Über die Kummerschen logarithmischen Hilfsfunktionen.

Von PETER DÉNES in Budapest.

Im folgenden bezeichnen l eine ungerade Primzahl, ζ eine primitive l-te Einheitswurzel, $R(\zeta)$ den Kreiskörper der l-ten Einheitswurzeln, $\lambda = 1-\zeta$, $\mathfrak{l} = (\lambda)$. Dann gilt $\mathfrak{l}^{l-1} = (l)$.

KUMMER[1]) führte im Jahre 1852 den Begriff „Logarithmus einer Kreiskörperzahl ω bezüglich auf den Modul l^{n+1}" ein, welcher auch selbst eine Zahl in $R(\zeta)$ ist. Die Anwendung dieser Logarithmen erleichtert die Rechnung mit Kreiskörperzahlen, da sich die Multiplikation auf Addition, die Potenzierung auf Multiplikation mit einer ganzen rationalen Zahl reduziert; immerhin ergibt sich das Resultat nur als ein Kongruenzrest nach dem Modul l^{n+1}. KUMMER ermittelte ferner[2]) eine Methode zur Berechnung dieser Logarithmen. Bei dieser Methode verwendet er die logarithmische Hilfsfunktion $\log \omega(e^v)$, welche derart definiert wird, dass man in der „Darstellung" der ganzen Zahl ω aus $R(\zeta)$:

$$\omega = \sum_{i=0}^{s} a_i \zeta^i, \tag{1}$$

wo $a_0, a_1, \ldots, a_s$ ganze rationale Zahlen sind, e^v anstatt ζ setzt. $\omega(e^v)$ und $\log \omega(e^v)$ sind differentiierbare Funktionen des Veränderlichen v.

Obwohl MERTENS[3]) zeigte, daß die von KUMMER angegebene Berechnungsmethode des Logarithmus der Zahl ω bezüglich auf den Modul l^{n+1} nicht richtig ist, haben sich die logarithmischen Hilfsfunktionen in der Lösung gewisser Probleme der Kreiskörpertheorie sehr bewährt, da diese Hilfsfunktionen — unter anderem — auch zur Vereinfachung und Reduktion der Rechnungsoperationen geeignet sind. Schon KUMMER[4]) wendet die logarithmischen Hilfsfunktionen zum Ausdrücken des Potenzcharakters der Kreiskörpereinheiten

---

[1]) E. KUMMER, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *Journal f. d. reine u. angew. Math.*, **44** (1852), 93—146; s. insbesondere S. 130.

[2]) A. a. O. [1]), S. 134 ff.

[3]) F. MERTENS, Über den Kummerschen Logarithmus einer komplexen Zahl des Bereichs einer primitiven l-ten Einheitswurzel in bezug auf den Modul l^{n+1}, wo l eine ungerade Primzahl bedeutet, *Sitzungsber. Akad. d. Wiss. Wien*, **126** (1917), 1337—1343.

[4]) A. a. O [1]) S. 101 ff.

in geschlossener Form an. Die Methoden von KUMMER hat VANDIVER[5]) zur Bestimmung der Potenzcharakter gewisser Kreiskörperzahlen weiter entwickelt. HILBERT[6]) hat allein vermittelst der logarithmischen Hilfsfunktionen — also ohne die Kummerschen Logarithmen — die Struktur der Einheiten der regulären Kreiskörper untersucht. Ein ähnlicher allgemeiner Strukturaufschluß der Einheiten der irregulären Kreiskörper war bis jetzt zufolge der unten anzugebenden Gründe nicht möglich. Das Ziel der vorliegenden Arbeit ist die hierzu nötigen Hilfsmittel zu schaffen. Die Ergebnisse der Strukturuntersuchungen der irregulären Kreiskörpereinheiten werden in einer späteren Arbeit festgelegt.

Die Hauptschwierigkeit liegt darin, daß die Zahl ω zufolge der Identität

$$g(\zeta) = 1 + \zeta + \zeta^2 + \cdots + \zeta^{l-1} = 0 \tag{2}$$

unendlich viele Darstellungen (1) hat, so daß zu jeder Zahl ω unendlich viele verschiedene Hilfsfunktionen gehören. Ist in (1) $s \leqq l-2$, so ist ω in der eindeutig bestimmten *Normalform* gegeben:

$$\omega^* = \sum_{i=0}^{l-2} b_i \zeta^i, \tag{3}$$

wo $b_0, b_1, \ldots, b_{l-2}$ ganze rationale Zahlen bezeichnen. Diese Normalform wird später auch mit einem Stern bezeichnet. Zu der Normalform der Zahl ω gehören die Funktionen $\omega^*(e^v)$ und $\log \omega^*(e^v)$.

Theoretisch kann man aus einer gegebenen Funktion $\log \omega^*(e^v)$ und der ganzen rationalen Zahl ω_0^*, welche durch die Einsetzung $v = 0$ aus $\omega^*(e^v)$ entsteht, die kanonische Form (3) von ω aufstellen, falls $\omega_0^* \not\equiv 0$. Bedeutet nämlich der Operator D_z, daß man z-mal nach v differentiiert und dann $v = 0$ setzt, so ist

$$D_m \log \omega^*(e^v) = F\left[\frac{1}{\omega_0^*}, D_1\omega^*(e^v), \ldots, D_m\omega^*(e^v)\right], \tag{4}$$

wo F ein ganzzahliges Polynom der Veränderlichen $\frac{1}{\omega_0^*}$, $D_j\omega^*(e^v)$ $(j = 1, \ldots, m)$ darstellt. Aus den auf $m = 1, \ldots, l-2$ bezüglichen Gleichungen (4) kann man $D_j\omega^*(e^v)$ $(j = 1, \ldots, l-2)$ bestimmen, indem man nach (3)

$$D_j\omega^*(e^v) = \sum_{i=1}^{l-2} b_i \cdot i^j \qquad (j = 1, \ldots, l-2) \tag{5}$$

einsetzt.

Die Gleichungen (5) ergeben die Werte $b_1, \ldots, b_{l-2}$; b_0 ergibt sich dann aus

$$\omega_0^* = b_0 + b_1 + \cdots + b_{l-2}.$$

Wird (4) nur als eine Kongruenz nach dem Modul einer Potenz von l angewendet, so ist die schärfere Bedingung $\omega_0^* \not\equiv 0 \pmod{l}$ notwendig; dies

[5]) H. S. VANDIVER, On power characters of singular integers in a properly irregular cyclotomic field, *Transactions American Math. Soc.*, **32** (1930), 391—408.

[6]) D. HILBERT, *Théorie des corps de nombres algébraiques* (1913), §. 138, S. 232—235.

bedeutet, daß die Zahl ω prim zu l ist. Das geschilderte Prinzip ist auch dann anwendbar, wenn $\log \omega(e^r)$ (statt $\log \omega^*(e^r)$) und ω_0 angegeben sind, aber in diesem allgemeinen Falle werden die Rechnungen komplizierter.

Bei der Strukturuntersuchung der regulären Kreiskörpereinheiten genügt es, die Gleichungen (4) als eine Kongruenz modulo l zu betrachten. Die Unbestimmtheit der verschiedenen Darstellungen (1) von ω stört dabei nicht, weil die Kongruenzen

$$D_k \log \omega_1(e^r) \equiv D_k \log \omega_2(e^r) \pmod{l} \quad (k = 1, \ldots, l-2)$$

zwischen zwei beliebigen Darstellungen ω_1 und ω_2 der zu l primen Zahl ω des Körpers $R(\zeta)$ erfüllt sind[7]). Bei der Untersuchung der Einheiten der irregulären Kreiskörper muss man demgegenüber in den Kongruenzen auch höhere Potenzen von l als Modul anwenden. Die Ausarbeitung der Rechnungsmittel der Sätze dieser Arbeit wurde erst durch den Beweis der folgenden Kummerschen Vermutung ermöglicht[8]):

Sind ω_1 und ω_2 zwei zu l prime ganze Zahlen im Körper $R(\zeta)$, für welche $\omega_1 \equiv \omega_2 \pmod{l^{n+1}}$ gilt und ist k eine ganze rationale Zahl, welche nicht durch $l-1$ teilbar ist, so ist

$$D_{kl^n} \log \omega_1(e^r) \equiv D_{kl^n} \log \omega_2(e^r) \pmod{l^{n+1}}, \tag{6}$$

wo $\log \omega_1(e^r)$ und $\log \omega_2(e^r)$ sich auf beliebige Darstellungen von ω_1 und ω_2 beziehen.

In der vorliegenden Arbeit wird unser Zweck nicht die Normalform von ω aus einer gegebenen Funktion $\log \omega(e^r)$ (und aus ω_0^*) aufzustellen, da dies zur Feststellung der Einheitenstruktur nicht notwendig ist, sondern wir setzen für jede zu l prime Zahl ω des Körpers $R(\zeta)$

$$\omega \equiv f_0 + f_t \lambda^{n(l-1)+t} \pmod{l^{n(l-1)+t+1}}, \tag{7}$$

wo f_0, f_t zu l prime ganze rationale Zahlen, $0 \leqq t \leqq l-1$ und $n \geqq 0$ sind, und stellen uns den Zweck die Restklassen $f_0 \bmod l^{n+1}$ und $f_t \bmod l$ zu bestimmen. (Diese Restklassen und die Zahlen n, t sind offenbar eindeutige Funktionen von ω).

Zunächst beweisen wir zwei Hilfssätze.

Hilfssatz 1. *Erfüllt die Zahl ω des Körpers $R(\zeta)$ die Kongruenz* (7), *so gelten die folgenden Kongruenzen:*

a) *im Falle* $n = 0$:

$$D_k \log \omega^*(e^r) \equiv 0 \pmod{l} \quad (k = 1, 2, \ldots, t-1), \tag{8}$$

$$D_t \log \omega^*(e^r) \equiv (-1)^t \cdot \frac{t! \cdot f_t}{\omega_0^*} \pmod{l}. \tag{9}$$

[7]) Vgl. D. Hilbert, a. a. O. [6]) §. 131, S. 213—216, insbesondere Fußnote S. 215.

[8]) P. Dénes, Proof of a conjecture of Kummer, *Publicationes Math. Debrecen*, 2 (1952), 208—214.

b) *im Falle* $n > 0$:

$$D_{k_1 s_1 \ldots k_n s_n} \log \omega^*(e^v) \equiv 0 \pmod{l^{v-1}} \quad (k = 1, 2, \ldots, t-1). \tag{10}$$

$$D_{t-s_1 t \ldots s_n} \log \omega^*(e^v) \equiv (-1)^t \cdot \frac{l^v \cdot t! \cdot f_t}{\omega_0^*} \pmod{l^{v+1}}, \tag{11}$$

wo $s_1, s_2, \ldots, s_n$ *beliebige nicht negative ganze Zahlen sind.*

Beweis: a) $n = 0$. Die Normalform der Zahl ω kann auch als

$$\omega^* \equiv \sum_{k=0}^{t-2} c_k \lambda^k \tag{12}$$

geschrieben werden, wobei $c_0, \ldots, c_{t-2}$ eindeutig bestimmte ganze rationale Zahlen sind. Aus (7) und (12) folgen

$$c_k \equiv 0 \pmod{l} \quad (k = 1, 2, \ldots, t-1). \tag{13}$$

$$c_t \equiv f_t \pmod{l}. \tag{14}$$

Wird nämlich (12) als eine Kongruenz nach dem Modul l^2 untersucht, so ist, falls $t > 1$,

$$\omega^* \equiv c_0 + c_1 \lambda \pmod{l^2},$$

woraus folgt $l | c_1$. Ist $t > 2$ und nimmt man den Modul l^3 zu Hilfe, so folgt $l | c_2$. Schließlich erhält man

$$\omega^* \equiv c_0 + c_t \lambda^t \pmod{l^{t-1}},$$

woraus wegen (7) die Kongruenz (14) folgt.

Zwischen den Koeffizienten b und c der Gleichungen (3) und (12) gelten die folgenden Beziehungen:

$$b_i \equiv (-1)^i \sum_{k=i}^{t-2} \binom{k}{i} c_k \qquad (i = 0, 1, \ldots, l-2) \tag{15}$$

$$c_k \equiv (-1)^k \sum_{i=k}^{l-2} \binom{i}{k} b_i \qquad (k = 0, 1, \ldots, l-2) \tag{16}$$

Die Entwicklung von $\binom{j}{k}$ nach Potenzen von j liefert:

$$\binom{j}{k} = \frac{g_{k1} \cdot j + g_{k2} \cdot j^2 + \cdots + g_{kk} \cdot j^k}{k!} \quad (j, k = 1, \ldots, l-2,\ j \geq k), \tag{17}$$

wo $g_{11}, \ldots, g_{l-2, l-2}$ rationale ganze Zahlen und

$$g_{kk} = 1 \qquad (k = 1, \ldots, l-2) \tag{18}$$

sind. Setzt man nun die aus den Gleichungen (5) berechneten Werte $b_1, \ldots, b_{l-2}$ in (16), so ergibt sich

$$c_k = \frac{(-1)^k}{k!} \sum_{j=1}^{k} g'_{kj} \cdot D_j \omega^*(e^v) \qquad (k = 1, \ldots, l-2) \tag{19}$$

und man kann die Identität $g'_{kj} = g_{kj}$ einfach zeigen, indem man die Werte $D_j \omega^*(e^v)$ aus (5) in (19) setzt und die erhaltenen Gleichungen mit (16) vergleicht.

Wird nacheinander $k = 1, \ldots, t$ in (13), (18) und (19) eingesetzt, so ergeben sich wegen (14)

(20) $$D_k \omega^*(e^r) \equiv 0 \pmod{l} \qquad (k = 1, 2, \ldots, t-1).$$

(21) $$D_t \omega^*(e^r) \equiv (-1)^t \cdot t! \cdot f_t \pmod{l}.$$

Drückt man schließlich $D_k \log \omega^*(e^r)$ nacheinander für die Werte $k = 1, \ldots, t$ gemäß (4) aus, so wird vermittelst (20)

$$D_k \log \omega^*(e^r) \equiv \frac{1}{\omega_0^*} D_k \omega^*(e^r) \pmod{l} \quad (k = 1, 2, \ldots, t).$$

Hieraus folgt der Beweis für $n = 0$.

b) $n > 0$. Nach (7) gilt

$$\omega^* \equiv f_0 \pmod{l^{n(l-1)+1}}.$$

Ist ω^* nach einer Potenz von l, etwa $l^N (N > 0)$, als Modul mit einer rationalen ganzen Zahl kongruent, so ist die letztere Zahl nach demselben Modul auch mit c_0 in (12) kongruent, da die übrigen Glieder $c_k \lambda^k (k = 1, \ldots, l-2)$ nach dem Modul l^N nicht mit einer durch l^N nicht teilbaren rationalen ganzen Zahl kongruent sind. Daher ist, da $c_0 = \omega_0^*$,

$$\omega_0^* \equiv f_0 \pmod{l^{n(l-1)+1}}$$

und weil ω_0^* eine rationale ganze Zahl ist und $t > 0$, auch

(22) $$\omega_0^* \equiv f_0 \pmod{l^{n+1}}.$$

Hiermit erhält man aus (12)

(23) $$\omega^* \equiv f_0 + \sum_{k=1}^{l-2} c_k \lambda^k \pmod{l^{n+1}}.$$

Man kann leicht zeigen, daß die Koeffizienten $c_1, \ldots, c_{l-2}$ durch l^n, ja sogar die Koeffizienten $c_1, \ldots, c_{l-1}$ durch l^{n+1} teilbar sind. Aus (7) und (23) wird nämlich

(24) $$c_1 \lambda + c_2 \lambda^2 + \cdots + c_{l-2} \lambda^{l-2} \equiv 0 \pmod{l^{n(l-1)+1}}.$$

Betrachtet man (24) als eine Kongruenz modulo l^2, so ergibt sich, daß c_1 durch l, also als eine ganze rationale Zahl auch durch l teilbar ist. Die Untersuchung nach dem Modul l^3 zeigt dann $l \mid c_2$. So weiter schließend sehen wir, dass die Koeffizienten $c_3, \ldots, c_{l-2}$ durch l teilbar sind. Folglich kann man (24) so schreiben:

$$\frac{c_1}{l} \lambda + \frac{c_2}{l} \lambda^2 + \cdots + \frac{c_{l-2}}{l} \lambda^{l-2} \equiv 0 \pmod{l^{n(l-1)+1}},$$

wo $\frac{c_1}{l}, \ldots, \frac{c_{l-2}}{l}$ ganze rationale Zahlen sind. Das angewendete Verfahren kann man n-mal wiederholen, wodurch sich schließlich die Kongruenz

$$\frac{c_1}{l^n} \lambda + \frac{c_2}{l^n} \lambda^2 + \cdots + \frac{c_{l-2}}{l^n} \lambda^{l-2} \equiv 0 \pmod{l}$$

ergibt, wo $\frac{c_1}{l^n}, \ldots, \frac{c_{l-2}}{l^n}$ ganze rationale Zahlen sind. Diese Kongruenz kann dann in gleicher Weise nach den Moduln $l^2, \ldots, l^n$ untersucht werden. So ergibt sich die Richtigkeit unserer Behauptung:

$$c_1 \equiv c_2 \equiv \cdots \equiv c_{l-1} \equiv 0 \pmod{l^{n+1}}, \tag{25}$$

$$c_l \equiv c_{l+1} \equiv \cdots \equiv c_{l-2} \equiv 0 \pmod{l^n}. \tag{26}$$

Aus (15), (25), (26) folgen

$$b_i \equiv 0 \pmod{l^n} \quad (i = 1, 2, \ldots, l-2). \tag{27}$$

Somit gilt jetzt für die Normalform der Zahl ω

$$\omega^* = b_0 + l^n \sum_{i=1}^{l-2} b_i' \zeta^i, \tag{28}$$

bzw.

$$\omega^* = \omega_0^* + l^n \sum_{k=1}^{l-2} c_k' \lambda^k, \tag{29}$$

wo $b_1', \ldots, b_{l-2}'$, $c_1', \ldots, c_{l-2}'$ ganze rationale Zahlen bezeichnen.

Die Funktion $\log \omega^*(\varepsilon^v)$ kann durch die unendliche Reihe

$$\log \frac{\omega^*(\varepsilon^v)}{\omega_0^*} = \sum_{j=1}^{\infty} (-1)^{j-1} \cdot \frac{1}{j} \left[\frac{\omega^*(\varepsilon^v) - \omega_0^*}{\omega_0^*} \right]^j$$

ausgedrückt werden. In einer früheren Arbeit[9]) habe ich gezeigt, daß bei Anwendung des Operators D_m $(m > 0)$ auf diese unendliche Summe nur eine endliche Anzahl, und zwar genau m, von den Gliedern der Summe zu berücksichtigen sind:

$$D_m \log \omega^*(\varepsilon^v) = \sum_{j=1}^{m} (-1)^{j-1} \cdot \frac{1}{j} D_m \left| \frac{\omega^*(\varepsilon^v) - \omega_0^*}{\omega_0^*} \right|^j \tag{30}$$

Der Summand ist wegen (29) kongruent

$$(-1)^{j-1} \cdot \frac{1}{j \cdot \omega_0^{*j}} \; l^{nj} \cdot D_m \left| \sum_{k=1}^{l-2} c_k' (1 - \varepsilon^v)^k \right|^j \tag{31}$$

mod l^{n+1}. Es sei j in (31) genau durch die r-te Potenz von l teilbar: $j = j' \cdot l^r$, wobei j' prim zu l ist. (31) ist dann mindestens durch die $(nj'l^r - r)$-te Potenz von l teilbar, da ω_0^* prim zu l ist. Offensichtlich ist

$$n \cdot j' \cdot l^r - r \geqq n + 1, \qquad \text{wenn } j \geqq 1, \quad n > 0.$$

Folglich entsteht aus (30) die Kongruenz

$$D_m \log \omega^*(\varepsilon^v) \equiv \frac{D_m \omega^*(\varepsilon^v)}{\omega_0^*} \pmod{l^{n+1}}, \quad nm > 0. \tag{32}$$

---

[9]) A. a. O. [8]) Lemma B, S. 207.

Verwendet man den Operator D_m auf (28), so wird

$$D_m\omega^*(e^v) \equiv l^n \sum_{i=1}^{l-2} b_i' \cdot i^m \tag{33}$$

und hieraus folgt wegen

$$i^{k+s_k(l-1)} \equiv i^k \pmod{l}, \quad (i = 1, 2, \ldots, l-2),$$

wo s_k beliebige nicht negative ganze Zahlen bezeichnen, die Kongruenz

$$D_{k+s_k(l-1)}\omega^*(e^v) \equiv D_k\omega^*(e^v) \pmod{l^{n+1}}, \tag{34}$$

welche mit (32) zusammen

$$D_{k+s_k(l-1)} \log \omega^*(e^v) \equiv D_k \log \omega^*(e^v) \pmod{l^{n+1}}, \tag{35}$$

ergibt. Nun bilden wir die Normalfunktion von ω aus der Normalform (29)

$$\omega^*(e^v) = \omega_0^* + l^n \sum_{k=1}^{l-2} c_k'(1-e^v)^k, \tag{36}$$

woraus wegen (25), (26)

$$\begin{aligned} D_k\omega^*(e^v) &\equiv 0 \pmod{l^{n+1}} \quad (k = 1, 2, \ldots, t-1), \\ D_t\omega^*(e^v) &\equiv (-1)^t \cdot t! \cdot l^n \cdot c_t' \pmod{l^{n+1}} \end{aligned} \tag{37}$$

folgen. Aus (7) und (25) können wir aber auf $c_t' \equiv f_t \pmod{l}$ schließen, weshalb

$$D_t\omega^*(e^v) \equiv (-1)^t \cdot t! \cdot l^n \cdot f_t \pmod{l^{n+1}} \tag{38}$$

gilt. Die Kongruenzen (32), (35), (37) und (38) liefern den vollständigen Beweis des Hilfssatzes.

In den folgenden wird von ω nicht mehr vorausgesetzt, daß es in seiner Normalform bekannt ist. Es gilt dann der folgende

Hilfssatz 2. *Erfüllt die Zahl ω des Körpers $R(\zeta)$ die Kongruenz* (7), *so bestehen die folgenden Kongruenzen:*

a) *im Falle* $n = 0$:

$$D_k \log \omega(e^v) \equiv 0 \pmod{l} \quad (k = 1, 2, \ldots, t-1), \tag{39}$$

$$D_t \log \omega(e^v) \equiv (-1)^t \cdot \frac{t! \cdot f_t}{\omega_0} \pmod{l}, \tag{40}$$

$$f_0 \equiv \omega_0 \pmod{l};$$

b) *im Falle* $n > 0$:

$$D_{jl^y} \log \omega(e^v) \equiv 0 \pmod{l^{y+1}} \quad (y = 1, \ldots, n-1; i = 1, \ldots, l-2), \tag{41}$$

$$D_{kl^n} \log \omega(e^v) \equiv 0 \pmod{l^{n+1}} \quad (k = 1, 2, \ldots, t-1), \tag{42}$$

$$D_{tl^w} \log \omega(e^v) \equiv (-1)^t \cdot \frac{l^w \cdot t! \cdot f_t}{\omega_0} \pmod{l^{w+1}}, \tag{43}$$

wo w eine ganze rationale Zahl bezeichnet, $w \geqq n$, und

$$f_0 \equiv \omega_0 - \frac{l}{l-1} \cdot D_{l^{n(l-1)}}\omega(e^v) \pmod{l^{n+1}}. \tag{44}$$

Beweis: a) $n = 0$. Zufolge (2) hängen die verschiedenen Darstellungen der Zahl ω durch eine Gleichung

$$\omega = \omega^* + \xi \cdot g(\zeta) \tag{45}$$

zusammen, wo ξ eine ganze Zahl in $R(\zeta)$ ist. Diese kann in der Form

$$\xi = x_0 + \varphi\lambda$$

angenommen werden, wo φ ebenfalls eine ganze Zahl in $R(\zeta)$ und x_0 eine ganze rationale Zahl bedeutet. Hieraus folgen die Gleichungen

$$\omega_0 = \omega_0^* + l x_0, \tag{46}$$

$$\omega(e^r) = \omega^*(e^r) + x_0 \cdot g(e^v) + \varphi(e^r) \cdot [1 - e^{lr}] \tag{47}$$

und aus (46) die Kongruenz

$$\omega_0 \equiv \omega_0^* \pmod{l}. \tag{48}$$

Der Beweis für $n = 0$ ist hiermit erledigt, da (39), (40) aus (8), (9), (48) und der Kummer—Hilbertschen Relation[7])

$$D_k \log \omega(e^r) - D_k \log \omega^*(e^r) \pmod{l} \quad (k = 1, \ldots, l-2) \tag{49}$$

folgen.

b) $n > 0$. Nach dem oben schon erwähnten Kummerschen Satz ist[8])

$$D_{k,l^n} \log \omega(e^r) \equiv D_{k,l^n} \log \omega^*(e^r) \pmod{l^{n+1}} \tag{50}$$

für $l-1 \nmid k$. Die Kongruenz (41) folgt dann unmittelbar aus (32), (33) und (50). Wählt man ferner s_k in (10), (11) folgenderweise:

$$s_k = k \frac{l^n - 1}{l - 1} \qquad (k = 1, 2, \ldots, l-2), \tag{51}$$

so können (42) und (43) einfach mittels der Kongruenzen (10), (11), (48) und (50) bestätigt werden.

Wird der Operator $D_{l^n(l-1)}$ auf (47) angewendet, so erhält man

$$D_{l^n(l-1)}\omega(e^r) = D_{l^n(l-1)}\omega^*(e^r) + x_0 \sum_{i=1}^{l-1} i^{l^n(l-1)} + D_{l^n(l-1)}\varphi(e^v) \cdot [1 - e^{lr}]. \tag{52}$$

Nach (3) gilt

$$D_{l^n(l-1)}\omega^*(e^v) \equiv 0 \pmod{l^n},$$

ferner gilt wegen

$$D_{l^n(l-1)} e^{sr}[1 - e^{lr}] = s^{l^n(l-1)} - (l+s)^{l^n(l-1)} \equiv 0 \pmod{l^{n+1}}$$

auch

$$D_{l^n(l-1)}\varphi(e^r) \cdot [1 - e^{lr}] \equiv 0 \pmod{l^n}. \tag{53}$$

Hieraus und aus (52) folgt zunächst:

$$D_{l^n(l-1)}\omega(e^r) \equiv x_0(l-1) \pmod{l^n},$$

dann wegen (22) und (46) auch (44). Damit ist der Hilfssatz 2 vollständig bewiesen.

Diese Hilfssätze sind umkehrbar. So erhalten wir z. B. aus dem Hilfssatz 2 den folgenden, für unsere weiteren Forschungen wichtigen Satz:

Satz 1. *Ist ω eine zu l prime Zahl aus dem Körper $R(\zeta)$ und $\omega(e^v)$ eine gewisse, zu ω gehörige Funktion, für die die Kongruenzen*

(54) $$D_{in}\log\omega(e^v)\equiv 0 \pmod{l^{y+1}} \quad (y=1,\ldots,n-1;\ i=1,\ldots,l-2).$$

(55) $$D_{kl^n}\log\omega(e^v)\equiv 0 \pmod{l^{n+1}} \quad (k=1,\ldots,t-1).$$

(56) $$D_{ln}\log\omega(e^v)=q\equiv 0 \pmod{l^{n+1}} \quad 0<t<l-1$$

bestehen, so ist

$$\omega\equiv f_0+f_t\lambda^{n(l-1)+t} \pmod{l^{n(l-1)+t+1}},$$

wo f_0 und f_t zu l prime ganze rationale Zahlen sind und

(44) $$f_0\equiv\omega_0+\frac{l}{l-1}D_{ln(l-1)}\omega(e^v) \pmod{l^{n+1}}$$

(57) $$f_t\equiv(-1)^t\cdot\omega_0\cdot\frac{q}{l^n\cdot t!} \pmod{l}$$

gelten.

Beweis: Setzt man nämlich

$$\omega\equiv f_0'+f_{t'}'\lambda^{n'(l-1)+t'} \pmod{l^{n'(l-1)+t'+1}}, \quad 0<t'<l-1,$$

wo f_0' und $f_{t'}'$ zu l prime ganze rationale Zahlen sind, so gelten nach Hilfssatz 2 die Kongruenzen:

(58) $$D_{in}\log\omega(e^v)\equiv 0 \pmod{l^{n'+1}} \quad (y=1,\ldots,n'-1;\ i=1,\ldots,l-2),$$

(59) $$D_{in'}\log\omega(e^v)\equiv 0 \pmod{l^{n'+1}} \quad (i=1,\ldots,t'-1),$$

(60) $$D_{ln'}\log\omega(e^v)\equiv 0 \pmod{l^{n'+1}}.$$

Wäre nun $n'>n$, so steht (58) in einem Widerspruch mit (56). Ist $n'<n$, so stehen (54) und (60) im Widerspruch. Es ist also $n'=n$. Ist etwa $t'>t$, so widerspricht (56) mit (59). Umgekehrt, wenn $t'<t$, so ergeben (55) und (60) einen Widerspruch. Es muß also $t'=t$ sein.

Die Kongruenz (44) wurde bereits im Hilfssatze 2 bewiesen. Es bleibt also nur noch die Bestätigung von (57) übrig. Ist $n=0$, so erhält man (57) einfach aus (40). Ist $n>0$, so ist q durch l^n teilbar. Nach (32) und (34) hat man nämlich

$$D_{ln-1}\log\omega^*(e^v)\equiv D_{ln}\log\omega^*(e^v) \pmod{l^{n+1}} \quad 0<t<l-1,$$

woraus auf Grund von (50)

$$D_{ln-1}\log\omega(e^v)\equiv D_{ln}\log\omega(e^v) \pmod{l^n}$$

folgt; dies ergibt mit (54) und (56) zusammen $q\equiv 0 \pmod{l^n}$. Die Richtigkeit von (57) folgt also einfach aus den Kongruenzen (43), (48) und (56). Somit haben wir Satz 1 bewiesen.

In diesem Satz kann manchmal Schwierigkeiten verursachen, daß man zur Bestimmung von f_0 gemäß (44) auch die Funktion $\omega(e^v)$ kennen muß,

die, wie auch $\log \omega(e^v)$, nicht immer in brauchbarer Form zur Verfügung steht. Die Kenntnis dieser Funktion ist überflüssig, wenn die Bedingungen des nächsten Satzes erfüllt sind:

Satz 2. *Ist ω eine zu l prime Zahl des Körpers $R(\zeta)$, welche mit einer rationalen ganzen Zahl nach dem Modul l^n kongruent ist und bezeichnet $\omega(e^v)$ eine beliebige Funktion von ω, $\omega^*(e^v)$ die Normalfunktion von ω, so ist zu*

$$\omega_0 \equiv \omega_0^* \pmod{l^{n+1}} \tag{61}$$

notwendig und hinreichend, daß

$$D_{l^{n(l-1)}} \log \omega(e^v) \equiv 0 \pmod{l^n} \tag{62}$$

ist.

Beweis: Wir nehmen $n > 0$ an, weil (61) für $n = 0$ wegen (48) trivial erfüllt ist. Aus (45) folgt

$$\omega(e^v) = \omega^*(e^v) + \xi(e^v) \cdot g(e^v), \tag{63}$$

also auch

$$D_{l^{n(l-1)}} \log \omega(e^v) \equiv \sum_{j=1}^{m} (-1)^{j-1} \cdot \frac{1}{j} \cdot D_{l^{n(l-1)}} \left[\frac{\omega^*(e^v) - \omega_0^* + \xi(e^v) \cdot g(e^v)}{\omega_0} \right]^j \pmod{l^n}, \tag{64}$$

wobei die Zahl m nach Lemma C meiner zitierten Arbeit[10]) endlich ist, weil die hierzu notwendige Bedingung $\omega_0 \equiv \omega_0^* \pmod{l}$ erfüllt ist.

Nach (29) ist $[\omega^*(e^v) - \omega_0^*]$ durch l^n teilbar; (64) vereinfacht sich also nach dem Modul l^n:

$$D_{l^{n(l-1)}} \log \omega(e^v) \equiv \sum_{j=1}^{m} (-1)^{j-1} \cdot \frac{1}{j \cdot \omega_0^{*j}} D_{l^{n(l-1)}} \xi^j(e^v) \cdot g^j(e^v) \pmod{l^n}.$$

Wird die Zahl ξ wieder in der Form $\xi = x_0 + \varphi\lambda$ geschrieben, wo x_0 eine ganze rationale Zahl und φ eine Zahl in $R(\zeta)$ ist, so folgt

$$\xi^j(e^v) \cdot g^j(e^v) \equiv x_0^j \cdot g^j(e^v) + (1 - e^{le}) \cdot H(e^v),$$

wo $H(e^v)$ ein ganzzahliges Polynom in e^v bezeichnet. Mit Hilfe von (53) wird also ferner

$$D_{l^{n(l-1)}} \log \omega(e^v) \equiv \sum_{j=1}^{m} (-1)^{j-1} \cdot \frac{1}{j \cdot \omega_0^{*j}} D_{l^{n(l-1)}} x_0^j \cdot g^j(e^v) \pmod{l^n}.$$

Schreibt man $g'(e^v)$ für $\frac{dg(e^v)}{dv}$, so folgt aus der obigen Kongruenz

$$D_{l^{n(l-1)}} \log \omega(e^v) \equiv D_{l^{n(l-1)}} \frac{x_0}{\omega_0} g(e^v) + \sum_{j=2}^{m} (-1)^{j-1} \frac{x_0^j}{\omega_0^{*j}} D_{l^{n(l-1)-1}} g^{j-1}(e^v) \cdot g'(e^v) \pmod{l^n}. \tag{65}$$

[10]) A. a. O. [8]), Lemma C, S. 207.

Nach Lemma D meiner zitierten Arbeit[11]) ist jedes Glied nach dem Summenzeichen durch l teilbar. Man kann also mit Rücksicht auf

$$D_{l^n(l-1)}g(e^r) \equiv l-1 \pmod{l^n}$$

schreiben:

$$D_{l^n(l-1)} \log \omega(e^r) \equiv \frac{(l-1)x_0}{\omega_0^*} + x_0^2 \cdot l \cdot Q \pmod{l^n}, \tag{66}$$

wo Q eine ganze, bzw. eine solche gebrochene rationale Zahl ist, deren Nenner prim zu l ist.

Wir zeigen zuerst, daß (62) eine notwendige Bedingung zum Erfülltsein von (61) ist. Aus (46) und (61) folgt

$$x_0 \equiv 0 \pmod{l^n},$$

und wenn man dies in (66) einsetzt, so folgt (62).

Das Bestehen von (62) ist auch hinreichend für (61). Aus (62) und (66) folgt nämlich

$$x_0 \left[\frac{l-1}{\omega_0^*} + l \cdot x_0 \cdot Q \right] \equiv 0 \pmod{l^n}, \tag{67}$$

und da der Ausdruck in den Klammern nach der obigen Feststellung bezüglich Q prim zu l ist, ist die einzige Lösung von (67)

$$x_0 \equiv 0 \pmod{l^n};$$

setzt man dieses Ergebnis in (46), so erhält man (61).

(Eingegangen am 7. April 1952.)

[11]) A. a. O. [8]), Lemma D S. 208.