Werk

Titel: Zwei Existenztheoreme über algebraische Zahlkörper

Autor: HASSE, H.

Jahr: 1926

PURL: https://resolver.sub.uni-goettingen.de/purl?235181684_0095|log17

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Zwei Existenztheoreme über algebraische Zahlkörper.

Von

Helmut Hasse in Halle a. d. S.

1. In Beantwortung einer von Herrn W. Krull aufgeworfenen Frage[1]) beweise ich folgenden Satz:

Satz 1. *Es sei k ein beliebiger algebraischer Zahlkörper, ferner $\mathfrak{p}_\iota$, $(\iota = 1, \ldots, s)$ irgendwelche s verschiedenen Primideale aus k und zu jedem dieser $\mathfrak{p}_\iota$ ein System $(e_{\iota\varkappa}, f_{\iota\varkappa})$, $(\varkappa = 1, \ldots, r_\iota)$ von r_ι Paaren natürlicher Zahlen gegeben, die nur der einen Bedingung genügen, daß alle s Summen $\sum_{\varkappa=1}^{r_\iota} e_{\iota\varkappa} f_{\iota\varkappa}$ einen und denselben Wert n haben. Dann existieren unendlich viele algebraische Körper K über k, in denen für die $\mathfrak{p}_\iota$ Zerlegungen der Form*

$$\mathfrak{p}_\iota = \prod_{\varkappa=1}^{r_\iota} \mathfrak{P}_{\iota\varkappa}^{e_{\iota\varkappa}}, \qquad \mathfrak{P}_{\iota\varkappa} \text{ vom Relativgrade } f_{\iota\varkappa}, \qquad (\iota = 1, \ldots, s)$$

in Primidealpotenzen bestehen.

Beweis. Es sei $\mathfrak{p}$ eines der gegebenen Primideale, das zur natürlichen Primzahl p gehöre und den Grad f_0 habe, und $(e_\varkappa, f_\varkappa)$ eins der zu $\mathfrak{p}$ gegebenen Zahlenpaare, das Relativordnung und Relativgrad eines Primteiles $\mathfrak{P}_\varkappa$ von $\mathfrak{p}$ in dem zu bestimmenden Oberkörper von k werden soll. Ferner sei $k(\mathfrak{p})$ die zu $\mathfrak{p}$ gehörige Henselsche Erweiterung von k und π eine genau durch $\mathfrak{p}^1$ teilbare Zahl (Primzahl) aus $k(\mathfrak{p})$. Wir konstruieren dann zuerst den durch eine primitive $(p^{f_0 f_\varkappa} - 1)$-te Einheitswurzel $w_\varkappa$ erzeugten zyklischen Körper $k(w_\varkappa, \mathfrak{p})$ vom Grade $f_\varkappa$ über $k(\mathfrak{p})$ und darüber den durch eine Wurzel $\Pi_\varkappa$ der reinen Gleichung $x^{e_\varkappa} - \pi = 0\,(\mathfrak{p})$

[1]) Siehe W. Krull, Algebraische Theorie der zerlegbaren Ringe, Math Ann. 92, S. 207–208. Die dortige Frage bezieht sich auf den Spezialfall: „k rational" des Satzes. Für „k rational, $s = 1$" vgl. auch Ö. Ore, Math. Zeitschr. 20, § 4. Nach brieflicher Mitteilung an den Verf. kann Herr Ore auch den allgemeinen Fall meines Satzes 1 mit den dortigen Hilfsmitteln erledigen.

erzeugten Körper $k(\Pi_\varkappa, w_\varkappa, \mathfrak{p})$ vom Grade $e_\varkappa$ über $k(w_\varkappa, \mathfrak{p})$, also $e_\varkappa \cdot f_\varkappa$ über $k(\mathfrak{p})$. Nach den Elementen der Henselschen Theorie der algebraischen Zahlkörper hat dann der Primteiler $\mathfrak{P}_\varkappa$ von $k(\Pi_\varkappa, w_\varkappa, \mathfrak{p}) = k(\mathfrak{P}_\varkappa)$ den Relativgrad $f_\varkappa$ und die Relativordnung $e_\varkappa$ bezüglich $\mathfrak{p}$. Es sei $g_\varkappa(x) \equiv 0 (\mathfrak{p})$ die in $k(\mathfrak{p})$ irreduzible Grundgleichung mit höchstem Koeffizienten 1 für ein ganzes, primitives Element (etwa $w_\varkappa + \Pi_\varkappa$) von $k(\mathfrak{P}_\varkappa)$. Ist dann $\bar{g}_\varkappa(x)$ irgendein ganzzahliges Polynom $e_\varkappa \cdot f_\varkappa$-ten Grades mit höchstem Koeffizienten 1 in $k(\mathfrak{p})$, für das

$$g_\varkappa(x) \equiv \bar{g}_\varkappa(x) \mod \mathfrak{p}^{N_\varkappa + 1}$$

gilt, so hat auch der Primteiler $\overline{\mathfrak{P}}_\varkappa$ des durch $\bar{g}_\varkappa(x) \equiv 0 (\mathfrak{p})$ definierten algebraischen Körpers $k(\overline{\mathfrak{P}}_\varkappa)$ den Relativgrad $f_\varkappa$ und die Relativordnung $e_\varkappa$, wenn nur $N_\varkappa$ hinreichend groß gewählt ist, nämlich so groß, daß erstens auch $\bar{g}_\varkappa(x)$ in $k(\mathfrak{p})$ irreduzibel ist, (wozu nach K. Hensel, Theorie der algebraischen Zahlen, Leipzig 1908, S. 68 genügt, daß $N_\varkappa$ nicht kleiner als die Ordnungszahl (in $\mathfrak{p}$) der Diskriminante von $g_\varkappa(x)$ ist), und zweitens die kleinstmögliche positive Ordnungszahl $f_\varkappa$ der Relativnorm eines ganzen Elementes von $k(\mathfrak{P}_\varkappa)$ dieselbe Bedeutung auch für $k(\overline{\mathfrak{P}}_\varkappa)$ hat, (wozu $N_\varkappa \geqq f_\varkappa$ genügt, weil dann die Restklassenringe mod $\mathfrak{p}^{f_\varkappa + 1}$ von

$$k(\mathfrak{P}_\varkappa) \cong k(x, \mathfrak{p};\ \mathrm{mod}\ g_\varkappa(x)) \quad \text{und} \quad k(\overline{\mathfrak{P}}_\varkappa) \cong k(x, \mathfrak{p};\ \mathrm{mod}\ \bar{g}_\varkappa(x))$$

isomorph sind, und somit auch in $k(\overline{\mathfrak{P}}_\varkappa)$ kein Element von niedrigerer positiver Relativnorm-Ordnung als $f_\varkappa$ existiert, aber sicher eins mit dieser Minimalordnung der Relativnorm vorhanden ist).

Wir denken uns nun ein System von solchen ganzzahligen Polynomen $g_{\iota\varkappa}(x)$ mit höchstem Koeffizienten 1, wie eben $g_\varkappa(x)$ für alle gegebenen $(e_{\iota\varkappa}, f_{\iota\varkappa})$ in den betreffenden $k(\mathfrak{p}_\iota)$ konstruiert, bilden damit die Produkte

$$(1) \qquad G_\iota(x) = \prod_{\varkappa=1}^{r_\iota} g_{\iota\varkappa}(x) \qquad (\mathfrak{p}_\iota), \qquad (\iota = 1, \ldots, s),$$

die nach Voraussetzung sämtlich denselben Grad n und höchsten Koeffizienten 1 haben, und bestimmen dann ein Polynom $G(x)$ mit ganzen Koeffizienten aus k und höchstem Koeffizienten 1 durch die Kongruenzen

$$(2) \qquad G(x) \equiv G_\iota(x) \bmod g_\iota^{M_\iota + 1}, \qquad (\iota = 1, \ldots, s),$$

in denen über die M_ι weiter unten verfügt wird, und die nach dem über die $G_\iota(x)$ Bemerkten und wegen der Verschiedenheit der $\mathfrak{p}_\iota$ immer erfüllbar sind. Damit $G(x)$ irreduzibel in k wird, fügen wir zu (2) noch eine Kongruenzbedingung

$$G(x) \equiv x^n + \gamma \bmod \mathfrak{q}^2$$

für ein von den $\mathfrak{p}_\iota$ verschiedenes Primideal $\mathfrak{q}$ hinzu, wobei γ irgendeine genau durch $\mathfrak{q}^1$ teilbare Zahl aus k ist, so daß $G(x)$ irreduzibel in $k(\mathfrak{q})$ und um so mehr in k wird.

Der durch $G(x) = 0$ über k definierte Relativkörper K vom Grade n hat dann die verlangten Eigenschaften, wenn die M_ι hinreichend groß gewählt sind. In der Tat zerfällt $G(x)$ gemäß (2) und (1) nach dem Modul $\mathfrak{p}_\iota^{M_\iota+1}$ in die irreduziblen Faktoren $g_{\iota\varkappa}(x)$, $(\varkappa = 1, \ldots, r_\iota)$ und somit auch in $k(\mathfrak{p}_\iota)$ in irreduzible Faktoren $\bar{g}_{\iota\varkappa}(x)$ mit höchstem Koeffizienten 1:

$$G(x) = \prod_{\varkappa=1}^{r_\iota} \bar{g}_{\iota\varkappa}(x) \qquad (\mathfrak{p}_\iota),$$

wenn $M_\iota \geqq$ alle obigen $N_{\iota\varkappa}$, $(\varkappa = 1, \ldots, r_\iota)$ gewählt ist (K. Hensel, l. c.). Dabei ist (l. c. S. 69, Anm.)

$$\bar{g}_{\iota\varkappa}(x) \equiv g_{\iota\varkappa}(x) \bmod \mathfrak{p}_\iota^{M_\iota+1-\varrho_\iota},$$

wobei ϱ_ι eine feste, allein durch die Ordnungszahlen gewisser Resultanten aus den $g_{\iota\varkappa}(x)$, $(\varkappa = 1, \ldots, r_\iota)$ bestimmte, natürliche Zahl. Wählt man also jeweils $M_\iota \geqq$ alle $N_{\iota\varkappa} + \varrho_\iota$, so entsprechen den r_ι irreduziblen Faktoren $\bar{g}_{\iota\varkappa}(x)$, $(\varkappa = 1, \ldots, r_\iota)$ von $G(x)$ in $k(\mathfrak{p}_\iota)$ nach obigem sicher Primteiler $\overline{\mathfrak{P}}_{\iota\varkappa}$ der vorgeschriebenen Relativordnungen und Relativgrade von $\mathfrak{p}_\iota$ in K.

Indem man zu den gegebenen Zerlegungsbedingungen des Satzes noch eine weitere für ein von $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ verschiedenes Primideal $\mathfrak{p}_{s+1}$ hinzufügt, die von der im eben erhaltenen Körper K realisierten abweicht, erhält man einen weiteren, von K verschiedenen Körper der verlangten Art, usf. unendlich viele. Damit ist Satz 1 vollständig bewiesen.

Auf die schwierigere Frage, ob ein entsprechender Satz gilt, wenn man verlangt, daß K relativ-Galoissch zu k ist, und dementsprechend die zu einem $\mathfrak{p}_\iota$ gegebenen $(e_{\iota\varkappa}, f_{\iota\varkappa})$ sämtlich dasselbe Paar (e_ι, f_ι) und dann alle Produkte $e_\iota f_\iota r_\iota = n$ sind, gedenke ich an späterer Stelle einzugehen.

2. Die ähnliche Frage, ob es zu einer irgendwie vorgegebenen, endlichen Gruppe $\mathfrak{G}$ stets einen (bzw. unendlich viele) Galoissche Relativkörper K über k mit der Galoisschen Relativgruppe $\mathfrak{G}$ gibt, gehört bekanntlich zu den schwierigsten, bis heute ungelösten Problemen der höheren Algebra. Ich behandle im folgenden eine damit verwandte Frage, die sich auf den speziellen Fall, daß $\mathfrak{G}$ eine Abelsche Gruppe ist, bezieht. Dann ist zunächst die Existenz unendlich vieler relativ-Abelscher Körper über k mit der Gruppe $\mathfrak{G}$ nicht schwer einzusehen. Sind nämlich $l_1^{\nu_1}, \ldots, l_s^{\nu_s}$ die Invarianten von $\mathfrak{G}$ und $p_1, \ldots, p_s$ irgendein System von verschiedenen natürlichen Primzahlen mit den Kongruenzeigenschaften

$$p_\iota \equiv 1 \bmod l_\iota^{\nu_\iota}, \qquad (\iota = 1, \ldots, s),$$

deren es bekanntlich unendlich viele gibt, so hat der Körper $p_1 \dots p_s$-ten Einheitswurzeln einen Unterkörper K_0, der über dem rationalen Körper R die Gruppe $\mathfrak{G}$ hat.

Da k nur mit endlich vielen der bei jedesmaliger, durchweg neuer Wahl des Systems $p_1, \dots, p_s$ entstehenden Kreiskörper Teilkörper gemeinsam haben kann, können so auch unendlich viele zu k teilerfremde K_0 gefunden werden, und dann ist jedesmal der komponierte Körper $K = (k, K_0)$ relativ-Abelsch zu k mit der Gruppe $\mathfrak{G}$.

Die bei dieser Konstruktion auftretenden, das genannte Problem für den speziellen Grundkörper R lösenden Körper K_0 haben überdies die besondere Eigenschaft, daß die sie zusammensetzenden, den s Invarianten $l_\iota^{\nu_\iota}$ entsprechenden zyklischen Körper je nur eine einzige, zu der betreffenden Invariante prime Primzahl p_ι in ihrer Diskriminante enthalten, und alle diese p_ι verschieden sind. Diese Eigenschaft geht für die obigen $K = (k, K_0)$ relativ zu k verloren, weil ja die p_ι in k im allgemeinen in verschiedene Primidealpotenzen zerfallen. Es gelingt jedoch, indem man den obigen Gedankengang zur Konstruktion von K_0 über R von vorneherein im Grundkörper k durchführt, also unter Vermeidung der nachträglichen Komposition mit k, ein ganz entsprechendes Resultat auch für k zu gewinnen. Wenn ich diesen Beweis im folgenden mitteile, so geschieht es nicht so sehr des Resultates halber, als vielmehr wegen der eigentümlichen Schwierigkeiten, die sich der Durchführung des obigen, einfachen Gedankenganges infolge des Auftretens von Einheiten in k entgegenstellen, und die ich mit einer im Prinzip auf das Reziprozitätsgesetz der $l^\varkappa$-ten Potenzreste hinauslaufenden Schlußweise überwinde. Ich beschränke mich daher auch auf die folgende, eine nicht unbeträchtliche Einschränkung der obigen allgemeinen Behauptung in sich tragende Formulierung des zu beweisenden Satzes:

Satz 2. *Es sei $\mathfrak{G}$ eine endliche Abelsche Gruppe mit den Invarianten $l_1^{\nu_1}, \dots, l_s^{\nu_s}$ und k ein algebraischer Zahlkörper, der die l_1-ten, $\dots$, l_s-ten und für $l_\iota = 2$ sogar die 2^2-ten Einheitswurzeln enthält und dessen Klassenzahl prim zu allen l_ι, also zur Ordnung von $\mathfrak{G}$ ist. Dann existieren unendlich viele relativ-Abelsche Körper K mit der Relativgruppe $\mathfrak{G}$ über k derart, daß in den Relativdiskriminanten der K zusammensetzenden, den s Invarianten $l_\iota^{\nu_\iota}$ entsprechenden s relativ-zyklischen Körper je nur ein einziges, zu der betreffenden Invariante primes Primideal ersten Grades $\mathfrak{p}_\iota$ von k enthalten ist, und alle diese $\mathfrak{p}_\iota$ voneinander verschieden sind.*

Nach allgemeinen Sätzen ist übrigens dann die Relativdiskriminante von K nach k durch

$$\mathfrak{d} = \prod_{\iota=1}^{s} \mathfrak{p}_\iota^{n\left(1-\frac{1}{l_\iota^{\nu_\iota}}\right)}$$

gegeben, wo $n = \prod_{\iota=1}^{s} l_\iota^{\nu_\iota}$ die Ordnung von $\mathfrak{G}$, gleichzeitig den Relativgrad von k bezeichnet.

Dem eigentlichen Beweis schicke ich folgenden, auch an sich wegen seiner einfachen Formulierung bemerkenswerten Hilfssatz voraus:

Hilfssatz. *Es sei k ein beliebiger algebraischer Zahlkörper und K der durch Adjunktion der m-ten Einheitswurzeln zu k entstehende relativ-Abelsche Körper über k. Dann ist K Klassenkörper zu der durch*

$$N(\mathfrak{a}) \equiv 1 \bmod m$$

definierten Idealgruppe in k, einerlei, welche Einheitswurzeln schon in k vorkommen.

Beweis. Nach bekannten Sätzen über Klassenkörper[2]) genügt es, den Beweis für den Fall zu führen, daß m eine Primzahlpotenz l^ϱ ist. Wir verwenden dann das Kriterium T. Satz 32 und stellen zur dazu erforderlichen Herleitung der Zerlegungsgesetze in K genau dieselben Betrachtungen an, die man zur Herleitung der Zerlegungsgesetze im Körper der l^ϱ-ten Einheitswurzeln über dem rationalen Körper verwendet.

Es sei $\mathfrak{p}$ ein zu l primes Primideal ersten Grades aus k und f der kleinste positive Exponent, für den

$$(N(\mathfrak{p}))^f = p^f \equiv 1 \bmod l^\varrho$$

ist, wobei $p = N(\mathfrak{p})$ die $\mathfrak{p}$ zugeordnete rationale Primzahl bezeichnet. Ist dann $\mathfrak{P}$ ein Primteiler von $\mathfrak{p}$ in K, so entsteht der (endliche) Körper der Restklassen mod $\mathfrak{P}$ aus dem Restklassenkörper mod $\mathfrak{p}$ durch Adjunktion einer primitiven l^ϱ-ten Einheitswurzel ζ. Da letzterer mit dem Restklassenkörper mod p identisch ist ($\mathfrak{p}$ hat den Grad 1), läßt sich jede Restklasse $\mathsf{A} \bmod \mathfrak{P}$ in der Form

$$\mathsf{A} \equiv \varphi(\zeta) \bmod \mathfrak{P}$$

als ganze, ganzzahlige rationale Funktion von ζ darstellen, und daraus folgt in bekannter Weise:

$$\mathsf{A}^{p^f} \equiv \varphi(\zeta^{p^f}) \equiv \varphi(\zeta) \equiv \mathsf{A} \bmod \mathfrak{P},$$

so daß jedenfalls $f \geqq f_0$ gilt, wo f_0 der Grad von $\mathfrak{P}$ ist. Andererseits gilt für diesen Grad f_0 nach dem Fermatschen Satz:

$$\zeta^{p^{f_0}-1} \equiv 1 \bmod \mathfrak{P},$$

---

[2]) T. Takagi, Über eine Theorie des relativ-Abelschen Zahlkörpers, Journ. Coll. Science, Tokio 1920, **41**, Art. 9, im folgenden zitiert mit T. Obige Sätze siehe T., Satz 6 sowie den aus der Definition S. 18 oben und Satz 6 sich unmittelbar ergebenden Satz, daß dem Durchschnitt mehrerer Klassengruppen das Kompositum der zugehörigen Klassenkörper als Klassenkörper zugeordnet ist.

und somit $p^{f_0} - 1 \equiv 0 \bmod l^e$, weil $\mathfrak{P}$ prim zu l ist. Nach Bestimmung von f ist also $f_0 \geqq f$, und somit nach obigem $f_0 = f$. Hieraus folgt, daß ein zu l primes Primideal ersten Grades $\mathfrak{p}$ aus k, da ein solches überdies nicht in der Relativdiskriminante von K aufgeht, dann und nur dann in K in verschiedene Primidealfaktoren ersten Grades zerfällt, wenn

$$N(\mathfrak{p}) \equiv 1 \bmod l^e$$

ist. Nach T. Satz 32 ist demnach K Klassenkörper zur Idealgruppe

$$N(\mathfrak{a}) \equiv 1 \bmod l^e, \qquad \text{w. z. b. w.}^{3})$$

Wir wenden uns nunmehr zum Beweis von Satz 2. Auch hier genügt es, wie ohne weitere Ausführungen leicht einzusehen ist, sich auf den Fall, daß $\mathfrak{G}$ zyklisch von der Ordnung l^ν ist, zu beschränken, also zu beweisen:

Satz 2a. *Ist l^ν irgendeine Primzahlpotenz und k ein algebraischer Körper, der die l-ten und im Falle $l = 2$ sogar die 2^2-ten Einheitswurzeln enthält und dessen Klassenzahl prim zu l ist, so existieren unendlich viele relativ-zyklische Körper l^ν-ten Grades über k, in deren Relativdiskriminante nur ein einziges, zu l primes Primideal ersten Grades $\mathfrak{p}$ aus k aufgeht.*

Beweis. Es seien die l^μ-ten Einheitswurzeln die höchsten in k vorkommenden, deren Ordnung eine Potenz von l ist (also $\mu \geqq 1$ und sogar $\mu \geqq 2$ für $l = 2$), und K der durch Adjunktion der $l^{\mu+\nu}$-ten Einheitswurzeln zu k entstehende, relativ-zyklische Körper über k. (K ist auch für $l = 2$ relativ-zyklisch zu k, eben infolge unserer Annahme $\mu \geqq 2$ für $l = 2$, die gerade in Hinsicht hierauf, abweichend gegen $l \neq 2$, gemacht ist.) Bezeichnet allgemein k_ϱ den Körper der l^ϱ-ten Einheitswurzeln (über R), so haben k und $k_{\mu+\nu}$ den Durchschnitt k_μ; so daß K der aus den relativ zu k_μ teilerfremden Körpern k und $k_{\mu+\nu}$ komponierte Körper ist und somit denselben Relativgrad l^ν über k, wie — bekanntlich — $k_{\mu+\nu}$ über k_μ hat. (Hier tritt die Annahme $\mu \geqq 1$ in Erscheinung; für $\mu = 0$ wäre ja der letztere Relativgrad $l^{\nu-1}(l-1)$). Ersetzt man in dieser Betrachtung ν durch $\nu + 1$, so ergibt sich, daß K nicht die primitiven $l^{\mu+\nu+1}$-ten Einheitswurzeln enthält, was für das Folgende wesentlich ist.

Nunmehr seien

$$\zeta, \xi, \varepsilon_1, \ldots, \varepsilon_r \quad \text{bzw.} \quad \mathsf{Z}, \Xi, \mathsf{E}_1, \ldots, \mathsf{E}_s$$

je ein vollständiges System von Grundeinheiten für k bzw. K. Dabei bezeichnen ζ bzw. Z je eine primitive l^μ-te bzw. $l^{\mu+\nu}$-te Einheitswurzel

[3]) Man darf nicht etwa schließen, daß die Idealgruppe $N(\mathfrak{a}) \equiv 1 \bmod m$ eine *reine* Kongruenzklassengruppe *ohne Vorzeichenvorschriften* sei. Schon im Falle $k = R$ bedeutet ja unsere Forderung: $N(a) = |a| \equiv 1 \bmod m$, definiert also eine Kongruenzklassengruppe $\bmod m$ *mit Vorzeichenbedingung*.

(als die höchsten in k bzw. K), deren Ordnung eine Potenz von l ist, ferner ξ bzw. Ξ je eine Einheitswurzel höchster zu l primer Ordnung in k bzw. K und $\varepsilon_1, \ldots, \varepsilon_r$ bzw. $\mathsf{E}_1, \ldots, \mathsf{E}_s$ je ein System von Einheitswurzeln verschiedener Grundeinheiten in k bzw. K von den bekannten Anzahlen r bzw. s, die uns hier nicht näher interessieren. Es bestehen dann Relationen der Form

$$\varepsilon_\iota = \mathsf{Z}^{a_\iota} \Xi^{b_\iota} \prod_{\varkappa=1}^{s} \mathsf{E}_\varkappa^{c_{\iota\varkappa}}, \qquad (\iota = 1, \ldots, r). \tag{3}$$

Wir zeigen zunächst, daß mindestens eine der hierbei auftretenden r-reihigen Determinanten der rechteckigen Matrix $(c_{\iota\varkappa})$, $\begin{pmatrix} \iota = 1, \ldots, r \\ \varkappa = 1, \ldots, s \end{pmatrix}$ prim zu l ist. Wären nämlich diese Determinanten sämtlich durch l teilbar, so wären die r Zeilen von $(c_{\iota\varkappa})$ mod l linear abhängig, und somit bestände eine Relation

$$\varepsilon = \varepsilon_1^{x_1} \ldots \varepsilon_r^{x_r} = \mathsf{Z}^{\sum_{\iota=1}^{r} a_\iota x_\iota} \Xi^{\sum_{\iota=1}^{r} b_\iota x_\iota} \mathsf{E}_0^l,$$

wo nicht alle $x_\iota \equiv 0 \bmod l$, also ε eine Einheit aus k ist, die in k nicht l-te Potenz ist, und wo E_0 eine Einheit aus K bezeichnet. Da Ξ sicher l-te Potenz einer Einheit aus K ist, kann diese Relation unter Einführung einer neuen Einheit E_{00} aus K und mit der Abkürzung $\sum_{\iota=1}^{r} a_\iota x_\iota = a$ in der Form

$$\varepsilon = \mathsf{Z}^a \mathsf{E}_{00}^l$$

geschrieben werden. Wäre hierin $a \not\equiv 0 \bmod l$, so würde folgen, daß

$$K(\sqrt[l]{\varepsilon}) = K(\sqrt[l]{\mathsf{Z}})$$

wäre. Da aber $K(\sqrt[l]{\mathsf{Z}})$ als relativ-zyklischer Körper $l^{\nu+1}$-ten Grades über k nicht mit dem über k aus zwei zyklischen Körpern der Grade l und l^ν komponierten Körper

$$K(\sqrt[l]{\varepsilon}) = \left(k(\sqrt[l]{\varepsilon}),\ K\right)$$

identisch sein kann, müßte $a \equiv 0 \bmod l$ sein, also unsere Relation die Form

$$\varepsilon = \mathsf{E}^l$$

mit einer weiteren Einheit E aus K haben. Daraus folgte aber, daß der Körper $k(\sqrt[l]{\varepsilon})$, der nach dem Gesagten zyklisch vom Grade l über k ist, in K enthalten und somit mit dem einzigen Unterkörper $k(\sqrt[l]{\zeta})$ dieser Art von K identisch wäre, was

$$\varepsilon = \zeta^c \varepsilon_0^l, \qquad (0 < c < l)$$

zur Folge hätte. Eine solche Relation widerspricht aber, wenn man für ε und ε_0 ihre Darstellungen durch die Grundeinheiten einführt, der Unabhängigkeit der letzteren. Also sind die r Zeilen von $(c_{\iota\varkappa}) \bmod l$ linear unabhängig (insbesondere $r \leqq s$, was natürlich auch anderweitig klar), und somit mindestens eine der r-reihigen Determinanten prim zu l, so daß das lineare Kongruenzensystem

$$\sum_{\varkappa=1}^{s} c_{\iota\varkappa} x_\varkappa \equiv -a_\iota \bmod l^{\mu+\nu}, \qquad (\iota = 1, \ldots, r)$$

eine (ganzzahlige) Lösung $(x_1, \ldots, x_s) \bmod l^{\mu+\nu}$ zuläßt. Setzt man dann

$$\mathsf{E}_\varkappa = \mathsf{Z}^{x_\varkappa} \mathsf{H}_\varkappa, \qquad (\varkappa = 1, \ldots, s),$$

so sind auch $\mathsf{H}_1, \ldots, \mathsf{H}_s$ ein mit $\mathsf{E}_1, \ldots, \mathsf{E}_s$ gleichberechtigtes Grundeinheitensystem für K, bei dessen Einführung die Relationen (3) übergehen in

$$\varepsilon_\iota = \Xi^{b_\iota} \prod_{\varkappa=1}^{s} \mathsf{H}_\varkappa^{c_{\iota\varkappa}}, \qquad (\iota = 1, \ldots, r). \tag{4}$$

Es sei jetzt C der Komplex derjenigen Idealklassen $\bmod l^{\mu+\nu+1}$ [4]), für deren Ideale $\mathfrak{A}$

$$N(\mathfrak{A}) \equiv 1 + c\, l^{\mu+\nu} \bmod l^{\mu+\nu+1}, \qquad (0 < c < l)$$

ist. Ferner sei H diejenige Idealgruppe in K, nach der der Körper

$$\mathsf{K} = K\left(\sqrt[l^{\mu+\nu}]{\mathsf{H}_1}, \ldots, \sqrt[l^{\mu+\nu}]{\mathsf{H}_s}\right)$$

Klassenkörper ist. Da die Relativdiskriminante von K nach K nur Primteiler von l enthält, so ist das eine gewisse Gruppe von Idealklassen nach einem Modul $\mathfrak{L}$, der nur Primteiler von l enthält. Wäre nun für alle Ideale $\mathfrak{A}$ aus H

$$N(\mathfrak{A}) \equiv 1 \bmod l^{\mu+\nu+1},$$

so wäre H in derjenigen Idealgruppe enthalten, zu der der Körper $K\sqrt[l]{Z})$ der $l^{\mu+\nu+1}$-ten Einheitswurzeln über K nach unserem Hilfssatz Klassenkörper ist, also nach T. Satz 6 umgekehrt der Körper $K(\sqrt[l]{Z})$ in K enthalten. Das bedeutete aber, daß ersterer Körper mit einem der zyklischen Unterkörper l-ten Grades von K über K identisch wäre, und somit eine Relation bestände:

$$\mathsf{Z} = \mathsf{H}_1^{y_1} \ldots \mathsf{H}_s^{y_s} \mathsf{H}^l \quad (\text{nicht alle } y_\iota \equiv 0 \bmod l),$$

---

[4]) D. h. Nebengruppen in der Gruppe aller zu l primen Ideale in K zu dem Kongruenzstrahl

$$\mathsf{A} \equiv 1 \bmod l^{\mu+\nu+1}.$$

Die Vorzeichenbedingung A total positiv, die eigentlich noch hinzuzufügen wäre, ist wegen $\mu \geqq 1$ bzw. $\mu \geqq 2$ überflüssig, da k und K deswegen total imaginär sind.

wo H eine Einheit in K ist, was genau wie oben der Unabhängigkeit des Grundeinheitensystems $\mathsf{Z}, \Xi, \mathsf{H}_1, \ldots, \mathsf{H}_s$ widerspräche.

Somit haben H und C Ideale gemeinsam, und dann natürlich auch mindestens eine ganze Idealklasse $\bmod l^{\mu+\nu+1}\mathfrak{L}$. In letzterer gibt es dann nach T. Satz 5 unendlich viele Primideale $\mathfrak{P}$ vom ersten Grade.

Es sei jetzt $\mathfrak{P}$ ein beliebiges solches Primideal ersten Grades aus dem Durchschnitt von H und C, $p = N(\mathfrak{P}) \equiv 1 \bmod l^{\mu+\nu}$, aber $\not\equiv 1 \bmod l^{\mu+\nu+1}$ die zugeordnete natürliche Primzahl und $\mathfrak{p} = n(\mathfrak{P})$ die Relativnorm nach k, gleichzeitig das $\mathfrak{P}$ in k zugeordnete Primideal. Wegen der Zugehörigkeit von $\mathfrak{P}$ zu H zerfällt $\mathfrak{P}$ in jedem Relativkörper $K\left(\sqrt[l^{\mu+\nu}]{\mathsf{H}_\varkappa}\right)$, $(\varkappa = 1, \ldots, s)$ in verschiedene Primideale ersten Grades, und daher sind $\mathsf{H}_1, \ldots, \mathsf{H}_s$ sämtlich $l^{\mu+\nu}$-te Potenzreste $\bmod \mathfrak{P}$. In der Tat sind ja wegen des Zerfallens von $\mathfrak{P}$ die Gleichungen

$$x^{l^{\mu+\nu}} - \mathsf{H}_\varkappa = 0\,(\mathfrak{P}), \qquad (\varkappa = 1, \ldots, s)$$

in der Henselschen Erweiterung $K(\mathfrak{P})$ sämtlich in Linearfaktoren zerlegbar, also auch die entsprechenden Kongruenzen $\bmod \mathfrak{P}$. Da Ξ sicher $l^{\mu+\nu}$-ter Potenzrest $\bmod \mathfrak{P}$ ist, sind dann nach (4) auch $\varepsilon_1, \ldots, \varepsilon_\nu$ sämtlich $l^{\mu+\nu}$-te Potenzreste $\bmod \mathfrak{P}$, aber auch $\bmod \mathfrak{p}$, weil die Restklassen $\bmod \mathfrak{P}$ und $\bmod \mathfrak{p}$ dieselben sind (nämlich $0, 1, \ldots, p-1$). Ebenso ist natürlich das obige ξ ein $l^{\mu+\nu}$-ter Potenzrest $\bmod \mathfrak{p}$. Da nun $p-1$ *genau* durch $l^{\mu+\nu}$ teilbar ist, haben $\xi, \varepsilon_1, \ldots, \varepsilon_\nu$ als $l^{\mu+\nu}$-te Potenzreste $\bmod \mathfrak{p}$ zu l prime Exponenten $\bmod \mathfrak{p}$, während ζ als einzige der Grundeinheiten von k natürlich den durch l teilbaren Exponenten l^μ nach dem Modul $\mathfrak{p}$ hat.

Nun betrachten wir die Gruppe der primen Restklassen $\bmod \mathfrak{p}$ in k, die zyklisch von der Ordnung $p-1$ ist. Die Anzahl der durch sie gelieferten Idealklassen (nach dem Strahl $\alpha \equiv 1 \bmod \mathfrak{p}$) ist nach T. Satz 7 durch $\frac{p-1}{(E:E_0)}$ gegeben, wo $(E:E_0)$ den Index der Gruppe E_0 aller Einheiten $\equiv 1 \bmod \mathfrak{p}$ in der Gruppe E aller Einheiten von k bezeichnet. Da nun nach obigem alle Grundeinheiten von k bis auf ζ zu l prime Exponenten $\bmod \mathfrak{p}$ haben, während ζ den Exponenten l^μ hat, ist $(E:E_0) = l^\mu q$, wo q ein zu l primer Teiler von $p-1$ ist, und somit $\frac{p-1}{(E:E_0)}$ genau durch l^ν teilbar. Somit hat die durch Hauptideale gelieferte Untergruppe der Gruppe aller Idealklassen $\bmod \mathfrak{p}$ einen direkten zyklischen Faktor der Ordnung l^ν. Es sei nun $(\gamma_1), \ldots, (\gamma_g)$ ein Repräsentantensystem (von Hauptidealen) für diese Untergruppe, wobei (γ_1) dem direkten Faktor der Ordnung l^ν entsprechen möge. Ferner sei $\mathfrak{a}_1, \ldots, \mathfrak{a}_a$ ein solches zu $\mathfrak{p}$ primes Repräsentantensystem der absoluten Basisklassen von k, daß die frühesten, in der Hauptklasse liegenden Potenzen $\mathfrak{a}_1^{e_1} = (\alpha_1), \ldots, \mathfrak{a}_a^{e_a} = (\alpha_a)$ sogar in der durch $(\gamma_2), \ldots, (\gamma_g)$ erzeugten Idealgruppe $\bmod \mathfrak{p}$ liegen.

Daß eine solche Wahl der $\mathfrak{a}_1, \ldots . \mathfrak{a}_a$ möglich ist, ergibt sich aus unserer Annahme über die Klassenzahl von k, nach der $e_1, \ldots, e_a$ prim zu l sind. Man kann nämlich aus diesem Grunde $\mathfrak{a}_1, \ldots, \mathfrak{a}_a$ als l^ν-te Potenzen eines anderen solchen Repräsentantensystems $\mathfrak{a}_1', \ldots ., \mathfrak{a}_a'$ wählen, und dann liegen ersichtlich $(\alpha_1) = (\alpha_2'^{l^\nu}), \ldots, (\alpha_a) = (\alpha_a'^{l^\nu})$ in der verlangten Idealgruppe mod $\mathfrak{p}$, weil $\gamma_1^{l^\nu} \equiv 1 \bmod \mathfrak{p}$ ist. Durch diese Konstruktion ist nun erreicht, daß die durch (γ_1) erzeugte Idealgruppe mod $\mathfrak{p}$ auch direkter Faktor der Gruppe *aller* Idealklassen mod $\mathfrak{p}$ (nicht nur von deren aus den Hauptidealen bestehenden Untergruppe) ist. Der zum komplementären direkten Faktor gehörige Klassenkörper $\mathfrak{K}$ hat dann die verlangten Eigenschaften. Erstens ist nämlich $\mathfrak{K}$ relativ-zyklisch zu k vom Grade l^ν, weil die zugehörige Klassengruppe den Index l^ν und eine zyklische Faktorgruppe hat. Zweitens kann die Relativdiskriminante von $\mathfrak{K}$ nach k höchstens das zu l prime Primideal ersten Grades $\mathfrak{p}$ enthalten, weil die zugehörige Klassengruppe entweder den Führer $\mathfrak{p}$ oder den Führer 1 hat. Der Führer jener Klassengruppe ist aber wirklich $\mathfrak{p}$, und nicht 1, da die absoluten Idealklassen immer nur „zum l^ν-ten Teil“ zu ihr gehören. Daher enthält die Relativdiskriminante auch sicher $\mathfrak{p}$. (T. S. 96 Mitte und Satz 23.)

Da für $\mathfrak{p}$ nach dem Beweis unendlich viele Primideale zur Auswahl stehen, gibt es somit unendlich viele verschiedene Körper der verlangten Art, womit Satz 2a und somit Satz 2 bewiesen ist.

Daß man die Annahme über die Klassenzahl von k in Satz 2 und 2a entbehren kann, gedenke ich an späterer Stelle im Rahmen einer Verallgemeinerung der beiden in dieser Arbeit untersuchten Problemstellungen darzulegen. Ob man aber mit den Mitteln des hier durchgeführten Beweises auch in den ausgeschlossenen Fällen, wo k nicht die erforderlichen Einheitswurzeln enthält, zum Ziele kommt, vermag ich nicht zu übersehen, halte es jedoch für sehr wahrscheinlich.

Kiel, den 15. Dezember 1924.

(Eingegangen am 16. 12. 1924.)