+2}},$$

woraus durch vollständige Induktion folgt, daß:

$$f(\zeta) = g(\zeta) + h(\zeta) (1 - \zeta)^{n+1}, \quad n \text{ der Index von } \mathfrak{C},$$

)

wird, wo $g(S)$ ein kanonisches Polynom, und $h(\zeta)$ ganz ist. Daher muß:

$$f(S) \equiv g(S) + h(S) (1 - S)^{n+1} + k(S) (1 + S + \dots + S^{l-1})$$

identisch in S sein. $h(S)$ und $k(S)$ sind Polynome. Daraus folgt:

$$\mathfrak{C}^{f(S)} = \mathfrak{C}^{g(S)},$$

da ja $\mathfrak{C}^{(1-S)^{n+1}} = 1$ ist. Außerdem ist $f(1) \equiv d_0 \equiv g(1) \pmod{l}$.

9. Hilfssatz: Durchläuft $f(S)$ alle Polynome und ist n der Index von \mathfrak{C} , so stellt $\mathfrak{C}^{f(S)}$ genau l^{n+1} verschiedene Komplexe dar. Man erhält alle diese Komplexe, wenn man für $f(S)$ die l^{n+1} möglichen verschiedenen kanonischen Polynome vom Grade n nimmt.

Wegen Hilfssatz 8 gibt es sicher nicht mehr als l^{n+1} Komplexe. Man hat nur noch zu beweisen, daß aus $\mathfrak{C}^{g_1(S)} = \mathfrak{C}^{g_2(S)}$, wo $g_1(S)$ und $g_2(S)$ kanonisch sind, auch $g_1(S) \equiv g_2(S)$ folgt, oder daß aus $\mathfrak{C}^{g(S)} = 1$, $g(S) \equiv 0$ folgt. Wäre nämlich $g(S)$ nicht identisch null, so gäbe es ein größtes m , so daß: $g(S) \equiv (1 - S)^m g^*(S)$, $m \leq n$, wird, wo $g^*(S)$ wieder kanonisch und $g^*(1) \neq 0$ ist. Nach Hilfssatz 3 ist dann $\mathfrak{C}^{(1-S)^m} = 1$, was unmöglich ist, da $m \leq n$ und n der Index von \mathfrak{C} ist. Also muß $g(S)$ identisch null sein.

Wir führen jetzt folgende wichtige Definition ein:

Definition: Ist l^a die Anzahl der ambigen Komplexe, so heiße ein System von a Komplexen \mathfrak{C}_h mit den Indices n_h , $h = 1, 2, \dots, a$, ein System von (relativen) Grundkomplexen, wenn:

1. die ambigen Komplexe $\mathfrak{A}_h = \mathfrak{C}_h^{(1-S)^{n_h}}$, $h = 1, 2, \dots, a$, eine Basis aller l^a ambigen Komplexe bilden, und wenn:

2. jeder der Komplexe:

$$\mathfrak{C} = \prod_{h=1}^a \mathfrak{C}_h^{f_h(S)}$$

dann und nur dann die $(1 - S)$ te symbolische Potenz eines Komplexes wird, wenn alle Polynome $f_h(S)$ der Bedingung genügen, daß $f_h(1)$, $h = 1, 2, \dots, a$, durch l teilbar ist.

4. Satz: In K existiert ein System von a (relativen) Grundkomplexen.

Zum Beweise nehmen wir zuerst an, daß die Indices aller Komplexe in K null seien. Dann sind alle Komplexe ambig: $\mathfrak{C}^{1-S} = 1$, und bilden wegen $\mathfrak{C}^l = 1$ eine Abelsche Gruppe vom Typus:

$$(l, l, \dots, l), a \text{ mal } l.$$

Diese besitzt eine Basis $\mathfrak{C}_h, h = 1, 2, \dots, a$, die das System von Grundkomplexen bildet. Zugleich sieht man, daß man jeden Komplex durch die \mathfrak{C}_h eindeutig darstellen kann:

$$\mathfrak{C} = \prod_{h=1}^a \mathfrak{C}_h^{x_h}, \quad 0 \leq x_h < l .$$

Sind nicht alle Indices null, so nehmen wir die l^a ambigen Komplexe \mathfrak{A} und stellen sie durch eine Basis $\mathfrak{A}_h, h = 1, 2, \dots, a$, dar:

$$\mathfrak{A} = \prod_{h=1}^a \mathfrak{A}_h^{x_h}, \quad 0 \leq x_h < l .$$

Für jedes dieser $\mathfrak{A} \neq 1$ bestimmen wir den *größten* Exponenten n , so daß:

$$\mathfrak{A} = \mathfrak{C}^{(1-S)^n}, \quad n \geq 0 ,$$

wird, wo \mathfrak{C} ein beliebiger Komplex ist. n muß der Index von \mathfrak{C} sein. Unter allen \mathfrak{A} bestimmen wir dasjenige *mit einem größten Index* n_1 . Wir dürfen es als die Basisgröße \mathfrak{A}_1 wählen, und es sei:

$$\mathfrak{A}_1 = \mathfrak{C}_1^{(1-S)^{n_1}}, \quad n_1 \geq 1 .$$

Die Untergruppe der ambigen Komplexe, die $\mathfrak{A}_1^{x_1}, x_1 = 1, 2, \dots, l - 1$ *nicht* mehr enthält, stellen wir wieder durch die Basis $\mathfrak{A}_2, \mathfrak{A}_3, \dots, \mathfrak{A}_a$ dar, betrachten also nur noch die ambigen Komplexe:

$$\mathfrak{A} = \prod_{h=2}^a \mathfrak{A}_h^{x_h}, \quad 0 \leq x_h < l .$$

Unter diesen besitze:

$$\mathfrak{A}_2 = \mathfrak{C}_2^{(1-S)^{n_2}}, \quad n_1 \geq n_2 ,$$

ein größtes n_2 . So fahren wir fort, und erhalten a -ambige Komplexe \mathfrak{C}_h mit den Indices $n_h, h = 1, 2, \dots, a$, wo

$$n_1 \geq n_2 \geq \dots \geq n_a ;$$

es wird:

$$\mathfrak{A}_h = \mathfrak{C}_h^{(1-S)^{n_h}}, \quad h = 1, 2, \dots, a ,$$

eine Basis aller ambigen Komplexe bilden. Wegen der Konstruktion der \mathfrak{C}_h kann keiner derselben die $(1 - S)$ te symbolische Potenz eines Komplexes sein.

Die \mathfrak{C}_h bilden ein System von Grundkomplexen. Ist nämlich:

$$\prod_{h=1}^a \mathfrak{C}_h^{f_h(S)} = \mathfrak{C}^{1-S},$$

so ersetze man nach Hilfssatz 8 die $f(S)$ durch die kanonischen Polynome:

$$\prod_{h=1}^a \mathfrak{C}_h^{g_h(S)} = \mathfrak{C}^{1-S}.$$

Sind alle $g_h(1) = 0$, so müssen nach Hilfssatz 8 auch alle $f(1)$ durch l teilbar sein, was zu beweisen war. Wären dagegen nicht alle $g_h(1) = 0$, so können wir alle diejenigen Faktoren $\mathfrak{C}_h^{g_h(S)}$, für die $g_h(1) \neq 0$ ist, nach rechts nehmen und mit \mathfrak{C} vereinigen. Es bleibt also nur noch:

$$\mathfrak{C}_\nu^{g_\nu(S)} \mathfrak{C}_\mu^{g_\mu(S)} \dots = \mathfrak{C}^{*1-S}, \quad n_\nu \geq n_\mu \geq \dots, \quad \nu < \mu < \dots,$$

wo jetzt alle $g_\nu(1), g_\mu(1)$ nicht null sind. Wir erheben beide Seiten in die $(1-S)^{n_\nu}$ te symbolische Potenz, so wird:

$$\mathfrak{A}_\nu^{g_\nu(1)} \dots = \mathfrak{C}^{*(1-S)^{n_\nu+1}}, \quad g_\nu(1) \neq 0,$$

wo links ein ambiger Komplex $\neq 1$ steht. Dies ist gegen die Konstruktion der \mathfrak{C}_h . Denn n_ν sollte die größte Zahl sein, so daß

$$\mathfrak{A} = \mathfrak{A}_\nu^{x_\nu} \dots = \mathfrak{C}^{(1-S)^{n_\nu}}$$

wird, während oben ein solches \mathfrak{A} die $(1-S)^{n_\nu+1}$ te symbolische Potenz eines Komplexes wird. Daher müssen alle $g_h(1)$ null sein.

5. Satz: *Ist \mathfrak{C}_h ein System von Grundkomplexen, so läßt sich jeder Komplex \mathfrak{C} in der Form darstellen:*

$$\mathfrak{C} = \prod_{h=1}^a \mathfrak{C}_h^{f_h(S)}.$$

Wir setzen von jetzt an stets voraus, daß das System von Grundkomplexen so abgezählt ist, daß $n_1 \geq n_2 \geq \dots \geq n_a$. Ist nun \mathfrak{C} ambig, so ist er sicher durch die \mathfrak{C}_h darstellbar. Wäre aber \mathfrak{C} eine Komplex mit einem Index $n \geq 1$, der nicht durch die \mathfrak{C}_h darstellbar wäre, so ist $\mathfrak{A} = \mathfrak{C}^{(1-S)^n}$ ambig, also durch die \mathfrak{C}_h darstellbar. Es sei nun $m > 0$ und $\leq n$ die kleinste Zahl, so daß $\mathfrak{C}^{(1-S)^m}$ noch durch die \mathfrak{C}_h darstellbar ist:

$$\mathfrak{C}^{(1-S)^m} = \prod_{h=1}^a \mathfrak{C}_h^{g_h(S)}, \quad g_h(S) \text{ kanonische Polynome, } 0 < m \leq n.$$

Dann müssen nach Definition der Grundkomplexe wegen $m > 0$ alle $g_h(1) = 0$, also $g_h(S)$ durch $(1 - S)$ teilbar sein: $g_h(S) \equiv (1 - S)g_h^*(S)$, wo die $g_h^*(S)$ wieder kanonisch sind. Somit muß:

$$\mathfrak{C}^{(1-S)^{m-1}} \prod_{h=1}^a \mathfrak{C}_h^{-g_h^*(S)}$$

ambig, also wieder durch die \mathfrak{C}_h darstellbar sein. Es wäre also auch $\mathfrak{C}^{(1-S)^{m-1}}$ durch die \mathfrak{C}_h darstellbar, gegen Annahme. Es muß daher \mathfrak{C} selbst durch die \mathfrak{C}_h darstellbar sein.

6. Satz: *Jeder Komplex \mathfrak{C} kann auf eine und nur auf eine Weise durch ein System von Grundkomplexen \mathfrak{C}_h in der Form:*

$$\mathfrak{C} = \prod_{h=1}^a \mathfrak{C}_h^{g_h(S)}, \quad g_h(S) \text{ kanonische Polynome } n_h \text{ ten Grades,}$$

dargestellt werden.

Zum Beweis braucht nur nachgewiesen zu werden, daß aus

$$\prod_{h=1}^a \mathfrak{C}_h^{g_h(S)} = 1, \quad g_h(S) \text{ kanonische Polynome,}$$

stets $g_h(S) \equiv 0, h = 1, 2, \dots, a$, folgt. Gilt erstere Beziehung zwischen den \mathfrak{C}_h , so sind jedenfalls alle $g_h(S)$ durch $(1 - S)$ teilbar, da 1 die $(1 - S)$ te symbolische Potenz einer ambigen Klasse ist.

Sind nicht alle $g_h(S)$ identisch null, so nehmen wir an, daß alle $g_h(S) \not\equiv 0$ durch $(1 - S)^m, m > 0$, teilbar seien, dagegen nicht mehr alle durch $(1 - S)^{m+1}$, d. h. daß in allen $g_h(S)$ der Form

$$d_0 + d_1(1 - S) + \dots + d_n(1 - S)^n$$

die Koeffizienten $d_0 = d_1 = \dots = d_{m-1} = 0$, dagegen wenigstens ein $d_m \neq 0$ ist. Dann ist $g_h(S) = (1 - S)^m g_h^*(S), h = 1, 2, \dots, a$, und für wenigstens ein $h = k$ ist $g_k^*(1) \neq 0$. Die $g_h^*(S)$ sind kanonische Polynome vom Grade $n_h - m$ oder identisch null. Nun ist

$$\mathfrak{A} = \prod_{h=1}^a \mathfrak{C}_h^{(1-S)^{m-1} g_h^*(S)}$$

nach Annahme ein ambiger Komplex, also durch die $\mathfrak{A}_h = \mathfrak{C}_h^{(1-S)^{n_h}}$ als Basis darstellbar:

$$\mathfrak{A} = \prod_{h=1}^a \mathfrak{C}_h^{-x_h(1-S)^{n_h}}, \quad 0 \leq x_h < l.$$

Somit ist auch:

$$\prod_{h=1}^a \mathfrak{C}_h^{g'_h(S)} = 1, \quad \text{wo } g'_h(S) \equiv (1 - S)^{m-1} g_h^*(S) + x_h (1 - S)^{n_h}$$

wieder kanonisch ist.

Es seien alle $g'_h(S)$ durch $(1 - S)^{m'}$, nicht aber durch $(1 - S)^{m'+1}$ teilbar. Dann ist $m' < m$. Denn für $h = k$ ist $g'_k(S)$ genau durch $(1 - S)^{m-1}$ teilbar, da $m \leq n_k$; somit ist $m' \leq m - 1$. Durch Fortsetzung dieses Verfahrens kann eine Relation gefunden werden, deren $g_h(S)$ nicht mehr alle durch $(1 - S)$ teilbar sind. Dies widerspricht aber der Definition der Grundklassen. Somit müssen alle $g_h(S)$ identisch null sein.

Aus dem bewiesenen Satze folgt, daß es genau l^C verschiedene Komplexe gibt, wo

$$C = \sum_{h=1}^a (n_h + 1)$$

ist. Denn jedes $\mathfrak{C}_h^{g'_h(S)}$ ergibt l^{n_h+1} verschiedene Komplexe. Da jeder Komplex genau l^{h-c} -Klassen nach Hilfssatz 1 besitzt, so hat H in der Klassenzahl l^H von K den Wert: $H = h - c + \sum_{h=1}^a (n_h + 1)$.

7. Satz: Ist l^h die Klassenzahl von k , l^H die Klassenzahl von K , so ist:

$$H = h - c + \sum_{h=1}^a (n_h + 1),$$

wo c die Anzahl der Klassen von k ist, die in K Hauptklasse werden, und die n_1, n_2, \dots, n_a die Indices eines Systems von a Grundkomplexen in K sind.

4. Die Klassennormen

Ist \mathfrak{R} irgend eine Klasse von K und \mathfrak{J} ein zu \mathfrak{F} teilerfremdes Ideal von \mathfrak{R} , so werden alle Ideale von \mathfrak{R} , die zu \mathfrak{F} teilerfremd sind, durch $(A)\mathfrak{J}$ gegeben, wo die A erlaubte Zahlen von K sind. Die Normen aller dieser Ideale zu k sind dann durch $(n(A))N(\mathfrak{J})$ gegeben. $\mathfrak{i} = N(\mathfrak{J})$ ist ein festes Ideal von k . Daher liegen alle Ideale $(N(A))\mathfrak{i}$ in einer Strahlklasse \mathfrak{s} von $k(\mathfrak{f})$ (Satz 2). Wir setzen daher:

$$\mathfrak{s} = N(\mathfrak{R}),$$

und nennen die Strahlklasse \mathfrak{s} die *Norm der Klasse* \mathfrak{R} . Wegen

$$N(\mathfrak{J}_1)N(\mathfrak{J}_2) = N(\mathfrak{J}_1\mathfrak{J}_2), \quad N(A_1)N(A_2) = N(A_1A_2)$$

genügt die Norm der Bedingung: $N(\mathfrak{R}_1)N(\mathfrak{R}_2) = N(\mathfrak{R}_1\mathfrak{R}_2)$.

Umgekehrt heißt jede Strahlklasse \mathfrak{s} von $k(\mathfrak{f})$, die unter den Normen der Klassen \mathfrak{R} von K auftritt, *Klassennorm*. Die Aufgabe ist, *die Zahl der Klassennormen zu berechnen*. Man sagt, alle Klassen \mathfrak{R} , deren Norm dieselbe Klasse \mathfrak{s} in $k(\mathfrak{f})$ ergeben, liegen im selben *Geschlechte*. Alle Klassen von K , deren Norm die Hauptstrahlklasse von $k(\mathfrak{f})$ ist, bilden das *Hauptgeschlecht*.

Nach dem Satze 6 kann jede Klasse \mathfrak{R} von K , die etwa den Komplex \mathfrak{C} erzeugt, in der Form:

$$\mathfrak{R} = \mathfrak{f} \prod_{h=1}^a \mathfrak{R}_h^{g_h(S)}, \quad g_h(S) \text{ ein kanonisches Polynom,}$$

dargestellt werden. Dabei werde \mathfrak{C}_h durch \mathfrak{R}_h erzeugt, $h = 1, 2, \dots, a$ und \mathfrak{f} ist eine der l^{h-c} -Klassen von \mathfrak{R} , die Ideale von k enthalten (Hilfsatz 1). Wir nennen die \mathfrak{R}_h , $h = 1, 2, \dots, a$ ein *System von Grundklassen*.

Nun wird:

$$N(\mathfrak{R}) = N(\mathfrak{f}) \prod_{h=1}^a N(\mathfrak{R}_h)^{d_h}, \quad 0 \leq d_h \leq l - 1, \quad h = 1, 2, \dots, a.$$

Sind alle $N(\mathfrak{R}_h)$, $h = 1, 2, \dots, a$ von einander unabhängig, so stellt das Produkt genau l^a Klassen von $k(\mathfrak{f})$ dar. l^a ist daher die größte Zahl, die durch dieses Produkt erhalten werden kann. Es fragt sich, wie viele Klassen \mathfrak{s} von $K(\mathfrak{f})$ die Norm $N(\mathfrak{f})$ darstellen kann. Ist die Klassengruppe von k vom Typus $(l^{h_1}, l^{h_2}, \dots, l^{h_t})$, $h_1 + h_2 + \dots + h_t = h$, und sind \mathfrak{f}_ν , $\nu = 1, 2, \dots, t$, die entsprechenden Basisklassen, so wissen wir, daß diese Klassengruppe als Untergruppe die l^{s^*} verschiedenen Klassen enthält, deren Normen, resp. deren l te Potenzen in die Hauptstrahlklasse von $k(\mathfrak{f})$ fallen. Wegen der Struktur dieser Untergruppe dürfen wir voraussetzen, daß ihre Basis durch $\mathfrak{f}_\nu^{l^{h_\nu-1}}$, $\nu = 1, 2, \dots, s^*$ gegeben werde. In ihr befinden sich auch die l^c -Klassen, die in K Hauptklasse werden. Nun läßt sich jede Norm einer Klasse \mathfrak{f} so darstellen:

$$N(\mathfrak{f}) = \prod_{\nu=1}^t (\mathfrak{f}_\nu^l)^{x_\nu},$$

und wir haben abzuzählen, wie viele Strahlklassen von $k(\mathfrak{f})$ sich in dieser Form befinden. In den ersten s^* Faktoren braucht x_ν nur die Zahlen $0, 1, \dots, l^{h_\nu-1}$ zu durchlaufen, bei den weiteren dagegen alle l^{h_ν} Zahlen, da erst die $l^{h_\nu+1}$ te Potenz von \mathfrak{f}_ν in der Hauptstrahlklasse von $k(\mathfrak{f})$ liegen wird. Somit stellen alle $N(\mathfrak{f})$ genau l^{h-s^*} verschiedene Strahlklassen von $k(\mathfrak{f})$ dar, da ja $\sum_{\nu=1}^t h_\nu = h$ ist.

Die Gesamtzahl der Klassennormen ist also höchstens l^{h-s^*+a} , und zwar wird diese Maximalzahl dann und nur dann erreicht, wenn die Klassen $N(\mathfrak{R}_h)$, $h = 1, 2, \dots, a$, unter sich und mit den $N(\mathfrak{f})$ unabhängig sind. Setzt man für a den Wert nach Satz 3 ein, so erhält man höchstens

$$l^{h-s^*+s+u+e^*-d} \text{ Klassennormen,}$$

und diese Zahl ist wegen (1), (2), $s \leq s^* - c$ kleiner als:

$$l^{h+u-e-1} = l^{h(\mathfrak{f})-1} .$$

1. Hauptsatz: *Die Zahl der verschiedenen Strahlklassen von $k(\mathfrak{f})$, die Klassennormen in K sind, ist:*

$$\leq l^{h-s^*+s+u+e^*-d} \leq l^{h(\mathfrak{f})-1} ,$$

wo das erste Gleichheitszeichen nur eintreten kann, wenn die Normen aller Grundklassen unter sich und mit den Normen aller Klassen \mathfrak{f} in K unabhängig sind; und wo das zweite Gleichheitszeichen nur eintritt, wenn $s = s^* - c$, $e^* = c + d - e - 1$ gilt.

5. Existenz der Geschlechter

In bekannter transzendenter Weise kann man beweisen, daß es wenigstens $l^{h(\mathfrak{f})-1}$ -Klassen von $k(\mathfrak{f})$ geben muß, die Klassennormen sind, daß also wenigstens $l^{h(\mathfrak{f})-1}$ Geschlechter existieren⁸⁾. Wegen des I. Hauptsatzes muß daher:

$$e + e^* = c + d - 1, s = s^* - c$$

sein. Die erste Gleichung sagt aus, daß alle Grundeinheiten von k , die nicht Norm einer Einheit von K sind, entweder Norm einer gebrochenen Zahl von K , oder nicht Normenrest (mod. \mathfrak{f}) sind. Die Zahl der ersten ist genau e^* , die der zweiten e . Somit:

8. Satz: *Jede Einheit von k , die Normenrest (mod. \mathfrak{f}) ist, ist Norm einer Zahl von K .*

Die zweite Gleichung sagt aus, daß jede Klasse \mathfrak{f} in K , deren Norm in der Hauptstrahlklasse von $k(\mathfrak{f})$ liegt, die $(1 - S)$ te symbolische Potenz einer Klasse ist. l^c derselben fallen ja in die Hauptklasse von K .

⁸⁾ Siehe etwa Hilbert, a. a. O. p. 308 u. ff. und vor allem Takagi, a. a. O. p. 18.

9. Satz: *Jede Klasse \mathfrak{f} in K , deren Relativnorm $N(\mathfrak{f})$ in die Hauptstrahlklasse von $k(\mathfrak{f})$ fällt, ist die $(1 - S)$ te symbolische Potenz einer Klasse von K .*

Weiter folgt aus der Existenz, daß auch das erste Gleichheitszeichen im I. Hauptsatz gelten muß. Daher müssen die Klassen von $k(\mathfrak{f})$:

$$N(\mathfrak{R}_1), N(\mathfrak{R}_2), \dots, N(\mathfrak{R}_a)$$

alle unter sich und mit den $N(\mathfrak{f})$ unabhängig sein. Ist nun

$$\mathfrak{R} = \mathfrak{f} \prod_{h=1}^a \mathfrak{R}_h^{g_h(S)}, \quad g_h(S) \text{ ein kanonisches Polynom,}$$

eine beliebige Klasse von K , so ist:

$$\mathfrak{s} = N(\mathfrak{R}) = N(\mathfrak{f}) \prod_{h=1}^a N(\mathfrak{R}_h)^{g_h(1)}, \quad \text{wo } 0 \leq g_h(1) < l \text{ ist.}$$

Soll nun \mathfrak{s} die Hauptstrahlklasse 1 sein, so ist dies wegen der Unabhängigkeit nur möglich, wenn in $k(\mathfrak{f})$:

$$N(\mathfrak{f}) = 1, \quad g_h(1) = 0, \quad h = 1, 2, \dots, a,$$

wird. Dann ist aber nach Satz 9 $\mathfrak{f} = \mathfrak{R}^{*1-S}$, und alle $g_h(S)$ durch $(1 - S)$ teilbar, also \mathfrak{R} selbst die $(1 - S)$ te symbolische Potenz einer Klasse. Alle Klassen \mathfrak{R} , für die $\mathfrak{s} = 1$ ist, bilden das Hauptgeschlecht. Daraus der

2. Hauptsatz: *In K existieren genau $l^{h(\mathfrak{f})-1}$ verschiedene Geschlechter, wo $l^{h(\mathfrak{f})}$ die Klassenzahl von $k(\mathfrak{f})$ ist, und jede Klasse des Hauptgeschlechtes ist die $(1 - S)$ te symbolische Potenz einer Klasse.*

(Eingegangen den 26. Juni 1944.)