9. *Über die Einheiten und Idealklassen des Galoisschen Zahlkörpers und die Theorie der Kreiskörper der l -ten Einheitswurzeln.*

VON T. MORISHIMA.

(Eingegangen am 5. Juni, 1933.)

Einleitung.

In dieser Arbeit verallgemeinern wir die Ergebnisse von Herrn F. Pollaczek⁽¹⁾ und stellen zugleich noch andere Untersuchungen über die Kreiskörper der l -ten Einheitswurzeln an. Zu unseren Zwecken verwenden wir Teilergebnisse der nachstehenden Arbeiten:

F. Pollaczek, Über die irregulären Kreiskörper der l -ten und l^2 -ten Einheitswurzeln. Math. Zeitschr. **21** (1924).

Ph. Furtwängler, Über die Reziprozitätsgesetze der l -ten Potenzreste in algebraischen Zahlkörpern, worin l eine ungerade Primzahl bedeutet. Math. Ann. **58**.

Ph. Furtwängler, Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörpers. Math. Ann. **63**.

Ph. Furtwängler, Die Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern. I. Teil Math. Ann. **67**, II. Teil Math. Ann. **72**.

Ph. Furtwängler, Über eine Eigenschaft der Kreiskörper. Journal für reine und angewandte Mathematik, **140**.

D. Hilbert, Die Theorie der algebraischen Zahlkörper. Bericht, erstattet der Deutschen Mathematiker-Vereinigung, 1897.

J. Westlund, On the Class Number of the Cyclotomic Number Field $k(e^{\frac{2\pi i}{n}})$ Transactions of the American Mathematical Society, Vol. **4**, 1903.

T. Takagi, Über eine Theorie des relativ Abel'schen Zahlkörpers. Journal of the College of Science, Imperial University of Tokyo, Vol. **XII**, 9 (1920).

T. Takagi, Zur Theorie des Kreiskörpers. Journal für die reine und angewandte Mathematik, **157** (1927).

(¹) Math. Zeitschr. **21**, (1924).

H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Jahresbericht der deutschen Mathematiker-Vereinigung, **XXXV**, **XXXVI** (1926, 1927).

A. Speiser, Theorie der Gruppen von endlicher Ordnung, 1927.

T. Morishima, Über die Fermatsche Vermutung, IX. Proceedings of the Physico-Mathematical Society of Japan, Vol. **14**, 9 (1932).

Inhalt.

KAPITEL I.

Einheiten und Idealklassen des Galoisschen Zahlkörpers.

§ 1.	Transformationen der Matrizen, I.	84
§ 2.	Transformationen der Matrizen, II.	89
§ 3.	Einheiten und Idealklassen des Galoisschen Zahlkörpers.	95
§ 4.	Einheiten und Idealklassen der relativ zyklischen Zahlkörper.	100

KAPITEL II.

Kreiskörper der l^v -ten Einheitswurzeln.

§ 1.	Einheiten und Idealklassen der Kreiskörper.	104
§ 2.	Basis der irregulären Idealklassengruppe des Kreiskörpers der l^v -ten Einheitswurzeln.	108
§ 3.	Irreguläre Kreiskörper der l -ten Einheitswurzeln.	113
§ 4.	Der erste Faktor der Klassenzahl des Kreiskörpers der l^v -ten Einheitswurzeln.	118
§ 5.	Der l^v -te Potenzrestcharakter im Kreiskörper der l^v -ten Einheitswurzeln.	121

KAPITEL I.

Einheiten und Idealklassen des Galoisschen Zahlkörpers.

In diesem Kapitel sei l eine Primzahl.

§ 1.

Transformationen der Matrizen, I.

Satz 1. Wenn für eine quadratische Matrix A der ganzen rationalen Zahlen die Gleichung

$$A^h \equiv E \pmod{l^n}$$

mit E als Einheitsmatrix gilt, wobei die Ordnung h von A ein Teiler von $l-1$ ist, n eine ganze rationale Zahl bedeutet, so existiert eine ganzzahlige Matrix T , deren Determinante $|T|=1$ ist, so daß TAT^{-1} einer Diagonalmatrix mod l^n kongruent wird.

Beweis(²): Im Falle $l=2$ ist der Satz trivial. Also sei $l>2$. Eine lineare homogene Substitution vom Grade $m \bmod l^n$ besteht aus m Gleichungen von der Gestalt:

$$\left. \begin{aligned} x_1' &\equiv a_{11}x_1 + a_{12}x_2 + \dots + a_{1m}x_m \\ x_2' &\equiv a_{21}x_1 + a_{22}x_2 + \dots + a_{2m}x_m \\ &\vdots \\ x_m' &\equiv a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mm}x_m \end{aligned} \right\} (\text{mod } l^n).$$

Sie ist eindeutig bestimmt durch die quadratische Matrix:

$$A = (a_{ik}).$$

Man übt nun auf x_1 der Reihe nach die Substitutionen $E, A, \dots, A^{h-1}$ aus und erhält so h lineare Formen:

$$y_1 = x_1, \quad y_2, \dots, \quad y_n.$$

Versteht man unter r eine primitive Wurzel modulo l^n , so bildet man weiter die h Linearformen:

$$y_i + r^{-ail} \quad y_2 + r^{-2ail} \quad y_3 + \dots + r^{-(h-1)ail} \quad y_h \equiv z_i \pmod{l^n},$$

$$(i=0, 1, \dots, h-1),$$

wobei $\alpha \cdot h = l - 1$ ist. $z_0, z_1, \dots, z_{h-1}$ sind Linearformen von $x_1, x_2, \dots, x_m$. Übt man auf die Variablen x die Substitution A aus, so erfahren $y_1, y_2, \dots, y_h$ eine zyklische Vertauschung. Daher bleibt z_0 modulo l^{n-1} ungeändert, und z_i geht modulo l^n über in $\gamma^{a h^{i-1}} z_i$.

Die h Linearformen der $x : z_0, z_1, \dots, z_{h-1}$ verschwinden modulo l sicher nicht sämtlich, denn ihre Summe ist $\equiv hy_1 \equiv hx_1 \pmod{l}$. Aber es können zwischen ihnen Beziehungen bestehen. Wir wählen ein System von modulo l linear unabhängigen z aus, so daß alle übrigen sich modulo l linear durch sie ausdrücken lassen. Wenn unter den h Formen z nicht m modulo l linear unabhängige vorkommen, so gibt es noch weitere Formen von $x_1, x_2, \dots, x_m$, die sich nicht modulo l linear durch $z_0, z_1, \dots, z_{h-1}$ ausdrücken lassen. Hierfür kann man eine der Variablen x_i ($i \neq 1$) wählen, denn wenn sich alle x modulo l linear durch die z ausdrücken lassen, so gilt dasselbe von allen ihren linearen Formen. Wir gehen von einer solchen neuen Form y'_1 aus und wiederholen unser Verfahren. Man erhält so $z'_0, z'_1, \dots, z'_{h-1}$, und darunter gibt es gewiß eine Form, die von den Formen $z_0, z_1, \dots, z_{h-1}$ modulo

(²) A. Speiser, Theorie der Gruppen von endlicher Ordnung, S. 147 (1927).

$$x(l-1) + yh = d \quad (1)$$

gilt. Wäre A mit einer Diagonalmatrix (a_{ii}) äquivalent, so wäre $(a_{ii})^h$ mit der Einheitsmatrix E modulo l kongruent, folglich für $i=1, 2, \dots$

$$a_{ii}^h \equiv 1 \pmod{l},$$

also nach (1)

$$a_{ii}^d \equiv 1 \pmod{l},$$

also $(a_{ii})^d$, folglich auch A^d mit E modulo l kongruent, wobei $d < h$; was nach der Voraussetzung unmöglich ist.

Nun kann man in analoger Weise folgenden Satz beweisen, wie bei Satz 1:

Satz 3. Wenn für eine ganzzahlige quadratische Matrix A in einem algebraischen Körper k , in dem l die e -te Potenz eines Primideals $\mathfrak{l}$ ist, die Gleichung

$$A^h \equiv E \pmod{l^n}$$

gilt, wobei die Ordnung h von A ein Teiler von $l-1$ ist, so existiert eine ganzzahlige Matrix T in k , deren Determinante $|T| \not\equiv 0 \pmod{\mathfrak{l}}$ ist, so daß TAT^{-1} einer Diagonalmatrix im rationalen Körper modulo l^n kongruent wird.

In Satz 3 sei speziell k der Kreiskörper k_v von ζ_v , wobei ζ_v eine primitive l^e -te Einheitswurzel ist. Dann ist das Primideal $\mathfrak{l} = (1 - \zeta_v)$ und gilt weiter der Satz:

Satz 4. Es sei A modulo l^n eine ganzzahlige quadratische Matrix in k_v , deren Ordnung h zu l prim ist. Damit A mit einer Diagonalmatrix in k_v modulo l^n äquivalent ist, ist dann notwendig und hinreichend, daß h ein Teiler von $l-1$ ist. Ist h durch l teilbar und A mit einer Diagonalmatrix in k modulo l^n äquivalent, so muß h ein Teiler von $l^e(l-1)$ sein, wobei, falls $k = k_v$ ist, $e = nl^{e-1}(l-1) - 1$ und, falls k rationaler Körper ist, $e = n - 1$.

Beweis: Falls h ein Teiler von $l-1$ ist, ist nach Satz 3 die Behauptung wahr. Falls $(h, l^e(l-1)) = d < h$ ist, gibt es zwei Zahlen x, y , so daß

$$xh + yl^e(l-1) = d \quad (2)$$

ist. Wäre A mit einer Diagonalmatrix (α_{ii}) modulo l^n äquivalent, so wäre $(\alpha_{ii})^h$ mit der Einheitsmatrix E modulo l^n kongruent, folglich für $i=1, 2, \dots$

$$\alpha_{ii}^h \equiv 1 \pmod{l^n},$$

also nach (2)

$$\alpha_{ii}^a \equiv \alpha_{ii}^{y_i^e(l-1)} \equiv \alpha_{ii}^{y_N(l^e)(Nl-1)} \equiv 1 \pmod{l^n},$$

wobei Nl die Norm von l bedeutet, $l^{e+1} = (l^n)$ ist. Daher wäre $(\alpha_{ii})^a$, also auch A^a mit E modulo l^n kongruent, was nach der Voraussetzung unmöglich ist.

Nun sei k ein beliebiger algebraischer Körper, in dem die Primidealzerlegung von l

$$(l) = l_1^{e_1} l_2^{e_2} \dots l_v^{e_v}$$

ist, für $i=1, 2, \dots, v$ die Norm von $l_i = l^{f_i}$, g_i primitive Wurzel modulo l_i , h' der größte gemeinsame Teiler von $l^{f_1}-1, l^{f_2}-1, \dots, l^{f_v}-1$, und $l^{f_i}-1 = h'h_i$ ($i=1, 2, \dots, v$). Ferner sei A modulo l^n eine ganzzahlige quadratische Matrix in k , deren Ordnung h ein Teiler von h' ist. Ähnlich wie beim Beweise von Satz 1 übt man auf x_1 der Reihe nach die Substitutionen $E, A, \dots, A^{h-1}$ aus und erhält so h lineare Formen:

$$y_1 = x_1, y_2, \dots, y_h,$$

und bildet man weiter die h Linearformen:

$$y_1 + g_i^{-ab} y_2 + g_i^{-2ab} y_3 + \dots + g_i^{-(h-1)ab} y_h \equiv z_a \pmod{l_i^{ne_i}} \\ (a=0, 1, \dots, h-1),$$

wobei $b = h''h_i l_i^{f_i(m_i-1)}$ und $h' = hh''$ ist. Ihre Summe: $\sum_{a=0}^{h-1} z_a$ ist $\equiv hy_1 \not\equiv 0 \pmod{l_i}$. Man kann weiter analog vorgehen, wie beim Beweise von Satz 1; es läßt sich zeigen, daß die Matrix A mittels einer geeigneten Transformation T_i , deren Determinante $|T_i| \not\equiv 0 \pmod{l_i}$, in eine Diagonalmatrix D_i modulo $l_i^{ne_i}$ transformiert werden kann, wobei die Elemente von T_i ganze Zahlen aus k sind und $i=1, 2, \dots, v$ ist.

Nun bestimmen wir ein System von v Zahlen $\alpha_1, \alpha_2, \dots, \alpha_v$ aus den Kongruenzen:

$$\left. \begin{aligned} \alpha_i &\equiv 1 \pmod{l_i^{ne_i}} \\ \alpha_i &\equiv 0 \pmod{\frac{l^n}{l_i^{ne_i}}} \end{aligned} \right\} \quad (i=1, 2, \dots, v).$$

Setzt man

$$T = \sum_{i=1}^v \alpha_i T_i, \\ D = \sum_{i=1}^v \alpha_i D_i,$$

wobei D eine Diagonalmatrix ist, so ist für $i=1, 2, \dots, \nu$

$$T \equiv T_i, D \equiv D_i \pmod{\mathfrak{l}_i^{n_i}},$$

also

$$TAT^{-1} \equiv T_iAT_i^{-1} \equiv D_i \equiv D \pmod{\mathfrak{l}_i^{n_i}},$$

folglich

$$TAT^{-1} \equiv D \pmod{l^n},$$

wobei $(|T|, l)=1$ ist. Hieraus folgt der Satz:

Satz 5. Wenn A modulo l^n eine ganzzahlige quadratische Matrix in einem algebraischen Körper k , deren Ordnung ein Teiler des größten gemeinsamen Teilers von $l^1-1, l^2-1, \dots, l^\nu-1$ ist, wobei f_i den Grad eines Primidealteilers $\mathfrak{l}_i$ von l bedeutet und $(l) = \prod_{i=1}^{\nu} \mathfrak{l}_i^{e_i}$ ist, so kann die Matrix A mittels einer geeigneten Transformation, deren Elemente ganze Zahlen aus k sind, in eine Diagonalmatrix modulo l^n transformiert werden.

In diesem Satze sei speziell k der Galoissche Körper, dann ist $e_1=e_2=\dots=e_\nu=e, f_1=f_2=\dots=f_\nu=f, h'=l^\nu-1$. Also gilt der Satz:

Satz 6. Es sei k der Galoissche Körper, A modulo l^n eine ganzzahlige quadratische Matrix in k , deren Ordnung ein Teiler von $l^\nu-1$ ist, wobei f den Grad eines Primidealteilers von l bedeutet. Dann kann A mittels einer geeigneten Transformation, deren Elemente ganze Zahlen aus k sind, in eine Diagonalmatrix modulo l^n transformiert werden.

In diesem Fall gilt weiter der Satz:

Satz 7⁽⁴⁾. Es sei A modulo l^n eine ganzzahlige quadratische Matrix im Galoisschen Körper k , deren Ordnung h zu l prim ist. Die Matrix A ist dann und nur dann mit einer Diagonalmatrix in k modulo l^n äquivalent, wenn h ein Teiler von $l^\nu-1$ ist.

Beweis: Falls h ein Teiler von $l^\nu-1$ ist, ist nach Satz 6 die Behauptung richtig. Falls $(h, l^\nu-1)=d < h$ ist, kann man analog vorgehen, wie beim Beweise von Satz 4.

§ 2.

Transformationen der Matrizen, II.

In diesem Paragraphen betrachten wir ganzzahlige Matrix von fol-

(⁴) Wenn A modulo l^n mit einer Diagonalmatrix in k äquivalent ist, so ist die Ordnung von A ein Teiler von $l^{f(n-1)}(l^f-1)$.

usw. teilbar sind. Übt man auf die Variablen x die Substitution A aus, so erfahren $y_1, y_2, \dots, y_h$ eine zyklische Vertauschung. Daher bleibt $z_0^{(1)}$ ungeändert, und $z_b^{(1)}$ geht über in $\tau^{abl_{n_1-1}} z_b^{(1)}$. Die h Linearformen der x :

$$\begin{aligned} \tilde{z}_0^{(i)} &= \tau_{im'+1}^{(0)} \mathcal{X}_{m'+1} + \tau_{im'+2}^{(0)} \mathcal{X}_{m'+2} + \dots + \tau_{im'+m_j}^{(0)} \mathcal{X}_{m'+m_j} \\ \tilde{z}_1^{(i)} &= \tau_{im'+1}^{(1)} \mathcal{X}_{m'+1} + \tau_{im'+2}^{(1)} \mathcal{X}_{m'+2} + \dots + \tau_{im'+m_j}^{(1)} \mathcal{X}_{m'+m_j} \\ &\vdots \\ \tilde{z}_{h-1}^{(i)} &= \tau_{im'+1}^{(h-1)} \mathcal{X}_{m'+1} + \tau_{im'+2}^{(h-1)} \mathcal{X}_{m'+2} + \dots + \tau_{im'+m_j}^{(h-1)} \mathcal{X}_{m'+m_j} \\ &\quad (i = m' + 1, \quad m' + 2, \quad \dots, \quad m' + m_j) \end{aligned}$$

verschwinden modulo l sicher nicht sämtlich, denn

$$\sum_{b=0}^{h-1} z_b^{(i)} \equiv \sum_{b=0}^{h-1} \tilde{z}_b^{(i)} \equiv h y_1^{(i)} \equiv h x_i \not\equiv 0 \pmod{l}.$$

Durch ähnliches Verfahren wie beim Beweise von Satz 1 kann man also ein System von m_j Linearformen $z_b^{(i)}$ auswählen, so daß die m_j Linearformen $\tilde{z}_b^{(i)}$ in $z_b^{(i)}$ modulo l linear unabhängig sind, wobei i, b ganze Zahlen aus $m'+1, m'+2, \dots, m'+m_j$, bzw. aus $0, 1, \dots, h-1$ sind. Für $j=1, 2, \dots, \nu$ erhält man schließlich die m Linearformen: $t_1, t_2, \dots, t_m$, deren Matrix

$$T = \begin{pmatrix} T_{11} & T_{12} & \dots & T_{1p} \\ \ell^{n_1 - n_2} T_{21} & T_{22} & \dots & T_{2p} \\ \dots & \dots & \dots & \dots \\ \ell^{n_1 - n_p} T_{p1} & \ell^{n_2 - n_p} T_{p2} & \dots & T_{pp} \end{pmatrix},$$

wobei T_{jj} die Matrix von m_j modulo l linear unabhängigen Formen $\bar{z}_b^{(t)}$, also die Determinante $|T_{jj}| \not\equiv 0 \pmod{l}$, also

$$|T| \equiv |T_{11}| + |T_{22}| + \dots + |T_{pp}| \not\equiv 0 \pmod{l}$$

ist, und welche sämtlich die Eigenschaft haben, daß nach Ausführung der Substitution A die Variable t übergeht in $r^{wt^{m-1}}$ t . Hieraus folgt der Satz :

Satz 8. *Es sei $\mathfrak{G}$ eine Gruppe ganzzahliger Matrizen von folgender Art:*

$$A = (l^{n_k - n_i} A_{ik}) \quad (i, k = 1, 2, \dots, v),$$

$$|A| \not\equiv 0 \pmod{l},$$

wobei A_{ik} eine Matrix von m_i Zeilen und m_k Spalten darstellt, die Elemente von A_{ik} ganze rationale Zahlen sind, und für $i > k$ $n_k - n_i > 0$, für $i \leq k$ $n_k - n_i = 0$ ist, und sei die Kongruenz in $l^{n_k - n_1} A_{1k}, l^{n_k - n_2} A_{2k}, \dots, l^{n_k - n_v} A_{vk}$ modulo l^{n_k} zu nehmen, wo $k=1, 2, \dots, v$ ist. Wenn die Ordnung h von A ein Teiler von $l-1$ ist, so gibt es eine Matrix T in $\mathfrak{G}$, so daß TAT^{-1} einer Diagonalmatrix in $\mathfrak{G}$ gleich wird.

Durch ähnliches Verfahren wie beim Beweise von Satz 2 erhält man weiter

Satz 9. Wenn A mit einer Diagonalmatrix in $\mathfrak{G}$ äquivalent ist, so muß die Ordnung von A ein Teiler von $l^{n-1}(l-1)$ sein.

Aus Satz 8 und Satz 9 folgt sogleich

Satz 10. Ist die Ordnung h von A zu l prim, so ist A dann und nur dann mit einer Diagonalmatrix in $\mathfrak{G}$ äquivalent, wenn h ein Teiler von $l-1$ ist.

Ferner kann man in analoger Weise folgenden Satz beweisen, wie bei Satz 8:

Satz 11. Es seien die Elemente von A_{ik} in allen Matrizen A von $\mathfrak{G}$ in Satz 8 ganze Zahlen in einem algebraischen Körper, in dem l die e -te Potenz eines Primideals $\mathfrak{l}$ ist, wobei die Determinanten $|A| \not\equiv 0 \pmod{\mathfrak{l}}$ sind. Wenn die Ordnung h von A ein Teiler von $l-1$ ist, so gibt es eine Matrix T in $\mathfrak{G}$, so daß TAT^{-1} einer Diagonalmatrix, deren Elemente ganze rationale Zahlen sind, gleich wird.

Weiter gilt allgemein

Satz 12. Es seien die Elemente von A_{ik} in allen Matrizen A von $\mathfrak{G}$ in Satz 8 ganze Zahlen in einem algebraischen Körper k , in dem die Primidealzerlegung von l

$$(l) = \mathfrak{l}_1^{e_1} \mathfrak{l}_2^{e_2} \dots \mathfrak{l}_j^{e_j}$$

ist, wobei die Determinanten $|A|$ zu l prim sind, und sei h' der größte gemeinsame Teiler von $l^{e_1}-1, l^{e_2}-1, \dots, l^{e_j}-1$, wobei $N(\mathfrak{l}_i) = l^{e_i}$ ($i=1, 2, \dots, j$) ist. Wenn die Ordnung h von A ein Teiler von h' ist, so ist A mit einer Diagonalmatrix in $\mathfrak{G}$ äquivalent.

Beweis: Man übt auf x_i der Reihe nach die Substitutionen $E, A, \dots, A^{h-1}$ aus und erhält so hm lineare Formen:

$$y_i^{(t)} = x_i, y_2^{(t)}, \dots, y_h^{(t)}, \quad (i=1, 2, \dots, m).$$

Versteht man unter g_s eine primitive Wurzel modulo $\mathfrak{l}_s$, so bildet man weiter die hm Linearformen:

$$y_1^{(t)} + g_s^{-ab} y_2^{(t)} + g_s^{-2ab} y_3^{(t)} + \dots + g_s^{-(h-1)ab} y_h^{(t)} = z_b^{(t)}$$

$$\begin{pmatrix} b=0, 1, \dots, h-1 \\ i=1, 2, \dots, m \end{pmatrix},$$

wobei $a=h''h_s l'^s(n_1 e_s-1)$, $h'=h h''$, $l'^s-1=h' h_s$ ist. Ihre Summe: $\sum_{b=0}^{h-1} z_b^{(i)}$ ist $\equiv h y_i^{(i)} \not\equiv 0 \pmod{l_s}$. Übt man auf die Variablen x die Substitution A aus, so bleibt $z_b^{(i)}$ ungeändert, und $z_b^{(i)}$ geht über in $g_s^{ab} z_b^{(i)}$, wobei die Kongruenz in Koeffizienten von x modulo $\mathfrak{l}_s^{n_1 e_s}$, bzw. modulo $\mathfrak{l}_s^{n_2 e_s}$, ..., bzw. modulo $\mathfrak{l}_s^{n_\nu e_s}$ zu nehmen ist, d. h. $z_b^{(i)} \pmod{\mathfrak{l}_s^{n_1 e_s}, \mathfrak{l}_s^{n_2 e_s}, \dots, \mathfrak{l}_s^{n_\nu e_s}}$ in $g_s^{ab} z_b^{(i)}$ übergeht. Man kann weiter analog vorgehen, wie beim Beweise von Satz 8; es läßt sich zeigen, daß die Matrix A mittels einer geeigneten Transformation T_s in $\mathfrak{G}$, deren Determinante $|T_s| \not\equiv 0 \pmod{l_s}$, in eine Diagonalmatrix $D_s \pmod{\mathfrak{l}_s^{n_1 e_s}, \mathfrak{l}_s^{n_2 e_s}, \dots, \mathfrak{l}_s^{n_\nu e_s}}$ transformiert werden kann. Wir bestimmen nun ein System von ν Zahlen $\alpha_1, \alpha_2, \dots, \alpha_\nu$ aus den Kongruenzen:

$$\left. \begin{aligned} \alpha_s &\equiv 1 \pmod{\mathfrak{l}_s^{n_1 e_s}} \\ \alpha_s &\equiv 0 \pmod{\frac{l^{n_1}}{\mathfrak{l}_s^{n_1 e_s}}} \end{aligned} \right\} \quad (s=1, 2, \dots, j).$$

Setzt man

$$\begin{aligned} T &= \sum_{s=1}^j \alpha_s T_s, \\ D &= \sum_{s=1}^j \alpha_s D_s, \end{aligned}$$

wobei D eine Diagonalmatrix ist, so ist für $s=1, 2, \dots, j$

$$T \equiv T_s, \quad D \equiv D_s \pmod{\mathfrak{l}_s^{n_1 e_s}, \mathfrak{l}_s^{n_2 e_s}, \dots, \mathfrak{l}_s^{n_\nu e_s}},$$

also

$$T A T^{-1} \equiv T_s A T_s^{-1} \equiv D_s \equiv D \pmod{\mathfrak{l}_s^{n_1 e_s}, \mathfrak{l}_s^{n_2 e_s}, \dots, \mathfrak{l}_s^{n_\nu e_s}},$$

folglich

$$T A T^{-1} \equiv D \pmod{l^{n_1}, l^{n_2}, \dots, l^{n_\nu}},$$

wobei $(|T|, l)=1$ ist.

In diesem Satze sei nun k der Galoissche Körper, dann ist $e_1=e_2=\dots=e_j=e$, $f_1=f_2=\dots=f_j=f$, $h'=l^f-1$, und kann man in analoger Weise folgenden Satz beweisen, wie bei Satz 4:

Satz 13. Wenn A mit einer Diagonalmatrix in $\mathfrak{G}$ äquivalent ist, so ist die Ordnung von A ein Teiler von $l^{f(n_1 e-1)}(l^f-1)$.

Folglich gilt weiter

Satz 14. Ist die Ordnung h von A zu l prim, so ist A dann und nur dann mit einer Diagonalmatrix in $\mathfrak{G}$ äquivalent, wenn h ein Teiler von $l-1$ ist.

Nun sei k ein algebraischer Körper, $\mathfrak{a}$ ein Ideal in k , α eine ganze Zahl von folgender Art:

$$\alpha \equiv 0 \pmod{\mathfrak{a}},$$

$$\alpha \not\equiv 0 \pmod{\mathfrak{a}^2},$$

und seien $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_j$ Primidealteiler von $\mathfrak{a}$, d. h.

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_j^{e_j}.$$

In k sei A eine ganzzahlige Matrix von folgender Art:

$$A = \begin{pmatrix} A_{11} & A_{12} \dots A_{1\nu} \\ \alpha^{n_1-n_2} A_{21} & A_{22} \dots A_{2\nu} \\ \dots & \dots \\ \alpha^{n_1-n_\nu} A_{\nu 1} & \alpha^{n_2-n_\nu} A_{\nu 2} \dots A_{\nu \nu} \end{pmatrix} \quad (1)$$

$$n_1 > n_2 > \dots > n_\nu,$$

wobei die Determinante $|A|$ zu $\mathfrak{a}$ prim ist, A_{ik} eine Matrix von m_i Zeilen und m_k Spalten darstellt, und sei die Kongruenz in $A_{1k}, A_{2k}, \dots, A_{kk}, \alpha^{n_k-n_{k+1}} A_{k+1,k}, \dots, \alpha^{n_k-n_\nu} A_{\nu k}$ modulo $\mathfrak{a}^{n_k}$ zu nehmen, wo $k=1, 2, \dots, \nu$ ist. Derartige Matrizen bilden dann eine Gruppe $\mathfrak{G}$. Für die Matrix (1) gilt

Satz 15. Wenn die Ordnung von A ein gemeinsamer Teiler von $p_1^{f_1}-1, p_2^{f_2}-1, \dots, p_j^{f_j}-1$ ist, wobei $N(\mathfrak{p}_i) = p_i^{f_i}$ ist, so gibt es eine Matrix T in $\mathfrak{G}$, so daß TAT^{-1} einer Diagonalmatrix in $\mathfrak{G}$ gleich wird.

Man kann in analoger Weise diese Behauptung beweisen, wie bei Satz 12. k sei insbesondere der Kreiskörper k_ν der ν -ten Einheitswurzeln, dann folgt aus Satz 15:

Satz 16. Es sei (λ) der Primidealteiler von l in k_ν , A eine ganzzahlige Matrix von folgender Art:

$$A = (\lambda^{n_k-n_i} A_{ik}) \quad (i, k=1, 2, \dots, \nu),$$

$$|A| \not\equiv 0 \pmod{\lambda},$$

wobei für $i > k$ $n_k - n_i > 0$, für $i \leq k$ $n_k - n_i = 0$ ist, und sei die Kongruenz in $\lambda^{n_k-n_1} A_{1k}, \lambda^{n_k-n_2} A_{2k}, \dots, \lambda^{n_k-n_\nu} A_{\nu k}$ modulo λ^{n_k} zu nehmen, wo $k=1, 2, \dots, \nu$ ist. Wenn die Ordnung von A ein Teiler von $l-1$ ist, so ist A mit

einer Diagonalmatrix im rationalen Körper modd $\lambda^{n_1}, \lambda^{n_2}, \dots, \lambda^{n_\nu}$ äquivalent.

In diesem Fall gilt weiter

Satz 17. Wenn A mit einer Diagonalmatrix in k , modd $\lambda^{n_1}, \lambda^{n_2}, \dots, \lambda^{n_\nu}$ äquivalent ist, so ist die Ordnung h von A ein Teiler von $l^{n_1-1}(l-1)$. Ist h also zu l prim, so ist A dann und nur dann mit einer Diagonalmatrix in k , modd $\lambda^{n_1}, \lambda^{n_2}, \dots, \lambda^{n_\nu}$ äquivalent, wenn h ein Teiler von $l-1$ ist.

§ 3.

Einheiten und Idealklassen des Galoisschen Zahlkörpers.

Es sei A eine Matrix in einem algebraischen Körper k , deren Ordnung h ist, wobei die Elemente von A zu l prime Nenner haben. Ist nun

$$A^{h'} = E + l^n B, \quad B \not\equiv 0 \pmod{l},$$

wobei h' ein echter Teiler von h , d. h. $h = h'h''$, $h'' = l^a h_1$, und B eine Matrix in k , deren Elemente zu l prime Nenner haben, ist, so ist

$$A^{h'h''} = E + h_1 l^a l^n B + \binom{h_1 l^a}{2} l^{2n} B^2 + \dots + l^{n h_1 l^a} B^{h_1 l^a},$$

also für $n > 0$

$$l^{n+a} B + \frac{h_1 l^a - 1}{2} l^{2n+a} B^2 \equiv 0 \pmod{l^{n+a+1}},$$

da

$$\binom{h_1 l^a}{i l^b} \equiv 0 \pmod{l^{a-b}}, \quad a \geq b$$

ist⁽⁵⁾; daher muß $l=2$ sein, wenn $n > 0$ ist, und, falls $l=2$ ist, entweder $n=1$, $a > 0$ oder $n=0$ sein; denn sonst wäre

$$B \equiv 0 \pmod{l}.$$

Im Falle $l > 2$ ist also $n=0$; im Falle $l=2$ ist entweder $n=0$ oder $n=1$, $h \equiv 0 \pmod{2}$. Nun sei $h = 2h_1 h_2$, $h_2 \neq 1$. Wäre $A^{h_1} = E + 2B$, so wäre $A^{2h_1} = E + 4B_1$, wobei $2h_1$ echter Teiler von h ist, was unmöglich ist. Folglich ist die Ordnung von A modulo 2 entweder $\frac{h}{2}$ oder h .⁽⁶⁾

Hieraus folgt der Satz:

(⁵) E. Artin und H. Hasse, Abh. Math. Sem. Hamburg, 6 (1928), S. 161.

(⁶) Setzt man $A = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}$, so ist $A^3 = E$, $A^3 = -E \equiv E \pmod{2}$.

Hilfssatz: *A sei eine Matrix in k , deren Elemente zu l prime Nenner haben, und h die Ordnung von A . Dann ist auch h die Ordnung von A modulo l^n , wobei n eine beliebige ganze rationale Zahl bedeutet und, falls $l > 2$ ist, $n > 0$, falls $l = 2$ ist, $n > 1$ ist.*

Ist ferner h ungerade, so ist auch h die Ordnung von A modulo 2. Ist aber h gerade, so ist die Ordnung von A modulo 2 entweder h oder $\frac{h}{2}$.

Nun sei k ein algebraischer Körper, k' ein normaler Körper, welcher k enthält, $\mathfrak{G}$ die Galoissche Gruppe von k' . In k sei eine Zahlengruppe $\mathfrak{o}$ vorgelegt, welche gegenüber der Substitution τ einer Untergruppe $\mathfrak{G}'$ von $\mathfrak{G}$ invariant ist, d. h. von der Art, daß mit einer Zahl η zugleich $\tau(\eta)$ darin enthalten ist. Ferner sei $\mathfrak{H}$ der Normalteiler von $\mathfrak{G}'$, deren Substitutionen τ' , abgesehen von dem Einheitswurzelfaktor ε , jede Einheit η von $\mathfrak{o}$ invariant lassen, d. h. von der Art, daß $\tau'(\eta) = \varepsilon\eta$ ist, σ eine Substitution der Faktorgruppe $\mathfrak{G}'/\mathfrak{H}$, deren Ordnung h ein Teiler von $l-1$ ist, dann gilt der Satz:

Satz 18. *In der Zahlengruppe $\mathfrak{o}$ läßt sich ein System von unabhängigen Einheiten $\eta_1, \eta_2, \dots, \eta_r$ angeben, derart, daß sich jede Einheit η in $\mathfrak{o}$ in der Form:*

$$\eta = \varepsilon \eta_1^{a_1} \eta_2^{a_2} \dots \eta_r^{a_r}$$

darstellen läßt, und für die Substitution σ von $\mathfrak{G}'/\mathfrak{H}$, deren Ordnung h ein Teiler von $l-1$ ist,

$$\sigma(\eta_i) = \varepsilon_i \eta_i^{e_i} \tilde{\eta}_i^{a_i} \quad (i=1, 2, \dots, r)$$

gilt, wobei $\varepsilon, \varepsilon_i$ Einheitswurzeln, $\tilde{\eta}_i$ Einheiten in $\mathfrak{o}$ darstellen, a_i eine beliebige ganze rationale Zahl bedeutet, und e_i ganze rationale Zahlen von folgender Art:

$$e_i^h \equiv 1 \pmod{l^n}$$

sind.

Beweis: Es sei $\varepsilon, \xi_1, \xi_2, \dots, \xi_r$ eine Basis der Gruppe aller Einheiten in $\mathfrak{o}$. Dann erhält man

$$\begin{aligned} \sigma(\xi_i) &= \varepsilon_i' \xi_1^{a_{i1}} \xi_2^{a_{i2}} \dots \xi_r^{a_{ir}} \\ (i=1, 2, \dots, r), \end{aligned} \quad (1)$$

wobei ε_i' Einheitswurzeln sind.

In diesen Gleichungen kann man wieder die Substitution σ aus-

führen und die Einheiten $\sigma^s(\xi_i)$ als Produkte der $\sigma(\xi_i)$ und daher der ξ_i darstellen. Dieses Verfahren kann fortgesetzt werden; da aber $\sigma^h(\xi_i) = \varepsilon_i'' \xi_i$ ist, sieht man, daß für die Matrix A der ganzen Zahlen a_{ik} die Gleichung

$$A^n = E$$

gelten muß, wobei E Einheitsmatrix ist. Nach Hilfssatz ist also die Ordnung von A modulo l^n ein Teiler von $l-1$. Folglich existiert nach Satz 1 eine ganzzahlige Matrix $T = (t_{ik})$, deren Determinante $|T| = 1$ ist, so daß TAT^{-1} einer Diagonalmatrix D modulo l^n kongruent wird.

Man geht nun von dem System der ξ_i mittels der Formeln

$$\eta_i = \xi_1^{t_{i1}} \xi_2^{t_{i2}} \dots \xi_r^{t_{ir}} \quad (i=1, 2, \dots, r)$$

zu neuen Einheiten η_i über, die wieder eine Basis bilden, da die Determinante $|T| = 1$ ist. Den Formeln (1) entspricht

$$\begin{aligned} \sigma(\eta_i) &= \varepsilon_i \eta_1^{a_{i1}} \eta_2^{a_{i2}} \dots \eta_r^{a_{ir}} \\ (i &= 1, 2, \dots, r) \end{aligned} \quad (2)$$

und für die Matrix $D' = (d_{ik})$ ergibt sich $D' = TAT^{-1}$ und

$$D' \equiv D \pmod{l^n}.$$

Also ist in (2) $d_{ii} \equiv \varepsilon_i \pmod{l^n}$, $d_{ik} \equiv 0 \pmod{l^n}$ für $i \neq k$.

Es sei von jetzt an k der Galoissche Körper, dann folgt aus Satz 18 sogleich:

Satz 19. *Es sei k ein normaler Körper, $\mathfrak{G}$ die Galoissche Gruppe von k , $\mathfrak{H}$ der Normalteiler von $\mathfrak{G}$, deren Substitutionen, abgesehen von dem Einheitswurzelfaktor, jede Einheit der Zahlengruppe $\mathfrak{o}$ in k invariant lassen, und σ eine Substitution der Faktorgruppe $\mathfrak{G}/\mathfrak{H}$, deren Ordnung h ein Teiler von $l-1$ ist. In k läßt sich ein System von r Grundeinheiten $\eta_1, \eta_2, \dots, \eta_r$ angeben mit der Eigenschaft*

$$\sigma(\eta_i) = \varepsilon_i \eta_i^{e_i} \tilde{\eta}_i^n \quad (i=1, 2, \dots, r),$$

wobei $\varepsilon, \varepsilon_i$ Einheitswurzeln in k , $\tilde{\eta}_i$ gewisse Einheiten in k darstellen, n eine beliebige ganze rationale Zahl bedeutet, und e_i ganze rationale Zahlen von folgender Art:

$$e_i^h \equiv 1 \pmod{l^n}$$

sind.

Nun seien $\eta_1, \eta_2, \dots, \eta_r$; $\xi_1, \xi_2, \dots, \xi_r$ zwei Systemen von Grundeinheiten in k und

$$\sigma(\eta_i) = \varepsilon_i \eta_1^{a_{i1}} \eta_2^{a_{i2}} \dots \eta_r^{a_{ir}}$$

$$\begin{aligned}
 (i=1, 2, \dots, r), \\
 \sigma(\xi_i) = \varepsilon_i' \xi_1^{b_{i1}} \xi_2^{b_{i2}} \dots \xi_r^{b_{ir}} \\
 (i=1, 2, \dots, r),
 \end{aligned}$$

wobei $\varepsilon_i, \varepsilon_i'$ Einheitswurzeln sind, σ eine Substitution von $\mathfrak{G}/\mathfrak{H}$ ist. Dann sind zwei Matrizen $A=(a_{ik})$ und $B=(b_{ik})$ äquivalent. Sei h die Ordnung von σ , so ist nach Hilfssatz auch h die Ordnung von A modulo l^n , wobei $n>0$ für $l>2$ und $n>1$ für $l=2$ ist. Ist also $(h, l-1)<h$, $h\neq 1$, so ist nach Satz 2 A mit keiner Diagonalmatrix im rationalen Körper P modulo l also auch modulo l^n äquivalent, wobei $l>2$ ist. Ist $l=2$, $h>2$, so ist auch nach Satz 2 und Hilfssatz A mit keiner Diagonalmatrix in P modulo 2 also auch modulo 2^n äquivalent. Ist $l=2$, $h=2$, so ist entweder $A\equiv E \pmod{2}$ oder A mit keiner Diagonalmatrix in P modulo 2 äquivalent. Hieraus folgt der Satz:

Satz 20. *Es sei σ eine Substitution der Faktorgruppe $\mathfrak{G}/\mathfrak{H}$, h die Ordnung von σ . Es sei noch $h>2$, falls $l=2$ ist. Ist $(h, l-1)<h$, $h\neq 1$, so existiert in $\mathfrak{o}$ kein System von Grundeinheiten $\eta_1, \eta_2, \dots, \eta_r$ von folgender Art:*

$$\sigma(\eta_i) = \varepsilon_i \eta_i^e \tilde{\eta}_i^n \quad (i=1, 2, \dots, r; n>0),$$

wobei ε_i Einheitswurzeln in k , $\tilde{\eta}_i$ Einheiten in k , e_i ganze rationale Zahlen darstellen.

Dieser Satz gilt auch für $l=2, h=2$, wenn $A\not\equiv E \pmod{2}$ ist. Nach Satz 19 und Satz 20 erhält man folgenden Satz:

Satz 21. *Damit in $\mathfrak{o}$ ein System von Grundeinheiten $\eta_1, \eta_2, \dots, \eta_r$ von folgender Art:*

$$\sigma(\eta_i) = \varepsilon_i \eta_i^e \tilde{\eta}_i^n \quad (i=1, 2, \dots, r; n>0),$$

wobei ε_i Einheitswurzeln, $\tilde{\eta}_i$ Einheiten sind und $l>2$ ist, existiert, ist notwendig und hinreichend, daß die Ordnung von σ ein Teiler von $l-1$ ist.

Nun sei $\tilde{h}=l^n q$ ($q\not\equiv 0 \pmod{l}$) die Klassenzahl des Körpers k , $j_1, j_2, \dots, j_m$ eine Normalbasis für die Gruppe der q -ten Potenzen der Idealklassen von einem Ring $\mathfrak{o}$ in k und l^{n_i} die Ordnung von j_i , wo $i=1, 2, \dots, m$; $n_1\geq n_2\geq \dots\geq n_m$ ist. Ferner sei $\mathfrak{H}$ der Normalteiler von $\mathfrak{G}$, deren Substitutionen jedes Element der Basis $j_1, j_2, \dots, j_m$ invariant lassen, σ eine Substitution der Faktorgruppe $\mathfrak{G}/\mathfrak{H}$. Dann gilt per Satz:

Nun sei auch

$$j_1'', j_2'', \dots, j_m''$$

eine beliebige Normalbasis für diese Klassengruppe und

$$\sigma j_i'' = j_1''^{b_{i1}} j_2''^{b_{i2}} \dots j_m''^{b_{im}} \\ (i=1, 2, \dots, m).$$

Dann sind die Matrix A in (3) und die Matrix $B=(b_{ik})$ äquivalent. Nach Satz 9 erhält man also:

Satz 23. *Ist $(h, l^{n_1-1}(l-1)) < h$, $h \neq 1$, so existiert in dieser Klassengruppe keine Normalbasis $j_1, j_2, \dots, j_m$ von folgender Art:*

$$\sigma j_i = j_i^{a_i} \\ (i=1, 2, \dots, m),$$

wobei a_i ganze rationale Zahlen sind.

Aus Satz 22 und Satz 23 folgt sogleich:

Satz 24. *Ist die Ordnung h von σ zu l prim, so gibt es in dieser Klassengruppe eine Normalbasis mit der Eigenschaft*

$$\sigma j_i = j_i^{a_i} \\ (i=1, 2, \dots, m)$$

dann und nur dann, wenn h ein Teiler von $l-1$ ist.

§ 4.

Einheiten und Idealklassen der relativ zyklischen Zahlkörper.

In diesem Paragraphen sei K ein Galoischer Körper. Im relativ zyklischen Körper K/k vom Primzahlgrade l , sei eine Zahlengruppe O vorgelegt, welche eine Kongruenzgruppe ist mit oder ohne Vorzeichenbedingung, und welche gegenüber der Substitution S des Relativkörpers invariant ist. Die Gesamtheit der Zahlen von O , welche im Grundkörper k enthalten sind, bildet dann eine Zahlengruppe o in k , welche auch eine Kongruenzgruppe ist. Wenn mit R, r bez. die Anzahl der Grundeinheiten in K, k also auch in O, o bezeichnet wird, dann ist, wenn l ungerade ist,

$$R-r=(l-1)(r+1),$$

dagegen, wenn $l=2$, also $K=k(\sqrt{\mu})$ relativ quadratisch ist,

$$R-r=r+1-v,$$

wenn v die Anzahl derjenigen reellen mit k konjugierten Körper be-

deutet, worin die mit μ konjugierten Zahlen negativ ausfallen; und gilt der folgende Satz:

Satz⁽⁷⁾. In der Zahlengruppe O läßt sich stets ein System von m Einheiten $H_1, H_2, \dots, H_m$ finden, derart, daß sich jede Einheit E in O in der Form:

$$E = H_1^{f_1(S)} H_2^{f_2(S)} \dots H_m^{f_m(S)} H^l [\xi]$$

darstellen läßt, wo H eine Einheit in O , $[\xi]$ eine Einheit in o oder aber eine Einheit in O , deren l -te Potenz in o liegt, bedeutet,

$$f_i(S) = u_i + u'_i(1-S) + \dots + u_i^{(l-2)}(1-S)^{l-2},$$

$$(i=1, 2, \dots, m)$$

und die Koeffizienten $u_i, u'_i, \dots, u_i^{(l-2)}$ sämtlich Zahlen aus der Reihe: $0, 1, 2, \dots, l-1$ sind.

Die Zahl m hat den folgenden Wert:

$$m=r+1, \text{ wenn } l \text{ ungerade ist,}$$

$$m=r+1-v, \text{ wenn } l=2 \text{ ist.}$$

In diesem Satze sind die $m(l-1)$ Einheiten

$$H_1, H_1^{1-S}, \dots, H_1^{(1-S)^{l-2}}; \dots; H_m, H_m^{1-S}, \dots, H_m^{(1-S)^{l-2}}$$

unabhängig in Bezug auf die Gruppe der Einheiten:

$$H^l[\xi],$$

also auch in Bezug auf die Gruppe der Einheiten:

$$[\xi].$$

Daher läßt sich jede Einheit E von O in der Gestalt

$$E^a = H_1^{f_1(S)} H_2^{f_2(S)} \dots H_m^{f_m(S)} [\xi] \quad (1)$$

darstellen, wobei ganze rationale Zahl a zu l prim ist,

$$f_i(S) = v_i + v'_i(1-S) + \dots + v_i^{(l-2)}(1-S)^{l-2}$$

$$(i=1, 2, \dots, m),$$

und die Koeffizienten $v_i, v'_i, \dots, v_i^{(l-2)}$ ganze rationale Zahlen sind⁽⁸⁾.

Nun sei $\mathfrak{G}$ die Galoissche Gruppe von K , $\mathfrak{S}$ der Normalteiler von $\mathfrak{G}$, deren Substitutionen τ , abgesehen von dem Faktor $[\xi]$, jede Einheit E von O invariant lassen, d. h. von der Art, daß $\tau(E)=[\xi]E$ ist, und σ

(7) T. Takagi, Journal of the College of Science, Imperial University of Tokyo, **XLI**, 9 (1920), S. 35.

(8) Durch ähnliches Verfahren wie beim Beweise des Hilfssatzes 31 (§146) in Berichten von D. Hilbert erhält man diese Ergebnisse.

eine Substitution der Faktorgruppe $\mathfrak{G}/\mathfrak{H}$, deren Ordnung h ist. Dann erhält man nach (1)

$$\sigma H_i^a = H_1^{f_{i1}(S)} H_2^{f_{i2}(S)} \dots H_m^{f_{im}(S)} [\xi] \\ (i=1, 2, \dots, m),$$

wobei a eine gewisse zu l prime ganze rationale Zahl; durch wiederholte Anwendung der Substitution σ und unter Beachtung der Beziehung $\sigma^h H_i = [\xi] H_i$ erkennt man, daß für die Matrix $A = (f_{ik}(\xi))$ die Gleichung

$$A^h = a^h E$$

gilt, wobei ξ eine primitive l -te Einheitswurzel und E Einheitsmatrix ist. Die Elemente der Matrix $A_1 = \frac{1}{a} A$, $A_1^h = E$, sind ganze oder gebrochene Zahlen aus $P(\xi)$ mit zu l primen Nennern, wobei $P(\xi)$ der Kreiskörper von ξ oder rationaler Körper ist. Nach Hilfssatz, § 3, ist also h die Ordnung von A_1 modulo l^n , wobei $n > 0$ für $l > 2$ und $n > 1$ für $l = 2$ ist. Wenn h ein Teiler von $l-1$ ist, so ist nach Satz 3 A_1 mit einer Diagonalmatrix im rationalen Körper P modulo l^n äquivalent; wenn $(h, l-1) < h$, $h \neq 1$, ist, so ist nach Satz 4 A_1 mit keiner Diagonalmatrix in P modulo l also auch modulo l^n äquivalent, wobei $l > 2$ ist. Daher kann man in analoger Weise folgenden Satz beweisen, wie bei Satz 18 und Satz 20.

Satz 25. *Es sei $l > 2$. In der Zahlengruppe O läßt sich ein System von $r+1$ Einheiten*

$$H_1, H_2, \dots, H_{r+1}$$

angeben, derart, daß die a -te Potenz jeder Einheit H in O in der Form

$$H^a = H_1^{f_1(S)} H_2^{f_2(S)} \dots H_{r+1}^{f_{r+1}(S)} [\xi]$$

geschrieben werden kann, und daß zugleich auch

$$\sigma H_i = H_i^a \tilde{H}_i^n [\xi_i] \quad (2)$$

$$(i=1, 2, \dots, r+1; n > 0)$$

gilt, dann und nur dann, wenn die Ordnung von σ ein Teiler von $l-1$ ist; hierbei bedeutet a gewisse ganze rationale Zahl, n eine beliebige ganze Zahl und darstellen $\tilde{H}_i$ Einheiten in O .

Für $l=2$ gilt der Satz:

Satz 26. *Es sei $l=2$, $h > 2$, $r+1-v > 1$. Dann existiert in O kein System von unabhängigen Einheiten*

$$H_1, H_2, \dots, H_{r+1-v}$$

mit der Eigenschaft (2).

Weiter gilt nach Satz 4:

Satz 27. Es sei $l > 2$, $(h, l^{l-2}(l-1)) < h$. Dann existiert in $\mathcal{O}$ kein System von unabhängigen Einheiten mit der Eigenschaft:

$$\begin{aligned} \sigma H_i &= H_i^{q_i(S)} \tilde{H}_i^{l^n} [\xi] \\ (i=1, 2, \dots, r+1; n > 0), \end{aligned}$$

wobei

$$\begin{aligned} g_i(S) &= a_i + a'_i(1-S) + \dots + a_i^{(l-2)}(1-S)^{l-2} \\ (i=1, 2, \dots, r+1) \end{aligned}$$

ist.

Nun sei $h' = l^n q'$ ($q' \not\equiv 0 \pmod{l}$) die Klassenzahl des Körpers K , $\mathcal{O}$ ein Ring in K , $\mathcal{G}$ die Galoissche Gruppe von K . Dann erhält man:

Satz⁽⁹⁾. Das System der q' -ten Potenzen der Idealklassen in $\mathcal{O}$ kann eindeutig in der Form

$$\mathfrak{S}_1^{F_1(S)} \mathfrak{S}_2^{F_2(S)} \dots \mathfrak{S}_m^{F_m(S)} j$$

dargestellt werden, wobei $\mathfrak{S}_i$ m bestimmte Klassen von K sind und für die Klassen $\mathfrak{S}_i$

$$\begin{aligned} \mathfrak{S}_i^{(1-S)^{n_i}} &= j_i, \quad \mathfrak{S}_i^{(1-S)^{n_i-1}} \neq j_i' \\ (i=1, 2, \dots, m) \end{aligned}$$

mit gewissen ganzen rationalen Zahlen $n_i > 0$ gilt; j bedeutet das System derjenigen Klassen, die Ideale aus k enthalten, und $F_i(S)$ ganzzahliges Polynom in S .

Es sei $\mathfrak{H}$ der Normalteiler von $\mathcal{G}$, deren Substitutionen jedes Element der Basis $\mathfrak{S}_i$, abgesehen von dem Faktor j , invariant lassen, σ eine Substitution der Faktorgruppe $\mathcal{G}/\mathfrak{H}$. Dann gilt der Satz:

Satz 28. Es sei die Ordnung h von σ ein Teiler von $l-1$. Das System der q' -ten Potenzen der Idealklassen in $\mathcal{O}$ ist in der Form:

$$\mathfrak{S}_1^{F_1(S)} \mathfrak{S}_2^{F_2(S)} \dots \mathfrak{S}_m^{F_m(S)} j$$

darstellbar, wobei für die Klassen $\mathfrak{S}_i$

$$\begin{aligned} \mathfrak{S}_i^{(1-S)^{n_i}} &= j_i, \quad \mathfrak{S}_i^{(1-S)^{n_i-1}} \neq j_i' \\ (n_1 \geq n_2 \geq \dots \geq n_m) \end{aligned} \tag{3}$$

und

$$\sigma \mathfrak{S}_i = \mathfrak{S}_i^{a_i} j_i'' \tag{4}$$

(⁹) Durch ähnliches Verfahren wie beim Beweise des Satzes von Ph. Furtwängler (Math. Ann. 63, §6.) erhält man diesen Satz.

gilt, ⁽¹⁰⁾ und n_i, a_i gewisse ganze rationale Zahlen sind und $\mathfrak{j}$ das System derjenigen Klassen, die Ideale aus k enthalten, bedeutet.

Beweis: Nach Satz 16 kann man in analoger Weise diesen Satz beweisen, wie bei Satz 22 und Satz 25.

Ferner gilt nach Satz 17:

Satz 29. Ist $(h, l^{n-1}(l-1)) < h$, $h \neq 1$, so existiert in dieser Klassengruppe keine Basis (3) mit der Eigenschaft

$$\sigma \mathfrak{S}_i = \mathfrak{S}_i^{G_i(S)} \mathfrak{j}_i'' \\ (i=1, 2, \dots, m),$$

wobei $G_i(S)$ ganzzahlige Polynome in S bedeuten.

Ist also h zu l prim, so existiert in dieser Klassengruppe eine Basis (3) mit der Eigenschaft (4) dann und nur dann, wenn h ein Teiler von $l-1$ ist.

KAPITEL II.

Kreiskörper der l^r -ten Einheitswurzeln.

In diesem Kapitel sei l eine ungerade Primzahl, k_r der Kreiskörper von ζ_r , wobei ζ_r eine primitive l^r -te Einheitswurzel ist, r eine primitive Wurzel modulo l^r und s die Substitution $(\zeta_r: \zeta_r^r)$.

§ 1.

Einheiten und Idealklassen der Kreiskörper.

In Satz 19 sei o die Gruppe reeller Einheiten in k_r . Dann ⁽¹¹⁾ sind s^o und $s^{\mu^{r-1}}$ die Elemente von $\mathfrak{S}$ und ist die Ordnung von s in $\mathfrak{S}/\mathfrak{S} \mu l^{r-1}$. Setzt man $\sigma = s^{l^{r-1}}$, so ist die Ordnung von σ ein Teiler von $l-1$. Also folgt aus Satz 19:

Satz 30. In k_r läßt sich ein System von Grundeinheiten $\eta_1, \eta_2, \dots, \eta_r$ angeben mit der Eigenschaft

$$\eta_i^{s^{l^{r-1}} - c_i} = \tilde{\eta}_i^{\mu} \\ (i=1, 2, \dots, r; \quad r = \mu l^{r-1} - 1),$$

(¹⁰) Man kann diese Beziehung auf folgende Gestalt transformieren:

$$\sigma \mathfrak{S}_i = \mathfrak{S}_i^{a_i}.$$

(Vgl. Kapitel II, §1, S. 108).

(¹¹) $\mu = \frac{l-1}{2}$.

wobei $\tilde{\eta}_i$ gewisse Einheiten in k_v darstellen, n eine beliebige ganze rationale Zahl bedeutet, und e_i ganze rationale Zahlen von folgender Art:

$$e_i^v \equiv 1 \pmod{l^n}$$

sind.

Ist $\sigma = s^{at^m}$, $m < v-1$, $(a, l) = 1$, so ist die Ordnung von $\sigma > l-1$. Also gilt nach Satz 20

Satz 31. In k_v existiert kein System von Grundeinheiten $\eta_1, \eta_2, \dots, \eta_r$ von folgender Art:

$$\eta_i^{s^{at^m - e_i}} = \tilde{\eta}_i^n$$

$$(i=1, 2, \dots, r; n > 0),$$

wobei $\tilde{\eta}_i$ Einheiten in k_v , e_i ganze rationale Zahlen darstellen und $m < r-1$, $(a, l) = 1$ ist.

Nun sei $h = l^n q$ ($q \not\equiv 0 \pmod{l}$) die Klassenzahl von k_v , $j_1, j_2, \dots, j_m$ eine Normalbasis für die Gruppe der q -ten Potenzen der Idealklassen von k_v und l^{n_i} die Ordnung von j_i , wo $i=1, 2, \dots, m$; $n_1 \geq n_2 \geq \dots \geq n_m$ ist. Dann folgt aus Satz 22.

Satz 32. In k_v läßt sich für die Gruppe der q -ten Potenzen der Idealklassen eine Normalbasis

$$j_1, j_2, \dots, j_m,$$

$$j_i^{n_i} = 1, \quad j_i^{n_i-1} \neq 1$$

$$(i=1, 2, \dots, m)$$

wählen, derart, daß zugleich auch

$$j_i^{s^{i^{v-1}}} = a_i = 1 \quad (i=1, 2, \dots, m)$$

gilt, wobei a_i gewisse ganze rationale Zahlen bedeuten.

Nun ist k_v ein relativ-zyklischer Oberkörper von k_{v-1} vom Relativgrad l . In Satz 25 sei $K = k_v$, $k = k_{v-1}$, O die Gruppe der reellen Einheiten von k_v , $S = s^{l^{v-2}(l-1)}$. Dann ist $[\xi]$ reelle Einheit von k_{v-1} und erhält man

Satz 33. In k_v läßt sich ein System von reellen Einheiten

$$H_1, H_2, \dots, H_r$$

angeben, derart, daß die a -te Potenz jeder reellen Einheit H in k_v in der Form

$$H^a = H_1^{f_1(S)} H_2^{f_2(S)} \dots H_r^{f_r(S)} \xi$$

geschrieben werden kann, wobei für die Einheiten H_i

$$H_i^{s^{p-2}S-a_i} = \tilde{H}_i^{l^n} \quad (1)$$

$$(i=1, 2, \dots, r'; \quad r'=\mu l^{p-2}; \quad n>0)$$

gilt, a eine bestimmte zu l prime ganze Zahl, a_i gewisse ganze rationale Zahl und n eine beliebige ganze Zahl bedeutet.

Beweis: Nach Satz 25 gilt für H_i

$$H_i^{\sigma-a_i} = \tilde{H}_i^{l^n} \xi_i, \quad (2)$$

wobei $\sigma = S s^{p-2}$ ist und für a_i

$$a_i^{\mu} \equiv 1 \pmod{l^n}$$

gilt. Durch Potenzierung dieser Beziehung mit

$$\frac{\sigma^{l-1} - a_i^{l-1}}{\sigma - a_i}$$

hat man also

$$\xi_i^{\frac{\sigma^{l-1} - a_i^{l-1}}{\sigma - a_i}} = \tilde{\xi}_i^{l^n}. \quad (3)$$

Andererseits gilt nach Satz 30 für ξ_i

$$\xi_i = \eta_i^{x_1} \eta_2^{x_2} \dots \eta_r^{x_r},$$

$$\eta_j^{\sigma-e_j} = \tilde{\eta}_j^{l^n} \quad (j=1, 2, \dots, r; \quad r=\mu l^{p-2}-1),$$

also für jede j , für welche $e_j \equiv a_i \pmod{l}$ ist,

$$\eta_j^{a_i-e_j} = \eta_j^{-(\sigma-a_i)} \tilde{\eta}_j^{l^n},$$

also

$$\eta_j^{x_j} = \eta_j^{(\sigma-a_i)} \tilde{\eta}_j^{l^n},$$

folglich

$$\xi_i = \eta_i^{(\sigma-a_i)} \eta_{n_1}^{x_{n_1}} \eta_{n_2}^{x_{n_2}} \dots \tilde{\eta}_i^{l^n},$$

wobei $a_i \equiv e_{n_1} \equiv e_{n_2} \equiv \dots \pmod{l^n}$ ist. Aus der Potenzierung dieser Beziehung mit

$$\frac{\sigma^{l-1} - a_i^{l-1}}{\sigma - a_i}$$

folgt nach (3)

$$\eta_{n_1}^{x_{n_1}} \frac{\sigma^{l-1} - a_i^{l-1}}{\sigma - a_i} \eta_{n_2}^{x_{n_2}} \frac{\sigma^{l-1} - a_i^{l-1}}{\sigma - a_i} \dots = \tilde{\eta}_i^{l^n},$$

also

$$\frac{x_{n_1}^{(l-1)a_1^{l-2}}}{\eta_{n_1}^{l-2}} \frac{x_{n_2}^{(l-1)a_2^{l-2}}}{\eta_{n_2}^{l-2}} \dots = \tilde{\eta}_i^{(lv)l^n},$$

folglich

$$x_{n_1} \equiv x_{n_2} \equiv \dots \equiv 0 \pmod{l^n},$$

also

$$\xi_i = \eta_i^{(\sigma - a_i)} \tilde{\eta}_i^{(v)l^n}. \quad (4)$$

Nach (2) und (4) erhält man also

$$\left(\frac{H_i}{\eta_i} \right)^{\sigma - a_i} = \tilde{H}_i^{l^n}.$$

Ersetzt man $\frac{H_i}{\eta_i}$ durch H_i , so erhält man die Form (1).

Ferner gilt der Satz:

Satz 34. In k_r existiert kein System von reellen Einheiten $H_1, H_2, \dots, H_r$ von folgender Art:

$$H_i^{s_i^{a_i m_i} s - a_i} = \tilde{H}_i^{l^n} \xi_i \\ (i=1, 2, \dots, r; r'=\mu l^{v-2}; n>0),$$

wobei $\tilde{H}_i$ Einheiten in k_r , a_i ganze rationale Zahlen darstellen und $m_i < v-2$, $(a, l)=1$ ist.

Dieser Satz gilt auch für $m=v-2$, wenn $a>1$ ist. Durch wiederholte Anwendung von Satz 33 erhält man

Satz 35. Es sei s_i die Substitution $(\xi_i: \xi_i')$, S_i die Substitution $s_i^{(i-1)l^{i-2}}$ ($i>1$). In k_r läßt sich ein System von reellen Einheiten

$$\eta_{i_1}, \eta_{i_2}, \dots, \eta_{i_{m_i}} \\ (i=1, 2, \dots, v; m_i=\mu l^{i-2}, i>1; m_1=\mu-1)$$

angeben, derart, daß die a -te Potenz jeder reellen Einheit η in k_r in der Form

$$\eta^a = \prod_{i=1}^v \prod_{j=1}^{m_i} \eta_{ij}^{f_j(s_i)}$$

geschrieben werden kann, wobei $\eta_{i_1}, \eta_{i_2}, \dots, \eta_{i_{m_i}}$ Einheiten in k_i darstellen, für η_{ij}

$$\eta_{ij}^{s_i^{l^{i-1}} - a_{ij}} = \tilde{\eta}_{ij}^{l^n}$$

$$(i=1, 2, \dots, v; j=1, 2, \dots, m_i; n>0)$$

gilt, a eine bestimmte zu l prime ganze rationale Zahl und a_{ij} gewisse ganze rationale Zahl bedeutet.

Aus Satz 28 folgt weiter

Satz 36. Das System der q -ten Potenzen der Idealklassen in k_v ist in der Form

$$\mathfrak{S}_1^{F_1(S)} \mathfrak{S}_2^{F_2(S)} \dots \mathfrak{S}_m^{F_m(S)} \mathfrak{j}$$

darstellbar, wobei für die Klassen $\mathfrak{S}_i$

$$\mathfrak{S}_i^{(1-S)^{n_i}} = \mathfrak{j}_i, \quad \mathfrak{S}_i^{(1-S)^{n_i-1}} \neq \mathfrak{j}_i' \\ (n_1 \geq n_2 \geq \dots \geq n_m)$$

und

$$\mathfrak{S}_i^{S^{p^2-a_i}} = 1$$

gilt, und n_i, a_i gewisse ganze rationale Zahlen sind, $\mathfrak{j}$ das System derjenigen Klassen, die Ideale aus k_{v-1} enthalten, und m den Rang der Idealklassen in Satz 32 bedeutet.

Beweis: In der Relativdiskriminante von k_v als relativ-zyklischen Oberkörpers von k_{v-1} geht nur das eine Primideal $\lambda_{v-1} = 1 - \zeta_{v-1}$ auf. Also ist m die Anzahl der Basiselemente der Idealklassen in Satz 32.⁽¹²⁾ Nun gilt nach Satz 28 für $\mathfrak{S}_i$

$$\mathfrak{S}_i^{\sigma-a_i} = \mathfrak{j}_i'',$$

wobei $\sigma = S^{p^2}$ und $a_i' \equiv 1 \pmod{(1-\zeta_1)^{n_i}}$ ist. Durch ähnliches Verfahren wie beim Beweise von Satz 33 erhält man nach Satz 32

$$\mathfrak{j}_i'' = \mathfrak{j}_i'''^{\sigma-a_i} \mathfrak{j}_i^{(iv)},$$

wobei $\mathfrak{j}_i^{(iv)\sigma-a_i'} = 1$ und $a_i' \equiv a_i \pmod{l}$ ist. Hieraus folgt nach einer kurzen Rechnung⁽¹³⁾

$$\mathfrak{S}_i^{\sigma-a_i} = 1.$$

§ 2.

Basis der irregulären Idealklassengruppe des Kreiskörpers der l^v -ten Einheitswurzeln.

In der durch die Basis $\mathfrak{j}_1, \mathfrak{j}_2, \dots, \mathfrak{j}_m$ in Satz 32 dargestellten irregulären Klassengruppe von k_v können m Untergruppen vom Index l hervorgehoben werden; die i -te dieser Untergruppen $\mathfrak{G}_i$ durchläuft alle Klassen $\mathfrak{j} = \mathfrak{j}_1^{x_1} \mathfrak{j}_2^{x_2} \dots \mathfrak{j}_m^{x_m}$, für welche $x_i \equiv 0 \pmod{l}$ ist. Es gibt nun

(¹²) Ph. Furtwängler, Math. Ann. 67, § 3.

(¹³) F. Pollaczek, Math. Zeitschr. 21, S. 18.

in der vollen Klassengruppe von k , eine einzige Untergruppe $\mathfrak{G}_l$ vom Index l , die $\mathfrak{G}'_l$ enthält und zu $\mathfrak{G}_l$ eine zugehörige singuläre Primärzahl⁽¹⁴⁾ ω_l , so daß

$$\left(\frac{\omega_l}{\mathfrak{j}_l}\right) = \zeta_1^c \neq 1, \quad \left(\frac{\omega_l}{\mathfrak{j}_k}\right) = 1 \quad (i \neq k) \quad (1)$$

ist, wobei

$$\left(\frac{\omega_l}{\mathfrak{j}_l}\right)$$

der l -te Potenzrestcharakter in k , ist und ω_l die der Klasse $\mathfrak{j}_l$ zugehörige singuläre Primärzahl genannt werden soll. Auf diese Gleichungen wenden wir die Substitution $\sigma = s^{p-1}$ an:

$$\left(\frac{\omega_l^\sigma}{\mathfrak{j}_l^\sigma}\right) = \zeta_1^{rc}, \quad \left(\frac{\omega_l^\sigma}{\mathfrak{j}_k^\sigma}\right) = 1.$$

Nun sind ω_l^σ zugleich mit ω_l singuläre Primärzahlen und ist $\mathfrak{j}_l^\sigma$ mit $\mathfrak{j}_l^{a_i}$ äquivalent,⁽¹⁵⁾ also

$$\left(\frac{\omega_l^\sigma}{\mathfrak{j}_l^{a_i}}\right) = \zeta_1^{rc}, \quad \left(\frac{\omega_l^\sigma}{\mathfrak{j}_l}\right) = \zeta_1^{\frac{r}{a_i}c},$$

wobei $\frac{r}{a_i}$ den zugehörigen Rest modulo l bedeutet, und da nach (1) auch

$$\left(\frac{\omega_l^{\frac{r}{a_i}}}{\mathfrak{j}_l}\right) = \zeta_1^{\frac{r}{a_i}c}$$

ist, hat man

$$\left(\frac{\omega_l^{\sigma - \frac{r}{a_i}}}{\mathfrak{j}_l}\right) = 1$$

und desgleichen

$$\left(\frac{\omega_l^{\sigma - \frac{r}{a_i}}}{\mathfrak{j}_k}\right) = 1 \quad (i \neq k).$$

Die Zahl $\omega_l^{\sigma - \frac{r}{a_i}}$ ist also in bezug auf die Ideale sämtlicher irregulären Klassen in Satz 32 l -ter Potenzrest, während in bezug auf die Ideale, deren Ordnungen zu l prim sind, jede singuläre Primärzahl und damit auch $\omega_l^{\sigma - \frac{r}{a_i}}$ l -ter Potenzrest ist. Daher muß $\omega_l^{\sigma - \frac{r}{a_i}}$ die l -te Potenz einer

⁽¹⁴⁾ Ph. Furtwängler, Math. Ann. **67**, § 16, Satz 10; **72**, § 4, Satz 6.

⁽¹⁵⁾ Ph. Furtwängler, a. a. O.

Zahl ω aus k_v sein.⁽¹⁶⁾

Setzt man nun

$$j_i^{n_i} = (\tilde{\rho}_i), \quad j_i^{\sigma - a_i} = (\tilde{\alpha}_i),$$

so ist

$$\tilde{\rho}_i^{\sigma - a_i} = \eta \tilde{\alpha}_i^{n_i}, \quad (2)$$

wobei η eine Einheit in k_v ist, und gilt für η

$$\eta^{\frac{\sigma^{l-1} - a_i^{l-1}}{\sigma - a_i}} = \eta'^{n_i},$$

also nach (4) in § 1, Kapitel II,

$$\eta = \eta''^{\sigma - a_i} \tilde{\eta}'^{n_i}.$$

Ersetzt man also in (2) $\tilde{\rho}_i$ durch $\tilde{\rho}_i = \eta'' \rho_i$, so ist

$$\rho_i^{\sigma - a_i} = \alpha_i^{n_i} \quad (i=1, 2, \dots, m). \quad (3)$$

Man setzt nun ω_i als Produkt der Zahlen ρ_i und einer Einheit an:

$$\omega_i = \rho_1^{x_1} \rho_2^{x_2} \dots \rho_m^{x_m} \eta \beta^l. \quad (4)$$

Durch Potenzierung dieser Beziehung mit $\sigma - \frac{r}{a_i}$ hat man

$$\rho_1^{x_1(a_1 - \frac{r}{a_i})} \rho_2^{x_2(a_2 - \frac{r}{a_i})} \dots \rho_m^{x_m(a_m - \frac{r}{a_i})} \eta^{\sigma - \frac{r}{a_i}} = \gamma^l,$$

da

$$\omega_i^{\sigma - \frac{r}{a_i}} = \omega^l$$

und

$$\rho_i^{\sigma - a_i} = \alpha_i^{n_i} \quad (i=1, 2, \dots, m)$$

ist. Hieraus folgt

$$x_1 \left(a_1 - \frac{r}{a_i} \right) \equiv x_2 \left(a_2 - \frac{r}{a_i} \right) \equiv \dots \equiv x_m \left(a_m - \frac{r}{a_i} \right) \equiv 0 \pmod{l}$$

und weiter

$$\eta^{\sigma - \frac{r}{a_i}} = \eta'^l$$

Für alle Indizes j , für die $a_j \equiv \frac{r}{a_i} \pmod{l}$ ist, muß also $x_j \equiv 0 \pmod{l}$ sein und ω_i ist daher bis auf eine l -te Potenz das Produkt derjenigen

⁽¹⁶⁾ T. Takagi, Journal of the College of Science, Imperial University of Tokyo, **XLI**, 9, S. 16.

ρ aus (3), deren zugehörige a kongruent $\frac{r}{a_i}$ modulo l sind, und, falls $\frac{r}{a_i}$ quadratischer Rest ist, der Einheit

$$\tilde{\eta} = H\eta^{e_j}$$

aus Satz 30, § 1, wobei die der Einheit η_j zugehörige Zahl e_j kongruent $\frac{r}{a_i}$ modulo l ist.

Es sei nun c irgendein quadratischer Rest modulo l und es möge in $j_1, j_2, \dots, j_m$ genau m_c Idealklassen j_k geben, deren zugehörige $a_k \equiv c \pmod{l}$ sind. Die diesen m_c Klassen zugehörigen m_c singulären Primärzahlen sind multiplikativ unabhängig voneinander und sind nach dem vorigen Absatz bis auf eine l -te Potenz Produkte solcher ρ_k , deren zugehörige $a_k \equiv \frac{r}{c} \pmod{l}$ sind; da $\frac{r}{c}$ quadratischer Nichtrest ist, tritt hier keine reelle Einheit η hinzu; denn für das η in (4) folgt aus $\eta^{\sigma - \frac{r}{c}} = \eta''$ leicht $\eta = \zeta_v^b \eta'''$. Es müssen daher auch mindestens m_c derartige ρ vorhanden sein und auch mindestens m_c Basisklassen j , deren zugehörige $a \equiv \frac{r}{c} \pmod{l}$ ist, da ζ_v nicht-primär ist. Wir wollen die genaue Anzahl dieser Basisklassen mit $m_{\frac{r}{c}} \geq m_c$ bezeichnen; zu ihnen gehören wiederum $m_{\frac{r}{c}}$ singuläre Primärzahlen ω , die Potenzprodukte solcher ρ , für deren a

$$a \equiv \frac{r}{c} = c \pmod{l}$$

gilt, sowie gegebenenfalls der Einheit $H\eta_k^{e_k}$ sind, wobei die der Einheit η_k zugehörige Zahl e_k kongruent c modulo l ist; die genaue Anzahl der letzteren ρ ist aber m_c und daher gilt

$$m_{\frac{r}{c}} \geq m_c \geq m_{\frac{r}{c}} - m',$$

wobei m' die Anzahl der Einheit η_k , deren zugehörige $e_k \equiv c \pmod{l}$ ist, bedeutet.

Es sollen nun die Ideale derjenigen Klassen j_i in Satz 32, deren a_i quadratische Nichtreste β sind, mit $p_1, p_2, \dots$ bezeichnet werden, wobei

$$p_i^{\sigma - \beta_i} \sim 1$$

ist; die Ideale der übrigen Klassen aber, deren a_i quadratische Reste α sind, mit $q_1, q_2, \dots$, wobei

$$q_i^{\sigma-\alpha_i} \sim 1$$

ist, und wir können nach dem Vorhergehenden den Satz aussprechen:

Satz 37. Wenn unter den Basiselementen der irregulären Klassen-
gruppe von k_v für einen bestimmten quadratischen Nichtrest β_0 genau
 m_{β_0} Klassen $p_{j_1}, p_{j_2}, \dots$ vorhanden sind, wobei

$$p_{j_i}^{\sigma-\beta_i} = 1$$

ist, so daß $\beta_{j_i} \equiv \beta_0 \pmod{l}$ ist, so gibt es entweder $m_{\beta_0} - m''$ oder⁽¹⁷⁾
 $m_{\beta_0} - m'$ Basisklassen $q_{k_1}, q_{k_2}, \dots$, deren zugehörige α_{k_i} kongruent
 $\frac{r}{\beta_0}$ modulo l sind, wobei

$$q_{k_i}^{\sigma-\alpha_{k_i}} = 1, \quad m' > m'' \geq 0$$

ist; insbesondere ist, wenn der zweite Fall eintritt und $m_{\beta_0} - m' \geq 0$ ist,
jede Einheit η_k in $\Pi \eta_k^{e_k}$ singuläre Primärzahl, wobei die der Einheit
 η_k zugehörige Zahl e_k kongruent $\frac{r}{\beta_0}$ modulo l ist.

Für die Klassen p folgt aus

$$p_i^{\sigma-\beta_i} = 1$$

und $\beta_i \equiv -1 \pmod{l^{n_i}}$

$$p_i^{\sigma^{\mu_i}+1} = 1$$

in k_v und im reellen Unterkörper μl^{v-1} -ten Grades k'_v , während aus
 $q_i^{\sigma-\alpha_i} = 1$

$$q_i^{\sigma^{\mu_i}+1} = q_i^2$$

in k_v und in k'_v folgt. Die Relativnormen der p -Klassen in bezug auf
 k'_v gehen also in die Hauptklasse über, während die Relativnormen der
 q -Klassen in k_v selbst q -Klassen äquivalent sind und in k'_v das System
der irregulären Klassen dieses Körpers vorstellen.

Da nun der zweite Faktor der Klassenzahl von k_v zugleich die
Klassenzahl von k'_v ist,⁽¹⁸⁾ so ist die Ordnung der Gruppe der q -Klassen
der höchsten im zweiten Faktor der Klassenzahl enthaltenen l -Potenz
gleich und daher die Ordnung der Gruppe der p -Klassen gleich der
höchsten l -Potenz im ersten Faktor.

(17) Wir nehmen positiven Wert:—Wenn $m_{\beta_0} - m' < 0$ ist, so ist $m_{\beta_0} \geq m_{\frac{r}{\beta_0}} \geq 0$.

(18) Vgl. J. Westlund, Transactions of the American Mathematical Society, Vol.
4, 1903.

§ 3.

Irreguläre Kreiskörper der l -ten Einheitswurzeln.

In diesem Paragraphen sei $\nu=1$, d. h. $k_\nu=k_1$. Nach § 2, Kapitel II, erhält man

Satz A⁽¹⁹⁾. Wenn unter den Basiselementen der irregulären Klassengruppe von k_1 für einen bestimmten quadratischen Nichtrest β_0 genau m_{β_0} Klassen $\mathfrak{p}_{j_1}, \mathfrak{p}_{j_2}, \dots$ vorhanden sind, wobei

$$\mathfrak{p}_{j_i}^{s-\beta_{j_i}}=1$$

ist, so daß $\beta_{j_i} \equiv \beta_0 \pmod{l}$ ist, so gibt es entweder m_{β_0} oder $m_{\beta_0}-1$ Basisklassen $\mathfrak{q}_{k_1}, \mathfrak{q}_{k_2}, \dots$, deren zugehörige α_{k_i} kongruent $\frac{r}{\beta_0}$ modulo l sind, wobei

$$\mathfrak{q}_{k_i}^{s-\alpha_{k_i}}=1$$

ist; insbesondere ist, wenn der zweite Fall eintritt, die Einheit η_k singuläre Primärzahl, wobei die der Einheit η_k zugehörige Zahl r^{2k} kongruent $\frac{r}{\beta_0}$ modulo l ist.⁽²⁰⁾

Nun sei $h=l^{n_i}q$ die Klassenzahl von k_i . In jeder Basisklasse $\mathfrak{j}_i$ der irregulären Klassengruppe von k_i existiert ein Ideal $\mathfrak{b}$, welches die q -te Potenz eines Primideales ersten Grades ist.⁽²¹⁾ Setzt man

$$\mathfrak{a}=\mathfrak{b}^{l^{n_i}-1},$$

wobei l^{n_i} die Ordnung von $\mathfrak{j}_i$ ist, so ist $\mathfrak{a}^l$ ein Hauptideal und nach Satz 32 auch $\mathfrak{a}^{s-r^{a_i}}$, $0 < a_i < l$, ein Hauptideal; andererseits ist auch⁽²²⁾

$$\prod_{j=0}^{l-2} \mathfrak{a}^{q_j s^{-j}} \sim 1 \quad (1)$$

und

$$\prod_j \mathfrak{a}^{r-j^{q_j}} \sim 1, \quad (23) \quad (2)$$

(¹⁹) F. Pollaczek, a. a. O., S. 22, Satz VI.

(²⁰) F. Pollaczek, ditto, S. 7, Satz II.

(²¹) H. Hasse, Jahresbericht der deutschen Mathematiker-Vereinigung, **XXXV**, Satz 13.

(²²) D. Hilbert, Bericht, § 109, S. 360.

(²³) T. Morishima, Proceedings of the Physico-Mathematical Society of Japan, **14**, 9, S. 454, Hilfssatz 1.

wobei $q_j = \frac{r^j r_j - r_{j+1}}{l}$, r_j der kleinste positive Rest modulo l von r^j ist, in zweitem Fall $\prod_j$ über alle Werte $r_j = 1, 2, \dots, \left[\frac{\nu l}{r} \right]$; (²⁴) $\nu = 1, 2, \dots, r-1$ ausdehnt. Daher ist nach (1)

$$\prod_j r_j r^{-j a_i} \sim 1,$$

also

$$\sum_j q_j r^{-j a_i} \equiv 0 \pmod{l}, \quad (3)$$

und nach (2)

$$\sum_j r_j r^{j a_i} \equiv 0 \pmod{l}. \quad (4)$$

Wenn $a_i \neq 1$ ungerade ist, so folgt aus (3)

$$\sum_j q_j r^{-j a_i} \equiv (-1)^{\frac{l+2-a_i}{2}} \frac{r^{l-a_i}-1}{r^{-a_i}(l-a_i)} B_{\frac{l-a_i}{2}} \equiv 0 \pmod{l}, \quad (25)$$

wobei für $a_i = 1$ $\sum_j q_j r^{-j} \not\equiv 0 \pmod{l}$ ist. Wenn $a_i \neq l-1$ gerade ist, so folgt aus (4)

$$\sum_j r_j r^{j a_i} \equiv (-1)^{\frac{a_i}{2}} \frac{r^{a_i}-1}{a_i r^{a_i-1}} B_{\frac{a_i}{2}} \equiv 0 \pmod{l}, \quad (26)$$

wobei für $a_i = l-1$ $\sum_j r_j r^{j a_i} \not\equiv 0 \pmod{l}$ ist. Hieraus folgt der Satz:

Satz 38. Wenn $B_m \not\equiv 0 \pmod{l}$, $0 < m < \mu$, ist, so existiert nicht derjenige $\mathfrak{p}$ -Klasse, deren zugehörige Zahl $r^{l^{n_i}-1(l-2m)}$ ist, wobei l^{n_i} die Ordnung von $\mathfrak{p}$ ist, und auch derjenige $\mathfrak{q}$ -Klasse, deren zugehörige Zahl $r^{l^{n_j}-12m}$ ist. Für $m = \mu$ gilt auch diese Behauptung, d.h. existieren nicht derjenige $\mathfrak{p}$ -Klasse und $\mathfrak{q}$ -Klasse, deren zugehörige Zahlen $r^{l^{n_i}-1}$ bzw. 1 sind.

Nun sei

$$E_n = E_n(\xi_1) = \prod_{i=0}^{\mu-1} \left[\sqrt{\frac{1-\xi_1^{r^{i+1}}}{1-\xi_1^{r^i}} \frac{1-\xi_1^{-r^{i+1}}}{1-\xi_1^{-r^i}}} \right] r^{2(\mu-i)n}$$

$$(n=1, 2, \dots, \mu-1)$$

und

$$l_i(\alpha) = \left[\frac{d^i \log \alpha(e^v)}{dv^i} \right]_{v=0}$$

$$(i=1, 2, \dots, l-1).$$

(²⁴) $[x]$: die größte ganze Zahl $\leq x$.

(²⁵) F. Pollaczek, a. a. O., S. 25, S. 26, Satz VIII. B_n : Bernoullische Zahl.

(²⁶) T. Morishima, a. a. O., S. 463.

Für E_n gilt dann⁽²⁷⁾

$$I_{2i}(E_n) \equiv 0 \pmod{l} \quad (i \neq n),$$

$$I_{2n}(E_n) \equiv \frac{(-1)^{n+1}(l-1)(r^{2n}-1)}{4n} B_n \pmod{l}$$

und

$$I_{2i-1}(E_n) \equiv 0 \pmod{l} \\ (i=1, 2, \dots, \mu).$$

Daher ist für alle $i=1, 2, \dots, l-1$

$$I_i(E_n) \equiv 0 \pmod{l},$$

dann und nur dann, wenn $B_n \equiv 0 \pmod{l}$ ist. Setzt man

$$E_n = a_0 + a_1 \zeta_1 + \dots + a_{l-1} \zeta_1^{l-1},$$

wobei a_i ganze rationale Zahlen sind, so ist

$$E_n(1) = a_0 + a_1 + \dots + a_{l-1} = r^{bl},$$

wobei b eine ganze rationale Zahl ist, und, wenn für alle $i=1, 2, \dots, l-1$

$$I_i(E_n) \equiv 0 \pmod{l},$$

also auch $B_n \equiv 0 \pmod{l}$ ist, so ist für $i=1, 2, \dots, l-1$

$$a_1 + 2^i a_2 + \dots + (l-1)^i a_{l-1} \equiv 0 \pmod{l},$$

also $a_1 \equiv a_2 \equiv \dots \equiv a_{l-1} \equiv 0 \pmod{l}$, folglich

$$E_n \equiv \sum_{i=0}^{l-1} a_i \equiv r^{bl} \pmod{\lambda l},$$

d. h. E_n eine Primärzahl, wobei $\lambda = 1 - \zeta_1$ ist. Wenn umgekehrt E_n primär ist, so ist $B_n \equiv 0 \pmod{l}$.

Es sei jetzt $\eta_1, \eta_2, \dots, \eta_r$ ein System von Grundeinheiten mit der Eigenschaft

$$\eta_i^{s-r^{2i}} = \eta_i^{r^i} \quad (i=1, 2, \dots, r).$$

Wenn E_n der l -ten Potenz einer Einheit ε nicht gleich ist, so ist

$$\eta_n = E_n^c \eta_n''^l,$$

da

$$E_n(\zeta_1^r) = E_n^{r^{2n}} \tilde{\eta}_n^l$$

ist, und auch

$$E_n = \eta_n^a \eta_n'''^l.$$

Hieraus folgt der Satz:

(²⁷) H. S. Vandiver, Trans. Am. Math. Soc., 31, 4, S. 620.

Hilfssatz. Ist für ein n

$$E_n \neq \varepsilon^l,$$

so ist η_n dann und nur dann primär, wenn $B_n \equiv 0 \pmod{l}$ ist.

Nun seien

$$p_{11}, p_{12}, \dots, p_{1\alpha_1},$$

$$p_{21}, p_{22}, \dots, p_{2\alpha_2},$$

$$\dots\dots\dots$$

$$p_{j1}, p_{j2}, \dots, p_{j\alpha_j}$$

alle p -Klassen, wobei für $k=1, 2, \dots, \alpha_i$

$$p_{ik}^{s-r^{n_{ik}-1}(l-2m_i)} = 1,$$

$$(i=1, 2, \dots, j)$$

sind, und für $i=1, 2, \dots, j'$ die Anzahl der q -Klassen, deren zugehörige Zahlen kongruent r^{2m_i} modulo l sind, d. h.

$$q_{ik}^{s-r^{2m_i}l^{n'_{ik}-1}} = 1,$$

$$(k=1, 2, \dots),$$

α_i-1 , für $i=j'+1, j'+2, \dots, j$ die Anzahl der q -Klassen, deren zugehörige Zahlen kongruent r^{2m_i} modulo l sind, α_i . Ferner sei t_1, t_0 die Anzahl der p -Klassen bzw. q -Klassen und

$$q_{ik}^{n'_{ik}} = (\rho_{ik}). \quad (5)$$

Dann sind

$$t_1 = \alpha_1 + \alpha_2 + \dots + \alpha_j,$$

$$t_0 = \alpha_1 + \alpha_2 + \dots + \alpha_j - j',$$

also

$$t_1 - t_0 = j',$$

und nach Satz A und §2 für $i=1, 2, \dots, j'$ alle ρ_{ik}, η_m primär, wobei $k=1, 2, \dots, \alpha_i-1$ und

$$\eta_{m_i}^{s-r^{2m_i}} = \eta_{m_i}'^l$$

sind. Andererseits folgt aus der Arbeit von Herrn Prof. Takagi⁽²⁸⁾

$$r^+ = t_1 - t_0^+,$$

wobei r^+ die Anzahl der Primärzahlen in Grundeinheiten η_{m_i} und t_0^+ die

(²⁸) Journal für die reine und angewandte Mathematik, 157 (1927), S. 238.

Anzahl der Primärzahlen in ρ_{ik} bedeutet. Daher ist

$$r^+ = t_1 - t_0^+ \geq t_1 - t_0 = j'.$$

Wenn insbesondere $t_0^+ = t_0$ ist, so ist

$$r^+ = j'.$$

Daher gilt nach Hilfssatz

Satz 39. Wenn für ein m

$$B_m \equiv 0 \pmod{l}, \quad E_m \not\equiv \varepsilon^l$$

ist und alle ρ_{ik} in (5) primär sind, so existiert in k_1 mindestens eine $\mathfrak{p}$ -Klasse mit der Eigenschaft

$$\mathfrak{p}^{s-\rho^{2m}(l-2m)} = 1,$$

und, wenn die Anzahl dieser $\mathfrak{p}$ -Klassen α ist, so existieren in k_1 genau $\alpha-1$ $\mathfrak{q}$ -Klassen, deren, zugehörige Zahlen kongruent r^{2m} modulo l sind.

Weiter gilt

Satz 40. Es seien

$$B_{m_1}, B_{m_2}, \dots, B_{m_t}$$

die durch l teilbaren Bernoullischen Zahlen, deren Anzahl genau t ist. Wenn alle ρ_{ik} in (5) primär sind, so ist

$$r^+ = j' \leq t.$$

Nun sei insbesondere der zweite Faktor h_2 der Klassenzahl von k_1 zu l prim, dann ist in Satz A $m_{\beta_0} = 1$, $t_0^+ = t_0 = 0$, also $r^+ = j' = j$, und⁽²⁹⁾ für alle m

$$E_m \not\equiv \varepsilon^l,$$

also nach Hilfssatz

$$r^+ = t.$$

Daher gilt

Satz B.⁽³⁰⁾ Es sei h_2 zu l prim und seien

$$B_{m_1}, B_{m_2}, \dots, B_{m_t}$$

die durch l teilbaren Bernoullischen Zahlen, deren Anzahl genau t ist. Dann existieren in k_1 genau t $\mathfrak{p}$ -Klassen

$$\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_t,$$

wobei

⁽²⁹⁾ H. S. Vandiver, Proc. Nat. Acad. Sci., 16, 11 (1930).

⁽³⁰⁾ H. S. Vandiver, a. a. O., 15, 3 (1929). Vgl. J. Herbrand, Journal de Math. Pures et Appliquées, **XI**, S. 417-441, (1932).

$$p_i^{s-r} l^{n_i-1(l-2m_i)} = 1 \quad (i=1, 2, \dots, t)$$

sind, und umgekehrt.⁽³¹⁾

Ferner sei $B_{m_i} \equiv 0 \pmod{l}$ und n_i die größte ganze Zahl, derart, daß

$$B_{\frac{n_i-1(2m_i-1)+1}{2}} \equiv 0 \pmod{l^{n_i}}$$

ist. Dann existiert nach Satz B eine Klasse p_i , wobei

$$p_i^{s-r} l^{n_i-1(l-2m_i)} = 1$$

ist, und ist l^{n_i} die Ordnung von p_i .

§ 4.

Der erste Faktor der Klassenzahl des Kreiskörpers der l^v -ten Einheitswurzeln.

Hier schließen wir eine Untersuchung über die Teilbarkeit des ersten Faktors h_v der Klassenzahl von k_v durch l an. Es sei $\mu_v = \frac{l^{v-1}(l-1)}{2}$, θ_v eine primitive $2\mu_v$ -te Einheitswurzel, $r_i^{(v)}$ der kleinste positive Rest modulo l^v von r^i und

$$q_l^{(v)} = \frac{r^v q_i^{(v)} - r_{i+1}^{(v)}}{l^v}.$$

Dann ist

$$\frac{h_v}{h_{v-1}} = \frac{\prod_{i=1}^{\mu_v} g_v(\theta_v^{2i-1})}{\frac{2^{\mu_v - \mu_{v-1}}}{l} \frac{r^{\mu_v} + 1}{r^{\mu_{v-1}} + 1}}, \quad (32)$$

wobei $g_v(\theta_v) = \sum_{i=0}^{2\mu_v-1} q_i^{(v)} \theta_v^i$ ist, und insbesondere

$$h_1 = \frac{g_1(\theta_1) g_1(\theta_1^3) \dots g_1(\theta_1^{l^1-2})}{(-1)^{\mu_1} 2^{\mu_1-1} \frac{r^{\mu_1} + 1}{l}}.$$

(31) Die Umkehrung gilt auch für $h_i \equiv 0 \pmod{l}$.

(32) J. Westlund, a. a. O.

Für die primitive 2μ -te Einheitswurzel kann $\theta_v = \theta_1 \zeta_{v-1}$ gesetzt werden und wir fassen die Faktoren im Zähler von $\frac{h_v}{h_{v-1}}$ folgendermaßen zusammen:

$$g_v(\theta_1 \zeta_{v-1}) g_v(\theta_1 \zeta_{v-1}^r) \dots g_v(\theta_1 \zeta_{v-1}^{2\mu_{v-1}-1}) \dots g_v(\theta_1^{t-2} \zeta_{v-1}) \dots g_v(\theta_1^{t-2} \zeta_{v-1}^{2\mu_{v-1}-1}).$$

Weiter gilt für $g_v(\theta_1^{t'})$

$$g_v(\theta_1^{t'}) = \sum_{i=0}^{l-2} \sum_{j=0}^{l^{v-1}-1} q_{2j\mu_1+i}^{(v)} \theta_1^{t'j} = \sum_{i=0}^{l-2} q_i^{(1)} \theta_1^{t'j} = g_1(\theta_1^{t'}),$$

wobei $t' = 2t - 1$ ist. Es seien $\mathfrak{L} = (l, r - \theta_1)$ und $\mathfrak{L}_{v-1} = (\mathfrak{L}, 1 - \zeta_{v-1})$ Ideale im Kreiskörper von θ_v . Dann ist

$$\mathfrak{L}_{v-1}^{l^{v-2}(l-1)} = \mathfrak{L}.$$

Für jeden Faktor $g_i(\theta_1^{t'})$ im Zähler von h_1 , der durch $\mathfrak{L}$ teilbar ist, enthält daher $g_v(\theta_1^{t'} \zeta_{v-1})$ das Ideal $\mathfrak{L}_{v-1}$ mindestens zur ersten Potenz, also ist

$$g_v(\theta_1^{t'} \zeta_{v-1}) g_v(\theta_1^{t'} \zeta_{v-1}^r) \dots g_v(\theta_1^{t'} \zeta_{v-1}^{2\mu_{v-1}-1})$$

mindestens durch $\mathfrak{L}$ teilbar. Wenn genau n unter den ersten $\mu_1 - 1$ Bernoullischen Zahlen durch l teilbar sind, so sind genau n Faktoren von h_1 durch $\mathfrak{L}$ teilbar, ⁽³³⁾ also ist $\frac{h_v}{h_{v-1}}$ mindestens durch l^n teilbar.

Nun ergibt die Entwicklung nach Potenzen von $1 - \zeta_{v-1}$

$$g_v(\theta_1^{t'} \zeta_{v-1}) = g_v(\theta_1^{t'}) - (1 - \zeta_{v-1}) \sum_{k=0}^{2\mu_{v-1}-1} k q_k^{(v)} \theta_1^{t'k} + (1 - \zeta_{v-1})^2 f(\theta_1, \zeta_{v-1}). \quad (1)$$

Notwendig und hinreichend dafür, daß $\frac{h_v}{h_{v-1}}$ durch l^{n+1} teilbar ist, ist das Bestehen der Kongruenz

$$g_v(\theta_1^{t'} \zeta_{v-1}) \equiv 0 \pmod{\mathfrak{L}_{v-1}^2}. \quad (2)$$

Soll diese Kongruenz erfüllt sein, so muß also nach (1)

$$\sum_{k=0}^{2\mu_{v-1}-1} k q_k^{(v)} \theta_1^{t'k} \equiv 0 \pmod{\mathfrak{L}}$$

sein. Weiter gilt

(33) F. Pollaczek, a. a. O., S. 25 (13'), (15).

$$g_v(r^{t'}) \equiv g_v(\theta_1^{t'}) + t' \frac{r - \theta_1}{\theta_1} \sum_k k q_k^{(v)} \theta_1^{kt'} \pmod{\mathfrak{L}^2}, \quad (34)$$

also

$$\begin{aligned} t'(1 - r^{t'-1}) \sum_k k q_k^{(v)} \theta_1^{kt'} &\equiv g_v(r^{t'}) - g_1(\theta_1^{t'}) \\ &\equiv g_v(r^{t'}) - g_1(r^{t'}) \pmod{\mathfrak{L}^2}, \end{aligned} \quad (3)$$

da $r^j \equiv \theta_1 \pmod{\mathfrak{L}^2}$ ist. Ferner gilt

$$\begin{aligned} g_1(r^{t'}) &\equiv - \frac{r^{t'+1} - 1}{2r^{t'}} \frac{(-1)^{\frac{t'+1}{2}} B_{\frac{t'+1}{2}}}{\frac{t'+1}{2}} \pmod{l^2}, \quad (35) \\ g_v(r^{t'}) &\equiv - \frac{r^{t'+1} - 1}{2r^{t'}} \frac{(-1)^{\frac{t'+1}{2}} B_{\frac{t'+1}{2}}}{\frac{t'+1}{2}} \quad (t' > 1) \pmod{l^2}. \quad (36) \end{aligned}$$

Sollen daher (2) erfüllt sein, so muß nach (3) die Kongruenz

$$\frac{B_{\frac{t'+1}{2} + \mu_1}}{\frac{t'+1}{2} + \mu_1} \equiv (-1)^{\mu_1} \frac{B_{\frac{t'+1}{2}}}{\frac{t'+1}{2}} \pmod{l^2} \quad (37)$$

bestehen. Also erhält man

Satz 41. Wenn genau n unter den $\mu_1 - 1$ ersten Bernoullischen Zahlen durch l teilbar sind, so ist $\frac{h_v}{h_{v-1}}$ mindestens durch l^n teilbar, wobei h_v den ersten Faktor der Klassenzahl von k_v bedeutet. Notwendig

(34) F. Pollaczek, a. a. O., S. 28.

(35) F. Pollaczek, a. a. O., S. 25 (13').

(36) Wir erheben die Gleichung $r_{k+1}^{(v)} = r r_k^{(v)} - l^v q_k^{(v)}$ zur $t' + 1$ -ten Potenz:

$$r_{k+1}^{(v)(t'+1)} \equiv (r r_k^{(v)})^{t'+1} - (t' + 1) l^v q_k^{(v)} (r r_k^{(v)})^{t'} \pmod{l^{2v}}$$

und erhalten daraus durch Summierung über $k = 0, 1, \dots, 2\mu_v - 1$

$$\begin{aligned} l^v g_v(r^{t'}) &\equiv \frac{r^{t'+1} - 1}{r^{t'}(t' + 1)} \sum_{i=0}^{v-1} \sum_{j=1}^{t'-1} (j + li)^{t'+1} \equiv \frac{r^{t'+1} - 1}{r^{t'}(t' + 1)} l^{v-1} \sum_{j=1}^{t'-1} j^{t'+1} \pmod{l^{v+2}}, \\ g_v(r^{t'}) &\equiv \frac{r^{t'+1} - 1}{r^{t'}(t' + 1)} \frac{1}{l} \sum_{j=1}^{t'-1} j^{t'+1} \equiv (-1)^{\frac{t'-1}{2}} \frac{r^{t'+1} - 1}{r^{t'}(t' + 1)} B_{\frac{t'+1}{2}} \pmod{l^2}. \end{aligned}$$

(37) F. Pollaczek, a. a. O., S. 28 (13'').

und hinreichend dafür, daß $\frac{h_\nu}{h_{\nu-1}}$ durch l^{n+1} teilbar ist, ist das Bestehen der Kongruenzen

$$\frac{B_{\mu_1+i}}{\mu_1+i} \equiv (-1)^{\mu_1} \frac{B_i}{i} \pmod{l^2}$$

und

$$B_i \equiv 0 \pmod{l}$$

für ein $i < \mu_1$.

§ 5.

Der l^ν -te Potenzrestcharakter im Kreiskörper der l^ν -ten Einheitswurzeln.

In diesem Paragraphen sei

$\nu > 1$,

p eine von l verschiedene ungerade Primzahl,

$\mathfrak{p}$ ein Primidealteiler von p in k_ν ,

$N\mathfrak{p} = p^f$, also $p^f \equiv 1 \pmod{l^\nu}$,

g eine primitive Wurzel modulo $\mathfrak{p}$,

$$\psi_a(\xi_\nu) = \psi = \sum_{\substack{i=0 \\ i \neq \frac{p^f-1}{2}}}^{p^f-2} \xi_\nu^{-(d+1)i + \text{ind}(g^i+1)}, \quad (38) \quad \psi \bar{\psi} = p^f,$$

wobei ind. in bezug auf $\mathfrak{p}$ und g genommen ist und $d \not\equiv 0, -1 \pmod{l}$ ist.

Hilfssatz 1. Für $m \geq 0$ ist

$$(\psi \bar{\psi})_0^{(2m+1)} \equiv 0 \pmod{l^\nu}. \quad (39)$$

Hilfssatz 2. Für $m > 0$ ist

$$(\psi \bar{\psi})_0^{(2m)} \equiv \begin{cases} 0 & \pmod{l^\nu}, \text{ wenn } m \not\equiv 0 \pmod{\mu} \text{ ist,} \\ 3 \frac{p^f-1}{l} & \pmod{l^\nu}, \text{ wenn } m \equiv 0 \pmod{\mu} \text{ ist.} \end{cases} \quad (40)$$

Beweis: Es ist

$$(38) \quad \bar{\psi} = \psi_a(\xi_\nu^{-1}).$$

$$(39) \quad (\psi \bar{\psi})_0^{(i)} = \left[\frac{d^i \psi_a(e^\nu) \bar{\psi}_a(e^\nu)}{d\nu^i} \right]_{\nu=0}.$$

$$(40) \quad \mu = \frac{l-1}{2}.$$

$$\begin{aligned}
(\psi\bar{\psi})_0^{(2m)} &\equiv \sum_{t=0}^{2m} \binom{2m}{t} (\psi)_0^{(2m-t)} (\bar{\psi})_0^{(t)} \\
&\equiv \sum_{t=0}^{2m} (-1)^t \binom{2m}{t} \sum_i [-(d+1)i + \text{ind}(g^i + 1)]^{2m-t} \\
&\quad \cdot \sum_j [-(d+1)j + \text{ind}(g^j + 1)]^t \\
&\equiv \sum_{i,j} \left[-(d+1)(i-j) + \text{ind}\left(\frac{g^i + 1}{g^j + 1}\right) \right]^{2m} \\
&\equiv \sum_{\substack{k,h=1 \\ k \neq h}}^{p^f-2} [-(d+1)k + h]^{2m} \\
&\equiv \sum_{k,h=1}^{p^f-2} [-(d+1)k + h]^{2m} - \sum_{k=1}^{p^f-2} (dk)^{2m} \\
&\equiv \begin{cases} 0 & (\text{mod } l^v) \text{ für } \mu \nmid m, \text{ (41)} \\ 3 \frac{p^f-1}{l} & (\text{mod } l^v) \text{ für } \mu \mid m. \end{cases}
\end{aligned}$$

Nun folgt aus $\psi\bar{\psi} \frac{d \log \psi(e^v)}{dv} = \bar{\psi} \frac{d\psi(e^v)}{dv}$

$$\sum_{t=0}^{2m} \binom{2m}{i} (\psi\bar{\psi})_0^{(t)} l_{2m+1-i}(\psi) = \sum_{t=0}^{2m} \binom{2m}{i} (\psi)_0^{(2m+1-i)} (\bar{\psi})_0^{(t)}. \text{ (42)}$$

Daher ist nach Hilfssatz 1 und Hilfssatz 2

$$\begin{aligned}
&l_{2m+1}(\psi) + 3 \frac{p^f-1}{l} \sum_{\substack{i \geq 0 \\ i(l-1) \leq 2m}} \binom{2m}{i(l-1)} l_{2m+1-i(l-1)}(\psi) \\
&\equiv \sum_{t=0}^{2m} (-1)^t \binom{2m}{t} \sum_{i,j} [-(d+1)i + \text{ind}(g^i + 1)]^{2m+1-t} [-(d+1)j + \text{ind}(g^j + 1)]^t \\
&\equiv \sum_{i,j} \left[-(d+1)i + \text{ind}(g^i + 1) \right] \left[-(d+1)(i-j) + \text{ind}\left(\frac{g^i + 1}{g^j + 1}\right) \right]^{2m} \\
&\equiv \sum_{\substack{k,h=1 \\ k \neq h}}^{p^f-2} [-(d+1)\text{ind}(g^k - 1) + \text{ind}(g^h - 1) + d\text{ind}(g^k - g^h)] [(d+1)k - h]^{2m}
\end{aligned}$$

(41) G. Polya und G. Szegő, Aufgaben und Lehrsätze II, S. 158, 246 (1925).

(42) Vgl. § 3, S. 114.

$$\begin{aligned}
 &\equiv \sum_{\substack{h, h'=1 \\ k+h}}^{p^f-2} [-(d+1)\text{ind}(g^h-1) + \text{ind}(g^k-1)][(d+1)k-h]^{2m} \\
 &\quad + d \sum_{\substack{h, h'=1 \\ k+h \neq p^f-1}}^{p^f-2} [\text{ind } g^k + \text{ind}(1-g^{h'})][dk-h']^{2m} \\
 &\equiv \sum_{h, h'=1}^{p^f-2} [-(d+1)\text{ind}(g^h-1) + \text{ind}(g^k-1)][(d+1)k-h]^{2m} \\
 &\quad + d \sum_{h, h'=1}^{p^f-2} [k + \text{ind}(g^{h'}-1)][dk-h']^{2m} + d^{2m+1} \sum_{h=1}^{p^f-2} h^{2m} \text{ind}(g^h-1) \\
 &\quad - (d+1)^{2m} d \sum_{k=1}^{p^f-2} k^{2m} \text{ind}(g^k-1) \\
 &\equiv (1 - (d+1)^{2m}) q l^{p-1} \sum_h \text{ind}(g^h-1) \sum_{i=1}^{2m} \binom{2m}{i(l-1)} h^{2m-i(l-1)} \\
 &\quad + [1 + d^{2m+1} - (d+1)^{2m+1}] \sum_h h^{2m} \text{ind}(g^h-1) \pmod{l^p}, \quad (1)
 \end{aligned}$$

wobei $p^f-1=ql^p$ ist. In der rechten Seite von (1) ist

$$1 - (d+1)^{2m} \equiv 0 \pmod{l},$$

wenn $\mu \mid m$ ist; und ist auch

$$\begin{aligned}
 &\sum_h \text{ind}(g^h-1) \sum_i \binom{2m}{i(l-1)} h^{2m-i(l-1)} \\
 &\equiv \sum_h h^{2m} \text{ind}(g^h-1) \sum_{i>0} \binom{2m}{i(l-1)} \equiv 0 \pmod{l}, \quad (43)
 \end{aligned}$$

wenn $\mu \nmid m$ ist. Daher ist nach (1) für $m > 0$

$$\begin{aligned}
 &l_{2m+1}(\psi) + 3ql^{p-1} \sum_{i=1}^{2m} \binom{2m}{i(l-1)} l_{2m+1-i(l-1)}(\psi) \\
 &\equiv [1 + d^{2m+1} - (d+1)^{2m+1}] \sum_h h^{2m} \text{ind}(g^h-1) \pmod{l^p}. \quad (2)
 \end{aligned}$$

Insbesondere ist für modulo l

$$(43) \quad \sum_{i=0}^{l-2} (1+i)^{2m} \equiv - \left(1 + \sum_{i>0} \binom{2m}{i(l-1)} \right) \equiv \begin{cases} -1 \pmod{l} & \text{für } \mu \nmid m, \\ -2 \pmod{l} & \text{für } \mu \mid m. \end{cases}$$

$$l_{2m+1}(\psi) \equiv [1 + d^{2m+1} - (d+1)^{2m+1}] \sum_h h^{2m} \text{ind}(g^h - 1) \pmod{l},$$

da $\nu > 1$ ist, also

$$l_{2m+1}(\psi) \equiv l_{2m+1+l(l-1)}(\psi) \pmod{l}.$$

Wenn $m \not\equiv 0 \pmod{\mu}$ ist, so ist $2m+1-i(l-1) > 2$, also

$$\begin{aligned} & \sum_{i \geq 0} \binom{2m}{i(l-1)} l_{2m+1-i(l-1)}(\psi) \\ & \equiv \sum_{i \geq 0} \binom{2m}{i(l-1)} l_{2m+1}(\psi) \equiv 0 \pmod{l}. \quad (^{44}) \end{aligned}$$

Wenn $m \equiv 0 \pmod{\mu}$ ist, so ist

$$\begin{aligned} & \sum_{i \geq 0} \binom{2m}{i(l-1)} l_{2m+1-i(l-1)}(\psi) \\ & \equiv \sum_{\substack{m \geq i \geq 0 \\ \mu}} \binom{2m}{i(l-1)} l_{2m+1}(\psi) + l_1(\psi) \\ & \equiv l_1(\psi) \equiv 0 \pmod{l}. \quad (^{45}) \end{aligned}$$

Daher folgt aus (2) für $2m \geq \nu$

$$\begin{aligned} l_{2m+1}(\psi) & \equiv [1 + d^{2m+1} - (d+1)^{2m+1}] \sum_{h=1}^{l^J-2} h^{2m} \text{ind}(g^h - 1) \\ & \equiv [1 + d^{2m+1} - (d+1)^{2m+1}] \sum_{h=0}^{q-1} \sum_{i=1}^{l^p-1} i^{2m} \text{ind}(g^{hl^p+i} - 1) \\ & \equiv [1 + d^{2m+1} - (d+1)^{2m+1}] \sum_{i=1}^{l^p-1} i^{2m} \text{ind} \prod_{h=0}^{q-1} (g^{hl^p+i} - 1) \\ & \equiv [1 + d^{2m+1} - (d+1)^{2m+1}] \sum_{i=1}^{l^p-1} i^{2m} \text{ind}(g^{qi} - 1) \\ & \equiv [1 + d^{2m+1} - (d+1)^{2m+1}] \sum_{i=0}^{2\mu l^p-1} i^{2m} \text{ind}(g^{qi} - 1) \pmod{l^p}. \quad (3) \end{aligned}$$

(⁴⁴) (⁴⁵) Vgl. S. 123.

Nun ist in k_v

$$g^a \equiv \zeta, \quad (\text{mod } \mathfrak{p}),$$

$$g^{a^{r^i}} - 1 \equiv \zeta_v^{r^i} - 1 \quad (\text{mod } \mathfrak{p}),$$

also

$$\text{ind}(g^{a^{r^i}} - 1) \equiv \text{ind}(\zeta_v^{r^i} - 1) \quad (\text{mod } l^v).$$

Aus (3) folgt also

$$\mathfrak{I}_{2m+1}(\psi) \equiv [1 + d^{2m+1} - (d+1)^{2m+1}] \sum_{i=0}^{2\mu l^{v-1}-1} r^{2mi} \text{ind}(\zeta_v^{r^i} - 1) \quad (\text{mod } l^v), \quad (4)$$

wobei $2m \equiv v$ ist. Andererseits ist

$$\begin{aligned} 2 \text{ind } E_{2\mu l^{v-1}-m} &\equiv \text{ind} \prod_{i=0}^{2\mu l^{v-1}-1} \left[\sqrt{\frac{1-\zeta_v^{r^{i+1}}}{1-\zeta_v^{r^i}}} \frac{1-\zeta_v^{-r^{i+1}}}{1-\zeta_v^{-r^i}} \right] r^{2mi} \\ &\equiv \sum_{i=0}^{2\mu l^{v-1}-1} r^{2mi} \text{ind} \frac{1-\zeta_v^{r^{i+1}}}{1-\zeta_v^{r^i}} \\ &\equiv \sum_i r^{2m(i-1)} \text{ind}(1-\zeta_v^{r^i}) - \sum_i r^{2mi} \text{ind}(1-\zeta_v^{r^i}) \\ &\equiv (r^{-2m} - 1) \sum_i r^{2mi} \text{ind}(1-\zeta_v^{r^i}) \quad (\text{mod } l^v). \end{aligned} \quad (5)$$

Folglich ist nach (4) und (5)

$$2 \text{ind } E_{\mu l^{v-1}-m} \equiv \frac{r^{-2m} - 1}{1 + d^{2m+1} - (1+d)^{2m+1}} \mathfrak{I}_{2m+1}(\psi) \quad (\text{mod } l^v).$$

Hieraus folgt der Satz:

Satz 42. Es sei $\mathfrak{p}$ ein beliebiges Primideal in k_v ,

$$E_m = \prod_{i=0}^{\mu l^{v-1}-1} \left[\sqrt{\frac{1-\zeta_v^{r^{i+1}}}{1-\zeta_v^{r^i}}} \frac{1-\zeta_v^{-r^{i+1}}}{1-\zeta_v^{-r^i}} \right] r^{2(2\mu l^{v-1}-m)i}$$

$\left(\frac{E_m}{\mathfrak{p}}\right)$ der l^v -te Potenzrestcharakter in k_v . Dann gilt

$$\left(\frac{E_m}{\mathfrak{p}}\right) = \zeta_v^{\alpha_m \mathfrak{I}_{2(l-1)l^{v-1}-2m+1}(\psi)}$$

$$(m=1, 2, \dots, \mu l^{\nu-1}-1),$$

wobei

$$a_m \equiv \frac{r^{2m}-1}{2(1+d^{-2m+1}-(1+d)^{-2m+1})} \pmod{l^\nu}$$

ist.