ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

416

ÜBER DEN ERSTEN FAKTOR DER KLASSENZAHL DES KREISKÖRPERS

VON

TAUNO METSÄNKYLÄ

HELSINKI 1967
SUOMALAINEN TIEDEAKATEMIA

doi:10.5186/aasfm.1968.416

Am 10 November 1967 vorgelegt von P. J. Myrberg und K. Inkeri

KESKUSKIRJAPAINO
HELSINKI 1967

Vorwort

Die vorliegende Dissertation ist unter der Leitung von Herrn Professor Dr. K. Inkeri entstanden. Für seinen anregenden Unterricht sowie für seine wertvollen Hinweise und Ratschläge, die mir beim Fortschreiten dieser Arbeit zuteil geworden sind, bin ich ihm zutiefst dankbar.

Mein aufrichtiger Dank gilt auch Herrn Dr. T. Lepistö für sein dieser Untersuchung entgegengebrachtes stetes Interesse und für eine Reihe nützlicher Bemerkungen, sowie Herrn Professor Dr. S. Hyyrö für einleuchtende Gespräche betreffend einige Probleme dieser Arbeit. Desgleichen danke ich bei dieser Gelegenheit Herrn Professor Dr. A. Tietäväinen, meinem nächsten begeisternden Vorbild, und allen meinen Kollegen, die beim Schaffen einer für Forschungsarbeit günstigen Atmosphäre mitgewirkt haben.

Für die sprachliche Durchsicht meines Manuskriptes bin ich Herrn Dr. B. Assmuth zu bestem Dank verpflichtet.

Ferner danke ich dem Wihuri-Fonds für die mir bewilligte geldliche Unterstützung sowie der Finnischen Akademie der Wissenschaften für die Aufnahme meiner Arbeit in ihre Annalen.

Turku, im November 1967

Tauno Metsänkylä

Inhaltsverzeichnis

Einleitung

1. Es sei $k(\zeta)$ der Körper, kurz der m-te Kreiskörper genannt, der durch Adjungieren einer primitiven m-ten Einheitswurzel ζ zum Körper der rationalen Zahlen entsteht. Wir nehmen an, dass $m(>1)$ entweder ungerade oder durch 4 teilbar ist; bekanntlich bedeutet dies keine Beschränkung beim Betrachten aller Kreiskörper.

Die Klassenzahl $H(m)$ von $k(\zeta)$ gestattet die Zerlegung

$$H(m) = H_1(m)H_2(m) ,$$

wobei die Faktoren der erste bzw. zweite Faktor der Klassenzahl genannt sind. In der vorliegenden Arbeit betrachten wir den ersten Faktor $H_1(m)$, und zwar seine verschiedene Darstellungen sowie einige seiner Teilbarkeitseigenschaften.

2. Bekanntlich ist $2H_1(m)$ eine ganzrationale Zahl, und wenn m eine Primzahlpotenz p^h ist, so gilt dasselbe sogar für $H_1(p^h)$ (s. [13]). Der explizite Ausdruck von $H_1(m)$, der schon von KUMMER hergeleitet wurde ([14], [16]; s. die Formel (1.2) unten), stellt aber diese Eigenschaft nicht direkt heraus, und es ist erst HASSE [6] gelungen, im allgemeinen Fall die Ganzzahligkeit von $2H_1(m)$ von diesem Ausdruck ausgehend nachzuweisen (vgl. auch [16]). Wir werden im ersten Kapitel dieser Arbeit den betreffenden Ausdruck derart umformen, dass sich eine solche Produktdarstellung für $2H_1(m)$ ergibt, deren sämtliche Faktoren Determinanten mit ganzrationalen Elementen sind. Nebenbei erhalten wir für $H_1(m)$ eine Darstellung, die sich als besonders geeignet für Teilbarkeitsbetrachtungen erweist. — Es sei erwähnt, dass früher »ganze» Determinantendarstellungen für $H_1(m)$ in den Spezialfällen $m = p(>2)$ und $m = p^h$ $(p \geqq 2)$ hergeleitet worden sind ([1], [11], [17], [18]).

Wir behandeln auch kurz die Darstellung von $H_1(p^h m)$ mittels $H_1(p^{h-1}m)$, wobei p eine nicht in m enthaltene Primzahl bedeutet. Aus unseren Ergebnissen geht u.a. die bekannte Tatsache ([6], Satz 41) hervor, dass unter der Annahme $m_1 | m_2$ der Quotient $H_1(m_2)/H_1(m_1)$ ganz ist, möglicherweise mit Ausnahme der Fälle, wo m_1 eine Primzahlpotenz und m_2 eine zusammengesetzte Zahl ist. (Doch setzen wir hier die von WEBER [23]

und WESTLUND [24] bewiesene Ganzzahligkeit von $H_1(p^h)/H_1(p^{h-1})$ als bekannt voraus.)

3. Im zweiten Kapitel betrachten wir die Teilbarkeit von $H_1(m)$ namentlich durch die Primteiler von m. Von den bekannten Ergebnissen dieser Art sei vor allem das KUMMERsche Kriterium für die Teilbarkeit von $H_1(p)$ durch p genannt. Ausserdem haben u.a. VANDIVER [22] (s. auch [7]), FURTWÄNGLER [3], POLLACZEK [21] und MORISHIMA [19], [20] die Teilbarkeit von $H_1(p)$ oder allgemeiner $H_1(p^h)$ durch p behandelt.

Durch Verallgemeinerung einer Methode von [21] können wir zuerst ein allgemeines Ergebnis (Satz 6) über die Teilbarkeit von $H_1(p^h m)$ durch p herleiten. Dann beschränken wir uns auf den Fall, wo m die Primteiler p und q mit $q \equiv 1 \pmod{p}$ enthält, und beweisen weitere Teilbarkeitssätze, die hauptsächlich auf einige Teilbarkeitseigenschaften gewisser rationaler Summen (s. § 10) begründet sind.

Unsere Ergebnisse gestatten es, m auf verschiedene Weise so zu wählen, dass $H(m)$ durch eine beliebig gegebene ganze Zahl n teilbar wird. Hinsichtlich ungerader n hat FRÖHLICH [2] diese Frage ganz anders behandelt; im Anschluss daran hat er gezeigt, dass unter den Voraussetzungen $p > 2$, $q \equiv 1 \pmod{p^2}$ die Klassenzahl des pq-ten Kreiskörpers durch p teilbar ist (vgl. unsere Sätze 8 und 9).

In diesem Zusammenhang seien noch die Untersuchungen von GUT [5] und KLEBOTH [12] angeführt. Nach GUT ist $H_1(4q)$ (q eine ungerade Primzahl) dann und nur dann durch q teilbar, wenn gewisse Bedingungen, die Bernoullische und Eulersche Zahlen betreffen, erfüllt sind. Aus den Betrachtungen KLEBOTHS folgt ein ähnliches Kriterium für die Teilbarkeit von $H_1(3q)$ (in [12] allerdings $H_1(6q)$) durch q. Unser Satz 10 zeigt, dass sich hierbei die Situation völlig ändert, wenn q durch q^k mit $k > 1$ ersetzt wird: eine hinreichende Bedingung dafür, dass $H_1(4q^k)$ bzw. $H_1(3q^k)$ durch q teilbar ist, lautet einfach $q \equiv 1 \pmod 4$ bzw. $\pmod 3$.

ERSTES KAPITEL. VERSCHIEDENE DARSTELLUNGEN DES ERSTEN FAKTORS DER KLASSENZAHL

§ 1. Die Ausgangsformel

4. Wir betrachten ungerade Charaktere mit dem Erklärungsmodul m (für Charaktere s. z.B. [8], § 13). Für jeden Teiler k von m sei P_k die Menge aller ungeraden Charaktere χ, die primitiv (mod k) sind, und sei ferner

$$P = \bigcup_{k \mid m} P_k .$$

Fasst man hier alle solche Werte von k zusammen, die genau dieselben verschiedenen Primteiler enthalten, so ergibt sich

$$P = \bigcup_{a \mid m} Q_a \tag{1.1}$$

mit

$$Q_a = \bigcup_{k \mid a} P_k ,$$

wobei a und k alle Teiler von m bzw. a durchlaufen, die die Bedingungen

$$(a, m/a) = 1 \quad \text{bzw.} \quad \omega(k) = \omega(a)$$

erfüllen. (Wie üblich bedeutet $\omega(n)$ die Anzahl der verschiedenen Primteiler von n.)

Die durch (1.1) aufgestellte Dekomposition der Charaktere $\chi \in P$ in Abteilungen Q_a hat folgende Eigenschaft, die später für uns wichtig ist: Zwei Charaktere χ_1 und χ_2 aus P gehören zu derselben Abteilung Q_a dann und nur dann, wenn $\chi_1(l)$ und $\chi_2(l)$ genau für dieselben Argumentwerte l verschwinden.

5. Der erste Faktor der Klassenzahl des m-ten Kreiskörpers lässt sich in der Form

$$H_1(m) = (2m)^{1-\varphi(m)/2}\, e(m) \prod_{\chi \in P} \sum_{l=1}^{m} (-\chi(l) l) \tag{1.2}$$

darstellen, wobei $\varphi(m)$ die Eulersche Funktion bedeutet und $e(m)$ gleich 1 für ungerades m und $\frac{1}{2}$ für gerades m ist ([16], [9], [4]). Eine zweite, seltener angewandte Form dieses Ausdrucks lautet

$$H_1(m) = 2me(m) \prod_{k \mid m} \prod_{\chi \in P_k} (2k)^{-1} \sum_{l=1}^{k} (-\chi(l)l) \tag{1.3}$$

(vgl. [6], S. 11). Um die Übereinstimmung dieser beiden Ausdrücke einzusehen, muss man den folgenden leicht beweisbaren Hilfssatz benutzen und überdies bemerken, dass die Anzahl der Charaktere χ von P gleich $\frac{1}{2}\varphi(m)$ ist.

Hilfssatz 1. *Ist χ ein von dem Hauptcharakter verschiedener Charakter* (mod k_1) *und gilt $k_1 \mid k_2$, so ist*

$$k_1 \sum_{l=1}^{k_2} \chi(l)l = k_2 \sum_{l=1}^{k_1} \chi(l)l \,.$$

Für die folgenden Betrachtungen stellen wir $H_1(m)$ in einer neuen Gestalt dar, und zwar beweisen wir den

Satz 1. *Es gilt*

$$H_1(m) = 2^{1-\omega(m)} \prod_{p^h \| m} H_1(p^h) \prod_{a}{}' T(a) \tag{1.4}$$

mit

$$T(a) = \prod_{\chi \in Q_a} (2a)^{-1} \sum_{l=1}^{a} (-\chi(l)l) \,, \tag{1.5}$$

wobei p eine Primzahl bedeutet und das mit einem Strich bezeichnete Produkt über alle Teiler a von m zu erstrecken ist, die den Bedingungen $(a, m/a) = 1$ und $\omega(a) > 1$ genügen. (Die Bezeichnung $p^h \| m$ bedeutet, dass m durch p^h, aber nicht durch p^{h+1} teilbar ist.)

Beweis. Beachtet man, dass alle $\chi \in Q_a$ Charaktere (mod a) sind, so kann man offenbar $H_1(m)$ parallel zu (1.3) in der Form

$$H_1(m) = 2me(m) \prod_{a} \prod_{\chi \in Q_a} (2a)^{-1} \sum_{l=1}^{a} (-\chi(l)l)$$

schreiben, wobei sich das äussere Produkt über alle Teiler a von m mit der Eigenschaft $(a, m/a) = 1$ erstreckt. Wenn man die Bezeichnungen von Satz 1 einführt, erhält man also

$$H_1(m) = 2me(m) \prod_{p^h \| m} T(p^h) \prod_{a}{}' T(a) \,.$$

Speziell gilt

$$H_1(p^h) = 2p^h e(p^h) T(p^h) ,$$

und aus beiden letztgenannten Formeln folgt wirklich die behauptete Beziehung (1.4).

§ 2. Umformung des Ausdrucks von $T(a)$

6. Die in (1.4) auftretenden Faktoren $T(a)$ sollen im folgenden wiederum in Faktoren zerlegt werden. Zuerst werden wir aber die Ausdrücke dieser $T(a)$ in einer neuen Gestalt schreiben.

Wir nehmen an, dass der Wert von a in $T(a)$ gleich

$$a = 2^h p_1^{h_1} \dots p_c^{h_c}$$

ist, wobei $p_1, \dots, p_c$ verschiedene ungerade Primteiler von m sind und ferner, wie aus der Bedingung $(a, m/a) = 1$ hervorgeht, $2^h \| m$ und $p_j^{h_j} \| m$ $(j = 1, \dots, c)$ gilt. Um den allgemeinsten Fall zu behandeln, müssen wir hier a als gerade und somit $h \geqq 2$ annehmen; wegen $\omega(a) > 1$ muss dann auch $c \geqq 1$ vorausgesetzt werden. — Es ist jedoch zu bemerken, dass die folgenden Ausführungen mit leicht ersichtlichen Veränderungen auch für das ungerade $a = p_1^{h_1} \dots p_c^{h_c}$ (mit $c \geqq 2$) gelten, sodass keine besondere Behandlung in diesem Fall nötig ist.

Zur Abkürzung bezeichnen wir in diesem Kapitel allgemein mit $\mathbf{x}_l$ die Zahlenfolge $x_1, x_2, \dots, x_l$. Wir setzen weiter

$$s = 2^{h-2}, \quad Z = \exp(2\pi i/s) ,$$

$$\varphi_j = \varphi(p_j^{h_j}) , \quad s_j = \tfrac{1}{2}\varphi_j, \quad Z_j = \exp(2\pi i/\varphi_j) \quad (j = 1, \dots, c)$$

und bezeichnen mit r_j eine primitive Wurzel (mod $p_j^{h_j}$) $(j = 1, \dots, c)$. Es sei noch $R_a(\bar{n}, n, \mathbf{n}_c)$ die eindeutige natürliche Zahl $< a$, die den Kongruenzen

$$R_a(\bar{n}, n, \mathbf{n}_c) \equiv \begin{cases} (-1)^{\bar{n}} 5^n \pmod{2^h} , \\ r_j^{n_j} \pmod{p_j^{h_j}} \quad (j = 1, \dots, c) \end{cases} \tag{2.1}$$

genügt. Ist kein Missverständnis möglich, werden wir oft $R(\bar{n}, n, \mathbf{n}_c)$ statt $R_a(\bar{n}, n, \mathbf{n}_c)$ schreiben.

Aus der Definition von $R(\bar{n}, n, \mathbf{n}_c)$ folgt leicht der folgende Hilfssatz, der später häufig angewandt wird.

Hilfssatz 2. *Ist* $\bar{n} - \bar{n}' = \pm 1$ *und* $n_j - n_j' = \pm s_j$ $(j = 1, \dots, c)$, *so gilt die Beziehung*

$$R(\bar{n}', n, \mathbf{n}_c') = a - R(\bar{n}, n, \mathbf{n}_c) .$$

7. Die Charaktermenge Q_a besteht aus allen ungeraden Charakteren (mod a), deren Führer genau die Primteiler $2, p_1, \ldots, p_c$ enthalten. Für jedes χ aus Q_a gilt mithin

$$\chi(l) = \begin{cases} 0 \text{ für } (l,a) > 1\,, \\ (-1)^{\bar{k}\bar{n}} Z^{kn} Z_1^{k_1 n_1} \ldots Z_c^{k_c n_c} \text{ für } (l,a) = 1\,, \end{cases} \tag{2.2}$$

wobei $\bar{n}, n, \mathbf{n}_c$ durch die Kongruenzen

$$l \equiv (-1)^{\bar{n}} 5^n \pmod{2^h}, \quad l \equiv r_j^{n_j} \pmod{p_j^{h_j}} \quad (j = 1, \ldots, c)$$

bestimmt sind und $\bar{k}, k, \mathbf{k}_c$ die Bedingungen

$$\begin{cases} 0 \leqq \bar{k} \leqq 1, \quad 0 \leqq k \leqq s-1; \quad 1 \leqq \bar{k} + k\,; \\ 1 \leqq k_j \leqq \varphi_j - 1 \quad (j = 1, \ldots, c)\,; \\ \bar{k} + k_1 + \ldots + k_c \text{ ungerade} \end{cases} \tag{2.3}$$

erfüllen. Man erhält genau alle χ von Q_a, indem man $\bar{k}, k, \mathbf{k}_c$ alle Werte unter den Bedingungen (2.3) durchlaufen lässt.

Wir setzen nun identisch

$$F(\bar{x}, x, \mathbf{x}_c) = \sum_{\bar{n}=0}^{1} \sum_{n=0}^{s-1} \sum_{n_1=0}^{\varphi_1-1} \ldots \sum_{n_c=0}^{\varphi_c-1} R_a(\bar{n}, n, \mathbf{n}_c) \bar{x}^{\bar{n}} x^n x_1^{n_1} \ldots x_c^{n_c}\,. \tag{2.4}$$

Angenommen, dass χ zu Q_a gehört, besteht dann die Beziehung

$$\begin{aligned} \sum_{l=1}^{a} \chi(l) l &= \sum_{\substack{l=1 \\ (l,a)=1}}^{a} l(-1)^{\bar{k}\bar{n}} Z^{kn} Z_1^{k_1 n_1} \ldots Z_c^{k_c n_c} \\ &= F((-1)^{\bar{k}}, Z^k, Z_1^{k_1}, \ldots, Z_c^{k_c})\,. \end{aligned} \tag{2.5}$$

Daher gilt nach (1.5)

$$T(a) = \prod_{\bar{k}, k, \mathbf{k}_c} (-2a)^{-1} F((-1)^{\bar{k}}, Z^k, Z_1^{k_1}, \ldots, Z_c^{k_c})\,, \tag{2.6}$$

wobei das Produkt über alle Werte von $\bar{k}, k, \mathbf{k}_c$ unter den Bedingungen (2.3) zu erstrecken ist.

8. Es sei Y_c die Menge aller Zahlenfolgen $w = (d, \mathbf{d}_c)$, wobei die Zahlen $d, d_1, \ldots, d_c$ gleich 0 oder 1 sind und ausserdem $d + d_1 + \ldots + d_c$ ungerade ist. Dann gilt der folgende

Satz 2. *Die in Satz 1 genannten Faktoren $T(a)$ von $H_1(m)$ besitzen (im Fall eines geraden $a = 2^h p_1^{h_1} \ldots p_c^{h_c}$) die Zerlegung*

$$T(a) = \prod_{w \in Y_c} T_w(a) \tag{2.7}$$

mit

$$T_w(a) = \prod\!\!\prod_w (-2a)^{-1} F((-1)^{\bar{k}}, Z^k, Z_{1^1}^k, \ldots, Z_c^{k_c}), \tag{2.8}$$

wobei F *durch* (2.4) *definiert ist und das Produkt* Π_w *sich über folgende, durch* $w = (d, \mathbf{d}_c)$ *bestimmte Werte von* $\bar{k}, k, \mathbf{k}_c$ *erstreckt:*

$$\begin{cases} \bar{k} = 1 \text{ und } k = 0, 1, \ldots, s-1, \text{ wenn } d = 1, \\ \bar{k} = 0 \text{ und } k = 1, 2, \ldots, s-1, \text{ wenn } d = 0; \\ k_j = 1, 3, \ldots, \varphi_j - 1, \text{ wenn } d_j = 1 \ (j = 1, \ldots, c), \\ k_j = 2, 4, \ldots, \varphi_j - 2, \text{ wenn } d_j = 0 \ (j = 1, \ldots, c). \end{cases} \tag{2.9}$$

Beweis. Wir vergleichen die in (2.6) und (2.8) auftretenden Faktoren $F' = (-2a)^{-1}F$ miteinander. Man sieht, dass bei Π_w jede Kombination der Werte von $\bar{k}, k, \mathbf{k}_c$ die Bedingungen (2.3) erfüllt, sodass die Faktoren F' von $T_w(a)$ auch Faktoren von $T(a)$ sind. Umgekehrt tritt jeder Faktor F' von $T(a)$ in genau einem $T_w(a)$ auf; um dieses $T_w(a)$ zu finden, muss man $w = (d, \mathbf{d}_c)$ so wählen, dass

$$d = \bar{k}, \quad d_j = \begin{cases} 1 \text{ für ungerades } k_j, \\ 0 \text{ für gerades } k_j \end{cases}$$

gilt. Somit ist der Satz bewiesen.

Anmerkung 1. Im Fall $2^2 \| a$ ist $T_w(a)$ für alle $w = (0, \mathbf{d}_c)$ wegen $s = 1$ ein leeres Produkt (vgl. (2.9)) und muss gleich 1 gesetzt werden. Dasselbe gilt im Fall $3 \| a$, also wenn etwa $p_{1^1}^{h_{1^1}} = 3$ ist, für alle $T_w(a)$ mit $w = (d, 0, d_2, \ldots, d_c)$.

Anmerkung 2. Hat a den ungeraden Wert $p_{1^1}^{h_{1^1}} \ldots p_c^{h_c}$, so müssen vorhin nur die von dem Faktor 2 herrührenden Bezeichnungen überall weggelassen werden. Somit setzt man z.B.

$$F(\mathbf{x}_c) = \sum_{n_1=0}^{\varphi_1 - 1} \ldots \sum_{n_c=0}^{\varphi_c - 1} R_a(\mathbf{n}_c) x_{1^1}^{n_{1^1}} \ldots x_c^{n_c} \tag{2.4'}$$

und versteht unter Y_c die Menge sämtlicher aus Nullen und Einsen gebildeten Folgen $w = (\mathbf{d}_c)$ mit ungeradem $d_1 + \ldots + d_c$. Dann besteht die Aussage (2.7) von Satz 2 mit

$$T_w(a) = \prod\!\!\prod_w (-2a)^{-1} F(Z_{1^1}^k, \ldots, Z_c^{k_c}), \tag{2.8'}$$

wobei das Produkt über die aus (2.9) hervorgehenden Werte von $\mathbf{k}_c$ zu erstrecken ist.

§ 3. Ganzrationalität von $T_w(a)$

9. Wir beweisen den folgenden

Satz 3. *Die durch* (2.8) (*und* (2.8′)) *definierten Zahlen* $T_w(a)$ *sind rational und ganz.*

Um die Rationalität von $T_w(a)$ einzusehen, muss man nur folgendes bemerken. Jede der Zahlen k_j im Produkt Π_w durchläuft entweder die Werte $1, 3, \ldots, \varphi_j - 1$ oder die Werte $2, 4, \ldots, \varphi_j - 2$. Im ersteren Fall durchläuft $Z_j^{k_j}$ die Wurzeln der Gleichung

$$x^{s_j} + 1 = 0 ,$$

im letzteren Fall die Wurzeln der Gleichung

$$x^{s_j-1} + x^{s_j-2} + \ldots + x + 1 = 0 .$$

Das Entsprechende gilt für k und Z^k: nimmt k in Π_w die Werte $0, 1, \ldots, s-1$ an, so durchläuft Z^k die Wurzeln der Gleichung

$$x^s - 1 = 0 ,$$

und beim Weglassen des Wertes 0 für k wird diese Gleichung durch

$$x^{s-1} + x^{s-2} + \ldots + x + 1 = 0$$

ersetzt. Weil alle hier genannten Gleichungen rationale Koeffizienten haben, ist das betreffende Produkt Π_w rational.

Wir bezeichnen für das folgende mit λ bzw. λ_j $(j = 1, \ldots, c)$ die Anzahl der Werte, die k bzw. k_j in (2.8) durchlaufen. Dass die Zahlen $T_w(a)$ ganz sind, ergibt sich nun aus

Hilfssatz 3. *Für jedes* F *aus* (2.8) *gilt*

$$F((-1)^{\bar{k}}, Z^k, Z_1^k, \ldots, Z_c^k) = -2aG_w(Z^k, Z_1^k, \ldots, Z_c^k) \tag{3.1}$$

mit

$$G_w(x, \mathbf{x}_c) = \sum_{n=0}^{\lambda-1} \sum_{n_1=0}^{\lambda_1-1} \ldots \sum_{n_c=0}^{\lambda_c-1} P(n, \mathbf{n}_c) x^n x_1^{n_1} \ldots x_c^{n_c} , \tag{3.2}$$

wobei die Koeffizienten $P(n, \mathbf{n}_c)$ *ganze rationale Zahlen sind.* (*Das Entsprechende gilt auch für die* F *aus* (2.8′).)

Satz 3 ist somit bewiesen, falls Hilfssatz 3 richtig ist.

10. Zum Beweis von Hilfssatz 3 können wir ohne Beschränkung annehmen, dass w in (2.8) die Form $(d, 1, \ldots, 1, 0, \ldots, 0)$ hat, also etwa

$$d_j = \begin{cases} 1 \text{ für } j = 1, \ldots, b\,, \\ 0 \text{ für } j = b+1, \ldots, c \end{cases}$$

mit $0 \leqq b \leqq c$ gilt. Somit hat man zwei Fälle, der eine mit $d = 1$ und der andere mit $d = 0$, die jedoch gleichzeitig behandelt werden können. (Was den Fall des ungeraden a angeht, wobei kein d existiert, so ist er genau dem Fall $d = 0$ analog.)

Aus der Definition von w folgt, dass die Zahl b gerade im Fall $d = 1$ und ungerade im Fall $d = 0$ ist. Ausserdem ist nach (2.9)

$$\lambda_j = \begin{cases} s_j \text{ für } j = 1, \ldots, b\,, \\ s_j - 1 \text{ für } j = b+1, \ldots, c\,, \end{cases} \tag{3.3}$$

$$\lambda = \begin{cases} s\,, \text{ wenn } d = 1\,, \\ s - 1\,, \text{ wenn } d = 0\,. \end{cases} \tag{3.4}$$

Wir betrachten ein beliebiges in (2.8) auftretendes

$$F = F((-1)^{\bar{k}}, Z^k, Z_1^k, \ldots, Z_c^k)$$

und setzen darin zur Abkürzung

$$\bar{x} = (-1)^{\bar{k}}\,, \quad x = Z^k\,, \quad x_j = Z_j^k \quad (j = 1, \ldots, c)\,.$$

Wie man aus dem vorigen Rationalitätsbeweis von $T_w(a)$ sieht, gilt dann

$$x_j^{s_j} = -1 \quad \text{für } j = 1, \ldots, b\,, \tag{3.5}$$

$$x_j^{s_j-1} = -1 - x_j - \ldots - x_j^{s_j-2} \quad \text{für } j = b+1, \ldots, c\,, \tag{3.6}$$

$$x^s = 1\,, \text{ wenn } d = 1\,, \tag{3.7}$$

$$x^{s-1} = -1 - x - \ldots - x^{s-2}\,, \text{ wenn } d = 0\,. \tag{3.8}$$

Der Ausdruck von F ist der Form nach eine Summe, wie aus (2.4) hervorgeht. Wendet man darauf die Beziehungen (3.5), (3.6) und (3.8) an sowie summiert man über $\bar{n}$, so ergibt sich

$$F = \sum_{n=0}^{\lambda-1} \sum_{n_1=0}^{\lambda_1-1} \ldots \sum_{n_c=0}^{\lambda_c-1} S(n, \mathfrak{n}_c) x^n x_1^{n_1} \ldots x_c^{n_c} \tag{3.9}$$

(vgl. (3.3) und (3.4)) mit ganzen rationalen Koeffizienten $S(n, \mathfrak{n}_c)$. Daraus erkennt man die Richtigkeit von Hilfssatz 3, indem man zeigt, dass die Zahlen $S(n, \mathfrak{n}_c)$ durch $2a$ teilbar sind. Um dies wiederum zeigen zu können, muss man das genannte Verfahren im einzelnen diskutieren.

11. Wir gehen also von der Formel (2.4) aus. Unter Anwendung von (3.5) sowie der Beziehung $x_j^{s_j} = 1$ für $j = b+1, \ldots, c$ gelangen wir zuerst zum Ausdruck

$$F = \sum_{\bar{n}=0}^{1} \sum_{n=0}^{s-1} \sum_{n_1=0}^{s_1-1} \cdots \sum_{n_c=0}^{s_c-1} Q(\bar{n}, n, \mathfrak{n}_c) \bar{x}^{\bar{n}} x^n x_1^{n_1} \ldots x_c^{n_c}$$

mit

$$Q(\bar{n}, n, \mathfrak{n}_c) = \sum_{\mathfrak{t}_c} [\pm R(\bar{n}, n, \mathfrak{t}_c)], \tag{3.10}$$

wobei über $t_j = n_j, n_j + s_j$ für jedes $j = 1, \ldots, c$ zu summieren ist. Ausserdem ist bei jedem Summanden das Plus- oder Minuszeichen zu wählen, je nachdem ob darin eine gerade oder ungerade Anzahl von $t_1, \ldots, t_b$ den grösseren Wert hat. Wird nun in F die Summierung über $\bar{n}$ durchgeführt, so ergibt sich

$$F = \sum_{n=0}^{s-1} \sum_{n_1=0}^{s_1-1} \cdots \sum_{n_c=0}^{s_c-1} \bar{Q}(n, \mathfrak{n}_c) x^n x_1^{n_1} \ldots x_c^{n_c}, \tag{3.11}$$

wobei wegen $\bar{x} = (-1)^{\bar{k}}$

$$\bar{Q}(n, \mathfrak{n}_c) = \sum_{\bar{n}=0}^{1} \sum_{\mathfrak{t}_c} [\pm R(\bar{n}, n, \mathfrak{t}_c)]$$

gilt. Hierin sind die Vorzeichen im Fall $d(= \bar{k}) = 0$ ebenso wie in (3.10) bestimmt, während im Fall $d = 1$ genau diejenigen $R(\bar{n}, n, \mathfrak{t}_c)$ mit dem Pluszeichen zu versehen sind, in denen eine gerade Anzahl von $\bar{n}, t_1, \ldots, t_b$ den grösseren Wert hat.

Die Glieder der vorigen Summe lassen sich so in Paare

$$\pm R(\bar{n}, n, \mathfrak{t}_c), \quad \pm R(\bar{n}', n, \mathfrak{t}_c') \tag{3.12}$$

zusammenfassen, dass jedesmal $\bar{n} \neq \bar{n}'$ und $t_j \neq t_j'$ $(j = 1, \ldots, c)$ gilt. Beachtet man, dass b im Fall $d = 0$ ungerade und im Fall $d = 1$ gerade ist, so ersieht man aus den oben dargelegten Vorzeichenregeln, dass das eine Glied in (3.12) niemals dasselbe Vorzeichen besitzt wie das andere. Mithin können wir annehmen, dass in (3.12) links das obere und rechts das untere Zeichen gilt.

Nach Hilfssatz 2 ist nun $R(\bar{n}', n, \mathfrak{t}_c') = a - R(\bar{n}, n, \mathfrak{t}_c)$. Durch Addieren der Zahlen in jedem Paar (3.12) kommt man demnach zum Ergebnis

$$\bar{Q}(n, \mathfrak{n}_c) = \sum_{\bar{n}, \mathfrak{t}_c} [2 R(\bar{n}, n, \mathfrak{t}_c) - a], \tag{3.13}$$

wobei die Summation sich über $\bar{n} = 0, 1$ und $t_j = n_j, n_j + s_j$ $(j = 1, \ldots, c)$ erstreckt derart, dass die folgende Zusatzbedingung erfüllt ist: im Fall $d = 0$ hat eine gerade Anzahl von $t_1, \ldots, t_b$ gleichzeitig den grösseren Wert, während im Fall $d = 1$ dasselbe für $\bar{n}, t_1, \ldots, t_b$ gilt.

Anmerkung 3. Es gibt Fälle, wo die Indizes in der vorigen Summe nicht ihre beiden Werte annehmen, und zwar genau dann, wenn die genannte Zusatzbedingung nur e i n e n Index betrifft. (Ist in der Tat $b = 1$ im Fall $d = 0$, so kann t_1 nur den Wert n_1 annehmen, und ebenso nimmt $\bar{n}$ im Fall $d = 1$ und $b = 0$ nur den Wert 0 an.)

Anmerkung 4. Ist $a = p_1^{h_1} \ldots p_c^{h_c}$, so gilt

$$F(\mathbf{x}_c) = \sum_{n_1=0}^{s_1-1} \ldots \sum_{n_c=0}^{s_c-1} \bar{Q}(\mathbf{n}_c) x_1^{n_1} \ldots x_c^{n_c} \tag{3.11'}$$

mit

$$\bar{Q}(\mathbf{n}_c) = \sum_{\mathbf{t}_c} [2R(\mathbf{t}_c) - a], \tag{3.13'}$$

wobei die Summation über solche Wertkombinationen von $\mathbf{t}_c$ zu erstrecken ist, die eine gerade Anzahl der Werte $n_j + s_j$ $(1 \leqq j \leqq b)$ enthalten.

12. Falls $b < c$ gilt, muss man den erhaltenen Ausdruck (3.11) von F ferner mittels (3.6) reduzieren. Wendet man (3.6) zuerst für $j = c$ an, so schreibt sich (3.11) in der Form, bei der die letzte Summe über $n_c = 0, 1, \ldots, s_c - 2$ zu erstrecken ist und die Koeffizienten gleich

$$\bar{Q}(n, \mathbf{n}_c) - \bar{Q}(n, \mathbf{n}_{c-1}, s_c - 1)$$

sind. Nach (3.13) lassen sich diese Koeffizienten weiter in der Gestalt

$$\sum_{\bar{n}, \mathbf{t}_{c-1}} 2[R(\bar{n}, n, \mathbf{t}_{c-1}, n_c) + R(\bar{n}, n, \mathbf{t}_{c-1}, n_c + s_c) - R(\bar{n}, n, \mathbf{t}_{c-1}, s_c - 1) - R(\bar{n}, n, \mathbf{t}_{c-1}, 2s_c - 1)]$$

darstellen. Nun ersieht man mit Hilfe von (2.1), dass der hierbei in den eckigen Klammern gesetzte Ausdruck $\equiv 0 \pmod{a}$ ist, sodass die betreffenden Koeffizienten durch $2a$ teilbar sind. Folglich enthalten auch die Koeffizienten $S(n, \mathbf{n}_c)$ in (3.9) den Teiler $2a$, wie zu zeigen war.

Es muss noch der Fall $b = c$ erledigt werden. In diesem Fall kann der Ausdruck (3.11) nur mittels (3.8) reduziert werden und bleibt also unverändert, wenn $d = 1$ gilt.

Ist $b = c = 1$, so gilt $d = 0$ und die Anwendung von (3.8) ergibt das Resultat

$$F = \sum_{n=0}^{s-2} \sum_{n_1=0}^{s_1-1} [\bar{Q}(n\ ,\ n_1) - \bar{Q}(s-1\ ,\ n_1)]\, x^n\, x_1^{n_1}\ .$$

Die Koeffizienten hierbei sind nach (3.13) gleich

$$(3.14)\quad 2[R(0\ ,\ n\ ,\ n_1) + R(1\ ,\ n\ ,\ n_1) - R(0\ ,\ s-1\ ,\ n_1) - R(1\ ,\ s-1\ ,\ n_1)]$$

und somit durch $2a$ teilbar.

Es sei $b = c \geqq 2$. Wir werden zeigen, dass jetzt $2a$ schon die Zahlen $\bar{Q}(n\ ,\ \mathfrak{n}_c)$ teilt.

Jeder Summierungsindex in (3.13) nimmt nunmehr seine beiden Werte an (s. Anm. 3). In bezug auf $\bar{n}$ bedeutet dies, dass (3.13) sich in der Form

$$\bar{Q}(n\ ,\ \mathfrak{n}_c) = \sum_{\mathfrak{t}_c}{}' [2R(0\ ,\ n\ ,\ \mathfrak{t}_c) - a] + \sum_{\mathfrak{t}_c}{}'' [2R(1\ ,\ n\ ,\ \mathfrak{t}_c) - a]$$

schreiben lässt. Im Fall $d = 0$ durchlaufen hierbei die Indizes in jeder der Summen Σ' und Σ'' dieselben Werte, während im Fall $d = 1$ jede Wertkombination von $\mathfrak{t}_c$ in Σ' eine gerade und in Σ'' eine ungerade Anzahl der Werte $n_j + s_j$ enthält. Man erkennt aber, dass es in Σ' und Σ'' jedenfalls gleich viele Summanden gibt. Daraus folgt, dass $\bar{Q}(n\ ,\ \mathfrak{n}_c)$ durch 2^{h+1} teilbar ist, denn die Summe zweier Glieder, von denen das eine aus Σ' und das andere aus Σ'' genommen ist, hat immer diese Eigenschaft. — Durch ähnliche Umformungen des Ausdrucks (3.13) zeigt man ebenso, dass $\bar{Q}(n\ ,\ \mathfrak{n}_c)$ durch p_j^{hj} $(j = 1\ ,\ \ldots\ ,\ c)$ teilbar ist, sodass man wirklich das Ergebnis $\bar{Q}(n\ ,\ \mathfrak{n}_c) \equiv 0 \pmod{2a}$ erreicht.

Von der letzten Betrachtung sei bemerkt, dass sie im Fall des ungeraden a eine kleine Modifikation (ausser den gewöhnlichen) benötigt: man muss die Teilbarkeit von $\bar{Q}(\mathfrak{n}_c)$ durch etwa $2p_1^{h_1}$ (statt $p_1^{h_1}$) feststellen.

Unser Hilfssatz ist somit bewiesen.

§ 4. Eine Determinantendarstellung für $T_w(a)$

13. Nach der Formel (2.8) samt Hilfssatz 3 besitzt $T_w(a)$ für $a = 2^h p_1^{h_1} \ldots p_c^{h_c}$ die Darstellung

$$(4.1)\qquad T_w(a) = \prod_w G_w\,(Z^k\ ,\ Z_1^{k_1}\ ,\ \ldots\ ,\ Z_c^{k_c})\ .$$

Wir betrachten einen beliebigen Faktor in diesem Produkt und setzen dabei wie vorhin

$$(4.2)\qquad x = Z^k\ ,\quad x_j = Z_j^{kj}\quad (j = 1\ ,\ \ldots\ ,\ c)\ .$$

Dann hat dieser Faktor die Form (3.2) und weiter nach den Beziehungen (3.3)—(3.8) folgende Eigenschaft: es gilt

$$(4.3)\qquad \begin{cases} x^{\lambda} = \text{entweder } 1 \text{ oder } -1 - x - \ldots - x^{\lambda-1}, \\ x_j^{\lambda_j} = \text{entweder } -1 \text{ oder } -1 - x_j - \ldots - x_j^{\lambda_j-1} \quad (j = 1, \ldots, c). \end{cases}$$

Wir schreiben kurz

$$(4.4)\qquad G_w(x, \mathbf{x}_c) = \sum_{\nu=0}^{N-1} c_{0\nu} X_\nu,$$

wobei $N = \lambda\lambda_1 \ldots \lambda_c$ ist und $X_0 (= 1), X_1, \ldots, X_{N-1}$ die Zahlen $x^n x_1^{n_1} \ldots x_c^{n_c}$ $(n = 0, \ldots, \lambda - 1;\ n_j = 0, \ldots, \lambda_j - 1$ für $j = 1, \ldots, c)$ in einer beliebig festgewählten Reihenfolge bedeuten. Dann gilt

$$X_\mu G_w(x, \mathbf{x}_c) = \sum_{\nu=0}^{N-1} c_{\mu\nu} X_\nu \quad (\mu = 0, \ldots, N-1)$$

mit ganzen rationalen $c_{\mu\nu}$, denn die Potenzen von x und x_j $(j = 1, \ldots, c)$ mit den Exponenten $\geqq \lambda$ bzw. λ_j lassen sich mittels (4.3) eliminieren.

Im folgenden beweisen wir den

Satz 4. *Die Zahl $T_w(a)$ ist gleich der Determinante*

$$D_w(a) = |c_{\mu\nu}| \quad (\mu, \nu = 0, \ldots, N-1).$$

Es sei bemerkt, dass HYYRÖ [10] einen etwas allgemeineren Satz bewiesen hat, der dieses Ergebnis enthält. Wir wollen jedoch für unseren Satz hier einen anderen Beweis vorlegen, und zwar diejenige bekannte Methode verallgemeinern, die häufig für die Darstellung der Produkte einfacherer Form als Determinante angewandt wird (s. z.B. [11], [17], [18]).

14. Es mögen für ein Moment $x, x_1, \ldots, x_c$ komplexe Veränderlichen bedeuten, und $X_0, \ldots, X_{N-1}$ seien durch dieselbe formale Definition bestimmt wie oben. Wir setzen

$$E(x, \mathbf{x}_c) = \sum_{\nu=0}^{N-1} e_\nu X_\nu$$

mit komplexen Koeffizienten e_ν und betrachten die Zahlen

$$(4.5)\qquad E(Z^k, Z_1^{k_1}, \ldots, Z_c^{k_c}) \qquad \begin{cases} k = 0, \ldots, s-1, \\ k_j = 1, \ldots, q_j - 1 \quad (j = 1, \ldots, c) \end{cases}$$

als Funktionen dieser Koeffizienten, also als Linearformen von N komplexen Veränderlichen. Es sei $\mathbf{R}_N$ der von diesen Veränderlichen bestimmte

N-dimensionale lineare Raum. Sind E_1 und E_2 zwei beliebige der fraglichen Linearformen, so bestimmt die Gleichung $E_1 - E_2 = 0$ einen $(N-1)$-dimensionalen Unterraum von $\mathbf{R}_N$, denn E_1 und E_2 können nicht identisch sein. Wir spezifizieren nun die Werte von $e_0, \ldots, e_{N-1}$ so, dass der entsprechende Punkt von $\mathbf{R}_N$ zu keinem von derartigen Unterräumen gehört. Dann sind die Zahlen (4.5) paarweise verschieden.

Wir setzen noch mit einer weiteren komplexen Veränderlichen t

$$\bar{G}_w(x, \mathfrak{x}_c, t) = G_w(x, \mathfrak{x}_c) + tE(x, \mathfrak{x}_c) = \sum_{\nu=0}^{N-1} c_{0\nu}(t) X_\nu , \tag{4.6}$$

wobei

$$c_{0\nu}(t) = c_{0\nu} + te_\nu \quad (\nu = 0, \ldots, N-1) \tag{4.7}$$

gilt. Es gibt dann solche Werte von t, sogar unendlich viele, dass die Zahlen

$$\bar{G}_w(Z^k, Z_1^{k_1}, \ldots, Z_c^{k_c}, t) \quad \begin{cases} k = 0, \ldots, s-1, \\ k_j = 1, \ldots, \varphi_j - 1 \ (j = 1, \ldots, c) \end{cases}$$

paarweise verschieden sind.

Wir geben nunmehr für $x, x_1, \ldots, x_c$ die in (4.2) angeführten Werte. Nach (4.6) gilt

$$\sum_{\nu=0}^{N-1} \bar{c}_{0\nu}(t) X_\nu = 0$$

mit

$$\begin{cases} \bar{c}_{00}(t) = c_{00}(t) - \bar{G}_w(x, \mathfrak{x}_c, t), \\ \bar{c}_{0\nu}(t) = c_{0\nu}(t) \text{ für } \nu = 1, \ldots, N-1. \end{cases} \tag{4.8}$$

Multipliziert man diese Gleichung mit X_μ, $\mu = 0, \ldots, N-1$, und wendet dann die Beziehungen (4.3) an, so erhält man ein Gleichungssystem von der Form

$$\sum_{\nu=0}^{N-1} \bar{c}_{\mu\nu}(t) X_\nu = 0 \qquad (\mu = 0, \ldots, N-1), \tag{4.9}$$

wobei die Koeffizienten $\bar{c}_{\mu\nu}(t)$ Summen mit den Gliedern $= \bar{c}_{0\nu}(t)$ sind. Es ist besonders zu bemerken, dass $\bar{c}_{00}(t)$ immer nur in $\bar{c}_{\mu\mu}(t)$ auftritt und mit dem Pluszeichen versehen ist. Man erkennt daher mit Hilfe von (4.8), dass die Determinante

$$\bar{D}(t) = |\bar{c}_{\mu\nu}(t)| \quad (\mu, \nu = 0, \ldots, N-1)$$

ein Polynom von $\bar{G}_w(x, \mathfrak{x}_c, t)$ mit dem höchsten Glied $(-\bar{G}_w(x, \mathfrak{x}_c, t))^N$ darstellt.

Das System (4.9) wird offenbar von allen solchen $(X_0, \ldots, X_{N-1})$ erfüllt, wobei die Zahlen $x = Z^k$, $x_j = Z_j^{k_j}$ $(j = 1, \ldots, c)$ in (4.1) auftreten. Dies bedeutet erstens, dass

$$\bar{D}(t) = 0 \tag{4.10}$$

gilt, und zweitens, dass die erhaltene Gleichung (4.10), die bezüglich $\bar{G}_w(x, \mathfrak{x}_c, t)$ vom N-ten Grade ist, alle solche $\bar{G}_w(Z^k, Z_1^{k_1}, \ldots, Z_c^{k_c}, t)$ als Wurzeln hat, wobei $G_w(Z^k, Z_1^{k_1}, \ldots, Z_c^{k_c})$ als Faktor in (4.1) auftritt. Die Anzahl dieser Faktoren ist gleich $\lambda\lambda_1 \ldots \lambda_c = N$, wie aus der Definition der λ und λ_j $(j = 1, \ldots, c)$ in Nr. 9 hervorgeht. Wenn wir also den Wert von t passend wählen, haben wir hier N paarweise verschiedene — und damit genau alle — Lösungen von (4.10). Folglich gilt für das konstante Glied $D(t)$ des Polynoms $\bar{D}(t)$

$$\prod_w \bar{G}_w (Z^k, Z_1^{k_1}, \ldots, Z_c^{k_c}, t) = D(t) .$$

Diese Gleichung ist bezüglich t höchstens vom N-ten Grade, hat aber unendlich viele Wurzeln t. Somit muss sie identisch bestehen. Für $t = 0$ ergibt sich unter Berücksichtigung von (4.6)

$$\prod_w G_w (Z^k, Z_1^{k_1}, \ldots, Z_c^{k_c}) = D(0) .$$

Die Zahl $D(t)$ ist gleich der Determinante, die aus $\bar{D}(t)$ durch die Substitution $\bar{G}_w(x, \mathfrak{x}_c, t) = 0$ entsteht. Nach (4.8) ist daher

$$D(t) = |c_{\mu\nu}(t)| \qquad (\mu, \nu = 0, \ldots, N-1) ,$$

wobei sich jedes $c_{\mu\nu}(t)$ aus $\bar{c}_{\mu\nu}(t)$ ergibt, indem man dabei $\bar{c}_{0\nu}(t)$ $(\nu = 0, \ldots, N-1)$ durch $c_{0\nu}(t)$ ersetzt.

Wir haben also das Resultat

$$T_w(a) = |c_{\mu\nu}(0)| = |c_{\mu\nu}| \qquad (\mu, \nu = 0, \ldots, N-1) ,$$

worin die letzte Gleichung unter Vergleichung der Definitionen von $c_{\mu\nu}(t)$ und $c_{\mu\nu}$ sowie unter Beachtung von (4.7) folgt.

Damit haben wir Satz 4 bewiesen.

Anmerkung 5. Die in Satz 4 eingeführte Bezeichnung $D_w(a)$ soll im folgenden die Determinantendarstellung von $T_w(a)$ für jedes in Frage kommende a bedeuten; im Fall eines ungeraden a hat $D_w(a)$ natürlich eine ganz entsprechende Form wie im vorigen Fall.

§ 5. Der Spezialfall $\omega(a) = 2$

15. Wir wollen obige allgemeine Betrachtungen auf den einfachsten Spezialfall $\omega(a) = 2$ anwenden, und zwar besonders solche Beziehungen heranziehen, die später für uns anwendbar sind.

In diesem Fall hat $T(a)$ die Zerlegung

$$T(a) = T_{w(1)}(a)T_{w(2)}(a)$$

mit $w(1) = (1\,,\,0)$ und $w(2) = (0\,,\,1)$. Wir bezeichnen die Indizes $w(1)$ und $w(2)$ im folgenden kurz mit 1 bzw. 2.

Es sei zuerst $a = p_1^{h_1}p_2^{h_2}$. Dann ist für $i = 1\,,\,2$

$$T_i(a) = \prod\nolimits_i (-2a)^{-1} F(Z_1^k\,,\,Z_2^l) = \prod\nolimits_i G_i(Z_1^k\,,\,Z_2^l)\,, \tag{5.1}$$

wobei Π_1 bzw. Π_2 über

$$k = 1\,,\,3\,,\ldots,\varphi_1 - 1; \quad l = 2\,,\,4\,,\ldots,\varphi_2 - 2$$

bzw.

$$k = 2\,,\,4\,,\ldots,\varphi_1 - 2; \quad l = 1\,,\,3\,,\ldots,\varphi_2 - 1$$

zu erstrecken ist. Wir beschränken uns wegen der Symmetrie auf $T_1(a)$ und setzen dabei $p_2^{h_2} > 3$ voraus, da Π_1 sonst leer ist.

Zur Vereinfachung der folgenden Bezeichnungen setzen wir

$$x = Z_1^k\,, \quad y = Z_2^l\,;$$

$$t = s_1\,, \quad u = s_2 \quad (s_j = \tfrac{1}{2}\varphi_j)\,.$$

Jetzt ist

$$F(x\,,\,y) = \sum_{i=0}^{\varphi_1-1}\sum_{j=0}^{\varphi_2-1} R_a(i\,,j)x^i\,y^j\,,$$

wobei weiter

$$\begin{cases} x^t = -1\,, \\ y^{u-1} = -1 - y - \ldots - y^{u-2} \end{cases} \tag{5.2}$$

gilt (vgl. (2.4'), (3.5) und (3.6)). Wir schreiben dem Beweisgang von Hilfssatz 3 folgend

$$\begin{aligned} F(x,y) &= \sum_{i=0}^{t-1}\sum_{j=0}^{u-1} [R(i,j) - R(i+t,j) + R(i,j+u) - R(i+t,j+u)]\,x^iy^j \\ &= \sum_{i=0}^{t-1}\sum_{j=0}^{u-1} 2[R(i,j) + R(i,j+u) - a]\,x^iy^j \\ &= \sum_{i=0}^{t-1}\sum_{j=0}^{u-2} 2[R(i,j) + R(i,j+u) - R(i,u-1) - R(i,2u-1)]\,x^iy^j\,. \end{aligned}$$

Demnach ist (vgl. Hilfssatz 3)

$$G_1(x\,,\,y) = (-\,2a)^{-1}\,F(x\,,\,y) = \sum_{i=0}^{t-1}\sum_{j=0}^{u-2} P(i\,,\,j)\,x^i\,y^j \tag{5.3}$$

mit ganzen Koeffizienten

$$P(i,j) = -\,a^{-1}\,[R(i,j) + R(i,j+u) - R(i,u-1) - R(i,2u-1)]\,. \tag{5.4}$$

Die Bildung der Determinantendarstellung $D_1(a)$ für $T_1(a)$ ist leicht durchzuführen. Dazu führen wir die Bezeichnungen

$$P_{ij}^n = -\,a^{-1}\,[R(i,j) + R(i,j+u) - R(i,n) - R(i,n+u)\,]\,, \tag{5.5}$$

$$A_j^n = \begin{bmatrix} P_{0j}^n & P_{1j}^n & \dots & P_{t-1,j}^n \\ -P_{t-1,j}^n & P_{0j}^n & \dots & P_{t-2,j}^n \\ \cdot & \cdot & \dots & \cdot \\ -P_{1j}^n & -P_{2j}^n & \dots & P_{0j}^n \end{bmatrix} \tag{5.6}$$

ein. Wegen $P_{ij}^n = -\,P_{in}^j$ und $P_{ij}^n - P_{ir}^n = P_{ij}^r$ gilt nun

$$\begin{cases} A_j^n = -\,A_n^j\,, \\ A_j^n - A_r^n = A_j^r\,. \end{cases} \tag{5.7}$$

Unter Beachtung von $P(i,j) = P_{ij}^{u-1}$ können wir $G_1(x\,,\,y)$ auch in der Gestalt

$$G_1(x\,,\,y) = \sum_{i=0}^{t-1} P_{i0}^{u-1}\,x^i + \sum_{i=0}^{t-1} P_{i1}^{u-1}\,x^i\,y + \dots + \sum_{i=0}^{t-1} P_{i,u-2}^{u-1}\,x^i\,y^{u-2}$$

darstellen. Um die Determinante $D_1(a)$ zu bekommen, muss man diesen Ausdruck mit jedem hier auftretenden x^iy^j der Reihe nach multiplizieren und die entstandenen Ausdrücke mittels (5.2) reduzieren. Führt man diesen Prozess zuerst mit den Multiplikatoren $1\,,\,x\,,\,\dots\,,\,x^{t-1}$ durch, so entstehen die t ersten Zeilen von $D_1(a)$; offenbar lauten sie in der Matrizenform

$$[A_0^{u-1}\quad A_1^{u-1}\dots A_{u-2}^{u-1}]\,.$$

Die t folgenden Zeilen bilden sich durch Multiplikation der erhaltenen t Ausdrücke mit y. Es ergibt sich daraus die Matrix

$$[-\,A_{u-2}^{u-1}\quad A_0^{u-1} - A_{u-2}^{u-1}\quad A_1^{u-1} - A_{u-2}^{u-1}\quad \dots\quad A_{u-3}^{u-1} - A_{u-2}^{u-1}]\,,$$

also nach (5.7)

$$[A_{u-1}^{u-2}\quad A_0^{u-2}\quad A_1^{u-2}\quad \dots\quad A_{u-3}^{u-2}]\,.$$

Fährt man auf diese Weise fort, d.h. multipliziert man immer die t letzten Ausdrücke mit y, so gewinnt man zuletzt das Resultat

$$(5.8)\qquad D_1(a) = \begin{vmatrix} A_0^{u-1} & A_1^{u-1} & A_2^{u-1} & \dots & A_{u-2}^{u-1} \\ A_{u-1}^{u-2} & A_0^{u-2} & A_1^{u-2} & \dots & A_{u-3}^{u-2} \\ A_{u-2}^{u-3} & A_{u-1}^{u-3} & A_0^{u-3} & \dots & A_{u-4}^{u-3} \\ \cdot & \cdot & \cdot & \dots & \cdot \\ A_2^1 & A_3^1 & A_4^1 & \dots & A_0^1 \end{vmatrix} .$$

Beispiel. Legt man die primitiven Wurzeln 2 (mod 5) und 3 (mod 7) zugrunde, so ergibt sich

$$D_1(5\cdot 7) = \left|\begin{array}{cc:cc} 1 & -1 & 0 & -1 \\ 1 & 1 & 1 & 0 \\ \hdashline 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{array}\right| , \qquad D_2(5\cdot 7) = \begin{vmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{vmatrix} .$$

(Die gebrochenen Linien trennen die Matrizenblöcke A_j^n voneinander.)

16. Zweitens sei a gerade. Um die Analogie mit dem vorigen Fall besser einzusehen, weichen wir hier von unserer allgemeinen Bezeichnungsweise ab und setzen $a = 2^h p_2^h$.

Jetzt gilt für $i = 1, 2$

$$(5.9)\qquad T_i(a) = \prod\nolimits_i (-2a)^{-1} F((-1)^{\bar{k}}, Z^k, Z_2^l) = \prod\nolimits_i G_i(Z^k, Z_2^l) ,$$

wobei $\bar{k}$ gleich 1 für $i = 1$ und gleich 0 für $i = 2$ ist und das Produkt Π_1 bzw. Π_2 sich über

$$k = 0, 1, \dots, s-1; \quad l = 2, 4, \dots, \varphi_2 - 2$$

bzw.

$$k = 1, 2, \dots, s-1; \quad l = 1, 3, \dots, \varphi_2 - 1$$

erstreckt. Wird weiter $x = Z^k$, $y = Z_2^l$ und $u = s_2$ gesetzt, so gilt

$$(5.10)\qquad \begin{cases} G_1(x, y) = (-2a)^{-1} F(-1, x, y) = \sum\limits_{i=0}^{s-1} \sum\limits_{j=0}^{u-2} P(i,j) x^i y^j , \\ G_2(x, y) = (-2a)^{-1} F(1, x, y) = \sum\limits_{i=0}^{s-2} \sum\limits_{j=0}^{u-1} P'(i, j) x^i y^j \end{cases}$$

mit ganzen Koeffizienten

$$(5.11)\qquad \begin{cases} P(i,j) = -a^{-1}[R(0,i,j) + R(0,i,j+u) - R(0,i,u-1) - R(0,i,2u-1)], \\ P'(i,j) = -a^{-1}[R(0,i,j) + R(1,i,j) - R(0,s-1,j) - R(1,s-1,j)] \end{cases}$$

(vgl. auch (3.14)).

Die Determinanten $D_1(a)$ und $D_2(a)$ bilden sich ganz entsprechend wie vorhin aus den Zahlen

$$(5.12)\quad \begin{cases} P_{ij}^{n} = -a^{-1}\,[R(0,i,j) + R(0,i,j+u) - R(0,i,n) - R(0,i,n+u)], \\ P_{ij}^{\prime n} = -a^{-1}\,[R(0,i,j) + R(1,i,j) - R(0,n,j) - R(1,n,j)]; \end{cases}$$

der einzige Unterschied ist, dass in den Matrizenblöcken von $D_1(a)$ die Vorzeichen der Elemente P_{ij}^{n} jetzt unverändert bleiben (statt der vorigen Beziehung $x^t = -1$ gilt nämlich jetzt $x^s = 1$).

Beispiel. Im Fall $a = 2^4 \cdot 5$ sehen $D_1(a)$ und $D_2(a)$ aus wie folgt:

$$D_1(2^4 \cdot 5) = \begin{vmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{vmatrix}, \qquad D_2(2^4 \cdot 5) = \left|\begin{array}{cc:cc:cc} 1 & 1 & 1 & 1 & 0 & 1 \\ -1 & 1 & -1 & 1 & -1 & 0 \\ \hdashline 0 & -1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ \hdashline -1 & 0 & -1 & -1 & 0 & 0 \\ 0 & -1 & 1 & -1 & 0 & 0 \end{array}\right| .$$

(Hierbei ist 2 als die primitive Wurzel (mod 5) gewählt.)

§ 6. Heraushebung der Faktoren 2

17. Aus den Sätzen 1 und 2 samt Anmerkung 2 folgt zusammengefasst, dass der erste Faktor der Klassenzahl die Darstellung

$$(6.1)\qquad H_1(m) = 2^{1-\omega(m)} \prod_{p^h \,||\, m} H_1(p^h) \prod_{a}{}' \prod_{w \in Y_c} T_w(a)$$

besitzt. Hieraus gelangt man zu einer »ganzen» Darstellung für $2H_1(m)$, indem man zeigt, dass genügend viele $T_w(a)$ gerade sind.

HASSE [6] hat die Teilbarkeit verschiedener Faktoren von $H_1(m)$ durch 2 eingehend behandelt. Wir betrachten hier dieselbe Frage unter einem neuen Gesichtswinkel, indem wir den folgenden Satz beweisen.

Satz 5. *Ist* $\omega(a) = 3$ *und* $w = (1\,,\,1\,,\,1)$, *so ist jede Zeilensumme in der Determinante* $D_w(a)$ *gerade.*

Dieser Satz hat zur Folge, dass in (6.1) sämtliche $T_w(a)$ mit $\omega(a) = 3$ und $w = (1\,,\,1\,,\,1)$ durch 2 teilbar sind. Die Anzahl dieser $T_w(a)$ ist

$$\binom{\omega(m)}{3} \geqq \omega(m) - 2 \qquad (\omega(m) \geqq 3)\,,$$

sodass die Ganzzahligkeit von $2H_1(m)$ dadurch wirklich nachgewiesen wird. (Vgl. [6], Satz 31 und Nr. 33.)

Als ein Beispiel für die in Satz 5 genannten $D_w(a)$ sei die folgende Determinante aufgestellt, die sich im Fall $a = 2^3 \cdot 5 \cdot 7$ mit den primitiven Wurzeln 2 (mod 5) und 3 (mod 7) ergibt:

0	0	0	1	−1	1	0	1	0	−1	1	0
0	0	1	0	1	−1	1	0	−1	0	0	1
0	−1	0	0	0	−1	−1	1	−1	0	0	−1
−1	0	0	0	−1	0	1	−1	0	−1	−1	0
0	1	−1	0	0	0	0	1	−1	1	0	1
1	0	0	−1	0	0	1	0	1	−1	1	0
1	0	0	1	0	−1	0	0	0	−1	−1	1
0	1	1	0	−1	0	0	0	−1	0	1	−1
1	−1	0	−1	0	1	−1	0	0	0	0	1
−1	1	−1	0	1	0	0	−1	0	0	1	0
0	1	1	−1	1	0	0	1	0	−1	0	0
1	0	−1	1	0	1	1	0	−1	0	0	0

Der Absolutwert dieser Determinante ist, auf der IBM 1130 berechnet, gleich $2^2 \cdot 5 \cdot 13 \cdot 37$.*

Es sei noch erwähnt, dass sich der Ausdruck von $H_1(m)$ jetzt in der Produktform darstellen lässt derart, dass dabei alle Faktoren (ausser $\frac{1}{2}$) Determinanten mit ganzen rationalen Elementen sind. Dafür sei $\bar{D}_w(a) = \frac{1}{2} D_w(a)$ die Determinante, die man aus dem in Satz 5 genannten $D_w(a)$ bekommt, indem man dabei zu einer Spalte alle übrigen Spalten addiert und dann die Elemente dieser Spalte durch 2 dividiert. Man hat dann die Darstellung

$$H_1(m) = \tfrac{1}{2} \prod_{p^h \| m} \Delta(p^h) \prod_a{}' \prod_{w \in Y_c} \Delta_w(a) \quad (\omega(m) \geqq 2) ,$$

wobei $\Delta(p^h)$ eine der bekannten Determinantendarstellungen von $H_1(p^h)$ bedeutet ([18], s. auch [17]) und $\Delta_w(a)$ gleich $D_w(a)$ oder $\bar{D}_w(a)$ passend zu wählen ist.

18. Im Beweis von Satz 5 müssen wir die Fälle $a = 2^h p_1^h p_2^h$ und $a = p_1^h p_2^h p_3^h$ getrennt behandeln. Wir setzen zur Abkürzung

$$t = s_1 , \quad u = s_2 , \quad v = s_3 \quad (s_j = \tfrac{1}{2}\varphi_j)$$

und beweisen zuerst einige Hilfssätze.

* Die Ausführung der Rechnungen zu diesem Beispiel verdanke ich Mag.phil. Ulla Huttunen und Cand.sc.nat. Eija Aronen.

Hilfssatz 4. *Ist* $g = p_1^h p_2^h$, *so gilt*

$$\sum_{i=0}^{t-1} \sum_{j=0}^{2u-1} [R_g(i, j) - R_g(i - \alpha, j - \beta)] \equiv 0 \pmod 2,$$

wobei α *und* β *beliebige ganze (rationale) Zahlen sind.*

Beweis. Wie aus (2.1) hervorgeht, ist $R_g(i, j)$ eine periodische Funktion seiner Argumente; die Periode von i ist gleich $\varphi_1 = 2t$ und diejenige von j gleich $\varphi_2 = 2u$. Dies bedeutet zunächst, dass die im Hilfssatz aufgestellte Summe unabhängig von β ist. Wir bezeichnen diese Summe mit $S(\alpha)$.

Nach Hilfssatz 2 gilt

$$S(\alpha) = \sum_{i=0}^{t-1} \sum_{j=0}^{2u-1} [R(i, j) + R(i - \alpha \pm t, j - \beta + u) - g],$$

woraus

$$S(\alpha) \equiv S(\alpha \pm t) - 2tug \equiv S(\alpha \pm t) \pmod 2$$

folgt. Daher können wir ohne Beschränkung $0 \leqq \alpha < t$ annehmen.

Es gilt zuerst $S(0) = 0$. Ist $0 < \alpha < t$, so schreiben wir

$$\sum_{i=0}^{t-1} [R(i, j) - R(i - \alpha, j)]$$

$$= \sum_{i=t-\alpha}^{t-1} R(i, j) - \sum_{i=0}^{\alpha-1} R(i - \alpha, j) + \sum_{i=0}^{t-\alpha-1} R(i, j) - \sum_{i=\alpha}^{t-1} R(i - \alpha, j)$$

$$= \sum_{i=t-\alpha}^{t-1} [R(i, j) - R(i + t, j)].$$

Dann ergibt sich

$$S(\alpha) = \sum_{i=t-\alpha}^{t-1} \sum_{j=0}^{u-1} [R(i, j) - R(i + t, j) + R(i, j + u) - R(i + t, j + u)],$$

also unter Anwendung von Hilfssatz 2

$$S(\alpha) = \sum_{i=t-\alpha}^{t-1} \sum_{j=0}^{u-1} [2R(i, j) + 2R(i, j + u) - 2g],$$

womit die behauptete Kongruenz bewiesen wird.

Hilfssatz 5. *Ist* $a = p_1^h p_2^h p_3^h$, *so gilt*

$$\sum_{i=0}^{t-1} \sum_{j=0}^{2u-1} \sum_{n=0}^{2v-1} R_a(i, j, n) \equiv 0 \pmod 2.$$

Beweis. Wir setzen innerhalb dieses Beweises kurz $p = p_3$ und $h = h_3$. Hat g dieselbe Bedeutung wie in Hilfssatz 4, so gilt $a = gp^h$ und nach (2.1)

$$R_a(i, j, n) \equiv R_g(i, j) \pmod{g} .$$

Ausserdem ist $0 < R_a < a$ und $0 < R_g < g$, sodass $R_a(i, j, n)$ mit $n = 0, \ldots, 2v - 1$ folglich $2v(= p^h - p^{h-1})$ verschiedene Zahlen von der Form

$$R_g(i, j) + \varrho g \qquad (0 \leqq \varrho < p^h) \tag{6.2}$$

durchläuft.

Es lassen sich nun leicht p^{h-1} Zahlen von der Form (6.2) finden, die durch p teilbar sind und daher nicht als Werte von $R_a(i, j, n)$ hervortreten können. In der Tat sei

$$p \equiv \begin{cases} r_1^{\alpha} \pmod{p_1^{h_1}} , \\ r_2^{\beta} \pmod{p_2^{h_2}} . \end{cases}$$

Dann gilt

$$p\, R_g(i - \alpha, j - \beta) \equiv R_g(i, j) \pmod{g} ,$$

also für $\tau = 0, \ldots, p^{h-1} - 1$

$$p[R_g(i - \alpha, j - \beta) + \tau g] = R_g(i, j) + \varrho_\tau\, g , \tag{6.3}$$

wobei die Werte von ϱ_τ offenbar zum Wertevorrat von ϱ gehören.

Hiermit bekommt man genau alle Werte von $R_a(i, j, n)$ für $n = 0, \ldots, 2v - 1$, indem man die Zahlen (6.3) von den Zahlen (6.2) ausschliesst. Demnach ist

$$\begin{aligned} \sum_{n=0}^{2v-1} R_a(i, j, n) &= \sum_{\varrho=0}^{p^h-1} [R_g(i, j) + \varrho g] - p \sum_{\tau=0}^{p^{h-1}-1} [R_g(i - \alpha, j - \beta) + \tau g] \\ &= p^h[R_g(i, j) - R_g(i - \alpha, j - \beta)] + va . \end{aligned}$$

Die im Hilfssatz genannte Summe schreibt sich somit in der Form

$$p^h \sum_{i=0}^{t-1} \sum_{j=0}^{2u-1} [R_g(i, j) - R_g(i - \alpha, j - \beta)] + 2tuva \tag{6.4}$$

und ist nach Hilfssatz 4 gerade.

Hilfssatz 5′. *Ist* $a = 2^h p_1^{h_1} p_2^{h_2}$, *so gilt*

$$\sum_{\bar{n}=0}^{1} \sum_{n=0}^{s-1} \sum_{i=0}^{t-1} \sum_{j=0}^{2u-1} R_a(\bar{n}, n, i, j) \equiv 0 \pmod{2^{h+1}} .$$

Beweis. Denken wir im vorigen Beweis die Primzahl $p = p_3$ durch 2 ersetzt, so bekommen wir für die hier in Frage stehende Summe den Ausdruck (6.4) mit $v = 2^{h-2}$.

19. Wir beweisen Satz 5 zuerst für $a = 2^h p_1^{h_1} p_2^{h_2}$. Im Fall $w = (1, 1, 1)$ ist $T_w(a)$ dann von der Form (2.8), wobei Π_w über $\bar{k} = 1$, $k = 0, 1, \ldots,$ $s - 1$ und $k_j = 1, 3, \ldots, \varphi_j - 1$ $(j = 1, 2)$ zu erstrecken ist. Nach Hilfssatz 3 und seinem Beweis ist weiter

$$G_w(x, x_1, x_2) = \sum_{n=0}^{s-1} \sum_{i=0}^{t-1} \sum_{j=0}^{u-1} P(n, i, j)\, x^n x_1^i x_2^j \tag{6.5}$$

mit ganzen Koeffizienten

$$P(n, i, j) = (-2a)^{-1}\, \bar{Q}(n, i, j) \tag{6.6}$$

(vgl. (3.1) und (3.11)). Der Ausdruck von $\bar{Q}(n, i, j)$ geht aus (3.13) hervor und zwar ist er

$$2[R(0, n, i, j) + R(0, n, i + t, j + u) + R(1, n, i, j + u) + R(1, n, i + t, j) - 2a]\,.$$

Unter Anwendung von Hilfssatz 2 können wir damit

$$\begin{aligned} \bar{Q}(n, i, j) = 2[&R(0, n, i, j) - R(1, n, i, j) \\ &+ R(1, n, i, j + u) - R(0, n, i, j + u)] \end{aligned} \tag{6.7}$$

schreiben.

Die Formeln (4.3) lauten jetzt $x^s = 1$, $x_1^t = -1$, $x_2^u = -1$. Daraus folgt, dass jede Zeile $c_{\mu 0}, \ldots, c_{\mu, N-1}$ $(\mu = 0, \ldots, N - 1)$ von $D_w(a)$ vom Vorzeichen abgesehen dieselben Elemente enthält. Es genügt somit zu zeigen, dass die Summe

$$S = \sum_{\nu=0}^{N-1} c_{0\nu}$$

gerade ist.

Vergleicht man die Formeln (4.4) und (6.5), so erkennt man, dass im vorliegenden Fall

$$S = \sum_{n=0}^{s-1} \sum_{i=0}^{t-1} \sum_{j=0}^{u-1} P(n, i, j) \tag{6.8}$$

ist. Wir stellen diese Formel mittels (6.6) und (6.7) in der folgenden, etwas komplizierten Form dar:

$$\begin{aligned} S = &- a^{-1} \sum_{n=0}^{s-1} \sum_{i=0}^{t-1} \sum_{j=0}^{u-1} [R(0, n, i, j) + R(1, n, i, j) \\ &\qquad + R(1, n, i, j + u) + R(0, n, i, j + u)] \\ &+ 2a^{-1} \sum_{n=0}^{s-1} \sum_{i=0}^{t-1} \sum_{j=0}^{u-1} [R(1, n, i, j) + R(0, n, i, j + u)]\,. \end{aligned}$$

Hierbei ist die erste Tripelsumme gleich der Summe von Hilfssatz 5′ und daher durch 2^{h+1} teilbar, während in der zweiten Tripelsumme jeder Summand durch 2^h teilbar ist. Beachten wir dazu, dass 2 genau zur h-ten Potenz in a steckt, so gewinnen wir das erwünschte Resultat $S \equiv 0 \pmod 2$.

20. Der Beweis im Fall $a = p_1^h p_2^h p_3^h$ ist etwas einfacher. Jetzt ist das Produkt Π_w mit $w = (1, 1, 1)$ über $k_j = 1, 3, \ldots, \varphi_j - 1$ $(j = 1, 2, 3)$ zu erstrecken, und es gilt also

$$G_w(x_1, x_2, x_3) = \sum_{i=0}^{t-1} \sum_{j=0}^{u-1} \sum_{n=0}^{v-1} P(i, j, n) x_1^i x_2^j x_3^n .$$

Dabei ist weiter (vgl. Anm. 4)

$$P(i, j, n) = (-2a)^{-1} \bar{Q}(i, j, n)$$

$$= -a^{-1}[R(i,j,n) + R(i,j+u,n+v) + R(i+t,j,n+v) + R(i+t,j+u,n) - 2a] ,$$

also nach Hilfssatz 2

$$P(i, j, n) \equiv -a^{-1}[R(i, j, n) + R(i, j+u, n+v) + R(i, j+u, n) + R(i, j, n+v)] \pmod 2 .$$

Bei der Bildung der Determinante $D_w(a)$ werden jetzt die Beziehungen $x_1^t = -1$, $x_2^u = -1$ und $x_3^v = -1$ angewandt, sodass die Zeilensummen wie vorhin zueinander kongruent (mod 2) sind. Die erste Zeilensumme ist gleich

$$S = \sum_{i=0}^{t-1} \sum_{j=0}^{u-1} \sum_{n=0}^{v-1} P(i, j, n) . \tag{6.9}$$

Wird hierin $P(i, j, n)$ durch den vorigen kongruenten Ausdruck ersetzt, so ergibt sich

$$S \equiv -a^{-1} \sum_{i=0}^{t-1} \sum_{j=0}^{2u-1} \sum_{n=0}^{2v-1} R(i, j, n) \equiv 0 \pmod 2 ,$$

wobei zuletzt von Hilfssatz 5 Gebrauch gemacht worden ist.

Der Beweis von Satz 5 ist damit vollendet.

21. Wir deuten noch auf eine Modifikation des vorigen Beweises hin, durch die sich die Teilbarkeit der betreffenden $T_w(a)$ durch 2 ohne die Determinantendarstellungen $D_w(a)$ nachweisen lässt. Dafür muss man zuerst wie oben zeigen, dass der Ausdruck (6.8) bzw. (6.9) durch 2 teilbar ist, und dann folgendermassen vorgehen (vgl. [6], Nr. 30).

Betrachten wir den Fall $a = 2^h p_1^h p_2^h$, so ist nach (4.1)

$$T_w(a) = \prod_w G_w(Z^k, Z_{1^1}^k, Z_{2^2}^k),$$

worin das Produkt über $k = 0, 1, \ldots, s-1$ und $k_j = 1, 3, \ldots, \varphi_j - 1$ $(j = 1, 2)$ zu erstrecken ist. Wir wählen für k_j $(j = 1, 2)$ speziell den Wert $\varphi_j/2^{\delta(j)}$, wobei $\delta(j)\,(>0)$ durch $2^{\delta(j)} \parallel \varphi_j$ definiert ist. Dann ist $Z_j^{kj} = \exp(2\pi i/2^{\delta(j)})$ eine Einheitswurzel, deren Ordnung eine Potenz von 2 ist, und dasselbe gilt für $Z^k Z_{1^1}^k Z_{2^2}^k$ mit beliebig festgewähltem k $(0 \leqq k \leqq s-1)$. Es sei 2^δ die Ordnung dieser Einheitswurzel und $\xi = \exp(2\pi i/2^\delta)$, und weiter sei $\mathfrak{b} = (1-\xi)$ der Primidealteiler von 2 im 2^δ-ten Kreiskörper. Nach (6.5) gilt nun in diesem Körper

$$G_w(Z^k, Z_{1^1}^k, Z_{2^2}^k) \equiv \sum_{n=0}^{s-1} \sum_{i=0}^{t-1} \sum_{j=0}^{u-1} P(n, i, j) \pmod{\mathfrak{b}},$$

denn jedes $Z^{kn} Z_{1^1}^{k\,i} Z_{2^2}^{k\,j}$ im Ausdruck von G_w ist kongruent zu 1 (mod $\mathfrak{b}$). Weil ferner die rechte Seite der erhaltenen Kongruenz gerade ist, ergibt sich $G_w \equiv 0 \pmod{\mathfrak{b}}$ und dadurch auch $T_w(a) \equiv 0 \pmod{\mathfrak{b}}$, woraus die Behauptung folgt.

Der Fall des ungeraden a kann analog behandelt werden. Dabei hat man zu bemerken, dass jedes k_j $(j = 1, 2, 3)$ in Π_w ungerade Werte annimmt und sich folglich derart festwählen lässt, dass die Ordnung von $Z_{1^1}^k Z_{2^2}^k Z_{3^3}^k$ eine Potenz von 2 ist.

§ 7. Die Beziehung zwischen $H_1(p^h m)$ und $H_1(p^{h-1} m)$

22. Es sei p eine Primzahl, die nicht in m enthalten ist, und sei $p^h \geqq 3$. Der erste Faktor der Klassenzahl des $p^h m$-ten Kreiskörpers lässt sich unter Anwendung von (6.1) mittels $H_1(m)$ ausdrücken: es ergibt sich

$$H_1(p^h m) = \tfrac{1}{2} H_1(p^h) H_1(m) \prod_a \prod_{w \in Y} T_w(p^h a), \tag{7.1}$$

wobei das äussere Produkt über alle Teiler $a\,(>1)$ von m mit der Eigenschaft $(a, m/a) = 1$ zu erstrecken ist und im inneren Produkt Y die bekannte durch $p^h a$ bestimmte Menge gewisser Zahlenfolgen bedeutet. (S. Nr. 8; eigentlich hätte man Y_l statt Y zu bezeichnen, wobei l die Anzahl der verschiedenen ungeraden Primteiler von $p^h a$ bedeutet.)

Ist auch $p^{h-1} \geqq 3$, so kann man ganz entsprechend $H_1(p^h m)$ mit Hilfe von $H_1(p^{h-1} m)$ ausdrücken. Mit den vorigen Bezeichnungen samt

$$K(p^h) = H_1(p^h)/H_1(p^{h-1}),$$
$$L_w(p^h a) = T_w(p^h a)/T_w(p^{h-1} a)$$

liefert die Formel (6.1) jetzt die Darstellung

$$H_1(p^h m) = K(p^h) H_1(p^{h-1} m) \prod_a \prod_{w \in Y} L_w(p^h a) . \tag{7.2}$$

Unsere Absicht ist es, im folgenden für $L_w(p^h a)$ einen Ausdruck herzuleiten, der im zweiten Kapitel anwendbar ist und ausserdem die Ganzheitsnatur von $L_w(p^h a)$ zum Vorschein bringt. Zuerst wollen wir jedoch eine Bemerkung über $K(p^h)$ machen.

23. Der Faktor $K(p^h)$ ist zuerst von WEBER [23] für $p = 2$ und von WESTLUND [24] für $p > 2$ behandelt worden. Diese haben einen Ausdruck für $K(p^h)$ auf eine ziemlich komplizierte Weise hergeleitet und darüber hinaus u.a. gezeigt, dass es sich um eine ganze Zahl handelt.

Wir finden es bemerkenswert, dass sich der genannte Ausdruck von $K(p^h)$ sehr einfach von (1.3) ausgehend ableiten lässt. In der Tat ergibt diese Formel zuerst (für $p^{h-1} \geqq 3$)

$$K(p^h) = p \prod_\chi (2p^h)^{-1} \sum_{l=1}^{p^h} (-\chi(l) l) , \tag{7.3}$$

wobei das Produkt über die ungeraden primitiven Charaktere $\chi \pmod{p^h}$ zu erstrecken ist. Setzt man $\varphi = \varphi(p^h)$ und

$$X = \begin{cases} \exp(2\pi i/\varphi) & \text{für } p > 2 , \\ \exp(2\pi i/\tfrac{1}{2}\varphi) & \text{für } p = 2 , \end{cases}$$

so lassen sich die von Null verschiedenen Werte der Charaktere $\pmod{p^h}$ $(p^h \geqq 3)$ in der folgenden Form darstellen:

$$\chi_k(l) = \begin{cases} X^{kn} \text{ für } l \equiv r^n \pmod{p^h}, \text{ wenn } p > 2 , \\ (-1)^{\bar{n}} X^{kn} \text{ für } l \equiv (-1)^{\bar{n}} 5^n \pmod{p^h}, \text{ wenn } p = 2 \end{cases}$$

(r bedeutet eine primitive Wurzel $\pmod{p^h}$, $p > 2$). Hierin erhält man genau alle ungeraden Charaktere $\chi_k \pmod{p^h}$, indem man k die Werte

$$\begin{cases} 1, 3, \ldots, \varphi - 1 \text{ für } p > 2 , \\ 0, 1, \ldots, \tfrac{1}{2}\varphi - 1 \text{ für } p = 2 \end{cases} \tag{7.4}$$

durchlaufen lässt (vgl. (2.2) und (2.3)). Angenommen, dass $p^{h-1} \geqq 3$ gilt, sind nun von diesen Charakteren χ_k genau diejenigen primitiv $\pmod{p^h}$, worin k nicht durch p teilbar ist. Die Anzahl solcher χ_k ist gleich $(\varphi - \varphi')/2$, mit $\varphi' = \varphi(p^{h-1})$, sodass (7.3) die Gestalt

$$K(p^h) = 2^{(\varphi'-\varphi)/2} p^{1+h(\varphi'-\varphi)/2} \prod_{p \nmid k} \sum_{l=1}^{p^h} (-\chi_k(l) l) \tag{7.5}$$

annimmt, wobei die Multiplikation also über die durch p unteilbaren Werte von (7.4) zu erstrecken ist. Im Fall $p > 2$ können wir hier die Minuszeichen bei χ_k weglassen, da $(\varphi - \varphi')/2$ gerade ist, und somit haben wir das Ergebnis von WESTLUND ([24], S. 204).

Im Fall $p = 2$ (und also $h \geqq 3$) geht man noch weiter. Unter Betrachtung der Kongruenzen

$$l \equiv \pm 5^x, \quad 2^{h-1} - l \equiv \pm 5^y \pmod{2^h}$$

erkennt man das Bestehen der Beziehung $\chi_k(2^{h-1} - l) = \chi_k(l)$, wenn χ_k primitiv (mod 2^h) ist. Da ausserdem $\chi_k(2^h - l) = -\chi_k(l)$ ist, gilt für die Summen in (7.5)

$$\sum_{l=1}^{2^h} (-\chi_k(l)l) = \sum_{l=1}^{2^{h-1}} \chi_k(l)(2^h - 2l) = 2^h \sum_{l=1}^{2^{h-2}} \chi_k(l)$$

(vgl. [6], S. 79—80). Demnach ist

$$K(2^h) = 2^f \prod_{2 \nmid k} \sum_{l=1}^{2^{h-2}} \chi_k(l)$$

mit $f = 1 + (\varphi' - \varphi)/2 = 1 - 2^{h-3}$, was das bekannte Resultat von WEBER ist ([23], S. 800—801).

24. Um $L_w(p^h a)$ zu untersuchen, gehen wir von dem Ausdruck von $T_w(p^h a)$ aus. Wir nehmen fortwährend $p^h \geqq 3$ an, setzen

$$X_h = \begin{cases} \exp(2\pi i/\varphi(p^h)) & \text{für } p > 2\,, \\ \exp(2\pi i/\tfrac{1}{2}\varphi(p^h)) & \text{für } p = 2 \end{cases}$$

und schreiben kurz (vgl. (4.1))

$$T_w(p^h a) = \prod_w G_{w,h}(X_h^{k(h)}, \mathbf{Z}^{\mathbf{k}}) \quad (w \in Y)\,, \tag{7.6}$$

wobei die Bezeichnung G_w durch $G_{w,h}$ ersetzt worden ist und $\mathbf{Z}^{\mathbf{k}}$ alle von a herrührenden Bezeichnungen repräsentiert. Ausserdem bedeutet w hier eine Folge von $\omega(p^h a)$ Zahlen, die gleich 1 oder 0 sind und die Werte der Exponenten $k(h)$ und $\mathbf{k}$ im Produkt Π_w bestimmen. Wir verabreden, dass das erste Glied von w die von $k(h)$ angenommenen Werte bestimmt; diese sind also

$$\begin{cases} 1, 3, \ldots, \varphi(p^h) - 1 \text{ oder } 2, 4, \ldots, \varphi(p^h) - 2 \text{ für } p > 2\,, \\ 0, 1, \ldots, \tfrac{1}{2}\varphi(p^h) - 1 \text{ oder } 1, 2, \ldots, \tfrac{1}{2}\varphi(p^h) - 1 \text{ für } p = 2\,, \end{cases} \tag{7.7}$$

je nachdem ob $w = (1, \ldots)$ oder $w = (0, \ldots)$ ist.

Durch jede Exponentenfolge $k(h), \mathbf{k}$ in Π_w wird ein Charakter $\chi \pmod{p^h a}$ bestimmt derart, dass

$$G_{w,h}(X_h^{k(h)}, \mathbf{Z}^{\mathbf{k}}) = (-2p^h a)^{-1} \sum_{l=1}^{p^h a} \chi(l) l \tag{7.8}$$

gilt (vgl. (3.1) und (2.5)).

Es sei jetzt $p^{h-1} \geqq 3$. Dann bestehen die vorigen Aussagen auch in dem Fall, dass h durch $h-1$ ersetzt ist.

Nimmt $k(h)$ in (7.8) irgendeinen durch p teilbaren Wert an, so ergibt sich mit festgewähltem $\mathbf{k}$

$$G_{w,h}(X_h^{k(h)}, \mathbf{Z}^{\mathbf{k}}) = (-2p^h a)^{-1} \sum_{l=1}^{p^h a} \chi'(l) l\,, \tag{7.9}$$

wobei χ' derjenige Charakter $(\mathrm{mod}\ p^{h-1}a)$ ist, den die Exponentenfolge $k(h)/p, \mathbf{k}$ bestimmt. Denkt man in (7.8) h durch $h-1$ ersetzt, bekommt man folglich

$$G_{w,h-1}(X_{h-1}^{k(h-1)}, \mathbf{Z}^{\mathbf{k}}) = (-2p^{h-1}a)^{-1} \sum_{l=1}^{p^{h-1}a} \chi'(l) l \tag{7.10}$$

mit $k(h-1) = k(h)/p$.

Nach Hilfssatz 1 sind die rechten Seiten von (7.9) und (7.10) gleich. Wir haben also das Ergebnis

$$G_{w,h}(X_h^{k(h)}, \mathbf{Z}^{\mathbf{k}}) = G_{w,h-1}(X_{h-1}^{k(h-1)}, \mathbf{Z}^{\mathbf{k}})\,, \quad k(h) = pk(h-1)\,. \tag{7.11}$$

Man hat nun zu beachten, dass $k(h-1)$ alle seine Werte annimmt, wenn $k(h)$ alle seine durch p teilbaren Werte durchläuft. Nach (7.11) ist somit das Produkt aller solchen Faktoren in Π_w, worin $k(h)$ durch p teilbar ist, gleich $T_w(p^{h-1}a)$. Daraus folgt die gesuchte Formel

$$L_w(p^h a) = \prod\nolimits_w' G_{w,h}(X_h^{k(h)}, \mathbf{Z}^{\mathbf{k}})\,, \tag{7.12}$$

wobei der Strich bedeutet, dass von Π_w alle durch p teilbaren Werte von $k(h)$ auszuschliessen sind.

Zuletzt wollen wir einen Hilfssatz heranziehen, der sich aus (7.11) durch Induktion ergibt, wenn man darin zuerst

$$X_h^{k(h)} = X_h^{pk(h-1)} = X_{h-1}^{k(h-1)}$$

setzt.

Hilfssatz 6. *Ist* $g \leqq h$ *und* $p^g \geqq 3$, *so gilt*

$$G_{w,h}(X_g^{k(g)}, \mathbf{Z}^{\mathbf{k}}) = G_{w,g}(X_g^{k(g)}, \mathbf{Z}^{\mathbf{k}})\,,$$

wobei $k(g)$ *einen beliebigen im Ausdruck*

$$T_w(p^g a) = \prod\nolimits_w G_{w,g}(X_g^{k(g)}, \mathbf{Z}^{\mathbf{k}})$$

auftretenden Wert hat.

ZWEITES KAPITEL. TEILBARKEITSEIGENSCHAFTEN DES ERSTEN FAKTORS DER KLASSENZAHL

§ 8. Über die Teilbarkeit von $H_1(p^h m)$ durch p

25. Auf der Grundlage der vorigen Ausführungen wollen wir einige Bemerkungen über die Teilbarkeit des Faktors $H_1(p^h m)$ durch p machen. Hier bedeutet p, wie in § 7, eine nicht in m steckende Primzahl mit $p^h \geqq 3$.

Betrachten wir die Formel (7.2), wobei $K(p^h)$ sowie sämtliche $L_w(p^h a)$ ganze Zahlen sind, so erkennen wir, dass in $H_1(p^h m)$ alle Primteiler von $H_1(p^{h-1}m)$ $(p^{h-1} \geqq 3)$ enthalten sind. In gewissen Fällen enthält aber $H_1(p^h m)$ bei wachsendem h den Primteiler p zur wachsenden Potenz, wie der folgende, die Faktoren $T_w(p^h a)$ von $H_1(p^h m)$ (s. (7.1)) betreffende Satz herausstellt.

Zur bequemeren Formulierung des Satzes schreiben wir den Ausdruck (7.6) von $T_w(p^h a)$ in der Form

$$T_w(p^h a) = \prod_{k(h)} C_{w,h}(X_h^{k(h)}) , \tag{8.1}$$

wobei $k(h)$ die aus (7.7) hervorgehenden Zahlen durchläuft und

$$C_{w,h}(X_h^{k(h)}) = \prod_{\mathbf{k}} G_{w,h}(X_h^{k(h)}, \mathbf{Z}^{\mathbf{k}}) \tag{8.2}$$

gesetzt ist (für Bezeichnungen s. Nr. 24). Es sei bemerkt, dass die Zahl $C_{w,h}(X_h^{k(h)})$ zum $\varphi(p^h)$-ten bzw. $\frac{1}{2}\varphi(p^h)$-ten Kreiskörper gehört, je nachdem ob $p > 2$ oder $p = 2$ ist.

Wir können jetzt den Satz aussprechen:

Satz 6. 1) *Es sei* $p > 2$ *und* $\mathfrak{p}$ *ein Primidealteiler von* p *im* $(p-1)$*-ten Kreiskörper. Sind von den Zahlen*

$$C_{w,1}(X_1^{k(1)}) \quad (k(1) = 1, 3, \ldots, p-2)$$

mit $w = (1, \ldots)$ *z durch* $\mathfrak{p}$ *teilbar, so gilt*

$$T_w(p^h a) \equiv 0 \pmod{p^{hz}} \quad (h \geqq 1) .$$

2) *Es sei* $p = 2$. *Ist* $T_w(4a)$ *durch* 2^z $(z \geqq 1)$ *teilbar, so gilt*

$$T_w(2^h a) \equiv 0 \pmod{2^{z+h-2}} \quad (h \geqq 2) .$$

26. Wir beweisen zuerst den ersten Teil des Satzes und nehmen also $p > 2$ an.

Aus den Voraussetzungen folgt nach (8.1) zunächst

$$T_w(pa) \equiv 0 \pmod{\mathfrak{p}^z} .$$

Da bekanntlich $\mathfrak{p}$ in p genau zur ersten Potenz aufgeht, ergibt sich hieraus die Behauptung im Fall $h = 1$.

Es genügt jetzt zu zeigen, dass für $h \geqq 2$ die ganzrationale Zahl

$$L_w(p^h a) = T_w(p^h a)/T_w(p^{h-1} a) = \prod_{p \nmid k(h)} C_{w,h}(X_h^{k(h)}) \tag{8.3}$$

(s. (7.12)) durch p^z teilbar ist. Dazu setzt man

$$\Theta_h = \exp(2\pi i/p^h) \quad (h \geqq 1)$$

und betrachtet die Ideale $\mathfrak{p}$ und $\mathfrak{a} = (\mathfrak{p}, 1 - \Theta_{h-1})$ des Körpers $k(X_1, \Theta_{h-1})$. Bekanntlich ist $\mathfrak{a}$ ein Primidealteiler von p, und seine $\varphi(p^{h-1})$-te Potenz ist gleich $\mathfrak{p}$.

Nach Hilfssatz 6 gilt für $h \geqq 2$

$$C_{w,h}(X_1^{k(1)}) = C_{w,1}(X_1^{k(1)}) \quad (k(1) = 1, 3, \ldots, p-2) ,$$

sodass jetzt $C_{w,h}(X_1^{k(1)})$ für z Werte von $k(1)$ durch $\mathfrak{p}$ teilbar ist. Für diese Werte von $k(1)$ besteht dann wegen $\Theta_{h-1} \equiv 1 \pmod{\mathfrak{a}}$ die Kongruenz

$$C_{w,h}(X_1^{k(1)} \Theta_{h-1}^n) \equiv 0 \pmod{\mathfrak{a}} \tag{8.4}$$

mit beliebigem ganzem n.

Man hat nun zu beachten, dass

$$X_1^{k(1)} \Theta_{h-1}^n = X_h^N \text{ mit } N = p^{h-1} k(1) + (p-1) n$$

ist. Gibt man hier für $k(1)$ seine Werte $1, 3, \ldots, p-2$ und für n alle durch p unteilbaren Werte der Folge $1, \ldots, p^{h-1} - 1$, so bekommt man $\frac{1}{2}(\varphi(p^h) - \varphi(p^{h-1}))$ Zahlen X_h^N, wobei die Werte von N ungerade, durch p unteilbar und paarweise inkongruent $(\mathrm{mod}\ \varphi(p^h))$ sind. Beim Vergleich dieser Werte von N mit den Werten von $k(h)$ in (8.3) (s. (7.7)) ersieht man, dass das über alle diese N erstreckte Produkt der Zahlen $C_{w,h}(X_h^N)$ gleich $L_w(p^h a)$ ist.

Wie aus (8.4) hervorgeht, gibt es unter den Zahlen $C_{w,h}(X_h^N)$ $z\varphi(p^{h-1})$ solche, die durch $\mathfrak{a}$ teilbar sind. Demnach ist $L_w(p^h a)$ durch die $z\varphi(p^{h-1})$-te Potenz von $\mathfrak{a}$, also durch $\mathfrak{p}^z$ teilbar, und dies beweist unsere Behauptung.

27. Der zweite Teil von Satz 6 wird bewiesen, indem man zeigt, dass unter der Annahme

$$T_w(4a) \equiv 0 \pmod{2^z} \tag{8.5}$$

die Zahl $L_w(2^h a)$ $(h \geqq 3)$ gerade ist.

Nach (8.1) folgt aus (8.5), dass $T_w(4a) = C_{w,2}(1)$ mit $w = (1, \ldots)$ sein muss (vgl. Anm. 1). Unter Berücksichtigung der Beziehung $C_{w,h}(1) = C_{w,2}(1)$, die sich aus Hilfssatz 6 ergibt, kann man somit aus (8.5) die Kongruenz

$$C_{w,h}(1) \equiv 0 \pmod{2}$$

folgern.

Es gilt nun im 2^{h-2}-ten Kreiskörper $k(X_h)$, worin $\mathfrak{b} = (1 - X_h)$ der Primidealteiler von 2 ist, die Beziehung

$$C_{w,h}(X_h) \equiv C_{w,h}(1) \equiv 0 \pmod{\mathfrak{b}}\,.$$

Daher enthält $L_w(2^h a)$, das von der Form (8.3) mit $p = 2$ ist, den Teiler $\mathfrak{b}$ und ist also gerade.

§ 9. Sätze über die Teilbarkeit von $T_1(p^h q^k)$. Folgerungen

28. Es seien p und q verschiedene Primzahlen, $p \geqq 2$ und $q > 2$, und sei $a = p^h q^k$ mit $p^h \geqq 3$ und $k \geqq 1$. Im folgenden beschäftigen wir uns mit dem Faktor

$$T_1(p^h q^k) = T_{w(1)}(p^h q^k) \quad (w(1) = (1, 0))$$

von $T(p^h q^k)$ (s. Nr. 15), und zwar betrachten wir seine Teilbarkeit namentlich durch p.

Hierbei ist sogleich zu bemerken, dass unter der Annahme $p^h q^k \mid m$ die Zahl $H_1(m)$ sämtliche Primteiler von $T_1(p^h q^k)$ enthält, möglicherweise einen Primteiler 2 ausgenommen. In der Tat, wenn zuerst $p^{h'} \parallel m$, $q^{k'} \parallel m$ gilt, so ergibt (6.1) unter Beachtung der Resultate von § 6 die Beziehung $H_1(m) = \frac{1}{2} T_1(p^{h'} q^{k'}) N_1$, wobei N_1 eine ganzrationale Zahl ist. Hier ist weiter $T_1(p^{h'} q^{k'}) = T_1(p^h q^k) N_2$ mit ganzrationalem N_2, wie die Ausführungen von § 7 zeigen.

Es gilt also der

Satz 7. *Ist $p^h q^k \mid m$, so besteht die Kongruenz*

$$2H_1(m) \equiv 0 \pmod{T_1(p^h q^k)}\,.$$

Unser Hauptziel ist der Nachweis der untenstehenden drei Sätze. Dabei bedeuten p und q, wie durchweg in den folgenden Betrachtungen,

ungerade Primzahlen. (Ausserdem bedeutet die Bezeichnung $[x]$ wie üblich die grösste ganze Zahl $\leqq x$.)

Zuerst haben wir als eine Anwendung von Satz 6 den

Satz 8. *Es gilt*

$a)$ $T_1(p^h q) \equiv 0 \pmod{p^{h(p-3)/2}}$, *wenn* $q \equiv 1 \pmod{p}$ $(h \geqq 1)$,
$b)$ $T_1(p^h q) \equiv 0 \pmod{p^{h(p-1)/2}}$, *wenn* $q \equiv 1 \pmod{p^2}$ $(h \geqq 1)$,
$c)$ $T_1(2^h q) \equiv 0 \pmod{2^h}$, *wenn* $q \equiv 1 \pmod{8}$ $(h \geqq 2)$.

Erfüllt q grössere Forderungen als im vorigen Satz, so enthält $T_1(a)$ den Teiler p bzw. 2 zur wesentlich höheren Potenz:

Satz 9. *a) Ist* $h \geqq 1$, $b \geqq 0$ *und* $q \equiv 1 \pmod{p^{h+b}}$, *so gilt*

$$T_1(p^h q) \equiv 0 \pmod{p^M} \text{ mit } M = \tfrac{1}{2}(p^h + p^{h-1}) - r(h, b),$$

wobei $r(h, 0) \leqq [\frac{1}{2}(h+3)]$ *und* $r(h, b) \leqq [\frac{1}{2}(1 + hp^{-b})]$ *für* $b \geqq 1$ *ist.*
b) Ist $h \geqq 2$, $b \geqq 0$, $h + b \geqq 3$ *und* $q \equiv 1 \pmod{2^{h+b}}$, *so gilt*

$$T_1(2^h q) \equiv 0 \pmod{2^M} \quad \text{mit} \quad M = 2^h + b \cdot 2^{h-2} - h - 1.$$

Die Sätze 8 und 9 besagen nichts von den beiden Fällen

$$a = 3q \text{ mit } q \equiv 1 \pmod{3},\ q \not\equiv 1 \pmod{9};$$
$$a = 4q \text{ mit } q \equiv 1 \pmod{4},\ q \not\equiv 1 \pmod{8}.$$

Im folgenden Satz, der von etwas anderem Typ ist, sind auch diese Fälle enthalten.

Satz 10. *Es gilt für* $k \geqq 1$

$a)$ $T_1(3q^k) \equiv 0 \pmod{\varphi(q^k)/6}$, *wenn* $q \equiv 1 \pmod{3}$,
$b)$ $T_1(4q^k) \equiv 0 \pmod{\varphi(q^k)/4}$, *wenn* $q \equiv 1 \pmod{4}$.

Wir haben als Beispiele zu den vorigen Sätzen einige Werte von $T_1(a)$ berechnet. Es sei in diesem Zusammenhang erwähnt, dass die Werte von $H_1(m)$ für alle $m \leqq 100$ bekannt sind ([15], [6]).

Folgende Werte schliessen sich zunächst an Satz 9 an (vgl. auch Sätze 8 und 10):

$$T_1(5 \cdot 11) = 5, \quad T_1(3 \cdot 19) = 3^2, \quad T_1(3^2 \cdot 19) = 3^6 \cdot 19 \cdot 109,$$
$$T_1(2^2 \cdot 17) = 2^3, \quad T_1(2^3 \cdot 17) = 2^6 \cdot 3^2, \quad T_1(2^4 \cdot 17) = 2^{12} \cdot 3^2 \cdot 13 \cdot 17 \cdot 41.$$

Als Beispiele zu Satz 10 mögen noch

$$T_1(3 \cdot 13) = 2, \quad T_1(3 \cdot 31) = 5 \cdot 151, \quad T_1(3 \cdot 7^2) = 7 \cdot 29 \cdot 673,$$
$$T_1(4 \cdot 13) = 3, \quad T_1(4 \cdot 5^2) = 5 \cdot 11, \quad T_1(4 \cdot 29) = 2^6 \cdot 3 \cdot 7$$

dienen.

29. Mittels der vorigen Sätze lässt sich das folgende Problem auf verschiedene Weise lösen: Für eine gegebene ganze Zahl n ist ein solcher Kreiskörper zu finden, dessen erster Faktor der Klassenzahl durch n teilbar ist.

Es sei etwa $n = 2^g p_1^{g_1} \dots p_r^{g_r}$, wobei $p_1, \dots, p_r$ paarweise verschiedene ungerade Primzahlen sind und $g \geqq 0$, $g_j > 0$ $(j = 1, \dots, r)$ gilt. Sind nun $q, q_1, \dots, q_r$ weitere paarweise verschiedene ungerade Primzahlen $(q \neq p_j, q_i \neq p_j$ für $i, j = 1, \dots, r)$ und enthält m den Teiler

$$2^h p_1^{h_1} \dots p_r^{h_r} q q_1 \dots q_r \tag{9.1}$$

mit $h \geqq 2$, $h_j \geqq 1$ $(j = 1, \dots, r)$, so gilt

$$H_1(m) = \tfrac{1}{2} T_1(2^h q)\, T_1(p_1^{h_1} q_1) \dots T_1(p_r^{h_r} q_r) N$$

(s. § 6), wobei N eine ganzrationale Zahl ist. Nach Satz 8 oder Satz 9 folgt daraus $H_1(m) \equiv 0 \pmod{n}$, wenn nur die Exponenten $h, h_1, \dots, h_r$ genügend gross sind und $q, q_1, \dots, q_r$ gewisse Kongruenzen von der Form

$$q \equiv 1 \pmod{2^l}, \quad q_j \equiv 1 \pmod{p_j^{l_j}} \quad (j = 1, \dots, r)$$

erfüllen.

Unter Zuhilfenahme von Satz 10 lassen sich viele weitere Lösungen für m finden, z.B.

$$m = 3 q q_1 \dots q_r \tag{9.2}$$

mit

$$q \equiv 1 \pmod{3 \cdot 2^{g+2}}, \quad q_j \equiv 1 \pmod{6 p_j^{g_j}} \quad (j = 1, \dots, r)\,.$$

— Offenbar genügt es auch, das Produkt $q q_1 \dots q_r$ in (9.1) und (9.2) durch eine einzige Primzahl q zu ersetzen, die dann die Kongruenzen

$$q \equiv 1 \pmod{2^l p_1^{l_1} \dots p_r^{l_r}} \text{ bzw. } q \equiv 1 \pmod{12n}$$

erfüllen muss.

§ 10. Hilfsbetrachtungen

30. Bei der Behandlung von $T_1(a)$ mit $a = p^h q^k$ oder $2^h q^k$ werden wir dieselben Bezeichnungen wie im ersten Kapitel, besonders in § 5, benutzen; dabei muss man nur $p_1^{h_1}$ durch p^h und $p_2^{h_2}$ durch q^k ersetzt denken. Demgemäss bedeutet r_1 bzw. r_2 eine primitive Wurzel $(\bmod p^h)$ bzw. $(\bmod q^k)$, und weiter ist

$$s = 2^{h-2}, \quad t = \tfrac{1}{2}\varphi(p^h), \quad u = \tfrac{1}{2}\varphi(q^k),$$
$$Z = e^{2\pi i/s}, \quad Z_1 = e^{2\pi i/2t}, \quad Z_2 = e^{2\pi i/2u}.$$

Ausserdem brauchen wir u.a. die in Nr. 6 definierten Zahlen $R(i,j) = R_a(i,j)$ mit $a = p^h q^k$ und $R(0,i,j) = R_a(0,i,j)$ mit $a = 2^h q^k$, sowie die Zahlen $P(i,j)$, die durch (5.4) für $a = p^h q^k$ und durch (5.11) für $a = 2^h q^k$ gegeben sind.

31. Wir sprechen zunächst einige Hilfssätze aus.

Hilfssatz 7. *Ist* $a = p^h q^k$ *und* $q \equiv 1 \pmod{p^h}$, *so gilt*

$$\sum_{j=0}^{2u-1} R(i,j) = ua \quad (i = 0, \ldots, t-1) .$$

Beweis. Bedeutet R_i, $i = 0, \ldots, t-1$, den kleinsten positiven Rest von $r_1^i \pmod{p^h}$, so besteht die Kongruenz

$$R(i,j) \equiv R_i \pmod{p^h} .$$

Unter Berücksichtigung der Annahme $q \equiv 1 \pmod{p^h}$ erkennt man jetzt, dass $R(i,j)$ bei $j = 0, \ldots, 2u-1$ diejenigen Werte durchläuft, die man bekommt, indem man von den Zahlen

$$R_i + Np^h \quad (N = 0, \ldots, q^k - 1)$$

die Zahlen

$$q(R_i + np^h) \quad (n = 0, \ldots, q^{k-1} - 1)$$

ausschliesst (vgl. den Beweis von Hilfssatz 5). Demnach lässt sich die betreffende Summe leicht berechnen.

Auf dieselbe Weise beweist man den

Hilfssatz 7′. *Ist* $a = 2^h q^k$ *und* $q \equiv 1 \pmod{2^h}$, *so gilt*

$$\sum_{j=0}^{2u-1} R(0,i,j) = ua \quad (i = 0, \ldots, s-1) .$$

In den folgenden Hilfssätzen ist speziell $k = 1$ gesetzt.

Hilfssatz 8. *Ist* $a = p^h q$ *und entweder*

(I) $$q \equiv 1 \pmod{p^{h+1}}, \; c \geqq 1$$

oder

(II) $$q \equiv 1 \pmod{p^h}, \; 1 \leqq c \leqq t-1,$$

so gilt

$$\sum_{i=0}^{t-1} \sum_{j=0}^{u-2} P(i,j) r_1^{(2c-1)i} \equiv 0 \pmod{p} .$$

Beweis. Nach der Definition (5.4) von $P(i,j)$ gilt für $i = 0, \ldots, t-1$

$$a\sum_{j=0}^{u-2} P(i,j) = u(R(i,u-1) + R(i,2u-1)) - \sum_{j=0}^{2u-1} R(i,j)\,.$$

Aus

$$R(i,u-1) + R(i,2u-1) \equiv \begin{cases} 2r_1^i \pmod{p^h}\,, \\ 0 \pmod{q} \end{cases}$$

folgt wegen $q \equiv 1 \pmod{p^h}$, dass hierbei

$$R(i,u-1) + R(i,2u-1) = 2r_1^i q + n_i a \tag{10.1}$$

mit ganzem n_i gilt. Unter Beachtung von Hilfssatz 7 bekommen wir also

$$a\sum_{j=0}^{u-2} P(i,j) = 2ur_1^i q + (n_i - 1)ua\,.$$

Das erhaltene Ergebnis liefert ferner die Kongruenz

$$\sum_{i=0}^{t-1}\sum_{j=0}^{u-2} P(i,j) r_1^{(2c-1)i} \equiv ((q-1)/p^h)\sum_{i=0}^{t-1} r_1^{2ci} \pmod{p}\,,$$

da $u = \frac{1}{2}(q-1)$ durch p teilbar ist. Unter den Voraussetzungen (I) ist hier $(q-1)/p^h$ durch p teilbar und die behauptete Kongruenz somit richtig. Unter den Voraussetzungen (II) gilt zuerst $r_1^{2c} - 1 \equiv 0 \pmod{p^h}$, andererseits aber

$$(r_1^{2c} - 1)\sum_{i=0}^{t-1} r_1^{2ci} = r_1^{2ct} - 1 \equiv 0 \pmod{p^h}\,,$$

sodass

$$\sum_{i=0}^{t-1} r_1^{2ci} \equiv 0 \pmod{p}$$

ist. Damit ist der Beweis beendet.

Hilfssatz 8'. *Ist* $a = 2^h q$ *und entweder*

$$h = 2 \quad \textit{und} \quad q \equiv 1 \pmod 8 \tag{I'}$$

oder

$$h \geqq 3 \quad \textit{und} \quad q \equiv 1 \pmod{2^h}\,, \tag{II'}$$

so gilt

$$\sum_{i=0}^{s-1}\sum_{j=0}^{u-2} P(i,j) \equiv 0 \pmod 2.$$

Beweis. Auf ähnliche Schlussweise wie im vorigen Beweis gewinnt man die Kongruenz

$$\sum_{i=0}^{s-1}\sum_{j=0}^{u-2} P(i,j) \equiv ((q-1)/2^h) \sum_{i=0}^{s-1} 5^i \pmod 2 .$$

Hierbei ist auf der rechten Seite entweder der Quotient oder die Summe $\equiv 0 \pmod 2$, je nachdem ob die Voraussetzungen (I') oder (II') bestehen.

§ 11. Beweis der Sätze 8 und 9

32. Wie aus (5.1) hervorgeht, besitzt $T_1(p^h q)$ den Ausdruck

$$T_1(p^h q) = \prod_{c=1}^{t}\prod_{d=1}^{u-1} G_1(Z_1^{2c-1}, Z_2^{2d}) , \tag{11.1}$$

wobei nach (5.3)

$$G_1(Z_1^{2c-1}, Z_2^{2d}) = \sum_{i=0}^{t-1}\sum_{j=0}^{u-2} P(i,j) Z_1^{(2c-1)i} Z_2^{2dj}$$

ist.

Wir wählen für das folgende eine primitive $(p-1)$-te Einheitswurzel ϑ_1 und eine primitive p^{h-1}-te Einheitswurzel ϑ_2 derart, dass $Z_1 = \vartheta_1\vartheta_2$ gilt.

Es sei jetzt $q \equiv 1 \pmod{p^h}$ mit $h \geqq 1$. Wir setzen $f = (q-1)/p^h$, sodass f eine gerade ganze Zahl ist und

$$Z_2^f = \exp(2\pi i/p^h)$$

gilt. Dann enthält p im Körper $k(\vartheta_1, Z_2^f)$ den Primidealteiler

$$\mathfrak{a} = (p, \vartheta_1 - r_1, 1 - Z_2^f) \tag{11.2}$$

genau zur $2t$-ten Potenz.

Nach Hilfssatz 8 gilt

$$\sum_{i=0}^{t-1}\sum_{j=0}^{u-2} P(i,j) r_1^{(2c-1)i} \equiv 0 \pmod{\mathfrak{a}^{2t}} \quad (c = 1, \ldots, t-1) . \tag{11.3}$$

Weiter bestehen für $v = 0, \ldots, h-1$ die Kongruenzen

$$\vartheta_1^{p^v} \equiv r_1^{p^v} , \ \vartheta_2^{p^v} \equiv 1 , \ Z_2^{fp^v} \equiv 1 \pmod{\mathfrak{a}^{p^v}} . \tag{11.4}$$

Daher genügen diejenigen Faktoren $G_1(Z_1^{2c-1}, Z_2^{2d})$ von $T_1(p^h q)$, worin $1 \leqq c \leqq t-1$ und $2d = fg$ mit $1 \leqq g \leqq p^h - 1$ ist, der Kongruenz

$$G_1(Z_1^{2c-1}, Z_2^{fg}) \equiv 0 \pmod{\mathfrak{a}^{p^v}} \quad (0 \leqq v \leqq h-1) , \tag{11.5}$$

falls $2c-1$ und g durch p^v teilbar sind.

Es bedeute nun m_v bzw. n_v $(v = 0, \ldots, h-1)$ die Anzahl der obigen Werte von $2c-1$ bzw. g, die durch p^v teilbar sind. Dann gilt offenbar

$$T_1(p^h q) \equiv 0 \pmod{\mathfrak{a}^K} \tag{11.6}$$

mit

$$K = m_0 n_0 + \sum_{v=1}^{h-1} m_v n_v (p^v - p^{v-1}) .$$

Beachtet man, dass

$$m_0 = t-1, \quad m_v = \tfrac{1}{2}(p-1)p^{h-v-1} \quad (v = 1, \ldots, h-1) ,$$
$$n_v = p^{h-v} - 1 \quad (v = 0, \ldots, h-1)$$

ist, so bekommt man für K den Ausdruck

$$K = (t-1)(p^h - 1) + tp^{-1}(p^h - hp + h - 1).$$

Aus (11.6) lässt sich ferner

$$T_1(p^h q) \equiv 0 \pmod{p^M} \tag{11.7}$$

schliessen, wobei M die kleinste ganze Zahl $\geqq K/2t$ ist. Es ergibt sich durch eine einfache Ausrechnung

$$M = \tfrac{1}{2}(p^h + p^{h-1}) - r$$

mit

$$r = [\tfrac{1}{2}(h+1) - \tfrac{1}{2}p^{-1}(h-1) + \tfrac{1}{2}t^{-1}(p^h - 1)] \leqq [\tfrac{1}{2}(h+3)] ,$$

und somit ist der erste Teil von Satz 9 im Fall $b = 0$ bewiesen.

33. Zweitens sei $q \equiv 1 \pmod{p^{h+b}}$ mit $h \geqq 1$ und $b \geqq 1$. Setzt man jetzt $f = (q-1)/p^{h+b}$, so kann man die obige Schlussfolgerung wiederholen.

Im vorliegenden Fall enthält p das Ideal (11.2) genau zur $2tp^b$-ten Potenz. Ausserdem gilt (11.3) auch für $c = t$, wie aus Hilfssatz 8 hervorgeht.

Definiert man m_v und n_v entsprechend wie vorhin, so hat man nunmehr

$$m_v = \tfrac{1}{2}(p-1)p^{h-v-1} , \quad n_v = p^{h+b-v} - 1 \quad (v = 0, \ldots, h-1) .$$

Man erhält also die Kongruenz (11.6) mit

$$K = t(p^{h+b} - 1) + tp^{-1}(p^{h+b} - p^{b+1} - hp + p + h - 1)$$

und daraus weiter die Kongruenz (11.7) mit

$$M = \tfrac{1}{2}(p^h + p^{h-1}) - [\tfrac{1}{2} + \tfrac{1}{2}p^{-b-1}(hp - h + 1)] .$$

Dadurch wird der Beweis des ersten Teiles von Satz 9 vollendet.

34. Wir setzen nun in den Ausführungen von Nr. 32 und Nr. 33 insbesondere $h = 1$ ein.

Unter der Annahme $q \equiv 1 \pmod{p}$ sind nach (11.5) gewisse Faktoren $G_1(Z_1^{2c-1}, Z_2^{2d})$ von $T_1(pq)$ durch $\mathfrak{a}$ teilbar, und zwar diejenigen, worin $1 \leqq c \leqq t-1$ und $2d = fg$ mit $1 \leqq g \leqq p-1$ ist. Demnach erhält man

$$\prod_{d=1}^{u-1} G_1(Z_1^{2c-1}, Z_2^{2d}) \equiv 0 \pmod{\mathfrak{a}^{p-1}} \quad (c = 1, \ldots, t-1) .$$

Hierbei ist weiter $\mathfrak{a}^{p-1} = (p, \vartheta_1 - r_1)$ ein Primidealteiler von p im $(p-1)$-ten Kreiskörper $k(\vartheta_1)$. Man erkennt also, dass die Voraussetzungen des ersten Teiles von Satz 6 mit $z = t-1$ erfüllt sind, sodass nach diesem Satz

$$T_1(p^h q) \equiv 0 \pmod{p^{h(t-1)}} \quad (h \geqq 1)$$

gilt. Damit haben wir die Behauptung *a*) von Satz 8 bewiesen.

Es sei $q \equiv 1 \pmod{p^{h+b}}$ mit $h = b = 1$. Dann bekommt man entsprechend wie oben das Resultat

$$\prod_{d=1}^{u-1} G_1(Z_1^{2c-1}, Z_2^{2d}) \equiv 0 \pmod{\mathfrak{a}^{p^2-1}} \quad (c = 1, \ldots, t) ,$$

wobei $\mathfrak{a}$ ein Ideal mit der Eigenschaft $\mathfrak{a}^{(p-1)p} = (p, \vartheta_1 - r_1)$ ist. Hiernach sind die Voraussetzungen des ersten Teiles von Satz 6 mit $z = t$ erfüllt, und die Behauptung *b*) von Satz 8 ist also richtig.

35. Wir wenden uns dem Fall $a = 2^h q$ zu. Jetzt ist nach (5.9) und (5.10)

$$T_1(2^h q) = \prod_{c=0}^{s-1} \prod_{d=1}^{u-1} G_1(Z^c, Z_2^{2d})$$

mit

$$G_1(Z^c, Z_2^{2d}) = \sum_{i=0}^{s-1} \sum_{j=0}^{u-2} P(i,j) Z^{ci} Z_2^{2dj} .$$

Um den zweiten Teil von Satz 9 zu beweisen, nehmen wir $q \equiv 1 \pmod{2^{h+b}}$ mit $h \geqq 2$, $b \geqq 0$ und $h + b \geqq 3$ an.

Es bedeute jetzt f die gerade ganze Zahl $(q-1)/2^{h+b-1}$. Dann gilt

$$Z_2^f = \exp(2\pi i / 2^{h+b-1}) ,$$

und das Ideal

$$\mathfrak{b} = (1 - Z_2^f)$$

ist ein Primteiler von 2 im 2^{h+b-1}-ten Kreiskörper; bekanntlich ist die 2^{h+b-2}-te Potenz von $\mathfrak{b}$ gleich 2.

Aus Hilfssatz 8′ folgt die Kongruenz

$$\sum_{i=0}^{s-1}\sum_{j=0}^{u-2} P(i,j) \equiv 0 \pmod{\mathfrak{b}^{\varepsilon^{h+b-2}}}.$$

Beachtet man dazu, dass

$$Z \equiv 1 \pmod{\mathfrak{b}^{2^{b+1}}},$$
$$Z^{2^v} \equiv 1 \pmod{\mathfrak{b}^{2^{v+b+1}}} \quad (v = 1, \ldots, h-3),$$
$$Z_2^{2^v f} \equiv 1 \pmod{\mathfrak{b}^{2^v}} \quad (v = 0, \ldots, h+b-2)$$

gilt, so kann man von den Faktoren $G_1(Z^c, Z_2^{fg})$ $(c = 0, \ldots, s-1;$ $g = 1, \ldots, 2^{h+b-1} - 1)$ von $T_1(2^h q)$ folgendes aussagen: es ist

$$G_1(Z^c, Z_2^{fg}) \equiv 0 \pmod{\mathfrak{b}^{2^v}}$$

für

$$\begin{cases} v = 0, \ldots, b, \text{ wenn } 2^v \mid g, \\ v = b+1, \ldots, h+b-2, \text{ wenn } 2^{v-b-1} \mid c,\ 2^v \mid g. \end{cases}$$

Von den hier auftretenden Werten von c sind nun $m_v = 2^{h-v-2}$ durch 2^v teilbar $(v = 0, \ldots, h-2)$, und die entsprechende Anzahl bei g ist $n_v = 2^{h+b-v-1} - 1$ $(v = 0, \ldots, h+b-2)$. Es ergibt sich demgemäss

$$T_1(2^h q) \equiv 0 \pmod{\mathfrak{b}^K}$$

mit

$$K = m_0 n_0 + \sum_{v=1}^{b} m_0 n_v \cdot 2^{v-1} + \sum_{v=b+1}^{h+b-2} m_{v-b-1} n_v \cdot 2^{v-1}$$
$$= 2^{2h+b-2} + b \cdot 2^{2h+b-4} - (h+1)2^{h+b-2}.$$

Dies bedeutet weiter, dass $T_1(2^h q)$ durch die behauptete Potenz von 2 teilbar ist.

Im Spezialfall $h = 2$, $b = 1$ lautet das erhaltene Ergebnis

$$T_1(4q) \equiv 0 \pmod{2^2} \text{ für } q \equiv 1 \pmod 8.$$

Nach Satz 6 folgt daraus die Behauptung $c)$ von Satz 8.

§ 12. Beweis von Satz 10

36. Für den Beweis von Satz 10 nehmen wir zuerst an, dass $a = 3q^k$ mit $q \equiv 1 \pmod 3$ gilt.

Die Zahl $T_1(a)$ ist als eine Determinante $D_1(a)$ darstellbar, deren Gestalt aus (5.8) und (5.6) hervorgeht. Im vorliegenden Fall sind wegen

$t = 1$ die Elemente einer jeden Zeile von $D_1(a)$ (von der Reihenfolge abgesehen)

$$P^n_{00}, \ldots, P^n_{0j}, \ldots, P^n_{0,u-1} \quad (j \neq n),$$

wobei n der Zeilenindex $(1 \leqq n \leqq u-1)$ ist. Nach (5.5) sind also die Zeilensummen

$$S_n = \sum_{j=0}^{u-1} P^n_{0j} = a^{-1}\{u(R(0,n) + R(0,n+u)) - \sum_{j=0}^{2u-1} R(0,j)\}.$$

Analog zu (10.1) gewinnt man jetzt das Resultat

$$R(0,n) + R(0,n+u) = 2q^k + \varrho_n a$$

mit ganzem ϱ_n. Wendet man überdies Hilfssatz 7 an, so ergibt sich

$$S_n = 2u/3 + \varrho_n u - u = (3\varrho_n - 1)\varphi(q^k)/6.$$

Dies hat ferner die Beziehung

$$D_1(a) \equiv 0 \pmod{\varphi(q^k)/6}$$

zur Folge, sodass die Behauptung $a)$ von Satz 10 richtig ist.

Um die Richtigkeit der Behauptung $b)$ einzusehen, geht man in derselben Weise vor. Unter der Annahme $a = 4q^k$ mit $q \equiv 1 \pmod 4$ wird die Determinante $D_1(a)$ von ähnlicher Form wie vorhin sein, und ihre Zeilensummen sind nach (5.12)

$$S_n = \sum_{j=0}^{u-1} P^n_{0j} = a^{-1}\{u(R(0,0,n) + R(0,0,n+u)) - \sum_{j=0}^{2u-1} R(0,0,j)\}.$$

Unter Anwendung von Hilfssatz 7′ schliesst man daraus

$$S_n = (2\varrho_n - 1)\varphi(q^k)/4,$$

wobei die ganze Zahl ϱ_n die entsprechende Bedeutung hat wie oben. Folglich gilt

$$D_1(a) \equiv 0 \pmod{\varphi(q^k)/4},$$

wie zu zeigen war.

Universität Turku
Turku, Finnland

Literatur

[1] CARLITZ, L. — OLSON, F. R.: Maillet's determinant. - Proc. Amer. Math. Soc. 6 (1955), 265—269.

[2] FRÖHLICH, A.: On a method for the determination of class number factors in number fields. - Mathematika 4 (1957), 113—121.

[3] FURTWÄNGLER, PH.: Über die Klassenzahlen der Kreisteilungskörper. - J. Reine Angew. Math. 140 (1911), 29—32.

[4] GUT, M.: Die Zetafunktion, die Klassenzahl und die Kroneckersche Grenzformel eines beliebigen Kreiskörpers. - Comment. Math. Helv. 1 (1929), 160—226.

[5] —»— Eulersche Zahlen und Klassenanzahl des Körpers der $4l$-ten Einheitswurzeln. - Comment. Math. Helv. 25 (1951), 43—63.

[6] HASSE, H.: Über die Klassenzahl Abelscher Zahlkörper. Berlin (1952).

[7] —»— Vandiver's congruence for the relative class number of the pth cyclotomic field. - J. Math. Anal. Appl. 15 (1966), 87—90.

[8] —»— Vorlesungen über Zahlentheorie. 2. Aufl., Berlin, Göttingen, Heidelberg, New York (1964).

[9] HILBERT, D.: Theorie der algebraischen Zahlkörper. - Jber. Deutsch. Math.-Verein. 4 (1897).

[10] HYYRÖ, S.: Über eine Determinantenidentität und den ersten Faktor der Klassenzahl des Kreiskörpers. - Ann. Acad. Sci. Fenn., Ser. A I 398 (1967).

[11] INKERI, K.: Über die Klassenzahl des Kreiskörpers der l-ten Einheitswurzeln. - Ann. Acad. Sci. Fenn., Ser. A I 199 (1955).

[12] KLEBOTH, H.: Untersuchung über Klassenzahl und Reziprozitätsgesetz im Körper der $6l$-ten Einheitswurzeln und die Diophantische Gleichung $X^{2l} + 3^l Y^{2l} = Z^{2l}$ für eine Primzahl l grösser als 3. - Inaugural-Dissertation, Zürich (1955).

[13] KRONECKER, L.: Über die Klassenanzahl der aus Wurzeln der Einheit gebildeten complexen Zahlen. - Monatsb. Preuss. Akad. Wiss. Berlin (1863). Werke I, 125—131.

[14] KUMMER, E.: Bestimmung der Anzahl nicht äquivalenter Classen für die aus λ-ten Wurzeln der Einheit gebildeten complexen Zahlen und die idealen Factoren derselben. - J. Reine Angew. Math. 40 (1850), 93—116.

[15] —»— Über die Klassenanzahl der aus n-ten Einheitswurzeln gebildeten complexen Zahlen. - Monatsb. Preuss. Akad. Wiss. Berlin (1861), 1051—1053.

[16] —»— Über die Klassenanzahl der aus zusammengesetzten Einheitswurzeln gebildeten complexen Zahlen. - Monatsb. Preuss. Akad. Wiss. Berlin (1863), 21—28.

[17] LEPISTÖ, T.: On the first factor of the class number of the cyclotomic field and Dirichlet's L-functions. - Ann. Acad. Sci. Fenn., Ser. A I 387 (1966).

[18] METSÄNKYLÄ, T.: Bemerkungen über den ersten Faktor der Klassenzahl des Kreiskörpers. - Ann. Univ. Turku., Ser. A I 105 (1967).

[19] MORISHIMA, T.: Über die Einheiten und Idealklassen des Galoisschen Zahlkörpers und die Theorie der Kreiskörper der l^v-ten Einheitswurzeln. - Japan. J. Math. 10 (1933), 83—126.

[20] —»— Über die Theorie der Kreiskörper der l^v-ten Einheitswurzeln II. - Japan. J. Math. 11 (1934), 225—240.

[21] POLLACZEK, F.: Über die irregulären Kreiskörper der l-ten und l^2-ten Einheitswurzeln. - Math. Z. 21 (1924), 1—38.

[22] VANDIVER, H. S.: On the first factor of the class number of a cyclotomic field. - Bull. Amer. Math. Soc. 25 (1919), 458—461.

[23] WEBER, H.: Lehrbuch der Algebra II. 2. Aufl., Braunschweig (1899).

[24] WESTLUND, J.: On the class number of the cyclotomic number field $k(e^{2\pi i/p^n})$. - Trans. Amer. Math. Soc. 4 (1903), 201—212.

Gedruckt Januar 1968