ZUR KLASSENZAHL IN REINEN ZAHLKÖRPERN VON UNGERADEN PRIMZAHLGRADE.

VON

L. HOLZER

in GRAZ.

In der vorliegenden Arbeit bezeichne:

l eine ungerade natürliche Primzahl.

R sei der natürliche Zahlkörper.

ζ sei eine primitive l-te Einheitswurzel, $k = R(\zeta)$, $\lambda = 1 - \zeta$.

m sei eine ganze rationale Zahl u. zw. sei $m \not\equiv 1 \pmod{l}$

Es sei $\Omega = R(\sqrt[l]{m})$, $\Omega_i = R(\zeta^i \sqrt[l]{m})$ mit $0 \leqq i < l$, so dass $\Omega_0 = \Omega$ wird.

r' sei eine primitive Kongruenzwurzel mod. l in R.

s sei die erzeugende Substitution $\zeta \mid \zeta^{r'}$ der Gruppe k/R, $N_1 = \sum_{i=0}^{l-2} s^i$.

K sei der Körper Ωk, es ist $K > \Omega_i$ für jedes i.

σ sei die erzeugende Substitution $\sqrt[l]{m} \mid \zeta \sqrt[l]{m}$ der Gruppe K/k,

$\Delta = 1 - \sigma$, $N = 1 + \sigma + \sigma^2 + \cdots + \sigma^{l-1}$.

Automorphismen und Homomorphismen mögen in üblicher Art durch symbolische Exponenten bezeichnet werden.

Sind G, H zwei Gruppen, so bezeichne $[G, H]$ den Durchschnitt, $H < G$ heisst: H ist Untergruppe von G, ist in diesem Falle der Index endlich, so heisse er $(G:H)$.

Gruppen von Zahlen und Idealen mögen im allgemeinen wie üblich durch dieselben Buchstaben wie die Repräsentanten der Gruppenelemente bezeichnet werden.

Zahlen in R sollen mit kleinen lateinischen Buchstaben, Zahlen in k mit kleinen griechischen, Zahlen in K mit grossen griechischen Buchstaben bezeich-

net werden. Analog sollen kleine und grosse deutsche Buchstaben Ideale in k, bzw. K i. a. darstellen.

Insbesondere sei $\mathfrak{a}$, $\mathfrak{A}$ die Gruppe aller Ideale $\neq 0$ in k, K, ebenso (α), (A) die Gruppe aller Hauptideale $\neq 0$ in bzw. diesen Körpern. Gruppen von Zahlen und Idealen sollen nach einem — stets aus dem Zusammenhang ersichtlichen — Erklärungsmodul erklärt sein.

(c) sei die Gruppe der Hauptideale $\neq 0$ in R.

H sei die Idealgruppe K/k, f ihr Führer, S_f der Idealstrahl nach dem Führer, $\eta_f \equiv 1 \bmod f$ eine erzeugende Zahl von S_f, also $H = \mathfrak{A}^N S_f$. Weiter sei $H_f = (A)^N S_f$.

k' sei der umfassendste reelle Teilkörper von k, also der Durchschnitt von k mit dem Körper aller reellen Zahlen. Es ist dann $s' = s^{\frac{l-1}{2}}$ die erzeugende Substitution k/k', zugleich die einzige von der identischen verschiedene.

Mit p als natürlicher Primzahl, A als natürlicher Zahl, d als ganzer Zahl aus R soll $p^A \| d$ heissen: $d \equiv 0 \bmod p^A$, $\not\equiv 0 \bmod p^{A+1}$.

h_0 sei die Klassenzahl in k, h die in K, h' die in Ω.

Wesentliche Primteiler einer ganzen Zahl d aus R sollen die natürlichen Primzahlen p heissen mit $p^A \| d$, $A \not\equiv 0 \bmod l$.

Ausdrücklich bemerken wir, dass im Gegensatz zu dem meist angewendeten Gebrauch m zunächst in § 2 nicht notwendig von l-ten Potenzen frei sein. In §§ 3, 4, 5 hingegen gelte für jedes $p^A \| m$: $A \not\equiv 0 \bmod l$.

$S(\alpha)$ bezeichne die Absolutspur einer Zahl α in k.

ε bedeutet Einheiten in k, ε' solche in k'.

Zitieren werden wir vor allem die Berichte des Herrn H. Hasse in den Jahresber. d. Deutschen Math. Vereinigung und zwar Teil I (Bd. 35) und Teil I a (Bd. 36) als Hasse I und Hasse I a nach dem vereinigt gebundenen Sonderabdruck, Teil II (Reziprozitätsgesetze) als Hasse II.

§ 1 gibt die notwendigen Grundlagen.

§ 2 gibt den Beweis folgenden Satzes: Kann der Zahl m mit $m^{l-1} \equiv 1 \bmod l^2$ eine Zahl m' zugeordnet werden mit folgenden Eigenschaften:

(1) Es sei $m' = a^l + l^l b^l$, wo a und b ganze Zahlen aus R sind, weiter $a \not\equiv 0 \bmod l$ ist.

(2) Mit den Abkürzungen $m_1 = a + lb$, $n = \frac{m'}{m_1}$, also n und m_1 ganz gelte $n \not\equiv_{(l)} 1$.

(3) Alle wesentlichen Primteiler von m' sind wesentliche Primteiler von m und umgekehrt; dann ist die Klassenzahl in Ω durch l teilbar (Anm. 1).

Der Satz kann in gewissem Sinne als Verallgemeinerung eines Satzes von FUETER (in der Abhandlung: Über die Gleichung $\alpha^3 + \beta^3 + \gamma^3 = 0$, Heidelberger Sitzungsberichte 1913) betrachtet werden: in $R(\sqrt[3]{a^3 + 27\,b^3})$ mit $a \not\equiv 0 \bmod. 3$, $b \not\equiv 0$ ist die Klassenzahl durch 3 teilbar (Anm. 2).

Betont werde: Satz 3 ist für $l = 3$ spezialisiert, insofern allgemeiner als er bei diesem Werte von l behauptet: Sei $m^2 \equiv 1 \bmod. 9$.

Gibt es eine Zahl $a^3 + 27\,b^3$ mit $a \not\equiv 0 \bmod. 3$, $b \not\equiv 0$, so dass die wesentlichen Primfaktoren von $a^3 + 27\,b^3$ die wesentlichen Primteiler von m sind, und $a^2 - 3\,ab + 9\,b^2$ kein Kubus ist, so ist die Klassenzahl in $R(\sqrt[3]{m})$ durch l teilbar. Andrerseits setzt Fueters Satz nicht voraus, dass $a^2 - 3\,ab + 9\,b^2$ kein Kubus ist.

Von jetzt ab sei m von l-ten Potenzen frei angenommen.

Die Sätze von §§ 3, 4 können wie folgt zusammengefasst werden:

Die Klassengruppe in Ω hat mindestens z durch l teilbare Invarianten, wenn

(I) entweder sich unter den Primfaktoren von m $\frac{l-1}{2} + z$ solche p_i mit $p_i \equiv 1 \bmod. l$ finden (Satz 4)

(II) oder sich unter den Primteilern von m — ausser eventuell l — nur solche vorfinden, die primitive Wurzeln mod. l sind, und zwar für $m^{l-1} \not\equiv 1 \bmod. l^2$ in der Anzahl $\frac{l-1}{2} + z$, hingegen für $m^{l-1} \equiv 1 \bmod. l^2$ in der Anzahl $\frac{l+1}{2} + z$ (Satz 6).

Für $l = 3$ gilt noch:

Satz 5: Hat m insgesamt u natürliche Primteiler $p_i \equiv 1 \bmod. 9$, v natürliche Primteiler $q_i \equiv 1 \bmod. 3$, $\not\equiv 1 \bmod. 9$, so sind mit $v' = \max.(v - 1, 0)$ mindestens $u + v'$ Invarianten der Klassengruppe von Ω durch l teilbar.

Es gelten noch folgende Sätze:

Satz, 6a, 6b: Ist $h_0 \not\equiv 0 \bmod. l$ und ist m entweder natürliche Primzahl, Primitivwurzel mod. l oder aber Produkt zweier solcher natürlicher Primzahlen p_i und ist in letzterem Falle $m^{l-1} \equiv 1 \bmod. l^2$, dagegen $p_i^{l-1} \not\equiv 1 \bmod. l^2$, so ist $h' \not\equiv 0 \bmod. l$.

In § 5 wird gezeigt:

Ist $l \equiv -1 \bmod. 4$, $k_1 = k(\sqrt{-l})$, hat m insgesamt u natürliche Primteiler

p_i mit $p_i^2 \equiv 1 \bmod. l^2$, v natürliche Primteiler q_j mit $q_j^2 \equiv 1 \bmod. l$, aber $q_j^2 \not\equiv 1 \bmod. l^2$ und ist wieder $v' = \max.(v-1, 0)$, so hat die Klassengruppe von $k_1(\sqrt{m}) = \Omega(\sqrt{-l})$ mindestens $u+v'$ durch l teilbare Invarianten.

§ 1.

Fast alle unsere Ergebnisse beruhen auf dem folgenden Satz oder verwandten Sätzen.

Satz 1: Gibt es eine Hauptidealgruppe (β) in k zwischen (α) und H_f, die (c) nicht als Untergruppe hat, so ist die Klassenzahl in Ω durch l teilbar.

Beweis: Sei f' die kleinste natürliche Zahl, die $\equiv 0 \bmod. f$ ist; die Gruppe $(d) = [(\beta), (c)]$ ist nach f' erklärbar (in R), weiter ist $(d) < (c)$, es gibt mithin nach dem Primzahlensatze unzählig viele zu f und l prime natürliche Primzahlen p in R mit folgenden Eigenschaften:

(1) (p) ist nicht Element von (d),

(1) $p \equiv r' \bmod. l$.

Dass beide Bedingungen vereinbar sind, folgt ausser aus dem Primzahlsatz einfach daraus, dass die zu l primen Restklassen mod. l eine Gruppe der Ordnung $l-1$ bilden, während $((c):(d))$ eine Potenz von l ist.

Wegen (2) bleibt (p) in k Primideal.

Da K/R normal ist, ist $H^s = H$, da K/R nichtabelsch ist, so lässt s kein Element einer Nebenklasse von $\mathfrak{A}/H$ invariant, der Durchschnitt jeder Nebenklasse mit (c) fällt leer aus, es folgt $(c) < H$, d. h. (p) steht in H.

Nach dem Zerlegungssatz zerfällt also (p) in K/k:

$$(p) = \prod_{i=1}^{l} \mathfrak{P}_i = \mathfrak{P}_1^N. \tag{3}$$

Da aber (p) nicht in (β), somit nicht in H_f steht, so ist (p) nicht Norm eines Hauptideals, also $\mathfrak{P}_i$ $(1 \leqq i \leqq l)$ kein Hauptideal.

Nun brauchen wir:

Hilfssatz 1: Ist J ein Ideal in K, $J^N = (\gamma)$ ein Hauptideal, das nicht Element von H_f ist, $J^q \sim 1$, $J^u + 1$ für $0 < u < q$, so ist $l \mid q$.

Beweis: Offenbar ist $((\alpha): H_f) = l^v$ mit v ganz rational > 0. Denn aus $v = 0$ folgte $H \geqq (\alpha)$ im Widerspruch dazu, dass K/k nicht unverzweigt ist.

Sei $J^q = (M)$.

Wäre $q \not\equiv 0 \bmod. l$, so gäbe es zwei ganze Zahlen aus R mit

$$qx + ly = 1.$$

Man hätte dann

$$(\gamma) = (\gamma^{qx+ly}) = (M^x \gamma^y)^N,$$

im Widerspruch dazu, dass (γ) nicht in H_f steht.

Wir folgern sofort:

Hilfssatz 2: Jedes $\mathfrak{P}_i$ steht in K in einer Klasse mit durch l teilbarer Ordnung.

Die Zerlegung (3) zeigt, dass die Zerlegungsgruppe jedes $\mathfrak{P}_i$ in Bezug auf R die Ordnung l hat, also zyklisch von dieser Ordnung ist. Der Zerlegungskörper ist einer der Körper Ω_j. Da zu konjugierten Primidealen konjugierte Zerlegungskörper gehören, hat jedes $\mathfrak{P}_i$ einen der Körper Ω_j als Zerlegungskörper k_z, etwa $\mathfrak{P}$ den Körper Ω. Der Trägheitskörper k_t von $\mathfrak{P}$ bezüglich R ist natürlich K, da $\mathfrak{P}$ in K/R nicht kritisch ist. Da beim Übergang k_t/k_z keine Zerlegung, sondern nur eine Graderhöhung des Ideals $\mathfrak{p}'$ in Ω mit $\mathfrak{P}|\mathfrak{p}'$ eintritt, so ist $\mathfrak{P} = \mathfrak{p}'$ schon Primideal in Ω. Nach Hilfssatz 2 ist mithin die Klassenzahl in Ω durch l teilbar, w. z. b. w.

Bemerkung: fast genau so beweist sich der allgemeinere

Satz 1 a: Mit $R \leqq k_1 \leqq k$, weiter (α_1) als Gruppe aller Hauptideale in k_1 gebe es in k eine Zwischengruppe (β) zwischen (α) und H_f, die (α_1) nicht als Untergruppe hat. Dann ist die Klassenzahl in $\Omega^{(1)} = \Omega k_1$ durch l teibar.

Bei Satz 2 wollen wir die Bezeichnungen aus Satz 1 verwenden. Wir haben:

Satz 2: Ist die Faktorgruppe $(c)/(d)$, die vom Typus $(l, l, \ldots, l)$ ist, von der Ordnung l^t, so hat die Klassengruppe von Ω mindestens t durch l teilbare Invarianten.

Beweis: Es seien $c_1, c_2, \ldots, c_t$ ein System von Basisklassen von $(c)/(d)$. Dann gilt:

(1) $c_i^l = 1$ $(1 \leqq i \leqq t)$.

(2) $\prod_{i=1}^{t} c_i^{x_i} = 1$ hat $x_i \equiv 0 \bmod. l$ für jedes i zur Folge.

Es seien weiter $p^{(i)} \equiv r'$ mod. l natürliche nicht kritische Primzahlen mit Primteilern in bezw. c_i. Ihre Existenz — und zwar für jedes i in unzähliger Menge — folgt aus dem Primzahlensatze genau wie bei Satz 1. $\mathfrak{P}^{(i)} | p^{(i)}$ sei der Primteiler ersten Grades, als Ideal in Ω betrachtet, in K ist $\mathfrak{P}^{(i)}$ vom Grade $l - 1$.

Eine Beziehung

$$\prod_{i=1}^{t} \mathfrak{P}^{(i)u_i} \underset{(l)}{\sim} 1 \text{ in } \Omega$$

hätte zunächst eine Beziehung genau gleicher Art in K, und daher auch eine solche

$$\prod_{i=1}^{t} \mathfrak{P}^{(i)t'u_i} \sim 1 \text{ in } K$$

zur Folge, wo $t' \not\equiv 0$ mod. l ist.

Normenbildung in K/k ergäbe, dass

$$\prod_{i=1}^{t} (p^{(i)})^{t'u_i}$$

Element von H_f ist. Es wäre auch

$$\prod_{i=1}^{t} (p^{(i)})^{u_i}$$

Element von H_f, also von (d). Es folgte

$$\prod_{i=1}^{t} c_i^{u_i} = 1,$$

also jedes $u_i \equiv 0$ mod. l.

Ist also C_i die l-Klasse von $\mathfrak{P}^{(i)}$ in Ω, so ist eine Gleichung

$$\prod_{i=1}^{t} C_i^{x_i} = 1$$

nur so möglich, dass alle $x_i \equiv 0$ mod. l sind, d. h. die Klassengruppe in Ω hat mindestens t durch l teilbare Invarianten.

Auch hier ergibt sich ganz analog mit den Bezeichnungen von Satz 1 a, ausserdem

$$[(\beta), (\alpha_1)] = (\delta)$$

folgender Satz:

Satz 2 a: Hat die Faktorgruppe $(\alpha_1)/(\delta)$ die Ordnung l^t, so hat die Klassengruppe von $\Omega^{(1)}$ mindestens t durch l teilbare Invarianten.

§ 2.

Wir kommen zu Satz 3. Sei $m^{l-1} \equiv 1 \bmod. l^2$.

Der Zahl m lasse sich eine ganze Zahl m' aus R zuordnen, so dass

(1) $m' = a^l + l^l b^l$ mit a, b ganz aus R, $a \not\equiv 0 \bmod. l$.

(2) Mit $m_1 = a + lb$, $n = \dfrac{m'}{m_1}$, also m_1, n ganz, gelte $n \underset{(l)}{\not\equiv} 1$.

(3) Alle wesentlichen Primteiler von m' sind wesentliche Primteiler von m und umgekehrt.

Dann ist die Klassenzahl in Ω durch l teilbar.

Beweis: Ohne Einschränkung der Allgemeinheit kann $(a, b) = 1$ angenommen werden. Mit $\mu = a + lb\zeta$, wo offenbar $\mu \mid n$ gilt, ist $(\lambda, \mu) = (1)$.

Wir verwenden Hilfssatz 4:

Die Zahlengruppe (β) der Zahlen mit

$$\left(\frac{\beta}{m_1}\right) = \left(\frac{\beta}{\mu}\right)$$

enthält alle Erzeugenden von Elementen aus H_f, insbesondere alle Einheiten, es ist also $(\beta) \geqq H_f$.

Beweis von Hilfssatz 4:

In k gelte die Idealzerlegung mit den $\mathfrak{p}_i$ und $\mathfrak{q}_j$ als Primidealen

$$(m_1) = \mathfrak{p}_1^{a_1} \ldots \mathfrak{p}_s^{a_s} j^l, \quad (\mu) = \mathfrak{q}_1^{b_1} \ldots \mathfrak{q}_{s'}^{b_{s'}} j'^l,$$

wo alle a_i und $b_j \not\equiv 0 \bmod. l$ seien, j und j' sind nicht notwendig Primideale. Dann ist mindestens ein $\mathfrak{q}_j$ vorhanden oder $s' \geqq 1$. Denn $(\mu) \underset{(l)}{=} (1)$ hätte wegen $n = \mu^{N_1}$ zur Folge:

$$n \underset{(l)}{=} 1$$

im Widerspruch zur Voraussetzung.

Kritisch in K/k sind genau

$$\mathfrak{p}_1, \ldots, \mathfrak{p}_s; \ \mathfrak{q}_1, \ldots, \mathfrak{q}_{s'}.$$

Hier tritt die Voraussetzung ein, dass alle wesentlichen Primteiler von m' wesentliche Primteiler von m sind und umgekehrt.

Sei $\mathfrak{r}$ irgend ein $\mathfrak{p}_i$ oder $\mathfrak{q}_j$.

Für $\mathfrak{r}$ ist dann Normenrest und l-ter Potenzrest gleichbedeutend, da $\mathfrak{r} \neq (\lambda)$ ist. Es ist weiter, für alle η_f: $\eta_f \equiv 1 \bmod \mathfrak{r}$ wegen $\mathfrak{r} | f$. Es folgt für jedes zu f prime $A: \left(\frac{A^N \eta_f}{\mathfrak{r}}\right) = 1$, also

$$\left(\frac{A^N \eta_f}{m_1}\right) = \left(\frac{A^N \eta_f}{\mu}\right) = 1. \tag{4}$$

Für Einheiten ε von k ist

$$\left(\frac{m_1 \mu^{-1}}{\varepsilon}\right) = 1.$$

Da aber $m_1 \mu^{-1} \equiv 1 \bmod l\lambda$, also $m_1 \mu^{-1}$ l-primär ist, so folgt (nach Hasse II)

$$1 = \left(\frac{\varepsilon}{m_1 \mu^{-1}}\right) \text{ oder } \left(\frac{\varepsilon}{m_1}\right) = \left(\frac{\varepsilon}{\mu}\right). \tag{5}$$

Aus (4) und (5) folgt:

Hilfssatz 5: Die Zahlengruppe β mit $\left(\frac{\beta}{m_1}\right) = \left(\frac{\beta}{\mu}\right)$ erfüllt $\beta > \varepsilon$, $(\beta) > H_f$, weiter $((\alpha):(\beta)) = l$.

Wir brauchen noch

Hilfssatz 6: Unter den $\mathfrak{q}_i$ gibt es keine absolutkonjugierten Primideale.

Beweis: Wäre mit ganzem rationalem u $\mathfrak{q}_i^{s^u} = \mathfrak{q}_j$, so folgte

$$\mathfrak{q}_j | \mu^{s^u}.$$

Da auch $\mathfrak{q}_j | \mu$ gilt, so bliebe $\mathfrak{q}_j | \mu - \mu^{s^u} = b\, l (\zeta - \zeta^t)$, wo $t \equiv r'^u \bmod l$ ist.

Ist $r'^u \not\equiv 1 \bmod l$, so wäre $l(\zeta - \zeta^t) \not\equiv 0 \bmod \mathfrak{q}_j$, also folgte $\mathfrak{q}_j | b$ und damit auch $\mathfrak{q}_j | a$ im Widerspruch zu $(a, b) = 1$.

Es bleibt $r'^u \equiv 1 \bmod l$, d. h. $u \equiv 0 \bmod (l-1)$, also $s^u = 1$, d. h. $\mathfrak{q}_i = \mathfrak{q}_j$.

Nun folgt Hilfssatz 6 a: (β) umfasst nicht alle rationalen Ideale.

Beweis: Aus $m' \equiv 0 \bmod \mathfrak{q}_j$, $m_1 \not\equiv 0 \bmod \mathfrak{q}_j$ folgt für die natürliche Primzahl $q_j \equiv 0 \bmod \mathfrak{q}_j$ sofort $a^l \equiv -(lb)^l$, $a \not\equiv -lb \bmod q_j$, d. h. $q_j \equiv 1 \bmod l$. $\mathfrak{q}_j$ ist also Primideal ersten Grades, die Restklassenkörper mod. q_j in R und mod. $\mathfrak{q}_j$ in k sind 1-isomorph.

Ist c Nichtrest mod. q_1, Rest mod. q_j für $j > 1$, was nach Hilfssatz 6 wegen $q_j \neq q_1$ erfüllbar ist, so bleibt

$$\left(\frac{c}{q_1}\right) \neq 1, \left(\frac{c}{q_2}\right) = \cdots = \left(\frac{c}{q_{s'}}\right) = 1,$$

mithin

$$\left(\frac{c}{\mu}\right) \neq 1,$$

hingegen trivialerweise

$$\left(\frac{c}{m_1}\right) = 1.$$

Es ist

$$\left(\frac{c}{m_1}\right) \neq \left(\frac{c}{\mu}\right),$$

(c ist kein Element von β).

Aus Hilfssatz 5 und 7 folgt im Verein mit Satz 1 der Satz 3.

§ 3.

Von jetzt ab sei m als von l-ten Potenzen frei angenommen.

Mit Hilfe der Kummer-Takagischen Formel (Hasse II, § 21, 3, S. 169) beweisen wir den

Satz 4: Erfüllen $\frac{l-1}{2} + z\,(z > 0)$ natürliche Primzahlen $p_i \mid m$ die Kongruenz $p_i \equiv 1 \bmod. l$, so sind mindestens z Invarianten der Klassengruppe von Ω durch l teilbar.

Beweis: Wir setzen $\frac{l-1}{2} + z = u$.

Sei $\mathfrak{p}_i (0 < i \leqq u)$ ein (nicht näher bestimmter) Primteiler von p_i in k. Dann ist $\mathfrak{p}_i$ vom ersten Grad. Mit r_{-i} als kleinstem positivem ganzem Rest von $r'^{-i} \bmod. l$ ist dann mit der Abkürzung

$$f(s) = \sum_{j=0}^{l-2} r_{-j} s^j, \text{ also } f(r') \equiv -1 \bmod. l \tag{6}$$

das Ideal $\mathfrak{p}_i^{f(s)} = (\vartheta_i)$ ein Hauptideal in k. (ϑ_i) kann durch eine Lagrangesche Wurzelzahl erzeugt werden. (vgl. Hilbert, Zahlbericht § 108, Satz 135).

Es werde $\vartheta_i^{l-1} = \pi_i$ gesetzt.

Es seien weiter

$$\varkappa_1, \varkappa_2, \ldots, \varkappa_{l-1}$$

die Takagischen Einseinheiten. Für ein beliebiges $\alpha \equiv 1 \bmod. \lambda$ aus k sind dann durch

$$\alpha \equiv \prod_{j=1}^{l-1} \varkappa_j^{t_j(\alpha)} \bmod. \lambda l$$

die ganzen rationalen Exponenten $t_j(\alpha) \bmod. l$ eindeutig bestimmt.

Nach erwähnter Formel gilt für jede Einheit $\varepsilon \equiv 1 \bmod. \lambda$

$$\left(\frac{\varepsilon}{\pi_i}\right) = \zeta^{\sum_{j=1}^{l-1} j\, t_j(\pi_i) t_{l-j}(\varepsilon)}$$

Das gibt für ein beliebiges $\delta = \prod_{i=1}^{u} \pi_i^{a_i}$

$$\left(\frac{\varepsilon}{\delta}\right) = \zeta^{\sum_{i,j=1}^{l-1} a_i j\, t_j(\pi_i) t_{l-j}(\varepsilon)}$$

Nun können wir in k jede $(l-1)$-te Potenz einer Einheit aus Einheiten $\varepsilon_1 = \zeta$, $\varepsilon_i = \eta_i^{l-1}$, wo die η_i für $1 < i \leqq \frac{l-1}{2}$ Grundeinheiten in k sind, multiplikativ aufbauen.

Dabei ist jedes $\varepsilon_k \equiv 1 \bmod. \lambda \left(1 \leqq k \leqq \frac{l-1}{2}\right)$.

Es hat dann das System der $\frac{l-1}{2}$ Kongruenzen in $a_1, \ldots, a_u$

$$\sum_{i=1}^{u} a_i \sum_{j=1}^{l-1} j\, t_j(\pi_i)\, t_{l-j}(\varepsilon_k) \equiv 0 \bmod. l, \tag{7}$$

wo $k = 1, 2, \ldots, \frac{l-1}{2}$ sei, $u - \varrho(\mathfrak{M})$ linear unabhängige Lösungen, wenn $\mathfrak{M}$ die Matrix aus $\frac{l-1}{2}$ Zeilen und u Spalten

$$\mathfrak{M} = (j\, t_j(\pi_i)\, t_{l-j}(\varepsilon_k))$$

und $\varrho(\mathfrak{M})$ ihr Rang mod. l ist. Nun ist offenbar

$$\varrho(\mathfrak{M}) \leqq \min. \left(\frac{l-1}{2}, u\right) = \frac{l-1}{2},$$

d. h

$$u - \varrho(\mathfrak{M}) \geqq \varepsilon.$$

Das System (7) hat also sicher z (vielleicht mehr) linear unabhängige Lösungen mod. l:

$$(a_{11}, \ldots, a_{u1}), \ldots, (a_{1z}, \ldots, a_{uz}). \tag{8}$$

Das System (8) ergeben mit

$$\delta_{ij} = \prod_{i=1}^{u} \pi_i^{a_{ij}}$$

insgesamt z l-unabhängige Zahlen $\delta_1, \ldots, \delta_z$, so dass

$$\left(\frac{\varepsilon^{l-1}}{\delta_j}\right) = 1$$

für jede Einheit in k gilt. Wegen $\left(\frac{\varepsilon}{\delta_j}\right) = \left(\frac{\varepsilon^{l-1}}{\delta_j}\right)^{-1}$ gilt daher für jedes ε:

$$\left(\frac{\varepsilon}{\delta_j}\right) = 1. \tag{9}$$

Wir haben nun:

Hilfssatz 7: Es ergeben sich mithin z Zahlengruppen β_j definiert durch

$$\left(\frac{\beta_j}{\delta_j}\right) = 1,$$

so dass $((\alpha):(\beta_j)) = l$ und $\beta_j > \varepsilon$ ist.

Wir haben nun:

Hilfssatz 8: $(\beta_j) \geqq H_f$.

Beweis: Für jedes $A^N \eta_f$ gilt $\left(\frac{A^N \eta_f}{\delta_j}\right) = 1$, da für die Primfaktoren von δ_j als in K/k kritische, zu λ teilerfremde Primideale Normenrest und l-ter Potenzrest zusammenfallen. Also bleibt $A^N \eta_f \leqq \beta_j$, d. h. $H_f \leqq \beta_j$.

Hilfssatz 9: $[(\beta_1), \ldots, (\beta_z)] \geqq H_f$.

Der Beweis folgt unmittelbar aus Hilfssatz 8.

Hilfssatz 10: Für jedes ganze rationale c, das zu l prim ist, gilt

$$\left(\frac{c}{\pi_i}\right) = \left(\frac{c}{\mathfrak{p}_i}\right)^{-1}.$$

Beweis: Es ist $\left(\frac{c}{\pi_i}\right) = \left(\frac{c}{\mathfrak{p}_i}\right)^{f(s)}$. Ist nun $\left(\frac{c}{\mathfrak{p}_i}\right) = \zeta^A$, so folgt

$$\left(\frac{c}{\pi_i}\right) = \zeta^{Af(r')} = \zeta^{-A},$$

letzteres wegen (6).

Hifssatz 11: Mit $[(c), (\beta_1), \ldots, (\beta_z)] = (d)$ ist $(c)/(d)$ vom Typus $(l, l, \ldots, l)$ und der Ordnung l^z.

Beweis: Es sei in R die Zahl c_i Rest mod. p_j für $j \neq i$, dagegen Nichtrest mod. p_i. Dann werde $\mathfrak{p}_i$ speziell so gewählt, dass

$$\left(\frac{c_i}{\mathfrak{p}_i}\right) = \zeta^{-1}, \quad \left(\frac{c_i}{\mathfrak{p}_j}\right) = 1 \text{ für } i \neq j.$$

Also ist nach Hilfssatz 10:

$$\left(\frac{c_i}{\pi_i}\right) = \zeta, \quad \left(\frac{c_i}{\pi_j}\right) = 1 \text{ für } i \neq j.$$

Die $z\,(1 \leqq i \leqq z)$ Systeme von z Kongruenzen mod. l

$$\sum_{n=1}^{u} a_{nj} x_n \equiv 0 \text{ für } j \neq i, \quad \sum_{n=1}^{u} a_{ni} x_n \equiv 1 \tag{10}$$

haben jedes mindestens eine Lösung; denn die Linearformen der linken Seiten sind mod. l linear unabhängig.

Eine Lösung des i-ten Systems von (10) sei

$$(x_{i1}, \ldots, x_{in}).$$

Es ist daher

$$\sum_{n=1}^{u} a_{nj} x_{in} \equiv 0 \text{ mod. } l \text{ für } i \neq j, \quad \sum_{n=1}^{u} a_{ni} x_{in} \equiv 1 \text{ mod. } l. \tag{11}$$

Wir setzen

$$\varphi_j = \prod_{n=1}^{u} c_n^{x_{jn}} (1 \leqq j \leqq z).$$

Dann wird:

$$\left(\frac{\varphi_j}{\mathfrak{d}_{j'}}\right) = \prod_{n,\,t=1}^{u} \left(\frac{c_n}{\pi_t}\right)^{x_{jn}\, a_{tj'}} = \prod_{n=1}^{u} \left(\frac{c_n}{\pi_n}\right)^{x_{jn}\, a_{nj'}},$$

also

$$\left(\frac{\varphi_j}{\delta_{j'}}\right) = \zeta^{\sum_{n=1}^{u} a_{nj'} x_{jn}}$$

und nach der Formel (11):

$$\left(\frac{\varphi_j}{\delta_{j'}}\right) = 1 \text{ für } j \neq j', \qquad \left(\frac{\varphi_j}{\delta_j}\right) = \zeta. \tag{12}$$

also (φ_j) kein Element von (β_j), w. z. b. w.

Die Komplexe $A_j = \varphi_j(d)$ sind dann Nebenklassen von $(c)/(d)$, es ist $A_j^l = 1$.

Eine Gleichung

$$\prod_{j=1}^{z} A_j^{y_j} = 1$$

oder

$$\prod_{j=1}^{z} \varphi_j^{y_j} \equiv 1\,(d) \text{ (Anm. 3)}$$

ergibt für jedes j:

$$1 = \prod_{j'=1}^{z} \left(\frac{\varphi_{j'}}{\delta}\right)^{y_{j'}} = \left(\frac{\varphi_j}{\delta_j}\right)^{y_j}, \text{ d. h. } y_j \equiv 0 \bmod. l.$$

Mithin sind die A_j unabhängige Basisklassen von $(c)/(d)$, also $(c)/(d)$ von Typus $(l, \ldots, l)$ und von der Ordnung l^z.

Hieraus und aus Satz 2 folgt Satz 4.

Insbesondere genügt es z. B. für $l = 3$, dass es zwei Primteiler $p_i \equiv 1$ mod. 3 von m gibt, dann ist die Klassenzahl in Ω durch 3 teilbar. Ebenso ergibt sich Teilbarkeit der Klassenzahl in $R(\sqrt[5]{m})$ durch 5, wenn m drei Primteiler $\equiv 1\,(5)$ hat.

Für $l = 3$ können wir noch etwas mehr schliessen:

Satz 5: Sei $l = 3$, m habe u natürliche Primteiler $p_i \equiv 1$ mod. 9, v natürliche Primteiler $q_i \equiv 1$ mod. 3, $\not\equiv 1$ mod. 9. Es sei $v' \equiv \max.(v - 1, 0)$. Dann sind mindestens $u + v'$ Invarianten der Klassengruppe von Ω durch l teilbar.

Beweis: In $k = R(\sqrt{-3})$ gibt es nur die sechs Einheiten ± 1, $\pm \zeta$, $\pm \zeta^2$. Sind $\mathfrak{p}_i | p_i$, $\mathfrak{q}_j | q_j$ Primideale in k, so ist $\left(\frac{\zeta}{\mathfrak{p}_i}\right) = 1$, $\left(\frac{\zeta}{\mathfrak{q}_j}\right) \neq 1$ für jedes i, j. Ist $v > 1$, so gilt für jedes ganze rationale x mit $0 < x < v$

$$\left(\frac{\zeta}{\mathfrak{q}_{1+x}}\right) = \left(\frac{\zeta}{\mathfrak{q}_1}\right)^{n_x}$$

mit $n_x = 1$ oder $n_x = -1$.

Die Bedingungen

$$\left(\frac{\beta_j}{\mathfrak{p}_j}\right) = 1 \text{ (für } 1 \leqq j \leqq u)$$

$$\left(\frac{\beta_{u+x}}{\mathfrak{q}_{1+x}}\right) = \left(\frac{\beta_{u+x}}{\mathfrak{q}_1}\right)^{n_x} \text{ (für } 0 < x < v)$$

geben dann $u + v'$ Zahlengruppen β_i mit den Eigenschaften

(1) $\varepsilon < \beta_i$,

(2) $(\alpha : \beta_i) = l = 3$.

Es folgt

$$(\mathfrak{a}) : (\beta_i) = 3.$$

Die weitere Schlussweise ist genau wie früher.

§ 4.

Wesentlich andere Beweismittel braucht der Satz:

Satz 6: Hat die Zahl m, eventuell von l abgesehen, nur natürliche Primfaktoren $p_i \equiv r'^x \bmod. l$ mit $(x, l-1) = 1$ und zwar letztere in der Zahl $\frac{l+1}{2} + z\,(z > 0)$, wenn $m^{l-1} \equiv 1 \bmod. l^2$, dagegen in der Zahl $\frac{l-1}{2} + z$ für $m^{l-1} \not\equiv 1 \bmod. l^2$, so hat die Klassengruppe von Ω mindestens z durch l teilbare Invarianten.

Bemerkung: In den Teil der Voraussetzung $m^{l-1} \not\equiv 1 \bmod. l^2$ ist der Fall $m \equiv 0 \bmod. l$ von selbst inbegriffen.

Beweis: Ist die natürliche Primzahl $p \neq l$, p/m, so ist auf Grund der Voraussetzung p Primitivwurzel mod. l, es ist (p) in k Primideal, in K wird $(p) = \mathfrak{P}'$. Für $\mathfrak{P}$ ist also bezüglich R der Körper R Zerlegungs-, der Körper k hingegen Trägheitskörper. Bezüglich des Körpers Ω hat also $\mathfrak{P}$ den Körper Ω als Zerlegungs-, K als Trägheitskörper, also ist $\mathfrak{P}$ schon Primideal (ersten Grades) in Ω.

$\mathfrak{P}$ gehört einer Klasse $\vartheta(A)$ in K an, die durch stark ambige Ideale mit $\vartheta^A = (1)$ erzeugt wird. Es ist

$$(\mathfrak{H}(\mathcal{A}):(\mathcal{A})) = h_0 l^M \tag{13}$$

mit

$$M = d + q - (r + 2).$$

(Hasse I a, § 13, S. 99, Formel (7)). Hiebei ist $r = \frac{l-3}{2}$. Bezüglich der übrigen Bezeichnungen sei auf die angegebene Quelle verwiesen. In unserem Falle ist

$$d = \frac{l+1}{2} + z = r + 2 + z,\ q \geqq 0,\ \text{also}\ M \geqq z.$$

(A) Im Falle $m^{l-1} \equiv 1 \bmod. l^2$ sind alle Teiler der Relativdiskriminante von K/k schon Ideale in Ω. Also hat Ω eine durch l teilbare Klassenzahl. Genauer gesagt: es gibt in der Klassengruppe von Ω mindestens z durch l teilbare Invarianten. Denn die l-ten Potenzen aller Teiler der Relativdiskriminante sind hier Hauptideale.

Führen wir dies genauer aus! Aus $(\mathfrak{H}(\mathcal{A}):(\mathcal{A})) = h_0 l^M$ mit $M > 0$ folgt, dass die Teiler der Relativdiskriminante mindestens l^M Klassen aufbauen. Denn wir haben:

$$(\mathfrak{H}(\mathcal{A}):(\mathcal{A})) = (\mathfrak{H}(\mathcal{A}):\mathfrak{a}(\mathcal{A}))(\mathfrak{a}(\mathcal{A}):(\mathcal{A})).$$

Hier ist der zweite Index

$$h_0 l^{-y},$$

wenn l^y Klassen von k in K in die Hauptklasse übergehen. Es bleibt

$$(\mathfrak{H}(\mathcal{A}):\mathfrak{a}(\mathcal{A})) = l^{M+y}$$

und die Faktorgruppe des Index links wird durch Ideale $\mathfrak{H}$ von der Form

$$\mathfrak{a} \prod_i \mathfrak{P}_i^{a_i}$$

aufgebaut; es heisst dies: es gibt

$$l^{M+y} \geqq l^M$$

mal mehr Klassen in K, die durch stark ambige Ideale, als solche, die durch Ideale in k erzeugt werden. Als Repräsentanten dieser Idealklassenfaktorgruppe $\mathfrak{H}(\mathcal{A})/\mathfrak{a}(\mathcal{A})$ können also l^{M+y} Primidealprodukte

$$\prod_{i=1}^{n} \mathfrak{P}_i^{a_{ij}} \qquad (0 \leqq j < l^{M+y})$$

angesehen werden. Die l^{M+y} Klassen

$$(\mathcal{A})\prod_{i=1}^{u}\mathfrak{P}_i^{a_{ij}}$$

sind dann durchwegs Klassen, die schon Ideale aus Ω enthalten. Die l-te Potenz aller dieser Klassen ist die Hauptklasse.

Es folgt Satz 6 wegen $M+y \geqq M \geqq z$ (Anm. 5).

(B) Ganz ähnlich sind die Schlüsse für $m^{l-1} \not\equiv 1 \bmod. l^2$, wo also entweder $l \parallel m^{l-1}-1$ oder $l \mid m$ ist.

Der letztere Fall werde kurz erörtert. Sei hier der (einzige) Primteiler von l in K mit L bezeichnet. Dann ist

$$L^l=(\lambda),\ L^{l(l-1)}=(l). \tag{14}$$

L^{l-1} ist Primideal in Ω. Die Klasse C von L in K ist entweder die Hauptklasse oder gehört zum Exponenten l. Dasselbe gilt von der Klasse des Primideals L^{l-1} in Ω.

Ist L^{l-1} in Ω kein Hauptideal, dann auch in K nicht. Denn wegen (14) liegt L^{l-1} in K in der Klasse C^{-1}. Dann gilt:

Da K/Ω zyklisch vom Grade $l-1$ ist, der Relativgrad aber zur Ordnung l von L^{l-1} in Ω prim ist, kann C^{-1} nicht die Hauptklasse sein, es folgt $C \neq 1$, d. h. L ist kein Hauptideal.

Das Gegenstück ist

Satz 6 a: Ist k regulär, weiter m Primzahl und Primitivwurzel mod. l, so ist in Ω und K die Klassenzahl nicht durch l teilbar.

Beweis: Sei $m=p$. Für $p^{l-1} \equiv 1 \bmod. l^2$ ist dann $f=(p)$, für $p^{l-1} \not\equiv 1 \bmod. l^2$ ist dann $f=(p\lambda^2)$. Die Anzahl a der ambigen Klassen entscheidet dann darüber, ob die Klassenzahl in K durch l teilbar ist, aus $a \not\equiv 0 \bmod. l$ folgt $h \not\equiv 0 \bmod. l$ (Moryja, Proceedings Tokyo 1933). Die Umkehrung: aus $h \not\equiv 0 \bmod. l$ folgt $a \not\equiv 0 \bmod. l$ ist trivial.

Ist $h' \not\equiv 0 \bmod. l$ und $\mathfrak{M}$ ein Ideal in Ω, das kein Hauptideal ist, wo aber $\mathfrak{M}^l=(\Gamma)$ in Ω Hauptideal ist, so kann $\mathfrak{M}$ auch nicht in K Hauptideal sein. Denn wir hätten bei Annahme $\mathfrak{M}=(A)$ durch Relativnormbildung $K/\Omega: \mathfrak{M}^{l-1}=(B)$ mit $B=N_{K/\Omega}A$. Es folgte $\mathfrak{M}=(\Gamma B^{-1})$ also $\mathfrak{M}$ schon in Ω Hauptideal.

Es folgt: aus $l \mid h'$ folgt $l \mid h$ oder

aus $h \not\equiv 0 \bmod. l$ folgt $h' \not\equiv 0 \bmod. l$.

Es ist (Hasse I a, § 13, S. 98, Formel (13)) mit den dortigen Bezeichnungen

$$a = h_0 l^x \text{ mit } x = d + q^* - (r+2). \tag{15}$$

(A) Ist $p^{l-1} \equiv 1 \bmod l^2$, so ist $d = 1$. Weiter ist $q^* = r + 1$.

Um letzteres zu zeigen, gehen wir so vor: jede Einheit ε in k erfüllt

$$\left(\frac{\varepsilon}{p}\right) = 1. \tag{16}$$

(16) folgt für $\varepsilon = \zeta$ aus

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

für jedes rationale zu l prime n, für ε als Einheit in k' durch Anwendung von s'. Da jede Einheit in sich bekanntlich als

$$\varepsilon = \zeta^A \varepsilon' \tag{17}$$

darstellen lässt, folgt (16). (Man kann auch die Tatsache, dass p l-primär ist, in Anwendung bringen, aus ihr folgt $\left(\frac{\varepsilon}{p}\right) = \left(\frac{p}{\varepsilon}\right) = 1$).

Es bleibt somit $x = 0$ oder $a = h_0 \not\equiv 0 \bmod l$, letzteres ist die Voraussetzung, dass k regulär ist. Also bleibt unter Anwendung des Satzes von Moryja:

Aus $h_0 \not\equiv 0 \bmod l$ folgt hier $h \not\equiv 0 \bmod l$ und auch $h' \not\equiv 0 \bmod l$ (Anm. 4)

(B) Für $p^{l-1} \not\equiv 1 \bmod l^2$ wird $d = 2$. Weiter ist $q^* = r$.

Letzteres beweist man so: Es ist $\left(\frac{\zeta}{p}\right) \neq 1$, somit ζ nicht Relativnorm, dagegen ist für jedes ε' aus k' $\left(\frac{\varepsilon'}{p}\right) = 1$, was wie vorhin gezeigt wird. Also ist ε' Rest nach (p), weil (p) Primideal ist, somit Normenrest. Weiter ist $\varepsilon' \underset{(l)}{\equiv} 1 \bmod \lambda^2$, somit Normenrest mod. λ^2. (mod. $\lambda^2 \| f$ sind Normenrest und l-ter Potenzrest dasselbe, was im Falle $\lambda^b | f$, $b > 2$ für diese b nicht mehr richtig ist.) Also ist ε' Normenrest nach $(p)\lambda^2 = (f)$, somit als Einheit, die Normenrest ist, auch Relativnorm. Es bleibt $q^* = r$, $x = 0$, somit $a \not\equiv 0 \bmod l$. Der weitere Schluss ist wie vorhin.

Es gilt auch noch

Satz 6 b: Ist $m^{l-1} \equiv 1 \bmod l^2$, $m = p_1^q p_2^b$, $p_i^{l-1} \not\equiv 1 \bmod l^2$, $p_i \equiv r'^{x_i} \bmod l$ mit $(x_i, l-1) = 1$ für $i = 1, 2$, ist weiter k regulär, so ist $h \not\equiv 0 \bmod l$, also auch $h' \not\equiv 0 \bmod l$.

Beweis: Für jedes p_i gilt $\left(\frac{\zeta}{p_i}\right) \neq 1$, $\left(\frac{\varepsilon'}{p_i}\right) = 1$, also ist wieder $q^* = r$. Weiter ist $d = 2$ wegen $f = (p_1 p_2)$. Der weitere Schluss ist genau wie bei Satz 6 a, (B).

§ 5.

Nun beweisen wir

Satz 7. Ist $l \equiv -1 \mod 4$, und hat m insgesamt u natürliche Primteiler p_i mit $p_i^2 \equiv 1 \mod l^2$, v natürliche Primteiler q_j mit $q_j^2 \equiv 1 \mod l$, $q_j^2 \not\equiv 1 \mod l^2$, so hat die Klassengruppe in $\Omega(\sqrt{-l}) = \Omega_1$ mindestens $u + v'$ durch l teilbare Invarianten. Hiebei ist $v' = \max.(v - 1, 0)$ und $u + v > 0$.

Beweis: Es seien $\mathfrak{p}_i$ und $\mathfrak{q}_j$ (nicht näher bestimmte) Primteiler von p_i und q_j in k. Wir nehmen $\mathfrak{p}$ als Repräsentanten eines $\mathfrak{p}_i$, $\mathfrak{q}$ als Repräsentanten eines $\mathfrak{q}_j$.

Für $\mathfrak{p}$ ist

$$\left(\frac{\zeta}{\mathfrak{p}}\right) = 1. \tag{18}$$

Mit der Abkürzung $\mathfrak{p}' = \mathfrak{p}^{s'}$ ist offenbar auch

$$\left(\frac{\zeta}{\mathfrak{p}'}\right) = 1. \tag{19}$$

Aus (18) und (19) folgt

$$\left(\frac{\zeta}{\mathfrak{p}\mathfrak{p}'}\right) = 1. \tag{20}$$

Weiter gilt für jedes ε'

$$\left(\frac{\varepsilon'}{\mathfrak{p}\mathfrak{p}'}\right) = 1. \tag{21}$$

Aus (17), (20) und (21) folgt

$$\left(\frac{\varepsilon}{\mathfrak{p}\mathfrak{p}'}\right) = 1 \tag{22}$$

für jede Einheit ε in k.

Sei $v > 0$. Es ist dann genau wie früher mit $\mathfrak{q}^{s'} = \mathfrak{q}'$:

$$\left(\frac{\varepsilon'}{\mathfrak{q}\mathfrak{q}'}\right) = 1 \tag{23}$$

hingegen

$$\left(\frac{\zeta}{\mathfrak{q}_i}\right) = \left(\frac{\zeta}{\mathfrak{q}_i'}\right) = \zeta^{A_i} \neq 1.$$

Die Gleichung

$$\left(\frac{\zeta}{\prod_{i=1}^{v}(\mathfrak{q}_i\,\mathfrak{q}_i')^{a_i}}\right)=1 \tag{24}$$

ist genau dann erfüllt, wenn

$$\sum_{i=1}^{v} A_i\,a_i \equiv 0 \bmod. l \tag{25}$$

ist. Da diese Kongruenz $v'=v-1$ linear unabhängige Lösungen mod. l hat, ergeben sich $v-1$ l-unabhängige Ideale

$$b_1,\ \ldots,\ b_j,\ \ldots,\ b_{v-1},$$

mit folgenden Eigenschaften:

Ist $(a_{1j},\ \ldots,\ a_{vj})$ eine der linear unabhängigen Lösungen von (25) so soll

$$b_j=\prod_{i=1}^{v}(\mathfrak{q}_i\,\mathfrak{q}_i')^{a_{ij}} \tag{26}$$

sein. Es gibt nach (25):

$$\left(\frac{\zeta}{b_j}\right)=1, \tag{27}$$

nach (26)

$$\left(\frac{\varepsilon'}{b_j}\right)=1, \tag{28}$$

somit nach (17)

$$\left(\frac{\varepsilon}{b_j}\right)=1 \tag{29}$$

für jedes ε in k.

Durch

$$1=\left(\frac{\beta}{\mathfrak{p}_i\,\mathfrak{p}_i'}\right),\quad 1=\left(\frac{\beta}{b_j}\right)$$

sind im Falle $v=0$ insgesamt u, für $v>0$ hingegen $u+v-1$, also in jedem Falle $u+v'$ Zahlengruppen gegeben, wo jede Einheit enthalten ist.

Sei k_1 der Körper $R\left(\sqrt{(-1)^{\frac{l-1}{2}}\,l}\right)$, also $k_1<k$. Nach Voraussetzung ist $l\equiv -1$ mod. 4, also $k_1=R(\sqrt{-l})$ imaginärquadratisch, also kein Teilkörper von k' und für jedes primitive, also nicht zu R gehörende Element γ von k_1 gibt $\gamma^{s'}\neq\gamma$.

In k_1 bestimmen wir zu jedem Ideal $\mathfrak{p}_i$ und $\mathfrak{q}_j$ das Primideal $\mathfrak{p}_i^{(1)}$ und $\mathfrak{q}_j^{(1)}$ mit $\mathfrak{p}_i \mid \mathfrak{p}_i^{(1)}$, bzw. $\mathfrak{q}_j \mid \mathfrak{q}_j^{(1)}$. Sei $\mathfrak{r}$ für den Augenblick Repräsentant der $\mathfrak{p}_i$ und $\mathfrak{q}_j$, $\mathfrak{r}' = \mathfrak{r}^{s'}$. Dann gilt für $\mathfrak{r} \mid r$ mit r als natürlicher Primzahl und $\mathfrak{r} \mid \mathfrak{r}^{(1)}$, $\mathfrak{r}' \mid \mathfrak{r}^{(2)}$, wo $\mathfrak{r}^{(1)}$ und $\mathfrak{r}^{(2)}$ Primideale in k_1 sind:

(A) Im Falle $r \equiv 1 \bmod. l$ ist $\mathfrak{r}^{(1)}$ und $\mathfrak{r}^{(2)}$ verschieden, beide sind vom ersten Grad (wie $\mathfrak{r}$ und $\mathfrak{r}'$ in k).

Hier kommt zur Geltung, dass k_1 gegenüber s' nicht elementeweis invariant ist.

(B) Im Falle $r \equiv -1 \bmod. l$ gilt $\mathfrak{r} = \mathfrak{r}'$, $\mathfrak{r}^{(1)} = \mathfrak{r}^{(2)} = (r)$ (als Ideal in k_1 betrachtet). (r) in k_1 und $\mathfrak{r}$ in k sind vom zweiten Grad.

Hier kommt wieder $l \equiv -1 \bmod. 4$ zur Geltung. Es ist

$$\left(\frac{-l}{r}\right)_2 = \left(\frac{r}{-l}\right)_2 = \left(\frac{-1}{l}\right)_2 = -1,$$

also bleibt (r) in k_1 Primideal.

Es kommt nun folgender Schluss:

Zu jedem $\mathfrak{r}$ der Sorte (A) gibt es unzählig viele zu f prime γ in k_1, so dass γ Rest von $\mathfrak{r}^{(2)}$ und jedem von $\mathfrak{r}$ verschiedenen $\mathfrak{p}_i$ und $\mathfrak{q}_j$, auch von $\mathfrak{p}_i'$ und $\mathfrak{q}_j'$, aber $\left(\frac{\gamma}{\mathfrak{r}}\right) = \zeta$ ist. Es ist dann

$$\left(\frac{\gamma}{\mathfrak{r}'}\right) = 1,$$

also

$$\left(\frac{\gamma}{\mathfrak{r}\mathfrak{r}'}\right) = \zeta, \tag{30}$$

hingegen

$$\left(\frac{\zeta}{\mathfrak{p}_i\,\mathfrak{p}_i'}\right) = 1, \text{ bzw. } \left(\frac{\zeta}{\mathfrak{q}_i\,\mathfrak{q}_i'}\right) = 1$$

für jedes

$$\mathfrak{p}_i \neq \mathfrak{r},\ \mathfrak{q}_j \neq \mathfrak{r}. \tag{30 b}$$

Einem Primideal $\mathfrak{r}$ der Sorte (B) ordnen wir ein γ zu, Zahl von k_1, die prim zu f, Nichtrest von (r) in k_1, u. zw. so dass $\left(\frac{\gamma}{\mathfrak{r}}\right) = \zeta^{\frac{l+1}{2}}$ ist. hingegen Rest aller von $\mathfrak{r}$ verschiedenen $\mathfrak{p}_i$ und $\mathfrak{q}_j$, auch von den bezüglichen $\mathfrak{p}_i'$ und $\mathfrak{q}_j'$ sein soll. Dann ist

$$\left(\frac{\gamma}{\mathfrak{r}\mathfrak{r}'}\right) = \zeta \tag{31}$$

wegen $\mathfrak{r} = \mathfrak{r}'$, dagegen

$$\left(\frac{\gamma}{\mathfrak{p}_i\,\mathfrak{p}_i'}\right) = 1, \quad \left(\frac{\gamma}{\mathfrak{q}_j\,\mathfrak{q}_j'}\right) = 1$$

für jedes von $\mathfrak{r}$ verschiedene $\mathfrak{p}_i$ und $\mathfrak{q}_j$.

Mit der fortlaufenden Numerierung

$$\mathfrak{r}_1 = \mathfrak{p}_1, \ldots, \mathfrak{r}_u = \mathfrak{p}_u, \ \mathfrak{r}_{u+1} = \mathfrak{q}_1, \ldots, \mathfrak{r}_{u+v} = \mathfrak{q}_v$$

sei die Zahl γ_i in dieser Art dem Primideal $\mathfrak{r}_i$ zugeordnet.

Wir bestimmen nun $u + v'\,(v' \geqq 0)$ Zahlen μ_j, wie folgt:

I. Es ist $\mu_i = \gamma_j$ für $j \leqq u$.

II. Ist b_j durch (26) bestimmt, so hat das Kongruenzsystem mod. l, das völlig dem System (10) gleicht, mindestens eine Lösung.

Man hat hier zum Unterschied von (10) v' solche Gleichungssysteme. Eine Lösung des j-ten sei analog wie damals durch

$$(x_{j1}, \ldots, x_{jv})$$

gegeben.

Wir setzen dann

$$\mu_{u+j} = \prod_{t=1}^{v} \gamma_{u+t}^{x_{jt}}.$$

Mit

$$\text{(I)} \quad \partial_j = \mathfrak{r}_j \mathfrak{r}_j' \text{ für } j \leqq u,$$

$$\text{(II)} \quad \partial_j = b_{j-u} \text{ für } j > u$$

gilt:

$$\left(\frac{\mu_j}{\partial_j}\right) = \zeta, \quad \left(\frac{\mu_j}{\partial_{j'}}\right) = 1 \text{ für } j \neq j'.$$

Der Beweis ist für min. $(j, j') \leqq u$ fast trivial, für $j > u$ und $j' > u$ völlig analog dem der Formel (12).

Der weitere Nachweis ist unter Anwendung des Satzes 2 b völlig analog dem Schluss des § 3.

Anmerkungen.

1. Es wäre eigentlich nicht notwendig, $m' \not\equiv_{(l)} 1$, sondern nur $b \neq 0$ vorauszusetzen, da sich bekanntlich elementarzahlentheoretisch sonst aus $m' \equiv_{(l)} 1$ sich $n' \equiv_{(l)} 1$ ergibt. Wegen der Ungeklärtheit des Fermatproblems wäre allerdings vielleicht $m' \equiv_{(l)} 1$ möglich, ohne dass $b = 0$ ist.

2. Für $l = 3$ ist sicher $a^3 + 27\,b^3$ kein Kubus für $b \neq 0$, was stillschweigend vorausgesetzt wird.

3. Heisst bekanntlich in der normalen Gruppenkongruenzschreibweise: $\prod_{j=1}^{z} C_j^{y_j}$ ist Element von (d), vgl. z. B. H. Zassenhaus, Gruppentheorie (1937), S. 9 f.

4. Über die nähere Schlussweise vgl. den folgenden Beweis beim Satz 6 a, Teil (B).

5. Man kann auch durch Betrachtung des l-Klassenkörpers L von Ω zum Ziel kommen, indem nach dem Satze Hasse II, § 25, VII, S. 145 sich für $h' \equiv 0$ mod. l der Körper LK/K als abelsch unverzweigt, $(LK:K)$ als Potenz von l und auch leicht $LK > K$ erweist. In Hasse, autographierte Vorlesungen (1933) erscheint zitierter Satz auf S. 121 als Verschiebungssatz.