Sitzungsberichte

der

mathematisch-naturwissenschaftlichen Abteilung

der

Bayerischen Akademie der Wissenschaften zu München

1944. Heft III

Sitzungen Oktober-Dezember

München 1947

Verlag der Bayerischen Akademie der Wissenschaften

In Kommission beim Biederstein Verlag München

Published 1947 under Military Government Information Control License No. US-E-178

Druck der C. H. Beck'schen Buchdruckerei in Nördlingen
Printed in Germany. Auflage 1000

Über die Herstellung einer Basis für die ganzen Zahlen eines algebraischen Zahlkörpers.

Von **Heinrich Tietze** in München.

Vorgelegt am 13. Oktober 1944.

1. In einer früheren Mitteilung[1] wurde ein einfacher Beweis für einen Satz gegeben, den man in etwas anderer Gestalt schon bei Dedekind finden kann (vgl. Nr. **2**, Satz 2), der aber nicht sehr bekannt geworden ist. Der Satz lautet:

Satz 1. Es sei ϑ eine algebraische Zahl vom Grad n, wobei wir ϑ als ganz voraussetzen wollen; $\alpha_1, \ldots, \alpha_n$ seien n unabhängige ganze Zahlen des Zahlkörpers $K(\vartheta)$,

$$D = D(\alpha_1, \ldots, \alpha_n) = m^2 w \tag{1}$$

ihre Diskriminante, dabei $m > 0$, w quadratfrei und $\geqq 0$, $D = \Delta^2$ und

$$\Delta = \Delta(\alpha_1, \ldots, \alpha_n) = |\alpha_1^{(\mu)}, \ldots, \alpha_n^{(\mu)}|_{\mu = 0, \ldots, n-1} = \pm m\sqrt{w},$$

unter $\alpha_\nu, \alpha_\nu', \ldots, \alpha_\nu^{(n-1)}$ die n zu α_ν konjugierten Zahlen (inclusive α_ν) verstanden. Wenn dann für rationale $c_1, \ldots, c_n$ die Zahl

$$\omega = c_1\alpha_1 + \ldots + c_n\alpha_n \tag{2}$$

aus $K(\vartheta)$ ganz ist, dann sind alle mc_ν ganz rational[2]. Anders gesagt: Der Modul aller ganzen Zahlen aus $K(\vartheta)$ enthält nur Zahlen des Moduls $\left[\frac{\alpha_1}{m}, \ldots, \frac{\alpha_n}{m}\right]$.

---

[1] Sitzungsberichte der Bayerischen Akademie der Wissenschaften, Mathemat.-naturwiss. Abteilung, Jahrgang 1942, S. 8*–10*, Bericht über die Sitzung vom 14. März 1942, Punkt 3.

[2] Werden nämlich die n Gleichungen, die aus (2) durch Hinzunahme der konjugierten Gleichungen entstehen, nach den c_ν aufgelöst: $c_\nu = \Gamma_\nu : \Delta$, so sind die Zahlen $c_\nu^2 D = (mc_\nu)^2 w$ ganz und zugleich rational, die rationalen Zahlen mc_ν können somit nicht gebrochen sein.

Im besonderen Fall $\alpha_\nu = \vartheta^{\nu-1}$ $(\nu = 0, \ldots, n-1)$, $D = D(\vartheta) = m^2 w$ sind also die ganzen Zahlen aus $K(\vartheta)$ nicht nur, – wie bekannt und wie bei Herstellung einer Basis allgemein benutzt wird, – im Modul $\left[\frac{1}{D}, \frac{\vartheta}{D}, \ldots, \frac{\vartheta^{n-1}}{D}\right]$, sondern speziell in $\left[\frac{1}{m}, \frac{\vartheta}{m}, \ldots, \frac{\vartheta^{n-1}}{m}\right]$ enthalten[3].

Als Anwendung des Satzes 1 werde nun in Nr. **3** der besondere Fall $\vartheta = \sqrt[3]{G}$, G ganz rational und kubusfrei, besprochen[4] und eine Basis für $K\left(\sqrt[3]{G}\right)$ hergestellt, wobei man auf eben jene Fallunterscheidung in Körper „erster" und „zweiter Art" stößt, die Dedekind l. c.[4] in §§ 3, 4 durch Untersuchung der Primidealzerlegung der Zahl 3 aufgestellt hat.

Mit der Ermittelung einer Basis ist zugleich die Bestimmung der Körperdiskriminante d geleistet. Andererseits hat U. Wegner[5] für jede beliebige ungerade Primzahl p die Körperdiskriminante von $K\left(\sqrt[p]{G}\right)$ angegeben und für $p = 3$ deckt sich die vorerwähnte Fallunterscheidung mit einer bei Wegner auf-

---

[3] Wohl aber ist für $n = 2$, $\vartheta = \sqrt{G}$, $\Delta = -2\sqrt{G}$, $D = 4G$, wo $m = 2$ wird, allgemein bekannt, daß alle ganzen Zahlen aus $K(\vartheta)$ zu $\left[\frac{1}{2}, \frac{\vartheta}{2}\right]$ gehören.

Es sei gestattet, hier einen in gleicher Richtung liegenden tieferen Satz anzuführen, auf den mich freundlicherweise Herr Hecke aufmerksam gemacht hat, als ich ihm im ersten Vierteljahr 1942 über die Bemerkung im Text geschrieben hatte: Gemäß Satz 104 in E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen (1923), S. 135, gilt: Sei $F(x) = 0$ die irreduzible Gleichung für ϑ. Dann ist $F'(\vartheta) = \mathfrak{f} \cdot \mathfrak{d}$ durch die Körperdifferente $\mathfrak{d}$ teilbar und jede ganze durch $\mathfrak{f}$ (den Führer des Ringes $R(\vartheta)$) teilbare Zahl gehört zu $R(\vartheta)$. Wenn also k eine ganz rationale durch $\mathfrak{f}$ teilbare Zahl ist, so ist für beliebiges ganzes $\omega = \sum_{\nu=0}^{n-1} c_\nu \vartheta^\nu$ die Zahl $\omega k \equiv 0 \pmod{\mathfrak{f}}$, also ω gleich einer Ringzahl dividiert durch k; d. h. die Koeffizienten c_ν haben die Eigenschaft: $c_\nu k$ ist ganz. Das besagt, wie Herr Hecke besonders beifügte, manchmal mehr und manchmal weniger als die Bemerkung im Text.

[4] Vgl. hiezu R. Dedekind, Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern, Journal für Math. 121 (1900), S. 40–123 = Gesammelte mathematische Werke, Bd. II, Arbeit XXIX, S. 148–235.

[5] U. Wegner, Journal für Math. 168 (1932). [Zur Zeit steht mir allerdings nur eine kurze seinerzeit gemachte Notiz über diese Arbeit zur Verfügung.]

tretenden. Bei Körpern $K\left(\sqrt[p]{G}\right)$ „erster Art" verschafft uns nun das Wegnersche Resultat auch die Herstellung einer Basis; bei Körpern „zweiter Art" ergibt sich über die Basis zumindest eine gewisse Teilaussage (siehe Nr. **4**).

Ob sich die in Nr. **3** für $p = 3$ mit Hilfe elementarer Kongruenzen gemachten Ausführungen zur direkten Bestimmung von Basis und Körperdiskriminante auf eine beliebige ungerade Primzahl verallgemeinern lassen, mag dahingestellt bleiben. Allemal bedarf es dabei der Aufstellung der algebraischen Gleichung für die Zahlen ω des Körpers, um diese Gleichung (geschrieben mit höchstem Koeffizienten 1) auf Ganzzahligkeit ihrer Koeffizienten untersuchen zu können. Die zur Aufstellung dieser Gleichung führenden Betrachtungen lassen sich nun ausdehnen auf $K(\vartheta)$ für $\vartheta = \left(\sqrt[n]{G}\right)$ mit beliebigem n, wobei die ganze rationale Zahl $G > 1$ durch keine n-te Potenz einer ganzen Zahl > 1 teilbar und daher in der Gestalt

$$G = g_1 g_2^2 \cdots g_s^s \quad (s = n - 1) \tag{3}$$

bei quadratfreiem

$$g = g_1 g_2 \cdots g_s \tag{4}$$

darstellbar sei[6]. Die ganzen rationalen Zahlen g_λ mögen dabei für $\lambda \geqq 2$ positiv angenommen werden, während g_1 positiv oder negativ sein kann. Wird dann für $\nu = 0, 1, \ldots, s$ die Zahl

$$G^\nu = Q_\nu^n R_\nu \tag{5}$$

dargestellt[6a] als Produkt einer n-ten Potenz einer ganzen ratio-

[6] Welche von den n Wurzeln der Gleichung $x^n - G = 0$ für $\vartheta = \sqrt[n]{G}$ genommen wird, ist gleichgültig.

[6a] Die Darstellung (5) ist eindeutig bezüglich der absoluten Beträge von Q_ν und R_ν, nicht aber bezüglich ihrer Vorzeichen. Aus einer Darstellung gewinnt man eine zweite durch Multiplikation von Q_ν bzw. von Q_ν und R_ν mit -1, je nachdem n gerade oder ungerade ist. Die später gewählte Darstellung (26) (vgl. Anm. 17a) läßt sich für ein $G > 0$ (und daher $g_1 > 0$) einfach durch die Forderung $Q_\nu > 0$ kennzeichnen (allgemein durch die Forderung, daß Q_ν das Vorzeichen der $\left[\frac{\nu}{n}\right]$-ten Potenz von g_1, also von G, habe). Bei ungeradem n (insbesondere also in dem Fall $n = p$ in Nr. 4) kann man übrigens stets $G > 0$ annehmen, da dann die Körper $K\left(\sqrt[n]{-G}\right)$ und $K\left(\sqrt[n]{G}\right)$ übereinstimmen.

nalen Zahl Q_ν und einer durch keine n-te Potenz > 1 teilbaren Zahl R_ν, dann sind die Zahlen[7]

$$\alpha_\nu = \frac{1}{Q_\nu}\vartheta^\nu \tag{6}$$

ganz und es ist leicht, sowohl $D(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ als die algebraische Gleichung zu bestimmen, der eine mit rationalen Koeffizienten c_ν dargestellte Zahl $\omega = \Sigma\, c_\nu\, \alpha_\nu$ des Körpers $K(\vartheta)$ genügt (siehe Nr. **5–8**, Gleichung (35) und (47)).

2. Der in der Einleitung (Nr. **1**) erwähnte Dedekind'sche Satz läßt sich folgendermaßen aussprechen:

Satz 2. Haben ϑ, n, $\alpha_1, \ldots, \alpha_n$, $D = D(\alpha_1, \ldots, \alpha_n)$ die gleiche Bedeutung wie in Satz 1 und wird für eine gemäß (2) mit rationalen c_ν dargestellte ganze Zahl ω mit $m(\omega)$ die kleinste positive ganze rationale Zahl bezeichnet, sodaß alle Zahlen $c_\nu m(\omega)$ ganz sind und somit ω zum Modul $\left[\frac{\alpha_1}{m(\omega)}, \ldots, \frac{\alpha_n}{m(\omega)}\right]$ gehört, dann ist $D(\alpha_1, \ldots, \alpha_n)$ durch $(m(\omega))^2$ teilbar[8].

Im Rahmen einer allgemeinen Theorie der Moduln gewinnt Dedekind diesen Satz aus der Gleichung[9]

$$D(\mathfrak{a}) = (m(\omega))^2\, D(\mathfrak{b}), \tag{7}$$

wobei $\mathfrak{a}$ den Modul $[\alpha_1, \ldots, \alpha_n]$ und $\mathfrak{b}$ den von Dedekind mit $\mathfrak{a} + [\omega]$ bezeichneten „größten gemeinsamen Teiler" der Moduln $\mathfrak{a}$ und $[\omega]$, also den Modul

$$\mathfrak{b} = [\alpha_1, \ldots, \alpha_n, \omega] = [\beta_1, \ldots, \beta_n],$$

ferner $\beta_1, \ldots, \beta_n$ eine Basis von $\mathfrak{b}$ bedeutet. Für den Fall $m(\omega) > 1$, also $|D(\mathfrak{b})| < |D(\mathfrak{a})|$, wo somit $\mathfrak{a}$ nicht alle ganzen Zahlen aus $K(\vartheta)$ umfaßt und ω nicht zu $\mathfrak{a}$ gehört, ist allbekannt, wie diese Entwicklungen dazu dienen, von der Körperbasis $\mathfrak{a}$ auf die Existenz einer anderen Körperbasis $\mathfrak{b}$ mit absolut-kleinerer Diskri-

---

[7] Von Nr. **3** angefangen empfiehlt es sich, die betrachteten n unabhängigen Zahlen mit $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ anstatt mit $\alpha_1, \alpha_2, \ldots, \alpha_n$ zu bezeichnen.

[8] Vgl. Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, 4. Auflage (1894), Supplement XI, § 175, S. 538, Satz I, = R. Dedekind, Gesammelte mathematische Werke, Bd. III, Arbeit XLVI, S. 104.

[9] Vgl. l. c.[8], S. 538 (= Werke III, S. 104), Gleichung (15); l. c. steht m, Δ statt $m(\omega)$, D.

minante und derart (mit endlich vielen Schritten) auf die Existenz einer Minimalbasis (mit absolut-kleinster Diskriminante) zu schließen.

Da aber, wie aus (7) und der Definition von m gemäß (1) ersichtlich, notwendig $m(\omega)$ ein Teiler von m sein muß, so besagt Satz 2 gerade die Zugehörigkeit jeder ganzen Zahl ω aus $K(\vartheta)$ zum Modul $\left[\frac{\alpha_1}{m}, \ldots, \frac{\alpha_n}{m}\right]$. Der Dedekindsche Satz 2 deckt sich also mit Satz 1 und wird zudem von Dedekind, l. c.[8], S. 539 = Werke, Bd. III, S. 105|106, im speziellen Fall $n = 2$ zur Feststellung der in Anm. 3 angeführten Zugehörigkeit der ganzen Zahlen aus $K\left(\sqrt{G}\right)$ zum Modul $\left[\frac{1}{2}, \frac{1}{2}\sqrt{G}\right]$ herangezogen.

3. Wir wollen nun, wie gesagt, Satz 1 anwenden auf die Ermittelung einer Basis in $K(\vartheta)$ für den Fall $\vartheta = \sqrt[3]{G}$, wo G ganz rational und kubusfrei sei. Wir setzen $G = g_1 g_2^2$, wo $g_1 g_2$ quadratfrei; für[10]

$$\alpha_0 = 1, \quad \alpha_1 = \vartheta, \quad \alpha_2 = \frac{1}{g_2}\vartheta^2 = \sqrt[3]{g_1^2 g_2}$$

ist dann[11]

$$D(\alpha_0, \alpha_1, \alpha_2) = -3m^2 \text{ mit } m = 3 g_1 g_2$$

und nach Satz 1 sind für jede ganze Zahl $\omega = \Sigma c_\nu \alpha_\nu$ die Zahlen $m_\nu = m c_\nu$ ganz. Aus der Gleichung

$$m\omega = m\omega\alpha_0 = \Sigma m_\nu \alpha_\nu$$

und den daraus durch Multiplikation mit α_1 bzw. α_2 unter Beachtung von

$$\alpha_1\alpha_1 = g_2\alpha_2, \quad \alpha_1\alpha_2 = g_1 g_2 = g_1 g_2 \alpha_0, \quad \alpha_2\alpha_2 = g_1\alpha_1 \qquad (8)$$

erhaltenen Gleichungen, gewinnt man nun, wenn man diese drei Gleichungen als linear-homogen in α_0, α_1, α_2 auffaßt, durch Nullsetzen der Determinante[12]:

$$0 = (m_0 - m\omega)^3 - 3 g_1 g_2 m_1 m_2 (m_0 - m\omega) + g_1 g_2^2 m_1^3 + g_1^2 g_2 m_2^3. \qquad (9)$$

[10] Vgl. Anm. 7, Nr. 1.

[11] Vgl. die allgemeine Formel (47), Nr. 8.

[12] Vgl. in Nr. 5 die analoge allgemeine Rechnung für $\vartheta = \sqrt[n]{G}$ sowie (41), Nr. 6.

Soll ω ganz sein, also einer algebraischen Gleichung mit ganzen rationalen Koeffizienten und höchstem Koeffizienten 1 genügen, so erhält man in einfacher Weise die folgenden Kongruenzen (wobei schrittweise

$$m_0 = g_1 g_2 l_0, \quad m_1 = g_1 n_1, \quad m_2 = g_2 n_2,$$
$$n_1 = g_2 l_1, \quad n_2 = g_1 l_2$$

gesetzt wird): Zunächst

$$3\, m_0 \equiv 0 \pmod{m}, \quad 3\,(m_0^2 - g_1 g_2 m_1 m_2) \equiv 0 \pmod{m^2},$$
$$m_0^3 + g_1 g_2^2 m_1^3 + g_1^2 g_2 m_2^3 - 3\, g_1 g_2 m_0 m_1 m_2 \equiv 0 \pmod{m^3};$$

hieraus

$$m_1 m_2 \equiv 0 \pmod{g_1 g_2}, \quad g_2 m_1^3 + g_1 m_2^3 \equiv 0 \pmod{g_1^2 g_2^2},$$

somit

$$m_1^3 \equiv 0 \pmod{g_1}, \quad m_2^3 \equiv 0 \pmod{g_2},$$

also

$$g_1^2 n_1^3 + g_2^2 n_2^3 \equiv 0 \pmod{g_1 g_2},$$
$$n_1^3 \equiv 0 \pmod{g_2}, \quad n_2^3 \equiv 0 \pmod{g_1}$$

und daher

$$l_0^2 - g_1 g_2 l_1 l_2 \equiv 0 \pmod{3} \tag{10}$$

$$l_0^3 + g_1 g_2^2 l_1^3 + g_1^2 g_2 l_2^3 - 3\, g_1 g_2 l_0 l_1 l_2 \equiv 0 \pmod{3^3}, \tag{11}$$

wobei die l_ν nur mod. 3 zu betrachten sind, da die m_ν nur mod. m in Betracht kommen. Wir unterscheiden die Fälle

A) $g_1 g_2 \equiv 0 \pmod{3}$, etwa $g_1 = 3\, h_1$, $g_2 = h_2$, $h_1 h_2 \not\equiv 0 \pmod{3}$; wegen (10) ist $l_0 \equiv 0 \pmod{3}$, woraus nach (11) sich

$$h_2 l_1^3 + 3\, h_1 l_2^3 \equiv 0 \pmod{3^2},$$

also $l_1 \equiv 0 \pmod{3}$ und hierauf $l_2 \equiv 0$ ergibt: alle drei Zahlen m_0, m_1, m_2 sind also durch $m = 3 g_1 g_2$ teilbar und es bilden α_0, α_1, α_2 eine Basis.

B) $g_1 g_2 \not\equiv 0$, also $g_1^2 \equiv g_2^2 \equiv 1 \pmod{3}$, $g_2 \equiv \pm g_1 \pmod{3}$, wegen (11) somit

$$0 \equiv l_0^3 + g_1 l_1^3 + g_2 l_2^3 \equiv l_0 + g_1 (l_1 \pm l_2) \pmod{3}.$$

Also ist

$$l_0^2 \equiv (-g_1 (l_1 \pm l_2))^2 \equiv (l_1 \pm l_2)^2 \pmod{3}$$

oder $0 \equiv (l_1 \pm l_2)^2 - l_0^2$, wegen (10) somit

$$0 \equiv (l_1 \pm l_2)^2 \mp l_1 l_2 \equiv (l_1 \mp l_2)^2 \pmod 3.$$

Wir können also $l_1 = l$, $l_2 = \pm l$, $l_0 = g_1 l$ setzen. Dann ist (10) erfüllt und (11) führt auf

$$l^3 g_1 (g_2 \mp g_1)^2 \equiv 0 \pmod{3^3}.$$

Soll diese Kongruenz für ein $l \not\equiv 0 \pmod 3$ erfüllbar sein, so ist dafür $g_2 \mp g_1 \equiv 0 \pmod 9$ notwendig und hinreichend.

Somit: Wenn

$$g_1 g_2 \not\equiv 0 \pmod 3 \text{ und } g_2 \equiv \pm g_1 \pmod 9 \tag{12}$$

ist, dann sind die nicht zum Modul $[\alpha_0, \alpha_1, \alpha_2]$ gehörigen ganzen Zahlen notwendig von der Gestalt $\frac{1}{3} l(g_1 + \alpha_1 \pm \alpha_2)$ mit $l \equiv +1$ oder $-1 \pmod 3$. Demnach bilden $1, \alpha, \omega$ eine Basis, wo α eine der Zahlen α_1, α_2 und $\omega = \frac{1}{3}(k_1 + \alpha_1 \pm \alpha_2)$ ist mit $k_1 \equiv g_1 \pmod 3$. Man hat dann die Körperdiskriminante $d = \frac{1}{9} D = -3 (g_1 g_2)^2$. Beispielsweise ist für $G = 8036 = 14^2 \cdot 41$ mit $41 \equiv 14 \pmod 9$ die Zahl $\omega = \frac{1}{3}\left(-1 + (14^2 \cdot 41)^{\frac{1}{3}} + (41^2 \cdot 14)^{\frac{1}{3}}\right)$ ganz: es ist $\omega^3 + \omega^2 - 191\,\omega - 1233 = 0$.

In allen anderen Fällen B), wo also (12) nicht gilt, ist (ebenso wie im Fall A)) $1, \alpha_1, \alpha_2$ eine Basis und $d = D$.

Damit ist die von Dedekind l. c.[4] aufgestellte Fallunterscheidung gewonnen. Er spricht im Falle (12), der sich auch durch

$$g_1^2 \equiv g_2^2 \pmod 9 \tag{13}$$

charakterisieren läßt, von einem reinen kubischen Körper „zweiter Art", in allen anderen, durch das Nichtbestehen der Kongruenz (13) charakterisierten Fällen (A oder B) von einem Körper „erster Art". Wir führen noch die Körper zweiter Art mit $G < 100$ an. Sie ergeben sich mit dem oberen bzw. unteren Vorzeichen $(\pm)$ in (12) für $G = 10, 19, 37, 44, 46, 55, 73, 82, 91$ bzw. $G = 26, 28, 35, 53, 62, 71, 89$ (dabei erscheint $G = g_1^2 g_2 = 98$ schon bei $g_1 g_2^2 = 28$).

4. Unter Heranziehung eines von U. Wegner, l. c.[5] gewonnenen Resultates läßt sich die soeben für $p = 3$ an Hand elemen-

tarer Kongruenzen gefundene Fallunterscheidung in Körper erster und zweiter Art übertragen auf reine Körper $K\left(\sqrt[p]{G}\right)$, deren Grad p irgend eine ungerade Primzahl ist, wobei sich für die Körper erster Art die vollständige Aufstellung einer Basis ergibt. Wir setzen

$$p-1=s, \qquad \tfrac{1}{2}(p-1)=v$$
$$G=g_1 g_2^2 \dots g_s^s, \text{ wo } g_1 g_2 \dots g_s \text{ quadratfrei,}$$
$$\lambda\nu = p q_{\lambda\nu} + r_{\lambda\nu} \text{ mit } 0 \leqq r_{\lambda\nu} < p$$
$$(\lambda = 1, \dots, s;\ \nu = 0, 1, \dots, s)$$

und erhalten in den Zahlen[13]

$$\alpha_\nu = \frac{\vartheta^\nu}{g_1^{q_1\nu} \dots g_s^{q_s\nu}} = \sqrt[p]{g_1^{r_1\nu} \dots g_s^{r_s\nu}} \text{ für } \nu = 0, 1 \dots, s \qquad (14)$$

ein System unabhängiger ganzer Zahlen des durch $\vartheta = \sqrt[p]{G}$ definierten Körpers $K(\vartheta)$. Ist λ eine festgewählte unter den Zahlen $1, \dots, s$, dann durchlaufen die Zahlen $r_{\lambda\nu}$ $(\nu = 0, 1, \dots, s)$ ein volles Restsystem mod. p, woraus

$$\sum_{\nu=0}^{s} r_{\lambda\nu} = \sum_{\nu=0}^{s} \nu = \frac{ps}{2} \qquad (15)$$

und wegen (14)

$$(\alpha_0 \alpha_1 \dots \alpha_s)^2 = (g_1 \dots g_s)^s \qquad (16)$$

folgt. Die zu ϑ bzw. α_ν konjugierten Größen $\vartheta^{(\mu)}$ bzw. $\alpha_\nu^{(\mu)}$ $(\mu = 0, 1, \dots, s)$ ergeben sich vermöge

$$\vartheta^{(\mu)} = \varepsilon^\mu \vartheta, \quad \alpha_\nu^{(\mu)} = \varepsilon^{\mu\nu} \alpha_\nu$$

mittels irgend einer primitiven p-ten Einheitswurzel ε. Somit ist die Determinante

$$\Delta = \Delta(\alpha_0, \dots, \alpha_s) = |\alpha_\nu^{(\mu)}| = \Delta_p \alpha_0 \dots \alpha_s$$

und die Diskriminante

$$D = D(\alpha_0, \dots, \alpha_s) = \Delta^2 = D_p (\alpha_0 \dots \alpha_s)^2 = \\ = (-1)^v p^p (g_1 \dots g_s)^s = m^2 w, \qquad (17)$$

wenn

$$\Delta_p = \Delta(1, \varepsilon, \dots, \varepsilon^s) = |\varepsilon^{\mu\nu}|_{\mu,\nu=0,1,\dots,s},$$

[13] Über die Exponenten $r_{\lambda\nu}$ in (14) vgl. auch Anm. 18.

ferner $D_p = \Delta_p^2 = (-1)^v p^p$ die Diskriminante der Gleichung $x^p - 1 = 0$ ist[14] und

$$m = (p\, g_1 \ldots g_s)^v, \qquad w = (-1)^v p \tag{18}$$

gesetzt wird. Wir bezeichnen mit d die Körperdiskriminante von $K\left(\sqrt[p]{G}\right)$. Je nachdem nun

$$G^s \not\equiv 1 \text{ oder } \equiv 1 \pmod{p^2} \tag{19}$$

ist, ist nach U. Wegner[15] d oder $p^2 d$ gleich

$$(-1)^v p^p (g_1 \ldots g_s)^s = D(\alpha_0, \ldots, \alpha_s).$$

Spricht man im einen oder im anderen Fall wieder von einem Körper erster oder zweiter Art, so ist bei einem Körper erster Art wegen $d = D(\alpha_0, \ldots, \alpha_s)$ notwendig $\alpha_0, \ldots, \alpha_s$ eine Basis.

Dagegen muß es bei einem Körper zweiter Art wegen $|D(\alpha_0, \ldots, \alpha_s)| > |d|$ notwendig ganze Zahlen ω geben, die nicht zum Modul $[\alpha_0, \ldots, \alpha_s]$ gehören und es muß dann für eine solche Zahl ω gemäß (7) offenbar $m(\omega) = p$, die Zahl ω also von der Gestalt

$$\omega = \frac{1}{p} \sum_{\nu=0}^{s} m_\nu \alpha_\nu$$

mit ganzen rationalen Koeffizienten m_ν sein, von denen wenigstens einer, etwa m_μ, nicht durch p teilbar ist. In einem Körper zweiter Art bilden dann $\alpha_0, \ldots, \alpha_{\mu-1}, \omega, \alpha_{\mu+1}, \ldots, \alpha_s$ eine Basis.

Man kann der Kennzeichnung der Körper erster und zweiter Art durch (19) noch eine andere Gestalt geben, wenn man beachtet, daß $\varphi(p^2) = ps$ und daher für eine zu p teilerfremde ganze rationale Zahl x nach dem Fermatschen Satz $x^{ps} \equiv 1 \pmod{p^2}$

[14] Wird nämlich $x^p - 1 = f(x)$ gesetzt, so hat man $D_p = (-1)^{pv} \prod_\mu f'(\varepsilon^\mu) = (-1)^v p^p \prod \varepsilon^\mu$ nebst $\prod \varepsilon^\mu = 1$. Vgl. die ähnlich verlaufende Bestimmung von D in Nr. 8.

[15] Vgl. l. c.[5], wo übrigens das Vorzeichen $(-1)^v$ von d nicht weiter betrachtet und nur $|d|$ bestimmt wird.

ist. Ersetzt man demgemäß auf der rechten Seite von (19) die Zahl 1 durch die mit

$$x = g_{v+1} \cdots g_s \tag{20}$$

gebildete Zahl x^{p^s}, so wird klar, daß sich die Fallunterscheidung (19) in die Gestalt

$$(g_1 g_2^2 \cdots g_v^v)^s \not\equiv \text{ oder } \equiv (g_s g_{s-1}^2 \cdots g_{v+1}^v)^s \pmod{p^2} \tag{21}$$

bringen läßt. Dabei wurde zunächst die Zahl (20) zu p teilerfremd vorausgesetzt; die Gleichwertigkeit von (19) mit (21) gilt aber offenbar auch, wenn eine der Zahlen $g_{v+1}, \ldots, g_s$ durch p teilbar, und dann notwendig alle anderen unter den Zahlen $g_1, \ldots, g_s$ speziell also $g_1, \ldots, g_v$ zu p teilerfremd sind (wobei natürlich ein Körper erster Art vorliegt).

Für $p = 3$ geht (21) über in die Dedekindsche, auf das Bestehen oder Nichtbestehen der Kongruenz (13) gegründete Unterscheidung.

5. Ist für eine beliebige natürliche Zahl n die Zahl G gemäß (3), Nr. **1**, gegeben, $\vartheta = \sqrt[n]{G}$ und $\alpha_0 = 1, \alpha_1, \ldots, \alpha_s$ gemäß (6) bestimmt, dann ist es nicht schwer, die algebraische Gleichung für irgend eine Zahl

$$\omega = \sum_{\nu=0}^{s} c_\nu \alpha_\nu \tag{22}$$

des Körpers $K(\vartheta)$ aufzustellen. Es kommt dabei nur darauf an, – so, wie es für $n = 3$ die Gleichungen (8) leisten, – die Produkte $\alpha_\mu \alpha_\nu$ linear durch die α_ν auszudrücken. Man erhält dann[16] durch Multiplikation von (22) mit $\alpha_0, \alpha_1, \ldots, \alpha_s$ ein System linear-homogener Gleichungen in den α_ν; und Nullsetzen der Determinante liefert die gewünschte Gleichung für ω (siehe unten (35)).

Zunächst haben wir uns etwas näher mit den in Nr. **1** eingeführten Zahlen Q_ν, R_ν zu befassen, deren Definition gemäß (5) – ebenso wie die Definition der α_ν gemäß (6) – wir auf beliebige ganze ν ausdehnen. Setzen wir

$$\lambda\nu = n q_{\lambda\nu} + r_{\lambda\nu} \text{ mit } 0 \leq r_{\lambda\nu} < n, \tag{23}$$

[16] Vgl. Dedekind, l. c.[8], Suppl. XI, § 164, S. 470 = Werke III, S. 37.

sodaß[17]

$$q_{\lambda\nu} = \left[\frac{\lambda\nu}{n}\right] \tag{24}$$

wird, so folgt aus

$$G = \prod_{\lambda=1}^{s} g_\lambda^\lambda \tag{25}$$

gemäß (5) unmittelbar[17a]

$$Q_\nu = \prod_\lambda g_\lambda^{q_{\lambda\nu}}, \qquad R_\nu = \prod_\lambda g_\lambda^{r_{\lambda\nu}} \tag{26}$$

und

$$Q_{\nu+n} = G \cdot Q_\nu, \qquad R_{\nu+n} = R_\nu \tag{27}$$

sowie unter Beachtung von $\vartheta^{\nu+n} = G\,\vartheta^\nu$ gemäß (6)

$$\alpha_{\nu+n} = \alpha_\nu. \tag{28}$$

Zwecks späterer Verwendung vermerken wir noch die Formeln

$$\rho_\lambda = \sum_{\nu=0}^{n-1}{}' r_{\lambda\nu} = \frac{1}{2}\, n\,(n - t_\lambda), \tag{29}$$

$$\sigma_\lambda = \sum_{\nu=0}^{n-1}{}' q_{\lambda\nu} = \frac{1}{2}\,(n\lambda - n - \lambda + t_\lambda), \tag{30}$$

wobei

$$t_\lambda = (n, \lambda) \tag{31}$$

den größten gemeinsamen Teiler von n und λ bedeutet; wird nämlich $n = t_\lambda n^*$, $\lambda = t_\lambda \lambda^*$, $r_{\lambda\nu} = t_\lambda r^*_{\lambda\nu}$ gesetzt, so durchlaufen[18] für $\nu = 0, 1, \ldots, n-1$ die Zahlen $r^*_{\lambda\nu}$ insgesamt t_λ-mal ein volles Restsystem $0, 1, \ldots, n^* - 1$ modulo n^*, was

---

[17] Unter $[\xi]$ werde die größte ganze Zahl $\leqq \xi$ verstanden.

[17a] Daß neben der Bestimmung von Q_ν, R_ν gemäß (26), die durch ihre Einfachheit nahegelegt wird, noch eine zweite (in den Vorzeichen abweichende) möglich ist, wurde bereits in Anm. 6a erwähnt.

[18] Ist speziell $n = p$ prim, $1 \leqq \lambda \leqq p - 1$, somit $t_\lambda = 1$, so deckt sich (29) mit (15). Natürlich gilt analog: Wenn wir ν festhalten, u. zw. als eine zu n teilerfremde Zahl, so durchlaufen zugleich mit λ auch die Zahlen $r_{\lambda\nu}$ (das sind die im Ausdruck (26) für $R_\nu = \alpha_\nu^n$ auftretenden Exponenten) das System der Zahlen $1, 2, \ldots, n-1$. Im besonderen treten also, wenn $n = p$ prim und ν eine der Zahlen $1, \ldots, p-1$ ist, in $\alpha_\nu = \sqrt[p]{R_\nu}$ unter der Wurzel als Exponenten der Zahlen g_λ alle Zahlen $1, \ldots, p-1$ auf.

$$\rho_\lambda = t_\lambda \sum_{\mu=0}^{n^*-1} t_\lambda \mu = \frac{1}{2} t_\lambda^2 n^* (n^* - 1)$$

und somit (29) ergibt, woraus dann (30) vermöge

$$n\sigma_\lambda + \rho_\lambda = \sum_{\nu=0}^{n-1} (n q_{\lambda\nu} + r_{\lambda\nu}) = \sum_{\nu=0}^{n-1} \lambda\nu = \frac{1}{2} \lambda n(n-1)$$

gewonnen wird.

Weiters folgt aus (6) für beliebige ganzzahlige μ, ν

$$\vartheta^{\mu+\nu} = Q_{\mu+\nu}\alpha_{\mu+\nu} = Q_\mu Q_\nu \alpha_\mu \alpha_\nu.$$

Wenn wir also

$$G_{\mu,\nu} = \frac{Q_{\mu+\nu}}{Q_\mu Q_\nu} \tag{32}$$

setzen, wobei wegen (27) $G_{\mu+n,\nu} = G_{\mu,\nu}$ ist, die Indizes von $G_{\mu,\nu} = G_{\nu,\mu}$ also nur modulo n von Bedeutung sind, so ergibt sich

$$\alpha_\mu \alpha_\nu = G_{\mu,\nu} \alpha_{\mu+\nu} \tag{33}$$

und damit die gewünschte Darstellung der Produkte $\alpha_\mu\alpha_\nu$ linear durch die α_ν. Ehe wir nun die Gleichung (22) der Reihe nach mit $\alpha_0, \alpha_1, \ldots, \alpha_s$ multiplizieren, denken wir uns auch die Definition der c_ν gemäß der Festsetzung $c_{\nu+n} = c_\nu$ auf beliebige Indizes ν ausgedehnt, sodaß wir (22) in der Gestalt

$$0 = \sum_{(\nu)} (c_\nu - \delta_{\nu,0}\omega)\alpha_\nu \tag{34}$$

schreiben können, wenn wir unter $\sum_{(\nu)}$ eine Summe verstehen, bei der ν ein volles Restsystem mod. n durchläuft, das bekannte Zeichen $\delta_{\mu,\nu}$ aber in dem allgemeineren Sinne zu verstehen ist, daß $\delta_{\mu,\nu} = 1$ oder 0 ist, je nachdem $\mu \equiv \nu$ oder $\mu \not\equiv \nu$ (mod. n) ist. Multiplikation von (34) mit α_μ ($\mu = 0, 1, \ldots,$) liefert nun gemäß (33) das in den α_ν lineare Gleichungssystem

$$0 = \sum_{(\nu)} (c_\nu - \delta_{\nu,0}\omega) G_{\mu,\nu}\alpha_{\mu+\nu} =$$

$$= \sum_{(\nu)} (c_{\nu-\mu} - \delta_{\nu-\mu,0}\omega) G_{\mu,\nu-\mu}\alpha_\nu$$

$$(\mu = 0, 1, \ldots, s)$$

mit den Koeffizienten

$$a_{\mu\nu} = (c_{\nu-\mu} - \delta_{\nu-\mu,\,0}\,\omega)\,G_{\mu,\,\nu-\mu}.$$

Durch Nullsetzen der Determinante bekommt man die gesuchte Gleichung n-ten Grades für ω:

$$0 = |\,(c_{\nu-\mu} - \delta_{\nu-\mu,\,0}\,\omega)\,G_{\mu,\,\nu-\mu}\,|, \tag{35}$$

wobei die μ-te Zeile ausführlich durch

$$c_{n-\mu}\,G_{\mu,\,n-\mu},\ \ldots,\ c_{n-1}\,G_{\mu,\,n-1},\ c_0 - \omega,\ c_1\,G_{\mu,\,1},\ \ldots$$
$$\ldots,\ c_{n-\mu-1}\,G_{\mu,\,n-\mu-1}$$

gegeben ist[19]. Dabei tritt ω offenbar nur in der Hauptdiagonale auf, deren sämtliche Glieder $a_{\mu\mu} = c_0 - \omega$ sind, da

$$G_{\mu,\,0} = G_{0,\,\mu} = 1 \tag{36}$$

ist, wie aus (32) wegen $Q_0 = 1$ folgt.

6. Die weiteren Aussagen, die wir über die Glieder der Determinante (35) noch erwähnen wollen, stützen sich auf die folgenden Aussagen über die Funktion $[\xi]$ (vgl. Anm. 17):

(a) Für beliebige reelle Zahlen $\xi_1, \ldots, \xi_m$ genügt

$$X = [\xi_1 + \ldots + \xi_m] - [\xi_1] - \ldots - [\xi_m]$$

der Ungleichung

$$0 \leqq X < m$$

und X hat als ganze Zahl somit einen der Werte $0, 1, \ldots, m-1$.

(b) Es hat

$$Y = [\xi] + [-\xi]$$

den Wert 0 oder -1, je nachdem die reelle Zahl ξ ganz oder nicht ganz ist.

Man sieht nämlich sofort, daß X bzw. Y sich nicht ändern, wenn ein ξ_μ bzw. ξ um eine ganze Zahl geändert wird, sodaß man die Richtigkeit von (a) und (b) nur für $0 \leqq \xi_\mu < 1$ bzw. $0 \leqq \xi < 1$ festzustellen braucht.

---

[19] Für $\mu = 0$ bzw. $\mu = n-1$ entfallen in der betreffenden Zeile natürlich die Glieder vor bzw. nach $c_0 - \omega$.

Wird nun

$$G_{\mu,\nu} = \prod_{\lambda} g_{\lambda}^{\gamma_{\lambda,\mu,\nu}} \tag{37}$$

gesetzt, so gewinnt man aus (32), (26) und (24)

$$\gamma_{\lambda,\mu,\nu} = \left[\frac{\lambda(\mu+\nu)}{n}\right] - \left[\frac{\lambda\mu}{n}\right] - \left[\frac{\lambda\nu}{n}\right],$$

und die Aussage (a) für $m = 2$ zeigt, daß in (37) jeder Exponent $\gamma_{\lambda,\mu,\nu}$ nur einen der Werte 0 oder 1 hat.

Man bestätigt dies z. B. bei $n = 4$ an den Formeln (wegen $G_{0,\mu}$ vgl. (36)):

$$\begin{aligned} G_{1,1} &= g_2 g_3, \quad G_{1,2} = g_3, \quad G_{1,3} = g_1 g_2 g_3, \\ G_{2,2} &= g_1 g_3, \quad G_{2,3} = g_1, \quad G_{3,3} = g_1 g_2, \end{aligned} \tag{38}$$

die man übrigens am einfachsten aus

$$\begin{aligned} Q_0 = Q_1 = 1, \quad Q_2 = g_2 g_3, \quad Q_3 = g_2 g_3^2, \quad Q_4 = Q_5 = g_1 g_2^2 g_3^3, \\ Q_6 = g_1 g_2^3 g_3^4 \end{aligned} \tag{39}$$

vermöge (32) gewinnt[20]. Die Gleichung (35) für ω wird hier

$$0 = \begin{vmatrix} c_0 - \omega, & c_1, & c_2, & c_3 \\ c_3 g_1 g_2 g_3, & c_0 - \omega, & c_1 g_2 g_3, & c_2 g_3 \\ c_2 g_1 g_3, & c_3 g_1, & c_0 - \omega, & c_1 g_3 \\ c_1 g_1 g_2 g_3, & c_2 g_1, & c_3 g_1 g_2, & c_0 - \omega \end{vmatrix}. \tag{40}$$

Multipliziert man in dieser Determinante zwei symmetrisch zur Hauptdiagonale liegende Glieder $a_{\mu\nu}$ und $a_{\nu\mu}$ und läßt darin den Faktor $c_{\mu-\nu} c_{n-\mu+\nu}$ weg, so erhält man allemal $g_1 g_2 g_3$ außer bei $a_{02} a_{20}$ und $a_{13} a_{31}$, wo sich $g_1 g_3$ ergibt. Wir kommen auf diese Bemerkung in Nr. **7** zurück.

Analog erhält man für $n = 3$, wo $Q_0 = Q_1 = 1$, $Q_2 = g_2$, $Q_3 = Q_4 = g_1 g_2^2$ ist, die Gleichung

---

[20] Um die Exponenten von g_1, g_2, g_3 in Q_ν zu erhalten, braucht man gemäß (24) nur festzustellen, wie oft $n = 4$ in den betreffenden Exponenten in G^ν, d. h. in jeder der Zahlen ν, 2ν, 3ν aufgeht. Bei häufigeren derartigen Rechnungen wird man sich praktisch das Anschreiben der $g_1, \ldots, g_3$ sparen und Tabellen für die Exponentensysteme anlegen oder etwa abgekürzt z. B. $G = (1, 2, 3)$, $G^2 = (2, 4, 6)$ $R_2 = (2, 0, 2)$, $Q_2 = (0, 1, 1)$, $Q_3 = (0, 1, 2)$, $Q_5 = (1, 2, 3)$, $G_{2,3} = (1, 0, 0)$ schreiben.

$$0 = \begin{vmatrix} c_0 - \omega, & c_1, & c_2 \\ c_2 G_{1,2}, & c_0 - \omega, & c_1 G_{1,1} \\ c_1 G_{2,1}, & c_2 G_{2,2}, & c_0 - \omega \end{vmatrix} = \begin{vmatrix} c_0 - \omega, & c_1, & c_2 \\ c_2 g_1 g_2, & c_0 - \omega, & c_1 g_2 \\ c_1 g_1 g_2, & c_2 g_1, & c_0 - \omega \end{vmatrix}, \quad (41)$$

die wir in etwas anderer Gestalt schon in (9) vor uns hatten.

7. Wir betrachten nun noch in (35) zwei zur Hauptdiagonale symmetrisch liegende Glieder

$$a_{\mu\nu} = c_{\nu-\mu} G_{\mu,\nu-\mu} \text{ und } a_{\nu\mu} = c_{\mu-\nu} G_{\nu,\mu-\nu},$$

wobei etwa im Falle

$$\mu - \nu = \varkappa > 0$$

unter $c_{\nu-\mu} = c_{-\varkappa}$ soviel wie $c_{n-\varkappa}$ zu verstehen ist (s. o.); gemäß (32) ist dann

$$G_{\mu,\nu-\mu} \cdot G_{\nu,\mu-\nu} = \frac{1}{Q_\varkappa Q_{-\varkappa}} = \prod_\lambda g_\lambda^{\beta_{\lambda,\varkappa}}, \quad (42)$$

wenn wir

$$-\beta_{\lambda,\varkappa} = q_{\lambda\varkappa} + q_{\lambda(-\varkappa)} = \left[\frac{\lambda\varkappa}{n}\right] + \left[-\frac{\lambda\varkappa}{n}\right]$$

setzen. Die Aussage (b) lehrt dann, daß in (42) der Exponent $\beta_{\lambda,\varkappa} = 0$ ist nur in dem Falle, daß $\lambda\varkappa = \lambda(\mu - \nu)$ durch n teilbar, d. h. daß

$$\mu \equiv \nu \left(\text{mod. } \frac{n}{t_\lambda}\right) \quad (43)$$

ist (wegen $t_\lambda = (n, \lambda)$ siehe (31), Nr. **5**); in allen anderen Fällen ist $\beta_{\lambda,\varkappa} = 1$ und somit, wenn (43) für kein λ gilt,

$$G_{\mu,\nu-\mu} \cdot G_{\nu,\mu-\nu} = \prod_\lambda g_\lambda = g. \quad (44)$$

Im obigen Beispiel $n = 4$ (in Nr. **6**), wo $\lambda = 1, 2, 3$ ist, ferner μ und ν die Werte 0, 1, 2, 3 durchlaufen, kann für $\mu \neq \nu$ offenbar (43) nur bestehen, wenn $\frac{n}{t_\lambda} < 4$ und dann notwendig $\lambda = 2$ und ($\mu > \nu$ angenommen) $\mu = 2$, $\nu = 0$ oder $\mu = 3$, $\nu = 1$ ist. Tatsächlich hat[21] g_2 sowohl in $G_{2,2} \cdot G_{0,2} = g_1 g_3$, als in

[21] Vgl. auch (38) und (40) in Nr. **6**.

$G_{3,2} \cdot G_{1,2} = g_1 g_3$ den Exponenten $\beta_{\lambda,\varkappa} = \beta_{2,2} = 0$, während für alle anderen Wertepaare μ, ν sich (44) ergibt.

Im besonderen Fall, daß $n = p$ eine Primzahl ist und somit für jeden Wert $\lambda = 1, \ldots, p-1$ sich $t_\lambda = (p, \lambda) = 1$ ergibt, ist für kein Paar von Indizes $\mu \neq \nu$ (beide $< p$) die Kongruenz (43) erfüllt und es gilt daher ausnahmslos (44). Somit: Zwei symmetrisch zur Hauptdiagonale liegende Glieder der Gleichung (35) liefern nach Weglassung der Faktoren $c_{\mu-\nu}$, $c_{n+\nu-\mu}$ als Produkt (im Falle $n = p$) stets $g = g_1 g_2 \cdots g_{p-1}$, wie man dies auch im Beispiel (41) bestätigt sieht.

8. Aus den gemäß (26) bestimmten Zahlen Q_ν gewinnt man auch die Diskriminante $D = D(\alpha_0, \alpha_1, \ldots, \alpha_n)$. Denn wegen (6) ist

$$\begin{aligned} \Delta(\vartheta) &= \Delta(1, \vartheta, \ldots, \vartheta^{n-1}) = \\ &= Q_0 Q_1 \cdots Q_{n-1} \Delta(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}), \end{aligned} \tag{45}$$

wobei gemäß (26) und (30)

$$Q_0 Q_1 \cdots Q_{n-1} = \prod g_\lambda^{\sigma_\lambda}$$

ist. Wegen[22]

$$D(\vartheta) = (\Delta(\vartheta))^2 = (-1)^{\frac{(n-1)(n-2)}{2}} n^n G^{n-1} \tag{46}$$

ist daher

$$D = (\Delta(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}))^2 = (-1)^{\frac{(n-1)(n-2)}{2}} n^n \prod_\lambda g_\lambda^{\tau_\lambda}, \tag{47}$$

wobei die Exponenten τ_λ gemäß (25), (30) und (31) durch

$$\tau_\lambda = \lambda(n-1) - 2\sigma_\lambda = n - t_\lambda = n - (n, \lambda) \tag{48}$$

gegeben sind[23]. Es ist leicht, aus (47) die Zerlegung von D gemäß (1) in die Gestalt $m^2 w$ zu gewinnen, wobei man bei n sowie bei λ zwischen geraden und ungeraden Werten unterscheiden wird.

---

[22] Wenn $F(x) = x^n - G = 0$ die Gleichung für ϑ ist und $\vartheta^{(\mu)}$ für $\mu = 0, 1, \ldots, n-1$ die n konjugierten Wurzeln sind, dann ist ja

$$(-1)^{\frac{n(n-1)}{2}} (\Delta(\vartheta))^2 = \prod_\mu f'(\vartheta^{(\mu)}) = n^n \left(\prod_\mu \vartheta^{(\mu)}\right)^{n-1}$$

und $\prod \vartheta^{(\mu)} = (-1)^{n-1} G$, woraus sich (46) ergibt. Vgl. Nr. 4, wo für $n = p$ ähnlich verfahren wurde.

[23] Ist n eine ungerade Primzahl p, so wird $(p, \lambda) = 1$ und (47) deckt sich mit (17).