Studien aus der Zahlentheorie.

Von J. **Frischauf.**

I. Theorie der Kreistheilung [1]).

Zu den schönsten Anwendungen der Zahlentheorie auf Gegenstände der Analysis und Geometrie gehört unstreitig die von Gauß gegründete Theorie der Kreistheilung, d. i. die Theorie der Gleichung

$$x^n-1=0. \tag{1}$$

Unter der großen Anzahl von Sätzen, welche sich aus dieser Theorie folgern lassen, dürften die geometrischen Sätze über die in einen Kreis construirbaren regulären Polygone wohl zu den interessantesten gehören. Bei der Schwierigkeit, mit welcher das Studium der hierher gehörigen Untersuchungen für den Anfänger verbunden ist, dürfte nachstehende das Wichtigste dieser Theorie umfassende Darstellung von Interesse sein; der Vollständigkeit halber dürfte auch die Aufführung mancher bei Gauß gegebener Sätze und Beweise zu entschuldigen sein.

Bei der Untersuchung der vorliegenden Gleichung (1) beschränken wir uns auf den Fall, wo n eine (ungerade) Primzahl ist. Eine Wurzel dieser Gleichung $x=1$ ist reell, die übrigen $n-1$, deren Complex mit Ω bezeichnet werden soll, sind imaginär.

Dividirt man die Gleichung (1) durch $x-1$, so erhält man

$$X=x^{n-1}+x^{n-2}+\ldots\quad+x^2+x+1=0. \tag{2}$$

Alle Wurzeln dieser Gleichung sind in dem Ausdrucke

$$r=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$$

[1]) Gauß. Disquisitiones arithm. sectio septima. — Abel. Mémoire sur une classe particulière d'équations résolubles algebraiquement. — Crelle, Journal, Bd. IV.

enthalten, wo $k=1, 2, 3, \ldots n-1$ ist. Da aus $r^n=1$ auch

$$r^n = r^{2n} = r^{3n} = \ldots \quad = r^{en} = 1$$

folgt, so können die Wurzeln Ω auch in der Form

$$r, r^2, r^3, \ldots r^{n-1}$$

gedacht werden, oder in der Form

$$r^\lambda, r^{2\lambda}, r^{3\lambda} \ldots r^{(n-1)\lambda},$$

wenn λ durch n nicht theilbar ist; es ist daher

$$X = (x-r^\lambda)(x-r^{2\lambda})\ldots(x-r^{(n-1)\lambda}).$$

Ist g eine primitive Wurzel der Primzahl n, so sind die Potenzen

$$g^0, g^1, g^2, \ldots g^{n-2}$$

mit den Zahlen $1, 2, 3 \ldots n-1$ (ohne Rücksicht auf die Ordnung) nach dem Modulus n congruent, es sind daher die Wurzeln von Ω auch in der Form

$$r^\lambda, r^{g\lambda}, r^{g^2\lambda}, \ldots r^{g^{n-2}\lambda}$$

enthalten. Um nicht in eine zu complicirte Schreibweise zu gerathen, so soll nach Gauß (disquis. arithm. art. 342) $r, r^2 \ldots r^\lambda$ durch $[1], [2] \ldots [\lambda]$ bezeichnet werden. Dabei ist offenbar

$$[\lambda][\mu] = [\lambda+\mu].$$

Die Wurzeln von Ω sind daher

$$[\lambda], [\lambda g], [\lambda g^2], \ldots [\lambda g^{n-2}].$$

Ist $n-1=ef$, ferner G eine andere primitive Wurzel von n, setzt man $g^e=h$, $G^e=H$; so ist der Complex

$$[1], [h], h^2], \ldots [h^{f-1}]$$

identisch mit dem Complexe

$$[1], [H], [H^2], \ldots [H^{f-1}].$$

Denn ist $G \equiv g^\omega \pmod{n}$, $\mu < f$, so ist $G^\mu \equiv g^{\omega\mu} \pmod{n}$; ist ferner $\nu \equiv \omega\mu \pmod{f}$, wo $\nu < f$ genommen wird, so ist

$$e\nu \equiv e\omega\mu (\text{mod. } ef = n-1),$$

also

$$G^{\mu e} \equiv g^{\omega\mu e} \equiv g^{\nu e} (\text{mod. } n) \text{ oder } H^{\mu} \equiv h^{\nu}, \text{ mithin } [H^{\mu}] = [h^{\nu}],$$

d. h. je ein Glied des ersten Complexes mit irgend einem Gliede des zweiten identisch.

Dieser Complex von f-Wurzeln, welcher von dem speciellen Werthe der primitiven Wurzel unabhängig ist, soll mit $(f, 1)$ bezeichnet werden, dasselbe gilt auch von dem Complexe

$$[\lambda], [\lambda h], [\lambda h^2], \ldots [\lambda h^{f-1}],$$

welcher mit (f, λ), Periode f, λ genannt, bezeichnet werden soll.

Da $h^f \equiv 1 (\text{mod. } n)$, so ist $[\lambda h^f] = [\lambda]$, $[\lambda h^{f+1}] = [\lambda h], \ldots$ d. h. (f, λ) ist mit $(f, \lambda h)$, $(f, \lambda h^2) \ldots$ identisch; oder haben zwei Perioden aus gleich viel Gliedern f eine Wurzel gemeinsam, so sind sie identisch.

Die Wurzeln Ω sind identisch mit den Gliedern der Periode $(n-1, 1)$, diese sind:

$$\begin{array}{l} [1], [g], [g^2], \ldots [g^{e-1}] \\ [g^e], [g^{e+1}], [g^{e+2}], \ldots [g^{2e-1}] \\ [g^{2e}], g^{2e+1}], [g^{2e+2}], \ldots [g^{3e-1}] \\ \\ [g^{(f-1)e}], [g^{(f-1)e+1}], [g^{(f-1)e+2}], \ldots [g^{fe-1}]; \end{array}$$

ordnet man vertical, so gibt die 1te Reihe $(f, 1)$, die 2te Reihe (f, g), die 3te Reihe $(f, g^2) \ldots$ die $e$te Reihe (f, g^{e-1}). Die Periode $(n-1, 1)$ kann daher aus den e-Perioden $(f, 1)$, (f, g), $(f, g^2), \ldots (f, g^{e-1})$ zusammengesetzt gedacht werden.

Ebenso ist $(n-1, \lambda)$ aus (f, λ), $(f, \lambda g)$, $(f, \lambda g^2), \ldots (f, \lambda g^{e-1})$ zusammengesetzt.

Ist $n-1 = abc$, so setze man $a = e$, $bc = f$, und man erhält a-Perioden

$$(bc, 1), (bc, g), (bc, g^2) \ldots (bc, g^{a-1}).$$

Jede dieser Perioden hat die Form (bc, λ), auf ganz analoge Art erhält man dafür die c-Perioden

$$(b, \lambda), (b, \lambda g^a), \ldots (b, \lambda g^{ac-a}).$$

Im Folgenden soll unter Periode in der Regel der numerische Werth der Summe der Glieder verstanden werden.

Lehrsatz. Ist $n-1=ef$, sind ferner (f,λ_1), (f,λ_2), . . (f,λ_e) die e-Perioden, in welche man nach dem Vorigen die Periode $(n-1,\lambda)$ zerfällen kann; so lassen sich:

1. diese Perioden durch eine Gleichung des e^{ten} Grades bestimmen.

Beweis. Setzt man

$$R_\nu=(f,\lambda_1)^\nu+(f,\lambda_2)^\nu+\ldots+(f,\lambda_e)^\nu,$$

so folgt aus

$$(f,\lambda)=(f,\lambda h)=(f,\lambda h^2)=\ldots=(f,\lambda h^{f-1})$$

$$(f,\lambda)^\nu=\frac{1}{f}\left\{(f,\lambda)^\nu+(f,\lambda h)^\nu+(f,\lambda h^2)^\nu+\ldots+(f,\lambda h^{f-1})^\nu\right\}$$

$$R_\nu=\frac{1}{f}\left\{\begin{array}{l}(f,\lambda_1)^\nu+(f,\lambda_1 h)^\nu+\ldots+(f,\lambda_1 h^{f-1})^\nu\\ +(f,\lambda_2)^\nu+(f,\lambda_2 h)^\nu+\ldots+(f,\lambda_2 h^{f-1})^\nu\\ +\ldots\\ +\ldots\\ +(f,\lambda_e)^\nu+(f,\lambda_e h)^\nu+\ldots+(f,\lambda_e h^{f-1})^\nu\end{array}\right\}$$

Es ist daher R_ν eine ganze symmetrische Function der sämmtlichen Wurzeln der Gleichung $X=0$, also bekannt. Setzt man successive $\nu=1, 2, 3, \ldots e$, so lassen sich aus R_1, R_2, R_3, . . R_e die Coëfficienten der Gleichung mit (f,λ_1), (f,λ_2), . . (f,λ_e) als Wurzeln bestimmen.

2. Die f-Wurzeln einer Periode (f,λ) werden durch Auflösung einer Gleichung vom Grade f erhalten.

Beweis. Denn ist z. B. (f,λ_1) eine solche Periode, ferner

$$x^f+A_1'x^{f-1}+A_1''x^{f-2}+\ldots+A_1^{(f-1)}x+A^{(f)}=0$$

die Gleichung mit den f-Wurzeln der Periode (f,λ_1), so setze man, wenn $\psi(\lambda_1)$ irgend einen der Coëfficienten A_1', A_1'' . . $A_1^{(f)}$ bedeutet:

$$t_\nu=(f,\lambda_1)^\nu\,\psi(\lambda_1)+(f,\lambda_2)^\nu\,\psi(\lambda_2)+\ldots+(f,\lambda_e)^\nu\,\psi(\lambda_e).$$

Wegen

$$(f, \lambda_1)^\nu \psi(\lambda_1) = (f, \lambda_1 h)^\nu \psi(\lambda_1 h) = \ldots = (f, \lambda_1 h^{f-1})^\nu \psi(\lambda_1 h^{f-1})$$

u. u. w. folgt

$$t_\nu = \frac{1}{f} \left\{ \begin{array}{l} (f,\lambda_1)^\nu \psi(\lambda_1) + (f,\lambda_1 h)^\nu \psi(\lambda_1 h) + \ldots + (f,\lambda_1 h^{f-1})^\nu \psi(\lambda_1 h^{f-1}) \\ + (f,\lambda_2)^\nu \psi(\lambda_2) + (f,\lambda_2 h)^\nu \psi(\lambda_2 h) + \ldots + (f,\lambda_2 h^{f-1})^\nu \psi(\lambda_2 h^{f-1}) \\ + \cdot \\ + (f,\lambda_e)^\nu \psi(\lambda_e) + (f,\lambda_e h)^\nu \psi(\lambda_e h) + \ldots + (f,\lambda_e h^{f-1})^\nu \psi(\lambda_e h^{f-1}) \end{array} \right\}$$

Der Ausdruck t_ν ist, wie aus dieser Form hervorgeht, bekannt.

Setzt man $\nu = 0, 1, 2, 3, \ldots e-1$, und bezeichnet man der Kürze halber $(f,\lambda_1), (f,\lambda_2), \ldots (f,\lambda_e)$ mit $y_1, y_2, \ldots y_e$; so hat man folgende Gleichungen:

$$\begin{aligned} \psi(\lambda_1) + \psi(\lambda_2) + \ldots + \psi(\lambda_e) &= t_0 \\ y_1\psi(\lambda_1) + y_2\psi(\lambda_2) + \ldots + y_e\psi(\lambda_e) &= t_1 \\ \\ y_1^{e-1}\psi(\lambda_1) + y_2^{e-1}\psi(\lambda_2) + \ldots + y_e^{e-1}\psi(\lambda_e) &= t_{e-1}. \end{aligned}$$

Multiplicirt man diese Gleichungen resp. mit $P_0, P_1, \ldots P_{e-2}, 1$ und addirt man, so wird:

$$\psi(\lambda_1) = \frac{t_0 P_0 + t_1 P_1 + t \ldots + t_{e-2} P_{e-2} + t_{e-1}}{P_0 + y_1 P_1 + \quad + y_1^{e-2} P_{e-2} + y_1^{e-1}},$$

wo die Eliminationsfactoren $P_0, P_1, \ldots P_{e-2}$ durch die Entwicklung von

$$Y = (y-y_2)(y-y_3)\ldots(y-y_e) = y^{e-1} + P_{e-2}y^{e-2} + \ldots + P_1 y + P_0$$

erhalten werden. Diese Eliminationsfactoren lassen sich durch y_1 ausdrücken. Multiplicirt man Y mit $y-y_1$, so wird:

$$\begin{aligned} Y(y-y_1) = y^e + (P_{e-2} - y_1)y^{e-1} + (P_{e-3} - P_{e-2}y_1)y^{e-2} + \ldots \\ + (P_0 - P_1 y_1)y - P_0 y_1 = (y-y_1)(y-y_2)\ldots(y-y_e). \end{aligned}$$

Da diese Gleichung identisch ist mit der Gleichung zur Bestimmung von $y_1, y_2, \ldots y_e$, so sind also die Coëfficienten

$$P_{e-2} - y_1, \; P_{e-3} - P_{e-2}y_1, \ldots - P_0 y_1,$$

durch die Coëfficienten der Gleichung $X = 0$ gegeben.

Der Nenner in $\psi(\lambda_1)$ ist auch darstellbar durch:

$$(y_1-y_2)(y_1-y_3)\,..\,(y_1-y_e)=Y_1\,,$$

wegen der Verschiedenheit von $y_1, y_2, .. y_e$ kann er nie Null werden.

Setzt man in $A'_1, A''_1, .. A^{(f)}_1$ statt y_1, die Werthe $y_2, y_3, ... y_e$; so erhält man die übrigen Gleichungen vom Grade f.

Ist $n-1=abc$, so setze man $e=a$, $f=bc$. Man erhält dadurch a-Gleichungen vom Grade bc. Da die Wurzeln einer Periode von bc-Gliedern sich in b-Perioden von c-Gliedern zerfällen lassen, so läßt sich jede dieser Gleichungen vom Grade bc in b-Gleichungen vom Grade c zerlegen.

Ist $n-1=2^\alpha.3^\beta.5^\gamma...$, so reducirt sich die Auflösung von $X=0$, auf die Auflösung von α-Gleichungen vom Grade 2, β-Gleichungen vom Grade 3, γ-Gleichungen vom Grade 5, u. s. w.

Ist $n-1=2^\alpha$, so hat man α quadratische Gleichungen aufzulösen.

Damit in diesem Falle n eine Primzahl ist, muß α die Form 2^ν haben; denn wäre $\alpha=\zeta\eta$, wo ζ ungerade ist, so wäre $2^{\zeta\eta}+1=(2^\eta)^\zeta+1$ durch $2^\eta+1$ theilbar.

Für $\nu=0, 1, 2, 3, 4, ..$ erhält man $\alpha=1, 2, 4, 8, 16, ..$, $n=3, 5, 17, 257, 65537, ...$

Setzt man in $r=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$ die Zahl $k=1$, so liefert der reelle Theil einer Wurzel den Ausdruck für $\cos\frac{2\pi}{n}$.

Da der Ausdruck in dem zuletzt erwähnten Falle nur Quadratwurzeln enthält, so kann er geometrisch construirt werden. Es ist daher die Construction aller regulären Polygone, deren Seitenzahl eine Primzahl von der Form $2^\alpha+1$ ist, möglich.

Beispiel I. $\quad n=7\,,\quad x^7=1.$

$$n-1=6,\ e=3\,,\ f=2\,,\ g=3.$$

Die Periode (6, 1) zerfällt in

$$(2, 1)=y_1,\ (2, 3)=y_2,\ (2, 2)=y_3,$$

$$y_1+y_2+y_3=-1\,,\ y_1^2+y_2^2+y_3^2=5\,,\ y_1^3+y_2^3+y_3^3=-4.$$

$$y^3+y^2-2y-1=0$$

$y_1 = -0\cdot 44503$ y_1 enthält die Wurzeln [1], [6]

$y_2 = -1\cdot 80193$ y_2 [3], [4]

$y_2 = +1\cdot 24697$ y_3 [2], [5]

Gleichung für x

$$x^2-yx+1=0$$

$x_1 = -0\cdot 2225+0\cdot 9749\,i$, $x_4 = -0\cdot 9010-0\cdot 4339\,i$

$x_2 = -0\cdot 2225-0\cdot 9749\,i$, $x_5 = +0\cdot 6235+0\cdot 7818\,i$

$x_3 = -0\cdot 9010+0\cdot 4339\,i$, $x_6 = +0\cdot 6235-0\cdot 7818\,i$

Aus der Natur der geometrischen Functionen ist klar, daß die Wurzeln $x_1, x_2 \ldots x_6$ den Bogen

$$\frac{2\pi}{7}.2\,,\quad \frac{2\pi}{7}.5\,,\quad \frac{2\pi}{7}.3\,,\quad \frac{2\pi}{7}.4\,,\quad \frac{2\pi}{7}\,,\quad \frac{2\pi}{7}.6$$

entsprechen.

Beispiel II. $n=17$ $x^{17}=1.$

$g=3.$

$\theta = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. 10, 11, 12, 13, 14, 15$

$g^\theta \equiv 1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6 \pmod{17}$

Die Periode (16, 1) zerfällt in die Perioden (8, 1), (8, 3) $e=2$

(8, 1) (4, 1), (4, 9)

(8, 3) (4, 3), (4, 10)

(4, 1) (2, 1), (2, 13)

u. s. w. Dabei ist der numerische Werth von:

$$(16, 1) = -1$$

$(8, 1)+(8, 3) = (16, 1)$ $(8, 1)(8, 3) = -4$

$(4, 1)+(4, 9) = (8, 1)$ $(4, 1)(4, 9) = -1$

$(4, 3)+(4, 10) = (8, 3)$ $(4, 3)(4, 10) = -1$

$(2, 1)+(2, 13) = (4, 1)$ $(2, 1)(2, 13) = (4, 3)$

$(2, 9)+(2, 15) = (4, 9)$ $(2, 9)(2, 15) = (4, 10)$

$(2. 3)+(2, 5) = (4, 3)$ $(2, 3)(2, 5) = (4, 9)$

$(2, 10)+(2, 11) = (4, 10)$ $(2, 10)(2, 11) = (4, 1).$

Die Periode (2, 1) besteht aus den Wurzeln [1] und [16]; (2, 13) besteht aus [13] und [4], u. s. w.

Versteht man unter [1] die bestimmte Wurzel

$$\cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17},$$

so ist

$$(2, 1) = 2\cos\frac{2\pi}{17}$$

Setzt man Kürze halber

$$\frac{2\pi}{17} = \omega,$$

so ist

$$(4, 1) = 4\cos\frac{5\omega}{2}\cos\frac{3\omega}{2},\quad (4, 9) = 4\cos 5\omega\cos 3\omega$$

$$(4, 3) = 4\cos 4\omega\cos\omega,\quad (4, 10) = 4\cos\frac{13\omega}{2}\cos\frac{\omega}{2}$$

(4, 1) und (4, 3) sind positiv, (4, 9) und (4, 10) negativ.

Wegen

$$\cos 5\omega = -\cos(\pi - 5\omega) = -\cos\frac{7\pi}{17}$$

$$\cos\frac{13\omega}{2} = -\cos\left(\pi - \frac{13\omega}{2}\right) = -\cos\frac{4\pi}{17},$$

ist

$$(8, 1) = 4\cos\frac{3\pi}{17}\cos\frac{5\pi}{17} - 4\cos\frac{6\pi}{17}\cos\frac{7\pi}{17}$$

positiv,

$$(8, 3) = 4\cos\frac{2\pi}{17}\cos\frac{8\pi}{17} - 4\cos\frac{\pi}{17}\cos\frac{4\pi}{17}$$

negativ.

Es ist daher

$$(8, 1) = -\tfrac{1}{2} + \sqrt{17},\quad (8, 3) = -\tfrac{1}{2} - \tfrac{1}{2}\sqrt{17}$$

$$(4. 1) = -\tfrac{1}{4} + \tfrac{1}{4}\sqrt{17} + \tfrac{1}{4}\sqrt{34 - 2\sqrt{17}}$$

$$(4, 3) = -\tfrac{1}{4} - \tfrac{1}{4}\sqrt{17} + \tfrac{1}{4}\sqrt{34 + 2\sqrt{17}}$$

$$(2, 1) = -\tfrac{1}{8} + \tfrac{1}{8}\sqrt{17} + \tfrac{1}{8}\sqrt{34 - 2\sqrt{17}}$$

$$+\tfrac{1}{4}\sqrt{\left\{17 + 3\sqrt{17} - 4\sqrt{34 + 2\sqrt{17}} + \tfrac{1}{3}\sqrt{34 - 2\sqrt{17}}(\sqrt{17} - 1) = R\right\}}$$

$$R = 17+3\sqrt{17}-2\sqrt{34+2\sqrt{17}}$$
$$-\tfrac{1}{2}\left\{4\sqrt{34+2\sqrt{17}}-\sqrt{34-2\sqrt{17}}(\sqrt{17}-1)=X\right\}$$

Setzt man

$$4=\sqrt{\sqrt{17}-1}\quad\sqrt{\sqrt{17}+1}\,,$$

so wird

$$X=2\sqrt{2\sqrt{17}}\quad\sqrt{\sqrt{17}-1}=2\sqrt{34-2\sqrt{17}}$$

$$\cos\frac{2\pi}{17}=-\tfrac{1}{16}+\tfrac{1}{16}\sqrt{17}+\tfrac{1}{16}\sqrt{34-2\sqrt{17}}$$
$$+\tfrac{1}{8}\sqrt{17+3\sqrt{17}-2\sqrt{34+2\sqrt{17}}-\sqrt{34-2\sqrt{17}}}\,.$$

II. Beitrag zur Theorie der Pell'schen Gleichung.

Unter der Pell'schen Gleichung versteht man bekanntlich die unbestimmte Gleichung

$$t^2-u^2D=\sigma^2,$$

wo t und u unbestimmte ganze Zahlen bedeuten. Die Auflösung dieser, in der Theorie der quadratischen Formen (auf welchen Fall wir uns hier beschränken) so wichtigen Gleichung geschieht nach Gauß (disquis. arithm. art. 197 sgg.) für positive Werthe der Determinante D dadurch, daß man sämmtliche Transformationen einer reducirten Form von der Determinante D in sich selbst bestimmt. Bestimmt man nämlich zu einer reducirten Form fortwährend die nach rechts und links benachbarten reducirten Formen, so bilden alle diese Formen eine Periode von einer geraden Anzahl einander verschiedener Formen. Durch die Transformation einer Form durch die Glieder einer einzigen Periode hindurch in sich selbst, erhält man die sogenannte kleinste Auflösung T und U der Pell'schen Gleichung.

Je nach der Verschiedenheit der reducirten Form, welche als Ausgangspunkt gewählt wird, erhält man die Werthe T und U auf verschiedenem Wege; es hat allerdings keine Schwierigkeit indirect die Identität aller dieser Auflösungen nachzuweisen; wegen der Wichtigkeit dieser Gleichung dürfte ein directer Beweis für die Unabhängigkeit der kleinsten Auflösung der Pell'schen Gleichung von dem Ausgangspunkte der reducirten Formen nicht ohne Interesse sein.

Es seien $\varphi_0 = (a, b, c)$ und $\varphi_1 = (a', b', c')$ zwei benachbarte reducirte Formen, φ_1 der Form φ_0 nach rechts benachbart, ω_0 und ω_1 ihre ersten Wurzeln; so ist nach der Bezeichnung von Gauß

$$\pm\omega_0 = (k_0, k_1, k_2, \ldots\ldots k_{2nh-1}, \pm\omega_0)\,,$$

$$\mp\omega_1 = (k_1, k_2, k_3, \ \ldots k_{2nh-1}, k_0, \mp\omega_1)\,;$$

oder

$$\pm\omega_0 = \frac{[k_0, k_1, k_2, \ldots k_{2nh-1}, \pm\omega_0]}{[k_1, k_2, \ldots\ \ldots k_{2nh-1}, \pm\omega_0]}\,,$$

oder

$$\pm\omega_0 = \frac{[k_0, k_1, \ldots k_{2nh-2}] + [k_0, k_1, \ldots k_{2nh-1}] . \pm\omega_0}{[k_1, k_2, \ldots k_{2nh-2}] + [k_1, k_2 \ldots k_{2nh-1}] . \pm\omega_0}\,;$$

also

$$\omega_0 = \frac{\pm[k_0, k_1, \ldots k_{2nh-2}] + [k_0, k_1, \ldots k_{2nh-1}]\omega_0}{[k_1, k_2, \ldots k_{2nh-2}] \pm [k_1, k_2, \ldots k_{2nh-1}]\omega_0}$$

Eben so ist

$$\omega_1 = \frac{\mp[k_1, k_2, \ldots k_{2nh-1}] + [k_1, k_2, \ldots k_{2nh-1}, k_0]\omega_1}{[k_2, k_3, \ldots k_{2nh-1}] \mp [k_2, k_3, \ldots k_{2nh-1}, k_0]\omega_1}\,,$$

wo h jede beliebige positive Zahl bedeutet.

Ist $\begin{pmatrix}\alpha_0, \beta_0\\ \gamma_0, \delta_0\end{pmatrix}$ eine Substitution, wodurch φ_0 in φ_0 übergeht, $\begin{pmatrix}\alpha_1, \beta_1\\ \gamma_1, \delta_1\end{pmatrix}$ eine Substitution, wodurch φ_1 in φ_1 übergeht; so ist

$$\alpha_0 = \ [k_1, k_2, \ldots k_{2nh-2}]\,,\quad \beta_0 = \pm[k_1, k_2, \ldots k_{2nh-1}]$$

$$\gamma_0 = \pm[k_0, k_1 \ldots k_{2nh-2}]\,,\quad \delta_0 = \ [k_0, k_1, \ldots k_{2nh-1}]$$

$$\alpha_1 = \ [k_2, k_3, \ldots k_{2nh-1}]\,,\quad \beta_1 = \mp[k_2, k_3, \ldots k_{2nh-1}, k_0]$$

$$\gamma_1 = \mp[k_1, k_2, \ldots k_{2nh-1}]\,,\quad \delta_1 = \ [k_1, k_2, \ldots k_{2nh-1}, k_0].$$

Aus der Substitution $\begin{pmatrix}\alpha_0, \beta_0\\ \gamma_0, \delta_0\end{pmatrix}$ erhält man nach den Formeln

$$\alpha_0 = \frac{t_0 - bu_0}{\sigma}\,,\quad \beta_0 = -\frac{cu_0}{\sigma}\,,\quad \gamma_0 = \frac{au_0}{\sigma}\,,\quad \delta_0 = \frac{t + bu_0}{\sigma}$$

eine Auflösung t_0, u_0 der Pell'schen Gleichung.

Ebenso erhält man durch die Transformation $\begin{pmatrix} \alpha_1, & \beta_1 \\ \gamma_1, & \delta_1 \end{pmatrix}$ eine Auflösung t_1, u_1 der Pell'schen Gleichung nach den Formeln:

$$\alpha_1 = \frac{t_1 - b'u_1}{\sigma}, \quad \beta_1 = -\frac{c'u_1}{\sigma}, \quad \gamma_1 = \frac{a'u_1}{\sigma}, \quad \delta_1 = \frac{t_1 + b'u_1}{\sigma}.$$

Aus der Übereinstimmung der Vorzeichen der ersten Wurzel und des ersten Coëfficienten einer reducirten Form überzeugt man sich leicht, daß die Auflösungen t_0, u_0 und $t_1\ u_1$ positive Auflösungen der Pell'schen Gleichung sind.

Bedeutet h für beide Formen dieselbe Zahl, so ist wegen

$$\gamma_1 = -\beta_0$$
$$c = a',$$

auch

$$u_1 = \frac{\sigma\gamma_1}{a'} = -\frac{\sigma\beta_0}{c} = u_0,$$
$$t_1 = \sqrt{\sigma^2 + Du_1^2} = \sqrt{\sigma^2 + Du_0^2} = t_0,$$

d. h. je zwei gleichvielte Transformationen zweier benachbarter reducirter Formen führen zu derselben Auflösung der Pell'schen Gleichung. Daraus folgt, daß auch die kleinsten positiven Auflösungen, welche durch zwei benachbarte reducirte Formen erhalten werden, identisch sind.

Sind nun $\varphi_0, \varphi_1, \varphi_2 \ldots \varphi_{2n-1}$ die $2n$ reducirten Formen einer Periode, so liefern φ_0 und φ_1, φ_1 und $\varphi_2, \ldots \varphi_{2n-2}$ und φ_{2n-} resp. dieselbe kleinste Auflösung der Pell'schen Gleichung, woraus unmittelbar die Identität aller dieser Auflösungen erhellt.

Anmerkung. Daß $u_0 = u_1$, $t_0 = t_1$ ist, läßt sich auch auf folgende Art beweisen. Es ist

$$t_0 = \frac{\sigma}{2}(\alpha_0 + \delta_0),$$

$$t_1 = \frac{\sigma}{2}(\alpha_1 + \delta_1)$$

Nun ist

$$\alpha_1 + \delta_1 = [k_2, k_3, \ldots k_{2n-2}, k_{2n-1}] + [k_1, k_2, \ldots k_{2n-1}, k_0],$$

wo der Einfachheit halber $h = 1$ gesetzt wurde.

Aus

$$[k_1, k_2, \ldots h_{2n-1}, k_0] = [k_1, k_2, \ldots k_{2n-2}] + [k_1, k_2, \ldots k_{2n-1}]k_0$$

folgt

$$\alpha_1 + \delta_1 = [k_2, k_3, \ldots k_{3n-1}] + \alpha_0 + [k_1, k_2, \ldots k_{2n-1}]k_0.$$

Wegen

$$[k_0, k_1, k_2, \ldots k_{2n-1}] = [k_2, k_3, \ldots k_{2n-1}] + [k_1, k_2, \ldots k_{2n-1}]k_0$$

$$\alpha_1 + \delta_1 = \alpha_0 + [k_0, k_1, k_2, \ldots k_{2n-1}]$$

$$= \alpha_0 + \delta_0 \; ;$$

also

$$t_1 = t_0.$$

Aus dieser Gleichung folgt wieder, wegen

$$t^2 - u^2 D = \sigma^2 ,$$

daß $u_1 = u_0$ ist.